Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

J.192

(11/2005)

SERIE J: REDES DE CABLE Y TRANSMISIÓN DE PROGRAMAS RADIOFÓNICOS Y TELEVISIVOS, Y DE OTRAS SEÑALES MULTIMEDIA

Módems de cable

Pasarela residencial para soportar la entrega de servicios de datos por cable

Recomendación UIT-T J.192

UIT-T

Unión Internacional de Telecomunicaciones

Recomendación UIT-T J.192

Pasarela residencial para soportar la entrega de servicios de datos por cable

Resumen

La presente Recomendación describe una pasarela residencial al proponer un conjunto de características basadas en IP que podrán añadirse a un módem de cable o incorporarse en un dispositivo autónomo. Este conjunto permitirá que los operadores de cable ofrezcan a sus clientes un conjunto adicional de servicios ampliado basados en la red doméstica, que incluye gestión de la calidad de servicio (QoS), determinación del dispositivo y el servicio, seguridad mejorada, gestión de la barrera contra fuegos, características de gestión y configuración centradas en la red doméstica, traducción de la dirección de la red gestionada, direccionamiento y tratamiento mejorados de paquetes y diagnósticos de los dispositivos de la red LAN. Esta Recomendación se fundamenta en las referencias arquitectónicas conformes con la Rec. UIT-T J.190.

Esta Recomendación representa una mejora a la Rec. UIT-T J.191, y conserva como fundamento la mayor parte de su funcionalidad, basándose en la misma para ofrecer características avanzadas adicionales. Un objetivo de diseño esencial de los equipos que respondan a esta Recomendación es la interoperabilidad con los que sean conformes con la Rec. UIT-T J.191. Por ejemplo, se emplean bases de información de gestión (MIB) para la funcionalidad fundamental. Por consiguiente, una cabecera de red basada en J.192 podrá gestionar una instalación mixta basada en J.191 y J.192.

Orígenes

La Recomendación UIT-T J.192 fue aprobada el 29 de noviembre de 2005 por la Comisión de Estudio 9 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

PREFACIO

La UIT (Unión Internacional de Telecomunicaciones) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

Recomendación UIT-T J.192

Pasarela residencial para soportar la entrega de servicios de datos por cable

1 Alcance

La presente Recomendación describe una pasarela residencial al proponer un conjunto de características basadas en IP que podrán añadirse a un módem de cable o incorporarse en un dispositivo autónomo. Este conjunto permitirá que los operadores de cable ofrezcan a sus clientes un conjunto adicional de servicios ampliado basados en la red doméstica, que incluye la gestión de la calidad de servicio (QoS, *quality of service*), la determinación del dispositivo y el servicio, una seguridad mejorada, la gestión de la barrera contra fuegos, características de gestión y provisión centradas en la red doméstica, la traducción de la dirección de la red gestionada, un direccionamiento y tratamiento mejorados de paquetes y diagnósticos de los dispositivos de la red LAN. Esta Recomendación se fundamenta en las referencias arquitectónicas conformes con la Rec. UIT-T J.190.

Esta Recomendación representa una mejora a la Rec. UIT-T J.191, y conserva como fundamento la mayor parte de su funcionalidad, basándose en la misma para ofrecer características avanzadas adicionales. Un objetivo de diseño esencial de los equipos que respondan a esta Recomendación es la interoperabilidad con los que sean conformes con la Rec. UIT-T J.191. Por ejemplo, se emplean bases de información de gestión (MIB, *management information base*) para la funcionalidad fundamental. Por consiguiente, una cabecera basada en J.192 podrá gestionar una instalación mixta basada en J.191 y J.192.

La funcionalidad esencial, adicional a la de la Rec. UIT-T J.191, que se define en esta Recomendación incluye:

- determinación del dispositivo y el servicio para aplicaciones y servicios en la LAN;
- manejo de traducción de la dirección de red (NAT, *network address translation*) para clientes de la RPV con IPSec y para los servidores locales;
- lenguaje e informes de configuración normalizados de la barrera contra fuegos;
- funcionalidad de la barrera contra fuegos básica normalizada;
- control paternal simple;
- calidad de servicio para la red LAN, que se gestiona en la pasarela residencial.

El texto no normativo que hace referencia a la funcionalidad UPnP se incluye en esta Recomendación como ejemplo de implementaciones de calidad de servicio (QoS) y gestión de la red doméstica y se escribe entre corchetes y marcados tal como se indica a continuación: " {texto informativo: … }". Todos los textos incluidos entre ese tipo de corchetes no tienen carácter normativo.

2 Referencias

2.1 Referencias (normativas)

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de

las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

– Recomendación UIT-T J.112 Anexo B (2004), *Especificaciones de interfaces de servicios de datos por cable: Especificación de la interfaz de radiofrecuencia*.

– Recomendación UIT-T J.125 (2004), *Privacidad de enlace para la implementación de módems de cable*.

– Recomendación UIT-T J.126 (2004), *Especificación de dispositivos módems de cable incorporados*.

– Recomendación UIT-T J.161 (2001), *Requisitos de los códecs de audio para la prestación de servicios de audio bidireccionales por redes de televisión por cable que utilizan módems de cable*.

– Recomendación UIT-T J.162 (2005), *Protocolo de señalización de llamada de red para la prestación de servicios dependientes del tiempo por redes de televisión por cable que utilizan módems de cable*.

– Recomendación UIT-T J.163 (2005), *Calidad de servicio dinámica para la prestación de servicios en tiempo real por las redes de televisión por cable que utilizan módems de cable*.

– Recomendación UIT-T J.164 (2005), *Requisitos de los mensajes de evento para el soporte de servicio en tiempo real transmitidos mediante redes de televisión por cable que utilizan módems de cable*.

– Recomendación UIT-T J.167 (2005), *Requisitos del aprovisionamiento de un dispositivo adaptador de terminal de medios para la entrega de servicios en tiempo real por redes de televisión por cable que utilizan módems de cable*.

– Recomendación UIT-T J.170 (2005), *Especificación de la seguridad de IPCablecom*.

– Recomendación UIT-T J.175 (2005), *Protocolo de servidor de audio*.

– Recomendación UIT-T J.178 (2005), *Señalización entre servidores de gestión de llamadas IPCablecom*.

– Recomendación UIT-T J.191 (2004), *Lote de características basadas en el protocolo Internet para mejorar los módems de cable*.

– Recomendación UIT-T X.690 (2002) | ISO/CEI 8825-1:2002, *Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de las reglas de codificación básica, de las reglas de codificación canónica y de las reglas de codificación distinguida*.

– Recomendación UIT-T X.509 (2005) | ISO/CEI 9594-8:2005, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos.*

– ANSI/SCTE 22-1-2002, *DOCSIS 1.0, Radio Frequency Interface*.

– ANSI/SCTE 23-3-2005, *DOCSIS 1.1 Part 3: Operations Support System Interface*.

– FIPS 140-2 (2001), *Security Requirements for Cryptographic Modules*, Department of Commerce, NIST.

– FIPS 180-1 (1995), *Secure Hash Algorithm*, Department of Commerce, NIST.

– IANAifType MIB Definitions, http://www.iana.org/assignments/ianaiftype-mib.

– IEEE 802.11-1999-MIB-D6.2, *IEEE 802.11 Management Information Base.*

– IEEE 802.11A-1999, *IEEE Standard for Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: High Speed Physical Layer in the 5 GHz Band, Annex D.*

– IEEE 802.11B/Cor1-2001, *Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 2: Higher Speed Physical Layer (PHY) Extension in the 2.4 GHz band, Corrigendum 1, Annex D.*

– IEEE 802.11D, *IEEE Standard for IT. Telecommunications and information exchange between systems – LAN/MAN Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 3: Specification for operation in additional regulatory domains, Annex D.*

– IEEE 802.11G-2003, *IEEE Standard for IT. Telecommunications and information exchange between systems – LAN/MAN Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, Annex D.*

– ISO/IEC 8802-2 (ANSI/IEEE Std 802.2):1998, *Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 2: Logical link control.*

– ISO/IEC 10038 (ANSI/IEEE Std 802.1D):1993, *Information technology – Telecommunications and information exchange between systems – Local area networks – Media access control (MAC) bridges.*

– IETF RFC 347 (1972), *Echo Process*.

– IETF RFC 768 (1980), *User Datagram Protocol (UDP)*.

– IETF RFC 791 (MIL STD 1777) (1981), *DARPA Internet Program, Protocol Specification. Internet Protocol.*

– IETF RFC 792 (1981), *DARPA Internet Program, Protocol Specification. Internet Control Message Protocol (ICMP)*.

– IETF RFC 793 (1981), *DARPA Internet Program, Protocol Specification. Transmission Control Protocol*.

– IETF RFC 868 (1983), *Time Protocol*.

– IETF RFC 919 (1984), *Broadcasting Internet Datagrams*.

– IETF RFC 922 (1984), *Broadcasting Internet datagrams in the presence of subnets*.

– IETF RFC 1034 (1987), *Domain Names – Concepts and Facilities*.

– IETF RFC 1035 (1987), *Domain Names – Implementation and Specification*.

– IETF RFC 1122 (1989), *Requirements for Internet Hosts – Communication Layers*.

– IETF RFC 1123 (1989), *Requirements for Internet Hosts – Application and Support*.

– IETF RFC 1157 (1990), *A Simple Network Management Protocol (SNMP)*.

– IETF RFC 1213 (1991), *Management Information Base for Network Management of TCP/IP-based Internets MIB-II.*

– IETF RFC 1350 (1992), *The TFTP Protocol (Revision 2)*.

– IETF RFC 1510 (1993), *The Kerberos Network Authentication Service (V5).*

– IETF RFC 1812 (1995), *Requirements for IP Version 4 Routers*.

– IETF RFC 1889 (1996), *RTP: A Transport Protocol for Real-Time Applications*.

– IETF RFC 1901 (1996), *Introduction to Community-based SNMPv2*.

– IETF RFC 2011 (1996), *SNMPv2 Management Information Base for the Internet Protocol using SMIv2*.

– IETF RFC 2013 (1996), *SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2*.

– IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*.

– IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol*.

– IETF RFC 2132 (1997), *DHCP Options and BOOTP Vendor Extensions*.

– IETF RFC 2236 (1997), *Internet Group Management Protocol, Version 2*.

– IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

– IETF RFC 2315 (1998), *PKCS #7*, *Cryptographic Message Syntax*, Version 1.5.

– IETF RFC 2349 (1998), *TFTP Timeout Interval and Transfer Size Options*.

– IETF RFC 2401 (1998), *Security Architecture for the Internet Protocol*.

– IETF RFC 2402 (1998), *IP Authentication Header*.

– IETF RFC 2406 (1998), *IP Encapsulating Security Payload (ESP).*

– IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*.

– IETF RFC 2474 (1998), *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*.

– IETF RFC 2578 (1999), *Structure of Management Information Version 2 (SMIv2)*.

– IETF RFC 2579 (1999), *Textual Conventions for SMIv2*.

– IETF RFC 2580 (1999), *Conformance Statements for SMIv2*.

– IETF RFC 2616 (1999), *Hypertext Transfer Protocol – HTTP/1.1*.

– IETF RFC 2663 (1999), *IP Network Address Translator (NAT) Terminology and Considerations*.

– IETF RFC 2669 (1999), *DOCSIS Cable Device MIB – Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems*.

– IETF RFC 2670 (1999), *Radio Frequency (RF) Interface Management Information Base for MCNS/DOCSIS compliant RF interfaces*.

– IETF RFC 2786 (2000), *Diffie-Hellman USM Key Management Information Base and Textual Convention*.

– IETF RFC 2863 (2000), *The Interfaces Group MIB*.

– IETF RFC 3022 (2001), *Traditional IP Network Address Translator (Traditional NAT).*

– IETF RFC 3046 (2001), *DHCP Relay Agent Information Option*.

– IETF RFC 3280 (2002), *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

– IETF RFC 3291 (2002), *Textual Conventions for Internet Network Addresses*.

– IETF RFC 3396 (2002), *Encoding Long Options in the Dynamic Host Configuration Protocol (DHCPv4)*.

– IETF RFC 3410 (2002), *Introduction and Applicability Statements for Internet-Standard Management Framework*.

– IETF RFC 3411 (2002), *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*.

– IETF RFC 3412 (2002), *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*.

– IETF RFC 3413 (2002), *Simple Network Management Protocol (SNMP) Applications*.

– IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

– IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*.

– IETF RFC 3416 (2002), *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*.

– IETF RFC 3417 (2002), *Transport Mappings for the Simple Network Management Protocol (SNMP)*.

– IETF RFC 3418 (2002), *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*.

– IETF RFC 3584 (2003), *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*.

– W3C Working Draft, World Wide Web Consortium (W3C), *Simple Object Access Protocol (SOAP) Version 1.2*, 19 de diciembre de 2002, http://www.w3.org/2000/xp/Group/#drafts.

– W3C Working Draft, World Wide Web Consortium (W3C) *XML Protocol (XMLP) Requirements*, 26 de junio de 2002, http://www.w3.org/TR/2002/WD-xmlp-reqs-20020626.

2.2 Referencias (informativas)

– IANA Port Numbers, http://www.iana.org/assignments/port-numbers.

– IETF RFC 2644 (1999), *Changing the Default for Directed Broadcasts in Routers*.

– IETF RFC 3164 (2001), *The BSD Syslog Protocol*.

– IETF RFC 3235 (2002), *Network Address Translator (NAT)-Friendly Application Design Guidelines*.

– IETF RFC 3435 (2003), *Media Gateway Control Protocol (MGCP) Version 1.0*.

– [draft-ietf-ipcdn-bpiplus-mib-05]

DOCSIS Baseline Privacy Plus MIB – Management Information Base for DOCSIS Cable Modems and Cable MÓdem Termination Systems for Baseline Privacy Plus, IETF Internet Draft, http://www.watersprings.org/pub/id/draft-ietf-ipcdn-bpiplus-mib-05.txt.

– Federal Information Processing Standards Publications (FIPS PUB) 186 (1994), *Digital Signature Standard (DSS)*.

– Fenner W., *et al., IGMP-based Multicast Forwarding ("IGMP Proxying")*, IETF Internet Draft, http://www.ietf.org/internet-drafts/draft-ietf-magma-igmp-proxy-01.txt.

– RSA Laboratories (1999), *PKCS #1, v2.0: RSA Cryptography Standard.*

– SCTE 22-3-2002, *DOCSIS 1.0 Part 3: Operations Support System Interface*.

– UDA 1.0 UPnP™ Device Architecture, Version 1.0, 8 de junio de 2000 http://www.upnp.org/download/UPnPDA10_20000613.htm.

– UQA UPnP™ QoS Architecture 1.0, 10 de marzo de 2005, http://www.upnp.org.

– UQD UPnP™ QosDevice 1.0 Service Definition Document, 10 de marzo de 2005.

– UQM UPnP™ QosManager 1.0 Service Definition Document, 10 de marzo de 2005.

– UQPH UPnP™ QosPolicyHolder 1.0 Service Definition Document, 10 de marzo de 2005.

– UIGD, InternetGatewayDevice:1, Device Template Version 1.01 for Universal Plug and Play Version 1.0, 12 de noviembre de 2001, http://www.upnp.org.

– UWIC WANIPConnection:1 Service Template Version 1.01 For UPnP™ Version 1.0, 12 de noviembre de 2001, http://www.upnp.org.

3 Definiciones

En esta Recomendación se definen los términos siguientes.

3.1 portal de seguridad de IPCable2Home (CSP, *IPCable2Home security portal*): Elemento funcional que facilita funciones de gestión de seguridad y de traducción entre el sistema híbrido de fibra coaxial (HFC) y la red doméstica.

3.2 PS integrado: Elemento de servicios de portal que no emplea una interfaz autónoma para conectarse a un módem de cable (CM).

3.3 dispositivo de acceso en la vivienda (HA, *home access*): Grupo de elementos lógicos que se utiliza para lograr el acceso mediante HFC a las redes de IPCable2Home, que se denomina pasarela residencial en esta Recomendación.

3.4 dispositivo de cliente en la vivienda (HC, *home client*): Grupo de elementos lógicos que se utiliza para aportar funcionalidad a las aplicaciones de cliente, denominado anfitrión de IPCable2Home en esta Recomendación.

3.5 dispositivo IP de la red LAN: Representa un dispositivo IP normal que habrá de residir en las redes domésticas y que se prevé que incluirá una pila de protocolos TCP/IP así como un cliente DHCP.

3.6 servicios de portal (PS, *portal services*): Elemento funcional que ofrece funciones de gestión y traducción entre el sistema HFC y la red doméstica.

3.7 PS autónomo: Elemento de servicios de portal que se conecta al módem de cable empleando únicamente una interfaz autónoma.

4 Abreviaturas y Convenios

4.1 Abreviaturas, siglas o acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas, siglas o acrónimos.

A/V Audio/vídeo (*audio/video*)

ALG Pasarela de capa de aplicación (*application layer gateway*)

APP Aplicación (*application*)

ASP Apoderado específico de aplicación (*application specific proxy*)

BP Punto de frontera (*boundary point*)

BPSC	Configuración de servicios de portal en bloque (*bulk portal services configuration*)
CA	Autoridad de certificación (*certification authority*)
CAP	Portal de direcciones de IPCable2Home (*IPCable2Home address portal*)
CAT	Traducción de dirección de IPCable2Home (*IPCable2Home address translation*)
CDC	Cliente DHCP de IPCable2Home (*IPCable2Home DHCP client*)
CDP	Portal DHCP de IPCable2Home (*IPCable2Home DHCP portal*)
CDS	Servidor DHCP de IPCable2Home (*IPCable2Home DHCP server*)
CM	Módem de cable (*cable módem*)
CMP	Portal de gestión de IPCable2Home (*IPCable2Home management portal*)
CMS	Servidor de gestión de llamadas (*call management server*)
CMTS	Sistema de terminación de módem de cable (*cable módem termination system*)
C-NAPT	Traducción de dirección y puerto de la red IPCable2Home (*IPCable2Home network address and port translation*)
C-NAT	Traducción de dirección de la red IPCable2Home (*IPCable2Home network address translation*)
CNP	Portal de denominación de IPCable2Home (*IPCable2Home naming portal*)
CPU	Unidad central de procesamiento (*central processing unit*)
CQoS	Calidad de servicio de IPCable2Home (*IPCable2Home quality of service*)
CQP	Portal de QoS de IPCable2Home (*IPCable2Home QoS portal*)
CRG	Pasarela residencial de IPCable2Home (*IPCable2Home residential gateway*)
CRL	Lista de revocación de certificados (*certificate revocation list*)
CSP	Portal de seguridad de IPCable2Home (*IPCable2Home security portal*)
CTL	Laboratorio de prueba de certificación (*certification testing laboratory*)
CTP	Portal de prueba de IPCable2Home (*IPCable2Home test portal*)
CVC	Certificado de verificación de código (*code verification certificate*)
CVS	Signatura de verificación de código (*code verification signature*)
CxP	Subfunción de servicios de portal de IPCable2Home (*IPCable2Home portal services sub-function*)
CH	Anfitrión de IPCable2Home (*IPCable2Home host*)
DER	Reglas de codificación distinguidas (*distinguished encoding rules*)
DHCP	Protocolo dinámico de configuración de anfitrión (*dynamic host configuration protocol*)
DNS	Servidor de nombres de dominio (*domain name server*)
DOCSIS	Especificación de interfaz del servicio de datos por cable (*data-over-cable service interface specification*)
DoS	Denegación de servicio (*denial of service*)
DQoS	Calidad de servicio dinámica (*PacketCable*) (*dynamic quality-of-service*)

E-MTA	Adaptador de terminal multimedia integrado (*embedded multimedia terminal adapter*)
FTP	Protocolo de transferencia de ficheros (*file transfer protocol*)
FW	Barrera contra fuegos (*firewall*)
GMT	Tiempo medio de Greenwich (*Greenwich mean time*)
HA	Acceso a la vivienda (*home access*)
HE	Extremo de cabecera (*headend*)
HEX	Hexadecimal (*hexadecimal*)
HFC	Híbrido fibra coaxial (*hybrid fiber coax*)
ICMP	Protocolo de mensajes de control Internet (*Internet control message protocol*)
IETF	Grupo de tareas especiales de ingeniería en Internet (*Internet Engineering Task Force*)
IGMP	Protocolo de gestión del grupo Internet (*Internet group management protocol*)
IP	Protocolo Internet (*Internet protocol*)
IPCDN	Red de datos de IP por cable – Grupo de tareas del IETF (*IP over cable data network – a working group of the IETF*)
IPF	Filtro de paquetes entrantes (*inbound packet filter*)
IPSec	Seguridad del protocolo Internet (*Internet protocol security*)
KDC	Centro de distribución de claves (*key distribution centre*)
LAN	Red de área local (*local area network*)
LAN-Pass	Dirección de transferencia de la red de área local (*passthrough local area network address*)
LAN-Trans	Dirección traducida de la red de área local (*translated local area network address*)
MAC	Control de acceso a medios (*media access control*)
MBP	Punto de frontera de gestión (*management boundary point*)
MCF	Función de cliente de gestión (*management client function*)
MGCP	Protocolo de control de pasarela de medios (*media gateway control protocol*)
MIB	Base de información de gestión (*management information base*)
MPLS	Conmutación por etiquetas multiprotocolo (*multiprotocol label switching*)
MSF	Función de servidor de gestión (*management server function*)
MTA	Adaptador de terminal multimedia (*multimedia terminal adapter*)
NAPT	Traducción de dirección y portal de red (*network address and portal translation*)
NAT	Traducción de dirección de red (*network address translation*)
NCS	Señalización de llamada basada en la red (*network-based call signalling*)
NMS	Sistema de gestión de red (*network management system*)
NS	Servidor de nombres oficial (*authoritative name server*)
OID	Identificador de objeto (*object identifier*)
OPF	Filtro de paquetes salientes (*outbound packet filter*)

OSI	Interconexión de sistemas abiertos (*open systems interconnection*)
OSS	Sistema de soporte de operaciones (*operations support system*)
PDU	Unidad de datos de protocolo (*protocol data unit*)
PF	Filtro de paquetes (*packet filteri*)
PING	Buscador de paquetes entre redes (*packet inter-network grouper*)
PKI	Infraestructura de claves públicas (*public key infrastructure*)
PKINIT	Autenticación inicial mediante criptografía de clave pública (*public-key cryptography for initial authentication*)
PS	Servicios de portal (*portal services*)
PS WAN-Data	Interfaz de datos entre el elemento de servicios de portal de IPCable2Home y la red de área extensa (*IPCable2Home portal services element WAN data interface*)
PS WAN-Man	Interfaz de gestión entre el elemento de servicios de portal de IPCable2Home y la red de área extensa (*IPCable2Home portal services element WAN management interface*)
QBP	Punto de frontera de calidad de servicio (*quality of service boundary point*)
QCC	Cliente de características de calidad de servicio (*quality of service characteristics client*)
QCS	Servidor de características de calidad de servicio (*quality of service characteristics server*)
QFM	Retransmisión y acceso a los medios con calidad de servicio (*quality of service forwarding and media access*)
QoS	Calidad de servicio (*quality of service*)
RAM	Memoria de acceso aleatorio (*random access memory*)
RDN	Nombre distinguido relativo (*relative distinguished name*)
RFC	Petición de comentarios (*request for comments*)
RG	Pasarela residencial (*residential gateway*)
ROM	Memoria de sólo lectura (*read only memory*)
RSA	Rivest, Shamir, Adleman (véase el glosario)
RSVP	Protocolo de reserva de recursos (*resource reservation protocol*)
RTCP	Protocolo de control en tiempo real (*real-time control protocol*)
RTP	Protocolo de transporte en tiempo real (*real-time transport protocol*)
SDP	Protocolo de descripción de sesión (*session description protocol*)
SHA-1	Algoritmo de traceo seguro 1 (*secure hash algorithm 1*)
S-MTA	Adaptador de terminal de multimedia autónomo (*standalone multimedia terminal adapter*)
SNMP	Protocolo simple de gestión de red (*simple network management protocol*)
SoA	Comienzo de autoridad (*start of authority*)
SPF	Filtrado dinámico de paquetes (*stateful packet filtering*)
SYSLOG	Registro de sistema (*system log*)

TCP	Protocolo de control de transmisión (*transmission control protocol*)
TFTP	Protocolo de transferencia de ficheros trivial (*trivial file transfer protocol*)
TLS	Seguridad de capa de transporte (*transport layer security*)
TLV	Tipo-longitud-valor (*type-length-value*)
ToD	Hora del día (*time of day*)
UDP	Protocolo de datagrama de usuario (*user datagram protocol*)
URL	Localizador de recurso uniforme (*uniform resource locator*)
USFS	Conmutador de retransmisión selectiva en sentido ascendente (*upstream selective forwarding switch*)
USM	Modelo de seguridad de usuario (*user security model*)
UTC	Tiempo universal coordinado (*coordinated universal time*)
VACM	Modelo de control de acceso basado en vistas (*view-based access control model*)
VoIP	Voz sobre el protocolo Internet (*voice over Internet protocol*)
WAN	Red de área extensa (*wide area network*)
WAN-Data	Sector de direcciones de datos de la red de área extensa (*wide area network data address realm*)
WAN-Man	Sector de direcciones de gestión de la red de área extensa (*wide area network management address realm*)

4.2 Convenios

En esta Recomendación se escriben con mayúsculas las palabras que se emplean para destacar la importancia de algunos requisitos particulares. Estas palabras son:

"DEBE(N)"	Esta palabra o el adjetivo "REQUERIDO" significan que el elemento es un requisito absoluto de la presente Recomendación.
"NO DEBE(N)"	Esta frase significa que el elemento constituye una prohibición absoluta en la presente Recomendación.
"DEBERÍA(N)"	Esta palabra o el adjetivo "RECOMENDADO" significa que, en determinadas circunstancias, puede haber motivos justificados para ignorar este elemento, aunque deben tenerse en cuenta todas las repercusiones, estudiando detenidamente todas y cada una de las circunstancias antes de optar por una alternativa diferente.
"NO DEBERÍA(N)"	Esta expresión significa que, en determinadas circunstancias, puede haber razones por las que la actuación consignada resulte aceptable e incluso útil, debiendo considerarse todas las repercusiones y estudiando cuidadosamente todas las circunstancias antes de emprender las acciones descritas en este epígrafe.
"PUEDE(N)"	Esta palabra y el adjetivo "OPCIONAL(ES)" indican que este elemento es opcional. Por ejemplo, un fabricante puede optar por incorporar este elemento por exigencias de un mercado determinado o porque aporta mejoras significativas al producto, mientras que otro fabricante puede optar por suprimir dicho elemento.

5 Arquitectura de referencia

El objetivo del sistema IPCable2Home es facilitar la distribución de nuevos servicios del sistema de cable a los dispositivos instalados en la vivienda, complementando las infraestructuras de CableMÓdem y de IPCablecom, y permitiendo la distribución de sus servicios. En particular, el sistema IPCable2Home proporciona una infraestructura, mediante la especificación de un entorno de conexión en red doméstica, por la que se pueden distribuir, gestionar y soportar servicios de IPCablecom y de otras aplicaciones conexas.

La presente Recomendación permite la evolución de una pasarela residencial (CRG) interoperable. El propósito es la creación de un entorno centralizado en una pasarela residencial que puede ser configurada por un operador de cable y que podrá interactuar significativamente con dispositivos en la vivienda basados en IP (dispositivos IP de la red LAN). Esto permite al operador de cable poder controlar la gestión, configuración, calidad de servicio y seguridad asociadas a la pasarela residencial. Además, se especifican la mensajería de determinación, la QoS con prioridades y los diagnósticos simples a distancia de los dispositivos en la vivienda. {texto informativo: también se especifica la calidad de servicio de la mensajería necesaria para la distribución de la política a aplicaciones que funcionan en anfitriones conformes con la QoS UPnP.} A continuación se presenta un resumen de las capacidades incluidas en esta Recomendación:

Gestión, determinación y configuración

- gestión y configuración a distancia del dispositivo pasarela residencial;
- apoderado simple de diagnósticos de la pasarela residencial para los dispositivos en la vivienda basados en IP;
- configuración automática de los dispositivos pasarela residencial;
- determinación de los dispositivos en la vivienda basados en IP y sus aplicaciones correspondientes;
- gestión de la pasarela residencial a partir de la red LAN.

Direccionamiento y tratamiento de paquetes

- traducción de direcciones de una a varias, para los dispositivos en la vivienda;
- traducción de direcciones una a una, para los dispositivos en la vivienda;
- direccionamiento sin traducción para los dispositivos en la vivienda (en el caso de aplicaciones que no aceptan la traducción de direcciones);
- protección del tráfico HFC contra las comunicaciones entre los dispositivos en la vivienda;
- manejo de direccionamiento doméstico durante interrupciones del sistema HFC;
- servidor DNS simple en la pasarela residencial;
- soporte de NAT para los clientes de RPV con IPsec;
- soporte de NAT para los servidores IP en la vivienda que emplean traducción de direcciones;
- Configuración de cliente de NAT.

Calidad de servicio (QoS)

- funcionalidad de puenteo transparente de la pasarela residencial para los mensajes de QoS de IPCablecom de/a aplicaciones conformes con IPCablecom;
- capacidad para asignar prioridades al tráfico (acceso a medios diferenciados) para aplicaciones específicas;
- capacidad para asignar prioridades a las colas en la pasarela residencial junto con la funcionalidad de tratamiento de paquetes;

- {texto informativo: proporciona servicios de gestor de QoS UPnP y tenedor de política (PolicyHolder) para anfitriones UPnP.}

Seguridad

- autenticación de la pasarela residencial;
- mensajes de gestión segura entre la red de datos por cable y la pasarela residencial;
- descarga segura de ficheros de configuración y de software;
- seguridad facultativa de los ficheros de configuración;
- gestión a distancia de la barrera contra fuegos de la pasarela residencial;
- configuración e informes normalizados de la barrera contra fuegos;
- control paternal simple.

En el resto de esta cláusula se examina la arquitectura de referencia de IPCable2Home bajo seis perspectivas distintas:

- lógica (cláusula 5.1);
- funcional (cláusula 5.2);
- de interfaz de mensajería (cláusula 5.3);
- de información (cláusula 5.4);
- operacional (cláusula 5.5);
- de interfaz física (cláusula 5.6).

5.1 Arquitectura de referencia lógica

En esta cláusula se introducen los conceptos de los elementos lógicos de IPCable2Home y los dispositivos IPCable2Home, tal como se ilustra en la figura 5-1.

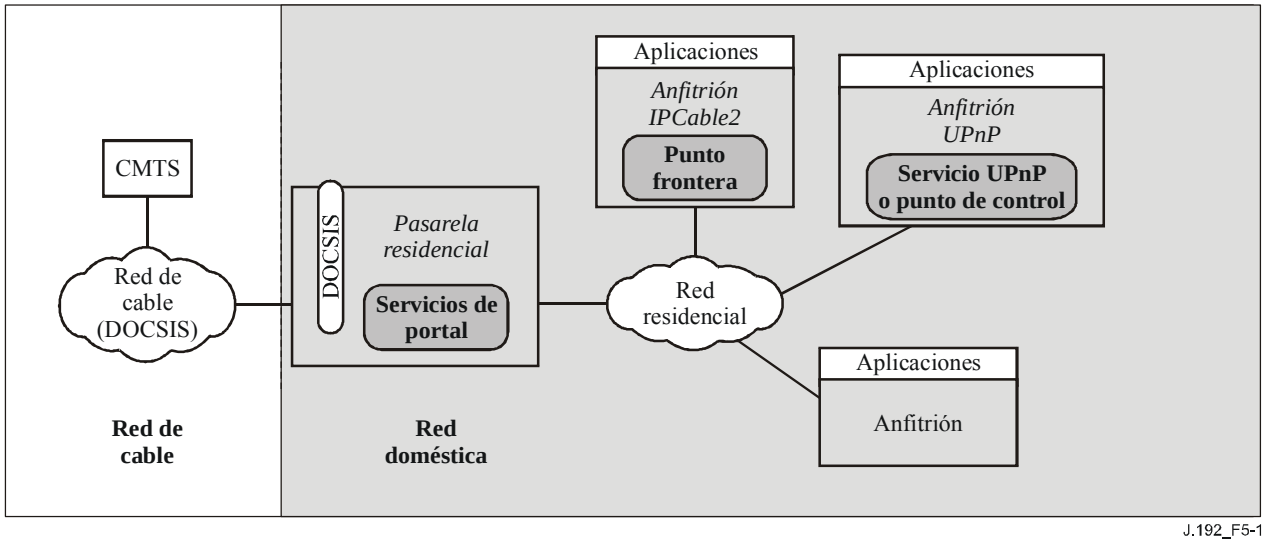


Figura 5-1/J.192 – Conceptos lógicos esenciales de IPCable2Home

5.1.1 Dispositivos de IPCable2Home

En la arquitectura de IPCable2Home se identifican los dispositivos para asignar un contexto tangible a los elementos lógicos que se describen en 5.1.2. Las definiciones de los dispositivos son una manera informativa de ilustrar la topología de la red doméstica y de los elementos lógicos que se ubican en la misma red, pero que no se consideran definitivos o restrictivos. Los dispositivos de IPCable2Home incluyen la pasarela residencial y el anfitrión de IPCable2Home.

La pasarela residencial (HA en la Rec. UIT-T J.190) representa la ubicación física del elemento lógico de servicios de portal (PS, *portal services*), que se describe en 5.1.2.1. Consta de una sola interfaz WAN, un solo elemento lógico PS y puede tener una o varias interfaces LAN.

El término dispositivo IP de LAN se refiere a cualquier anfitrión LAN que implemente una pila IPv4, incluyendo un cliente DHCP. Un dispositivo de este tipo que implemente la funcionalidad de IPCable2Home, se denomina *dispositivo anfitrión de IPCable2Home* (HC en la Rec. UIT-T J.190). {texto informativo: Un dispositivo IP de LAN que implemente la funcionalidad UPnP, se denomina dispositivo anfitrión UPnP. Un dispositivo IP de LAN sin funcionalidad de IPCable2Home ni funcionalidad UPnP se denomina anfitrión.}

El dispositivo anfitrión de IPCable2Home representa la ubicación física del punto de frontera (BP, *boundary point*). El BP se define en 5.1.2.3 y permite el interfuncionamiento de anfitriones y pasarelas residenciales IPCable2Home. El anfitrión de IPCable2Home sólo tiene una interfaz LAN.

{texto informativo: El dispositivo anfitrión UPnP representa la ubicación física de los servicios UPnP o la funcionalidad de punto de control. El anfitrión UPnP interactúa con la pasarela residencial CableHome utilizando la determinación UPnP y los mensajes de QoS UPnP para comunicar los atributos de su dispositivo y establecer una QoS en la LAN doméstica.}

IPCable2Home hace la hipótesis de que existe una topología de conexión en red doméstica con un solo módem de cable (CM, *cable módem*) DOCSIS y una pasarela residencial de IPCable2Home en la LAN doméstica. Se supone que el CM DOCSIS es la única conexión directa al enlace HFC. De manera ideal, la pasarela residencial de IPCable2Home se conectará directamente al CM sin ningún otro dispositivo entre ellos, de modo que la pasarela residencial proporcione la protección especificada a la red doméstica. Todos los anfitriones de la LAN se conectan a la red LAN que se encuentra detrás de la pasarela residencial de IPCable2Home.

5.1.2 Elementos lógicos

El marco arquitectónico introduce el concepto de elementos lógicos. Los elementos lógicos de IPCable2Home son entidades funcionales delimitadas lógicamente que pueden emitir y responder a mensajes específicos. Estos elementos funcionan en la capa del protocolo IP y por encima de la misma, permaneciendo por consiguiente independientes de cualquier tecnología de red física. Además, tienen la capacidad de recopilar y comunicar información según proceda para determinar, gestionar y distribuir servicios por las redes de IPCable2Home. IPCable2Home define una entidad lógica específica para cada dispositivo de IPCable2Home: la entidad lógica del PS encapsula la funcionalidad de IPCable2Home definida para las pasarelas residenciales, y la entidad lógica del BP encapsula la funcionalidad definida para los anfitriones de IPCable2Home (véase en 5.1.1 una descripción de los dispositivos de IPCable2Home).

5.1.2.1 Servicios de portal (PS)

Se trata de un elemento lógico de un dispositivo pasarela residencial que ofrece servicios de seguridad, gestión, configuración, direccionamiento y calidad de servicio locales y agregados. El término "portal" indica los servicios que establecen la interfaz entre las redes WAN y LAN. En esta cláusula se describen las características del elemento lógico de servicios de portal.

5.1.2.1.1 PS autónomo y PS con módem de cable integrado

Las dos componentes principales posibles en una pasarela residencial, el módem de cable (CM) y el elemento de servicios de portal (PS), pueden utilizar recursos de hardware y software compartidos o independientes. Este uso compartido de recursos entre CM y el PS permite distinguir entre PS autónomo y PS integrado.

Un PS autónomo NO DEBE compartir componentes de hardware o software con un CM. La separación del CM del PS autónomo DEBE ser vista por el PS como una simple desconexión de su red WAN, es decir, el PS seguirá estando plenamente funcional como si estuviera desconectado de

la red WAN. De lo contrario, el PS se considerará integrado. Con estas definiciones, es posible que el PS pueda residir en el mismo recinto físico que un CM, y aún poder considerarse como un PS autónomo.

El CM y el PS se consideran elementos independientes en los casos autónomo e integrado, y responden a direcciones de gestión únicas. En el caso integrado, el CM y el PS comparten componentes de hardware o de software, pero desde el punto de vista de la gestión, se trata de entidades independientes.

En la figura 5-2 se ilustran los PS autónomo e integrado. En ambos casos, se considera que la combinación de un CM y un PS es lo que constituye el concepto de dispositivo HA.

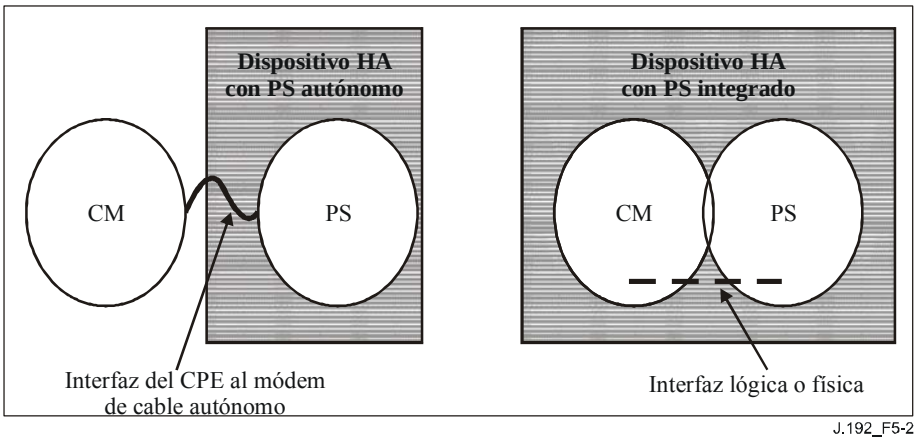


Figura 5-2/J.192 – PS autónomo y PS con CM integrado

5.1.2.2 {texto informativo: Servicio y puntos de control UPnP

Un anfitrión UPnP encapsula la funcionalidad lógica UPnP tales como servicios o puntos de control UPnP. Siendo el PS una entidad lógica especificada por CableHome, interactúa con elementos lógicos de la LAN que no están especificados por CableHome. El PS proporciona servicios limitados a todos los dispositivos IP de la LAN, así como servicios adicionales para interaccionar con los servicios y puntos de control UPnP. La arquitectura CableHome utiliza mensajes conformes con UPnP entre el PS y los servicios y puntos de control UPnP de la LAN. En la arquitectura UPnP [UDA 1.0], los mensajes de control se inician desde el punto de control UPnP, a lo que responden los servicios UPnP.}

5.1.2.3 Punto de frontera *(*BP*)*

Un punto frontera (BP) es un elemento lógico que encapsula toda la funcionalidad de IPCable2Home definida para un anfitrión de IPCable2Home en la LAN doméstica.

5.1.3 Sectores de direcciones

Un sector de direcciones se define como "el dominio de la red en el que las direcciones de red se asignan unívocamente a entidades susceptibles de recibir datagramas dirigidos a ellas" [RFC 2663]. En la presente Recomendación, los sectores de direcciones se clasifican en sector de direcciones de la WAN y sector de direcciones de la LAN (véase la figura 5-3).

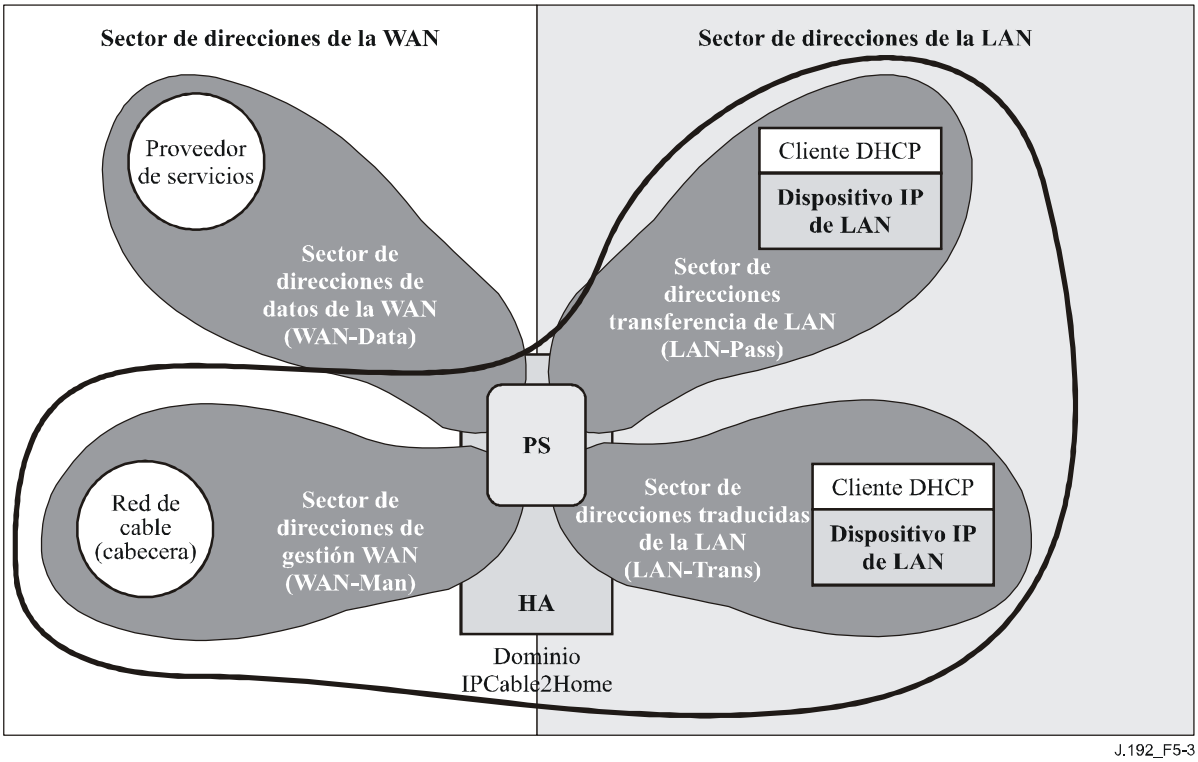


Figura 5-3/J.192 – Sectores de direcciones de IPCable2Home

Las direcciones de la WAN pertenecen a uno de los dos siguientes sectores: el sector de direcciones de gestión de la WAN (WAN-Man) o el sector de direcciones de datos de la WAN (WAN-Data). Las direcciones de la LAN pertenecen asimismo a uno de los siguientes sectores: el sector de direcciones transferencia de la LAN (LAN-Pass, *passthrough LAN address*) o el sector de direcciones traducidas de la LAN (LAN-Trans). Las propiedades de estos sectores de direccionamientos son las siguientes:

- El sector de direcciones de gestión de la WAN (WAN-Man, *WAN management address realm*) tiene por objeto transportar por la red de cable el tráfico de gestión de la red entre el sistema de gestión de la red y el elemento PS. Las direcciones de este sector suelen pertenecer al espacio privado de direcciones IP.
- El sector de direcciones de datos de la WAN (WAN-Data, *WAN data address realm*) tiene por objeto transportar el tráfico de la aplicación del abonado por la red de cable y más allá de ésta, como por ejemplo, el tráfico entre los dispositivos IP de la LAN y anfitriones de Internet. Las direcciones de este sector suelen pertenecer al espacio público de direcciones IP.
- El sector de direcciones traducidas de la LAN (LAN-Trans) tiene por objeto transportar tráfico de la aplicación del abonado y de gestión por la red doméstica entre dispositivos IP de LAN y el elemento PS. Las direcciones de este sector suelen pertenecer al espacio de direcciones IP privadas, y es normal que las reutilicen distintos abonados.
- El sector de direcciones transferencia de la LAN (LAN-Pass) tiene por objeto transportar tráfico de la aplicación del abonado, como por ejemplo el tráfico entre dispositivos IP de LAN y anfitriones de Internet, por la red doméstica, la red de cable e incluso fuera de éstos. Las direcciones de este sector suelen pertenecer al espacio público de direcciones IP.

En el lado de la LAN, las direcciones del sector de direcciones transferencia de la LAN (LAN-Pass) se extraen directamente de las direcciones del sector de direcciones de datos de la WAN. Éstas son utilizadas por los dispositivos IP de LAN y por aplicaciones tales como los servicios IPCablecom

que no soportan la traducción de direcciones y necesitan una dirección IP direccionable mundialmente. Además, en el lado de la LAN, a los dispositivos IP de LAN se les pueden asignar direcciones traducidas del sector de direcciones traducidas de la LAN (LAN-Trans).

A las interfaces LAN físicas en el PS se les asigna un índice de acuerdo con la MIB grupo de interfaces [RFC 2863], tal como se describe en 6.3.3.1.4.8, MIB de grupo de interfaces. En la misma cláusula se define para el PS una interfaz LAN virtual que permite agregar las interfaces LAN físicas. Igualmente, en la misma cláusula también se define para el PS una interfaz LAN virtual que permite agregar sólo las interfaces LAN radioeléctricas físicas. La dirección IP correspondiente al lado LAN que se definió para el PS se "vincula" a la interfaz virtual formada por "todas" las interfaces LAN físicas. Las funciones de DHCP y de servidor de nombres de dominio del PS, y la función de encaminador del PS, son aplicaciones que se implementan en el PS direccionado, utilizando la dirección IP del lado LAN vinculada a la interfaz LAN virtual formada por "todas" las interfaces LAN físicas.

5.2 Modelo de referencia funcional de IPCable2Home

Las funciones de IPCable2Home son servicios basados en IP definidos en esta Recomendación que se han de implementar mediante el PS o la red de datos del operador del cable, y aceptan la distribución de servicios basados en el sistema de cable. Estas funciones se definen para cada uno de los ámbitos de especificación principales: configuración, gestión, seguridad y calidad de servicio.

Los subelementos representan agrupaciones de funcionalidad conexa en el PS. El elemento lógico PS puede incluir múltiples subelementos y, a su vez, estos subelementos pueden contener subgrupos de funciones (es decir, subelementos dentro de subelementos).

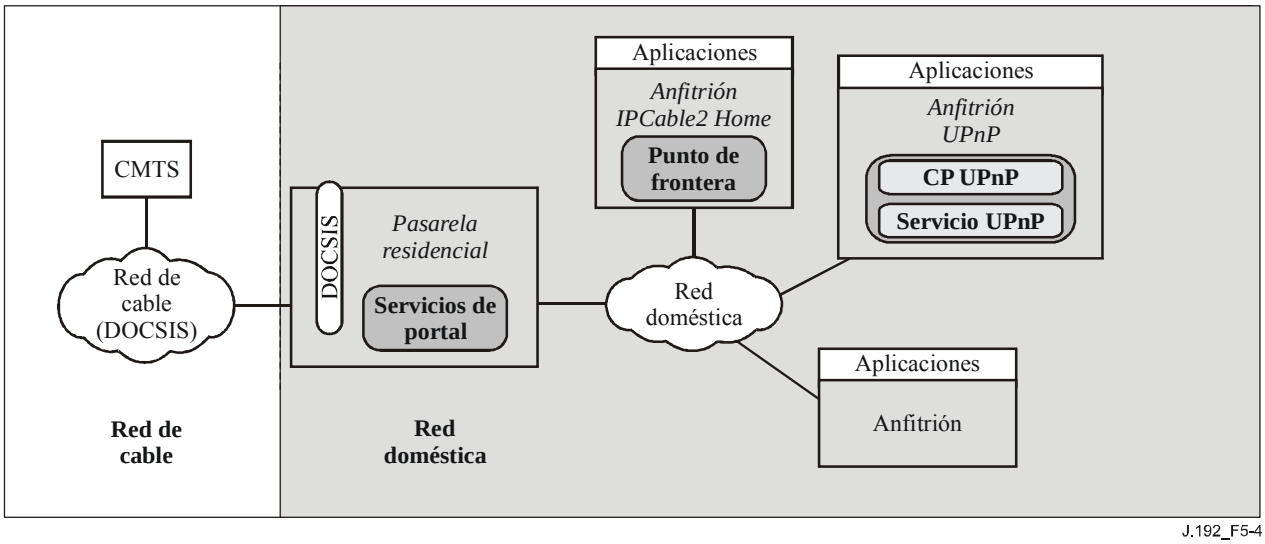


Figura 5-4/J.192 – Subelementos de IPCable2Home

El PS incluye varios subelementos, que se describen más adelante.

5.2.1 {texto informativo: Relación entre CableHome y UPnP}

La arquitectura IPCable2Home utiliza mensajes conformes con UPnP para gestionar e interaccionar con dispositivos anfitriones UPnP. Por lo tanto, la funcionalidad de algunos subelementos PS se describe en términos de puntos de control UPnP y servicios UPnP. Por ejemplo, el PS incluye la funcionalidad servicio IGD WANIpConnection UPnP [UWIC] para permitir la configuración de la funcionalidad traducción de dirección IPCable2Home (CAT, *IPCable2Home Address Translation*)

desde los anfitriones UPnP. Igualmente, el PS utiliza la funcionalidad punto de control UPnP para determinar los servicios y dispositivos UPnP presentes en la red doméstica. (Véase la figura 5-5.)

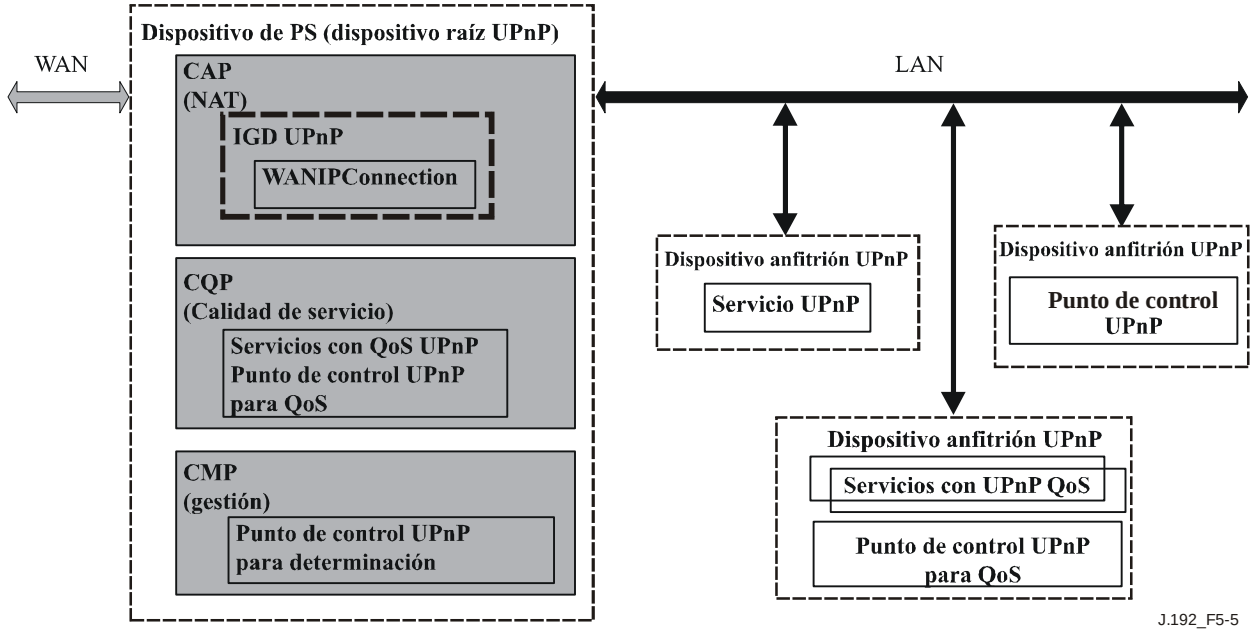


Figura 5-5/J.192 – Jerarquía de dispositivos y servicios UPnP del servicio de portal IPCable2Home}

5.2.2 Funciones de gestión y configuración de IPCable2Home

Para soportar los requisitos durante la configuración y gestión de los anfitriones en la red doméstica, IPCable2Home utiliza funciones correspondientes que residen en la red de datos por cable, y define funciones para el PS. Las funciones de gestión y configuración basadas en la red de cable incluyen diversos servicios utilizados por los procesos de gestión y configuración definidos para IPCable2Home. Las funciones de gestión y configuración de los servicios de portal se ubican en la pasarela residencial e incluyen funcionalidad de tipo servidor, tipo cliente y de otros tipos. En los cuadros 5-1 y 5-2 se muestran ejemplos de funciones de la red de cable y del PS, y las mismas se ilustran en la figura 5-6.

Cuadro 5-1/J.192 – Funciones de gestión de la red de cable

Funciones	Descripción
Servidor DHCP de la red de cable	Es un componente de la red de cable que aporta al PS información de direcciones de los sectores de direcciones WAN-Man y WAN-Data
Servidores de gestión de la red de cable	Servidores de mensajería de gestión, descarga y notificación de eventos de IPCable2Home que incluyen protocolos como SNMP, SYSLOG, y TFTP [RFC 2349]
Servidor de hora del día de la red de cable	El servidor de hora del día (ToD, *time of day*) proporciona a los clientes la hora del día actual.

Cuadro 5-2/J.192 – Funciones de gestión y configuración del PS

Funciones del portal de gestión	Descripción
Portal de direcciones de IPCable2Home (CAP)	El CAP, en el PS, interconecta los sectores de direcciones de las redes WAN y LAN para el tráfico de datos. Véase CAT/transferencia) {texto informativo: también proporciona la interfaz del servicio WANIpConnection IGD UPnP para puntos de control UPnP a fin de configurar el cuadro de traducción de direcciones IPCable2Home (CAT).}
Traducción de direcciones de IPCable2Home (CAT)	Se trata de una subfunción del CAP que traduce direcciones de red IP pública del lado WAN-Data del CAP a direcciones de red IP privada en una subred lógica simple del lado LAN-Trans.
Transferencia	Se trata de una subfunción del CAP que puentea paquetes del lado WAN-Data del CAP al lado LAN-Pass sin introducir modificaciones.
Portal de gestión de IPCable2Home (CMP)	Función que proporciona interfaces entre el operador y la base de datos del PS {texto informativo: también determina varios anfitriones UPnP y servicios UPnP ofrecidos por ellos utilizando el proceso de determinación UPnP.}
Portal DHCP de IPCable2Home (CDP)	Funciones de información de dirección (por ejemplo, las que se transmiten mediante DHCP) incluyendo un servidor para el sector LAN y un cliente para los sectores WAN.
Portal de denominación de IPCable2Home (CNP)	Ofrece un servicio DNS simple a los dispositivos IP de LAN que necesitan servicios de denominación.
Portal de prueba de IPCable2Home (CTP)	Ofrece medios a distancia para iniciar mensajes PING y bucles en la red LAN.
Servidor HTTP	Se trata del protocolo de transporte utilizado para transportar mensajes SOAP (protocolo simple de acceso a objetos) por la red LAN. El PS incluye un servidor HTTP que proporciona datos cuando recibe peticiones del BP.
Analizadores sintácticos XML y SOAP	Se utilizan para efectos de mensajería en la red LAN. El PS incluye ambos analizadores sintácticos.

Para la comunicación con las funciones de gestión del PS anteriormente enumeradas (véase el cuadro 5-3) en los dispositivos IP de LAN pueden existir las funciones siguientes, aunque no sean exigibles de forma obligada por esta Recomendación.

Cuadro 5-3/J.192 – Posibles funciones de gestión y configuración de dispositivos IP de LAN

Funciones de cliente de gestión	Descripción
Cliente DHCP del dispositivo IP de LAN	La función del cliente DHCP de IPCable2Home es un componente en la vivienda que se emplea durante el proceso de configuración del dispositivo IP de LAN para que pueda solicitar de manera dinámica direcciones IP.
{texto informativo: Punto de control o servicios UPnP}	{texto informativo: UPnP es el protocolo utilizado para transportar mensajes de gestión y determinación en la LAN.}

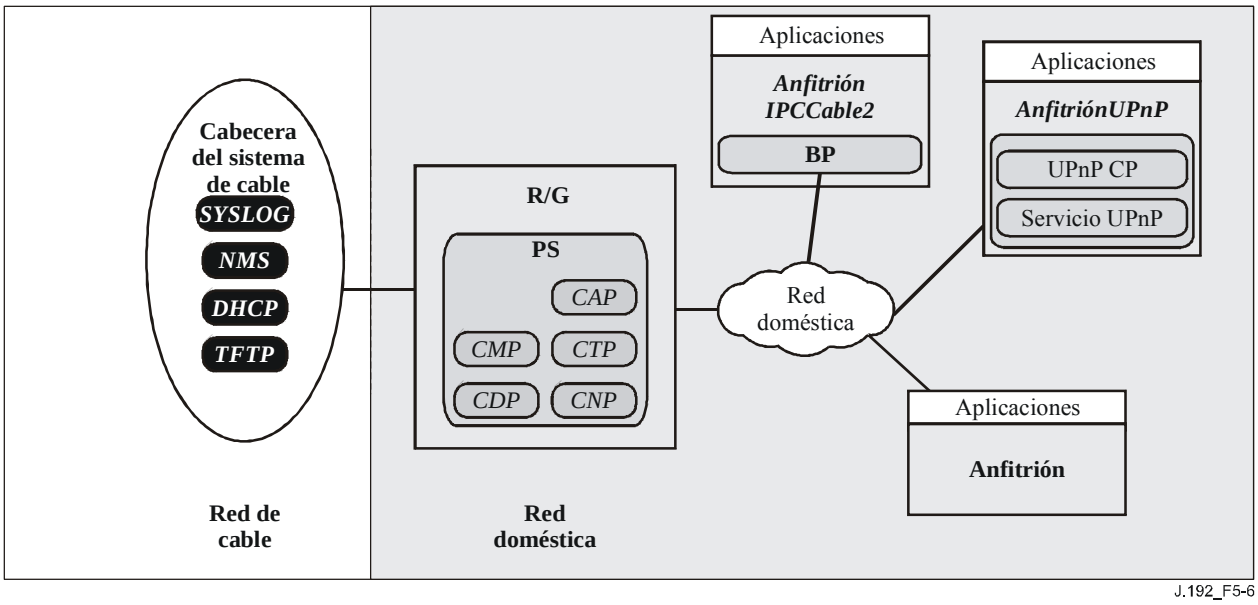


Figura 5-6/J.192 – Elementos de gestión de IPCable2Home

5.2.3 Funciones de seguridad de IPCable2Home

A modo de soporte de los requisitos de seguridad de IPCable2Home (véase 11.2.1), IPCable2Home emplea funciones de seguridad que residen en la red de datos por cable, y define funciones para el PS. Las funciones de seguridad de la red de cable incluyen servidores para la distribución, criptación y autenticación de claves. Las funciones de seguridad de los servicios de portal se ubican en la pasarela residencial e incluyen funciones de cliente y otras. En los cuadros 5-4 y 5-5 se presentan ejemplos de funciones de seguridad basadas en la red de cable y del PS que se ilustran en la figura 5-7.

Cuadro 5-4/J.192 – Funciones de seguridad de los servicios de portal

Funciones de seguridad de los servicios de portal	Descripción
Portal de seguridad de IPCable2Home (CSP)	El CSP se comunica con los servidores de seguridad de la cabecera e incluye funciones que facilitan la participación del lado cliente en los procesos de autenticación, intercambio de claves y gestión de certificados. Otras funciones de seguridad incluyen procesos de seguridad de los mensajes de gestión, participación en la descarga segura y gestión a distancia de la barrera contra fuegos.
Barrera contra fuegos (FW)	Proporciona la funcionalidad que permite proteger la red doméstica contra ataques malintencionados.

Cuadro 5-5/J.192 – Función de seguridad de la red de cable

Funciones de seguridad de la red de cable	Descripción
Servidores del centro de distribución de claves (KDC)	Proporcionan servicios de seguridad al CSP e incluyen funciones que intervienen en los procesos de autenticación e intercambio de claves.

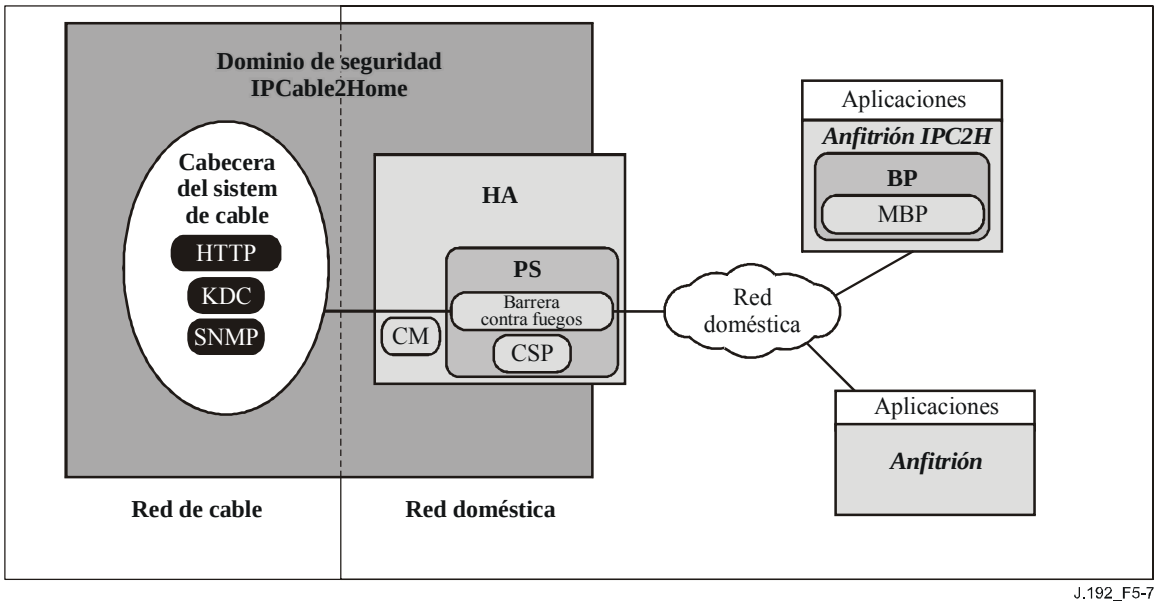


Figura 5-7/J.192 – Elementos de seguridad de IPCable2Home

5.2.4 Funciones de calidad de servicio de IPCable2Home

Para soportar los requisitos de calidad de servicio (véase 10.2.1), IPCable2Home determina funciones para el PS y el BP. Las funciones de QoS del BP se ubican en los anfitriones de IPCable2Home e incluyen una función cliente y funciones de otros tipos. En los cuadros 5-6 y 5-7 se presentan ejemplos de las funciones de QoS del PS y del BP y se ilustran en la figura 5-8.

Cuadro 5-6/J.192 – Funciones de QoS de los servicios de portal

Funciones de QoS del servicio de portal	Descripción
Servidor de política de QoS (QPS)	Esta funcionalidad mantiene un repositorio de política de QoS para varios dispositivos y aplicaciones en la red doméstica, y comunica la política de QoS {texto informativo: cuando lo solicita la entidad gestora (QoSManager) de QoS UPnP.}
Acceso a retransmisión y medios con QoS (QFM)	La QFM es responsable de priorizar el encolamiento y la retransmisión de paquetes así como del acceso al medio compartido priorizado en el PS.
{texto informativo: interfaz del servicio de dispositivos con QoS UPnP (QD)}	1) Esta interfaz de servicio hace que el PS CableHome negocie la QoS de la red de acceso utilizando la interfaz CH-PCMM para flujos de tráfico en la red de acceso y la red doméstica. 2) La interfaz recibe peticiones del clasificador de tráfico {texto informativo: de las entidades QoSManager UPnP y las coloca en la base de datos del PS.}Estos clasificadores son utilizados por la funcionalidad QFM para la clasificación de paquetes.
Servicio gestor de QoS (QM)	{texto informativo: un servicio gestor de QoS UPnP en el PS garantiza que existe al menos un servicio gestor de QoS UPnP para puntos de control UPnP para solicitar QoS en la LAN doméstica.}
Funcionalidad de QoS del punto de control del PS	Esta entidad actúa como un punto de control para diversos servicios de QoS {texto informativo: UPnP} en la LAN doméstica. La lógica de la determinación de QoS de este punto de control es responsable de recopilar información relacionada con la QoS de los diversos servicios con QoS {texto informativo: UPnP} de la LAN doméstica y de almacenarlos en la base de datos PS. La entidad también captura anuncios de QoS {texto informativo: UPnP}, eventos y genera acciones necesarias para los diversos servicios con QoS {texto informativo: UPnP.}

Para la comunicación con las funciones de gestión del PS anteriormente enumeradas (véase el cuadro 5-7) es habitual que en los dispositivos IP de LAN existan las funciones siguientes, aunque esta Recomendación no las exija de forma obligatoria.

Cuadro 5-7/J.192 – Función de QoS del BP

Funciones de QoS del servicio de portal	Descripción
{texto informativo: Puntos de control o servicios de QoS UPnP.}	{texto informativo: QoS UPnP es el protocolo utilizado para transportar mensajes de QoS en la LAN. }

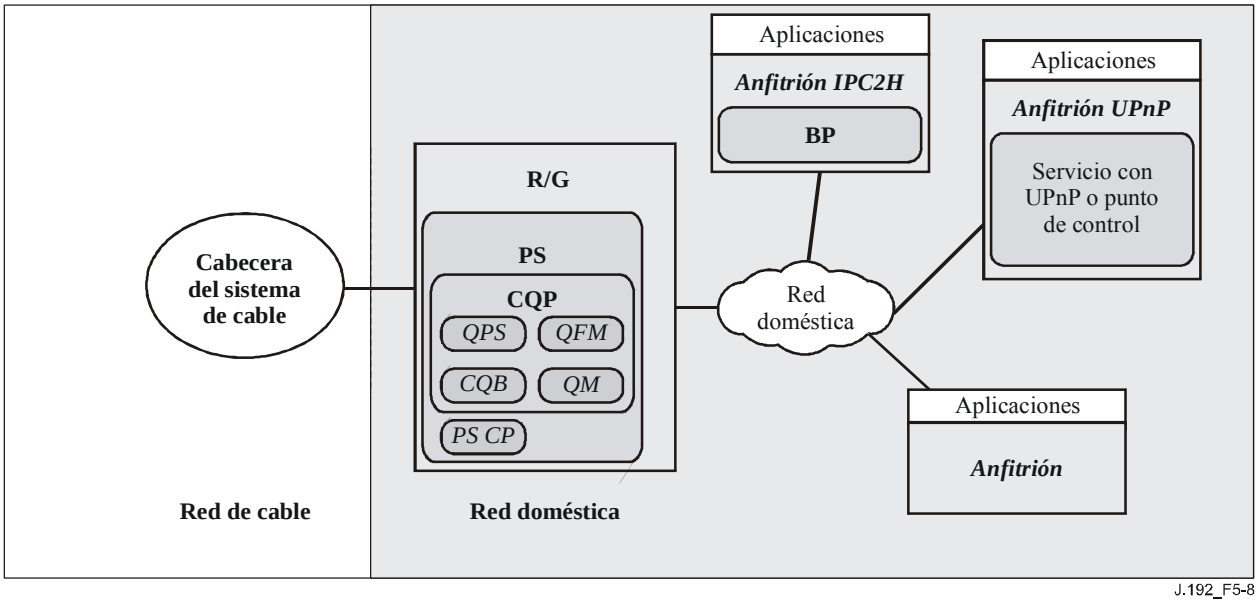


Figura 5-8/J.192 – Elementos de QoS de IPCable2Home

5.3 Modelo de interfaz de mensajería de IPCable2Home

La comunicación entre las funciones en la red de datos por cable, la pasarela residencial y los dispositivos IP de LAN pasa por interfaces de mensajería que se identifican y etiquetan en la figura 5-9. Gracias a los elementos que participan en la comunicación pueden diferenciarse los tipos de esas interfaces.

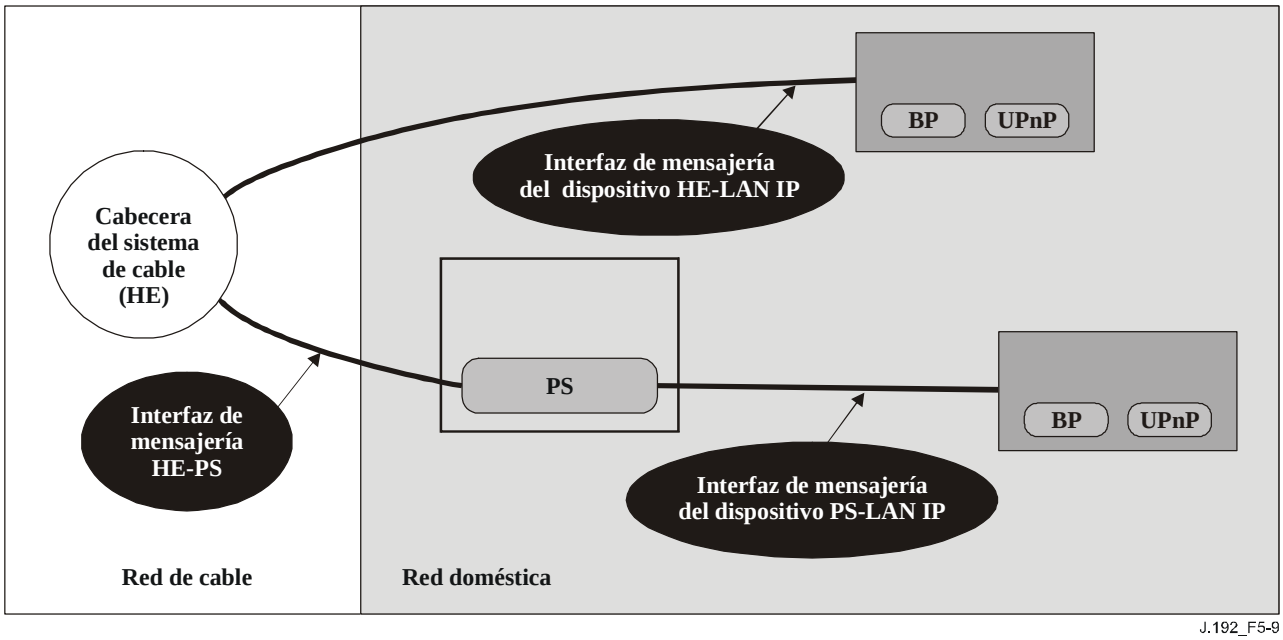


Figura 5-9/J.192 – Interfaces de referencia de IPCable2Home

En el cuadro 5-8 se identifican las interfaces para las que IPCable2Home especifica mensajes.

Cuadro 5-8/J.192 – Trayectos de interfaz válidos para cada una de las funcionalidades

Funcionalidad	Protocolo	Interfaz		
		HE-PS	HE dispositivo IP de LAN	PS dispositivo IP de LAN
Servicio de nombre	DNS	Sin especificar	Sin especificar	Esta Recomendación
Descarga de software	TFTP	Esta Recomendación	Sin especificar	Sin especificar
Obtención de dirección	DHCP	Esta Recomendación	Sin especificar	Esta Recomendación
Gestión (simple) (en bloque)	SNMP TFTP o HTTP	Esta Recomendación Esta Recomendación	Sin especificar Sin especificar	Sin especificar Sin especificar
Notificación de eventos	SNMP SYSLOG	Esta Recomendación Esta Recomendación	Sin especificar	Sin especificar
QoS	Protocolos de QoS de IPCablecom, SNMP {texto informativo: QoS UPnP}	Sin especificar Esta Recomendación Sin especificar	IPCablecom Sin especificar Sin especificar	Sin especificar Sin especificar Esta Recomendación
Seguridad (distribución de claves)	Kerberos	Esta Recomendación	Sin especificar	Sin especificar
Seguridad (autenticación)	Kerberos o TLS	Esta Recomendación	Sin especificar	Sin especificar
Ping	ICMP	Esta Recomendación	Sin especificar	Esta Recomendación
Bucle/eco	UDP/TCP	Sin especificar	Sin especificar	Esta Recomendación
Determinación de la aplicación	SNMP SOAP/XML	Esta Recomendación	Sin especificar	Esta Recomendación
Determinación del dispositivo	SNMP {texto informativo: determinación UPnP/SSDP}	Esta Recomendación Sin especificar	Sin especificar Sin especificar	Sin especificar Esta Recomendación

5.4 Modelo de referencia de información de IPCable2Home

El funcionamiento del modelo de gestión se basa en el almacenamiento de información que se mantiene en el PS mediante varios de sus subelementos (CAP, CDP, CMP, etc.). Estos subelementos necesitan un medio para interfuncionar mediante intercambio de información, y la base de datos del PS es una entidad conceptual que representa dicho almacenamiento. La base de datos del PS no es una base de datos específica real por sí misma, sino que se trata de una herramienta que facilita la comprensión de la información intercambiada entre los distintos elementos de IPCable2Home.

En la figura 5-10 se ilustra la relación entre la base de datos y las funciones del PS. En el cuadro 5-9 se describe la información normal correspondiente a cada una de esas funciones. En la figura 5-11 se da un ejemplo detallado de una implementación en la que se indica el conjunto de información, las funciones de las que se deduce la información y las relaciones entre las funciones y la información.

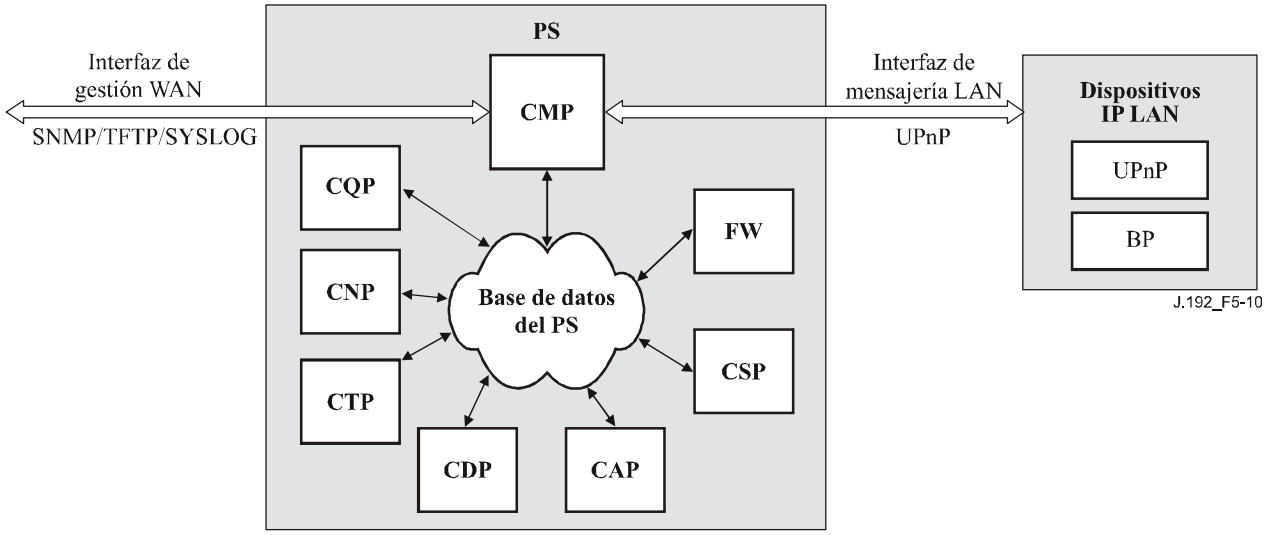


Figura 5-10/J.192 – Relación entre las funciones y la base de datos del PS

En la base de datos del PS se almacena una gran cantidad de relaciones de datos. El CMP aporta la interfaz de gestión de la red WAN (SNMP) a la base de datos del PS. Las funciones en el PS acceden y examinan las relaciones de datos en la base de datos del PS. Además, estas funciones pueden permitir la recuperación de información de la base de datos del PS que es mantenida por otras funciones en el PS.

Cuadro 5-9/J.192 – Ejemplos de información convencional en la base de datos del PS

Nombre	Utilización (en general)
Información de CDP	Información correspondiente a las direcciones obtenidas y atribuidas a través de DHCP.
Información de CAP	Información asociada a las correspondencias de traducción de direcciones de IPCable2Home.
Información de CMP	Información correspondiente al estado de las funciones del PS. Información relativa a los anfitriones de {texto informativo: dispositivos y servicios del anfitrión UPnP recopilados mediante los mensajes de determinación UPnP.}
Información de CTP	Información correspondiente a los resultados de las pruebas de la red LAN realizadas por el CMP.
Información de CNP	Información correspondiente a la determinación del nombre del dispositivo IP LAN.
Información de USFS	Información correspondiente a la función de conmutación de retransmisión selectiva en sentido ascendente.
Información de CSP	Información correspondiente a la autenticación, intercambio de claves, etc.
Información de la barrera contra fuegos	Información correspondiente al comportamiento de la barrera contra fuegos (conjunto de normas), sus eventos y registros históricos.

Cuadro 5-9/J.192 – Ejemplos de información convencional en la base de datos del PS

Nombre	Utilización (en general)
Información de eventos	Información correspondiente al registro histórico local de todos los eventos, trampas, etc., genéricos.
Información CQP	Política de QoS recibida del operador de cable e información de QoS recibida dispositivos anfitriones con QoS {texto informativo: UPnP} y puntos de control {texto informativo: mediante mensajes de QoS UPnP.}

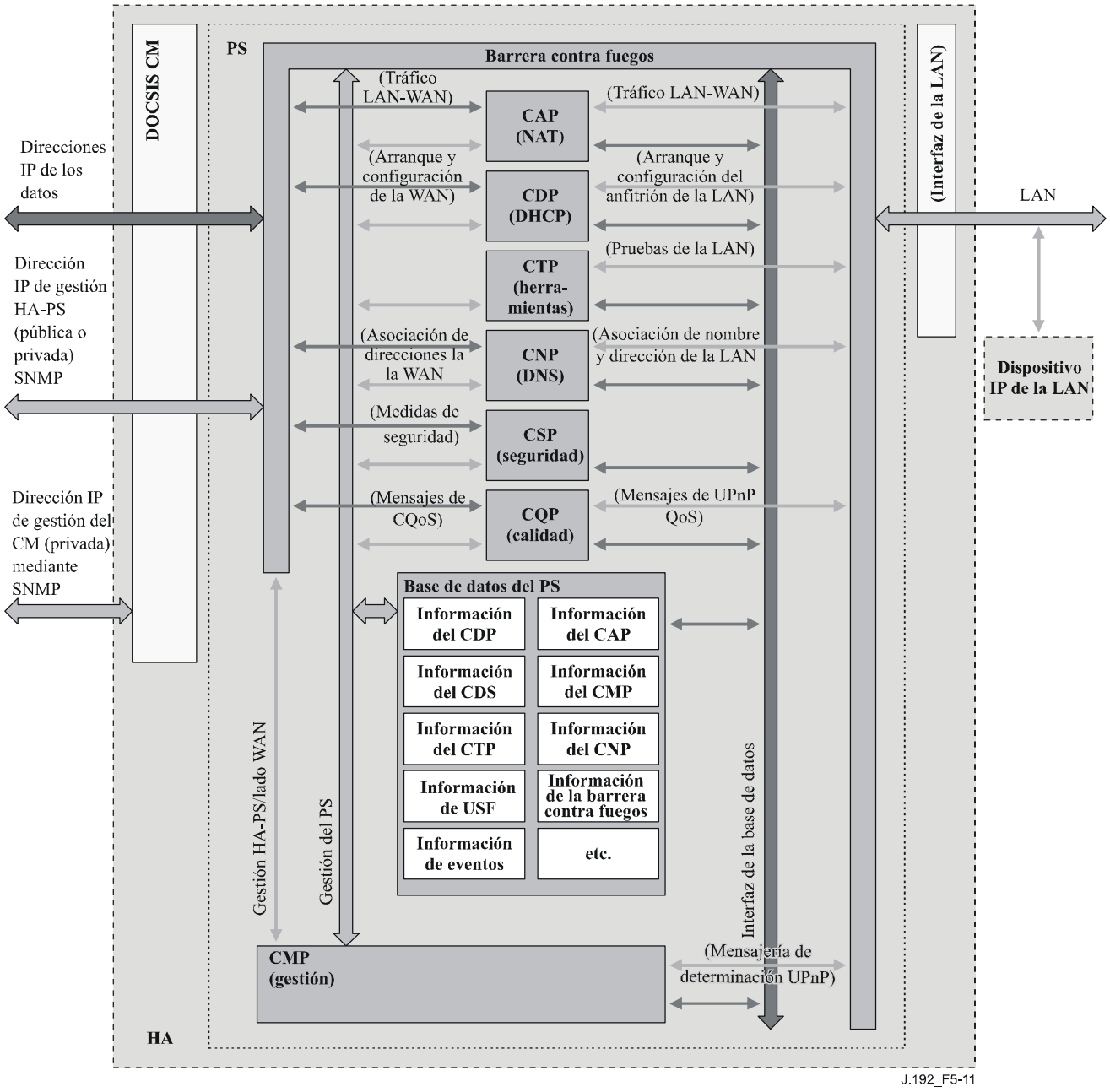


Figura 5-11/J.192 – Ejemplo detallado de implementación de la base de datos del PS

El PS se gestiona en primera instancia desde la red WAN a través del CMP y, en gran medida, se incluye el acceso a la información en la base de datos del PS. La gestión se emplea para la inicialización y la configuración de las funciones del PS, así como de los diagnósticos a distancia o el estado de la red LAN. Los diagnósticos podrán apoyarse en el CTP para conseguir una mejor visibilidad del estado actual de la LAN. Se puede medir la conectividad y la calidad de funcionamiento elemental de la red.

El CNP es el servidor de nombres de dominio (DNS, *domain name server*) de la LAN. El CDP configura todos los dispositivos IP de LAN del sector LAN-Trans para que utilicen el CNP como servidor de nombres principal. El CNP determina los nombres de los anfitriones, en texto, de los dispositivos IP de LAN, devolviendo sus direcciones IP correspondientes y, además, permite que los dispositivos IP de LAN hagan referencia a los servidores DNS externos con relación a las peticiones que no pueden satisfacerse a partir de la información local.

El CDP incluye las funciones de dirección que le permiten funcionar como servidor DHCP en el sector LAN-Trans e implementar un cliente DHCP en los sectores de la WAN.

El CAP crea correspondencias de traducción de direcciones entre los sectores de direcciones WAN-Data y LAN-Trans. Además, es responsable de las decisiones de conmutación por retransmisión selectiva en sentido ascendente, necesarias para preservar el ancho de banda del canal HFC (WAN) en sentido ascendente del tráfico de la LAN exclusivamente local. Por último, el CAP incluye la función de transferencia, que permite puentear tráfico entre los sectores de direcciones de la LAN y de la WAN.

El CPS ofrece capacidades de autenticación del PS, así como actividades de intercambio de claves.

El CQP forma parte de un sistema que habilita la QoS de IPCable2Home y asigna prioridades al tráfico de IPCable2Home y proporciona funciones de acceso a medios diferenciados.

5.5 Modos de funcionamiento de IPCable2Home

La funcionalidad del elemento de servicios de portal es compatible con una diversidad de infraestructuras de la red de cable, a las que se puede dar cabida mediante varios modos de funcionamiento distintos del PS. Éstos permiten que el PS funcione adecuadamente en una infraestructura de configuración exclusiva del módem de cable (Rec. UIT-T J.112 ó J.122), así como en una infraestructura de configuración de módem de cable más IPCablecom. La infraestructura de IPCable2Home de configuración de módem de cable más IPCablecom se consolida en las infraestructuras de CableMÓdem para habilitar servicios adicionales, e incorpora diversas capacidades similares a las que existen en un sistema de configuración de IPCable2Home.

Puede establecerse que el PS sea completamente configurado y gestionado por el operador de cable, o que funcione como una pasarela residencial sin gestión ni configuración (excepto para adquirir una licencia de dirección IP y configuración mediante DHCP). Además, un PS integrado puede ser inhabilitado a fin de que el dispositivo en sobre el que se implemente sólo se despliegue como módem de cable.

En el modo de funcionamiento completamente configurado y gestionado, el PS recibe la información de dicho modo de funcionamiento en los mensajes [RFC 2131] y [RFC 2132] DHCP cuando arranca y solicita una dirección de red utilizando DHCP. En función de la información que de los mensajes DHCP, el PS puede configurarse para funcionar en uno de los dos modos de configuración siguientes:

- Modo de configuración DHCP.
- Modo de configuración SNMP.

Si el PS no se configura para que funcione en cualquiera de los dos modos, se supondrá que no está disponible el soporte interno, y pasará por defecto al funcionamiento en modo CableHome aletargado. En este modo, la pasarela residencial se considerará plenamente operacional desde el punto de vista del usuario, aunque no podrá ser configurada o gestionada por el operador. Si un PS está integrado en un dispositivo con un módem de cable que sea conforme con [eDOCSIS], el PS integrado puede ser configurado directamente a través del módem de cable para funcionar en el modo CableHome aletargado. El operador de cable también puede "apagar", o inhabilitar, la funcionalidad PS en un dispositivo con módem de cable integrado y PS integrado directamente a través del módem de cable.

Si el PS se configura para funcionar en el modo de configuración DHCP, tendrá la capacidad para iniciar una sesión de seguridad de capa de transporte (TLS, *transport layer security*) por HTTP, a fin de proporcionar la descarga asegurada de los ficheros de configuración del PS y de la barrera contra fuegos.

Si el PS se encuentra en el modo de configuración DHCP, podrá funcionar en uno de dos submodos de gestión de red:

- Modo NmAccess.
- Modo de coexistencia SNMPv3.

Si el PS se encuentra en el modo de configuración SNMP, podrá funcionar únicamente en el modo de gestión de red de coexistencia SNMPv3.

En la figura 5-12 se ilustran los distintos modos de funcionamiento del PS y los activadores correspondientes a cada uno de ellos. Véase 7.3.3.2.4, Requisitos del CDC para obtener una descripción completa de la determinación del modo de configuración.

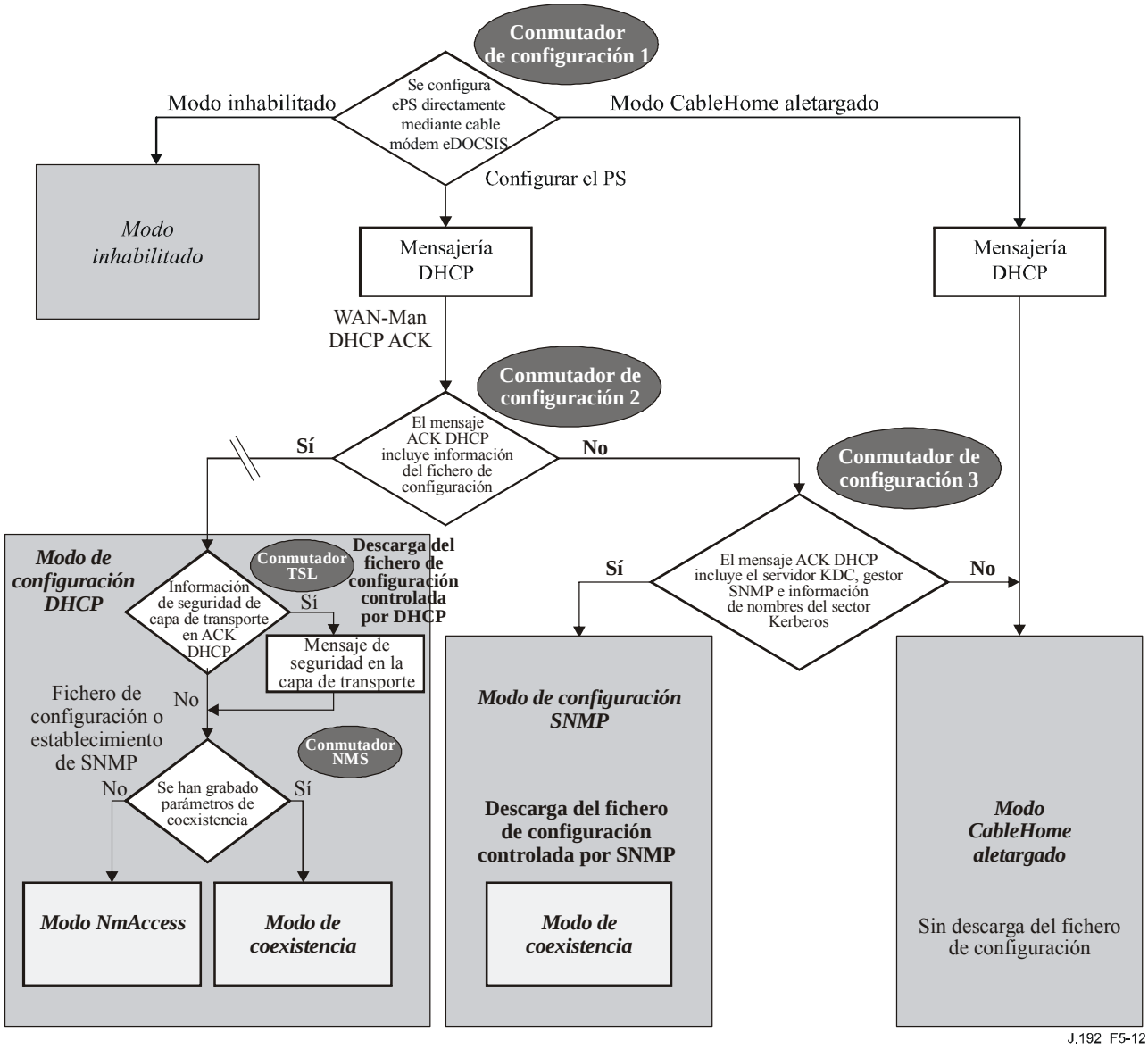


Figura 5-12/J.192 – Modos de funcionamiento del PS

En el cuadro 5-10 se describen las infraestructuras en las que se pretende que funcionen cada uno de los modos del PS.

Cuadro 5-10/J.192 – Infraestructuras de PS

Modo	Capacidad directamente afectada	Infraestructura deseada
Modo de configuración SNMP	Descarga del fichero de configuración	Infraestructura de configuración de CableMÓdem más IPCablecom
Modo de configuración DHCP	Descarga del fichero de configuración	Infraestructuras de CableMÓdem con soporte de IPCable2Home
Modo de configuración DHCP: con TLS/HTTP	Descarga segura del fichero de configuración	Infraestructuras de CableMÓdem con soporte de IPCable2Home y TLS

Cuadro 5-10/J.192 – Infraestructuras de PS

Modo	Capacidad directamente afectada	Infraestructura deseada
Modo de configuración DHCP: modo de gestión de red NmAccess	Versión SNMP empleada entre el NMS y el PS	Infraestructura de J.112 (1998) (SNMPv1/v2) con soporte de IPCable2Home
Modo de configuración DHCP: modo de gestión de red de coexistencia SNMP	Versión SNMP empleada entre el NMS y el PS	J.112 y J.122, y las infraestructuras de configuración de CableMÓdem más IPCablecom (SNMPv3) con soporte de IPCable2Home
Modo de IPCable2Home aletargado	Configuración y gestión	Sin soporte de IPCable2Home
Modo deshabilitado	Configuración, gestión, traducción de dirección, reenvío de tráfico y barrera contra fuegos	Infraestructuras DOCSIS 1.0, 1.1 y 2.0 con el soporte IPCable2Home. Permite la instalación de un dispositivo con módem de cable integrado y PS integrado sólo como módem de cable

5.6 Interfaces físicas en la pasarela residencial

Hay muchos tipos de interfaces físicas que se pueden aplicar a un dispositivo que incluya funcionalidad de PS. A continuación se describen varias de esas interfaces:

- Interfaces de funcionamiento en red WAN, hacia la red de cable a través del módem de cable que funciona como un puente transparente para un PS con un módem de cable integrado, y otras interfaces de funcionamiento en red WAN previstas para conexión WAN en el caso de un PS autónomo.
- Interfaces de funcionamiento en red LAN, para conexión a dispositivos IP de LAN y anfitriones de IPCable2Home.
- Interfaces de prueba de hardware, tales como JTAG y otros desarrollos patentados, que se integran en los circuitos integrados y que no siempre disponen de controles de software para desactivar las interfaces. Esas interfaces son máquinas de estado de hardware que se mantienen pasivas hasta que sus líneas de entrada se activan con datos. Aunque este tipo de interfaces puede utilizarse para leer y escribir datos, se necesita un conocimiento específico de los circuitos integrados y la disposición de la tarjeta y por consiguiente son difíciles de "atacar". Las interfaces de prueba del hardware PUEDEN residir en un dispositivo que disponga de funcionalidad PS. Estas interfaces NO DEBEN etiquetarse o documentarse para utilización de los clientes.
- Interfaces de acceso a gestión, también denominadas puertos de consola, que en realidad son trayectos de comunicaciones (por lo general RS-232, pero también podría ser Ethernet, etc.) y software de depuración que interactúa con el usuario. El software invita al usuario a introducir datos y acepta instrucciones para leer y escribir datos en el PS. Si se desactiva el software de esta interfaz, se desactivará a su vez el trayecto de comunicaciones físico. Un PS NO DEBE dar acceso a las funciones del PS a través de la interfaz de acceso a la gestión. (Las funciones del PS se definen en esta Recomendación.) El acceso a las funciones del PS DEBE autorizarse únicamente a través de las interfaces recomendadas específicamente para tal efecto en la presente Recomendación, por ejemplo, acceso controlado por el operador a través de SNMP.
- Interfaces de diagnóstico de sólo lectura, que pueden implementarse de diversas maneras y se utilizan para proporcionar servicios de depuración, localización y reparación de averías e

información de estado del PS útiles para los usuarios. Un PS PUEDE tener interfaces de diagnóstico de sólo lectura.

- En algunos productos se podrían implementar funciones de capa superior (como es el caso de las funciones de la red de datos en las instalaciones del cliente) que podrían necesitar que el usuario las configure. Un PS PUEDE ofrecer la capacidad para configurar funciones distintas de IPCable2Home. El PS DEBERÍA implementar una interfaz de usuario para permitir la configuración por parte del usuario de funciones que no sean IPCable2Home y funciones CableHome. La interfaz de usuario permite el acceso de éste a funciones de gestión definidas por CableHome (es decir, a objetos MIB definidos por IPCable2Home), pero se exige la adhesión a las reglas de acceso establecidas por el operador. Véase 6.3.3.1.4.2.2.

6 Herramientas de gestión

6.1 Introducción/síntesis

Las herramientas de gestión de IPCable2Home permiten al operador de cable disponer de la funcionalidad necesaria para supervisar y configurar el elemento de servicios de portal (PS) {texto informativo: a fin de determinar dispositivos anfitriones UPnP y los servicios UPnP que ofrecen,} para verificar a distancia la conectividad entre los dispositivos de PS y de IP de LAN e informar sobre el estado y los eventos de excepción en el PS. En esta cláusula se describen y determinan los requisitos para esas capacidades.

A continuación se enumeran las diferencias entre las herramientas de gestión definidas en la Rec. UIT-T J.191 y las que se definen en esta Recomendación:

- Esta Recomendación añade el requisito de que el PS permita la gestión SNMP desde cualquier interfaz LAN.
- {texto informativo: Esta Recomendación añade el requisito de que el PS acepte mensajes de determinación UPnP para que los operadores de cable puedan determinar la existencia de varios dispositivos UPnP y sus capacidades en la LAN doméstica.}
- Esta Recomendación añade al PS los siguientes objetos de MIB:
  - los necesarios para soportar la calidad de servicio con prioridades en la red LAN;
  - los necesarios para soportar una funcionalidad reforzada de la barrera contra fuegos;
  - {texto informativo: los que permiten al operador de cable visualizar los atributos y capacidades de los dispositivos anfitriones UPnP de la LAN.}

6.1.1 Objetivos

Los objetivos de las herramientas de gestión de IPCable2Home son:

- {texto informativo: Proporcionar un medio para que el operador del sistema de cable determine los dispositivos anfitriones UPnP.}
- Dotar a los operadores de sistemas de cable de visibilidad sobre los dispositivos IP de LAN.
- {texto informativo: Dotar a los operadores de sistemas de cable de visibilidad sobre las aplicaciones y servicios ofrecidos por dispositivos anfitriones UPnP.}
- Definir un conjunto mínimo de herramientas de diagnóstico a distancia que permitirá al operador del sistema de cable verificar la conectividad entre el elemento de servicios de portal y cualquier dispositivo IP de LAN.
- Dotar a los operadores de sistemas de cable del acceso, a través de las MIB, a los datos internos del elemento PS y de la capacidad de supervisar los parámetros específicos de IPCable2Home y de configurar o reconfigurar las capacidades específicas de IPCable2Home, según proceda.

- Proporcionar un medio para informar con relación a las excepciones y otros eventos en forma de trampas SNMP, mensajes a un registro histórico local o mensajes a un registro histórico del sistema (SYSLOG) en la red de cable.

6.1.2 Hipótesis

Las hipótesis relativas al entorno de gestión de la red IPCable2Home incluyen lo siguiente:

- Los dispositivos conformes con IPCable2Home implementan el conjunto de protocolos (IPv4) del protocolo Internet.
- {texto informativo: Los dispositivos anfitriones UPnP implementan protocolos de determinación de dispositivos y servicios UPnP, tal como se especifica en la Arquitectura de dispositivos UPnP 1.0 [UDA 1.0].}
- Se utiliza el SNMP para el intercambio de mensajes de gestión entre el NMS de la red de cable y el PS en la pasarela residencial de IPCable2Home. El protocolo SNMP da al NMS la visibilidad hacia las interfaces en el PS, a través del acceso a los datos internos del PS, mediante las MIB necesarias.
- Puede utilizarse cualquiera de los protocolos SNMPv1/v2c/v3 como protocolo de gestión entre el NMS y el elemento de servicios de portal de IPCable2Home.
- Los dispositivos IP de LAN implementan un cliente DHCP.
- La pasarela residencial de IPCable2Home y los dispositivos IP de LAN aceptan ICMP.
- La utilidad PING proporciona la funcionalidad suficiente para que el operador de cable pueda obtener la información deseada relativa a la conectividad entre el elemento PS y los dispositivos IP de LAN.

6.2 Arquitectura de gestión

6.2.1 Directrices para el diseño del sistema

En el cuadro 6-1 se relacionan las directrices de diseño del sistema correspondiente a las herramientas de gestión. Esta relación ha proporcionado las orientaciones necesarias para el desarrollo de las especificaciones de las herramientas de gestión de IPCable2Home.

Cuadro 6-1/J.192 – Directrices de diseño del sistema relativo a las herramientas de gestión

Referencia	Directrices de diseño del sistema relativo a las herramientas de gestión
Mgmt 1	El PS implementará los protocolos SNMPv1/v2c/v3 para facilitar el acceso a los datos internos de los servicios de portal.
Mgmt 2	El PS deberá ser capaz de emitir una instrucción de petición ICMP (Ping) destinada a cualquier dispositivo IP de LAN especificado por el operador del cable y de almacenar los resultados en la base de datos del PS. Los resultados de la prueba Ping a distancia serán accesibles a través de los objetos de la MIB de CTP.
Mgmt 3	El PS deberá tener la capacidad de ejecutar una prueba de la velocidad de la conexión con un dispositivo IP de LAN específico que determine el operador del cable y de almacenar los resultados en la base de datos del PS. Los resultados de la prueba de la velocidad de la conexión a distancia serán accesibles a través de los objetos de la MIB de CTP.
Mgmt 4	El elemento PS debe ser capaz de informar con relación a los eventos.

Cuadro 6-1/J.192 – Directrices de diseño del sistema relativo a las herramientas de gestión

Referencia	Directrices de diseño del sistema relativo a las herramientas de gestión
Mgmt 5	{texto informativo: El elemento PS debe ser capaz de comunicarse con los anfitriones UPnP en los sectores LAN-Pass y LAN-Trans para fines del intercambio de los atributos de los dispositivos, las prioridades de QoS y la información de los servicios y aplicaciones del anfitrión UPnP.}
Mgmt 6	En el supuesto de que el PS pierda la conectividad con la red de datos del sistema de cable y sus aplicaciones, las funciones de determinación y de mensajes de LAN deben continuar funcionando.

6.2.2 Descripción del sistema de herramientas de gestión

Como se muestra en la figura 6-1, la arquitectura de las herramientas de gestión de IPCable2Home consta de los siguientes componentes:

1) portal de gestión de IPCable2Home (CMP);
2) portal de prueba de IPCable2Home (CTP);
3) base de información de gestión (MIB); y
4) sistema de gestión de red SNMP (NMS) que forma parte de la red de cable.

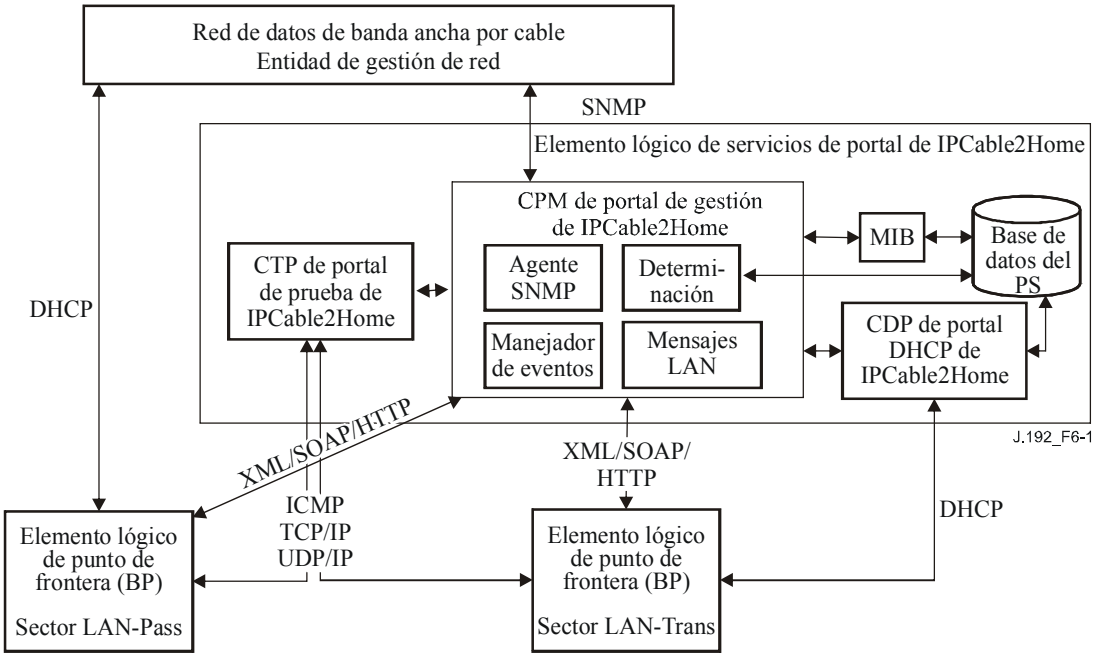


Figura 6-1/J.192 – Arquitectura de gestión de IPCable2Home

El NMS de la red de datos por cable supervisa y configura el PS accediendo a la base de datos del PS, a través de las MIB que se especifican en 6.3.3.1.4.7. {texto informativo: El operador del sistema de cable accede a atributos del dispositivo anfitrión UPnP y de la pasarela residencial de IPCable2Home a través de la MIB PSDev [véase E.4] y de la MIB de QoS [véase E.7], y configura los dispositivos anfitriones de IPCable2Home con las políticas de QoS (en forma de prioridades de QoS), utilizando el PS como un apoderado. El PS IPCable2Home implementa un punto de control UPnP (CP de PS) para obtener información de determinación de los dispositivos anfitriones UpnP.}

El NMS puede también comunicarse directamente con los dispositivos IP de LAN en el sector LAN-Pass de IPCable2Home.

El portal DHCP de IPCable2Home, que se describe en la cláusula de herramientas de configuración (cláusula 7), desempeña un papel importante en el proceso de determinación básica del dispositivo IP de LAN. El dispositivo IP de LAN, mediante comunicación DHCP entre los dispositivos IP de LAN y el CDP, proporciona su dirección de hardware y puede suministrar información de configuración al CMP a través de códigos de opción DHCP. El CMP utilizará la información para rellenar los objetos del cuadro de direcciones de LAN de la MIB del CDP (cabhCdpLanAddrTable).

Los elementos funcionales CMP y CTP residen en el PS. El elemento lógico PS puede residir conjuntamente con un módem de cable integrado o autónomo, sin funcionalidad de módem de cable integrado, como se describe en 5.1.2.1.1.

El CM y el PS son entidades de gestión separadas e independientes. En el caso de un PS con un módem de cable integrado, no es implícita la compartición de datos entre el CM y el PS, con las siguientes excepciones:

1) la descarga de la copia imagen de software se controla mediante la MIB del módem de cable,

2) la MIB de SNMP [RFC 3418], el grupo SNMP de la MIB-2 (mib-2 11) [RFC 1213], el grupo IP y el grupo ICMP de la MIB de SNMPv2 para IP [RFC 2011], así como la MIB de SNMPv2 para UDP [RFC 2013] podrán compartirse entre el PS y el CM.

En un PS con un módem de cable integrado, se accede a los objetos docsDevSoftware del módem de cable para establecer, iniciar y supervisar la descarga de una copia imagen simple de software combinada. Este proceso se describe en 11.8, Descarga segura de software para el PS.

Con motivo de esta independencia de gestión, el CM y el PS responden a direcciones IP de gestión distintas e independientes. Los objetos de la MIB del CM sólo son visibles cuando el gestor accede a ellos a través de la dirección IP de gestión del CM, y no son visibles a través de la dirección IP de gestión del PS (y viceversa). Los derechos de acceso del SNMP a las entidades PS y CM DEBEN establecerse de manera independiente. El sistema IPCable2Home no excluye la utilización de un agente simple de SNMP para un PS con un CM integrado.

El elemento de servicios de portal soporta los protocolos SNMPv1, SNMPv2c y SNMPv3. En 5.5 se introdujeron los modos de configuración soportados por un elemento de servicios de portal de IPCable2Home, y en la cláusula 7 se dan mayores detalles con relación a estos modos. El modo de configuración en el que funciona el PS determina parcialmente la versión de SNMP que utiliza el PS. En la cláusula 6.3.3 se da información más detallada.

6.3 Elemento lógico del PS – Portal de gestión de IPCable2Home (CMP)

El portal de gestión de IPCable2Home (CMP) es un subelemento del elemento lógico PS. Se emplea como el centro del control de gestión del PS y también para la determinación de los dispositivos existentes en la red LAN.

El CMP agrega e interconecta información de gestión en los sectores WAN-Man y LAN-Trans, ya que no son accesibles directamente entre ellos.

6.3.1 Objetivos de CMP

Los objetivos del portal de gestión de IPCable2Home son:

- Facilitar que el NMS pueda ver y actualizar a distancia la información de configuración del portal de direcciones de IPCable2Home (CAP).
- Permitir que el NMS vea y actualice a distancia la información de configuración de la barrera contra fuegos.

- Permitir la prueba de la conectividad a distancia entre la pasarela residencial de IPCable2Home y los dispositivos IP de LAN en el sector LAN-Trans, a través del portal de prueba de IPCable2Home (CTP).
- Permitir la configuración a distancia de los parámetros de direccionamiento del dispositivo IP de LAN.
- Permitir visualizar la información del dispositivo IP de LAN que se obtuvo a través del portal DHCP de IPCable2Home (CDP).
- {texto informativo: Facilitar el acceso del operador del sistema de cable a los atributos de los dispositivos anfitriones UPnP y sus servicios UPnP, obtenidos mediante el proceso de determinación de UPnP.}
- Permitir el examen de los resultados de la supervisión de la calidad de funcionamiento de los dispositivos IP de LAN efectuada mediante el portal de prueba de IPCable2Home (CTP).
- Permitir que el NMS acceda a otros parámetros de configuración del PS.
- Facilitar la seguridad al permitir el acceso a los parámetros de seguridad, y la utilización de SNMPv1/v2c/v3 en el modo de gestión de red adecuado.
- Proporcionar la capacidad para inhabilitar segmentos de la red LAN.

6.3.2 Directrices de diseño del CMP

Las directrices de diseño del CMP se relacionan en el cuadro 6-2. La lista proporciona la orientación para la especificación de la funcionalidad del CMP.

Cuadro 6-2/J.192 – Directrices de diseño del sistema CMP

Referencia	Directrices de diseño del sistema CMP
CMP 1	Las interfaces deben soportar las características de gestión y diagnóstico, y las funciones necesarias para los servicios propios del sistema de cable que hayan de prestarse a través de la red doméstica.
CMP 2	La desconexión entre los proveedores de servicios de banda ancha y la red doméstica no debe desactivar ni degradar las funciones internas de conexión en esta red.
CMP 3	La red doméstica tendrá la capacidad de recuperación tras una interrupción de corriente, y los dispositivos conectados a la red doméstica deben regresar al estado de funcionamiento en el que estaban antes de la interrupción.
CMP 4	Los dispositivos de la red doméstica deben instalarse y configurarse fácilmente para que funcionen como cualquier otro electrodoméstico.
CMP 5	{texto informativo: El PS y el anfitrión UPnP deben soportar el protocolo de determinación UPnP para la adquisición de los atributos del dispositivo anfitrión UPnP y de los servicios UPnP que implementan.}
CMP 6	{texto informativo: El PS proporcionará al operador del sistema de cable, cuando así se solicite, la información relativa a los atributos del dispositivo anfitrión IPCable2Home y de los servicios UPnP que implementan.}
CMP 7	{texto informativo: El intercambio de mensajes del protocolo de determinación en la red LAN doméstica no debe degradar perceptiblemente la calidad de funcionamiento de la red LAN doméstica.}
CMP 8	{texto informativo: Los mensajes del protocolo de determinación no deberán propagarse a la red WAN.}

6.3.3 Descripción del sistema CMP

El CMP se encargará de las siguientes capacidades importantes de IPCable2Home:

- Permitir la gestión de las funciones de los servicios de portal desde el sistema de gestión de red (NMS, *network management system*) de la red de datos del operador del sistema de cable, dándole acceso a la base de datos del PS y a sus variables de estado a través de los objetos de la base de información de gestión (MIB) específicos de IPCable2Home.
- Permitir al abonado la visibilidad de la base de datos del PS a través de los objetos de la MIB específicos de IPCable2Home.
- Permitir el intercambio de prioridades de QoS entre el PS y el BP.
- {texto informativo: Permitir al gestor la determinación a distancia de los dispositivos conectados a la red LAN doméstica y a los servicios UPnP que utilizan.}
- Procesar y registrar históricamente los mensajes de eventos.

El CMP consta de las siguientes tres funciones que le permiten soportar las responsabilidades de gestión y determinación relacionadas anteriormente. Estas funciones se muestran además en la figura 6-1:

1) *Función de agente SNMP*

   Esta función permite recibir y procesar los mensajes SNMP de la interfaz WAN a través de la dirección IP de WAN-Man y de la interfaz LAN a través de la dirección IP del encaminador del servidor del PS. Esta función permite el acceso a los objetos de la MIB para fines de supervisión y/o configuración de la funcionalidad del PS y del dispositivo IP de LAN.

2) *Función de tratamiento de eventos WAN*

   El CMP envía informes de eventos a la red de datos del operador de cable en la WAN conforme a los valores del cuadro docsDevEvent. En el anexo B se presenta la relación de los eventos soportados.

3) *Función de determinación*

   {texto informativo: El CMP, a través de su funcionalidad determinación UPnP, obtiene la información relativa a cada uno de los dispositivos del anfitrión UPnP y de sus servicios UPnP. El CMP almacena esta información en la base de datos del PS y la pone a disposición de una entidad de gestión SNMP, a través de la MIB de PSDev [véase E.4] y de la MIB de QoS [véase E.7].}

Estas funciones se describen en las cláusulas 6.3.3.1 a 6.3.3.3.

6.3.3.1 Función de agente SNMP del CMP

6.3.3.1.1 Objetivos de la función de agente SNMP

Estos objetivos son:

- Recibir y procesar los mensajes SNMP que llegan a través de las interfaces WAN-Man y de encaminador del servidor del PS (LAN).
- Proporcionar al gestor de SNMP el acceso a la base de datos del PS a través de las MIB específicas de IPCable2Home.
- Vigilar el cumplimiento de las reglas de acceso a la base de datos del PS definidas por docsDevNmAccessTable y las vistas de VACM.
- Soportar los procesos de autenticación y criptación/descriptación de SNMP definidos en las normas RFC del IETF.
- Respetar las reglas y directrices de implementación de SNMP definidas en las normas RFC del IETF.

6.3.3.1.2 Directrices de diseño del sistema relativo a la función de agente SNMP

Las directrices de diseño del sistema que se relacionan en el cuadro 6-3 permiten orientar la evolución de los requisitos de la función de agente SNMP.

Cuadro 6-3/J.192 – Directrices para el diseño del sistema

Referencia	Directrices para el diseño del sistema sobre la función de agente SNMP
Agente 1 de SNMP	El PS debe permitir el acceso a distancia a los parámetros gestionables en la base de datos del PS, a través de MIB específicas.
Agente 2 de SNMP	El PS deberá implementar un agente SNMP que sea compatible con los sistemas de gestión de la red de datos por cable.
Agente 3 de SNMP	El PS debe aceptar los métodos de control de acceso que permitan al operador del sistema de cable configurar el control del acceso a la base de datos del PS.

6.3.3.1.3 Descripción del sistema relativo a la función de agente SNMP

La función de agente SNMP de CMP desempeña el papel central del control de gestión para acceder a la gestión en el lado de la WAN y permite obtener información de los elementos de gestión de la red WAN y de la red LAN, y además interconecta la gestión de dichos elementos. Esta función también soporta los mensajes de gestión mediante SNMP a través de cualquier interfaz LAN.

El CMP puede funcionar en cualquiera de tres modos de gestión de red:

- Modo de configuración SNMP/modo de gestión de coexistencia SNMPv3.
- Modo de configuración DHCP/modo de gestión conforme al cuadro NmAccess.
- Modo de configuración DHCP/modo de gestión de coexistencia SNMPv3.

Modo de configuración SNMP/modo de gestión de coexistencia SNMP

Tal y como se describe en 5.5, si se emplea el modo de configuración SNMP, el PS pasará a funcionar, por defecto, en el modo de coexistencia SNMPv3 con SNMPv1 y SNMPv2 inhabilitados, y utilizará Kerberos para distribuir las claves. Se soportan los modelos de seguridad específica de usuario (USM, *user-based security model*) [RFC 3414] y de control de acceso basado en vistas (VACM, *view-based access control model*) [RFC 3415] para facilitar que el operador del sistema de cable pueda aplicar las políticas de gestión relativas al acceso a las MIB especificadas.

Modo de configuración DHCP/modo de gestión conforme al cuadro NmAccess

Tal y como se describe en 5.5, si se emplea el modo de configuración DHCP, el PS pasará a funcionar, por defecto, en el modo conforme al cuadro NmAccess. Bajo este modo de funcionamiento, el acceso a la gestión se controla mediante el cuadro NmAccess de la MIB del dispositivo DOCSIS [RFC 2669] y podrán soportarse los protocolos SNMPv1/v2c.

El PS DEBE aplicar las reglas siguientes para determinar si permite el acceso SNMP desde una dirección IP de origen dada (SrcIpAddr):

> Si (docsDevNmAccessIp == "255.255.255.255"), permite el acceso desde cualquier SrcIpAddr.
>
> Si ((docsDevNmAccessIp AND docsDevNmAccessIpMask) == (SrcIpAddr AND docsDevNmAccesIpMask)), permite el acceso desde SrcIpAddr

El PS DEBE asignar 0.0.0.0 como valor por defecto de docsDevNmAccessIpMask.

En el cuadro 6-4 se muestra las reglas para docsDevNmAccessIp y docsDevNmAccessIpMask antes descritas mediante el suministro de valores de muestra de la MIB y con acceso garantizado para cada combinación.

Cuadro 6-4/J.192 – Ejemplo: Acceso a la MIB concedido para diversos valores de docsDevNmAccessIp y docsDevNmAccessIpMask

docsDevNmAccessIp	docsDevNmAccessIpMask	Acceso
255.255.255.255	Cualquier máscara de dirección IP	Cualquier NMS
Cualquier dirección IP	0.0.0.0	Cualquier NMS
Cualquier dirección IP excepto 255.255.255.255	255.255.255.255	Un solo NMS
0.0.0.0	255.255.255.255	Sin NMS

Modo de configuración DHCP/modo de gestión de coexistencia SNMPv3

Si el PS funciona en el modo de configuración DHCP, el operador del sistema de cable podrá rellenar el cuadro de coexistencia a través de mensajes de petición de establecimiento de SNMP o del fichero de configuración del PS, configurando de esa manera el PS para que pueda funcionar en el modo de gestión de coexistencia de SNMPv3. En el caso de un PS que se ha configurado para que funcione en el modo de coexistencia de SNMPv3, el acceso a la gestión se controla conforme a [RFC 3584], y podrán aceptarse los protocolos SNMPv1/v2c/v3, además podrán soportarse USM y VACM, y las claves de SNMPv3 se distribuirán utilizando [RFC 2786] y los TLV en el fichero de configuración del PS.

En el cuadro 6-5 se presentan las definiciones de los términos específicos al CMP.

Cuadro 6-5/J.192 – Definición de términos

Control de gestión	Acceso de lectura o escritura a un conjunto de parámetros que controla o supervisa el comportamiento del PS.
Base de datos del PS	Conjunto de parámetros que controla o supervisa el comportamiento del elemento PS, pudiendo ser leído por el sistema de gestión de la red WAN. Puede considerarse como un depósito de información que describe el estado actual del PS.
Usuario	De acuerdo con lo definido en SNMP (sección 2.1 de [RFC 3414]), un usuario tiene un nombre asociado, definiciones de seguridad asociadas y acceso a una vista.
Vista	Una vista es un conjunto de objetos de la MIB y de los derechos de acceso a esos objetivos. Cada vista posee un nombre y corresponde a un usuario (sección 2.4 de [RFC 3415]).
Autorización final	Única autoridad que establece, modifica o suprime identificadores de usuario, claves de autenticación, claves de criptación, y derechos de acceso a la base de datos del PS. Este usuario es responsable de todas las operaciones de gestión de seguridad.
Usuario de mantenimiento	Usuario que suele realizar únicamente operaciones de sólo lectura en la base de datos del PS. Por lo general, se utiliza para supervisión y contabilidad de la calidad de funcionamiento.
Usuario administrador	Usuario que suele efectuar operaciones tanto de lectura como de escritura en la base de datos del PS. Estas operaciones se utilizan para la configuración y la gestión de averías.

Como ejemplo de los tipos de información que pueden leerse o manipularse a través del control de gestión de IPCable2Home pueden citarse los valores de la política de la barrera contra fuegos, las correspondencias NAT configuradas por el NMS, el arranque de las herramientas de diagnóstico a distancia y el acceso a sus resultados, el estado del PS, la información de la determinación del dispositivo y de aplicaciones y la configuración del intervalo de direcciones de la LAN. Como se explicará más adelante, las diversas interfaces de mensajería de gestión pueden tener derechos de acceso a conjuntos de parámetros diferentes. Un PS conforme acepta el acceso a su base de datos a través de la jerarquía de la MIB desde las redes WAN y LAN mediante el empleo de SNMP. Los dispositivos del anfitrión de IPCable2Home conformes también podrán intercambiar mensajes con la pasarela residencial al utilizar datos con formato XML que se transportan a través de HTTP. En la figura 6-2 se presentan las interfaces de mensajería de gestión:

- NMS – CMP: intercambio de mensajes de gestión entre el NMS de la red de cable y el CMP.
- CMP – anfitrión de IPCable2Home/LAN-Trans: intercambio de mensajes entre el CMP y los anfitriones de IPCable2Home en el sector LAN-Trans.
- CMP – anfitrión de IPCable2Home/LAN-Pass: intercambio de mensajes entre el CMP y los anfitriones de IPCable2Home en el sector LAN-Pass.
- NMS – dispositivo IP de LAN: intercambio de mensajes de gestión entre el NMS de la red de cable y dispositivos IP de la red LAN en el sector LAN-Pass. Estos mensajes de gestión quedan fuera del alcance de la presente Recomendación.

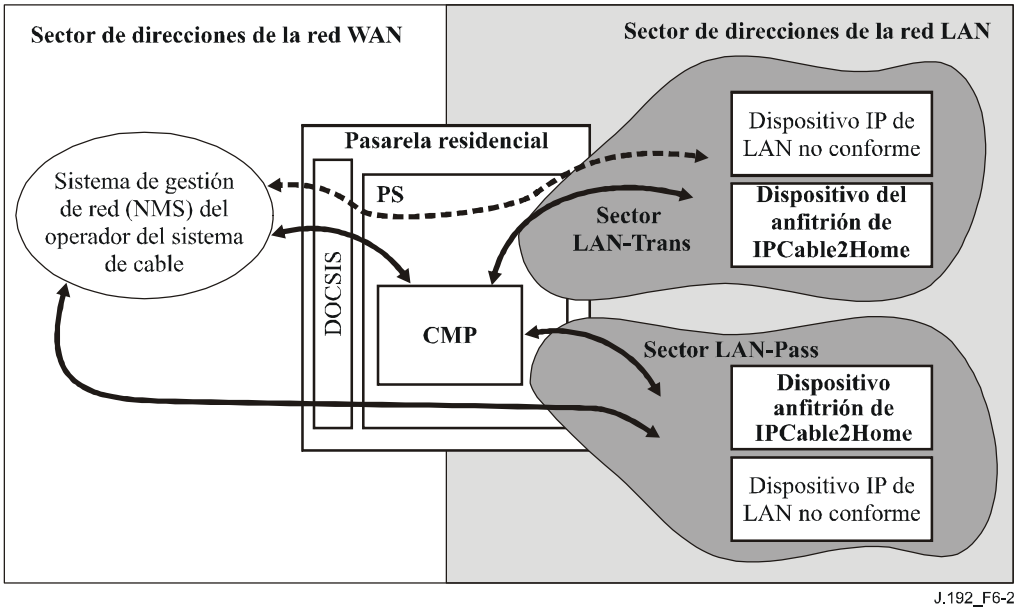


Figura 6-2/J.192 – Interfaces para los mensajes de gestión de IPCable2Home

El CMP es en primera instancia una entidad a la que se accede por la red WAN (NMS) y controlada por la WAN, aunque también se permite el acceso desde la interfaz LAN del PS (dirección del encaminador del servidor – por lo general, la pasarela por defecto de los dispositivos IP de LAN en el sector LAN-Trans). Adicionalmente, se puede solicitar al CMP que informe al NMS de la red de cable a cerca de eventos o de ficheros de registro histórico del sistema de transferencia, según proceda. En la figura 6-3, se ilustra un ejemplo de implementación del CMP, para la conducción de conceptos relativos a la funcionalidad del CMP.

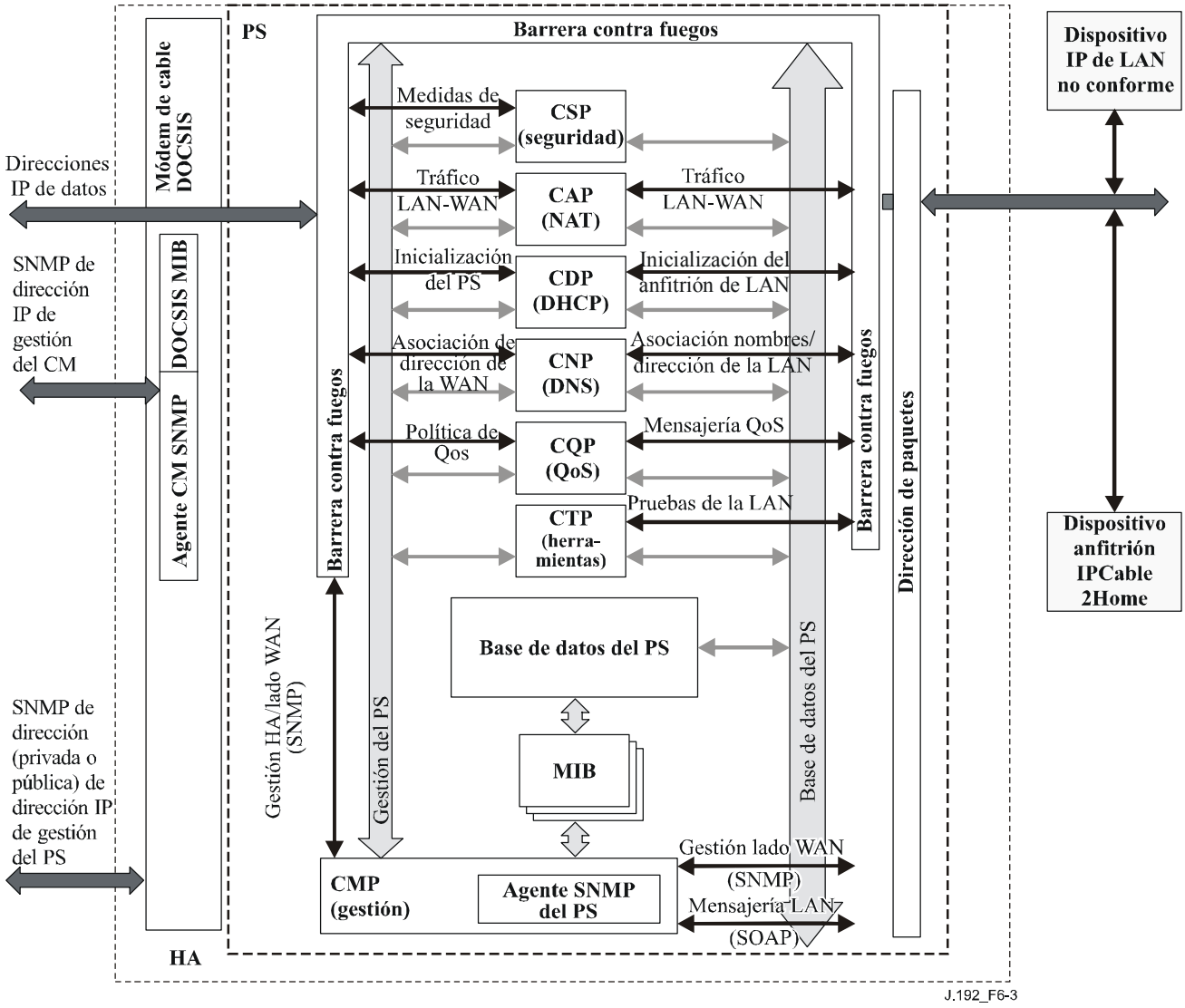


Figura 6-3/J.192 – Diagrama de bloques del PS

Las herramientas de gestión del NMS emplean SNMP para acceder al PS y gestionar objetos en el mismo. Si el PS está funcionando en el modo de coexistencia SNMPv3, el protocolo SNMPv3 ofrece al PS autenticación del usuario a través del operador del NMS, acceso basado en vistas a los objetos de la base de información de gestión (MIB) en el PS y criptación de los mensajes de gestión en el caso de que se solicite.

La función del agente SNMP del CMP tiene la tarea de hacer corresponder el ID del objeto (OID) y el ejemplar del OID en todas las hojas de los bloques funcionales del PS, como es el caso del CAP o la memoria local tal como la base de datos del PS.

Un operador del NMS de la red de datos por cable puede acceder o "gestionar" anfitriones IPCable2Home de dos maneras. De un lado, accediendo directamente a los anfitriones IPCable2Home utilizando direcciones de transferencia entre la red de cable y el elemento del dispositivo LAN (BP) que va a gestionarse. De otra parte, también puede acceder a los atributos del perfil del dispositivo BP a través de la MIB PSDev en el PS y a una lista de aplicaciones del BP y a sus prioridades a través de la MIB de QoS en el PS. El operador del sistema de cable accede a estas MIB a través de una petición de establecimiento (set) de SNMP o de mensajes de petición de obtención (get) de SNMP emitidos a la dirección IP de la WAN-Man del PS y el PS, fungiendo como apoderado de gestión, accede a un BP utilizando SOAP/HTTP. El operador del sistema de

cable puede aportar la política de QoS en el PS, en forma de prioridades de QoS para las aplicaciones del anfitrión IPCable2Home, a través de SNMP.

6.3.3.1.4 Requisitos de la función de agente SNMP

El PS DEBE implementar un agente SNMP conforme a las normas RFC del IETF, como se indica en 6.3.3.1.4.1, Requisitos del protocolo SNMP.

Cuando funciona en el modo de configuración DHCP o SNMP (cabhPsDevProvMode = dhcpmode(1) o snmpmode(2)), el agente SNMP en el PS DEBE recibir y procesar exclusivamente mensajes SNMP dirigidos a su dirección IP procedentes de la WAN y dirigidos a su dirección IP WAN-Man.

Cuando funciona en el modo de configuración DHCP o SNMP (cabhPsDevProvMode = dhcpmode(1) o snmpmode(2)), y si el modo de tratamiento de paquetes primario es NAPT o NAT (cabhCapPrimaryMode = napt(1) o nat(2)), el agente SNMP en el PS DEBE recibir y procesar exclusivamente todos los mensajes SNMP procedentes de la LAN y dirigidos a la dirección del encaminador del servidor CDP del lado LAN (cabhCdpServerRouter).

Cuando funciona en el modo de configuración DHCP o SNMP (cabhPsDevProvMode = dhcpmode(1) o snmpmode(2)), y si el modo de tratamiento de paquetes primario es transferencia (Passthrough) (cabhCapPrimaryMode = passthrough(3)), el agente SNMP del PS DEBE recibir y procesar exclusivamente mensajes SNMP de la LAN dirigidos a su dirección IP de LAN del PS bien conocida de su lado LAN (192.168.0.1).

Cuando funciona en el modo CableHome aletargado (cabhPsDevProvMode = dormantCHmode(3)) y esafePsCableHomeModeStatus = dormantCHMode(3) [Rec. UIT-T J.126], el agente SNMP del PS DEBE ignorar todos los mensajes SNMP de la WAN y DEBE recibir y procesar exclusivamente mensajes SNMP pocedentes de la LAN dirigidos a su dirección del encaminador del servidor CDP del lado LAN (cabhCdpServerRouter)

El PS DEBE ignorar los mensajes SNMP que se reciban a través de cualquier interfaz LAN dirigidos a la dirección IP de la WAN-Man del PS.

En el caso de un PS que resida conjuntamente con un módem de cable integrado, es decir, un PS integrado, el PS y el módem de cable DEBEN responder a direcciones IP de gestión distintas e independientes.

El PS DEBE implementar tipos de mensajes de eco y de respuesta de eco de ICMP (tipo 8 y tipo 0) como se describe en [RFC 792], y responder adecuadamente a las peticiones Ping que se reciban por cualquier interfaz.

Si el PS se encuentra funcionando en el modo de configuración DHCP (indicado mediante un valor '1' en cabhPsDevProvMode) DEBE emplear por omisión SNMPv1/v2c para los mensajes de gestión con el NMS y seguir las reglas de los modos NmAccess y de coexistencia que se describen en 6.3.3.1.4.2.1, Modos de gestión de red para un PS que funciona en el modo de configuración DHCP.

Si el PS se encuentra funcionando en el modo de configuración SNMP (indicado por un valor '2' en el objeto cabhPsDevProvMode de la MIB), DEBE utilizar el protocolo SNMPv3 para los mensajes de gestión con el NMS, observando las reglas descritas en 6.3.3.1.4.3, Modo de gestión de red para un PS que funciona en el modo de configuración SNMP.

Si el PS se encuentra funcionando en el modo de coexistencia SNMP, el valor por defecto de la autorización final DEBE ser Administrador de la red WAN (CHAdministrator).

El PS DEBE incluir – en el orden que se especifica más adelante – la versión de hardware, el nombre del fabricante, la versión de la copia imagen de la memoria ROM de arranque, la versión de software y el número de modelo en el objeto sysDescr (según [RFC 3418]). El formato de la información específica incluida en sysDescr DEBE ser conforme con el cuadro 6-6:

Cuadro 6-6/J.192 – Formato de los campos sysDescr

Informar	Formato de cada uno de los campos
Versión de hardware	HW_REV: <versión de hardware>
Nombre del fabricante	VENDOR: <nombre del fabricante>
Memoria ROM de arranque	BOOTR: <versión de la ROM de arranque>
Versión de software	SW_REV: <versión de software>
Número de modelo	MODEL: <número de modelo>

El objeto sysDescr DEBE constar de una lista de cinco pares tipo/valor indicados entre corchetes angulares. La separación entre el tipo y el valor es ": ", es decir dos puntos y un espacio. Por ejemplo, un objeto sysDescr de un PS del fabricante X, con versión de hardware 5.2, versión de la memoria ROM de arranque 1.4, versión de software 2.2, y número de modelo X se representaría de la siguiente manera:

cualquier texto<<HW_REV: 5.2, VENDOR: X; BOOTR: 1.4;
SW_REV: 2.2; MODEL: X>> cualquier texto

El PS DEBE informar en el objeto sysDescr toda la información necesaria para determinar qué versiones de software y de política de la barrera contra fuegos son susceptibles de cargarse en el PS. Si algunos campos del objeto sysDescr no pueden aplicarse, el PS DEBE informar el valor "NINGUNO (NONE)". Por ejemplo, un PS sin BOOTR informará "BOOTR: NONE".

El valor del objeto de la MIB docsDevSwCurrentVers DEBE contener la misma información de versión de software que la incluida en la misma información correspondiente al objeto sysDescr.

Cuando un PS y un CM están integrados en el mismo dispositivo, los objetos sysDescr y docsDevSwCurrentVers del PS DEBEN informar los mismos valores que los del CM.

El objeto sysObjectID del grupo de sistema MIB-2 [RFC 3418] DEBE implementarse y mantenerse durante los ciclos de reinicialización y conexión de la alimentación del dispositivo.

El objeto sysUpTime del grupo de sistema MIB-2 [RFC 3418] DEBE implementarse. Este objeto representa el tiempo transcurrido desde la reinicialización del sistema.

El objeto sysContact del grupo de sistema MIB-2 [RFC 3418] DEBE implementarse y mantenerse durante los ciclos de reinicialización y conexión de la alimentación del dispositivo. Este objeto devuelve el nombre del usuario o del administrador del sistema si se conoce.

El objeto sysLocation del grupo de sistema MIB-2 [RFC 3418] DEBE implementarse y mantenerse durante los ciclos de reinicialización y conexión de la alimentación del dispositivo.

El objeto sysServices del grupo de sistema MIB-2 [RFC 3418] DEBE implementarse y mantenerse durante los ciclos de reinicialización y conexión de la alimentación del dispositivo.

El objeto sysName del grupo del sistema de la MIB-2 [RFC 3418] DEBE implementarse y mantenerse durante los ciclos de reinicialización y conexión de la alimentación del dispositivo. La consulta a sysName devuelve el nombre del sistema.

La MIB del grupo de interfaces [RFC 2863] DEBE implementarse conforme al anexo A y a los requisitos expuestos en 6.3.3.1.4.8.

El grupo SNMP de la MIB-2 [RFC 3418] DEBE implementarse.

El objeto snmpSetSerialNo del grupo snmpSet [RFC 3418] DEBE implementarse. Este objeto es un bloqueo consultivo que permite la cooperación de varias entidades SNMPv2, todas desempeñando un papel gestor, para la utilización de la operación del conjunto SNMPv2.

El PS DEBE contar los octetos de LAN a WAN y de WAN a LAN según como se define en cabhPsDevLanIpTrafficTable [véase E.4], conforme al valor de cabhPsDevLanIpTrafficEnabled [véase E.4].

Cuando los objetos MIB del elemento PS se ponen a los valores de fábrica por defecto utilizando los objetos MIB cabhCapSetToFactory, cabhCdpSetToFactory, cabhCtpSetToFactory o cabhPsDevSetToFactory la funcionalidad del PS correspondiente DEBE utilizar esos valores por defecto para el funcionamiento sin tener que reconfigurar el elemento PS.

6.3.3.1.4.1 Requisitos del protocolo SNMP

El PS DEBE respetar o implementar, según proceda, las siguientes normas RFC del IETF:

- "A Simple Network Management Protocol" [RFC 1157].

  NOTA 1 – Esta norma RFC fue denominada "histórica" en [RFC 3410]. El PS debe soportar SNMPv1.

- "Introduction to Community-based SNMPv2" [RFC 1901].

  NOTA 2 – Esta norma RFC fue denominada "histórica" en [RFC 3410]. El PS debe soportar el protocolo SNMPv2c.

- "Introduction and Applicability Statements for Internet Standard Management Framework" [RFC 3410].
- "An Architecture for Describing Simple Network Management Protocol Management Frameworks" [RFC 3411].
- "Message Processing and Dispatching for SNMP" [RFC 3412].
- "Simple Network Management Applications" [RFC 3413].
- "User-based Security Model (USM) for version 3 of the Simple Network Management Protocol" [RFC 3414].
- "View-based Access Control Model (VACM) for the Simple Network Management Protocol" [RFC 3415].
- "Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)" [RFC 3416].
- "Transport Mappings for the Simple Network Management Protocol" [RFC 3417].
- "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)" [RFC 3418].
- "Coexistence between Version 1, Version 2, and Version 3 of the Internet-Standard Network Management Framework" [RFC 3584].

A efectos de soporte de SMIv2, el PS DEBE implementar las siguientes normas RFC del IETF:

- "Structure of Management Information Version 2 (SMIv2)" [RFC 2578].
- "Textual Conventions for SMIv2" [RFC 2579].
- "Conformance Statements for SMIv2" [RFC 2580].

6.3.3.1.4.2 Requisitos del modo de gestión de red

En la cláusula 5.5 se introducen dos modos de configuración (modo de configuración DHCP y modo de configuración SNMP) y dos modos de gestión de red (modo conforme a NmAccessTable y modo de coexistencia SNMPv3) que deben ser soportados por el PS. En las

cláusulas 7.3.3.1 y 7.3.3.2 se dan detalles adicionales con relación al funcionamiento del PS en cada uno de los dos modos de configuración, además del modo de operación CableHome aletargado.

En esta cláusula se describen las reglas para los modos de gestión de red que debe soportar el PS. En la cláusula 6.3.3.1.4.2.1 se describen los modos de gestión de red para un PS que funciona en el modo de configuración DHCP. En la cláusula 6.3.3.1.4.3 se describen los modos de gestión de red para un PS que funciona en el modo de configuración SNMP.

El PS puede funcionar en el modo de gestión de red de coexistencia SNMPv3, sin tener en cuenta si se configuró para funcionar en el modo de configuración DHCP o en el modo de configuración SNMP. Por defecto, funcionará en el modo de coexistencia SNMPv3 cuando utilice el modo de configuración SNMP. Si funciona en el modo de configuración DHCP, el PS pasará por defecto a funcionar en el modo de gestión de red conforme a NmAccessTable, pero puede configurarse para funcionar en el modo de coexistencia de SNMPv3.

El control del acceso a las MIB implementado por el PS depende del modo de gestión de red en el que se haya configurado el funcionamiento del PS. Si el PS se ha configurado para funcionar en el modo de gestión de red conforme a NmAccesTable, el acceso a la MIB se controla mediante escritura a docsDevNmAccessTable [RFC 2669]. Si por el contrario funciona en el modo de coexistencia SNMPv3, el acceso a las MIB se controla mediante los cuadros de SNMPv3 ([RFC 3584], [RFC 3413], [RFC 3414] y [RFC 3415]). Estos cuadros podrán ser configurados por el NMS a través de instrucciones de establecimiento (set) de SNMP, o bien mediante el fichero de configuración del PS. En la cláusula 6.3.3.1.4.6, Correspondencia de los campos TLV con las filas del cuadro SNMPv3 creado, se describe cómo se hacen corresponder los parámetros de configuración del fichero de configuración del PS con esos cuadros de SNMPv3.

6.3.3.1.4.2.1 Modos de gestión de red de un PS que funciona en el modo de configuración DHCP

El PS DEBE soportar la coexistencia de SNMPv1, SNMPv2c y SNMPv3 y SNMP según se describe en [RFC 3411] a [RFC 3415] y [RFC 3584]. Además, el PS DEBE aceptar el modo NmAccessTable conforme a [RFC 2669]. El soporte de los modos de gestión de red de un PS que funciona en el modo de configuración DHCP está sujeto a las directrices que se describen en 6.3.3.1.4.2.2, 6.3.3.1.4.3 y 6.3.3.1.4.4.

6.3.3.1.4.2.2 Funcionamiento básico de un PS que funciona en el modo de configuración DHCP

El funcionamiento inicial del PS configurado en el modo de configuración DHCP puede considerarse que consta de tres etapas: 1) comportamiento del PS después de su configuración para el modo de configuración DHCP, pero antes de que se haya configurado el modo de gestión de red a través del fichero de configuración del PS; 2) determinación del modo de gestión de red; y 3) comportamiento del PS tras haberse configurado su modo de gestión de red. Las reglas de funcionamiento de cada una de estas etapas son:

1) Una vez configurado el PS para funcionar en el modo de configuración DHCP (indicado mediante un valor de '1' para cabhPsDevProvMode (DHCPmode)), pero antes de que se haya configurado para el modo de gestión de red, el PS DEBE funcionar como se indica a continuación:
   - Se descartan todos los paquetes SNMP.
   - Ninguna de las MIB de SNMPv3 (Community MIB, TARGET-MIB, VACM-MIB, USM-MIB, NOTIFICATION-MIB) serán accesibles al gestor de SNMP en el NMS.
   - Ninguno de los elementos en SNMP-USM-DH-OBJECTS-MIB será accesible al gestor de SNMP en el NMS.

- El fichero de configuración del PS especificado en DHCP OFFER se descarga y se procesa.
- Se DEBERÁ completar el procesamiento satisfactorio de todos los elementos de la MIB en el fichero de configuración del PS antes de dar comienzo al cálculo de los valores públicos en el cuadro usmDHKickstart.

2) Si un PS se encuentra funcionando en el modo de configuración DHCP, el contenido de fichero de configuración del PS determinará el modo de gestión de red, según se describe a continuación:

- El PS se encontrará en el modo SNMPv1/v2c docsDevNmAccess si el fichero de configuración del PS incluye ÚNICAMENTE el valor del cuadro docsDevNmAccess para el control de acceso al SNMP.
- Si el fichero de configuración del PS no incluye elementos de control de acceso al SNMP (docsDevNmAccessTable o snmpCommunityTable o TLV 34.1/34.2 o TLV 38), en ese caso el PS se encontrará en el modo NmAccess.
- Si el fichero de configuración del PS incluye el valor snmpCommunityTable y/o los tipos 34.1/34.2 de TLV y/o el tipo 38 de TLV, en ese caso el PS se encontrará en el modo de coexistencia de SNMP. Por lo tanto, cualquier intento de anotación al cuadro docsDevNmAccessTable será ignorado.

3) Tras completar el proceso de configuración que se describe en 13.2 (indicado mediante el valor 'pass' (1) en cabhPsDevProvState), el PS funcionará en uno de los dos modos de gestión de red. Este modo se determinará mediante el contenido del fichero de configuración del PS, como se describió anteriormente. A continuación se presentan las reglas de funcionamiento del PS para cada uno de los dos modos de gestión de red:

Modo NmAccess utilizando SNMPv1/v2c

- El PS DEBE procesar los paquetes SNMPv1/v2c y descartar los paquetes SNMPv3.
- docsDevNmAccessTable controla el acceso y los destinos de las trampas como se describe en [RFC 2669]. El PS que funcione en el modo de gestión de red NmAccess DEBE hacer cumplir la política de acceso a gestión, como se define en el cuadro NmAccess, para cualquier acceso a los objetos de la MIB específicos de IPCable2Home, sin tener en cuenta la interfaz (como por ejemplo, una interfaz gráfica de usuario, GUI, específica de un fabricante) o el protocolo de acceso que se utilicen.
- No se dispondrá de acceso a ninguna de las MIB de SNMPv3 (Community MIB, TARGET-MIB, VACM-MIB, USM-MIB, NOTIFICATION-MIB).

Si el PS se encuentra funcionando en el modo SNMP v1/v2c NmAccess DEBE disponer de la capacidad para enviar trampas conforme lo especifique el siguiente objeto de la MIB (extensión MIB propuesta para el cuadro docsDevNmAccess):

```
DocsDevNmAccessTrapVersion OBJECT-TYPE
     SYNTAX INTEGER {
               DisableSNMPv2trap(1),
               EnableSNMPv2trap(2),
                }
     MAX-ACCESS read-create
     STATUS current
     DESCRIPTION
          "Specifies the TRAP version that is sent to this NMS. Setting
          this object to disableSNMPv2trap(1) causes the trap in SNMPv1
          format to be sent to particular NMS. Setting this object to
          EnableSNMPv2trap(2) causes the trap in SNMPv2 format be sent to
          particular NMS" DEFVAL { DisableSNMPv2trap }
     ::={docsDevNmAcessEntry 8}
```

Modo de coexistencia utilizando SNMPv1/v2c/v3

Durante el modo de coexistencia SNMPv3, el PS DEBE soportar los requisitos "Inicialización de SNMPv3" y "Modificaciones de claves DH " especificados en 11.4.4.1.3 y 11.4.4.1.4. Esos requisitos incluyen el cálculo de los parámetros públicos del cuadro de arranque (Kickstart) Diffie-Hellman de USM. Las siguientes reglas para el funcionamiento del PS se aplican durante el cálculo de los parámetros públicos (valores) y después del mismo como se indica:

Durante el cálculo de los valores públicos usmDHKickstartTable:

- El PS NO DEBE permitir ningún acceso SNMP desde la red WAN.
- El PS PUEDE seguir permitiendo el acceso desde la red LAN con las limitaciones configuradas por la MIB de USM, MIB comunitaria y VACM-MIB.

Después del cálculo de los valores públicos usmDHKickstartTable:

- El PS DEBE enviar la trampa de arranque en frío o de arranque en caliente indicando que ya es gestionable plenamente con SNMPv3.
- Los paquetes SNMPv1/v2c/v3 se procesan según lo descrito en [RFC 3411], [RFC 3412], [RFC 3413], [RFC 3414], [RFC 3415] y [RFC 3584].
- No se puede acceder a docsDevNmAccessTable.
- snmpCommunityTable, Notification MIB, Target MIB, VACM-MIB y USM-MIB determinan el control de acceso y los destinos de las trampas. El PS DEBE hacer cumplir la política de acceso a la gestión, según lo determine la vista VACM configurada por el operador del sistema de cable para cualquier acceso a los objetos MIB específicos de IPCable2Home, sin tener en cuenta la interfaz (como por ejemplo, una interfaz gráfica de usuario, GUI, específica de un fabricante) o el protocolo de acceso que se utilicen.
- La Community MIB controla la traducción de la cadena comunitaria de paquetes SNMPv1/v2c al nombre de seguridad que selecciona las anotaciones en la MIB de USM. El control de acceso es responsabilidad de la MIB de VACM.
- La MIB de USM y la MIB de VACM controlan los paquetes SNMPv3.
- Los destinos de las trampas se especifican en la MIB objetivo y en la MIB de notificación.

En el caso de un fallo que no permita completar la inicialización de SNMPv3 de un usuario (es decir, el NMS no puede acceder al PS a través de la PDU de SNMPv3), el cuadro de usuario USM de ese usuario DEBERÁ suprimirse, el PS se encontrará en el modo de coexistencia y permitirá el acceso con SNMPv1/v2c únicamente si las anotaciones en la MIB comunitaria (y anotaciones conexas) están configuradas.

6.3.3.1.4.3 Modo de gestión de red de un PS que funciona en el modo de configuración SNMP

Si el PS se encuentra funcionando en el modo de configuración SNMP tras la recepción de un mensaje DHCP ACK (indicado mediante el valor '2' (SNMPmode) para cabhPsDevProvMode), funcionará en el modo de coexistencia SNMPv3 utilizando SNMPv3 por defecto para el intercambio de mensajes de gestión con el NMS, y empleando Kerberos para el intercambio de material importante con el KDC, apegándose a las reglas descritas en esta cláusula. De la misma manera que cuando el PS se encuentra funcionando en el modo de configuración DHCP y ha sido configurado para el modo de gestión de red de coexistencia de SNMPv3, si el PS se encuentra funcionando en el modo de configuración SNMP y en el modo de gestión de red de coexistencia de SNMPv3 es necesario que ignore los intentos de configuración de docsDevNmAccessTable.

6.3.3.1.4.4 Vistas de gestión

Los controles de gestión definidos para IPCable2Home se encuentran en la función CMP del PS. Los valores, basados en el modo de gestión, definen los derechos de acceso que se conceden a un usuario para acceder a la base de datos de los servicios de portal, a través de las MIB específicas de IPCable2Home mediante SNMP desde las interfaces del encaminador del servidor de la LAN o de WAN-Man del PS. Mediante la presente Recomendación se define un usuario único.

El concepto de las vistas de gestión se introdujo con SNMPv3 y se definió en [RFC 3410] a [RFC 3415] y en [RFC 3584]. Se trata de un método para especificar que usuarios están autorizados para acceder a cuales objetos de la MIB.

En la figura 6-4 se ilustran algunas vistas de gestión posibles para el PS. En esta Recomendación se definen una vista de administrador de la WAN (vista CHAdministrator) y un usuario administrador de la WAN (usuario CHAdministrator). Es posible establecer otras vistas y usuarios, como es el caso de la vista de mantenimiento de la WAN, la vista del administrador de la LAN o la vista del usuario de la LAN mediante la autorización final (CHAdministrator), siguiendo las reglas definidas en [RFC 3414] y [RFC 3415].

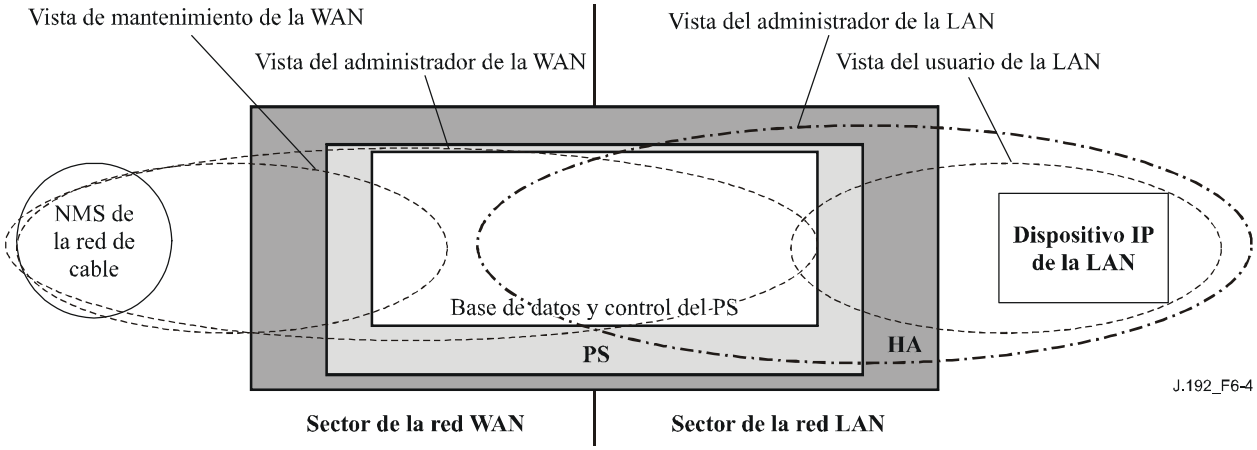


Figura 6-4/J.192 – Vistas de gestión

Los parámetros gestionados que define IPCable2Home se almacenan en la base de datos del PS. Como se muestra en la figura 6-4, hay un concepto de vistas de acceso en la base de datos y el control del PS, que permite la gestión simultánea de las redes LAN y WAN al definir vistas de gestión en la base de datos y en el control del PS. Las vistas son un mecanismo que da privacidad y seguridad, y la política puede establecerse independientemente del usuario CHAdministrator.

La autorización final (usuario CHAdministrator) tiene sus propios identificadores de usuarios y claves, y las siguientes responsabilidades:

- Establecimiento de todas las vistas de acceso en las interfaces de gestión de las redes LAN y WAN.
- Creación y gestión de todos los perfiles de usuarios incluidos los identificadores de usuarios, las claves y los privilegios de acceso a la base de datos del PS.
- Determinación de la política de acceso en los lados de las redes LAN y WAN.

Las descripciones del modo de funcionamiento del modelo de control de acceso basado en vistas y del modelo de seguridad basado en el usuario pueden encontrarse en las normas [RFC 3414] y [RFC 3415].

La vista CHAdministrator permite el acceso pleno de lectura y de escritura a todas las MIB especificadas por IPCable2Home.

Los requisitos de la vista de gestión se especifican en 6.3.3.1.4.5.

6.3.3.1.4.4.1 Control de acceso a la red WAN

IPCable2Home define dos métodos para controlar el acceso a parámetros gestionables a través de las MIB definidas para IPCable2Home. Mediante docsDevNmAccessTable [RFC 2669] se define el acceso de gestión cuando el PS funciona en el modo de gestión de red NmAccess (véase 6.3.3.1.4.2.2). Cuando el PS funciona en el modo de gestión de red de coexistencia SNMPv3 (véase 6.3.3.1.4.2.2), en el modelo de seguridad del usuario (USM) [RFC 3414] y en el modelo de control de acceso basado en vistas (VACM) [RFC 3415], se utilizan los valores del cuadro para controlar el acceso a objetos MIB especificados para IPCable2Home, con independencia de la interfaz (como por ejemplo, una interfaz gráfica de usuario) a través de la que se recibe la petición. El VACM define un conjunto de servicios que pueden utilizarse para verificar los derechos de acceso. Los grupos VACM definen los derechos de acceso al CMP.

Como se define en la sección 2.4 de [RFC 3415], una "vista de MIB" es un conjunto particular de tipos de objetos gestionados que se puede definir, que se emplea en IPCable2Home para soportar la gestión de la red WAN del PS. El acceso al usuario CHAdministrator y su vista se determina en 11.4.4.1.3 y 6.3.3.1.4.5. En 12.3.1 se da un ejemplo de la secuencia del acceso a la base de datos del PS desde la interfaz WAN.

6.3.3.1.4.4.2 Seguridad

El SNMPv3 proporciona la seguridad de los mensajes de gestión. En la cláusula 11 figura una descripción detallada de la utilización de SNMPv3. El CMP puede utilizar SNMP v3 para contrarrestar las amenazas identificadas en el anexo C.

Como protección contra los ataques de reproducción, se utiliza un reloj en tiempo real que asigna sellos de tiempo a los mensajes. En 11.4 se especifican los requisitos de seguridad de los mensajes de gestión.

6.3.3.1.4.5 Requisitos del modelo de control de acceso basado en vistas (VACM)

Para lograr el acceso controlado a la información de gestión y la creación de distintos sectores de gestión para un PS que funciona en el modo de coexistencia SNMP v3, DEBE emplearse el modelo de control de acceso basado en vistas (VACM) que se define en [RFC 3415].

La vista de administrador de la red WAN DEBE implementarse en un elemento de servicios de portal conforme. Las vistas por defecto distintas de la vista de administrador de la red WAN NO DEBEN estar a disposición del PS. PODRÁN crearse otras vistas mediante la autorización final a través del NMS de la red de cable al configurar la MIB de VACM.

La especificación del usuario para la vista de administrador de la red WAN DEBE implementarse de la siguiente manera:

vacmSecurityModel	3 (USM)
vacmSecurityName	'CHAdministrator'
vacmGroupName	'CHAdministrator'
vacmSecurityToGroupStorageType	permanent
vacmSecurityToGroupStatus	active

La especificación de grupo de la vista CHAdministrator DEBE implementarse como se indica a continuación:

CHAdministrator Group	
vacmGroupName	'CHAdministrator'
vacmAccessContextPrefix	"

vacmAccessSecurityModel	3 (USM)
vacmAccessSecurityLevel	AuthPriv
vacmAccessContextMatch	exact
vacmAccessReadViewName	'CHAdministratorView'
vacmAccessWriteViewName	'CHAdministratorView'
vacmAccessNotifyViewName	'CHAdministratorView'
vacmAccessStorageType	permanent
vacmAccessStatus	active

La vista VACM para la vista CHAdministrator DEBE implementarse como se indica a continuación:

CHAdministratorView subtree 1.3.6.1 (Entire MIB)

6.3.3.1.4.6 Correspondencia de campos TLV con filas del cuadro SNMPv3 creado

En esta cláusula se dan los pormenores de cómo se establece la correspondencia del elemento del fichero de configuración *receptor de notificación del SNMP* (tipo 38 de TLV) con los cuadros funcionales de SNMPv3. Véase 7.4.4.1.10, Receptor de notificación SNMP, para encontrar una descripción del parámetro de configuración TLV tipo 38. En 11.4.4.2.2 se presentan los pormenores del intercambio de las claves de inscripción para el funcionamiento con SNMP v3.

El PS, al recibir un elemento tipo 38 del fichero de configuración, DEBE efectuar anotaciones en el cuadro de la MIB según el procedimiento descrito en los cuadros 6-7, snmpNotifyTable a 6-16, vacmSecurityToGroupTable, empleando para tal efecto los valores transferidos en el TLV como se describe más adelante. Como referencia a continuación se relacionan los cuadros MIB que el PS debe rellenar cuando recibe un elemento tipo 38 de fichero de configuración:

- snmpNotifyTable;
- snmpTargetAddrTable;
- snmpTargetAddrExtTable;
- snmpTargetParamsTable;
- snmpNotifyFilterProfileTable;
- snmpNotifyFilterTable;
- snmpCommunityTable;
- usmUserTable;
- vacmSecurityToGroupTable;
- vacmAccessTable;
- vacmViewTreeFamilyTable.

Un fichero de configuración de PS puede incluir elementos MIB de TLV (tipo 28) que efectúan anotaciones en cualquiera de los 11 cuadros antes relacionados.

En esta cláusula, los cuadros muestran la colocación de los campos del elemento TLV del fichero de configuración del PS (rótulos encerrados en corchetes angulares <>) en los cuadros SNMP V3.

A continuación se muestra la correspondencia entre los campos TLV y los rótulos <TAG> del cuadro:

PS<IP Address> TLV 38.1

<Port> TLV 38.2

<Trap type> TLV 38.3

<Timeout> TLV 38.4

<Retries> TLV 38.5

<Filter OID> TLV 38.6

<Security Name> TLV 38.7

Estos cuadros se muestran en el mismo orden en el que el agente los examinará cuando se genere una notificación, a fin de determinar a quién se deberá enviar y cómo se debe rellenar el contenido del paquete de notificación.

snmpNotifyTable

Crea dos filas con valores fijos, si están presentes uno o más de los elementos TLV.

Cuadro 6-7/J.192 – snmpNotifyTable [RFC 3413]

SNMP-NOTIFICATION-MIB	Primera fila	Segunda fila
Nombre de columna (* = parte del índice)	Valor de la columna	Valor de la columna
* snmpNotifyName	"@PSconfig_inform"	"@PSconfig_trap"
snmpNotifyTag	"@PSconfig_inform"	"@PSconfig_trap"
snmpNotifyType	inform(2)	trap(1)
snmpNotifyStorageType	volátil	volátil
snmpNotifyRowStatus	active(1)	active(1)

snmpTargetAddrTable

Crea una fila por cada elemento TLV en el fichero de configuración del PS.

Cuadro 6-8/J.192 – snmpTargetAddrTable [RFC 3413]

SNMP-TARGET-MIB	Nueva fila
Nombre de columna (* = parte del índice)	Valor de columna
* snmpTargetAddrName	"@PSconfig_n", donde n va de 0 a m – 1, y m es el número de elementos TLV del receptor de notificaciones en el fichero de configuración del PS
snmpTargetAddrTDomain	snmpUDPDomain – snmpDomains
snmpTargetAddrTAddress (dirección IP y puerto UDP del receptor de notificaciones)	CADENA DE OCTETOS (6) Octetos 1-4: <IP Address> Octetos 5-6: <Port>
snmpTargetAddrTimeout	<Timeout> desde el TLV
snmpTargetAddrRetryCount	<Retries> desde el TLV
snmpTargetAddrTagList	Si <Trap type> == 1, 2 ó 4 "@PSconfig_trap" De lo contrario, si <Trap type> = 3 ó 5 "@PSconfig_inform"
snmpTargetAddrParams	"@PSconfig_n" (mismo valor de snmpTargetAddrName)
snmpTargetAddrStorageType	volátil
snmpTargetAddrRowStatus	active(1)

snmpTargetAddrExtTable

Crea una fila por cada elemento TLV en el fichero de configuración del PS.

Cuadro 6-9/J.192 – snmpTargetAddrExtTable [RFC 3584]

SNMP-COMMUNITY MIB	Nueva fila
Nombre de columna (* = parte del índice)	Valor de columna
* snmpTargetAddrName	"@PSconfig_n", donde n va de 0 a m –1, y m es el número de elementos TLV del receptor de notificaciones en el fichero de configuración del PS
snmpTargetAddrMask	<zero length octet string>
snmpTargetAddrMMS	0

snmpTargetParamsTable

Crea una fila por cada elemento TLV en el fichero de configuración. Si <Trap type> es 1, 2 ó 3, o si el campo <Security Name> tiene longitud cero, crea el cuadro de la siguiente manera:

Cuadro 6-10/J.192 – snmpTargetParamsTable para <Trap Type> 1, 2 ó 3 [RFC 3413]

SNMP-TARGET-MIB	Nueva fila
Nombre de columna (* = parte del índice)	Valor de columna
* snmpTargetParamsName	"@PSconfig_n", donde n va de 0 a m –1, y m es el número de elementos TLV del receptor de notificaciones en el fichero de configuración del PS
snmpTargetParamsMPModel SYNTAX: SnmpMessageProcessingModel	Si <Trap type> = 1 SNMPv1(0) De lo contrario, si <Trap type> = 2 ó 3 SNMPv2c(1) De lo contrario, si <Trap type> = 4 ó 5 SNMPv3(3)
snmpTargetParamsSecurityModel SYNTAX: SnmpSecurityModel	Si <Trap type> = 1 SNMPv1(1) De lo contrario, si <Trap type> = 2 ó 3 SNMPv2c(2) De lo contrario, si <Trap type> = 4 ó 5 USM(3) NOTA – Las correspondencias entre los tipos de protocolo SNMP y el valor en este cuadro difieren de snmpTargetParamsMPModel.
snmpTargetParamsSecurityName	"@PSconfig"
snmpTargetParamsSecurityLevel	noAuthNoPriv
snmpTargetParamsStorageType	volátil
snmpTargetParamsRowStatus	active(1)

Si <Trap type> es 4 ó 5, y el campo <Security Name> tiene una longitud distinta de cero, se crea el cuadro de la siguiente manera:

Cuadro 6-11/J.192 – snmpTargetParamsTable para <Trap Type> 4 ó 5 [RFC 3413]

SNMP-TARGET-MIB	Nueva fila
Nombre de columna (* = parte del índice)	Valor de columna
* snmpTargetParamsName	"@PSconfig_n", donde n va de 0 a m –1, y m es el número de elementos TLV del receptor de notificaciones en el fichero de configuración del PS
snmpTargetParamsMPModel SYNTAX: SnmpMessageProcessingModel	Si <Trap type> = 1 SNMPv1(0) De lo contrario, si <Trap type> = 2 ó 3 SNMPv2c(1) De lo contrario, si <Trap type> = 4 ó 5 SNMPv3(3)
snmpTargetParamsSecurityModel SYNTAX: SnmpSecurityModel	If <Trap type> = 1 SNMPv1(1) De lo contrario, si <Trap type> = 2 ó 3 SNMPv2c(2) De lo contrario, si <Trap type> = 4 ó 5 USM(3) NOTA – La correspondencia de los tipos de protocolo SNMP al valor en este cuadro difieren de snmpTargetParamsMPModel.
snmpTargetParamsSecurityName	<Security Name>
snmpTargetParamsSecurityLevel	Nivel de seguridad de <Security Name>
snmpTargetParamsStorageType	volátil
snmpTargetParamsRowStatus	active(1)

snmpNotifyFilterProfileTable

Crea una fila por cada TLV que tenga un campo <Filter Length> distinto de cero.

Cuadro 6-12/J.192 – snmpNotifyFilterProfileTable [RFC 3413]

SNMP-NOTIFICATION-MIB	Nueva fila
Nombre de columna (* = Parte del índice)	Valor de columna
*snmpTargetParamsName	"@PSconfig_n", donde n va de 0 a m –1, y m es el número de elementos TLV del receptor de notificaciones en el fichero de configuración del PS
snmpNotifyFilterProfileName	"@PSconfig_n", donde n va de 0 a m –1, y m es el número de elementos TLV del receptor de notificaciones en el fichero de configuración del PS
snmpNotifyFilterProfileStorType	volátil
snmpNotifyFilterProfileRowStatus	active(1)

snmpNotifyFilterTable

Crea una fila por cada TLV que tenga un campo <Filter Length> distinto de cero.

Cuadro 6-13/J.192 – snmpNotifyFilterTable [RFC 3413]

SNMP-NOTIFICATION-MIB	Nueva fila
Nombre de columna (* = Parte del índice)	Valor de columna
* snmpNotifyFilterProfileName	"@PSconfig_n", donde n va de 0 a m –1, y m es el número de elementos TLV del receptor de notificaciones en el fichero de configuración del PS
* snmpNotifyFilterSubtree	<Filter OID> desde el TLV
snmpNotifyFilterMask	<Zero length octet string>
snmpNotifyFilterType	Included(1)
snmpNotifyFilterStorageType	volátil
snmpNotifyFilterRowStatus	active(1)

snmpCommunityTable

Crea una fila con valores fijos si están presentes 1 o más TLV. Esto provoca que las notificaciones SNMPv1 y v2c incluyan la cadena comunitaria en snmpCommunityName.

Cuadro 6-14/J.192 – snmpCommunityTable [RFC 3584]

SNMP-COMMUNITY-MIB	Nueva fila
Nombre de columna (* = Parte del índice)	Valor de columna
* snmpCommunityIndex	"@PSconfig"
snmpCommunityName	"public"
snmpCommunitySecurityName	"@PSconfig"
snmpCommunityContextEngineID	<The PS engineID>
snmpCommunityContextName	<Zero length octet string>
snmpCommunityTransportTag	<Zero length octet string>
snmpCommunityStorageType	volátil
snmpCommunityStatus	active(1)

usmUserTable

Crea una fila con valores fijos, si están presentes uno o más TLV. Se crea una fila cada vez que se determina el ID de la máquina de un receptor de trampas. Esto permite especificar el nombre de usuario de los receptores de notificaciones distantes para enviarles las notificaciones.

Se crea una fila en usmUserTable. A continuación, cuando se determina el ID de la máquina de cada receptor de notificaciones, el agente utiliza una copia de esta fila en una nueva fila y sustituye el valor 0x00 en la columna usmUserEngineID por el valor recién determinado.

Cuadro 6-15/J.192 – usmUserTable [RFC 3414]

SNMP-USER-BASED-SM-MIB	Nueva fila
Nombre de columna (* = Parte del índice)	Valor de columna
* usmUserEngineID	0
* usmUserName	"@PSconfig" Cuando se crean otras filas, ésta se sustituye por el campo <Security Name> del elemento TLV.
usmUserSecurityName	"@PSconfig" Cuando se crean otras filas, ésta se sustituye por el campo <Security Name> del elemento TLV.
usmUserCloneFrom	<don't care> – no es posible clonar esta fila
usmUserAuthProtocol	Ninguna. Cuando se crean otras filas, ésta se sustituye por Ninguna (None) o MD5, en función del nivel de seguridad del usuario v3.
usmUserAuthKeyChange	<don't care> – sólo escritura
usmUserOwnAuthKeyChange	<don't care> – sólo escritura
usmUserPrivProtocol	Ninguna. Cuando se crean otras filas, ésta se sustituye por Ninguna (None) o DES, en función del nivel de seguridad del usuario v3.
usmUserPrivKeyChange	<don't care> – sólo escritura
usmUserOwnPrivKeyChange	<don't care> – sólo escritura
usmUserPublic	<zero length string>
usmUserStorageType	volátil
usmUserStatus	active(1)

vacmSecurityToGroupTable

Crea tres filas con valores fijos, si están presentes uno o más TLV.

Se trata de las tres filas con valores fijos, que se emplean para las anotaciones de TLV con el campo <Trap Type> puesto a 1, 2 ó 3 o con un campo <Security Name>, de longitud cero.

Cuadro 6-16/J.192 – vacmSecurityToGroupTable [RFC 3415]

SNMP-VIEW-BASED-ACM-MIB	Primera fila	Segunda fila	Tercera fila
Nombre de columna (* = Parte del índice)	Valor de columna	Valor de columna	Valor de columna
* vacmSecurityModel	SNMPv1(1)	SNMPv2c(2)	USM(3)
* vacmSecurityName	"@PSconfig"	"@PSconfig"	"@PSconfig"
vacmGroupName	"@PSconfigv1"	"@PSconfigv2"	"@PSconfigUSM"
vacmSecurityToGroupStorageType	volátil	volátil	volátil
vacmSecurityToGroupStatus	active(1)	active(1)	active(1)

6.3.3.1.4.7 Requisitos de la MIB de IPCable2Home

El PS DEBE implementar cada uno de los objetos de la MIB que se relacionan en el anexo A. Si la columna "persistencia" de un objeto relacionado de la MIB en el anexo A indica el valor Sí, el PS DEBE conservar el valor del objeto durante los ciclos de energía eléctrica o los rearranques del PS, poniendo a disposición el mismo valor para efectos de acceso mediante un gestor de SNMP justo después de completar la configuración (cabhPsDevProvState = pass(1)), a continuación de un rearranque que estaba disponible para efectos de acceso mediante dicho gestor de SNMP justo antes del rearranque.

Los objetos MIB necesarios pertenecen a los siguientes documentos relativos a la MIB:

- MIB de grupo de interfaces [RFC 2863];
- MIB del dispositivo de cable DOCSIS [RFC 2669];
- MIB de definición de CableLabs (véase E.6);
- MIB PSDev de IPCable2Home [véase E.4];
- MIB de CAP de IPCable2Home [véase E.1];
- MIB de CDP de IPCable2Home [véase E.2];
- MIB de CTP de IPCable2Home [véase E.3];
- MIB de seguridad de IPCable2Home [véase E.5];
- MIB de QoS de IPCable2Home [véase E.7];
- [draft-ietf-ipcdn-bpiplus-mib-05];
- MIB IP (SNMPv2) [RFC 2011];
- MIB UDP (SNMPv2) [RFC 2013];
- Clave USM Diffie-Hellman [RFC 2786];
- MIB de dirección INET [RFC 3291];
- MIB IF de DOCS [RFC 2670];
- MIB ifType de IANA [IANAType];
- MIB IEEE 802.11 [802dot11MIB].

En una pasarela residencial de IPCable2Home o en cualquier otro dispositivo con un PS y un módem de cable integrados, las entidades de gestión del módem de cable y del PS (CMP) DEBEN reaccionar con direcciones IP de gestión distintas e independientes. En la Rec. UIT-T J.112 y en la presente Recomendación se especifican algunos de los mismos objetos de la MIB, pero si en el mismo dispositivo están integrados un módem de cable conforme a J.112 y un elemento PS conforme a IPCable2Home, se exige que cada uno mantenga su propio ejemplar independiente de objetos de la MIB específicos, que estarán accesibles a través de distintas direcciones IP de gestión, con excepción del grupo SNMP de MIB 2 y la MIB de SNMPv2, que PODRÁN ser comunes al módem de cable y al elemento de servicios de portal y compartirse entre ellos, y PODRÁ accederse a los mismos a través de la dirección IP de gestión del módem de cable o de la dirección IP de gestión del PS.

En el caso de un PS con un módem de cable integrado, la descarga de una copia imagen simple del software combinado del módem de cable y de los servicios de portal, se controla mediante el módem de cable. Los siguientes objetos de grupo docsDevSoftware [RFC 2669] NO DEBEN implementarse para un PS con un módem de cable integrado, es decir, esos objetos DEBEN ser accesibles únicamente a través de la dirección IP de gestión del módem de cable:

- docsDevSwServer;
- docsDevSwFilename;
- docsDevSwAdminStatus;
- docsDevSwOperStatus.

El grupo de objetos docsDevSoftware DEBE implementarse en un PS autónomo. La modificación de esos objetos (como se describe en 11.8.4) a través del operador del sistema de cable para fines de la descarga de la copia imagen del software del PS autónomo DEBE dar por resultado el funcionamiento adecuado de la descarga segura del software.

En el caso de un PS con un módem de cable integrado, los objetos de la MIB del módem de cable DEBEN estar visibles y accesibles únicamente cuando el gestor acceda a ellos a través de la dirección IP de gestión del módem de cable, y nunca a través de cualquier dirección IP de gestión del PS, con excepción del grupo SNMP de MIB-2 y de la MIB de SNMPv2 que están autorizados a compartirse entre las entidades de gestión del CM y el PS.

En el caso de un PS con un módem de cable integrado, los objetos de la MIB específicos de IPCable2Home DEBEN estar visibles y accesibles únicamente cuando el gestor accede a ellos a través de la dirección IP de gestión del PS (dirección IP de la WAN-Man del PS), o a través de la dirección IP del encaminador del servidor de la LAN del PS, y en ningún caso a través de la dirección IP de gestión del módem de cable, con excepción del grupo SNMP de MIB 2 y de la MIB de SNMPv2 que están autorizados a compartirse entre las entidades de gestión del CM y del PS.

En la figura 6-5 se ilustra la jerarquía genérica de la MIB. Los OID específicos necesarios para las MIB particulares se relacionan en el anexo A.

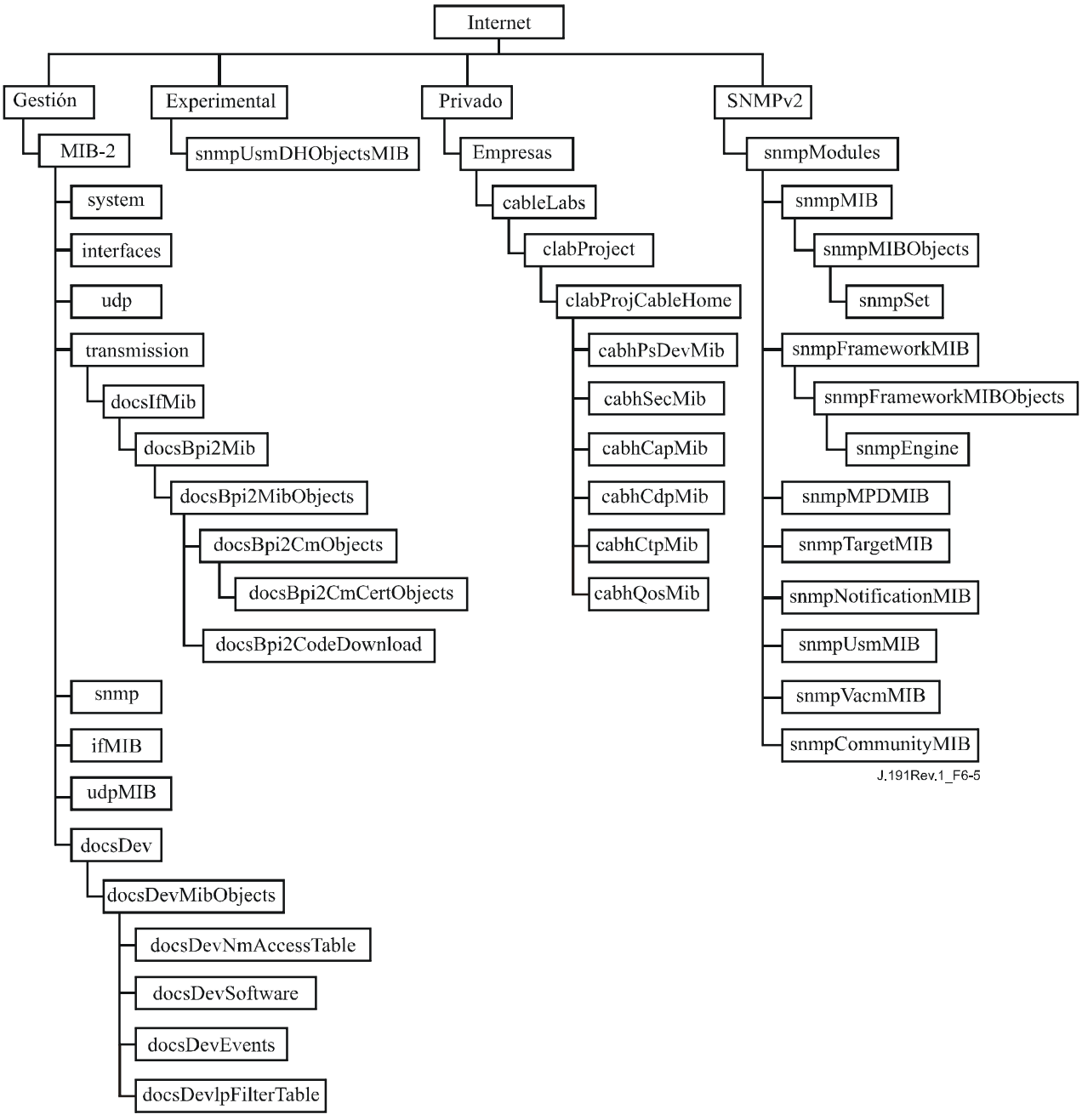


Figura 6-5/J.192 – Jerarquía de la MIB de IPCable2Home

6.3.3.1.4.8 MIB de grupo de interfaces

La MIB de grupo de interfaces [RFC 2863] representa una herramienta muy potente que permite a los operadores del sistema de cable conocer el estado de todas las interfaces físicas en el elemento de servicios de portal, así como examinar sus estadísticas correspondientes. Una *interfaz física* es aquella que dispone de un conector en el exterior del recinto del dispositivo, y cuyo objeto *ifConnectorPresent* es verdadero (true). A fin de facilitar la utilización adecuada de esta MIB, resulta indispensable un método de numeración de las interfaces. Por consiguiente, los elementos del PS tendrán que cumplir con los siguientes requisitos:

El PS DEBE implementar un ejemplar de ifEntry para la interfaz de WAN-Data del elemento PS, aún en el caso de que la interfaz sea interna, tal y como es el caso de un PS integrado que emplea un diseño de circuitos integrados.

El PS DEBE implementar un ejemplar de ifEntry por cada interfaz física de la LAN del elemento PS.

El PS DEBE implementar un ejemplar de ifEntry para una interfaz de "interfaces de LAN agregadas", que se identifican mediante el valor 255 de ifIndex.

El PS DEBE implementar un ejemplar de ifEntry para una interfaz (virtual) "Interfaz LAN radioeléctrica agregada" (virtual), que represente el superconjunto de todas las interfaces LAN radioeléctricas físicas implementadas sobre el producto e identificadas mediante el valor 254 de ifIndex.

Las interfaces ifTable del PS DEBEN numerarse como se indica en el cuadro 6-17.

Cuadro 6-17/J.192 – Numeración de interfaces en ifTable

Interfaz	Descripción
1	Interfaz de WAN-Man
2	Interfaz de WAN-Data
2 + n	Cada una de las interfaces de la LAN
254	Interfaz de LAN radioeléctrica agregada
255	Interfaz de LAN agregada

Si un determinado ifAdminStatus = down da la interfaz, esa interfaz NO DEBE aceptar o retransmitir ningún tráfico. El objeto ifAdminStatus correspondiente al valor 255 de ifIndex DEBE proporcionar el control administrativo de todas las interfaces de la LAN y DEBE implementarse como lectura-escritura.

El PS DEBE asignar el valor other(1) a las anotaciones ifTable [RFC 2863] ifType correspondientes al valor 255 de ifIndex. El PS DEBE asignar el valor other(1) a las anotaciones ifTable ifType correspondientes al valor 254 de ifIndex. Un elemento PS integrado DEBE asignar el valor other(1) a las anotaciones ifTable ifType correspondientes a los valores 1 y 2 de ifIndex. Un elemento PS autónomo DEBE asignar el valor adecuado IANAifType [IANAType] al valor ifTable ifType correspondiente a los valores 1 y 2 de ifIndex.

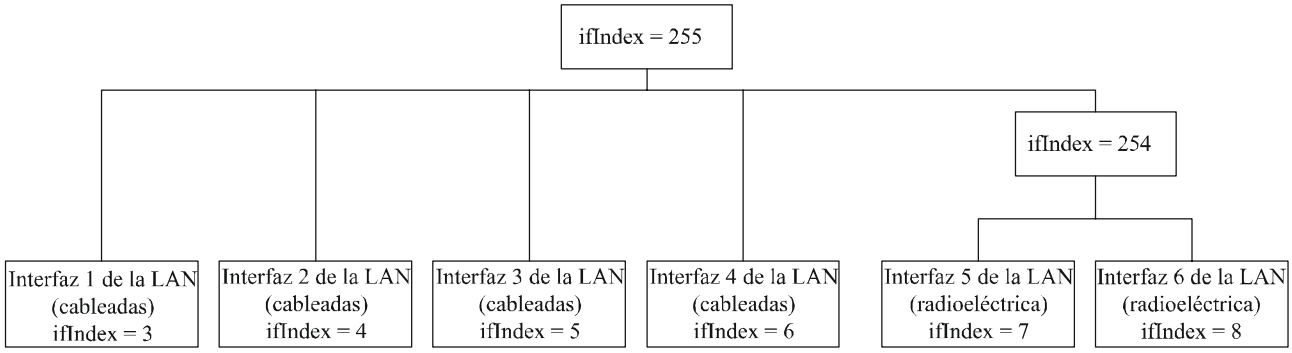
El valor ifTable ifPhysAddress correspondiente al valor 255 de ifIndex DEBE ser una cadena de octetos con longitud cero.

El valor ifTable ifPhysAddress correspondiente al valor 254 de ifIndex DEBE ser una cadena de octetos con longitud cero.

Los contadores ifTable de las interfaces de la WAN relativas a los valores 1 y 2 de ifIndex DEBEN compartirse entre las dos interfaces. El PS PUEDE implementar los contadores ifTable para los valores 254 y 255 de ifIndex.

Las interfaces del PS DEBE implementarse de conformidad con las definiciones de capa y de subcapa descritas en la sección 3.1 de [RFC 2863], estando todas las interfaces PS comprendidas entre (3 a 254) implementadas como subcapas de la interfaz 255, y todas las interfaces físicas LAN radioeléctricas PS implementadas como subcapas de la interfaz 254.

El grupo de pila de interfaces (ifStack) de [RFC 2863] DEBE implementarse para identificar las relaciones entre la interfaz de "interfaces de la LAN agregadas" de capa superior y las subinterfaces de la LAN (cableadas) de capa inferior para identificar las relaciones entre la interfaz de "Interfaces LAN agregadas" de capa superior y la interfaz de "Interfaces LAN radioeléctricas agregadas" de capa inferior, así como para identificar la relación entre la interfaz de "Interfaces LAN radioeléctricas agregadas" y las subinterfaces de la LAN radioeléctricas de capa inferior. En la figura 6-6 se ilustra la utilización del grupo ifStack en el caso de un PS con cuatro interfaces LAN cableadas y dos interfaces radioeléctricas.



Implementación de ifStack para este ejemplo:

ifStackHigherLayer	0	1	0	2	0	255	255	255	255	255	254	254	3-8
ifStackLowerLayer	1	0	2	0	255	3	4	5	6	254	7	8	0

Figura 6-6/J.192 – Ejemplo de implementación de ifStack

6.3.3.1.4.9 MIB de LAN radioeléctrica IEEE 802.11

Si el PS implementa la funcionalidad de LAN radioeléctrica IEEE 802.11, DEBE soportar la MIB radioeléctrica 802.11 y las extensiones aplicables a las implementaciones [802.11A-1999], [802.11B/Cor1-1999], [802.11D], [802.11G-2003] tal como se especifica en el anexo A.

Cuadro 6-18/J.192 – Requisitos del módulo MIB IEEE 802.11

Estructura MIB	Notas
dot11StationConfigEntry	Requerida
dot11WEPDefaultKeysTable	Requerida
dot11PrivacyEntry	Requerida
dot11OperationEntry	Requerida
dot11PhyTxPowerEntry	Requerida
dot11PhyDSSSEntry	Requerida para 802.11B y 802.11G
dot11PhyOFDMTable	Requerida si se soporta 802.11A
cabhPsDev802dot11BaseTable	Requerida
dot11AuthenticationAlgorithmsEntry	Opcional

Cuadro 6-18/J.192 – Requisitos del módulo MIB IEEE 802.11

Estructura MIB	Notas
dot11MultiDomainCapabilityEntry	Opcional
dot11PhyOperationEntry	Opcional
dot11RegDomainsSupportEntry	Opcional
dot11SupportedDataRatesTxEntry	Opcional
dot11SupportedDataRatesRxEntry	Opcional
dot11PhyHRDSSSTable	Opcional, sólo si se soporta 802.11B
dot11PhyERPTable	Opcional, sólo si se soporta 802.11G

En las subcláusulas siguientes se detallan los requisitos específicos de IPCable2Home para los requisitos de las MIB enumeradas en el cuadro 6-18

6.3.3.1.4.9.1 Requisitos específicos de la MIB 802.11

Los objetos MIB 802.11 no enumerados en el anexo A se consideran OPCIONALES y PUEDE no ser necesario crear ejemplares de los mismos en los cuadros requeridos.

Si se crean ejemplares de objetos MIB 802.11 OPCIONALES aquí definidos, ello indica que se implementan las primitivas del protocolo asociadas con las capas de gestión PHY o MAC, por lo DEBE informarse de los valores siguientes:

– Los contadores y las estadísticas DEBEN incrementarse según su funcionamiento.
– Los objetos MIB dinámicos con SINTAXIS de sólo lectura DEBEN informar valores exactos.
– Los objetos MIB configurables con SINTAXIS de lectura-escritura PUEDEN ser implementados como de sólo lectura.

6.3.3.1.4.9.1.1 Requisitos de dot11StationConfigEntry

Los objetos MIB dot11BeaconPeriod, dot11DTIMPeriod y dot11AssociationResponseTimeOut PUEDEN implementarse como de sólo lectura.

El objeto MIB dot11OperationalRateSet, que PUEDE tener acceso de sólo lectura, DEBE corresponder a valores en el contexto de cabhPsDev802dot11PhyOperMode. Si el objeto MIB dot11OperationalRateSet implementa un acceso de lectura-escritura, una operación de establecimiento de SNMP a una velocidad de datos inexistente en el contexto de cabhPsDev802dot11PhyOperMode DEBE producir un informe de error SNMP 'wrongValue' ('valor erróneo').

El soporte de características multidominio [802.11D] varía ente dominios de regulación, en particular en el caso del dominio regulatorio 0x00 (FCC) (Estados Unidos de América) es OPCIONAL soportar los OBJETOS MIB dot11MultiDomainCapabilityImplemented, dot11MultiDomainCapabilityEnabled y dot11CountryString, y en caso de ser implementado, dot11MultiDomainCapabilityImplemented DEBE ser 'falso'.

6.3.3.1.4.9.1.2 Requisitos de dot11WEPDefaultKeysTable

El PS DEBE implementar la cláusula de SINTAXIS del objeto MIB dot11WEPDefaultKeyValue SYNTAX como "OCTET STRING (0|5|13)"que significa que se soportan claves de 40 bits y 104 bits.

El PS PUEDE soportar solamente una anotación para este cuadro, en cuyo caso dot11WEPDefaultKeyID PUEDE tener accesos de solo lectura, o bien, DEBE estar restringido al valor 0, para evitar fallos de configuración no detectados.

6.3.3.1.4.9.1.3 Requisitos de dot11OperationEntry

Los objetos MIB dot11RTSThreshold y dot11FragmentationThreshold PUEDEN tener accesos de solo lectura.

6.3.3.1.4.9.1.4 Requisitos de dot11PhyTxPowerEntry

El PS DEBERÍA implementar los valores de los objetos MIB de dot11PhyTxPowerEntry en mW equivalentes a un valor incluido en la gama de porcentajes de la potencia máxima de salida del dispositivo para el modo de funcionamiento configurado en cabhPsDev802dot11PhyOperMode, tal como se describe en el cuadro 6-19. Esta configuración simplifica la fijación del valor de potencia transmitida del objeto MIB dot11CurrentTxPowerLevel.

Si el PS es conforme a los valores de configuración del cuadro 6-19, DEBE soportar los ocho ejemplares (1..8) del objeto MIB dot11NumberSupportedPowerLevels, lo cual permite que la implementación soporte 8 ó 4 niveles de potencia. A modo de ejemplo, la columna situada más a la izquierda indica los valores de los objetos MIB en dot11PhyTxPowerEntry para la banda inferior de UNII definida en el cuadro 89 de [802.11A-1999]. En particular, los niveles impares (1, 3, 5, 7) representan referencias determinísticas al 100%, 75%, 50% y 25% de la potencia máxima del dispositivo; mientras que los niveles pares (2, 4, 6, 8) tienen valores de potencia en los rangos de los correspondientes números impares superior e inferior (1-3, 3-5, 5-7, 7-).

Cuadro 6-19/J.192 – Niveles de potencia recomendados

Nivel de potencia	Valor en mW % relativo respecto al nivel de potencia máxima del PS	Valor en mW % Límite superior	Valor en mW % Límite inferior	Banda 5,15-5,25 GHz 40 (mW)
Dot11TxPowerLevel1	100%	100%	100%	40
Dot11TxPowerLevel2	100%-75%	100%	75%	40-30
Dot11TxPowerLevel3	75%	75%	75%	30
Dot11TxPowerLevel4	75%-50%	75%	50%	30-20
Dot11TxPowerLevel5	50%	50%	50%	20
Dot11TxPowerLevel6	50%-25%	50%	25%	20-10
Dot11TxPowerLevel7	25%	25%	25%	10
Dot11TxPowerLevel8	25%-12%	25%	12%	10-5

6.3.3.1.4.9.1.5 dot11PhyDSSSEntry

El PS DEBE soportar el objeto MIB dot11CurrentChannel para implementaciones conformes con los modos PHY 802.11B/Cor1-2001 ó 802.11G-2003.

6.3.3.1.4.9.1.6 Requisitos de dot11PhyOFDMEntry

El PS DEBE implementar dot11PhyOFDMEntry si funciona en un modo conforme con PHY 802.11A.

6.3.3.1.4.9.2 Ampliaciones de configuración de IPCable2Home para requisitos de MIB 802.11

Si el PS implementa la funcionalidad LAN radioeléctrica IEEE 802.11, DEBE implementar los objetos MIB según el OBJECT IDENTIFIER cabhPsDevPs802dot11.

6.3.3.1.4.9.2.1 Requisitos de cabhPsDev802dot11BaseEntry

El objeto MIB cabhPsDev802dot11BaseAdvertiseSSID PUEDE implementarse como de sólo lectura.

6.3.3.1.4.10 Requisitos de ipNetToMediaTable

El cuadro ipNetToMediaTable [RFC 2011] hace corresponder las direcciones IP con las direcciones físicas, y su utilización es sencilla si se asocia cada una de las direcciones IP con una interfaz física, y si cada interfaz física se asocia a su vez a una dirección física. No obstante, el PS implementa distintas direcciones de IP que pueden aplicarse a varias interfaces físicas, y relaciona la interfaz física de la WAN con dos direcciones de hardware. El PS también implementa varios modos de tratamiento de paquetes primario, lo cual también afecta a ipNetToMediaTable. El PS DEBE relacionar en el cuadro ipNetToMediaTable cada una de las direcciones IP que forman parte de su configuración activa, creando una anotación por cada valor IP distinto y soportado por el cuadro 6-20 para los modos de tratamiento de paquetes primario NAPT y NAT (incluyendo el modo mixto), y respetando los valores del cuadro 6-21 para el modo de tratamiento de paquetes primario de transferencia (Passthrough).

Cuadro 6-20/J.192 – Anotaciones estáticas del PS en ipNetToMediaTable para NAPT, NAT y modos mixtos

ipNetToMediaAddress	ipNetToMediaPhysAddress	ipNetToMediaIfIndex	ipNetToMediaType
Dirección IP de WAN-Man	Dirección hardware de WAN-Man	1	static(4)
1ª dirección IP de WAN-Data	Dirección hardware de WAN-Data	2	static(4)
2ª dirección IP de WAN-Data	Dirección hardware de WAN-Data	2	static(4)
N-ésima dirección IP de WAN-Data	Dirección hardware de WAN-Data	2	static(4)
Dirección IP del encaminador del servidor CDP	Cadena de octetos de longitud cero	255	static(4)
Dirección IP de LAN del PS bien conocida (si es distinta de la IP del encaminador servidor)	Cadena de octetos de longitud cero	255	static(4)

Cuadro 6-21/J.192 – Anotaciones estáticas del PS en ipNetToMediaTable para el modo de transferencia

ipNetToMediaAddress	ipNetToMediaPhysAddress	ipNetToMediaIfIndex	ipNetToMediaType
Dirección IP de WAN-Man	Dirección de hardware de WAN-Man	1	static(4)
Dirección IP de LAN del PS bien conocida encaminador del servidor	Cadena de octetos de longitud cero	255	static(4)

El elemento PS DEBE ir conociendo de forma dinámica las direcciones IP y hardware de los dispositivos de capa 3 de la OSI de cada una de sus interfaces LAN físicas activas y de sus interfaces WAN activas. Las direcciones IP y hardware que son conocidas por el elemento PS, junto con los números ifIndex de PS adecuados y la información ipNetToMediaType, DEBEN ser accesibles al NMS (a través del CMP) mediante la ipNetToMediaTable [RFC 2011]. El valor de ipNetToMediaType de todas las Anotaciones en ipNetToMediaTable conocidas dinámicamente DEBE ser dynamic(3).

En la ipNetToMediaTable del PS NO DEBE aparecer como anotación una fila para el CM del PS ya que, desde la perspectiva de éste último, el CM actúa como un puente transparente.

Como resultado de haber completado el proceso de configuración del PS, éste DEBE crear una nueva fila en ipNetToMediaTable que represente al encaminador del siguiente de salto de la interfaz WAN-Man y que incluya un valor 1 para ifIndex, valores específicos de ipNetToMediaPhysAddress y de ipNetToMediaNetAddress para dicho encaminador y un valor de ipNetToMediaType igual a dynamic(3). Si el PS tiene una interfaz WAN-Data activa, DEBE crear una nueva fila en su ipNetToMediaTable que representa al encaminador del siguiente de salto de la interfaz WAN-Data y que incluya un valor 2 para ifIndex, valores específicos de ipNetToMediaPhysAddress y ipNetToMediaNetAddress para dicho encaminador y un valor de ipNetToMediaType igual a dynamic(3).

El elemento PS DEBE suprimir las anotaciones en su ipNetToMediaTable con el valor dynamic(3) de ipNetToMediaType una vez que expire el temporizador de inactividad específico de la implementación.

6.3.3.1.5 Control de la interfaz de usuario del PS

El CMP soporta la configuración de la interfaz de usuario (UI, *user interface*), si se implementa alguna, mediante un conjunto de objetos definidos en la MIB PSDev (véase E.4). Estos objetos permiten que el operador de cable seleccione la interfaz de usuario que se presenta al usuario cuando éste apunta su navegador web a la dirección IP del encaminador del servidor del PS. La MIB permite seleccionar entre la UI de un fabricante local, la UI de un operador de cable y la UI del servidor de red, y permite inhabilitar la UI. La MIB permite también que el operador de cable configure un registro de acceso y contraseña para la UI del abonado. Véase en el anexo E la MIB miscelánea de la interfaz de usuario de IPCable2Home.

6.3.3.2 Función de notificación de eventos del CMP

El CMP debe soportar el manejo y notificación de eventos generados por el PS, para el dominio de la WAN. Los mensajes de eventos definidos por IPCable2Home para el elemento PS pueden notificarse al receptor de notificaciones del operador del sistema de cable a través de la trampa SNMP, mediante un mensaje de registro histórico de sistema que se envía al registro histórico del sistema del operador de cable, o mediante un registro histórico local en el PS accesible a través de objetos de la MIB específicos. Los eventos definidos para el PS se relacionan en el anexo B, Formato y contenido de eventos, SYSLOG y trampas SNMP. Se trata de los mismos procesos definidos en las especificaciones de DOCSIS para el informe de eventos en los módems de cable.

No es necesario que los dispositivos del anfitrión de IPCable2Home soporten mensajes de eventos. Por consiguiente, en la presente Recomendación no se definen los mensajes de eventos del dominio de la LAN.

Notificación de eventos del dominio WAN

IPCable2Home utiliza mecanismos de informe de eventos [RFC 2669] y de control de los eventos que genera el PS (CMP). En [RFC 2669] se define un formato normalizado para notificar los eventos, sin tomar en cuenta el tipo de mensaje, incluyendo un cuadro local de registro histórico de

eventos en el cual se conservarán determinadas anotaciones durante los rearranques del PS. Obsérvese que los eventos podrán ser generados por cualquier parte de un PS, pero el CMP registra y/o notifica el evento ya sea localmente o a un servidor de syslog o de trampas.

6.3.3.2.1 Objetivos de la función de notificación de eventos

Los objetivos de la función notificación de eventos del CMP son:

- permitir la transferencia de mensajes no solicitados del PS al NMS a través de la red WAN en forma de trampas SNMP y de mensajes SYSLOG;
- permitir el registro histórico de la información de estado y de excepción en la base de datos del PS (registro histórico local);
- permitir el acceso a la información de estado y de excepción del registro histórico local a través de objetos de la MIB;
- conservar la compatibilidad con el informe de eventos definido en las especificaciones de DOCSIS.

6.3.3.2.2 Directrices de diseño del sistema de la función de notificación de eventos

Las directrices de diseño del sistema, que se relacionan en el cuadro 6-22, dan la orientación para la especificación de la función de notificación de eventos del CMP.

Cuadro 6-22/J.192 – Directrices de diseño del sistema de la función de notificación de eventos del CMP

Referencia	Directrices
EvRep 1	El PS debe soportar la notificación de información de estado y de excepción como notificaciones SNMP, mensajes SYSLOG y mensajes de registro histórico local volátiles y no volátiles.
EvRep 2	El PS debe soportar el estrangulamiento y la limitación configurable de eventos.
EvRep 3	El PS debe soportar prioridades de eventos configurables.

6.3.3.2.3 Descripción del sistema de la función de notificación de eventos

La notificación de eventos permite que un elemento pueda notificar el estado o una condición de error de un mensaje no solicitado. IPCable2Home soporta cuatro tipos de notificaciones de eventos:

1) notificación o trampa SNMP;
2) mensajes SYSLOG;
3) registro histórico local no volátil;
4) registro histórico local volátil.

Resulta necesaria la utilización de la MIB de dispositivo DOCSIS [RFC 2669] para poder configurar el PS con relación al destino de envío de trampas SNMP (notificaciones) y mensajes SYSLOG y para los valores de inhibición y estrangulamiento de eventos. La notificación de eventos del PS es plenamente configurable. En esta Recomendación se determina si el PS debe notificar eventos a los que se ha asignado una prioridad particular (véase el cuadro 6-23) y si la MIB del dispositivo DOCSIS permitirá la configuración de la prioridad de cada evento. Además, la MIB del dispositivo DOCSIS mantendrá el control estadístico de la ocurrencia de cada evento. El cuadro de eventos (docsDevEventTable) en la MIB del dispositivo DOCSIS incluye una anotación por cada evento único informado por el PS, un contador del número de ocurrencias de cada anotación de evento único y el momento en el que se efectuó la última anotación de cada evento.

IPCable2Home define el procedimiento para reindexar el cuadro de eventos en el caso de que se reinicialice el PS de modo que se pierdan las anotaciones volátiles del registro histórico local.

Cuando se pierden esas anotaciones es necesario que el PS reindexe el cuadro de eventos de manera que se indexen secuencialmente las anotaciones restantes (volátiles) del registro histórico local.

6.3.3.2.4 Requisitos de la función de notificación de eventos

En 6.3.3.2.4.1 a 6.3.3.2.4.9 se especifican los requisitos del PS para la función notificación de eventos del CMP.

6.3.3.2.4.1 Notificación de eventos

El PS DEBE generar eventos asíncronos que indiquen los eventos y situaciones importantes conforme a lo especificado (véase el anexo B). Los eventos podrán almacenarse en un REGISTRO HISTÓRICO de eventos internos, en memoria no volátil, notificarse a otras entidades SNMP (como mensajes SNMP Trap o Inform), o enviarse como un mensaje de eventos SYSLOG al servidor SYSLOG cuya dirección IP se transfirió en la opción 7 del DHCP del mensaje DHCP OFFER recibido del servidor DHCP de la cabecera a través de las interfaces WAN-Man del PS.

El PS DEBE soportar los siguientes mecanismos de notificación de eventos:

- registro histórico local de eventos donde podrán identificarse determinadas anotaciones en el registro local que se conservan durante un rearranque del PS;
- SNMP Trap e Inform;
- SYSLOG.

El PS DEBE implementar el cuadro docsDevEvControlTable conforme a [RFC 2669] para controlar la notificación de eventos. El PS DEBE soportar los siguientes valores de bits para el objeto docsDevEvReporting [RFC 2669]:

- local-nonvolatile(0);
- traps(1);
- syslog(2);
- local-volatile(3).

Los mensajes de petición SNMP SET dirigidos al objeto docsDevEvReporting [RFC 2669] que utilicen los siguientes valores DEBEN dar por resultado un error 'valor erróneo' ('Wrong Value') para las PDU de SNMP:

- 0x20 = Solamente SYSLOG
- 0x40 = Solamente trap
- 0x60 = Solamente (trap + SYSLOG)

Un evento notificado mediante Trap, SYSLOG, o Inform también DEBE generar una anotación en el registro histórico local, ya sea volátil o no volátil conforme al cuadro 6-23, y de acuerdo a lo que se describe en 6.3.3.2.4.2.

6.3.3.2.4.2 Registro histórico local de eventos

El PS DEBE mantener un cuadro de eventos de registro histórico local que almacene los eventos ya sea como locales volátiles o como locales no volátiles. Los eventos almacenados como locales no volátiles DEBEN conservarse tras los rearranques del PS. El cuadro de eventos del histórico local DEBE organizarse como una memoria intermedia cíclica con una capacidad mínima de 10 anotaciones. El cuadro de eventos del histórico local DEBE ser accesible a través de docsDevEventTable definido en [RFC 2669].

Las descripciones de los eventos NO DEBEN superar los 255 bytes de longitud, que es el máximo definido para SnmpAdminString.

El EventId es un entero de 32 bits sin signo. Los EventIds comprendidos entre 0 y (2^{31}– 1) están reservados. El EventId DEBE convertirse con arreglo a los códigos de error definidos en el

anexo B. Los EventId que van de 2^{31} a (2^{32} – 1) DEBEN utilizarse como específicos del fabricante de acuerdo con el siguiente formato:

- El bit 31 estará activado para indicar un evento específico del fabricante.
- Los bits 30-16 contendrán los 15 bits finales del número de fabricante del SNMP.
- Los bits 15-0 están destinados a la numeración de eventos del fabricante.

El objeto [RFC 2669] docsDevEvIndex permite la ordenación relativa de los eventos en el registro histórico. La calificación de los eventos del registro histórico local como volátiles locales y no volátiles locales exige un método de sincronizar los valores docsDevEvIndex entre ambos tipos de eventos tras un rearranque del PS. Tras éste, DEBE utilizarse el siguiente procedimiento para sincronizar los valores docsDevEvIndex correspondientes a los elementos volátiles y no volátiles:

- Los valores de docsDevEvIndex correspondientes a los eventos del registro histórico local calificados como no volátiles locales DEBEN renumerarse desde 1.
- El registro histórico local DEBE inicializarse, acto seguido, con los eventos calificados como no volátiles locales en el mismo orden que tenían antes del rearranque.
- Los eventos subsiguientes anotados en el histórico local, calificados como volátiles locales o bien como no volátiles locales, DEBEN utilizar valores de incremento de docsDevEvIndex.

La reinicialización del registro histórico local iniciada por medio de un SNMP SET del objeto docsDevEvControl RFC 2669 DEBE suprimir todos los eventos del histórico local, incluidos los eventos del histórico calificados como volátiles locales o como no volátiles locales.

6.3.3.2.4.3 SNMP Trap y SNMP Inform

El PS DEBE soportar la PDU SNMP Trap (trampa) descrita en RFC 3411 así como la PDU SNMP Inform descrita en RFC 3411. Inform es una variante de trap y exige que el servidor receptor acuse recibo de la llegada de una PDU InformRequest con una PDU InformResponse.

Cuando se activa en el PS una trampa SNMP normal, DEBE enviar notificaciones para cualquier evento de dicha categoría cuya prioridad sea "error" o "notice".

El PS PUEDE soportar eventos específicos del fabricante. Caso de soportarse, los eventos PS específicos del fabricante que puedan comunicarse mediante SNMP Trap DEBEN describirse en una MIB privada distribuida con el PS. En la definición de una SNMP Trap específica de un fabricante, la declaración de OBJECTS de la definición de la trampa privada DEBERÍA contener como mínimo los objetos indicados a continuación:

- EvLeve;
- EvIdText;
- umbral d eventos (de haberlos en la trampa);
- IfPhysAddress (dirección física asociada a la dirección IP WAN-Man del PS).

Se pueden incluir más objetos en la sentencia OBJECTS si así se desea.

6.3.3.2.4.4 SYSLOG

Los mensajes SYSLOG emitidos por el PS DEBEN adoptar el siguiente formato:

<nivel>PortalServicesElement[fabricante]: <eventId> texto

siendo:

Nivel – presentación en ASCII de la prioridad del evento, encerrada entre paréntesis angulares, interpretada como el OR binario o la facilidad por defecto (128) y la prioridad del evento (0-7). El nivel obtenido puede estar comprendido entre 128 y 135.

Fabricante – nombre del fabricante correspondiente a los mensajes SYSLOG específicos del fabricante o "CABLEHOME" para los mensajes de IPCable2home normales.

EventId – presentación en ASCII del número INTEGER en formato decimal, encerrado entre paréntesis angulares, que identifica de modo exclusivo el tipo de evento. Este EventID DEBE ser el mismo número almacenado en el objeto docsDevEvId de docsDevEventTable. Para los eventos de IPCable2home normales, este número se convierte utilizando el código de errores de acuerdo con las siguientes reglas:

- El número es un decimal de ocho dígitos.
- Los dos primeros dígitos (los situados más a la izquierda) son el código ASCII (decimal) correspondiente a la letra del código de error.
- Los cuatro dígitos siguientes están ocupados por los dos o tres dígitos existentes entre la letra y el punto del código de error relleno a ceros por la izquierda.
- Los dos últimos dígitos se rellenan con el número que hay tras el punto del código de error relleno a ceros por la izquierda.

Por ejemplo, el evento D04.2 se convierte en 68000402 y el evento I114.1 se convierte en 73011401.

Obsérvese que de este modo sólo se utiliza una pequeña fracción del espacio numérico disponible reservado a IPCable2home (0 a 2^{31} – 1). La primera letra de un código de error siempre va en mayúsculas.

texto – para los mensajes normales, esta cadena DEBE contener la descripción textual definida en el anexo B.

Ejemplo del evento syslog correspondiente al evento D04.2: "Time of the day received in invalid format":

<132>PortalServicesElement[CABLEHOME]: <68000402> Time of the day received in invalid format.

El número 68000402 del ejemplo anterior es el asignado a este evento concreto.

6.3.3.2.4.5 Formato de los eventos

Los mensajes de eventos de gestión de IPCable2Home PUEDEN contener las informaciones siguientes:

- Contador de eventos – indicador de la secuencia de eventos.
- Hora del evento – momento de la ocurrencia del evento.
- Prioridad del evento – gravedad de la situación. [RFC 2669] define ocho niveles de gravedad. La gravedad del evento por defecto puede modificarse a un valor distinto para cada evento específico a través de la interfaz SNMP.
- Número de empresa del evento – este número identifica el evento como evento normal o bien como evento definido por el fabricante.
- ID del evento – identifica exactamente el evento cuando está combinado con el número de empresa del evento. Los fabricantes definen sus propios ID de eventos. Los eventos de gestión normal de IPCable2Home se definen en el anexo B. Cada evento de gestión descrito en este anexo tiene asignado un ID de evento.
- Texto del evento – describe el evento de manera inteligible.
- Dirección WAN-Man-MAC del PS – describe la dirección MAC del elemento PS utilizado para la gestión del dispositivo.
- Dirección WAN-Data-MAC del PS – describe la dirección MAC del elemento PS que se emplea facultativamente para los datos.

El formato exacto de esta información para las trampas e informativos se define en el anexo B. El formato para los mensajes SYSLOG se define en la sección de requisitos de esta subcláusula.

6.3.3.2.4.6 Prioridades de los eventos

En RFC 2669 se definen ocho niveles de prioridad distintos y los mecanismos de información correspondientes a cada nivel. Los eventos normales especificados en esta Recomendación utilizan los siguientes niveles de prioridad.

– **Evento de emergencia (prioridad 1)**

  Se reserva para errores de tipo 'fatal' del equipo físico o de los programas específicos del fabricante que impiden el funcionamiento normal del sistema y provocan el rearranque del sistema informador. Los fabricantes pueden definir sus propios conjuntos de eventos de emergencia. Como ejemplos de estos eventos se pueden citar 'no memory buffers available (no hay memoria intermedia disponible)', 'memory test failure (prueba de memoria fallida)' etc.

– **Evento de alerta (prioridad 2)**

  Avería grave que provoca el rearranque del sistema informador a pesar de no ser provocado por un mal funcionamiento del equipo físico ni del software. Tras recuperarse del evento, el sistema DEBE enviar la notificación de arranque en frío o caliente.

– **Evento crítico (prioridad 3)**

  Avería grave que impide que el dispositivo transmita datos aunque puede recuperarse sin necesidad de rearrancar el sistema. Tras recuperarse de un evento crítico, el PS DEBE enviar la notificación Link Up (enlace activo). Como ejemplos de estos eventos se pueden citar los problemas del fichero de configuración del PS o la incapacidad de obtener una dirección IP a través del DHCP.

– **Evento de error (prioridad 4)**

  Avería que podría interrumpir el flujo normal de datos pero que no provoca el rearranque del dispositivo. Los eventos de error pueden comunicarse en tiempo real utilizando el mecanismo Trap o el SYSLOG.

– **Evento de alarma (prioridad 5)**

  Avería que podría interrumpir el flujo normal de datos. Los informes de SYSLOG y Trap están desactivados por defecto para este nivel.

– **Evento de notificación (prioridad 6)**

  Evento de importancia que no constituye una avería y que puede comunicarse en tiempo real utilizando el mecanismo Trap o el SYSLOG. Como ejemplo de eventos NOTICE se pueden citar 'Cold Start', 'Warm Start', 'Link Up' y 'SW upgrade successful'.

– **Evento informativo (prioridad 7)**

  Evento de importancia que no constituye una avería pero que puede ser útil para el seguimiento del funcionamiento normal del dispositivo.

– **Evento de depuración (prioridad 8)**

  Reservado para eventos no críticos específicos del fabricante.

La prioridad asociada a los eventos normales NO DEBE modificarse.

En el cuadro 6-23 se muestran los tipos de notificación por defecto correspondientes a las diversas prioridades de evento. El PS DEBE implementar los tipos de notificación por defecto, definidos en el cuadro 6-23, Tipos de notificación por defecto de las prioridades de eventos del PS, para las ocho

prioridades de evento. Por ejemplo, el tipo de notificación por defecto para los eventos de emergencia y alerta consiste en inscribirlos en el registro histórico local como Alertas no volátiles.

Cuadro 6-23/J.192 – Tipos de notificación por defecto de las prioridades de eventos del PS

Prioridad del evento	No volátil local (bit 0)	SNMP trap (bit 1)	SYSLOG (bit 2)	Volátil local (bit 3)	Nota
1 Emergencia	Sí	No	No	No	Específico del fabricante
2 Alerta	Sí	No	No	No	Esta Recomendación
3 Crítico	Sí	No	No	No	Esta Recomendación
4 Error	Sí	Sí	Sí	No	Esta Recomendación
5 Aviso	Sí	Sí	Sí	No	Esta Recomendación
6 Notificación	No	Sí	Sí	Sí	Esta Recomendación
7 Informativo	No	No	No	No	Esta Recomendación y específico del fabricante
8 Depuración	No	No	No	No	Específico del fabricante

El PS DEBE tener la capacidad para que pueda configurarse de modo que genere todos los tipos de notificación para cada nivel de prioridad de evento relacionado en el cuadro 6-23.

6.3.3.2.4.7 Eventos normalizados

El PS DEBE enviar las siguientes trampas SNMP genéricas, definidas en [RFC 3418] y [RFC 2863]:

- coldStart [RFC 3418];
- linkUp [RFC 2863];
- linkDown [RFC 2863];
- SNMP authentication-Failure [RFC 3418] (fallo de autenticación SNMP).

El PS DEBE poder generar notificaciones de eventos correspondientes a los eventos normales relacionados en el anexo B.

6.3.3.2.4.8 Estrangulamiento y limitación de eventos

El PS DEBE soportar el estrangulamiento y la limitación de SNMP Trap/Inform y SYSLOG descritos en [RFC 2669].

El PS DEBE considerar que dos eventos son idénticos si sus EventId son idénticos.

[RFC 2669] especifica cuatro estados de estrangulamiento:

- unconstrained(1) (sin restricciones) hace que los mensajes Trap y SYSLOG se transmitan sin tener en cuenta los valores umbral.
- maintainBelowThreshold(2) (mantener por debajo del umbral) hace que la transmisión de los mensajes Trap y SYSLOG se suprima si el número de trampas sobrepasa el umbral.
- stopAtThreshold(3) (detenerse en el umbral) provoca el cese de la transmisión de las trampas cuando se alcanza el umbral, no reanudándose hasta que se le indique.
- inhibited(4) (inhibido) provoca la supresión de todas las transmisiones de mensajes Trap y SYSLOG.

Un evento sencillo DEBE tratarse como tal a efectos del cómputo del umbral, o sea un evento que provoca un mensaje Trap y un mensaje SYSLOG sigue tratándose como un único evento.

6.3.3.2.4.9 Notificación de eventos de descarga segura de software

En el cuadro B.1, se describen los eventos correspondientes a las actualizaciones del software de los servicios de portal, en tres categorías: inicio de actualización del software (SW UPGRADE INIT), fracaso general de la actualización del software y éxito de la actualización del software. Estos eventos tienen aplicación únicamente en el PS autónomo, ya que la actualización del software (que se denomina también descarga segura de software) de un PS con un módem de cable integrado se controla y gestiona a través del módem de cable DOCSIS. En la cláusula 11.8, Descarga segura de software para el PS, se describen los requisitos para la descarga segura de software en las dos clases de elementos de servicios de portal. El PS, según se define en 5.1.2.1, NO DEBE generar eventos con las categorías indicadas en el cuadro B.1, Eventos definidos para IPCable2Home, como eventos de "inicio de actualización de software" (SW UPGRADE INIT), eventos de "fracaso general de actualización del software" (SW UPGRADE GENERAL FAILURE) o eventos de "éxito de actualización de software" (SW UPGRADE SUCCESS).

{texto informativo:

6.3.3.3 Función de determinación del CMP

6.3.3.3.1 Objetivos de la función de determinación

Los objetivos de la función de determinación del CMP se relacionan a continuación:

- Permitir que los operadores del sistema de cable dispongan de la visibilidad necesaria de los dispositivos del anfitrión UPnP de IPCable2Home y de los atributos de los dispositivos de la pasarela residencial de IPCable2Home.
- Permitir que los operadores del sistema de cable dispongan de la visibilidad necesaria de servicios UpnP sobre dispositivos del anfitrión UPnP de IPCable2Home.

Hipótesis

Las hipótesis para la capacidad de determinación del CMP incluyen lo siguiente:

- Los dispositivos del anfitrión de IPCable2Home, los dispositivos del anfitrión UPnP, y los dispositivos de la pasarela residencial de IPCable2Home aplican el conjunto de protocolos de Internet (IPv4).
- Los dispositivos anfitriones de UpnP implementan un dispositivo UPnP para la determinación, la descripción y el control, tal como especifica la arquitectura de dispositivos UPnP.
- Los dispositivos anfitriones UPnP implementan opcionalmente servicios con QoS UpnP.

6.3.3.3.1.1 Directrices de diseño del sistema de la función de determinación

Las directrices de diseño del sistema relacionadas en el cuadro 6-24 proporcionan la orientación para la evolución de la especificación de la función de determinación del CMP.

Cuadro 6-24/J.192 – Directrices de diseño del sistema de determinación del PS

Referencia	Directrices
Determinación 1	El PS implementará una funcionalidad de determinación de dispositivos UPnP coherente con la arquitectura 1.0 de dispositivos UpnP.
Determinación 2	El PS debe proporcionar al operador del sistema de cable, cuando así se solicite, información relativa a los dispositivos UPnP en la red LAN doméstica.
Determinación 3	El PS implementará una funcionalidad de punto de control UpnP coherente con la arquitectura 1.0 de dispositivos UPnP para la determinación, descripción y control de dispositivos y servicios UpnP.
Determinación 4	El PS implementará una jerarquía de servicios y dispositivos UpnP especificada.
Determinación 5	Los mensajes del protocolo de determinación UPnP no deberán difundirse a la red WAN.

6.3.3.3.2 Descripción del sistema de la función de determinación

La finalidad de la función de determinación del CMP es permitir que el operador del sistema de cable disponga de la información relativa a los dispositivos anfitriones UpnP y los servicios UPnP disponibles en la LAN del abonado.

La función de determinación del PS proporciona un depósito central de información de dispositivos UPnP y servicios UPnP disponibles en la LAN del abonado. El PS implementa un punto de control UPnP (PS CP) que le permite determinar todos los dispositivos y ejemplares de servicio UPnP en la red doméstica. Además, la función de determinación puede solicitar información adicional sobre dispositivos y servicios UPnP específicos, en forma de documentos de descripción de servicios y dispositivos UPnP.

6.3.3.3.3 Requisitos de la función de determinación

1) Cuando la MIB cabhPsDevUpnpCommand se fija en discoveryInfo y cabhPsDevUpnpCommandUpdate se fija en verdadero, el PS DEBE invocar la determinación UPnP mediante M-Search con el objetivo de búsqueda (ST, *search target*) de upnp:rootdevice y un valor máximo de espera (MX) igual o inferior a 3 segundos, tal como se especifica en la arquitectura de dispositivos UPnP (UDA1.0).

2) El PS DEBE rellenar su base de datos con la información de descripción de dispositivos que está accesible mediante el cuadro de la MIB cabhPsDevUpnpInfoTable. Cuando se actualiza la base de datos PS con información de determinación recibida como respuesta a M-Search, el PS DEBE filtrar la información en función de la MIB cabhPsDevUpnpCommandIp.
   - Si cabhPsDevUpnpCommandIp se fija como 255.255.255.255, el PS DEBE rellenar su base de datos con información de determinación recibida de todos los dispositivos UPnP raíz de la red doméstica, y también DEBE incluir su propia información de determinación de dispositivos UPnP.
   - Si cabhPsDevUpnpCommandIp se fija como 192.168.0.1, el PS DEBE rellenar su base de datos con su propia información de determinación de dispositivo UPnP.

3) Todos los URI que el PS ofrece para comunicaciones UPnP DEBEN utilizar direcciones IP y NO DEBEN utilizar nombres de anfitrión.

4) Si el PS desea modificar la descripción de un dispositivo o los ficheros de descripción de un servicio DEBE, en primer lugar, abandonar la red UPnP enviando un mensaje ssdp:byebye y volver a unirse a la red UPnP con los nuevos ficheros XML utilizando un mensaje ssdp:alive.

5) El PS DEBE enviar todos sus anuncios de determinación con el encabezamiento HTTP LOCATION de 192.168.0.1

6) El deviceType del dispositivo raíz del PS DEBE ser urn:schemas-cablelabs-com:device:CableHomePSDevice:1.

7) El PS DEBE anunciar el Dispositivo IGD 1.0 como un dispositivo integrado del dispositivo raíz CableHomePS.

8) El PS DEBE anunciar todos los servicios con QoS UPnP como servicios del dispositivo raíz del PS CableHome.

9) El PS DEBE anunciar la siguiente jerarquía como parte de su documento de descripción de dispositivos UPnP:

- CableHomePSDevice
  - IGD Device 1.0
    - IGD WAN Device 1.0
      - IGD WANConnection Device 1.0
        - IGD WANIPConnection Service 1.0
  - QoS Manager Service 1.0
  - QoS Policy Holder Service 1.0
  - QoS Device Service 1.0 (Optional)

(Véase en el apéndice I un ejemplo de esta jerarquía.)

10) A fin de proporcionar una única denominación para todos los dispositivos UPnP en la descripción del dispositivo raíz PS CableHome, se propone utilizar el siguiente formato para los nombres de dispositivos singulares para todos los dispositivos UPnP en el PS CableHome.

- El formato del nombre de dispositivo singular CableHomePSDevice DEBERÍA ser CableHomePSDevice-1_0-00aabbccddee, donde 00aabbccddee corresponde a la dirección MAC WAN-MAN del PS.
- El formato del nombre de dispositivo singular InternetGatewayDevice DEBERÍA ser InternetGatewayDevice-1_0-00aabbccddee, donde 00aabbccddee corresponde a la dirección MAC WAN-MAN del PS.
- El formato del nombre de dispositivo singular WANConnectionDevice DEBERÍA ser WANConnectionDevice-1_0-00aabbccddee, donde 00aabbccddee corresponde a la dirección MAC WAN-MAN del PS.

11) Cuando se inhabilita un servicio UpnP implementado por el PS, éste DEBE comportarse de la forma siguiente:

- El PS DEBE enviar en difusión el mensaje SSDP:byebye para dicho servicio.
- El PS NO DEBE anunciar el servicio inhabilitado en los anuncios SSDP futuros.
- El PS NO DEBE devolver el servicio inhabilitado en la descripción del dispositivo raíz.
- El PS NO DEBE responder a M-SEARCH para el servicio inhabilitado.
- El PS NO DEBE responder a una acción para el servicio inhabilitado.

}

6.4 Portal de prueba de IPCable2Home (CTP) del elemento lógico del PS

6.4.1 Objetivos del CTP

Los objetivos del portal de prueba de IPCable2Home incluyen:

- Facilitar los diagnósticos de fallos de dispositivo IP de LAN y de los anfitriones de IPCable2Home.
- Facilitar la visibilidad a los dispositivos IP de LAN y a los anfitriones de IPCable2Home, así como el acceso a sus números y tipos.
- Facilitar la supervisión de la calidad de funcionamiento de los dispositivos IP de LAN y de los anfitriones de IPCable2Home.

6.4.2 Directrices de diseño del CTP

En el cuadro 6-25 se relacionan las directrices de diseño del sistema relativo al portal de prueba. Varias de esas directrices son comunes a las del CMP. Esta relación proporciona la orientación necesaria para la especificación de la funcionalidad del CTP.

Cuadro 6-25/J.192 – Directrices de diseño del sistema CTP

Referencia	Directrices
CTP 1	Se necesitan interfaces que soporten las características de gestión y diagnóstico, así como las funciones requeridas para soportar los servicios particulares del sistema de cable que se configuran a través de la red doméstica.
CTP 2	Se necesitan capacidades de supervisión local y a distancia, que permitan supervisar el funcionamiento de la red doméstica y ayudar al abonado y al operador del sistema de cable a identificar los ámbitos de problemas.
CTP 3	El NMS de la red de cable necesita un método para recopilar información de identificación relativa a cada dispositivo IP conectado a la red doméstica.
CTP 4	El NMS de la red de cable necesita un método para detectar si un dispositivo conectado se encuentra en estado de funcionamiento.

6.4.3 Descripción del sistema CTP

El CTP (portal de prueba de IPCable2Home) incluye las "herramientas a distancia" mediante las cuales el NMS puede recopilar información adicional del dispositivo de la LAN. Las pruebas deberán realizarse a distancia, ya que puede resultar problemático atravesar una función de traducción de dirección de red (NAT) de un encaminador. Por ejemplo, un mensaje ping de la red WAN a la red LAN no atravesará un PS, salvo que el CAP haya sido configurado previamente para aceptar este tipo de tráfico. El CTP es un apoderado local destinado a interpretar y ejecutar a distancia la clase de fallo/diagnóstico de los mensajes SNMP que recibe del operador del NMS. Estas pruebas de los dispositivos IP de LAN y de los anfitriones de IPCable2Home se definen basándose en problemas que probablemente se produzcan en las redes domésticas del tipo IPCable2Home 1.1: diagnósticos de conectividad y caudal.

Estas funciones reciben el nombre de herramienta de velocidad de la conexión del CTP y herramienta de ping a distancia del CTP. Permiten al centro de soporte a los clientes del operador del sistema de cable y al centro de operaciones de la red obtener mayor información relativa a la conexión entre el elemento PS y los dispositivos IP de LAN, y los anfitriones de IPCable2Home en la vivienda.

6.4.3.1 Función herramienta de velocidad de la conexión del CTP

6.4.3.1.1 Objetivos de la función herramienta de velocidad de la conexión

El objetivo de esta función es permitir que el gestor del sistema de IPCable2Home recoja a distancia los criterios de medición relativos a la calidad de funcionamiento de la red LAN doméstica entre el PS y un dispositivo IP de LAN o un anfitrión de IPCable2Home particular.

6.4.3.1.2 Directrices de diseño del sistema de la herramienta de velocidad de la conexión

Las directrices de diseño relacionadas en el cuadro 6-25, Directrices de diseño del sistema CTP, se utilizaron para orientar la especificación de la función de la herramienta de la velocidad de la conexión.

6.4.3.1.3 Descripción del sistema de la función herramienta de velocidad de la conexión

La función de la herramienta de velocidad de la conexión se utiliza para obtener una medición aproximada de la calidad de funcionamiento del caudal en el enlace entre el PS y un dispositivo IP de LAN o un anfitrión de IPCable2Home. La función envía una ráfaga de paquetes entre el PS y el dispositivo IP de LAN o el anfitrión de IPCable2Home sometido a prueba, y se efectúa la medición del tiempo de ida y vuelta de la ráfaga. Por lo general, el operador del NMS introduce algunos parámetros y activa la función, y los resultados se almacenan en la base de datos del PS para su recuperación posterior, a través de la MIB del CTP [(véase E.3].

La función velocidad de la conexión se apoya en los dispositivos IP de LAN y en los anfitriones IPCable2Home para disponer de una "función de bucle" o "servicio de eco" integrado. La autoridad de números asignados por Internet (IANA, *Internet assigned numbers authority*) ha destinado el puerto 7 de servicio de eco tanto para TCP como para UDP [RFC 347]. El valor por defecto de la dirección IP de origen (cabhCtpConnSrcIp) es el mismo del valor de la pasarela por defecto de la red LAN del PS (cabhCdpServerRouter). El valor de cabhCtpConnSrcIp podrá fijarse a cualquier dirección IP válida de WAN-Data del PS o a cualquier dirección IP válida de interfaz de la LAN del PS. La dirección IP de WAN-Man del PS no se utiliza como la dirección IP del origen para una herramienta CTP ya que cuando está presente la misma pero no está presente una dirección IP de WAN-Data del PS, el PS funcionará en modo de tratamiento de paquetes primario de transferencia y el operador del sistema de cable podrá probar los dispositivos IP de LAN y los anfitriones de IPCable2Home directamente desde la consola del NMS, si lo desea. Esta característica de prueba funciona en los dispositivos IP de LAN y en los anfitriones de IPCable2Home de los sectores de direcciones LAN-Trans o LAN-Pass que hayan implementado la función de servicio de eco, como se describe en la norma [RFC 347].

En la cláusula a continuación, relativa a los requisitos verificables del CTP, se relacionan los parámetros y las respuestas de las herramientas de velocidad de la conexión. En la cláusula 12.2.1.1 se dan detalles sobre el funcionamiento de dicha herramienta.

6.4.3.1.4 Requisitos de la función herramienta de velocidad de la conexión

El PS DEBE implementar la herramienta de velocidad de la conexión, y DEBE cumplir con los valores por defecto y las gamas de valores definidos para los objetos específicos de la herramienta de velocidad de la conexión de la MIB del CTP [(véase E.3].

El PS DEBERÍA transmitir los bytes de datos de prueba tan rápido como sea posible cuando se use la herramienta de velocidad de la conexión.

El PS DEBE utilizar el puerto 7 como puerto de destino cuando se use la herramienta de velocidad de la conexión.

El PS NO DEBE emitir paquetes por ninguna interfaz WAN cuando se use la función de la herramienta de velocidad de la conexión.

Cuando el NMS activa el CTP para iniciar la herramienta de velocidad de la conexión al poner cabhConnControl = start(1), el PS DEBE:

- reinicializar el temporizador;
- poner cabhCtpConnStatus = running(2);
- transmitir el número de paquetes igual al valor de cabhCtpConnNumPkts, cada uno con un tamaño igual al valor de cabhCtpConnPktSize, a la dirección IP igual al valor de cabhCtpConnDestIp y al puerto número 7, utilizando el protocolo especificado por cabhCtpConnProto;
- iniciar el temporizador con el primer bit transmitido;
- detener el temporizador cuando se recibe el último bit del dispositivo IP de LAN objetivo o cuando el valor del temporizador alcanza el valor de cabhCtpConnTimeOut, si no hubiera ocurrido lo anterior;
- cuando el temporizador llega al final, poner cabhCtpConnStatus = complete(3) y notificar el evento correspondiente (véase el anexo B – Eventos del CTP);
- almacenar el valor del temporizador (en milisegundos) en cabhCtpConnRTT;
- si se alcanza el fin del temporizador de la prueba de la herramienta de la velocidad de conexión antes de que se reciba el último bit del dispositivo IP de LAN o del anfitrión de IPCable2Home objetivo, notificar el evento correspondiente (véase el anexo B – Eventos del CTP);
- calcular el caudal como se describe en el requisito a continuación y almacenar el valor en cabhCtpConnThroughput.

Si el NMS detiene la herramienta velocidad de la conexión al poner el objeto cabhCtpConnControl = abort(2), o por cualquier otra razón, antes de que se reciba el último bit del dispositivo IP de LAN y del anfitrión de IPCable2Home objetivo, o antes de que se alcance su fin el temporizador de la prueba de la herramienta de velocidad de la conexión, el PS DEBE poner cabhCtpConnStatus = aborted(4) y notificar el evento correspondiente (véase el anexo B – Eventos del CTP).

Si la función herramienta de velocidad de la conexión se encuentra en ejecución, el PS DEBE determinar el caudal de ida y vuelta promedio entre el PS y el dispositivo IP de LAN o el anfitrión de IPCable2Home cuya dirección se transfirió en cabhCtpConnDestIp (dispositivo IP de LAN objetivo) en kbit/s, redondear el número al entero más próximo y almacenar el resultado en cabhCtpConnThroughput.

El PS DEBE reinicializar cabhCtpConnPktsSent, cabhCtpConnPktsRecv, cabhCtpConnRTT y cabhCtpConnThroughput, cada uno a un valor de 0, cuando se inicia la herramienta de velocidad de la conexión (es decir, cuando el valor de cabhCtpConnControl se pone a start(1)).

El tiempo de ida y vuelta (RTT, *round-trip time*) de la herramienta velocidad de la conexión se mide en el PS como el tiempo desde el primer bit del primer paquete enviado al último bit del último paquete recibido. El RTT es válido únicamente si el número de los paquetes recibidos es igual al número de los paquetes transmitidos.

El PS DEBE permitir que la dirección IP de destino de la herramienta de velocidad de la conexión (cabhCtpConnDestIp) se ponga a cualquier dirección IPv4 válida de cualquier dispositivo IP de LAN, al que se pueda acceder por cualquier interfaz LAN del PS en el que esté funcionando la herramienta de velocidad de la conexión del CTP.

La fijación del objeto control de la herramienta de velocidad de la conexión, cabhCtpConnControl, al valor start(1) DEBE activar la ejecución de la herramienta de velocidad de la conexión.

La fijación del objeto control de la herramienta de velocidad de la conexión, cabhCtpConnControl, al valor abort(2) DEBE dar por resultado la terminación de la herramienta de velocidad de la conexión.

El valor por defecto de cabhCtpConnStatus es notRun(1), indicando que la herramienta de velocidad de la conexión aún no ha sido ejecutada.

El PS DEBE poner el valor de cabhCtpConnStatus a running(2) si la herramienta ha recibido la instrucción de arrancar, no ha recibido instrucción de terminar, y si el temporizador de velocidad de la conexión no ha llegado a su fin.

El PS DEBE fijar el valor de cabhCtpConnStatus a complete(3) cuando el CTP recibe el último paquete enviado por la herramienta de velocidad de la conexión.

El PS DEBE fijar el valor de cabhCtpConnStatus a aborted(4) si la herramienta de velocidad de la conexión se detiene después de haber sido iniciada mediante la fijación SNMP del valor abort(2) al objeto cabhCtpConnControl, o si por el contrario la prueba se detiene antes de que se reciba el último paquete enviado por la herramienta de velocidad de conexión, y antes de la expiración del temporizador (cabhCtpConnTimeOut) de la herramienta de velocidad de la conexión.

El PS DEBE fijar el valor de cabhCtpConnStatus a timedOut(5) si expira el temporizador (cabhCtpConnTimeOut) de la herramienta de velocidad de la conexión antes de que el CTP reciba el último paquete enviado por la herramienta de velocidad de la conexión.

El PS NO DEBE utilizar ninguna dirección IP para la dirección IP de origen de la herramienta de la velocidad de la conexión (cabhCtpConnSrcIp) excepto una dirección IP actual y válida de WAN-Data del PS (es decir, un valor de objeto cabhCdpWanDataAddrIp activo) o una dirección IP actual y válida de interfaz de la LAN del PS. Si se configura un valor no válido para cabhCtpConnSrcIp, el PS DEBE tratar la ejecución de la prueba como un caso abortado y poner el objeto cabhCtpConnStatus de estado de la herramienta de velocidad de la conexión a 'abortado' notificando el evento correspondiente (véase el cuadro B.1).

6.4.3.2 Función de herramienta Ping del CTP

6.4.3.2.1 Objetivos de la función de herramienta Ping

El objetivo de esta función es permitir que el gestor del sistema pueda probar o verificar a distancia la conectividad entre el PS y un determinado dispositivo IP de LAN.

6.4.3.2.2 Directrices de diseño del sistema de la función de herramienta Ping

Las directrices de diseño relacionadas en el cuadro 6-25, Directrices de diseño del sistema CTP, se utilizaron para orientar la especificación de la función herramienta Ping.

6.4.3.2.3 Descripción del sistema de la función de herramienta Ping

Se invoca la función herramienta Ping para probar la conectividad entre el PS y dispositivos IP de LAN particulares o dispositivos del anfitrión de IPCable2Home. El NMS podrá ensamblar los resultados de múltiples pruebas de la herramienta Ping para una exploración de los dispositivos IP de LAN o de los anfitriones de IPCable2Home de la red. El cuadro del DHCP del CDP contiene una relación histórica de los dispositivos, pero únicamente de aquellos que emplean DHCP. La herramienta Ping puede recoger el estado actual incluyendo el de los clientes no DHCP. Para evitar la complejidad del PS, se prevé que el NMS incremente el valor de la dirección y almacene los resultados en la herramienta NMS para llevar a cabo la exploración de una subred de LAN.

La herramienta PING se inicia mediante una serie de mensajes de petición de establecimiento SNMP emitidos por la consola del NMS de la red de cable a la dirección de gestión del PS.

Los detalles del funcionamiento de la herramienta Ping se presentan en 12.2.1.2.

6.4.3.2.4 Requisitos de la función de herramienta Ping

La herramienta Ping del CTP DEBE implementarse empleando la facilidad de "Eco" del protocolo de mensajes de control Internet (ICMP, *Internet control message protocol*). El CTP emitirá una petición de eco ICMP, siendo lo previsible que el dispositivo IP de LAN devuelva la respuesta correspondiente.

El CTP DEBE ignorar, y excluir del recuento de cabhCtpPingNumRecv, cualquier respuesta de eco que se reciba después de la expiración de cabhCtpPingTimeOut.

El PS DEBE implementar la herramienta Ping del CTP, y DEBE cumplir con los valores por defecto y las gamas de valores determinadas para los objetos específicos de la herramienta Ping de la MIB del CTP [véase E.3].

Cuando el NMS activa el PS para iniciar el funcionamiento de la herramienta Ping al fijar cabhPingControl = start(1), el PS DEBE:

- fijar cabhCtpPingStatus = running(2);
- emitir todos los mensajes Ping (peticiones ICMP) especificados por el valor cabhCtpPingNumPkts, a la dirección IP definida por el valor de cabhCtpPingDestIp, empleando el valor de cabhCtpPingSrcIp como la dirección de origen de cada petición. El tamaño de cada trama de prueba emitida es el valor de cabhCtpPingPktSize. El límite temporal de cada mensaje Ping (par petición/respuesta de eco ICMP) es el valor de cabhCtpPingTimeOut;
- si el valor de cabhCtpPingNumPkts es mayor que 1, esperar el tiempo necesario definido por el valor de cabhCtpPingTimeBetween entre cada petición Ping emitida por el CTP.

Si el CTP recibe todas las respuestas de Ping antes de que expire sus respectivas temporizaciones, el PS DEBE poner cabhCtpPingStatus = complete(3) y notificar el evento correspondiente (véase el anexo B – Eventos del CTP).

Si el NMS detiene la herramienta Ping fijando el objeto cabhCtpPingControl = abort(2) o por cualquier otro motivo, antes de que se reciba el último bit del dispositivo IP de LAN objetivo y antes de que expire el temporizador, el PS DEBE fijar cabhCtpPingStatus = aborted(4) y notificar el evento correspondiente (véase el anexo B – Eventos del CTP).

Si expira el temporizador de al menos uno de los mensajes Ping antes de que se reciba su respuesta del dispositivo IP de LAN objetivo, el PS DEBE poner cabhCtpPingStatus = timedOut(5) y notificar el evento correspondiente (véase el anexo B – Eventos del CTP).

Cuando se inicia la función herramienta Ping del CTP, el PS DEBE determinar el tiempo de ida y vuelta promedio entre el PS y el dispositivo IP de LAN o el dispositivo del anfitrión de IPCable2Home cuya dirección se transfirió en cabhCtpPingDestIp (dispositivo de IP de LAN objetivo), de todas las peticiones Ping definidas por cabhCtpPingNumPkts, y almacenar el resultado en cabhCtpPingAvgRTT. Cuando se inicia la función herramienta Ping del CTP, el PS DEBE determinar los tiempos de ida y vuelta mínimos y máximos entre el PS y el dispositivo IP de LAN objetivo, de todas las peticiones Ping definidas por cabhCtpPingNumPkts y almacenar los valores en cabhCtpPingMinRTT y cabhCtpPingMaxRTT, respectivamente.

Si se produce un error ICMP durante la ejecución de la herramienta Ping, el PS DEBE aumentar el valor de cabhCtpPingNumIcmpError y registrar el error en cabhCtpPingIcmpError. El último error de ICMP que se produzca debe reemplazar allí el último error que se haya escrito.

El PS DEBE reinicializar cabhCtpPingNumSent, cabhCtpPingNumRecv, cabhCtpPingAvgRTT, cabhCtpPingMaxRTT, cabhCtpPingMinRTT, cabhCtpPingNumIcmpError y cabhCtpPingIcmpError, cada uno a un valor de 0 cuando se inicia la herramienta Ping (es decir, cuando el valor de cabhCtpPingControl se fija a start(1)).

El RTT de la herramienta Ping se mide en el PS como el tiempo transcurrido desde el último bit de cada paquete de petición de eco ICMP transmitido por la herramienta Ping del CTP, al momento en que se recibe el último bit del paquete de respuesta de eco ICMP correspondiente.

El PS DEBE permitir que la dirección IP de destino de la herramienta Ping (cabhCtpPingDestIp) se fije a cualquier dirección IPv4 válida de cualquier dispositivo IP de LAN o dispositivo del anfitrión de IPCable2Home accesible, a través de cualquier interfaz LAN del PS en el que esté funcionando la herramienta Ping del CTP.

El PS NO DEBE emitir paquetes a través de ninguna interfaz WAN cuando ejecute la función de la herramienta Ping.

El PS NO DEBE utilizar ninguna dirección IP como dirección IP de origen de la herramienta Ping (cabhCtpPingSrcIp), excepto una dirección IP actual válida de WAN-Data del PS (es decir, un valor de objeto cabhCdpWanDataAddrIp activo) o una dirección IP actual válida de interfaz de LAN del PS. Si se configura un valor no válido para cabhCtpPingSrcIp, el PS DEBE tratar la ejecución de la prueba como un caso abortado y fijar el objeto cabhCtpPingStatus de estado de la herramienta Ping a "abortado" y notificar el evento correspondiente (véase el cuadro B.1).

7 Herramientas de configuración

7.1 Introducción y visión general

El elemento de servicios de portal y los dispositivos IP de LAN deben inicializarse y configurarse convenientemente a fin de intercambiar información inteligible entre sí, con los elementos conectados a la red de cable y con Internet. Las herramientas de configuración de IPCable2Home permiten realizar esta inicialización y configuración sin interrupciones y con una intervención mínima por parte del usuario. Los operadores de cable pueden asimismo ofrecer a los abonados servicios de datos de alta velocidad de valor añadido mediante la definición de procesos, gracias a los cuales aquellos pueden facilitar y adaptar la inicialización y configuración del PS y el dispositivo IP de LAN. Las tres herramientas de configuración definidas para acometer estas tareas son las siguientes:

- La función portal DHCP (CDP) del elemento de servicios de portal.
- La herramienta de configuración de los servicios de portal en bloque (BPSC, *bulk portal services configuration*).
- El cliente de hora del día del elemento de servicios de portal.

7.1.1 Objetivos

A continuación se relacionan los objetivos de las herramientas de configuración:

- Permitir que el PS obtenga una dirección de red por su interfaz WAN que se utilizará para la gestión del PS.
- Permitir que el PS obtenga una o más direcciones de red por su interfaz WAN que se utilizarán para el intercambio de tráfico entre los dispositivos IP de LAN y la red Internet, o entre los dispositivos del anfitrión de IPCable2Home y la red Internet.
- Permitir que el PS solicite y obtenga los parámetros de configuración en un fichero de configuración.
- Permitir que el PS obtenga la hora del día actual a partir de los servicios de hora del día en la red de datos del operador del sistema de cable.
- Permitir que el PS asigne licencias de dirección de red a los dispositivos IP de LAN y a los dispositivos del anfitrión de IPCable2Home.
- Permitir que el PS asigne parámetros de configuración a los dispositivos IP de LAN y a los dispositivos del anfitrión de IPCable2Home.

7.1.2 Hipótesis

A continuación se relacionan las hipótesis de funcionamiento de las herramientas de configuración:

- Los dispositivos de IP de LAN y los dispositivos del anfitrión de IPCable2Home implementan un cliente DHCP conforme a [RFC 2131].
- El sistema de configuración de la red por cable implementa un servidor del DHCP como se define en [RFC 2131].
- Si el servidor del DHCP del sistema de configuración de la red de cable soporta la opción 61 del DHCP (opción de identificador de cliente), las interfaces IP de WAN-Man y de WAN-Data podrán compartir una dirección MAC común.
- Los dispositivos IP de LAN y los dispositivos del anfitrión de IPCable2Home pueden soportar varias opciones DHCP y extensiones BOOTP de fabricante, autorizadas según [RFC 2132].
- La configuración del PS en bloque se llevará a cabo a través de la descarga de un fichero de configuración de PS que contenga uno o más parámetros, utilizando el protocolo trivial de transferencia de ficheros (TFTP, *trivial file transfer protocol*) [RFC 1350] o el protocolo de transferencia de hipertexto (HTTP, *hypertext transfer protocol*) [RFC 2616] con seguridad de capa de transporte (TLS) [RFC 2246].
- El servidor DHCP de la cabecera proporcionará una opción DHCP, a la interfaz de WAN-Man, que señala hacia un servidor de hora del día en la red de la cabecera.

7.2 Arquitectura de configuración

7.2.1 Modos de configuración

Se soportan tres modos de configuración denominados: modo de configuración DHCP (modo DHCP), modo de configuración SNMP (modo SNMP) y modo CableHome aletargado. En el cuadro 7-1 se presenta una comparación de estos tres modos.

Cuadro 7-1/J.192 – Modos de configuración

	Modo DHCP	**Modo SNMP**	**Modo CableHome aletargado**
Campos DHCP y códigos facultativos	Recibe información del fichero de configuración en los campos 'siaddr' y 'file'. No recibe la opción 122.	No recibe información del fichero de configuración. Recibe valores válidos de las subopciones 3, 6 y 10 de la opción 122.	No recibe información del fichero de configuración ni de la opción 122, o recibe una combinación no válida de información del fichero de configuración y de las subopciones de la opción 122.
Activador del fichero de configuración del PS	Activado por la presencia de información del servidor TFTP en el mensaje DHCP.	Activado por el NMS mediante el mensaje SNMP.	El PS no recibe el fichero de configuración.
Requisito del fichero de configuración del PS	Es necesaria la descarga del fichero de configuración del PS.	No es necesaria la descarga del fichero de configuración del PS.	No es necesario el fichero de configuración del PS.

El comportamiento específico de las herramientas de configuración depende del modo de configuración que emplee el PS.

En la cláusula 13, Procesos de configuración, se describe la secuencia de los eventos correspondientes a los modos de configuración DHCP y SNMP.

7.2.2 Descripción de la arquitectura de configuración

En la figura 7-1 se ilustra la arquitectura de configuración. Los elementos de los servicios de portal interactúan con las funciones del servidor en la red de cable por la interfaz HFC, o con los dispositivos del anfitrión de IPCable2Home para satisfacer las directrices de diseño del sistema relacionadas en 7.3.2.

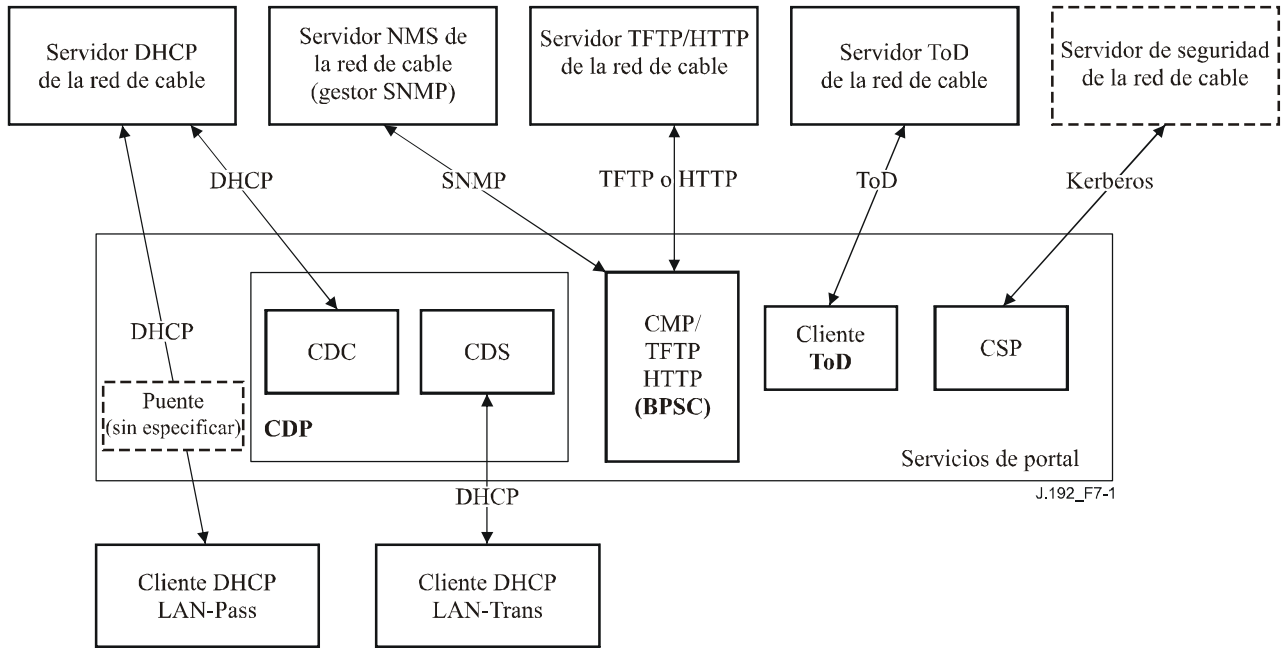


Figura 7-1/J.192 – Arquitectura de configuración

7.3 Elemento lógico del PS – Portal DHCP (CDP)

El portal DHCP de IPCable2Home (CDP) es un subelemento lógico del elemento lógico del PS. El CDP desempeña dos papeles principales: obtención de licencias de dirección de red para el PS y asignación de licencias de dirección de red a los dispositivos IP de LAN y a los dispositivos del anfitrión de IPCable2Home en la red LAN, y se trata de una de las tres herramientas de configuración que se introducen en 7.1. En la presente cláusula se describen los objetivos, las directrices de diseño del sistema, la descripción del sistema y los requisitos que corresponden al CDP.

7.3.1 Objetivos del CDP

Los objetivos del CDP incluyen:

- habilitar las funciones de cliente del PS para que pueda comunicarse con las funciones del servidor correspondiente en la red de datos por cable;
- proporcionar al PS los parámetros de configuración inicial para que disponga de la capacidad para que pueda seguir autoconfigurándose.

7.3.2 Directrices de diseño del sistema CDP

Las siguientes directrices de diseño (cuadro 7-2) controlan las capacidades definidas para el CDP:

Cuadro 7-2/J.192 – Directrices de diseño del sistema del CDP

Número	Directrices
CDP 1	Los mecanismos de direccionamiento serán controlados por el operador y facilitarán que éste disponga del conocimiento de los elementos de la red IPCable2Home y de los dispositivos IP de LAN, y el acceso a éstos.
CDP 2	Los procesos de adquisición y gestión de direcciones no exigirán la intervención humana (suponiendo que ya se haya establecido una cuenta de usuario o vivienda).
CDP 3	La adquisición y gestión de direcciones serán escalables a fin de soportar el aumento previsto del número de dispositivos IP de LAN.
CDP 4	Es preferible que las direcciones de los dispositivos IP de LAN permanezcan inalteradas tras eventos tales como un ciclo de alimentación o un cambio de proveedor de servicios de Internet.
CDP 5	Se suministrará un mecanismo de supervisión y control del número de dispositivos IP de LAN del sector LAN-Trans.
CDP 6	En el hogar, la comunicación continuará funcionando como se previó durante las caídas del servidor de direcciones de la cabecera. Se prestará soporte de direccionamiento a los dispositivos IP de LAN recién añadidos y a las direcciones cuya validez haya expirado durante las caídas del servidor de direcciones remoto.
CDP 7	Se conservarán las direcciones IP siempre que sea posible (esto afecta tanto a las direcciones encaminables mundialmente como a las direcciones de gestión de la red de cable privada).

7.3.3 Descripción del sistema del portal DHCP de IPCable2Home

El portal DHCP de IPCable2Home (CDP) es la entidad lógica encargada de las actividades de direccionamiento. Entre las responsabilidades de petición y atribución de direcciones del CDP en el entorno de IPCable2Home se encuentran las siguientes:

- Asignación de direcciones IP, mantenimiento de direcciones IP y entrega de parámetros de configuración (a través del DHCP) a los dispositivos IP de LAN del sector de direcciones LAN-Trans.
- Adquisición de una dirección WAN-Man y de alguna o ninguna dirección IP WAN-Data y de los parámetros de configuración DHCP asociados para el elemento de servicios de portal.
- Información al portal de nombres de IPCable2Home (CNP) como soporte de los servicios de nombre de servidor del dispositivo IP de LAN.

El PS mantiene dos direcciones de hardware, una que se utilizará para conseguir una dirección IP para fines de gestión y la otra que podría usarse para la obtención de una o varias direcciones IP para los datos. A fin de evitar la violación de la dirección de hardware, el PS no permite la modificación de ninguna de las dos direcciones de hardware.

El elemento de servicios de portal exige una dirección IP en la red LAN doméstica para que desempeñe un papel en la misma como encaminador (véase la cláusula 8, Tratamiento de paquetes y traducción de direcciones), servidor DHCP (CDS) y servidor DNS (véase la cláusula 9, Resolución de nombres). El PS atiende a una única dirección IP en el lado LAN para cada una de dichas funcionalidades. El PS ha de comunicar la dirección IP para cada una de dichas funcionalidades del servidor a los dispositivos IP de la LAN en los campos facultativos del DHCP OFFER y ACK. A fin de poder identificar inequívocamente los valores de dichas opciones,

cada una de dichas direcciones de servidor se identifican mediante objetos MIB diferentes en el PS, que se relacionan más adelante en el cuadro 7-2.

Dirección del encaminador (pasarela por defecto)	cabhCdpServerRouter	Opción 3
Dirección del servidor de nombres de dominio (DNS)	cabhCdpServerDnsAddress	Opción 6
Dirección del servidor del protocolo dinámico de configuración de anfitrión (DHCP) (CDS)	cabhCdpServerDhcpAddress	Opción 54

El valor por defecto de cabhCdpServerRouter es 192.168.0.1. Sin embargo, el NMS puede fijar cabhCdpServerRouter a un valor diferente.

El valor de cabhCdpServerDhcpAddress siempre es el mismo que el de cabhCdpServerRouter y NMS no puede cambiar directamente su valor.

El valor por defecto de cabhCdpServerDnsAddress es igual al valor de cabhCdpServerRouter. Sin embargo, el NMS puede cambiarlo a un valor distintos (por ejemplo, el servidor DNS de la red de datos del operador de cable) de forma que el dispositivo IP de LAN pueda dirigir sus consultas DNS a un servidor diferente del servidor DNS del PS.

Por lo tanto, el PS siempre observa la dirección IP asignada a cabhCdpSeverRouter para su funcionalidad de encaminador del lado LAN, servidor de nombres (DNS) y servidor DHCP.

Como se muestra en la figura 7-2, las capacidades del CDP están integradas en dos elementos funcionales que residen en el CDP:

- servidor DHCP de IPCable2Home (CDS).
- cliente DHCP de IPCable2Home (CDC).

La figura 7-2 ilustra asimismo la interacción entre los componentes del CDP y los sectores de direcciones presentados en la cláusula 5. El CDC intercambia mensajes DHCP con el servidor DHCP de la red de cable (sector de direcciones de gestión de la WAN) para obtener una dirección IP y opciones del DHCP para el PS, a efectos de gestión. El CDC podría intercambiar asimismo mensajes del DHCP con el servidor del DHCP de la red de cable (sector de direcciones WAN-Data) para obtener alguna o ninguna dirección IP en representación de los dispositivos IP de LAN del sector LAN-Trans. El CDS intercambia mensajes DHCP con los dispositivos IP de LAN en el sector LAN-Trans, asigna direcciones IP privadas, otorga licencias y puede ofrecer opciones DHCP a los clientes DHCP de dichos dispositivos IP de LAN.

Los dispositivos IP de LAN del sector LAN-Pass reciben sus direcciones IP, sus licencias y las opciones DHCP directamente del servidor DHCP de la red de cable. El CDP se limita a hacer de puente para los mensajes DHCP entre el servidor DHCP de la red de cable y los dispositivos IP de LAN del sector LAN-Pass.

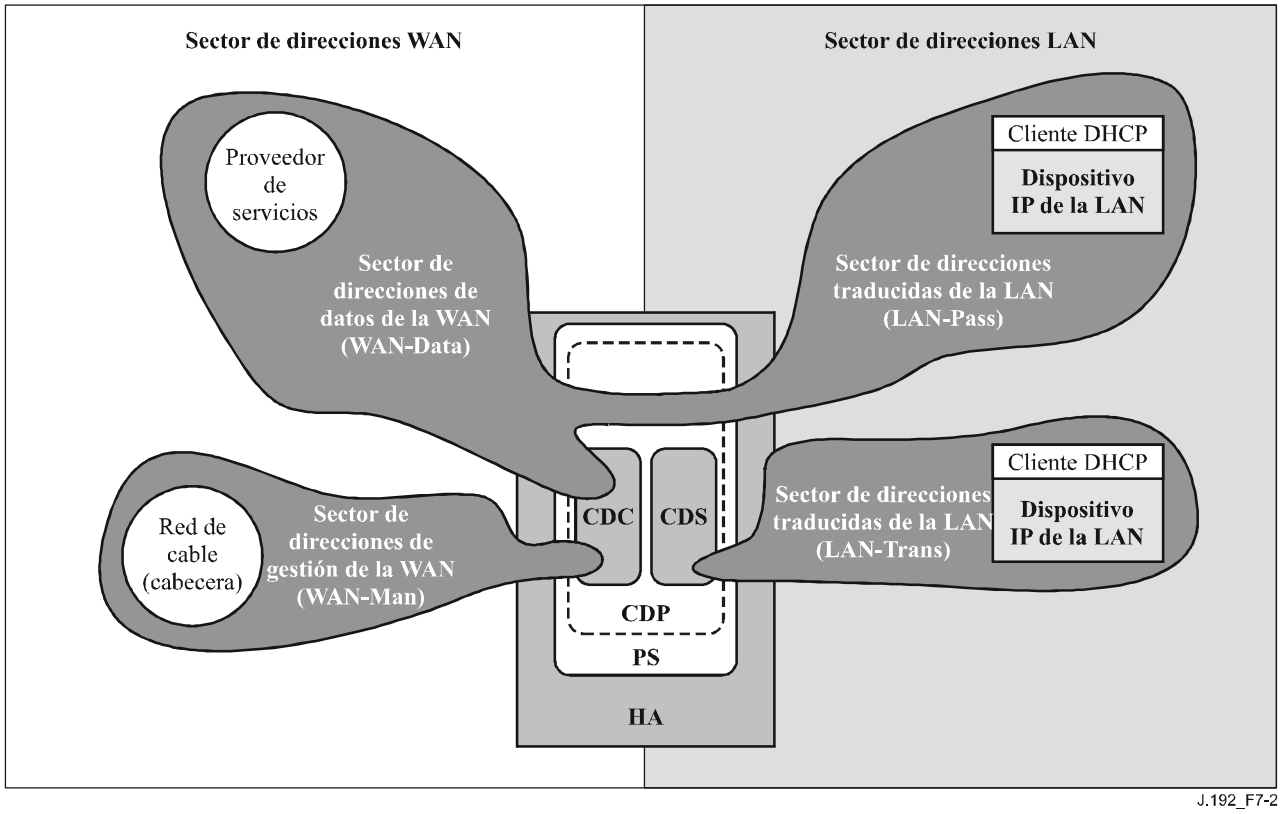


Figura 7-2/J.192 – Funciones del CDP

Un PS integrado puede configurarse en cualquiera de los cuatro modos de funcionamiento, tal como se describe en 5.5, en función del valor del objeto esafePsCableHomeModeControl de la MIB eSAFE eDOCSIS [eDOCSIS1] (sólo ePS) y de los valores de los campos y opciones del encabezamiento DHCP del mensaje DHCP ACK recibido del servidor DHCP del operador de cable. Si el valor de esafePsCableHomeModeControl se fija en provSystem(2), el PS integrado intenta adquirir la licencia de la dirección IP de la WAN-MAN del PS y actuar en función de los valores y opciones de la cabecera DHCP. Si el valor de esafePsCableHomeModeControl es dormantCHMode(3), es necesario que el PS integrado intente adquirir una licencia de dirección IP para utilizarla en su función de traducción de puerto y dirección de red (NAPT) (véase cláusula 8, Tratamiento de paquetes y traducción de direcciones) y para no tener en cuenta el campo del encabezamiento DHCP y los valores opcionales que lo configurarían para funcionar en un modo distinto al modo CableHome aletargado. En 7.3.3.2.4 figura una descripción completa del modo CableHome aletargado. Si esafePsCableHomeModeControl se fija como inhabilitado(1), el PS integrado no intenta la configuración y funciona en el modo inhabilitado tal como se describe en 7.3.3.2.4.

Un PS autónomo siempre ha de intentar adquirir una licencia de dirección IP de WAN-Man de PS y se configura para poder funcionar en cualquiera de los tres modos de funcionamiento, según sean los valores de los campos y opciones del encabezamiento DHCP. Un PS autónomo no puede ser configurado para funcionar en el modo inhabilitado. Para más información, véase 7.3.3.2.4.

7.3.3.1 Subelemento del servidor DHCP (CDS)

El CDS es un subelemento del elemento lógico CDP del PS, y representa la función encargada de asignar licencias de dirección de red a los dispositivos IP de LAN en el sector LAN-Trans. Además, se encarga de suministrar información de configuración a los dispositivos IP de LAN a través de códigos de opción del DHCP, conforme a [RFC 2132]. El CDS debe ejecutar esta función ya sea que el PS tenga una conexión WAN activa, o no la tenga.

7.3.3.1.1 Objetivos de la función CDS

Los objetivos de la función CDS incluyen:

- asignar licencias de dirección de red a los dispositivos IP de LAN en el sector LAN-Trans conforme a los valores de la MIB del CDP y a [RFC 2131];
- asignar información de configuración conforme a [RFC 2132];
- satisfacer los objetivos relativos al funcionamiento en ausencia de una conexión WAN, atribuyendo licencias de dirección IP de LAN-Trans y proporcionando información de configuración a los dispositivos IP de LAN cuando así lo soliciten, siempre que el PS se encuentre en funcionamiento, y tenga o no una conexión WAN activa;
- no atribuir licencias de dirección IP ni proporcionar información de configuración a los dispositivos IP de LAN para los cuales el PS haya sido configurado a modo de tratarlos como existentes en el sector LAN-Pass.

7.3.3.1.2 Directrices de diseño del sistema de la función CDS

En el cuadro 7-3 se presentan las directrices para desarrollar las especificaciones de esta función.

Cuadro 7-3/J.192 – Directrices de diseño del sistema de la función servidor DHCP de IPCable2Home (CDS)

Número	Directrices
CDS 1	Ofrece un medio para que los dispositivos IP de LAN pueden obtener licencias de dirección de red e información de configuración del sector LAN-Trans.
CDS 2	El mecanismo para atribuir direcciones IP de LAN-Trans e información de configuración debe funcionar independientemente de que el PS tenga una conexión WAN a la red de datos del operador del sistema de cable, o no la tenga.
CDS 3	El mecanismo para atribuir licencias de dirección IP de LAN-Trans e información de configuración no atribuirá ni esas licencias ni esa información a los dispositivos IP de LAN en el sector LAN-Pass.

7.3.3.1.3 Descripción del sistema de la función CDS

El CDS es un servidor DHCP normal definido en [RFC 2132], incluyéndose entre sus fines los siguientes:

- El CDS asigna direcciones y entrega parámetros de configuración del DHCP a los dispositivos IP de LAN que reciben una dirección del sector de direcciones LAN-Trans. El CDS se entera de las opciones DHCP por el sistema NMS y proporciona estas opciones DHCP a los dispositivos IP de LAN. Si las opciones DHCP no hubieran sido proporcionadas por el sistema NMS (por ejemplo, cuando el PS arranca o durante una desconexión del cable), el CDS utilizaría los valores por defecto integrados (DefVals) de las opciones requeridas.
- El CDS es capaz de proporcionar servicios de direccionamiento DHCP a los dispositivos IP de LAN, con independencia del estado de conectividad de la WAN.
- El número de direcciones que el CDS suministra a los dispositivos IP de LAN se puede controlar por medio del sistema NMS. El comportamiento del CDS cuando se sobrepasa el límite, ajustable por el operador de cable, también puede configurarse mediante el NMS. Entre las posibles acciones del CDS cuando se supera dicho límite se encuentran:
  1) asignar una dirección IP LAN-Trans y tratar la interconexión CAT de la WAN a la LAN como se haría normalmente si no se hubiera superado el límite; y

2) no asignar direcciones a los dispositivos IP de LAN solicitantes.

Un valor 0 para el umbral de dirección indica el máximo umbral posible para el grupo de direcciones IP de LAN-Trans definido por los valores del grupo "start" (cabhCdpLanPoolStart) y "end" (cabhCdpLanPoolEnd).

- A falta de información horaria procedente del servidor de hora del día (ToD, *time of day*), el CDS utiliza el tiempo de arranque por defecto del PS, es decir las 00:00.0 (medianoche) GMT, el 1 de enero 1970, actualiza los plazos de expiración de las licencias activas en el sector LAN-Trans para volver a sincronizarse con los clientes DHCP en los dispositivos IP de LAN y mantiene las licencias basadas en dicho instante de arranque hasta que el PS se sincronice con el servidor de hora del día de la red de cable.
- Durante el proceso de rearranque del PS, el CDS se mantiene inactivo hasta ser activado por el PS.
- Si el modo de tratamiento de paquetes primario del PS (cabhCapPrimaryMode) se hubiera fijado a Passthrough (transferencia) y se hubiera completado el proceso de configuración del PS (indicado por cabhPsDevProvState = pass(1)), se desactivaría el CDS.

Los dispositivos IP de LAN pueden recibir direcciones que residan en el sector LAN-Pass. Como muestra la figura 7-2, las peticiones de direcciones LAN-Pass son atendidas por la infraestructura de direccionamiento de la WAN y no por el PS. Los procesos de direccionamiento de LAN-Pass tendrán lugar cuando el PS se configure para funcionar en modo de transferencia o en modo mixto puenteo/encaminamiento (véase 8.3.4.3, Requisitos de la transferencia, si se desean obtener más detalles). En dichos casos, las interacciones DHCP tendrán lugar directamente entre los dispositivos IP de LAN y los servidores de la red de datos por cable, no especificándose el proceso en la presente Recomendación.

En esta Recomendación, los términos **atribución dinámica** y **atribución manual** se utilizan conforme a [RFC 2132]. Las **opciones DHCP configuradas por el CDS**, objetos cabhCdpServer en la MIB del CDP, son opciones del DHCP que pueden ser configuradas por el NMS, y ofrecidas por el CDS a los dispositivos IP de LAN a los que se les asigna una dirección de LAN-Trans. Las opciones DHCP configuradas por el CDS antes referidas se conservan tras un ciclo de alimentación del PS y el sistema NMS podrá establecer, leer, escribir y suprimir dichos objetos. Estas opciones se conservan también durante los periodos de desconexión del cable ofreciéndose dichos objetos a los dispositivos IP de LAN a los que se les ha asignado una dirección LAN-Trans. La conservación permanente de las opciones DHCP en la memoria del CDS es congruente con la sección 2.1 de [RFC 2132]. Los valores por defecto de dichas opciones del DHCP se definen en el cuadro 7-4 pudiendo el NMS reinicializa las opciones DHCP configuradas por el CDS, objetos cabhCdpServer y cabhCdpLanAddrTable a sus valores por defecto, al escribir en el objeto de la MIB cabhCdpSetToFactory.

Los objetos del umbral de direcciones del CDS (cabhCdpLanTrans) contienen los parámetros de control de eventos utilizados por el CDS para indicar al CMP que genere una notificación al sistema de gestión de cabecera cuando el número de direcciones LAN-Trans asignadas por el CDS supere el umbral preestablecido.

El objeto contador de direcciones (cabhCdpLanTransCurCount) es un valor que indica el número de direcciones LAN-Trans asignadas por el CDS con licencias DHCP activas.

El objeto umbral de direcciones (cabhCdpLanTransThreshold) es un valor que indica al sistema de gestión de la cabecera la generación de una notificación. La notificación se genera cuando el CDS asigna una dirección al dispositivo IP de LAN que provoca que el contador de direcciones (cabhCdpLanTransCurCount) sobrepase el umbral de direcciones (cabhCdpLanTransThreshold).

La acción de umbral sobrepasado (cabhCdpLanTransAction) es la emprendida por el CDS cuando el contador de direcciones (cabhCdpLanTransCurCount) sobrepasa el umbral de direcciones (cabhCdpLanTransThreshold). Si la acción de umbral sobrepasado (cabhCdpLanTransAction)

permite que se asignen direcciones una vez sobrepasado el contador, se genera una notificación cada vez que se asigna una dirección. Las acciones definidas son las siguientes:

a) asignar una dirección LAN-Trans con normalidad; y

b) no asignar dirección alguna al siguiente dispositivo IP de LAN que efectúe una petición.

El contador de direcciones (cabhCdpLanTransCurCount) continúa actualizándose durante los periodos de desconexión del cable.

La MIB del CDS contiene asimismo los parámetros comienzo del grupo de direcciones (cabhCdpLanPoolStart) y final del grupo de direcciones (cabhCdpLanPoolEnd). Estos parámetros indican el intervalo de direcciones del sector LAN-Trans que el CDS puede asignar a dispositivos IP de LAN.

El cuadro de direcciones LAN del CDP (cabhCdpLanAddrTable) contiene la lista de parámetros asociados a las direcciones asignadas a los dispositivos IP de LAN con direcciones LAN-Trans. Entre estos parámetros se encuentran:

- Los identificadores de cliente mencionados en la sección 9.14 de [RFC 2132] (cabhCdpLanAddrClientID).
- Las direcciones IP de LAN asignadas al cliente (cabhCdpLanAddrIp).
- Una indicación de si la dirección se asignó manualmente (a través del CMP) o dinámicamente (a través del CDP) (cabhCdpLanAddrMethod).

El CDS almacena información de identificación del dispositivo IP de LAN en el objeto de la MIB cabhCdpLanAddrClientID. El CDS utiliza el valor transferido en el campo chaddr del mensaje DHCP REQUEST enviado por el dispositivo IP de LAN para este fin.

El CDS crea una anotación en el cuadro CDP (cabhCdpLanAddrTable) cuando asigna una dirección IP a un dispositivo IP de LAN. El CDS puede crear anotaciones en el cuadro CDP (cabhCdpLanAddrTable) durante los periodos de desconexión del cable.

El cuadro CDP (cabhCdpLanAddrTable) mantiene un tiempo de licencia DHCP para cada uno de los dispositivos IP de LAN.

Las anotaciones del cuadro CDP (cabhCdpLanAddrTable) proporcionadas por el NMS se conservan durante los periodos de desconexión del cable y se mantienen tras un ciclo de alimentación del PS.

7.3.3.1.4 Requisitos de la función CDS

El PS DEBE cumplir con los requisitos del servidor conforme a la sección 4.3 de [RFC 2131].

El PS DEBE soportar la asignación dinámica y manual de direcciones conforme a la sección 1 de [RFC 2131].

La asignación manual de direcciones IP del PS DEBE soportarse efectuando anotaciones en cabhCdpLanAddrTable de la MIB del CDP, creadas a través del sistema NMS o del fichero de configuración del PS.

Como soporte de la asignación dinámica de direcciones IP, el PS DEBE ser capaz de crear, modificar y suprimir anotaciones en cabhCdpLanAddrTable de los dispositivos asignados a la dirección LAN-Trans.

El PS DEBE conservar las anotaciones del cuadro (cabhCdpLanAddrTable) de gestión de direcciones de LAN del CDP durante una interrupción del cable y después de un ciclo de alimentación del PS. El PS DEBE ser capaz de ofrecer servicios de direccionamiento DHCP a los dispositivos IP de LAN cuando así lo habilite el PS, independientemente del estado de conectividad de la WAN.

Después de la reinicialización o del rearranque del PS, éste NO DEBE intercambiar mensajes DHCP con los dispositivos IP de LAN hasta que el PS active el CDS.

El PS DEBE activar el CDS, es decir, el PS DEBE comenzar a responder a los mensajes DHCP DISCOVER y DHCP REQUEST recibidos a través de cualquier interfaz LAN del PS, bajo cualquiera de las siguientes condiciones (véase además la figura 13-2, Modos de configuración de IPCable2Home – Parte 1):

- Cuando el PS se encuentra funcionando en el modo de configuración DHCP, tras de que el CDC haya recibido una licencia de dirección IP de WAN-Man del PS y el PS haya recibido y procesado adecuadamente un fichero de configuración del PS.
- Cuando el PS se encuentra funcionando en el modo de configuración SNMP, tras de que el CDC haya recibido una licencia de dirección IP de WAN-Man del PS haya efectuado la autenticación ante el servidor del centro de distribución de claves (KDC, *key distribution centre*) y haya sido admitido satisfactoriamente por el NMS.
- Cuando fracasa el primer intento del CDC para conseguir una licencia de dirección IP del sector WAN-Man del PS.
- Cuando el PS se encuentra funcionando en el modo de configuración DHCP y fracasa el primer intento para descargar o procesar el fichero de configuración del PS.
- Cuando el PS se encuentra funcionando en el modo de configuración SNMP y fracasa el intento de autenticación ante el servidor KDC.
- Cuando el PS se encuentra funcionando en el modo de configuración SNMP y se activa para descargar un fichero de configuración del PS antes de que se inicie el funcionamiento del CDS, y fracasa el primer intento para descargar o procesar el fichero de configuración del PS.

El PS DEBE asignar una dirección IP disponible única de la gama de direcciones que comienza con cabhCdpLanPoolStart y termina con cabhCdpLanPoolEnd, a cada dispositivo de IP de LAN en el sector LAN-Trans que solicite una dirección IP utilizando DHCP, si el número de direcciones IP ya asignado por el CDS es menor que el valor de cabhCdpLanTransThreshold.

Si el valor de cabhCdpLanTransThreshold es 0, el PS DEBE tratar el umbral como si se le hubiera asignado el valor más grande posible para el tamaño del grupo de direcciones IP de LAN-Trans (definido por los valores de arranque (cabhCdpLanPoolStart) y de terminación (cabhCdpLanPoolEnd) del grupo de direcciones IP de LAN-Trans).

El PS DEBE mantener el parámetro contador de direcciones (cabhCdpLanTransCurCount) que indica el número de licencias de dirección LAN-Trans activas otorgadas a los dispositivos IP de LAN.

El PS DEBE aumentar el recuento de direcciones cada vez que se otorga una licencia para una dirección LAN-Trans a un dispositivo IP de LAN y DEBE disminuirlo cada vez que se suprime una dirección de LAN-Trans o expira una licencia de dirección de LAN-Trans.

El PS DEBE comparar el parámetro contador de direcciones (cabhCdpLanTransCurCount) con el parámetro umbral de dirección (cabhCdpLanTransThreshold) tras asignar una dirección LAN-Trans. Si ese parámetro contador de direcciones sobrepasa el parámetro de umbral de dirección (cabhCdpLanTransThreshold), el PS DEBE generar una notificación de acuerdo al mecanismo de notificación de eventos que se define en 6.3.3.2, Función de notificación de eventos del CMP y en el anexo B. Si el parámetro contador de direcciones (cabhCdpLanTransCurCount) rebasa el parámetro umbral de dirección (cabhCdpLanTransThreshold), el PS DEBE ser capaz de tomar las medidas necesarias relativas al umbral excedido para el siguiente mensaje DHCP DISCOVER de la LAN: asignar una dirección LAN-Trans como normal o no asignar ninguna dirección.

Si cabhCdpLanTransCurCount iguala o excede a cabhCdpLanTransThreshold y un dispositivo IP de LAN solicita una licencia de dirección IP adicional, el PS DEBE tomar la medida particular indicada por el parámetro configurado medida de umbral excedido (cabhCdpLanTransAction).

El PS DEBE asignar direcciones IP y distribuir los parámetros de configuración DHCP relacionados en el cuadro 7-4 para los cuales el CDS tiene un valor válido, únicamente a los dispositivos IP de LAN que reciben una dirección del sector de direcciones LAN-Trans.

Si el operador de cable proporciona valores para una fila en cabhCdpLanAddrTable, el PS (CDS) DEBE ofrecer una licencia (es decir, tratar de asignar) para la dirección IP cabhCdpLanAddrIp configurada, al dispositivo IP de LAN cuya dirección de hardware corresponde al cabhCdpLanAddrClientID proporcionado, en respuesta a un mensaje DHCP DISCOVER que se recibió del dispositivo IP de LAN.

Si el CDS asigna una licencia activa de una dirección IP a un dispositivo IP de LAN, el PS DEBE suprimir esa dirección del grupo de direcciones IP disponibles para asignarlas a dispositivos IP de LAN.

Si el CDS recibe una petición de licencia de un dispositivo IP de LAN y no puede satisfacerla debido a la falta de direcciones en el grupo de direcciones IP (definido por cabhCdpLanPoolStart y cabhCdpLanPoolEnd), el PS DEBE notificar el evento conforme al anexo B y al mecanismo de notificación de eventos que se define en 6.3.3.2, Función de notificación de eventos del CMP.

Cuando se crea una licencia activa para el dispositivo IP de LAN, el PS DEBE almacenar el valor transferido en el campo chaddr del mensaje DHCP REQUEST enviado por el dispositivo IP de LAN.

El PS DEBE soportar todos los objetos MIB del CDP, incluidos todos los objetos cabhCdpLanAddrTable, cabhCdpLanPool, cabhCdpServer y cabhCdpLanTrans.

La función CDS del PS DEBE soportar las opciones DHCP obligatorias indicadas en la columna de soporte de protocolo del CDS en el cuadro 7-4, Opciones DHCP del CDS.

El CDS DEBE incluir en los mensajes DHCP OFFER y DHCP ACK que envía a sus clientes DHCP, la subopción 101 de la opción código 43 del DHCP que incluye la cadena "CableHome1.1 LAN-Trans" (sin espacios y sin las comillas) como información de la subopción, únicamente en respuesta a los mensajes DHCP DISCOVER y DHCP REQUEST que incluyen la opción código 60 del DHCP que incluye a su vez el valor de cadena "CableHome1.1BP" (sin espacios y sin las comillas).

El CDS NO DEBE incluir la subopción 101 de la opción código 43 del DHCP en los mensajes DHCP OFFER y DHCP ACK que envíe a cualquier cliente DHCP que no haya proporcionado el valor de cadena "*CableHome1.1BP*" en la opción código 60 del DHCP, en sus mensajes DHCP DISCOVER y DHCP REQUEST.

La función CDS del PS DEBE soportar la oferta de los valores por defecto indicados en la columna de valores por defecto de fábrica del CDS en el cuadro 7-4, Opciones DHCP del CDS, si la opción DHCP no ha sido configurada con otros valores.

Si el modo de tratamiento de paquetes primario del PS (cabhCapPrimaryMode) se ha fijado a transferencia y el proceso de configuración del PS se ha completado (indicado por cabhPsDevProvState = pass(1)), en ese caso la función CDS del PS DEBE inhabilitarse.

La función CDS del PS NO DEBE responder a los mensajes DHCP que reciba a través de cualquier interfaz WAN, ni originar mensajes DHCP por ninguna interfaz WAN.

La función CDS del PS NO DEBE distribuir ninguna opción DHCP con valor nulo a ningún dispositivo IP de LAN.

El CDS NO DEBE ofrecer una licencia de dirección IP 192.168.0.1, es decir, el CDS NO DEBE transmitir una oferta DHCP o un mensaje DHCP Ack con el valor 192.168.0.1 en el campo yiaddr.

Se distingue específicamente el caso en que el PS está en el estado de cabhPsDevProvState denominado de configuración inProgress(2). En ese caso, cuando el PS proporciona una licencia de la dirección DHCP al cliente o clientes CPE de la LAN, DEBE fijar el valor 60 para la opción 51, tiempo o duración de la licencia de la dirección IP, en lugar del valor 3600 especificado en el cuadro 7-4.

Cuadro 7-4/J.192 – Opciones DHCP del CDS

Número de la opción	Función de la opción	Soporte del protocolo CDS (M) Obligatorio u (O) Opcional	Datos por defecto de fábrica del CDS	Nombre del objeto MIB
0	Rellenar	M	N/A	N/A
255	Terminar	M	N/A	N/A
1	Máscara de subred	M	255.255.255.0	cabhCdpServerSubnetMask
2	Diferencia horaria	M	0	cabhCdpServerTimeOffset
3	Opción del encaminador	M	192.168.0.1	cabhCdpServerRouter
6	Servidor de nombres de dominio	M	192.168.0.1	cabhCdpServerDnsAddress
7	Servidor de anotaciones históricas	M	0.0.0.0	cabhCdpServerSyslogAddress
12	Nombre del servidor	M	N/A	N/A
15	Nombre de dominio	M	Cadena nula	cabhCdpServerDomainName
23	Tiempo de vida por defecto	M	64	cabhCdpServer TTL
26	MTU de la interfaz	M	N/A	cabhCdpServerInterfaceMTU
43	Información específica del fabricante	M	Seleccionado por el fabricante	cabhCdpServerVendorSpecific
43.101	Subopción 101 de información específica del fabricante	M (nota)	Cadena: "CableHome 1.1 LAN-Trans" (sin espacios)	N/A
50	Dirección IP solicitada	M	N/A	N/A
51	Tiempo de licencia de la dirección IP	M	3600 segundos	cabhCdpServerLeaseTime
54	Identificador del servidor	M	192.168.0.1	cabhCdpServerDhcpAddress
55	Lista de petición de parámetros	M	N/A	N/A
60	Identificador de la clase de fabricante	M	N/A	N/A
61	Identificador del cliente	O	N/A	N/A
NOTA – El CDS debe incluir la subopción 101 de la opción 43 del DHCP con la cadena CableHome 1.1 LAN-Trans sin espacios en los mensajes DHCP OFFER y DHCP ACK que envía y que son exclusivamente conformes con los dispositivos IP de LAN. La conformidad con IPCable2Home de los dispositivos IP de LAN se indica mediante la cadena CableHome1.1BP en los mensajes DHCP DISCOVER y DHCP REQUEST.				

7.3.3.2 Función de cliente DHCP del CDP (CDC)

7.3.3.2.1 Objetivos de la función CDC

Los objetivos de la función CDC del CDP incluyen:

- obtener una licencia de dirección IP para la pila de protocolos IP del PS, que se emplea para los mensajes de gestión y la transferencia de ficheros entre los servidores de la red del operador de cable y el PS;
- obtener información de configuración del servidor DHCP de la red del operador de cable;
- determinar el modo de configuración en el que debe funcionar el PS;
- obtener una o varias licencias de dirección IP para la correspondencia con los dispositivos IP de LAN en el sector LAN-Trans.

7.3.3.2.2 Directrices de diseño del sistema de la función CDC

Las directrices que se relacionan en el cuadro 7-5 se utilizaron para orientar la especificación de la función CDC.

Cuadro 7-5/J.192 – Directrices de diseño del sistema de la función de cliente DHCP de IPCable2Home (CDC)

Número	Directrices
CDC 1	Ofrece un medio por el cual el PS puede conseguir una licencia de dirección de red e información de configuración para su interfaz WAN-Man.
CDC 2	Ofrece un medio por el cual el PS puede conseguir una o varias licencias de dirección de red e información de configuración para su interfaz WAN-Data.
CDC 3	El mecanismo para atribuir licencias de dirección IP de LAN-Trans e información de configuración no atribuirá dichas licencias ni dicha información a los dispositivos IP de LAN en el sector LAN-Pass.

7.3.3.2.3 Descripción del sistema de la función CDC

El CDC es un cliente DHCP normal definido en [RFC 2131], incluyéndose entre sus fines los siguientes:

- El CDC lanza peticiones a los servidores DHCP de la cabecera para la adquisición de direcciones del sector WAN-Man pudiendo lanzar peticiones a los servidores DHCP de cabecera para la adquisición de direcciones en los sectores de direcciones WAN-Data. El CDC interpreta asimismo ciertos parámetros de configuración DHCP y actúa sobre ellos.
- El CDC determina en qué modo de configuración ha de funcionar el PS, basándose en información que recibe en el mensaje DHCP ACKNOWLEDGE de su servidor DHCP.
- El CDC soporta la adquisición de una dirección IP WAN-Man y de ninguna o alguna dirección IP WAN-Data.
- El CDC soporta la opción de identificador de clase de fabricante (opción 60 del DHCP), la opción de información específica del fabricante (opción 43 del DHCP), y la opción de identificador del cliente (opción 61 del DHCP).
- Por defecto, el CDC adquirirá una única dirección IP para ser utilizada simultáneamente por las interfaces WAN-Man y WAN-Data a fin de reducir al mínimo las modificaciones necesarias de los servidores DHCP de cabecera existentes. En esta situación por defecto no se exige la utilización de un identificador de cliente (opción 61 del DHCP) por parte del CDC.

- El CDC de un PS autónomo genera una petición de renovación de licencia cuando el PS detecta que se ha caído el enlace de WAN con el módem de cable y ha sido posteriormente restablecido. El PS autónomo puede considerar que la pérdida de sincronización y posterior sincronización del enlace de la WAN con el módem de cable es equivalente a una reinicialización del módem de cable. Dado que cuando se reinicializa el módem de cable pierde cualquier anotación APR que retransmita información a las direcciones MAC que el PS autónomo tuviera antes de la reinicialización, es necesario un mecanismo para que el módem de cable vuelva a reconocer todas las direcciones MAC del PS que reciben tramas de RF a través del mismo. El PS autónomo utiliza la información de pérdida y recuperación para iniciar la renovación DHCP de todas las licencias de direcciones IP que hubieran sido adquiridas mediante DHCP y que aún sean válidas. Dicho mensaje de renovación DHCP permite al módem de cable conocer las direcciones MAC del PS autónomo y restablecer la retransmisión de MAC que debe llevar a acabo para las tramas en RF destinadas al dispositivo PS autónomo.

El CDP soporta diversas opciones DHCP y extensiones BOOTP del fabricante, contempladas en [RFC 2132].

El CDC determina el modo de configuración en el que ha de funcionar el PS basándose en información que recibe del servidor DHCP en el mensaje DHCP ACK, como se describe en 5.5, Modelos de funcionamiento de IPCable2Home. El modo de configuración de un PS integrado puede también realizarse mediante un módem de cable conforme con eDOCSIS, fijando el valor del objeto MIB esafePsCableHomeModeControl [Rec. UIT-T J.126]. Si esafePsCableHomeModeControl se fija en provSystem(2), el ePS es necesario para iniciar el proceso de configuración, y el CDC determina el modo de configuración. Si esafePsCableHomeModeControl se fija en disabledMode(1) o dormantCHMode(3), el CDC no participa en la determinación del modo de configuración o de funcionamiento.

Modo de funcionamiento de la configuración DHCP

El PS funciona en el modo de configuración DHCP si recibe un nombre de fichero válido para el fichero de configuración del PS en el campo *file* y una dirección IP válida en el campo *siaddr* del mensaje DHCP ACK, y *no* recibe las subopciones 3, 6 ó 10 de la opción 122 del DHCP.

A continuación se resume el comportamiento del PS cuando funciona en el modo de configuración DHCP:

- necesita descargar un fichero de configuración del PS de un servidor de ficheros de red del sistema de cable;
- por defecto utiliza SNMPv1 y SNMPv2c para los mensajes de gestión;
- por defecto utiliza docsDevNmAccessTable de la MIB del dispositivo DOCSIS [RFC 2669] para el control de acceso a la base de datos del PS a través de MIB específicas;
- podrá configurarse de manera que utilice la seguridad de capa de transporte (TLS) [RFC 2246] para autenticar y criptar el fichero de configuración del PS (véase 11.9, Seguridad del fichero de configuración del PS en el modo de configuración DHCP);
- podrá configurarse para que funcione en el modo de coexistencia SNMPv3, utilizando la gestión de claves Diffie-Hellman [RFC 2786], (véase 6.3.3.1.4.2.2).

Modo de funcionamiento de la configuración SNMP

El PS funciona en el modo de configuración SNMP si recibe la opción 122 del DHCP con los campos de subopción 3, 6 y 10, y *no* recibe un nombre de fichero válido en el campo *file* ni una dirección IP válida en el campo *siaddr* del mensaje DHCP ACK.

A continuación se resume el comportamiento del PS durante su funcionamiento en el modo de configuración SNMP:

- No es necesario descargar un fichero de configuración de PS del servidor de ficheros de la red de cable. En cualquier momento, el PS podrá activarse para que descargue un fichero de configuración del PS pero funcionará utilizando los parámetros por defecto de fábrica si no se descarga un fichero de configuración del PS.
- Un temporizador configurable (cabhPsDevProvisioningTimer) controla el tiempo que debe esperar el PS para ser activado a fin de descargar un fichero de configuración una vez realizada la autenticación con el KDC y haber emitido un informe SNMP de admisión de configuración. El valor de cabhPsDevProvState cambia de inProgress(2) a pass(1) una vez transcurrido el tiempo especificado por cabhPsDevProvisioningTimer si no se activa el PS para descargar un fichero de configuración. Si el gestor de SNMP activa el PS para la descarga de un fichero de configuración antes de que haya vencido el temporizador de configuración, el valor de cabhPsDevProvState no cambia a pass(1) hasta que el PS haya descargado con éxito y completado el procesamiento del fichero de configuración del PS.
- El PS funciona por defecto en el modo coexistencia SNMPv3 con el soporte de SNMPv1 y SNMPv2 *inhabilitado* (véase 11.4, Mensajería de gestión segura hacia el PS).
- El PS utiliza por defecto el modelo de seguridad basado en el usuario de SNMPv3 [RFC 3414] y el modelo de control de acceso basado en vistas de SNMPv3 [RFC 3415] para poder controlar el acceso a la base de datos del PS a través de MIB específicas (véase 11.4).
- El PS utiliza el intercambio de mensajes Kerberos con un servidor del centro de distribución de claves cuya dirección IP haya sido proporcionada al PS en la subopción 51 de la opción 177 del DHCP, y emplea un oyente AP para autenticar los mensajes SNMPv3 (véase 11.4.4.2, Algoritmos de seguridad para SNMPv3 en el modo de configuración SNMP).
- El PS puede configurarse de modo que reciba y procese mensajes SNMPv1 y SNMPv2c así como mensajes SNMPv3.

Modo CableHome aletargado

El PS funcionará en el modo CableHome aletargado si no recibe la combinación de campo *file*, campo *siaddr* o las subopciones de la opción código 122 del DHCP para configurarlo en el modo de configuración DHCP, ni la combinación de estos campos y subopciones para configurarlo en el modo de configuración SNMP. Un PS integrado puede también configurarse para funcionar en el modo CableHome aletargado a través de una MIB de módem de cable integrado que sea conforme con eDOCSIS [Rec. UIT-T J.126]. Si el valor del objeto MIB eSAFE eDOCSIS esafePsCableHomeModeControl es dormantCHMode(3), el PS integrado ha de funcionar en el modo CableHome aletargado, con independencia de los valores de los campos field y siaddr o de la opción 122 del DHCP presente en los mensajes DHCP recibidos del servidor DHCP del operador de cable.

Cuando el PS se encuentra funcionando en el modo CableHome aletargado, su comportamiento ha de ser el descrito en 7.3.3.2.4, incluyendo lo siguiente. Este modo de funcionamiento se diseña a modo de permitir que el PS funcione y realice funciones de pasarela residencial cuando se conecte a una red de datos por cable que aún no soporte los sistemas de configuración y de gestión de IPCable2Home:

- rechazar cualquier mensaje SNMP que se reciba por cualquier interfaz WAN.
- inhabilitar la función de cliente TFTP.
- inhabilitar las notificaciones de eventos SYSLOG.

- detener el temporizador de configuración.
- habilitar la funcionalidad de CNP, CAP, USFS y CDS.

Es necesario que el PS incluya ciertos campos facultativos del DHCP en los mensajes DHCP DISCOVER y DHCP REQUEST que emite a los servidores DHCP de la red de cable. La opción de identificador de clase de fabricante (opción 60 del DHCP) define una clase de dispositivo CableLabs. En esta Recomendación, la opción identificador de clase de fabricante incluirá la cadena "CableHome1.1", para identificar un elemento lógico de servicios de portal (PS) conforme, cuando el CDC solicite una dirección de WAN-Man o WAN-Data.

La opción de información específica de fabricante (opción 43 del DHCP) identifica con mayor detalle el tipo de dispositivo y sus capacidades. Esta opción describe el tipo de componente que efectúa la petición (CM o PS integrado o autónomo), los componentes incluidos en el dispositivo (CM, MTA, PS, etc.), el número de serie del dispositivo, y además acepta parámetros específicos de dispositivo. La opción 43 del DHCP y sus subopciones se definen en 7.3.3.2.4.

En los cuadros 7-6 y 7-7 se indican con detalle los requisitos necesarios para soportar las opciones 60 y 43 del DHCP. En el cuadro 7-8 se proporcionan los detalles relativos a otras opciones facultativas y obligatorias del DHCP.

El parámetro contador de direcciones IP de WAN-Data de la MIB de CDP (cabhCdpWanDataIpAddrCount) representa el número de licencias de dirección IP que el CDC ha de tratar de obtener para el lado WAN de las correspondencias entre NAT y NAPT. El valor por defecto de cabhCdpWanDataIpAddrCount es cero, lo que significa que, por defecto, el CDC conseguirá sólo una dirección IP de WAN-Man.

7.3.3.2.3.1 Opción 61 del cliente eDHCP

El elemento PS puede tener una o más direcciones IP de WAN asociadas con una o más interfaces de capa de enlace (por ejemplo, MAC). Por consiguiente, el CDC no puede confiar sólo en una dirección MAC como un valor único de identificador de cliente.

Esta Recomendación permite la utilización de la opción de identificador de cliente (opción 61 del DHCP), sección 9.14 de [RFC 2132], para identificar de forma única la interfaz WAN lógica asociada a una dirección IP particular.

Es necesario que el PS tenga dos direcciones de hardware: una que se empleará para identificar de forma única la interfaz WAN lógica asociada con la dirección IP de WAN-Man (dirección de hardware de WAN-Man) y la otra para identificar de forma única la interfaz WAN lógica asociada con las direcciones IP de WAN-Data (dirección de hardware de WAN-Data).

7.3.3.2.3.2 Modos de direccionamiento WAN

A fin de facilitar la compatibilidad con tantos sistemas de configuración del operador de cable como sea posible, el CDC deberá soportar los siguientes modos de direccionamiento WAN configurables:

Modo 0 de direccionamiento WAN

El elemento PS utiliza una sola dirección IP de WAN, obtenida mediante DHCP utilizando la dirección del hardware de WAN-Man. El elemento PS tiene una interfaz IP de WAN-Man y ninguna interfaz IP de WAN-Data. Este modo de direccionamiento sólo podrá aplicarse cuando el modo de tratamiento de paquetes primario del PS (cabhCapPrimaryMode) se fije a transferencia (véase 8.3.2). Por lo general, el servidor DHCP de la cabecera del operador del sistema de cable no necesita modificaciones de software para soportar este modo de direccionamiento. Durante el modo 0 de direccionamiento WAN, el valor de cabhCdpWanDataIpAddrCount es cero.

Modo 1 de direccionamiento WAN

El elemento PS utiliza una sola dirección IP de WAN, obtenida mediante DHCP utilizando la dirección de hardware de WAN-Man. El elemento PS tiene una interfaz IP de WAN-Man y una de WAN-Data. Esta dos interfaces comparten una sola dirección IP común. Este modo de direccionamiento sólo puede aplicarse cuando el modo de tratamiento de paquetes primario del PS (cabhCapPrimaryMode) se fije a NAPT. Por lo general, el servidor DHCP de la cabecera del operador del sistema de cable no necesita modificar el software para soportar este modo de direccionamiento. Durante el modo 1 de direccionamiento WAN, el valor de cabhCdpWanDataIpAddrCount es cero.

Modo 2 de direccionamiento WAN

El elemento PS obtiene una dirección IP de WAN-Man utilizando la dirección única de hardware de WAN-Man, y se configura posteriormente mediante el NMS para solicitar una o más direcciones únicas de IP de WAN-Data. El elemento PS tendrá una interfaz IP de WAN-Man y una o varias interfaces IP de WAN-Data. Todas las direcciones IP de WAN-Data compartirán una dirección de hardware común que es única a partir de la dirección de hardware de WAN-Man. Las dos o más interfaces (una de WAN-Man y una o varias de WAN-Data) tienen, cada una, su propia dirección IP no compartida. El operador del sistema de cable configura el CDP para que funcione en el modo 2 de direccionamiento WAN al escribir un valor distinto de cero en cabhCdpWanDataIpAddrCount, a través del fichero de configuración del PS o de una petición de establecimiento SNMP. Este modo de direccionamiento puede aplicarse cuando el modo de tratamiento de paquetes primario del PS (cabhCapPrimaryMode) se fija a NAPT o NAT. El servidor DHCP de la cabecera del operador de cable podría tener que modificar el software para poder soportar los ID de cliente (opción 61 del DHCP) de modo que pueda asignar múltiples direcciones IP a la dirección única de hardware de WAN-Data.

Existen cuatro posibles casos de direccionamiento IP de WAN-Data:

1) El PS se configura de modo que no solicite ninguna dirección IP de WAN-Data. No se necesitan los ID de cliente de WAN-Data.

2) El PS se configura de modo que solicite una o varias direcciones IP de WAN-Data y que no haya anotaciones en cabhCdpWanDataAddrClientId configuradas por el operador en la MIB del CDP. El PS debe autogenerar tantos ID de cliente de WAN-Data únicos como el valor de cabhCdpWanDataIpAddrCount.

3) El PS se configura de modo que solicite una o varias direcciones IP de WAN-Data y que haya por lo menos tantas anotaciones en cabhCdpWanDataAddrClientId configuradas por el operador como el valor de cabhCdpWanDataIpAddrCount, es decir, el operador habrá proporcionado suficientes valores de ID de cliente de WAN-Data. El PS no autogenera ningún ID de cliente.

4) El PS se configura de modo que solicite una o varias direcciones IP de WAN-Data y que haya menos anotaciones en cabhCdpWanDataAddrClientId configuradas por el operador que el valor de cabhCdpWanDataIpAddrCount, es decir, el operador ha proporcionado algunos valores de ID de cliente de WAN-Data pero no los suficientes. El PS debe autogenerar suficientes ID de cliente de WAN-Data únicos adicionales hasta alcanzar el valor de cabhCdpWanDataIpAddrCount.

Si el operador del sistema de cable desea que el PS obtenga una o varias direcciones IP de WAN-Data, que sean distintas de las direcciones IP de WAN-Man, se debe seguir el siguiente procedimiento:

En todos los modos de direccionamiento WAN, el PS solicita en primer lugar una dirección IP de WAN-Man utilizando la dirección de hardware de WAN-Man.

El procedimiento que se describe más adelante supone que el PS ya ha obtenido una dirección de IP de WAN-Man:

1) El operador del sistema de cable facultativamente asigna al PS varios ID de cliente particulares únicos, al escribir valores en las anotaciones cabhCdpWanDataAddrClientId de las MIB cabhCdpWanDataAddrTable del CDP, a través del fichero de configuración del PS o de mensajes de petición de establecimiento SNMP.

2) El operador del sistema de cable configura el CDP de modo que funcione en el modo 2 de direccionamiento WAN al escribir un valor distinto de cero en cabhCdpWanDataIpAddrCount a través del fichero de configuración del PS o del mensaje de petición de establecimiento SNMP.

3) Tras haber configurado el CDP para que funcione en el modo 2 de direccionamiento WAN como se describió en el paso 2, el PS verifica si el NMS ha suministrado los valores de ID de cliente como se describió en el paso 1. Si se ha suministrado cierto número de valores de ID de cliente mayor que el valor de cabhCdpWanDataIpAddrCount o igual a él, el PS los utilizará en la opción 61 del DHCP cuando se soliciten direcciones IP de WAN-Data. Si los valores de ID de cliente no han sido suministrados, es decir, no existen las anotaciones cabhCdpWanDataAddrClientId, o si el número de valores de ID de cliente suministrados es menor que el valor de cabhCdpWanDataIpAddrCount, el PS genera cierto número de valores de ID de cliente únicos de modo que en combinación con los ID de cliente suministrados, el número total de ID de cliente únicos será igual al valor de cabhCdpWanDataIpAddrCount. El PS genera valores de ID de cliente utilizando la dirección de hardware de WAN-Data sólo para la primera dirección IP de WAN-Data solicitada, y concatenando la dirección de hardware de WAN-Data con un contador que tenga 8 bits de longitud para la segunda dirección de IP de WAN-Data y para todas las subsiguientes. Si el NMS no ha suministrado los ID de cliente, el primer valor del contador de 8 bits será 0x02 (que indica la segunda dirección de IP de WAN-Data solicitada), el segundo valor de contador será 0x03, etc.

   Ejemplo para el caso cuando el NMS no ha suministrado los ID de cliente:

   Dada la dirección de hardware de WAN-Data 0xCDCDCDCDCDCD.

   ID de cliente generado por el PS para la primera dirección IP de WAN-Data solicitada: 0xCDCDCDCDCDCD.

   ID de cliente generado por el PS para la segunda dirección IP de WAN-Data solicitada: 0xCDCDCDCDCDCD02.

   ID de cliente generado por el PS para la tercera dirección IP de WAN-Data solicitada: 0xCDCDCDCDCDCD03.

   ID de cliente generado por el PS para la enésima dirección IP de WAN-Data solicitada: 0xCDCDCDCDCDCDn ($n \leq 0xFF$).

   Si el NMS ha suministrado algunos ID de cliente, pero el número es menor que el valor de cabhCdpWanDataIpAddrCount, el PS generará suficientes ID de cliente adicionales hasta alcanzar el valor de cabhCdpWanDataIpAddrCount. El PS los generará agregando un valor de 8 bits a la dirección de hardware de WAN-Data, comenzando con 0x02, a menos que se duplique un ID de cliente ya suministrado. Si los ID de cliente suministrados por el NMS siguen el mismo formato (dirección de hardware con un valor de 8 bits), el PS debe utilizar un valor de recuento único para no duplicar un ID de cliente ya suministrado.

   A continuación se presenta un ejemplo del caso cuando el NMS ha suministrado los ID de cliente (tres valores de ID de cliente suministrados, cabhCdpWanDataIpAddrCount = 5):

   Dada la dirección de hardware de WAN-Data 0xCDCDCDCDCDCD.

   Primer ID de cliente suministrado para la primera dirección de IP de WAN-Data: 0x0A0A0A0A0A1A.

Segundo ID de cliente suministrado para la segunda dirección IP de WAN-Data: 0x0A0A0A0A0A2A.

Tercer ID de cliente suministrado para la tercera dirección IP de WAN-Data: 0x0A0A0A0A0A3A.

Primer ID de cliente generado por el PS para la cuarta dirección IP de WAN-Data solicitada: 0xCDCDCDCDCDCD02.

Segundo ID de cliente generado por el PS para la quinta dirección IP de WAN-Data solicitada: 0xCDCDCDCDCDCD03.

4) El PS añade los valores de ID de cliente que genera como anotaciones cabhCdpWanDataAddrClientId al final de cabhCdpWanDataAddrTable.

5) El PS (CDC) solicita (repitiendo el proceso DHCP DISCOVER tantas veces como sea necesario) tantas direcciones IP de WAN-Data únicas según el valor de cabhCdpWanDataIpAddrCount, utilizando la dirección de hardware de WAN-Data en el campo chaddr del mensaje DHCP y los valores de ID de cliente del paso 3 en la opción 61 del DHCP, comenzando con la primera anotación cabhCdpWanDataAddrClientId de cabhCdpWanDataAddrTable. No se permite que el CDC solicite más direcciones IP de WAN-Data que el valor de cabhCdpWanDataIpAddrCount, aun en el caso de que el número de ID de clientes suministrados sea mayor que el valor de cabhCdpWanDataAddrTable.

7.3.3.2.4 Requisitos del CDC

El PS DEBE implementar una función de cliente DHCP conforme a los requisitos del cliente de [RFC 2131].

En ambos tipos de configuraciones, integrado y autónomo, el PS DEBE implementar dos direcciones de hardware de WAN únicas: la dirección de hardware de WAN-Man y la dirección de hardware de WAN-Data del PS. El valor numérico de la segunda DEBE seguir secuencialmente al valor numérico de la primera. Las direcciones de hardware de WAN-Man y de WAN-Data del PS DEBEN permanecer iguales a las fijadas por el fabricante. El PS NO DEBE permitir su modificación.

En ambos casos, PS integrado y autónomo, el elemento PS DEBE tener direcciones de hardware de la interfaz de la WAN distintas de la dirección de hardware del módem de cable.

El PS DEBE difundir el mensaje DHCP DISCOVER de acuerdo a los requisitos del cliente de [RFC 2131] y tratar de obtener una licencia de dirección de IP de WAN-Man del PS durante el proceso de arranque del PS.

El PS DEBE fijar cabhPsDevProvState a inProgress (2) cuando difunde el mensaje DHCP DISCOVER por primera vez, a continuación del rearranque del dispositivo o de la reinicialización del PS. El PS ignora los campos y opciones del encabezamiento DHCP utilizados para determinar el modo de configuración y no es necesario que fije cabhPsDevProvState a inProgress (2) cuando efectúa la renovación de su licencia de dirección IP a través del DHCP.

Como consecuencia del proceso de renovación de su licencia de dirección IP, el PS fija el objeto estado de configuración (cabhPsDevProvState) al valor pass(1) o fail(2). Cuando renueva su licencia o sus licencias de direcciones IP WAN-Man o WAN-Data, el PS DEBE actualizar su hora del sistema y sus objetos MIB conexos (cabhPsDevDateTime) en función del valor de la opción 2 del DHCP (desplazamiento horario) del mensaje DHCP ACK si el valor de cabhCdpTimeOffsetSelection es useDhcpOption2(1), O en función del valor de cabhCdpSnmpSetTimeOffset si el valor de cabhCdpTimeOffsetSelection es useSnmpSetOffset(2), Y ajustando una hora el horario durante el periodo de aplicación del horario de ahorro de energía, es decir, cuando el valor de cabhCdpDaylightSavingTimeEnable es enabled(1). Cuando renueva su licencia o licencias de direcciones IP de WAN-Man o WAN-Data, el PS DEBE actualizar su

información de licencia, incluyendo la actualización de los valores de cabhCdpWanDataAddrLeaseCreateTime y cabhCdpWanDataAddrLeaseExpireTime según proceda, en función del valor de la opción 51 del DHCP (hora de concesión de licencia de dirección IP). Cuando renueva su licencia o licencias de direcciones IP WAN-Man o WAN-Data, el PS DEBE ignorar las subopciones 3, 6 y 10 de la opción 122 del DHCP, y los campos file y saddr del encabezamiento DHCP.

El PS DEBE utilizar la dirección de hardware de WAN-Man del PS en el campo *chaddr* y en la opción 61 del DHCP, en los mensajes DHCP DISCOVER y DHCP REQUEST, cuando solicite una dirección IP de WAN-Man del servidor DHCP de la cabecera.

Si el valor de cabhCdpWanDataIpAddrCount es cero, el PS DEBE utilizar la dirección IP de WAN-Man para las interfaces de WAN-Man y de WAN-Data.

Si el valor de cabhCdpWanDataIpAddrCount es mayor que cero, el PS DEBE solicitar el mismo número de direcciones IP de WAN-Data únicas del servidor DHCP de la cabecera que el valor de cabhCdpWanDataIpAddrCount.

El PS (CDC) NO DEBE tratar de obtener más direcciones de IP de WAN-Data que el valor de cabhCdpWanDataIpAddrCount.

El PS DEBE utilizar un cabhCdpWanDataAddrClientId único en la opción 61 del DHCP para cada dirección IP de WAN-Data solicitada del servidor DHCP de la cabecera.

El PS DEBE utilizar la dirección de hardware de WAN-Data como el valor en el campo *chaddr* del mensaje DHCP por cada dirección IP de WAN-Data solicitada del servidor DHCP de la cabecera.

Cuando el PS autónomo tiene constancia de que se ha producido la pérdida, y posterior recuperación, del enlace WAN entre el PS autónomo y el módem de cable, DEBE iniciar una renovación DHCP para todas las licencias de direcciones IP obtenidas mediante DHCP y que sigan siendo válidas. Este mensaje de renovación DHCP permite al módem de cable conocer las direcciones MAC del PS autónomo y restablecer la retransmisión MAC necesaria para las tramas en RF destinadas al dispositivo PS autónomo.

Se supone que en la mayoría de los dispositivos PS integrados, cuando se produce la reinicialización del módem de cable, también se reinicializa el dispositivo PS integrado a fin de evitar inconsistencias entre los estados de ambos dispositivos. Cuando el PS autónomo tenga constancia de que se ha producido la pérdida, y posterior recuperación, del enlace WAN entre el PS autónomo y el módem de cable, DEBE iniciar la renovación DHCP de todas las licencias de direcciones IP obtenidas mediante DHCP y que sigan siendo válidas.

Cuando el PS (CDC) solicita direcciones IP de WAN-Data del servidor DHCP de la cabecera, el PS DEBE utilizar anotaciones cabhCdpWanDataAddrClientId para la opción 61 del DHCP en el orden en que aparecen las anotaciones en cabhCdpWanDataAddrTable, comenzando con la primera anotación.

Si se configura un valor distinto de cero para cabhCdpWanDataIpAddrCount, y si el número de anotaciones cabhCdpWanDataAddrClientId es menor que el valor de cabhCdpWanDataIpAddrCount, el PS DEBE generar tantos ID de cliente de WAN-Data únicos como sea necesario para llevar el número total de anotaciones cabhCdpWanDataAddrClientId al valor de cabhCdpWanDataIpAddrCount, y añadir cada anotación generada al final de cabhCdpWanDataAddrTable.

Si el PS genera los ID de cliente de WAN-Data, la primera anotación cabhCdpWanDataAddrClientId de cabhCdpWanDataAddrTable DEBE ser la dirección de hardware de WAN-Data.

Si el PS genera los ID de cliente de WAN-Data, cualquier anotación cabhCdpWanDataAddrClientId generada por el PS distinta de la primera anotación de

cabhCdpWanDataAddrTable DEBE ser la dirección de hardware de WAN-Data con un valor de 8 bits añadido al final, comenzando con 0x02, a menos que el valor ya exista como una anotación cabhCdpWanDataAddrClientId, en cuyo caso el PS DEBE generar el ID de cliente como la dirección de hardware de WAN-Data a la que se añade el siguiente valor de 8 bits disponible.

El PS DEBE implementar la opción de información específica del fabricante (opción 43 del DHCP) tal como se especifica en los cuadros 7-7 y 7-8. Más adelante se presenta información adicional sobre la opción 43 del DHCP y sus subopciones. La definiciones de las subopciones de la opción 43 del DHCP DEBEN se conformes con los requisitos de [RFC 2132].

La opción comienza con un octeto de tipo cuyo valor es el número 43, seguido de un octeto de longitud. El octeto de longitud va seguido del número de octetos de datos indicado en el octeto de longitud. El valor de dicho octeto no incluye los dos octetos que especifican el marcador y la longitud.

La opción 43 del DHCP es una opción compuesta. El contenido de la opción 43 está formado por una o más subopciones. Las subopciones que soporta la opción 43 del DHCP son las siguientes: 1, 2, 3, 4, 5, 6, 11, 12, 13 y 14. Una subopción comienza con un octeto marcador que contiene el código de la subopción, seguido de un octeto de longitud que indica el número total de octetos de datos. El valor del octeto de longitud no incluye a dicho octeto o al octeto marcador. La longitud del octeto va seguida de octetos "longitud" de los datos de la subopción.

A continuación se define la codificación de cada subopción de la opción 43. En los cuadros 7-7 y 7-8 se describe el objetivo de cada subopción.

El PS DEBE codificar la subopción 1 de la opción 43 del DHCP mediante un número de octetos igual al valor del octeto longitud de esta subopción, donde cada octeto codifica una subopción solicitada.

El PS DEBE codificar cada una de las subopciones 2, 3, 4, 5, 6, 12, 13 y 14 de la opción 43 del DHCP como una cadena de caracteres del conjunto de caracteres ASCII NVT, sin un valor NULO de terminación.

Un PS autónomo DEBE enviar la subopción 2 de la opción 43 del DHCP incluyendo la cadena de caracteres "SPS" (sin comillas).

Un PS integrado DEBE enviar la subopción 2 de la opción 43 del DHCP incluyendo la cadena de caracteres "EPS" (sin comillas).

Un PS autónomo DEBE enviar la subopción 3 de la opción 43 del DHCP incluyendo la cadena de caracteres "SPS" (sin comillas).

Un PS integrado DEBE enviar la subopción 3 de la opción 43 del DHCP incluyendo una lista separada por comas de todos los tipos de dispositivos del dispositivo completo, incluyendo al menos la cadena de caracteres separados por comas "ECM:EPS" (sin comillas).

Si el PS solicita licencia para una dirección IP WAN-Man del PS, DEBE enviar la subopción 11 de la opción 43 del DHCP con el valor 0x01, codificado como número binario, en sus mensajes DHCP DISCOVER y DHCP REQUEST.

Si el PS solicita licencia para una dirección IP WAN-Data del PS, DEBE enviar la subopción 11 de la opción 43 del DHCP con el valor 0x02, codificado como número binario, en sus mensajes DHCP DISCOVER y DHCP REQUEST.

En el cuadro 7-6 se resume cómo han de fijarse los valores de la subopción 11 de la opción 43 del DHCP para las interfaces WAN del PS.

Cuadro 7-6/J.192 – Valores de la subopción 11 de la opción 43 del DHCP

Identidad del elemento	Descripción y comentarios
PS WAN-Man = 0x01	Identifica la petición de una dirección para un sector WAN-Man
PS WAN-Data = 0x02	Identifica la petición de una dirección para un sector WAN-Data

La longitud de las subopciones 4, 5, 6, 12, 13 y 14 es como máximo de 255 octetos. Por lo tanto, la longitud total de la opción 43 puede exceder los 255 octetos. Si el número total de octetos de todas las subopciones de la opción 43 DHCP supera los 255 octetos, el PS DEBE ser conforme con RFC 3396 para dividir la opción en varias opciones más pequeñas.

EL PS DEBE implementar la opción identificador de clase de fabricante (opción 60 del DHCP) tal como se especifica en los cuadros 7-7 y 7-8.

En el caso de un PS integrado con módem de cable, tanto el módem de cable como el elemento PS envían peticiones DHCP independientes. En el cuadro 7-7 se describe cómo el PS DEBE fijar el contenido de las opciones 60 y 43 para el mismo cuando el elemento PS está integrado con un módem de cable y se solicitan direcciones de gestión WAN (WAN-Man) y direcciones de datos WAN diferenciadas del PS.

Cuadro 7-7/J.192 – Opciones del DHCP para las peticiones de direcciones de WAN-Man y de WAN-Data de un PS integrado

Opciones de petición DHCP	Valor	Descripción
El DHCP de los servicios de portal integrados solicita una dirección de WAN-Man		
Opción 60 del CPE	"CableHome1.1"	
Subopción 1 de la opción 43 del CPE	vector de subopción de petición	Lista de subopciones (de la opción 43) que devolverá el servidor. No se ha definido ninguna.
Subopción 2 de la opción 43 del CPE	"EPS"	PS integrado
Subopción 3 de la opción 43 del CPE	"ECM:EPS"	Lista de dispositivos integrados (CM y PS integrados)
Subopción 4 de la opción 43 del CPE	por ejemplo, "123456"	Número de serie del dispositivo CM/PS
Subopción 5 de la opción 43 del CPE	por ejemplo, "v3.2.1"	Número de versión del hardware del CM/PS
Subopción 6 de la opción 43 del CPE	por ejemplo, "1.0.2"	Número de versión del software del CM/PS
Subopción 11 de la opción 43 del CPE	PS WAN-Man (0x01)	Determina que se está solicitando una dirección del sector WAN-Man del PS
Subopción 12 de la opción 43 del CPE	por ejemplo, "ABC Inc. CM-PS123..."	Descripción del sistema CM/PS a partir de sysDescr
Subopción 13 de la opción 43 del CPE	por ejemplo, "CM-PS123-1.0.2...."	Revisión de los microprogramas del CM/PS desde docsDevSwCurrentVers
Subopción 14 de la opción 43 del CPE	por ejemplo, "1.2.3..."	Versión del fichero de política de la barrera contra fuegos a partir de cabhSec2FirewallPolicyFileCurrentVersion

Cuadro 7-7/J.192 – Opciones del DHCP para las peticiones de direcciones de WAN-Man y de WAN-Data de un PS integrado

Opciones de petición DHCP	Valor	Descripción
El DHCP de los servicios de portal integrados solicita una dirección de WAN-Data		
Opción 60 del CPE	"CableHome1.1"	
Subopción 1 de la opción 43 del CPE	vector de subopción de la petición	Lista de subopciones (de la opción 43) que devolverá el servidor. No se ha definido ninguna.
Subopción 2 de la opción 43 del CPE	"EPS"	PS integrado
Subopción 3 de la opción 43 del CPE	"ECM:EPS"	Lista de dispositivos integrados (CM y PS integrados)
Subopción 4 de la opción 43 del CPE	por ejemplo, "123456"	Número de serie del dispositivo CM/PS
Subopción 11 de la opción 43 del CPE	PS WAN-Data (0x02)	Determina que se está solicitando una dirección del sector WAN-Data del PS

En el cuadro 7-8 se describe cómo DEBE el PS fijar el contenido de las opciones 60 y 43, cuando se trate de un dispositivo autónomo.

Cuadro 7-8/J.192 – Opciones del DHCP para peticiones de direcciones de WAN-Man y de WAN-Data de un PS autónomo

Opciones de petición DHCP	Valor	Descripción
El DHCP de los servicios de portal autónomos solicita una dirección de WAN-Man		
Opción 60 del CPE	"CableHome1.1"	
Subopción 1 de la opción 43 del CPE	vector de subopción de la petición	Lista de subopciones (de la opción 43) que devolverá el servidor. No se ha definido ninguna.
Subopción 2 de la opción 43 del CPE	"SPS"	PS autónomo
Subopción 3 de la opción 43 del CPE	"SPS"	Lista de los dispositivos integrados (únicamente el PS autónomo)
Subopción 4 de la opción 43 del CPE	por ejemplo, "123456"	Número de serie del dispositivo
Subopción 5 de la opción 43 del CPE	por ejemplo, "v3.2.1"	Número de versión del hardware del CM/PS
Subopción 6 de la opción 43 del CPE	por ejemplo, "1.0.2"	Número de versión del software del CM/PS
Subopción 11 de la opción 43 del CPE	PS WAN-Man (0x01)	Determina que se está solicitando una dirección del sector WAN-Man del PS
Subopción 12 de la opción 43 del CPE	por ejemplo, "ABC Inc. CM-PS123..."	Descripción del sistema CM/PS a partir de sysDescr
Subopción 13 de la opción 43 del CPE	por ejemplo, "CM-PS123-1.0.2..."	Revisión de los microprogramas del CM/PS desde docsDevSwCurrentVers
Subopción 14 de la opción 43 del CPE	por ejemplo, "1.2.3..."	Versión del fichero de la política de la barrera contra fuegos a partir de cabhSec2FirewallPolicyFileCurrentVersion

Cuadro 7-8/J.192 – Opciones del DHCP para peticiones de direcciones de WAN-Man y de WAN-Data de un PS autónomo

Opciones de petición DHCP	Valor	Descripción
El DHCP de los servicios de portal autónomos solicita una dirección WAN-Data		
Opción 60 del CPE	"CableHome1.1"	
Subopción 1 de la opción 43 del CPE	vector de subopción de la petición	Lista de subopciones (de la opción 43) que devolverá el servidor. No se ha definido ninguna
Subopción 2 de la opción 43 del CPE	"SPS"	PS autónomo
Subopción 3 de la opción 43 del CPE	"SPS"	Lista de los dispositivos integrados (únicamente el PS autónomo)
Subopción 4 de la opción 43 del CPE	por ejemplo, "123456"	Número de serie del dispositivo
Subopción 11 de la opción 43 del CPE	PS WAN-Data (0x02)	Determina que se está solicitando una dirección del sector WAN-Data del PS

Si se desea una descripción detallada del contenido del objeto sysDescr del PS, véase 6.3.3.1.4, Requisitos de la funcionalidad del agente SNMP.

El PS DEBE soportar las opciones del DHCP señaladas como obligatorias en la columna de soporte del protocolo CDC del cuadro 7-9. En el mismo cuadro se relacionan las opciones del DHCP cuyo soporte es obligatorio y facultativo para el CDC.

Cuadro 7-9/J.192 – Opciones DHCP del CDC

Número de opción	Función de la opción	Soporte del protocolo CDC (M) obligatorio
0	Relleno	M
255	Fin	M
1	Máscara de subred	M
2	Opción de desplazamiento de tiempo	M
3	Opción de encaminador	M
4	Opción de servidor de tiempo	M
6	Servidor de nombres de dominio	M
7	Servidor de registro histórico (syslog)	M
12	Nombre de anfitrión	M
15	Nombre de dominio	M
23	Tiempo de vida por defecto	M
26	Interfaz MTU	M
43	Información específica de fabricante	M
50	Dirección IP solicitada	M
51	Tiempo de la licencia de la dirección IP	M
54	Identificador de servidor	M
55	Lista de peticiones de parámetros	M

Cuadro 7-9/J.192 – Opciones DHCP del CDC

Número de opción	Función de la opción	Soporte del protocolo CDC (M) obligatorio
60	Identificador de clase de fabricante	M
61	Identificador de cliente	M
122	Subopción 3 – Dirección de la entidad SNMP del proveedor de servicio	M
122	Subopción 6 – Nombre del sector de configuración del sector Kerberos	M
122	Subopción 10 – Dirección IP del servidor Kerberos	M

El PS DEBE incluir las opciones DHCP que se señalan como obligatorias en el cuadro 7-10 en los mensajes DHCP DISCOVER y DHCP REQUEST que se envían al servidor DHCP de la red de cable.

Cuadro 7-10/J.192 – Opciones DHCP del CDC en los mensajes DISCOVER y REQUEST

Número de opción	Función de la opción	Inclusión en el protocolo CDC (M) obligatorio
255	Fin	M
43	Información específica de fabricante	M
50	Dirección IP solicitada	M
55	Lista de solicitudes de parámetros	M (solamente DHCP REQUEST)
60	Identificador de clase de fabricante	M
61	Identificador de cliente	M

El PS DEBE solicitar las opciones DHCP señaladas como obligatorias en el cuadro 7-11, en la opción 55 del DHCP (Lista de peticiones de parámetros) [RFC 2132] que se envía en los mensajes DHCP DISCOVER y DHCP REQUEST.

Cuadro 7-11/J.192 – Opciones DHCP del CDC solicitadas en la opción 55

Número de opción	Función de la opción	Inclusión en el protocolo CDC (M) obligatorio
1	Máscara de subred	M
2	Opción de desplazamiento de tiempo	M
3	Opción de encaminador	M
4	Opción de servidor de tiempo	M
6	Servidor de nombres de dominio	M
7	Servidor de registro histórico (syslog)	M
15	Nombre de dominio	M
23	Tiempo de vida por defecto	M
26	MTU de la interfaz	M
51	Tiempo de la licencia de dirección IP	M
54	Identificador del servidor	M
122	Opción de configuración de cliente CableLabs	M

La lista siguiente identifica las acciones que ha de tomar el PS si alguna de las opciones del DHCP requeridas en la opción 55 del DHCP (enumeradas en el cuadro 7-11) no existe en el mensaje DHCP OFFER que recibe del servidor DHCP.

1) Si la opción 1 del DHCP (Máscara de subred) no existe en el mensaje de oferta de licencia DHCP que el PS ha recibido del servidor DHCP, la respuesta es incompleta y el PS DEBE generar un Event ID 68000301 Y reactivar el proceso de configuración mediante la difusión de un mensaje DHCP DISCOVER a través de su interfaz WAN.

2) Si la opción 2 del DHCP (Desplazamiento de tiempo) no existe en el mensaje de oferta de licencia DHCP que el PS ha recibido del servidor DHCP, la oferta de licencia no se considera incompleta y el PS puede aceptar la licencia.

3) Si la opción 3 del DHCP (Encaminador) no existe en el mensaje de oferta de licencia DHCP que el PS ha recibido del servidor DHCP, la oferta de licencia no se considera incompleta y el PS puede aceptar la licencia.

4) Si la opción 4 del DHCP (Servidor de tiempo) no existe en el mensaje de oferta de licencia DHCP que el PS ha recibido del servidor DHCP, la respuesta es incompleta y el PS DEBE generar un Event ID 68000301 Y reactivar el proceso de configuración mediante la difusión de un mensaje DHCP DISCOVER a través de su interfaz WAN.

5) Si la opción 6 del DHCP (Servidor de nombres de dominio) no existe en el mensaje de oferta de licencia DHCP que el PS ha recibido del servidor DHCP, la respuesta es incompleta y el PS DEBE generar un Event ID 68000301 Y reactivar el proceso de configuración mediante la difusión de un mensaje DHCP DISCOVER a través de su interfaz WAN.

6) Si la opción 7 del DHCP (Servidor de registro histórico) no existe en el mensaje de oferta de licencia DHCP que el PS ha recibido del servidor DHCP, la oferta de licencia no se considera incompleta y el PS puede aceptar la licencia.

7) Si la opción 15 del DHCP (Nombre de dominio) no existe en el mensaje de oferta de licencia DHCP que el PS ha recibido del servidor DHCP, la oferta de licencia no se considera incompleta y el PS puede aceptar la licencia.

8) Si la opción 23 del DHCP (Tiempo de vida IP por defecto) no existe en el mensaje de oferta de licencia DHCP que el PS ha recibido del servidor DHCP, la oferta de licencia no se considera incompleta y el PS puede aceptar la licencia.

9) Si la opción 26 del DHCP (MTU de la interfaz) no existe en el mensaje de oferta de licencia DHCP que el PS ha recibido del servidor DHCP, la oferta de licencia no se considera incompleta y el PS puede aceptar la licencia.

10) Si la opción 51 del DHCP (Tiempo de la licencia de la dirección IP) no existe en el mensaje de oferta de licencia DHCP que el PS ha recibido del servidor DHCP, la respuesta es incompleta y el PS DEBE generar un Event ID 68000301 Y reactivar el proceso de configuración mediante la difusión de un mensaje DHCP DISCOVER a través de su interfaz WAN.

11) Si la opción 54 del DHCP (Identificador del servidor) no existe en el mensaje de oferta de licencia DHCP que el PS ha recibido del servidor DHCP, la oferta de licencia no se considera incompleta y el PS puede aceptar la licencia.

12) Si la opción 122 del DHCP (Opción de configuración de cliente CableLabs) no existe en el mensaje de oferta de licencia DHCP que el PS ha recibido del servidor DHCP, la oferta de licencia no se considera incompleta y el PS puede aceptar la licencia.

Si el PS no recibe una oferta de licencia completa después de agotar el número máximo de reintentos, DEBE funcionar en el modo aletargado descrito en 7.3.3.2.4.

El PS DEBE soportar una dirección de la entidad gestora de de entidad SNMP del proveedor de servicio (subopción 3 de la opción 122 del DHCP) configurada como una dirección IPv4. El formato de la subopción 3 de la opción 122 del DHCP se describe en [RFC 3495].

El PS DEBE soportar un nombre del sector Kerberos (subopción 6 de la opción 122 del DHCP). El PS necesita un nombre de sector Kerberos que permita una consulta al DNS relativa a la dirección de la entidad del centro de distribución de claves (KDC) del proveedor de servicios. El formato de la subopción 6 de la opción 122 del DHCP descrita en [RFC 3495].

El PS DEBE soportar una dirección IP de un servidor de centro de distribución de Kerberos (KDC) (subopción 10 de la opción 122 del DHCP). La subopción de la dirección IP del servidor KDC permite informar al PS sobre la dirección de red de uno o varios servidores del centro de distribución de claves.

La codificación de la subopción de la dirección del servidor KDC se describe en [RFC 3634].

Cuando la primera interfaz de WAN-Data del PS no tenga una licencia DHCP vigente, DEBE utilizar por defecto los siguientes parámetros de IP:

– Dirección IP de WAN-Data de "repliegue": 192.168.100.5.
– Máscara de red: 255.255.255.0.
– Pasarela por defecto: 192.168.100.1.

La finalidad de la dirección IP de WAN-Data de "repliegue" es facilitar el acceso a la dirección IP de diagnóstico del módem de cable (192.168.100.1) desde un dispositivo IP de LAN siempre que no haya una dirección IP WAN-Data regular disponible en el PS. La dirección IP de WAN-Data de "repliegue" DEBE utilizarse únicamente como la porción de dirección IP de WAN de la tupla dinámica NAT o NAPT de una correspondencia de direcciones entre C-NAT y C-NAPT respectivamente, con la dirección IP de diagnóstico del módem de cable (192.168.100.1). El PS DEBE tener por defecto la dirección IP WAN-Data de "repliegue" inmediatamente después del encendido y siempre que las actuales licencias de dirección IP de WAN-Data hayan expirado y no haya quedado activa ninguna dirección IP WAN-Data, a fin de seguir proporcionando acceso continuo a las capacidades de diagnóstico del CM. El PS NO DEBE utilizar la dirección IP de WAN-Data de "repliegue" cuando el PS se configura para que funcione en el modo de tratamiento de paquetes primario de transferencia.

El PS NO DEBE utilizar la dirección IP de WAN-Data de "repliegue" para ninguna correspondencia de C-NAT o de C-NAPT cuando el PS tiene una licencia de dirección IP de WAN-Man y de WAN-Data del PS. Si un servidor DHCP en la interfaz WAN del PS ofrece una licencia al PS (CDC) para la dirección IP 192.168.100.5, es decir, la misma dirección de IP de WAN-Data de "repliegue", el PS (CDC) PUEDE aceptarla y utilizarla como la dirección IP de WAN-Data para una correspondencia de C-NAT o de C-NAPT.

Aun cuando esté utilizando la dirección IP de WAN-Data por defecto 192.168.100.5, el PS DEBE continuar realizando una determinación DHCP DISCOVERY cada 10 segundos hasta que se otorgue una licencia DHCP válida a esa interfaz de WAN-Data del PS (o a la interfaz WAN-Man, si WAN-Man y WAN-data están compartiendo una dirección IP).

Cuando un PS está tratando de obtener una dirección IP de WAN-Man para su interfaz WAN-Man, DEBE insertar siempre su dirección de hardware de la WAN en el campo de ID de cliente (opción 61 del DHCP) en el mensaje DHCP DISCOVER.

Si durante ese intento, el CDC no recibe ningún mensaje DHCP OFFER, el PS DEBE registrar el ID de evento 68000100 en el registro histórico local y volver a difundir un mensaje DHCP DISCOVER (es decir, rearrancar la secuencia de configuración en el caso de esta condición de fallo) – repitiendo el intento de obtención de la licencia DHCP hasta en cinco ocasiones. Si después del quinto intento el CDC no recibe DHCP OFFER, el PS DEBE utilizar la dirección IP de WAN de "repliegue", la máscara de red y la pasarela por defecto, como se describió anteriormente, y

continuar tratando de conseguir una dirección IP de WAN-Man válida difundiendo DHCP DISCOVER por su interfaz WAN cada 10 segundos hasta que se otorgue la licencia DHCP válida para la dirección IP de WAN-Man.

Cuando un PS que funcione en el modo 2 de direccionamiento WAN (tal como se describe en 7.3.3.2) se encuentra en fase de conseguir una dirección IP WAN-Data para una interfaz WAN-Data que utilizará una dirección IP diferente de la interfaz WAN-Man, DEBE incluir la opción Identificador de cliente (cabhCdpWanDataAddrClientId) en el mensaje DHCP DISCOVER. Para permitir dichas ID de clientes WAN-Data específicas, el CDC DEBE permitir que el sistema NMS cree Anotaciones de cabhCdpWanDataAddrClientId en cabhCdpWanDataAddrTable.

Si un PS funciona en el modo 2 de direccionamiento WAN (tal como se describe en 7.3.3.2) el PS DEBE intentar obtener una dirección IP, mediante DHCP, para cada ID específico de cliente (cabhCdpWanDataAddrClientId) de cabhCdpWanDataAddrTable, hasta el límite definido por cabhCdpWanDataIpAddrCount.

El PS DEBE continuar retransmitiendo el mensaje de difusión DHCP DISCOVER mediante un algoritmo de reducción exponencial aleatorizado, coherente con el descrito en [RFC 2131], hasta que obtiene una licencia de dirección IP WAN-Man de PS y/o IP WAN-Data de PS válidas, según convenga.

Si el PS (CDC) obtiene con éxito la dirección IP WAN-Man (es decir, recibe un DHCP ACK de un servidor DHCP a través de la interfaz WAN-Man del PS) en su primer intento, y si el PS funciona en el modo configuración DHCP, el PS DEBE intentar la sincronización de la hora del día con el servidor de ToD enviando para ello una petición de ToD, tal como se describe en 7.5.4, antes de intentar la descarga del fichero de configuración del PS.

Si el PS (CDC) no tiene éxito en conseguir la dirección IP WAN-Man (es decir, vence la temporización de la petición DHCP de conformidad con [RFC 2131]) en su primer intento, el PS DEBE arrancar el CDS (es decir, iniciar el funcionamiento del CDS), de forma que éste pueda atender peticiones DHCP de dispositivos IP de la LAN en el sector LAN-Trans.

La función CDC del PS solamente DEBE responder a mensajes DHCP recibidos o enviados a través de una interfaz WAN.

Cuando expira la licencia DHCP de WAN-Man, el PS DEBE borrar todas las anotaciones de filas de cabhCdpWanDnsServerTable.

Modos de funcionamiento para la configuración del PS

En esta cláusula se describen los requisitos del PS para el funcionamiento en los modos que se presentan en 5.5.

Si un PS está integrado como un eSAFE con un módem de cable conforme con eDOCSIS [eDOCSIS1], y el objeto MIB esafePsCableHomeModeControl de eDOCSIS se fija en provSystem(2), el PS integrado DEBE tratar de obtener una licencia de dirección IP WAN-Man del PS, y adherirse a los requisitos del modo de configuración DHCP, modo de configuración SNMP, o modo CableHome aletargado, tal como se describe más adelante. En lo que sigue, se definen requisitos adicionales para el funcionamiento del PS integrado en función del valor de esafePsCableHomeModeControl.

Modo de configuración DHCP

Si durante el proceso de obtención de una licencia para la dirección IP de WAN-Man del PS el CDC recibe, en el mensaje DHCP ACK [RFC 2131] del servidor DHCP en la red de cable, una dirección IP válida en el campo 'siaddr' y un nombre de fichero válido en el campo 'file' y no recibe las subopciones 3, 6 ó 10 (combinación 1 válida) de la opción 122 del DHCP, el PS DEBE fijar cabhPsDevProvMode a dhcpmode(1) y tratar de sincronizar la hora del día con el servidor ToD, tal como se describe en 7.5.4, Requisitos de la función cliente de hora del día. En función del valor de

los campos siaddr y file del encabezamiento del mensaje DHCP, puede requerirse que el PS intente descargar un fichero de configuración. Véase la cláusula 7.4.4.2, Requisitos para la activación de BPSC.

Modo de configuración SNMP

Si durante el proceso de obtención de una licencia para la dirección IP de WAN-Man del PS el CDC recibe un mensaje DHCP ACK del servidor DHCP en la red de cable que incluya la opción 122 del DHCP con una dirección IP válida (dirección del gestor de SNMP) en la subopción 3, un nombre de sector Kerberos válido en la subopción 6 y una dirección IP válida (dirección IP del servidor Kerberos) en la subopción 10, y no recibe una dirección IP válida en el campo 'siaddr' ni tampoco un nombre de fichero válido en el campo 'file' (combinación 2 válida), el PS DEBE fijar cabhPsDevProvMode a snmpmode(2) e iniciar el funcionamiento del CDS y tratar de sincronizar la hora del día con el servidor ToD y proceder a la autenticación ante el servidor KDC como se describe en 11.3.4, Requisitos de la infraestructura de autenticación. El PS que funcione en el modo de configuración SNMP puede también ser configurado para tratar de descargar un fichero de configuración. Véase 7.4.4.2, Requisitos para la activación de BPSC.

Modo CableHome aletargado

Si durante el proceso de obtención de una licencia para la dirección IP de WAN-Man del PS el CDC recibe, en el mensaje DHCP ACK del servidor DHCP en la red de cable, cualquier combinación de las subopciones 3, 6 y 10 de la opción 122 del DHCP, el campo 'siaddr' y el campo 'file' distinta de las dos combinaciones válidas que se describieron anteriormente, el PS habrá recibido una configuración DHCP no válida y DEBE registrar el evento con ID 68000301 (véase el cuadro B.1, Eventos definidos para IPCable2Home) Y realizar lo siguiente suponiendo que está conectado a través de un módem de cable a una red de datos por cable que no soporta la configuración de CableHome (modo CableHome aletargado):

- Inhabilitar el agente SNMP (CMP) para acceder a la interfaz WAN. Mantener el agente SNMP habilitado para la recepción de mensajes a través de la interfaz LAN (es decir, los mensajes SNMP dirigidos a la dirección del encaminador del servidor del PS).
- Inhabilitar el cliente TFTP.
- Inhabilitar la notificación de eventos SYSLOG.
- Aceptar la licencia de dirección IP (CPE) ofrecida y utilizarla como la dirección de WAN-Data del PS en el cuadro de correspondencias CAP, incluyendo la asignación de la dirección a cabhCdpWanDataAddrIp y rellenando el resto de las anotaciones del cuadro de direcciones de WAN-Data del CDP (cabhCdpWanDataAddrTable). El PS se mantendrá funcionando sin una dirección IP de WAN-Man, que es un modo diferente de cualquiera de los modos de direccionamiento WAN que se describieron en 7.3.3.2.3.2.
- Detener el temporizador de configuración.
- Fijar el valor de cabhPsDevProvMode a dormantCHmode(3).
- Fijar el valor de cabhPsDevProvState a fail(3).
- Habilitar el CDS.
- Habilitar la funcionalidad de CAP y de USFS.
- Habilitar el CNP.
- Habilitar la barrera contra fuegos.
- Funcionar con los parámetros que se suministraron anteriormente, incluyendo los valores de los objetos MIB persistentes. El PS funcionando en el modo CableHome aletargado NO DEBE reinicializar sus objetos MIB a los valores de fábrica por defecto.

Un PS integrado también puede configurarse para funcionar en modo CableMÓdem aletargado mediante el objeto MIB eSAFE de eDOCSIS esafePsCableHomeModeControl [eDOCSIS1]. Si el objeto esafePsCableHomeModeControl del módem de cable conforme con eDOCSIS integrado se fija en dormantCHMode(3), el ePS ha de intentar obtener una licencia de dirección IP y funcionar en el modo CableHome aletargado, tal como se ha descrito anteriormente, con independencia de los valores del DHCP y de los campos de fichero, o de la presencia o ausencia de la opción 122 del DHCP y de sus subopciones en los mensajes DHCP OFFER y DHCP ACK. Véase el cuadro 7-12.

Modo inhabilitado

Cuando un PS integrado se configura para funcionar en el modo inhabilitado mediante la MIB eSAFE de eDOCSIS (esafePsCableHomeModeControl = disabledMode(1)) [eDOCSIS1], el PS integrado DEBE:

- liberar su licencia de dirección IP WAN-Man IP y cualquier licencia de dirección IP WAN-Data que tuviera, o bien, detener cualquier intento de conseguir una licencia de dirección IP WAN-Man o WAN-Data, descartando para ello los mensajes DHCP OFFER, DHCP ACK o cualquier otro mensaje DHCP;
- actuar como un puente transparente tal como se define en [ISO/CEI 10038], entre el sector WAN-Data y el sector LAN-Pass, actuando como puente transparente para todos los tipos de tramas que un módem de cable debe permitir pasar de conformidad con las especificaciones DOCSIS [DOCSIS1], [DOCSIS9];
- NO realizar ninguna función de encaminamiento transparente C-NAT o C-NAPT;
- inhabilitar el servidor DHCP (CDS), el servidor HTTP, el agente SNMP y la funcionalidad DNS (CNP);
- inhabilitar la barrera contra fuegos;
- descartar todos los paquetes dirigidos a la dirección del encaminador servidor del PS (cabhCdpServerRouter) o a la dirección IP LAN " bien conocida" del PS, 192.168.0.1; y
- dar prioridad al procesamiento de la conmutación de retransmisión selectiva ascendente (USFS, *upstream selective forwarding switch*) sobre las decisiones de puente LAN-a-WAN.

La única forma de configurar un PS para que funcione en el modo inhabilitado es fijar el valor de un objeto MIB eSAFE esafePsCableHomeModeControl del módem de cable eDOCSIS a disabled(1). El modo inhabilitado no se aplica a un PS autónomo ya que no está integrado como un eSAFE con un módem de cable eDOCSIS.

Puede hacerse que el PS integrado deje de estar en el modo inhabilitado fijando el valor del objeto MIB eSAFE esafePsCableHomeModeControl del módem de cable a provSystem(2) o a dormantCHMode(3) [eDOCSIS1].

Cuando el PS se modifica (es decir, se hace que abandone) administrativamente desde el modo inhabilitado, el PS DEBE fijar todos los objetos MIB CableHome a sus valores de fábrica por defecto.

En el cuadro 7-12 se definen las acciones que ha de tomar un PS integrado cuando se fija el objeto MIB eSAFE de eDOCSIS esafePsCableHomeModeControl [eDOCSIS1] para cada modo de funcionamiento del PS. El ePS DEBE tomar la acción enumerada en el cuadro 7-12 si funciona en alguno de los modos de la primera columna, 'Modo ePS actual', y el objeto MIB eSAFE de eDOCSIS esafePsCableHomeModeControl se fija con un valor de la segunda columna, 'esafePsCableHomeModeControl'. Obsérvese que el modo ePS actual de la primera columna del cuadro 7-12 se instrumenta en el objeto MIB eDOCSIS esafePsCableHomeModeStatus.

Cuadro 7-12/J.192 – Acciones requeridas del ePS para los valores de esafePsCableHomeModeControl

Modo ePS actual	esafePsCableHomeModeControl	Acciones ePS requeridas
Modo inhabilitado	disabledMode(1)	No se requiere acción alguna
Modo CableHome aletargado	disabledMode(1)	Toma las acciones enumeradas en la cláusula Modo inhabilitado
Modo CableHome	disabledMode(1)	Toma las acciones enumeradas en la cláusula Modo inhabilitado
Modo inhabilitado	provSystem(2)	Reinicia el proceso de configuración comenzando con la difusión de DHCP DISCOVER a través de la interfaz WAN
Modo CableHome aletargado	provSystem(2)	Reinicia el proceso de configuración comenzando con la difusión de DHCP DISCOVER a través de la interfaz WAN
Modo CableHome	provSystem(2)	Reinicia el proceso de configuración comenzando con la difusión de DHCP DISCOVER a través de la interfaz WAN
Modo inhabilitado	dormantCHMode(3)	– Reinicia el proceso de configuración comenzando con la difusión de DHCP DISCOVER a través de la interfaz WAN – No incluye las subopciones 2-14 de la opción 43 del DHCP en los mensajes DHCP DISCOVER/REQUEST – No incluye 'CableHome1.0' o 'CableHome1.1' como valor de la opción 60 DHCP
		– No incluye la opción 122 del DHCP en la lista de petición de parámetros de la opción 55 del DHCP – Ignora los campos file y siaddr del encabezamiento DHCP en los mensajes DHCP OFFER y DHCP ACK: no descarga un fichero de configuración y no funciona en el modo configuración DHCP o en el modo configuración SNMP, con independencia de los valores de los campos field y siaddr del DHCP y de las opciones DHCP. – Toma las acciones enumeradas en la cláusula modo CableHome aletargado.
Modo CableHome aletargado	dormantCHMode(3)	No se requiere acción alguna

Cuadro 7-12/J.192 – Acciones requeridas del ePS para los valores de esafePsCableHomeModeControl

Modo ePS actual	esafePsCableHomeModeControl	Acciones ePS requeridas
Modo CableHome	dormantCHMode(3)	– Reinicia el proceso de configuración comenzando con la difusión de DHCP DISCOVER a través de la interfaz WAN – No incluye las subopciones 2-14 de la opción 43 del DHCP en los mensajes DHCP DISCOVER/REQUEST – No incluye 'CableHome1.0' o 'CableHome1.1' como valor de la opción 60 del DHCP – No incluye la opción 122 del DHCP en la lista de petición de parámetros de la opción 55 del DHCP – Ignora los campos file y siaddr del encabezamiento DHCP en los mensajes DHCP OFFER y DHCP ACK: no descarga un fichero de configuración y no funciona en el modo configuración DHCP o en el modo configuración SNMP, con independencia de los valores de los campos file y siaddr del encabezamiento DHCP y de las opciones DHCP. – Toma las acciones enumeradas en la cláusula modo CableHome aletargado.

7.4 Función del PS – Configuración de los servicios de portal en bloque (BPSC)

7.4.1 Objetivos de la función de configuración de los servicios de portal en bloque

Los objetivos fundamentales de la función BPSC son solicitar, recibir y procesar parámetros de configuración del PS y de la barrera contra fuegos.

7.4.2 Directrices de diseño del sistema de la función de configuración de los servicios de portal en bloque

Las directrices indicadas en el cuadro 7-13 permiten orientar la especificación de las capacidades de la función de configuración del PS en bloque:

Cuadro 7-13/J.192 – Directrices de diseño del sistema de los servicios de portal en bloque

Número	Directrices
BPSC 1	Ofrece un mecanismo por medio del cual el PS podrá descargar y procesar ficheros de configuración del PS y de la barrera contra fuegos.

7.4.3 Descripción del sistema relativa a la función de configuración de los servicios de portal en bloque

Por lo general, la configuración de los servicios de portal en bloque se realiza durante la configuración del elemento PS, mediante el procesamiento de los valores de configuración incluidos en el fichero de configuración. No obstante, este proceso puede iniciarse en cualquier momento. En esta cláusula el término "fichero de configuración" se utiliza para representar el fichero de configuración del PS o el de la barrera contra fuegos. Los requisitos específicos de cada tipo de fichero de configuración se identificarán con la etiqueta del fichero correspondiente, es decir, fichero de configuración del PS o fichero de configuración de la barrera contra fuegos. La herramienta de configuración del PS en bloque consta de los siguientes componentes:

- Formato del fichero de configuración.
- Modos de activación del proceso de descarga.
- Medios de autenticación del fichero.
- Medios de notificación hacia el origen del estado de la descarga del fichero de configuración y de otras consideraciones.

La configuración del PS en bloque (BPSC) es una herramienta que pueden utilizar los operadores para modificar los valores de configuración del PS y de la barrera contra fuegos en bloque, a través del fichero de configuración. Por lo general, el fichero de configuración incluirá muchos valores, ya que la utilidad fundamental de la que disponen los ficheros de configuración es la capacidad de modificar cierto número de valores de configuración con una intervención mínima del operador del sistema de cable. No obstante, se prevé que el fichero de configuración de la barrera contra fuegos se utilizará únicamente para valores específicos de la barrera contra fuegos.

El proceso de configuración del PS en bloque podrá tener el mismo comportamiento que los sucesivos establecimientos SNMP (SNMP Set) realizados manualmente por un operador. El fichero de configuración es una herramienta destinada a que los operadores sean más productivos y lograr que las modificaciones extensas de configuración sean menos propensas a errores.

Es importante observar que un PS que funciona en el modo de configuración SNMP no necesita cargar el fichero de configuración del PS antes de poder funcionar. Se prevé que un PS que funcione en el modo de configuración SNMP se inicializará él mismo a un estado conocido y que un PS podría funcionar por un tiempo indefinido aún sin la carga del fichero de configuración del PS. No obstante, un PS aceptará y procesará un fichero de configuración de PS cuando se los suministre.

7.4.4 Requisitos de la función de configuración de los servicios de portal en bloque

Un PS que funcione en el modo de configuración DHCP DEBE descargar y procesar un fichero de configuración del PS.

Un PS que funcione en el modo de configuración SNMP DEBE ser capaz de funcionar sin un fichero de configuración del PS, pero DEBE ser capaz de descargarlo y procesarlo si se activa para ello, como se describe en 7.3.3.2. No es necesario que el PS descargue un fichero de configuración de la barrera contra fuegos en ninguno de los modos de configuración DHCP o SNMP.

Los valores del objeto MIB transferidos en el fichero de configuración del PS tendrán precedencia sobre los valores de los objetos de la MIB existentes y DEBEN suprimirlos.

7.4.4.1 Requisitos del formato del fichero de configuración

Los datos de configuración del PS o de la barrera contra fuegos DEBEN estar contenidos en un fichero que se descarga a través de TFTP o HTTPS. El fichero de configuración DEBE consistir en varios valores de configuración (uno por parámetro), cada uno de la forma "Tipo Longitud Valor (TLV, *type length value*)". En el cuadro 7-14 se proporcionan las definiciones de estos términos.

Cuadro 7-14/J.192 – Definiciones de los TLV

Tipo	Identificador de un solo octeto que define el parámetro
Longitud	Campo de dos octetos que especifica la longitud del campo valor (sin incluir los campos de tipo y de longitud)
Valor	Conjunto de octetos que especifica el tamaño de la longitud que contiene el valor específico del parámetro

Los valores de configuración DEBEN acomodarse sucesiva y directamente en el fichero, lo que representa un tren de octetos (sin marcadores de registro). El PS DEBE ser capaz de recibir y procesar adecuadamente un fichero de configuración que se haya rellenado con un número entero de palabras de 32 bits, y de poder recibir y procesar adecuadamente un fichero de configuración que no haya sido rellenado con un número entero de palabras de 32 bits. Véase 7.4.4.1.1 para encontrar una definición del concepto de relleno. Los valores de configuración se dividen en tres tipos:

- valores de configuración que es necesario que estén presentes;
- valores de configuración específicos de IPCable2Home adicionales o facultativos que PUEDEN estar presentes;
- valores de configuración específicos de fabricante.

Un fichero de configuración del PS PUEDE incluir distintos parámetros, pero los únicos parámetros que necesariamente DEBEN ser incluidos en el fichero de configuración del PS son la verificación de integridad del mensaje (MIC, *message integrity check*) del PS (tipo 53) y el marcador de fin de datos (tipo 255). Un fichero de configuración de barrera contra fuegos PUEDE contener varios parámetros de TLV tipo 28 para la configuración del contra fuegos, pero el único parámetro que necesariamente DEBE estar incluido en el fichero de configuración de la barrera contra fuegos es el marcador de fin de datos (tipo 255). Si el fichero de configuración de la barrera contra fuegos contiene una verificación de integridad de mensaje del PS (MIC) (tipo 53), el PS DEBE ignorarlo.

Para facilitar la gestión uniforme del PS, éste DEBE soportar un fichero de configuración que tenga hasta 64 K-bytes de longitud.

Cada elemento de servicios de portal DEBE soportar los tipos de parámetros de configuración 0, 9, 10, 21, 28, 32, 33, 34, 38, 43, 53 y 255, que se describen en esta cláusula. Cada parámetro TLV en el fichero de configuración de la barrera contra fuegos describe un atributo de esta última. Ya que la barrera contra fuegos de IPCable2Home se configura accediendo a la MIB de seguridad de IPCable2Home (véase 11.6.4, Requisitos de la barrera contra fuegos), por lo general un fichero de configuración de la barrera contra fuegos incluye valores de configuración TLV tipo 28, que a su vez incluyen objetos MIB de SNMP. La información de configuración de la barrera contra fuegos específica de fabricante podrá transferirse al PS en el fichero de configuración de la barrera contra fuegos utilizando el valor tipo 43 (TLV-43) de configuración específica de fabricante. Si el fichero de configuración no incluye los atributos necesarios, el PS DEBE rechazar el fichero.

El tamaño del valor en el campo longitud de cualquier parámetro de configuración incluido en un fichero de configuración de IPCable2Home DEBE ser de 2 octetos.

El valor longitud de cada tipo descrito en las descripciones de TLV en esta cláusula es la longitud real en octetos del campo valor.

7.4.4.1.1 Valor de configuración del relleno

Éste no tiene campos longitud o valor y solamente se utiliza a continuación del marcador de fin de datos para rellenar el fichero hasta alcanzar un número entero de palabras de 32 bits.

Tipo	Longitud	Valor
0	---	---

7.4.4.1.2 Nombre del fichero de actualización de software

Se trata del nombre del fichero de actualización de software para el dispositivo de IPCable2Home. Este nombre se especifica con la calificación completa del directorio. Se prevé que el fichero residirá en un servidor TFTP identificado en una opción de los valores de configuración.

Tipo	Longitud	Valor
9	Variable	Nombre de fichero

7.4.4.1.3 Control de acceso a escritura SNMP

Este objeto permite inhabilitar el acceso de SNMP "Set" a objetos particulares de la MIB. Cada ejemplar de este objeto controla el acceso a todos los objetos de la MIB que pueden sobreescribirse, y cuyos prefijos ID de objeto (OID) concuerden. Este objeto puede repetirse para inhabilitar el acceso a cualquier número de objetos de la MIB.

Tipo	Longitud	Valor
10	n	Prefijo de OID más bandera de control

Siendo n el tamaño de la codificación del prefijo OID más 1 byte de la bandera de control conforme a las reglas de codificación básica en ASN.1 [Rec. UIT-T X.690 | ISO/CEI 8825-1].

La bandera de control puede tener los siguientes valores:

0 – permite el acceso a la escritura

1 – impide el acceso a la escritura

Es posible utilizar cualquier prefijo OID. El OID nulo 0.0 puede utilizarse para controlar el acceso a todos los objetos de la MIB. (El OID descrito en 1.3.6.1 tendrá el mismo efecto.)

Cuando hay múltiples ejemplares de este objeto y se trasladan, tendrá precedencia el prefijo más largo (más específico).

Por consiguiente, un ejemplo podría ser:

someTable impide el acceso a la escritura

someTable.1.3 permite el acceso a la escritura

Este ejemplo impide el acceso a todos los objetos de someTable excepto en el caso de someTable.1.3.

7.4.4.1.4 Servidor TFTP de actualización de software

Se trata de la dirección IP del servidor TFTP en el que reside el fichero de actualización de software del dispositivo de IPCable2Home.

Tipo	Longitud	Valor
21	4	ip1, ip2, ip3, ip4

7.4.4.1.5 Objeto MIB de SNMP de primera fase con longitud ampliada

Este objeto permite que se establezcan los valores de los objetos MIB SNMP a través del proceso de registro TFTP, previo al conjunto de establecimientos SNMP realizados con TLV-28. El propósito de este TLV es incluir exclusivamente aquellos establecimientos SNMP que deban tener lugar antes que otros para garantizar un funcionamiento correcto, tal como ocurre con los objetos SetToFactory (por ejemplo, cabhPsDevSetToFactory) que borran los objetos MIB persistentes. Es previsible que TLV-28 incluya establecimientos SNMP que no tengan prioridad.

El valor de este parámetro es una vinculación de variable SNMP (VarBind), conforme a [RFC 3416]. La VarBind se codifica de acuerdo a las reglas de codificación básica de ASN.1, como si formase parte de una PDU de petición de establecimiento SNMP.

Tipo	Longitud	Valor
27	Variable	Vinculación variable

El PS DEBE tratar la vinculación de variable, en un TLV tipo 27, como si formase parte de una petición de establecimiento SNMP con las siguientes advertencias:

- DEBE tratar la petición como si estuviera plenamente autorizada (no puede rechazarla por falta de privilegios).
- No aplican las disposiciones de control de escritura SNMP.
- El PS no genera una respuesta SNMP.
- Este objeto PUEDE repetirse con distintos VarBinds para "establecer el valor" de un conjunto de objetos MIB. Todos los establecimientos de SNMP que existan en un fichero de configuración en TLVs tipo 27 DEBEN tratarse simultáneamente. Cada VarBind DEBE estar limitado 65 535 bytes.
- Este objeto DEBE ser procesado antes que ningún TLV tipo 28 incluido en el fichero de configuración.

7.4.4.1.6 Objeto MIB de SNMP con longitud ampliada

Este objeto permite que los objetos MIB de SNMP arbitrarios se fijen a través del proceso de registro TFTP, siendo el valor una vinculación variable de SNMP (VarBind), conforme a [RFC 3416]. La VarBind se codifica de acuerdo a las reglas de codificación básica de ASN.1, como si formase parte de la petición de establecimiento SNMP (SNMP Set).

Tipo	Longitud	Valor
28	Variable	Vinculación variable

El PS DEBE tratar la vinculación variable, en un TLV tipo 28, como si formase parte de una petición de establecimiento SNMP con las siguientes advertencias:

- DEBE tratar la petición como plenamente autorizada (no puede rechazar la petición por falta de privilegios).
- No pueden aplicarse las disposiciones de control de escritura SNMP (véase la cláusula anterior).
- El PS no genera ninguna respuesta SNMP.
- Este objeto PUEDE repetirse con distintas VarBinds para "establecer" cierto número de objetos de la MIB. Todas las peticiones de establecimiento SNMP que existan en un fichero de de configuración en un TLV tipo 28 DEBEN tratarse simultáneamente. Cada VarBinds debe limitarse a 65 535 bytes.

7.4.4.1.7 Certificado de verificación de código del fabricante

Se trata del certificado de verificación de código del fabricante (M-CVC, *manufacturer's code verification certificate*) para la descarga segura de software. Véase 11.8.4.4.2, Inicialización de red.

Tipo	Longitud	Valor
32	Variable	CVC del fabricante (ASN.1 codificada en DER)

7.4.4.1.8 Certificado de verificación de código del cofirmante

Se trata del certificado de verificación de código del cofirmante (C-CVC, *co-signer's code verification certificate*) para la descarga segura de software. Véase 11.8.4.4.2, Inicialización de la red.

Tipo	Longitud	Valor
33	Variable	CVC del cofirmante (ASN.1 codificada en DER)

7.4.4.1.9 Valor de arranque (Kickstart) de SNMPv3

(Véase C.1.2.8, Especificación de RFI DOCSIS 1.1 SP-RFIv1.1-I09-020830.)

Los elementos de servicios de portal conformes DEBEN comprender el siguiente TLV y sus subelementos, y poder arrancar el acceso de SNMPv3 al PS sin tomar en cuenta si el PS está funcionando en el modo NmAccess o en el modo de coexistencia (véase 6.3.3, Descripción del sistema CMP y 6.3.3.1.4.2, Requisitos del modo de gestión de red).

Tipo	Longitud	Valor
34	n	Compuesto

En el fichero de configuración pueden incluirse hasta cinco de estos objetos. Cada uno da por resultado la adición de una fila a usmDHKickstartTable y usmUserTable y además produce la generación de un número público de agente para esas filas.

7.4.4.1.9.1 Nombre de seguridad de arranque (Kickstart) de SNMPv3

Tipo	Longitud	Valor
34.1	2-16	Nombre de seguridad codificado en UTF8

En el caso del conjunto de caracteres ASCII, las codificaciones en UTF8 y en ASCII son idénticas. Por lo general, esto se especificará como uno de los usuarios USM integrados en IPCable2Home, por ejemplo, "CHAdministrator".

El nombre de seguridad NO termina en cero. Esto se notifica en usmDHKickStartTable como usmDHKickStartSecurityName y en usmUserTable como usmUserName y usmUserSecurityName.

7.4.4.1.9.2 Número público del gestor de arranque (Kickstart) de SNMPv3

Tipo	Longitud	Valor
34.2	n	Número público Diffie-Hellman del gestor expresado como una cadena de octetos

Se trata del número público Diffie-Hellman deducido a partir de un número aleatorio generado de manera privada (por el gestor o el operador) y transformado conforme a [RFC 2786]. Esto se notifica en usmDHKickStartTable como usmKickstartMgrPublic. Cuando se combina con el objeto notificado en la misma fila de usmKickstartMyPublic, puede utilizarse para deducir las claves en la fila correspondiente en usmUserTable.

7.4.4.1.10 Receptor de notificaciones SNMP

Tipo	Longitud	Valor
38	n	Compuesto

Este elemento de fichero de configuración del PS especifica una estación de gestión de red que recibirá las notificaciones del PS cuando se encuentre en el modo de gestión de red de coexistencia. Este TLV (38) consta de varios sub-TLV dentro del elemento del fichero de configuración del TLV. Podrán incluirse hasta 10 de estos elementos en el fichero de configuración del PS. En 6.3.3.1.4.6,

Correspondencia de los campos TLV con las filas del cuadro SNMPv3 creado, se dan detalles con relación al modo de correspondencia del elemento del fichero de configuración con los cuadros funcionales de SNMPv3.

Todos los campos multi-byte de este sub-TLV DEBEN colocarse en el orden de los bytes de la red.

7.4.4.1.10.1 Sub-TLV 38.1 – Dirección IP del receptor de trampas

Dirección IPv4 del receptor de trampas, en código binario.

Tipo	Longitud	Valor
38.1	4	Dirección IP

7.4.4.1.10.2 Sub-TLV 38.2 – Número de puerto UDP del receptor de trampas

Número del puerto UDP del receptor de trampas en código binario.

Tipo	Longitud	Valor
38.2	2	Puerto UDP

Si no existe este sub-TLV en un fichero de configuración, se utilizará el valor por defecto 162.

7.4.4.1.10.3 Sub-TLV 38.3 – Tipo de trampa enviada por el PS (Nota 2)

Tipo de trampa.

Tipo	Longitud	Valor
38.3	2	Tipo de trampa

El PS DEBE soportar los siguientes valores de tipo de trampa:

1 = Trampa SNMPv1 en un paquete SNMPv1

2 = Trampa SNMPv2c en un paquete SNMPv2c

3 = Informe SNMP en un paquete SNMPv2c

4 = Trampa SNMPv2c en un paquete SNMPv3

5 = Informe SNMP en un paquete SNMPv3

7.4.4.1.10.4 Sub-TLV 38.4 – Fin de temporización

Fin de temporización, en milisegundos, que se utiliza para enviar mensajes de informe de SNMP.

Tipo	Longitud	Valor
38.4	2	0-65 535

7.4.4.1.10.5 Sub-TLV 38.5 – Reintentos

Número de reintentos cuando se envía un informe, después de haber enviado el informe por primera vez.

Tipo	Longitud	Valor
38.5	2	0 – 65 535

7.4.4.1.10.6 Sub-TLV 38.6 – Parámetros de filtrado de la notificación

Tipo	Longitud	Valor
38.6	n	OID de filtro

Siendo n el tamaño del identificador de objeto filtro codificado en ASN.1.

El OID de filtro es un identificador de objeto con formato ASN.1 del valor snmpTrapOID que identifica las notificaciones que se deben enviar al receptor de notificaciones. Se enviará esta notificación y todas las que estén debajo de ella.

Si este sub-TLV no está presente, el receptor de notificaciones recibirá todas las notificaciones generadas por el agente SNMP.

7.4.4.1.10.7 Sub-TLV 38.7 – Nombre de seguridad que debe utilizarse cuando se envía la notificación SNMP V3

Tipo	Longitud	Valor
38.7	2-16	Nombre de seguridad codificado en UTF8

Este sub-TLV no es necesario para el tipo de trampa = 1, 2 ó 3. El PS DEBE ignorar el sub-TLV 38.7 si el tipo de trampa en el sub-TLV 38.3 es 1, 2 ó 3. Si no se suministra el sub-TLV 38.7 para un tipo de trampa 4 ó 5, el PS DEBE enviar la notificación de SNMPv3 en el nivel de seguridad noAuthNoPriv utilizando el nombre de seguridad "@PSconfig". (Véase la nota 2.)

Nombre de seguridad (SecurityName)

Se trata del nombre de seguridad de SNMPv3 que se utiliza cuando se envía una notificación SNMPv3. Se utiliza únicamente si el tipo de trampa se fija a 4 ó 5. Este nombre DEBE especificarse en un TLV tipo 34 del fichero de configuración como parte del procedimiento de arranque DH. Las notificaciones DEBEN enviarse utilizando las claves de autenticación y de privacidad calculadas por el PS durante el procedimiento de arranque DH.

NOTA 1 – Cuando el PS recibe uno de estos elementos TLV DEBE introducir anotaciones en los siguientes cuadros, a fin de provocar la transmisión de la trampa deseada: snmpNotifyTable, snmpTargetAddrTable, snmpTargetParamsTable, snmpNotifyFilterProfileTable, snmpNotifyFilterTable, snmpCommunityTable, usmUserTable, vacmSecurityToGroupTable, vacmAccessTable y vacmViewTreeFamilyTable.

NOTA 2 – Tipo de trampa: la cadena comunitaria para las trampas en los paquetes SNMPv1 y v2 DEBE ser "pública". El nombre de seguridad en las trampas e informes de los paquetes SNMPv3 en los que no se ha especificado nombre de seguridad DEBE ser "@PSconfig" y en este caso el nivel de seguridad DEBE ser NoAuthNoPriv.

NOTA 3 – OID de filtro: SNMPv3 permite la especificación de los OID de trampa que se van a enviar a un receptor de trampas. El OID de filtro en el elemento de configuración especifica el OID de la raíz de un subárbol de filtros de trampa. Todas las trampas con un OID de trampa incluido en este sub-árbol de filtro de trampas DEBEN enviarse al receptor de trampas.

NOTA 4 – El fichero de configuración del PS podrá contener también elementos MIB de TLV (TLV-28) que efectúan anotaciones en cualquiera de los 10 cuadros relacionados en la nota 1. El PS DEBE ignorar los elementos MIB de TLV que utilizan columnas de índice que comienzan con los caracteres "@PSconfig".

7.4.4.1.11 Información específica de fabricante

Si se proporciona información específica de fabricante al PS, ésta DEBE codificarse en el campo de información específica de fabricante (VSIF, *vendor-specific information field*) (código 43) utilizando el campo ID de fabricante, para especificar qué tuplas TLV se deben aplicar a qué productos del fabricante. El primer sub-TLV de un VSIF correctamente constituido es un sub-TLV de ID de fabricante específico (código 43.1). El PS DEBE rechazar el fichero de configuración si cualquiera de los TLV del VSIF (tipo 43) no está correctamente constituido.

Un fichero de configuración de PS puede tener varios VSIF que incluyan los mismos o diferentes sub-TLV de ID de fabricante. El PS sólo procesará aquellos VSIF que tengan un sub-TLV de ID de fabricante que concuerde con un ID de fabricante e ignorará los VSIF con sub-TLV de ID de fabricante para los que exista dicha concordancia. Es posible añadir subtipos específicos de fabricante después del tipo 43.1.

Tipo	Longitud	Valor
43	N	Valores específicos de fabricante

Sub-TLV 43.1 – Tipo de ID de fabricante.

Identificación del fabricante especificada por los tres bytes del identificador único de organización del fabricante del PS.

Tipo	Longitud	Valor
43.1	3	v1, v2, v3

7.4.4.1.12 Verificación de integridad del mensaje del PS (PS MIC)

Tipo	Longitud	Valor
53	20	Troceo SHA de 160 bits (20 octetos)

Este parámetro incluye un troceo (PS MIC, *PS message integrity check*) que se calcula mediante un algoritmo troceo seguro (SHA-1, *Secure Hash Algorithm*), definido en NIST, FIPS PUB 180-1: Secure Hash Standard, abril de 1995. Este TLV se utiliza únicamente en el fichero de configuración justo antes del marcador de fin de datos.

7.4.4.1.13 Marcador de fin de datos

Se trata de un marcador especial para indicar el fin de los datos. Este marcador no tiene campos de longitud o de valor.

Tipo	Longitud	Valor
255	---	---

7.4.4.2 Requisitos para la activación de BPSC

La transferencia del fichero de configuración, del servidor TFTP o del servidor HTTPS en la red de datos por cable al PS, se inicia mediante un evento denominado activador. Requisitos para activar la transferencia de un fichero de configuración del PS o de un fichero de configuración de la barrera contra fuegos del servidor TFTP o del servidor HTTPS al PS, son los que se indican a continuación.

El modo de activación de la descarga del fichero de configuración del PS depende del modo de configuración en el que esté funcionando el PS. El CMP DEBE leer el valor de cabhPsDevProvMode (véase 7.3.3.2.4) antes de iniciar cualquier descarga del fichero de configuración del PS. El método de activación de la descarga del fichero de configuración de la barrera contra fuegos no depende del modo de configuración.

7.4.4.2.1 Activador de la descarga del fichero de configuración del PS para el modo de configuración DHCP

Si el PS recibe la dirección del servidor TFTP o HTTPS en el campo 'siaddr' y el nombre del fichero de configuración del PS en el campo 'file' del mensaje ACK DHCP Y el valor de cabhPsDevProvState = inProgress(2), el PS DEBE combinar la dirección del servidor y el nombre del fichero de configuración del PS para formar un valor codificado en URL y escribir ese valor en el objeto cabhPsDevProvConfigFile de la MIB de PSDev. El PS DEBE utilizar el siguiente formato para el valor codificado en URL de la dirección IP del servidor TFTP y del nombre del fichero de configuración del PS:

tftp://IPv4_address_of_the_TFTP_server/full_path_ to_the_PS_Configuration_File/PS_Configuration_File_name

El PS DEBE utilizar el siguiente formato para el valor codificado en URL de la dirección IP del servidor HTTPS y del nombre del fichero de configuración del PS:

https://IPv4_address_of_the_HTTPS_server/full_path_ to_the_PS_Configuration_File/PS_Configuration_File_name

La descarga del fichero de configuración del PS, mediante un PS que funciona en el modo de configuración DHCP, se activa por la presencia de la ubicación (dirección IP del servidor TFTP o HTTPS) y el nombre del fichero de configuración del PS en el mensaje DHCP emitido al PS (CDC) por el servidor DHCP en la red de cable. Véase 7.3.3.2.4, Requisitos del CDC.

Si el PS (CDC) se encuentra funcionando en el modo de configuración DHCP (indicado por el valor de cabhPsDevProvMode), después de que recibe un mensaje ACK DHCP del servidor DHCP en la red de cable, y la dirección IP en el campo 'siaddr' no concuerda con la primera dirección IP en la opción 72 de DHCP Y el valor de cabhPsDevProvState = inProgress(2), el PS DEBE emitir una petición TFTP Get al servidor identificado en el campo 'siaddr' del mensaje DHCP para descargar el fichero de configuración.

Si el PS (CDC) se encuentra funcionando en el modo de configuración DHCP (indicado por el valor de cabhPsDevProvMode), después de que recibe un mensaje DHCP ACK del servidor DHCP en la red de cable, y la dirección IP en el campo 'siaddr' concuerda con la primera dirección IP en la opción 72 de DHCP, y el objeto de la MIB cabhPsDevTodSyncStatus tiene un valor '1' (el acceso al ToD fue satisfactorio), en ese caso el PS DEBE establecer una sesión TLS como se describe en la cláusula 11, y emitir una petición HTTP Get al servidor identificado en el campo 'siaddr' del mensaje DHCP, para descargar el fichero de configuración.

Si el PS (CDC) se encuentra funcionando en el modo de configuración DHCP (indicado por el valor de cabhPsDevProvMode), después de que recibe un mensaje ACK DHCP del servidor DHCP en la red de cable, y la dirección IP en el campo 'siaddr' concuerda con la primera dirección IP en la opción 72 de DHCP, y el objeto de la MIB cabhPsDevTodSyncStatus tiene un valor '2' (el acceso al ToD fracasó), el PS DEBE esperar hasta que el objeto de la MIB cabhPsDevTodSyncStatus tenga un valor '1' (el acceso al ToD fue satisfactorio), antes de establecer una sesión TLS como se describe en la cláusula 11, y de emitir una petición HTTP Get al servidor identificado en el campo 'siaddr' del mensaje DHCP, para descargar el fichero de configuración.

La modificación de cabhPsDevProvConfigFile NO DEBE activar un PS que funciona en el modo de configuración DHCP para que descargue un fichero de configuración. Un PS que funcione en el modo de configuración DHCP DEBE tratar cabhPsDevProvConfigFile como un objeto de sólo lectura.

7.4.4.2.2 Activador de la descarga del fichero de configuración del PS para el modo de configuración SNMP

Si el PS se encuentra funcionando en el modo de configuración SNMP (indicado por el valor de cabhPsDevProvMode), la descarga de su fichero de configuración NO DEBE ocurrir antes de que se complete el proceso de establecimiento de SNMPv3 (véase 11.4, Mensajería de gestión segura para el PS, para obtener los detalles relativos al proceso de establecimiento de SNMP).

Si el PS se encuentra funcionando en el modo de configuración SNMP (indicado por el valor de cabhPsdevProvMode), el elemento PS NO DEBE iniciar una descarga de fichero de configuración del PS si el objeto de la MIB cabhPsDevTodSyncStatus tiene un valor '2' (el acceso al ToD fracasó).

Si el PS funciona en el modo de configuración SNMP y el tiempo transcurrido desde que ha enviado el informe de admisión de configuración descrito en el cuadro 13-3, a continuación de la autenticación KDC, es igual al valor de cabhPsDevProvisioningTimer Y no se ha activado la descarga de un fichero de configuración por parte del PS, éste DEBE fijar el valor de cabhPsDevProvState a pass(1) y continuar con el proceso de configuración para el modo de configuración SNMP, tal como se describe en 13.4. Si el PS funciona en el modo de configuración SNMP y se activa la descarga de un fichero de configuración de PS cuando el tiempo transcurrido desde que ha generado el informe de admisión de configuración es inferior al valor de of cabhPsDevProvisioningTimer, el PS NO DEBE fijar el valor de cabhPsDevProvState a pass(1) hasta que se realice satisfactoriamente la descarga y procesamiento del fichero especificado de

configuración de PS. Si el PS funciona en el modo de configuración SNMP y ha sido activado para descargar de un fichero de configuración de PS, DEBE fijar el valor de cabhPsDevProvState a pass(1) cuando haya completado satisfactoriamente la descarga y el procesamiento del fichero de configuración del PS.

Cuando el PS que se encuentra funcionando en el modo de configuración SNMP (indicado por el valor de cabhPsDevProvMode), emite una petición TFTP para poder descargar un fichero de configuración de PS (sujeto a las condiciones descritas en otros requisitos, más adelante), el PS DEBE completar la fase de descarga. Cuando el PS (CMP) concluye satisfactoriamente la descarga del fichero de configuración del PS solicitado, DEBE procesarlo antes de emitir una nueva petición TFTP por otro fichero de configuración de PS.

El PS DEBE tratar de descargar y procesar el fichero de configuración cuyo nombre y dirección se especifican en cabhPsDevProvConfigFile cuando recibe una instrucción de establecimiento SNMP para el objeto cabhPsDevProvConfigFile, si las siguientes condiciones son verdaderas:

- el PS se encuentra funcionando en el modo de configuración SNMP;
- el objeto de la MIB cabhPsDevTodSyncStatus tiene un valor '1' (el acceso al ToD fue satisfactorio); y
- cabhPsDevProvConfigFileStatus = idle(1).

El formato de cabhPsDevProvConfigFile DEBE ser una dirección IP de servidor TFTP codificada en URL y un nombre de fichero de configuración.

Si el PS (CMP) que funciona en el modo de configuración SNMP recibe una petición de establecimiento SNMP desde el NMS para actualizar el valor de cabhPsDevProvConfigFile y cabhPsDevProvConfigFileStatus = busy(2), o si el objeto cabhPsDevProvConfigHash no tiene un valor válido, en ese caso el PS DEBE rechazar la petición de establecimiento.

7.4.4.2.3 Activación del fichero de configuración de la barrera contra fuegos

La descarga del fichero de configuración de la barrera contra fuegos se activa cuando el valor utilizado para ESTABLECER (SET) el valor del objeto de la MIB cabhSec2FwPolicyFileURL, mediante el fichero de configuración del PS o la instrucción SNMP SET, difiere del valor de la MIB cabhSec2FwPolicySuccessfulFileURL. Si el valor utilizado para ESTABLECER (SET) el valor del objeto de la MIB cabhSec2FwPolicyFileURL, mediante el fichero de configuración del PS o una instrucción SNMP SET, es el mismo del valor de la MIB cabhSec2FwPolicySuccessfulFileURL, NO DEBE activarse la descarga del fichero de configuración de la barrera contra fuegos.

Cuando se ha activado una descarga, el PS DEBE utilizar el prefijo del valor del objeto MIB cabhSecFwPolicyFileURL para determinar si se utiliza TFTP (tftp://) o una sesión TLS (https://), tal como se define en la cláusula 11 para la descarga del fichero de configuración de la barrera contra fuegos.

7.4.4.2.4 Funcionamiento posterior a la activación

Una vez efectuada la activación, el PS DEBE utilizar un cliente TFTP conforme a [RFC 1350] y a [RFC 2348] o HTTP conforme a [RFC 2616] para descargar los ficheros de configuración.

Se debe utilizar un mecanismo de señalización para notificar a la entidad de gestión que el PS se encuentra procesando un fichero de configuración. El objeto cabhPsDevProvConfigFileStatus de la MIB Dev del PS tiene por objeto fungir como este mecanismo de señalización.

Si un PS no se encuentra solicitando, descargando o procesando un fichero de configuración, DEBE fijar cabhPsDevProvConfigFileStatus = idle(1). Cuando el PS ha emitido una petición TFTP para un fichero de configuración especificado en cabhPsDevProvConfigFile, DEBE fijar cabhPsDevProvConfigFileStatus = busy(2). Cuando el PS completa el procesamiento del fichero de configuración del PS, DEBE fijar cabhPsDevProvConfigFileStatus = idle(1).

Una vez efectuada la activación para descargar un fichero de configuración, el elemento PS DEBE seguir tratando de descargar el fichero de configuración especificado de la ubicación determinada hasta que se logre la descarga satisfactoria y se calcule con éxito la generación correspondiente, como se describe en 7.4.4.3, Requisitos de autenticación de la verificación del fichero de configuración y del modo de configuración SNMP. Si el primer intento no es satisfactorio, el PS DEBE utilizar un temporizador adaptativo para TFTP y HTTPS basándose en la reducción exponencial binaria que se describe más adelante, hasta que reciba con éxito el fichero solicitado del servidor en la red de datos por cable:

- cada reintento se llevará a cabo de 2^n segundos a continuación del intento anterior, siendo n = [1, 2, 3, 4 ó 5] para el contador de reintentos del fichero de configuración del PS o de la barrera contra fuegos;
- n = 1 para el primer reintento y a continuación se incrementa en uno para cada intento subsiguiente hasta n = 5;
- si el PS no obtiene con éxito el fichero de configuración del PS solicitado después del intento con n = 5, n debe reiniciar en 1 y el PS debe rearrancar el proceso de adquisición de la dirección IP de WAN-Man mediante DHCP.
- si el PS no obtiene con éxito el fichero de configuración de la barrera contra fuegos solicitado después del intento con n = 5, n debe reiniciar en 1 y el PS debe continuar su funcionamiento normal, es decir, no debe rearrancar el proceso de adquisición de la dirección IP de WAN-Man.

El PS DEBE intercambiar mensajes TFTP y HTTPS únicamente a través de la interfaz WAN-Man del PS. El PS DEBE rechazar cualquier fichero de configuración que no se reciba a través de dicha interfaz.

Cuando se completa la descarga del fichero de configuración y el mismo se autentica adecuadamente, como se describe en 7.4.4.3, Requisitos de autenticación de la verificación del fichero de configuración y del modo de configuración SNMP del PS, el PS DEBE procesar los TLV incluidos en el fichero como se describe más adelante. Véase 7.4.4.4, Requisitos de procesamiento del fichero de configuración y de la notificación de estado, por lo que se refiere a los detalles específicos del tratamiento de errores y de la generación de eventos durante el procesamiento del fichero de configuración.

El PS DEBE utilizar los parámetros extraídos del fichero de configuración para fijar los objetos gestionados en la base de datos del PS. Este proceso equivale funcionalmente a una operación SET SNMP, pero no se apoya en los permisos de acceso del usuario o basados en vistas. El PS DEBE actualizar incondicionalmente los objetos gestionados en la base de datos del PS correspondientes a los OID reconocidos.

El PS DEBE traducir los elementos TLV-27 del fichero de configuración a una sola PDU SNMP que contenga (n) OID/ejemplar y componentes de valor de la MIB (varbinds de SNMP) y traducir los elementos TLV-28 del fichero de configuración a una sola PDU SNMP que contenga (n) OID/ejemplar y componentes de valor de la MIB (varbinds de SNMP). Conforme a [RFC 3416], la PDU SNMP única generada por el fichero de configuración TLV-27 será tratada "como si se produjera simultáneamente", la PDU SNMP única generada por el fichero de configuración TLV-28 será tratada "como si se produjera simultáneamente" y el PS DEBE comportarse congruentemente, sin tener en cuenta el orden en que aparecen los elementos TLV-27 o TLV-28 en el fichero de configuración o en las PDU SNMP. El requisito de la PDU SNMP única generada por el fichero de configuración es congruente con el comportamiento de los paquetes PDU SNMP recibidos de un gestor de SNMP: el orden de las varbind de la PDU SNMP no tiene importancia, y no existe un límite definido para la PDU SNMP MAX. Una vez construida una PDU SNMP única, el PS la procesa y determina la aceptación o rechazo de la configuración del PS basándose en las reglas de procesamiento del fichero de configuración, descritas en 7.4.4.4, Requisitos de procesamiento del

fichero de configuración y de la notificación de estado del PS. Al procesar la PDU SNMP, el PS DEBE soportar CreateAndGo para la creación de filas.

El PS DEBE actualizar el tamaño del fichero de configuración del PS en el objeto cabhPsDevProvConfigFileSize de la MIB.

El PS DEBE actualizar el número de TLV procesados (es decir, los TLV que tienen por objeto modificar la configuración del PS de acuerdo con su propio campo valor) y el número de TLV ignorados (es decir, los TLV necesarios para modificar la configuración del PS conforme a sus propios campos valor que no son satisfactorios) a partir del fichero de configuración del PS, en los objetos de la MIB cabhPsDevProvConfigTLVProcessed y cabhPsDevConfigTLVRejected, respectivamente[1]. Los tipos 255 (marcador de fin de datos), 53 (PS MIC), 0 (valor de configuración de relleno) del parámetro de configuración y los pares de campos tipo y longitud que abarcan sub-TLV no especifican valores en los campos valor previstos para modificar la configuración del PS y por consiguiente NO DEBEN tenerse en cuenta en los valores de cabhPsDevProvConfigTLVProcessed y cabhPsDevConfigTLVRejected.

7.4.4.3 Requisitos de autenticación de la verificación del fichero de configuración y del modo de configuración SNMP

El algoritmo que se utiliza para autenticar el fichero de configuración depende del modo de configuración en el que esté funcionando el PS (véase 5.5, Modos de funcionamiento de IPCable2Home). El PS soporta dos modos de configuración: DHCP y SNMP. El modo de configuración DHCP soporta dos métodos de autenticación del fichero de configuración, que dependen de la información recibida en el campo 'siaddr' del mensaje ACK DHCP.

En las siguientes subcláusulas se describen los algoritmos y los requisitos de seguridad necesarios para verificar el troceo del fichero de configuración basándose en el modo de configuración del elemento PS. Este elemento DEBE soportar ambos algoritmos de seguridad especificados en 7.4.4.3.1, Verificación del fichero de configuración del PS para el modo de configuración DHCP y 7.4.4.3.2, Algoritmo de autenticación del fichero de configuración del PS para el modo de configuración SNMP.

7.4.4.3.1 Verificación del fichero de configuración del PS para el modo de configuración DHCP

Cuando el PS funciona en el modo de configuración DHCP utiliza el método de verificación del fichero de configuración basada en troceo, o autentica el mensaje en el que se transfiere el fichero, dependiendo de la configuración del sistema de configuración del operador de cable.

El PS DEBE conducir la verificación del fichero de configuración basada en troceo que se describe más adelante:

1) Cuando el generador del fichero de configuración del sistema de configuración crea un nuevo fichero de configuración de PS o modifica un fichero existente, dicho generador crea un troceo mediante el algoritmo SHA-1 (algoritmo troceo seguro) del contenido del fichero de configuración del PS, considerándolo como una cadena de bytes. El marcador de fin de datos y cualquier relleno que vengan a continuación no se incluyen en el cálculo del troceo.
2) El generador del fichero de configuración añade el valor del troceo, calculado en el paso 1, al fichero de configuración del PS como el último valor de TLV (inmediatamente antes del marcador de fin de datos) utilizando un TLV tipo 53. A continuación, el fichero de configuración del PS lo pone a disposición del servidor TFTP que corresponda.

---

[1] Conforme a esas definiciones, un TLV que no puede configurar satisfactoriamente el PS se cuenta dos veces, una por cabhPsDevProvConfigTLVProcessed y otra por cabhPsDevProvConfigTLVRejected. Un TLV que configura con éxito el PS se cuenta una sola vez por cabhPsDevProvConfigTLVProcessed.

3) El elemento PS descarga el fichero de configuración del PS.

4) El PS DEBE actualizar el objeto de la MIB cabhPsDevProvConfigHash con el valor del troceo del TLV que se creó en los pasos 1 y 2.

5) El elemento PS DEBE calcular el troceo SHA-1 del contenido del fichero de configuración del PS excluyendo el troceo TLV (utilizado para configurar el objeto de la MIB cabhPsDevProvConfigHash), el marcador de fin de datos y cualquier relleno a continuación. Si el valor del troceo calculado y el valor del objeto de la MIB cabhPsDevProvConfigHash son idénticos, se verifica la integridad del fichero de configuración del PS y DEBE procesarse este último; de lo contrario, el fichero DEBE rechazarse.

7.4.4.3.2 Algoritmo de autenticación del fichero de configuración del PS para el modo de configuración SNMP

El procedimiento para verificar la generación aleatoria del fichero de configuración del PS mediante el elemento PS en el modo de configuración SNMP es el siguiente:

1) Cuando el generador del fichero de configuración del sistema de configuración crea un nuevo fichero de configuración de PS o modifica un fichero existente, dicho generador creará un troceo SHA-1 (algoritmo troceo seguro) de todo el contenido del fichero de configuración del PS, considerándolo como una cadena de bytes. El marcador de fin de datos y cualquier relleno a continuación no se incluyen en el cálculo del troceo.

2) El NMS envía el valor de dicho troceo calculado en el paso 1 al elemento PS mediante un ESTABLECIMIENTO SNMP (SNMP SET). El PS actualiza su objeto de la MIB cabhPsDevProvConfigHash con el nuevo valor.

3) El NMS envía el nombre y la ubicación del fichero de configuración del PS mediante un ESTABLECIMIENTO SNMP. El PS actualiza su objeto de la MIB cabhPsDevProvConfigFile con el nuevo valor.

4) El elemento PS descarga el fichero nombrado del servidor TFTP configurado. Si el fichero de configuración del PS incluye el TLV tipo 53, el PS DEBERÁ ignorarlo.

5) El elemento PS DEBE calcular un troceo SHA-1 del contenido del fichero de configuración del PS excluyendo el TLV 53 en su caso, el marcador de fin de datos y cualquier relleno a continuación. Si los valores calculado y del objeto de la MIB cabhPsDevProvConfigHash son idénticos, se verifica la integridad del fichero de configuración del PS y DEBE procesarse este último; de lo contrario, el fichero DEBE rechazarse.

7.4.4.3.3 Verificación del fichero de configuración de la barrera contra fuegos

El PS debe utilizar la verificación del fichero de configuración de la barrera contra fuegos en el fichero de configuración de la barrera contra fuegos como se describe en esta cláusula si el fichero se proporciona en el modo de configuración SNMP o DHCP sin utilizar HTTPS/TLS como se describe en 11.9, Seguridad del fichero de configuración del PS en el modo de configuración DHCP.

Si el fichero de configuración de la barrera contra fuegos se descargó sin la utilización de HTTP/TLS, el PS DEBE seguir el procedimiento descrito en los pasos 1 a 5 a continuación para verificar la integridad de dicho fichero:

1) El generador del fichero de configuración de la barrera contra fuegos crea un troceo SHA-1 de todo el contenido del fichero, considerándolo como una cadena de bytes.

2) El sistema de configuración envía el valor del troceo calculado en el paso 1 al elemento PS en cualquiera de las dos siguientes maneras:

   a) modifica el objeto de la MIB cabhSec2FwPolicyFileHash mediante la TLV tipo 28 en el fichero de configuración del PS;

b) envía una instrucción de establecimiento SNMP para actualizar el objeto de la MIB cabhSec2FwPolicyHash.

3) El sistema de configuración envía el nombre y la ubicación del fichero de configuración de la barrera contra fuegos para activar su descarga en cualquiera de las dos siguientes maneras:

   a) modifica el objeto de la MIB cabhSec2FwPolicyFileURL a través del TLV tipo 28 en el fichero de configuración del PS;

   b) envía una instrucción de establecimiento de SNMP para actualizar el objeto de la MIB cabhSec2FwPolicyURL.

4) Si cabhSecFwPolicyFileOperStatus no es inProgress (1) y el valor utilizado para ESTABLECER (SET) el objeto de la MIB cabhSec2FwPolicyFileURL es distinto del valor de la MIB cabhSec2FwPolicySuccessfulFileURL, el elemento PS DEBE descargar inmediatamente el fichero nombrado desde el servidor configurado.

5) El PS DEBE calcular el troceo SHA-1 de todo el contenido del fichero de configuración de la barrera contra fuegos y compararla con la representada por el valor del objeto de la MIB cabhSec2FwPolicyFileHash. Si los valores de troceo calculados y del objeto anterior son idénticos, se verifica la integridad del fichero de configuración de la barrera contra fuegos y el PS DEBE utilizar ese fichero para configurar la barrera contra fuegos, de lo contrario el PS DEBE rechazar el fichero.

7.4.4.4 Procesamiento del fichero de configuración y requisitos de notificación de estado

El PS DEBE notificar el estado de la descarga del fichero de configuración y sus condiciones de error utilizando el proceso de notificación de eventos descrito en 6.3.3.2, Función de notificación de eventos del CMP.

En el cuadro 7-15 se identifican los modos de éxito y de fracaso que pueden encontrarse durante la descarga y el procesamiento del fichero de configuración del PS, y las medidas que DEBE tomar el PS cuando detecta alguno de estos modos.

Cuadro 7-15/J.192 – Condiciones de procesamiento del fichero de configuración

Condiciones	Medida
Fracaso de TFTP – se envió la petición Get y no se recibió respuesta	Notificar un evento (ID de evento 68000500) y reintentar TFTP.
Fracaso de HTTPS – se envió la petición Get, no se recibió respuesta o fracasó la conexión con el servidor HTTPS	Notificar un evento (ID de evento 68002000) y reintentar HTTPS.
Fracaso de TFTP – no se encontró el fichero de configuración	Notificar un evento (ID de evento 68000600) y reintentar TFTP.
Fracaso de HTTPS – fracasó el intento de descarga del fichero de configuración, no se ha excedido el número máximo de reintentos	Notificar un evento (ID de evento 68003000) y reintentar HTTPS.
Fracaso de TFTP – paquetes en desorden	Notificar un evento (ID de evento 68000700) y reintentar TFTP.
Fracaso de la descarga de TFTP – fracasó el intento de descarga del fichero de configuración y se alcanzó el número máximo de reintentos	Notificar un evento (ID de evento 68000900) y reinicializar.

Cuadro 7-15/J.192 – Condiciones de procesamiento del fichero de configuración

Condiciones	Medida
Fracaso de HTTPS – fracasó el intento de descarga del fichero de configuración, se realizó el número máximo de reintentos	Notificar un evento (ID de evento 68003100) y reinicializar.
Descarga satisfactoria del fichero de configuración	Notificar un evento (ID de evento 68001000 si para la descarga del evento se utilizó TFTP (no se utilizó TLS) o ID de evento 68003200 si para la descarga del evento se utilizó HTTP/TLS) e iniciar la verificación o autenticación del fichero de configuración.
Fracaso de la verificación de autenticación del fichero de configuración	Notificar un evento (ID de evento 68000800) y reinicializar. No se debe tratar de procesar el fichero.
El fichero de configuración es demasiado largo	Notificar un evento (ID de evento 73040102) y reinicializar. No se debe tratar de procesar el fichero.
No hay marcador de fin de datos	Notificar un evento (ID de evento 7340102) y reinicializar. No se debe tratar de procesar el fichero.
OID TLV-27 o TLV-28 duplicado	Notificar un evento (ID de evento 73040102), rechazar el fichero de configuración y reinicializar. Preserva los valores de todos los objetos que existían antes del intento de procesamiento del fichero de configuración erróneo. No se requiere que el PS restablezca los valores de los objetos MIB que habían sido asignados antes del intento de procesamiento del fichero de configuración si se ha establecido la única PDU SNMP creada a partir de los parámetros de TLV-27. Véase la cláusula sobre el funcionamiento posterior a la activación.
Duplicación de TLV-9, TLV-21, TLV-32, TLV-33 o de Sub-TLV en un único TLV-34, TLV-38, TLV-43	Notificar un evento (73040102), rechazar el fichero de configuración y reinicializar. Mantener todos los objetos que existían antes de tratar de procesar este fichero de configuración erróneo.
Tipo reconocido pero valor erróneo u OID de TLV-27 o TLV-28 válidos pero valor de MIB erróneo	Notificar un evento (ID de evento 73040102), rechazar el fichero de configuración y reinicializar. Conservar todos los valores de objeto que existían antes de tratar de procesar este fichero de configuración erróneo. No se requiere que el PS restablezca los valores que habían sido asignados antes del intento de procesamiento del fichero de configuración si se ha establecido la única PDU SNMP creada a partir de los parámetros de TLV-27. Véase la cláusula sobre el funcionamiento posterior a la activación.
Se encontró un OID de SNMP que no se reconoce	Ignorar el TLV en cuestión y notificar un evento (ID de evento 73040100). Continuar el procesamiento del fichero.
El campo de tipo no es válido para el PS	Ignorar el TLV en cuestión y notificar un evento (ID de evento 73040101). Continuar el procesamiento del fichero.

Véase el anexo B para obtener una lista de los eventos incluyendo los relacionados en el cuadro 7-15 e información relativa a la forma en que se notifican los eventos.

7.4.4.4.1 Intento no satisfactorio de descarga del fichero de configuración – Se autorizan reintentos de TFTP o de HTTPS

Si el contador de reintentos del fichero de configuración del PS es menor que 5 y se alcanza el fin de temporización de la petición TFTP o HTTPS Get, el fichero de configuración del PS no se

encontró en el servidor, o fracasó la petición TFTP o HTTPS Get debido al desorden de los paquetes, el PS DEBE iniciar el funcionamiento de las funciones CDS y CNP, notificar el evento adecuado y reintentar la descarga del fichero de configuración del PS, conforme con el algoritmo de reintentos que se describe en 7.4.4.2.4, Funcionamiento posterior a la activación.

Si el contador de reintentos del fichero de configuración de la barrera contra fuegos es menor que 5 y se alcanza el fin de temporización de la petición TFTP o HTTP Get, el fichero en cuestión no se encuentra en el servidor o fracasa el TFTP o HTTP Get, debido al desorden de los paquetes, el PS DEBE continuar su funcionamiento normal, notificar el evento adecuado y reintentar la descarga del fichero de configuración de la barrera contra fuegos, conforme con el algoritmo de reintentos que se describe en 7.4.4.2.4, Funcionamiento posterior a la activación.

7.4.4.4.2 Intento no satisfactorio de descarga del fichero de configuración – Se agotaron los reintentos de TFTP o HTTPS

Si el contador de reintentos del fichero de configuración del PS indica 5 y el PS no ha podido descargar satisfactoriamente el fichero de configuración del PS, el PS DEBE notificar el evento identificado en el cuadro 7-15, Condiciones de procesamiento del fichero de configuración, para indicar el fracaso del proceso de descarga del fichero de configuración del PS y liberar su dirección IP de WAN-Man del PS conforme a [RFC 2131], rearrancando el proceso de obtención de la dirección IP de WAN-Man mediante DHCP.

Si el contador de reintentos del fichero de configuración de la barrera contra fuegos indica 5 y el PS no ha podido descargar con éxito el fichero de configuración del PS, éste DEBE notificar el evento identificado en el cuadro 7-15, Condiciones de procesamiento del fichero de configuración, para señalar el fallo del proceso de descarga del fichero de configuración de la barrera contra fuegos y continuar su funcionamiento normal. Si el fichero de configuración de la barrera contra fuegos no puede descargarse con éxito, el PS DEBE funcionar como lo hacía antes del intento fallido de descarga del fichero en cuestión.

7.4.4.4.3 Descarga satisfactoria del fichero de configuración del PS

La descarga satisfactoria de este fichero se define como la recepción completa y correcta por el elemento PS del contenido del fichero de configuración del PS dentro del periodo de temporización de TFTP y el cálculo a cargo del PS de los valores del troceo del fichero de configuración del PS sin errores resultantes de dicho cálculo.

Si el PS descarga satisfactoriamente el fichero de configuración del PS, DEBE reiniciar el contador de reintentos de obtención del fichero de configuración del PS a cero y notificar el evento correspondiente a 'modo de fallo' de la descarga satisfactoria de TFTP en el cuadro 7-15, Condiciones de procesamiento del fichero de configuración.

7.4.4.4.4 Descarga no satisfactoria del fichero de configuración del PS

Si fracasa la verificación del fichero de configuración del PS como se especifica en 7.4.4.3, Requisitos de autenticación de la verificación del fichero de configuración y del modo de configuración SNMP, o en 11.9, Seguridad del fichero de configuración del PS en el modo de configuración DHCP, el PS DEBE detener el proceso de configuración, rechazar el fichero de configuración del PS, notificar el evento adecuado y rearrancar el proceso de obtención de la dirección IP de WAN-Man mediante DHCP.

Si el fichero de configuración del PS no contiene el TLV de fin de datos (TLV-255), ni PS MIC TLV (TLV-53), o es demasiado largo para poder procesarlo, el PS DEBE detener el proceso de configuración, rechazar el fichero de configuración del PS, notificar el evento adecuado y rearrancar el proceso de adquisición de la dirección IP de WAN-Man mediante DHCP.

Si el fichero de configuración del PS contiene elementos TLV-27 o TLV-28 duplicados (duplicado significa que dos o más objetos de la MIB de SNMP tienen un identificador de objeto (OID)

idéntico), el PS DEBE detener el proceso de configuración, rechazar el fichero de configuración del PS, notificar el evento adecuado y rearrancar el proceso de adquisición de la dirección IP de WAN-Man mediante DHCP.

Si el fichero de configuración del PS contiene un campo de tipo reconocido, pero un campo de valor erróneo o un OID de TLV-27 o TLV-28 válido con un valor de MIB erróneo, el PS DEBE detener el proceso de configuración, rechazar el fichero de configuración del PS, notificar el evento adecuado y rearrancar el proceso de adquisición de la dirección IP de WAN-Man mediante DHCP.

Si el fichero de configuración del PS contiene un campo de tipo no reconocido o un elemento TLV-27 o TLV-28 con un OID no reconocido, el PS DEBE ignorar ese TLV, notificar el evento adecuado y continuar con el procesamiento del fichero de configuración del PS.

Si el PS completa el procesamiento de la única PDU SNMP creada a partir del parámetro TLV-27, y determina que existen elementos TLV-28 duplicados, o elementos TLV-28 con un valor erróneo, no es preciso que el PS restablezca los objetos MIB que han sido modificados mediante el parámetro TLV-27 a sus valores previos, antes de rechazar el fichero de configuración, notificar el evento y reiniciar el PS.

7.4.4.4.5 Descarga satisfactoria del fichero de configuración de la barrera contra fuegos

La descarga satisfactoria de este fichero se define como la recepción completa y correcta del fichero por parte del elemento PS dentro del periodo de temporización de TFTP o HTTPS y la validación del fichero libre de errores definida por el procedimiento de verificación de la integridad que se describe en 7.4.4.3, Requisitos de autenticación de la verificación del fichero de configuración y del modo de configuración SNMP. Después de que el PS logra descargar satisfactoriamente el fichero de configuración de la barrera contra fuegos, el PS DEBE actualizar la MIB cabhSec2FwPolicySuccessfulFileURL con el mismo valor de la MIB cabhSec2FwPolicyFileURL.

Si el PS logra descargar satisfactoriamente el fichero de configuración de la barrera contra fuegos, DEBE reiniciar el contador de reintentos de dicho fichero a cero y notificar el ID de evento 80013500 (véase el cuadro B.1, Eventos definidos para IPCable2Home). Tras la descarga y el proceso satisfactorio del fichero de configuración de la barrera contra fuegos por parte del PS, la barrera contra fuegos DEBERÁ funcionar de acuerdo con la configuración del fichero descargado.

7.4.4.4.6 Descarga no satisfactoria del fichero de configuración de la barrera contra fuegos

Si fracasa la verificación del fichero de configuración de la barrera contra fuegos según 7.4.4.3, Requisitos de autenticación de la verificación del fichero de configuración y del modo de configuración SNMP, el PS DEBE continuar su funcionamiento normal, rechazar el fichero de configuración de la barrera contra fuegos y notificar el evento adecuado que se identifica en el cuadro B.1, Eventos definidos para IPCable2Home.

Si el fichero de configuración de la barrera contra fuegos contiene elementos TLV-27 o TLV-28 duplicados (duplicado significa que dos o más objetos de la MIB de SNMP tienen un identificador de objeto (OID) idéntico), el PS DEBE continuar su funcionamiento normal, rechazar el fichero de configuración de la barrera contra fuegos y notificar el evento adecuado que se identifica en el cuadro B.1, Eventos definidos para IPCable2Home.

Si el fichero de configuración de la barrera contra fuegos contiene un campo de tipo reconocido pero un campo valor erróneo, o un valor de OID de TLV-27 o TLV-28 con un valor de MIB erróneo, el PS DEBE continuar su funcionamiento normal, rechazar el fichero de configuración de la barrera contra fuegos y notificar el evento adecuado que se identifica en el cuadro B.1, Eventos definidos para IPCable2Home.

Si el fichero de configuración de la barrera contra fuegos contiene un campo tipo no reconocido o un elemento TLV-27 o TLV-28 con un OID no reconocido, el PS DEBE ignorar ese TLV, notificar

el evento adecuado que se identifica en el cuadro B.1, Eventos definidos para IPCable2Home, y continuar el procesamiento del fichero de configuración de la barrera contra fuegos.

Si la descarga del fichero de configuración de la barrera contra fuegos fracasa por cualquier razón, la barrera contra fuegos DEBE funcionar de acuerdo con la configuración anterior al intento de descarga fallido.

7.5 Función del PS – Cliente hora del día

7.5.1 Objetivos de la función de cliente hora del día

El objetivo de la función de cliente hora del día del PS es obtener la hora del día actual del servidor de hora del día en la red del operador de cable.

7.5.2 Directrices de diseño del sistema de la función cliente hora del día

La directriz que se presenta en el cuadro 7-16 da la orientación para la especificación de las capacidades determinadas para la función cliente hora del día del PS.

Cuadro 7-16/J.192 – Directrices de diseño del sistema del cliente hora del día

Número	Directrices
ToD 1	Ofrece un mecanismo mediante el cual el PS puede lograr la sincronización de tiempo con la red de la cabecera.

7.5.3 Descripción del sistema de la función cliente hora del día

El elemento de servicios de portal utiliza un cliente hora del día conforme a [RFC 868], a fin de lograr la sincronización de tiempo con un servidor de tiempo en la red de datos del operador de cable. La sincronización de tiempo es esencial para las funciones de seguridad del PS así como para la mensajería de eventos.

Cuando el cliente DHCP del CDC solicita una dirección IP – del servidor DHCP de la red de datos del operador de cable – para la interfaz WAN-Man, el cliente DHCP recibirá la dirección IP del servidor de tiempo de la red de datos del operador de cable en la opción 4 de DHCP.

Una vez que la pila de protocolos de IP de WAN-Man comienza a utilizar la dirección IP recibida del servidor DHCP de la red de datos del operador de cable, el PS debería enviar una consulta de tiempo conforme a [RFC 868] al servidor de tiempo. Si éste ofrece una respuesta válida, el PS utiliza la hora UTC adquirida del servidor de tiempo y un desplazamiento horario para establecer la hora del día actual. El desplazamiento horario proporciona el ajuste a partir de la UTC de la zona horaria en la que reside el PS.

Una fuente de información del desplazamiento horario es el servidor DHCP, que puede incluir la información en la opción 2 del DHCP (opción de desplazamiento horario) de los mensajes DHCP OFFER y DHCP ACK. Alternativamente, el operador de cable puede configurar el PS con un desplazamiento horario escribiendo en el objeto MIB [véase E.2] cabhCdpSnmpSetTimeOffset. Otro objeto MIB CDP, cabhCdpTimeOffsetSelection, permite que el operador de cable configure el PS para utilizar el desplazamiento horario proporcionado en la opción 2 del DHCP o bien en cabhCdpSnmpSetTimeOffset. Otro posible ajuste de desplazamiento horario es el correspondiente al horario de ahorro de energía (horario de verano) en las zonas donde éste sea aplicable. El objeto MIB CDP cabhCdpDaylightSavingTimeEnable permite al operador de cable configurar el PS y añadir una hora al desplazamiento horario para ajustarse al horario de ahorro de energía. Para más información, véase [véase E.2].

Una vez que el PS adquiere la hora UTC del servidor de tiempo, así como el desplazamiento horario adecuado (determinado por el valor de cabhCdpTimeOffsetSelection), los combina, aplica el horario de ahorro de energía cuando proceda (si cabhCdpDaylightSavingTimeEnable se fija como

enabled(1)), actualiza el valor como valor actual en el objeto MIB IPCable2Home cabhPsDevDateTime, y comienza a utilizar esta hora del día para las indicaciones de tiempo en los mensajes de eventos y para las funciones de seguridad.

7.5.4 Requisitos de la función cliente hora del día

El elemento de servicios de portal DEBE implementar un cliente hora del día.

El cliente hora del día de los servicios de portal DEBE cumplir con el protocolo de hora del día [RFC 868] y utilizar únicamente el protocolo UDP.

Después de un reinicio, y antes de que el PS se sincronice con un servidor de hora del día (ToD), el elemento de servicios de portal DEBE inicializar su tiempo a 00:00.0 (medianoche) GMT, 1 de enero de 1970.

Si el PS recibe la opción 4 de DHCP (opción de servidor de tiempo) en el mensaje ACK DHCP, DEBE almacenar la dirección IP del servidor de tiempo del que el PS aceptó una respuesta, como el valor de cabhPsDevTimeServerAddr.

Un PS integrado DEBE utilizar la hora del día válida adquirida más recientemente del servidor ToD para el reloj de hora del día del sistema, aunque ello signifique sustituir la hora del sistema adquirida por el CM o la hora del sistema originalmente inicializada a la hora de referencia (00:00.0 (medianoche) GMT, del 1 de enero de 1970).

Si el valor de cabhPsDevTodSyncStatus es true(1), es decir, si la hora local ya se ha establecido, no es necesario que el cliente hora del día genere una petición de ToD.

El PS DEBE enviar y recibir mensajes ToD solo a través de su interfaz WAN-Man.

El PS DEBE utilizar el valor de cabhPsDevDateTime para cualquier función que demande la hora del día, y que necesita sólo una precisión al segundo más próximo.

El proceso de adquisición de la hora del día de IPCable2Home consta de dos fases: la fase de intento de sincronización inicial de la hora del día (intento inicial) y la fase de reintento de sincronización de la hora del día (reintento). Si el PS sincroniza con éxito la hora del día con el servidor hora del día (ToD) durante la fase de intento inicial, no realiza la fase de reintento. Cuando el PS recibe un mensaje DHCP ACK, y el valor de cabhPsDevTodSyncStatus es false(2) (falso), entra en la fase de intento inicial para intentar la sincronización con un servidor ToD. En 7.5.4.1 se describe el comportamiento del PS durante el intento inicial. La cláusula 7.5.4.2 describe el comportamiento requerido del PS si éste ha de iniciar la fase de reintento de la hora del día.

7.5.4.1 Requisitos del intento de sincronización inicial de la hora del día

Si el PS funciona en el modo de configuración DHCP o en el modo de configuración SNMP (cabhPsDevProvMode = dhcpmode(1) o snmpmode(2)), DEBE intentar la sincronización con un servidor de hora del día cuya dirección se haya transferido al PS en la opción 4 del DHCP del mensaje DHCP ACK, de conformidad con [RFC 868]. Cuando un PS funciona en el modo CableHome aletargado no se le exige que intente la sincronización con un servidor de hora del día.

Si el PS no tiene éxito en la sincronización con un servidor de hora del día (ToD) en su primer intento, DEBE intentar la sincronización con el siguiente servidor ToD en el orden enumerado en la opción 4 del DHCP, hasta que consiga sincronizarse con un servidor, o hasta que realice intentos infructuosos con cada uno de los servidores ToD enumerados. El PS DEBE notificar el evento adecuado (véase el cuadro B.1) para cada intento infructuoso de sincronización con un servidor de hora del día. Un intento de sincronización con un servidor de hora del día es un intento individual de acceso tal como se describe en [RFC 868], iniciado por el PS, sobre el puerto 37 de un servidor de hora del día. Un intento de sincronización infructuoso con un servidor de hora del día es un intento como consecuencia del cual el PS NO recibe información horaria válida del servidor de hora

del día, o bien, cuando como consecuencia de un intento de resolución de la dirección (IP) de red del servidor de hora del día, el PS no consigue adquirir dicha dirección de red del servidor.

Si el PS consigue sincronizar con éxito con un servidor hora del día, DEBE hacer lo siguiente:

- fijar el valor de cabhPsDevTodSyncStatus en true(1);
- fijar como valor de cabhCdpServerTimeOffset el valor de la opción 2 del DHCP (desplazamiento horario) del mensaje DHCP ACK si el valor de cabhCdpTimeOffsetSelection es useDhcpOption2(1), O el valor cabhCdpSnmpSetTimeOffset si el valor de cabhCdpTimeOffsetSection es useSnmpSetOffet(2);
- fijar como valor de cabhPsDevDateTime la hora UTC adquirida del servidor de tiempo, más el desplazamiento horario de la opción 2 del DHCP incluida en el mensaje DHCP ACK, O del valor de cabhCdpSnmpSetTimeOffset, de acuerdo con el valor de cabhCdpTimeOffsetSelection más una hora para el ajuste al horario de ahorro de energía durante el periodo correspondiente si el valor de cabhCdpDaylightSavingTimeEnable es enabled(1);
- fijar como valor de cabhPsDevTimeServerAddr la dirección IP del servidor de hora del día con el que el PS ha sincronizado su hora;
- si la función CDS del PS dispone de licencias de dirección LAN IP, actualizar cabhCdpLanAddrCreateTime con el valor de cabhPsDevDateTime y fijar que el valor de cabhCdpLanAddrExpire sea cabhCdpLanAddrCreateTime, más el valor de cabhCdpServerLeaseTime, para cada licencia activa;
- continuar el proceso de configuración definido en la cláusula 13.

Si un PS integrado que funcione en el modo de configuración DHCP no consigue sincronizar con éxito con ninguno de los servidores de hora del día enumerados en la opción 4 de DHCP del mensaje DHCP ACK, después de haberlo intentado con cada uno de ellos, DEBE intentar adquirir la hora del sistema del módem de cable. Un PS integrado que funcione en el modo de configuración SNMP no tiene que intentar la adquisición de la hora del sistema del módem de cable.

Si un PS integrado que funcione en el modo de configuración DHCP no consigue sincronizar con éxito con ninguno de los servidores de hora del día en su primer intento con cada uno de ellos Y tiene éxito en la adquisición de la hora del sistema del módem de cable, DEBE hacer lo siguiente:

- fijar el valor de cabhPsDevTodSyncStatus en false(2);
- fijar como valor de cabhPsDevDateTime la hora del sistema de módem de cable;
- si la función CDS del PS integrado dispone de licencias de direcciones LAN IP, se actualiza cabhCdpLanAddrCreateTime con el valor de cabhPsDevDateTime (hora del módem de cable) y se fija que el valor de cabhCdpLanAddrExpire sea cabhCdpLanAddrCreateTime, más el valor decabhCdpServerLeaseTime, para cada licencia activa;
- iniciar el proceso de reintento de sincronización de la hora del día definido en 7.5.4.2 Y continuar el proceso de configuración descrito en el cláusula 13.

Un PS integrado que funcione en el modo de configuración DHCP que no consiga sincronizarse con éxito con ninguno de los servidores de hora del día en su primer intento con cada uno de ellos y tampoco tenga éxito en la adquisición de la hora del sistema del módem de cable, DEBE hacer lo siguiente:

- fijar el valor de cabhPsDevTodSyncStatus en false(2);
- fijar como valor de cabhPsDevDateTime la hora de referencia (00:00.0 (medianoche) GMT, del 1 de enero de 1970);

- si su función CDS dispone de licencias de dirección LAN IP, actualizar cabhCdpLanAddrCreateTime con el valor de cabhPsDevDateTime (hora de referencia) y fijar que el valor de cabhCdpLanAddrExpire sea cabhCdpLanAddrCreateTime más el valor de cabhCdpServerLeaseTime, para cada licencia activa;
- iniciar el proceso de reintento de sincronización de la hora del día definido en 7.5.4.2 Y continuar con el proceso de configuración descrito en el cláusula 13;
- notificar el evento adecuado (véase el cuadro B.1) por cada intento infructuoso de sincronización con el servidor hora del día.

Un PS autónomo que funcione en el modo de configuración DHCP que no consiga sincronizar con éxito con ninguno de los servidores de hora del día en su primer intento con cada uno de ellos, DEBE hacer lo siguiente:

- fijar el valor de cabhPsDevTodSyncStatus en false(2);
- fijar como valor de cabhPsDevDateTime la hora de referencia (00:00.0 (medianoche) GMT, del 1 de enero de 1970);
- si su función CDS dispone de licencias de dirección LAN IP, actualizar cabhCdpLanAddrCreateTime con el valor de cabhPsDevDateTime (hora de referencia) y fijar que el valor de la hora cabhCdpLanAddrExpire sea cabhCdpLanAddrCreateTime más el valor de cabhCdpServerLeaseTime, para cada licencia activa;
- iniciar el proceso de reintento de sincronización de la hora del día definido en 7.5.4.2 Y continuar con el proceso de configuración descrito en el cláusula 13;
- notificar el evento adecuado (véase el cuadro B.1) por cada intento infructuoso de sincronización con el servidor hora del día.

Un PS que funcione en el modo de configuración SNMP que no consiga sincronizar con éxito con ninguno de los servidores de hora del día enumerados en la opción 4 del mensaje DHCP ACK en el primer intento con cada uno de ellos, DEBE iniciar el proceso de reintento de sincronización de la hora del día definido en la cláusula 7.5.4.2. Un PS que funcione en el modo de configuración SNMP que no consiga sincronizar con éxito con ninguno de los servidores de hora del día NO DEBE continuar el proceso de configuración definido en la cláusula 13. El requisito de tener que notificar un evento por cada intento de sincronización infructuoso con un servidor hora del día se aplica al PS que funcione en el modo de configuración SNMP.

7.5.4.2 Requisitos del reintento de sincronización de la hora del día

Un PS que funcione en el modo de configuración DHCP que no consiga sincronizar con éxito con ninguno de los servidores de hora del día enumerados en la opción 4 del mensaje DHCP ACK y para el que cabhPsDevTodSyncStatus = false(2), DEBE continuar intentándolo hasta que consiga tener éxito y notificar el evento adecuado (véase el cuadro B.1) por cada intento infructuoso.

Mientras que sea cabhPsDevTodSyncStatus = false(2), un PS que funcione en el modo de configuración SNMP DEBE continuar intentando la sincronización con los servidores de hora del día enumerados en la opción 4 del mensaje DHCP ACK, hasta un total de seis intentos (el intento inicial más cinco reintentos) e notificar el evento adecuado (véase el cuadro B.1) por cada intento infructuoso.

El cliente hora del día del PS NO DEBE exceder más de 3 peticiones de ToD por cada servidor de hora del día en un periodo de 5 minutos. El PS que intenta sincronizar con un servidor ToD DEBE, como mínimo, emitir una petición de ToD por cada periodo de 5 minutos.

Un PS que funcione en el modo de configuración SNMP y que no se sincronice con ninguno de los servidores de hora del día después de intentarlo seis veces con cada servidor ToD enumerado en la opción 4 del mensaje DHCP ACK, DEBE hacer lo siguiente:

- fijar el valor de cabhPsDevTodSyncStatus = false(2);

- realizar el registro histórico del ID de evento 68000403 (véase el anexo B, cuadro B.1) de conformidad con la prioridad configurada para el evento y el siguiente procedimiento definido en 6.3.3.2 Función de informes de eventos del CMP;
- reiniciar el proceso de provisión, enviando inicialmente un mensaje DHCP DISCOVER;
- notificar el evento adecuado (véase el cuadro B.1) para cada intento no exitoso de sincronización con el servidor de la hora del día.

7.6 Función del BP – Cliente DHCP

7.6.1 Objetivos de la función del cliente DHCP del BP

El objetivo de la función del cliente DHCP del BP es obtener una licencia de dirección IP y parámetros de configuración para el BP desde el servidor DHCP del sistema.

7.6.2 Directrices de diseño del sistema de la función de cliente DHCP del BP

Las directrices relacionadas en el cuadro 7-17 orientan la especificación de la función de cliente DHCP del BP.

Cuadro 7-17/J.192 – Directrices de diseño del sistema relativo a la función de cliente DHCP del BP

Número	Directrices
BP DHC 1	Ofrece un medio con el cual el BP puede obtener una licencia de dirección de red e información de configuración.

7.6.3 Descripción del sistema relativa a la función de cliente DHCP del BP

La función de cliente DHCP del BP es la encargada de obtener una licencia de dirección IP del servidor DHCP del sistema. El servidor podría ser la función CDS del subelemento CDP del PS o bien un servidor DHCP en la red de datos del operador de cable, dependiendo de cómo se configure el modo de tratamiento de paquetes del PS. La función de cliente DHCP del BP también obtiene información de configuración transferida en los campos de opción de DHCP del servidor DHCP del sistema.

7.6.4 Requisitos de la función de cliente DHCP del BP

El BP DEBE implementar una función de cliente DHCP conforme a los requisitos de cliente de [RFC 2131].

Cuando se efectúa una reinicialización el BP DEBE emitir un mensaje de difusión DISCOVER DHCP para obtener una licencia de dirección IP.

El BP DEBE soportar las opciones y subopciones de DHCP indicadas como obligatorias (M) en el cuadro 7-18.

El BP DEBE incluir los siguientes códigos de opción DHCP, en cada mensaje DISCOVER DHCP y REQUEST DHCP que envía:

- código 55 de opción DHCP, relación de petición de parámetros;
- código 60 de opción DHCP, identificador de clase de fabricante, con la cadena "CableHome1.1BP" (sin espacios y sin comillas);
- código 255 de opción DHCP, Fin.

Cuadro 7-18/J.192 – Opciones de DHCP necesarias para el cliente DHCP del BP

Número de opción	Función de la opción	Soporte obligatorio (M) u opcional (O)	Valor de fábrica por defecto
0	Relleno	–	N/A
255	Fin	M	N/A
1	Máscara de subred	M	N/A
2	Desplazamiento de tiempo	O	0
3	Opción de encaminador	M	N/A
6	Servidor de nombres de dominio	M	N/A
7	Servidor de registro histórico	M	N/A
12	Nombre de anfitrión	O	N/A
15	Nombre de dominio	M	Cadena nula
23	Tiempo de vida, por defecto	M	N/A
26	MTU de interfaz	M	N/A
43	Información específica del fabricante	M	Seleccionada por el fabricante
50	Dirección IP solicitada	M	Valor nulo o seleccionado por el fabricante
51	Tiempo de la licencia de la dirección IP	M	N/A
54	Identificador del servidor	M	N/A
55	Lista de peticiones de parámetros	M	N/A
60	Identificador de clase de fabricante	M	"CableHome1.1BP"
61	Identificador de cliente	O	N/A

8 Tratamiento de paquetes y traducción de direcciones

8.1 Introducción/síntesis

8.1.1 Objetivos

Los objetivos fundamentales que controlan las capacidades de tratamiento de paquetes incluyen:

- Ofrecer una funcionalidad de traducción de direcciones de fácil manejo por el cable, que dote al operador de cable de visibilidad y capacidad de gestión de los dispositivos en la vivienda, sin menoscabo de las arquitecturas de encaminamiento orientadas a fuentes basadas en cable.
- Evitar el tráfico superfluo en el cable y en la red doméstica.
- Mantener direcciones IP públicas mundialmente direccionables, así como direcciones de gestión privada en la red de cable.
- Facilitar el encaminamiento de tráfico en la vivienda mediante la asignación de direcciones de red a los dispositivos IP de LAN de modo que puedan residir en la misma subred lógica.

8.1.2 Hipótesis

- Se supone que cuando los servidores de configuración del operador de cable suministran múltiples direcciones IP mundialmente direccionables a los dispositivos del cliente en una vivienda, esas direcciones no residirán necesariamente en la misma subred.

- Se supone que el cambio del proveedor de servicios de Internet ocurrirá en pocas ocasiones, con una frecuencia semejante a la del cambio del operador principal de larga distancia en la vivienda.

8.2 Arquitectura

En esta cláusula se describen los conceptos esenciales de la funcionalidad de tratamiento de paquetes y de traducción de direcciones de IPCable2Home.

8.3 Elemento lógico del PS – Portal de direcciones de IPCable2Home

El portal de direcciones de IPCable2Home (CAP) es un subelemento del elemento lógico de servicios de portal. Sus funciones son el encaminamiento de tráfico entre las redes LAN y WAN, el encaminamiento de tráfico de LAN a LAN y la realización de funciones de traducción de direcciones y de puertos.

8.3.1 Objetivos del CAP

Los objetivos del CAP se relacionan a continuación y en 8.1.1:

- Encaminamiento de los paquetes IP entre dispositivos IP de LAN, y entre éstos y la pasarela por defecto de los servicios de portal en la red WAN.
- Ofrecer la capacidad de traducción de direcciones de red y de puertos (NAPT, *network and port address translation*) para la correspondencia entre una sola dirección IP mundial en la interfaz WAN del PS y una o varias direcciones IP privadas en la red LAN.
- Ofrecer la capacidad de traducción de direcciones de red (NAT) para la correspondencia 1 a 1 entre direcciones IP mundiales en la interfaz WAN del PS y direcciones IP privadas en la red LAN.
- Mantener en LAN el tráfico entre dispositivos IP de LAN y no permitir que éste atraviese WAN.

8.3.2 Directrices de diseño del sistema CAP

Se especifica la funcionalidad del portal de direcciones de IPCable2Home basándose en las directrices del cuadro 8-1.

Cuadro 8-1/J.192 – Directrices de diseño del sistema CAP

Número	Directrices
CAP 1	Los mecanismos de direccionamiento serán controlados por el operador y ofrecerán el conocimiento del operador sobre los dispositivos de IPCable2Home y a la accesibilidad a los mismos.
CAP 2	El direccionamiento no debe afectar de ninguna manera a las arquitecturas actuales de encaminamiento por la red de cable.
CAP 3	Los mecanismos de gestión de tráfico deberán aislar la red de cable del tráfico generado por las comunicaciones par a par en la vivienda.
CAP 4	Las direcciones IP se mantendrán siempre que sea posible (tanto direcciones mundialmente direccionables como las direcciones privadas de gestión de la red por cable).
CAP 5	{texto informativo: El CAP permite que los dispositivos LAN UPnP configuren correspondencias de traducción de direcciones de red, pero en la medida que no entre en conflicto con las políticas del operador.}

8.3.3 Descripción del sistema CAP

La funcionalidad de traducción de direcciones y de tratamiento de paquetes la proporciona la entidad funcional conocida como portal de direccionamiento de IPCable2Home (CAP). El CAP comprende los siguientes elementos de traducción de direcciones y de retransmisión de paquetes:

- traducción de direcciones de IPCable2Home (CAT);
- función de transferencia (Passthrough) de IPCable2Home;
- conmutador de retransmisión selectiva en sentido ascendente (USFS).

La función del CAT ofrece un mecanismo para interconectar los sectores de direcciones de WAN-Data y de LAN-Trans (a través de la traducción de direcciones), como se muestra en la figura 8-1, mientras que la función de transferencia (Passthrough) ofrece un mecanismo para interconectar los sectores de direcciones de WAN-Data y de LAN-Pass (mediante puenteo). La función de CAT es conforme con la traducción de dirección de red (NAT) tradicional de acuerdo con la sección 2 de [RFC 3022]. Como en el caso de la NAT tradicional, existen dos variantes de CAT, conocidas como encaminamiento transparente de la traducción de dirección de red de IPCable2Home (C-NAT) y encaminamiento transparente de la traducción de dirección y de puertos de la red IPCable2Home (C-NAPT). El encaminamiento transparente de C-NAT es la versión conforme a IPCable2Home de la NAT básica, según la sección 2.1 de [RFC 3022] y el encaminamiento transparente de C-NAPT es la versión conforme a IPCable2Home de NAPT según la sección 2.2 de [RFC 3022].

De acuerdo con [RFC 3022], el encaminamiento transparente de C-NAT es "un método mediante el cual se establece una correspondencia entre las direcciones IP de un grupo con las de otro, que es transparente a los usuarios de extremo" y el encaminamiento transparente de C-NAPT "es un método mediante el cual múltiples direcciones de red y sus puertos TCP/UDP (protocolo de control de transmisión/protocolo de datagrama de usuario) se traducen a una sola dirección de red y a sus puertos TCP/UDP". Además, conforme a [RFC 3022], la finalidad de la funcionalidad de C-NAT y de C-NAPT es "ofrecer un mecanismo para conectar un sector con direcciones privadas a un sector externo con direcciones únicas registradas mundialmente".

La función de transferencia de IPCable2Home es un proceso de puenteo especificado por IPCable2Home que interconecta los sectores de direcciones de WAN-Data y de LAN-Pass sin traducir las direcciones.

El conmutador de retransmisión selectiva en sentido ascendente (USFS) define una función en el CAP con la capacidad para limitar el tráfico en la red doméstica de modo que permanezca en dicha red, aun cuando los dispositivos que generen ese tráfico residan en distintas subredes IP lógicas. Particularmente, esta función permite retransmitir el tráfico originado en una dirección IP de uno de los sectores de direcciones LAN, destinado a direcciones IP en uno de los sectores de direcciones LAN, directamente a su destino. Esta funcionalidad de retransmisión directa evita que el tráfico pase por la red HFC, y permite interconectar los sectores de direcciones de LAN-Trans y de LAN-Pass.

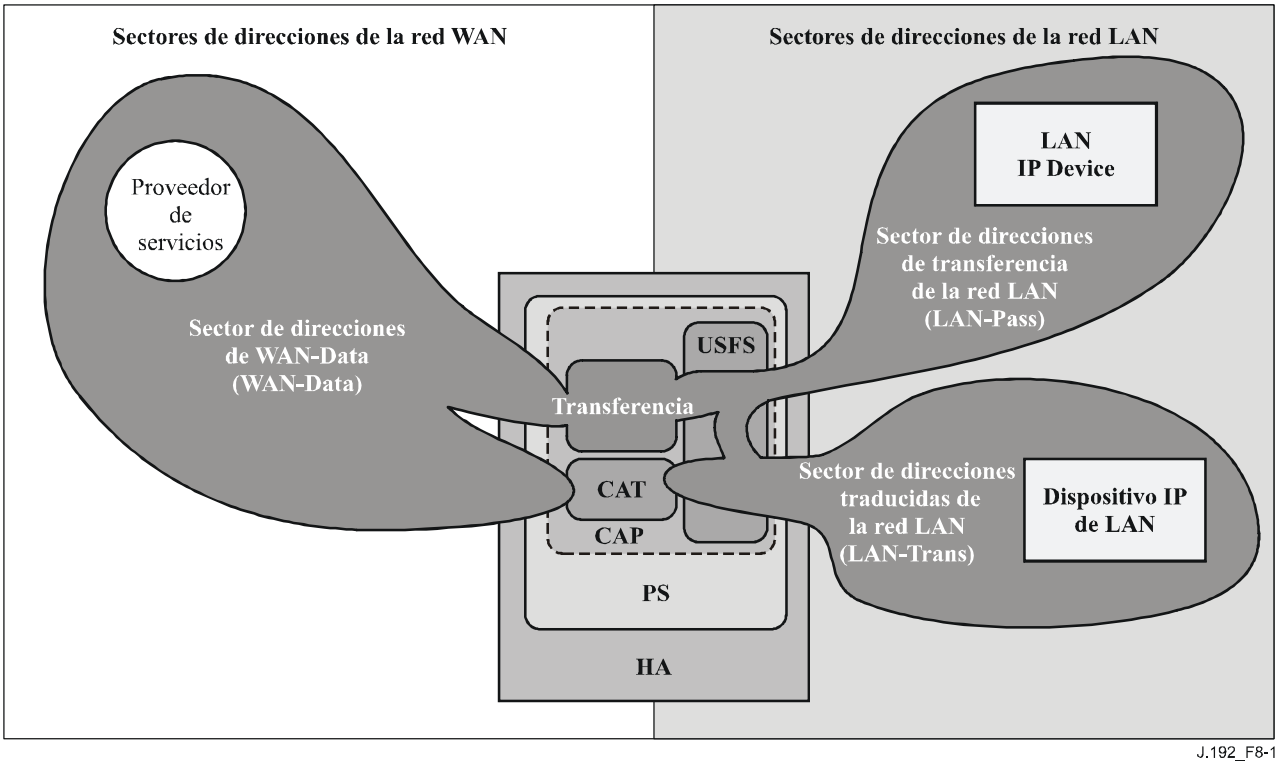


Figura 8-1/J.192 – Funciones del portal de direcciones de IPCable2Home (CAP)

En esta Recomendación, los términos vinculación de direcciones, desvinculación de direcciones, traducción de direcciones y sesión se utilizan tal y como se definen en [RFC 2663]. Además, IPCable2Home define el término correspondencia como la información necesaria para realizar el encaminamiento transparente de C-NAT y de C-NAPT.

En particular, una correspondencia de C-NAT se define como una tupla de la forma (dirección IP de WAN-Data, dirección IP de LAN-Trans) que establece una correspondencia de uno a uno entre las direcciones de WAN-Data y de LAN-Trans. De manera similar, una correspondencia de C-NAPT se define como una tupla de la forma (dirección IP de WAN-Data y puerto TCP/UDP, dirección IP de LAN-Trans y puerto TCP/UDP) que establece una correspondencia de uno a varios entre una sola dirección de WAN-Data y múltiples direcciones de LAN-Trans. En el caso de tráfico ICMP (como ping), se utiliza un identificador de ICMP en lugar del número de puerto TCP/UDP.

El tráfico de LAN a WAN se define como los paquetes originados por los dispositivos IP de LAN y destinados a dispositivos en el lado de la red WAN del PS. El tráfico WAN a LAN se define como los paquetes originados por los anfitriones de la red WAN y destinados a dispositivos IP de LAN. El tráfico LAN a LAN se define como los paquetes originados por dispositivos IP de LAN y destinados a dispositivos IP de LAN en la misma subred o en una distinta.

8.3.3.1 Modos de tratamiento de paquetes

Existe la posibilidad de configurar el elemento de servicios de portal a través del objeto de la MIB cabhCapPrimaryMode, de modo que funcione en uno de los tres modos de tratamiento de paquetes primarios cuando maneja tráfico de LAN a WAN y de WAN a LAN: modo de transferencia, modo de encaminamiento transparente de C-NAT y modo de encaminamiento transparente de C-NAPT. Además, los modos primarios C-NAT o C-NAPT también pueden funcionar en un modo híbrido que se describe más adelante.

En el modo de transferencia, el CAP actúa como un puente transparente [ISO/CEI 10038] entre el sector de WAN-Data y el sector de LAN-Pass. En el modo de transferencia, las decisiones de

retransmisión se determinan en primer lugar en la capa 2 de OSI (capa de enlace de datos). En este modo, el CAP no realiza ninguna función de encaminamiento transparente de C-NAT o de C-NAPT. El PS que puentea tráfico para dispositivos IP LAN-Pass debe poder transferir todas las tramas de la capa 2 de la OSI que deba transferir un módem de cable conforme con DOCSIS, incluyendo tramas SNAP [ISO/CEI 8802-2] y DIX Ethernet Versión 2.0.

El CAP soporta la retransmisión de capa 3 de OSI (capa de red) en los modos de encaminamiento transparente de C-NAT y de C-NAPT, que se describen más adelante.

En el modo de C-NAT, el elemento PS (CDC) obtiene una o más direcciones de IP que se utilizan para el tráfico de WAN-Data durante el proceso de arranque del PS. Después de su obtención, a través de DHCP, estas direcciones de IP se utilizan como la porción de la dirección IP de WAN-Data de las tuplas de correspondencia de C-NAT creadas dinámicamente. Estas direcciones IP de WAN conforman un grupo de direcciones disponible para las correspondencias de C-NAT creadas dinámicamente. Si existe una dirección IP disponible en el grupo de direcciones IP de WAN-Data, el CAP crea una correspondencia de C-NAT dinámica en cuanto detecta tráfico IP de LAN a WAN que no tiene una correspondencia disponible. Si no existe una dirección IP disponible en el grupo de direcciones IP de WAN-Data, la correspondencia de C-NAT dinámica no podrá crearse, y el tráfico se descartará, generando un evento (véase el anexo B).

La parte de la dirección IP de LAN-Trans de las tuplas de correspondencia de C-NAT creadas dinámicamente la proporciona el grupo de direcciones IP definidas por el operador de cable en la MIB del CDP de IPCable2Home. El CAP introduce la tupla de las direcciones IP de WAN-Data y de LAN-Trans únicas en el cuadro de correspondencias de CAP, junto con otros parámetros que incluyen los números de puerto de las redes WAN y LAN, el método de correspondencia y el protocolo de transporte que se utiliza para la correspondencia. El CAP no traducirá el número de puerto de las correspondencias de C-NAT: los números de puerto de origen y de destino en el encabezamiento de UDP o de TCP no sufrirán ningún cambio. Cuando el PS se encuentra funcionando en el modo de tratamiento de paquetes primario de NAT (cabhCapPrimaryMode = nat(2)), el CAP introducirá el valor 0 en las anotaciones de número de puerto de las redes WAN y LAN en el cuadro de correspondencias de CAP. Además, el CAP introducirá el valor 0 en las anotaciones de los números de puerto de las redes WAN y LAN en el cuadro de correspondencias de CAP relativas a las anotaciones de retransmisión del puerto estático proporcionado en el cuadro de correspondencias de CAP, cuando el PS se encuentra funcionando en el modo de tratamiento de paquetes primario de NAPT (cabhCapPrimaryMode = napt(1)). En el caso de que se introduzca una anotación de retransmisión de puerto estático en el cuadro de correspondencias de CAP para un PS que funciona en el modo de tratamiento de paquetes primario de NAPT, la anotación de número de puerto con un valor 0 servirá para dos fines:

1) indicar al CAP que los números de puerto no se deben traducir, es decir, que los puertos son "comodines"; y

2) para indicar a cualquiera que pretenda leer el cuadro de correspondencias de CAP que la correspondencia del puerto estático es efectivamente una correspondencia de C-NAT, señalando por consecuencia una diferencia entre las anotaciones de retransmisión de puerto estático (correspondencias de C-NAT) (puerto número 0) y las correspondencias de C-NAPT (número de puerto distinto de cero).

   Véase 8.3.3.2, Funcionalidad DMZ del CAP (retransmisión de puerto estático con comodines de puerto), para obtener información más detallada relativa al funcionamiento de la retransmisión de puerto estático del CAP.

Las correspondencias de C-NAT dinámicas del tráfico UDP se suprimen cuando expira un periodo de inactividad (fin de temporización), cabhCapUdpTimeWait. Las correspondencias de C-NAT dinámicas del tráfico TCP se suprimen cuando expira un periodo de inactividad, cabhCapTcpTimeWait, o termina una sesión TCP. Las correspondencias de C-NAT dinámicas del tráfico ICMP se suprimen cuando expira un periodo de inactividad, cabhCapIcmpTimeWait.

Además, es posible que se creen o se supriman correspondencias de C-NAT estáticas cuando el sistema NMS escribe en el cuadro de la MIB cabhCapMappingTable, o suprime información en el mismo.

En el modo de C-NAPT (modo por defecto de fábrica para el sistema) el elemento PS (CDC) obtiene una dirección IP, que se utiliza para el tráfico de WAN-Data. Después de obtener esta dirección IP a través de DHCP, se utiliza como la parte de la dirección IP de WAN-Data de las tuplas de correspondencia de C-NAPT creadas dinámicamente. Si ya se ha obtenido la dirección IP de WAN-Data, se crean correspondencias de C-NAPT dinámicas cuando el CAP detecta tráfico IP de la red LAN a la red WAN que no dispone de una correspondencia. Si la dirección IP de WAN-Data aún no ha sido obtenida (es decir, no tiene una licencia de DHCP activa), no se puede crear la correspondencia de C-NAPT dinámica, y se descarta ese tráfico, generando un evento normal (véase el anexo B).

Las correspondencias de C-NAPT dinámicas del tráfico UDP se suprimen cuando expira un periodo de inactividad, cabhCapUdpTimeWait. Las correspondencias de C-NAPT dinámicas del tráfico TCP se suprimen cuando expira un periodo de inactividad, cabhCapTcpTimeWait, o cuando termina una sesión TCP. Las correspondencias de C-NAPT dinámicas del tráfico ICMP se suprimen cuando expira un periodo de inactividad, cabhCapIcmpTimeWait. Además, es posible que se creen o se supriman correspondencias de C-NAPT estáticas cuando el sistema NMS escribe en el cuadro de la MIB cabhCapMappingTable, o cuando suprime información del mismo.

En la figura 8-2 se muestra un proceso de correspondencia de C-NAPT dinámica convencional con un paquete TCP. En este ejemplo, el PS se configura del modo que funcione en el modo NAPT y se supone que ya se ha obtenido una dirección IP de WAN y que el dispositivo IP de LAN ya ha conseguido una dirección IP del sector LAN-Trans.

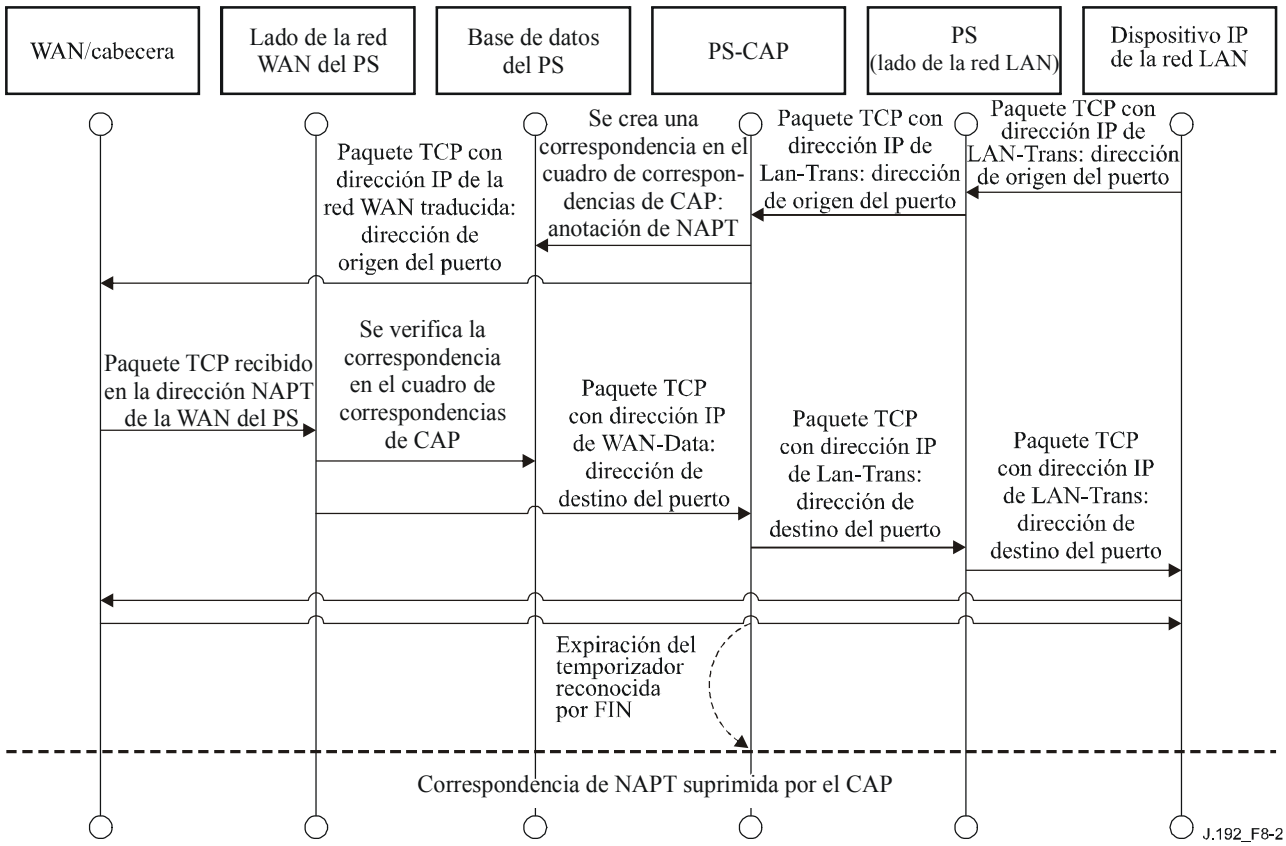


Figura 8-2/J.192 – Diagrama de la secuencia de configuración del PS (cuadro de correspondencias de CAP – NAPT)

El PS puede funcionar también en un modo híbrido de puenteo y encaminamiento. En tal caso, el NMS establece el modo primario en encaminamiento transparente C-NAT o C-NAPT, y el NMS escribe en el cuadro transferencia (cabhCapPassthroughTable) una dirección MAC o varias pertenecientes a dispositivos IP de LAN cuyo tráfico vaya a ser puenteo. En dicho modo híbrido, el PS examina las direcciones MAC de las tramas recibidas para determinar si debe puentear las tramas en modo transparente o debe ejecutar funciones de encaminamiento transparente C-NAT o C-NAPT en la capa IP. Cuando se trate de tráfico LAN-a-WAN, el PS examinará la dirección MAC de origen, y si ésta existiese en el cabhCapPassthroughTable, la trama se puentearía transparentemente a la interfaz WAN-Data. Cuando se trata de tráfico WAN-a-LAN el PS examina la dirección MAC de destino y si ésta existiera en cabhCapPassthroughTable, la trama se puentearía transparentemente a la interfaz LAN adecuada. Si la dirección MAC no existe en cabhCapPassthroughTable, el paquete lo procesan las funciones de capa superior, y entre ellas la función de encaminamiento transparente C-NAT/C-NAPT.

Se supone que cuando el PS se encuentra en el modo de encaminamiento (C-NAT/C-NAPT), procesará tráfico de difusión conforme a [RFC 919], [RFC 922], [RFC 1812] y [RFC 2644]. Además, se supone que cuando el PS está en el modo de transferencia, ese tráfico de difusión se puenteará a todas las interfaces.

Cuando el PS se encuentra en el modo de puenteo/encaminamiento híbrido, y recibe tráfico de difusión originado por un dispositivo en el cuadro de transferencia, se prevé que el PS puenteará el tráfico de difusión a todas las interfaces. Cuando el PS se encuentra en el modo de puenteo/encaminamiento híbrido, y recibe tráfico de difusión por cualquier interfaz WAN, se prevé que el PS puenteará ese tráfico de difusión a todas las interfaces LAN.

Obsérvese que la funcionalidad de USFS (véase 8.3.3.4) se aplica en cada uno de los tres modos de tratamiento de paquetes primarios, e independientemente de si se encuentra en uso o no el modo híbrido. Las decisiones de retransmisión de USFS tendrán precedencia sobre otras decisiones de retransmisión que pudieran reenviar tráfico potencialmente desde la red LAN a la red WAN.

8.3.3.2 Funcionalidad DMZ del CAP (retransmisión de puerto estático con comodines de puerto)

Cuando el PS se configura para funcionar en el modo de tratamiento de paquetes primario de C-NAPT y se crea estáticamente una correspondencia de C-NAPT con números de puertos WAN y LAN fijados a cero (es decir, cuando se ha creado una anotación DMZ), el CAP tratará el tráfico entrante de un modo especial, retransmitiendo todo el tráfico de WAN a LAN no asociado con una sesión C-NAPT existente, o una correspondencia estática de C-NAPT existente, a la dirección IP de LAN (dirección IP de DMZ) especificada en este tipo especial de correspondencia de C-NAPT (anotación de DMZ).

El CAP procesará los paquetes de la siguiente manera:

1) Verifica todos los paquetes entrantes de WAN a LAN para examinar si están asociados con una sesión existente especificada por una correspondencia dinámica de C-NAPT. Si éste es el caso, el paquete se traduce como se especifica y se retransmite.

2) Si no existe la asociación antes referida el CAP verifica si hay una correspondencia de C-NAPT estática asociada con el paquete. Si éste es el caso, el paquete se traduce como se especifica y se retransmite.

3) De no tratarse del caso indicado en el punto anterior, el CAP verifica si hay una correspondencia de C-NAPT estática para esta dirección IP de WAN con el número de puerto fijado a 0. Si es así, el CAP traduce la dirección IP a la dirección IP de LAN especificada en esta correspondencia estática de C-NAPT especial. Obsérvese que, en este caso, la C-NAPT no traduce el puerto. Después de la traducción de la dirección, se retransmite el paquete.

NOTA – Si ninguno de los casos anteriores es verdadero, el paquete se descarta.

Cuando se cree una anotación de DMZ en el CAP para una dirección IP de LAN asignada dinámicamente por el PS (CDS), éste ha de crear una reserva de licencia de dirección IP para dicha dirección. Ello garantiza que no se modifica la dirección IP del dispositivo LAN establecida para la funcionalidad DMZ cuando se renueva la licencia. El PS puede obtener la dirección IP del DMZ en cabhCdpLanAddrTable. Si en dicho cuadro existe una anotación para la que el valor de cabhCdpLanAddrMethod es igual a dynamicActive(4) o a dynamicInactive(3), el PS ha de sustituirla por una que represente una reserva de licencia de dirección IP, es decir, una cuyo valor de cabhCdpLanAddrMethod sea a psReservationActive(6) o psReservationInactive(5), respectivamente. Si no existe una anotación que se corresponda con la dirección IP del DMZ en cabhCdpLanAddrTable, el PS no tiene que crear una reserva de licencia de dirección IP para dicha dirección IP. En este caso, es posible que la dirección IP del DMZ se asigne de forma estática al dispositivo IP de la LAN.

Cuando para una dirección IP de la LAN (anfitrión DMZ), se suprime una anotación DMZ de cabhCapMappingTable, el PS ha de eliminar la correspondiente reserva de licencia de dirección IP que había creado internamente (identificada mediante cabhCdpLanAddrMethod=psReservationActive(6)) del cabhCdpLanAddrTable en la medida en que el docsDevFilterIpTable o el cabhSec2FwLocalFilterIpTable no tenga una anotación regla de filtro de la barrera contra fuegos que lo requiera (véase 11.6.4.3.3, Conjunto de reglas de fábrica por defecto).

8.3.3.3 Soporte de red privada virtual (RPV) en el CAP

El PS debe implementar una característica de *transferencia de RPV* que permita que los clientes de RPV basados en IPSec [RFC 2401] intercambien claves utilizando el protocolo de intercambio de claves de Internet [RFC 2409]. Se soporta un solo cliente RPV en la vivienda a la vez y se supone que ese cliente satisface las siguientes condiciones:

- el dispositivo IP de LAN se encuentra en el sector de LAN-Trans, es decir, tiene una dirección IP de LAN-Trans;
- el dispositivo IP de LAN utiliza IPSec como protocolo de RPV;
- el dispositivo IP de LAN utiliza el intercambio de claves de Internet para intercambiar de manera dinámica claves de criptación con el servidor de la RPV.

Esta Recomendación no limita el número de clientes de RPV en el sector de LAN-Pass (es decir, los dispositivos IP de LAN cuyas direcciones MAC se encuentren en el cuadro de transferencia del PS) que pueden acceder simultáneamente a los servidores de la RPV fuera de la vivienda.

Para que un cliente de la RPV pueda funcionar adecuadamente, debe estar activo un fichero de política de la barrera contra fuegos en el PS que permita abrir los puertos adecuados para el tráfico entrante (WAN-a-LAN), particularmente el puerto 500, para el tráfico de intercambio de claves de Internet (IKE, *Internet key exchange*).

Cuando se intercambian las claves de manera dinámica utilizando el intercambio de claves de Internet (IKE) [RFC 2406] antes de iniciar una sesión de IPSec, el CAP traducirá las direcciones de red del modo usual y asociará adicionalmente el puerto 500 como un puerto entrante para la dirección IP privada (LAN-Trans) del dispositivo que inició la conexión de RPV. Esto garantizará que los mensajes IKE entrantes serán retransmitidos adecuadamente al cliente de la RPV. Las sesiones de IPsec se definen en el CAP mediante el puerto utilizado para el tráfico entrante y saliente, el puerto utilizado para el intercambio de claves, la dirección del servidor de la RPV y la dirección del cliente de la RPV.

Aun cuando la barrera contra fuegos haya abierto el puerto 500, el tráfico entrante por ese puerto sólo será retransmitido por el CAP después de que un cliente en el sector de direcciones de LAN-Trans haya iniciado una sesión de IPSec.

Si un segundo cliente de la RPV en la vivienda trata de iniciar una sesión de IPsec con un servidor de la RPV distinto el CAP cambiará la posición de los puertos utilizados en la dirección IP de WAN-Data para el intercambio de tráfico y de claves y traducirá esos puertos a los puertos normales de la dirección IP de cliente de la RPV en el sector de la LAN-Trans. Asimismo, se podrán soportar clientes adicionales de la RPV. No obstante, el CAP no soporta más de un cliente de la RPV en la vivienda que se conecte al mismo servidor de la RPV.

IPsec tiene tres modos que pueden utilizarse para las RPV. El PS debe soportar el modo de tunelización de cabida útil de seguridad encapsulada [RFC 2406]. No es necesario el soporte del modo de transporte de cabida útil de seguridad encapsulada [RFC 2406], ni el modo de encabezamiento de autenticación IP [RFC 2402].

8.3.3.4 Resumen de la conmutación de retransmisión selectiva en sentido ascendente

En ciertos casos, un dispositivo IP de LAN del sector de direcciones LAN-Pass residirá en una subred IP lógica distinta que los demás dispositivos IP de LAN conectados al mismo elemento PS. Es importante evitar que el tráfico entre dichos dispositivos IP de LAN atraviese la red HFC. La conmutación de retransmisión selectiva en sentido ascendente (USFS) proporciona la función que evita el antedicho tráfico HFC no deseado.

Más concretamente, el USFS encamina el tráfico con origen y destino en la red doméstica, directamente a su destino. El tráfico con origen en dispositivos IP de LAN con destino a direcciones IP exteriores al sector de direcciones de la LAN atraviesa la funcionalidad de puenteo y encaminamiento CAP sin perturbaciones.

La funcionalidad USFS utiliza el cuadro de traducción de direcciones IP del elemento PS (definido en [RFC 2011]). Este cuadro, el ipNetToMediaTable [RFC 2011], contiene una lista de direcciones MAC, subdirecciones IP correspondientes, y números de índice de interfaz PS de las interfaces físicas a las que están asociadas estas direcciones. El USFS consultará este cuadro antes de adoptar decisiones sobre el encaminamiento del flujo de tráfico LAN-a-WAN. Para rellenar el ipNetToMediaTable el PS obtiene las direcciones MAC e IP y sus asociaciones. Para cada interfaz física asociada, el PS obtiene todas las direcciones IP LAN-Trans y LAN-Pass junto con las vinculaciones MAC asociadas pudiendo obtenerse éstas de diferentes maneras. Entre los métodos de obtención de direcciones IP/MAC específicos del fabricante se encuentran los siguientes: espionaje ARP, supervisión de tráfico y consulta de las anotaciones del CDP. Las anotaciones se suprimen del ipNetToMediaTable una vez transcurrido un periodo razonable de inactividad.

El USFS inspecciona todo el tráfico IP recibido de las interfaces PS LAN. Si se comprueba (en el ipNetToMediaTable) que la dirección IP de destino reside en la interfaz PS LAN, la dirección de destino de enlace de datos de la trama original, que es la dirección de la pasarela por defecto, se modifica a la del dispositivo IP de LAN de destino, y el tráfico se entrega a la funcionalidad de la retransmisión y acceso a los medios de QoS (QFM, *QoS forwarding and media access*) (véase 10.2, Arquitectura de calidad de servicio) en el PS para retransmitirlo a la interfaz LAN del PS adecuada conforme a la prioridad del paquete. Si no se encuentra una dirección IP de destino concordante en el ipNetToMediaTable, el paquete se entrega en su forma original a la función de encaminamiento transparente C-NAT/C-NAPT o la función de puenteo transferencia (dependiendo del modo de tratamiento de paquetes activo).

8.3.3.5 Lista de control de acceso MAC

A fin de ayudar a reducir o suprimir el potencial hurto de servicios y otros accesos no autorizados a los recursos de la LAN del abonado, IPCable2Home permite utilizar una lista de control de acceso. Se trata de una lista con las direcciones hardware de los dispositivos IP de la LAN con los que el PS cursa tráfico. La lista se implementa como un cuadro MIB (cabhPsDevAccessControlTable) y consta de una lista de direcciones físicas. El control administrativo del cuadro de control de acceso lo suministra un objeto MIB escalable, cabhPsDevAccessControlEnable. El control de acceso se habilita por cada tipo de interfaz. Un tipo de interfaz queda habilitado a realizar el control de acceso

fijando el correspondiente bit del objeto cabhPsDevAccessControlEnable. Cuando el bit correspondiente a un tipo de interfaz se fija en (1), el PS cursa tráfico hacia o desde cualquier dispositivo IP de la LAN a través de dicho tipo de interfaz, cuya dirección física o hardware es un elemento del cuadro de control de acceso, pero no cursa tráfico a través de dicho tipo de interfaz hacia o desde un dispositivo IP de la LAN cuya dirección física no sea un elemento del cuadro de control de acceso. Cuando no se fija el bit correspondiente a un tipo de interfaz, el PS no utilizará el cuadro de control de acceso a la hora de determinar si cursa tráfico hacia o desde dispositivos a través de dicho tipo de interfaz. Véase la descripción del cuadro de control de acceso en [E.4].

8.3.3.6 Multidifusión

El CAP soporta tráfico de multidifusión de la red WAN a la red LAN puenteando de manera transparente mensajes IGMP en sentido descendente [RFC 2236] y paquetes de multidifusión por IP en sentido descendente. Además, durante el modo de encaminamiento transparente C-NAT/C-NAPT, el CAP realiza una traducción de direcciones de los mensajes IGMP en sentido ascendente originados por dispositivos IP de LAN que residen en el dominio LAN-Trans. El CAP retransmite el tráfico IGMP originado en la red WAN a la red LAN para facilitar que los anuncios alcancen los dispositivos IP de LAN. Uno de estos dispositivos determinará a qué multidifusión desea incorporarse y enviará un mensaje "join" de multidifusión. A continuación, la fuente de la multidifusión podrá pasar datos al dispositivo IP de LAN. Cuando ya no se desea el servicio de multidifusión, el dispositivo IP de LAN podrá ignorar el servicio y el tren alcanzará su fin de temporización, o bien podrá enviar un mensaje "leave" de IGMP a la cadena para interrumpir la transmisión del tráfico. En la figura 8-3 se presenta un ejemplo detallado de procesos IGMP y multidifusión que pasan a través de un PS.

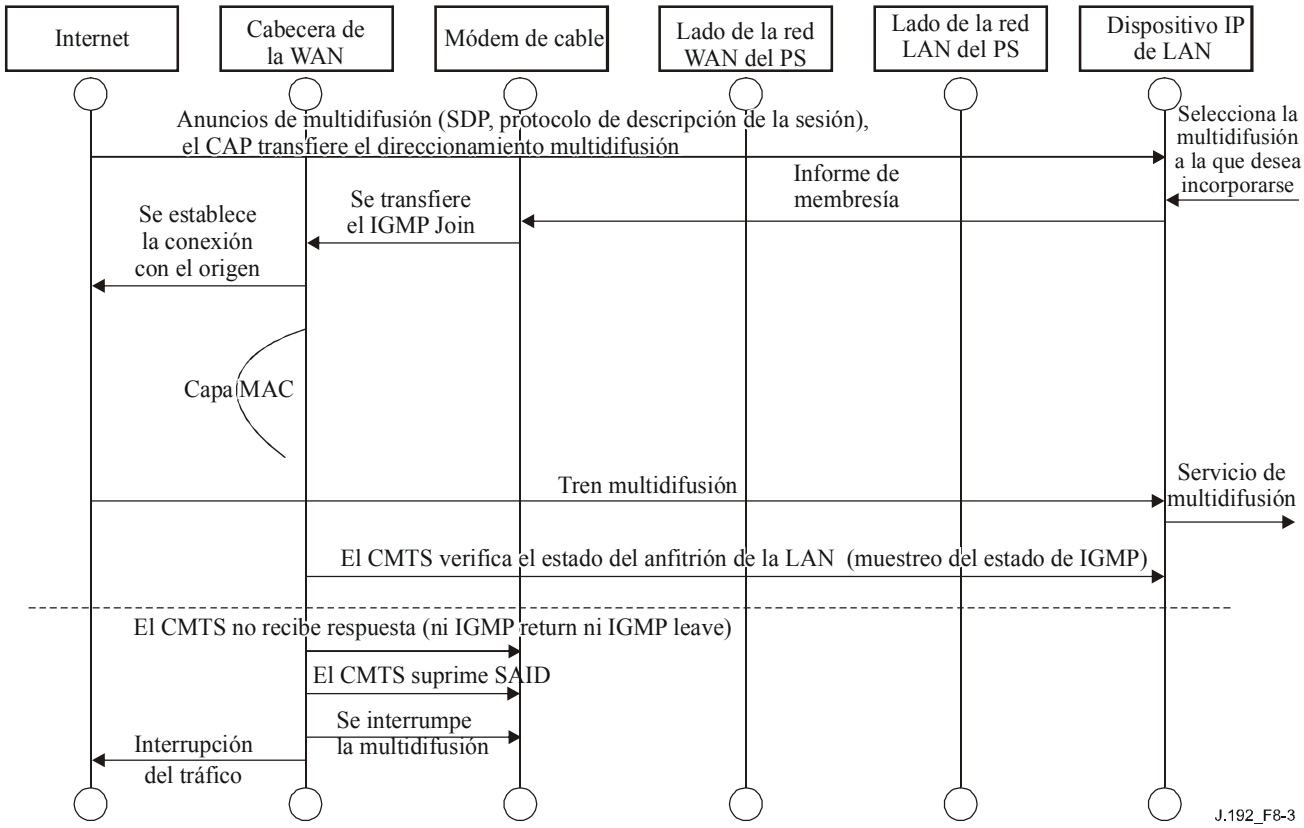


Figura 8-3/J.192 – Multidifusión a través de la secuencia de IGMP

{texto informativo:

8.3.3.7 Configuración del C-NAPT mediante el servicio WANIPConnection UPnP

El PS implementa el servicio WANIPConnection UPnP (UWIC, *UPnP WANIPConnection*) para permitir que las aplicaciones de LAN que sean conformes con UPnP configuren las correspondencias de puertos en el CAP.

El PS declara el servicio WANIPConnection UPnP en la descripción del dispositivo InternetGatewayDevice UPnP. El PS sólo anuncia el servicio WANIPConnection cuando funciona en el modo NAPT.

8.3.3.7.1 Relación entre variables WANIPConnection y objetos cabhCapMappingTable

El PS enumera todas las correspondencias de traducción de direcciones de red en cabhCapMappingTable. Ello incluye las correspondencias creadas dinámicamente por el PS por gestión mediante SNMP, y por dispositivos LAN mediante UPnP. Existen varios objetos en cabhCapMappingTable que tienen una variable de la correspondencia definida en la especificación del servicio InternetGatewayDevice UPnP [UIGD]. En el cuadro 8-2 se muestran las relaciones entre objetos cabhCapMappingTable y variables del servicio WANIPConnection.

Cuadro 8-2/J.192 – Objetos cabhCapMappingTable y variables de servicios WANIPConnection conexas

cabhCapMappingTable	WANIPConnection
cabhCapMappingWanAddr	ExternalIpAddress
cabhCapMappingWanPort	ExternalPort
cabhCapMappingLanAddr	InternalClient
cabhCapMappingLanPort	InternalPort
cabhCapMappingProtocol	PortMappingProtocol
cabhCapMappingCreateTime	N/A
cabhCapMappingLastUpdate	N/A
cabhCapMappingDuration	PortMappingLeaseDuration
cabhCapMappingRowDescription	PortMappingDescription
cabhCapMappingNumPorts	N/A
cabhCapMappingMethod	N/A
cabhCapMappingRemoteHost	RemoteHost
CabhCapMappingEnable	PortMappingEnabled
N/A No disponible	

En la cláusula siguiente se describe cómo utiliza el PS estas variables y objetos en el contexto de acciones del servicio WANIPConnection.

8.3.3.7.2 Análisis de acciones

El PS sólo habilita el servicio WANIPConnection cuando funciona en el modo NAPT. En los restantes modos (es decir, NAT, transferencia o modo inhabilitado) el PS inhabilita el servicio WANIPConnection.

El PS soporta las acciones de servicio WANIPconnection siguientes con el fin de que los dispositivos UPnP creen, modifiquen, supriman y lean correspondencias de puertos: GetNATRSIPStatus, AddPortMapping, DeletePortMapping, GetGenericPortMappingEntry, GetSpecificPortMappingEntry y GetExternalIPAddress.

El PS implementa la acción GetNATRSIPStatus (por cada UWIC) para informar a los puntos de control UPnP solicitantes si la NAPT está habilitada o no. La respuesta del PS a esta acción depende de si el dispositivo solicitante está en el dominio LAN-Trans o LAN-Pass. Para dispositivos en el dominio LAN-Trans, el PS responde que la NAPT está habilitada, y para dispositivos en el dominio LAN-Pass, que está inhabilitada.

Los puntos de control UPnP pueden crear nuevas correspondencias en el PS invocando la acción AddPortMapping. El PS incluye correspondencias creadas mediante esta acción en cabhCapMappingTable, con un valor de cabhCapMappingMethod de UPnP (3). El PS crea una nueva correspondencia cuando las variables ExternalPort y PortMappingProtocol de la acción no concuerdan con un puerto y un protocolo que esté siendo utilizado, tal como se define en UPnP. El PS también crea una nueva correspondencia si las variables de la acción concuerdan con el puerto externo (ExternalPort), el protocolo de correspondencia de puerto (PortMappingProtocol) y el cliente interno (InternalClient) de una correspondencia existente, pero no concuerdan con el anfitrión distante (RemoteHost) de la correspondencia.

Los puntos de control pueden modificar las correspondencias NAPT en el PS mediante la acción AddPortMapping. Tal como se define en UPnP, esta acción especifica una correspondencia ya existente cuando RemoteHost, ExternalPort, PortMappingProtocol e InternalClient concuerdan con la misma. El PS permite que los puntos de control modifiquen correspondencias creadas exclusivamente mediante UPnP. El PS no permite que los puntos de control modifiquen las correspondencias que se crean en el PS mediante SNMP. Cuando el PS recibe un AddPortMapping que concuerda con una anotación que fue creada mediante SNMP, no modifica la anotación pero en respuesta a la acción devuelve su acuerdo (OK).

Los puntos de control pueden invocar la acción DeletePortMapping para suprimir una correspondencia en el PS. Cuando se ejecuta esta acción, el PS suprime una correspondencia si ésta fue creada mediante UPnP. En cualquier otro caso, el PS no suprime la correspondencia y devuelve un error.

Cuando un punto de control invoca la acción GetGenericPortMappingEntry, el PS devuelve correspondencias que el PS creó dinámicamente y correspondencias creadas en el PS mediante SNMP o UPnP. En concreto, el PS devuelve todas las correspondencias que existan en cabhCapMappingTable cuyo valor de cabhCapMappingProtocol sea UDP(3) o TCP(4). En el caso de correspondencias que el PS haya creado dinámicamente o creadas en el PS mediante SNMP, el PS devuelve como RemoteHost una cadena vacía, y un valor 1 (True) para PortMappingEnabled.

Cuando se recibe una acción GetSpecificPortMappingEntry, el PS verifica las anotaciones de cabhCapMappingTable y devuelve la que concuerda con los parámetros de la anotación RemoteHost, ExternalPort y PortMappingProtocol de la acción.

En respuesta a una acción GetExternalIPAddress, el PS devuelve la dirección IP de WAN-Data actual.

}

8.3.3.8 Ejemplos de tratamiento de paquetes de IPCable2Home

Esta cláusula pretende notificar el proceso del tratamiento de paquetes. La figura 8-4 muestra un ejemplo de las posibles etapas de procesamiento de paquetes para el tráfico unidifusión LAN-a-WAN, mientras que la figura 8-5 muestra un ejemplo de las posibles etapas de procesamiento de paquetes para el tráfico unidifusión WAN-a-LAN.

NOTA – Estos ejemplos tienen exclusivamente carácter informativo y no suponen requisitos ni implementación específica alguna.

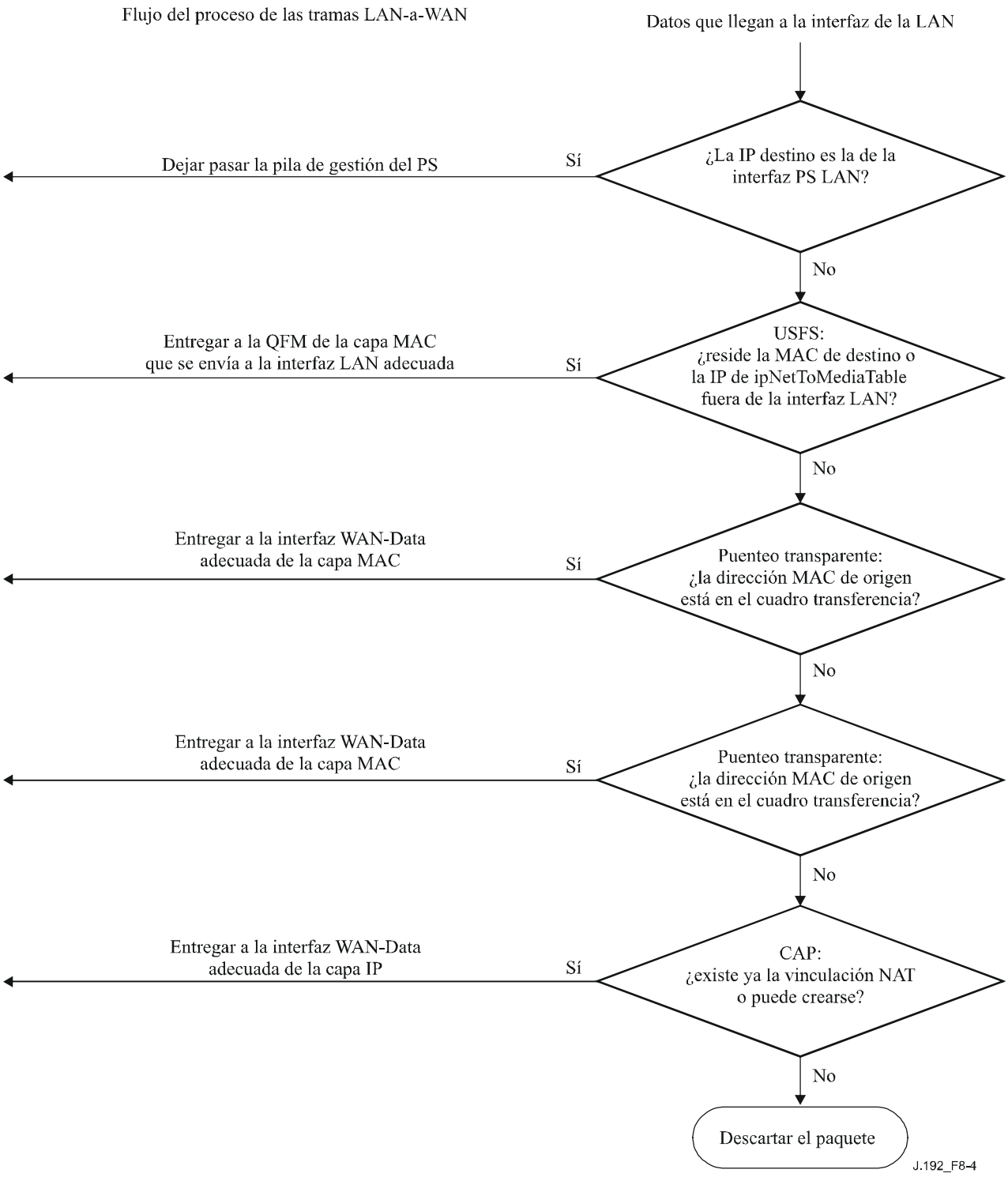


Figura 8-4/J.192 – Ejemplo de procesamiento de paquetes LAN-a-WAN

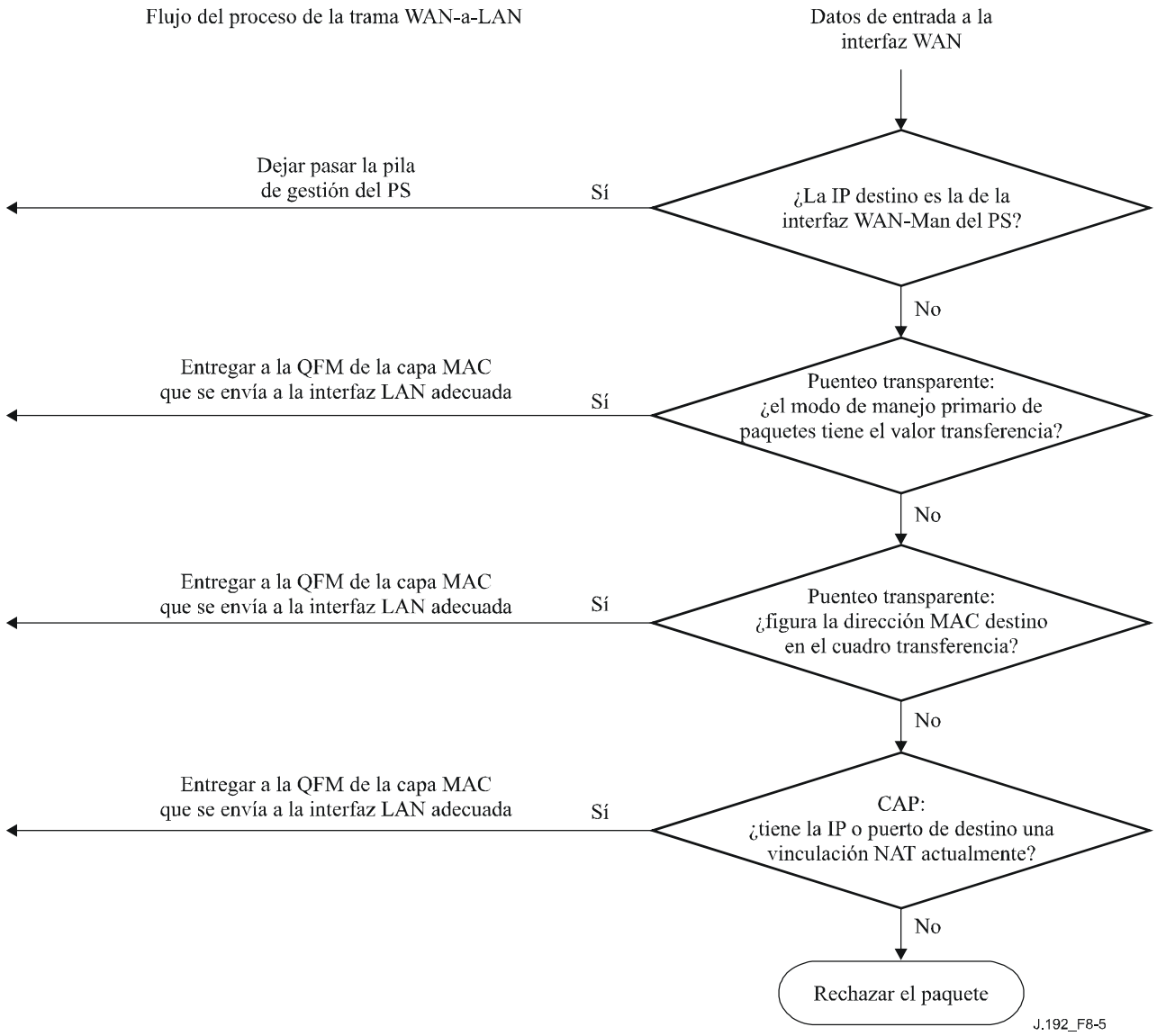


Figura 8-5/J.192 – Ejemplo de procesamiento de paquetes WAN-a-LAN

8.3.4 Requisitos del CAP

8.3.4.1 Requisitos generales

Todas las interfaces de IP lógicas en el elemento de servicios de portal DEBEN ser conformes a las secciones 3 y 4 de [RFC 1122] y [RFC 1123], a fin de permitir la comunicación normal con los anfitriones de Internet.

El PS DEBE soportar el tráfico de multidifusión de WAN-a-LAN puenteando de manera transparente los mensajes IGMP de WAN-a-LAN y los paquetes de multidifusión IP de WAN-a-LAN que se definen en [RFC 2236].

Si el modo de tratamiento de paquetes primario, cabhCapPrimaryMode, se fija a transferencia, se DEBEN puentear de modo transparente todos los mensajes IGMP de LAN-a-WAN.

Si el modo de tratamiento de paquetes primario, cabhCapPrimaryMode, se fija a C-NAPT, la dirección IP del origen de todos los mensajes IGMP de LAN-a-WAN, originados por dispositivos de LAN que residen en el dominio LAN-Trans, DEBE traducirse a la dirección IP de WAN-Data que se esté utilizando para las correspondencias de C-NAPT, y a continuación se retransmitirá a la red WAN.

Si el modo de tratamiento de paquetes primario, cabhCapPrimaryMode, se fija a C-NAT, la dirección IP de origen de todos los mensajes IGMP de LAN-a-WAN, originados por dispositivos IP de LAN que residen en el dominio LAN-Trans y que tienen una dirección IP que forma parte de una correspondencia C-NAT existente, DEBE traducirse a la dirección IP de WAN-Data que está siendo utilizada en esa correspondencia de C-NAT, y a continuación retransmitirse a la red WAN.

8.3.4.2 Requisitos del tratamiento de paquetes

El PS DEBE soportar el modo transferencia, el modo de encaminamiento transparente C-NAT y el modo de encaminamiento transparente C-NAPT, además el PS DEBE soportar la selección de este modo primario de tratamiento de paquetes mediante el objeto de la MIB cabhCapPrimaryMode.

Si el modo primario de tratamiento de paquetes, cabhCapPrimaryMode, tiene el valor C-NAT, el PS DEBE asegurarse de que exista una dirección IP disponible en el grupo de direcciones IP WAN-Data suministrada por la cabecera (con una licencia activa DHCP) antes de intentar utilizar esta dirección IP como parte de la correspondencia C-NAT. Si el CAP no pudiera crear una correspondencia C-NAT, por haberse agotado el grupo de direcciones IP WAN-Data, debería generar un evento normal (definido en el anexo B).

El PS DEBE fijar a cero los números de puerto de las redes WAN y LAN (cabhCapMappingWanPort y cabhCapMappingLanPort, respectivamente) del cuadro de correspondencias del CAP para cada correspondencia de C-NAT dinámica que cree.

Si el operador del sistema de cable crea o modifica una fila en el cuadro de correspondencias del CAP, es decir, si se crea una fila mediante el método de correspondencia estática (cabhCapMappingMethod = static(1)), y no se especifican los objetos de número de puerto de la fila (cabhCapMappingLanPort y cabhCapMappingWanPort), el PS DEBE anotar cero para cabhCapMappingLanPort y cabhCapMappingWanPort en esa fila.

El PS NO DEBE traducir el número de puerto de ningún paquete cuya dirección IP aparezca en el cuadro de correspondencias del CAP con un número de puerto igual a cero.

Si el modo primario de tratamiento de paquetes, cabhCapPrimaryMode, tiene el valor C-NAT, el PS DEBE asegurarse de que exista una dirección IP de la WAN actual (con una licencia activa DHCP de la configuración de la cabecera) antes de intentar utilizar esta dirección IP como parte de la correspondencia C-NAPT. Si el CAP no pudiera crear una correspondencia C-NAPT, por haberse agotado el grupo de direcciones IP de la WAN o el número de puertos, DEBE generar un evento normal (definido en el anexo B).

El tráfico de unidifusión entre redes LAN no DEBE encaminarse o puentearse nunca por una interfaz de la red WAN.

Cuando la licencia DHCP de una dirección IP de WAN-Data (que forma parte de la correspondencia de C-NAT o de C-NAPT) expira, todas las correspondencias asociadas con esa dirección DEBEN suprimirse de cabhCapMappingTable.

8.3.4.3 Requisitos del modo de transferencia

Cuando el modo primario de tratamiento de paquetes del CAP, cabhCapPrimaryMode, se fija al modo transferencia, el PS DEBE actuar como un puente transparente, definido en [ISO/CEI 10038], entre los sectores WAN-Data y LAN-Pass, y NO DEBE ejecutar función alguna de encaminamiento transparente C-NAT ni C-NAPT. Un PS que actúe como puente transparente para dispositivos LAN-Pass (cabhCapPrimaryMode = passthrough(3) o cabhCapPrimaryMode = napt(1) con anotaciones en cabhCapPassthroughTable) DEBE puentear de forma transparente todos los tipos de tramas que según las especificaciones DOCSIS deba transferir un módem de cable. Aunque el modo primario de tratamiento de paquetes sea transferencia, el procesamiento USFS DEBE tener prioridad frente a las decisiones de puenteo LAN-a-WAN.

8.3.4.4 Requisitos de encaminamiento transparente de C-NAT y de C-NAPT

Cuando el modo primario de tratamiento de paquetes (cabhCapPrimaryMode) tiene el valor C-NAT, el PS DEBE soportar los procesos de traducción de direcciones C-NAT de conformidad con los requisitos NAT básicos definidos en [RFC 3022].

Cuando el modo primario de tratamiento de paquetes (cabhCapPrimaryMode) tiene el valor C-NAPT, el PS DEBE soportar los procesos de traducción de direcciones C-NAPT de conformidad con los requisitos NAPT básicos definidos en [RFC 3022].

Independientemente del modo primario de tratamiento de paquetes el PS DEBE soportar la creación y supresión de correspondencias estáticas C-NAT y C-NAPT, mediante la autorización al sistema NMS para leer, crear y suprimir (a través del CMP) anotaciones de correspondencia CAP estáticas (cabhCapMappingTable).

Las correspondencias estáticas C-NAT y C-NAPT creadas por el NMS DEBEN conservarse en los rearranques del PS.

El PS DEBE soportar la creación de correspondencias dinámicas C-NAT y C-NAPT, iniciadas por tráfico TCP, UDP o ICMP LAN-a-WAN. El PS DEBE autorizar al sistema NMS la lectura (a través del CMP) de anotaciones de correspondencia CAP dinámicas (cabhCapMappingTable).

El PS DEBE soportar la supresión de correspondencias dinámicas C-NAT y C-NAPT si una correspondencia determinada está asociada a una sesión TCP y dicha sesión TCP termina o se supera el límite de inactividad del TCP, cabhCapTcpTimeWait, para dicha correspondencia.

El PS DEBE soportar la supresión de correspondencias dinámicas C-NAT y C-NAPT si una determinada correspondencia está asociada a una sesión UDP y se supera el límite de inactividad del UDP, cabhCapUdpTimeWait, para dicha correspondencia.

El PS DEBE soportar la supresión de correspondencias dinámicas C-NAT y C-NAPT si una determinada correspondencia está asociada a una sesión ICMP y se supera el límite de inactividad del ICMP, cabhCapIcmpTimeWait, para dicha correspondencia.

Las correspondencias dinámicas C-NAT y C-NAPT NO DEBEN conservarse tras los rearranques del PS.

En el cuadro de correspondencias CAP (cabhCapMappingTable) se crea una correspondencia entre una dirección IP privada de un dispositivo IP de la LAN del sector LAN-Trans y un número de puerto (dupla privada: cabhCapMappingLanAddr y cabhCapMappingLanPort) y entre una dirección IP pública y un número de puerto (dupla pública: cabhCapMappingWanAddr y cabhCapMappingWanPort), para una sesión establecida por el dispositivo IP de la LAN. A la combinación de dupla privada y dupla pública se denomina vinculación de traducción o correspondencia. La vinculación de traducción se representa como una anotación del cuadro de correspondencias CAP, y es creada automáticamente por el PS cuando el dispositivo IP de la LAN del sector LAN-Trans envía tráfico destinado a un dispositivo en la WAN a través del PS que actúa como pasarela por defecto del dispositivo IP de la LAN, creado automáticamente por el PS en las condiciones definidas para soportar {texto informativo: el servicio de conexión IP de WAN UPnP } según 8.3.3.7, o mediante la configuración directa del cuadro de correspondencias CAP utilizando un fichero de configuración de PS o mensajes de petición de establecimiento SNMP. Las correspondencias de las direcciones IP de C-NAT y C-NAPT (duplas privada y pública y vinculación de traducción) DEBEN ser coherentes y no cambiar para un dispositivo IP LAN dado una vez que se crean las correspondencias y hasta que se eliminan.

Cada dupla privada de un cuadro de correspondencias CAP DEBE tener asociada la misma dupla pública cada vez que aparezca en el cuadro de correspondencias CAP, con independencia del valor de la dirección IP del anfitrión remoto (cabhCapMappingRemoteHostAddr) para dicha anotación. Es decir, una dupla privada siempre está asociada a la misma dupla pública. Esta restricción prohíbe la implementación de un NAT simétrico como el descrito en [RFC 3489].

Si existe una correspondencia en el cuadro de correspondencias CAP para un dispositivo IP de LAN del sector LAN-Trans con un valor específico de cabhCapMappingRemoteHostAddr, y llega tráfico a la interfaz LAN del PS procedente del mismo dispositivo IP de LAN con la misma dirección IP de origen y el mismo número de puerto de origen pero con destino a una dirección IP de anfitrión distante diferente, el PS DEBE crear una nueva anotación en el cuadro de correspondencias CAP, con la misma dupla privada (cabhCapMappingLanAddr y cabhCapMappingLanPort) y dupla pública (cabhCapMappingWanAddr y cabhCapMappingWanPort) y con una anotación cabhCapMappingRemoteHostAddr que tenga el valor de la nueva dirección IP de destino. Es decir, para la misma dupla privada, el PS ha de utilizar la misma dupla pública para la vinculación. Por lo tanto, el PS ha de crear una anotación nueva y exclusiva en el cuadro de correspondencias CAP con un valor de dirección IP de anfitrión distante diferente pero con la misma vinculación de traducción privada – pública que la anotación previa. El resultado puede ser que la vinculación privada – pública (dupla privada y dupla pública para una anotación del cuadro de correspondencias CAP) aparezca en varias ocasiones en el cuadro de correspondencias CAP, pero con distintos valores de dirección IP de anfitrión distante en cada caso.

8.3.4.5 Requisitos de soporte de la red privada virtual

Cuando el CAP está funcionando en el modo primario de tratamiento de paquetes de C-NAT o de C-NAPT (indicado por el valor de cabhCapPrimaryMode), el PS DEBE reconocer las sesiones de IPSec iniciadas por clientes de la RPV en el sector LAN-Trans, crear las correspondencias adecuadas en el cuadro de correspondencias del CAP y hacer corresponder el puerto 500 del tráfico entrante (WAN a LAN) con la dirección IP de LAN-Trans vinculada con el dispositivo IP de LAN que inició la sesión.

Cuando el CAP está funcionando en el modo primario de tratamiento de paquetes de C-NAT o de C-NAPT (indicado por el valor de cabhCapPrimaryMode) y reconoce una sesión de IPSec cuando ya se ha establecido otra correspondencia en el cuadro de correspondencias del CAP con un servidor RPV distinto, el PS PUEDE crear correspondencias para la nueva sesión, por ejemplo, cambiando el puerto.

Si el CAP recibe tráfico entrante por el puerto 500 y no existe una sesión IPSec RPV activa, en ese caso DEBEN descartarse los paquetes que se reciben por ese puerto.

El PS DEBE soportar sesiones IPsec que utilicen el modo de tunelización de cabida útil de seguridad encapsulada según [RFC 2406].

8.3.4.6 Requisitos de la funcionalidad DMZ del CAP

Cuando el modo primario de tratamiento de paquetes (cabhCapPrimaryMode) se fija a C-NAPT y hay una correspondencia estática de C-NAPT con el número de puerto de la red WAN fijado a 0 y el número de puerto LAN fijado a 0 (es decir, cuando se ha creado una anotación DMZ en el CAP), en ese caso el PS DEBE traducir las direcciones IP especificadas en la correspondencia (anotación DMZ)de los paquetes que no estén asociados con una correspondencia de C-NAPT dinámica o estática existente.

Cuando se crea una anotación DMZ en el cuadro de correspondencias CAP para una dirección IP de LAN asignada dinámicamente por el PS (CDS), éste DEBE crear para dicha dirección una reserva de licencia de dirección IP. El PS DEBE determinar si la dirección IP de DMZ es asignada dinámicamente por el CDS, por ejemplo, buscándola en cabhCdpLanAddrTable. Si en dicho cuadro existe una anotación con valores de cabhCdpLanAddrMethod iguales a dynamicActive(4) o dynamicInactive(3), el PS DEBE sustituir dicha anotación por una que represente una reserva de licencia para dicha dirección IP del cuadro, es decir, una cuyo valor de cabhCdpLanAddrMethod sea psReservationActive(6) o psReservationInactive(5), respectivamente. Si no existe una anotación en el cuadro de correspondencias del CAP que se corresponda con la dirección IP de DMZ en cabhCdpLanAddrTable, el PS NO DEBE crear una reserva de licencia para dicha dirección IP.

Cuando se suprime una anotación de DMZ de cabhCapMappingTable para una dirección IP de LAN (anfitrión DMZ), el PS DEBE eliminar de cabhCdpLanAddrTable la correspondiente reserva de licencia de dirección IP que había creado internamente (identificada mediante cabhCdpLanAddrMethod = psReservationActive(6)) en la medida en que docsDevFilterIpTable o cabhSec2FwLocalFilterIpTable no contenga la regla de filtrado de la barrera contra fuegos necesaria.

8.3.4.7 Requisitos del modo de puenteo/encaminamiento híbrido

El PS DEBE soportar el modo híbrido puenteo/encaminamiento descrito en 8.3, en el que el modo primario de tratamiento de paquetes del CAP, cabhCapPrimaryMode, tiene el valor de encaminamiento transparente C-NAT o C-NAPT y donde el CAP puentea asimismo el tráfico de modo transparente para direcciones MAC específicas. Si el modo primario de tratamiento de paquetes del CAP, cabhCapPrimaryMode, tiene el valor de encaminamiento transparente C-NAT o C-NAPT y el NMS ha escrito una dirección MAC, perteneciente a un dispositivo IP de LAN, en el cabhCapPassthroughTable, el PS DEBE puentear transparentemente el tráfico LAN-a-WAN que tiene origen en dicha dirección MAC y el tráfico WAN-a-LAN destinado a dicha dirección MAC.

Cuando se encuentra en el modo híbrido puenteo/encaminamiento descrito en 8.3, la función USFS DEBE aplicarse a todo el tráfico recibido que tenga su origen en la LAN.

8.3.4.8 Requisitos del USFS

La funcionalidad de conmutación de retransmisión selectiva en sentido ascendente (USFS) DEBE aplicarse al procesamiento de paquetes, con independencia del modo de tratamiento de paquetes del CAP (transferencia, C-NAT, C-NAPT o híbrido puenteo/encaminamiento).

La función USFS DEBE inspeccionar todo el tráfico IP que tenga origen en las interfaces PS LAN, para determinar si la dirección IP de destino de un paquete es la del dispositivo que reside en la interfaz PS LAN. Si la dirección IP de destino de un paquete inspeccionado por el USFS es la de un dispositivo IP de LAN que reside fuera de la interfaz PS LAN, la función USFS DEBE sustituir la dirección de destino de la capa MAC, dentro del encabezamiento de la capa 2 del paquete, por la dirección MAC de dicho dispositivo IP de LAN de destino y entregar la trama a la entidad de retransmisión y acceso a los medios con QoS (QMF) (véase 10.3.1) en el PS, para que se retransmita por la interfaz LAN física adecuada conforme a la prioridad del paquete.

El USFS NO DEBE retransmitir ningún paquete destinado a un dispositivo IP de LAN por ninguna interfaz de WAN.

{texto informativo*:*

8.3.4.9 Configuración C-NAPT utilizando los requisitos del servicio WANIPConnection UPnP

El PS DEBE implementar el servicio WANIPConnection del InternetGatewayDevice UPnP tal como se define en UWIC.

El PS sólo DEBE habilitar el servicio WANIPConnection cuando funcione en el modo NAPT (cabhCapPrimaryMode = napt(1)) Y cuando cabhCapUpnpPortForwardingEnable = true(1). El PS NO DEBE habilitar el servicio WANIPConnection cuando funcione en los modos NAT, Transferencia, o Inhabilitado, o cuando cabhCapUpnpPortForwardingEnable = false(2). Si el servicio WANIPConnection está inhabilitado, el PS DEBE suprimir todas las correspondencias creadas mediante el servicio WANIPConnection.

Cuando el PS está configurado en el modo NAPT, DEBE soportar las acciones WANIPconnection (UWIC) siguientes a fin de permitir que los dispositivos UPnP creen, modifiquen, supriman y lean correspondencias de puertos: GetNATRSIPStatus, AddPortMapping, DeletePortMapping, GetGenericPortMappingEntry, GetSpecificPortMappingEntry y GetExternalIPAddress.

Si el PS está configurado en el modo NAPT y recibe una petición GetNATRSIPStatus UWIC de un dispositivo del dominio LAN-Trans, DEBE responder que el NAT está habilitado. Si el PS está configurado en el modo NAPT y recibe una petición GetNATRSIPStatus de un dispositivo del dominio LAN-Pass, DEBE responder que el NAT está inhabilitado.

El PS DEBE enumerar las correspondencias creadas mediante la acción AddPortMapping en cabhCapMappingTable cuyo valor de cabhCapMappingMethod sea UPnP (3). El PS DEBE crear una nueva correspondencia cuando las variables ExternalPort y PortMappingProtocol de la acción AddPortMapping no se correspondan con el puerto y protocolo actualmente utilizados en otra correspondencia. El PS DEBE crear una nueva correspondencia si las variables de la acción concuerdan con el puerto externo (ExternalPort), el protocolo de correspondencia del puerto (PortMappingProtocol) y con el cliente interno (InternalClient) de una correspondencia existente, pero no concuerdan con el anfitrión distante de la correspondencia.

El PS DEBE permitir que los puntos de control modifiquen, mediante la acción AddPortMapping (UWIC), correspondencias cuyo valor de cabhCapMappingMethod sea UPnP (3). Es previsible que el PS entienda que la acción AddPortMapping se refiere a una correspondencia ya existente cuando las variables de acción RemoteHost, ExternalPort, PortMappingProtocol e InternalClient concuerden con la correspondencia y PS NO DEBE modificar las correspondencias cuyo valor de cabhCapMappingMethod sea static (1) en respuesta a la acción AddPortMapping. Sin embargo, si la acción AddPortMapping especifica una correspondencia existente cuyo valor de cabhCapMappingMethod sea static(1), el PS DEBE devolver su acuerdo (OK) en respuesta a la acción.

Cuando se invoca la acción DeletePortMapping, el PS DEBE suprimir la correspondencia que concuerde con la petición si el valor del cabhCapMappingMethod de la correspondencia es UPnP(3). Si el valor del cabhCapMappingMethod de la correspondencia a suprimir es static(1) o dynamic(2), el PS DEBE ignorar la acción DeletePortMapping y devolver el código de error 501 (acción fallida).

Cuando un punto de control invoca la acción GetGenericPortMappingEntry, el PS DEBE devolver todas las correspondencias de cabhCapMappingTable cuyo valor de cabhCapMappingProtocol sea UDP(3) o TCP(4).

Cuando se recibe una acción GetSpecificPortMappingEntry, el PS DEBE verificar las anotaciones de cabhCapMappingTable y devolver la anotación, si la hubiera, que concuerde con los parámetros de anotación de la acción RemoteHost, ExternalPort y PortMappingProtocol.

Como respuesta a una acción GetExternalIPAddress, el PS DEBE devolver la dirección IP actual de WAN-Data.

}

9 Resolución de nombres

9.1 Introducción y presentación

9.1.1 Objetivos

Entre los objetivos de la resolución de nombres se encuentran:

- Proporcionar el servicio de nombres de dominio (DNS) desde un servidor del PS a los clientes DNS de los dispositivos IP de LAN, incluso estando el cable desconectado.
- Permitir que los abonados se refieran a los dispositivos locales mediante nombres de dispositivos intuitivos en vez de por direcciones IP.
- Mediante consultas recurrentes a servidores DNS distantes, proporcionar respuestas a los clientes DNS de LAN cuando solicitan la determinación de nombres de anfitrión no locales.

- Proporcionar una recuperación fácil del servicio DNS una vez reestablecida la conectividad del cable tras la desconexión.

9.1.2 Hipótesis

Entre las hipótesis de funcionamiento de los servicios de gestión de nombres se encuentran las siguientes:

- El servidor DNS del elemento PS es el único servidor DNS con autoridad frente a los dispositivos IP de LAN del sector LAN-Trans.
- El elemento PS no prestará el servicio DNS a los dispositivos IP de LAN del sector LAN-Pass.
- Si el elemento PS utiliza varias direcciones WAN-Data, se utilizará la información del servidor DNS de la WAN obtenida durante el último proceso de adquisición de direcciones WAN-Data (DHCP).

9.2 Arquitectura

9.2.1 Directrices de diseño del sistema

véase el cuadro 9-1.

Cuadro 9-1/J.192 – Directrices de diseño del sistema de resolución de nombres

Referencia	Directrices
Name Rsln 1	Proporcionar el servicio de nombres de dominio (DNS) desde un servidor del PS a los clientes DNS de dispositivos IP de LAN, para la resolución de nombres de los dispositivos IP de LAN (independientemente del estado de la conexión de la WAN).
Name Rsln 2	Proporcionar respuestas del DNS, mediante consultas recurrentes, comenzando con un servidor DNS de la red de cable, para clientes del DNS en los dispositivos IP de LAN, para la resolución de nombres de anfitrión que no sean locales.

9.2.2 Descripción del sistema

En esta cláusula se presenta un resumen de los servicios de determinación de nombres de IPCable2Home en el elemento PS.

9.2.2.1 Resumen funcional de la resolución de nombres

El portal de denominación de IPCable2Home (CNP, *IPCable2Home naming portal*) es un servicio que funciona en el PS y constituye un servidor DNS sencillo para los dispositivos IP de LAN del sector de direcciones LAN-Trans. Sin embargo, la funcionalidad CNP para el sector de direcciones LAN-Trans se obvia si la MIB cabhCdpServerDnsAddress tiene un valor distinto de cabhCdpServerRouter. Los dispositivos IP de LAN del sector LAN-Pass no utilizan el CNP, porque son atendidos por servidores DNS exteriores al hogar.

Por lo general, el CDP configura todos los dispositivos IP de LAN del sector LAN-Trans para que utilicen el CNP como su servidor de nombres de dominio. El servicio CNP del sector LAN-Trans no depende del estado de conexión de la WAN. El CNP efectúa las tareas siguientes:

- Resuelve los nombres de servidor para los dispositivos IP de LAN, devolviendo sus correspondientes direcciones IP.
- Proporciona respuestas del DNS, mediante consultas recurrentes comenzando por un servidor DNS en la red de cable, cuando haya consultas que no puedan resolverse por la información local del PS. Esto ocurre cuando la información del servidor DNS de la WAN está disponible en el PS. De lo contrario, el CNP devuelve un error que indica que el nombre no puede resolverse en dicho momento.

La utilización del CNP como servidor DNS primario en la LAN evita la necesidad de reconfigurar los dispositivos IP de LAN cuando se modifica el estado de conexión de la WAN y permite asimismo modificar la asignación de servidor DNS externo sin tener que reconfigurar los dispositivos IP de LAN.

9.2.2.2 Funcionamiento de la resolución de nombres

Cuando se solicita a la función CNP del PS que resuelva un nombre de servidor, ejecuta el proceso de consulta mostrado en la figura 9-1. El CNP responde a las consultas iniciales DNS normales [RFC 1035], dirigidas a cabhCdpServerDnsAddress, en todas las búsquedas de nombres. El CNP se encarga de efectuar consultas recurrentes a los servidores DNS externos, comenzando con la primera anotación cabhCdpWanDnsServerIp en el cuadro cabhCdpWanDnsServerTable del CDP, cuando un dispositivo IP de LAN efectúa una consulta y de enviar a ese dispositivo una respuesta o un mensaje de error.

El CNP se apoya en el cuadro cabhCdpLanAddrTable del CDP, para obtener los nombres de anfitrión asociados con las direcciones IP actuales de los dispositivos IP de LAN activos. Mientras un dispositivo IP de LAN conserve una licencia DHCP activa con el CDP y haya proporcionado un nombre de anfitrión al CDP (como parte de su proceso de adquisición de una dirección IP) el CNP podrá determinar su nombre. Si el nombre de anfitrión solicitado para su determinación no puede encontrarse en cabhCdpLanAddrTable, el CNP efectúa consultas recurrentes a los servidores DNS externos (de los cuales se obtiene información del primero mediante el CDC a través de las opciones de DHCP).

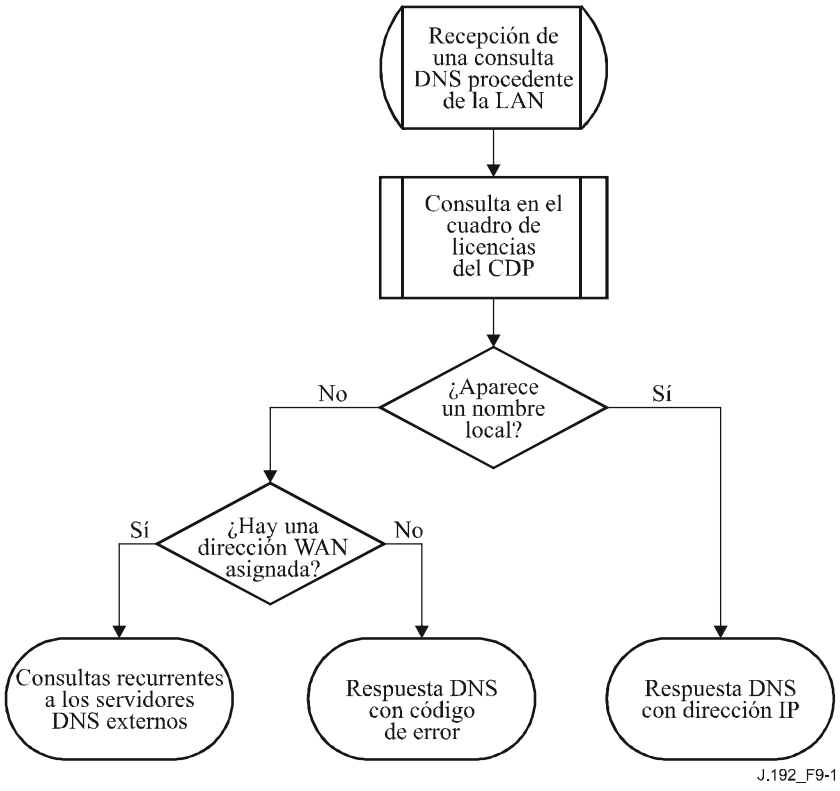


Figura 9-1/J.192 – Procesamiento de los paquetes del CNP

Una consulta normal de DNS especifica un nombre de dominio objetivo (QNAME), un tipo de consulta (QTYPE, *query type*) y una clase de consulta (QCLASS, *query class*), y solicita los registros de recursos concordantes. El CNP responde las consultas DNS con QCLASS = IN, y QTYPE = A, NS, SOA o PTR definidos en [RFC 1035]. No es necesario el soporte de transferencia de zona ni el DNS por TCP.

Como el CNP es un servidor DNS autorizado dentro del sector LAN-Trans, proporcionará registros de comienzo de autoridad (SOA, *start of authority*) y servidor de nombres (NS, *authoritative nameserver*) autorizado a petición. A continuación se da un ejemplo de los campos de registro SOA (véase la sección 3.3.13 de [RFC 1035]):

Cuadro 9-2/J.192 – Campos del registro SOA

Campo RDATA de [RFC 1035]	Objeto de la MIB del CDP de IPCable2Home
MNAME	cabhCdpServerDomainName
RNAME	Sin especificar
SERIAL	Sin especificar
REFRESH	Sin especificar
RETRY	Sin especificar
EXPIRE	Sin especificar
MINIMUM	Sin especificar

El campo MNAME es el nombre de dominio del sector de direcciones LAN-Trans. El CNP utiliza el valor almacenado en cabhCdpServerDomainName como nombre del dominio del sector de direcciones LAN-Trans.

El campo RNAME es el buzón de la persona responsable del dominio. Si el PS mantuviera una dirección de correo electrónico para el administrador, esta información podría especificarse en dicho campo.

El campo SERIAL es un número de 32 bits sin signo que identifica la versión de la información de zona. Como esta Recomendación no especifica las transferencias de zona, el valor de este campo no se especifica.

9.3 Requisitos de la resolución de nombres

El CNP DEBE ajustarse al formato normal de los mensajes DNS y soportar las consultas normales DNS, de acuerdo con lo descrito en [RFC 1034] y [RFC 1035].

El CNP es un servidor sin memoria de estado que DEBE poder aceptar consultas y enviar respuestas en paquetes UDP [RFC 768].

El CNP DEBE soportar el modo recurrente, como se define en [RFC 1034].

El CNP responde a las consultas relativas a nombres, comenzando con la información local en el PS, y sus mensajes de respuesta DEBEN incluir una respuesta o un error.

El CNP DEBE responder únicamente a consultas de DNS dirigidas a la dirección IP representada por el valor del objeto de la MIB cabCdpServerRouter (es decir, la dirección IP del lado LAN del PS).

El CNP NO DEBE responder a ninguna consulta de DNS dirigida a las direcciones de WAN-Man o de WAN-Data del PS.

Cuando se recibe una consulta inicial de determinación de nombre de anfitrión de un dispositivo IP de LAN, el CNP DEBE acceder a cabhCdpLanAddrTable del CDP para examinar los nombres de anfitrión asociados con la direcciones IP de las que se han otorgado licencias a los dispositivos IP de LAN.

Independientemente de la existencia de anotaciones cabhCdpWanDnsServerIp en la MIB cabhCdpWanDnsServerTable del CDP, si el nombre del anfitrión puede determinarse mediante

el CNP a partir de los datos locales, el CNP DEBE responder a la consulta de determinación del nombre de anfitrión con la dirección IP del dispositivo IP de LAN nombrado.

Si el nombre de anfitrión consultado no puede determinarse mediante el CNP a partir de los datos locales, y el cuadro cabhCdpWanDnsServerTable del CDP se ha rellenado con al menos una anotación cabhCdpWanDnsServerIp, la función CNP del PS DEBE tratar de resolver la consulta del nombre de anfitrión mediante consultas recurrentes a los servidores DNS externos, comenzando con el servidor DNS representado por la primera anotación cabhCdpWanDnsServerIp en cabhCdpWanDnsServerTable. En esta consulta, el CNP DEBE utilizar la dirección IP de WAN-DATA como dirección IP de origen para el mensaje de consulta al DNS. Se supone que el operador ha facilitado al CNP una dirección IP pública como WAN-DATA-IP; si no es así, el operador proporciona el encaminamiento entre la dirección IP de WAN-DATA privada y el servidor de DNS que el operador utiliza en la cabecera.

Si el nombre del anfitrión no puede determinarse mediante el CNP a partir de los datos locales y no existen anotaciones cabhCdpWanDnsServerIp en el cuadro cabhCdpWanDnsServerTable, la función CNP del PS DEBE responder a la consulta de determinación del nombre de anfitrión con el error correspondiente especificado en [RFC 1035].

El CNP DEBE responder a las consultas de DNS de tipo QCLASS = IN y QTYPE = A, NS, SOA o PTR, SRV [RFC 2782] y ENUM [RFC 3761].

Las respuestas del CNP a las consultas de DNS DEBEN cumplir con la sección 3.3 de [RFC 1035], con el bit de respuesta autorizada fijado a '1' en la sección del encabezamiento (véase la sección 4.1.1 de [RFC 1035]).

Como el CNP es un servidor DNS autorizado del sector LAN-Trans, DEBE proporcionar registros de comienzo de autoridad (SOA) y servidor de nombres autorizado (NS) a petición. Los campos del registro SOA (véase la sección 3.3.13 de [RFC 1035]) DEBEN contener una anotación para el campo MNAME que sea igual al valor del objeto de la MIB cabhCdpServerDomainName del CDP.

Aunque no se haya fijado cabhCdpServerDomainName, el CNP DEBE proporcionar servicio DNS a los dispositivos IP de LAN.

9.3.1 Registros de tipo ENUM, NAPTR y SRV del DNS

9.3.1.1 Consultas ENUM y respuesta en el CNP [RFC 3761]

En esta cláusula se describe el comportamiento del CNP cuando recibe una consulta DNS de tipo ENUM de clientes CPE de LAN.

El CNP DEBE aceptar consultas de tipo ENUM de dispositivos CPE de LAN y hacerlas llegar al operador de cable utilizando la dirección cabhCdpWanDnsServerIp, cuando se rellena dicha MIB y el servidor DNS del operador de cable es alcanzable.

El CNP DEBE intentar consultar al servidor DNS del operador de cable representado en cabhCdpWanDnsServerIp en busca de los registros NAPTR correspondientes a las consultas de tipo ENUM del dispositivo CPE de LAN, tal como se especifica en [RFC 3761].

Si el CNP obtiene los registros NAPTR como consecuencia de la consulta ENUM, el CNP DEBE remitir dichos registros, "tal como los recibe", a los clientes CPE de LAN.

El CNP no necesita implementar el sistema dinámico de determinación de delegación (DDDS, *dynamic delegation discovery system*), especificado en [RFC 3401-3404]. Es suficiente con que el CNP pueda enviar las consultas DNS de tipo ENUM a los servidores DNS del operador de cable representados en cabhCdpWanDnsServerIp. Se supone que si un operador proporciona servicios a sus abonados de CableHome que necesitan resolver consultas DNS de tipo ENUM, permitirá que dichas consultas se resuelvan en el servidor o servidores incluidos en la MIB cabhCdpWanDnsServerIp.

9.3.1.2 Consultas SRV y respuesta en el CNP [RFC 2782]

En esta cláusula se describe el comportamiento del CNP cuando recibe consultas DNS del tipo SRV de clientes CPE de LAN.

El CNP DEBE aceptar consultas de tipo SRV de dispositivos CPE de LAN y remitirlas al operador utilizando la dirección cabhCdpWanDnsServerIp, cuando dicha MIB tiene datos y el servidor DNS del operador es alcanzable.

El CNP DEBE intentar consultar al servidor DNS del operador representado en cabhCdpWanDnsServerIp, en busca de los registros NAPTR correspondientes a las consultas DNS de tipo SRV del dispositivo CPE de LAN, tal como se especifica en [RFC 3761].

Si el CNP obtiene registros SRV como consecuencia de la consulta, el CNP DEBE remitir dichos registros, "tal como los recibe", a los clientes CPE de LAN.

Es suficiente que el CNP pueda remitir las consultas de tipo SRV a los servidores DNS del operador incluidos en cabhCdpWanDnsServerIp. También debe señalarse que si un operador proporciona servicios a abonados de CableHome que necesiten resolver consultas DNS de tipo SRV, permitirá que se resuelvan dichas consultas en el servidor o servidores incluidos en la MIB cabhCdpWanDnsServerIp.

10 Calidad de servicio

10.1 Introducción

En esta cláusula se describe el entorno de IPCable2Home que facilita que las aplicaciones de funcionamiento en red doméstica que se ejecutan sobre dispositivos conectados a la red doméstica utilicen características de QoS soportadas por un protocolo LAN. Este entorno proporciona un mecanismo de gestión que asigna prioridades a los flujos de datos para soportar el tráfico de aplicaciones en tiempo real, como es el caso de VoIP, flujo continuo de A/V, y juegos de vídeo, utilizando acceso a los medios con prioridades y colas. La QoS de IPCable2Home complementa los mecanismos de QoS de IPCablecom y J.112, y permite la gestión del tráfico de QoS por la red HFC. {texto informativo: IPCable2Home utiliza mensajes de QoS del tipo "conexión y funcionamiento universal" (UPnPTM, *universal plug and play*) en la interfaz o interfaces de la LAN.}

En esta Recomendación se definen los requisitos de QoS necesarios para los elementos y subelementos del PS, que permiten a las aplicaciones establecer distintos niveles de QoS en la red doméstica y que los operadores y los usuarios puedan comunicar el tratamiento de prioridad deseado a las aplicaciones habilitadas por el operador y {texto informativo: habilitadas por UPnP} en la red doméstica.

10.1.1 Objetivos

Los objetivos de la QoS de IPCable2Home son:

{ texto informativo:

- Habilitar aplicaciones de funcionamiento en red doméstica que permitan establecer transmisión de datos con prioridades entre anfitriones UPnP, así como entre éstos y la pasarela residencial utilizando mensajería conforme con UPnP.
- Habilitar aplicaciones de funcionamiento en red doméstica para establecer la transmisión de datos con prioridad entre anfitriones y entre los anfitriones y la pasarela residencial IPCable2Home utilizando mensajes conformes con UPnP.

}

10.1.2 Hipótesis

Se efectúan las siguientes hipótesis para la QoS de IPCable2Home:

{texto informativo:

- Las aplicaciones que se benefician de la aplicación de QoS pueden funcionar en dispositivos anfitriones CableLabs o en dispositivos conformes con QoS UPnP.}
- Las aplicaciones del anfitrión de IPCable2Home podrían incluir servicios de IPCablecom.

{texto informativo:

NOTA – Cualquier dispositivo anfitrión de LAN que desee recibir con QoS los servicios del operador deberá cumplir la especificación UPnP QoS 1.0 y el sistema de operación del dispositivo, y la pila de protocolos de la red deberán tener capacidades de QoS adecuadas.}

10.2 Arquitectura de QoS

La arquitectura de la calidad de servicio de IPCable2Home (CQoS) consta del elemento funcional pasarela residencial de IPCable2Home (PS y subelementos en el PS). Los desarrolladores de la pasarela residencial en el hogar implementan uno o varios de estos elementos en función del conjunto de características deseadas para estos productos. Los elementos básicos de CQoS se presentan en 10.2.3.

10.2.1 Directrices de diseño del sistema

Las directrices completas de diseño del sistema de QoS de IPCable2Home se relacionan en el cuadro 10-1 siguiente.

Cuadro 10-1/J.192 – Directrices de diseño del sistema de QoS de IPCable2Home

Número	Directrices
QoS 1	Acceso a los medios con QoS: IPCable2Home definirá una función de gestión de capa 3 que controle el acceso a la transmisión utilizando prioridades en los medios compartidos para el elemento lógico PS. Proporcionará acceso a los medios mediante prioridades a varios dispositivos y aplicaciones en la red doméstica.
QoS 2	Retransmisión de QoS: El PS debe soportar un mecanismo de colas que asigne prioridades a los paquetes que se reciben de múltiples interfaces (LAN o WAN) y que habrán de retransmitirse/reenviarse a través de las interfaces de LAN.
QoS 3	{texto informativo: Gestión de la política de QoS: IPCable2Home especificará un mecanismo de señalización y gestión para la comunicación de las políticas de QoS entre el PS y los BP que necesiten QoS, así como entre el PS y dispositivos conformes con la QoS UPnP, en una red doméstica. Este mecanismo se agregará y gestionará en el PS.}
QoS 4	Señalar las capacidades del PS adecuadas para permitir la integración con multimedios IPCablecom a fin de disponer de QoS extremo a extremo en el futuro.

{texto informativo:

10.2.2 Relación con QoS UPnP

La arquitectura CQoS utiliza mensajes conformes con la QoS UPnP entre los elementos con QoS. En la arquitectura UPnP, los mensajes de control se inician desde elementos punto de control UPnP y se responde a ellos mediante elementos de servicio UPnP. Por lo tanto, los elementos o subelementos de las entidades del PS se describen en términos del punto de control con QoS UPnP y de los elementos de servicio con QoS UPnP (UQA).

La arquitectura UPnP también se caracteriza como una arquitectura distribuida en la que hay múltiples ejemplares de un determinado servicio en la HN que pueden utilizarse de forma intercambiable. Mientras que la arquitectura CQoS describe ciertos servicios con QoS UPnP contenidos en el PS, pueden existir otros dispositivos en la HN que también implementen los mismos servicios con QOS UPnP. Cuando las descripciones o los requisitos del PS se escriben utilizando terminología del elemento con QoS UPnP, puede haber interacción con dispositivos que no sean PS. Por ejemplo, en la descripción de un punto de control que interactúe con un servicio QosManager, el punto de control puede estar interactuando con la funcionalidad gestor de QoS de otro dispositivo en lugar de interactuar con el servicio gestor de QoS del PS.}

10.2.3 Descripción del sistema de QoS de IPCable2Home

La arquitectura de CQoS consta de las siguientes entidades:

- Elemento de servicios de portal (PS).
- Subelemento del portal de calidad de servicio de IPCable2Home (CQP).
- {texto informativo: anfitriones UPnP con capacidades de QoS.}

El equipo de la red de datos por cable (cabecera) gestiona las funciones de QoS de IPCable2Home.

10.2.3.1 Subelemento CQP

El elemento PS incluye un subelemento de portal de calidad de servicio de IPCable2Home (CQP), que se comporta como un portal de CQoS para anfitriones UPnP con capacidades de QoS. Su función principal es habilitar QoS basada en las prioridades para los dispositivos en la red doméstica. Maneja colas/retransmisión y acceso a los medios basados en las prioridades para el tráfico que origina el PS, así como para el tráfico que transita por el mismo. Además, se encarga de la comunicación de las políticas de QoS {texto informativo: al gestor o gestores de QoS UPnP [UQM] en el hogar cuando funciona como único servicio tenedor de política de QoS UPnP [UQPH, UPnP QoS Policy Holder].}

10.2.3.2 Funcionalidad de QoS en CQP

Los subelementos CQP tienen las funcionalidades siguientes:

- Intermediario de QoS de IPCable2Home (CQB): Responsable de fijar la QoS en la red doméstica así como en la red de acceso. Esta entidad también configura la QoS en el PS IPCable2Home. El CQB consta de las funcionalidades siguientes:
  - **Retransmisión y acceso a los medios con prioridades de QoS (QFM)**: Especifica colas y retransmisión de paquetes con prioridades así como el acceso a medios compartidos con prioridades en el PS.
  - **Interfaz multimedia IPCable2Home-IPCablecom (CH-PCMM)**: Interfaz que permite solicitar al PS IPCable2Home la QoS de la red de acceso de conformidad con la arquitectura multimedia de IPCablecom [Rec. UIT-T J.179]. La interfaz CH-PCMM también puede recibir solicitudes de establecimiento de QoS de HN de entidades PCMM de la WAN. En base a dicha petición, la entidad intermediario de QoS de CH puede utilizar puntos de control de QoS de CH para establecer una QoS de HN. Los requisitos específicos de esta interfaz requieren estudios adicionales.
  - {texto informativo: **Interfaz de servicio de dispositivos con QoS UPnP (QD)**: El CQB puede incluir una interfaz de servicio de dispositivos con QoS UPnP (UQD, *UPnP QoS device*) con los fines siguientes:
    1) Mediante esta interfaz, el PS recibe peticiones de clasificadores de tráfico de las entidades gestoras de QoS UPnP (UQM, *UPnP QoS manager*) en la LAN y las ubica en la base de datos del PS. La funcionalidad QFM utiliza estos clasificadores para clasificar los paquetes.

2) Utilizando esta interfaz de servicio, el PS puede activar una petición de QoS en la red de acceso para los flujos de tráfico que circulan a lo largo de las redes de acceso y doméstica, utilizando la interfaz CH-PCMM a definir ulteriormente.

}

{texto informativo:

- **Servidor de política de QoS (QPS)**: Esta funcionalidad se encarga de mantener un repositorio de políticas de QoS para múltiples dispositivos y aplicaciones en la red doméstica y para la comunicación de dicha política cuando la solicita una entidad gestora de QoS UPnP [UQM] de la LAN. El QPS utiliza la interfaz del servicio tenedor de política de QoS UPnP [UQPH] para comunicar las políticas de QoS de la LAN doméstica. El QPS tiene una interfaz MIB en el lado WAN para que los operadores gestionen y tengan acceso a políticas de QoS.
- **Servicio gestor de QoS (QM)**: El CQP debe implementar el servicio gestor de QoS UPnP (UQM). Este requisito garantiza que exista al menos un servicio gestor de QoS UPnP para que los puntos de control UPnP soliciten QoS en la LAN doméstica.
- **Funcionalidad de QoS del punto de control del PS (QCP)**: Esta entidad actúa como un punto de control para diversos servicios de QoS UPnP en la LAN doméstica. Es responsable de capturar anuncios de QoS UPnP, eventos y de generar actuaciones necesarias para varios servicios de QoS UPnP en la LAN.
    1) La lógica de determinación de QoS de este punto de control es responsable de recopilar la información conexa de QoS de varios servicios con QoS UPnP en la LAN doméstica, y almacenarlos en la base de datos del PS. Los operadores de cable acceden a esta información de la base de datos del PS en la WAN a través de la interfaz de la MIB SNMP.
    2) La lógica del intermediario de QoS IPCable2Home de este punto de control es responsable de establecer la QoS en la LAN doméstica utilizando mensajes de QoS UPnP bajo la dirección del intermediario de QoS IPCable2Home. Dicha lógica es también responsable de solicitar una QoS en la red de acceso utilizando la interfaz CH-PCMM.

}

{texto informativo:

10.2.3.3 Funcionalidad de QoS en anfitriones UPnP

La funcionalidad de QoS de un anfitrión UPnP consta de uno o varios de los siguientes servicios de QoS UPnP:

- servicio gestor de QoS UPnP (UQM);
- servicio de dispositivo con QoS UPnP (UQD);
- servicio gestor de QoS UPnP (UQPH).

El anfitrión UPnP también puede implementar un punto de control UPnP que solicite QoS en la LAN doméstica.

}

10.2.3.4 Clases de dispositivos físicos y elementos funcionalidades e interfaces de mensajería de CQoS

En la figura 10-1 se presenta un ejemplo de la relación entre los dispositivos de IPCable2Home y los elementos funcionales de CQoS. La figura 10-2 representa las interfaces de mensajería entre varios elementos funcionales de la arquitectura CQoS sin que la misma implique una implementación concreta. {texto informativo: Las flechas a trazos indican una comunicación interna potencial cuando interactúan las entidades de QoS UPnP en el PS.}

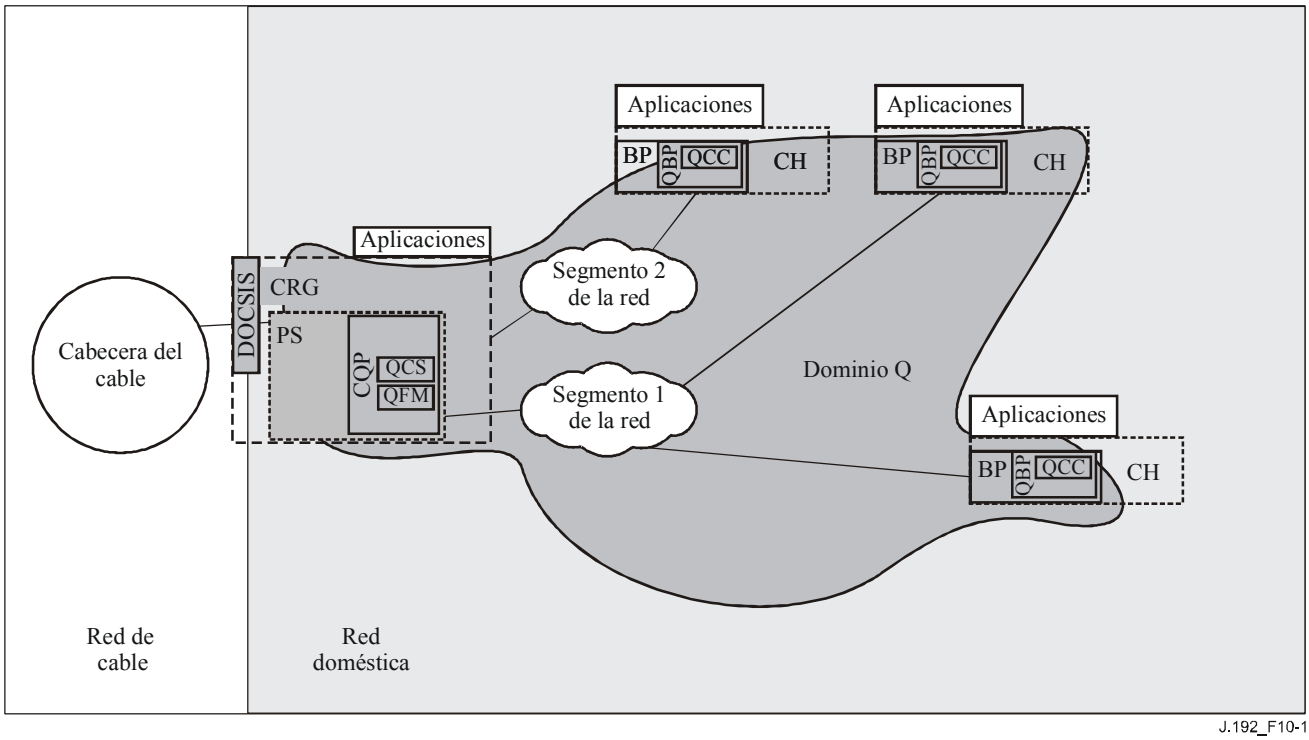


Figura 10-1/J.192 – Ejemplo de elementos funcionales de CQoS

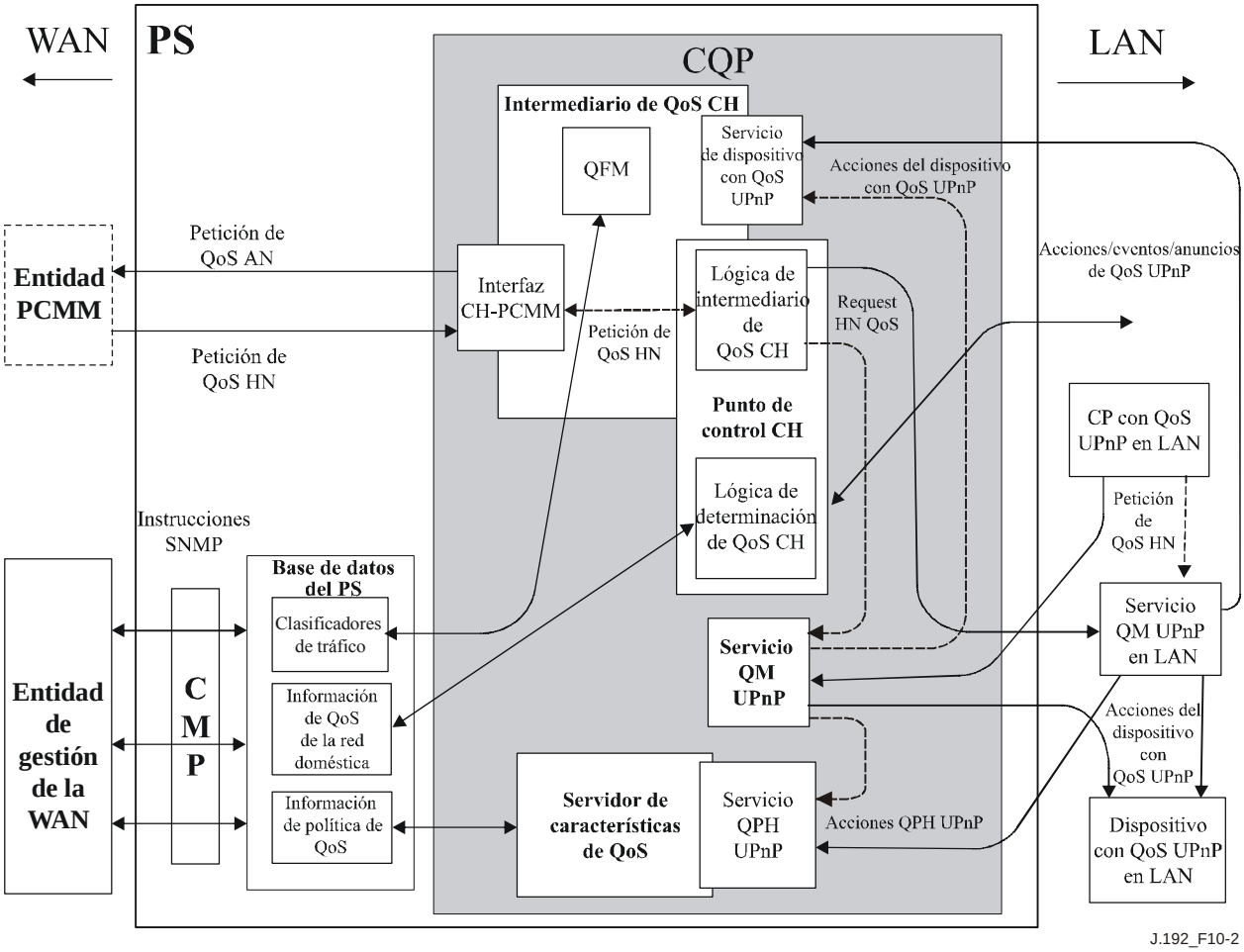


Figura 10-2/J.192 – Interfaces de mensajería de la arquitectura de QoS CableHome

10.2.3.5 Prioridades de IPCable2Home y sus correspondencias

10.2.3.5.1 Prioridades de IPCable2Home

En la presente Recomendación se definen tres prioridades de QoS distintas:

- {texto informativo:

  Número de la importancia del tráfico UPnP.}
- prioridades de encolamiento IPCable2Home;
- prioridades de acceso a los medios IPCable2Home.

{texto informativo:

10.2.3.5.1.1 Número de importancia del tráfico (TIN, TrafficImportanceNumber) UPnP

El número de importancia del tráfico UPnP (TIN según UQPH) no es lineal sino que sigue el mismo esquema de numeración que los valores de prioridad de los paquetes del anexo G de ISO/CEI 1038. Este esquema de numeración se muestra en el cuadro 10-2. Los operadores de cable asignan un valor de TrafficImportanceNumber UPnP a un flujo de tráfico en el cuadro de políticas de QoS (cabhQos2PolicyTable) (según E.7) almacenado en la base de datos PS.

Cuadro 10-2/J.192 – Esquema de numeración para TrafficImportanceNumber UPnP

Número de importancia del tráfico UPnP
7 (el más alto)
6
5
4
3
0 (mayor esfuerzo posible)
2
1 (el más bajo)

NOTA – Los valores 1 y 2 de TrafficImportanceNumber UPnP indican una prioridad inferior a 0 (0 se asigna típicamente a sistemas preexistentes de tráfico basado en el mayor esfuerzo posible).

}

10.2.3.5.1.2 Prioridades de encolamiento de IPCable2Home

En el PS, los paquetes pueden provenir de múltiples interfaces y estar destinados a una sola interfaz. Cada interfaz puede implementar una función de encolamiento. A fin de asignar prioridades de QoS al tráfico que pasa a través del PS en la vivienda, en esta Recomendación se especifica la funcionalidad de encolamiento con prioridades para cada interfaz en el PS. Para este fin, se designa una cola particular en una interfaz asignándole una determinada prioridad. Esto se conoce como prioridad de encolamiento de IPCable2Home. Esta prioridad puede identificarse para cada paquete a transmitir por cada interfaz del PS, de manera que el paquete pueda colocarse en una cola adecuada. Esta prioridad de encolamiento orientada a colas se deduce del

{texto informativo:

TrafficImportanceNumber UPnP asignado al flujo de tráfico, utilizando el número de colas soportadas por una interfaz del PS. Esta correspondencia se realiza tal como se especifica en ISO/CEI 1038, anexo G}

10.2.3.5.1.3 Prioridades de acceso a los medios de IPCable2Home

En esta Recomendación se define un sistema de acceso a los medios con prioridades de QoS en el cual el tráfico por medios compartidos puede ser priorizado en función de la prioridad asignada al paquete. Por consiguiente, una tecnología de medios compartidos puede soportar criterios de QoS con un esquema de prioridades tal que un paquete con una prioridad superior reciba un acceso preferencial a los medios compartidos, a diferencia de un paquete con una prioridad inferior. Varias tecnologías que emplean medios compartidos soportan un número variable de prioridades de acceso a los medios. (Por ejemplo, WMM Wi-Fi soporta cuatro prioridades de acceso a los medios, HomePNA soporta ocho prioridades de acceso a los medios, HomePlug soporta cuatro prioridades). {texto informativo: La prioridad de acceso a los medios de IPCable2Home de los paquetes se deduce de su TrafficImportanceNumber UPnP, en base al número de prioridades de acceso a los medios soportadas por la tecnología de medios compartidos de capa 2 de la interfaz. Esta correspondencia se realiza tal como se especifica en ISO/CEI 10038, anexo G.} Los valores de la prioridad de acceso a los medios de IPCable2Home son niveles lógicos que representan un nivel de preferencia que de un paquete para el acceso a los medios.

10.3 CQP del subelemento lógico del PS

El CQP incluye las funcionalidades CQB, QM, QCP y QPS que se muestran en la figura 10-1. La funcionalidad CQB se describe en 10.3.1. Mientras que la QPS se describe en 10.3.2. La funcionalidad QM se describe en 10.3.3. La funcionalidad QCP se describe en 10.3.4.

10.3.1 Intermediario de QoS de IPCable2Home (CQB)

El CQB consta de la funcionalidad de retransmisión y acceso a los medios con QoS (QFM) y opcionalmente de una interfaz de servicio de dispositivos con QoS.

10.3.1.1 Retransmisión y acceso a los medios con QoS (QFM)

La QFM en el PS es responsable de la retransmisión y el acceso a los medios con prioridades para los paquetes que van del PS a la red LAN doméstica. En esta cláusula se describe la funcionalidad de QFM en el PS y se especifican los requisitos del PS asociados.

10.3.1.1.1 Objetivos de la retransmisión y el acceso a los medios con QoS

Los objetivos de la funcionalidad de la retransmisión y el acceso a los medios con QoS incluyen:

- Ordenar los paquetes que se reciben de múltiples interfaces del PS retransmitiéndolos a una interfaz LAN de destino conforme a sus prioridades y a las capacidades de las colas en las interfaces LAN.
- Asignar un acceso con prioridad a los medios compartidos durante la transmisión del paquete en las interfaces LAN basándose en la prioridad de paquete y en las capacidades de acceso a los medios mediante prioridades de las interfaces de la LAN.

10.3.1.1.2 Directrices de diseño de la retransmisión y acceso a los medios con QoS

Véase el cuadro 10-3.

Cuadro 10-3/J.192 – Directrices de diseño del sistema QFM

Número	Directrices
QFM.1	La QFM puede aplicarse a los paquetes hacia y desde los sectores de direcciones de LAN-Trans y de LAN-Pass.
QFM.2	La QFM puede determinar la prioridad de los paquetes utilizando la información de clasificación de paquetes disponible en la base de datos del PS.
QFM.3	La QFM puede ordenar los paquetes entrantes de modo que salgan por las interfaces LAN conforme a sus prioridades.
QFM.4	La QFM debería poder utilizar distintos números de colas por interfaz.
QFM.5	{texto informativo: La QFM hace corresponder el TrafficImportanceNumber UPnP del paquete a la prioridad de encolamiento de IPCable2Home de acuerdo con la correspondencia definida.}
QFM.6	La QFM puede proporcionar acceso a los medios compartidos en cada interfaz LAN, mediante prioridades, conforme a la prioridad de los paquetes y las capacidades de acceso a los medios con prioridad de la interfaz LAN.
QFM.7	{texto informativo: La QFM hace corresponder el TrafficImportanceNumber de UPnP del paquete a la prioridad de acceso a los medios de IPCable2Home conforme a la correspondencia definida.}
QFM.8	La QFM debería poder utilizar interfaces que acepten distintos números de prioridades para el acceso a los medios.

10.3.1.1.3 Hipótesis sobre el diseño de la retransmisión y acceso a los medios con QoS

- Cada interfaz LAN del PS puede soportar menos de ocho colas.
- El número máximo de colas soportadas por una interfaz LAN del PS es ocho.

- Cada tecnología de funcionamiento en red LAN del PS puede soportar menos de ocho prioridades de acceso a los medios.
- El número máximo de prioridades de acceso a los medios soportadas por una tecnología de funcionamiento en red LAN del PS es ocho.

10.3.1.1.4 Descripción del sistema de retransmisión y acceso a los medios con QoS

La QFM ofrece un mecanismo al PS para ordenar y transmitir los paquetes en una interfaz LAN de salida de acuerdo con las prioridades asignadas. Gracias a la asignación de prioridades a los paquetes y a la acción de la QFM, los paquetes que pasan a través del PS hacia la red LAN doméstica disponen de acceso con prioridad a los medios compartidos de la LAN. La QFM es responsable de las tres funciones siguientes.

1) {texto informativo: Proceso de clasificación para identificar el número de importancia del tráfico (TIN) UPnP del paquete.}
2) encolamiento con prioridad;
3) acceso a los medios con prioridad.

{texto informativo:

10.3.1.1.4.1 Clasificación de los paquetes para identificar el TrafficImportanceNumber UPnP

Los paquetes que pasan a través del PS y destinados a la interfaz de la LAN, pueden tener su origen en la WAN (tráfico WAN-LAN descendente) o en otra interfaz LAN del PS (tráfico LAN-LAN interno doméstico). Para el tráfico LAN-LAN interno doméstico, la QFM puede realizar opcionalmente la clasificación de paquetes. Sin embargo, para tráfico WAN-LAN descendente, la QFM debe realizar la clasificación de paquetes para determinar el UportanceNumber (TIN) adecuado si la interfaz LAN de salida soporta varias colas o varias prioridades.

A fin de realizar la clasificación de los paquetes, el PS examina el paquete para poder identificar el TrafficImportanceNumber UPnP del mismo. El PS examina la IP de origen, el puerto de origen, la IP de destino, el puerto de destino y el tipo de protocolo del paquete, e intenta encontrar una primera concordancia en los cuadros clasificadores almacenados en la base de datos del PS representados mediante la MIB cabhQos2TrafficClassTable (anexo A). Si el PS encuentra una anotación que concuerde, utiliza el valor de cabhQos2TrafficClassImpNum MIB correspondiente a dicha anotación como TrafficImportanceNumber UPnP del paquete. Si no se encuentra una anotación que concuerde, el PS asigna al paquete un TrafficImportanceNumber UPnP de valor 0. El PS utiliza este número de importancia del tráfico UPnP para determinar la prioridad de encolamiento IPCable2Home del paquete y la prioridad de acceso a los medios IPCable2Home.

10.3.1.1.4.2 Encolamiento con prioridad

Existe la posibilidad de que el número de colas soportadas por una interfaz en el PS, al que se destina el paquete, no sea el mismo que los ocho niveles de TrafficImportanceNumber UPnP. Por lo tanto, el PS hace corresponder el valor del TrafficImportanceNumber UPnP al valor de la prioridad de encolamiento de IPCable2Home tal como se define en [802.1D], anexo G. A continuación el PS coloca el paquete en una cola adecuada de la interfaz de destino que corresponde a dicho valor de prioridad de encolamiento de IPCable2Home.

La QFM interroga a todas las colas de cada interfaz saliente conforme a sus prioridades a fin de extraer los paquetes que se van a transmitir por los medios compartidos. Cada vez que la QFM va a extraer un paquete de las colas de una interfaz PS particular, comienza siempre su interrogación en primer lugar con la cola que tiene la prioridad más alta. Si esta última no tiene paquetes para transmitir, la QFM interroga a la siguiente cola con la prioridad más alta del resto de las colas en la jerarquía hasta que encuentra un paquete que tenga que transmitirse en una de las colas. Los paquetes se extraen de cada cola en el orden en que llegaron. Por lo tanto, el método de colas que

utiliza la QFM puede describirse como primero en entrar, primero en salir, con prioridades, atendiendo en primer lugar la cola con la prioridad más alta.

10.3.1.1.4.3 Acceso a los medios con prioridad

Cuando la QFM extrae un paquete del conjunto de colas de una interfaz, el paquete debe transmitirse por el medio compartido de la LAN con una prioridad adecuada. Por consiguiente, la QFM hace corresponder el valor del número de importancia del tráfico UPnP del paquete con el valor de la prioridad de acceso a los medios de IPCable2Home, tal como se define en [802.1D], anexo G. Este valor determina el nivel de preferencia que debería utilizar el paquete para acceder a los medios compartidos. Por esa razón, los fabricantes deben garantizar que se mantienen las preferencias relativas de acceso a los medios como lo exigen los valores de la prioridad de acceso a los medios de IPCable2Home, cuando se transmiten los paquetes por los medios compartidos de la red LAN.

}

10.3.1.1.4.4 Soporte de las aplicaciones de IPCablecom

Dado que el objetivo en términos de QoS es ofrecer calidad de servicio sólo en la red doméstica, esta Recomendación no tiene en cuenta de forma específica la QoS de la red de acceso. No obstante, esta Recomendación permite que las aplicaciones de la red doméstica puedan establecer sesiones de datos con prioridad entre el CMTS y el dispositivo de la pasarela residencial IPCable2Home, utilizando mensajes conformes con IPCablecom, tal como se especifica en la Rec. UIT-T J.191. Por lo tanto, los requisitos necesarios para soportar esta funcionalidad en el PS están incluidos en las especificaciones de QoS, de la misma forma que en la Rec. UIT-T J.191.

El PS actúa como puente transparente y retransmite los mensajes con QoS de IPCablecom entre el CMTS y las aplicaciones IPCablecom. Los datos de la aplicación están asociados con un flujo de servicio DOCSIS de acuerdo a un clasificador creado en la interfaz del CM, en función de la información de los mensajes IPCablecom (tal como RSVP PATH).

Dado que el requisito del PS es retransmitir los mensajes con QoS de IPCablecom, el hecho de soportar esa función no dependerá del NMS. Por consiguiente, esta función CQP es la misma para los dos modos de configuración DHCP y SNMP (véase 5.5).

Los mensajes con QoS de IPCable2Home sobre la red de acceso o red HFC se definen en las Recs. UIT-T J.161 y J.163 relativas a IPCablecom. La gestión de las políticas de QoS de IPCable2Home y las funciones de control de admisión para la QoS de la red de acceso también se definen en las Recs. UIT-T J.161 y J.163.

10.3.1.1.5 Requisitos de la retransmisión y el acceso a medios con QoS

10.3.1.1.5.1 Requisitos de la clasificación de paquetes

El PS PUEDE realizar la clasificación de los paquetes del tráfico LAN-LAN.

Si en el caso del tráfico de WAN a LAN una interfaz LAN de salida implementa varias colas o prioridades, el PS DEBE clasificar los paquetes.

A fin de clasificar los paquetes, el PS DEBE tomar las acciones siguientes:

1) El PS DEBE examinar la dirección IP de origen y de destino, el puerto de origen y de destino y el tipo de protocolo del paquete, y buscar una primera anotación concordante (es decir, con el número índice más bajo) en el cuadro clasificador del PS, (cabhQos2TrafficClassTable) almacenado en la base de datos del PS (véase el anexo A).
2) {texto informativo: El PS DEBE utilizar como número de importancia del tráfico UPnP de dicho paquete el valor de la MIB cabhQos2TrafficClassImpNum de la anotación que concuerde.

3) Si en el cuadro de clasificación no se encuentra ninguna anotación que concuerde, el PS DEBE asignar al paquete el número 0 de importancia del tráfico UPnP.

}

10.3.1.1.5.2 Requisitos del encolamiento con prioridad

{texto informativo:

El PS DEBE almacenar en la base de datos del PS el número de colas implementadas por cada una de sus interfaces presentes en la base de datos del PS, información a la que puede accederse a través de una MIB cabhQos2PsIfAttribIfNumQueues [véase E.7].

El PS DEBE hacer corresponder el valor del número de importancia del tráfico UPnP del paquete identificado durante el proceso de clasificación con el valor de la prioridad de encolamiento de IPCable2Home tal como se especifica en [802.1D], anexo G, utilizando el número de colas cabhQos2PsIfAttribIfNumQueues) [véase E.7] implementadas en la interfaz a través de la que se transmite el paquete. El PS DEBE poner correctamente el paquete en la cola de interfaz de destino de acuerdo con el valor de prioridad de encolamiento de IPCable2Home para el que se haya establecido la correspondencia.

El PS DEBE interrogar varias colas en cada una de las interfaces LAN conforme a sus prioridades para extraer los paquetes que han de transmitirse por el medio compartido. Cada vez que el PS tiene que extraer un paquete de las distintas colas de una interfaz particular, el PS DEBE comenzar su interrogación siempre con la cola que tenga la prioridad más alta en primer lugar. Si esta última no tiene paquetes que deban transmitirse, el PS DEBE interrogar la siguiente cola con la prioridad más alta del resto de las colas en la jerarquía, hasta que encuentre el siguiente paquete disponible con la prioridad más alta que deba transmitirse. En todos los casos, el PS DEBE extraer los paquetes de cada cola en el orden en que se reciben.

10.3.1.1.5.3 Requisitos del acceso al medio con prioridad

El PS DEBE almacenar el número de prioridades de acceso a los medios de capa 2 nativas que soportan cada una de sus interfaces en la base de datos del PS a la que puede accederse a través de una MIB cabhQos2PsIfAttribIfNumPriorities [véase E.7].

Después de que el paquete se extrae de las colas de una interfaz particular, el PS DEBE establecer una correspondencia entre el número de importancia del tráfico UPnP del paquete y las prioridades de acceso a los medios de IPCable2Home, tal como se define en [802.1D], anexo G, utilizando el número de prioridades de acceso a los medios (cabhQos2PsIfAttribIfNumPriorities) que soporta esa interfaz. El PS DEBE transmitir el paquete mediante la tecnología de medios compartidos de modo que se mantenga el acceso preferencial de los medios, de acuerdo con el valor de prioridad de acceso a medios de IPCable2Home.

}

10.3.1.1.5.4 Requisitos del soporte de aplicaciones de IPCablecom

El PS DEBE comportarse como un puente transparente y retransmitir los mensajes de QoS de IPCablecom [Rec. UIT-T J.161], [Rec. UIT-T J.163] entre el CMTS y las aplicaciones de IPCablecom. Los datos de la aplicación se asocian a un flujo de servicio del CM de acuerdo con un clasificador que se crea en la interfaz del CM, basándose en la información incluida en los mensajes de IPCablecom (tales como RSVP PATH).

Como el requisito del PS para IPCable2Home es simplemente retransmitir los mensajes de QoS de IPCablecom, no hay dependencia del NMS para soportar esta función. Por lo tanto, esta función CQP se mantiene idéntica para ambos modos de configuración DHCP y SNMP (véase 5.5).

{texto informativo:

10.3.1.2 Interfaz de servicio del dispositivo con QoS UPnP (QDS)

10.3.1.2.1 Objetivos de la interfaz de servicio del dispositivo con QoS UPnP

Los objetivos de la interfaz de servicio del dispositivo con QoS UPnP son:

- Proporcionar una interfaz para que un servicio gestor de la QoS UPnP establezca la QoS de la red doméstica en las interfaces LAN del PS CableHome.
- Proporcionar una interfaz en un PS CableHome para detectar la necesidad de QoS en la red de acceso para una sesión que se extienda por la red de acceso y por la red doméstica.

10.3.1.2.2 Directrices de diseño de la interfaz de servicio del dispositivo con QoS UPnP

Véase el cuadro 10.4.

Cuadro 10-4/J.192 – Directrices de diseño de la interfaz de servicio del dispositivo con QoS UPnP

Número	Directrices
QDS.1	El QDS proporciona una interfaz para que una entidad de gestión de QoS UPnP establezca la QoS de la red doméstica en el PS CableHome
QDS.2	El QDS establece clasificadores de paquetes en el PS CableHome.
QDS.3	El QDS detecta la necesidad de negociación de la QoS de la red de acceso para una sesión.

10.3.1.2.3 Hipótesis relativas a la interfaz de servicio de dispositivos con QoS UPnP

Los puntos de control de la LAN doméstica pueden utilizar la entidad de gestión de QoS en la LAN doméstica (UQM) que no forme parte del PS CableHome para establecer la QoS.

10.3.1.2.4 Descripción de la interfaz de servicio del dispositivo con QoS UPnP

El PS CableHome puede implementar opcionalmente una interfaz de servicio de dispositivo con QoS UPnP (UQD) en el lado de la LAN. Si se implementa, el servicio del dispositivo con QoS UPnP se anuncia como parte del dispositivo raíz del PS CableHome. El servicio del dispositivo con QoS UPnP proporciona una interfaz de forma que la entidad de gestión de la QoS UPnP de la LAN pueda configurar el PS CableHome con los valores adecuados de QoS. Cuando una entidad de gestión de la QoS UPnP invoca una acción SetUpTrafficQoS relativa a la QoS del PS CableHome, éste establece clasificadores de paquetes utilizando la información del TrafficDescriptor UPnP que se pasa como argumento de entrada de la acción. La QFM utiliza dichos clasificadores para clasificar los paquetes. Si una dirección IP de origen o de destino del TrafficDescriptor UPnP reside en la WAN, el PS CableHome detecta que es necesario establecer una QoS en la red de acceso para dicha sesión.

10.3.1.2.5 Requisitos de la interfaz de servicio del dispositivo con QoS UPnP

El PS PUEDE implementar un servicio del dispositivo con QoS UPnP (UQD).

Si el PS implementa un servicio del dispositivo con QoS UPnP, debe cumplir los requisitos siguientes.

El PS DEBE anunciar el servicio del dispositivo con QoS UPnP como un servicio integrado en el dispositivo raíz del PS CableHome.

El PS DEBE poder procesar la acción GetQoSCapabilities del servicio del dispositivo con QoS UPnP. Cuando se recibe esta acción, el PS DEBE devolver EXCLUSIVAMENTE los atributos de sus interfaces en el lado LAN representados por la MIB ifTable en el argumento de salida QoSDeviceCapabilities de la acción, tal como se representa en el cuadro 10-5.

Cuadro 10-5/J.192 – Valores de la MIB ifTable y de la variable de estado QoSDeviceCapabilities UPnP

Valores de la MIB IfTable	Valores XML de la variable de estado QoSDeviceCapabilities UPnP
IfIndex	InterfaceId
IfPhysAddress	MacAddress
IfType	IanaTechnologyType
IfSpeed	MaxPhyRate

El PS DEBE poder procesar la acción GetQosState del servicio del dispositivo con QoS UPnP. Cuando se recibe esta acción, el PS DEBE devolver todos los clasificadores de paquetes representados por la MIB cabhQos2TrafficClassTable, en el argumento de salida XML ListOfTrafficDescriptors y el número total de clasificadores de paquetes en el argumento de salida NumberOfTrafficDescriptors. El PS también DEBE devolver QoSStateId como un argumento de salida.

El PS DEBE soportar la acción SetupTrafficQos del servicio del dispositivo con QoS UPnP. Cuando se recibe esta acción, el PS DEBE utilizar el argumento de entrada SetupTrafficDescriptor para establecer un clasificador de paquetes en la base de datos del PS que sea accesible mediante la MIB cabhQos2TrafficClassTable del PS.

El PS DEBE soportar la recepción de la acción ReleaseTrafficQos del servicio del dispositivo con QoS UPnP. Cuando se recibe esta acción, el PS DEBE suprimir la anotación del clasificador de paquetes almacenada en su base de datos e identificada mediante el argumento de entrada ReleaseTrafficHandle de la acción.

}

{texto informativo:

10.3.2 Servidor de política de QoS del PS (QPS)

El servidor de política de QoS (QPS) del PS actúa como un repositorio de política de QoS de la red doméstica establecida por el operador de cable y el usuario doméstico. El QPS tiene una interfaz SNMP en el lado WAN para que los operadores de cable gestionen las políticas de QoS. En el lado LAN, el QPS tiene una interfaz del servicio tenedor de política de QoS UPnP (UQPH) para comunicar las políticas de QoS a petición de una entidad gestora de la QoS UPnP. El QPS puede tener también una interfaz LAN no especificada que permita a los usuarios domésticos gestionar políticas de QoS por sí mismos. En esta cláusula se presenta la descripción de la funcionalidad de QPS y de los requisitos del PS asociados.

10.3.2.1 Objetivos del servidor de política de QoS

- Establecer un conjunto de criterios mediante los cuales las aplicaciones y servicios puedan solicitar y utilizar políticas de QoS para el tráfico en la red doméstica.
- Permitir al operador de cable y al usuario configurar políticas de QoS en el PS de IPCable2Home.
- Ofrecer un mecanismo para que la red de datos de cable comunique las políticas de QoS deseadas al PS y a continuación a los dispositivos conformes con la QoS UPnP mediante cualquier gestor de QoS de la red doméstica.

10.3.2.2 Directrices de diseño del servidor de política de QoS

Véase el cuadro 10-6.

Cuadro 10-6/J.192 – Directrices de diseño del QCS

Número	Directrices
QPS.1	El QPS debe recibir información de la política de QoS del servidor de gestión de red (NMS) situado en la cabecera de la red y del usuario doméstico en el lado LAN.
QPS.2	La cabecera y el usuario situado en el hogar podrán actualizar la información de la política de QoS suministrada al QPS. La información actualizada sólo se obtiene cuando un gestor de QoS hace una solicitud.
QPS.3	La información de política de QoS suministrada al QPS desde la cabecera de la red puede contener reglas de política que no pueden ser actualizadas por un usuario doméstico (HomeUser). El QPS utilizará mensajes UPnP.
QPS.4	El QPS debe utilizar una interfaz de contenido de mensaje definida (MIB) para proporcionar información de diversas aplicaciones en la red LAN doméstica al servidor de gestión de la red (NMS) de la cabecera.

10.3.2.3 Hipótesis relativas al servidor de política de QoS

IPCable2Home utiliza mensajes de QoS UPnP para el intercambio de información sobre política de QoS entre el PS y anfitriones UPnP de entidades con QoS conformes con UPnP y que pueden tener más de un servicio o aplicación definidos.

10.3.2.4 Descripción del sistema del servidor de política de QoS

El QPS mantiene una base de datos de políticas de QoS del tráfico en el PS. El QPS puede recibir información de reglas relativas a la política desde la cabecera de la red, a través de la descarga del fichero de configuración inicial del PS, o a través de una interfaz MIB en el CMP. El QPS también puede recibir información de reglas sobre la política desde el usuario doméstico a través de una interfaz LAN (como por ejemplo, un servidor HTTP) no especificada en CableHome 1.1, que también debe estar presente en la base de datos de políticas de tráfico del QPS. El QPS comunicará la información sobre política a cualquier gestor de QoS UPnP (UQM) cuando las aplicaciones o servicios en la LAN soliciten su utilización para el acceso con prioridad a los medios.

10.3.2.4.1 Intercambio de información de la WAN

Desde el lado de la red WAN, la cabecera del operador del sistema de cable proporciona al PS las políticas de QoS de tráfico en un fichero de configuración del PS o empleando una interfaz MIB SNMP. El NMS, en la cabecera, puede leer y actualizar (cambiar/modificar/suprimir) estas políticas de QoS de tráfico de la base de datos del PS mediante una interfaz MIB SNMP.

10.3.2.4.1.1 Envío al PS de información de política de QoS de IPCable2Home de la WAN

La cabecera proporciona al PS una lista ordenada de políticas de QoS de tráfico que el operador de cable desea que utilicen las aplicaciones y servicios. Esta información se suministra al PS a través de un fichero de configuración en el momento de la inicialización del PS o a través de instrucciones SNMP SET desde la cabecera. El PS almacena esta información en su base de datos a la que puede accederse a través del cuadro MIB cabhQos2PolicyTable.

El PS también puede recibir peticiones del NMS para actualizar (añadir/modificar/suprimir) estas políticas de QoS de tráfico para aplicaciones y servicios existentes en su cuadro de política utilizando SNMP. En respuesta a esas peticiones, el PS actualiza (añade/modifica/suprime) la información sobre política incluida en la base de datos del PS accesible mediante la MIB cabhQos2PolicyTable y utilizando una interfaz SNMP. Véase la figura 10-3.

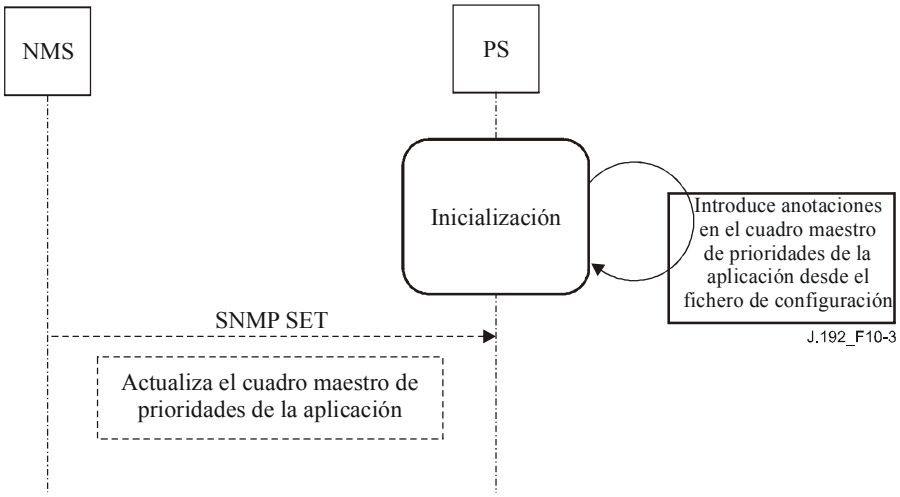


Figura 10-3/J.192 – Intercambio y procesamiento de información de la WAN en el PS

10.3.2.4.2 Interfaz del servicio tenedor de política de QoS UPnP (QPH) para LAN

En el lado de la LAN, el servicio tenedor de políticas de QoS UPnP (QPH, *QoS policy holder*) presenta una interfaz directa con cualquier gestor de QoS UPnP para la adquisición de la política de tráfico para un descriptor de tráfico específico. En respuesta a una petición de política de tráfico del gestor de QoS UPnP, el servicio QPH devuelve los valores de TrafficImportanceNumber, UserImportanceNumber y AdmissionPolicyEnabled del correspondiente descriptor de tráfico. Si no se encuentra una concordancia, el QPS devuelve el valor 0 para TrafficImportance Number y para UserImportanceNumber.

10.3.2.5 Requisitos del servidor de política de QoS

10.3.2.5.1 Requisitos del intercambio de información de la WAN

El PS DEBE almacenar en la base de datos del PS una relación de políticas de tráfico proporcionadas por el operador de cable, a la que puede accederse a través de la interfaz MIB SNMP cabhQos2PolicyTable. El PS DEBE soportar actualizaciones (añadir/modificar/suprimir) de esta cabhQos2PolicyTable a través de un fichero de configuración en el momento de la inicialización del PS, o a través de instrucciones SNMP SET desde la cabecera.

10.3.2.5.2 Requisitos del servicio QPH UPnP

El PS DEBE soportar al menos (32) anotaciones en la fila 'operatorOnly' de cabhQos2PolicyTable.

El PS DEBE soportar al menos (32) anotaciones en la fila 'homeUser' de cabhQos2PolicyTable.

El PS DEBE soportar al menos (32) anotaciones en la fila 'operatorForHomeUser' de cabhQos2PolicyTable.

El PS DEBE soportar la acción 'GetTrafficPolicy' del servicio tenedor de política de QoS UPnP (UQPH).

En respuesta a una acción GetTrafficPolicy del servicio QPH UPnP, el PS DEBE realizar las acciones siguientes.

1) El PS DEBE encontrar la primera concordancia de la regla de política de QoS en la cabhQos2PolicyTable. El PS DEBE procesar las reglas basadas en el índice del cuadro SNMP y en la MIB cabhQos2PolicyRuleOrder. Es decir, el PS DEBE procesar en primer lugar todas las anotaciones de fila que sean cabhQos2PolicyTable:'operatorOnly', seguidas de las anotaciones 'homeUser', y finalmente las anotaciones 'operatorForHomeUser'.

Además, de entre dichas anotaciones de "propietario" individual, el PS procesa aquellas con el valor numérico más bajo de cabhQos2PolicyRuleOrder.

2) Una vez que el PS encuentra en cabhQos2PolicyTable una primera anotación de fila concordante, DEBE devolver el valor de la MIB cabhQos2PolicyTraffImpNum (véase E.7) como argumento de salida "trafficImportanceNumber" de la acción GetTrafficPolicy.

3) El PS DEBE devolver también el valor del objeto MIB cabhQos2PolicyAdmissionPolicyEnable como un argumento de salida admissionPolicyEnable de la acción GetTrafficPolicy.

4) El PS DEBE devolver también el valor del objeto MIB cabhQos2PolicyUserImportanceNumber como argumento de salida "userImportanceNumber" de la acción GetTrafficPolicy.

5) Si no se encuentra una anotación concordante en el cuadro de política, el PS DEBE devolver el valor 0 para los argumentos de salida "trafficImportanceNumber" y "userImportanceNumber". En ese caso, el PS DEBE devolver el valor del objeto MIB cabhQos2PolicyAdmissionPolicyEnable como argumento de salida admissionPolicyEnable de la acción GetTrafficPolicy. Además, DEBE crear una anotación de regla de política de tráfico del tipo "UPnP" en la MIB cabhQos2PolicyTable con el descriptor de tráfico UPnP transmitido en la acción GetTrafficPolicy. Para dicha anotación, el PS DEBE poner a 0 el cabhQosPolicyTraffImpNum. El usuario o el operador pueden modificar dichas anotaciones, y en ese caso, el PS DEBE modificar la anotación a "homeUser" u "operatorForHomeUser", respectivamente. El PS NO DEBE cambiar las anotaciones del tipo "upnp" a "operatorOnly".}

{texto informativo:

10.3.3 Servicio gestor de QoS UPnP (QM)

10.3.3.1 Objetivos del servicio gestor de QoS UPnP

Garantizar que existe al menos un servicio gestor de QoS UPnP para puntos de control que sean conformes con UPnP y que soliciten QoS en la LAN doméstica.

10.3.3.2 Directrices de diseño del servicio gestor de QoS UPnP

El CQP implementa la funcionalidad completa de gestor de QoS UPnP en cada UQM.

10.3.3.3 Hipótesis del servicio gestor de QoS UPnP

En la LAN doméstica pueden existir otros gestores de QoS UPnP.

10.3.3.4 Descripción del sistema del servicio gestor de QoS UPnP

El PS implementa el servicio gestor de QoS UPnP exactamente como se define en UQM. El servicio gestor de QoS UPnP del PS no tiene una interfaz o controlabilidad con la WAN dado que es autónomo.

10.3.3.5 Requisitos del servicio gestor de QoS UPnP

El PS DEBE implementar la funcionalidad gestor de QoS UPnP para cada UQM.

El PS DEBE anunciar el servicio gestor de QoS UPnP como parte del dispositivo raíz del PS CableHome.

El PS DEBE soportar la acción RequestTrafficQos del servicio gestor de QoS UPnP.

Cuando un punto de control de UPnP invoca la acción QM:RequestTrafficQos del PS, éste DEBE hacer lo siguiente:

1) Tal como ocurre para UQM, si el PS encuentra varios ejemplares del servicio tenedor de política de QoS UPnP, DEBE utilizar el cuadro de política por defecto del gestor de QoS UPnP y DEBE devolver el TrafficImportanceNumber de UPnP en función de dicho cuadro por defecto.

2) Si el PS encuentra que sólo el servicio tenedor de política de QoS UPnP reside en el PS, éste DEBE utilizar los valores de TrafficImportanceNumber, UserImportanceNumber y AdmissionPolicyEnable de UPnP extraídos de la MIB cabhQosPolicyTable cuando se invoca la acción QD:SetUpTrafficQos sobre varios ejemplares del servicio de dispositivo con QoS UPnP en la LAN.

3) Si el servicio tenedor de política de QoS del PS está inhabilitado y el PS encuentra un único tenedor de política de QoS UPnP externo al PS, éste DEBE solicitar la acción QPH:GetTrafficPolicy a dicho servicio tenedor de políticas de QoS y DEBE utilizar los valores devueltos de TrafficImportanceNumber, UserImportanceNumber y AdmissionPolicyEnable UPnP.

4) El PS PUEDE hacer una llamada a la acción QD:GetPathInformation sobre ejemplares del servicio de dispositivo con QoS (UQD) en la LAN.

5) Para distribuir el TrafficImportanceNumber (número de importancia del tráfico) UPnP, el PS DEBE invocar la acción QD:SetUpTrafficQos sobre el ejemplar del servicio de dispositivo con QoS en el origen, y PUEDE invocar la acción QD:SetUpTrafficQos sobre otros ejemplares del servicio de dispositivo con QoS en la LAN.

El PS DEBE soportar la acción UpdateTrafficQos del servicio gestor de QoS UPnP.

Cuando un punto de control UPnP invoca la acción QM:UpdateTrafficQos del PS, éste DEBE realizar lo siguiente:

1) El PS DEBE, en primer lugar, invocar la acción QD:ReleaseTrafficQos sobre el ejemplar del servicio de dispositivo con QoS en el origen y PUEDE invocar la acción QD:ReleaseTrafficQos sobre otros ejemplares del servicio de dispositivo con QoS en la LAN.

2) El PS DEBE invocar entonces a QD:SetUpTrafficQos sobre el ejemplar del servicio de dispositivo con QoS en el origen y PUEDE invocar QD:SetUpTrafficQos sobre los ejemplares del servicio de dispositivo con QoS en el trayecto con el descriptor de tráfico actualizado que proporciona el punto de control en la acción QM:UpdateTrafficQos.

El PS DEBE soportar la acción ReleaseTrafficQos del servicio gestor de QoS UPnP.

Cuando un punto de control UPnP invoca la acción QM:ReleaseTrafficQos sobre el PS, éste DEBE invocar la acción QD:ReleaseTrafficQos sobre el ejemplar de servicio del dispositivo con QoS de origen y PUEDE solicitarlo para otros ejemplares del servicio de dispositivo con QoS de la LAN.

El PS DEBE soportar la acción BrowseAllTrafficDescriptors del gestor de QoS UPnP.

Cuando un punto de control UPnP invoca la acción QM:BrowseAllTrafficDescriptors sobre el PS, éste DEBE invocar la acción GetQosState sobre todos los ejemplares conocidos de servicio de dispositivos con calidad, y devolver la información al punto de control.

10.3.4 Funcionalidad de QoS del punto de control del PS (QCP)

La funcionalidad de QoS del punto de control del PS (QCP) actúa como punto de control para todos los ejemplares de servicio con QoS UPnP en la red doméstica. Realiza las funciones asociadas a un punto de control para la determinación, descripción y control del dispositivo y el servicio. Otra función importante del punto de control de QoS del PS es implementar la lógica para el establecimiento de QoS en la red de acceso en respuesta a peticiones de QoS de la red doméstica realizadas a través de QoS UPnP; y establecer QoS en la red doméstica en respuesta a peticiones de QoS de la red de acceso realizadas a través de la interfaz CH-PCMM.

10.3.4.1 Objetivos de la funcionalidad de QoS del punto de control del PS

- Permitir que los operadores de cable puedan recopilar información sobre diversos dispositivos y servicios UPnP con capacidad de QoS en la LAN doméstica.
- Permitir que el PS CableHome solicite QoS en la red doméstica utilizando mensajes de QoS UPnP.

10.3.4.2 Directrices de diseño del sistema de la funcionalidad de QoS del punto de control del PS

Véase el cuadro 10-7.

Cuadro 10-7/J.192 – Directrices de diseño del sistema de la funcionalidad de QoS del punto de control del PS

Número	Directrices
QPSCP.1	El punto de control del PS implementará un control lógico coherente con la QoS UPnP.
QPSCP.2	El punto de control del PS puede implementar la inteligencia necesaria para solicitar QoS en la LAN (mediante la QoS UPnP) en respuesta a una petición de QoS en la red de acceso realizada a través de la interfaz PCMM.

10.3.4.3 Hipótesis sobre la funcionalidad de QoS del punto de control del PS

La LAN doméstica consta de dispositivos anfitriones UPnP que implementan una funcionalidad de QoS coherente con la QoS-UPnP.

10.3.4.4 Descripción del sistema de funcionalidad de QoS del punto de control del PS

La funcionalidad de QoS del punto de control del PS tiene los componentes siguientes:

- Lógica de determinación de la QoS.
- Lógica del intermediario de QoS de CableHome.

10.3.4.4.1 Lógica de determinación de la QoS

La lógica de determinación de la QoS es responsable de la determinación y descripción de todas las entidades con QoS UPnP en la LAN doméstica.

El punto de control del PS actúa como un punto de control UPnP responsable de la determinación, descripción, control, etc., tal como establece la arquitectura de dispositivos 1.0 UPnP (UDA 1.0). La funcionalidad de QoS del punto de control del PS es específicamente responsable de ejecutar las invocaciones de las acciones de QoS UPnP que sean necesarias sobre los ejemplares de servicio con QoS UPnP de la red doméstica.

CableHome define la MIB cabhPsDevUpnpCommandUpdate para pedir al PS que actualice su cabhPsDevUpnpInfoTable según las restricciones especificadas en cabhPsDevUpnpInfoIp y cabhPsDevUpnpCommand.

Si la MIB cabhPsDevUpnpCommand se fija como qosDeviceCapabilities y cabhPsDevUpnpCommandUpdate se fija como verdadero, la funcionalidad de punto de control de QoS del PS invoca la acción QD:GetQosCapabilities sobre la dirección IP especificada en cabhPsDevUpnpInfoIp. El PS almacena información sobre la capacidad del dispositivo que devuelve el dispositivo con QoS en la base de datos del PS, información que es accesible a través de la MIB cabhPsDevUpnpInfoTable.

Si la MIB cabhPsDevUpnpCommand se fija como qosDeviceState y cabhPsDevUpnpCommandUpdate se fija como verdadero, la funcionalidad de QoS del punto de control del PS invoca la acción QD:GetQosState() sobre la dirección IP especificada en cabhPsDevUpnpCommandIp. El PS almacena información sobre la capacidad del dispositivo

devuelta por el dispositivo con QoS en la base de datos del PS, y que es accesible a través de la MIB cabhPsDevUpnpInfoTable.

10.3.4.4.2 Lógica del intermediario de QoS de CableHome

La lógica del intermediario de QoS de CableHome del punto de control del PS es responsable de fijar la QoS en la red doméstica como respuesta a una petición realizada desde la interfaz CH-PCMM.

Tal como se explica en 10.2, Arquitectura de QoS, la entidad intermediaria de QoS de CableHome puede implementar una interfaz CH-PCMM en el lado de la WAN para negociar la QoS en la red de acceso de flujos que circulen por la red doméstica y por la red de acceso. El PS puede recibir una petición de QoS para la red doméstica desde la interfaz CH-PCMM. El punto de control del PS es responsable de establecer la QoS en la red doméstica en respuesta a dicha petición. Debe observarse que los requisitos actuales de la interfaz CH-PCMM y del establecimiento de QoS en la red doméstica en respuesta a peticiones desde la interfaz CH-PCMM se definirán en futuras especificaciones de CableHome.

10.3.4.5 Requisitos de la funcionalidad de QoS del punto de control del PS

1) Cuando la MIB cabhPsDevUpnpCommand [véase E.4] se fija como qosDeviceCapabilities y cabhPsDevUpnpCommandUpdate [véase E.4] se fija como verdadero, el PS DEBE invocar la acción QD:GetQosCapabilities() sobre la dirección IP especificada en cabhPsDevUpnpInfoIp [véase E.4].
2) El PS DEBE almacenar la información sobre la capacidad del dispositivo que devuelve el dispositivo con QoS en respuesta a la acción QD:GetQosCapabilities() en la base de datos del PS, información que es accesible mediante la MIB cabhPsDevUpnpInfoTable [véase E.4].
3) Cuando la MIB cabhPsUpnpCommand se fija como qosDeviceState y cabhPsDevUpnpCommandUpdate se fija como verdadero, el PS DEBE invocar la acción QD:GetQosState() sobre la dirección IP especificada en cabhPsDevUpnpInfoIp.

El PS DEBE almacenar la información sobre la capacidad del dispositivo que devuelve el dispositivo con QoS en respuesta a la acción QD:GetQosCapabilities() en la base de datos del PS, información que es accesible mediante la MIB cabhPsDevUpnpInfoTable.}

11 Seguridad

11.1 Introducción y generalidades

En esta cláusula se definen las interfaces, los protocolos y los requisitos funcionales de seguridad necesarios para proteger el PS y sus funciones.

Para poder garantizar la distribución de servicios IP multimedia fiables a dispositivos de cliente en una red doméstica, se necesita una pasarela residencial segura con mecanismos de seguridad que permitan proteger dichos servicios contra el acceso, la supervisión y la interrupción ilegales. Toda tecnología de seguridad tiene como fin proteger valores, por ejemplo en los servicios pagados. Se presentan amenazas a los trenes de estos últimos servicios siempre que un usuario de una red percibe el valor, invierte esfuerzo y dinero, e inventa una técnica para no tener que hacer los pagos necesarios (véase el anexo C). Algunos usuarios de red pueden llegar hasta extremos inesperados cuando perciben que es posible robar algún valor. Añadir una tecnología de seguridad a fin de proteger valores tiene un costo asociado, a saber, cuanto más dinero se gaste mayor será la seguridad (la eficacia de la seguridad tiene entonces un carácter económico).

La arquitectura de seguridad se centra principalmente en garantizar la seguridad de la LAN contra ataques a la red, así como en asegurar las comunicaciones entre el PS y los servidores de la

cabecera. Gracias a la funcionalidad del PS, es posible establecer la base para la utilización de otras aplicaciones y servicios prestados por el operador de cable a la LAN doméstica. Dichas aplicaciones pueden tener su propia seguridad independientemente de la arquitectura de seguridad de IPCable2Home. IPCablecom especifica interfaces para aplicaciones multimedia y posee su propia arquitectura de seguridad, véase [Rec. UIT-T J.170].

11.1.1 Objetivos

Entre los objetivos del modelo de seguridad se incluyen:

- Emplear una tecnología de seguridad rentable que obligue a todo usuario que intente robar o interrumpir los servicios de red a invertir una cantidad absurda de dinero o tiempo para poder hacerlo.
- Asegurar la red IPCable2Home que se utiliza para ofrecer servicios de alto valor basados en el cable, de tal manera que sea tan segura como las tecnologías CableMÓdem e IPCablecom en la red HFC.
- Lograr la compatibilidad de los mecanismos de seguridad, siempre que sea posible, con las Recomendaciones de seguridad de CableMÓdem e IPCablecom.
- Colaborar con el operador, desde la LAN, en lo que se refiere a una identidad segura que dificulte a un usuario promedio acceder sin autorización a la red HFC y a los servicios basados en el cable.

11.1.2 Hipótesis

Las hipótesis de este entorno de seguridad son:

- Se supone que el PS integrado tiene un módem de cable conforme a J.112 o J.122.
- La seguridad de los servicios de poco valor en la red doméstica es menor.
- No se especifican configuraciones internas y en IPCable2Home se supone que el operador efectúa configuraciones mínimas a fin de funcionar en esos modos.

11.2 Arquitectura de seguridad

La arquitectura de seguridad se basa en la definida en la cláusula 5, Arquitectura de referencia. En ella se define un elemento de servicios de portal (PS), que incluye funciones de gestión, configuración, seguridad y QoS.

De igual manera, la arquitectura incluye el siguiente conjunto de elementos en la cabecera: sistema de terminación de módem de cable (CMTS, *cable modem termination system*), servidor de protocolo dinámico de configuración de anfitrión (DHCP, *dynamic host configuration protocol*) [RFC 2131], sistema de gestión de red, servidor de protocolo trivial de transferencia de ficheros (TFTP) en la red de cable, cliente TFTP en el PS, servidor de protocolo de transferencia de hipertexto (HTTP) en la red de cable, cliente HTTP en el PS, servidor de seguridad de capa de transporte (TLS) [RFC 2246] en la red de cable, cliente TLS en el PS, y servidor de centro de distribución de claves (KDC) en la red de cable.

La arquitectura de seguridad está destinada principalmente a garantizar la seguridad de la LAN contra ataques a la red, así como a asegurar las comunicaciones entre el PS y los servidores de la cabecera.

11.2.1 Directrices de diseño del sistema

En el cuadro 11-1 se enumeran los requisitos de diseño de seguridad que se utilizan en el desarrollo de la arquitectura de seguridad.

Cuadro 11-1/J.192 – Directrices de diseño del sistema de seguridad

Referencia	Directrices
SEC1	Incluye el diseño necesario para comunicar las credenciales de autenticación de los elementos.
SEC2	Se suministran credenciales de autenticación para el PS y los servidores internos cruciales. Estas credenciales han de definir una utilización específica y garantizar una fuente de confianza.
SEC3	Se pueden autenticar los mensajes de gestión de red entre la cabecera de la red de cable y el PS y, facultativamente, criptarlos para protegerlos contra supervisión y control no autorizados.
SEC4	La barrera contra fuegos aceptará ficheros de configuración que tengan un lenguaje y formato normalizados (nota).
SEC5	El operador de cable podrá gestionar a distancia barreras contra fuegos conformes mediante el fichero de configuración o instrucciones SNMP.
SEC6	La barrera contra fuegos incluirá un conjunto de reglas por defecto que permitan obtener la funcionalidad mínima prevista.
SEC7	Provisión del soporte necesario para IPCablecom a través de la barrera contra fuegos.
SEC8	Se establecerá un conjunto mínimo de requisitos en las capacidades de filtrado de la barrera contra fuegos para paquetes, puertos, direcciones IP y hora del día.
SEC9	El operador de cable podrá, gracias a una interfaz de registro detallado de eventos de la barrera contra fuegos, supervisar y revisar la actividad de la barrera contra fuegos, tal como ha sido configurada.
SEC10	La barrera contra fuegos soportará las aplicaciones de uso común en casos específicos.
SEC11	La barrera contra fuegos protegerá la LAN y WAN de ataques comunes a la red.
SEC12	Se definirá en detalle la gestión de los eventos y los conjuntos de reglas para la barrera contra fuegos mediante la MIB de seguridad.
SEC13	El operador de cable podrá descargar con seguridad imágenes de software al elemento PS.
SEC14	El operador de cable podrá autenticar y, facultativamente, criptar el transporte de ficheros de configuración para el PS o la barrera contra fuegos.
NOTA – Los requisitos de fichero de configuración de la barrera contra fuegos se definen en 7.4, Función PS – Configuración de los servicios de portal en bloque (BPSC).	

Si bien esta cláusula se limita al alcance de la arquitectura de seguridad especificada, a fin de satisfacer estos requisitos primarios de seguridad del sistema, se reconoce que en algunos casos puede ser necesario tener seguridad adicional y el operador de cable tiene la potestad de actuar conforme a ello. Puede haber otras protecciones de seguridad provenientes de necesidades particulares de los operadores de cable o de los fabricantes. En esta Recomendación no se restringe el uso de dichas protecciones adicionales, siempre que no generen conflictos con sus objetivos y directrices.

11.2.2 Descripción del sistema

La arquitectura de seguridad incluye los siguientes elementos de seguridad:

- dominio de seguridad;
- función de servicios de portal (PS);
- función del portal de seguridad del cable (CSP, *cable security portal*);
- barrera contra fuegos (FW, *firewall*);
- centro de distribución de claves (KDC);
- servidor HTTPS con TLS.

En la arquitectura se define el elemento PS dentro de una pasarela residencial. Sólo algunas pocas interfaces especificadas tienen seguridad, conforme a las directrices de diseño de sistema. En la figura 11-1 se indica la relación entre los diversos elementos que tienen seguridad.

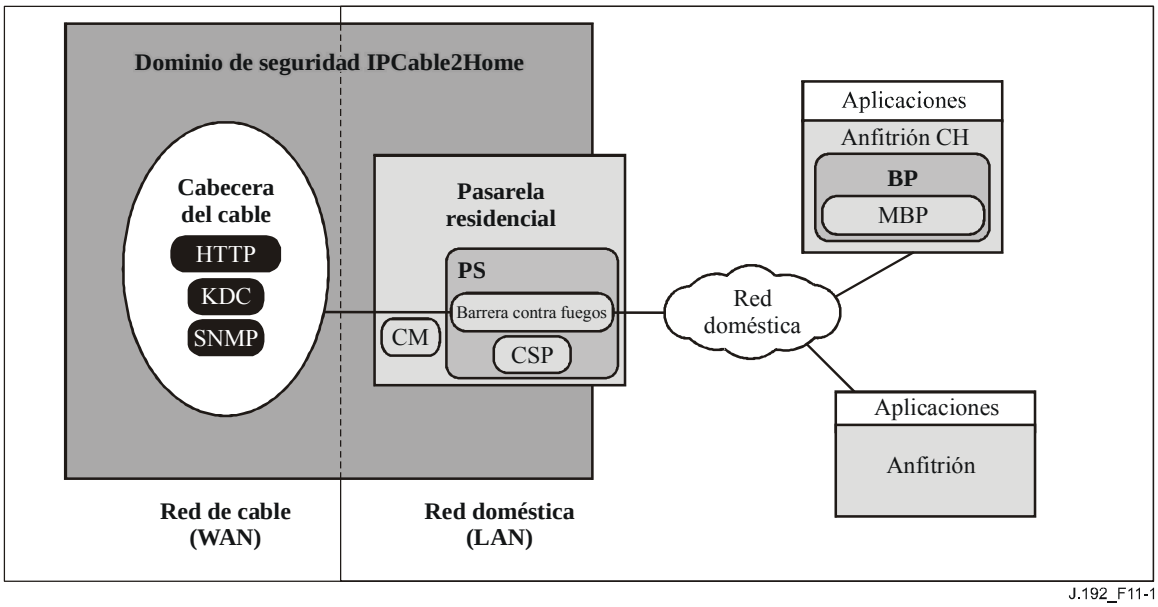


Figura 11-1/J.192 – Elementos de seguridad de IPCable2Home

11.2.2.1 Dominio de seguridad

El dominio de seguridad que se define en la figura 11-1 abarca el elemento PS en la pasarela residencial y los servidores de la cabecera ilustrados, con seguridad específica. En él se define la frontera del ámbito de influencia directa en que la funcionalidad de seguridad se extiende a la pasarela residencial desde la cabecera de la red de cable. El elemento PS se encuentra completamente dentro del dominio de seguridad, salvo por la funcionalidad USFS del lado LAN. El CSP y la barrera contra fuegos funcionan como elementos de frontera entre el dominio de seguridad y el dominio no seguro.

11.2.2.2 Subelementos de seguridad relacionados con el PS

El PS incluye los siguientes elementos de seguridad:

- portal de seguridad del cable (CSP)
- barrera contra fuegos (FW)

El CSP funciona como un portal de seguridad para otros subelementos del PS, por ejemplo, al negociar las claves SNMPv3, bien sea a través del algoritmo Diffie-Helman o Kerbero, según proceda. De ser activado por el operador de cable, el CSP garantiza la seguridad del SNMPv3 entre el NMS y el PS y proporciona la capacidad de validar y verificar certificados digitales a efectos de autenticación y criptación. Si el operador de cable así lo dispone durante el intercambio DHCP, el CSP inicia, gestiona y cierra una sesión TLS tendiente a descargar de una manera segura los ficheros de configuración del PS y de la barrera contra fuegos.

La funcionalidad de barrera contra fuegos del PS protege al usuario y a la red HFC contra tráfico no deseado proveniente de sectores de direcciones WAN, LAN o PS, como por ejemplo ataques deliberados a la red doméstica, así como limitaciones de tráfico provenientes de aplicaciones de control paternal. Entre los requisitos de seguridad se cuenta con reglas específicas para que los operadores de cable puedan realizar la gestión a distancia.

11.2.2.3 Servidor del centro de distribución de claves (KDC)

Este servidor es necesario siempre que el operador de cable utilice IPCable2Home con modo de configuración SNMP. Si hay un servidor KDC en la cabecera, se utilizará para proporcionar los servicios de autenticación mutua y distribución de claves mediante el protocolo Kerberos. De haberlo, el KDC se comunicará con la función CSP a fin de establecer dichos servicios.

11.3 Infraestructura de autenticación del dispositivo PS

En esta cláusula se describe la autenticación del dispositivo PS y su comunicación al KDC y al servidor HTTPS.

11.3.1 Objetivos de la infraestructura de autenticación de dispositivo

Es importante establecer la identidad segura del elemento PS a fin de:

- Reducir la posibilidad de que se clonen el dispositivo y el software, así como del robo de servicios. Las pasarelas están en un entorno ampliamente distribuido en el que el acceso físico del cliente a la pasarela ocurre en los locales de éste. La provisión de una identidad segura disminuye el riesgo de manipulación no deseada del dispositivo de hardware de la pasarela.
- Establecer la fuente de confianza. Gracias a la PKI se obtiene una fuente de confianza establecida que proviene del fabricante.

11.3.2 Directrices de diseño del sistema de infraestructura de autenticación

Véase el cuadro 11-2.

Cuadro 11-2/J.192 – Directrices de diseño del sistema de infraestructura de autenticación

Referencia	Directrices
SEC1	Incluye el diseño necesario para comunicar las credenciales de autenticación de elementos IPCable2Home.
SEC2	Se suministrarán credenciales de autenticación para los servidores CPE y los servidores internos cruciales, que definirán la utilización específica de éstos y garantizarán una fuente de confianza.

11.3.3 Descripción del sistema de infraestructura de autenticación

Antes de intercambiar cualquier tipo de información significativa, es importante saber, a efectos de seguridad, con quién se está comunicando. La autenticación permite obtener una identidad segura y se compone de tres partes: la credencial de identidad, la verificación de la validez de la credencial de identidad, y los medios comunes para transmitir con seguridad la información de identidad. Así pues, se especifica una credencial de identificación normalizada para la industria, el certificado X.509, junto con [RFC 3280] para su utilización en los certificados, y Kerberos, que es un protocolo de comunicaciones común para autenticación mutua. El elemento PS y el KDC intercambian certificados X.509 durante la operación PKINIT Kerberos, que viene incluida en mensajes de petición AS y respuesta AS. El certificado de elemento PS proporciona la identidad del elemento PS asociado mediante la vinculación criptográfica de la dirección MAC de WAN-Man de dicho elemento con el certificado de clave pública. Cada lado valida la información del certificado y verifica la cadena del certificado hasta la raíz. Una vez que se ha establecido la confianza, se envía la información de las claves SNMPv3 desde el KDC hasta el elemento PS. En esta cláusula, sobre autenticación, se describe la utilización de los certificados Kerberos y X.509.

11.3.4 Requisitos de la infraestructura de autenticación

11.3.4.1 Autenticación de elementos a través de Kerberos

Se especifica la autenticación siempre que haya en la cabecera un KDC que soporte IPCable2Home. En tal caso, conviene que el operador de cable disponga el elemento PS en el modo de configuración SNMP (como se describe en 5.5) a fin de aprovechar el protocolo especificado de autenticación mutua con la utilización de Kerberos, gracias a la extensión PKINIT. Kerberos es un protocolo para asegurar la autenticación mutua, a fin de proporcionar las claves y el establecimiento de comunicación solamente entre partes autenticadas en la red IPCable2Home. Puesto que este modelo ya ha sido especificado en otro proyecto de la UIT, es decir, IPCablecom, en IPCable2Home se hace referencia a dicho modelo siempre que resulte adecuado.

IPCablecom requiere de varios objetos MIB Kerberos, suplen la funcionalidad Kerberos requerida por IPCable2Home. Estos objetos se definen en la MIB de seguridad y se describen en las cláusulas sobre objetos de la MIB.

Si las opciones DHCP así lo requieren, el PS inicia su comunicación con el KDC inmediatamente después que éstas se procesan durante la configuración. Estas opciones, que se especifican en 7.3.3.2.4, requieren que se incluya la subopción 10 de la opción 122, que contiene el valor de la dirección IP del KDC, que se ha de incluir con las otras opciones DHCP, y que DEBE ser utilizada por el PS a fin de establecer su comunicación con el KDC. Si bien en IPCablecom se requiere un nombre DNS como parte de las opciones DHCP, éste no es el caso en IPCable2Home y, por tanto, el PS debe obtener la dirección IP del KDC a fin de poder encontrar el centro de distribución de claves adecuado.

11.3.4.1.1 Kerberos/PKINIT

Si se dispone el elemento PS en el modo de configuración SNMP, se especifica la utilización de Kerberos con la extensión de clave pública PKINIT para la autenticación de elementos IPCable2Home y el soporte de los requisitos de gestión de clave. Los elementos IPCable2Home (cliente) se autentican por sí mismos con el KDC mediante el protocolo PKINIT, tras lo cual reciben un tique Kerberos destinado a su propia autenticación con un servidor particular.

En el modo de configuración SNMP, el elemento PS, el NMS (es decir, el gestor SNMP) y el KDC DEBEN seguir la especificación de Kerberos/PKINIT, tal como se define en 6.4 y 6.5 de la Rec. UIT-T J.170, a menos que se indique lo contrario en la presente Recomendación. El KDC de IPCable2Home es equivalente o idéntico al KDC MSO de IPCablecom (en IPCablecom se especifica la utilización de varios KDC). En la especificación IPCable2Home se habla de sistemas de gestión de red (NMS) a fin de proporcionar la funcionalidad SNMP. En lo que respecta al conjunto de especificaciones de IPCablecom, obsérvese que se utiliza el término servidor de configuración para indicar la funcionalidad de SNMP. Aunque esta funcionalidad suele ser compatible con ambas especificaciones, éstas no son idénticas puesto que se requiere información específica de IPCablecom y de IPCable2Home. El elemento PS DEBE actuar como el cliente ante el KDC. En la especificación de seguridad de IPCablecom, el MTA es el cliente y cabe esperar que las implementaciones de IPCable2Home utilicen dicha funcionalidad para el elemento PS. Este elemento utiliza Kerberos para la gestión de claves SNMP, así como para la autenticación de dispositivos. En la cláusula sobre PKI (véase 11.3.4.2) se especifican los certificados utilizados en PKINIT para IPCable2Home. Siempre que se especifique un certificado de dispositivo MTA para IPCablecom, éste suministra un certificado para el elemento PS (certificado de elemento PS) y las implementaciones de este elemento DEBEN incluirlo.

No se aplican a IPCable2Home las siguientes cláusulas de la funcionalidad Kerberos [Rec. UIT-T J.170]:

- cláusula 6.4.2.1.3, Preautenticador para la ubicación de servidor de configuración;
- cláusula 6.4.5, Ubicaciones de servidor Kerberos y convenios de denominación.

- cláusula 6.4.6, Nombres principales de MTA;
- cláusula 6.4.7, Correspondencia de dirección MAC MTA con FQDN MTA;
- cláusula 6.4.9, Versiones de claves de servicio;
- cláusula 6.5.2.1, Mensajes Rekey;
- cláusula 6.5.3, IPSec Kerberizado.

11.3.4.1.2 Variables de autenticación específicas de IPCable2Home

En el modelo IPCablecom hay algunos nombres específicos de variable para Kerberos, en la arquitectura de red IPCablecom. Para que IPCable2Home pueda utilizar este modelo, se DEBEN reemplazar los siguientes nombres de variable:

- pktcKdcToMtaMaxClockSkew, definido en la especificación de seguridad de IPCablecom, por KdcToClientMaxClockSkew.
- pktcSrvrToMtaMaxClockSkew, definido en la especificación de seguridad de IPCablecom, por SrvrToClientMaxClockSkew.
- mtaprovsrvr, definido en la especificación de seguridad de IPCablecom, con provsrvr.

En las implementaciones Kerberos de IPCable2Home se DEBE ignorar la porción de campo del identificador de objeto (OID) que dice clabProjIPCablecom (2), dentro de AppSpecificTypedData, y de los mensajes KRB-ERROR.

11.3.4.1.3 Perfil para ubicaciones del servidor y convenios de denominación Kerberos

Aunque los nombres de sector Kerberos PUEDEN tener la misma sintaxis que un nombre de dominio, siempre DEBEN estar en mayúsculas. Se DEBEN seguir los detalles del sector Kerberos conforme al anexo B/J.170.

Los convenios del KDC enumerados en 6.4.5.2/J.170 tienen carácter informativo, y se prevé que el KDC ejecutará las funciones necesarias en los sistemas soporte interiores, a fin de intercambiar la información adecuada con el NMS (servidor de configuración o gestor de SNMP). El elemento PS suministra al KDC la dirección IP del servidor de configuración en la petición AS, siendo ésta la información necesaria para que se establezca el contacto adecuado entre el KDC y el servidor de configuración.

Un nombre principal de elemento PS DEBE ser del tipo NT-SRV-INST y tener exactamente dos componentes: el primero DEBE ser la cadena " PS" (sin las comillas), y el segundo DEBE ser la dirección WAN-Man-MAC:

PSElement/<WAN-Man-MAC>

siendo <WAN-Man-MAC> la dirección MAC de WAN-Man del elemento PS. El formato de la <WAN-Man-MAC> DEBE ser "XX:XX:XX:XX:XX:XX" (sin las comillas), siendo X un carácter hexadecimal de la dirección MAC. Los caracteres hexadecimales a-f DEBEN indicarse en minúsculas.

El nombre principal de un elemento NMS DEBE ser del tipo NT-SRV-HST y tener exactamente dos componentes: el primero DEBE ser la cadena "provsrvr" (sin incluir las comillas), y el segundo DEBE ser la dirección de la entidad SNMP del proveedor de servicio, a saber:

provsrvr/<SNMP entity address>

La <SNMP manager address> DEBE ser la dirección IP del gestor SNMP del proveedor de servicio (Opción 122, subopción 3, de CDC DHCP) escrita con notación separada por puntos y dentro de paréntesis cuadrados (por ejemplo [12.34.56.78]).

11.3.4.2 Infraestructura de clave pública (PKI)

Se utilizan certificados de clave pública con arreglo a la especificación X.509 y a [RFC 3280] del IETF.

11.3.4.2.1 Requisitos de certificado genérico

En esta cláusula se describe lo que se suele denominar estructura genérica, puesto que todos los certificados comparten estos requisitos. Todos los certificados especificados en esta cláusula DEBEN incluir la siguiente información:

- **Versión de certificado** – DEBE ser [Rec. UIT-T X.509], v3, y denominada v2 en el certificado real. Todos los certificados DEBEN ser conformes a [RFC 3280], salvo cuando se indique explícitamente la falta de dicha conformidad en esta cláusula. Cuando en esta Recomendación se solicite no conformidad para cierto contenido, no necesariamente se tratará de no conformidad de los formatos. Toda petición específica de no conformidad de formatos se describirá explícitamente.
- **Tipo de clave pública** – En las jerarquías de certificados descritas en 11.3.4.2.2 se utilizan claves públicas RSA. El OID subjectPublicKeyInfo.algorithm que se utiliza DEBE ser 1.2.840.113549.1.1.1 (rsaEncryption). El exponente público de todas las claves RSA DEBE ser F_4 – 65537.
- **Extensiones** – Las extensiones (subjectKeyIdentifier, authorityKeyIdentifier, KeyUsage y BasicContraints) DEBEN ser conformes a [RFC 3280]. Cualquier otra extensión de certificado, de haberla, se DEBE etiquetar como no crucial. Las etiquetas de codificación son [c:crucial, n:no crucial; m:obligatoria, o:opcional] y se identifican en el cuadro de cada certificado.
- **subjectKeyIdentifier** – Esta extensión, que se incluye en todos los certificados conforme a [RFC 3280] (por ejemplo, todos los certificados salvo los de dispositivo y auxiliar), DEBE incluir el valor keyIdentifier compuesto del troceo SHA-1 de 160 bit del valor de la cadena de bits (BIT STRING) subjectPublicKey (excluyendo la etiqueta, longitud y cantidad de bits no utilizados de la codificación ASN-1) (véase [RFC 3280]).
- **authorityKeyIdentifier** – Esta extensión, que se incluye en todos los certificados conforme a [RFC 3280], DEBE incluir el subjectKeyIdentifier del certificado del emisor (véase [RFC 3280]), excepto en el caso de los certificados raíz.
- **KeyUsage** – Esta extensión se DEBE utilizar en todos los certificados de autoridad de certificación (CA, *certification authority*) y en todos los certificados de verificación de código (CVC, *code verification certificates*). En los primeros, esta extensión DEBE marcarse como crucial con un valor de keyCertSign y cRLSign. En los certificados CVC, se la DEBE marcar como crucial con un valor de digitalSignature y keyEncipherment. Los certificados de entidad final PUEDEN utilizar la extensión keyUsage como se enumera en [RFC 3280].
- **BasicConstraints** – Se DEBE utilizar esta extensión para todos los certificados CA y CVC y se la DEBE marcar como crucial. Los valores en cada certificado de basicConstraints DEBEN marcarse como se especifica en los cuadros 11-3 a 11-14, descripción de certificado.
- **Algoritmo de firma** – El mecanismo de firma que se utiliza DEBE ser el SHA-1 [FIPS 186] con criptación RSA. El OID específico es 1.2.840.113549.1.1.5.
- **SubjectName y IssuerName** – Cuando no se pueda codificar una cadena como PrintableString, se la DEBE codificar como UTF8String (tag [UNIVERSAL 12]).

Cuando se trate de codificar un nombre X.500:

- Cada RelativeDistinguishedName (RDN) DEBE contener solamente un elemento único del conjunto de atributos X.500.
- El orden de los RDN en un nombre X.500 DEBE ser idéntico al orden en el que se presentan en esta Recomendación.
- **serialNumber** – DEBE ser un entero único y positivo, atribuido por la CA a cada certificado (es decir, el nombre del emisor y el número de serie identifican un certificado único). Las CA DEBEN forzar que serialNumber será un entero no negativo. El fabricante NO DEBE imponer o suponer una relación entre el número de serie del certificado y el número de serie del módem para el cual se emite el certificado.

  Dado el carácter único de los requisitos indicados, cabe esperar que los números de serie contengan números enteros grandes. Los usuarios de certificado DEBEN poder utilizar valores de serialNumber de hasta 20 octetos. Las CA conformes a la especificación NO DEBEN utilizar valores de serialNumber mayores que 20 octetos.

11.3.4.2.2 Jerarquías de certificado

Se utilizan tres jerarquías diferentes de certificado, a saber:

1) cadena del fabricante, que se utiliza para identificar a los fabricantes autorizados;
2) cadena de verificación de código, que se utiliza para identificar las imágenes de software conformes a esta Recomendación;
3) cadena de proveedor de servicio, que se utiliza para identificar los dispositivos de la red de proveedor de servicio útiles para autenticación mutua de los dispositivos de abonado.

Las jerarquías de certificado descritas en esta Recomendación se pueden aplicar a todos los proyectos relacionados en los que se necesiten certificados. En ellos, se puede adoptar la jerarquía correspondiente, gracias a la cual es posible obtener una estructura de certificados compartida y más genérica. Con todo, en cada proyecto es posible efectuar ajustes específicos a los requisitos que se adapten a sus necesidades particulares. El objetivo es crear una PKI que pueda ser reutilizada en cada proyecto. Si bien puede haber diferencias en los certificados de entidad final necesarios en cada proyecto, si estos certificados se superponen, es posible utilizar un certificado de entidad final para varios servicios en la infraestructura de cable. Así, por ejemplo, tanto IPCablecom como IPCable2Home requieren de un KDC para el proveedor de servicios, y cuando éste utilice ambas arquitecturas de red en sus sistemas, es posible utilizar el mismo KDC y el mismo certificado KDC para comunicarse en ambos. En este caso, el KDC de IPCable2Home es equivalente al KDC MSO IPCablecom (en IPCablecom se especifica la utilización de varios KDC).

En la figura 11-2, se utilizan las abreviaturas CA y CVC para autoridad de certificado y certificado de verificación de código, respectivamente.

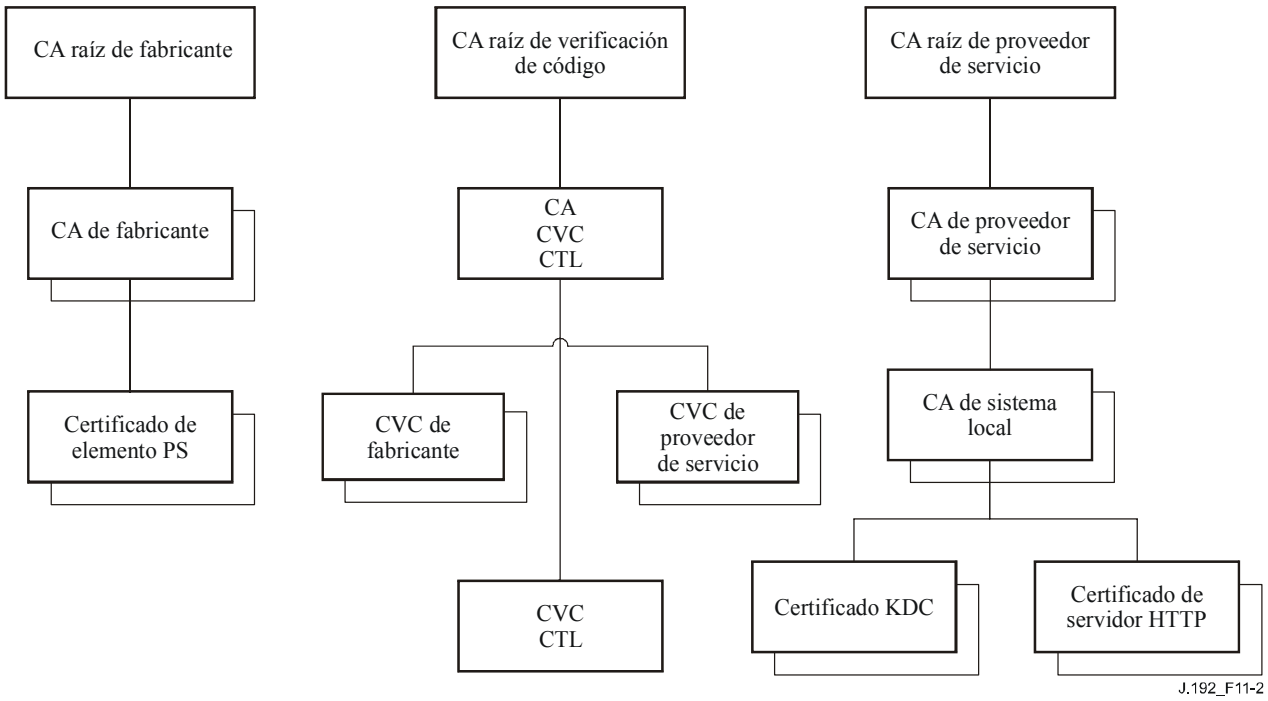


Figura 11-2/J.192 – Jerarquía de certificados de IPCable2Home

11.3.4.2.2.1 Jerarquía del certificado de fabricante

La jerarquía del certificado de fabricante, o cadena de fabricante, tiene su raíz en una CA raíz de fabricante, que se utiliza para emitir certificados de autoridad de certificación (CA) de fabricante para un conjunto de fabricantes autorizados. Éstos solicitan certificados de elemento PS a una CA de primer nivel (por ejemplo, una CA de fabricante o una CA de fabricante en anfitrión). Esta cadena se utiliza para la autenticación de dispositivos domésticos.

En los cuadros a continuación se especifican los valores para los campos requeridos de conformidad con [RFC 3280]. Se DEBEN seguir los valores específicos para la jerarquía de certificado de fabricante conforme a los cuadros 11-3, 11-4, 11-5 y 11-6. Cuando no se indique específicamente en los cuadros un campo requerido, se DEBEN seguir las directrices dadas en [RFC 3280]. De igual manera, se DEBEN incluir las extensiones genéricas especificadas en 11.3.4.2, sobre PKI.

Certificado de CA raíz de fabricante

Este certificado (véase el cuadro 11-3) se DEBE verificar como parte de la cadena de certificados que incluye al mismo, al certificado de CA de fabricante y al certificado del elemento PS.

Cuadro 11-3/J.192 – Certificado de CA raíz de fabricante

Formato de nombre del sujeto	C=<country> (país) O=<Company Name> (nombre de la empresa) CN=[Company Name] CA Raíz del fabricante
Utilización prevista	Este certificado se utiliza para emitir certificados de CA de fabricante
Firmado por	Auto firmado
Periodo de validez	De 20 a 30 años

Cuadro 11-3/J.192 – Certificado de CA raíz de fabricante

Longitud del módulo	2048
Extensiones	KeyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], basicConstraints [c,m](cA=true)

Certificado de CA de fabricante

Si el fabricante emite un certificado de CA y éste se utiliza para emitir el certificado del elemento de PS, dicho certificado se DEBE verificar como parte de la cadena de certificados que contiene el certificado de CA raíz de fabricante, el certificado de CA de fabricante, y el certificado del elemento PS.

El estado/provincia, la ciudad, y el local del fabricante son atributos facultativos. Un fabricante PUEDE tener más de un certificado de CA de fabricante. En tal caso, el elemento PS DEBE tener acceso a los certificados adecuados, que se verifican mediante la correspondencia del nombre del emisor en el certificado de elemento PS con el nombre de sujeto en el certificado de CA de fabricante. El authorityKeyIdentifier del certificado de elemento PS DEBE corresponder con el subjectKeyIdentifier del certificado de fabricante, tal como se describe [RFC 3280].

Cuadro 11-4/J.192 – Certificado de CA de fabricante

Formato de nombre del sujeto	C=<country> O=<CompanyName> [ST=<state/province>] (estado/provincia) [L=<city>] (ciudad) OU= <organization unit> (unidad organizacional) [OU=<Manufacturer's Facility>] (local del fabricante) CN=<CompanyName> Mfg CA
Utilización prevista	Este certificado es emitido a cada fabricante por una autoridad de certificación, CA raíz de fabricante, y puede ser asignado a cada elemento PS bien sea durante la fabricación o durante la actualización del código de campo. Aparece como un parámetro de sólo lectura en el elemento PS. Este certificado emite certificados de elemento PS. Junto con el certificado de CA raíz de fabricante y el certificado del elemento PS, sirve para autenticar la identidad del elemento PS. La lista facultativa de las facilidades del fabricante puede incluir el nombre y/o la ubicación de éstas.
Firmado por	CA raíz de fabricante de la jerarquía
Periodo de validez	20 años
Longitud de módulo	2048
Extensiones	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints[c,m](cA=true, pathLenConstraint=0)

El nombre de la compañía en el campo organización (O) PUEDE ser diferente del nombre de la compañía en el campo nombre común (CN, *common name*).

Certificado de CA de fabricante

Cuando el certificado de CA de fabricante en anfitrión se utiliza para emitir el certificado de elemento PS, se DEBE verificar como parte de una cadena de certificados que contenga el certificado de CA raíz de fabricante, el certificado de CA de fabricante en el anfitrión, y el certificado de elemento PS.

El estado/provincia, ciudad y local del fabricante son atributos opcionales. El authorityKeyIdentifier del certificado de elemento PS DEBE concordar con el subjectKeyIdentifier del certificado de CA de fabricante en anfitrión descrito en [RFC 3280].

Cuadro 11-5/J.192 – Certificado CA de fabricante en anfitrión

Formato de nombre del sujeto	C=<country> O=<Company Name> [ST=<state/province>] [L=<city>] OU=<CA Identifier>] CN=<CompanyName> Mfg CA
Utilización prevista	Este certificado es emitido por la autoridad de certificación CA raíz de fabricante, y puede ser asignado a cada elemento PS durante la fabricación o durante la actualización del código de campo. Aparece como un parámetro de sólo lectura en el elemento PS. Este certificado emite certificados de elemento PS. Junto con el certificado de CA raíz de fabricante y el certificado del elemento PS, sirve para autenticar la identidad del elemento PS.
Firmado por	CA de fabricante
Periodo de validez	20 años
Longitud del módulo	2048
Extensiones	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints[c,m](cA=true, pathLenConstraint=0)

El nombre de la compañía en el campo organización (O) PUEDE ser diferente del nombre de la compañía en el campo nombre común (CN).

Certificado de elemento PS

Se DEBE verificar el certificado de elemento PS como parte de una cadena de certificados que contiene el certificado de CA raíz de fabricante, el certificado de CA de fabricante o el certificado CA de fabricante en anfitrión y el certificado del elemento PS.

Los atributos estado/provincia, ciudad, nombre de producto y local del fabricante son facultativos.

La dirección MAC de WAN-Man del elemento PS DEBE expresarse como seis pares de cifras hexadecimales separadas por dos puntos, por ejemplo, "00:60:21:A5:0A:23". Los caracteres HEX Alpha (A-F) DEBEN expresarse con mayúsculas.

Un certificado de elemento PS es permanente y no puede ser ni renovado ni reemplazado y, por tanto, tiene un periodo de validez mayor que la vida media esperada de funcionamiento del dispositivo en cuestión.

Cuadro 11-6/J.192 – Certificado de elemento PS

Formato de nombre del sujeto	C=<country> O=<Company Name> [ST=<state/province>] [L=<city>] OU=<organization unit> [OU=<Product Name>] (nombre de producto) [OU=<Manufacturer's Facility>] CN=<WAN-Man MAC Address>
Utilización prevista	Este certificado es emitido por una CA de fabricante e instalado en la fábrica. El servidor NMS no puede actualizarlo. Es un parámetro de lectura únicamente en el elemento PS. Se utiliza para autenticar la identidad del elemento PS.
Firmado por	CA de fabricante
Periodo de validez	Más de 20 años
Longitud del módulo	1024, 1536, 2048
Extensiones	keyUsage[c,m](digitalSignature, keyEncipherment, authorityKeyIdentifier [n,m]

11.3.4.2.2.2 Jerarquía de certificado de verificación de código

La jerarquía de certificado de verificación de código (CVC), o cadena de verificación de código, tiene su raíz en una CA raíz de verificación de código, que emite el certificado de CA de verificación de código. La CA de verificación de código se utiliza para emitir CVC a un conjunto de fabricantes y proveedores de servicio autorizados. La CA de verificación de código también emite los CVC. Esta cadena se utiliza específicamente para autenticar descargas de software. La PKI de IPCable2Home permite que haya varios CVC de fabricante, una CVC y varias CVC de proveedor de servicio.

CableLabs será responsable de registrar nombres de abonados CVC autorizados. Es responsabilidad de la CA de verificación de código CableLabs garantizar que el nombre de la organización de cada abonado CVC sea diferente. Cuando se asignen nombres de organizaciones a cofirmantes de ficheros de código DEBEN seguirse las directrices siguientes.

- El nombre de la organización utilizado para autoidenticación como agente cofirmante de código en un CVC DEBE ser asignado por CableLabs.
- El nombre DEBE ser una cadena imprimible de ocho dígitos hexadecimales que distingue a un agente firmante de código del resto.
- Cada dígito hexadecimal del nombre DEBE elegirse de entre el conjunto de caracteres 0-9 (0x30-0x39) o A-F (0x41-0x46).
- La cadena que consta de ocho dígitos 0 no está permitida y NO DEBE ser utilizada en un CVC.

En los cuadros siguientes se indican los valores específicos para los campos requeridos conforme a [RFC 3280]. Dichos valores, en el caso de la jerarquía de certificado de verificación de código, se DEBEN seguir, con arreglo a los cuadros 11-7, 11-8, 11-9, 11-10 y 11-11 siguientes. De no existir el campo requerido en los cuadros, se DEBEN seguir las directrices que aparecen en [RFC 3280]. Asimismo, se DEBEN incluir las extensiones genéricas especificadas en 11.3.4.2 sobre PKI.

Certificado de CA raíz de verificación de código

Se DEBE verificar este certificado como parte de la cadena de certificados que contiene el certificado de CA raíz de verificación de código, el CA de verificación de código y los certificados de verificación de código.

Cuadro 11-7/J.192 – Certificado de CA raíz de verificación de código

Formato de nombre del sujeto	C=<country> O=<Company Name> CN= [Company Name] CA raíz de CVC
Utilización prevista	Este certificado se utiliza par firmar certificados de CA de verificación de código
Firmado por	Autofirmado
Periodo de validez	De 20 a 30 años
Longitud del módulo	2048
Extensiones	KeyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], basicConstraints [c,m](cA=true)

Certificado de CA de verificación de código

Se DEBE verificar este certificado como parte de la cadena de certificados que contiene el certificado de CA raíz de verificación de código, el certificado de CA de verificación de código y el certificado de verificación de código. Un PS autónomo sólo DEBE soportar una CA de CVC a la vez.

Cuadro 11-8/J.192 – Certificado de CA de verificación de código

Formato de nombre de sujeto	C=<country> O=<Company Name><Eight(8) character hexidecimal value> CN= [Company Name] CVC CA
Utilización prevista	La CA raíz de verificación de código emite este certificado a la autoridad de certificados. Este certificado emite certificados de verificación de código.
Firmado por	CA raíz de verificación de código de la jerarquía
Periodo de validez	20 años
Longitud del módulo	2048
Extensiones	KeyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints [c,m](cA=true, pathLenConstraint=0)

Certificado de verificación de código de fabricante

Se DEBE verificar este certificado como parte de la cadena de certificados que contiene el certificado de CA raíz de verificación de código, el certificado de CA de verificación de código y los certificados de verificación de código.

Cuadro 11-9/J.192 – Certificado de verificación de código de fabricante

Formato de nombre del sujeto	C=<country> O=<CompanyName> [ST=<state/province>] [L=<city>] CN=<CompanyName> Mfg CVC
Utilización prevista	La CA de verificación de código emite este certificado a cada fabricante autorizado. El operador de cable lo utiliza en el conjunto de políticas a fin de permitir la descarga segura de software. El CompanyName en los campos O y CN puede ser diferente.
Firmado por	CA de verificación de código
Periodo de validez	Hasta 10 años
Longitud del módulo	1024, 1536, 2048
Extensiones	keyUsage[c,m](digitalSignature, keyEncipherment), extendedKeyUsage [c,m] (id-kp-codeSigning), authorityKeyIdentifier [n,m]

Certificado de verificación de código

El certificado de verificación de código DEBE verificarse como parte de una cadena de certificados que contiene el certificado de CA raíz de verificación de código, el certificado de CA de verificación de código y el certificado de verificación de código.

Cuadro 11-10/J.192 – Certificado de verificación de código

Formato de nombre del sujeto	C=<country> O=<Eight(8) character hexadecimal value> CN=<Company Name>CVC
Utilización prevista	La CA de verificación de código emite este certificado, que es utilizado para autenticar el código certificado. El operador de cable lo utiliza en el conjunto de políticas para permitir la descarga segura de software.
Firmado por	CA de verificación de código
Periodo de validez	Hasta 10 años
Longitud del módulo	1024, 1536, 2048
Extensiones	keyUsage[c,m](digitalSignature, keyEncipherment), extendedKeyUsage [c,m] (id-kp-codeSigning), authorityKeyIdentifier [n,m]

Certificado de verificación de código del proveedor de servicio

El certificado de verificación de código del proveedor de servicio DEBE verificarse como parte de una cadena de certificados que contiene el certificado de CA raíz de verificación de código, el certificado de CA de verificación de código y el certificado de verificación de código del proveedor de servicio.

Cuadro 11-11/J.192 – Certificado de verificación de código del proveedor de servicio

Formato de nombre del sujeto	C=<country> O=<Eight(8) character hexadecimal value> [ST=<state/province>] [L=<city>] CN=<CompanyName> CVC del proveedor de servicio
Utilización prevista	La CA de verificación de código emite este certificado a cada proveedor de servicio autorizado. El operador de cable lo utiliza en el conjunto de políticas a fin de permitir la descarga segura de software. El CompanyName en los campos O y CN puede ser diferente.
Firmada por	CA de verificación de código
Periodo de validez	Hasta 10 años
Longitud del módulo	1024, 1536, 2048
Extensiones	keyUsage[c,m](digitalSignature, keyEncipherment), extendedKeyUsage [c,m] (id-kp-codeSigning), authorityKeyIdentifier [n,m]

11.3.4.2.2.3 Jerarquía de certificado del proveedor de servicio

La jerarquía de certificado del proveedor de servicio, o cadena del proveedor de servicio, tiene su raíz en una CA raíz del proveedor de servicio, que se utiliza para emitir certificados destinados a un conjunto de proveedores de servicio autorizados. Se puede utilizar la CA del proveedor de servicio para emitir certificados facultativos de CA de sistema local o certificados auxiliares. Cuando la CA del proveedor de servicio no emita estos últimos, la CA de sistema local lo hará. Los certificados auxiliares son los certificados de entidad final en la red del operador de cable.

En los cuadros a continuación se indican los valores específicos para los campos requeridos de conformidad con [RFC 3280]. Estos valores específicos para la jerarquía de certificado del proveedor de servicio DEBEN ser los indicados en los cuadros 11-12 a 11-16. Si no aparece específicamente un campo requerido en los cuadros, se DEBEN seguir las directrices de [RFC 3280]. Asimismo, se DEBEN incluir las extensiones genéricas para IPCable2Home, tal como se especifica en 11.3.4.2 sobre PKI.

Certificado de CA raíz del proveedor de servicio

Se DEBE verificar este certificado como parte de la cadena de certificados que contiene el certificado de CA raíz del proveedor de servicio, el certificado de CA del proveedor de servicio, el certificado facultativo de CA de sistema local y los certificados auxiliares.

Cuadro 11-12/J.192 – Certificado de CA raíz del proveedor de servicio

Formato de nombre del sujeto	C=<country> O=<CompanyName> CN=<CompanyName> CA raíz del proveedor de servicio
Utilización prevista	Este certificado se utiliza para emitir certificados de CA del proveedor de servicio.
Firmado por	Autofirmado
Periodo de validez	De 20 a 30 años

Cuadro 11-12/J.192 – Certificado de CA raíz del proveedor de servicio

Longitud del módulo	2048
Extensiones	KeyUsage [c,m] (keyCertSign, cRL Sign), subjectKeyIdentifier [n,m], basicConstraints [c,m](cA=true)

Certificado de CA del proveedor de servicio

Se DEBE verificar este certificado como parte de la cadena de certificados que contiene el certificado de CA raíz del proveedor de servicio, el certificado de CA del proveedor de servicio, el certificado facultativo de CA de sistema local y los certificados auxiliares.

Cuadro 11-13/J.192 – Certificado de CA del proveedor de servicio

Formato de nombre del sujeto	C=<country> O=<CompanyName> CN=<CompanyName> CA del proveedor de servicio
Utilización prevista	La CA raíz del proveedor de servicio emite este certificado a cada proveedor de servicio. A fin de facilitar su actualización, se configura cada elemento de red con el atributo OrganizationName del SubjectName del certificado de CA del proveedor de servicio. Éste es el único atributo en el certificado que debe permanecer constante. Este certificado aparece como un parámetro de lectura/escritura en el objeto MIB que identifica el atributo OrganizationName para el sector Kerberos de IPCable2Home. El elemento IPCable2Home no acepta certificados del proveedor de servicio que no correspondan con este valor del atributo OrganizationName en el SubjectName. Si la cabecera contiene un KDC que soporte IPCable2Home, el elemento PS deberá realizar el primer intercambio PKINIT con el KDC inmediatamente después de un rearranque, instante en el que los cuadros MIB no han sido aún configurados. Si bien en ese momento el cliente Kerberos de IPCable2Home DEBE aceptar cualquier atributo OrganizationalName del proveedor de servicio, más adelante DEBE verificar que el valor añadido en el objeto MIB de este sector sea el mismo que el que había en la respuesta inicial PKINIT. Esta CA emite certificados de CA de sistema local o certificados auxiliares.
Firmado por	CA raíz del proveedor de servicio
Periodo de validez	20 años
Longitud del módulo	2048
Extensiones	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints[c,m](cA=true, pathLenConstraint=1)

El CompanyName en el campo Organization (O) PUEDE ser diferente del CompanyName en el campo CommonName (CN).

Certificado de CA de sistema local

Este certificado es facultativo para el proveedor de servicio. De haberlo, se DEBE verificar como parte de la cadena de certificados que contiene el certificado de CA raíz del proveedor de servicio, el certificado de CA del proveedor de servicio, el certificado facultativo de CA de sistema local y los certificados auxiliares.

Cuadro 11-14/J.192 – Certificado de CA de sistema local

Formato de nombre del sujeto	C=<country> O=<CompanyName> OU=<Local System Name> (Nombre de sistema local) CN=<CompanyName> CA de sistema local
Utilización prevista	Este certificado es facultativo y, de haberlo, es emitido por la CA del proveedor de servicio. Esta CA emite certificados auxiliares. Se permite que los servidores de red se muevan libremente entre las CA regionales del mismo proveedor de servicio.
Firmado por	CA del proveedor de servicio
Periodo de validez	20 años
Longitud de módulo	1024, 1536, 2048
Extensiones	keyUsage[c,m](keyCertSign, cRLSign), subjectKeyIdentifier [n,m], authorityKeyIdentifier [n,m], basicConstraints[c,m](cA=true, pathLenConstraint=0)

El CompanyName en el campo Organization (O) PUEDE ser diferente del CompanyName en el campo CommonName (CN).

Certificado de KDC

Se DEBE verificar este certificado como parte de la cadena de certificados que contiene el certificado de CA raíz del proveedor de servicio, el certificado de CA del proveedor de servicio, el certificado facultativo de CA de sistema local y los certificados auxiliares (por ejemplo, los certificados KDC).

El certificado KDC DEBE incluir el subjectAltName PKINIT de Kerberos, tal como se especifica en 8.2.3.4.1//J.170, Certificado de centro de distribución de claves.

Cuadro 11-15/J.192 – Certificado de KDC

Formato de nombre del sujeto	C=<country> O=<Company Name> [OU=<Local System Name>] OU=<Company Name> Key Distribution Centre CN=<DNS Name
Utilización prevista	Este certificado es emitido bien por la CA del proveedor de servicio o bien por la CA de sistema local. Se emite a fin de autenticar la identidad del KDC ante los clientes Kerberos durante los intercambios PKINIT. Se hace llegar al elemento PS dentro de la respuesta PKINIT.
Firmado por	CA del proveedor de servicio o CA de sistema local
Periodo de validez	20 años
Longitud de módulo	1024, 1536, 2048
Extensiones	keyUsage[c,o](digitalSignature) authorityKeyIdentifier[n,m](keyIdentifier= <subjectKeyIdentifier value from CA certificate>) subjectAltName[n,m] (véase el anexo C/J.170)

Certificado de servidor HTTPS

Se DEBE verificar este certificado como parte de la cadena de certificados que contiene el certificado de CA raíz del proveedor de servicio, el certificado de CA del proveedor de servicio, el certificado facultativo de CA de sistema local y los certificados auxiliares (por ejemplo, los certificados KDC).

Cuadro 11-16/J.192 – Certificado de servidor HTTPS

Formato de nombre del sujeto	C=<country> O=<CompanyName> [OU=<Local System Name>] OU=<CompanyName> Servidor HTTPS CN=<DNS Name>
Utilización prevista	Este certificado es emitido bien por la CA del proveedor de servicio o por la CA de sistema local. Se utiliza para autenticar la identidad del servidor HTTPS ante los clientes HTTP para la sesión TLS durante la configuración. Se transmite al elemento PS dentro del mensaje de certificado de servidor TLS.
Firmado por	CA del proveedor de servicio o CA de sistema local
Periodo de validez	20 años
Longitud de módulo	1024, 1536, 2048
Extensiones	keyUsage[c,m](digitalSignature, keyEncipherment, dataEncipherment), extendedKeyUsage[n,m] (id-kp-serverAuth), authorityKeyIdentifier [n,m]

11.3.4.2.3 Validación de certificado

La validación de certificados IPCable2Home incluye la validación de una cadena de certificados, que va desde los certificados de entidad final hasta la raíz válida. Por ejemplo, se verifica la firma en el certificado de elemento PS mediante el certificado de CA de fabricante, y luego la firma en este último mediante el certificado de CA raíz de fabricante, el cual aparece autofirmado, y se recibe desde una fuente de confianza de manera segura. Se utiliza la clave pública presente en el certificado de CA raíz de fabricante para validar la firma en el mismo certificado.

Las reglas exactas de validación de la cadena de certificados DEBEN ser completamente conformes con [RFC 3280], donde se denominan "Validación de trayecto de certificado". En general, los certificados X.509 soportan un conjunto arbitrario de reglas destinadas a determinar si el nombre del emisor de un certificado corresponde al nombre de sujeto del otro. Estas reglas son tales que se PUEDE declarar la correspondencia de dos campos de nombre, aun cuando la comparación binaria de ellos no la indique. En [RFC 3280] se recomienda a las autoridades de certificación restringir la codificación de los campos de nombre de tal manera que en una implementación se pueda declarar la correspondencia o desacuerdo mediante una simple comparación binaria. La seguridad de IPCable2Home sigue esta recomendación. Así las cosas, el campo tbsCertificate.issuer codificado en DER de un certificado IPCable2Home DEBE corresponder exactamente con el campo tbsCertificate.subject codificado en DER de su certificado de emisor. Una implementación PUEDE comparar el nombre de un emisor con el nombre de sujeto mediante una operación binaria de comparación entre los campos tbsCertificate.issuer y tbsCertificate.subject codificados en DER.

No se verifica ni se hace obligatoria la validación de los periodos de validez de la anidación, de conformidad con las normas actuales. En el momento de emitir un certificado, la fecha de inicio de validez de cualquier certificado de entidad final DEBE ser la misma que la fecha de inicio del periodo de validez del certificado de la CA que lo emite o posterior a ésta. Tras la renovación de un certificado de CA, las fechas de inicio de los certificados de entidad final PUEDEN ser anteriores que la fecha de inicio del certificado de la CA emisora. El final de la validez de certificados de entidad final PUEDE ser anterior, el mismo o posterior al final de la validez de la CA emisora, como se especifica en los cuadros de certificados de IPCable2Home.

11.3.4.2.3.1 Validación de la cadena de fabricante y de la verificación de la raíz

El KDC validará la cadena de certificados de fabricante. No se suele incluir explícitamente el primer certificado en la cadena de certificados que se envía por el medio. De incluirse explícitamente el certificado de CA raíz de fabricante, la parte que verifica DEBE saberlo con antelación a fin de verificarlo. El certificado de CA raíz de fabricante que se envía NO DEBE contener ningún cambio, salvo tal vez el número de serie del certificado, el periodo de validez y el valor de la firma. De haber otros cambios diferentes a éstos en el certificado de CA raíz de fabricante que se envió, comparándolo con el certificado de CA de raíz de fabricante conocido, el KDC que efectuó la comparación DEBE considerar infructuosa la verificación de certificado.

11.3.4.2.3.2 Validación de la cadena de verificación de código y de la verificación de la raíz

Antes de iniciar el proceso de descarga de software, un servidor interno puede verificar la validez de la cadena de verificación de código. Para más información, véase en la cláusula 11.8 relativa a la descarga segura de software.

11.3.4.2.3.3 Validación de la cadena del proveedor de servicio y de la verificación de la raíz

El elemento PS DEBE validar la cadena de certificados de fabricante. No se suele incluir explícitamente el primer certificado en la cadena de certificados que se envía por el medio. De incluirse explícitamente el certificado de CA raíz de fabricante, la parte que verifica DEBE saberlo con antelación a fin de verificarlo. El certificado de CA raíz de fabricante que se envía NO DEBE contener ningún cambio, salvo tal vez el número de serie del certificado, el periodo de validez y el

valor de la firma. De haber otros cambios diferentes a éstos en el certificado de CA raíz del proveedor de servicio que se envió, comparándolo con el certificado de CA de raíz del proveedor de servicio conocido, el elemento PS que efectuó la comparación DEBE considerar infructuosa la verificación de certificado.

11.3.4.2.4 Revocación de certificado

Este tema está fuera del alcance de la presente Recomendación.

11.4 Mensajería de gestión segura hacia el PS

El algoritmo de seguridad utilizado para inicializar la mensajería de gestión SNMP depende del modo de configuración del elemento PS (véase 5.5). En IPCable2Home, hay tres modos de configuración, a saber, el modo de configuración DHCP, el modo de configuración SNMP y el modo aletargado. El primero de ellos posee submodos adicionales que permiten identificar si ha sido configurado para el modo NmAccess o el modo de coexistencia. El segundo, requiere de SNMPv3 para la mensajería de gestión.

En las cláusulas a continuación se describen los algoritmos de seguridad y los requisitos necesarios para inicializar la mensajería de gestión SNMP, basándose en el modo de configuración del elemento PS. Este elemento DEBE soportar los algoritmos de seguridad SNMPv3 especificados en 11.4.4.1.2 y 11.4.4.2.

11.4.1 Objetivos de la mensajería de gestión segura

Se persigue la seguridad de los mensajes de gestión para:

- Disponer de opciones para criptar los mensajes de gestión de red hacia el PS.
- Disponer de opciones para autenticar los mensajes de gestión de red al PS.
- Proporcionar seguridad, si fuere posible, en la mensajería de gestión sin que sea necesario implementar protocolos adicionales.
- Disponer de directrices y requisitos mínimos para los algoritmos de criptación y autenticación.

11.4.2 Directrices de diseño del sistema de mensajería de gestión segura

Referencia	Directrices
SEC3	Los mensajes de gestión de red entre la cabecera de la red de cable y el PS se pueden autenticar y, facultativamente, criptar, para protegerlos contra la supervisión y el control no autorizados.

11.4.3 Descripción del sistema de mensajería de gestión segura

Durante varios años se ha incorporado SNMP en los productos de la industria del cable. Los equipos propios del operador de cable pueden soportar SNMPv1, v2 o v3. Se requiere que el PS soporte la mensajería de gestión de estas tres versiones. No existe seguridad intrínseca en las dos primeras versiones, mientras que la tercera tiene algoritmos básicos de autenticación y criptación como los definidos en [RFC 3410], [RFC 3415] y [RFC 3584], e IPCable2Home especifica la utilización de la seguridad definida en los RFC. En SNMPv3 no se especifica cómo se deben configurar las claves a fin de iniciar los procesos de criptación y autenticación y, por ende, en la siguiente cláusula se especifican algunos detalles para generar y establecer el intercambio de claves.

11.4.4 Requisitos de la mensajería de gestión segura

11.4.4.1 Algoritmos de seguridad para SNMP en el modo de configuración DHCP

En este modo, se puede configurar el elemento PS para los modos NmAccess o de coexistencia. En este último, se puede configurar el elemento PS para mensajería de gestión SNMPv1, SNMPv2, y/o SNMPv3.

11.4.4.1.1 Modo NmAccess

Si el elemento PS emplea el modo de configuración DHCP con modo NmAccess, la gestión de red basada en SNMP en este elemento no utiliza SNMPv3 y, por tanto, no es necesario inicializar las funciones de seguridad de SNMPv3. En 6.3.3.1 se define la inicialización del enlace de gestión con SNMPv1/v2.

11.4.4.1.2 Modo de coexistencia

Si el elemento PS emplea el modo de configuración DHCP con modo de coexistencia y se establece que el protocolo de mensajería de gestión sea SNMPv3 (véase 6.3.3.1), el elemento PS DEBE utilizar la seguridad SNMPv3 especificada en [RFC 3414]. El PS DEBE soportar autenticación y privacidad SNMPv3. Es muy recomendable que el operador de cable tenga activada constantemente la autenticación SNMPv3, y utilizar la privacidad SNMPv3, siempre que el operador tenga la capacidad de tratar la carga adicional necesaria para la criptación.

A fin de establecer claves SNMPv3 en el modo de configuración DHCP, todas las interfaces SNMP de IPCable2Home DEBEN utilizar el procedimiento de inicialización y cambios de clave SNMPv3, tal como se define en 2.2 de DOCSIS 1.1 Operations Support Systems Interface specification, [ANSI/SCTE 23-3 de 2005] (reemplace las expresiones "CM" por "elemento PS" y "conforme a DOCSIS 1.1" por "conforme a IPCable2Home").

Asimismo, a fin de soportar inicialización y cambios de clave SNMPv3 en el modo de configuración DHCP, el elemento PS DEBE poder recibir los TLV de tipo 34, 34.1 y 34.2, como se define en B.C.1.2.8 de la especificación de la interfaz de radiofrecuencia DOCSIS 1.1, [J.112 anexo B] e implementar el mecanismo de modificación de claves especificado en [RFC 2786], que incluye el objeto MIB usmDHKickstartTable.

11.4.4.1.3 Inicialización de claves SNMPv3

La autorización final (CHAdministrator) genera un par de números por cada nombre con un límite de cinco nombres distintos de seguridad. Para comenzar, CHAdministrator genera un número aleatorio Rm.

Luego, utiliza la ecuación DH para traducir Rm en un número público z. La ecuación es:

$$z = g \text{ ^ } Rm \text{ MOD } p$$

donde g pertenece al conjunto de parámetros Diffie-Hellman, y p es el número primo de esos parámetros.

Se crea el fichero de configuración PS a fin de incluir el par (nombre de seguridad, número público). El PS DEBE soportar por lo menos cinco pares. Por ejemplo:

TLV tipo 34.1 (nombre de seguridad de arranque rápido Kickstart SNMPv3) = CHAdministrator

TLV tipo 34.2 (número público de arranque rápido Kickstart SNMPv3) = z

El PS DEBE soportar las anotaciones de VACM definidas en 6.3.3.1.4.5 y sólo DEBEN estar activas las anotaciones especificadas por el nombre de seguridad correspondiente en el fichero de configuración PS.

Durante el proceso de rearranque del PS, se DEBEN rellenar los valores anteriores (nombre de seguridad y número público) en usmDHKickstartTable.

A esta altura se cumple que:

usmDHKickstartMgrpublic.1 = "z" (cadena de octeto)

usmDHKickstartSecurityName.1 = "CHAdministrator"

Cuando se fija usmDHKickstartMgrpublic.n a un valor válido durante el registro, se crea una fila correspondiente en usmUserTable que contiene los siguientes valores:

usmUserEngineID: localEngineID

usmUserName: usmDHKickstartSecurityName.n value

usmUserSecurityName: usmDHKickstartSecurityName.n value

usmUserCloneFrom: ZeroDotZero

usmUserAuthProtocol: usmHMACMD5AuthProtocol [RFC 2104]

usmuserAuthKeyChange: (que se deduce del valor establecido)

usmUserOwnAuthKeyChange: (que se deduce del valor establecido)

usmUserPrivProtocol: usmDESPrivProtocol

usmUserPrivKeyChange: (que se deduce del valor establecido)

usmUserOwnPrivKeyChange: (que se deduce del valor establecido)

usmUserPublic

usmUserStorageType: permanent

usmUserStatus: active

NOTA – En el caso de anotaciones de dhKickstart (PS) en usmUserTable, Permanente quiere decir que se DEBEN escribir más no borrar y que no se salvaguardan entre rearranques.

Tras haber completado la inicialización (indicada por un valor '1' (pass) para cabhPsDevProvState), el PS:

1) Genera un número aleatorio xa para cada fila que tiene valores en usmDHKickstartTable, cuyos usmDHKickstartSecurityName y usmDHKickstartMgrPublic tienen una longitud diferente de cero.

2) Utiliza la ecuación DH para traducir xa a un número público c (para cada fila identificada anteriormente).

$$C = g \wedge xa \text{ MOD } p$$

donde g pertenece al conjunto de parámetros Diffie-Hellman, y p es el número primo de dichos parámetros.

usmDHKickstartMyPublic.1 = "c" (cadena de octetos)

usmDHKickstartMgrPublic.1 = "z" (cadena de octetos)

usmDHKickstartSecurityName.1 = "CHAdministrator"

3) Calcula el secreto compartido sk, siendo sk = z ^xa mod p.

4) Utiliza sk para estimar las claves de privacidad y de autenticación para cada fila en usmDHKickstartTable y fija los valores en usmUserTable.

Tal como se especifica en [RFC 2786], las claves de privacidad y autenticación del nombre de usuario correspondiente, "CHAdministrator" en este caso, se derivan de sk mediante la aplicación de la función de derivación de PBKDF2 definida en PKCS#5 v2.0.

clave de privacidad ← PBKDF2(salt = 0xd1310ba6,
iterationCount = 500,
keyLength = 16,
prf = id-hmacWithSHA1) [RFC 2104]

clave de autenticación ← PBKDF2(salt = 0x98dfb5ac,
iterationCount = 500,
keyLength = 16 (usmHMACMD5AuthProtocol) [RFC 2104],
prf = id-hmacWithSHA1) [RFC 2104]

Luego, tras haber completado el PS (CMP) su proceso de inicialización SNMPv3, DEBE permitir un nivel de acceso adecuado a un securityName válido, mediante las claves de autenticación y/o privacidad correctas.

El PS DEBE rellenar con claves adecuadas los cuadros correspondientes, como se especifica en las normas RFC relacionadas con SNMPv3 y [RFC 2786].

5) A continuación se describe el proceso que utiliza el gestor para calcular las claves de autenticación y privacidad únicas del PS.

El gestor SNMP accede al contenido de usmDHKickstartTable a través del nombre de seguridad de 'dhKickstart', sin necesidad de autenticación.

El PS DEBE proporcionar anotaciones preinstaladas en el cuadro USM y en los cuadros VACM a fin de crear correctamente el 'dhKickstart' de usuario de nivel de seguridad noAuthNoPriv, que tenga acceso de lectura solamente al grupo de sistema y a usmDHkickstartTable.

Si el PS está en el modo de coexistencia y se ha configurado para utilizar SNMPv3, la especificación de grupo para la vista dhKickstart DEBE implementarse así:

dhKickstart Group

vacmGroupName 'dhKickstart'

vacmAccessContextPrefix"

vacmAccessSecurityModel 3 (USM)

vacmAccessSecurityLevel NoAuthNoPriv

vacmAccessContextMatch exact

vacmAccessReadViewName 'dhKickstartView'

vacmAccessWriteViewName"

vacmAccessNotifyViewName"

vacmAccessStorageType permanent

vacmAccessStatus active

La vista VACM de la vista dhKickstart se DEBE implementar así:

Subárbol dhKickstartView 1.3.6.1.2.1.1 (Grupo de Sistema) y 1.3.6.1.3.101.1.2.1 (usmDHkickstartTable)

El gestor SNMP obtiene el valor del número usmDHKickstartMypublic del PS, asociado con el securityName para el cual desea deducir las claves de autenticación y privacidad. El gestor puede, utilizando el número aleatorio privado, calcular el secreto compartido DH, a partir del cual puede deducir las claves de autenticación y confidencialidad operacional para el securityName que ha de utilizar en la comunicación con el PS.

11.4.4.1.4 Cambios de clave Diffie-Hellman

El PS DEBE soportar el mecanismo de cambio de clave especificado en la cláusula anterior así como en [RFC 2786].

11.4.4.2 Algoritmos de seguridad para el SNMPv3 en el modo de configuración SNMP

Si se configura el elemento PS en el modo SNMP, la gestión de red basada en SNMP dentro del elemento PS DEBE funcionar en SNMPv3 con la seguridad especificada por [RFC 3414]. El PS DEBE soportar autenticación y privacidad SNMPv3. Se alienta enfáticamente al operador de cable a que mantenga activada constantemente la autenticación SNMPv3. Se recomienda la utilización de la privacidad SNMPv3 siempre que el operador sea capaz de tratar la carga adicional a fines de criptación. Para establecer las claves SNMPv3 en el modo de configuración SNMP, el PS DEBE utilizar la gestión de claves SNMPv3 de tipo Kerberos, como se especifica en 11.4.4.2.1.

11.4.4.2.1 SNMPv3 de tipo Kerberos

Se DEBE seguir el perfil de gestión de claves de tipo Kerberos específico para SNMPv3, como se define en 6.5.4/J.170.

11.4.4.2.2 Algoritmos de criptación de SNMPv3

Se DEBEN seguir los identificadores de transformada de criptación para la gestión de claves SNMPv3 de tipo Kerberos, como se define en 6.3.1/J.170.

11.4.4.2.3 Algoritmos de autenticación SNMPv3

Se DEBEN seguir los algoritmos de autenticación para la gestión de claves SNMPv3 de tipo Kerberos, como se define en la cláusula 6.3.2/J.170.

11.4.4.2.4 Identificadores de máquina SNMPv3

Puesto que el gestor y el cliente SNMP DEBEN verificar que los identificadores (ID) de la máquina SNMPv3 en los mensajes de petición y respuesta AP se basen en el nombre principal Kerberos adecuado en la etiqueta [J.170], se utilizan las reglas siguientes para generar los ID de dicha máquina SNMPv3:

Regla 1: El ID de máquina SNMPv3 DEBE tener el formato definido en [RFC 3411], es decir, se fija el primer bit a 1 (uno) y se utiliza el valor adecuado para los primeros cuatro bytes [RFC 3411].

Regla 2: El quinto byte DEBE tener el valor 4 (cuatro), a fin de indicar que los bytes que van a continuación, hasta un total de 27, se deben considerar como texto y se definen así:

- Los caracteres del nombre principal NMS se DEBEN utilizarse para los bytes de ID de máquina, empezando por el 6º byte.
- La secuencia de bytes, que indica el nombre principal NMS, DEBE ir seguida de un byte y se considera como un valor hexadecimal de 8 bits. Cada valor singular identifica una determinada máquina SNMP en el dispositivo (elemento o servidor NMS). No se DEBE utilizar el valor 0 (cero).
- La cadena de texto que comienzo en el 6º byte DEBE terminar con un carácter Nulo.

NOTA – Si se sigue lo indicado en [RFC 3411], es posible utilizar otros formatos. No obstante, con la anterior selección se pretende reducir la complejidad de implementación que tendría si se permitieran todos los enfoques señalados en [RFC 3411].

11.4.4.2.5 Proceso de anotación en usmUserTable

En 6.3.3.1.4.5, Requisitos del modelo de control de acceso basado en vistas (VACM), se define la configuración de seguridad SNMPv3 para el usuario "CHAdministrator" del operador de cable. El CHAdministrator es la máxima autoridad en materia de gestión del elemento de servicios de portal. También se pueden definir otros usuarios. En la presente cláusula, se define un usuario USM específicamente para el proceso de configuración. En particular, se define el mismo para permitir que se especifique un receptor de notificación para cabhPsDevProvEnrollTrap y cabhPsDevInitTrap, que ha de ser comunicado por el PS durante el proceso de configuración (véase el cuadro 13-1, Descripción de los flujos para los procesos de configuración WAN-Man del PS en

modo de configuración DHCP, paso CHPSWMD-11; cuadro 13-3, Descripción de los flujos para los procesos de configuración WAN-Man del PS en modo de configuración SNMP, pasos CHPSWMS-11 y CHPSWMS-13; y cláusula 13.4.3, Informes de conclusión de la admisión a la configuración y de la configuración).

Los msgSecurityParameters en los mensajes SNMPv3 transportan un campo msgUserName que especifica el usuario en nombre del cual se intercambia el mensaje y con cuya información de seguridad se producen los campos msgAuthenticationParameters y msgPrivacyParameters. A fin de que la máquina SNMP de un elemento IPCable2Home pueda procesar estos mensajes, es necesario introducir la información requerida en usmUserTable [RFC 3414] para la máquina del elemento.

Se DEBE rellenar usmUserTable con la siguiente información en el elemento PS justo después de que se haya recibido el mensaje de respuesta AP:

- usmUserEngineID: el ID de la máquina SNMP local, como se define en 11.4.4.2.4, Identificadores de máquina SNMPv3.
- usmUserName: CHAdministratorxx:xx:xx:xx:xx:xx, siendo xx:xx:xx:xx:xx:xx la dirección de hardware WAN-Man del dispositivo.
- usmUserSecurityName: CHAdministratorxx:xx:xx:xx:xx:xx, siendo xx:xx:xx:xx:xx:xx la dirección de hardware WAN-Man del dispositivo.
- usmUserCloneFrom: 0.0.
- usmUserAuthProtocol: indica el protocolo de autenticación escogido por el usuario, del mensaje de respuesta AP.
- usmUserAuthKeyChange: valor por defecto ""
- usmUserOwnAuthKeyChange: valor por defecto ""
- usmUserPrivProtocol: indica el protocolo de criptación escogido por el usuario, del mensaje de respuesta AP.
- usmUserPrivKeyChange: valor por defecto ""
- usmUserOwnPrivKeyChange: valor por defecto"".
- usmUserPublic: valor por defecto ""
- usmUserStorageType: permanente.
- usmUserStatus: activo.

Se PUEDEN crear nuevos usuarios SNMPv3 mediante la clonación estándar SNMPv3, como se define en [RFC 3414].

Tras la recepción del mensaje de respuesta AP, DEBE rellenarse el cuadro seguridad para el grupo de VACM [RFC 3415] con la siguiente información en el PS:

- vacmSecurityModel: 3(usm).
- vacmSecurityName: CHAdministratorxx:xx:xx:xx:xx:xx.
- vacmGroupName: CHAdministratorSNMP.
- vacmSecurityToGroupStatus: activo.

En el PS, tras la recepción de mensaje de respuesta AP, DEBE rellenarse el cuadro de acceso VACM [RFC 3415] con la siguiente información, vinculada con vacmSecurityToGroupTable definido anteriormente:

- vacmAccessContentPrefix: ""
- vacmAccessSecurityModel: 3(usm).
- vacmAccessSecurityLevel: AuthNoPriv.
- vacmAccessContextMatch: exact(1).

- vacmAccessReadViewName: CHAdministratorView.
- vacmAccessWriteViewName: CHAdministratorView.
- vacmAccessNotifyViewName: CHAdministratorNotifyView.
- vacmAccessStorageType: permanente.
- vacmAccessStatus: activo.

En el PS tras la recepción del mensaje de respuesta AP se DEBEN rellenar siete filas del árbol de vistas VACM [RFC 3415] con la siguiente información:

- vacmViewTreeFamilyName: CHAdministratorNotifyView.
- vacmViewTreeFamilySubtree: cabhPsDevProvEnrollTrap.
- vacmViewTreeFamilyType: incluido.
- vacmViewTreeFamilyMask: ""
- vacmViewTreeFamilyName: CHAdministratorNotifyView.
- vacmViewTreeFamilySubtree: cabhPsDevBase.
- vacmViewTreeFamilyType: incluido.
- vacmViewTreeFamilyMask: ""
- vacmViewTreeFamilyName: CHAdministratorNotifyView.
- vacmViewTreeFamilySubtree: docsDevSoftware.
- vacmViewTreeFamilyType: incluido.
- vacmViewTreeFamilyMask: ""
- vacmViewTreeFamilyName: CHAdministratorNotifyView.
- vacmViewTreeFamilySubtree: cabhPsDevInitTrap.
- vacmViewTreeFamilyType: incluido.
- vacmViewTreeFamily Mask: ""
- vacmViewTreeFamilyName: CHAdministratorNotifyView.
- vacmViewTreeFamilySubtree: cabhPsDevBase.
- vacmViewTreeFamilyType: incluido.
- vacmViewTreeFamily Mask: ""
- vacmViewTreeFamilyName: CHAdministratorNotifyView.
- vacmViewTreeFamilySubtree: docsDevEventTable.
- vacmViewTreeFamilyType: incluido.
- vacmViewTreeFamily Mask: ""
- vacmViewTreeFamilyName: CHAdministratorNotifyView.
- vacmViewTreeFamilySubtree: cabhPsDevProv.
- vacmViewTreeFamilyType: incluido.
- vacmViewTreeFamily Mask: ""

11.5 CQoS en el PS

CQoS es un puente transparente para la QoS de IPCablecom y LAN-a-LAN. Se aseguran los mensajes DQoS IPCablecom entre el MTA y el CMTS, CMS o CM mediante la especificación de seguridad IPCablecom. No se prevé que IPCable2Home añada seguridad a los mensajes IPCablecom. Al considerarse que la amenaza de ataques en el entorno doméstico es extremadamente baja, los mensajes de QoS LAN-a-LAN en IPCable2Home en la vivienda no están

asegurados. No cabe esperar que IPCable2Home añada seguridad a los mensajes IPCablecom. Al no haber requisitos de seguridad para que el elemento PS garantice la seguridad de los mensajes CQoS originados en la WAN, no se depende de los servidores internos para soportar esta función.

11.6 Barrera contra fuegos en el PS

Una de las principales preocupaciones de las empresas que utilizan las redes ha sido, durante décadas, la seguridad. Esta preocupación se desplaza cada vez más al ámbito de la seguridad y privacidad de usuarios domésticos que suelen tener un módem de cable (CM) siempre conectado. Puesto que el abonado promedio puede carecer del conocimiento técnico necesario o del tiempo para mantener la operación más segura de sus computadores domésticos, se hace necesario instalar una barrera contra fuegos como primera línea de defensa que proteja los computadores no asegurados y otros dispositivos IP LAN en la vivienda.

11.6.1 Objetivos e hipótesis relativos a la barrera contra fuegos de IPCable2Home

Objetivos

- Facilitar al operador de cable una configuración normalizada e interoperable para la barrera contra fuegos.
- Facilitar al operador de cable un conjunto mínimo de funcionalidades requeridas para la barrera contra fuegos.
- Activar la supervisión de los eventos en la barrera contra fuegos mediante el mecanismo de mensajería de eventos.
- Proteger la red doméstica y los dispositivos IP LAN en dicha red del tráfico WAN-a-LAN no deseado.
- Proteger la HFC del tráfico LAN-a-WAN no deseado.
- Proteger el PS de ataques y del tráfico considerado como indeseable por el operador de cable.
- Garantizar que la barrera contra fuegos procesará paquetes a velocidad suficientemente alta como para que el filtrado no produzca congestión, independientemente de la complejidad o tamaño del conjunto de reglas.
- Garantizar el soporte de aplicaciones identificadas a través de la barrera contra fuegos en casos específicos.
- Facilitar al operador de cable la capacidad para supervisar y cambiar las reglas utilizadas por la barrera contra fuegos.
- Garantizar que existan las configuraciones de seguridad adecuadas en el sistema de la barrera contra fuegos (por ejemplo, reglas y políticas de filtrado).
- Identificar los tipos de ataques que han de ser registrados por la barrera contra fuegos y especificar el tipo de registro de tal modo que el operador pueda consultarlo cuando sea necesario.
- Soportar IPCablecom a través de la barrera contra fuegos.
- Informar al administrador, en tiempo real, de los eventos definidos como importantes.
- Proporcionar un conjunto de reglas de fábrica por defecto a fin de garantizar la coherencia cuando se reinicialice la barrera contra fuegos.

Hipótesis

- La barrera contra fuegos trata todos los paquetes destinados a la LAN o provenientes de la misma conforme a la política en vigor, sin importar el modo de direccionamiento, la CAT o la transferencia (por ejemplo, el modo de direccionamiento no tiene efecto en su funcionamiento).

- La barrera contra fuegos empieza a funcionar inmediatamente después de que se recibe el mensaje de configuración completa, sin importar el modo de configuración que se utilice.
- Se puede utilizar SNMP, en particular la mensajería SNMP dirigida al portal de gestión de IPCable2Home (CMP), para configurar el conjunto de reglas de la barrera contra fuegos de IPCable2Home. Es decir, este conjunto se representa externamente como una colección de objetos MIB.
- Los objetos MIB controlan las acciones de registro emprendidas por la barrera contra fuegos.
- La barrera contra fuegos aplicará las reglas y política de filtrado junto con la verificación de las direcciones traducidas conocidas por la CAT en el PS.

11.6.2 Directrices de diseño del sistema de barrera contra fuegos

En el cuadro 11-17 figuran las directrices de diseño de sistema de la barrera contra fuegos que dieron origen a las especificaciones de la barrera contra fuegos de IPCable2Home.

Cuadro 11-17/J.192 – Directrices de diseño del sistemas de seguridad IPCable2Home

Referencia	Directrices
SEC4	La barrera contra fuegos aceptará los ficheros de configuración que se reciban en lenguaje y formato normalizados (nota).
SEC5	El operador de cable podrá gestionar a distancia las barreras contra fuegos conformes a la norma, a través del fichero de configuración o de instrucciones SNMP.
SEC6	La barrera contra fuegos conforme a la norma incluirá un conjunto de reglas por defecto, a fin de proporcionar un conjunto mínimo previsto de funcionalidades.
SEC7	Proporcionará el soporte necesario para IPCablecom a través de la barrera contra fuegos.
SEC8	Se atribuirá un conjunto mínimo de requisitos en las capacidades de filtrado de la barrera contra fuegos para paquetes, puertos, direcciones IP, ToD, etc.
SEC9	Gracias a una interfaz de registro detallado de eventos en la barrera contra fuegos, el operador de cable podrá supervisar y revisar la actividad de ésta, conforme a su configuración.
SEC10	La barrera contra fuegos soportará las aplicaciones comúnmente utilizadas en casos específicos.
SEC11	La barrera contra fuegos protegerá a las redes LAN y WAN de los ataques comunes provenientes de la red.
SEC12	La gestión de los eventos y el conjunto de reglas para la barrera contra fuegos se definirá en detalle mediante la MIB de seguridad.
NOTA – En 7.4, Función del PS – Configuración de los servicios de portal en bloque (BPSC), se definen los requisitos de fichero de configuración de la barrera contra fuegos.	

11.6.3 Descripción de sistema de barrera contra fuegos

En general, las barreras contra fuegos se componen de una combinación de: filtrado de paquetes (PF, *packet filter*), filtrado dinámico de paquetes (SPF, *stateful packet filtering*), pasarela de capa aplicación (ALG, *application level gateway*) y apoderado de servidor de aplicaciones (ASP, *application server proxy*). El componente más comúnmente utilizado en estas barreras contra fuegos es el módulo de filtrado de paquetes, ya que permite establecer a cuáles trenes de paquetes se les autoriza cruzar la barrera contra fuegos y a cuáles no. Cada decisión al respecto se basa en información de configuración estática (el conjunto de reglas) que se ha incluido en los mecanismos de filtrado (política) de la barrera contra fuegos, y gracias a los cuales se permitirá pasar o no a los

paquetes, sobre la base de la inspección de los campos del encabezamiento del paquete, a saber, direcciones IP de origen y destino, número de los puertos de protocolo de origen y destino, tipo de protocolo, etc. Dependiendo del nivel de seguridad que se desee obtener, puede ser necesario configurar en la barrera contra fuegos una gran cantidad de filtros. Es tarea del operador de cable encontrar el equilibrio entre la complejidad de ese conjunto de reglas y las necesidades de los usuarios. En esta Recomendación se pretende especificar un conjunto importante de filtros de configuración, que se gestionan a través de objetos MIB, de tal manera de que se puedan configurar particularmente, de ser necesario, diversos tipos de servicios (protocolos y aplicaciones).

En un módulo de filtrado dinámico de paquetes (SPF) se utiliza información de estado acumulada correspondiente a los paquetes que pertenecen a la misma conexión cuando ésta toma decisiones de descarte de paquetes. El SPF distingue entre los diversos protocolos y trata la conexión de cada uno de ellos adecuadamente. El módulo SPF almacena y utiliza información encontrada en los encabezamientos de capas de red y transporte de los paquetes.

La pasarela de capa aplicación (ALG) es una componente que sabe cómo extraer la información necesaria para rastrear la conexión desde la capa de aplicación del paquete. Ahora bien, puesto que algunos protocolos incorporan información de control de conexión en la capa de aplicación, el SPF añade las ALG a fin de seguir la traza de la conexión. Se requiere la ALG específica (por ejemplo FTP-ALG, IPSec-ALG) a fin de poder utilizar cada protocolo necesario para soportar IPCable2Home. Por ejemplo, el protocolo FTP en modo activo incorpora el número de puerto TCP que se utilizará más adelante para la transferencia de datos. Es necesario entonces utilizar una FTP ALG para rastrear el estado de todas las conexiones FTP. En el anexo D figura más información sobre requisitos de ALG.

Un apoderado de servidor de aplicaciones (ASP) realiza un filtrado en función de características únicas del protocolo de capa de aplicación o de mensajes específicamente destinados a los protocolos cliente-servidor. Gracias a la utilización de los ASP se obtienen diversos beneficios de seguridad, por ejemplo, es posible añadir listas de control de acceso a los protocolos, en las que los usuarios o sistemas se obligan a emplear algún tipo de autenticación antes de que obtengan el acceso. Un ASP, además de ser específico al protocolo, tiene conocimiento de éste y puede ser configurado para bloquear solamente algunas de sus subsecciones. Cuando el servicio de portal funciona en alguno de sus dos modos de encaminamiento transparente: C-NAT o C-NAPT, el ASP permite el funcionamiento de aplicaciones que no soportan NAT. Se puede configurar, por ejemplo, un ASP FTP a fin de que bloquee el tráfico proveniente de usuarios no autenticados, al mismo tiempo que garantiza el acceso selectivo a las instrucciones "put" y "get" a aquellos autenticados, según en qué sentido se emitan éstas.

El tipo de combinación que se escoja de filtro de paquetes, las SPF AGL y los ASP en una barrera contra fuegos concreta depende del equilibrio entre la calidad de funcionamiento y el nivel de seguridad. En general, al tratarse de mecanismos de capa de red, los filtros de paquete tienden a permitir una calidad de funcionamiento mejor que la de las ALG/ASP, pues estas últimas son mecanismos de la capa de aplicación. Un compromiso entre estos dos factores que se utiliza con frecuencia consiste en utilizar el filtrado dinámico de paquetes (SPF), que permite guardar y utilizar la información de estado acumulada de los paquetes que pertenecen a la misma conexión, a fin de utilizarla en las decisiones relativas a descartar o no un paquete.

Tanto los SPF como los ASP incluyen un proceso de filtrado que se basa en la política de seguridad, a fin de alcanzar el nivel deseado de seguridad en un sitio. No obstante, si bien los servicios permitidos y la forma en que se los utiliza en la barrera contra fuegos vienen determinados por la política de seguridad, en ésta no se explica detalladamente la configuración específica de la barrera contra fuegos. El conjunto de reglas se pone en términos lisibles para una persona, que son entonces interpretados por la barrera contra fuegos e implementados en la política de filtrado en el lenguaje interno de ésta. Los filtros examinan cada paquete y deciden cuáles pueden ser reenviados por la barrera contra fuegos y cuáles no.

A continuación se presenta un diagrama general (figura 11-3) de la barrera contra fuegos y las funciones de las diversas componentes de ésta a las que se hace referencia en esta Recomendación.

NOTA – En este diagrama no se indica ninguna arquitectura o implementación técnica específica. Éste ha de servir solamente como referencia lógica.

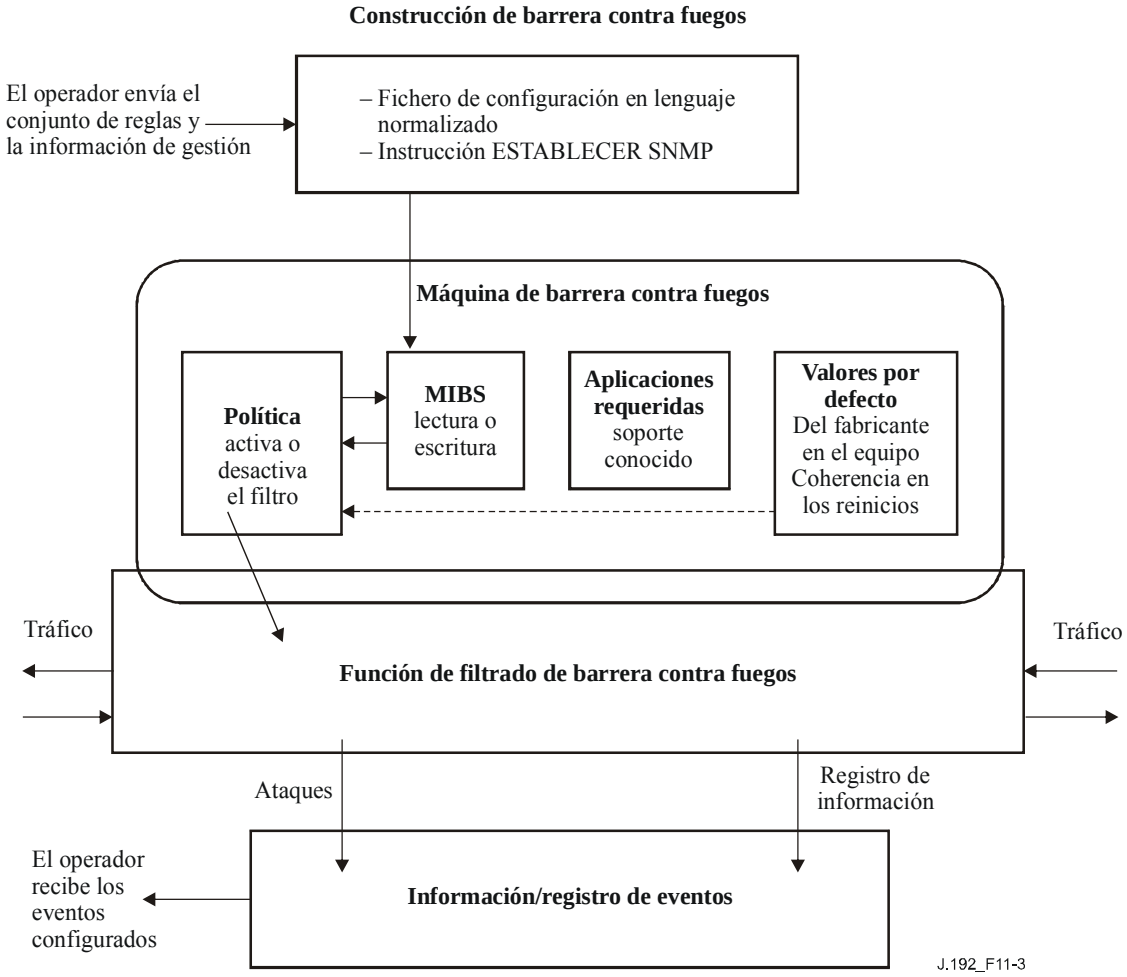


Figura 11-3/J.192 – Referencia lógica de barrera contra fuegos

11.6.4 Requisitos de la barrera contra fuegos

11.6.4.1 Lenguaje del fichero de configuración para la barrera contra fuegos

El conjunto de reglas escogido por el operador de cable puede configurarse en la barrera contra fuegos, a través de un fichero de configuración PS o descargando un fichero de configuración de barrera contra fuegos. En esta cláusula, fichero de configuración significa bien el del PS o el de la barrera. Se definen el lenguaje y formato del fichero de configuración, que contienen el conjunto de reglas que se aplica a determinado producto de barrera contra fuegos.

El PS DEBE poder recibir e interpretar ficheros de configuración de barrera contra fuegos construidos utilizando los TLV con el formato que se describe en 7.4.4.1, Requisitos del formato del fichero de configuración. Dentro de la barrera contra fuegos, el compilador traduce el lenguaje de política al formato interno propio del fabricante. Se DEBE utilizar el TLV tipo 28 para a todos los objetos MIB de barrera contra fuegos. El lenguaje de los ficheros de configuración del PS y de barrera contra fuegos ha de ser el mismo. En la cláusula 7 se definen los requisitos que ha de cumplir el procesamiento del fichero de configuración de barrera contra fuegos.

11.6.4.2 Configuración de barrera contra fuegos

El PS soporta, aunque no sea obligatorio para el operador, la gestión a distancia de las funciones de la barrera contra fuegos. La barrera contra fuegos del PS DEBE aceptar los conjuntos de reglas configurados en bloque, a través de los ficheros de configuración de la barrera contra fuegos del PS o configurados individualmente mediante instrucciones SNMP SET. El PS NO DEBE activar la barrera contra fuegos mientras el valor de cabhPsDevProvState = inProgress(2). Cuando se utiliza un fichero de configuración para configurar conjuntos de reglas, una vez concluida la descarga y el procesamiento del fichero de configuración, es decir, cuando cabhPsDevProvState = pass(1), DEBEN aplicarse inmediatamente las reglas para la barrera contra fuegos del fichero de configuración, quedando disponibles para su utilización en el PS sin necesidad de rearrancarlo.

Si por algún motivo el PS no puede procesar el fichero de configuración, es decir, si cabhPsDevProvState = fail(3), el PS DEBE utilizar las reglas del filtro de la barrera contra fuegos existentes indicadas por el objeto cabhSec2FwPolicySelection.

11.6.4.3 Política y conjunto de reglas de la barrera contra fuegos

La política indica cómo debe realizar el filtrado del tráfico la barrera contra fuegos en base a ciertas reglas. La política acepta el conjunto de reglas a aplicar mediante la función de filtrado, puesto que ésta no tiene ningún significado como ente independiente, ya que solamente es un conjunto de capacidades. Las capacidades de filtrado de la barrera contra fuegos, junto con la política aplicable, proporcionan a la LAN la protección propia de la barrera contra fuegos. Los filtros de barrera contra fuegos inspeccionan constantemente cada paquete o conexión con el fin de aplicar una de las dos acciones permitidas: permitir o negar su paso.

IPCable2Home define tres componentes como posibles formas de aplicar la política de la barrera contra fuegos en función de la configuración:

- Reglas generales de comportamiento – es el comportamiento esperado para aceptar o rechazar flujos de tráfico. Estas reglas se aplican siempre salvo que haya una excepción escrita en el conjunto de reglas de fábrica por defecto IPCable2Home o en el conjunto de reglas configuradas.
- Conjunto de reglas de fábrica por defecto IPCable2Home – son las reglas de fábrica por defecto de filtrado de la barrera contra fuegos utilizadas como excepciones a las reglas generales de comportamiento. Estas reglas también pueden utilizarse conjuntamente con el conjunto de reglas configuradas.
- Conjunto de reglas configuradas – conjunto de reglas configuradas utilizadas como excepciones a las reglas generales de comportamiento. Estas reglas también pueden utilizarse conjuntamente el conjunto de reglas de fábrica por defecto IPCable2Home.

Las reglas generales de comportamiento, el conjunto de reglas de fábrica por defecto IPCable2Home y el conjunto de reglas configuradas se aplican al tráfico de inicio de sesión y no al tráfico de respuesta.

Puede ocurrir que el PS reciba tráfico del MTA de IPCablecom, por lo que conviene repasar brevemente el soporte necesario para este adaptador de terminal multimedia. En 11.6.4.4 se describe el soporte de IPCableCom, que consiste en conjuntos de reglas de fábrica por defecto para IPCable2Home más los protocolos necesarios a fin de permitir que la mensajería IPCablecom atraviese la barrera contra fuegos. Asimismo, en el anexo D se indica cuáles puertos se deben abrir para el MTA. Gracias al soporte de IPCableCom se puede configurar, gestionar y prestar servicios a través de la barrera contra fuegos.

11.6.4.3.1 Política de barrera contra fuegos y sectores de direcciones

En esta Recomendación se define el concepto de sectores de direccionamiento IP para direcciones IP de WAN y LAN. Aunque se considera que el PS forma parte de la LAN, los paquetes que provienen del PS o que le están destinados no se consideran tráfico LAN a efectos del filtrado de la barrera contra fuegos. En su lugar, se utiliza la dirección IP específica del PS. Los paquetes que provienen del PS o que le están destinados se indican mediante la utilización de la dirección IP de WAN-Man, la dirección IP de encaminador de servidor PS o la dirección IP fija 192.168.0.1 (que puede ser, aunque no es obligatorio, la dirección IP de encaminador de servidor PS). Siendo así, la barrera contra fuegos distinguirá el tráfico saliente y entrante al PS en el conjunto de reglas de fábrica por defecto y en el conjunto de reglas configuradas. El comportamiento de la barrera contra fuegos es independiente de los sectores de direccionamiento definidos en 5.1.3. Las reglas de la barrera contra fuegos no se ven afectadas por el modo de tratamiento de paquetes primario o los modos de direccionamiento de la WAN.

11.6.4.3.2 Comportamiento general de la barrera contra fuegos

La barrera contra fuegos del PS ha de filtrar el tráfico en función de las reglas generales de comportamiento especificadas. Estas reglas se especifican para proporcionar un nivel básico de comportamiento de filtrado de la barrera contra fuegos del PS. El comportamiento general se aplica salvo que se defina una excepción en el conjunto de reglas por defecto o configuradas. Los estados definidos en las reglas generales de comportamiento son permitir o rechazar tráfico. Cuando las reglas generales de comportamiento están activas, el operador de cable espera que el PS filtre el tráfico de la forma normalizada. El PS DEBE aplicar a cada paquete las reglas generales de comportamiento de filtrado de la barrera contra fuegos, tal como se especifica en el cuadro 11-18 sobre las reglas generales de comportamiento de la barrera contra fuegos IPCable2Home>>, salvo que la barrera contra fuegos se configure para utilizar otra regla escrita del conjunto de reglas de fábrica por defecto (cabhSec2FwFactoryDefaultFilterTable, véase E.5 o del conjunto de reglas configuradas (docsDevFilterIpTable).

Los filtros de la barrera contra fuegos en el lado LAN y en el lado WAN utilizan los filtros de paquetes del lado LAN (LPF, *LAN side packet filters*) y los filtros de paquetes del lado WAN (WPF, *WAN side packet filter*) respectivamente. El comportamiento por defecto se especifica en términos de los LPF y los WPF. Para una descripción detallada de la arquitectura de la barrera contra fuegos véase 11.6.4.6.1.

Cuadro 11-18/J.192 – Reglas generales de comportamiento de la barrera contra fuegos

Dispositivo origen	Dirección IP de destino	Regla general de comportamiento, WPF	Regla general de comportamiento, LPF
Cualquier dispositivo WAN	Dirección IP WAN-Man del PS	Negar todo	N/A
	Dirección IP WAN-Datos del PS	Negar todo	N/A
	Cualquier dirección IP LAN (modo transferencia)	Negar todo	Permitir todo
Dispositivo PS: Dirección IP WAN-Man O WAN-Datos	Cualquier dirección IP WAN	Permitir todo	N/A
	Cualquier dirección IP LAN	N/A	Negar todo
Dispositivo PS: Dirección IP del encaminador servidor O 192.168.0.1	Cualquier dirección IP WAN	Negar todo	N/A
	Cualquier dirección IP LAN	N/A	Permitir todo
Cualquier dispositivo LAN	Dirección IP del encaminador servidor PS O 192.168.0.1	N/A	Permitir todo
	WAN-Man PS O Dirección IP WAN-Datos	N/A	Negar todo
	Cualquier dirección IP WAN	Permitir todo	Permitir todo
N/A: No aplicable. El ejemplar de tráfico no pasa por la interfaz.			

11.6.4.3.3 Conjunto de reglas de fábrica por defecto

El conjunto de reglas de fábrica por defecto define un conjunto de reglas de filtrado que se aplican cuando se selecciona la opción de conjunto de reglas por defecto del objeto cabhSec2FwPolicySelection. El conjunto de reglas de fábrica por defecto IPCable2Home DEBE codificarse de forma permanente en el hardware del PS en el momento de la fabricación. El PS DEBE utilizar el conjunto de reglas de fábrica por defectoIPCable2Home cuando el objeto cabhSec2FwPolicySelection se fije en factoryDefault(1) o en factoryDefaultAndConfiguredRuleset (3). En el cuadro 11-19 se especifica el conjunto de reglas de fábrica por defecto. Ambos sectores de direcciones LAN, LAN-Trans y LAN-Pass, son tratados de igual manera por el conjunto de reglas de fábrica por defecto y etiquetados como direcciones IP LAN. La barrera contra fuegos DEBE poder consultar direcciones en el cuadro de correspondencias CAT a fin de aplicar políticas sobre la base de la dirección IP del dispositivo del anfitrión real. El cuadro basa la información en el inicio de sesión, no en el tráfico permitido. Por tanto, el conjunto de reglas de fábrica por defecto de la barrera contra fuegos se DEBE implementar para el inicio de sesión y no para el tráfico que se devuelve en respuesta a una sesión permitida. El tráfico que retorna como consecuencia de una petición de quien lo inicia, se interpreta como información de estado para una sesión, por lo que la barrera verificará el estado de la sesión tras haber verificado las políticas, a fin de garantizar que no se rechace un paquete que forme parte de la sesión en curso.

Cuadro 11-19/J.192 – Política de fábrica por defecto de la barrera contra fuegos

Dispositivo origen	Dirección IP de destino	Regla general de comportamiento, WPF	Regla general de comportamiento, LPF	Lista de excepciones del protocolo de filtrado (número de regla)
Cualquier dispositivo IP WAN	Dirección IP WAN-Man del PS	Negarltodo	N/A	Permitir ICMP (1) Permitir SNMP (2,3)
	Dirección IP WAN-Datos del PS	Negar todo	N/A	Permitir ICMP (15)
	Dirección IP del encaminador servidor del PS O 192.168.0.1	Negar todo	N/A	Ninguna
	Cualquier dirección IP LAN (modo transferencia)	Negar todo	Permitir todo	Permitir ICMP (4)
Dispositivo PS: Dirección IP WAN- Man O WAN-Datos	Cualquier dirección IP WAN	Permitir todo	N/A	Ninguna
	Cualquier dirección IP LAN	N/A	Negar todo	Permitir ICMP (5,16)
Dispositivo PS: Dirección IP del encaminador servidor O 192.168.0.1	Cualquier dirección IP WAN	Negar todo	N/A	Ninguna
	Cualquier dirección IP LAN	N/A	Permitir todo	Ninguna
Cualquier dispositivo LAN	Dirección IP del encaminador servidor o del PS O 192.168.0.1	N/A	Permitir todo	Ninguna
	Dirección IP WAN-Man O WAN-Datos del PS	N/A	Negar todo	Permitir ICMP (6,17)
	Cualquier dirección IP WAN	Permitir todo	Permitir todo	Negar Syslog (13,14)

El conjunto de reglas de fábrica por defecto de la barrera contra fuegos IPCable2Home enumeradas en el cuadro 11-20 DEBE implementarse en el objeto MIB cabhSec2FwFactoryDefaultFilterTable. El encabezamiento de las columnas se corresponden con los objetos MIB definidos en la MIB de seguridad (Security) IPCable2Home, pero dado que los nombres de los objetos son bastante largos, en el cuadro sólo se representa la parte variable del nombre del objeto. Las reglas que incluyen la dirección IP de WAN-Datos del PS se enumeran comenzando por el índice del cuadro 15, ya que el operador de cable puede facultativamente configurar una o más direcciones IP de WAN-Datos en el PS. Este cuadro puede rellenarse correctamente cuando el PS termina la configuración en función de cómo haya configurado el operador de cable las direcciones IP.

Cuadro 11-20/J.192 – Reglas de fábrica por defecto de la barrera contra fuegos

Índice del cuadro	Control	IfIndex	Dirección	Saddr	Smask	Daddr	Dmask	Protocolo	SourcePortLow	SourcePortHigh	DestPortLow	DestPortHigh	Continue
1	Permitir	1	1	WAN IP (0.0.0.0)	(0.0.0.0)	PS WAN-Man	(255.255.255.255)	1	0	65535	0	65535	true
2	Permitir	1	1	WAN IP (0.0.0.0)	(0.0.0.0)	PS WAN-Man	(255.255.255.255)	6	0	65535	161	161	true
3	Permitir	1	1	WAN IP (0.0.0.0)	(0.0.0.0)	PS WAN-Man	(255.255.255.255)	17	0	65535	161	161	true
4	Permitir	1	1	WAN IP (0.0.0.0)	(0.0.0.0)	LAN IP (0.0.0.0)	(0.0.0.0)	1	0	65535	0	65535	true
5	Permitir	255	2	PS WAN-Man	(255.255.255.255)	LAN IP (0.0.0.0)	(0.0.0.0)	1	0	65535	0	65535	true
6	Permitir	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	PS WAN-Man	(255.255.255.255)	1	0	65535	0	65535	true
7	Negar	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	6	0	65535	88	88	true
8	Negar	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	17	0	65535	88	88	true
9	Negar	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	6	0	65535	749	749	true
10	Negar	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	17	0	65535	749	749	true
11	Negar	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	6	0	65535	1293	1293	true
12	Negar	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	17	0	65535	1293	1293	true
13	Negar	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	6	0	65535	514	514	true
14	Negar	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	WAN IP (0.0.0.0)	(0.0.0.0)	17	0	65535	514	514	true
15	Permitir	1	1	WAN IP (0.0.0.0)	(0.0.0.0)	PS WAN-Data	(255.255.255.255)	1	0	65535	0	65535	true
16	Permitir	255	2	PS WAN-Data	(255.255.255.255)	LAN IP (0.0.0.0)	(0.0.0.0)	1	0	65535	0	65535	true
17	Permitir	255	1	LAN IP (0.0.0.0)	(0.0.0.0)	PS WAN-Data	(255.255.255.255)	1	0	65535	0	65535	true

El operador de cable puede configurar el PS con cualquier conjunto de reglas de barrera contra fuegos mediante el fichero de configuración o la instrucción establecimiento SNMP (SNMP Set). Cuando un operador de cable envía reglas al PS, dichas reglas se denominan conjunto de reglas configuradas. El PS DEBE almacenar las reglas configuradas en docsDevFilterIpTable [RFC 2669] y la información de programación de cualquier regla, en los objetos MIB definidos por IPCable2Home en cabhSec2FwFilterScheduleTable (véase E.5). El conjunto de reglas configuradas solo está activo para el filtrado si la barrera contra fuegos está habilitada y la selección de política se fija en configuredRuleset(2) o factoryDefaultAndConfiguredRuleset(3). El conjunto de reglas configuradas puede eliminarse de docsDevFilterIpTable fijando el valor de cabhSec2FwClearPreviousRuleset como true(1) (verdadero).

11.6.4.3.4 Conjunto de reglas configuradas

La política de filtrado de la barrera contra fuegos IPCable2Home puede configurarse creando reglas de filtrado en docsDevFilterIpTable y/o cabhSec2FwLocalFilterIpTable (véase 11.6.4.9.3). Se considera que dichas reglas de filtrado constituyen el conjunto de reglas configuradas. Las reglas de filtrado definidas en el conjunto de reglas configuradas se utilizan como excepciones a las reglas generales de comportamiento. El conjunto de reglas configuradas puede también utilizarse conjuntamente con las reglas de fábrica por defecto. Cuando se hace así, las reglas de filtrado

definidas en el conjunto de reglas configuradas se utilizan como excepciones a las reglas generales de comportamiento y al conjunto de reglas de fábrica por defecto.

Tanto docsDevFilterIpTable como cabhSec2FwLocalFilterIpTable tienen capacidades similares de configuración de reglas de filtrado. Disponer de ambos cuadros de filtros facilita la gestión del conjunto de reglas configuradas. Por ejemplo, docsDevFilterIpTable puede utilizarse para definir reglas genéricas de filtrado aplicables a múltiples dispositivos y cabhSec2FwLocalFilterIpTable puede utilizarse para definir reglas de filtrado específicas locales o de cliente que sólo se apliquen a dicho dispositivo. El operador puede también permitir al cliente configurar sus propias reglas de filtrado en cabhSec2FwLocalFilterIpTable.

El objeto MIB cabhSec2FwPolicySelection permite al operador seleccionar el conjunto de reglas de filtrado que se encuentran activas (véase 11.6.4.9.1). Si tanto docsDevFilterIpTable como cabhSec2FwLocalFilterIpTable están activas, es posible que haya reglas de filtrado en ambos cuadros que entren en conflicto. Por ejemplo, para el mismo paquete una regla de filtrado puede indicar permitir y otra regla, negar. Para resolver el conflicto entre ambas se utiliza el objeto MIB cabhSec2FwPolicyConfiguredRulesetPriority, que determina la prioridad de las reglas de filtrado. En caso de conflicto entre reglas de filtrado del conjunto de reglas configuradas, conjunto de reglas de fábrica por defecto y reglas generales de comportamiento, el PS DEBE dar prioridad al conjunto de reglas configuradas.

Cuando se crea una anotación a la regla de filtrado de la barrera contra fuegos en docsDevFilterIpTable o en cabhSec2FwLocalFilterIpTable que sea aplicable a una única dirección IP de LAN asignada dinámicamente por el PS (CDS), éste DEBE crear una reserva de licencia de dirección IP para dicha dirección. Ello garantiza que la dirección IP del dispositivo LAN que aplica la anotación de regla de filtrado de la barrera contra fuegos, no se modifica cuando se renueva la licencia. Una anotación a regla de filtrado de la barrera contra fuegos aplicable a una única dirección IP de origen o de destino tiene la máscara 255.255.255.255.

El PS DEBE determinar si la dirección IP de origen o de destino única de la correspondiente anotación de la regla de filtrado de la barrera contra fuegos es asignada dinámicamente por el CDS, por ejemplo, identificándola en cabhCdpLanAddrTable. Si existe la correspondiente anotación en dicho cuadro con un valor de cabhCdpLanAddrMethod igual a dynamicActive(4) o a dynamicInactive(3), el PS DEBE sustituir dicha anotación por una que represente una reserva de licencia para dicha dirección IP en el cuadro, es decir, una cuyo valor de cabhCdpLanAddrMethod sea valorpsReservationActive(6) o psReservationInactive(5) respectivamente. Si la correspondiente anotación no existe en cabhCdpLanAddrTable, el PS NO DEBE crear una reserva de licencia para dicha dirección IP. En ese caso, es posible que la dirección IP se asigne estáticamente al dispositivo IP de LAN.

Cuando una anotación de regla de filtro de barrera contra fuegos se elimina de la docsDevFilterIpTable o cabhSec2FwLocalFilterIpTable aplicable a una dirección IP asignada dinámicamente por el PS (CDS), éste DEBE eliminar de cabhCdpLanAddrTable la correspondiente reserva de licencia de dirección IP que había sido creada internamente (identificada mediante cabhCdpLanAddrMethod=psReservationActive(6)), en tanto que no exista la correspondiente anotación DMZ en cabhCapMappingTable que la requiera.

11.6.4.4 Soporte de IPCablecom

Cuando el operador utilice IPCablecom, es posible que la barrera contra fuegos deba dejar pasar tráfico desde el MTA y hacia él, dependiendo de la configuración de red y el dispositivo. Cuando se utilice una red IPCablecom, la barrera contra fuegos NO DEBE contradecir los protocolos definidos por el conjunto de Recomendaciones IPCablecom. Puede ocurrir que el operador de cable deba configurar la barrera contra fuegos con otras reglas adicionales a fin de garantizar que IPCablecom pueda funcionar a través de ésta. En el cuadro 11-21 figura una lista de especificaciones que tienen

requisitos de puerto único para la comunicación con el MTA. No obstante, no es una lista completa de todas las especificaciones IPCablecom.

Cuadro 11-21/J.192 – Especificaciones IPCablecom 1.x relevantes para la barrera contra fuegos de IPCable2Home

Descripción	Especificación
Especificación de códec de audio/vídeo	[Rec. UIT-T J.161]
Especificación de la calidad de servicio dinámica	[Rec. UIT-T J.163]
Especificación de protocolo de señalización de llamada basada en la red	[Rec. UIT-T J.162]
Especificación de configuración de dispositivo MTA	[Rec. UIT-T J.167]
Especificación de seguridad	[Rec. UIT-T J.170]
Especificación de mecanismo de evento de gestión	[Rec. UIT-T J.164]
Especificación de protocolo de servidor de audio	[Rec. UIT-T J.175]
Especificación de señalización de servidor de gestión de llamada	[Rec. UIT-T J.178]

La lista de los protocolos IPCablecom requeridos por el MTA proviene de las especificaciones indicadas. En el anexo D, Aplicaciones mediante traducción de direcciones de IPCable2Home y la barrera contra fuegos, figuran los números de puerto atribuidos por IANA para los puertos que necesitan los protocolos específicos de IPCablecom para pasar a través de la barrera contra fuegos. Los protocolos definidos en IPCablecom son:

- Configuración SNMPv3, DHCP, DNS, TFTP, SYSLOG
- Tren de medios RTP, RTCP
- QoS RSVP
- Seguridad Kerberos, IPSec
- Señalización de llamada de red MGCP, SDP

NOTA – SDP no requiere ningún puerto específico.

{texto informativo:

11.6.4.5 Soporte del servicio DMZ y WanIPConnection UPnP

Las correspondencias CAP de DMZ y WANIPConnection UPnP (UWIC) permiten que el tráfico no solicitado originado en la WAN atraviese la función CAP (NAPT) del PS. Para ello, el PS ha de crear reglas de filtrado de la barrera contra fuegos que correspondan con anotaciones de la tabla de correspondencias CAP de DMZ y UWIC que permitan el paso de dicho tráfico.

Cuando una aplicación LAN conforme con UPnP configure una correspondencia de puerto en cabhCapMappingTable, el valor del objeto MIB cabhCapMappingMethod será UPnP(3) (véase 8.3.4.9). Para cada anotación en cabhCapMappingTable cuyo objeto MIB cabhCapMappingMethod tenga el valor UPnP(3), el PS DEBE crear la correspondiente regla de filtrado de la barrera contra fuegos que permita el paso del tráfico no solicitado de WAN-a-LAN. Cuando se elimine una anotación en cabhCapMappingTable cuyo objeto MIB cabhCapMappingMethod tenga el valor UPnP(3), el PS DEBE eliminar la correspondiente regla de filtrado de la barrera contra fuegos.

Una anotación DMZ de cabhCapMappingTable tiene los valores de los puertos WAN y LAN puestos a cero (véase 8.3.3.2). Para cada anotación DMZ de cabhCapMappingTable, el PS DEBE crear la correspondiente regla de filtrado de barrera contra fuegos que permita el paso del tráfico de WAN-a-LAN. Cuando se elimina una anotación DMZ de cabhCapMappingTable, el PS DEBE eliminar la correspondiente regla de filtrado de la barrera contra fuegos.
}

11.6.4.6 Filtrado de barrera contra fuegos

En esta cláusula se especifican los requisitos del componente de filtrado de paquetes de la barrera contra fuegos. El filtro de paquetes especificado examina cada paquete y determina si debe permitir o impedir su paso a través de la barrera contra fuegos. En particular, examina los campos del encabezamiento de paquete y toma decisiones paquete por paquete, basándose en los contenidos de dichos campos y en el conjunto de reglas configuradas.

11.6.4.6.1 Conjunto mínimo de capacidades de filtrado

A efectos de IPCable2Home, no basta con tener simplemente una NAT o un filtro de paquetes, pues, a fin de proveer una solución segura y flexible, la barrera contra fuegos DEBE implementar un ASP o una barrera contra fuegos con SPF. Se necesitan también requisitos específicos de estas técnicas de filtrado con el fin de alcanzar un nivel suficiente de productos para la industria de cable que se puedan probar, que sean de fiar y que interfuncionen. El componente ASP/SPF de la barrera contra fuegos controla los flujos de tráfico asociados con protocolos de la capa de aplicación que no pueden ser controlados efectiva y transparentemente mediante el filtrado estático. Los mecanismos de filtrado examinarán las aplicaciones que se hayan establecido dinámicamente en sesiones IP, TCP, UDP o ICMP. La actividad de los puertos, las direcciones IP, y la programación (calendario) se gestiona como si fuera una "sesión" dentro de la barrera contra fuegos. Asimismo, gracias al apoderado específico de la aplicación, es posible que funcionen aplicaciones que no soporten NAT mientras el PS está en uno de sus dos modos transparentes de encaminamiento, a saber, C-NAT o C-NAPT.

Con independencia del tipo de barrera contra fuegos que se haya implementado, la correspondiente al PS DEBE conocer la sesión y poder rastrear la información sobre un par de direcciones IP (origen y destino), junto con la política en vigor válida para la dirección IP especificada. Por sesión se entiende el emparejamiento de direcciones IP, petición por petición. Cada petición incluye el establecimiento de una correspondencia con la política autorizada para dicha sesión, que consta de una dirección IP, un puerto de aplicación y una prohibición.

En la arquitectura de filtro de paquetes de la barrera contra fuegos se especifican filtros de paquetes diferentes para el lado WAN y para el lado LAN en el PS. El filtro de paquetes del lado WAN examina paquetes en la interfaz WAN originados en el dominio de la WAN, en el dominio de la LAN o en los componentes internos del PS. El filtro de paquetes del lado LAN examina paquetes en la interfaz LAN agregada originados en el dominio LAN, en el dominio WAN o en los componentes internos del PS. Pueden aplicarse reglas diferentes a los filtros de paquetes de los lados WAN y LAN.

Los componentes del PS están ubicados de una forma relacionada con la barrera contra fuegos, tal como se muestra en la figura 11-4. Los paquetes que recibe el PS de los dominios WAN o LAN son filtrados por la barrera contra fuegos antes de alcanzar cualquiera de los componentes del PS que no sean de la barrera contra fuegos, es decir, CDP, CNP, CSP, CQP, CMP y CAP, con la excepción del USFS. Igualmente, los paquetes que debe transmitir el PS a los dominios WAN o LAN pasarán a través de los componentes no pertenecientes a la barrera contra fuegos antes de alcanzar el WPF o el LPF.

Los WPF y LPF también actúan sobre los paquetes originados en los componentes internos del PS. Estos paquetes son filtrados por el WPF y el LPF antes de ser retransmitidos a los dominios WAN o LAN, respectivamente.

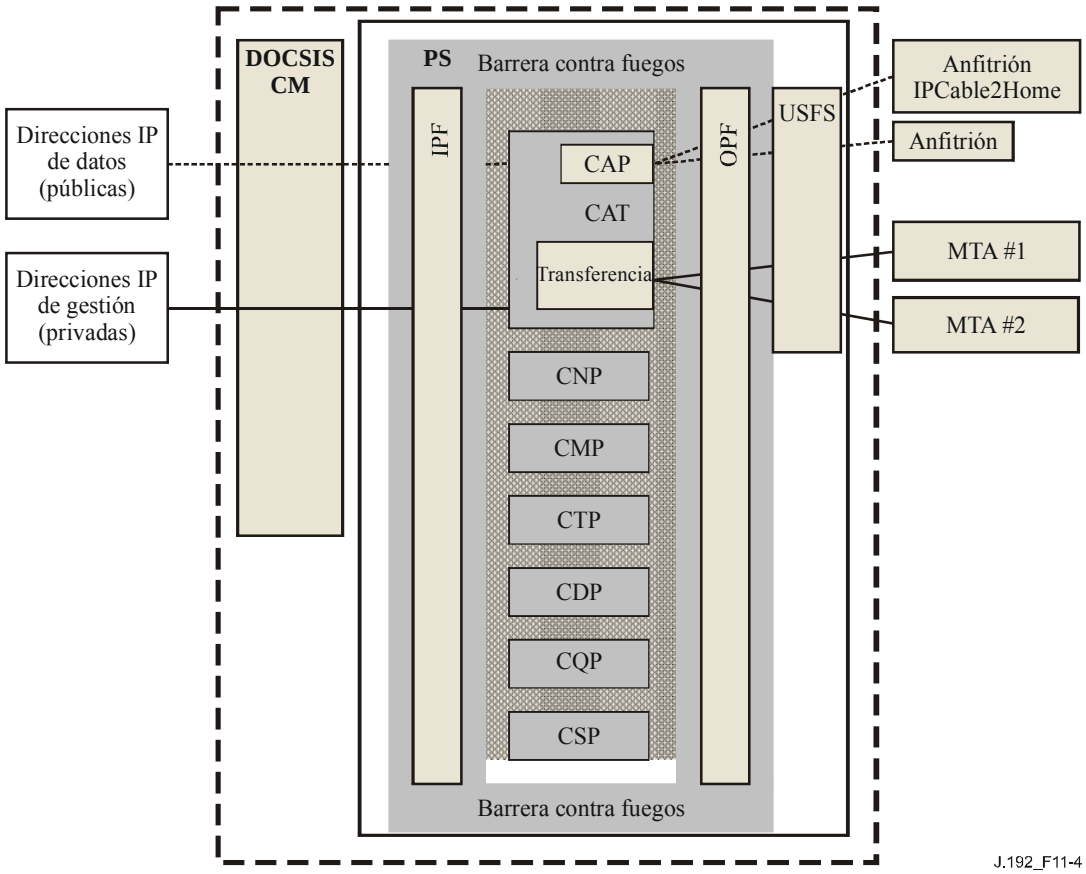


Figura 11-4/J.192 – Funcionalidad de barrera contra fuegos dentro del PS

Se utilizan las siguientes definiciones de filtrado:

- PERMITIDO (ALLOW), es decir, "se deja pasar el paquete".
- PROHIBIDO (DENY), es decir, "se elimina el paquete".

Los filtros WPF y LPF de la barrera contra fuegos DEBEN comportarse de la siguiente manera:

- La barrera contra fuegos DEBE filtrar el tráfico en función de la política definida de IPCable2Home, tal como se describe en 11.6.4.3, Política y conjunto de reglas de la barrera contra fuegos, en los casos en los que no haya una regla explícita que seguir cuando se verifica un paquete.
- La barrera contra fuegos DEBE prohibir el paso de paquetes reproducidos bien sea desde la LAN o desde la WAN.
- La barrera contra fuegos DEBE crear un "estado" para todos los paquetes permitidos que inician una sesión. Un paquete se aceptará si existe una regla estática que permite paquetes conformes a dicho criterio, o bien hay un estado que implica que debe dejarse pasar el paquete, como resultado de una sesión saliente permitida.
- La barrera contra fuegos NO DEBERÍA permitir tráfico saliente TCP antes de establecerse una sesión TCP (es decir, antes de completar una toma de contacto TCP "3-way" (3 pasos)).
- Se DEBEN prohibir los paquetes que tengan una de las siguientes opciones IP: ruta flexible de origen (LSRR, *loose-source-route*), ruta estricta de origen (SSRR, *strict-source-route*), y ruta de registro (RR, *record-route*).

Existen muchos tipos de ataques a la red que pueden ser filtrados por la barrera contra fuegos. En estos ataques se utilizan diversos métodos y herramientas contra los dispositivos que pertenecen a la red. La lista correspondiente es bastante larga y cambia con una frecuencia tal, que ningún

documento publicado actualmente puede tenerla al día. En esta Recomendación se mencionan algunos de los ataques más conocidos, a efectos de consideraciones generales de seguridad. La barrera contra fuegos DEBERÍA proteger contra los barridos de puerto o red lanzados desde la LAN o desde la WAN, contra la inundación de paquetes o los paquetes deformados, contra la siguiente lista de ataques por denegación de servicio: "Ping of Death", "Teardrop", "Bonk", "Nestea", "SYN Flood", "LAND Attack", "IP Spoofing", "Smurf Attack", "WinNuke", y todo tipo de mensajería de alta frecuencia que se origine en dispositivos IP de LAN, como por ejemplo mensajes BP_Init o DHCP DISCOVER.

11.6.4.6.2 Criterios de filtrado

La acción por defecto consiste en prohibir el tráfico iniciado en direcciones IP de WAN, direcciones IP de WAN-Man del PS, o direcciones IP de encaminador de servidor del PS. El conjunto de reglas se establecen, por tanto, para permitir cierto tráfico proveniente de dichas direcciones. De igual manera, se permite por defecto el tráfico proveniente de direcciones IP de LAN, a menos que se haya configurado explícitamente su prohibición, por lo que el conjunto de reglas se establece para prohibir cierto tipo de tráfico proveniente de estas direcciones. Aunque en esta cláusula no se especifican todas las capacidades de filtrado previstas, sí figura una lista del conjunto mínimo de criterios ampliado mediante objetos MIB especificados. Los filtros de paquetes entrantes y salientes DEBEN examinar el tráfico a fin de comprobar cuándo una regla permite su paso, basándose en los siguientes criterios de filtrado:

- dirección IP de origen;
- dirección IP de destino;
- protocolo IP ("de siguiente nivel"); por ejemplo, TCP, UDP, ICMP, IPsec AH, IPsec ESP;
- puertos de origen y destino de TCP o UDP;
- información de inicio de conexión de los paquetes TCP (es decir, la ausencia del bit ACK), para el seguimiento de la sesión;
- seguimiento de número de secuencia de las sesiones.

Esta información de paquete se utiliza como criterio para comprobar si los paquetes entrantes cumplen determinada regla y, por ende, en la toma de decisiones particulares de filtrado (permitir, prohibir). La barrera contra fuegos DEBE verificar las direcciones IP de origen y destino para comprobar si se les aplica alguna regla. Cuando el conjunto de reglas prohíba el reenvío de tráfico hacia una dirección IP o desde ella, la barrera contra fuegos DEBE rechazar el paquete, al menos que éste deba pasar como resultado de su estado.

NOTA – El filtrado, de acuerdo con la política en vigor, incluye más requisitos que, aunque deben ser aplicados, no se consideran parte de los criterios de filtrado incorporados.

11.6.4.6.3 Arquitectura de filtrado

El filtro de paquetes de la barrera contra fuegos tendrá la capacidad de filtrar el tráfico con diferentes criterios de filtrado para el tráfico originado en WAN, LAN o PS. La barrera contra fuegos DEBE:

- Filtrar paquetes en la interfaz WAN que se originan en cualquiera de los lados de la misma. Las reglas de filtrado en el lado de la WAN del PS se identifican mediante el valor 1 (uno) de IfIndex y se aplica a todo el tráfico originado y dirigido a la WAN.
- Filtrar paquetes en la interfaz de interfaces LAN agregadas del PS, valor 255 de ifIndex, originados a ambos lados de la interfaz.
- Filtrar paquetes que se originan dentro del PS y dirigidos hacia la LAN o la WAN.
- Aplicar sólo los filtros actualmente habilitados.
- Aplicar el filtrado de los paquetes antes de cualquier procesamiento de ASP/SPF

- Aplicar el filtrado a los paquetes que recibe el PS antes de pasarlos a cualquiera de los componentes del PS que no pertenezcan a la barrera contra fuegos. Sin embargo, puesto que la barrera contra fuegos no es necesaria para poder realizar el filtrado del tráfico interior de la LAN (LAN – LAN), el tráfico originado en el lado LAN y recibido por el PS encuentra al USFS antes que al LPF.

El WPF DEBE exhibir el siguiente comportamiento general:

- Realizar el filtrado tal como se define en 11.6.4.3.
- Rechazar todos los paquetes que entran en el PS desde la WAN y que tienen direcciones origen que pertenecen a los sectores de direcciones LAN-Pass o LAN-Trans.
- Rechazar todos los paquetes que tengan direcciones de origen de difusión o multidifusión.

El LPF DEBE tener el siguiente comportamiento general:

- Realizar el filtrado tal como se define en 11.6.4.3.
- Rechazar todos los paquetes que tengan direcciones de origen de difusión o multidifusión.

11.6.4.7 Informe de eventos en la barrera contra fuegos

La información que proviene de la barrera contra fuegos es crucial para las labores de gestión y supervisión de rutina, y también porque genera los eventos adecuados en caso de ataques especificados. Se pueden usar los eventos generados por ella a fin de detectar intrusos, ataques de tipo (denegación de servicio, DoS *denial of service*) y fallos o registros que tenga relación con el sistema de la barrera contra fuegos. Cuando hay grandes cantidades de datos, el análisis y clasificación de los registros puede ser bastante dispendioso. Asimismo, de enviarse demasiados eventos al operador de cable, puede haber un consumo exagerado de ancho de banda (muchas barreras contra fuegos enviando al mismo tiempo eventos a su NMS). El operador habrá de decidir cuáles elementos se han de activar para supervisar la barrera contra fuegos y con que frecuencia desea recibir los eventos. La activación de la información de eventos se hace separadamente de aquella del conjunto de reglas para los criterios de filtrado de la barrera contra fuegos. Una vez se hayan puesto los objetos MIB que habilitan eventos de tal manera que se permita a la barrera contra fuegos realizar el seguimiento de tipos definidos de eventos, ésta registrará y enviará mensajes relacionados con el evento especificado, de conformidad con esta cláusula y con el anexo B.

El operador de cable tiene la posibilidad de activar o desactivar cada tipo de eventos especificados mediante el objeto MIB SNMP, a través de un fichero de configuración o de una instrucción SNMP Set. Conviene utilizar el SNMPv3 para asegurar los mensajes SNMP que contengan información relativa a la barrera contra fuegos.

11.6.4.7.1 Eventos de la barrera contra fuegos

Gracias a estos eventos, el operador de cable puede evaluar a distancia el nivel de actividad de intrusos y de las modificaciones a la barrera contra fuegos en determinados elementos del PS. La generación de eventos se basa en cambios de gestión del conjunto de reglas, en los eventos detectados por la barrera contra fuegos y habilitados por dicho conjunto de reglas, o en los eventos TFTP/HTTP basados en la descarga. Estos últimos, cuando están destinados a descarga de la barrera contra fuegos, se DEBEN enviar con arreglo al anexo B.

La barrera contra fuegos DEBE poder registrar los siguientes tipos de eventos:

TIPO 1: Se DEBEN registrar todos los intentos, tanto de clientes de LAN como de WAN, de atravesar la barrera contra fuegos que violen la política de seguridad, siempre que este tipo se hubiere activado a través del objeto MIB cabhSec2FwEventEnable. Se registran todos los intentos de conexión que hayan sido descartados como consecuencia de una violación de la política. Un ataque se define como un paquete (es decir que cada paquete se cuenta como un ataque), que intenta atravesar la barrera contra fuegos y viola la política en vigor. Cuando se haya habilitado este tipo y se alcance el umbral, el PS DEBE enviar inmediatamente el evento 80010201.

TIPO 2: Se DEBEN registrar los intentos de ataque identificados como denegación de servicio, siempre que esté activo este tipo, a través del objeto MIB cabhSec2FwEventEnable. Se define un ataque del tipo 2 como cualquier intento que se considere que perturbe el servicio, como por ejemplo la saturación de paquetes duplicados (se considera que 10 paquetes son un intento), o paquetes deformados o intentos de conexión sin permiso provenientes del mismo anfitrión, en múltiples ocasiones. Cuando se haya habilitado este tipo, y se alcance el umbral permitido, el PS DEBE enviar inmediatamente el evento 80010202.

TIPO 3: Se DEBE registrar cualquier cambio efectuado a los objetos MIB cabhSec2FwPolicyFileURL, cabhSec2FwPolicyFileCurrentVersion o cabhSec2FwEnable cuando esté activado este tipo, a través del objeto MIB cabhSec2FwEventEnable. El seguimiento de los cambios en la configuración de la barrera contra fuegos otorga al operador de cable un conocimiento valioso y eficaz, a efectos de corregir errores. Cuando esté habilitado este tipo y se alcance el umbral, el PS DEBE enviar inmediatamente el evento 80010203.

TIPO 4: Se DEBEN registrar todos los intentos infructuosos de modificar los objetos MIB cabhSec2FwPolicyFileURL y cabhSec2FwEnable cuando esté activado este tipo, a través de la MIB cabhSec2FwEventEnable. De estar habilitado este tipo y si se alcanza el umbral, el PS DEBE enviar inmediatamente el evento 80010204.

TIPO 5: Se DEBEN registrar los paquetes entrantes permitidos que provienen de la WAN cuando esté activado este tipo, a través del objeto MIB cabhSec2FwEventEnable. Gracias a este tipo, el operador de cable puede supervisar el tráfico en caso de que existan indicios de detección de intromisión o ataques DoS del lado WAN. De estar habilitado este tipo y si se alcanza el umbral, el PS DEBE enviar inmediatamente el evento 80010205.

TIPO 6: Se DEBEN registrar los paquetes salientes permitidos que provienen de la LAN cuando esté activado este tipo, a través del objeto MIB cabhSec2FwEventEnable. Gracias a este tipo, el operador de cable puede supervisar el tráfico en caso de que existan indicios de ataques provenientes de una LAN doméstica a través de la WAN. De estar habilitado este tipo y de alcanzarse el umbral, el PS DEBE enviar inmediatamente el evento 80010206.

Se definen los tipos de evento para IPCable2Home a efectos de supervisión solamente. Es potestad de cada operador de cable evaluar y ejecutar la respuesta necesaria a los eventos detectados e informados por la barrera contra fuegos.

11.6.4.7.2 Registros de la barrera contra fuegos

La información de registro de la barrera contra fuegos DEBE almacenarse en el PS por cada tipo de registro habilitado, conforme a lo indicado en 11.6.4.7.1. Para cada tipo de evento habilitado, el PS DEBE registrar la información especificada en cabhSec2FwLogTable cuando el cómputo de eventos alcance un umbral dado en el intervalo de registro. El cómputo de eventos, el umbral y el intervalo se definen para cada tipo de evento en cabhSec2FwEventControlTable (cabhSec2FwEventCount, cabhSec2FwEventThreshold y cabhSec2FwEventInterval según 11.6.4.9.2). Cualquier evento que se registre en cabhSec2FwLogTable también DEBE registrarse en docsDevEventTable, siempre que se cumplan las restricciones adicionales por estrangulamiento aplicables a docsDevEventTable especificadas en 6.3.3.2.4.8.

Si la tabla de registros históricos está llena, el PS DEBE eliminar la anotación más antigua y añadir la nueva. Si cabhSec2FwEventThreshold no está puesto a cero, cabhSec2FwEventEnable está habilitado y cabhSec2FwEventInterval no está puesto a cero, el PS DEBE seguir registrando eventos del tipo habilitado. Una vez que cabhSec2FwEventLogReset se haya puesto a 1 a fin de borrar el registro, y si cabhSec2FwEventEnable está habilitado, cabhSec2FwEventCount DEBE iniciar su cuenta desde cero.

El PS, como mínimo DEBE soportar el registro de 40 anotaciones en el cuadro de registros de la barrera contra fuegos (cabhSec2FwLogTable). Cuando se habilita un tipo de evento, el PS DEBE

registrar la información requerida por el mismo a una velocidad mínima de 1 evento cada 5 segundos, también cuando esté siendo atacado. Se prevé que el PS no consumirá la mayor parte de sus recursos de computación en las actividades de registro y que cuando esté sometido a un ataque DEBERÍA poder hacer pasar el tráfico a velocidad normal y funcionar normalmente.

Cuando no se efectúa adecuadamente el registro puede haber varios problemas. Registrar todos los eventos y paquetes es bastante complejo, prolongado y difícil de entender. Es difícil buscar un ítem en particular en una gran cantidad de información. Con todo, cuando se limita el registro a pocos tipos de eventos el operador de cable no dispondrá de información suficiente para depurar las intrusiones o detectar los ataques. Cabe observar que es posible entrar sin permiso a aquellos registros que no estén criptados. De tener acceso a la información de registro, un atacante puede adquirir un conocimiento importante de los diversos servicios que funcionan en los dispositivos del anfitrión de LAN o del PS.

En IPCable2Home es necesario registrar un determinado conjunto de información para cada tipo de evento habilitado. La función de registro DEBE registrar paquetes de cada tipo de conformidad con las reglas propias de cada uno de ellos. Los requisitos relativos a la fecha y hora se asumen en la hipótesis de que estas dos variables tendrán la precisión correspondiente a la última actualización del reloj del PS durante la secuencia de configuración.

Se DEBE registrar en el cabhSec2FwLogTable de los tipos de eventos 1, 2, 5 y 6, la siguiente información, cada vez que se presente un evento, a menos que se especifique lo contrario:

- Número de evento – Se DEBE registrar conforme al anexo B, una vez, al inicio del registro.
- Prioridad de evento – Se DEBE registrar conforme al anexo B, una vez, al inicio del registro.
- Fecha y hora – Cuando ocurre el evento:
  - DEBE incluir el día, el mes y las cuatro cifras del año;
  - DEBE incluir la hora, los minutos y los segundos.
- Protocolo – El que se indica en el campo del encabezamiento IP (1 = ICMP; 2 = IGMP; 6 = TCP; 17 = UDP).
- Dirección IP de origen.
- Dirección IP de destino.
- Puerto de origen (TCP y UDP).
- Puerto de destino (TCP y UDP).
- Tipo de mensaje (ICMP) – En [RFC 2474] se define el ICMP. Cuando la barrera contra fuegos bloquee un paquete ICMP el registro DEBE indicar un número que señale de qué tipo de mensaje ICMP se trataba. 0 – Respuesta de eco, 3 – Destino inaccesible, 4 – Disminución de tráfico de origen, 5 – Redireccionamiento, 8 – Petición de eco, 9 – Anuncio de encaminador, 10 – Petición de encaminador, 11 – Rebasamiento de tiempo, 12 – Problema de parámetro, 13 – Petición de indicación de tiempo, 14 – Respuesta de indicación de tiempo, 15 – Petición de información, 16 – Respuesta de información, 17 – Petición de máscara de dirección, 18 – Respuesta de máscara de dirección.
- Conteo de reproducción – Cuando se esté registrando un ataque de reproducción, la barrera contra fuegos NO DEBERÍA registrar cada evento de ataque. No obstante, SÍ DEBERÍA registrar la cantidad de ataques hasta que se alcance el valor del umbral especificado para dicho tipo.
- Nombre del cuadro del filtro de concordancias (cuando sea aplicable) – cuando el evento se genera debido a la concordancia de un paquete con una anotación del cuadro de reglas del filtro, DEBE suministrarse el nombre del cuadro del filtro (docsDevFilterIpTable, cabhSec2FwFactoryDefaultFilterTable o cabhSec2FwLocalFilterIpTable).

- Índice del cuadro del filtro de concordancias (cuando sea aplicable) – cuando el evento se genera debido a debido a la concordancia de un paquete con una anotación del cuadro de reglas del filtro, DEBE suministrarse el índice del cuadro del filtro.
- Descripción del filtro de concordancias (cuando sea aplicable) – cuando el evento se genera debido a una concordancia de paquetes de una anotación en el cuadro de reglas del filtro, DEBE suministrarse la descripción del filtro.

En el cabhSec2FwLogTable para el evento de tipo 3 se DEBE registrar la siguiente información de cada evento, a menos que se especifique lo contrario:

- Número de evento – Se DEBE registrar conforme al anexo B, una vez, al inicio del registro.
- Prioridad de evento – Se DEBE registrar conforme al anexo B, una vez, al inicio del registro.
- Fecha y hora – Cuando ocurre el evento:
  - DEBE incluir el día, el mes y las cuatro cifras del año;
  - DEBE incluir la hora, los minutos y los segundos.
- Dirección IP de origen.
- Objeto MIB modificado.

En el cabhSec2FwLogTable para el evento tipo 4 se DEBE registrar el siguiente tipo de información de cada evento, a menos que se especifique lo contrario:

- Número de evento – Se DEBE registrar conforme al anexo B, una vez, al inicio del registro.
- Prioridad de evento – Se DEBE registrar conforme al anexo B, una vez, al inicio del registro.
- Fecha y hora – Cuando ocurre el evento:
  - DEBE incluir el día, el mes y las cuatro cifras del año;
  - DEBE incluir la hora, los minutos y los segundos.
- Dirección IP de origen.
- Intento de modificación del objeto MIB.

11.6.4.8 Aplicaciones a través de la barrera contra fuegos

Como parte del conjunto mínimo de capacidades, la barrera contra fuegos DEBE poder permitir que aplicaciones especificadas, como se define en el anexo D, atraviesen el PS y lleguen al destino previsto. La barrera contra fuegos aplica el conjunto de reglas en vigor a la política a fin de garantizar que se prevean las aperturas adecuadas para soportar tráfico específico entre la LAN y la WAN, así como hacia el PS y desde el mismo. El PS NO DEBE limitar el número de sesiones o conexiones a soportar simultáneamente, salvo que se especifique otra cosa en el anexo D, Aplicaciones mediante CAT y la barrera contra fuegos.

La política de la barrera contra fuegos se aplica al tráfico a medida que éste intenta atravesarla. Se procesan primero los paquetes en la barrera contra fuegos antes de enviarlos al PS, para que siga su procesamiento, o a la WAN o LAN de destino. Se aplica la política a las direcciones IP, puertos y hora del día de origen y destino. En el anexo D figuran los requisitos y se dan más detalles al respecto.

11.6.4.9 Objetos MIB de la barrera contra fuegos

Los objetos MIB de barrera contra fuegos constan de tres partes principales, a saber:

1) un conjunto para gestionar la configuración de la barrera contra fuegos;
2) uno para supervisar y registrar eventos; y
3) uno para gestionar el conjunto de reglas propiamente dicho.

Se DEBEN utilizar los requisitos para los objetos MIB de barrera contra fuegos junto con el documento MIB de seguridad [véase E.5].

11.6.4.9.1 Objetos MIB de gestión de conjunto de reglas de la barrera contra fuegos

En el PS DEBEN implementarse los siguientes objetos de gestión de la barrera contra fuegos:

cabhSec2FwPolicyFileURL – Contiene el nombre del fichero de conjunto de reglas de política y la dirección IP del servidor TFTP o HTTPS donde está dicho fichero, en un formato URL TFTP o HTTPS. Se activa la descarga del fichero del conjunto de reglas de política cuando el valor utilizado para ESTABLECER (SET) esta MIB sea diferente del valor de la MIB cabhSec2FwPolicySuccessfulFileURL. Véase 7.4.4.2.3, Activación de fichero de configuración de la barrera contra fuegos.

Cuando falle la descarga del fichero de configuración de barrera contra fuegos, el PS NO DEBE actualizar la MIB cabhSec2FwPolicySuccessfulFileURL con el mismo valor de la MIB cabhSec2FwPolicyFileURL. En todo caso, el objeto MIB cabhSec2FwPolicyFileURL DEBE incluir el valor SET bien sea por el fichero de configuración del PS o mediante una instrucción SET SNMP. Cuando se reinicie el PS, se DEBE asignar este valor al objeto MIB cabhSec2FwPolicyFileURL.

CabhSec2FwPolicySuccessfulFileURL – Contiene el nombre del fichero de conjunto de reglas de política y la dirección IP del servidor TFTP que incluye dicho fichero, en un formato URL TFTP o HTTPS, que haya sido utilizado para activar la última descarga exitosa. De no haber habido aún una descarga, este MIB deberá tener el valor Nulo.

cabhSec2FwPolicyFileHash – Define el compendio SHA-1 para el fichero del conjunto de reglas correspondiente.

cabhSec2FwPolicyFileOperStatus – Indica el estado operacional de la descarga del fichero de configuración de la barrera contra fuegos y DEBE incluir los tres estados siguientes:

- inProgress(1) – hay una descarga de fichero de configuración de barrera contra fuegos en curso.
- complete(2) – la descarga del fichero de configuración de barrera contra fuegos ha sido completada con éxito.
- failed(3) – el último intento de descarga de fichero de configuración de barrera contra fuegos fracasó.

cabhSec2FwPolicyFileCurrentVersion – Etiqueta puesta por el operador del cable que se utiliza para rastrear diversas versiones de conjuntos de regla configurados. Cuando esta etiqueta está establecida por SNMP o un fichero de configuración, su valor esta modificado y las reglas de filtro de barrera contra fuegos configurado son modificadas. Sin embargo, como las reglas de filtro de barreras contra fuegos se pueden modificar utilizando SNMP después de la configuración inicial por el fichero de política (fichero de configuración de barrera contra fuegos), el valor de esta etiqueta (por ejemplo, la versión vigente del fichero de política), puede no corresponder correctamente a la configuración de barrera contra fuegos actualmente vigente. Si no ha sido configurado antes, este objeto DEBE contener la cadena "null".

cabhSec2FwEnable – Permite activar y desactivar la barrera contra fuegos. Cuando este objeto sea inhabilitado, la barrera contra fuegos DEBE desactivarse completamente. Cuando sea habilitado, la barrera contra fuegos DEBE activarse inmediatamente sin que sea necesario rearrancar el PS.

cabhSec2FwClearPreviousRuleset – Permite al operador suprimir las anotaciones de la regla de filtrado de docsDevFilterIpTable.

cabhSec2FwPolicySelection – Permite la selección de la política de filtrado tal como se define mediante las opciones siguientes:

- factoryDefault (1) – Indica que la barrera contra fuegos está utilizando la configuración de fábrica por defecto definida en 11.6.4.3.3. Si el objeto MIB cabhSec2FwPolicySelection se fija como factoryDefault (1), la barrera contra fuegos realiza el filtrado teniendo en cuenta el conjunto de reglas de fábrica por defecto de cabhSec2FwFactoryDefaultFilterTable.
- configuredRulesetBoth (2) – Indica que la barrera contra fuegos está utilizando el conjunto de reglas configuradas definido mediante docsDevFilterIpTable y cabhSec2FwLocalFilterIpTable. Si el objeto MIB cabhSec2FwPolicySelection se fija como configuredRulesetBoth (2), los filtros de la barrera contra fuegos realizan el filtrado teniendo en cuenta las reglas definidas en docsDevFilterIpTable y cabhSec2FwLocalFilterIpTable.
- factoryDefaultAndConfiguredRulesetBoth (3) – Indica que la barrera contra fuegos está utilizando el conjunto de reglas de fábrica por defecto y el conjunto de reglas configuradas definidas en docsDevFilterIpTable y cabhSec2FwLocalFilterIpTable. Si el objeto MIB cabhSec2FwPolicySelection se fija como factoryDefaultAndConfiguredRulesetBoth (3), el PS DEBE realizar el filtrado teniendo en cuenta las reglas de fábrica por defecto especificadas por IPCable2Home en cabhSec2FwFactoryDefaultFilterTable y las reglas de filtrado definidas en docsDevFilterIpTable y cabhSec2FwLocalFilterIpTable.
- configuredRulesetDocsDevFilterIpTable (4) – Indica que la barrera contra fuegos está utilizando el conjunto de reglas configuradas definidas mediante docsDevFilterIpTable. Si el objeto MIB cabhSec2FwPolicySelection se fija como configuredRulesetDocsDevFilterIpTable (4), la barrera contra fuegos realiza el filtrado teniendo en cuenta el conjunto de reglas configuradas de docsDevFilterIpTable.
- configuredRulesetCabhSec2FwLocalFilterIpTable (5) – Indica que la barrera contra fuegos está utilizando el conjunto de reglas configuradas definidas por la cabhSec2FwLocalFilterIpTable. Si el objeto MIB cabhSec2FwPolicySelection se fija como configuredRulesetDocsDevFilterIpTable (5), la barrera contra fuegos realiza el filtrado teniendo en cuenta el conjunto de reglas configuradas de cabhSec2FwLocalFilterIpTable.
- factoryDefaultAndConfiguredRulesetDocsDevFilterIpTable (6) – Indica que la barrera contra fuegos está utilizando el conjunto de reglas de fábrica por defecto y el conjunto de reglas configuradas definidas mediante DocsDevFilterIpTable. Si el objeto MIB cabhSec2FwPolicySelection se fija como factoryDefaultAndConfiguredRulesetDocsDevFilterIpTable (6) el PS DEBE realizar el filtrado teniendo en cuenta el conjunto de reglas de fábrica por defecto IPCable2Home especificadas en cabhSec2FwFactoryDefaultFilterTable y el conjunto de reglas configuradas de docsDevFilterIpTable.
- factoryDefaultAndConfiguredRulesetCabhSec2FwLocalFilterIpTable (7) – Indica que la barrera contra fuegos está utilizando el conjunto de reglas de fábrica por defecto y el conjunto de reglas configuradas definidas mediante cabhSec2FwLocalFilterIpTable. Si el objeto MIB cabhSec2FwPolicySelection se fija como factoryDefaultAndConfiguredRuleset cabhSec2FwLocalFilterIpTable (7), el PS DEBE realizar el filtrado teniendo en cuenta el conjunto de reglas de fábrica por defecto IPCable2Home especificadas en cabhSec2FwFactoryDefaultFilterTable y el conjunto de reglas configuradas de cabhSec2FwLocalFilterIpTable.

cabhSec2FwEventSetToFactory – Permite al operador de cable borrar todos los eventos que estén actualmente fijados en el cuadro de eventos. El PS DEBE borrar inmediatamente el cabhSec2FwEventControlTable cuando este objeto se ponga a verdadero.

cabhSec2FwEventLastSetToFactory – Este objeto permite saber cuándo fue borrado por última vez el cuadro de eventos.

cabhSec2FwConfiguredRulesetPriority – Define qué regla de filtrado del conjunto de reglas configuradas tiene prioridad cuando existe alguna contradicción entre una regla de filtrado de docsDevFilterIpTable y una regla de filtrado de cabhSec2FwLocalFilterIpTable, tal como indican las opciones siguientes:

- docsDevFilterIpTable (1) – Indica que las reglas de filtrado de docsDevFilterIpTable tienen prioridad sobre cualesquiera filtros contradictorios que puedan existir en cabhSec2FwLocalFilterIpTable.
- cabhSec2FwLocalFilterIpTable (2) – Indica que las reglas de filtrado de cabhSec2FwLocalFilterIpTable tienen prioridad sobre cualesquiera filtros contradictorios que puedan existir en docsDevFilterIpTable.

cabhSec2FwClearLocalRuleset – Permite al operador suprimir las anotaciones de la regla de filtrado de cabhSec2FwLocalFilterIpTable.

11.6.4.9.2 Objetos MIB para eventos de la barrera contra fuegos

Se DEBEN implementar en el PS los siguientes objetos de eventos de barrera contra fuegos, como se define en la MIB de seguridad y se incluyen en el cabhSec2FwEventControlTable:

cabhSec2FwEventType – Atribuye el tipo de evento que se debe buscar en el cuadro. En 11.6.4.7.1 se definen los tipos de eventos.

cabhSec2FwEventEnable – Activa o desactiva el conteo y registro de los eventos de barrera contra fuegos según su tipo, como se indica en cabhSec2FwEventType. Los requisitos de registro se definen en la cláusula sobre datos de registro (véase 11.6.4.7.2). Este objeto equivale a un simple interruptor "activar/desactivar". Si cambia el valor habilitar, el PS DEBE enviar inmediatamente el evento adecuado (8001010x). Si se habilita este valor, la barrera contra fuegos DEBE registrar los eventos en el cabhSec2FwLog. La barrera contra fuegos NO DEBE contar, enviar eventos o recolectar datos de registro relativos a ataques cuando esté inhabilitado este objeto. Valor por defecto = false.

cabhSec2FwEventThreshold – Número de ataques que se han de contar antes de enviar el evento adecuado, según el tipo, tal como se indica en cabhSec2FwEventType. Si el valor se pone a cero, la barrera contra fuegos NO DEBE contar, enviar eventos, o recolectar datos de registro para este tipo. Valor por defecto = 0.

cabhSec2FwEventInterval – Indica el intervalo de tiempo en horas disponible para contar y registrar tipos de eventos en una barrera contra fuegos, tal como lo indica cabhSec2FwEventType. Este intervalo tiene valor en tanto que no se alcance el objeto cabhSec2FwEventThreshold. Si el objeto MIB cabhSec2FwEventInterval vale cero, no hay intervalo atribuido y el PS NO DEBE contar, enviar o registrar eventos. Valor por defecto = 0.

cabhSec2FwEventCount – Indica el valor actual del conteo de ataques, hasta el valor cabhSec2FwEventThreshold, según el tipo, como se indica en cabhSec2FwEventType. La barrera contra fuegos DEBE iniciar el conteo de ataques desde cero cada vez que se habilite el objeto MIB cabhSec2FwEventEnable, se haya superado el cabhSec2FwEventInterval o el valor de cabhSec2FwEventCount sea igual al de cabhSec2FwEventThreshold. Cuando la cantidad de ataques contabilizada en cabhSec2FwEventCount sea igual al umbral fijado en cabhSec2FwEventThreshold, antes del final del intervalo definido por el objeto cabhSec2FwEventInterval, el PS DEBE enviar inmediatamente el evento adecuado (8001020x). Valor por defecto = 0.

cabhSec2FwEventLogReset – Cuando se pone a verdadero ("true"), se borra el cuadro de registro del tipo de evento especificado. La lectura de este objeto siempre produce un resultado falso ("false"). Valor por defecto = false.

cabhSec2FwEventLogLastReset – Indica cuándo fue la última vez que se borró el registro.

11.6.4.9.3 Objetos MIB del conjunto de reglas configuradas de la política de la barrera contra fuegos

Los objetos MIB de política de barrera contra fuegos proporcionan al operador de cable una forma de configurar las reglas que ha de utilizar la barrera contra fuegos para filtrar el tráfico. El operador puede crear cualquier conjunto de reglas configurado que se necesite para filtrar el tráfico que pasa a través de la barrera en el PS. Los objetos MIB de reglas configuradas de política de filtrado de barrera contra fuegos se basan en el conjunto mínimo de requisitos de filtrado. La capacidad de filtrado de la barrera contra fuegos es similar a los filtros que se definen en objetos MIB CM de la industria del cable, especificados en [RFC 2669]. Siendo así, en IPCable2Home utiliza algunos de los objetos de filtrado que ya han sido definidos en dicha referencia y añade algunos objetos MIB particulares de la barrera contra fuegos, a la MIB de seguridad.

En [RFC 2669] se presenta el cuadro docsDevFilterIpTable donde figuran las propiedades básicas de filtrado. Este cuadro incluye una secuencia, docsDevFilterIpEntry, de objetos MIB. Cada fila describe reglas asociadas con direcciones IP que se comparan con los paquetes IP que atraviesan la barrera contra fuegos. La plantilla contiene direcciones IP de origen y destino (y sus máscaras asociadas), el protocolo de nivel superior (por ejemplo TCP, UDP), así como las gamas de puertos de destino y origen. cabhSec2FwLocalFilterIpTable es similar a docsDevFilterIpTable y puede utilizarse también para definir propiedades de filtrado. Tanto docsDevFilterIpTable como cabhSec2FwLocalFilterIpTable constituyen el núcleo de la implementación de la política para el conjunto de reglas configuradas. Es en dichas MIB donde se define y construye la política del conjunto de reglas configuradas.

En IPCable2Home se define una extensión docsDevFilterIPTable, la cabhSec2FwFilterScheduleTable, donde figuran atributos de filtro para el instante de arranque, instante de fin y día de la semana a las correspondientes anotaciones en docsDevFilterIPTable. Estos atributos también existen en cabhSec2FwLocalFilterIpTable y permiten que una regla o filtro que se puede activar en función del día de la semana, (lunes, martes, miércoles, jueves, viernes, sábado o domingo), durante un intervalo que va desde el instante de arranque hasta el final. Estos valores de tiempo del filtro pueden utilizarse en aplicaciones de control paterno. Por ejemplo, es posible que un padre de familia solicite que se prohíban las comunicaciones entre la WAN y el computador de un niño de lunes a viernes de 9 pm a 7 am y sábados y domingos de 10 pm a 8 am. El cuadro cabhSec2FwFilterScheduleTable también proporciona un atributo de descripción que puede utilizarse para hacer comentarios/anotaciones que permitan identificar para qué se utiliza la anotación de filtro. Las anotaciones de reglas de filtrado del objeto MIB docsDevFilterIpTable siempre DEBEN aplicarse si sus objetos MIB cabhSec2FwFilterScheduleTable asociados tienen los valores siguientes:

- cabhSec2FwFilterScheduleStartTime = 0;
- cabhSec2FwFilterScheduleEndTime = 2359; y
- cabhSec2FwFilterScheduleDOW = 0xFE.

Las anotaciones de reglas de filtro del objeto MIB cabhSec2FwLocalFilterIpTable siempre DEBEN aplicarse si sus objetos MIB tienen los valores siguientes:

- cabhSec2FwLocalFilterStartTime = 0;
- cabhSec2FwLocalFilterEndTime = 2359; y
- cabhSec2FwLocalFilterDOW = 0xFE.

La combinación de los filtros que se define en [RFC 2669] y en la MIB de seguridad hace posible que se cree cualquier tipo de reglas basándose en cualquier combinación de dirección IP de origen, dirección IP de destino, puerto de origen, puerto de destino, hora del día, y día de la semana.

Cuando el PS no encuentre ninguna correspondencia al comparar cada paquete entrante o saliente con las reglas en el docsDevFilterIpTable, cabhSec2FwLocalFilterIpTable, o cabhSec2FwFactoryDefaultFilterTable, DEBE aplicar las reglas generales de comportamiento y el conjunto mínimo de capacidades y arquitectura de la barrera contra fuegos, tal como se define en 11.6.4.3.1 y 11.6.4.3.3. Se DEBE ignorar la bandera docsDevFilterIpDefault que se define en [RFC 2669].

Se DEBEN implementar los siguientes objetos MIB de [RFC 2669], con el fin de crear la versión IPCable2Home de la docsDevFilterIpTable. A menos que se especifique lo contrario en esta cláusula, la funcionalidad es la que se define en [RFC 2669]:

- docsDevFilterIpTable >>DocsDevFilterIpEntry
  - **docsDevFilterIpIndex**
    - Coherente con [RFC 2669], se aplica siempre el filtro que tenga el índice inferior, es decir que se verifica el filtro y luego el PS DEBE continuar verificando filtros y aplicará el que tenga el índice mayor en caso de conflicto.
  - **docsDevFilterIpStatus**
  - **docsDevFilterIpControl**
    - El PS DEBE ignorar la configuración (3) para política; IPCable2Home no utiliza el cuadro de política.
  - **docsDevFilterIpIfIndex**
    - Este objecto DEBE utilizar un valor por defecto de 255 (interfaces LAN agregadas)
    - El PS DEBE soportar los valores 1 (uno), para filtros en el lado WAN del PS, y 255 (la interfaz de 'interfaces LAN agregadas') para filtros en el lado LAN del PS.
  - **docsDevFilterIpDirection**
    - Para IPCable2Home, este valor representa el sentido en relación con el docsDevFilterIpIfIndex asignado a esta regla en particular, es decir, el PS DEBE representar el sentido del tráfico (entrante, saliente o ambos), en relación con el ifIndex indicado. Los valores de ifIndex asignados por el fabricante DEBEN seguir la misma regla para la aplicación del sentido. Por ejemplo, IPCable2Home asigna el número 255 a la interfaz LAN agregada. En ese caso, el PS verá como tráfico entrante de ifIndex 255 a todo el tráfico procedente de la LAN y que se dirija al PS o lo atraviese, y como tráfico saliente de ifIndex 255 a todo el tráfico dirigido a la LAN procedente del PS o que lo atraviese.
  - **docsDevFilterIpBroadcast**
    - Se prevé que su valor por defecto sea siempre falso. Por consiguiente, la regla se aplicará a todo el tráfico.
  - **docsDevFilterIpSaddr**
  - **docsDevFilterIpSmask**
  - **docsDevFilterIpDaddr**
  - **docsDevFilterIpDmask**
  - **docsDevFilterIpProtocol**
  - **docsDevFilterIpSourcePortLow**
  - **docsDevFilterIpSourcePortHigh**

- **docsDevFilterIpDestPortLow**
- **docsDevFilterIpDestPortHigh**
- **docsDevFilterIpMatches**
  - Puesto que las reglas de filtrado se aplican al tráfico de inicio de sesión, este objeto DEBE, como mínimo, contar el número de veces que existe concordancia con el filtro cuando se intenta el inicio de una sesión.
- **docsDevFilterIpTos**
  - Se puede ignorar este objeto, su función no es necesaria.
- **docsDevFilterIpTosMask**
  - Se puede ignorar este objeto, su función no es necesaria.
- **docsDevFilterIpContinue**
  - Se DEBE poner siempre este objeto a verdadero, de tal forma que el PS continúe hasta haber verificado todos los filtros. A diferencia del RFC 2669, este objeto NO DEBE activar un descarte hasta en tanto no se hayan verificado todos los filtros y no haya filtros posteriores que soliciten que se acepte el paquete.
- **docsDevFilterIpPolicyId**
  - Se puede ignorar este objeto, su función no es necesaria.

Además, la barrera contra fuegos DEBE soportar los siguientes objetos MIB, como se especifica en el documento MIB sobre seguridad:

- **cabhSec2FwFilterScheduleStartTime**
- **cabhSec2FwFilterScheduleEndTime**
- **cabhSec2FwFilterScheduleDOW**
- **cabhSec2FwFilterScheduleDescr**
- **cabhSec2FwLocalFilterIpTable**

11.6.4.9.4 Objetos MIB del conjunto de reglas de fábrica por defecto de la barrera contra fuegos

Los objetos MIB del conjunto de reglas de fábrica por defecto de la barrera contra fuegos IPCable2Home permiten al operador de cable visualizar las reglas de fábrica por defecto IPCable2Home, que constituyen excepciones a las reglas generales, o comportamiento general de la barrera contra fuegos definido en los cuadros 11-18 y 11-19. Para obtener más información sobre los objetos MIB del conjunto de reglas por defecto utilizados para el filtrado, véase la MIB de seguridad (Security) donde figura una descripción de cabhSec2FwFactoryDefaultFilterTable y sus anotaciones.

11.7 Objetos MIB de seguridad adicionales en el PS

En la cláusula relativa a la barrera contra fuegos (véase 11.6) se describen los objetos MIB de dicha barrera contra fuegos, y en esta cláusula se describen los otros objetos MIB de seguridad requeridos. Estos últimos se definen con más detalle en el anexo A y se los DEBE soportar como corresponda.

11.7.1 Objetos MIB de descarga segura de software

La descarga segura de software se efectúa conforme al diseño presentado en el anexo B/J.112 y, por tanto, es posible reutilizar los objetos MIB en el PS tal como lo hace un CM. Se define independientemente la estructura de la PKI para IPCable2Home y, por ende, se DEBEN utilizar algunas de las MIB de los certificados definidos por IPCable2Home, en lugar de las MIB J.112, en su versión actual [draft-ietf-ipcdn-bpiplus-mib-05].

El PS autónomo DEBE soportar los siguientes objetos MIB, como se define en CL-SP-MIB-CLABDEF-I03-030411 [véase E.6]:

- **clabCVCRootCACert** – CA raíz de verificación de código para validación de CVC.
- **clabCVCCACert** – CA de verificación de código para validación de CVC.
- **clabMfgCACert** – Certificado de CA de fabricante utilizado para almacenar el Cert CA Mfg.

El PS autónomo DEBE soportar los siguientes objetos MIB de descarga de software definidos en [draft-ietf-ipcdn-bpiplus-mib-05]:

- **docsBpi2CodeDownloadGroup** – Conjunto de objetos que proporcionan el soporte de descarga de software autenticado. El docsBpi2CodeDownloadGroup incluye:
  - **docsBpi2CodeDownloadStatusCode** – Resultado de la última verificación de CVC de fichero de configuración, verificación de CVC de SNMP o verificación de fichero de código.
  - **docsBpi2CodeDownloadStatusString** – Información adicional al código de estado.
  - **docsBpi2CodeMfgOrgName** – OrganizationName del fabricante del dispositivo.
  - **docsBpi2CodeMfgCodeAccessStart** – El valor actual del codeAccessStart del fabricante del dispositivo referenciado al tiempo medio de Greenwich (GMT, greenwich mean time).
  - **docsBpi2CodeMfgCvcAccessStart** – El valor actual del cvcAccessStart del fabricante de dispositivo referenciado al GMT.
  - **docsBpi2CodeCoSignerOrgName** – El organizationName del cofirmante.
  - **docsBpi2CodeCoSignerCodeAccessStart** – El valor actual del codeAccessStart del cofirmante referenciado al GMT.
  - **docsBpi2CodeCoSignerCvcAccessStart** – El valor actual del cvcAccessStart del cofirmante respecto al GMT.
  - **docsBpi2CodeCvcUpdate** – Activa el dispositivo para que verifique el CVC y actualice el valor cvcAccessStart.

11.7.2 Objetos MIB del fichero de configuración de seguridad

El PS DEBE soportar el siguiente objeto MIB de descarga de fichero de configuración, como se define en el MIB de seguridad:

cabhPsDevProvConfigHash – Función de troceo SHA-1 [FIPS 186] de todo el contenido del fichero de configuración, considerado como una cadena de bytes.

11.7.3 Objetos MIB del proveedor de servicio de seguridad

El PS DEBE soportar el siguiente objeto MIB de autenticación de proveedor de servicio, como se define en la MIB de seguridad:

clabSrvcPrvdrRootCACert – La CA raíz de proveedor de servicio utilizada para validar certificados de dispositivos en la red de dicho proveedor.

11.7.4 Objetos MIB del certificado de PS

El PS DEBE soportar el siguiente objeto MIB del certificado de PS, como se define en la MIB de seguridad:

cabhSecCertPsCert – El certificado de PS codificado en DER X.509, que se utiliza para proporcionar identidad segura al PS.

11.7.5 Objetos MIB de Kerberos

Los requisitos de Kerberos en el IPCable2Home constituyen un subconjunto de la funcionalidad necesaria para IPCablecom. Se requieren los siguientes objetos MIB para IPCable2Home y el PS DEBE soportarlos, como se define en la MIB de seguridad:

- **cabhSecKerbPKINITGracePeriod** – Número de minutos antes de que expire el tique actual para que el PS inicie una petición de un nuevo tique ante un KDC.
- **cabhSecKerbTGSGracePeriod** – Número de minutos antes de que expire el tique actual para que el PS inicie una petición de un nuevo tique ante un KDC.
- **cabhSecKerbUnsolicitedKeyMaxTimeout** – Valor máximo del temporizador para el intercambio Req/Rep (petición/respuesta) AP.
- **cabhSecKerbUnsolicitedKeyMaxRetries** – Número máximo de reensayos que se permite al PS para intentar la negociación Req/Rep AP.

11.8 Descarga segura de software para el PS

11.8.1 Objetivos de la descarga segura de software

Los objetivos de la descarga segura de software son los siguientes:

- El operador de cable puede cargar con seguridad, de ser necesario código en el PS.
- El operador de cable puede gestionar las descargas seguras utilizando distintas políticas de configuración.
- Gracias a la seguridad de la descarga se contará con la integridad, la autenticación y, de ser posible, la criptación.
- El PS descargará solamente las imágenes que son adecuadas para el dispositivo.

11.8.2 Directrices de diseño de descarga segura de software

Véase el cuadro 11-22.

Cuadro 11-22/J.192 – Directrices de diseño del sistema de seguridad IPCable2Home

Referencia	Directrices
SEC13	El operador de cable podrá descargar con seguridad imágenes de software hacia el elemento PS.

11.8.3 Descripción del sistema de descarga segura de software

La descarga segura de software consiste en garantizar que sólo se podrá descargar una copia imagen de software al PS si dicha imagen ha sido creada por el mismo fabricante. De igual manera, se garantiza que la imagen no haya sido modificada desde que el fabricante firmó la imagen de código. Puede ocurrir también que la imagen vaya firmada por el laboratorio de pruebas de certificación, como cofirmante, para garantizar así que ha sido certificada. A fin de tener una seguridad adicional en el proceso de descarga, el operador puede facultativamente cofirmar cualquier imagen para garantizar que sólo se carguen en el PS las imágenes que él ha aprobado. El mecanismo de control que permite asegurar la descarga del software consiste en insertar los certificados de verificación de código (CVC) en el fichero de configuración y que corresponden con los CVC de la imagen de código que se ha de descargar. Tras recibir uno o varios CVC en el fichero de configuración, se habilita al PS para descargar la nueva imagen de código cuando ésta se activa a través del fichero de configuración o de SNMP SET.

11.8.4 Requisitos para la descarga segura de software

Un elemento de PS autónomo DEBE poder descargar a distancia imágenes por software en la red. Como se describe en 6.3.3.2.4.9, la descarga segura de software hacia un PS integrado viene controlada por el módem de cable. La nueva imagen por software permite al operador de cable mejorar su funcionamiento, incluir nuevas funciones y características, corregir deficiencias de diseño y ofrecer un trayecto de migración para los dispositivos IPCable2Home a medida que esta norma evolucione. La capacidad de descarga de software DEBE permitir que se cambie la funcionalidad del elemento PS sin que sea necesario que el personal del operador de cable reconfigure visite cada instalación a y reconfigure cada unidad en el sitio de instalación. En el proceso de descarga segura de software a un PS autónomo hay que tener en cuenta los siguientes requisitos primarios del sistema:

- El mecanismo que se utiliza para la descarga de software DEBE ser la transferencia de archivos TFTP.
- Se DEBE iniciar la descarga de software de una de las dos formas siguientes:
  1) a través de una petición de establecimiento SNMP (SNMP SET) del NMS al docsDevSwAdminStatus; o bien
  2) a través del fichero de configuración del elemento PS.

  Si el nombre de fichero de actualización de software que aparece en el fichero de configuración no corresponde con la copia imagen de software actual del dispositivo, el elemento PS DEBE solicitar el fichero especificado al servidor de software a través de TFTP.
- El elemento PS DEBE verificar que la copia imagen de software descargada sea adecuada. De serlo, DEBE copiarla en una memoria permanente. Tras haber completado con éxito la transferencia de fichero, el dispositivo DEBE autoreiniciarse con la nueva imagen de código.
- Cuando, por cualquier razón, el elemento PS no pueda completar la transferencia del fichero, DEBE seguir aceptando nuevas descargas de software (sin la interacción de operador o usuario), aún si se interrumpen la energía eléctrica o la conexión entre un intento y otro.
- El elemento PS DEBE registrar los fallos de descarga de software e informarlos de forma asíncrona al gestor de red.
- Siempre que se actualice el software, a efectos de conformidad con una nueva versión de esta Recomendación, es crucial que éste DEBA funcionar con la versión anterior a fin de permitir una transición gradual de las unidades en la red.
- El elemento PS DEBE autenticar la copia imagen de software descargada.
- El elemento PS DEBE verificar que el código descargado no haya sido alterado si se le compara con el formato original suministrado por una fuente de confianza.
- El proceso de descarga de software DEBE suministrar al operador de cable un mecanismo para mejorar o reducir la versión de código de los elementos IPCable2Home.
- El proceso de descarga de software DEBE proporcionar opciones al operador de cable para que establezca sus propias políticas de descarga.
- El fabricante de fichero de código DEBE aplicar una firma de verificación de código (CVS) a la imagen de código y cualesquiera otros atributos autenticados, como se define en esta Recomendación para la firma digital con estructura PKCS#7 para el fichero de código; la clave privada que se utilice para aplicar la firma DEBE estar ligada a un certificado de clave pública que la encadene con la raíz CVC. La firma del fabricante autentica la fuente e integridad del fichero código.

- Un cofirmante (operador de cable o CTL) PUEDE cofirmar el fichero de código, además de la firma del fabricante.
- El elemento PS DEBE poder procesar una firma digital PKCS#7 y un certificado X.509, como se define en 11.8.4.1.1 y 11.3.4.1.1, respectivamente.
- El elemento PS DEBE poder actualizar el certificado CA raíz de CVC almacenado en el dispositivo una vez que el certificado ha sido validado en caso de estar contenido en un fichero de código como un TLV.
- El elemento PS DEBE poder reemplazar el o los certificados CA de fabricante almacenados en el dispositivo una vez que el certificado ha sido validado en caso de estar contenido en un fichero de código como un TLV.
- El elemento PS DEBE poder actualizar el certificado de CA de CVC almacenado en el dispositivo una vez que el certificado ha sido validado en caso de estar contenido en un fichero de código como un TLV.
- El elemento PS DEBE poder actualizar el certificado de CA raíz de proveedor de servicio almacenado en el dispositivo una vez que el certificado ha sido validado en caso de estar contenido en un fichero de código como un TLV.

La descarga facultativa del certificado de CA raíz de proveedor de servicio, del certificado de CA raíz de CVC, del certificado CA CVC, y/o del certificado CA de fabricante, como parte del fichero de código, es claramente independiente de la imagen del código y de los otros parámetros presentes en el fichero de descarga de código. Se puede cambiar el certificado de CA raíz de proveedor de servicio, el certificado de CA raíz de CVC, el certificado de CA de CVC, y/o el certificado de CA de fabricante, conocidos por el elemento PS, incluyendo los nuevos certificados en la imagen de código. La inclusión del certificado de CVC de fabricante y/o un CVC de cofirmante y el correspondiente CVS, permite al elemento PS verificar que la imagen de código no haya sido alterada desde que se añadieron a dicha imagen el certificado CA raíz de proveedor de servicio, el certificado de CA raíz de CVC, el certificado de CA de CVC, y/o el certificado de CA de fabricante, o los parámetros SignedData.

Un dispositivo de pasarela doméstica que sea conforme a IPCable2Home PUEDE incluir un módem de cable y un elemento PS, que pueden ser entidades independientes o estar incorporadas, como se define en la cláusula relativa a la arquitectura ((véase la cláusula 5).

- Si el elemento PS está integrado en un módem de cable, la imagen de PS/CM DEBE ser única, y sólo el módem de cable debe descargar el software.
- Si el elemento PS se compone de entidades autónomas autónomas, DEBE ser el elemento PS el que efectúe la descarga de software para los elementos IPCable2Home, como se describe más adelante en esta especificación.

11.8.4.1 Estructura del fichero de descarga de código para la descarga segura de software

A efectos de la descarga segura de software, se construye el fichero de descarga de código utilizando una estructura conforme a [RFC 2315] que haya sido definida en un formato específico para utilizarse con elementos PS. El fichero de código DEBE cumplir con [RFC 2315] y DEBE estar codificado en DER. Asimismo, DEBE corresponder a la estructura indicada en el cuadro 11-23.

Siempre que se descarguen certificados como parte del fichero de código, éstos PUEDEN incluirse en los campos que se especifican en el cuadro 11-23, y separados de la imagen de código real contenida en el campo CodeImage.

Cuadro 11-23/J.192 – Estructura de fichero de código

Fichero de código	Descripción
PKCS #7 Digital Signature {	
ContentInfo	
ContentType	SignedData
SignedData ()	Valor de contenido EXPLÍCITO de datos firmados: incluye CVS y CVS X.509
} end [RFC 2315] Digital Signature	
SignedContent {	
Download Parameters {	Formato de TLV obligatorio (tipo 28). (De no haber subTLV, la longitud es cero).
MfgCACerts ()	TLV facultativo para uno o varios certificados codificados en DER, cuyos formatos sean conformes al formato TLV de certificado de CA de fabricante (tipo 17)
clabServProvRootCACert ()	TLV facultativo para uno o varios certificados codificados DER, cuyos formatos sean conformes al formato TLV de certificado CA raíz de proveedor de servicio (tipo 50)
clabCVCRootCACert ()	TLV facultativo para un certificado codificado en DER, cuyo formato sea conforme al formato del TLV de certificado de CA raíz CVC (tipo 51)
clabCVCCACertificate ()	TLV facultativo para un certificado codificado en DER, cuyo formato sea conforme al formato del TLV de certificado de CA de CVC (tipo 52)
}	
CodeImage ()	Imagen de código actualizada
} end SignedContent	

11.8.4.1.1 Datos firmados

El fichero de descarga de código tendrá la información en un tipo de contenido de datos firmados [RFC 2315], como se muestra en el cuadro 11-24. Si bien se guarda la conformidad con [RFC 2315], la estructura del formato que se utiliza ha sido restringida a fin de facilitar el procesamiento efectuado por el PS para validad la firma. Los datos firmados [RFC 2315] DEBEN estar codificados en DER y corresponder exactamente con la estructura presentada más adelante, salvo por los cambios de orden necesarios para codificar en DER (por ejemplo, el orden de los atributos SET OF). El elemento PS DEBERÍA rechazar la firma [RFC 2315] siempre que los datos firmados [RFC 2315] no correspondan con la estructura codificada en DER.

Cuadro 11-24/J.192 – Datos firmados PKCS#7

Campo PKCS #7	Descripción
Signed Data {	
version	1
digestAlgorithms	SHA-1
contentInfo	
contentType	datos (SignedContent concatenado al final de la estructura PKCS#7)
certificates {	
mfgCVC	(REQUERIDO para todos los ficheros de código) (nota 1)
co-signerCVC	(FACULTATIVO; requerido para las cofirmas) (nota 2)
} *end certificates*	
signerInfos{	
MfgSignerInfo {	(REQUERIDO para todos los ficheros de código)
version	1
issuerAndSerialNumber	
issuer	
countryName	US
organizationName	CableLabs
commonName	CA raíz de CVC de CableLabs
serialNumber	<número de serie de CVC de Mfg>
digestAlgorithm	SHA-1
authenticatedAttributes	
contentType	datos (contentType de signedContent)
signingTime	UTCTime (GMT), YYMMDDhhmmssZ
messageDigest	(resumen del contenido junto con los atributos autenticados del firmante, como se define en [PKCS#7])
digestEncryptionAlgorithm	rsaEncryption
encryptedDigest	
} *end mfg signer info*	
CoSignerInfo {	(FACULTATIVO; requerido para las cofirmas)
version	1
issuerAndSerialNumber	
issuer	
countryName	US
organizationName	CableLabs
commonName	CableLabs CVC Root CA
serialNumber	<número de serie de CVC de cofirmante>
digestAlgorithm	SHA-1
authenticatedAttributes	
contentType	datos (contentType de signedContent)

Cuadro 11-24/J.192 – Datos firmados PKCS#7

Campo PKCS #7	Descripción
signingTime	UTCTime (GMT), YYMMDDhhmmssZ
messageDigest	(resumen del contenido junto con los atributos autenticados del firmante, como se define en [PKCS#7])
digestEncryptionAlgorithm	rsaEncryption
encryptedDigest	
} *end co-signer info*	
} *end signer infos*	
} *end signed data*	
NOTA 1 – El CVC del fabricante DEBE tener el formato especificado en el cuadro 11-9. NOTA 2 – El CVC del cofirmante DEBE tener el formato especificado en el cuadro 11-10 o cuadro 11-11 en función del tipo de cofirmante, que puede ser CTL o proveedor de servicio.	

11.8.4.1.2 Contenido firmado

El campo contenido firmado del fichero de código incluye la imagen de código y el campo de parámetros de descarga, que tal vez contenga a su vez los siguientes ítems facultativos:

- certificado de CA raíz de proveedor de servicio;
- certificado de CA raíz de CVC de laboratorio de prueba de certificación (CTL, *certification testing laboratory*);
- certificado de CA de CVC de CTL;
- certificado de CA de fabricante.

El formato de la imagen de código final es compatible con el elemento PS de destino. Para soportar los requisitos de firma [RFC 2315], se pone el contenido de código como tipo datos; es decir, una simple cadena de octetos. No se especifica aquí el formato de la imagen de código final que ha de ser definida por cada fabricante conforme a sus propios requisitos.

Cada fabricante DEBERÍA producir su código con mecanismos adicionales que permitan verificar si una imagen de código actualizada es compatible con el elemento PS de destino.

De haber un certificado en el campo contenido firmado, se prevé que éste reemplazará al certificado almacenado en el elemento PS. De poderse descargar e instalar el código con éxito, el elemento PS DEBE reemplazar su certificado almacenado con el nuevo que ha recibido en el campo contenido firmado después de que el certificado ha sido validado. Este nuevo certificado se utilizará en toda verificación subsiguiente.

11.8.4.1.3 Claves de firmado de código

La firma digital [RFC 2315] utiliza el algoritmo de criptación RSA [PKCS #1] con SHA-1 [FIPS 186]. El elemento PS DEBE poder verificar las firmas de fichero de código. El exponente público es F_4 (65537 decimal).

11.8.4.1.4 Certificado de CA de fabricante

Este atributo es un atributo de cadena que incluye un certificado de CA tipo X.509, como se define en [Rec. UIT-T X.509].

Tipo	Longitud	Valor
17	Variable	Certificado de CA tipo X.509 (ASN.1 codificado en DER)

11.8.4.1.5 Certificado de CA raíz de proveedor de servicio

Este atributo es una cadena que contiene un certificado de CA raíz de proveedor de servicio fijo X.509, como se define en [Rec. UIT-T X.509]. El elemento PS debe utilizar ese certificado en el modo de configuración SNMP a efectos de autenticación mutua.

Tipo	Longitud	Valor
50	Variable	Certificado de CA tipo X.509 (ASN.1 codificado en DER)

11.8.4.1.6 Certificado de CA raíz de CVC

Este atributo es una cadena que contiene un certificado de CA raíz CVC tipo X.509, como se define en [Rec. UIT-T X.509]. El elemento PS autónomo debe utilizar ese certificado durante el proceso de descarga segura de software.

Tipo	Longitud	Valor
51	Variable	Certificado de CA tipo X.509 (ASN.1 codificado en DER)

11.8.4.1.7 Certificado de CA de CVC

Este atributo es una cadena que contiene un certificado de CA de CVC tipo X.509, como se define en [Rec. UIT-T X.509]. El elemento PS autónomo debe utilizar ese certificado durante el proceso de descarga segura de software.

Tipo	Longitud	Valor
52	Variable	Certificado de CA tipo X.509 (ASN.1 codificado en DER)

11.8.4.2 Formato de CVC para descarga segura de software

El formato que se utiliza para el CVC para la descarga segura de software, es conforme a [Rec. UIT-T X.509]. No obstante, la estructura X.509 ha sido restringida en este caso a fin de facilitar el procesamiento que el elemento PS efectúa para validar el certificado y extraer la clave pública utilizada a fin de verificar el CVS. El CVC DEBE estar codificado en DER y ser conforme con los cuadros 11-9, 11-10 y 11-11 en función del tipo de CVC. El elemento PS DEBERÍA rechazar el CVC si no concuerda con el correspondiente cuadro.

11.8.4.2.1 Revocación de certificado

En esta Recomendación no se exige ni se define la utilización de listas de revocación de certificados (CRL, *certificate revocation lists*). No es necesario que el elemento PS soporte las CRL. Es facultad de los operadores definir y utilizar las CRL para contribuir a la gestión de los ficheros de código que reciben de los fabricantes. No obstante, existe un método para revocar certificados que se basa en la fecha de inicio de validez de éstos, y en el que se requiere que se entregue al elemento PS un CVC actualizado con una hora de inicio de validez actualizada. Una vez que el CVC se haya validado con éxito, la hora de inicio de validez X.509 actualizará el valor actual del cvcAccessStart del elemento PS.

11.8.4.3 Controles de acceso al fichero de código

A efectos de una descarga segura de software se incluyen en el fichero de código valores especiales de control para que el elemento PS los verifique antes de validar una imagen de código. Se DEBEN satisfacer las condiciones que se hayan asignado a estos valores de los parámetros de control antes de que el elemento PS valide el CVC o el CVS, y acepte la imagen de código.

11.8.4.3.1 Nombres de las organizaciones sujeto

El elemento PS podrá reconocer en cualquier momento hasta dos nombres a la vez, que considere agentes de confianza que firman código en el campo sujeto de un CVC de fichero de código, a saber:

- Fabricante de dispositivo: El nombre de fabricante en el campo de sujeto CVC del fabricante DEBE corresponder exactamente con el nombre de fabricante almacenado en la memoria permanente del elemento PS por el propio fabricante. El CVC de fabricante DEBE incluirse siempre en el fichero de código.
- Agente cofirmante: Se permite que otra organización de confianza cofirme ficheros de códigos destinados al dispositivo. En la mayoría de los casos se trata del operador de cable que controla el dominio de funcionamiento del dispositivo. El nombre de organización del cofirmante se comunica al elemento PS a través de un CVC de cofirmante en el fichero de configuración, cuando se inicializa el proceso de verificación de código de este elemento. El nombre de organización del cofirmante que aparece en el campo sujeto de CVC del cofirmante DEBE corresponder exactamente con el nombre de organización de cofirmante recibido previamente en el CVC de inicialización de cofirmante y almacenado por el elemento PS.

El elemento PS PUEDE efectuar una comparación binaria de los nombres de organización.

11.8.4.3.2 Controles dependientes del tiempo

Para disminuir la posibilidad de que un elemento PS reciba un fichero de código anterior por medio de un ataque de reproducción, los ficheros de código incluyen un valor de hora de firma en la estructura PKCS #7 que se puede utilizar para determinar el instante en que se firmó el código. El elemento PS DEBE mantener dos valores de tiempo UTC asociados con cada agente que firma código. Se DEBE almacenar y mantener un conjunto para el fabricante del dispositivo. De igual manera, cuando el fichero de código haya sido cofirmado, el elemento PS DEBE almacenar y mantener también un conjunto separado de valores temporales para el cofirmante.

Estos valores se utilizan para controlar el acceso del fichero de código al elemento PS, controlando caso por caso la validez del CVS y el CVC, a saber:

- codeAccessStart: valor de tiempo UTC de 12 bytes referido al tiempo medio de Greenwich (GMT).
- cvcAccessStart: valor de tiempo UTC de 12 bytes referido al GMT.

Los valores UTCTime en el CVC se DEBEN expresar como GMT y DEBEN incluir los segundos. Esto es, DEBEN expresarse de la siguiente manera: YYMMDDhhmmssZ. El campo del año (YY) DEBE interpretarse así:

- Siempre que YY sea mayor o igual a 50, el año se interpretará como 19YY.
- Cuando sea menor que 50 se lo hará como 20YY.

Se hará referencia siempre a estos valores con respecto al tiempo medio de Greenwich, de tal modo que el carácter (Z) de ASCII se pueda suprimir cuando el elemento PS lo almacene como codeAccessStart y cvcAccessStart.

El elemento PS DEBE mantener cada uno de estos valores de tiempo en un formato que contenga información de tiempo equivalente y precisión de hasta el formato UTC de 12 caracteres (es decir, YYMMDDhhmmss). El elemento PS DEBE comparar con precisión sus valores almacenados con los valores de tiempo UTC que recibe en un CVC. En esta Recomendación se discuten estos requisitos.

Los valores de codeAccessStart y cvcAccessStart correspondientes al fabricante del elemento PS NO DEBEN disminuir. Los mismos valores, en el caso del cofirmante, NO DEBEN disminuir en tanto que éste no cambie y el elemento PS mantenga los valores de control dependientes del tiempo del cofirmante.

11.8.4.4 Inicialización de la actualización de código

11.8.4.4.1 Inicialización de fabricante

Corresponde al fabricante instalar correctamente la versión de código inicial en el elemento PS.

Como soporte a la descarga segura de software, los valores de los controles dependientes del tiempo del fabricante se DEBEN cargar en la memoria permanente del elemento PS:

- organizationName del fabricante del elemento PS.
- Valores de control dependientes del tiempo del fabricante:
  - valor de inicialización codeAccessStart;
  - valor de inicialización cvcAccessStart.

El nombre de organización del fabricante del elemento PS DEBE estar siempre en el dispositivo. Se PUEDE almacenar el organizationName del fabricante del elemento PS en la imagen de código del dispositivo. El nombre de fabricante utilizado para la actualización del código no necesariamente coincide con el que se usa en el certificado de CA de fabricante.

Los valores de control dependientes del tiempo, codeAccessStart y cvcAccessStart, DEBEN inicializarse a un UTCTime compatible con la hora de inicio de validez del último CVC del fabricante. Durante el funcionamiento normal, se deben actualizar periódicamente estos valores a través de los CVC de fabricante que hayan sido recibidos y verificados por el elemento PS.

El fabricante DEBE inicializar los siguientes certificados en la memoria permanente del elemento PS autónomo:

- certificado de CA raíz de proveedor de servicio;
- certificado de CA raíz CVC;
- certificado de CA de CVC;
- certificado de CA de fabricante;
- certificado de elemento PS.

El fabricante DEBE inicializar los siguientes certificados en la memoria permanente del elemento del PS integrado:

- certificado de CA raíz de proveedor de servicio;
- certificado de CA de fabricante;
- certificado de elemento PS.

11.8.4.4.2 Inicialización de red

A fin de poder verificar el código, se utiliza el fichero de configuración del PS como medio autenticado en el que se puede iniciar el proceso de verificación de código. En dicho fichero, el elemento PS recibe los valores de configuración pertinentes a la verificación de actualización de código.

El fichero de configuración DEBERÍA incluir siempre el CVC más actualizado que se pueda aplicar al elemento PS de destino. Cuando se utilice el fichero de configuración para iniciar una actualización de código, éste DEBE contener un certificado de verificación de código (CVC) para inicializar el elemento PS, que podrá entonces aceptar ficheros de código conformes con esta Recomendación. Sin importar si se requiere o no una actualización de código, el elemento PS DEBE procesar un CVC en el fichero de configuración y puede incluir:

- Ningún CVC – El elemento PS NO DEBE aceptar un fichero de código.
- Sólo el CVC de fabricante – El elemento PS DEBE verificar que el CVC de fabricante se vincule a una raíz de CVC antes de aceptar el fichero de código. Cuando el fichero de configuración del elemento PS contenga solamente un CVC válido de fabricante, el dispositivo requerirá únicamente una firma de fabricante en los ficheros de código. En este caso, el elemento PS NO DEBE aceptar ficheros de código cofirmados.
- Sólo un CVC de cofirmante (operador de cable o CTL) – El elemento PS DEBE verificar que el CV de cofirmante se vincule a una raíz de CV antes de aceptar el fichero de código. Cuando el fichero de configuración del elemento PS contenga un CVC válido de cofirmante, lo utiliza para inicializar el dispositivo con un cofirmante. Una vez validado, el nombre del sujeto organizationName del CVC se convertirá en el cofirmante de código atribuido al elemento PS. Para que este elemento pueda aceptar después una imagen de código, el cofirmante y el fabricante del dispositivo DEBERÁN haber firmado el fichero de código.
- Un CVC de fabricante y uno de cofirmante – El elemento PS DEBE verificar que ambos CVC se relacionan con la raíz CVC antes de aceptar un fichero de código.

Como condición previa a que el elemento PS habilite la actualización de ficheros de código en la red, éste DEBE recibir un CVC válido en un fichero de configuración. Además, cuando el fichero de configuración del elemento PS no contenga un CVC válido, lo que significa que su capacidad para actualizar ficheros de código ha sido inhabilitada, el elemento PS DEBE rechazar toda información contenida en un CVC subsiguiente que se reciba a través del objeto MIB SNMP docsBpi2CodeCvcUpdate.

El nombre de organización del fabricante del elemento PS y los valores de control dependientes del tiempo del fabricante DEBEN estar incluidos siempre en el elemento PS. Cuando se inicialice dicho elemento para aceptar código cofirmado por un cofirmante adicional, se DEBEN almacenar y mantener, mientras funcione, el nombre de la organización y sus valores de control dependientes del tiempo correspondientes. Se DEBE atribuir espacio en la memoria del elemento PS para almacenar los siguientes valores de control de cofirmante:

- organizationName de agente cofirmante;
- valores de control dependientes del tiempo de cofirmante:
  - cvcAccessStart;
  - codeAccessStart.

Se DEBE almacenar el conjunto de estos valores de fabricante en la memoria permanente del elemento PS y es necesario que se conserven cuando se suspenda la alimentación de corriente del dispositivo o durante un rearranque.

Si se atribuye un cofirmante al elemento PS, el conjunto de valores CVC de aquél DEBE almacenarse en la memoria de éste. El elemento PS PUEDE mantenerlos en una memoria permanente que no se borre durante la interrupción de alimentación del dispositivo o durante un rearranque. No obstante, al atribuir un cofirmante a un elemento PS el CVC está siempre en el fichero de configuración, por lo que dicho elemento recibirá siempre los valores de control del cofirmante durante la fase de inicialización, sin que sea necesario almacenar los valores de control dependientes del tiempo del cofirmante tras una pérdida de alimentación o durante un proceso de rearranque.

11.8.4.4.3 Procesamiento de CVC

Con el fin de acelerar la entrega de un CVC actualizado sin que se requiera que el PS procese una actualización de código, PUEDE entregarse el CVC en el fichero de configuración o en un mensaje SNMP Set. El formato del CVC será el mismo siempre que esté en un fichero de código, uno de configuración o en un mensaje SNMP.

11.8.4.4.3.1 Procesamiento del CVC del fichero de configuración

Cuando se incluya un CVC en el fichero de configuración, el elemento PS DEBE verificarlo antes de aceptar cualquiera de las configuraciones de actualización de código que éste contenga. Al recibir el CVC en el fichero de configuración, el elemento PS DEBE seguir los siguientes pasos de validación y procedimiento. Cuando falle alguna de las siguientes pruebas de verificación, el elemento PS DEBE interrumpir inmediatamente el proceso de verificación del CVC y registrar el error, cuando corresponda. Si el fichero de configuración del PS no contiene un CVC que se pueda convalidar adecuadamente, el elemento PS NO DEBE descargar los ficheros de código de actualización sin importar si el proceso ha sido activado por el fichero de configuración de PS o a través del objeto MIB SNMP docsDevSwAdminStatus. Además, si el fichero de configuración del PS no incluye un CVC que se convalide adecuadamente (CVC del fabricante o del cofirmante), el elemento PS no necesita procesar los CVC que se reciban posteriormente, a través de un objeto MIB SNMP docsBpi2CodeCvcUpdate, y NO DEBE aceptar información proveniente de dichos CVC (es decir, el elemento del PS DEBE ignorar cualquier petición SNMP Set realizada al objeto MIB SNMP docsBpi2CodeCvcUpdate).

Al recibir el CVC en un fichero de configuración, el elemento PS DEBE:

1) Verificar que el CVC es conforme con la estructura y valores requeridos según 11.3.4.2.
2) Verificar el nombre de la organización del sujeto del CVC:
   a) Si se trata del CVC de fabricante (tipo 32), en ese caso:
      i) Si el organizationName es idéntico al nombre del fabricante del dispositivo, se trata del CVC del fabricante. En este caso, el elemento PS DEBE verificar que la hora de inicio de validez del CVC de fabricante sea mayor o igual que el valor cvcAccessStart del fabricante que se mantiene actualmente en dicho elemento.
      ii) Si el organizationName es diferente del nombre del fabricante del dispositivo, se DEBE rechazar este CVC y registrar el error.
   b) Si se trata de un CVC de cofirmante (tipo 33), en ese caso:
      i) Si el organizationName es idéntico al actual cofirmante de código del elemento PS, se trata del CVC de cofirmante actual y el elemento PS debe verificar que la hora de inicio de validez sea mayor o igual que el valor cvcAccessStart del cofirmante que mantiene actualmente dicho elemento.
      ii) Si el organizationName es diferente del nombre de cofirmante de código, entonces tras haber validado el CVC (y completado el registro), este sujeto nombre de organización se convertirá en el nuevo cofirmante de código del elemento PS. El elemento PS NO DEBE aceptar un fichero de código a menos que haya sido firmado por el fabricante y cofirmado por este cofirmante de código.
3) Validar la firma de quien emite el CVC utilizando la clave pública de CA de CVC de CTL en poder del elemento PS.
4) Validar la firma de la CA de CVC de CTL utilizando la clave pública de CA raíz de CVC de CTL en poder del elemento PS. A través de la verificación de la firma se autenticará el origen y se validará la confianza en los parámetros CVC.

5) Actualizar el valor actual de cvcAccessStart del elemento PS correspondiente al sujeto organizationName del CVC (es decir, fabricante o cofirmante) con el valor de la hora de inicio de validez del CVC validado. Cuando esta hora sea mayor que el valor actual de codeAccessStart del elemento PS, se actualiza el valor codeAccessStart de dicho elemento con el valor de la hora de inicio de validez. El elemento PS DEBERÍA descartar los restos del CVC de cofirmante.

11.8.4.4.3.2 Procesamiento del CVC recibido mediante SNMP

El elemento PS DEBE procesar los CVC recibidos a través del SNMP, siempre que se haya habilitado para actualizar ficheros de código, de lo contrario se DEBEN rechazar todos estos CVC. Al validar el CVC entregado a través del SNMP, el elemento PS DEBE efectuar los siguientes pasos de procedimiento:

NOTA – Cuando falle cualquiera de las siguientes etapas de verificación, el elemento PS DEBE interrumpir inmediatamente el proceso de verificación de CVC, registrar el error, cuando corresponda, y suprimir todo el resto del proceso de dicho paso.

El elemento PS DEBE:

1) Verificar que el CVC es conforme con la estructura y valores requeridos en 11.3.4.2.2.2.
2) Verificar el sujeto nombre de organización de CVC:
   a) Si el organizationName es idéntico al nombre del fabricante del dispositivo se trata del CVC del participante. En este caso, el elemento PS DEBE comprobar que la hora de inicio de validez de CVC del fabricante sea mayor que el valor de cvcAccessStart de fabricante presente en el elemento PS.
   b) Si el organizationName es idéntico al cofirmante actual de código del elemento PS, se trata entonces de un CVC de cofirmante y la hora de inicio de la validez DEBE ser mayor que el valor de cvcAccessStart de cofirmante presente en el elemento PS.
   c) Si el organizationName es diferente del nombre de fabricante de dispositivo o de cofirmante actual, el elemento PS DEBE rechazar inmediatamente este CVC.
3) Validar la firma de quien emite el CVC utilizando la clave pública de CA de CVC de CTL que tiene el elemento PS.
4) Validar la firma de quien emite el CVC utilizando la clave pública de CA raíz de CVC de CTL que tiene el elemento PS. La verificación de la firma permitirá autenticar el certificado y confirmar la confianza en la hora de inicio de validez del CVC.
5) Actualizar el valor actual de cvcAccessStart del sujeto utilizando el valor de la hora de inicio de validez de CVC validado. Si éste es mayor que el valor actual de codeAccessStart del elemento PS, actualizarlo haciéndolo igual al valor de inicio de validez.

11.8.4.5 Requisitos necesarios para la firma del código

11.8.4.5.1 Requisitos de la autoridad de certificación (CA)

La CA de CVC del laboratorio de prueba de certificación firma y emite los certificados de verificación de código (CVC). El CVC DEBE ser exactamente como se especifica en 11.3.4.2.2.2 en función del tipo de CVC.

En cualquier otro formato, se DEBE mantener toda la información y se DEBE reproducir el formato original; por ejemplo, como un entero de 32 bits diferente de cero, donde un entero cuyo valor sea 0 representa la ausencia de firmante de código.

11.8.4.5.2 Requisitos de CVC de fabricante

Para firmar sus ficheros de código, el fabricante DEBE obtener un CVC válido de la CA de CVC de CTL. Todas las imágenes de código de fabricante que se suministran a un operador de cable para la

actualización a distancia de un dispositivo se DEBEN firmar conforme a los requisitos definidos en esta Recomendación. Al firmar un fichero de código, el fabricante PUEDE optar por no actualizar el valor signingTime [RFC 2315] que se encuentra en su información de firmado. En la presente Recomendación se requiere que dicho valor sea mayor o igual que la de inicio de validez del CVC. Cuando estos valores sean iguales al firmar una serie de ficheros de código, será posible utilizar y reutilizar dichos ficheros. De esta manera, el operador de cable puede utilizar el fichero de código para actualizar o disminuir la versión de código de los dispositivos del fabricante. Los ficheros de código tendrán validez hasta que se genere un nuevo CVC y sea recibido por el elemento PS.

11.8.4.5.3 Requisitos del operador de cable

Cuando un operador de cable reciba ficheros de código de actualización de software provenientes de un fabricante, validará la imagen de código utilizando la clave pública de CA de CVC de CTL. De este modo, el operador podrá verificar que dicha imagen ha sido creada por el fabricante de confianza. El operador de cable puede verificar de nuevo el fichero de código en cualquier momento, repitiendo el proceso.

Cuando un operador de cable desee optar por cofirmar la imagen de código destinada a un dispositivo en su red, DEBE obtener un CVC válido de la CA de CVC de CTL.

Al firmar un fichero de código, el operador de cable DEBE cofirmar el contenido del fichero de conformidad con la norma de firmas PKCS #7, e incluir su CVC, como se define en 11.8.4.1.1. Si bien en IPCable2Home no es obligatorio que el operador de cable cofirme los ficheros de código. No obstante, si el operador sigue todas las reglas definidas en esta Recomendación para preparar un fichero de código, el elemento PS DEBE aceptarlo.

11.8.4.6 Proceso de activación

Se pueden iniciar descargas de código, sin importar el tipo de modo de configuración, durante los procesos de configuración y registro a través de una descarga iniciada mediante el fichero de configuración o, si se trata del funcionamiento normal, a través de una instrucción de descarga iniciada a través de SNMP. El elemento PS DEBE soportar ambos métodos.

NOTA – Antes de activar una descarga segura de software, se DEBE incluir información adecuada de CVC en el fichero de configuración. Si el operador decide utilizar la descarga iniciada a través de SNMP como método para activar la descarga segura de software, se recomienda que la información de CVC esté siempre presente en el fichero de configuración, de tal modo que el elemento PS la tenga inicializada, siempre que la necesite. De lo contrario, si se trata de una descarga iniciada con fichero de configuración como método de activación, la información de CVC DEBE estar presente en el fichero de configuración en el momento de rearrancar el dispositivo para obtener el fichero de configuración que activará el proceso de actualización.

11.8.4.6.1 Descarga de software iniciada a través de SNMP

Desde una estación de gestión de red se debe:

- Fijar docsDevSwServer a la dirección del servidor TFTP para actualizaciones de software.
- Fijar docsDevSwFilename al nombre de trayecto de fichero de la imagen de actualización de software.
- Fijar docsDevSwAdminStatus a Upgrade-from-mgt. El docsDevSwAdminStatus se DEBE conservar a lo largo de sucesivas reinicializaciones/rearranques, hasta que haya sido reemplazado por un gestor de SNMP o a través del fichero de configuración del elemento PS.

El estado por defecto de docsDevSwAdminStatus DEBE ser allowProvisioningUpgrade{2} hasta que sea reemplazado por ignoreProvisioningUpgrade{3}, tras una actualización exitosa de software iniciada a través del SNMP, o modificado por la estación de gestión. El docsDevSwOperStatus se DEBE conservar entre las reactivaciones para informar el resultado del último intento de actualización de software.

Cuando haya una pérdida de alimentación eléctrica o reinicializaciones que afecten a un elemento PS durante la actualización iniciada a través del SNMP, dicho elemento DEBE reanudar la actualización sin que sea necesaria la intervención del operador, tras lo cual:

- docsDevSwAdminStatus DEBE ser Upgrade-from-mgt{1}.
- docsDevSwFilename DEBE ser el nombre de fichero de la copia imagen de software que se ha de actualizar.
- docsDevSwServer DEBE ser la dirección del servidor TFTP que contiene la imagen de software que se ha de actualizar.
- docsDevSwOperStatus DEBE fijarse a inProgress{1}.
- docsDevSwCurrentVer DEBE ser la versión actual del software que está funcionando en el dispositivo.

Cuando el elemento PS alcance el número máximo de reintentos (max retries = 3) que resultan de varias pérdidas de alimentación eléctrica o reinicializaciones durante la actualización iniciada a través del SNMP, el estado del elemento PS DEBE satisfacer los siguientes requisitos tras haber sido registrado:

- docsDevSwAdminStatus DEBE fijarse a allowProvisioningUpgrade{2}.
- docsDevSwFilename DEBE ser el nombre de fichero del software que falló el proceso de actualización.
- docsDevSwServer DEBE ser la dirección del servidor TFTP que contiene el software que falló el proceso de actualización.
- docsDevSwOperStatus DEBE fijarse a other{5}.
- docsDevSwCurrentVer DEBE ser la versión actual del software que está funcionando en el dispositivo.

Cuando un elemento PS agote la cantidad requerida de reensayos TFTP emitiendo un total de 16 reensayos consecutivos, DEBE retornar a la última imagen de trabajo conocida, pasar a un estado de funcionamiento y cumplir con los siguientes requisitos:

- docsDevSwAdminStatus DEBE fijarse a allowProvisioningUpgrade{2}.
- docsDevSwFilename DEBE ser el nombre de fichero del software que falló el proceso de actualización.
- docsDevSwServer DEBE ser la dirección del servidor TFTP que contiene el software que falló el proceso de actualización.
- docsDevSwOperStatus DEBE fijarse a failed{4}.
- docsDevSwCurrentVer DEBE ser la versión actual de software que está funcionando en el dispositivo.

Cuando el elemento PS haya completado la actualización segura de software iniciada a través del SNMP, DEBE rearrancar y empezar a funcionar utilizando la imagen de software correcta. Cuando el dispositivo funcione, DEBE cumplir con los siguientes requisitos:

- Fijar su docsDevSwAdminStatus a ignoreProvisioningUpgrade{3}.
- Fijar su docsDevOperStatus a completeFromMgt{3}.
- Rearrancar.

El elemento DEBE utilizar adecuadamente el estado ignoreProvisioningUpgrade, a fin de ignorar el valor de actualización de software que haya podido ser incluido en su fichero de configuración. El PS DEBE empezar a funcionar con la imagen de software correcta y DEBE cumplir los siguientes requisitos:

- docsDevSwAdminStatus DEBE fijarse a ignoreProvisioningUpgrade{3}.

- docsDevSwFilename PUEDE ser el nombre de fichero del software que funciona actualmente en el elemento PS.
- docsDevSwServer PUEDE ser la dirección del servidor TFTP que contiene el software que funciona actualmente en el elemento PS.
- docsDevSwOperStatus DEBE fijarse a completeFromMgt{3}.
- docsDevSwCurrentVer DEBE ser la versión actual del software que funciona en el elemento PS.

Cuando este elemento descargue con éxito (o detecte durante la descarga), una imagen que no esté destinada al dispositivo:

- DocsDevSwAdminStatus DEBE fijarse a allowProvisioningUpgrade{2}.
- DocsDevSwFilename DEBE ser el nombre del fichero del software que no pudo efectuar la actualización.
- DocsDevSwServer DEBE ser la dirección del servidor TFTP que contiene el software que falló el proceso de actualización.
- DocsDevSwOperStatus DEBE fijarse a other{5}.
- DocsDevSwCurrentVers DEBE ser la versión actual del software que funciona en el dispositivo.

Cuando el elemento PS encuentre que la imagen descargada está alterada o corrupta, DEBE rechazarla. El elemento PS PUEDE reintentar la descarga si no se ha alcanzado aún el número máximo (MAX) de reintentos de secuencia TFTP. Cuando el elemento PS decida no reintentar y aún no se haya alcanzado el número MAX de reintentos de secuencia TFTP, el elemento DEBE regresar a la última imagen de trabajo conocida y pasar al estado de funcionamiento, generar una notificación de eventos adecuada como se especifica en 11.8.4.8 y cumplir con los siguientes requisitos:

- DocsDevSwAdminStatus DEBE fijarse a allowProvisioningUpgrade{2}.
- DocsDevSwFilename DEBE ser el nombre del fichero del software que no pudo efectuar la actualización.
- DocsDevSwServer DEBE ser la dirección del servidor TFTP que contiene el software que falló el proceso de actualización.
- DocsDevSwOperStatus DEBE fijarse a other{5}.
- DocsDevSwCurrentVer DEBE ser la versión actual del software que funciona en el dispositivo.

Cuando el elemento PS encuentre que la imagen descargada está alterada o corrupta, DEBE rechazarla. El elemento PS PUEDE reintentar la descarga de la nueva imagen si no se ha alcanzado aún el número MAX de reintentos de secuencia TFTP. Tras el decimosexto intento consecutivo de descarga fallida de software, el elemento PS DEBE retornar a la última imagen de trabajo conocida y pasar a un estado de funcionamiento. En este caso, es necesario que el elemento PS envíe dos notificaciones, a saber, una indicando que se ha alcanzado el límite de reensayos MAX de TFTP y la otra que la imagen está alterada. Inmediatamente después de llegar a su estado de funcionamiento, el elemento PS DEBE cumplir los siguientes requisitos:

- DocsDevSwAdminStatus DEBE fijarse a allowProvisioningUpgrade{2}.
- DocsDevSwFilename DEBE ser el nombre del fichero del software que no pudo efectuar la actualización.
- DocsDevSwServer DEBE ser la dirección del servidor TFTP que contiene el software que falló el proceso de actualización.
- DocsDevSwOperStatus DEBE fijarse a other{5}.

- DocsDevSwCurrentVer DEBE ser la versión actual del software que funciona en el dispositivo.

11.8.4.6.2 Descarga de software iniciada a través del fichero de configuración

La descarga de software iniciada a través el fichero de configuración comienza en un PS autónomo mediante la inclusión en su fichero de configuración de PS del parámetro nombre de fichero de actualización de software (TLV-9) Y el parámetro servidor TFTP de actualización del software (TLV-21). Un PS integrado DEBE ignorar TLV-9 y TLV-21 si están presentes en su fichero de configuración de PS, puesto que la actualización del software de un PS integrado está controlada por el módem de cable. Si tanto el parámetro nombre de fichero de actualización de software (TLV-9), con un valor válido, como el parámetro servidor TFTP de actualización del software (TLV-21), también con un valor válido, están incluidos en el fichero de configuración del PS del elemento PS autónomo, Y si el valor del parámetro nombre del fichero de actualización del software no concuerda con el nombre del fichero de la imagen por software actual, es decir, el valor de docsDevSwFilename, el elemento PS DEBE solicitar el fichero especificado a través del TFTP desde el servidor cuya dirección se incluyó en el parámetro servidor TFTP de actualización del software.

Si un PS autónomo recibe un fichero de configuración de PS en el que están presentes el parámetro nombre de fichero de actualización de software (TLV-9) y un valor de TLV-28 del objeto docsDevSwFilename Y los valores de TLV-9 y de docsDevSwFilename son distintos, el PS DEBE rechazar el fichero de configuración de PS, debe informar del ID de evento 73040102 (Formato/contenido de TLV no válido), guardar todos los valores de objetos que existieran antes de intentar procesar este fichero de configuración erróneo y hacer un reinicio.

NOTA – La dirección IP del servidor de software es un parámetro independiente. De haberlo, el elemento PS DEBE intentar la descarga del fichero especificado de este servidor. De lo contrario, DEBE intentar descargarlo del servidor de fichero de configuración.

Cuando el elemento PS haya alcanzado el número máximo de reintentos (max retries = 3) debidos a varias interrupciones de alimentación eléctrica, o de reinicializaciones durante la actualización iniciada a través del fichero de configuración, tras haber sido registrado el estado del elemento PS DEBE cumplir con los requisitos siguientes:

- docsDevSwAdminStatus DEBE fijarse a allowProvisioningUpgrade{2}.
- docsDevSwFilename DEBE ser el nombre de fichero del software que no pudo efectuar el proceso de actualización.
- docsDevSwServer DEBE ser la dirección del servidor TFTP que contiene el software que falló el proceso de actualización.
- docsDevSwOperStatus DEBE fijarse a other{5}.
- docsDevSwCurrentVer DEBE ser la versión actual de software que funciona en el dispositivo.

Cuando un elemento PS agote la cantidad requerida de reensayos TFTP, al emitir 16 reensayos consecutivos, DEBE retornar a la última imagen de trabajo conocida, pasar a un estado de funcionamiento y cumplir los siguientes requisitos:

- docsDevSwAdminStatus DEBE fijarse a allowProvisioningUpgrade{2}.
- docsDevSwFilename DEBE ser el nombre de fichero del software que no pudo efectuar el proceso de actualización.
- docsDevSwServer DEBE ser la dirección del servidor TFTP que contiene el software que falló el proceso de actualización.
- docsDevSwOperStatus DEBE fijarse a failed{4}.

- docsDevSwCurrentVer DEBE ser la versión actual de software que funciona en el dispositivo.

Tras haber completado la actualización segura de software iniciada a través del fichero de configuración, el elemento PS DEBE rearrancar y empezar a funcionar utilizando la imagen correcta de software. Una vez que se ha registrado el elemento PS:

- docsDevSwAdminStatus DEBE fijarse a allowProvisioningUpgrade{2}.
- docsDevSwFilename PUEDE ser el nombre del fichero del software que funciona actualmente en el dispositivo.
- docsDevSwServer PUEDE ser la dirección del servidor TFTP que contiene el software que funciona actualmente en el dispositivo.
- docsDevSwOperStatus DEBE fijarse a completeFromProvisioning{2}.
- docsDevSwCurrentVer DEBE ser la versión actual del software que está funcionando en el dispositivo.

11.8.4.7 Verificación de códigos

El elemento PS, para lograr la descarga segura de software, DEBE efectuar las pruebas de verificación presentadas en esta cláusula. Si cualquiera de ellas falla, o si se rechaza cualquier porción del fichero de código debido a un formato no válido, el elemento PS DEBE interrumpir inmediatamente el proceso de descarga, registrar el error, cuando corresponda, suprimir el resto del proceso hasta dicha etapa, y continuar el funcionamiento con su código actual.

Se pueden efectuar las siguientes pruebas de verificación en cualquier orden, siempre y cuando se realicen todas las que se presentan en esta cláusula:

1) El elemento PS DEBE validar la información de firma del fabricante verificando que el valor de signingTime [RFC 2315] sea:
   a) mayor o igual que el valor codeAccessStart del fabricante presente en el elemento PS;
   b) mayor o igual que la hora de inicio de validez del CVC de fabricante;
   c) menor o igual que la hora de fin de validez del CVC del fabricante.
2) El elemento PS DEBE validar el CVC del fabricante verificando que:
   a) el CVC sea exactamente el mismo que se especifica en el cuadro 11-8;
   b) el sujeto organizationName del CVC sea idéntico al nombre de fabricante almacenado actualmente en la memoria del elemento PS;
   c) la hora de inicio de validez del CVC sea mayor o igual que el valor de cvcAccessStart de fabricante presente en el elemento PS.
3) El elemento PS DEBE validar la firma de certificado utilizando la clave pública de CA de CVC de CTL presente en el elemento PS. A su vez, se valida la firma del certificado de CA de CVC de CTL mediante la clave pública de CA raíz de CVC de CTL presente en dicho elemento. Mediante la verificación de la firma se autentica el origen de la clave de verificación de código pública (CVK, *code verification key*) y se confirma la confianza en la clave.
4) El elemento PS DEBE verificar la firma de fichero de código de fabricante:
   a) El elemento PS DEBE aplicar una nueva función de troceo SHA-1 a SignedContent. Cuando el valor del messageDigest no corresponda con dicha función, el elemento PS DEBE considerar no válida la firma en el fichero de código.
   b) Cuando la firma no pueda verificarse todos los componentes del fichero de código (incluida la imagen de código), y algunos valores calculados a partir del proceso de verificación, DEBEN rechazarse y DEBERÍAN suprimirse inmediatamente.

5) Si se verifica la firma del fabricante y se requiere la firma de un agente cofirmante:

a) El elemento PS DEBE validar la información de firma de cofirmante verificando que:

i) La información de firma de cofirmante esté incluida en el fichero de código.

ii) El valor de signingTime [RFC 2315] sea igual o mayor que el valor correspondiente de codeAccessStart presente en el elemento PS.

iii) El valor de signingTime [RFC 2315] sea mayor o igual que la hora de inicio de validez del CVC correspondiente.

iv) El valor signingTime [RFC 2315] sea menor o igual que la hora correspondiente de fin de validez del CVC.

b) El elemento PS DEBE validar el CVC de cofirmante verificando que:

i) El sujeto organizationName de CVC sea idéntico al nombre de organización de cofirmante almacenada en ese momento en la memoria del elemento PS.

ii) El CVC sea exactamente el mismo que se especifica en el cuadro 11-9 o cuadro 11-10 en función del tipo de cofirmante (CTL o proveedor de servicio).

iii) La hora de inicio de validez de CVC sea mayor o igual que el valor de cvcAccessStart presente actualmente en el elemento PS para el sujeto correspondiente organizationName.

c) El elemento PS DEBE validar la firma del certificado mediante la clave pública de CA de CVC de CTL en su poder. A su vez, se valida la firma de certificado de CA de CVC de CTL mediante la clave pública de CA raíz de CVC de CTL presente en el mismo elemento. La verificación de la firma autentica el origen de la clave de verificación de código pública (CVK) del cofirmante y confirma la confianza en la clave.

d) El elemento PS DEBE verificar la firma del fichero de código de cofirmante.

e) El elemento PS DEBE aplicar una nueva función de troceo SHA-1, al SignedContent. Cuando el valor del messageDigest no corresponda a la nueva función de troceo, el elemento PS DEBE considerar la firma que aparece en el fichero de código como no válida.

f) Cuando la firma no pueda verificarse se DEBEN rechazar y DEBERÍAN suprimir inmediatamente todos los componentes del fichero de código (incluyendo la imagen de código) y cualquier valor que se calcule a partir del proceso de verificación.

6) Si se ha verificado la firma del fabricante y, facultativamente, la del cofirmante, la imagen de código se considera de confianza y se puede continuar con la instalación. Antes de instalar la imagen de código, se DEBERÍAN descartar inmediatamente todas las otras componentes del fichero de código y todos los valores calculados a partir del proceso de verificación, salvo los valores signingTime [RFC 2315] y el de inicio de validez del CVC.

7) Cuando no se pueda instalar el código, el elemento PS DEBE rechazar los valores signingTime [RFC 2315] y de inicio de validez del CVC que acaba de recibir en el fichero de código.

8) Si se termina con éxito la instalación, el elemento PS DEBE actualizar los controles de fabricante que varían con el tiempo utilizando los valores de la información de firma y CVC de fabricante:

a) Actualizar el valor actual de codeAccessStart utilizando el valor signingTime [RFC 2315].

b) Actualizar el valor actual cvcAccessStart utilizando el valor de inicio de validez del CVC.

9) Si se termina con éxito la instalación de código, y el fichero de código había sido cofirmado, el elemento PS DEBE actualizar los controles del cofirmante que varían con el tiempo utilizando los valores de la información de firma y CVC del cofirmante:

   a) Actualizar el valor actual de codeAccessStart utilizando el valor signingTime [RFC 2315].

   b) Actualizar el valor actual cvcAccessStart utilizando el valor de inicio de validez del CVC.

11.8.4.8 Códigos de error

Se definen estos códigos para indicar los posibles estados de fallo que ocurren durante el proceso de verificación de código de descarga segura de software.

1) Controles inadecuados de fichero de código:

   a) El sujeto organizationName de CVC del fabricante no corresponde con el nombre del fabricante del elemento PS.

   b) El sujeto organizationName de CVC del agente cofirmante de código no corresponde con el actual agente cofirmante de código del elemento PS.

   c) El valor signingTime [RFC 2315] del fabricante es menor que el valor codeAccessStart que tiene actualmente el elemento PS.

   d) El valor de la hora de inicio de validez [RFC 2315] del fabricante es menor que el valor cvcAccessStart que tiene actualmente el elemento PS.

   e) La hora de inicio de validez del CVC del fabricante es menor que el valor cvcAccessStart que tiene actualmente el elemento PS.

   f) El valor signingTime [RFC 2315] del fabricante es menor que la hora de inicio de validez del CVC.

   g) No hay extensión de utilización de clave ampliada o no es la correcta en el CVC del fabricante.

   h) El valor del signingTime [RFC 2315] del cofirmante es menor que el valor codeAccessStart que tiene actualmente el elemento PS.

   i) El valor de hora de inicio de validez [RFC 2315] del cofirmante es menor que el valor cvcAccessStart que tiene actualmente el elemento PS.

   j) La hora de inicio de validez de CVC de cofirmante es menor que el valor cvcAccessStart que tiene actualmente el elemento PS.

   k) El valor de signingTime [RFC 2315] de cofirmante es menor que la hora de inicio de validez del CVC.

   l) No hay extensión de utilización de clave ampliada o no es la correcta en el CVC de cofirmante.

2) Fallo en la validación de CVC de fabricante de fichero de código.

3) Fallo en la validación de CVS de fabricante de fichero de código.

4) Fallo en la validación de CVC de cofirmante de fichero de código.

5) Fallo en la validación de CVS de cofirmante de fichero de código.

6) Formato incorrecto de CVC de fichero de configuración (por ejemplo, no hay atributo de utilización de clave o no es correcto).

7) Fallo en la validación de CVC de fichero de configuración.

8) Formato incorrecto de CVC de SNMP:

   a) El sujeto organizationName de CVC para el fabricante no corresponde con el nombre de fabricante del dispositivo.

b) El sujeto organizationName de CVC para el agente cofirmante de código no corresponde con el agente actual cofirmante de código del elemento PS.

c) La hora de inicio de validez de CVC es menor o igual al valor cvcAccessStart de sujeto correspondiente que tiene actualmente el elemento PS.

d) No hay atributo de utilización de clave o es incorrecto.

9) Fallo de validación de CVC de SNMP.

11.8.4.9 Disminución de la versión de software

Proceso que consiste en suprimir la versión actualizada de la imagen de software descargada, y que hace que el dispositivo doméstico de cable retorne exactamente a su estado anterior.

Cuando el elemento PS recibe un fichero de código que tiene una hora de firmado posterior a la hora de firmado presente en su memoria, el dispositivo DEBE actualizarla utilizando el valor recibido.

Puesto que elemento PS no acepta ficheros de código que tengan horas de firmado anteriores a su valor almacenado internamente, para actualizar un dispositivo mediante un nuevo fichero de código sin necesidad de negar acceso a ficheros de código anteriores, el firmante (por ejemplo, el fabricante, el operador de cable o el CTL) puede decidir no actualizar la hora de firmado. De esta manera, el operador puede, gracias a varios ficheros de código que tienen la misma hora de firmado de código, disminuir sin dificultad la versión de una imagen de código de dispositivo (esto es, hasta que se actualice el CVC). Siendo así, el operador de cable dispone de varias ventajas que tendrá que balancear con las posibilidades de sufrir un ataque de reproducción de fichero de código.

Es posible también firmar el fichero de código anterior utilizando una hora de firmado igual o mayor que la hora de firmado de la última actualización.

11.9 Seguridad del fichero de configuración de PS en el modo de configuración DHCP

11.9.1 Objetivos de la infraestructura de seguridad del fichero de configuración

Se asegura el fichero de configuración a fin de:

- Disponer de un túnel autenticado entre el dispositivo de cliente PS y el servidor HTTPS, a fin de garantizar que los ficheros de configuración pasen seguros desde el operador de cable hasta el PS. Se incluye automáticamente una prueba de integridad cuando se autentica un mensaje.
- Criptar los ficheros de configuración durante el transporte para reducir la probabilidad de manipulaciones clandestinas en la barrera contra fuegos y en la configuración de PS.
- Reducir el riesgo de que una fuente no autorizada descargue un fichero de configuración al PS.

11.9.2 Directrices de diseño del sistema de seguridad del fichero de configuración

Véase el cuadro 11-25.

Cuadro 11-25/J.192 – Directrices de diseño del sistema de seguridad

Referencia	Directrices
SEC14	El operador de cable podrá autenticar y, facultativamente, criptar el transporte de los ficheros de configuración del PS o de la barrera contra fuegos.

11.9.3 Descripción del sistema de seguridad del fichero de configuración

En el modo de configuración DHCP, el operador de cable puede decidir activar la seguridad durante la descarga del fichero de configuración. Por "ficheros de configuración" se entiende, en esta cláusula, los de configuración del PS o de la barrera contra fuegos. La seguridad se consigue gracias al establecimiento de una sesión TLS entre el PS y el servidor HTTPS. En IPCable2Home se requiere que el PS comprenda esta opción de seguridad y utilice TLS en la secuencia de configuración a fin de proporcionar una sesión segura entre el servidor HTTPS y él mismo, a efectos de descargar su fichero de configuración y el de la barrera contra fuegos de manera segura. El protocolo TLS permite autenticar y criptar la sesión, de conformidad con la configuración activada por el operador de cable. Antes de enviar el mensaje de notificación de configuración completa Syslog y/o NMS, se suspende la sesión. Cuando la TLS se configure en capas dentro del protocolo HTTPS la activación, la gestión y los contenidos de la descarga del fichero de configuración se efectúan conforme a las normas de industria. En IPCable2Home se especifican los requisitos para una sesión TLS conforme a [RFC 2246]. Se articulan las opciones TLS de tal modo que se cree un conjunto mínimo de características que interfuncionen para el PS. En la cláusula 13 se describe en detalle el flujo de configuración con HTTP/TLS.

El protocolo TLS permite que haya un túnel de transporte criptado y autenticado para todas las aplicaciones que estén por encima de ella en la pila OSI. La estructura de capas del TLS no afecta al protocolo HTTP propiamente dicho. Las capas en cursiva y subrayadas en la pila se criptan para un paquete de datos TLS normalizado. El protocolo HTTP, que suele estar por encima de TCP, se apoya directamente en el TLS. Véase el cuadro 11-26.

Cuadro 11-26/J.192 – Criptación de TLS

Datos del fichero de configuración (cabida útil)
HTTP
TLS
TCP
IP
MAC
PHY

11.9.4 Requisitos de seguridad del fichero de configuración

El PS DEBE implementar la versión 1.0 del protocolo de seguridad de capa de transporte (TLS) que se define en [RFC 2246], salvo en los casos que se indiquen en la presente Recomendación. Estas excepciones se prevén para simplificar los requisitos de implementación y de prueba. En algunos casos, las excepciones constituyen un conjunto mínimo de requisitos que se alinean con otras tecnologías utilizadas por la industria de cable. Gracias a estos requisitos, el PS suministrará un nivel coherente de calidad de funcionamiento para los operadores de cable. Asimismo, en esta cláusula se aclaran las ambigüedades y se definen los procesos no definidos en las RFC, pero que son necesarios en IPCable2Home. Éste es el caso, en particular, durante el manejo de fallos.

NOTA – No se utilizará la característica del algoritmo de compresión de la TLS.

Se DEBE soportar la versión 1.0 de TLS (SSL3, TLSv1). El PS NO DEBE soportar versiones anteriores del TLS. Cuando el servidor intente utilizar dichas versiones, el PS DEBE rechazar los mensajes procedentes del mismo.

11.9.4.1 Activación del TLS

Para poder activar una descarga segura de fichero de configuración en el modo de configuración DHCP, el mensaje de acuse de recibo de DHCP (DHCP Ack) deberá incluir la dirección IP del servidor HTTPS en el campo siaddr. El DHCP Ack incluirá también la opción 72 con la dirección IP del servidor HTTPS. Si la dirección IP que aparece en el campo siaddr corresponde a la dirección IP en la opción 72, el PS DEBE establecer una sesión TLS con el servidor HTTPS en la dirección IP que figura en el mensaje de acuse de recibo (ack), antes de solicitar el fichero de configuración. El PS DEBE descargar el fichero de configuración utilizando HTTP/TLS, cuando la primera dirección IP en la opción 72 de TLV concuerde con dicha dirección IP en siaddr, del mensaje acuse de recibo de DHCP. Si el PS no recibe una concordancia en el mensaje DHCP Ack, NO DEBE iniciar una sesión TLS, pues los requisitos de esta cláusula no se aplican y el cliente PS DEBE utilizar el modo de configuración DHCP junto con el proceso especificado de descarga TFTP. En la cláusula 13 se especifican el diagrama de flujo de configuración y el cuadro de descripción. Cuando se incluyan también la opción 66 y la 72, y la dirección IP que aparece en la opción 72 sea la dirección IP del campo siaddr, el PS DEBE iniciar una sesión TLS con el servidor HTTPS y NO DEBE iniciar la descarga del servidor TFTP que figura en la opción 66.

Si el PS recibe la información necesaria para iniciar un fichero de configuración de barrera contra fuegos, tal como se especifica en la cláusula 7, ha de determinar si es necesario seguir o establecer una sesión TLS con un servidor HTTPS.

11.9.4.2 Prerrequisitos de sesión TLS

Antes de establecer una sesión TLS, el cliente PS DEBE sincronizar su reloj con el servidor ToD. En la cláusula 13 se suministran más detalles al respecto.

Asimismo, el cliente PS DEBE establecer la conexión TCP/IP con servidor HTTPS antes de enviar el mensaje ClientHello de TLS. Tras haber completado la descarga del fichero de configuración, el PS DEBE cerrar la conexión TCP/IP. El cliente PS DEBE utilizar el puerto #443 TCP, especificado por las normas IANA, para conectarse al servidor HTTP/TLS. Si el PS no consigue establecer con éxito una conexión TCP/IP DEBE registrar el evento 68002000 y reiniciar la configuración empleando el procedimiento de reintento definido en 7.4.4.2.4 Funcionamiento posterior a la activación, para gestionar los reintentos.

11.9.4.3 Mensajes TLS

A menos que se indique lo contrario, todos los mensajes son conformes a [RFC 2246].

11.9.4.3.1 Mensaje ClientHello

El cliente PS DEBE enviar un mensaje ClientHello al servidor HTTP/TLS a fin de poder iniciar la secuencia de toma de contacto de TLS. Después de que se haya enviado dicho mensaje, si no se ha podido establecer la sesión TLS tras cinco intentos, cada uno con una tolerancia de 30 segundos, el PS DEBE abortar la sesión y enviar el evento 68002100.

11.9.4.3.2 Procesamiento en el PS de los mensajes del servidor

El PS DEBE poder procesar los mensajes del servidor, como se define en [RFC 2246], salvo:

- HelloRequest: El PS DEBE ignorar los mensajes HelloRequest de un servidor. De esta manera se evita responder a peticiones malintencionadas provenientes de los servidores HTTPS. Sólo se podrá iniciar el proceso HTTP/TLS cuando el operador de cable haya configurado las opciones DHCP adecuadas. Cabe suponer que DHCP es de confianza, aunque no es asegurado por IPCable2Home.
- ServerCertificate: Cabe esperar que el servidor HTTPS envíe su certificado de dispositivo al PS dentro del mensaje ServerCertificate. Además de los requisitos [RFC 2246] para este mensaje, el cliente PS DEBE validar y verificar el certificado de servidor HTTPS. Si dicha

autenticación falla, se considera que ha fracasado la sesión TLS y el PS DEBE enviar el evento 68002200 con el código de error definido en [RFC 2246].

11.9.4.3.3 Mensaje ClientCertificate (certificado de cliente)

Cuando lo solicite el servidor HTTPS, el PS DEBE enviar su certificado de elemento PS y emitir el certificado CA de fabricante dentro del mensaje certificado de cliente. Se espera que dicho servidor validará y verificará los certificados de cliente PS antes de efectuar la toma de contacto. Cuando el servidor no pueda autenticar los certificados del PS, éste DEBE tratar el mensaje recibido como una alerta fatal, enviar el evento 68002200, con el código de error apropiado según [RFC 2246] y reiniciar la configuración utilizando el procedimiento de reintento definido en 7.4.4.2.4, Funcionamiento posterior a la activación.

11.9.4.4 Series de conjunto de cifrado y compresión de TLS

Se DEBE enumerar el conjunto de cifrado solicitado dentro del mensaje ClientHello. El soporte del conjunto de cifrado requerido constituye un subconjunto de [RFC 2246] necesario para armonizar con la tecnología que se utiliza en la industria del cable. El operador de cable habrá de escoger el algoritmo de criptación y autenticación adecuado en el servidor HTTPS para comunicarse con el PS y que sea conforme con su propio modelo de seguridad. Los conjuntos de cifrado que se requieren de acuerdo con esta especificación son subconjuntos de las que están disponibles, pudiendo el PS soportar otros más.

El PS DEBE soportar los siguientes algoritmos criptográficos:

- TLS_RSA_WITH_NULL_MD5;
- TLS_RSA_WITH_NULL_SHA;
- TLS_RSA_WITH_DES_CBC_SHA;
- TLS_RSA_WITH_3DES_EDE_CBC_SHA.

Ya que no es necesaria la característica de compresión del protocolo TLS, el cliente PS DEBE utilizar el tipo de compresión compressionMethod.null.

11.9.4.5 Interrupción de sesión TLS

Cuando el PS deba descargar otro fichero de configuración para la barrera contra fuegos inmediatamente después de haber recibido su fichero de configuración, y el primero deba descargarse del mismo servidor HTTPS del que se descargó el fichero de configuración del PS, cabe esperar que la sesión TLS permanecerá activa. El PS DEBE garantizar que la sesión TLS y la correspondiente a TCP/IP se cierren con cada servidor HTTPS después de que:

- El fichero de configuración PS se descarga, si y solamente si no se debe descargar ningún fichero de configuración de barrera contra fuegos del mismo servidor HTTPS, inmediatamente después de haber procesado el fichero de configuración PS.
- El fichero de configuración de barrera contra fuegos se descarga y procesa.

11.9.4.6 Eventos de TLS

En [RFC 2246] se define un protocolo de alerta para tratar el cierre y los errores relativos a TLS. Se DEBEN soportar las alertas y errores de TLS y utilizarlos como se define en [RFC 2246], salvo la alerta decompression_failure (30), puesto que no se soporta la compresión. El PS DEBE registrar todas las alertas de TLS mediante el evento 68002200 con el código de error adecuado definido en [RFC 2246] insertado en el campo texto de evento <P1>. Los errores que tengan que ver con certificados se DEBEN tratar como graves, puesto que el PS depende de la autenticación de servidor.

Cuando el cliente PS no haya recibido un mensaje del servidor HTTP/TLS en respuesta a un mensaje TLS enviado hasta en cinco ocasiones, con tolerancia de 30 segundos cada una, se considerará que ha fallado la conexión TLS y el PS DEBE enviar el evento 68002100.

11.9.4.7 Descarga y eventos de HTTP

Se DEBE iniciar la transferencia HTTP solamente después de que se haya completado la toma de contacto de TLS. El PS DEBE comunicarse con el servidor HTTP/TLS mediante el HTTP normalizado, como se define en [RFC 2616]. El cliente PS DEBE iniciar una petición HTTP versión 1.1 hacia el servidor solicitando el fichero de configuración de PS o de la barrera contra fuegos. El nombre de fichero de configuración de PS que se utiliza en la "petición GET" de HTTP DEBE ser idéntico al nombre de fichero que recibió el PS en el ack de DHCP. El nombre del fichero de configuración de barrera contra fuegos que se utiliza en la "petición GET" DEBE ser idéntico al nombre del fichero que recibe el PS en el fichero de configuración PS o a través de la instrucción SNMP set.

El cliente PS DEBE tratar todos los mensajes de estado de conformidad con [RFC 2616]. Cuando dicho cliente reciba un mensaje de estado HTTP que indique que no se puede completar la descarga HTTP, DEBE suspender la sesión, enviar el evento 68003000 utilizando el código de error adecuado de [RFC 2616] y reiniciar la configuración utilizando el procedimiento de reintento definido en 7.4.4.2.4, Funcionamiento posterior a la activación.

NOTA – Una vez se haya terminado dicha descarga, el PS DEBE enviar el evento 68003200.

11.10 Seguridad física

El PS debe mantener, en su memoria permanente, claves y otros valores criptográficos relacionados con la seguridad de la red. El PS DEBE negar acceso físico no autorizado a este material criptográfico.

El PS especifica el nivel de protección física de las claves requeridas en términos de los niveles de seguridad definidos en FIPS PUBS 140-2, Security Requirements for Cryptographic Modules. En particular, el PS DEBE cumplir con los requisitos de nivel 1 de seguridad FIPS PUBS 140-2.

Dicho nivel 1 requiere una protección física mínima mediante la utilización de ámbitos de calidad de producción y de prácticas de software recomendadas.

11.11 Algoritmos criptográficos

11.11.1 Tipo SHA-1

La implementación de SHA-1 en el PS DEBE utilizar el algoritmo de troceo SHA-1 que se define en [FIPS 180-1].

12 Procesos de gestión

12.1 Introducción y presentación

Esta cláusula contiene ejemplos de los procesos asociados a la utilización de las herramientas descritas en la cláusula 6 (Herramientas de gestión) y los procesos adicionales que facilitan otras funciones de gestión requeridas definidas en esta Recomendación. El acceso a la base de datos del PS y demás operaciones del PS del portal de gestión de IPCable2Home (CMP) se describen en la cláusula 6. Las reglas más representativas del acceso a la MIB figuran en 6.3.3.1.4.2.

Se exponen procesos relativos a la gestión y otros procesos descriptivos correspondientes a las siguientes situaciones:

- Procesos de las herramientas de gestión:
  - Funcionamiento del CTP:
    - herramienta de velocidad de la conexión;
    - herramienta ping.
- Funcionamiento del PS:
  - Acceso a la base de datos del PS.
  - Reconfiguración:
    - descarga de software del PS;
    - descarga del fichero de configuración del PS.
- Acceso a la MIB:
  - Configuración del VACM.
  - Configuración de la mensajería de eventos de gestión:
    - funcionamiento de la notificación de eventos CMP;
    - funcionamiento del estrangulamiento y limitación de eventos del CMP.

12.1.1 Objetivos

Esta cláusula se compone principalmente de texto informativo, destinado a facilitar la comprensión y no contiene ningún requisito. Los ejemplos describen la forma de utilizar las herramientas de gestión para poder conseguir funciones de gestión típicas. Se proporcionan asimismo gráficos secuenciales de procesos adicionales relativos a la gestión (es decir, los no definidos en la cláusula 6), incluidos los procesos de gestión o las etapas o fases de procesos asociados con el uso de las herramientas de gestión. Todos los procesos mostrados implican la interacción del elemento PS con los sistemas situados en la cabecera.

12.2 Proceso de las herramientas de gestión

Los procesos de las herramientas de gestión son los asociados con las herramientas de gestión necesarias definidas en la cláusula 6.

12.2.1 Funcionamiento del CTP

El portal de pruebas de IPCable2Home (CTP) proporciona capacidades para la herramienta de velocidad de la conexión y para la herramienta ping, descritas en 6.4.3.1 y 6.4.3.2 respectivamente.

12.2.1.1 Prueba de velocidad de conexión distante

La prueba de velocidad de conexión distante puede ser útil para la validación de los niveles de calidad de funcionamiento, la identificación de posibles errores de configuración y la determinación de otras características orientadas a la calidad de funcionamiento:

1) El sistema de gestión de red (NMS) comienza la prueba inicializando los parámetros de la prueba y activando la bandera de prueba de comienzo, a través de una petición SNMP SET.
2) El agente SNMP del CMP actualiza la base de datos del PS con los parámetros de prueba y notifica al CTP el comienzo de la prueba.
3) El CTP consulta la base de datos del PS para obtener los parámetros de la prueba.
4) El CTP emite una ráfaga de paquetes UDP con destino al puerto 7 del dispositivo IP de LAN especificado. El puerto 7 se reserva para el servicio de eco.

5) El dispositivo IP de LAN objetivo se limita a devolver al CTP un eco de la cabida útil del paquete UDP.

6) Una vez recibidos todos los paquetes, o alcanzado el límite temporal de la prueba, el CTP actualiza la base de datos del PS con los resultados de la prueba y activa la bandera de terminación de la prueba.

7) El NMS verifica la terminación del mandato comprobado que Status = complete.

8) El NMS solicita los resultados de la prueba mediante una petición SNMP GET.

9) El agente SNMP del CMP consulta la base de datos del PS para obtener los resultados de la prueba y los comunica en la respuesta SNMP GET. Si no se ha completado la prueba, los datos de prueba indican que la prueba continúa efectuándose. El NMS debe repetir la petición SNMP GET hasta que los resultados de la prueba indiquen la conclusión de la misma.

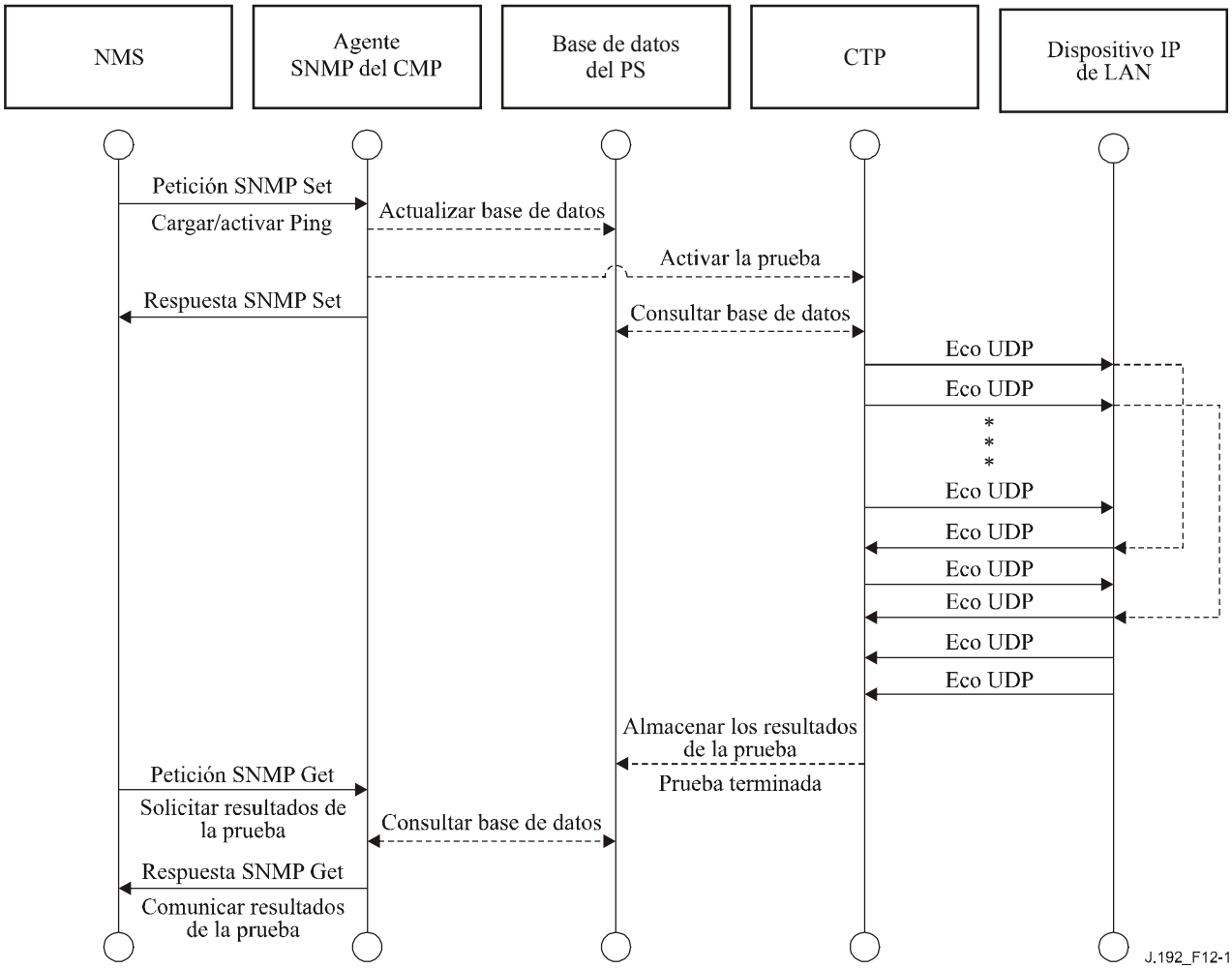


Figura 12-1/J.192 – Diagrama secuencial del proceso de la herramienta de velocidad de conexión

12.2.1.2 Proceso de la herramienta ping

La herramienta ping puede servir para validar el estado de la conectividad, los niveles de la calidad de funcionamiento e identificar posibles errores de configuración.

1) El NMS comienza la prueba inicializando los parámetros de la prueba y activando la bandera de comienzo de la prueba, mediante la petición SNMP SET.
2) El agente SNMP de CMP actualiza la base de datos del PS con los parámetros de la prueba y notifica al CTP el comienzo de la prueba.
3) El CTP consulta la base de datos del PS en busca de los parámetros de la prueba.
4) El CTP emite un paquete de petición de eco ICMP con destino al dispositivo IP de LAN especificado.
5) El dispositivo IP de LAN objetivo responde con una respuesta de eco ICMP.
6) El CTP actualiza la base de datos del PS con los resultados de la prueba y activa la bandera de terminación de la prueba.
7) El NMS verifica que se ha completado el mandato comprobando que Status = complete.
8) El NMS solicita los resultados de la prueba mediante una petición SNMP GET.
9) El agente SNMP del CMP consulta la base de datos del PS para obtener los resultados de la prueba y los comunica en la respuesta SNMP GET. Si no se hubiese completado la prueba, los datos de la prueba indicarían que la prueba sigue en marcha. El NMS debe repetir la petición SNMP GET hasta que los resultados de la prueba indiquen que se ha completado la misma.

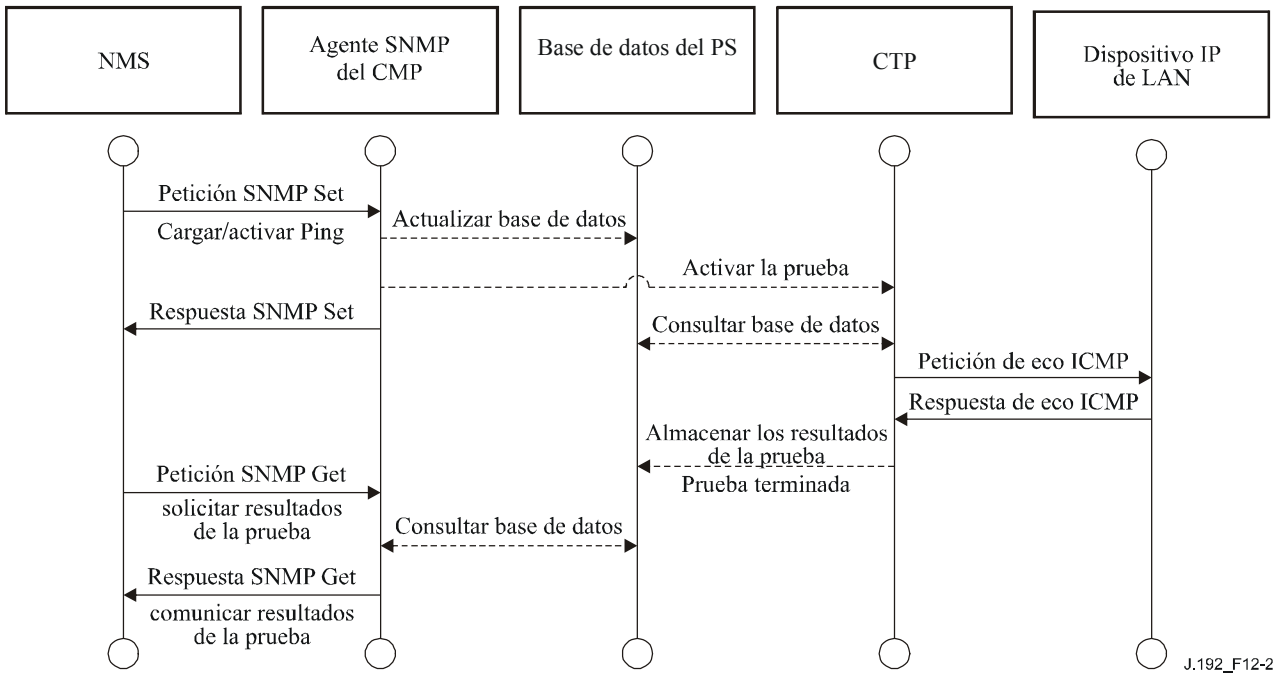


Figura 12-2/J.192 – Diagrama secuencial del proceso de la herramienta ping

12.3 Funcionamiento del PS

El portal de gestión de IPCable2Home (CMP) permite el acceso a la base de datos del PS a través de la interfaz WAN-Man del PS, de acuerdo con lo descrito en la cláusula 6. A continuación se describe la secuencia de mensajes para una operación típica de acceso a la base de datos del PS desde la interfaz WAN-Man del PS.

12.3.1 Acceso a la base de datos del PS

Los parámetros de configuración y gestión almacenados en la base de datos del PS son accesibles por el NMS a través de las MIB del SNMP. Los parámetros se recuperan mediante los mensajes de petición SNMP Get, siguiente petición SNMP Get y bloque SNPM Get emitidos por el NMS teniendo como destino la dirección WAN-Man del PS. Los parámetros pueden modificarse y pueden ejecutarse acciones (como por ejemplo las pruebas de velocidad de la conexión y las herramientas ping) mediante la emisión por parte del NMS de mensajes de petición SNMP Set con los parámetros adecuados, con destino a la dirección WAN-Man del PS.

La figura 12-3 describe la secuencia de mensajes de gestión correspondiente a un acceso típico a la base de datos del PS desde la interfaz WAN-Man del PS. La siguiente secuencia de mensajes supone que se ha establecido un enlace seguro SNMPv3.

1) El NMS lee datos de la base de datos del PS utilizando la "petición SNMP GET". La petición enumera los objetos específicos que el NMS desea obtener de la base de datos.
2) El agente SNMP del CMP consulta la base de datos del PS para obtener los parámetros especificados.
3) El SNMP del CMP comunica los datos al NMS mediante la "respuesta SNMP GET".

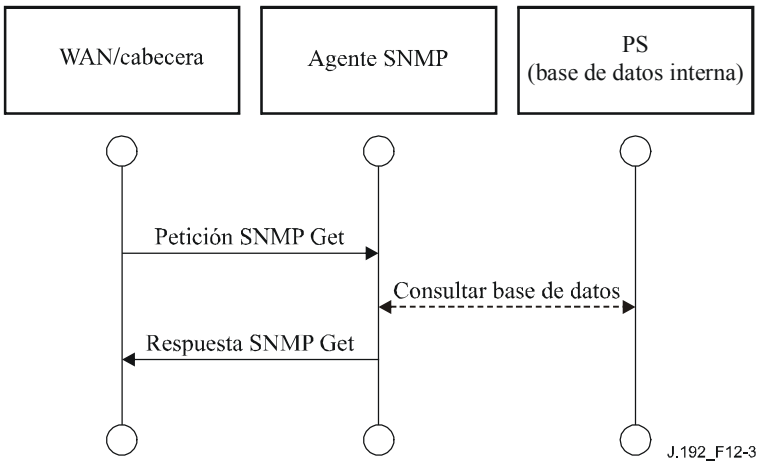


Figura 12-3/J.192 – Diagrama secuencial de acceso a la base de datos del PS desde la interfaz WAN-Man del PS

12.3.2 Reconfiguración

12.3.2.1 Descarga de software del PS

En la figura 12-4 se ilustra el proceso de descarga de software y de microprogramas (firmware) con destino a un PS en el modo de configuración SNMP, que se activan desde el NMS. Se comunica al PS dónde puede conseguir el nuevo fichero de código de software. Una vez completada la descarga del fichero de código, el PS comprobará que no se ha corrompido la imagen durante la descarga. Se efectúa la autenticación para verificar que el fichero de código es de confianza. Tras dicho paso, se rearranca el sistema.

Tras el rearranque, el PS reanuda su funcionamiento con la nueva copia imagen de software. Es posible que el PS necesite volver a configurarse tras la actualización del software, y que haya que proporcionar de nuevo las interfaces de la WAN (no se indica). Si el PS no acepta la nueva copia imagen de software, regresará a la versión de software anterior (copia de seguridad) e informará al NMS de los resultados.

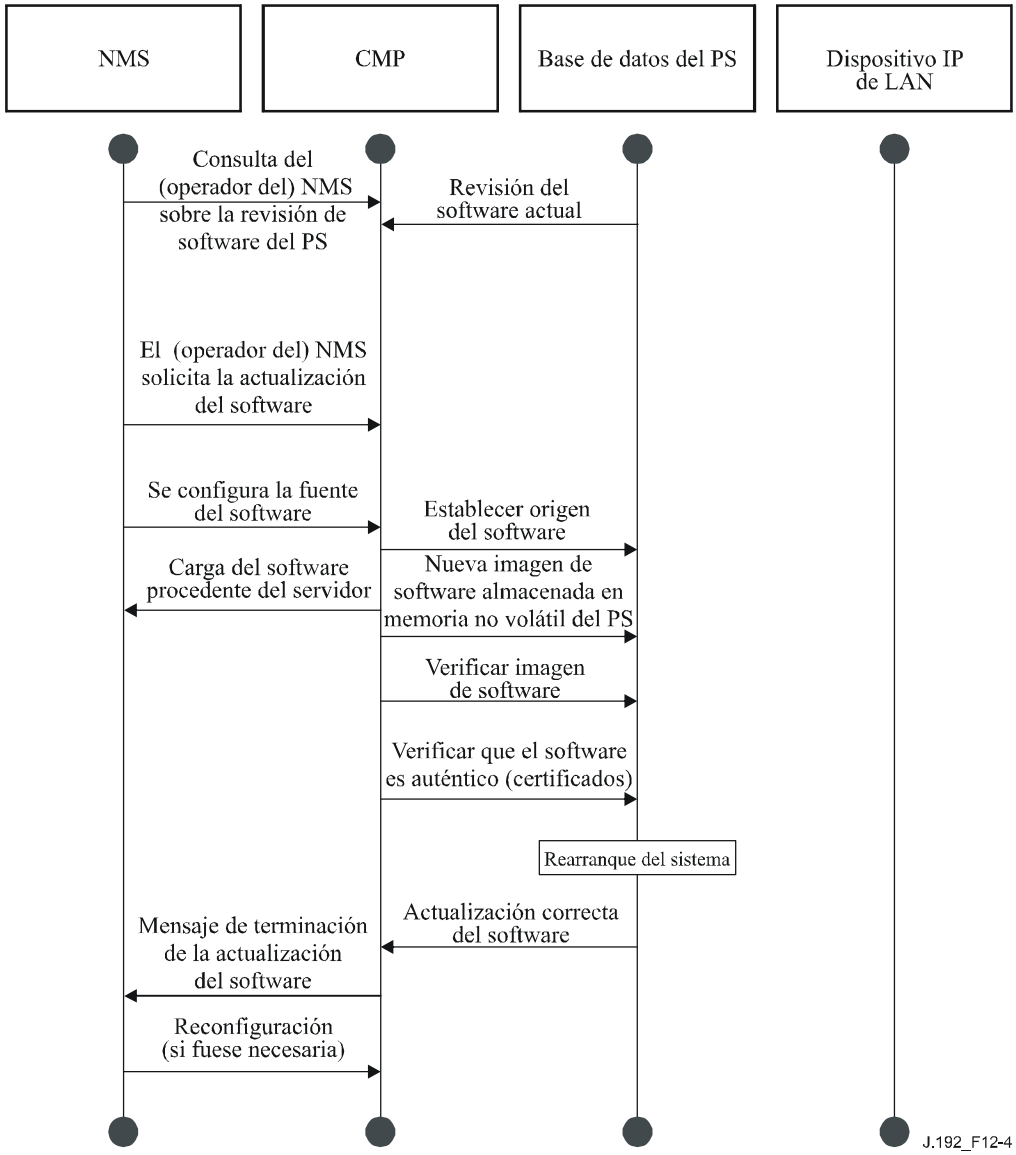


Figura 12-4/J.192 – Diagrama secuencial de la descarga de software del PS

12.3.2.2 Descarga del fichero de configuración del PS

La figura 12-5 ilustra la reconfiguración de un PS en el modo de configuración SNMP, mediante la descarga de un fichero de configuración, que se activa desde el NMS. El fichero de configuración llega al PS escribiendo en el PS el nombre del servidor y del fichero y activando en el PS la descarga del fichero. Una vez cargado el fichero de configuración, se interpretan los mandatos que contiene. Si no se entiende alguno de los mandatos o no son aplicables, se saltan y se genera un evento. Cuando el PS ha completado el proceso del fichero de configuración, graba el número de tuplas TLV procesadas y omitidas de los objetos correspondientes de la MIB.

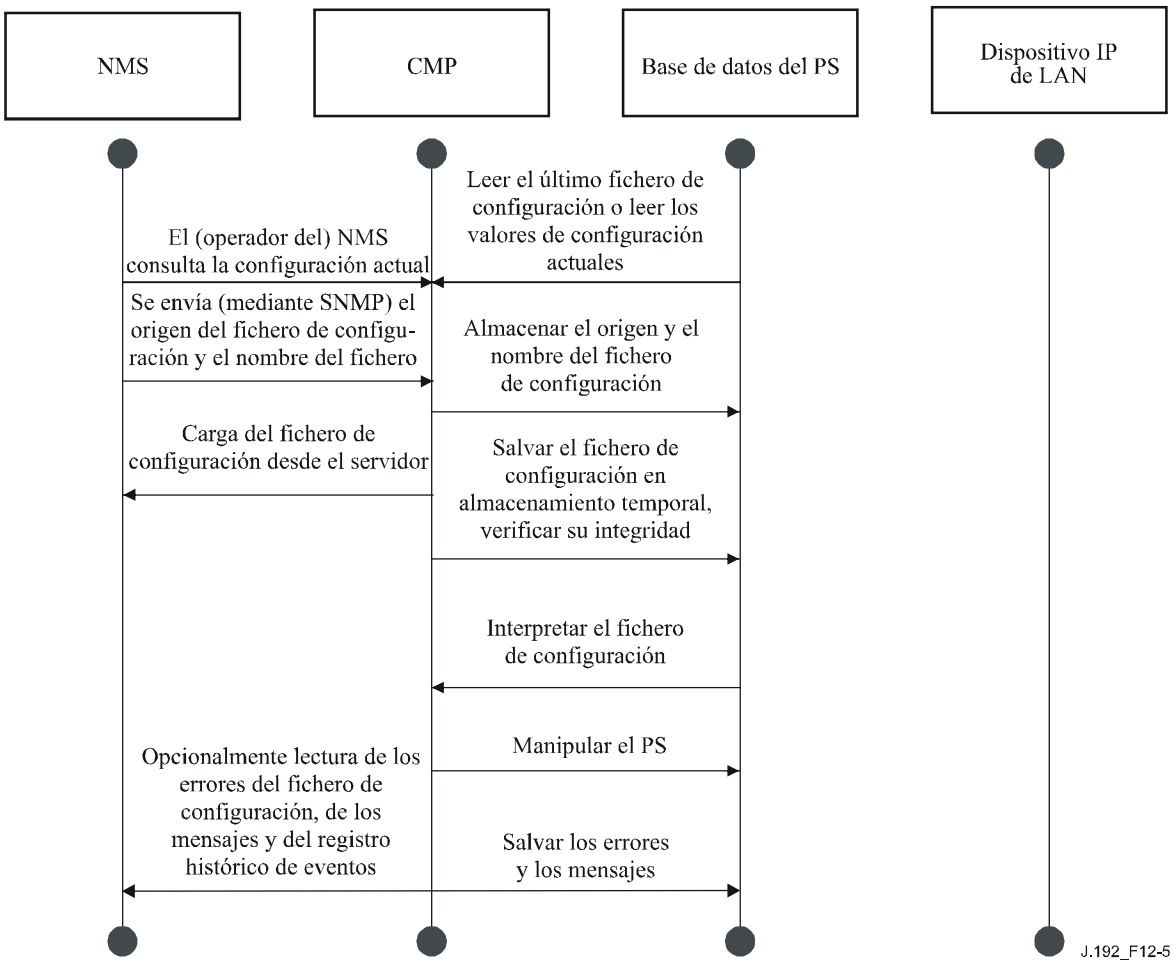


Figura 12-5/J.192 – Diagrama secuencial de la reconfiguración del PS (descarga del fichero de configuración)

12.4 Acceso a la MIB

12.4.1 Configuración del VACM

IPCable2Home especifica que el operador debe controlar el dominio de gestión de IPCable2Home. En la figura 12-6 se muestra un ejemplo de configuración de los parámetros del VACM.

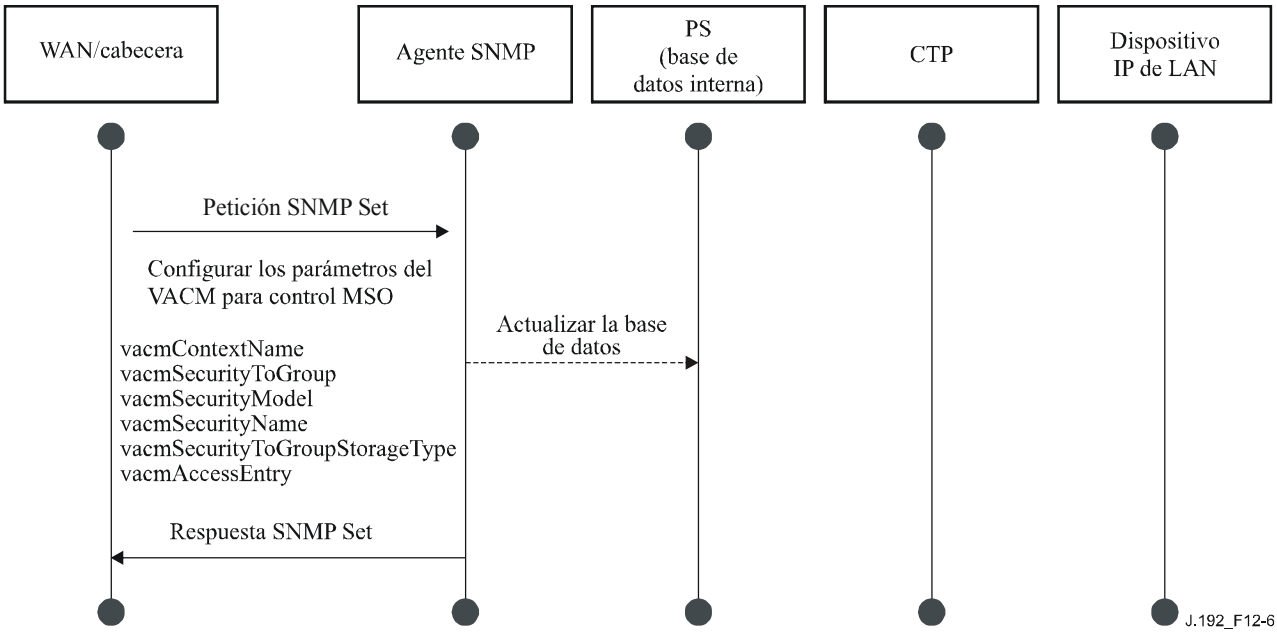


Figura 12-6/J.192 – Secuencia de configuración del PS (parámetros del VACM)

12.4.2 Configuración de la mensajería de eventos de gestión

12.4.2.1 Funcionamiento de la notificación de eventos del CMP

Los eventos de IPCable2Home se comunican mediante la anotación histórica local de eventos, los mensajes SNMP TRAP y SNMP INFORM y mediante SYSLOG. El mecanismo de notificación de eventos puede fijarlo o modificarlo el NMS mediante la emisión de un mensaje de petición SNMP Set dirigido a la dirección WAN-Man del PS.

La figura 12-7 ilustra la configuración de la base de datos del PS para almacenar eventos en ficheros de registro histórico local. Los eventos históricos locales son de dos tipos: no volátiles locales y volátiles locales. El NMS lee el contenido del registro histórico local y escribe dicho contenido en el sistema de anotaciones históricas de eventos de la cabecera. El rearranque del PS provoca que los eventos volátiles desaparezcan de la base de datos del PS. Los eventos no volátiles se mantienen tras los rearranques.

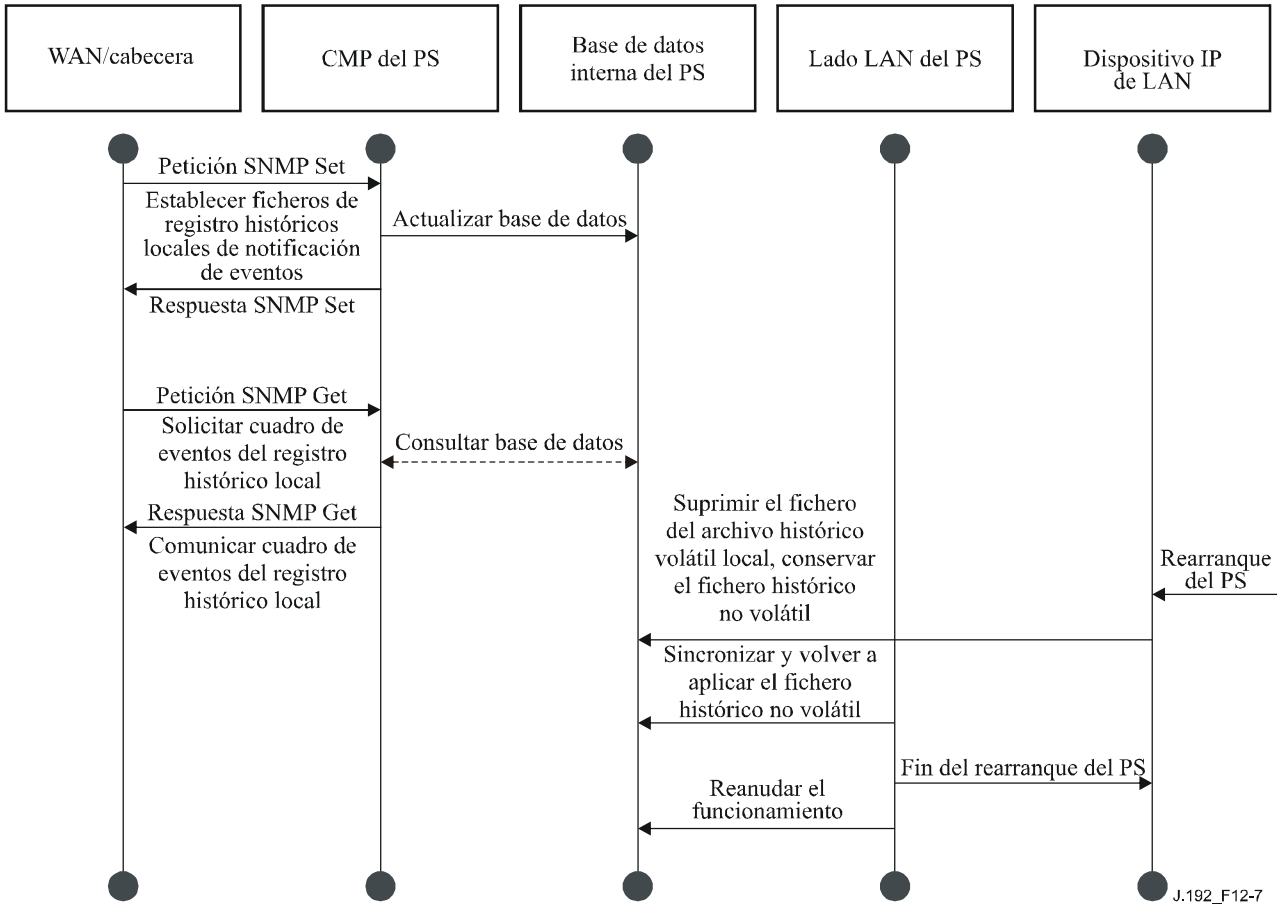


Figura 12-7/J.192 – Secuencia de la configuración del PS (control de eventos)

La figura 12-8 ilustra la descarga de un fichero de configuración para un PS que se encuentra en el modo de configuración SNMP. Este proceso se activa mediante una petición SNMP Set. El PS debe verificar este fichero antes de aceptarlo. En el ejemplo, se comunica un error TLV. Como la notificación de eventos se ha puesto en el modo SNMP TRAP, la dirección del servidor TRAP se recupera de la base de datos del PS y el evento se envía al servidor TRAP.

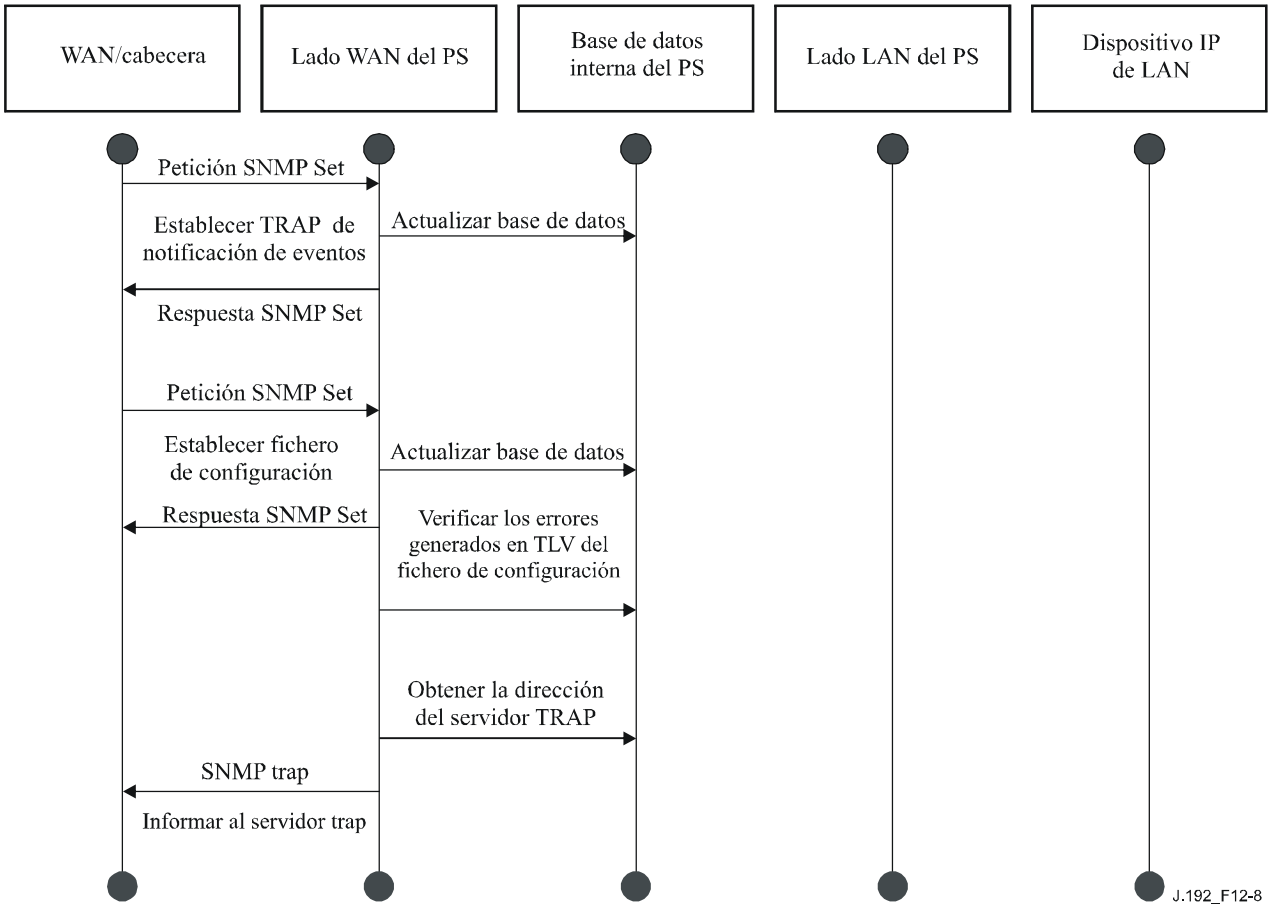


Figura 12-8/J.192 – Secuencia de descarga del fichero de configuración del PS (con TLV no válidos)

La figura 12-9 ilustra el proceso de obtención por parte de un dispositivo IP de LAN de una dirección IP del servidor DHCP local (CDS). La función CDS comprueba si hay direcciones IP disponibles en la base de datos del PS. En este caso, el CDS detecta que no hay direcciones IP disponibles del grupo de direcciones y genera un evento para SYSLOG.

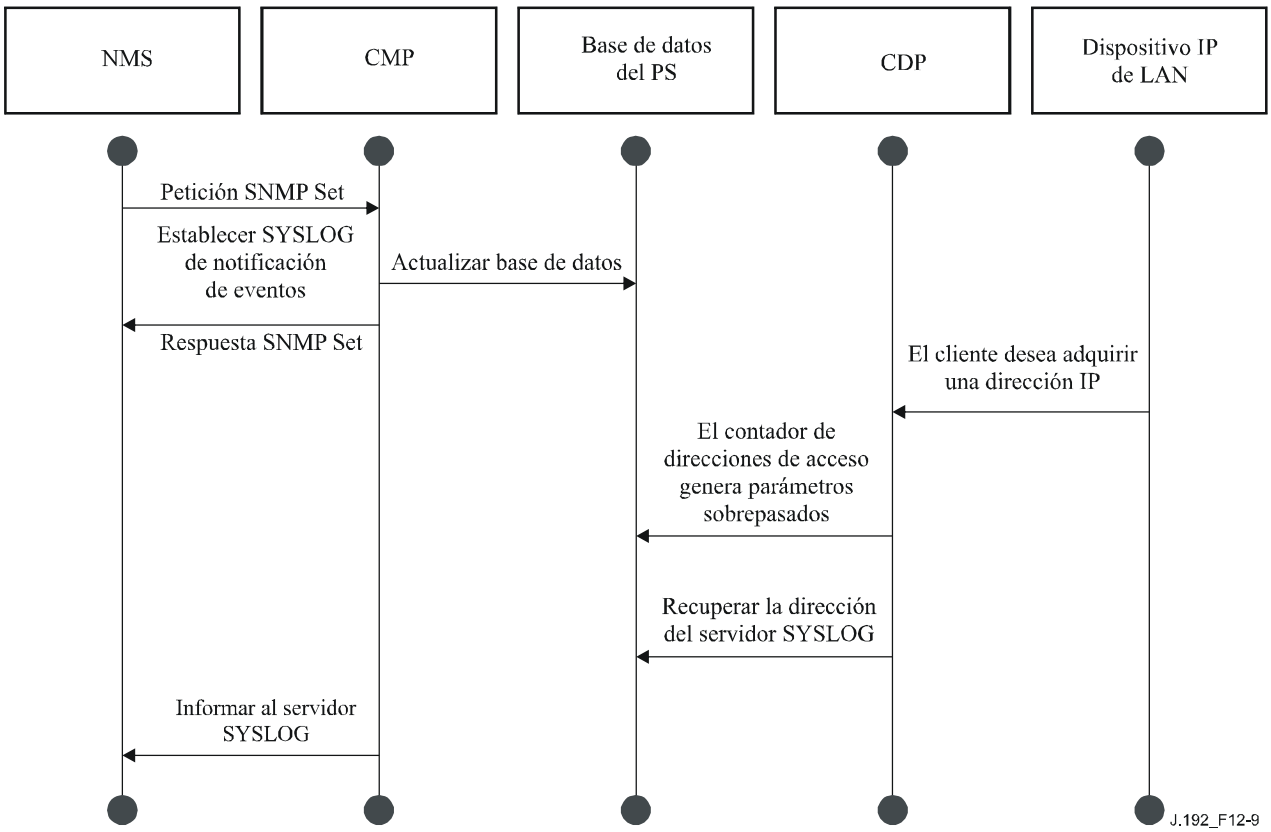


Figura 12-9/J.192 – Secuencia de adquisición de direcciones (la petición sobrepasa el contador suministrado)

12.4.2.2 Ejemplo de funcionamiento del estrangulamiento y limitación de eventos del CMP

Esta Recomendación proporciona un mecanismo de eventos de estrangulamiento a través de la funcionalidad CMP del PS. El estrangulamiento y limitación de eventos es muy flexible pudiendo incluir casos en los que todos los eventos se comuniquen y casos en los que no se comunique ningún evento al NMS. La cláusula 6.3.3.2.4.8 contiene una descripción del mecanismo de estrangulamiento y limitación de eventos del CMP.

El ejemplo de la figura 12-10 ilustra la configuración de la base de datos del PS para que devuelva eventos mediante el método SNMP INFORM. Inicialmente, se escriben varios mensajes INFORM en el fichero histórico local y se entregan al NMS. El mecanismo de estrangulamiento de eventos establece el límite del número de eventos que pueden enviarse al NMS en un determinado periodo de tiempo. Cuando se alcanza dicho límite, el PS detiene el envío de mensajes INFORM al NMS. Para reiniciar la notificación de eventos, el NMS DEBERÍA volver a habilitar la comunicación de eventos.

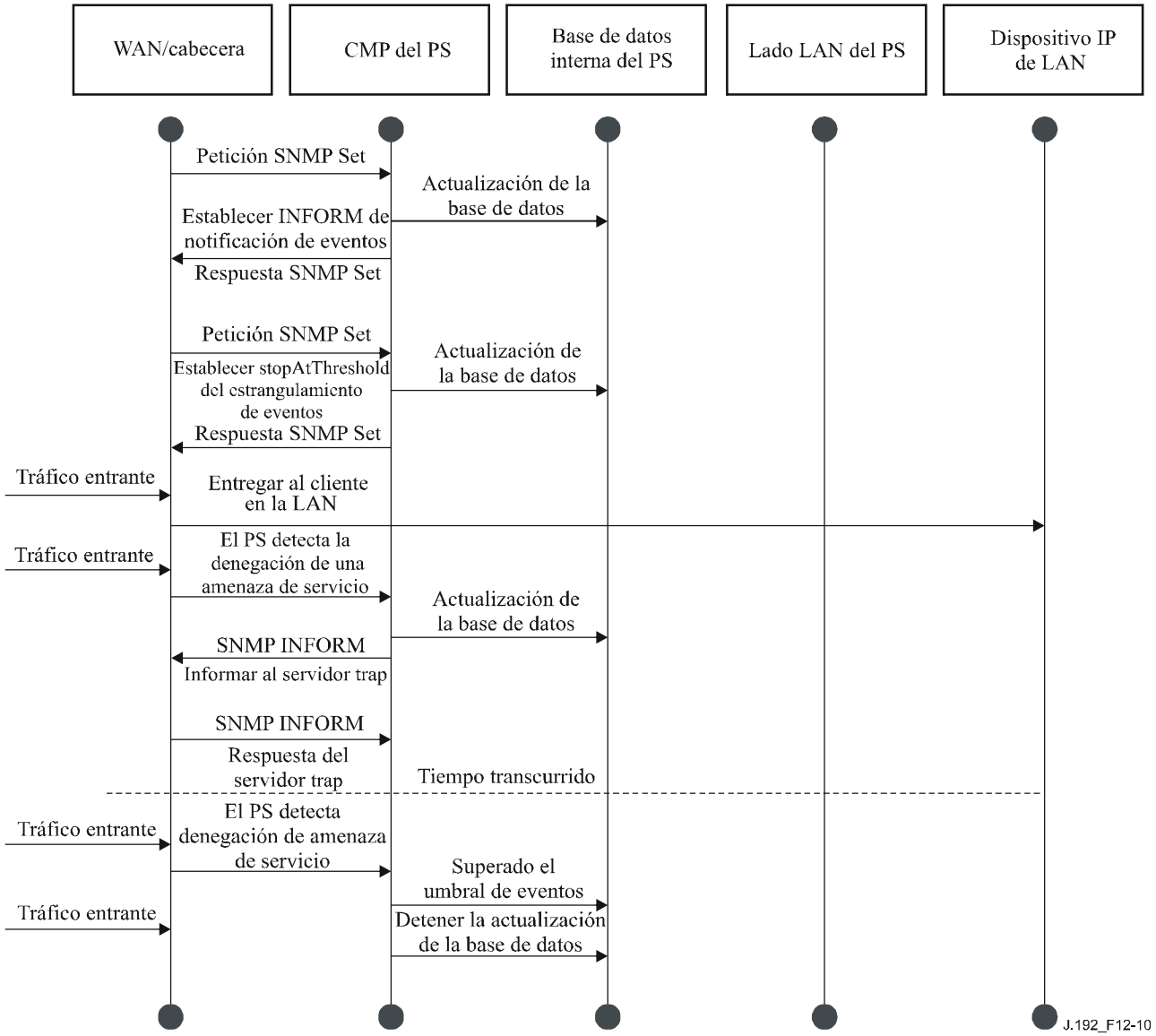


Figura 12-10/J.192 – Operación de estrangulamiento y limitación de eventos del CMP

13 Procesos de configuración

Esta cláusula describe los procesos implicados en la utilización de las herramientas de configuración, descritas en la cláusula 7. Para la configuración inicial del dispositivo IP de LAN y la configuración del elemento PS se descompone en las tres tareas siguientes:

1) adquisición de las direcciones de red;

2) adquisición de información del servidor;

3) descarga y procesamiento seguros del fichero de configuración del PS.

En esta cláusula se describen los procesos de configuración para cada uno de los siguientes casos de interés:

- WAN-Man del PS – Configuración de la funcionalidad de gestión basada en la WAN del PS.
- WAN-Data del PS – Configuración de las direcciones IP WAN-Data del PS que sirven para crear correspondencias CAT con dispositivos IP de LAN del sector de direcciones LAN-Trans.

- Dispositivo IP de LAN en el sector LAN-Trans – Configuración de un dispositivo IP de LAN con una dirección IP traducida.
- Dispositivo IP de LAN en el sector LAN-Pass – Configuración de un dispositivo IP de LAN con dirección IP que se transfiere a la WAN.

La configuración del elemento del módem de cable de un PS integrado es independiente y distinta de la configuración de IPCable2Home y ajena al objeto de la presente Recomendación. Se remite al lector a las especificaciones de CableMÓdem que describen la configuración del módem de cable.

Los elementos funcionales con los que interactúa el elemento PS durante los procesos de configuración enumerados anteriormente se identifican en la figura 13-1. El elemento funcional centro de distribución de claves (KDC) se muestra con una línea de perfil discontinua ya que se utiliza en el modo de configuración SNMP aunque no en el modo de configuración DHCP. Los demás elementos funcionales se utilizan en ambos modos de configuración.

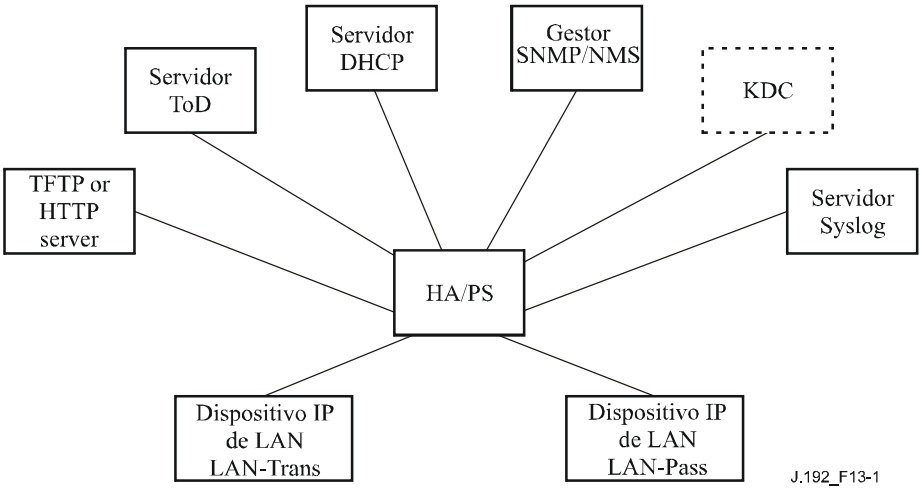


Figura 13-1/J.192 – Elementos funcionales de la configuración IPCable2Home

El servidor del protocolo de transferencia de fichero trivial (TFTP) o el servidor del protocolo de transferencia de hipertexto (HTTP) permite al PS el acceso al fichero de configuración del PS y cumple las reglas descritas en [RFC 1350]. El servidor de hora del día (ToD) proporciona al PS los medios de adquirir la hora actual en formato UTC como se explica en [RFC 868]. El protocolo dinámico de configuración de anfitrión (DHCP) proporciona al PS direcciones IP mundiales y/o privadas de acuerdo con [RFC 2131] y proporciona asimismo otra información mediante las opciones del DHCP de acuerdo con [RFC 2132]. El sistema de gestión de red (NMS) cumple con las versiones SNMPv1, SNMPv2 y SNMPv3 del protocolo simple de gestión de red (SNMP, *simple network management protocol*) como se describe en [RFC 3584]. El servidor del registro del sistema (SYSLOG, *system log*) maneja los mensajes de eventos generados por el PS y por los dispositivos IP de LAN en el hogar. El PS implementa clientes para estos servidores basados en la red de datos por cable y utiliza estas funciones de cliente durante los procesos de configuración descritos en esta cláusula para llevar a cabo las tareas enumeradas al principio de la misma.

13.1 Modos de configuración

Las cláusulas 5.5 y 7.2.1 introducen dos modos de configuración válidos soportados por el elemento de servicios de portal: el modo de configuración DHCP y el modo de configuración SNMP. El PS puede funcionar en un tercer modo, el modo CableHome aletargado, si no está configurado para funcionar en cualquiera de los dos modos de configuración válidos. En esta cláusula se presentan con mayor detalle los dos modos de configuración válidos. La figura 13-2 ilustra un posible flujo de eventos de los dos modos de configuración y del modo CableHome aletargado. El punto clave de la figura 13-2 es la disyuntiva utilizada por el PS para determinar el modo de configuración en el que operar.

El PS funciona en el modo de configuración DHCP (modo DHCP) si el servidor DHCP de la red de cable proporciona una dirección IP válida para el servidor TFTP o el servidor HTTP en el campo 'siaddr' del mensaje DHCP, proporciona un nombre de fichero válido para el fichero de configuración del PS en el campo 'file' del mensaje DHCP y NO proporciona las subopciones 3, 6 y 51 de la opción 177 del DHCP a la CDC del PS, durante la fase DHCPACK del proceso de inicialización. El modo de configuración DHCP tiene por objeto permitir que el PS funcione en una infraestructura DOCSIS 1.0 o DOCSIS 1.1, sin modificaciones a la red DOCSIS o con muy pocas modificaciones.

El modo de configuración SNMP del PS se activa cuando el servidor DHCP de la red de cable NO proporciona valores para 'siaddr' y 'file', y cuando el servidor DHCP de la red de cable SÍ envía las subopciones 3, 6 y 51 de la opción 177 del DHCP. El modo de configuración SNMP tiene por objeto permitir que el PS aproveche las características avanzadas de la infraestructura PacketCable.

Si el PS no recibe ninguno de los campos o de las subopciones definidos como activadores de los modos de configuración DHCP y SNMP, o si recibe una combinación no válida de esos campos y las opciones, pasará a funcionar por defecto en el modo CableHome aletargado. Un PS integrado como un eSAFE con un módem de cable conforme con eDOCSIS [eDOCSIS], también puede ser configurado mediante el objeto MIB esafePsCableHomeModeControl del módem de cable para funcionar en modo aletargado. Véase 7.3.3.2.4.

En las figuras 13-2 y 13-3 no se muestran todas las condiciones de error. Véase 7.2.2 para encontrar una descripción del comportamiento del PS en el caso de criterios de decisión incorrectos del modo de configuración.

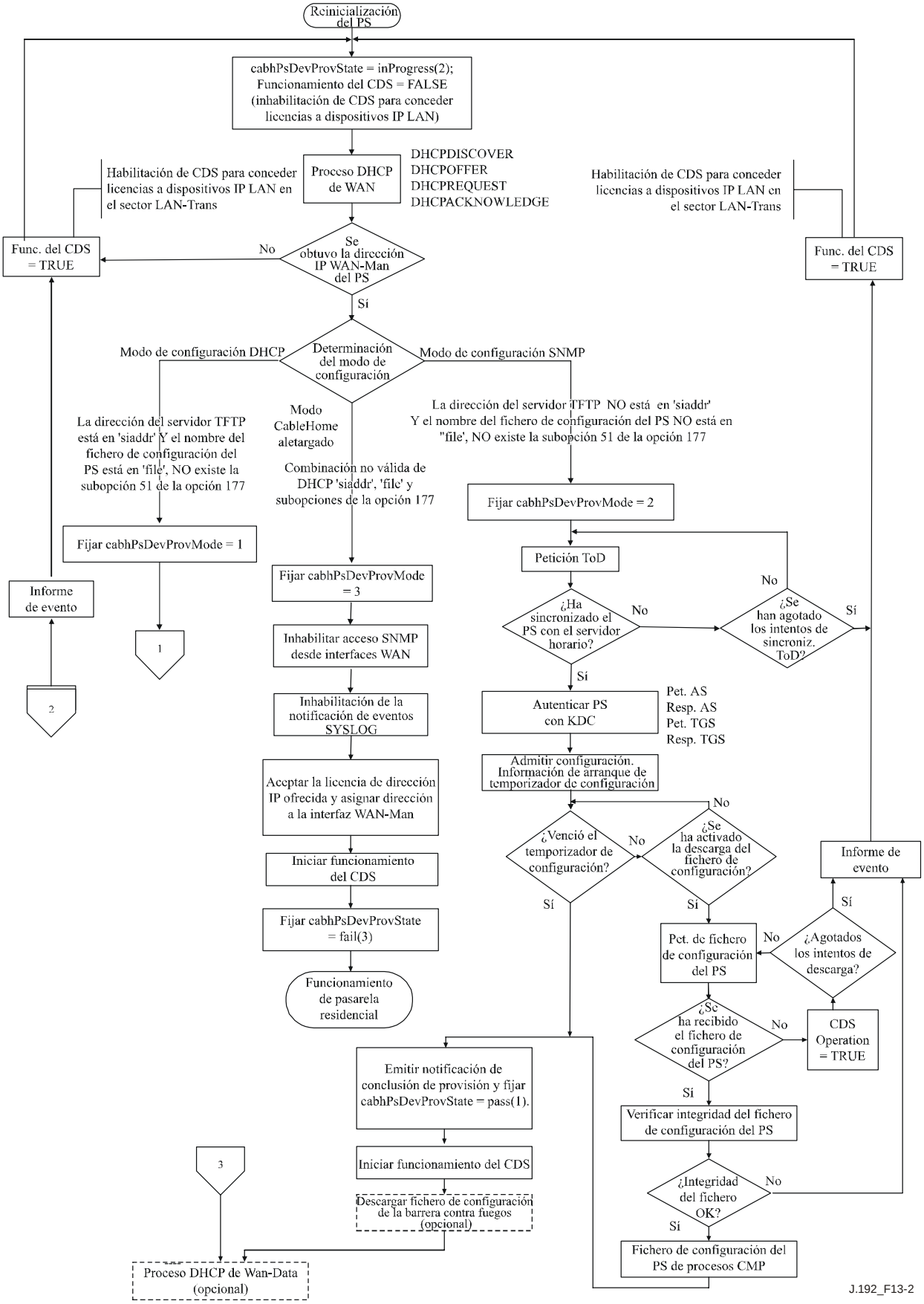


Figura 13-2/J.192 – Modos de configuración de IPCable2Home (Parte 1)

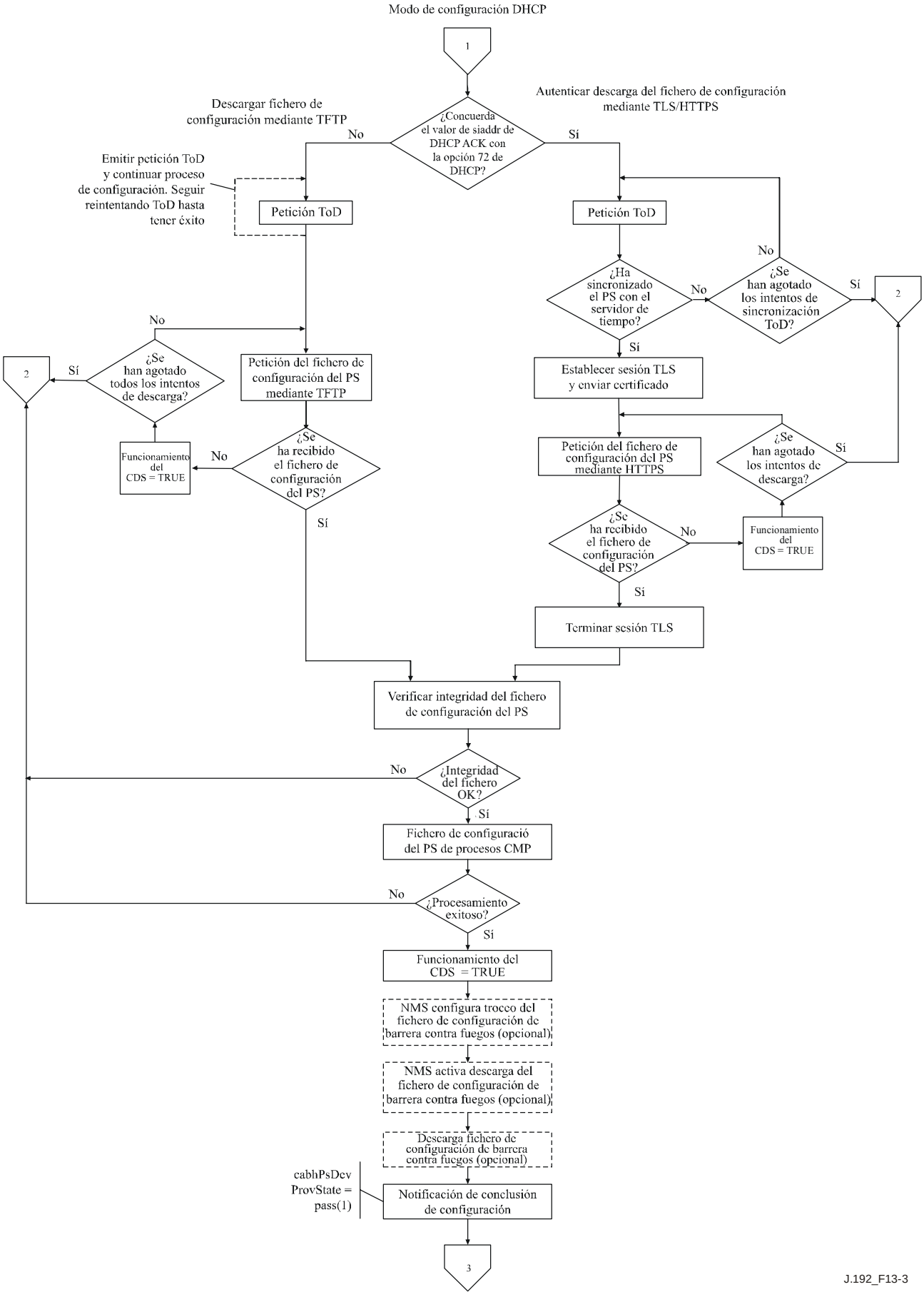


Figura 13-3/J.192 – Modos de configuración de IPCable2Home (Parte 2)

13.2 Proceso de configuración de la gestión del PS: modo de configuración DHCP

El PS solicita del sistema de configuración de la cabecera una dirección IP para el intercambio de los mensajes de gestión entre el NMS y el PS. El PS analiza el mensaje DHCP devuelto en el DHCP OFFER y toma una decisión en cuanto al modo de configuración bajo el que va a funcionar (véase 7.3.3.2.4). La cláusula 7.3.3.2.3.2 describe tres modos de direcciones WAN soportados para la adquisición de direcciones IP por parte del PS a obtener del servidor DHCP de la red de cable.

Si el PS adopta la decisión de que va a funcionar en el modo de configuración DHCP, utiliza la información del fichero de configuración del PS recibida en el mensaje DHCP como activador para descargar el fichero de configuración del PS de acuerdo con lo descrito en 7.3. La descarga del fichero de configuración del PS es un requisito para el PS cuando funciona en el modo de configuración DHCP pero es opcional para el PS cuando funciona en el modo de configuración SNMP.

En el modo de configuración DHCP el PS (CMP) utiliza por defecto el modo NmAccess para el intercambio de mensajes de gestión con el NMS, no obstante lo cual el NMS puede configurar el modo de coexistencia en el CMP. Estos modos de mensajería de gestión se describen en 6.3.3.

La figura 13-4 y el cuadro 13-1 describen la secuencia de mensajes necesaria para inicializar el funcionamiento del PS en el modo de configuración DHCP. El proceso para configurar la gestión de un PS que funciona en el modo de configuración DHCP es el mismo para el PS integrado con un módem de cable DOCSIS, que para el PS autónomo. La configuración del PS integrado NO DEBE efectuarse antes del proceso de configuración del módem de cable. La configuración de la gestión del PS autónomo DEBERÍA realizarse inmediatamente después de la puesta en marcha/reinicialización.

El proceso opcional de descarga del fichero de configuración de la barrera contra fuegos se muestra sombreado en la figura 13-4.

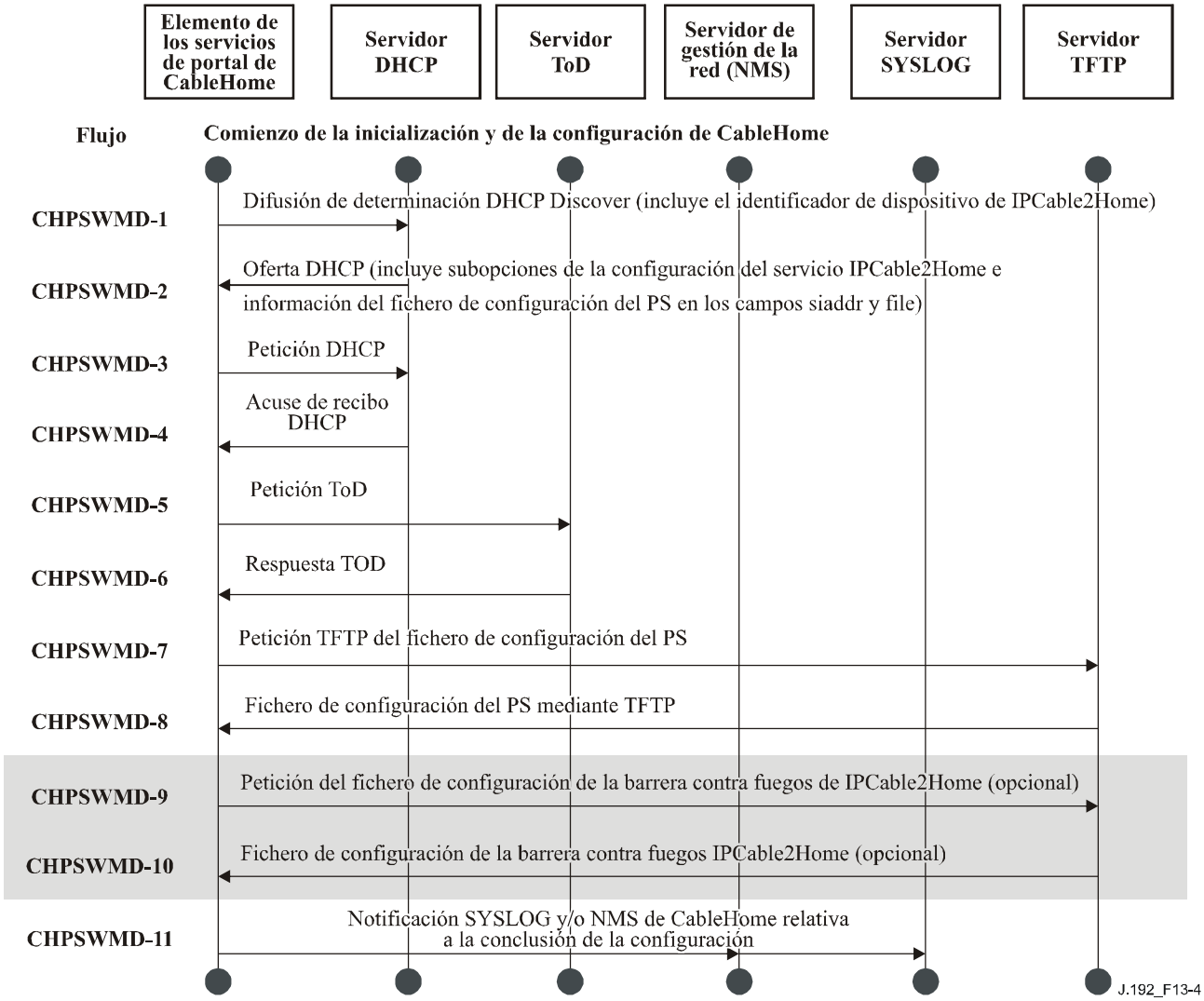


Figura 13-4/J.192 – Proceso de configuración de la gestión del PS – Modo de configuración DHCP

El cuadro 13-1 describe los mensajes CHPSWMD-1 a CHPSWMD-11 mostrados en la figura 13-4.

Cuadro 13-1/J.192 – Descripción de los flujos para los procesos de configuración WAN-Man del PS en el modo de configuración DHCP

Fase	Configuración WAN-Man del PS: modo de configuración DHCP	Secuencia normal	Secuencia de fallo
CHPSWMD-1	Difusión de determinación DHCP (DHCP Broadcast Discover) El CDP (CDC) envía un mensaje DHCP DISCOVER en modo difusión a fin de obtener la dirección IP de WAN-Man como se describe en 7.3.3.2.4. Dicho mensaje incluye opciones obligatorias relacionadas en el cuadro 7-10, Opciones DHCP del CDC, en los mensajes DISCOVER y REQUEST. Cuando el CDC difunde un mensaje DHCP DISCOVER, el PS fija cabhPsDevProvState a estado 'inProgress' (2).	Comenzar la secuencia de configuración.	Si falla el protocolo DHCP, comunicar un error y continuar reintentando mensajes DHCP Broadcast Discover hasta tener éxito (volver a la fase CHPSWMD-1). Si fracasa el primer intento para obtener una dirección IP de WAN-Man, el PS inicia el funcionamiento del CDS como se describe en 7.3.3.2.4.
CHPSWMD-2	OFERTA DHCP (DHCP OFFER)	CHPSWMD-2 DEBE tener lugar una vez completada CHPSWMD-1.	Si falla el protocolo DHCP volver a CHPSWMD-1 y comunicar el error.
CHPSWMD-3	PETICIÓN DHCP (DHCP REQUEST) El CDP DEBE enviar al servidor DHCP adecuado un mensaje DHCP REQUEST para aceptar el DHCP OFFER.	CHPSWMD-3 DEBE tener lugar una vez completada CHPSWMD-2.	Si falla el protocolo DHCP volver a CHPSWMD-1 y comunicar el error.
CHPSWMD-4	Acuse de recibo DHCP (DHCP ACK) El servidor DHCP envía al CDP un mensaje DHCP ACK que contiene una dirección IPv4 del PS. El PS modifica cabhPsDevProvMode basándose en la información que recibe en el mensaje DHCP ACK (véase 7.3.3.2.4). El PS almacena la dirección del servidor de hora del día en cabhPsDevTimeServerAddr. El PS modifica cabhPsDevProvMode basándose en la información que recibe en el mensaje DHCP ACK (véase 7.3.3.2.4).	CHPSWMD-4 DEBE tener lugar una vez completada CHPSWMD-3.	Si falla el protocolo DHCP volver a CHPSWMD-1 y comunicar el error.
CHPSWMD-5	Petición de hora del día (ToD) conforme a [RFC 868] El PS emite una petición ToD al servidor de tiempos identificado en la opción 4 del mensaje DHCP ACK.	CHPSWMD-5 DEBE tener lugar una vez completada CHPSWMD-4.	Continuar en CHPSWMD-6.

Cuadro 13-1/J.192 – Descripción de los flujos para los procesos de configuración WAN-Man del PS en el modo de configuración DHCP

Fase	Configuración WAN-Man del PS: modo de configuración DHCP	Secuencia normal	Secuencia de fallo
CHPSWMD-6	Respuesta ToD El servidor ToD debe responder la hora actual en formato UTC.	CHPSWMD-6 DEBE tener lugar una vez completada CHPSWMD-5.	Intentar la sincronización con el siguiente servidor de hora del día enumerado en la opción 4 DHCP del mensaje DHCP ACK. Si se ha intentado sin éxito la sincronización con cada uno de los servidores ToD como parte del intento inicial de sincronizar la hora, fijar cabhPsDevTodSyncStatus = false(2), intentar adquirir la hora del sistema del módem de cable (sólo para PS integrado), actualizar cabhPsDevDateTime, actualizar la hora de las licencias CDS y continuar con CHPSWMD-7. Para más información, véase 7.5.4.
CHPSWMD-7	Petición TFTP El PS funcionando en el modo de configuración DHCP envía al servidor TFTP una petición TFTP Get solicitando el fichero de datos de configuración especificado descrito en 7.4.4.	CHPSWMD-7 DEBE tener lugar una vez completada CHPSWMD-5. CHPSWMD-7 PUEDE tener lugar antes de completar CHPSWMD-6.	Continuar en CHPSWMD-8.
CHPSWMD-8	El servidor TFTP envía el fichero de configuración del PS. Cuando se recibe el fichero de configuración del PS, se verifica el troceo. Véase 7.4.4.1. A continuación se procesa dicho fichero. En relación con el contenido del fichero de configuración del PS véase 7.4.4. Facultativamente, se incluyen la dirección IP del servidor TFTP del fichero de configuración de la barrera contra fuegos, el nombre de dicho fichero y el troceo del fichero de configuración del PS, en caso de que haya un fichero de configuración de la barrera contra fuegos que tenga que cargarse, y éste sea el método seleccionado para especificarlo.	CHPSWMD-8 DEBE tener lugar una vez completada CHPSWMD-7.	Si falla la descarga TFTP, tomar una acción en función del error descrito en 7.4.4.4.

Cuadro 13-1/J.192 – Descripción de los flujos para los procesos de configuración WAN-Man del PS en el modo de configuración DHCP

Fase	Configuración WAN-Man del PS: modo de configuración DHCP	Secuencia normal	Secuencia de fallo
CHPSWMD-9	Petición TFTP – fichero de configuración de la barrera contra fuegos (opcional) Si el PS recibe información del fichero de configuración de la barrera contra fuegos (servidor TFTP de la barrera contra fuegos y nombre del fichero de configuración de la barrera contra fuegos) en el fichero de configuración del PS, el PS envía al servidor TFTP de configuración de la barrera contra fuegos una petición TFTP Get solicitando un fichero de configuración de la barrera contra fuegos (véase 11.6.4.2). Si el PS no recibe información del fichero de configuración de la barrera contra fuegos en el fichero de configuración del PS, el proceso de configuración del PS (en el modo de configuración DHCP) DEBE saltarse las fases CHPSWMD-9 y CHPSWMD-10 y continuar en la fase CHPSWMD-11.	Si CHPSWMD-9 tiene lugar, DEBE hacerlo una vez completada CHPSWMD-8.	Si falla el TFTP, continuar el funcionamiento del PS pero comunicar un error y continuar reintentado CHPSWMD-9.
CHPSWMD-10	El servidor TFTP envía el fichero de configuración de la barrera contra fuegos (opcional) Si tiene lugar la fase CHPSWMD-9, el servidor TFTP envía al PS una respuesta TFTP con el fichero solicitado. Tras la recepción del fichero de configuración de la barrera contra fuegos se calcula el troceo del fichero de configuración y se compara con el valor recibido en el fichero de configuración del PS. A continuación se procesa el fichero. Véase 11.6.4.	CHPSWMD-10 DEBE tener lugar una vez completada CHPSWMD-9.	Si falla el TFTP continuar con el funcionamiento del PS pero comunicar un error y continuar reintentando CHPSWMD-9. Si el proceso del fichero de configuración de la barrera contra fuegos provoca un error, continuar y comunicar el error como evento.

Cuadro 13-1/J.192 – Descripción de los flujos para los procesos de configuración WAN-Man del PS en el modo de configuración DHCP

Fase	Configuración WAN-Man del PS: modo de configuración DHCP	Secuencia normal	Secuencia de fallo
CHPSWMD-11	Configuración completada Si lo solicita el sistema de configuración, se requiere al PS que informe al mismo del estado de configuración del PS. El sistema de configuración podría solicitar al PS que enviase un mensaje SYSLOG, una trampa SNMP, o ambos. Si el PS completa con éxito todas las fases requeridas desde CHPSWMD-1 hasta CHPSWMD-10 y ha recibido una dirección de servidor SYSLOG en el DHCP OFFER, el PS DEBE enviar un mensaje de configuración completa al servidor SYSLOG con el estado de configuración fijo en PASS. Si el PS completa con éxito todas las fases de configuración desde CHPSWMD-1 a CHPSWMD-10 y ha recibido parámetros válidos del receptor de notificaciones, DEBE enviar una notificación de configuración completa (cabhPsDevInitTrap) con los parámetros adecuados al receptor de notificaciones. El PS DEBE actualizar el valor de cabhPsDevProvState con el estado 'pass' (1) cuando las fases de la configuración CHPSWMD-1 a CHPSWMD-11 se completen con éxito.	CHPSWMD-11 DEBE tener lugar una vez completada CHPSWMD-10.	Si falla la trampa SNMP, el servidor de configuración puede desconocer que ha concluido el proceso de configuración salvo que consulte el objeto cabhPsProvState.

13.3 Proceso para configurar el PS para efectos de gestión: modo de configuración DHCP con HTTP/TLS

El PS solicita una dirección IP del sistema de configuración de la cabecera que se utilizará para el intercambio de mensajes de gestión entre el NMS y el PS. El PS examina el mensaje DHCP devuelto en el mensaje OFFER DHCP y toma la determinación relativa al modo de configuración en el que habrá de funcionar (véase 7.3.3.2.4). En la cláusula 7.3.3.2.3.2 se describen tres modos de direccionamiento de red WAN aceptados por el PS para la obtención de direcciones IP desde el servidor DHCP en la red de cable.

Si el PS decide que habrá de funcionar en el modo de configuración DHCP, en ese caso utilizará la información del fichero de configuración del PS transferido en el mensaje DHCP, como un activador para descargar el fichero de configuración del PS. Si está presente la opción código 72 de DHCP en el mensaje DHCP ACK, y si su contenido concuerda con la dirección IP en el campo siaddr, la descarga se lleva a cabo utilizando HTTP por TLS, como se describe en 11.9.

En el modo de configuración DHCP, el PS (CMP) utiliza por defecto el modo NmAccessTable para el intercambio de mensajes de gestión con el NMS, aunque el NMS puede configurar facultativamente el CMP para el modo de coexistencia. Estos modos de mensajería de gestión se describen en 6.3.3.

En la figura 13-5 y en el cuadro 13-2 se describe la secuencia de los mensajes necesarios para inicializar un PS que funciona en el modo de configuración DHCP con HTTP/TLS. El proceso de configuración y gestión del PS que funciona en ese modo es el mismo para el PS integrado con un módem de cable DOCSIS que para el del PS autónomo. La configuración del PS integrado NO DEBE ocurrir antes del proceso de configuración del módem de cable. La configuración de la gestión del PS autónomo debería ocurrir inmediatamente después de la puesta en marcha/reinicialización.

En la figura 13-5 se muestra sombreado el proceso facultativo de descarga de un fichero de configuración de la barrera contra fuegos.

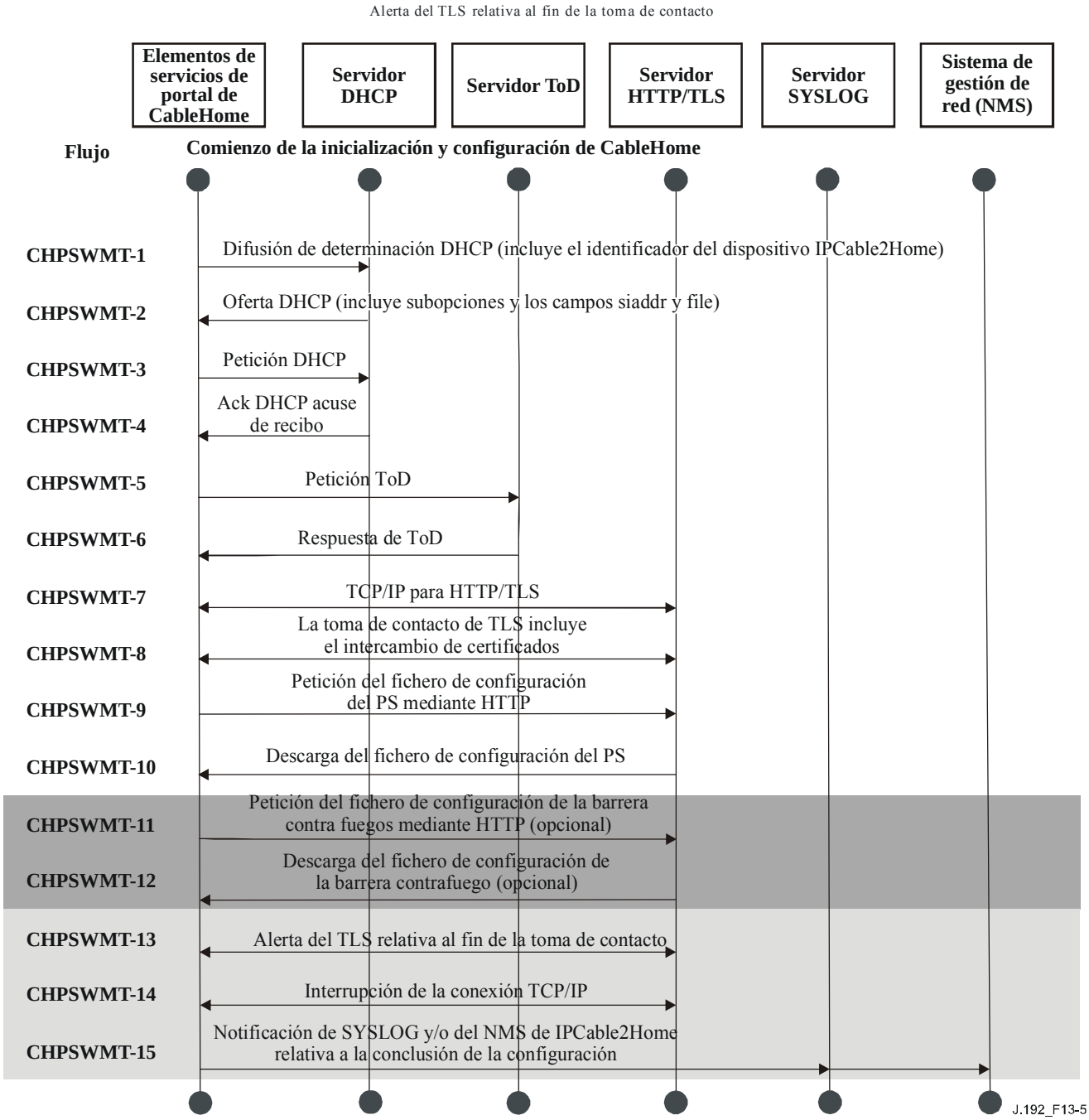


Figura 13-5/J.192 – Modo de configuración DHCP del proceso de configuración utilizando HTTP/TLS

En el cuadro 13-2 se describen los mensajes individuales CHPSWMT-1 – CHPSWMT-15 indicados en la figura 13-5. Si se requiere mayor información, véase 11.9, Seguridad del fichero de configuración del PS en el modo de configuración DHCP.

Cuadro 13-2/J.192 – Descripción de los flujos en modo de configuración DHCP utilizando HTTP/TLS

Fase del flujo	Configuración de la WAN-Man del PS: modo de configuración DHCP	Secuencia normal	Secuencia de fallo
CHPSWMT-1	Difusión de determinación DHCP (DHCP Broadcast Discover) El CDP (CDC) envía un mensaje DHCP DISCOVER en modo difusión a fin de obtener la dirección IP de WAN-Man, como se describe en 7.3.3.2.4. Esta difusión incluye las opciones obligatorias relacionadas en el cuadro 7-10, opciones DHCP del CDC, en los mensajes DISCOVER y REQUEST. Cuando el CDC difunde un mensaje DHCP DISCOVER, el PS fija cabhPsDevProvState al estado 'in Progress' (2).	Comienzo de la secuencia de configuración.	Si falla el protocolo DHCP, notificar el error y continuar reintentando la difusión de la determinación DHCP hasta tener éxito (volver a la fase CHPSWMT-1) Si ha fallado durante el primer intento para tratar de obtener una dirección IP de WAN-Man, el PS inicia el funcionamiento del CDS como se describe en 7.3.3.2.4.
CHPSWMT-2	OFERTA DHCP (DHCP OFFER)	CHPSWMT-2 DEBE tener lugar una vez completada CHPSWMT-1.	Si falla el protocolo DHCP, volver a CHPSWMT-1 y notificar el error.
CHPSWMT-3	PETICIÓN DHCP (DHCP REQUEST) El CDP envía un mensaje REQUEST DHCP al servidor DHCP apropiado para aceptar la OFFER DHCP.	CHPSWMT-3 DEBE tener lugar una vez completada CHPSWMT-2.	Si falla el protocolo DHCP, volver a CHPSWMT-1 y notificar el error.
CHPSWMT-4	ACUSE DE RECIBO DHCP (DHCP ACK) El servidor DHCP envía un mensaje DHCP ACK al CDP con la dirección IPv4 del PS. El PS almacena la dirección del servidor de hora del día en cabhPsDevTimeServerAddr. Si la dirección IP en el campo siaddr del mensaje DHCP ACK concuerda con la primera dirección IP en la opción 72, el PS inicia una sesión TLS y descarga el fichero de configuración del servidor HTTP. El PS modifica cabhPsDevProvMode basándose en la información recibida en el mensaje DHCP ACK. Véase 11.9, Seguridad del fichero de configuración del PS en el modo de configuración DHCP.	CHPSWMT-4 DEBE tener lugar una vez completada CHPSWMT-3.	Si falla el protocolo DHCP, volver a CHPSWMT-1 y notificar el error.

Cuadro 13-2/J.192 – Descripción de los flujos en modo de configuración DHCP utilizando HTTP/TLS

Fase del flujo	Configuración de la WAN-Man del PS: modo de configuración DHCP	Secuencia normal	Secuencia de fallo
CHPSWMT-5	Petición de hora del día (ToD) conforme a [RFC 868] El PS sincroniza su hora con el servidor de tiempo seleccionado a partir de la opción 4 de DHCP (opción de servidor de tiempo) en el mensaje ACK DHCP. Véase 7.5.4, Requisitos de la función cliente de hora del día.	CHPSWMT-5 DEBE tener lugar una vez completada CHPSWMT-4.	Continuar con CHPSWMT-6.
CHPSWMT-6	Respuesta TOD Se prevé que el servidor de ToD contestará con la hora actual en formato UTC.	CHPSWMT-6 DEBE tener lugar una vez completada CHPSWMT-5.	Intentar la sincronización con el siguiente servidor horario (ToD) enumerado en la opción 4 del mensaje DHCP ACK. Si se ha realizado un intento de sincronización fallido con cada uno de los servidores ToD como parte del intento inicial de sincronizar la hora del día, fijar cabhPsDevTodSyncStatus = false(2), actualizar cabhPsDevDateTime, actualizar las horas en que se dieron las licencias y continuar con CHPSWMT-7. Para información adicional véase 7.5.4.
CHPSWMT-7	Establecimiento de TCP/IP El PS que funciona en el modo de configuración DHCP establece una sesión TCP/IP para intercambiar mensajes de HTTP con el servidor HTTP en el sistema de configuración del operador de cable.	CHPSWMT-7 DEBE tener lugar una vez completada CHPSWMT-5. CHPSWMT-7 PUEDE tener lugar antes de completar CHPSWMT-6.	Si falla TCP/IP, reintentar conforme a la especificación. Si fallan todos los reintentos, volver a CHPSWMT-1 y notificar el error.
CHPSWMT-8	Toma de contacto de TLS El PS que funciona en el modo de configuración DHCP establece una sesión TLS con el servidor HTTPS.	CHPSWMT-8 DEBE tener lugar una vez completada CHPSWMT-7.	Si falla TLS, reintentar conforme a la especificación. Si fallan todos los reintentos, volver a CHPSWMT-1 y notificar el error.
CHPSWMT-9	Petición del fichero de configuración mediante HTTP El PS que funciona en el modo de configuración DHCP solicita el fichero de configuración del servidor HTTP.	CHPSWMT-9 DEBE tener lugar una vez completada CHPSWMT-8.	Si falla HTTP, reintentar conforme a la especificación. Si fallan todos los reintentos, volver a CHPSWMT-1 y notificar el error.

Cuadro 13-2/J.192 – Descripción de los flujos en modo de configuración DHCP utilizando HTTP/TLS

Fase del flujo	Configuración de la WAN-Man del PS: modo de configuración DHCP	Secuencia normal	Secuencia de fallo
CHPSWMT-10	El servidor HTTPS envía el fichero de configuración del PS El fichero se procesa. Véase 7.4.4 por lo que se refiere al contenido del fichero de configuración del PS. Facultativamente, se incluyen la dirección IP del servidor HTTP del fichero de configuración de la barrera contra fuegos y el nombre de ese fichero en el fichero de configuración del PS.	CHPSWMT-10 DEBE tener lugar una vez completada CHPSWMT-9.	Si falla la descarga de HTTP, notificar el error y volver a CHPSWMT- 9 (continuar reintentando la descarga del fichero de configuración del PS). Si el procesamiento del fichero de configuración del PS produce un error, continuar con CHPSWMT-13 y notificar el error como un evento.
CHPSWMT-11	Petición HTTP – Fichero de configuración de la barrera contra fuegos (opcional) Si el PS recibe información del fichero de configuración de la barrera contra fuegos (servidor TFTP y nombre del fichero de configuración de la barrera contra fuegos) en el fichero de configuración del PS, éste solicita el fichero de configuración de la barrera contra fuegos del servidor HTTP. Si el PS no recibe dicha información, el proceso de configuración del PS (modo de configuración DHCP) DEBE saltarse las fases CHPSWMT-11 y CHPSWMT-12 y continuar con la fase CHPSWMT-13.	Si CHPSWMT-11 tiene lugar, DEBE suceder una vez completada CHPSWMT-10.	Si falla HTTP, continuar con el funcionamiento del PS pero notificar el error y continuar reintentando CHPSWMT-13.
CHPSWMT-12	El servidor HTTP envía el fichero de configuración de la barrera contra fuegos (opcional) Si tiene lugar la fase CHPSWMT-11, el servidor HTTP envía una respuesta HTTP al PS incluyendo el fichero de configuración de la barrera contra fuegos solicitado.	CHPSWMT-12 DEBE tener lugar una vez completada CHPSWMT-11.	Si falla HTTP, continuar con el funcionamiento del PS pero notificar el error y continuar reintentando CHPSWMT-11. Si el procesamiento del fichero de configuración de la barrera contra fuegos produce un error, continuar y notificar el error como un evento.
CHPSWMT-13	Alerta del TLS relativa al fin de la toma de contacto El PS desconecta la sesión de TLS justo antes de enviar el mensaje de conclusión de la configuración.	CHPSWMT-13 DEBE tener lugar una vez completada CHPSWMT-12.	Continuar en la fase CHPSWMT-14. Si falla por causa de HTTP, reintentar conforme a la especificación. Si fallan todos los reintentos notificar el error.

Cuadro 13-2/J.192 – Descripción de los flujos en modo de configuración DHCP utilizando HTTP/TLS

Fase del flujo	Configuración de la WAN-Man del PS: modo de configuración DHCP	Secuencia normal	Secuencia de fallo
CHPSWMT-14	Desconexión de TCP/IP Se suprime la sesión TCP/IP entre el PS y el servidor HTTP.	CHPSWMT-14 DEBE tener lugar una vez completada CHPSWMT-13.	Si falla la interrupción de TCP/IP, notificar el error. Continuar en la fase 15.
CHPSWMT-15	Conclusión de la configuración Si lo solicita el sistema de configuración el PS debe informarle sobre el estado de la configuración del PS. El sistema de configuración podría solicitar al PS que envíe un mensaje SYSLOG o una trampa SNMP, o ambos. Si el PS completa con éxito todas las etapas requeridas de CHPSWMT-1 a CHPSWMT-14 y recibe la dirección del servidor SYSLOG en el mensaje DHCP OFFER, DEBE enviar un mensaje de conclusión de configuración al servidor SYSLOG con el estado de la configuración fijado a PASS. Si el PS completa con éxito todas las fases de configuración necesarias de CHPSWMT-1 a CHPSWMT-12 y ha recibido los parámetros válidos para docsDevNmAccessGroup identificando el receptor de trampas (docsDevNmAccessIP) y configurando la trampa de conclusión de configuración (cabhPsDevInitTrap) para 'leer únicamente con trampas' (fijar el control docsDevNmAccess a '4'. Véase [RFC 2669]), el PS DEBE enviar una trampa de conclusión de configuración (cabhPsDevInitTrap) con los parámetros adecuados al receptor de trampas.	CHPSWMT-15 DEBE tener lugar una vez completada CHPSWMT-14.	Si falla la trampa SNMP, es posible que el servidor de configuración no sepa que se completó el proceso de configuración a menos que interrogue al objeto cabhPsDevProvState.

Cuadro 13-2/J.192 – Descripción de los flujos en modo de configuración DHCP utilizando HTTP/TLS

Fase del flujo	Configuración de la WAN-Man del PS: modo de configuración DHCP	Secuencia normal	Secuencia de fallo
	Si expira el temporizador de configuración del PS antes de que se completen todas las fases necesarias de CHPSWMT-1 a CHPSWMT-14 y el PS ha recibido una dirección del servidor SYSLOG en el mensaje DHCP OFFER, el PS DEBE enviar un mensaje de conclusión de configuración al servidor SYSLOG con el estado de configuración fijado a FALLO (FAIL). Si el temporizador de configuración del PS expira antes de que se completen todas las fases necesarias de CHPSWMT-1 a CHPSWMT-14 y el PS ha recibido parámetros válidos para docsDevNmAccessGroup identificando el receptor de trampas (docsDevNmAccessIP) y configurando la trampa de conclusión de configuración (cabhPsDevInitTrap) para 'leer únicamente con trampas' (fijar el control docsDevNmAccess a '4'. Véase [RFC 2669]), el PS DEBE enviar una trampa de fallo de configuración (cabhPsDevInitRetryTrap) al receptor de trampas. El PS actualiza el valor de cabhPsDevProvState al estado 'pass' (1) cuando se completan satisfactoriamente las fases del flujo de configuración CHPSWMT-1 a CHPSWMT-14. Véase 7.5.4.		

13.4 Configuración de la gestión del PS: Modo de configuración SNMP

El PS solicita una dirección de red WAN-Man del servidor DHCP de cabecera para el intercambio de los mensajes de gestión entre las funciones de gestión del PS y el NMS de la red de cable. Si, en base el procedimiento descrito en 7.3.3.2.4, el PS determina que ha de operar en el modo de configuración SNMP, el PS asegura sus mensajes de gestión mediante SNMPv3, ciñéndose al procedimiento de autenticación descrito en 11.3.2.

El NMS de la red de cable puede opcionalmente encargar al PS (CMP) funcionando en el modo de configuración SNMP que descargue un fichero de configuración del PS del servidor TFTP. La notificación de la terminación del proceso de configuración se efectúa mediante el proceso de comunicación de eventos descrito en 6.3.3.2. El PS funcionará sin un fichero de configuración del PS si no recibe una activación para descargarlo.

En la figura 13-6 se ilustran los flujos de mensajes que han de utilizarse para la configuración del PS cuando funciona en el modo de configuración SNMP. El proceso de configuración de la interfaz de WAN-Man del PS es el mismo para el PS integrado que para el PS autónomo. La configuración del PS autónomo DEBERÍA tener lugar inmediatamente después de la puesta en marcha/reinicialización.

El proceso de configuración para la interfaz WAN-Man de un PS que funciona en el modo de configuración SNMP DEBE tener lugar de acuerdo con la secuencia descrita en la figura 13-6 y definida en detalle en el cuadro 13-3. Los pasos opcionales se muestran sombreados en la figura 13-6. Estos pasos opcionales pueden tener lugar inmediatamente después de la fase CHPSWMS-13 con posterioridad a ésta o no tener lugar en absoluto.

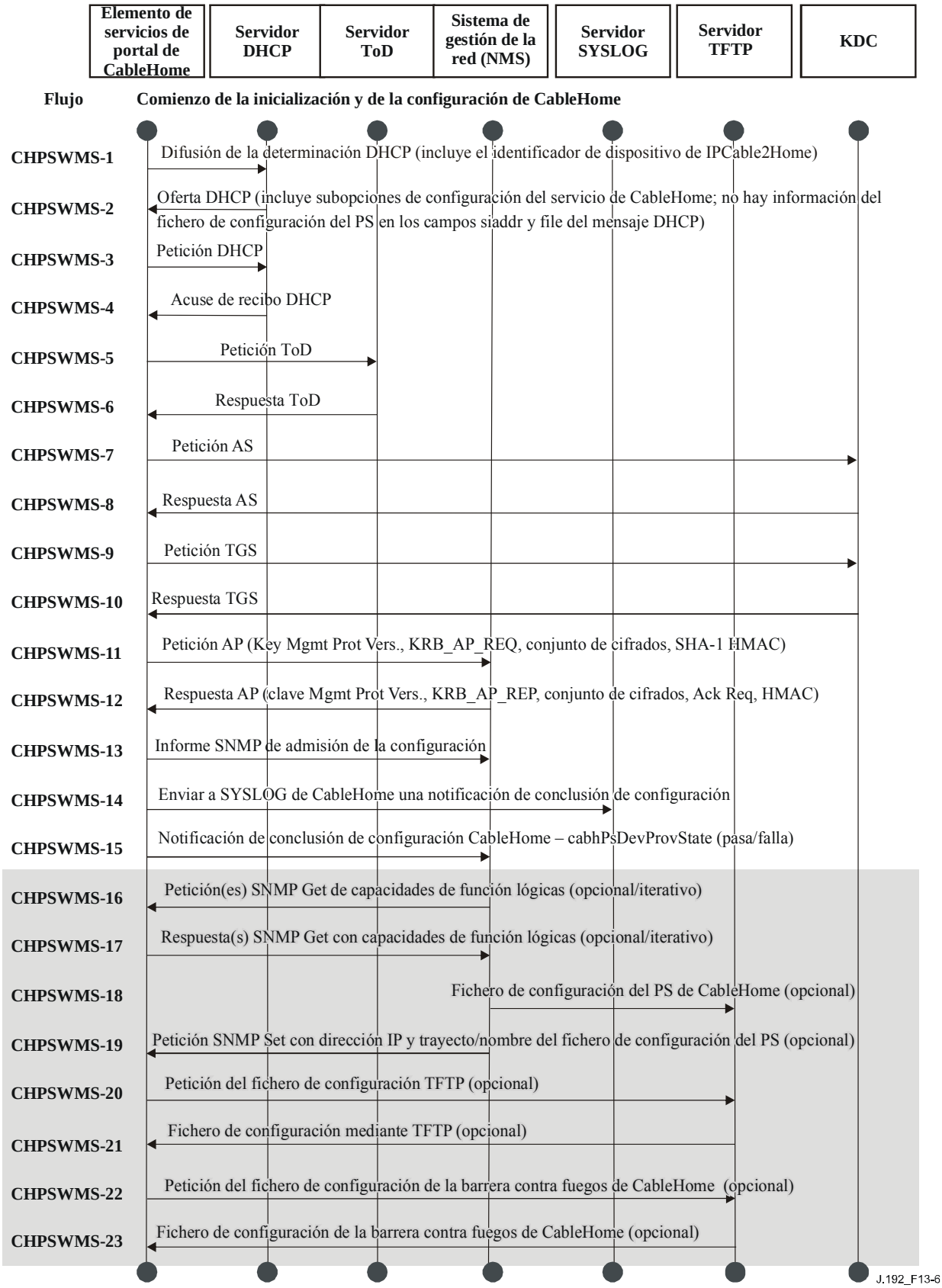


Figura 13-6/J.192 – Proceso de configuración de la gestión del PS – Modo de configuración SNMP

El cuadro 13-3 describe las fases particulares del proceso de configuración ilustrado en la figura 13-6.

Cuadro 13-3/J.192 – Descripción de los flujos del proceso de configuración WAN-Man del PS en el modo de configuración SNMP

Fase del flujo	Configuración WAN-Man del PS: modo de configuración SNMP	Secuencia normal	Secuencia de fallo
CHPSWMS-1	Difusión de determinación DHCP (DHCP Broadcast Discover) El CDP (CDC) envía un mensaje DHCP DISCOVER en modo difusión para obtener la dirección IP de WAN-Man como se describe en 7.3.3.2.4, Requisitos del CDC. Esta difusión incluye las opciones obligatorias relacionadas en el cuadro 7-10, Opciones DHCP del CDC en los mensajes DISCOVER y REQUEST. El PS inicia la supervisión del tiempo transcurrido Y fija cabhPsDevProvState al estado 'inProgress' (2) cuando el CDC difunde su mensaje inicial DHCP DISCOVER.	Comenzar la secuencia de configuración.	Si falla del protocolo DHCP, comunicar un error y continuar reintentando el mensaje de difusión de determinación DHCP hasta tener éxito (volver a CHPSWMS-1). Si falla el primer intento para obtener una licencia de dirección del servidor DHCP del operador de cable, iniciar el funcionamiento del CDS como se describe en 7.3.3.2.4, Requisitos del CDC.
CHPSWMS-2	OFERTA DHCP (DHCP OFFER)	CHPSWMS-2 DEBE tener lugar tras completarse CHPSWMS-1.	Si falla el protocolo DHCP, volver a CHPSWMS-1 y comunicar un error.
CHPSWMS-3	PETICIÓN DHCP (DHCP REQUEST) El CDP envía al servidor DHCP adecuado un mensaje DHCP REQUEST para aceptar el DHCP OFFER.	CHPSWMS-3 DEBE tener lugar tras completarse CHPSWMS-2.	Si falla el protocolo DHCP, volver a CHPSWMS-1.
CHPSWMS-4	ACUSE DE RECIBO DHCP (DHCP ACK) El servidor DHCP envía un mensaje DHCP ACK al CDC que incluye la dirección IPv4 de la interfaz WAN-Man del PS que se supone que contiene la opción código 122 de IPCable2Home, con las subopciones 3, 6 y 10 Y ninguna información del fichero de configuración del PS en los campos siaddr y file del mensaje DHCP. El PS modifica cabhPsDevProvMode basándose en la información recibida en el mensaje DHCP ACK (véase 7.3.3.2.4). El PS almacena la dirección del servidor de hora del día en cabhPsDevTimeServerAddr.	CHPSWMS-4 DEBE tener lugar tras completarse CHPSWMS-3.	Si falla el protocolo DHCP, volver a CHPSWMS-1 y comunicar un error.

Cuadro 13-3/J.192 – Descripción de los flujos del proceso de configuración WAN-Man del PS en el modo de configuración SNMP

Fase del flujo	Configuración WAN-Man del PS: modo de configuración SNMP	Secuencia normal	Secuencia de fallo
CHPSWMS-5	Petición de la hora del día (ToD) con arreglo a [RFC 868] El PS envía un mensaje de petición de ToD al servidor de tiempo identificado en la opción 4 de DHCP del mensaje DHCP ACK.	CHPSWMS-5 DEBE tener lugar tras completarse CHPSWMS-4.	Continuar en CHPSWMS-6.
CHPSWMS-6	Respuesta ToD El servidor ToD debe contestar con la hora actual en formato UTC.	CHPSWMS-6 DEBE tener lugar tras completarse CHPSWMS-5.	Reintentar la sincronización del servidor horario hasta cuatro ocasiones; si no lo consigue en cuatro intentos, intentar la sincronización con el siguiente servidor horario enumerado en la opción 4 de DHCP ACK; si tras cuatro intentos no con cada servidor horario tiene éxito, comunicar el error y volver a CHPSWMS-1.
CHPSWMS-7	Petición AS (nota 1) El PS envía el mensaje petición AS al KDC de IPCable2Home del MSO suministrado en la subopción 10 de la opción 122 de DHCP, para solicitar un tique Kerberos.	CHPSWMS-7 DEBE tener lugar tras completarse CHPSWMS-6.	Volver a CHPSWMS-1. El PS inicia el funcionamiento del CDS.
CHPSWMS-8	Respuesta AS El mensaje respuesta AS se recibe procedente del KDC de IPCable2Home de MSO con el tique Kerberos.	CHPSWMS-8 DEBE tener lugar tras completarse CHPSWMS-7.	Volver a CHPSWMS-1. El PS inicia el funcionamiento del CDS.
CHPSWMS-9	Petición TGS (opcional) Si el PS obtuvo el tique de concesión de tique (TGT, *ticket granting ticket*) en la fase CHPSWMS-8, envía el mensaje petición TGS al servidor KDC del MSO cuya dirección fue transferida al PS (CDC) en la subopción 10 de la opción 122 de DHCP.	CHPSWMS-9 DEBE tener lugar tras completarse CHPSWMS-8.	Volver a CHPSWMS-1. El PS inicia el funcionamiento del CDS.

Cuadro 13-3/J.192 – Descripción de los flujos del proceso de configuración WAN-Man del PS en el modo de configuración SNMP

Fase del flujo	Configuración WAN-Man del PS: modo de configuración SNMP	Secuencia normal	Secuencia de fallo
CHPSWMS-10	Respuesta TGS (opcional) Se recibe el mensaje respuesta TGS con el tique procedente del KDC de IPCable2Home del MSO.	Si CHPSWMS-9 tiene lugar, CHPSWMS-10 DEBE tener lugar tras completarse CHPSWMS-9.	Volver a CHPSWMS-1. El PS inicia el funcionamiento del CDS.
CHPSWMS-11	Petición AP El PS envía el mensaje petición AP al NMS (gestor de SNMP) solicitando información de claves para SNMPv3, como se describe en 11.3, Infraestructura de autenticación del dispositivo PS.	CHPSWMS-11 DEBE tener lugar tras completarse CHPSWMS-10.	Volver a CHPSWMS-1. El PS inicia el funcionamiento del CDS.
CHPSWMS-12	Respuesta AP El mensaje respuesta AP se recibe del NMS con la información de claves para SNMPv3. Obsérvese que el PS DEBE establecer claves SNMPv3 Y rellenar los cuadros de SNMPv3 asociados antes de que envíe un mensaje de informe de SNMPv3. Las claves y los cuadros se establecen utilizando la información en la respuesta de AP. Véase 11.3, Infraestructura de autenticación del dispositivo PS.	CHPSWMS-12 DEBE tener lugar tras completarse CHPSWMS-11.	Volver a CHPSWMS-1. El PS inicia el funcionamiento del CDS.
CHPSWMS-13	Informe SNMP de admisión de configuración Después de que el PS que funciona en el modo de configuración SNMP establece las claves de SNMPv3, DEBE enviar un INFORME SNMPv3 (SNMPv3 INFORM) (cabhPsDevProvEnrollTrap) solicitando la admisión al SNMP MANAGER cuya dirección IP fue transferida en la subopción 3 de la opción 122, en el mensaje DHCP ACK. Una vez que el PS envía la cabhPsDevProvEnrollTrap antes descrita, comienza la supervisión del tiempo transcurrido, tal como se describe en 7.4.4.2.2.	CHPSWMS-13 DEBE tener lugar tras completarse CHPSWMS-12.	Volver a CHPSWMS-1.

Cuadro 13-3/J.192 – Descripción de los flujos del proceso de configuración WAN-Man del PS en el modo de configuración SNMP

Fase del flujo	Configuración WAN-Man del PS: modo de configuración SNMP	Secuencia normal	Secuencia de fallo
CHPSWMS-14	SNMP Get (opcional) Si el sistema de configuración necesita capacidades adicionales de dispositivo, la solicita al PS mediante peticiones SNMPv3 Get. Iterativo: El NMS envía peticiones SNMPv3 GET del PS para obtener la información necesaria sobre capacidad del PS. La aplicación de configuración puede utilizar una GetBulkRequest para obtener varias informaciones en un único mensaje.	No está previsto que CHPSWMS-14 tenga lugar antes de completarse CHPSWMS-13.	Volver a CHPSWMS-1.
CHPSWMS-15	Respuesta SNMP Get (opcional) Iterativo: El PS responde a NMS los mensajes de petición Get-Request o GetBulkRequest con una respuesta Get para cada petición GET. Una vez terminados todos los Get y los GetBulk, el NMS envía el dato solicitado a la aplicación de configuración.	Si CHPSWMS-14 tiene lugar, CHPSWMS-15 DEBE suceder tras completarse CHPSWMS-14.	N/A
CHPSWMS-16	Creación del fichero de configuración Opcional: El sistema de configuración utiliza información de las fases de configuración del PS CHPSWMS-16 y CHPSWMS-17 para crear un fichero de configuración PS. El sistema de configuración efectúa un troceo sobre el contenido del fichero de configuración PS. Dicho troceo se envía al PS en la fase siguiente.	Si CHPSWMS-15 tiene lugar, CHPSWMS-16 DEBE suceder tras completarse CHPSWMS-15.	N/A

Cuadro 13-3/J.192 – Descripción de los flujos del proceso de configuración WAN-Man del PS en el modo de configuración SNMP

Fase del flujo	Configuración WAN-Man del PS: modo de configuración SNMP	Secuencia normal	Secuencia de fallo
CHPSWMS-17	SNMP Set (opcional) El sistema de configuración puede encargar al NMS que envíe un mensaje SNMP Set al PS con la dirección IP del servidor TFTP, el nombre del fichero de configuración del PS y el troceo del fichero de configuración descrito en 7.4.4.2.2, Activador de la descarga del fichero de configuración para el modo de configuración SNMP. Opcionalmente, en el fichero de configuración del PS se incluyen la dirección IP del servidor TFTP del fichero de configuración de la barrera contra fuegos, el nombre de dicho fichero y el troceo del mismo cuando hay que cargar un fichero de configuración de la barrera contra fuegos y se selecciona este método para especificarlo.	Si CHPSWMS-16 tiene lugar, CHPSWMS-17 DEBE suceder tras completarse CHPSWMS-16.	Volver a CHPSWMS-1 si se recibió el Set pero tuvo lugar un error de proceso.
CHPSWMS-18	Petición TFTP Si el NMS activa la descarga por parte del PS del fichero de configuración del PS descrito en 7.4.4.2.2, el PS envía al servidor TFTP una petición TFTP Get para solicitar el fichero de configuración del PS especificado.	Si CHPSWMS-17 tiene lugar, CHPSWMS-18 DEBE suceder tras completarse CHPSWMS-17.	Continuar en CHPSWMS-17.
CHPSWMS-19	El servidor TFTP envía el fichero de configuración Una vez recibido por el PS su fichero de configuración, calcula el troceo de éste y lo compara con el valor recibido en la fase CHPSWMS-17. A continuación el PS procesa su fichero de configuración. Opcionalmente, en el fichero de configuración del PS se incluye la dirección IP del servidor TFTP del fichero de configuración de la barrera contra fuegos, el nombre de dicho fichero y el troceo (*hash*) del mismo cuando hay que cargar un fichero de configuración de la barrera contra fuegos, y se selecciona este método para especificarlo.	Si CHPSWMS-18 tiene lugar, CHPSWMS-19 sucede tras completarse CHPSWMS-18.	Si falla la descarga TFTP, comunicar el error, continuar reintentando CHPSWMS-18 (continuar reintentando la descarga del fichero de configuración del PS). Si el procesamiento del fichero de configuración provocase un error, continuar y comunicar el error como evento.

Cuadro 13-3/J.192 – Descripción de los flujos del proceso de configuración WAN-Man del PS en el modo de configuración SNMP

Fase del flujo	Configuración WAN-Man del PS: modo de configuración SNMP	Secuencia normal	Secuencia de fallo
CHPSWMS-20	Mensaje SYSLOG Si el PS ha recibido una dirección de servidor SYSLOG en el mensaje DHCP ACK, DEBE enviar un mensaje de "conclusión de configuración a SYSLOG. Esta notificación incluirá el resultado, éxito-fracaso, de la operación de configuración. El formato general de este mensaje se define en el cuadro B.1, Eventos definidos para IPCable2Home, ID de evento 73001100 (véanse las notas y los detalles del mensaje).	CHPSWMS-20 DEBE tener lugar tras completarse CHPSWMS-19.	
CHPSWMS-21	Informe SNMP El PS DEBE enviar al NMS un SNMP INFORM (cabhPsDevInitTrap) con una notificación "conclusión de configuración" y fijar el valor de cabhPsDevProvState a pass(1) si se produce cualquiera de las circunstancias siguientes: – El PS no ha sido activado por el NMS para descargar un fichero de configuración antes de que haya transcurrido el tiempo especificado por el valor de cabhPsDevProvisioningTimer desde la información de admisión descrita en CHPSWMS-13. – El PS ha sido activado por el NMS para descargar un fichero de configuración dentro del plazo de tiempo definido por el valor de cabhPsDevProvisioningTimer después del informe de admisión, y el PS descargó y procesó con éxito el fichero de configuración de PS. No es necesario finalizar la descarga y procesado del fichero de configuración antes de que haya transcurrido el tiempo definido por el valor de cabhPsDevProvisioningTimer tras el informe de admisión. El PS NO DEBE enviar un SNMP INFORM (cabhPsDevInitTrap) que contenga una notificación de "conclusión de configuración" y DEBE fijar el valor de cabhPsDevProvState a fail(3), cuando el PS haya sido activado por el NMS para descargar un fichero de configuración antes de que transcurra el tiempo definido por el valor de cabhPsDevProvisioningTimer desde la emisión del informe de admisión Y haya fracasado la descarga y procesamiento del fichero de configuración el número máximo de reintentos definidos en 7.4.4.2.4, Funcionamiento posterior a la activación.	CHPSWMS-21 DEBE tener lugar tras completarse CHPSWMS-20.	Si el PS no recibe una respuesta al informe de conclusión de configuración, DEBE reintentar el envío del informe cabhPsDevInitTrap, hasta en cinco ocasiones como máximo, con un intervalo de 10 segundos entre los intentos. Si fracasan los 5 intentos, el PS DEBE rearrancar el proceso de inicialización: volver a CHPSWMS-1 y notificar el error.

Cuadro 13-3/J.192 – Descripción de los flujos del proceso de configuración WAN-Man del PS en el modo de configuración SNMP

Fase del flujo	Configuración WAN-Man del PS: modo de configuración SNMP	Secuencia normal	Secuencia de fallo
CHPSWMS-22	TFTP Request – Fichero de configuración de la barrera contra fuegos (opcional) El PS envía al servidor TFTP de configuración de la barrera contra fuegos una petición TFTP Get para solicitar el fichero de datos de configuración de la barrera contra fuegos especificado.	Si CHPSWMS-22 tiene lugar, DEBE suceder tras completarse CHPSWMS-21.	Volver a CHPSWMS-1.
CHPSWMS-23	El servidor TFTP envía el fichero de configuración de la barrera contra fuegos El servidor TFTP envía al PS una respuesta TFTP con el fichero solicitado. Una vez recibe el PS el fichero de configuración de la barrera contra fuegos, calcula el troceo de éste y lo compara con el valor recibido en la fase CHPSWMS-21. A continuación se procesa el fichero. Consúltese 7.4.4 correspondiente a la descripción del contenido del fichero de configuración del PS.	Si CHPSWMS-22 tiene lugar, CHPSWMS-23 DEBE suceder tras completarse CHPSWMS-22.	Si falla la descarga TFTP, continuar el funcionamiento del PS pero comunicar el error y continuar reintentando CHPSWMS-22. Si el procesamiento del fichero de configuración de la barrera contra fuegos provoca un error, continuar y comunicar el error como evento.
NOTA 1 – Las fases CHPSWMS-5 a CHIPSWMS-8 son opcionales en ciertos casos. Para más información véase la cláusula 11. NOTA 2 – Las operaciones SNMP Get y subsiguientes operaciones de respuesta SNMP Get son opcionales, dependiendo de la necesidad de información adicional para formar el fichero de configuración del PS, y también de la necesidad del fichero de configuración del PS.			

13.4.1 Descarga del fichero de configuración de WAN-Man del PS

El PS funcionando en el modo de configuración SNMP podría contener suficiente información por defecto desde fábrica para mantener el funcionamiento del lado LAN y WAN o de ambos, sin necesidad de descargar el fichero de configuración del PS. Si el PS funciona en el modo de configuración SNMP, el NMS podría activar la descarga del fichero de configuración del PS para que la configuración inicial sustituya los valores por defecto de fábrica o suministre información adicional.

El fichero de configuración de la barrera contra fuegos contiene información para proveer la función de barrera contra fuegos. La indicación de descarga del fichero de configuración de la barrera contra fuegos vendrá en el fichero de configuración del PS o en un SNMP Set durante la inicialización.

13.4.2 Temporizador de configuración del PS

Se proporciona un temporizador de configuración para garantizar que el PS continúe el proceso de configuración en el modo de configuración SNMP en caso de que el PS no esté activado para descargar un fichero de configuración del PS. El PS ha de supervisar el tiempo transcurrido desde que emite el informe SNMP de admisión de configuración. Si el PS no está activado para descargar un fichero de configuración durante el periodo de tiempo identificado por el temporizador de configuración, señaliza que ha concluido la configuración emitiendo un informe SNMP de conclusión de configuración y fija el valor de cabhPsDevProvState a pass(1). El objeto temporizador, cabhPsDevProvTimer, tiene un valor por defecto de cinco minutos. Para más información, véase 7.4.4.2.2.

13.4.3 Informes de conclusión de admisión a la configuración y de configuración

Sólo para el PS funcionando en el modo de configuración SNMP, el informe de admisión de configuración (cabhPsDevProvEnrollTrap) permite que el servidor de configuración determine si el PS está preparado para el fichero de configuración del PS.

Tanto en el modo de configuración DHCP como en el modo de configuración SNMP, la trampa de conclusión de la configuración (cabhPsDevInitTrap) indica si se ha completado o no la secuencia de configuración.

13.4.4 Configuración de SYSLOG

La dirección IP del servidor de syslog DEBE configurarse mediante el proceso DHCP. El evento syslog no se enviará si no está configurada la dirección IP del servidor syslog.

13.4.5 Estado de configuración y comunicación de errores

Como indican los cuadros 13-1 y 13-3, el fallo de las fases del proceso de configuración se suele traducir en la repetición del proceso desde la primera fase, CHPSWMD-1 o CHPSWMS-1.

13.5 Proceso de configuración WAN-Data del PS

El PS solicita cero o más direcciones de red WAN-Data al servidor DHCP de la red de cable para utilizarlas en el intercambio de datos entre los elementos conectados a Internet y a los dispositivos IP de LAN.

No hay diferencia entre el funcionamiento WAN-Data del PS en los modos de configuración DHCP y SNMP.

La figura 13-7 ilustra el flujo de mensajes que ha de utilizarse para la configuración de direcciones WAN-Data del PS. El proceso de configuración de las direcciones de WAN-Data del PS es el mismo para el PS integrado con un módem de cable DOCSIS que para el PS autónomo.

Si tiene lugar el proceso de configuración de direcciones WAN-Data del PS, DEBE seguir la secuencia que muestra la figura 13-7 y describe detalladamente el cuadro 13-4.

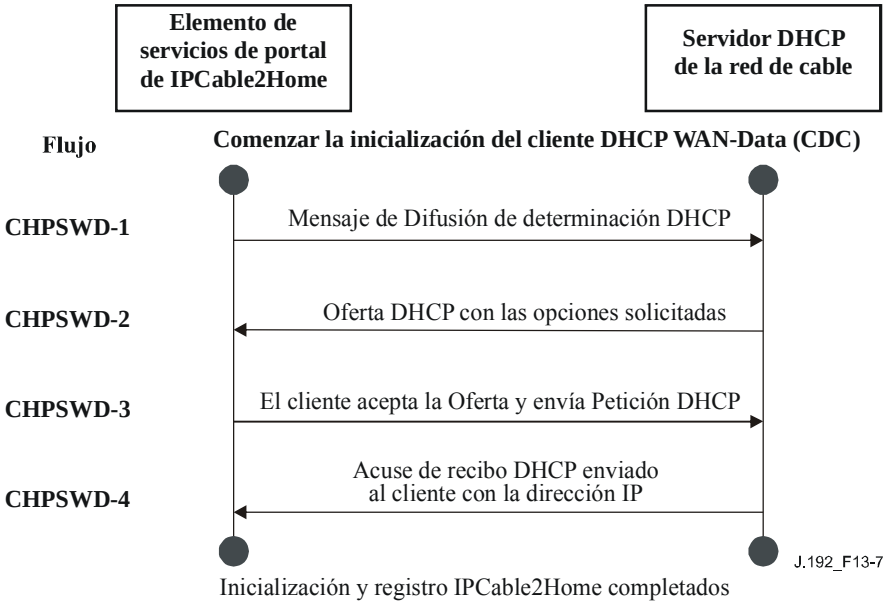


Figura 13-7/J.192 – Proceso de configuración WAN-Data del PS

Cuadro 13-4/J.192 – Descripción del flujo de la configuración WAN-Data del PS

Fase del flujo	Configuración de dirección WAN-Data del PS	Secuencia normal	Secuencia de fallo
CHPSWD-1	Difusión de determinación DHCP (DHCP Broadcast Discover) El PS envía un mensaje DHCP DISCOVER en modo difusión con las opciones obligatorias que figuran en el cuadro 7-10, Opciones DHCP del CDC en los mensajes DISCOVER y REQUEST.	Continuar en CHPSWD-2.	Si falla el protocolo DHCP, repetir CHPSWD-1.
CHPSWD-2	OFERTA DHCP (DHCP OFFER) El servidor DHCP situado en la cabecera recibe el paquete DHCP DISCOVER, asigna una dirección IP del grupo WAN-Data, construye un paquete DHCP OFFER y lo transmite al agente de enlace DHCP [RFC 3046] del CMTS.	Continuar en CHPSWD-3.	Si falla, el cliente agota el temporizador del protocolo DHCP y se repite la fase CHPSWD-1.
CHPSWD-3	PETICIÓN DHCP (DHCP REQUEST) El CDP envía al servidor DHCP adecuado un mensaje DHCP REQUEST para aceptar el DHCP OFFER, conforme a los requisitos del cliente en [RFC 2131].	CHPSWD-3 DEBE tener lugar tras completarse CHPSWD-2.	Si falla el protocolo DHCP, volver a CHPSWD-1.
CHPSWD-4	ACUSE DE RECIBO DHCP (DHCP ACK) El servidor DHCP envía al CDP un mensaje DHCP ACK con la dirección IPv4 de la interfaz WAN-Data del PS.	CHPSWD-4 DEBE tener lugar tras completarse CHPSWD-3. La configuración termina al completarse CHPSWD-4.	Si falla el protocolo DHCP, volver a CHPSWD-1.

13.6 Proceso de configuración: dispositivo IP de LAN en el sector LAN-Pass

Algunas aplicaciones de LAN doméstica no podrán funcionar adecuadamente con una dirección de red traducida. Para dar cabida a estas aplicaciones el PS se habilita de modo que funcione en el modo de transferencia (puenteo transparente). Como se describió en 8.3.3.1, Modos de tratamiento de paquetes, el puenteo tiene lugar cuando el NMS de la red de cable fija que el modo de tratamiento de paquetes primario (cabhCapPrimaryMode) es el de transferencia, o escribiendo direcciones MAC particulares del dispositivo IP de LAN en el cuadro de transferencia (cabhCapPassthroughTable). Cuando el PS se ha configurado para este propósito, los mensajes DHCP DISCOVER y DHCP REQUEST emitidos por un dispositivo IP de LAN serán tratados por el servidor DHCP de la red de cable y no por el CDS.

Se supone que un dispositivo IP de LAN no conforme con IPCable2Home implementa un cliente DHCP y solicita una licencia de dirección IP utilizando DHCP [RFC 2131]. Un dispositivo IP de LAN conforme a IPCable2Home, es decir, aquel que implementa la funcionalidad de BP que se define en esta especificación, debe implementar un cliente DHCP y solicitar una licencia de dirección IP mediante DHCP.

Anexo A

Objetos de la MIB

Este anexo relaciona todos los objetos de la MIB necesarios, según se indica en 6.3.3.1.4.1, Requisitos del protocolo SNMP, y en 6.3.3.1.4.7, Requisitos de la MIB de IPCable2Home e identifica el requisito de persistencia para cada uno de los objetos relacionados.

A continuación se define cómo se aplica en este anexo el término 'persistente':

Persistente: requisito de que el PS conserve el valor de un objeto de la MIB configurable (mediante el gestor o el propio PS) durante un rearranque o una reinicialización del PS.

En el caso de los objetos de la MIB con la anotación 'Sí' en la columna de persistencia, el valor del objeto inmediatamente a continuación de un rearranque o reinicialización del PS, DEBE ser el mismo que su valor justo antes del rearranque o reinicialización.

En el caso de los objetos de la MIB con la anotación 'No' en la columna de persistencia, el valor del objeto DEBE fijarse a su valor de fábrica por defecto (DEFVAL, *default value*) o, si no dispone de este valor, DEBE fijarse como cero o nulo, según proceda, inmediatamente a continuación de un rearranque o reinicialización del PS.

En el caso de objetos MIB con la anotación "–" en la columna de persistencia, se aplicará alguno de los siguientes valores:

- el valor del objeto inmediatamente a continuación del rearranque o reinicialización del PS lo determina el fabricante, ya que no existe un requisito particular para este valor; o
- el valor del objeto es determinístico basándose en la descripción de la MIB (el valor del objeto es fijo o puede deducirse de valores conocidos después del rearranque o reinicialización del PS).

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
Sistema mib-2 [RFC 1213]			
sysDescr	sólo lectura	–	N/A
sysObjectID	sólo lectura	–	N/A
sysUpTime	sólo lectura	–	N/A
sysContact	lectura-escritura	Sí	1
sysName	lectura-escritura	Sí	1
sysLocation	lectura-escritura	Sí	1
sysServices	sólo lectura	–	N/A
interfaces [RFC 2863]			
ifNumber	sólo lectura	–	N/A
ifTable/ ifEntry			
ifIndex	sólo lectura	–	N/A
ifDescr	sólo lectura	–	N/A
ifType	sólo lectura	–	N/A
ifMtu	sólo lectura	–	N/A
ifSpeed	sólo lectura	–	N/A

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
ifPhysAddress	sólo lectura	–	N/A
ifAdminStatus	lectura-escritura	No[2]	N/A
ifOperStatus	sólo lectura	–	N/A
ifLastChange	sólo lectura	–	N/A
ifInOctets	sólo lectura	–	N/A
ifInUcastPkts	sólo lectura	–	N/A
ifInDiscards	sólo lectura	–	N/A
ifInErrors	sólo lectura	–	N/A
ifInUnknownProtos	sólo lectura	–	N/A
ifOutOctets	sólo lectura	–	N/A
ifOutUcastPkts	sólo lectura	–	N/A
ifOutDiscards	sólo lectura	–	N/A
ifOutErrors	sólo lectura	–	N/A

[2] ifAdminStatus es persistente para ifIndex = 254 y no es persistente para otros valores de ifIndex.

ip [RFC 2011]			
ipForwarding	lectura-escritura	No	N/A
ipDefaultTTL	lectura-escritura	No	N/A
ipInReceives	sólo lectura	–	N/A
ipInHdrErrors	sólo lectura	–	N/A
ipInAddrErrors	sólo lectura	–	N/A
ipForwDatagrams	sólo lectura	–	N/A
ipInUnknownProtos	sólo lectura	–	N/A
ipInDiscards	sólo lectura	–	N/A
ipInDelivers	sólo lectura	–	N/A
ipOutRequests	sólo lectura	–	N/A
ipOutDiscards	sólo lectura	–	N/A
ipOutNoRoutes	sólo lectura	–	N/A
ipReasmTimeout	sólo lectura	–	N/A
ipReasmReqds	sólo lectura	–	N/A
ipReasmOKs	sólo lectura	–	N/A
ipReasmFails	sólo lectura	–	N/A
ipFragOKs	sólo lectura	–	N/A
ipFragFails	sólo lectura	–	N/A
ipFragCreates	sólo lectura	–	N/A
ipNetToMediaTable/ ipNetToMediaEntry			
ipNetToMediaIfIndex	sólo lectura	No	N/A
ipNetToMediaPhyAddress	sólo lectura	No	N/A
ipNetToMediaNetAddress	sólo lectura	No	N/A
ipNetToMediaType	sólo lectura	No	N/A

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
icmp			
icmpInMsgs	sólo lectura	–	N/A
icmpInErrors	sólo lectura	–	N/A
icmpInDestUnreachs	sólo lectura	–	N/A
icmpInTimeExcds	sólo lectura	–	N/A
icmpInParmProbs	sólo lectura	–	N/A
icmpInSrcQuenchs	sólo lectura	–	N/A
icmpInRedirects	sólo lectura	–	N/A
icmpInEchos	sólo lectura	–	N/A
icmpInEchosReps	sólo lectura	–	N/A
icmpInTimestamps	sólo lectura	–	N/A
icmpInTimestampsReps	sólo lectura	–	N/A
icmpInAddrMasks	sólo lectura	–	N/A
icmpInAddrMaskReps	sólo lectura	–	N/A
icmpOutMsgs	sólo lectura	–	N/A
icmpOutErrors	sólo lectura	–	N/A
icmpOutDestUnreachs	sólo lectura	–	N/A
icmpOutTimeExcds	sólo lectura	–	N/A
icmpOutParmProbs	sólo lectura	–	N/A
icmpOutSrcQuenchs	sólo lectura	–	N/A
icmpOutRedirects	sólo lectura	–	N/A
icmpOutEchos	sólo lectura	–	N/A
icmpOutEchosReps	sólo lectura	–	N/A
icmpOutTimestamps	sólo lectura	–	N/A
icmpOutTimestampReps	sólo lectura	–	N/A
icmpOutAddrMasks	sólo lectura	–	N/A
icmpOutAddrMaskReps	sólo lectura	–	N/A
udp [RFC 2013]			
udpInDatagrams	sólo lectura	–	N/A
udpNoPorts	sólo lectura	–	N/A
udpInErrors	sólo lectura	–	N/A
udpOutDatagrams	sólo lectura	–	N/A
udpTable/ udpEntry			
udpLocalAddress	sólo lectura	–	N/A
udpLocalPort	sólo lectura	–	N/A

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
transmission [draft-ietf-ipcdn-bpiplus-mib-05] **docsIfMib** **docsBpi2MIB** **docsBpi2MIBObjects** **docsBpi2CmObjects** **docsBpi2CmCertObjects**			
docsBpi2CodeDownloadGroup			
docsBpi2CodeDownloadStatusCode	sólo lectura	–	N/A
docsBpi2CodeDownloadStatusString	sólo lectura	–	N/A
docsBpi2CodeMfgOrgName	sólo lectura	Sí	1
docsBpi2CodeMfgCodeAccessStart	sólo lectura	Sí	1
docsBpi2CodeMfgCvcAccessStart	sólo lectura	Sí	1
docsBpi2CodeCoSignerOrgName	sólo lectura	–	N/A
docsBpi2CodeCoSignerCodeAccessStart	sólo lectura	–	N/A
docsBpi2CodeCoSignerCvcAccessStart	sólo lectura	–	N/A
docsBpi2CodeCvcUpdate	lectura-escritura	No	N/A
snmp [RFC 3418]			
snmpInPkts	sólo lectura	–	N/A
snmpInBadVersions	sólo lectura	–	N/A
snmpInBadCommunityNames	sólo lectura	–	N/A
snmpInBadCommunityUses	sólo lectura	–	N/A
snmpInASNParseErrs	sólo lectura	–	N/A
snmpEnableAuthenTraps	lectura-escritura	No	N/A
snmpSilentDrops	sólo lectura	–	N/A
ifMIB [RFC 2863] **ifMIBOjects**			
ifXTable/ *ifXEntry*			
ifName	sólo lectura	–	N/A
ifInMulticastPkts	sólo lectura	–	N/A
ifInBroadcastPkts	sólo lectura	–	N/A
ifOutMulticastPkts	sólo lectura	–	N/A
ifOutBroadcastPkts	sólo lectura	–	N/A
ifLinkUpDownTrapEnable	lectura-escritura	No	N/A
ifHighSpeed	sólo lectura	–	N/A
ifPromiscuousMode	lectura-escritura	No	N/A
ifConnectorPresent	sólo lectura	–	N/A
ifAlias	lectura-escritura	No	N/A
ifCounterDiscontinuityTime	sólo lectura	–	N/A

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
ifStackTable /ifStackEntry			
ifStackHigherLayer	sólo lectura	–	N/A
ifStackLowerLayer	sólo lectura	–	N/A
ifStackStatus	sólo lectura	–	N/A
docsDev [RFC 2669] docsDevMIBObjects			
docsDevNmAccessTable/ docsDevNmAccessEntry			
docsDevNmAccessIndex	inaccesible	–	N/A
docsDevNmAccessIp	lectura-creación	No	N/A
docsDevNmAccessIpMask	lectura-creación	No	N/A
docsDevNmAccessCommunity	lectura-creación	No	N/A
docsDevNmAccessControl	lectura-creación	No	N/A
docsDevNmAccessInterfaces	lectura-creación	No	N/A
docsDevNmAccessStatus	lectura-creación	No	N/A
docsDevNmAccessTrapVersion	lectura-creación	No	N/A
docsDevSoftware			
docsDevSwServer	lectura-escritura	Sí	1
docsDevSwFilename	lectura-escritura	Sí	1
docsDevSwAdminStatus	lectura-escritura	Sí	1
docsDevSwOperStatus	sólo lectura	Sí	1
docsDevSwCurrentVers	sólo lectura	–	N/A
docsDevEvent			
docsDevEvControl	lectura-escritura	No	N/A
docsDevEvSyslog	lectura-escritura	No	N/A
docsDevEvThrottleAdminStatus	lectura-escritura	No	N/A
docsDevEvThrottleInhibited	sólo lectura	–	N/A
docsDevEvThrottleThreshold	lectura-escritura	No	N/A
docsDevEvThrottleInterval	lectura-escritura	No	N/A
docsDevEvControlTable/ docsDevEvControlEntry			
docsDevEvPriority	inaccesible	–	N/A
docsDevEvReporting	lectura-escritura	No	N/A
docsDevEventTable/ docsDevEventEntry			
docsDevEvIndex	inaccesible	–	N/A
docsDevEvFirstTime	sólo lectura	Sí	10
docsDevEvLastTime	sólo lectura	Sí	10

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
docsDevEvCounts	sólo lectura	Sí	10
docsDevEvLevel	sólo lectura	Sí	10
docsDevEvId	sólo lectura	Sí	10
docsDevEvText	sólo lectura	Sí	10
docsDevFilter			
docsDevFilterIpTable/ docsDevFilterIpEntry			
docsDevFilterIpIndex	inaccesible	–	N/A
docsDevFilterIpStatus	lectura-creación	Sí	40
docsDevFilterIpControl	lectura-creación	Sí	40
docsDevFilterIpIfIndex	lectura-creación	Sí	40
docsDevFilterIpDirection	lectura-creación	Sí	40
docsDevFilterIpBroadcast	lectura-creación	No	N/A
docsDevFilterIpSaddr	lectura-creación	Sí	40
docsDevFilterIpSmask	lectura-creación	Sí	40
docsDevFilterIpDaddr	lectura-creación	Sí	40
docsDevFilterIpDmask	lectura-creación	Sí	40
docsDevFilterIpProtocol	lectura-creación	Sí	40
docsDevFilterIpSourcePortLow	lectura-creación	Sí	40
docsDevFilterIpSourcePortHigh	lectura-creación	Sí	40
docsDevFilterIpDestPortLow	lectura-creación	Sí	40
docsDevFilterIpDestPortHigh	lectura-creación	Sí	40
docsDevFilterIpMatches	sólo lectura	–	N/A
docsDevFilterIpTos	lectura-creación	No	N/A
docsDevFilterIpTosMask	lectura-creación	No	N/A
docsDevFilterIpContinue	sólo lectura	=	N/A
docsDevFilterIpPolicyId	lectura-creación	No	N/A
dot11			
dot11StationConfigTable/ dot11StationConfigEntry[3]			
dot11PrivacyOptionImplemented	sólo lectura	–	N/A
dot11DesiredSSID	lectura-escritura	Sí	1
dot11OperationalRateSet	lectura-escritura/ sólo lectura	Sí/–	1/N/A
dot11BeaconPeriod	lectura-escritura/ sólo lectura	Sí/–	1/N/A
dot11DTIMPeriod	lectura-escritura/ sólo lectura	Sí/–	1/N/A

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
dot11WEPDefaultKeysTable/ dot11WEPDefaultKeysEntry[3]			
dot11WEPDefaultKeyIndex	inaccesible	N/A	N/A
dot11WEPDefaultKeyValue	lectura-escritura	Sí	4
dot11PrivacyTable dot11PrivacyEntry[3]			
dot11PrivacyInvoked	lectura-escritura	Sí	1
dot11WEPDefaultKeyID	lectura-escritura	Sí	1
dot11OperationTable dot11OperationEntry[3]			
dot11MACAddress	sólo lectura	–	N/A
dot11RTSThreshold	lectura-escritura/ sólo lectura	Sí/–	1/N/A
dot11FragmentationThreshold	lectura-escritura/ sólo lectura	Sí/–	1/N/A
dot11PhyTxPowerTable dot11PhyTxPowerEntry[3]			
dot11NumberSupportedPowerLevels	sólo lectura	–	N/A
dot11TxPowerLevel1	sólo lectura	–	N/A
dot11TxPowerLevel2	sólo lectura	–	N/A
dot11TxPowerLevel3	sólo lectura	–	N/A
dot11TxPowerLevel4	sólo lectura	–	N/A
dot11TxPowerLevel5	sólo lectura	–	N/A
dot11TxPowerLevel6	sólo lectura	–	N/A
dot11TxPowerLevel7	sólo lectura	–	N/A
dot11TxPowerLevel8	sólo lectura	–	N/A
dot11CurrentTxPowerLevel	lectura-escritura	Sí	1
dot11PhyDSSSTable dot11PhyDSSSEntry[3]			
dot11CurrentChannel	lectura-escritura	Sí	1
dot11PhyOFDMTable dot11PhyOFDMEntry[3]			
dot11CurrentFrequency	lectura-escritura	Sí	1
dot11FrequencyBandsSupported	sólo lectura	–	N/A

[3] Los objetos MIB con un conjunto de requisitos de persistencia se indican para cada interfaz radioeléctrica que soporte la funcionalidad de la anotación incluida en la MIB.

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
private			
enterprises			
cableLabs			
clabProject			
clabProjCableHome			
cabhPsDevMib			
cabhPsDevBase			
cabhPsDevDateTime	lectura-escritura	No	N/A
cabhPsDevResetNow	lectura-escritura	No	N/A
cabhPsDevSerialNumber	sólo lectura	–	N/A
cabhPsDevHardwareVersion	sólo lectura	–	N/A
cabhPsDevWanManMacAddress	sólo lectura	–	N/A
cabhPsDevWanDataMacAddress	sólo lectura	–	N/A
cabhPsDevTypeIdentifier	sólo lectura	–	N/A
cabhPsDevSetToFactory	lectura-escritura	No	N/A
cabhPsDevTodSyncStatus	sólo lectura	–	N/A
cabhPsDevProvMode	sólo lectura	–	N/A
cabhPsDevLastSetToFactory	sólo lectura	–	N/A
cabhPsDevTrapControl	lectura-escritura	No	N/A
cabhPsDevProv			
cabhPsDevProvisioningTimer	lectura-escritura	No	N/A
cabhPsDevProvConfigFile	lectura-escritura	No	N/A
cabhPsDevProvConfigHash	lectura-escritura	No	N/A
cabhPsDevProvConfigFileSize	sólo lectura	–	N/A
cabhPsDevProvConfigFileStatus	sólo lectura	–	N/A
cabhPsDevProvConfigTLVProcessed	sólo lectura	–	N/A
cabhPsDevProvConfigTLVRejected	sólo lectura	–	N/A
cabhPsDevProvSolicitedKeyTimeout	lectura-escritura	Sí	1
cabhPsDevProvState	sólo lectura	–	N/A
cabhPsDevProvAuthState	sólo lectura	–	N/A
cabhPsDevTimeServerAddrType	sólo lectura	–	N/A
cabhPsDevTimeServerAddr	sólo lectura	–	N/A
cabhPsDevAttrib			
cabhPsDevPsAttrib			
cabhPsDevPsDeviceType	sólo lectura	–	N/A
cabhPsDevPsManufacturerURL	sólo lectura	–	N/A
cabhPsDevPsModelURL	sólo lectura	–	N/A
cabhPsDevPsModelUPC	sólo lectura	–	N/A

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
cabhPsDevPsStats			
cabhPsDevLanIpTrafficCountersReset	lectura-escritura	No	N/A
cabhPsDevLanIpTrafficCountersLastReset	sólo lectura	–	N/A
cabhPsDevLanIpTrafficEnabled	lectura-escritura	No	N/A
cabhPsDevLanIpTrafficTable/ cabhPsDevLanIpTrafficEntry			
cabhPsDevLanIpTrafficIndex	inaccesible	–	N/A
cabhPsDevLanIpTrafficInetAddressType	sólo lectura	–	N/A
cabhPsDevLanIpTrafficInetAddress	sólo lectura	–	N/A
cabhPsDevLanIpTrafficInOctets	sólo lectura	–	N/A
cabhPsDevLanIpTrafficOutOctets	sólo lectura	–	N/A
cabhPsDevPsAccessControl			
cabhPsDevAccessControlEnable	lectura-escritura	No	N/A
cabhPsDevAccessControlTable/ cabhPsDevAccessControlEntry			
cabhPsDevAccessControlIndex	inaccesible	–	N/A
cabhPsDevAccessControlPhysAddr	lectura-escritura	Sí	20
cabhPsDevAccessControlRowStatus	lectura-creación	Sí	20
cabhPsDevPsMisc cabhPsDevPsUI			
cabhPsDevUILogin	lectura-escritura	Sí	1
cabhPsDevUIPassword	lectura-escritura	Sí	1
cabhPsDevUISelection	lectura-escritura	Sí	1
cabhPsDevUIServerURL	lectura-escritura	Sí	1
cabhPsDevUISelectionDisabledBodyText	lectura-escritura	Sí	1
cabhPsDev802dot11BaseTable/ cabhPsDev802dot11BaseEntry[4]			
cabhPsDev802dot11BaseSetToDefault	lectura-escritura	–	N/A
cabhPsDev802dot11BaseLastSetToDefault	sólo lectura	–	N/A
cabhPsDev802dot11BaseAdvertiseSSID	lectura-escritura	Sí	1
cabhPsDev802dot11BasePhyCapabilities	sólo lectura	–	N/A
cabhPsDev802dot11BasePhyOperMode	lectura-escritura	Sí	1
cabhPsDev802dot11SecTable *cabhPsDev802dot11SecEntry*[4]			
cabhPsDev802dot11SecCapabilities	sólo lectura	–	N/A
cabhPsDev802dot11SecOperMode	lectura-escritura	Sí	1
cabhPsDev802dot11SecPassPhraseToWEPKey	lectura-escritura	Sí	1

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
cabhPsDev802dot11SecUsePassPhraseToWEPKeyAlg	lectura-escritura	Sí	1
cabhPsDev802dot11SecPSKPassPhraseToKey	lectura-escritura	Sí	1
cabhPsDev802dot11SecWPAPreSharedKey	lectura-escritura	Sí	1
cabhPsDev802dot11SecWPARekeyTime	lectura-escritura	Sí	1
cabhPsDev802dot11SecControl	lectura-escritura	No	N/A
cabhPsDev802dot11SecCommitStatus	sólo lectura	No	N/A
[4] Los objetos MIB con un conjunto de requisitos de persistencia se indican para cada interfaz radioeléctrica que soporte la funcionalidad de la anotación incluida en la MIB.			
cabhPsDevUpnp **cabhPsDevUpnpBase**			
cabhPsDevUpnpEnabled	lectura-escritura	Sí	1
cabhPsDevUpnpCommands			
cabhPsDevUpnpCommandIpType	lectura-escritura	No	N/A
cabhPsDevUpnpCommandIp	lectura-escritura	No	N/A
cabhPsDevUpnpCommand	lectura-escritura	No	N/A
cabhPsDevUpnpCommandUpdate	lectura-escritura	No	N/A
cabhPsDevUpnpLastCommandUpdate	sólo lectura	–	N/A
cabhPsDevUpnpCommandStatus	sólo lectura	–	N/A
cabhPsDevUpnpInfoTable/ *cabhPsDevUpnpInfoEntry*			
cabhPsDevUpnpInfoXmlFragment	sólo lectura	–	N/A
cabhSecMib *cabhSecCertObjects*			
cabhSecCertPsCert	sólo lectura	–	1
cabhSec2FwObjects **cabhSec2FwBase**			
cabhSec2FwEnable	lectura-escritura	Sí	N/A
cabhSec2FwPolicyFileURL	lectura-escritura	No	N/A
cabhSec2FwPolicyFileHash	lectura-escritura	No	N/A
cabhSec2FwPolicyFileOperStatus	sólo lectura	–	N/A
cabhSec2FwPolicyFileCurrentVersion	lectura-escritura	Sí	N/A
cabhSec2FwClearPreviousRuleset	lectura-escritura	No	N/A
cabhSec2FwPolicySelection	lectura-escritura	Sí	N/A
cabhSec2FwEventSetToFactory	lectura-escritura	No	N/A
cabhSec2FwEventLastSetToFactory	sólo lectura	–	N/A
cabhSec2FwPolicySuccessfulFileURL	sólo lectura	Sí	1
cabhSec2FwConfiguredRulesetPriority	sólo lectura	Sí	1
cabhSec2FwClearLocalRuleset	lectura-escritura	No	N/A

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
cabhSec2FwEvent			
cabhSec2FwEventControlTable/ cabhSec2FwEventControlEntry			
cabhSec2FwEventType	inaccesible	–	N/A
cabhSec2FwEventEnable	lectura-escritura	No	N/A
cabhSec2FwEventThreshold	lectura-escritura	No	N/A
cabhSec2FwEventInterval	lectura-escritura	No	N/A
cabhSec2FwEventCount	sólo lectura	–	N/A
cabhSec2FwEventLogReset	lectura-escritura	No	N/A
cabhSec2FwEventLogLastReset	sólo lectura	–	N/A
cabhSec2FwLogTable *cabhSec2FwLogEntry*			
cabhSec2FwLogIndex	inaccesible	–	N/A
cabhSec2FwLogEventType	sólo lectura	Sí	40
cabhSec2FwLogEventPriority	sólo lectura	Sí	40
cabhSec2FwLogEventId	sólo lectura	Sí	40
cabhSec2FwLogTime	sólo lectura	Sí	40
cabhSec2FwLogIpProtocol	sólo lectura	Sí	40
cabhSec2FwLogIpSourceAddr	sólo lectura	Sí	40
cabhSec2FwLogIpDestAddr	sólo lectura	Sí	40
cabhSec2FwLogIpSourcePort	sólo lectura	Sí	40
cabhSec2FwLogIpDestPort	sólo lectura	Sí	40
cabhSec2FwLogMessageType	sólo lectura	Sí	40
cabhSec2FwLogReplayCount	sólo lectura	Sí	40
cabhSec2FwLogMIBPointer	sólo lectura	Sí	40
cabhSec2FwLogMatchingFilterTableName	sólo lectura	Sí	40
cabhSec2FwLogMatchingFilterTableIndex	sólo lectura	Sí	40
cabhSec2FwLogMatchingFilterDescr	sólo lectura	Sí	40
cabhSec2FwFilter			
cabhSec2FwFilterScheduleTable *cabhSec2FwFilterScheduleEntry*			
cabhSec2FwFilterScheduleStartTime	lectura-creación	Sí	40
cabhSec2FwFilterScheduleEndTime	lectura-creación	Sí	40
cabhSec2FwFilterScheduleDOW	lectura-creación	Sí	40
cabhSec2FwFilterScheduleDescr	lectura-creación	Sí	40

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
cabhSec2FwLocalFilterIpTable/ cabhSec2FwLocalFilterIpEntry			
cabhSec2FwLocalFilterIpIndex	inaccesible	–	N/A
cabhSec2FwLocalFilterIpStatus	lectura-creación	Sí	40
cabhSec2FwLocalFilterIpControl	lectura-creación	Sí	40
cabhSec2FwLocalFilterIpIfIndex	lectura-creación	Sí	40
cabhSec2FwLocalFilterIpDirection	lectura-creación	Sí	40
cabhSec2FwLocalFilterIpSaddr	lectura-creación	Sí	40
cabhSec2FwLocalFilterIpSmask	lectura-creación	Sí	40
cabhSec2FwLocalFilterIpDaddr	lectura-creación	Sí	40
cabhSec2FwLocalFilterIpDmask	lectura-creación	Sí	40
cabhSec2FwLocalFilterIpProtocol	lectura-creación	Sí	40
cabhSec2FwLocalFilterIpSourcePortLow	lectura-creación	Sí	40
cabhSec2FwLocalFilterIpSourcePortHigh	lectura-creación	Sí	40
cabhSec2FwLocalFilterIpDestPortLow	lectura-creación	Sí	40
cabhSec2FwLocalFilterIpDestPortHigh	lectura-creación	Sí	40
cabhSec2FwLocalFilterIpMatches	sólo lectura	Sí	40
cabhSec2FwLocalFilterIpContinue	sólo lectura	Sí	40
cabhSec2FwLocalFilterIpStartTime	lectura-creación	Sí	40
cabhSec2FwLocalFilterIpEndTime	lectura-creación	Sí	40
cabhSec2FwLocalFilterIpDOW	lectura-creación	Sí	40
cabhSec2FwLocalFilterIpDescr	lectura-creación	Sí	40
cabhSec2FwFactoryDefault			
cabhSec2FwFactoryDefaultTable/ cabhSec2FwFactoryDefaultEntry			
cabhSec2FwFactoryDefaultIndex	inaccesible		
cabhSec2FwFactoryDefaultControl		–	N/A
cabhSec2FwFactoryDefaultIfIndex		–	N/A
cabhSec2FwFactoryDefaultDirection		–	N/A
cabhSec2FwFactoryDefaultSaddr		–	N/A
cabhSec2FwFactoryDefaultSmask		–	N/A
cabhSec2FwFactoryDefaultDaddr		–	N/A
cabhSec2FwFactoryDefaultDmask		–	N/A
cabhSec2FwFactoryDefaultProtocol		–	N/A
cabhSec2FwFactoryDefaultSourcePortLow		–	N/A
cabhSec2FwFactoryDefaultSourcePortHigh		–	N/A
cabhSec2FwFactoryDefaultDestPortLow		–	N/A
cabhSec2FwFactoryDefaultDestPortHigh		–	N/A
cabhSec2FwFactoryDefaultIFilterContinue		–	N/A

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
cabhSecKerbBase			
cabhSecKerbPKINITGracePeriod	lectura-escritura	No	N/A
cabhSecKerbTGSGracePeriod	lectura-escritura	No	N/A
cabhSecKerbUnsolicitedKeyMaxTimeout	lectura-escritura	No	N/A
cabhSecKerbUnsolicitedKeyMaxRetries	lectura-escritura	No	N/A
cabhCapMib **cabhCapObjects** **cabhCapBase**			
cabhCapTcpTimeWait	lectura-escritura	No	N/A
cabhCapUdpTimeWait	lectura-escritura	No	N/A
cabhCapIcmpTimeWait	lectura-escritura	No	N/A
cabhCapPrimaryMode	lectura-escritura	No	N/A
cabhCapSetToFactory	lectura-escritura	No	N/A
cabhCapLastSetToFactory	sólo lectura	–	N/A
CabhCapUpnpPortForwardingEnable	lectura-escritura	Sí	1
CabhCapUpnpTimeWait	lectura-escritura	No	N/A
cabhCapMap			
cabhCapMappingTable/ *cabhCapMappingEntry*			
cabhCapMappingIndex	inaccesible	–	N/A
cabhCapMappingWanAddrType	lectura-creación	Sí[5]	16
cabhCapMappingWanAddr	lectura-creación	Sí[5]	16
cabhCapMappingWanPort	lectura-creación	Sí[5]	16
cabhCapMappingLanAddrType	lectura-creación	Sí[5]	16
cabhCapMappingLanAddr	lectura-creación	Sí[5]	16
cabhCapMappingLanPort	lectura-creación	Sí[5]	16
cabhCapMappingMethod	sólo lectura	–	N/A
cabhCapMappingProtocol	lectura-creación	Sí[5]	16
cabhCapMappingRowStatus	lectura-creación	Sí	16
cabhCapMappingNumPorts	lectura-creación	Sí	16
cabhCapMappingRowDescr	lectura-creación	Sí	16
cabhCapMappingCreateTime	sólo lectura	No	N/A
cabhCapMappingLastUpdateTime	sólo lectura	No	N/A
cabhCapMappingDuration	lectura-creación	Sí	16
cabhCapMappingRemoteHostAddrType	sólo lectura	No	N/A
CabhCapMappingRemoteHostAddr	sólo lectura	No	N/A
CabhCapMappingEnable	sólo lectura	No	N/A

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
cabhCapPassthroughTable/ cabhCapPassthroughEntry			
cabhCapPassthroughIndex	inaccesible	–	N/A
cabhCapPassthroughMacAddr	lectura-creación	Sí	16
cabhCapPassthroughRowStatus	lectura-creación	Sí	16

[5] Los objetos cabhCapMappingEntry son persistentes si se configuran mediante el NMS y no lo son si se crean dinámicamente en base al tráfico saliente. Véase 8.3.4.4.

cabhCdpMib			
cabhCdpObjects			
cabhCdpBase			
cabhCdpSetToFactory	lectura-escritura	No	N/A
cabhCdpLanTransCurCount	sólo lectura	–	N/A
cabhCdpLanTransThreshold	lectura-escritura	No	N/A
cabhCdpLanTransAction	lectura-escritura	No	N/A
cabhCdpWanDataIpAddrCount	lectura-escritura	No	N/A
cabhCdpLastSetToFactory	sólo lectura		N/A
cabhCdpTimeOffsetSelection	lectura-escritura	Sí	1
cabhCdpSnmpSetTimeOffset	lectura-escritura	Sí	1
cabhCdpDaylightSavingTimeEnable	lectura-escritura	Sí	1
cabhCdpAddr			
cabhCdpLanAddrTable/ cabhCdpLanAddrEntry			
cabhCdpLanAddrIpType	inaccesible	–	N/A
cabhCdpLanAddrIp	inaccesible	–	N/A
cabhCdpLanAddrClientID	lectura-creación	Sí	16
cabhCdpLanAddrLeaseCreateTime	sólo lectura	–	N/A
cabhCdpLanAddrLeaseExpireTime	sólo lectura	–	N/A
cabhCdpLanAddrMethod	sólo lectura	Sí	16
cabhCdpLanAddrHostName	sólo lectura	Sí	16
cabhCdpLanAddrRowStatus	lectura-creación	Sí	16
cabhCdpWanDataAddrTable/ cabhCdpWanDataAddrEntry			
CabhCdpWanDataAddrIndex	inaccesible	–	N/A
CabhCdpWanDataAddrClientId	lectura-creación	No	N/A
CabhCdpWanDataAddrIpType	sólo lectura	–	N/A
CabhCdpWanDataAddrIp	sólo lectura	–	N/A
CabhCdpWanDataAddrRowStatus	lectura-creación	No	N/A
CabhCdpWanDataAddrLeaseCreateTime	sólo lectura	–	N/A
CabhCdpWanDataAddrLeaseExpireTime	sólo lectura	–	N/A

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
cabhCdpWanDnsServerTable/ cabhCdpWanDnsServerEntry			
cabhCdpWanDnsServerOrder	inaccesible	–	N/A
cabhCdpWanDnsServerIpType	sólo lectura	–	N/A
cabhCdpWanDnsServerIp	sólo lectura	–	N/A
cabhCdpServer			
cabhCdpLanPoolStartType	lectura-escritura	Sí	1
cabhCdpLanPoolStart	lectura-escritura	Sí	1
cabhCdpLanPoolEndType	lectura-escritura	Sí	1
cabhCdpLanPoolEnd	lectura-escritura	Sí	1
cabhCdpServerNetworkNumberType	lectura-escritura	Sí	1
cabhCdpServerNetworkNumber	lectura-escritura	Sí	1
cabhCdpServerSubnetMaskType	lectura-escritura	Sí	1
cabhCdpServerSubnetMask	lectura-escritura	Sí	1
cabhCdpServerTimeOffset	lectura-escritura	Sí	1
cabhCdpServerRouterType	lectura-escritura	Sí	1
cabhCdpServerRouter	lectura-escritura	Sí	1
cabhCdpServerDnsAddressType	lectura-escritura	Sí	1
cabhCdpServerDnsAddress	lectura-escritura	Sí	1
cabhCdpServerUseCableDataNwDnsAddr	lectura-escritura	No	N/A
cabhCdpServerSyslogAddressType	lectura-escritura	Sí	1
cabhCdpServerSyslogAddress	lectura-escritura	Sí	1
cabhCdpServerDomainName	lectura-escritura	Sí	1
cabhCdpServerTTL	lectura-escritura	Sí	1
cabhCdpServerInterfaceMTU	lectura-escritura	Sí	1
cabhCdpServerVendorSpecific	lectura-escritura	Sí	1
cabhCdpServerLeaseTime	lectura-escritura	Sí	1
cabhCdpServerDhcpAddressType	sólo lectura	–	N/A
cabhCdpServerDhcpAddress	sólo lectura	–	N/A
cabhCdpServerControl	lectura-escritura	No	N/A
cabhCdpServerCommitStatus	sólo lectura	–	N/A
cabhCtpMib **cabhCtpObjects** **cabhCtpBase**			
cabhCtpSetToFactory	lectura-escritura	No	N/A
cabhCtpLastSetToFactory	sólo lectura	–	N/A

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
cabpCtpConnSpeed			
cabhCtpConnSrcIpType	lectura-escritura	No	N/A
cabhCtpConnSrcIp	lectura-escritura	No	N/A
cabhCtpConnDestIpType	lectura-escritura	No	N/A
cabhCtpConnDestIp	lectura-escritura	No	N/A
cabhCtpConnProto	lectura-escritura	No	N/A
cabhCtpConnNumPkts	lectura-escritura	No	N/A
cabhCtpConnPktSize	lectura-escritura	No	N/A
cabhCtpConnTimeOut	lectura-escritura	No	N/A
cabhCtpConnControl	lectura-escritura	No	N/A
cabhCtpConnStatus	sólo lectura	–	N/A
cabhCtpConnPktsSent	sólo lectura	–	N/A
cabhCtpConnPktsRecv	sólo lectura	–	N/A
cabhCtpConnRTT	sólo lectura	–	N/A
cabhCtpConnThroughput	sólo lectura	–	N/A
cabhCtpPing			
cabhCtpPingSrcIpType	lectura-escritura	No	N/A
cabhCtpPingSrcIp	lectura-escritura	No	N/A
cabhCtpPingDestIpType	lectura-escritura	No	N/A
cabhCtpPingDestIp	lectura-escritura	No	N/A
cabhCtpPingNumPkts	lectura-escritura	No	N/A
cabhCtpPingPktSize	lectura-escritura	No	N/A
cabhCtpPingTimeBetween	lectura-escritura	No	N/A
cabhCtpPingTimeOut	lectura-escritura	No	N/A
cabhCtpPingControl	lectura-escritura	No	N/A
cabhCtpPingStatus	sólo lectura	–	N/A
cabhCtpPingNumSent	sólo lectura	–	N/A
cabhCtpPingNumRecv	sólo lectura	–	N/A
cabhCtpPingAvgRTT	sólo lectura	–	N/A
cabhCtpPingMaxRTT	sólo lectura	–	N/A
cabhCtpPingMinRTT	sólo lectura	–	N/A
cabhCtpPingNumIcmpError	sólo lectura	–	N/A
cabhCtpPingIcmpError	sólo lectura	–	N/A
cabhQos2Mib **cabhQos2MibObjects** **cabhQos2Base**			
cabhQos2SetToFactory	lectura-escritura	No	N/A
cabhQos2LastSetToFactory	sólo lectura	–	N/A

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
cabhQos2PsIfAttributes			
cabhQos2PsIfAttribTable/ cabhQos2PsIfAttribEntry			
cabhQos2PsIfAttribIfNumPriorities	sólo lectura	–	N/A
cabhQosInterfaceAttribIfNumQueues	sólo lectura	–	N/A
cabhQos2PolicyHolderObjects			
cabhQos2PolicyHolderEnabled	lectura-escritura	Sí	1
cabhQos2PolicyAdmissionControl	lectura-escritura	Sí	1
cabhQos2NumActivePolicyHolder	sólo lectura	–	N/A
cabhQos2PolicyTable/ cabhQos2PolicyEntry			
cabhQos2PolicyOwner	inaccesible	–	N/A
cabhQos2PolicyOwnerRuleId	inaccesible	–	N/A
cabhQos2PolicyRuleOrder	lectura-creación	Sí	32
cabhQos2PolicyAppDomain	lectura-creación	Sí	32
cabhQos2PolicyAppName	lectura-creación	Sí	32
cabhQos2PolicyServiceProvDomain	lectura-creación	Sí	32
cabhQos2PolicyServiceName	lectura-creación	Sí	32
cabhQos2PolicyPortDomain	lectura-creación	Sí	32
cabhQos2PolicyPortNumber	lectura-creación	Sí	32
cabhQos2PolicyIpProtocol	lectura-creación	Sí	32
cabhQos2PolicyIpType	lectura-creación	Sí	32
cabhQos2PolicySrcIp	lectura-creación	Sí	32
cabhQos2PolicyDestIp	lectura-creación	Sí	32
cabhQos2PolicySrcPort	lectura-creación	Sí	32
cabhQos2PolicyDestPort	lectura-creación	Sí	32
cabhQos2PolicyTraffImpNum	lectura-creación	Sí	32
cabhQos2PolicyUserImportance	lectura-creación	Sí	32
cabhQos2PolicyRowStatus	lectura-creación	Sí	32
cabhQos2DeviceObjects			
cabhQos2TrafficClassTable/ cabhQos2TrafficClassEntry			
cabhQos2TrafficClassMethod	inaccesible	–	N/A
cabhQos2TrafficClassIdx	inaccesible	–	N/A
cabhQos2TrafficClassProtocol	lectura-creación	–	N/A
cabhQos2TrafficClassIpType	lectura-creación	–	N/A
cabhQos2TrafficClassSrcIp	lectura-creación	–	N/A
cabhQos2TrafficClassDestIp	lectura-creación	–	N/A
cabhQos2TrafficClassSrcPort	lectura-creación	–	N/A

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
cabhQos2TrafficClassDestPort	lectura-creación	–	N/A
cabhQos2TrafficClassImpNum	lectura-creación	–	N/A
cabhQos2TrafficClassRowStatus	lectura-creación	–	N/A
experimental **snmpUSMDHObjectsMIB [RFC 2786]** **usmDHKeyObjects** **usmDHPublicObjects**			
usmDHParamaters	lectura-escritura	No	N/A
usmDHUserKeyTable/ *usmDHUserKeyEntry*			
usmDHUserAuthKeyChange	lectura-creación	No	N/A
usmDHUserOwnAuthKeyChange	lectura-creación	No	N/A
usmDHUserPrivKeyChange	lectura-creación	No	N/A
usmDHUserOwnPrivKeyChange	lectura-creación	No	N/A
usmDHKickstartGroup			
usmDHKickstartTable/ *usmDHKickstartEntry*			
usmDHKickstartIndex	inaccesible	–	N/A
usmDHKickstartMyPublic	sólo lectura	–	N/A
usmDHKickstartMgrPublic	sólo lectura	–	N/A
usmDHKickstartSecurityName	sólo lectura	–	N/A
snmpV2 **snmpModules** **snmpMIB** **snmpMIBObjects** **snmpSet**			
snmpSetSerialNo	lectura-escritura	No	N/A
snmpFrameworkMIB [RFC 3411] **snmpEngine**			
snmpEngineID	sólo lectura	Sí	1
snmpEngineBoots	sólo lectura	Sí	1
snmpEngineTime	sólo lectura	–	N/A
snmpEngineMaxMessageSize	sólo lectura	–	N/A
snmpMPDMIB [RFC 3412] **snmpMPDObjects** **snmpMPDStats**			
snmpUnknownSecurityModels	sólo lectura	–	N/A
snmpInvalidMsgs	sólo lectura	–	N/A
snmpUnknownPDUHandlers	sólo lectura	–	N/A

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
snmpTargetMIB [RFC 3413] **snmpTargetObjects**			
snmpTargetSpinLock	lectura-escritura	No	N/A
snmpTargetAddrTable/ *snmpTargetAddrEntry*			
snmpTargetAddrName	inaccesible	–	N/A
snmpTargetAddrTDomain	lectura-creación	No	N/A
snmpTargetAddrTAddress	lectura-creación	No	N/A
snmpTargetAddrTimeout	lectura-creación	No	N/A
snmpTargetAddrRetryCount	lectura-creación	No	N/A
snmpTargetAddrTagList	lectura-creación	No	N/A
snmpTargetAddrParams	lectura-creación	No	N/A
snmpTargetAddrStorageType	lectura-creación	No	N/A
snmpTargetAddrRowStatus	lectura-creación	No	N/A
snmpTargetParamsTable/ *snmpTargetParamsEntry*			
snmpTargetParamsName	inaccesible	–	N/A
snmpTargetParamsMPModel	lectura-creación	No	N/A
snmpTargetParamsSecurityModel	lectura-creación	No	N/A
snmpTargetParamsSecurityName	lectura-creación	No	N/A
snmpTargetParamsSecurityLevel	lectura-creación	No	N/A
snmpTargetParamsStorageType	lectura-creación	No	N/A
snmpTargetParamsRowStatus	lectura-creación	No	N/A
snmpUnavailableContexts	sólo lectura	–	N/A
snmpUnknownContexts	sólo lectura	–	N/A
snmpNotificationMIB [RFC 3413] **snmpNotifyObjects**			
snmpNotifyTable/ *snmpNotifyEntry*			
snmpNotifyName	inaccesible	–	N/A
snmpNotifyTag	lectura-creación	No	N/A
snmpNotifyType	lectura-creación	No	N/A
snmpNotifyStorageType	lectura-creación	No	N/A
snmpNotifyRowStatus	lectura-creación	No	N/A
snmpNotifyFilterProfileTable/ *snmpNotifyFilterProfileEntry*			
snmpNotifyFilterProfileName	lectura-creación	No	N/A
snmpNotifyFilterProfileStorType	lectura-creación	No	N/A
snmpNotifyFilterProfileRowStatus	lectura-creación	No	N/A

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
snmpNotifyFilterTable/ snmpNotifyFilterEntry			
snmpNotifyFilterSubtree	inaccesible	–	N/A
snmpNotifyFilterMask	lectura-creación	No	N/A
snmpNotifyFilterType	lectura-creación	No	N/A
snmpNotifyFilterStorageType	lectura-creación	No	N/A
snmpNotifyFilterRowStatus	lectura-creación	No	N/A
snmpUsmMIB [RFC 3414] **usmStats**			
usmStatsUnsupportedSecLevels	sólo lectura	–	N/A
usmStatsNotInTimeWindows	sólo lectura	–	N/A
usmStatsUnknownUserNames	sólo lectura	–	N/A
usmStatsUnknownEngineIDs	sólo lectura	–	N/A
usmStatsWrongDigests	sólo lectura	–	N/A
usmStatsDecryptionErrors	sólo lectura	–	N/A
usmUser			
usmUserSpinLock	lectura-escritura	No	N/A
usmUserTable/ usmUserEntry			
usmUserEngineID	inaccesible	–	N/A
usmUserName	inaccesible	–	N/A
usmUserSecurityName	sólo lectura	–	N/A
usmUserCloneFrom	lectura-creación	No	N/A
usmUserAuthProtocol	lectura-creación	No	N/A
usmUserAuthKeyChange	lectura-creación	No	N/A
usmUserOwnAuthKeyChange	lectura-creación	No	N/A
usmUserPrivProtocol	lectura-creación	No	N/A
usmUserPrivKeyChange	lectura-creación	No	N/A
usmUserOwnPrivKeyChange	lectura-creación	No	N/A
usmUserPublic	lectura-creación	No	N/A
usmUserStorageType	lectura-creación	No	N/A
usmUserStatus	lectura-creación	No	N/A
SNMP-VIEW-BASED-ACM-MIB [RFC 3415] **snmpVacmMIB** **vacmMIBObjects**			
vacmContextTable/ vacmContextEntry			
vacmContextName	sólo lectura	–	N/A

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
vacmSecurityToGroupTable/ vacmSecurityToGroupEntry			
vacmSecurityModel	inaccesible	–	N/A
vacmSecurityName	inaccesible	–	N/A
vacmGroupName	lectura-creación	No	N/A
vacmSecurityToGroupStorageType	lectura-creación	No	N/A
vacmSecurityToGroupStatus	lectura-creación	No	N/A
vacmAccessTable/ vacmAccessEntry			
vacmAccessContextPrefix	inaccesible	–	N/A
vacmAccessSecurityModel	inaccesible	–	N/A
vacmAccessSecurityLevel	inaccesible	–	N/A
vacmAccessContextMatch	lectura-creación	No	N/A
vacmAccessReadViewName	lectura-creación	No	N/A
vacmAccessWriteViewName	lectura-creación	No	N/A
vacmAccessNotifyViewName	lectura-creación	No	N/A
vacmAccessStorageType	lectura-creación	No	N/A
vacmAccessStatus	lectura-creación	No	N/A
vacmMIBViews			
vacmViewSpinLock	lectura-escritura	No	N/A
vacmViewTreeFamilyTable/ vacmViewTreeFamilyEntry			
vacmViewTreeFamilyViewName	inaccesible	–	N/A
vacmViewTreeFamilySubtree	inaccesible	–	N/A
vacmViewTreeFamilyMask	lectura-creación	No	N/A
vacmViewTreeFamilyType	lectura-creación	No	N/A
vacmViewTreeFamilyStorageType	lectura-creación	No	N/A
vacmViewTreeFamilyStatus	lectura-creación	No	N/A
snmpCommunityMIB [RFC 3584] snmpCommunityMIBObjects			
snmpCommunityTable/ snmpCommunityEntry			
snmpCommunityIndex	inaccesible	–	N/A
snmpCommunityName	lectura-creación	No	N/A
snmpCommunitySecurityName	lectura-creación	No	N/A
snmpCommunityContextEngineID	lectura-creación	No	N/A
snmpCommunityContextName	lectura-creación	No	N/A
snmpCommunityTransportTag	lectura-creación	No	N/A
snmpCommunityStorageType	lectura-creación	No	N/A
snmpCommunityStatus	lectura-creación	No	N/A

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.° de anotaciones persistentes
snmpTargetAddrExtTable/ snmpTargetAddrExtEntry			
snmpTargetAddrTMask	lectura-creación	No	N/A
snmpTargetAddrMMS	lectura-creación	No	N/A
clabSecCertObject			
clabSrvcPrvdrRootCACert	sólo lectura	–	N/A
clabCVCRootCACert	sólo lectura	–	N/A
clabCVCCACert	sólo lectura	–	N/A
clabMfgCACert	sólo lectura	–	N/A

Anexo B

Formato y contenido de eventos, SYSLOG y trampas SNMP

El cuadro B.1 resume el formato y el contenido de las anotaciones históricas locales de eventos, de los mensajes syslog y de las trampas SNMP (SNMP Traps).

Cada fila en el cuadro especifica un evento que el PS puede generar. El PS ha de comunicar estos eventos por cualquiera de los tres medios siguientes o por todos ellos: anotación histórica local de los eventos implementada por el cuadro local de eventos de [RFC 2669], SYSLOG y SNMP Trap. El formato SYSLOG se especifica en 6.3.3.2.4.4 y el formato de SNMP trap se define en el presente anexo según se indica en el cuadro B.1.

En la primera y segunda columnas del cuadro B.1 se indica la fase en que se produce el evento. La tercera columna indica la prioridad asignada al evento. Estas prioridades coinciden con las comunicadas en el objeto docsDevEvLevel de [RFC 2669] y en el campo LEVEL del mensaje SYSLOG.

La cuarta columna especifica el texto del evento, que se comunica en el objeto docsDevEvText de [RFC 2669] y el campo de texto del mensaje SYSLOG. La quinta columna proporciona información adicional sobre el texto del evento de la cuarta columna. Por ejemplo, algunos de los campos de texto del evento son constantes mientras que otros contienen información variable. Algunas de las variables sólo son necesarias en el SYSLOG, tal como se describe en la quinta columna. La sexta columna especifica el conjunto de códigos de error.

La séptima columna indica un número único de identificación del evento, que se asigna al objeto docsDevEvId y al campo <eventId> del mensaje syslog. La octava columna especifica la trampa SNMP, que notifica este evento al receptor de eventos SNMP.

Las reglas para generar un ID único de evento partiendo del código de error se describen en 6.3.3.2.4.4. Los ID de eventos del cuadro se expresan en formato decimal.

Para ilustrar más adecuadamente el cuadro, se presenta a continuación un ejemplo que utiliza la primera fila de la cláusula de eventos de actualización del software.

La primera y segunda columnas son "Actualización del SW" e " INICIO DE ACTUALIZACIÓN DEL SW". La prioridad del evento es "Notificación". El texto del evento es "INICIO de descarga del software – Mediante NMS". La quinta columna contiene "Únicamente para SYSLOG, añadir: dirección MAC: <P1> P1 = dirección MAC del PS". Esto es una nota sobre SYSLOG. Es decir, el cuerpo del texto del syslog sería "INICIO de descarga del software – Mediante NMS – dirección MAC: x1 x2 x3 x4 x5 x6".

La última columna "Nombre de la trampa" es cabhPsDevSwUpgradeInitTrap, cuyo formato se proporciona al final del presente anexo.

B.1 Descripción de las trampas

Todas las trampas se describen en la especificación de la MIB DEV del PS [anexo E.4].

Cuadro B.1/J.192 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de error	ID del evento	Nombre de la trampa
Errores DHCP antes de completar la configuración							
Inicio	CDC	Crítica	FALLÓ DHCP – Enviada determinación (Discover), no se recibe oferta		D01.0	68000100	
Inicio	CDC	Crítica	FALLÓ DHCP – Enviada petición (Request), no hay respuesta		D02.0	68000200	
Inicio	CDC	Crítica	FALLÓ DHCP – Información solicitada no soportada		D03.0	68000300	
Inicio	CDC	Error	ERROR DE DHCP – La respuesta no contiene TODOS los campos válidos O el PS no puede determinar el modo de configuración		D03.1	68000301	
Inicio	CDC	Alarma	ERROR de DHCP – El PS no pudo obtener todas las direcciones IP de WAN-Data para las que estaba configurado		P02.0	68000302	cabhPsDevCdpWanDataIpTrap
Errores de ToD antes de completar la configuración							
Inicio	ToD	Alarma	Enviada petición ToD – No se recibe respuesta Dirección del servidor de hora + <P1>	P1 = dirección IP del servidor hora del día	D04.1	68000401	cabhPsDevInitTrap
Inicio	ToD	Alarma	Recibida respuesta ToD – Formato de datos no válido Dirección del servidor de hora + <P1>	P1 = dirección IP del servidor hora del día	D04.2	68000402	cabhPsDevInitTrap

Cuadro B.1/J.192 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de error	ID del evento	Nombre de la trampa
Errores TFTP antes de completar la configuración							
Inicio	TFTP	Error	Falló TFTP – Enviada petición – No hay respuesta		D05.0	68000500	cabhPsDevInitTrap (La trampa es importante sólo para el modo de configuración SNMP.)
Inicio	TFTP	Error	Falló TFTP – NO ENCONTRADO el fichero de configuración	Únicamente para SYSLOG: añadir: nombre del fichero = <P1> P1 = nombre del fichero solicitado	D06.0	68000600	cabhPsDevInitTrap (La trampa es importante sólo para el modo de configuración SNMP.)
Inicio	TFTP	Error	Falló TFTP – Paquetes desordenados		D07.0	68000700	cabhPsDevInitTrap (La trampa es importante sólo para el modo de configuración SNMP.)
Inicio	TFTP	Error	Fichero TFTP completo – Pero falló la verificación del troceo SHA-1	Únicamente para SYSLOG: añadir: nombre del fichero = <P1> P1 = nombre del fichero TFTP	D08.0	68000800	cabhPsDevInitTrap (La trampa es importante sólo para el modo de configuración SNMP.)
Inicio	TFTP	Error	Falló TFTP – Sobrepasado el número máximo de reintentos	Únicamente para SYSLOG: añadir: número máximo de reintentos permitidos = <P1> P1 = número máximo de reintentos	D09.0	68000900	cabhPsDevInitTrap (La trampa es importante sólo para el modo de configuración SNMP.)

Cuadro B.1/J.192 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de error	ID del evento	Nombre de la trampa
TFTP exitoso							
Inicio	TFTP	Notificación	TFTP exitoso		D10.0	68001000	
TLS							
Inicio	TCP/IP	Crítica	Falló el PS al tratar de conectarse al servidor HTTP/TLS en su intento de descargar el fichero de configuración <P1>	P1 = 'PS' o 'barrera contra fuegos'	D20.0	68002000	
Inicio	TLS	Crítica	Expiró el temporizador de la conexión TLS y se excedió el número máximo de reintentos de descarga del fichero de configuración <P1>	P1 = 'PS' o 'barrera contra fuegos'	D21.0	68002100	
Inicio	TLS	Crítica	ERROR GRAVE del TLS <P1>, en su intento de descargar el fichero de configuración <P2>	P1 = Código de Error conforme a [RFC 2246] P2 = 'PS' o 'barrera contra fuegos'	D22.0	68002200	
HTTP							
Inicio	HTTP	Crítica	Falló la descarga del fichero de configuración, pero se efectúan reintentos. Error de HTTP. <P1>, en su intento de descargar el fichero de configuración <P2>	P1 = Códigos de estado conformes a [RFC 2616] P2 = 'PS' o 'barrera contra fuegos'	D30.0	68003000	

Cuadro B.1/J.192 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de error	ID del evento	Nombre de la trampa
Inicio	HTTP	Crítica	Falló la descarga del fichero de configuración. Debido a que expira el temporizador de la conexión y al número máximo de reintentos. Se abortó la operación, en su intento de descargar el fichero de configuración <P1>	P1 = 'PS' o 'barrera contra fuegos'	D31.0	68003100	
Inicio	HTTP	Crítica	Se completó con éxito la descarga segura del fichero de configuración, en su intento de descargar el fichero de configuración <P1>	P1 = 'PS' o 'barrera contra fuegos'	D32.0	68003200	
Análisis sintáctico TLV							
Inicio	ANALISIS SINTACTICO DE TLV	Alarma	TLV-27 o TLV-28 – OID no reconocido, en su intento de descargar el fichero de configuración <P1>	P1 = 'PS' o 'barrera contra fuegos'	I401.0	73040100	cabhPsDevInitTLV Unk nownTrap
Inicio	ANALISIS SINTACTICO DE TLV	Alarma	TLV desconocida	Únicamente para SYSLOG: TLV del fichero de configuración <P2> es <P1>, P1 = el TLV completo en hexadecimal P2 = 'PS' o 'barrera contra fuegos'	I401.1	73040101	cabhPsDevInitTLV Unk nownTrap

Cuadro B.1/J.192 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de error	ID del evento	Nombre de la trampa
Inicio	ANALISIS SINTACTICO DE TLV	Error	Formato o contenido TLV no válido	Únicamente para SYSLOG, añadir: TLV del fichero de configuración <P2> es <P1>, P1+= el TLV completo en hexadecimal P2 = 'PS' o 'barrera contra fuegos'	I401.2	73040102	
Configuración							
Inicio	Conclusión de configuración	Notificación	Conclusión de configuración	Únicamente para SYSLOG, añadir dirección MAC: <P1>. P1 = dirección MAC del PS	I11.0	73001100	cabhPsDevInitTrap
INICIO DE ACTUALIZACIÓN DEL SW (nota)							
Actualización del SW	INICIO DE ACTUALIZACIÓN DEL SW	Notificación	INICIO de descarga del software – Mediante NMS	Únicamente para SYSLOG, añadir: fichero de software: <P1> − Servidor de software: <P2>. P1 = nombre del fichero de software y P2 = dirección IP del servidor Tftp	E101.0	69010100	cabhPsDevSwUpgrade InitTrap
Actualización del SW	INICIO DE ACTUALIZA-CIÓN DEL SW	Notificación	INICIO de descarga de software – Mediante fichero de configuración <P1>	P1 = nombre del fichero de configuración del CM. Únicamente para SYSLOG, añadir: fichero de software: <P2> − Servidor de software: <P3>. P2 = nombre del fichero de software y P3 = dirección IP del servidor Tftp	E102.0	69010200	cabhPsDev SwUpgrade InitTrap

Cuadro B.1/J.192 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de error	ID del evento	Nombre de la trampa
FALLO GENERAL DE LA ACTUALIZACIÓN DEL SW (nota)							
Actualización del SW	FALLO GENERAL DE LA ACTUALI-ZACIÓN DEL SW	Error	Actualización de software fallida durante descarga – Superado máximo de reintentos (3)	Únicamente para SYSLOG, añadir: fichero de software: <P1> − Servidor de software: <P2>. P1 = nombre del fichero de software y P2 = dirección IP del servidor Tftp	E103.0	69010300	cabhPsDevSwUpgrade FailTrap
Actualización del SW	FALLO GENERAL DE LA ACTUALI-ZACIÓN DEL SW	Error	Actualización de software fallida antes de la descarga – Servidor ausente	Únicamente para SYSLOG, añadir: fichero de software: <P1> − Servidor de software: <P2>. P1 = nombre del fichero de software y P2 = dirección IP del servidor Tftp	E104.0	69010400	cabhPsDevSwUpgrade FailTrap
Actualización del SW	FALLO GENERAL DE LA ACTUALI-ZACIÓN DEL SW	Error	Actualización de software fallida antes de la descarga – Fichero ausente	Únicamente para SYSLOG, añadir: fichero de software: <P1> – Servidor de software: <P2>. P1 = nombre del fichero de software y P2 = dirección IP del servidor TFTP	E105.0	69010500	cabhPsDevSwUpgrade FailTrap
Actualización del SW	FALLO GENERAL DE LA ACTUALI-ZACIÓN DEL SW	Error	Actualización de software fallida antes de la descarga – Sobrepasado el número máximo de reintentos TFTP	Únicamente para SYSLOG, añadir: fichero de software: <P1> – Servidor de software: <P2>. P1 = nombre del fichero de software y P2 = dirección IP del servidor TFTP	E106.0	69010600	cabhPsDevSwUpgrade FailTrap

Cuadro B.1/J.192 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de error	ID del evento	Nombre de la trampa
Actualización del SW	FALLO GENERAL DE LA ACTUALI-ZACIÓN DEL SW	Error	Actualización de software fallida tras descarga – Fichero de software incompatible	Únicamente para SYSLOG, añadir: fichero de software: <P1> − Servidor de software: <P2>. P1 = nombre del fichero de software y P2 = dirección IP del servidor Tftp	E107.0	69010700	cabhPsDevSwUpgrade FailTrap
Actualización del SW	FALLO GENERAL DE LA ACTUALI-ZACIÓN DEL SW	Error	Actualización de software fallida tras descarga – Fichero de software corrompido	Únicamente para SYSLOG, añadir: fichero de software: <P1> – Servidor de software: <P2>. P1 = nombre del fichero de software y P2 = dirección IP del servidor TFTP	E108.0	69010800	cabhPsDevSwUpgrade FailTrap
Actualización del SW	FALLO GENERAL DE LA ACTUALI-ZACIÓN DEL SW	Error	Interrupción de la descarga de software – Fallo de la alimentación	Únicamente para SYSLOG, añadir: fichero de software: <P1> – servidor de software: <P2>. P1 = nombre del fichero de software y P2 = dirección IP del servidor Tftp	E109.0	69010900	cabhPsDevSwUpgrade FailTrap
ÉXITO DE LA ACTUALIZACIÓN DEL SW (nota)							
Actualización del SW	ÉXITO DE LA ACTUALIZA-CIÓN DEL SW	Notificación	Éxito del software descargado mediante NMS	Únicamente para SYSLOG, añadir: fichero de software: <P1> – Servidor de software: <P2>. P1 = nombre del fichero de software y P2 = dirección IP del servidor Tftp	E111.0	69011100	cabhPsDevSwUpgrade SuccessTrap

Cuadro B.1/J.192 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de error	ID del evento	Nombre de la trampa
Actualización del SW	ÉXITO DE LA ACTUALIZA-CIÓN DEL SW	Notificación	Éxito del software descargado mediante fichero de configuración	Únicamente para SYSLOG, añadir: fichero de software: <P1> – Servidor de software: <P2>. P1 = nombre del fichero de software y P2 = dirección IP del servidor Tftp	E112.0	69011200	cabhPsDevSwUpgrade SuccessTrap
Fallo del DHCP tras completarse la configuración							
DHCP	CDC	Error	Enviado DHCP RENEW – Sin respuesta		D101.0	68010100	cabhPsDevDHCPFail Trap
DHCP	CDC	Error	Enviado DHCP REBIND – Sin respuesta		D102.0	68010200	cabhPsDevDHCPFail Trap
DHCP	CDC	Error	Enviado DHCP RENEW – Opción DHCP no válida		D103.0	68010300	cabhPsDevDHCPFail Trap
DHCP	CDC	Error	Enviado DHCP REBIND – Opción DHCP no válida		D104.0	68010400	cabhPsDevDHCPFail Trap
Fallo de ToD tras completarse la configuración							
ToD	ToD	Alarma	Petición ToD enviada – No se recibe respuesta		D04.3	68000403	cabhPsDevTODFailTrap
ToD	ToD	Alarma	Respuesta ToD recibida – Formato de datos no válido		D04.4	68000404	cabhPsDevTODFail Trap

Cuadro B.1/J.192 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de error	ID del evento	Nombre de la trampa
Verificación del fichero de código							
Actualización del SW	FALLO GENERAL DE LA ACTUALI-ZACIÓN DEL SW	Error	Controles del fichero de código inadecuados	Únicamente para SYSLOG, añadir: fichero de código: <P1> – Servidor del fichero de código: <P2>. P1 = nombre del fichero de código, P2 = dirección IP del servidor del fichero de código	E201.0	69020100	cabhPsDevSwUpgrade FailTrap
Actualización del SW	FALLO GENERAL DE LA ACTUALI-ZACIÓN DEL SW	Error	Fallo en la validación CVC del fabricante del fichero de código	Únicamente para SYSLOG, añadir: fichero de código: <P1> – Servidor del fichero de código: <P2>. P1 = nombre del fichero de código, P2 = dirección IP del servidor del fichero de código	E202.0	69020200	cabhPsDevSwUpgrade FailTrap
Actualización del SW	FALLO GENERAL DE LA ACTUALI-ZACIÓN DEL SW	Error	Fallo en la validación CVS del fabricante del fichero de código	Únicamente para SYSLOG, añadir: fichero de código: <P1> – Servidor del fichero de código: <P2>. P1 = nombre del fichero de código, P2 = dirección IP del servidor del fichero de código	E203.0	69020300	cabhPsDevSwUpgrade FailTrap

Cuadro B.1/J.192 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de error	ID del evento	Nombre de la trampa
Actualización del SW	FALLO GENERAL DE LA ACTUALI-ZACIÓN DEL SW	Error	Fallo en la validación CVC del cofirmante del fichero de código	Únicamente para SYSLOG, añadir: fichero de código: <P1> – servidor del fichero de código: <P2>. P1 = nombre del fichero de código, P2 = dirección IP del servidor del fichero de código	E204.0	69020400	cabhPsDevSwUpgrade FailTrap
Actualización del SW	FALLO GENERAL DE LA ACTUALI-ZACIÓN DEL SW	Error	Fallo en la validación CVS del cofirmante del fichero de código	Únicamente para SYSLOG, añadir: fichero de código: <P1> – servidor del fichero de código: <P2>. P1 = nombre del fichero de código, P2 = dirección IP del servidor del fichero de código	E205.0	69020500	cabhPsDevSwUpgrade FailTrap
Verificación del CVC							
Actualización del SW	VERIFICACIÓN DEL CVC	Error	Formato CVC del fichero de configuración inadecuado – Servidor TFTP: <P1> – Fichero de configuración: <P2>	P1 = dirección IP del servidor TFTP P2 = nombre del fichero de configuración	E206.0	69020600	cabhPsDevSwUpgrade CVCFailTrap
Actualización del SW	VERIFICACIÓN DEL CVC	Error	Fallo en la validación CVC del fichero de configuración – Servidor TFTP: <P1> – Fichero de configuración: <P2>	P1 = dirección IP del servidor TFTP P2 = nombre del fichero de configuración	E207.0	69020700	cabhPsDevSwUpgrade CVCFailTrap
Actualización del SW	VERIFICACIÓN DEL CVC	Error	Formato SNMP CVC inadecuado – Gestor Snmp: <P1>	P1 = dirección IP del gestor SNMP	E208.0	69020800	cabhPsDevSwUpgrade CVCFailTrap

Cuadro B.1/J.192 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de error	ID del evento	Nombre de la trampa
Actualización del SW	VERIFICACIÓN DEL CVC	Error	Fallo en la validación CVC de SNMP – Gestor de Snmp: <P1>	P1 = dirección IP del gestor SNMP	E209.0	69020900	cabhPsDevSwUpgrade CVCFailTrap
Eventos del CDP							
CDP	CDS	Notificación	Intento de asignar más direcciones IP LAN TRANS de las permitidas		P01.0	80000100	cabhPsDevCDP ThresholdTrap
CDP	CDS	Notificación	No pudo suministrar el cliente de LAN DHCP – Se agotó el conjunto de direcciones IP		P03.0	80000300	cabhPsDevCdpLanIp PoolTrap
Eventos del CSP							
CSP	Barrera contra fuegos	Notificación	Cambio de estado de cabhSec2FwEventEnable para el Tipo 1. El nuevo valor es <P1>.	P1 = valor de cabhSec2FwEventType Enable para el Tipo 1	P101.1	80010101	cabhPsDevCSPTrap
CSP	Barrera contra fuegos	Notificación	Cambio de estado de cabhSec2FwEventEnable para el Tipo 2. El nuevo valor es <P1>.	P1 = valor de cabhSecFwEventType Enable para el Tipo 2	P101.2	80010102	cabhPsDevCSPTrap
CSP	Barrera contra fuegos	Notificación	Cambio de estado de cabhSec2FwEventEnable para el Tipo 3. El nuevo valor es <P1>.	P1 = valor de cabhSecFwEventType Enable para el Tipo 3	P101.3	80010103	cabhPsDevCSPTrap
CSP	Barrera contra fuegos	Notificación	Cambio de estado de cabhSec2FwEventEnable para el Tipo 4. El nuevo valor es <P1>.	P1 = valor de cabhSecFwEventType Enable para el Tipo 4	P101.4	80010104	cabhPsDevCSPTrap

Cuadro B.1/J.192 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de error	ID del evento	Nombre de la trampa
CSP	Barrera contra fuegos	Notificación	Cambio de estado de cabhSec2FwEventEnable para el Tipo 5. El nuevo valor es <P1>.	P1 = valor de cabhSecFwEventType Enable para el Tipo 5	P101.5	80010105	cabhPsDevCSPTrap
CSP	Barrera contra fuegos	Notificación	Cambio de estado de cabhSec2FwEventEnable para el Tipo 6. El nuevo valor es <P1>.	P1 = valor de cabhSecFwEventType Enable para el Tipo 6	P101.6	80010106	cabhPsDevCSPTrap
CSP	Barrera contra fuegos	Alarma	Se alcanzó el umbral de los eventos de la barrera contra fuegos tipo 1		P102.1	80010201	cabhPsDevCSPTrap
CSP	Barrera contra fuegos	Alarma	Se alcanzó el umbral de los eventos de la barrera contra fuegos tipo 2		P102.2	80010202	cabhPsDevCSPTrap
CSP	Barrera contra fuegos	Alarma	Se alcanzó el umbral de los eventos de la barrera contra fuegos tipo 3		P102.3	80010203	cabhPsDevCSPTrap
CSP	Barrera contra fuegos	Alarma	Se alcanzó el umbral de los eventos de la barrera contra fuegos tipo 4. Falló la fijación de <P1>. <P2>	P1 = se intentó modificar el objeto MIB (por ejemplo, cabhSec2FwPolicyFile URL) P2 = descripción textual del fallo	P102.4	80010204	cabhPsDevCSPTrap
CSP	Barrera contra fuegos	Alarma	Se alcanzó el umbral de los eventos de la barrera contra fuegos tipo 5		P102.5	80010205	cabhPsDevCSPTrap
CSP	Barrera contra fuegos	Alarma	Se alcanzó el umbral de los eventos de la barrera contra fuegos tipo 6		P102.6	80010206	cabhPsDevCSPTrap

Cuadro B.1/J.192 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de error	ID del evento	Nombre de la trampa
CSP	TFTP de la barrera contra fuegos	Crítica	Fracasó la descarga TFTP del fichero de políticas de la barrera contra fuegos: Se envió la petición y no se recibió respuesta. URL del fichero de política: <P1>	P1 = se solicitó el URL del fichero de políticas de la barrera contra fuegos	P130.0	80013000	cabhPsDevCSPTrap
CSP	TFTP de la barrera contra fuegos	Crítica	Fracaso de TFTP – No se encontró el fichero de políticas de barrera contra fuegos. URL del fichero de política: <P1>	P1 = se solicitó el URL del fichero de políticas de la barrera contra fuegos	P131.0	80013100	cabhPsDevCSPTrap
CSP	TFTP de la barrera contra fuegos	Crítica	Fracaso de TFTP – Fichero de políticas de la barrera contra fuegos no válido. URL del fichero de política: <P1>	P1 = se solicitó el URL de políticas de la barrera contra fuegos	P132.0	80013200	cabhPsDevCSPTrap
CSP	TFTP de la barrera contra fuegos	Crítica	Se completó la descarga del fichero de políticas de barrera contra fuegos pero fracasó la verificación de la generación SHA-1. URL del fichero de política: <P1> Hash: <P2>	P1 = se solicitó el URL del fichero de políticas de la barrera contra fuegos, P2 = valor del fichero de políticas de la barrera contra fuegos	P133.0	80013300	cabhPsDevCSPTrap
CSP	TFTP de la barrera contra fuegos	Crítica	La descarga del fichero de políticas de la barrera contra fuegos excedió el número máximo permitido de reintentos de TFTP. URL del fichero de política: <P1>	P1 = se solicitó el URL del fichero de políticas de la barrera contra fuegos	P134.0	80013400	cabhPsDevCSPTrap

Cuadro B.1/J.192 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de error	ID del evento	Nombre de la trampa
CSP	TFTP de la barrera contra fuegos	Notificación	La descarga TFTP del fichero de políticas de la barrera contra fuegos se completó con éxito. Fichero de política URL: <P1>	P1 = se solicitó el URL del fichero de políticas de la barrera contra fuegos Únicamente para SYSLOG: añadir: número máximo permitido de reintentos = <P2> P2 = número máximo permitido de reintentos	P135.0	80013500	cabhPsDevCSPTrap
Eventos de CAP							
CAP	C-NAT	Alarma	El CAP no puede establecer la correspondencia de C-NAT. No hay ninguna dirección IP de WAN-data disponible		P201.0	80020100	cabhPsDevCAPTrap
CAP	C-NAPT	Alarma	El CAP no puede establecer la correspondencia de C-NAT. No hay ninguna dirección IP de WAN-data disponible		P250.0	80025000	cabhPsDevCAPTrap
Eventos de CTP							
CTP	Herramienta de la velocidad de la conexión	Notificación	La prueba de la herramienta de velocidad de la conexión se completó satisfactoriamente. IP de origen: <P1>. IP de destino: <P2>. Protocolo: <P3>. Caudal: <P4>.	P1 = dirección IP del origen P2 = dirección IP del destino P3 = protocolo P4 = caudal	P301.0	80030100	cabhPsDevCtpTrap

Cuadro B.1/J.192 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de error	ID del evento	Nombre de la trampa
Eventos de CTP							
CTP	Herramienta de velocidad de la conexión	Notificación	La prueba de la herramienta de velocidad de la conexión alcanzó el fin de la temporización. IP de origen: <P1>. IP de destino: <P2>. Protocolo: <P3>. Valor del temporizador: <P4> ms.	P1 = dirección IP del origen P2 = dirección IP del destino P3 = protocolo (valor de cabhCtpConnProto) P4 = valor del temporizador que mide el tiempo de ejecución de la herramienta de velocidad de conexión (ms) (Referencia: claúsula Requisitos de la función herramienta de velocidad de la conexión)	P302.0	80030200	cabhPsDevCtpTrap
CTP	Herramienta de velocidad de la conexión	Notificación	Se abortó la prueba de la herramienta de velocidad de la conexión. IP de origen: <P1>. IP de destino: <P2>. Protocolo: <P3>. Valor del temporizador: <P4> ms	P1 = dirección IP del origen P2 = dirección IP del destino P3 = protocolo (valor de cabhCtpConnProto) P4 = valor del temporizador que mide el tiempo de ejecución de la herramienta de velocidad de conexión (ms). (Referencia: cláusula Requisitos de la función herramienta de velocidad de la conexión)	P303.0	80030300	cabhPsDevCtpTrap

Cuadro B.1/J.192 – Eventos definidos para IPCable2Home

Proceso	Subproceso	Prioridad del PS	Texto del evento	Notas y detalles del mensaje	Conjunto de códigos de error	ID del evento	Nombre de la trampa
CTP	Herramienta Ping	Notificación	Se completó satisfactoriamente la prueba de la herramienta Ping. IP de origen: <P1>. IP de destino: <P2>. Tiempo promedio de ida y vuelta: <P3>ms.	P1 = dirección IP del origen P2 = dirección IP del destino P3 = tiempo promedio de ida y vuelta	P320.0	80032000	cabhPsDevCtpTrap
CTP	Herramienta Ping	Notificación	La prueba de la herramienta Ping alcanzó el fin de temporización. IP de origen: <P1>. IP de destino: <P2>. Número de peticiones: <P3>. Número de respuestas <P4>.	P1 = dirección IP del origen P2 = dirección IP del destino P3 = número de peticiones enviadas P4 = número de respuestas recibidas	P321.0	80032100	cabhPsDevCtpTrap
CTP	Herramienta Ping	Notificación	Se abortó la prueba de la herramienta Ping. IP de origen: <P1>. IP de destino: <P2>. Número de peticiones: <P3>. Número de respuestas <P4>.	P1 = dirección IP del origen P2 = dirección IP del destino P3 = número de peticiones enviadas P4 = número de respuestas recibidas	P322.0	80032200	cabhPsDevCtpTrap
Eventos de QoS							
Determinación de UPnP	Búsqueda-M	Aviso	Hay activos varios tenedores de política UPnP		Q100.0	81010000	cabhPsDevUpnpMultiplePHTrap

NOTA – Los eventos de actualización del software (descarga segura de software) se aplican únicamente a los servicios de portal (PS) autónomos. La actualización del software se controla mediante el módem de cable DOCSIS en un PS integrado, de manera que el informe del evento de actualización del software se gestiona mediante el módem de cable en un PS integrado. Para más información véase en la cláusula 11.8, Descarga segura de software para el PS.

Anexo C

Amenazas de seguridad y medidas preventivas

Cuando se diseña una tecnología de seguridad es importante tener una idea precisa de las principales amenazas para una determinada aplicación o entorno. Esta información puede utilizarse para seleccionar las herramientas de seguridad y las tecnologías más eficaces destinadas a proteger y prevenir los ataques maliciosos.

Las principales amenazas de seguridad en las redes domésticas para abonados y operadores del sistema que se han advertido son las siguientes:

C.1 Robo del servicio: El robo de servicios se presenta en dos formas, acceso no autorizado a los servicios de cable y reproducción no autorizada del contenido del servicio.

El acceso no autorizado supone que un abonado o un tercero (por ejemplo, un vecino) tiene acceso a los servicios del cable que no ha pagado. Los dispositivos pueden "clonarse" o modificarse para que parezcan dispositivos autorizados de la red doméstica del abonado. Esto puede provocar asimismo la degradación de la calidad de funcionamiento del servicio ya que estos dispositivos consumen recursos adicionales de transporte de la red HFC y de las redes domésticas.

La reproducción no autorizada supone que un abonado o tercero (por ejemplo, un vecino) copie ilegalmente el contenido del servicio. En ciertos casos estas copias se distribuyen a otros consumidores sin la aprobación del operador ni del proveedor de contenidos.

C.2 Ataques de denegación del servicio (DoS*, denial of service)*: Los ataques de denegación del servicio pueden tener lugar cuando un tercero (atacante, abonado hostil, etc.) perturba la comunicación y configuración de servicio normales entre operadores y abonados. Se pueden insertar en la red doméstica transmisiones de datos ofensivas procedentes de fuentes o dispositivos aparentemente válidos, degradando gravemente el funcionamiento ordinario. Estas transmisiones de datos ofensivas podrían ampliarse asimismo a la red HFC del operador provocando en ella problemas de calidad de funcionamiento.

C.3 Confidencialidad del servicio: La amenaza a la confidencialidad del servicio supone la supervisión o recepción de información acerca de un abonado o de los servicios utilizados por éste, por parte de un tercero (vecino, atacante, etc.). Esto podría provocar el robo de la información de las contraseñas o de la configuración de los dispositivos permitiendo a los atacantes ampliar su acceso a los recursos de la red del abonado y a ficheros o datos confidenciales.

Hay varios métodos que pueden utilizarse para evitar las amenazas de seguridad antedichas. Desgraciadamente, no hay un solo método que permita evitarlas todas, no obstante lo cual, una combinación de métodos podría constituir el mejor sistema de defensa. Se pueden utilizar las siguientes medidas preventivas:

C.4 Autenticación: La autenticación supone la verificación de que las entidades emisora y receptora son quienes pretenden ser. Entre éstas se encuentran la fuente del servicio, el dispositivo receptor y el abonado.

La autenticación contribuye a evitar el robo del servicio al validar los dispositivos y usuarios finales, aunque no evita la copia ilegal de contenidos ni el acceso no autorizado por parte de terceros que supervisen el enlace. Evita razonablemente bien los ataques DoS porque se puede rechazar el tráfico cuando no proviene de un origen válido. En sí misma la autenticación no proporciona ningún soporte de confidencialidad de servicios, para lo que habría que usar la criptación.

C.5 Protección de copias: Los métodos de protección de copias limitan la posibilidad de que un dispositivo receptor haga copias no autorizadas de los contenidos del servicio.

La protección de copia contribuye a evitar el robo del servicio limitando el número máximo de copias que puede realizarse, pero no evita el acceso no autorizado a los servicios. No evita la DoS ni protege la confidencialidad del servicio. En general, esta medida preventiva se implementa en las capas superiores de la aplicación.

C.6 Criptación de datos: La criptación de datos evita la divulgación o acceso no autorizado a los datos.

La criptación de datos es un excelente modo de proporcionar confidencialidad sobre los datos y protección frente al robo del servicio. La criptación funciona impidiendo la lectura de los datos sin la clave de descriptación adecuada, no obstante lo cual no valida las entidades de origen y recepción y no proporciona protección contra copias una vez descriptados los datos. Tampoco evita los ataques DoS.

C.7 Barrera contra fuegos: Las aplicaciones de barrera contra fuegos evitan que el tráfico de la red pase de un dominio a otro sin satisfacer determinados criterios establecidos por el abonado o el operador. En las redes domésticas, las barreras contra fuegos se suelen ubicar en los dispositivos domésticos de pasarela que conectan la red HFC a la red doméstica.

Una aplicación barrera contra fuegos contribuye a evitar los ataques DoS y los de confidencialidad procedentes del lado de red de área extensa (WAN) de la barrera contra fuegos, aunque no evita el tipo de ataques procedente del lado de la red doméstica de la barrera contra fuegos. Tampoco protege del robo del servicio.

C.8 Seguridad de los mensajes de gestión: Este método de prevención implica la autenticación y criptación únicamente de los mensajes de gestión de la red. Los mensajes de gestión de la red se utilizan para la configuración de dispositivos, supervisión y control de la red, configuración de servicios y reservas de la calidad de servicio (QoS).

La seguridad de los mensajes de gestión constituye un buen mecanismo para evitar los ataques DoS mediante la autenticación y criptación de los mensajes de gestión. La información personal del abonado y de la configuración de la red queda asimismo protegida de los ataques de confidencialidad, aunque no ocurre lo mismo con el contenido de los servicios. Asimismo, la seguridad de mensajes de gestión no evita el robo del contenido de los servicios por parte de entidades no autorizadas.

Anexo D

Aplicaciones mediante CAT y la barrera contra fuegos

Durante la operación normal de la funcionalidad de la traducción de la dirección y la barrera contra fuegos, es posible que varios de los protocolos y las aplicaciones tengan impedimentos para funcionar como se tenía previsto. Las barreras contra fuegos podrán filtrar deliberadamente ciertas aplicaciones y protocolos con fines de seguridad. La política de la barrera contra fuegos podrá ser establecida explícitamente por el operador del sistema de cable de modo que permita la apertura de tantos puertos como sea necesario para el abonado, sin abrir puertos que no sean indispensables para la comunicación entre las redes LAN y WAN. La limitación de la apertura de puertos y de la iniciación de sesiones entre las redes LAN y WAN puede proporcionar protección contra los ataques a la red LAN doméstica. Si la política de la barrera contra fuegos impide que se abran los puertos, un atacante no podrá utilizar dichos puertos para tratar de dañar a la red LAN. La finalidad de este anexo es la de ofrecer un nivel mínimo de soporte para las aplicaciones que se utilizan comúnmente en casos particulares, y para apoyar al operador del sistema de cable con la configuración de los puertos comunes.

En [RFC 3235], Network Address Translator (NAT)-Friendly Application Design Guidelines, se describen varias directrices para la creación de aplicaciones de modo que no corran riesgos cuando funcionen en presencia de la funcionalidad de la traducción de direcciones de red. Se recomienda encarecidamente a los desarrolladores de aplicaciones que funcionarán en el entorno de IPCable2Home que se ciñan en la medida posible a dichas directrices.

Se sabe que la funcionalidad de NAT y la barrera contra fuegos afectan a diversos protocolos y aplicaciones cuando los nodos/anfitriones finales no se encuentran en el mismo sector de direcciones y deben atravesar un traductor de direcciones de red IP (NAT/CAT) y/o *encaminar* la barrera contra fuegos de modo que puentee los sectores. En muchos casos, la CAT y la barrera contra fuegos no puede proporcionar la transparencia deseada de la aplicación y el protocolo sin la ayuda de una pasarela de nivel de aplicación (ALG, *application level gateway*). En la presente Recomendación se supone que se implementa una ALG en la pasarela residencial para que las aplicaciones relacionadas en este anexo puedan funcionar a través de la CAT.

Las aplicaciones a través de la barrera contra fuegos se describen en términos del protocolo, números de puertos particulares, casos de relación entre las redes LAN y WAN y los sectores de direccionamiento. Los protocolos se dividen en dos cuadros; en uno se relacionan los protocolos que pueden gestionarse únicamente mediante la política y se etiqueta como aplicaciones que necesitan exclusivamente la política de la barrera contra fuegos; en el segundo se relacionan los protocolos que sólo pueden ser gestionados con la combinación de la política y las ALG, y se denomina aplicaciones que necesitan la política de la barrera contra fuegos y una ALG.

De acuerdo con la política establecida en la cláusula 11, los cuadros incluyen comentarios de información que permiten al lector establecer la correspondencia de las aplicaciones necesarias con aquellas que tienen requisitos de política particulares para IPCable2Home e IPCablecom. IPCable2Home necesita valores de fábrica por defecto para que los puertos puedan abrirse a través de la barrera contra fuegos durante las operaciones normales de la pasarela residencial. Los puntos marcados con IPCablecom en la columna de comentarios se incluirán, además de los valores de fábrica por defecto, para habilitar IPCablecom a través de la barrera contra fuegos. Los valores de la barrera contra fuegos que habilitan IPCablecom se relacionan en la columna de comentarios de cada uno de los cuadros y se especifican en la sección del fichero de configuración de la cláusula 11.

Además de las aplicaciones especificadas, el PS DEBERÍA soportar aplicaciones de juegos en línea a través de la CAT y la barrera contra fuegos. Estos juegos en línea se consideran una aplicación de usuario convencional. No obstante, en esta Recomendación no se especifican los juegos, ya que se

trata de una industria dinámica y los puertos correspondientes dependen de la popularidad actual de los juegos particulares.

D.1 Casos relativos a las relaciones

Los casos particulares pueden determinar el número de anfitriones que se comunican entre ellos a través del PS, junto con los requisitos de cada protocolo y aplicación. Cada aplicación/protocolo y caso particular necesita el soporte de CH CAT y de la barrera contra fuegos para que funcione adecuadamente. Los casos incluyen una definición "xxx a xxx" que indica el número de anfitriones de LAN que se comunican a anfitriones de la red WAN (por ejemplo, "uno a varios" define un anfitrión de LAN que se comunica con múltiples anfitriones de WAN simultáneamente). Estos casos incluyen:

- relación "uno a uno" para un solo ejemplar;
- relación "uno a uno" para múltiples ejemplares (es posible identificar el número de ejemplares necesarios);
- relación "uno a varios" para un solo ejemplar;
- relación "uno a varios" para múltiples ejemplares (es posible identificar el número de ejemplares necesarios);
- relación "varios a uno" para un solo ejemplar;
- relación "varios a uno" para múltiples ejemplares (si es necesario se identificará el número de ejemplares necesarios).

NOTA – El caso de "varios a varios" será el mismo que una relación "uno a uno" para múltiples ejemplares, una relación "uno a varios" para múltiples casos y/o una relación "varios a uno" para múltiples ejemplares.

Véanse las figuras D.1 a D.3.

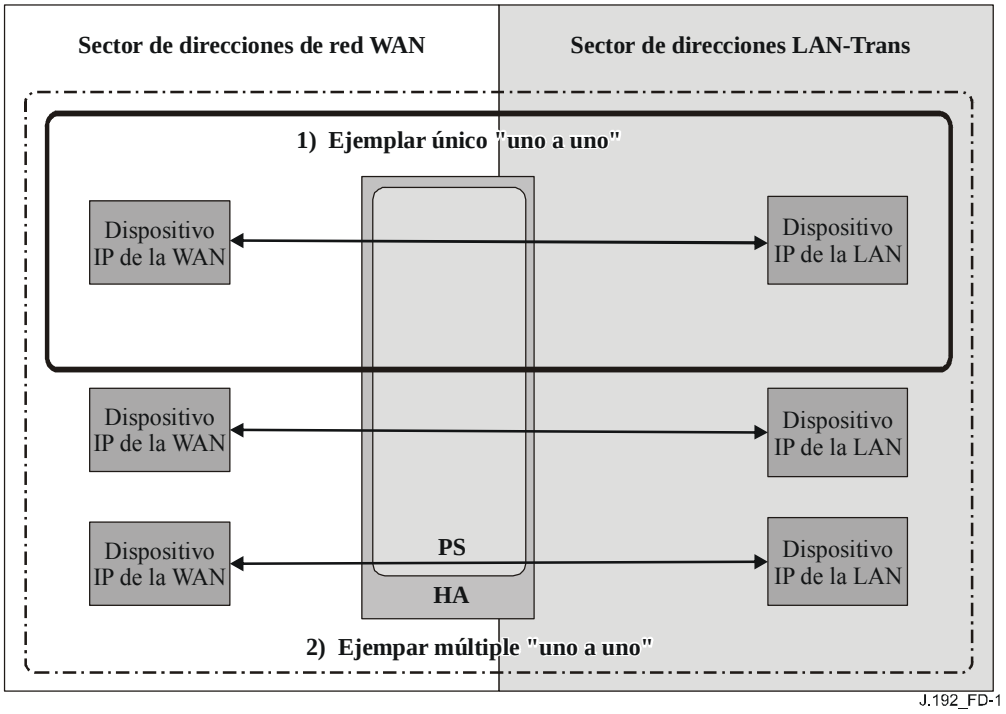


Figura D.1/J.192 – Escenarios de "uno a uno"

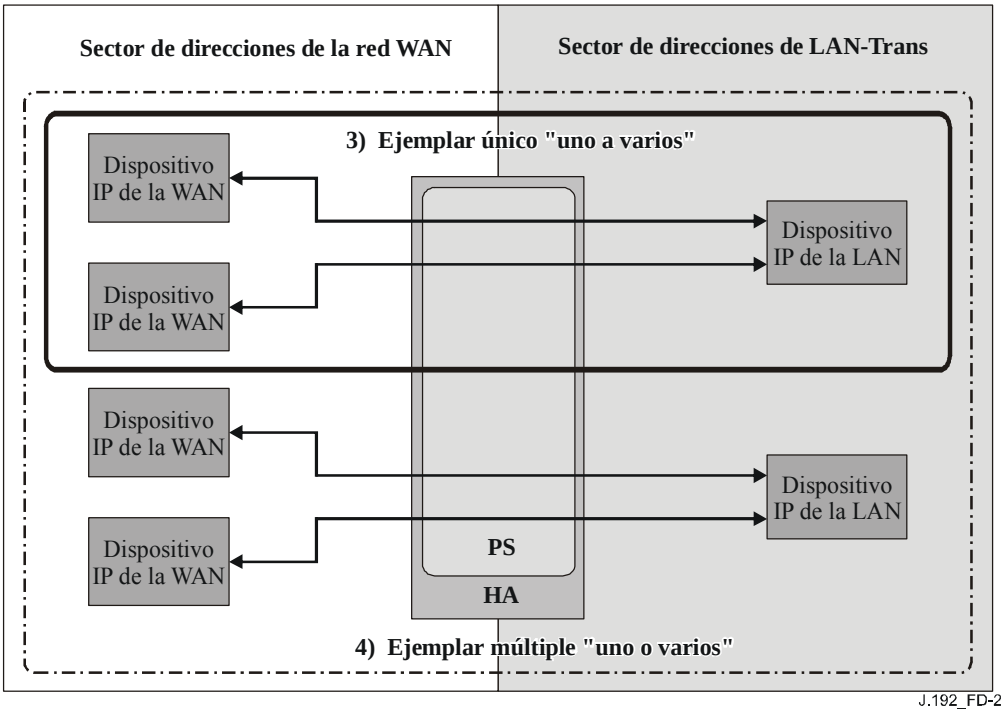


Figura D.2/J.192 – Escenarios de "uno a varios"

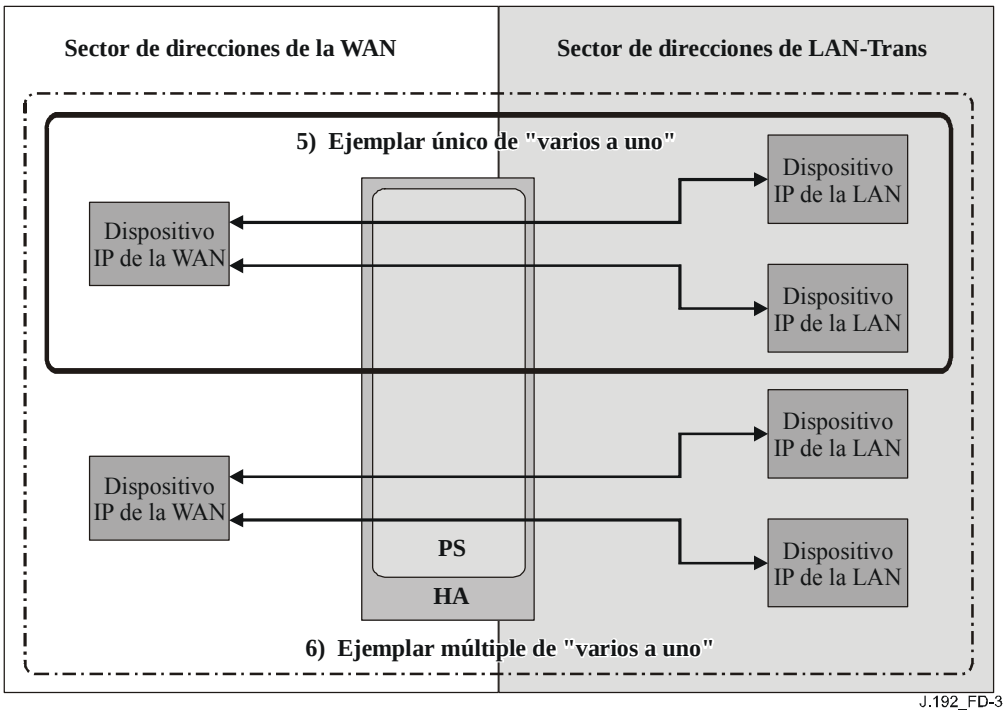


Figura D.3/J.192 – Escenarios de "varios a uno"

D.2 Aplicaciones que sólo necesitan la política de la barrera contra fuegos

En los cuadros D.1 y D.2 se identifican las aplicaciones y los protocolos que DEBEN soportarse a través de la CAT y la barrera contra fuegos. Esto no impide el soporte de aplicaciones y protocolos adicionales. Una CAT/barrera contra fuegos que pueda soportar esas aplicaciones y protocolos podrá soportar muchas otras aplicaciones y protocolos que no integren información de dirección,

puerto u otra que pueda verse afectada por la traducción de la dirección de la red, y que no tramiten sesiones entrantes.

La siguiente relación de protocolos y aplicaciones en el cuadro D.1 DEBE funcionar a través de las implementaciones de CAT y de la barrera contra fuegos. La barrera contra fuegos NO DEBE iniciar su funcionamiento antes de que el PS envíe el mensaje de conclusión de la configuración, en consecuencia, en este cuadro no se indican los protocolos necesarios para configurar el PS.

NOTA – Las aplicaciones que necesitan únicamente la configuración de la política de la barrera contra fuegos DEBEN soportarse en los seis (6) escenarios de relación a menos que se indique lo contrario en la columna de comentarios.

Cuadro D.1/J.192 – Protocolos necesarios para el funcionamiento a través de la CAT y de la barrera contra fuegos del CH

Aplicación/Protocolo	Puertos	Comentarios
AOL IM	TCP/5190, 5191, 5192, 5193 & 13784	Valor por defecto en Internet
CU-SeeMe	TCP/7648, 7649; UDP/7648, 7649, 24032	
DHCP		Valor por defecto en Internet
DNS	UDP/53	IPCablecom e IPCable2Home
FTPS	989 & 990	
HTTP	TCP/80	Valor por defecto en Internet
HTTPS	TCP/443	Valor por defecto en Internet
IGMP e IP Multidifusión		Se necesita el anexo CH 1.0
imap	143	
imap3	220	
IPSec	IKE > UDP/500 – ESP > raw IP/50	Intercambio de claves IKE, modo de tunelización, caso único de uno a uno (clave de soporte de CAT) Intercambio de claves IKE, modo de transporte, caso único de uno a uno (modo de transferencia), modo de transferencia entre pares de LAN e IPCablecom
IRC	TCP/6665-6669	
Kerberos	1293	IPCablecom y sector de direcciones del PS de IPCable2Home
L2TP	UDP/1701	
MediaPlayer (Windows)	TCP/80; 1755	
Microsoft Messenger	3330 – 3332	Valor por defecto en Internet mcs-calypsoicf 3330 mcs-messaging 3331 mcs-mailsvr 3332
MGCP	2427, 2727	IPCablecom
Par a par (eDonkey)	TCP/4662 UDP/4665	eDonkey

Cuadro D.1/J.192 – Protocolos necesarios para el funcionamiento a través de la CAT y de la barrera contra fuegos del CH

Aplicación/Protocolo	Puertos	Comentarios
Par a par (protocolo FastTrack P2P)	TCP/1214	KaZaA, Grokster, etc.
Par a par (protocolo Gnutella P2P)	TCP/6346	Gnutella, LimeWire, BearShare, Morpheus, etc.
Par a par (WinMX)	TCP/6699 UDP/6257	WinMX
Petición de eco PING ICMP	raw IP/1	IPCable2Home
POP3	TCP/110	Valor por defecto en Internet
PPTP	Control Port > TCP/1723 & GRE > raw IP/47	
RealAudio/RealMedia	TCP: 80;443;554	
RSVP		IPCablecom
RTSP	TCP/554	
RTCP		IPCablecom
RTP		IPCablecom
SMTP	TCP/25	Valor por defecto en Internet
SNMP	TCP/161 UDP/161	Sector de direcciones del PS de IPCable2Home e IPCablecom
SNMP trap	TCP/162 UDP/162	Sector de direcciones del PS de IPCable2Home e IPCablecom
SSH	TCP/22 UDP/22	Valor por defecto en Internet
syslog	UDP/514	Sector de direcciones del PS de IPCable2Home e IPCablecom
Telnet	UDP/23	Peticiones de sesión saliente. Valor por defecto en la red Internet
TFTP	UDP/69	IPCablecom
Traceroute	raw IP/1	Valor por defecto en Internet Se debe soportar la respuesta de todos los saltos entre el origen y el destino
Yahoo Messenger	TCP: 5050, 80 o cualquier valor disponible	Valor por defecto en Internet

NOTA – IANA había cancelado anteriormente la asignación de algunos números de puertos relacionados en esta cláusula, que sin embargo han sido asignados recientemente y ahora pertenecen a otra aplicación. RTP y Quicktime indican ambos 6970 a 6999, pero IANA ha asignado ahora los valores 6998 y 6999 a iatp-highpri e iatp-normalpri. IPCable2Home no pretende corregir este conflicto.

D.3 Aplicaciones que necesitan la política de la barrera contra fuegos y una ALG

En muchos casos la CAT y la barrera contra fuegos no pueden proporcionar la transparencia deseada para la aplicación y el protocolo. Como la CAT modifica las direcciones del nodo extremo (en el encabezamiento IP de un paquete) a lo largo de la *ruta*, algunas aplicaciones no pueden

funcionar a través de la CAT sin el apoyo de una ALG. Siempre que sea posible, se DEBEN utilizar ALG específicas de la aplicación conjuntamente con la CAT y la política de la barrera contra fuegos adecuada para proporcionar la deseada transparencia al nivel de la aplicación. La función de una ALG depende de la aplicación, y por consiguiente en el cuadro D.2 siguiente se presenta una relación de las aplicaciones, protocolos y los casos que DEBEN soportarse.

Cuadro D.2/J.192 – Aplicaciones que necesitan la política de la barrera contra fuegos y una ALG

Aplicación/ Protocolo	Puertos	(1) Caso único uno a uno	(2) Caso múltiple uno a uno	(3) Caso único uno a varios	(4) Caso múltiple uno a varios	(5) Caso único varios a uno	(6) Caso múltiple varios a uno	Comentarios
FTP	20/tcp, 21/tcp	X	X	X	X	X	X	
Microsoft Netmeeting (H.323)	TCP/389 ILS 522 ULS 1503 T.120 1720 establecimiento de la comunicación 1731 control de la llamada de audio Control dinámico de la llamada TCP RTP por UDP 1024-65 535 UDP dinámico	X	X	X	X	X	X	
MSN Messenger (H.323)	1863/tcp	X	X	X	X	X	X	Valor por defecto en la red Internet
Net2Phone	6801/udp (también solicita la apertura de 2 puertos adicionales no especificados UDPPORT=6801 UDPPORT=XXXX TCPPORT=XXXX El administrador de la red debe garantizar que UDPPORT 6801 está abierto. Para el otro UDPPORT y TCPPORT, el administrador puede utilizar cualquiera en la gama 1 a 30000.)	X	X	X	X			
Quicktime 5	RTSP/TCP/554 RTP/UDP 6970-6999	X	X	X	X	X	X	El soporte de Quicktime sin una ALG a través del puerto 80 da por resultado una calidad de funcionamiento inferior a la óptima
Window Messenger (SIP)		X	X					Disponible únicamente en Windows XP

Anexo E

Las MIB

E.1 Requisitos de la MIB portal de direccionamiento (CAP, IPCable2Home Addressing Portal)

La MIB CAP IPCable2Home DEBE implementarse tal como se define a continuación.

```
CABH-CAP-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    Unsigned32,
    Integer32           FROM SNMPv2-SMI
    TimeStamp,
    TruthValue,
    RowStatus,
    DateAndTime,
    PhysAddress         FROM SNMPv2-TC
    OBJECT-GROUP,
    MODULE-COMPLIANCE   FROM SNMPv2-CONF
    InetAddressType,
    InetAddress,
    InetPortNumber      FROM INET-ADDRESS-MIB
    clabProjCableHome   FROM CLAB-DEF-MIB
    SnmpAdminString     FROM SNMP-FRAMEWORK-MIB;

cabhCapMib MODULE-IDENTITY
    LAST-UPDATED    "200502110000Z" --February 11, 2005
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
            858 Coal Creek Circle
            Louisville, Colorado 80027
            U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com; mibs@cablelabs.com"
    DESCRIPTION
            "This MIB module supplies the basic management objects
            for the CableHome Address Portal (CAP) portion of
            the PS."
    ::=  { clabProjCableHome 3 }


    cabhCapObjects      OBJECT IDENTIFIER ::= { cabhCapMib 1 }
    cabhCapBase         OBJECT IDENTIFIER ::= { cabhCapObjects 1 }
    cabhCapMap          OBJECT IDENTIFIER ::= { cabhCapObjects 2 }
```

```
--=====================================================================
--
--    General CAP Parameters
--
--=====================================================================

cabhCapTcpTimeWait OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This object is the maximum inactivity time to wait before
            assuming TCP session is terminated. It has no relation to
            the TCP session TIME_WAIT state referred to in [RFC 793]."
    REFERENCE
            "CableHome 1.1 Specification, Packet Handling & Address
            Translation section."
    DEFVAL { 300 }
    ::= { cabhCapBase 1 }

cabhCapUdpTimeWait OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The inactivity time to wait before destroying
            CAP mappings for UDP."
    REFERENCE
            "CableHome 1.1 Specification, Packet Handling & Address
            Translation section."
    DEFVAL { 300 }  -- 5 minutes
    ::={ cabhCapBase 2 }

cabhCapIcmpTimeWait OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The inactivity time to wait before destroying
            CAP mappings for ICMP."
    REFERENCE
            "CableHome 1.1 Specification, Packet Handling & Address
            Translation section."
    DEFVAL { 300 }  --  5 minutes
    ::= { cabhCapBase 3 }

cabhCapPrimaryMode OBJECT-TYPE
    SYNTAX      INTEGER {
                    napt(1),        -- NAT with Port Translation Mode
                    nat(2),         -- Traditional NAT Mode
                    passthrough(3)  -- Passthrough/Bridging Mode
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Primary Packet-handling Mode of the Portal Services
            logical element (PS) of a CableHome compliant residential
            gateway device. This object configures operation of the PS
            packet handling functions.
```

```
            When the value of this object is napt(1), the PS is
            required to support the Network Address and Port
            Translation (NAPT) process in accordance with the NAPT
            requirements defined in IETF RFC 3022. When operating in
            NAPT Primary Packet Handling Mode, the PS supports the
            translation of multiple LAN-Trans IP addresses and their
            TCP/UDP ports into a single WAN-Data IP address and its
            TCP/UDP ports.

            When the value of this object is nat(2), the PS is required
            to support the Network Address Translation (NAT) process in
            accordance with the NAT equirements defined in IETF RFC
            3022. When operating in NAT Primary Packet Handling Mode,
            the PS supports the translation of multiple LAN-Trans IP
            addresses into the same number of unique WAN-Data IP
            addresses.

            When the value of this object is passthrough(3), the PS is
            required to act as a transparent bridge in accordance with
            IEEE 802.1D. When operating in Passthrough Primary Packet
            Handling Mode, the PS does not translate network addresses,
            and bridges all traffic between its LAN and WAN interfaces.

            The PS MUST delete dynamically-created row entries from
            the cabhCapMappingTable, i.e., those with
            cabhCapMappingMethod = dynamic(2), when the value of
            cabhCapPrimaryMode changes. The PS MUST NOT delete
            statically-created row entries from the cabhCapMappingTable
            where cabhCapMappingMethod = static(1), when the value of
            cabhCapPrimaryMode changes."
    REFERENCE
            "CableHome 1.1 Specification, Packet Handling & Address
            Translation section."
    DEFVAL { napt }
    ::= { cabhCapBase 4 }

cabhCapSetToFactory OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Reading this object always returns false(2). When the
            cabhCapSetToFactory object is set to true(1), the PS must
            take the following actions:

            1) Clear all entries in the cabhCapMappingTable and
               cabhCapPassthroughTable.
            2) Reset the following objects to their factory default
               values:
                 cabhCapTcpTimeWait,
                 cabhCapUdpTimeWait,
                 cabhCapIcmpTimeWait,
                 cabhCapPrimaryMode"
    REFERENCE
            "CableHome 1.1 Specification, Packet Handling & Address
            Translation section."
    ::= { cabhCapBase 5 }

cabhCapLastSetToFactory OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
            "The value of sysUpTime when cabhCapSetToFactory was
            last set to true. Zero if never reset."
    ::= { cabhCapBase 6 }

cabhCapUpnpPortForwardingEnable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This MIB is effective only when the PS is performing NAPT.
            If this MIB object is set to false(2), the PS MUST disable
            the UPnP WANIpConnection service in the CableHome PS. If
            this MIB object is set to true(1), the PS MUST enable the
            WANIpConnection service in the PS. When the primary packet
            handling mode of the PS is C-NAT (2) or Passthrough(3),
            setting this MIB to true(1) MUST return InconsistentValue
            error."
    REFERENCE
            "CableHome 1.1 Specification, Packet Handling & Address
            Translation section."
    DEFVAL { 1 }
    ::= { cabhCapBase 7 }

cabhCapUpnpTimeWait OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The inactivity time to wait before destroying
            CAP mappings created by UPnP control points. The
            value of 0 indicates inactivity time wait of
            infinity, i.e., a UPnP entry does not get destroyed
            based on inactivity period."
    REFERENCE
            "CableHome 1.1 Specification, Packet Handling & Address
            Translation section."
    DEFVAL { 0 }  --  0 seconds, inactivity time wait of infinity.
    ::= { cabhCapBase 8 }


--=====================================================================
--
--    cabhCapMappingTable (CAP Mapping Table)
--
--    The cabhCapMappingTable contains information pertaining to all
--    NAPT and NAT mappings in a CableHome(TM) compliant residential
--    gateway device.
--
--=====================================================================


cabhCapMappingTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCapMappingEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains IP address mappings between private
            network addresses, or network addresses and port
            numbers/ICMP Identifiers, assigned to devices on the
            subscriber's home LAN, and network addresses, or network
            addresses and port numbers/ICMP Identifiers on the WAN,
```

```
            presumed to be on a separate subnetwork than the private
            IP addresses.  The CAP Mapping Table is used by the
            CableHome Address Portal (CAP) function of the PS to make
            packet forwarding decisions."
    REFERENCE
            "CableHome 1.1 Specification, Packet Handling & Address
            Translation section."
    ::= { cabhCapMap 1 }

cabhCapMappingEntry OBJECT-TYPE
    SYNTAX      CabhCapMappingEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "List of the private IP (LAN) address-to-cable
            operator assigned IP (WAN) address mappings stored
            in the PS and used by the PS to make packet
            forwarding decisions."
    INDEX { cabhCapMappingIndex }
    ::= { cabhCapMappingTable 1 }

CabhCapMappingEntry ::= SEQUENCE {
    cabhCapMappingIndex               INTEGER,
    cabhCapMappingWanAddrType         InetAddressType,
    cabhCapMappingWanAddr             InetAddress,
    cabhCapMappingWanPort             InetPortNumber,
    cabhCapMappingLanAddrType         InetAddressType,
    cabhCapMappingLanAddr             InetAddress,
    cabhCapMappingLanPort             InetPortNumber,
    cabhCapMappingMethod              INTEGER,
    cabhCapMappingProtocol            INTEGER,
    cabhCapMappingRowStatus           RowStatus,
    cabhCapMappingNumPorts            Unsigned32,
    cabhCapMappingRowDescr            SnmpAdminString,
    cabhCapMappingCreateTime          DateAndTime,
    cabhCapMappingLastUpdateTime      DateAndTime,
    cabhCapMappingDuration            Integer32,
    cabhCapMappingRemoteHostAddrType InetAddressType,
    cabhCapMappingRemoteHostAddr      InetAddress,
    cabhCapMappingEnable              TruthValue
    }

cabhCapMappingIndex OBJECT-TYPE
    SYNTAX      INTEGER   (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The Index into the CAP Mapping Table."
    ::= { cabhCapMappingEntry 1 }

cabhCapMappingWanAddrType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The IP address type assigned on the WAN side."
    DEFVAL { ipv4 }
    ::= { cabhCapMappingEntry 2 }

cabhCapMappingWanAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
```

```
    DESCRIPTION
            "The IP address assigned by the cable operator's address
            (DHCP) server, and comprising the WAN-side IP address
            of the CAP Mapping tuple. This object is populated
            either dynamically by LAN-to-WAN outbound traffic or
            statically by the cable operator."
    ::= { cabhCapMappingEntry 3 }

cabhCapMappingWanPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The TCP/UDP port number or ICMP Identifier
            on the WAN side. A port number/Identifier of
            0 indicates either a NAT or a DMZ mapping.
            A non-zero port number/Identifier indicates
            a NAPT mapping. If the value of
            cabhCapMappingNumPorts MIB object is non-zero,
            this MIB represents a starting TCP/UDP port
            number on the WAN side for which a mapping
            entry is created."
    DEFVAL { 0 }
    ::= { cabhCapMappingEntry 4 }

cabhCapMappingLanAddrType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The IP address type assigned on the LAN side."
    DEFVAL { ipv4 }
    ::= { cabhCapMappingEntry 5 }

cabhCapMappingLanAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The IP address of the LAN-Trans IP Device. This object is
            populated either dynamically as a result of LAN-to-WAN
            outbound traffic or statically by the cable operator."
    ::= { cabhCapMappingEntry 6 }

cabhCapMappingLanPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The TCP/UDP port number or ICMP Identifier
            on the LAN side. A port number/Identifier
            of 0 indicates either a DMZ mapping or a NAT
            mapping. A non-zero port number/Identifier
            indicates a NAPT mapping. If the value of
            cabhCapMappingNumPorts MIB object is non-zero,
            then this MIB represents a starting TCP/UDP port
            number on the LAN side for which a mapping
            entry is created."
    DEFVAL { 0 }
    ::= { cabhCapMappingEntry 7 }
```

```
cabhCapMappingMethod OBJECT-TYPE
    SYNTAX      INTEGER {
                    static(1),
                    dynamic(2),
                    upnp(3)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Indicates how this mapping was created. Static means
            that it was provisioned, and dynamic means that it
            was handled by the PS itself. upnp (3) means that the
            CAP mapping entry was created by some UPnP compliant
            application."
    ::= { cabhCapMappingEntry 8 }

cabhCapMappingProtocol OBJECT-TYPE
    SYNTAX      INTEGER {
                    other(1),    -- any other protocol; e.g. IGMP
                    icmp(2),
                    udp(3),
                    tcp(4),
                    all(255)     -- covers all the protocols
                }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The protocol for this mapping entry. The value
            of other(1) represents a protocol other
            than ICMP, TCP, and UDP. Thus, when the value
            other(1) is specified for the cabhCapMappingProtocol
            value of a CAP Mapping Table entry,
            TCP, UDP or ICMP packets MUST NOT be forwarded even
            if the WAN and LAN IP address and port tuple
            of the packet matches with mapping entry.
            The value of all(255) represents all protocol types. Thus,
            when the cabhCapMappingProtocol value
            all(255) is specified for an entry in the CAP Mapping
            Table, traffic of all protocol types MUST be forwarded
            accordingly if the WAN and LAN IP address and port tuple
            in the packet matches the mapping entry."
    ::= { cabhCapMappingEntry 9 }

cabhCapMappingRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The RowStatus interlock for the creation and deletion
            of a cabhCapMappingTable entry. Changing the value of
            the IP address or port number columns of the CAP
            Mapping Table may have an effect on active traffic,
            so the PS will prevent modification of this table's
            columns and return an inconsistentValue error when
            cabhCapMappingRowStatus object is active(1).

            The PS must not allow RowStatus to be set to
            notInService(2) by a manager.

            A newly created row cannot be set to active(1) until
            the corresponding instances of cabhCapMappingWanAddr,
            cabhCapMappingLanAddr, and cabhCapMappingProtocol have
            been set.
```

```
            If the manager attempts to populate a row entry in
            the table with a non-unique value for the combination
            of cabhCapMappingWanAddr and range of WAN port(s)
            (identified by cabhCapMappingWanPort to
            cabhCapMappingWanPort + cabhCapMappingNumPorts -1),
            or a non-unique value for the combination of
            cabhCapMappingLanAddr and range of LAN port(s)
            (identified by cabhCapMappingLanPort to
            cabhCapMappingLanPort + cabhCapMappingNumPorts - 1),
            the PS MUST prevent the creation of this row and return
            an inconsistentValue error. This prevents creation of
            entries with overlapping port ranges in the CAP table.

            If the manager attempts to populate a row entry with
            a zero value for cabhCapMappingWanPort and a non-zero
            value for cabhCapMappingLanPort or a row entry with a
            zero value for cabhCapMappingLanPort and a non-zero value
            for cabhCapMappingWanPort, the PS MUST prevent the
            creation of this row and return an inconsistentValue
            error. This prevents creation of invalid NAT or NAPT entries.

            If the manager attempts to populate a row entry with non-zero
            values for both cabhCapMappingWanPort and
            cabhCapMappingLanPort, but a zero value for
            cabhCapMappingNumPorts, the PS MUST prevent
            the creation of this row and return an inconsistentValue
            error. This prevents creation of NAPT entries.

            When Primary Packet-handling Mode is NAPT
            (cabhCapPrimaryMode is napt(1)), provisioned rows can be
            set to active(1) regardless of whether the value to which
            cabhCapMappingWanPort, cabhCapMappingLanPort, and
            cabhCapMappingNumPorts have been set is zero or nonzero.

            When Primary Packet-handling Mode is NAT
            (cabhCapPrimaryMode is nat(2)), a newly created row can
            not be set to active(1) if a non-zero value has been set
            for cabhCapMappingWanPort, cabhCapMappingLanPort and
            cabhCapMappingNumPorts.

            In NAPT Primary Packet-handling mode, a row
            entry with zero values for cabhCapMappingWanPort,
            cabhCapMappingLanPort, and cabhCapMappingNumPorts
            objects represents a DMZ entry."
    ::={ cabhCapMappingEntry 10 }

cabhCapMappingNumPorts OBJECT-TYPE
    SYNTAX      Unsigned32(1..65535)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "This object represents the number of ports
            available for port translation
            on both LAN and WAN side.

            When both cabhCapMappingWanPort and
            cabhCapMappingLanPort are set to zero,
            the PS MUST ignore this MIB object, and
            such a row entry represents either a DMZ entry
            (when primary packet handling mode is NAPT) or
            a NAT entry (when primary packet handling mode is
            NAT).
```

```
            When a row entry is created with non-zero
            values for cabhCapMappingWanPort,
            cabhCapMappingLanPort, and cabhCapMappingNumPorts
            the PS MUST translate range of ports on
            the WAN side (identified by cabhCapMappingWanPort
            to cabhCapMappingWanPort + cabhCapMappingNumPorts-1)
            to range of ports on the LAN side (identified by
            cabhCapMappingLanPort to cabhCapMappingLanPort +
            cabhCapMappingNumPorts-1).

            The PS MUST ignore this MIB for a CAP mapping
            entry with the value of cabhCapMappingProtocol
            equal to icmp(2)."
    DEFVAL { 1 }
    ::= { cabhCapMappingEntry 11 }

cabhCapMappingRowDescr OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "A string value that can be used to describe
             the purpose or attributes of the CAP Mapping
             entry."
    DEFVAL { "" }
    ::= { cabhCapMappingEntry 12 }

cabhCapMappingCreateTime OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "For dynamic(2) and upnp(3) CAP mapping entries, the PS MUST
             set this MIB with date and time when the entry is created.
             The PS MUST set the value of this MIB to zero valued
             11-byte string for static CAP mapping entries. This MIB
             object MUST NOT persist across the PS reboot."
    ::= { cabhCapMappingEntry 13 }

cabhCapMappingLastUpdateTime OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The PS MUST set the value of this MIB
             to zero valued 11-byte string for static
             CAP mapping entries. For dynamic(2) CAP
             Mapping entries, the PS MUST set the value
             of this MIB to the value of cabhCapMappingCreateTime.
             For upnp(3) CAP mapping entries, the PS MUST
             set this MIB with date and time when the entry
             is last updated. When the upnp(3)entry is first
             created, the PS MUST set this MIB with the value
             of cabhCapMappingCreateTime MIB. This MIB object
             MUST NOT persist across the PS reboot."
    ::= { cabhCapMappingEntry 14 }

cabhCapMappingDuration OBJECT-TYPE
    SYNTAX      Integer32 (-1|0..2147483647)
    UNITS       "seconds"
    MAX-ACCESS  read-create
    STATUS      current
```

```
    DESCRIPTION
            "When a value greater than zero
             is assigned to this object, the PS MUST
             remove the CAP entry after the time
             duration, represented by
             this object, elapses starting from
             cabhCapMappingLastUpdateTime.

             When a value of 0 is assigned to this object,
             the PS MUST retain the CAP mapping entry
             until reboot or reset. The PS MUST retain
             a CAP mapping entry with cabhCapMappingDuration
             MIB set to 0 and cabhCapMappingMethod set
             to static(1) across the reboots. The PS MUST
             NOT retain a CAP mapping entry with
             cabhCapMappingDuration MIB set to 0 and
             cabhCapMappingMethod set to upnp(3) across
             the reboots.

             When a value of -1 is assigned for this
             MIB, the PS MUST ignore this MIB and
             MUST remove the CAP mapping entries
             based on TCP, UDP and ICMP inactivity
             time-wait depending upon their protocol
             type.

             When the cabhCapMappingMethod object is
             static(1), the default value for this object
             is 0.

             When the cabhCapMappingMethod object is
             dynamic(2), the PS MUST set the value of
             this object to -1.

             When the cabhCapMappingMethod object is
             upnp(3), the default value for this object
             is -1."

    ::= { cabhCapMappingEntry 15 }

cabhCapMappingRemoteHostAddrType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The IP address type for a remote host on the WAN side."
    DEFVAL { ipv4 }
    ::= { cabhCapMappingEntry 16 }

cabhCapMappingRemoteHostAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The IP address of the remote host for
            a CAP mapping entry. The packet traversing
            through the PS is either originated
            from or is destined to this remote host.
            The value of all zeros for this MIB object
            indicates any IP address for a remote host."
    DEFVAL { '00000000'h }
    ::= { cabhCapMappingEntry 17 }
```

```
cabhCapMappingEnable OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This MIB allows the PS to enable or disable
            a particular CAP mapping entry. When this MIB
            is set to true(1) for a CAP mapping entry, the
            PS MUST correctly route the traffic that
            matches this entry. When this MIB is set to
            false(2) for a CAP mapping entry, the PS MUST
            NOT route the traffic that matches this entry."
    DEFVAL { true }
    ::= { cabhCapMappingEntry 18 }

--========================================================================
--
--    cabhCapPassthroughTable (CAP Passthrough Table)
--
--    The cabhCapPassthroughTable contains the hardware addresses
--    for all LAN IP Devices for which the PS will bridge traffic at
--    OSI Layer 2 when the PS's cabhCapPrimaryMode is set to forward
--    traffic at OSI Layer 3 (NAPT/NAT) for all other hardware
--    addresses.
--
--========================================================================

cabhCapPassthroughTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCapPassthroughEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains hardware addresses of LAN IP Devices
            for which the PS will bridge traffic at OSI Layer 2."
    REFERENCE
            "CableHome 1.1 Specification, Packet Handling & Address
            Translation section."
    ::= {  cabhCapMap 2 }

cabhCapPassthroughEntry OBJECT-TYPE
    SYNTAX      CabhCapPassthroughEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "List of hardware addresses of LAN IP Devices for which
            the PS will bridge traffic at OSI Layer 2."
    INDEX { cabhCapPassthroughIndex }
::= { cabhCapPassthroughTable 1 }

CabhCapPassthroughEntry::=SEQUENCE {
    cabhCapPassthroughIndex         INTEGER,
    cabhCapPassthroughMacAddr       PhysAddress,
    cabhCapPassthroughRowStatus     RowStatus
    }

cabhCapPassthroughIndex OBJECT-TYPE
    SYNTAX      INTEGER (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The index into the CAP Passthrough Table."
    ::= { cabhCapPassthroughEntry 1 }
```

```
cabhCapPassthroughMacAddr OBJECT-TYPE
    SYNTAX      PhysAddress (SIZE(0..16))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "Hardware address of the LAN IP Device for which the PS
            MUST bridge traffic at OSI Layer 2."
    ::={ cabhCapPassthroughEntry 2 }

cabhCapPassthroughRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The RowStatus interlock for the creation and
            deletion of a cabhCapPassthroughTable entry.
            Any writable object in each row can be modified
            at any time while the row is active(1)."
    ::= { cabhCapPassthroughEntry 3 }
--
-- notification group is for future extension.
--

cabhCapNotification    OBJECT IDENTIFIER ::= {
    cabhCapMib 2 0 }
cabhCapConformance     OBJECT IDENTIFIER ::= {
    cabhCapMib 3 }
cabhCapCompliances     OBJECT IDENTIFIER ::= {
    cabhCapConformance 1 }
cabhCapGroups          OBJECT IDENTIFIER ::= {
    cabhCapConformance 2 }

--
--    Notification Group
--


-- compliance statements

cabhCapBasicCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
            "The compliance statement for devices that implement
            the CableHome Portal Services functionality."
    MODULE   --cabhCapMib

-- unconditionally mandatory groups

MANDATORY-GROUPS {
    cabhCapGroup
    }

OBJECT cabhCapMappingProtocol
    SYNTAX      INTEGER { icmp(2) }
    WRITE-SYNTAX  INTEGER { other(1), udp(3), tcp(4), all(255) }
    DESCRIPTION
            "icmp(2) applies only to dynamic entries."

    ::= { cabhCapCompliances 1 }
```

```
cabhCapGroup OBJECT-GROUP
    OBJECTS {
    cabhCapTcpTimeWait,
    cabhCapUdpTimeWait,
    cabhCapIcmpTimeWait,
    cabhCapPrimaryMode,
    cabhCapSetToFactory,
    cabhCapLastSetToFactory,
    cabhCapMappingWanAddrType,
    cabhCapMappingWanAddr,
    cabhCapMappingWanPort,
    cabhCapMappingLanAddrType,
    cabhCapMappingLanAddr,
    cabhCapMappingLanPort,
    cabhCapMappingMethod,
    cabhCapMappingProtocol,
    cabhCapMappingRowStatus,
    cabhCapPassthroughMacAddr,
    cabhCapPassthroughRowStatus,
    cabhCapMappingNumPorts,
    cabhCapMappingRowDescr,
    cabhCapMappingCreateTime,
    cabhCapMappingLastUpdateTime,
    cabhCapMappingDuration,
    cabhCapUpnpPortForwardingEnable,
    cabhCapUpnpTimeWait,
    cabhCapMappingRemoteHostAddrType,
    cabhCapMappingRemoteHostAddr,
    cabhCapMappingEnable
    }
    STATUS      current
    DESCRIPTION
            "Group of objects for CableHome CAP MIB."
    ::= { cabhCapGroups 1 }

END
```

E.2 Requisitos de la MIB portal DHCP IPCable2Home (CDP, IPCable2Home DHCP Portal)

La MIB CDP IPCable2Home DEBE implementarse tal como se define a continuación.

```
CABH-CDP-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    Integer32,
    Unsigned32              FROM SNMPv2-SMI
    PhysAddress,
    TruthValue,
    DateAndTime,
    TimeStamp,
    RowStatus               FROM SNMPv2-TC --RFC2579
    OBJECT-GROUP,
    MODULE-COMPLIANCE       FROM SNMPv2-CONF
    InetAddressType,
    InetAddress             FROM INET-ADDRESS-MIB
    SnmpAdminString         FROM SNMP-FRAMEWORK-MIB
    clabProjCableHome       FROM CLAB-DEF-MIB;

cabhCdpMib MODULE-IDENTITY
    LAST-UPDATED    "200412160000Z"  -- December 16, 2004
    ORGANIZATION    "CableLabs Broadband Access Department"
```

```
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
            858 Coal Creek Circle
            Louisville, Colorado 80027
            U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com; mibs@cablelabs.com"
    DESCRIPTION
            "This MIB module supplies the basic management objects
            for the CableHome DHCP Portal (CDP) portion of the PS
            database."
    ::=  { clabProjCableHome 4 }

cabhCdpObjects         OBJECT IDENTIFIER ::= { cabhCdpMib 1 }
cabhCdpBase            OBJECT IDENTIFIER ::= { cabhCdpObjects 1 }
cabhCdpAddr            OBJECT IDENTIFIER ::= { cabhCdpObjects 2 }
cabhCdpServer          OBJECT IDENTIFIER ::= { cabhCdpObjects 3 }

--
--    The following group describes the base objects in the CableHome
--    DHCP Portal.  The rest of this group deals with addresses defined
--    on the LAN side.
--

cabhCdpSetToFactory OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Reading this object always returns false(2). When the
            cabhCdpSetToFactory object is set to true(1), the PS must
            take the following actions:
            1) Clear all cabhCdpLanAddrEntries in the CDP LAN Address
               Table.
            2) The CDS must offer the factory default DHCP options
               at the next lease renewal time.
            3) Reset the following objects to their factory default
               values:

               cabhCdpLanTransThreshold,
               cabhCdpLanTransAction,
               cabhCdpWanDataIpAddrCount,
               cabhCdpTimeOffsetSelection,
               cabhCdpSnmpSetTimeOffset,
               cabhCdpDaylightSavingTimeEnable,
               cabhCdpLanPoolStartType,
               cabhCdpLanPoolStart,
               cabhCdpLanPoolEndType,
               cabhCdpLanPoolEnd,
               cabhCdpServerNetworkNumberType,
               cabhCdpServerNetworkNumber,
               cabhCdpServerSubnetMaskType,
               cabhCdpServerSubnetMask,
               cabhCdpServerTimeOffset,
               cabhCdpServerRouterType,
               cabhCdpServerRouter,
               cabhCdpServerDnsAddressType,
               cabhCdpServerDnsAddress,
               cabhCdpServerSyslogAddressType,
               cabhCdpServerSyslogAddress,
               cabhCdpServerDomainName,
               cabhCdpServerTTL,
```

```
                cabhCdpServerInterfaceMTU,
                cabhCdpServerVendorSpecific,
                cabhCdpServerLeaseTime,
                cabhCdpServerDhcpAddressType,
                cabhCdpServerDhcpAddress,
                cabhCdpServerCommitStatus"
::= { cabhCdpBase 1 }

cabhCdpLanTransCurCount OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The current number of active leases in the
            cabhCdpLanAddrTable (the number of row entries in the
            table that have a cabhCdpLanAddrMethod value of
            reservationActive(2) or dynamicActive (4)).  This count
            does not include expired leases or reservations not
            associated with a current lease."
    ::= { cabhCdpBase 2 }

cabhCdpLanTransThreshold OBJECT-TYPE
    SYNTAX      INTEGER (0..65533)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The threshold number of LAN-Trans IP addresses allocated
            or assigned above which the PS generates an alarm
            condition. Whenever an attempt is made to allocate a
            LAN-Trans IP address when cabhCdpLanTransCurCount is
            greater than or equal to cabhCdpLanTransThreshold, an
            event is generated. A value of 0 indicates that the CDP
            sets the threshold at the highest number of addresses in
            the LAN address pool."
    DEFVAL { 0 }
    ::= { cabhCdpBase 3 }

cabhCdpLanTransAction OBJECT-TYPE
    SYNTAX      INTEGER {
                    normal(1),
                    noAssignment(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The action taken when the CDS assigns a LAN-Trans
            address and the number of LAN-Trans addresses assigned
            (cabhCdpLanTransCurCount) is greater than the threshold
            (cabhCdpLanTransThreshold). The actions are as follows:
            normal - assign a LAN-Trans IP address as would
            normally occur if the threshold was not exceeded.
            noAssignment - do not assign a LAN-Trans IP address."
    DEFVAL { normal }
    ::= { cabhCdpBase 4 }

cabhCdpWanDataIpAddrCount OBJECT-TYPE
    SYNTAX      INTEGER ( 0..63 )
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This is the number of WAN-Data IP addresses the
            PS's CDC must attempt to acquire via DHCP. When
            this MIB object is incremented, the CDC MUST
            immediately attempt to acquire additional WAN-Data
```

```
            IP addresses. When this MIB object is decremented, the
            CDC MUST not renew the leases for the appropriate
            number of WAN-Data IP addresses."
    DEFVAL { 0 }
    ::= { cabhCdpBase 5 }

cabhCdpLastSetToFactory    OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The value of sysUpTime when cabhCdpSetToFactory was
            last set to true. Zero if never reset."
    ::= { cabhCdpBase 6 }

cabhCdpTimeOffsetSelection OBJECT-TYPE
    SYNTAX      INTEGER {
                useDhcpOption2 (1),
                useSnmpSetOffset(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This object selects the source to be used by the PS in
            determining the time offset to the time of day acquired
            from the time server. It is intended to be used in cases
            where the time zone information provisioned by the ToD
            server or DHCP Server (in DHCP Option 2) is different from
            the time zone where the provisioned device is physically
            located.

            Setting this object to useDhcpOption2(1) configures the PS
            to use the value of DHCP option 2 from the DHCP ACK message
            for time of day offset. Setting this object to
            useSnmpSetOffset(2) configures the PS to use the value of
            cabhCdpServerSnmpSetTimeOffset for time of day offset, and
            to ignore DHCP option 2. When the value of this object is
            changed, the PS MUST immediately begin using the time
            offset specified by the value of this object, regardless
            of which time offset the PS was using before the update
            occurred."
    DEFVAL { useDhcpOption2 }
 ::= { cabhCdpBase 7 }

cabhCdpSnmpSetTimeOffset OBJECT-TYPE
    SYNTAX      Integer32 (-43200..46800)  --  -12 to +13 hours (seconds)
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This object is intended to be used in cases where the
            service provider's provisioning system serves devices in
            multiple time zones, or for other times when the service
            provider wants UTC time offset to be provisioned in a
            device other than from the ToD server or from the DHCP
            Server (in DHCP option 2).

            This object allows a manager to set a value for UTC time
            offset. If DHCP option 2 is not present in the DHCP ACK
            message, or if the value of DHCP option 2 is null, and time
            offset information is not provided in the response received
            from the time of day server, the PS MUST add the value of
            cabhCdpServerTimeOffset to the UTC time acquired from the
            time of day server to create the current time of day.
```

```
            If the value of cabhCdpServerTimeOffsetSelection is
            useSnmpSetOffset(2), the PS adds the value of
            cabhCdpServerSnmpSetTimeOffset to the UTC time acquired
            from the time of day server to create the current time
            of day.

            If the value of cabhCdpServerTimeOffsetSelection is
            useDhcpOption2(1), the PS ignores
            cabhCdpServerSnmpSetTimeOffset."
    DEFVAL { 0 }
    ::= { cabhCdpBase 8 }

cabhCdpDaylightSavingTimeEnable OBJECT-TYPE
    SYNTAX      INTEGER{
                enabled(1),
                disabled(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This object allows a manager to configure the PS to adjust
            the current time of day based on Daylight Saving Time. If
            the value of this object is enabled(1), the PS adds 3600
            seconds and the time offset specified by
            cabhCdpServerTimeOffsetSelection to the UTC time acquired
            from the time of day server to create the current time of
            day during Daylight Saving Time, and adds only the time
            offset specified by cabhCdpServerTimeOffsetSelection to the
            UTC time acquired from the time of day server during
            standard time. The PS is responsible for knowing the date
            and time of each transition between Daylight Saving Time
            and standard time.

            If the value of this object is disabled(2), the PS adds
            only the time offset specified by
            cabhCdpServerTimeOffsetSelection to the UTC time acquired
            from the time of day server."
    DEFVAL { disabled }
    ::= { cabhCdpBase 9 }
--
--    CDP Address Management Tables
--
--========================================================================
--
--    cabhCdpLanAddrTable (CDP LAN Address Table)
--
--    The cabhCdpLanAddrTable contains the DHCP parameters
--    for each IP address served to the LAN-Trans realm.
--
--    This table contains a list of entries for the LAN side CDP
--    parameters. These parameters can be set
--    either by the CDP or by the cable operator through the CMP.
--
--========================================================================

cabhCdpLanAddrTable OBJECT-TYPE
       SYNTAX      SEQUENCE OF CabhCdpLanAddrEntry
       MAX-ACCESS  not-accessible
       STATUS      current
       DESCRIPTION
               "This table is a list of LAN-Trans realm parameters.
               This table has one row entry for each allocated
               LAN-Trans IP address.  Each row must have at least a
```

```
                valid cabhCdpLanAddrMethod, a cabhCdpLanAddrIpType, a
                unique cabhCdpLanAddrIp, and a unique
                cabhCdpLanAddrClientId value.

                Static/Manual address assignment: To create a new DHCP
                address reservation, the NMS creates a row with: an
                index comprised of a new cabhCdpLanAddrIp and its
                cabhCdpLanAddrIpType, a new unique
                cabhCdpLanAddrClientID, (an empty LeaseCreateTime and
                empty LeaseExpireTime,) and a
                cabhCdpLanDataAddrRowStatus of createAndGo(4).  If the
                syntax and values of the new row - indicating a
                reservation - are valid, the PS must set
                cabhCdpLanAddrMethod to reservationInactive(1) and
                cabhCdpLanDataAddrRowStatus to active(1).  When the PS
                grants a lease for a reserved IP, it must set the
                cabhCdpLanAddrMethod object for that row to
                reservationActive(2).  When a lease for a reserved IP
                expires, the PS must set the corresponding row's
                cabhCdpLanAddrMethod object to reservationInactive(1).
                For row entries that represent lease reservations - rows
                in which the cabhCdpLanAddrMethod object has a value of
                either reservationInactive(1) or reservationActive(2) -
                the cabhCdpLanAddrIpType, cabhCdpLanAddrIp,
                cabhCdpLanAddrClientID, cabhCdpLanAddrMethod, and
                cabhCdpLanAddrHostName object values must persist across
                PS reboots.

                Dynamic address assignment:  When the PS grants a lease
                for a non-reserved IP, it must set the
                cabhCdpLanAddrMethod object for that row to
                dynamicActive(4).  When a lease for a non-reserved IP
                expires, the PS must set the corresponding row's
                cabhCdpLanAddrMethod object to dynamicInactive(3).  The
                PS must create new row entries using cabhCdpLanAddrIp
                values that are unique to this table.  If all
                cabhCdpLanAddrIp values in the range defined by
                cabhCdpLanPoolStart and cabhCdpLanPoolEnd are in use in
                this table, the PS may overwrite the
                cabhCdpLanAddrClientId of a row that has a
                cabhCdpLanAddrMethod object with a value of
                dynamicInactive(3) with a new cabhCdpLanAddrClientId
                value and use that cabhCdpLanAddrIp as part of a new
                lease.  For row entries that represent active leases -
                rows in which the cabhCdpLanAddrMethod object has a
                value of dynamicActive(4) - the cabhCdpLanAddrIpType,
                cabhCdpLanAddrIp, cabhCdpLanAddrClientID,
                cabhCdpLanAddrMethod, and cabhCdpLanAddrHostName object
                values must persist across PS reboots."
    ::= { cabhCdpAddr 1 }

cabhCdpLanAddrEntry OBJECT-TYPE
    SYNTAX      CabhCdpLanAddrEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "List of general parameters pertaining to LAN-Trans IP
            address reservations and leases."
    INDEX { cabhCdpLanAddrIpType, cabhCdpLanAddrIp }
    ::= { cabhCdpLanAddrTable 1 }
```

```
CabhCdpLanAddrEntry ::= SEQUENCE {
    cabhCdpLanAddrIpType             InetAddressType,
    cabhCdpLanAddrIp                 InetAddress,
    cabhCdpLanAddrClientID           PhysAddress,
    cabhCdpLanAddrLeaseCreateTime    DateAndTime,
    cabhCdpLanAddrLeaseExpireTime    DateAndTime,
    cabhCdpLanAddrMethod             INTEGER,
    cabhCdpLanAddrHostName           SnmpAdminString,
    cabhCdpLanAddrRowStatus          RowStatus
    }

cabhCdpLanAddrIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The type of IP address assigned to the LAN IP Device
            in the LAN-Trans Realm."
    ::= { cabhCdpLanAddrEntry 1 }

cabhCdpLanAddrIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The address assigned to the LAN IP Device. This parameter
            is entered by the CDP when the CDS grants a lease to a
            LAN IP Device in the LAN-Trans realm and creates a row
            in this table. Alternatively, this parameter can be
            entered by the NMS through the CMP, when the NMS creates
            a new DHCP address reservation.  Each cabhCdpLanAddrIp
            in the table must fall within the range of IPs defined
            inclusively by cabhCdpLanPoolStart and
            cabhCdpLanPoolEnd.  The PS must return an
            inconsistentValue error if the NMS attempts to
            create a row entry with a cabhCdpLanAddrIP value that falls
            outside of this range or is not unique from all existing
            cabhCdpLanAddrIP entries in this table. The address type of
            this object is specified by cabhCdpLanAddrIpType."
    ::= { cabhCdpLanAddrEntry 2 }

cabhCdpLanAddrClientID OBJECT-TYPE
    SYNTAX      PhysAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The client's (i.e., LAN IP Device's) hardware address as
            indicated in the chaddr field of its DHCP REQUEST message.
            There is a one-to-one relationship between the hardware
            address and the LAN IP Device. This parameter is entered
            by the PS (CDP) when the CDS grants a lease to a LAN IP
            Device in the LAN-Trans realm and creates a row in this
            table. Alternatively this parameter can be created by the
            NMS through the CMP, when the NMS creates a new DHCP
            address reservation by accessing the
            cabhCdpLanDataAddrRowStatus object with an index
            comprised of a unique cabhCdpLanAddrIp and creating
            a row with a unique cabhCdpLanAddrClientID."
    ::= { cabhCdpLanAddrEntry 3 }

cabhCdpLanAddrLeaseCreateTime OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
            "This is the date and time when the LAN IP lease was
            created (if it has not yet been renewed) or last renewed.
            This MIB object contains a zero valued 11-byte string
            when a reservation is created for a LAN IP address
            and it maintains this value until the LAN IP Device
            acquires its lease and cabhCdpLanAddrMethod
            becomes reservationActive(2)."
    ::= { cabhCdpLanAddrEntry 4 }

cabhCdpLanAddrLeaseExpireTime OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This is the date and time when the LAN IP address lease
            expired or will expire. This MIB object contains a zero
            valued 11-byte string when a reservation is created for
            a LAN IP address and it maintains this value until the
            LAN IP Device acquires its lease and
            cabhCdpLanAddrMethod becomes reservationActive(2)."
    ::= { cabhCdpLanAddrEntry 5 }

cabhCdpLanAddrMethod OBJECT-TYPE
    SYNTAX      INTEGER {
                    mgmtReservationInactive(1),
                    mgmtReservationActive(2),
                    dynamicInactive(3),
                    dynamicActive(4),
                    psReservationInactive(5),
                    psReservationActive(6)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The IP allocation method indicated by this row.

            The value of mgmtReservationInactive(1)
            indicates an externally provisioned IP address
            reservation that has not yet been leased or that
            has an expired lease. This indicates an IP address
            lease reservation created either by an operator or
            a user.

            The value of mgmtReservationActive(2)
            indicates an externally provisioned IP address
            reservation that has an active lease. This indicates
            an IP address lease reservation created either
            by an operator or a user.

            The value of dynamicInactive(3) indicates an
            IP address that was once dynamically assigned to a
            LAN-Trans by the PS device but currently
            has an expired lease.

            The value of dynamicActive(4)indicates an IP
            Address that was dynamically assigned to a
            LAN-Trans device by the PS and has a current
            active lease.

            The value of psReservationInactive(5)
            indicates an IP address reservation created by some
            internal process of the PS and has not yet been
            leased or has an expired lease.
```

```
            The value of psReservationActive(6)
            indicates an IP address reservation created by some
            internal process of the PS that has an active lease."
    ::= { cabhCdpLanAddrEntry 6 }

cabhCdpLanAddrHostName OBJECT-TYPE
    SYNTAX      SnmpAdminString(SIZE(0..80))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This is the Host Name of the LAN IP address, based on DCHP
            option 12."
    ::= { cabhCdpLanAddrEntry 7 }

cabhCdpLanAddrRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The RowStatus interlock for creation and deletion of row
            entries. The PS must not allow the NMS to set RowStatus
            to notInService(2). The PS must assign a RowStatus of
            notInService(2) to any new row entry created with a
            non-unique, cabhCdpLanAddrClientID value. The PS must
            assign a RowStatus of notReady(3) to any new row entry
            created without a cabhCdpLanAddrClientID.  The PS will
            prevent modification of this table's columns and return an
            inconsistentValue error, if the NMS attempts to make such
            modifications while the RowStatus is active(1)."
    ::= { cabhCdpLanAddrEntry 8 }

--================================================================================
--
--    cabhCdpWanDataAddrTable (CDP WAN-Data Address Table)
--
--    The cabhCdpWanDataAddrTable contains the configuration or DHCP
--    parameters for each IP address mapping per WAN-Data IP Address.
--
--================================================================================

cabhCdpWanDataAddrTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCdpWanDataAddrEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains WAN-Data address realm information."
    ::= { cabhCdpAddr 2 }

cabhCdpWanDataAddrEntry OBJECT-TYPE
    SYNTAX      CabhCdpWanDataAddrEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "List of general parameter for CDP WAN-Data address realm."
    INDEX { cabhCdpWanDataAddrIndex }
    ::= { cabhCdpWanDataAddrTable 1 }

CabhCdpWanDataAddrEntry ::= SEQUENCE {
    cabhCdpWanDataAddrIndex        INTEGER,
    cabhCdpWanDataAddrClientId     OCTET STRING,
    cabhCdpWanDataAddrIpType       InetAddressType,
    cabhCdpWanDataAddrIp           InetAddress,
    cabhCdpWanDataAddrRenewalTime  Integer32,
```

```
    cabhCdpWanDataAddrRowStatus    RowStatus,
    cabhCdpWanDataAddrLeaseCreateTime DateAndTime,
    cabhCdpWanDataAddrLeaseExpireTime DateAndTime
    }

cabhCdpWanDataAddrIndex OBJECT-TYPE
    SYNTAX      INTEGER (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Index into table."
    ::= { cabhCdpWanDataAddrEntry 1 }

cabhCdpWanDataAddrClientId OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (1..80))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "A unique WAN-Data ClientID used when attempting
            to acquire a WAN-Data IP Address via DHCP."
    ::= { cabhCdpWanDataAddrEntry 2 }

cabhCdpWanDataAddrIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The address type assigned on the WAN-Data side."
    DEFVAL { ipv4 }
    ::= { cabhCdpWanDataAddrEntry 3 }

cabhCdpWanDataAddrIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The address assigned on the WAN-Data side."
    ::= { cabhCdpWanDataAddrEntry 4 }

cabhCdpWanDataAddrRenewalTime OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
            "This is the time remaining before the lease expires.
            This is based on DHCP Option 51."
    ::= { cabhCdpWanDataAddrEntry 5 }

cabhCdpWanDataAddrRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The RowStatus interlock for creation and deletion of row
            entries.  Any writable object in a row can be modified at
            any time while the row is active(1).  The PS must assign a
            RowStatus of notInService(2) to any new row entry created
            with a cabhCdpWanDataAddrClientId that is not unique within
            this table."
    ::= { cabhCdpWanDataAddrEntry 6 }
```

```
cabhCdpWanDataAddrLeaseCreateTime OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This is the date and time when the WAN-Data address lease
            was created (if it has not yet been renewed) or last
            renewed."
    ::= { cabhCdpWanDataAddrEntry 7 }

cabhCdpWanDataAddrLeaseExpireTime OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This is the date and time when the WAN-Data address
             lease expired or will expire."
    ::= { cabhCdpWanDataAddrEntry 8 }

--=================================================================
--
-- cabhCdpWanDnsServerTable (CDP WAN DNS Server Table)
--
-- The cabhCdpWanDnsServerTable is a table of 3 cable network
-- and Internet DNS Servers.
--
--=================================================================
cabhCdpWanDnsServerTable OBJECT-TYPE
    SYNTAX SEQUENCE OF CabhCdpWanDnsServerEntry
    MAX-ACCESS not-accessible
    STATUS current
    DESCRIPTION
            "This table contains the IP addresses of cable network and
            Internet DNS servers, in the order of preference in which
            the PS's CNP will query them, when it cannot resolve a DNS
            query using local information. Entries in this table are
            updated with the information contained in DHCP option 6,
            received during both the WAN-Man and WAN-Data IP
            acquisition processes."
    ::= { cabhCdpAddr 3 }

cabhCdpWanDnsServerEntry OBJECT-TYPE
    SYNTAX      CabhCdpWanDnsServerEntry
    MAX-ACCESS  not-accessible
    STATUS     current
    DESCRIPTION
            "List of cable network and Internet DNS servers."
    INDEX { cabhCdpWanDnsServerOrder }
    ::= { cabhCdpWanDnsServerTable 1 }

CabhCdpWanDnsServerEntry ::= SEQUENCE {
    cabhCdpWanDnsServerOrder  INTEGER,
    cabhCdpWanDnsServerIpType InetAddressType,
    cabhCdpWanDnsServerIp     InetAddress
    }

cabhCdpWanDnsServerOrder OBJECT-TYPE
    SYNTAX      INTEGER {
                    primary(1),
                    secondary(2),
                    tertiary(3)
                }
    MAX-ACCESS  not-accessible
    STATUS      current
```

```
    DESCRIPTION
            "The order of preference for cable network and Internet DNS
            servers, as listed in DHCP option 6 (Domain Server). Any
            time the CDC receives valid IP address information within
            DHCP option 6, as part of lease acquisition or renewal of
            a WAN-Man or WAN-Data IP, it must update this information
            into this table.  As entries in DHCP option 6 are listed in
            order of preference, the highest priority entry in DHCP
            option 6 must correspond to the row with a
            cabhCdpWanDnsServerOrder with a value of 1. If DHCP
            option 6 contains 1 valid IP address, the PS MUST update
            the row with a cabhCdpWanDnsServerOrder value of 1 and
            MUST NOT modify rows with
            cabhCdpWanDnsServerOrder values of 2 & 3
            (if they exist). If DHCP option 6 contains 2 valid
            IP addresses, the PS MUST update the rows with
            cabhCdpWanDnsServerOrder values of 1 and 2
            and MUST NOT modify the row with cabhCdpWanDnsServerOrder
            value of 3 (if it exists). If DHCP option 6 contains 3
            valid IP addresses, the PS MUST update rows with
            cabhCdpWanDnsServerOrder values of 1, 2, and 3.
            Any DNS server information included in DHCP option 6
            beyond primary, secondary and tertiary will not be
            represented in this table."
    ::= { cabhCdpWanDnsServerEntry 1 }

cabhCdpWanDnsServerIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
            "This parameter indicates the IP address type of a
            WAN DNS server."
    DEFVAL { ipv4 }
    ::= { cabhCdpWanDnsServerEntry 2 }

cabhCdpWanDnsServerIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This parameter indicates the IP address of a WAN DNS
            server. The type of this address is specified by
            cabhCdpWanDnsServerIpType."
    ::= { cabhCdpWanDnsServerEntry 3 }

--
--    DHCP Server Side (CDS) Option Values for the LAN-Trans realm
--

cabhCdpLanPoolStartType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Address type of the start of range LAN Trans IP
            Addresses."
    DEFVAL { ipv4 }
    ::= { cabhCdpServer 1 }

cabhCdpLanPoolStart OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
```

```
    DESCRIPTION
            "The start of range LAN Trans IP Addresses. The type of
            this address is specified by cabhCdpLanPoolStartType."
    DEFVAL { 'c0a8000a'h }    -- 192.168.0.10
    -- 192.168.0.0 is the network number
    -- 192.168.0.255 is broadcast
    -- address and 192.168.0.1
    -- is reserved for the router
    ::= { cabhCdpServer 2 }

cabhCdpLanPoolEndType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Address type of the end of range LAN Trans IP
            Addresses."
    DEFVAL { ipv4 }
    ::= { cabhCdpServer 3 }

cabhCdpLanPoolEnd OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The end of range for LAN-Trans IP Addresses. The type of
            this address is specified by cabhCdpLanPoolEndType."
    DEFVAL { 'c0a800fe'h }    -- 192.168.0.254
    ::= { cabhCdpServer 4 }

cabhCdpServerNetworkNumberType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The IP address type of the LAN-Trans network number."
    DEFVAL { ipv4 }
    ::= { cabhCdpServer 5 }

cabhCdpServerNetworkNumber OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The LAN-Trans network number. The type of this address is
            specified by cabhCdpServerNetworkNumberType."
    DEFVAL { 'c0a80000'h } --192.168.0.0
    ::= { cabhCdpServer 6 }

cabhCdpServerSubnetMaskType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Type of LAN-Trans Subnet Mask."
    DEFVAL { ipv4 }
    ::= { cabhCdpServer 7 }

cabhCdpServerSubnetMask OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
```

```
    DESCRIPTION
            "The PS MUST provide the value of this MIB
            object in option 1 (Subnet Mask) of
            DHCP OFFER and ACK messages sent to a LAN IP Device."
    DEFVAL { 'ffffff00'h }    -- 255.255.255.0
    ::= { cabhCdpServer 8 }

cabhCdpServerTimeOffset OBJECT-TYPE
    SYNTAX      Integer32 (-86400..86400) -- 0 to 24 hours (in seconds)
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The PS MUST provide the value of this MIB object in
            option 2 (Time Offset from Coordinated
            Universal Time-UTC) in the DHCP OFFER and ACK
            messages sent to the LAN IP Device."
    DEFVAL { 0 }    -- UTC
    ::= { cabhCdpServer 9 }

cabhCdpServerRouterType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Type of Address, Router for the LAN-Trans
            address realm."
    DEFVAL { ipv4 }
    ::= { cabhCdpServer 10 }

cabhCdpServerRouter OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The type of this address is specified by
            cabhCdpServerRouterType. The PS MUST
            provide the value of this MIB object in
            option 3 (Router IP address) of the DHCP
            OFFER and ACK messages sent to the LAN IP Device."
    DEFVAL { 'c0a80001'h }    -- 192.168.0.1
    ::= { cabhCdpServer 11 }

cabhCdpServerDnsAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Type of IP Addresses of the LAN-Trans address realm
            DNS servers."
    DEFVAL { ipv4 }
    ::= { cabhCdpServer 12 }

cabhCdpServerDnsAddress OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The default value of this MIB object is the
            same as the value of the cabhCdpServerRouter
            object. The NMS may set the value of this
            object to a value different than the value
            of cabhCdpServerRouter (e.g., DNS server in the
            cable data network) so that a LAN IP Device can direct its
```

```
            DNS queries to a server other than the PS DNS
            server. The type of this address is specified
            by cabhCdpServerDnsAddressType. The PS MUST
            provide the value of this MIB object in option 6
            (Domain Name Server) of DHCP OFFER and ACK
            messages sent to a LAN IP Device."
    ::= { cabhCdpServer 13 }

cabhCdpServerSyslogAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Type of IP Address of the LAN-Trans SYSLOG servers."
    DEFVAL { ipv4 }
    ::= { cabhCdpServer 14 }

cabhCdpServerSyslogAddress OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "If the value of this object is non-zero, the PS will
            include the value of this object in DHCP option 7
            (Log Servers) in DHCP OFFER and DHCP ACK messages
            sent to the LAN IP Device."
    DEFVAL { '00000000'h }    -- 0.0.0.0
    ::= { cabhCdpServer 15 }

cabhCdpServerDomainName OBJECT-TYPE
    SYNTAX      SnmpAdminString(SIZE(0..128))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The PS MUST provide the value of this MIB object
            in option 15 (Domain Name Option) of the DHCP
            OFFER and ACK messages sent to the LAN IP Device."
    DEFVAL { "" }
    ::= { cabhCdpServer 16 }

cabhCdpServerTTL OBJECT-TYPE
    SYNTAX      INTEGER (1..255)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The PS MUST provide the value of this MIB
             object in option 23 (Default IP TTL) of
             DHCP OFFER and ACK messages sent to a LAN IP Device."
    DEFVAL { 64 }
    ::= { cabhCdpServer 17 }

cabhCdpServerInterfaceMTU OBJECT-TYPE
    SYNTAX      Integer32 (0 | 68..4096)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The PS MUST provide the value of this MIB object in
            option 26 (Interface MTU Option) of the DHCP OFFER
            and ACK messages sent to the LAN IP Device. If the value
            of this object is 0, the PS must not include this option
            in its DHCP OFFER or DHCP ACK messages to LAN IP Devices."
    DEFVAL { 0 }
    ::= { cabhCdpServer 18 }
```

```
cabhCdpServerVendorSpecific OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0..255))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The PS MUST provide the value of this MIB object in
            option 43 (Vendor Specific Information) of the DHCP OFFER
            and ACK messages sent to the LAN IP Device. If the value of
            this object is ' 'h,  then the PS MUST NOT include this
            option in its DHCP OFFER or DHCP ACK messages to LAN IP
            Devices."
    DEFVAL { ''h }
    ::= { cabhCdpServer 19 }

cabhCdpServerLeaseTime OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The PS MUST provide the value of this MIB object in
            option 51 (IP Address lease time) of the DHCP OFFER and
            ACK messages sent to the LAN IP Device."
    DEFVAL { 3600 }
    ::= { cabhCdpServer 20 }

cabhCdpServerDhcpAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Type of LAN DHCP server IP address. The
            IP address of LAN DHCP server is provided by
            the PS in option 54 of DHCP OFFER or ACK."
    DEFVAL { ipv4 }
    ::= { cabhCdpServer 21 }

cabhCdpServerDhcpAddress OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The value of this MIB object is always the
            same as the value of the cabhCdpServerRouter
            object. The type of this address is specified
            by cabhCdpServerDhcpAddressType.
            The PS MUST provide the value of this MIB
            object in option 54 (DHCP server identifier)
            field of DHCP OFFER and ACK messages
            sent to a LAN IP device."
    ::= { cabhCdpServer 22 }


cabhCdpServerControl OBJECT-TYPE
    SYNTAX      INTEGER {
                    restoreConfig(1),
                    commitConfig(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The control for the CDS (DHCP Server) configuration.
            All changes to the cabhCdpServer MIB objects are reflected
            when reading the value of the MIB objects; however, those
```

```
            changes are NOT applied to the running configuration of
            the CDS until they are successfully committed via use
            of the cabhCdpServerControl object.

            If changes are made to the cabhCdpServer MIB objects which
            are not yet successfully committed to the CDS, the
            cabhCdpServerControl object can be used to roll back all
            changes to the last valid CDS configuration and discard
            all intermediate changes.

            restoreConfig - Setting cabhCdpServerControl to this value
            will cause any changes to the cabhCdpServer objects not yet
            committed be reset to the values from the current running
            configuration of the CDS.

            commitConfig - Setting cabhCdpServerControl to this value
            will cause the CDS to validate and apply the valid
            cabhCdpServer MIB settings to its running configuration.
            The cabhCdpServerCommitStatus object will detail the
            status of this operation."
    DEFVAL { restoreConfig }
    ::= { cabhCdpServer 23 }

cabhCdpServerCommitStatus OBJECT-TYPE
    SYNTAX      INTEGER {
                    commitSucceeded(1),
                    commitNeeded(2),
                    commitFailed(3)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Indicates the status of committing the current
            cabhCdpServer MIB object values to the running
            configuration of the CDS (DHCP Server).

            commitSucceeded - indicates the current cabhCdpServer
            MIB object values are valid and have been successfully
            committed to the running configuration of the CDS.

            commitNeeded - indicates that the value of one or more
            objects in cabhCdpServer MIB group have been changed
            but not yet committed to the running configuration
            of the CDS.

            commitFailed - indicates the PS was unable to commit the
            cabhCdpServer MIB object values to the running
            configuration of the CDS due to conflicts in those
            values."
    DEFVAL { commitSucceeded }
    ::= { cabhCdpServer 24 }

cabhCdpServerUseCableDataNwDnsAddr OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "If the value of this object is false(2), the PS will
            provide the DNS Server IP address as specified in
            cabhCdpServerDnsAddress MIB object in option 6
            (Domain Name Server) of the DHCP OFFER and ACK messages
            sent to a LAN IP Device.
```

```
            When the object cabhCdpServerUseCableDataNwDnsAddr is set
            to true(1), the PS must take the following actions:
            The PS will provide in option 6 (Domain Name Server), of
            the DHCP OFFER and ACK messages sent to a LAN IP Device,
            the DNS server address(es) which is/are being used by the
            PS itself, i.e., the DNS server address(es) provided to the
            PS in DHCP option 6 and made available through PS MIB
            object cabhCdpWanDnsServerIp.

            The LAN IP Device can then direct its DNS queries to a
            server other than the PS DNS server. The PS MUST provide
            the value of this."
    DEFVAL { false }
    ::= { cabhCdpServer 25 }

--
-- notification group is for future extension.
--

cabhCdpNotification OBJECT IDENTIFIER ::= { cabhCdpMib 2 }
cabhCdpNotifications OBJECT IDENTIFIER ::= { cabhCdpNotification 0 }
cabhCdpConformance  OBJECT IDENTIFIER ::= { cabhCdpMib 3 }
cabhCdpCompliances  OBJECT IDENTIFIER ::= { cabhCdpConformance 1 }
cabhCdpGroups       OBJECT IDENTIFIER ::= { cabhCdpConformance 2 }

--
--    Notification Group
--


-- compliance statements

cabhCdpBasicCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
            "The compliance statement for devices that implement
            the CableHome Portal Services functionality."
    MODULE   --cabhCdpMib


-- unconditionally mandatory groups

MANDATORY-GROUPS {
    cabhCdpGroup
    }

    ::= { cabhCdpCompliances 3 }

cabhCdpGroup OBJECT-GROUP
    OBJECTS {
    cabhCdpSetToFactory,
    cabhCdpLanTransCurCount,
    cabhCdpLanTransThreshold,
    cabhCdpLanTransAction,
    cabhCdpWanDataIpAddrCount,
    cabhCdpLastSetToFactory,
    cabhCdpTimeOffsetSelection,
    cabhCdpSnmpSetTimeOffset,
    cabhCdpDaylightSavingTimeEnable,

    cabhCdpLanAddrClientID,
    cabhCdpLanAddrLeaseCreateTime,
    cabhCdpLanAddrLeaseExpireTime,
    cabhCdpLanAddrMethod,
```

```
    cabhCdpLanAddrHostName,
    cabhCdpLanAddrRowStatus,

    cabhCdpWanDataAddrClientId,
    cabhCdpWanDataAddrIpType,
    cabhCdpWanDataAddrIp,
    -- cabhCdpWanDataAddrRenewalTime,
    cabhCdpWanDataAddrRowStatus,
    cabhCdpWanDataAddrLeaseCreateTime,
    cabhCdpWanDataAddrLeaseExpireTime,

    cabhCdpWanDnsServerIpType,
    cabhCdpWanDnsServerIp,

    cabhCdpLanPoolStartType,
    cabhCdpLanPoolStart,
    cabhCdpLanPoolEndType,
    cabhCdpLanPoolEnd,
    cabhCdpServerNetworkNumberType,
    cabhCdpServerNetworkNumber,
    cabhCdpServerSubnetMaskType,
    cabhCdpServerSubnetMask,
    cabhCdpServerTimeOffset,
    cabhCdpServerRouterType,
    cabhCdpServerRouter,
    cabhCdpServerDnsAddressType,
    cabhCdpServerDnsAddress,
    cabhCdpServerSyslogAddressType,
    cabhCdpServerSyslogAddress,
    cabhCdpServerDomainName,
    cabhCdpServerTTL,
    cabhCdpServerInterfaceMTU,
    cabhCdpServerVendorSpecific,
    cabhCdpServerLeaseTime,
    cabhCdpServerDhcpAddressType,
    cabhCdpServerDhcpAddress,
    cabhCdpServerControl,
    cabhCdpServerCommitStatus,
    cabhCdpServerUseCableDataNwDnsAddr
    }
    STATUS      current
    DESCRIPTION
            "Group of objects for CableHome CDP MIB."
    ::= { cabhCdpGroups 1 }

END
```

E.3 Requisitos de la MIB portal de pruebas IPCable2Home (CTP, IPCable2Home Test Portal)

La MIB CTP IPCable2Home DEBE implementarse tal como se define a continuación.

```
CABH-CTP-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE           FROM SNMPv2-SMI
    TimeStamp,
    TruthValue            FROM SNMPv2-TC
    OBJECT-GROUP,
    MODULE-COMPLIANCE     FROM SNMPv2-CONF
    InetAddressType,
    InetAddress           FROM INET-ADDRESS-MIB
    clabProjCableHome     FROM CLAB-DEF-MIB;
```

```
cabhCtpMib MODULE-IDENTITY
    LAST-UPDATED  "200404090000Z" -- April 9, 2004
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
            858 Coal Creek Circle
            Louisville, Colorado 80027
            U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com or mibs@cablelabs.com"
    DESCRIPTION
            "This MIB module defines control and monitoring objects
            for remote diagnostic tools for a CableHome LAN
            supported by the CableHome Test Portal (CTP) as
            defined and described in CableLabs' CableHome
            specifications."
    ::=  { clabProjCableHome 5 }

-- Textual conventions


cabhCtpObjects           OBJECT IDENTIFIER ::= { cabhCtpMib 1 }
cabhCtpBase              OBJECT IDENTIFIER ::= { cabhCtpObjects 1 }
cabhCtpConnSpeed         OBJECT IDENTIFIER ::= { cabhCtpObjects 2 }
cabhCtpPing              OBJECT IDENTIFIER ::= { cabhCtpObjects 3 }

--
--    The following group describes the base objects in the CableHome
--    Management Portal.
--

cabhCtpSetToFactory OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Setting this object to true(1) causes all the tables
            in the CTP MIB to be cleared, and all CTP MIB objects
            with default values set back to those default values.
            Reading this object always returns false(2)."
    ::={ cabhCtpBase 1 }

cabhCtpLastSetToFactory OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The value of sysUpTime when cabhCtpSetToFactory
            was last set to true. Zero if never reset."
    ::={ cabhCtpBase 2 }

--
--    Parameter and results from Connection Speed Command
--

cabhCtpConnSrcIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
```

```
    DESCRIPTION
            "The IP Address type used as the source address for the
            Connection Speed Test.
            The PS MUST NOT allow the value of cabhCtpConnSrcIpType
            to be changed if cabhCtpConnStatus = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpConnSrcIpType when the
            value of cabhCtpConnStatus is running(2)."
    DEFVAL { ipv4 }
    ::= { cabhCtpConnSpeed 1 }

cabhCtpConnSrcIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The IP Address used as the source address for the
            Connection Speed Test. The default value is the value
            of cabhCdpServerRouter (192.168.0.1). The type of
            this address is specified by cabhCtpConnSrcIpType.
            The PS MUST NOT allow the value of cabhCtpConnSrcIp
            to be changed if cabhCtpConnStatus = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpConnSrcIp when the
            value of cabhCtpConnStatus is running(2)."
    REFERENCE
            "CableHome Specification, Management Tools - PS
            Logical Element CableHome Test Portal (CTP) section."
    DEFVAL { 'c0a80001'h }    -- 192.168.0.1
    ::= { cabhCtpConnSpeed 2 }

cabhCtpConnDestIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The IP Address Type for the CTP Connection Speed Tool
            destination address.
            The PS MUST NOT allow the value of cabhCtpConnDestIpType
            to be changed if cabhCtpConnStatus = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpConnDestIpType when the
            value of cabhCtpConnStatus is running(2)."
    DEFVAL { ipv4 }
    ::={ cabhCtpConnSpeed 3 }

cabhCtpConnDestIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The IP Address used as the destination address for the
            Connection Speed Test. The type of this address is
            specified by cabhCtpConnDestIpType. The PS MUST NOT allow
            the value of cabhCtpConnDestIp to be changed if
            cabhCtpConnStatus = running(2). The PS MUST return
            inconsistentValue error to a manager that attempts
            to set the value of cabhCtpConnDestIp when the value of
            cabhCtpConnStatus is running(2)."
    ::= { cabhCtpConnSpeed 4 }
```

```
cabhCtpConnProto OBJECT-TYPE
    SYNTAX      INTEGER {
                    udp(1),
                    tcp(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The protocol used in the Connection Speed Test. TCP
            testing is optional.
            The PS MUST NOT allow the value of cabhCtpConnProto
            to be changed if cabhCtpConnStatus = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpConnProto when the
            value of cabhCtpConnStatus is running(2)."
    DEFVAL { udp }
    ::= { cabhCtpConnSpeed 5 }

cabhCtpConnNumPkts OBJECT-TYPE
    SYNTAX      INTEGER (1..65535)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The number of OSI Layer 3 (IP) packets the CTP is to
            send when triggered to execute the Connection Speed Tool.
            The PS MUST NOT allow the value of cabhCtpConnNumPkts
            to be changed if cabhCtpConnStatus = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpConnNumPkts when the
            value of cabhCtpConnStatus is running(2)."
    DEFVAL { 100 }
    ::= { cabhCtpConnSpeed 6 }

cabhCtpConnPktSize OBJECT-TYPE
    SYNTAX      INTEGER (64..1518)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The size of each OSI Layer 2 frame to be
            sent by the PS CableHome Test Portal
            function when configured to execute the
            Connection Speed remote diagnostic tool.
            The PS MUST NOT allow the value of cabhCtpConnPktSize
            to be changed if cabhCtpConnStatus = running(2).
            The PS MUST return inconsistentValue error
            to a manager that attempts to set the value of
            cabhCtpConnPktSize when the value of cabhCtpConnStatus
            is running(2)."
    REFERENCE
            "CableHome Specification, Management Tools - PS
            Logical Element CableHome Test Portal (CTP) section."
    DEFVAL { 1518 }
    ::= { cabhCtpConnSpeed 7 }

cabhCtpConnTimeOut OBJECT-TYPE
    SYNTAX      INTEGER (0..600000)           -- Max 10 minutes
    UNITS       "milliseconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The timeout value for the response.  A value of zero
            indicates no time out and can be used for TCP only.
            The PS MUST NOT allow the value of cabhCtpConnTimeOut
```

```
            to be changed if cabhCtpConnStatus = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpConnTimeOut when the
            value of cabhCtpConnStatus is running(2)."
    DEFVAL {30000}  -- 30 seconds
    ::= { cabhCtpConnSpeed 8 }

cabhCtpConnControl OBJECT-TYPE
    SYNTAX      INTEGER {
                    start(1),
                    abort(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The control for the Connection Speed Tool. Setting this
            object to start(1) causes the Connection Speed Tool to
            execute. Setting this object to abort(2) causes the
            Connection Speed Tool to stop running. This parameter
            should only be set via SNMP."
    DEFVAL  {abort }
    ::={ cabhCtpConnSpeed 9 }

cabhCtpConnStatus OBJECT-TYPE
    SYNTAX      INTEGER {
                    notRun(1),
                    running(2),
                    complete(3),
                    aborted(4),
                    timedOut(5)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object returns the status of the Connection Speed
            Tool. The value notRun(1) indicates that the Connection
            Speed Tool has not been run since the Portal Services
            element of the CableHome residential gateway was
            initialized or reset.

            The value running(2) indicates that the Connection Speed
            Tool was initiated by a manager
            (cabhCtpConnControl = start(1)) and the test has not
            timed out and the PS has not yet completed sending
            all the packets it was configured to send or it has not
            received all responses.

            The value complete(3) indicates that the Connection Speed
            Tool was initiated by a manager, successfully sent all the
            packets it was configured to send, received all responses,
            and is no longer sending packets or waiting for responses.

            The value aborted(4) indicates that the Connection Speed
            Tool was initiated by a manager then was terminated by the
            manager by setting cabhCtpConnControl = abort(2).
            The Connection Speed Tool is no longer sending packets or
            waiting for responses.

            The value timedOut(5) indicates that the Connection Speed Tool
            was initiated by a manager and had not received all responses
            from the client but the amount of time allowed for the
            Connection Speed Tool to execute, defined by the value of
            cabhCtpConnTimeOut, has transpired. The Connection Speed Tool
            is no longer sending packets or waiting for responses."
```

```
    DEFVAL { notRun }
    ::={ cabhCtpConnSpeed 10 }

cabhCtpConnPktsSent OBJECT-TYPE
    SYNTAX      INTEGER (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of packets the CTP sent after it was
            triggered to execute the Connection Speed Tool."
    ::= { cabhCtpConnSpeed 11 }

cabhCtpConnPktsRecv OBJECT-TYPE
    SYNTAX      INTEGER (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of packets the CTP received after it
            executed the Connection Speed Tool."
    ::= { cabhCtpConnSpeed 12 }

cabhCtpConnRTT OBJECT-TYPE
    SYNTAX      INTEGER (0..600000)
    UNITS       "millisec"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The resulting round trip time for the set of
            packets sent to and received from the target
            LAN IP Device."
    ::= { cabhCtpConnSpeed 13 }

cabhCtpConnThroughput OBJECT-TYPE
    SYNTAX      INTEGER (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The average round-trip throughput measured in
            kilobits per second."
    ::= { cabhCtpConnSpeed 14 }

--
--    Parameters and Results for Ping Command
--

cabhCtpPingSrcIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The IP Address Type for CTP Ping Tool source address.
            The PS MUST NOT allow the value of cabhCtpPingSrcIpType
            to be changed if cabhCtpPingStatus = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpPingSrcIpType when the
            value of cabhCtpPingStatus is running(2)."
    DEFVAL { ipv4 }
    ::={ cabhCtpPing 1 }

cabhCtpPingSrcIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
```

```
    DESCRIPTION
            "The IP Address used as the source address for the Ping
            Test. The default value is the value of
            CabhCdpServerRouter (192.168.0.1). The type of this
            address is specified by cabhCtpPingSrcIpType.
            The PS MUST NOT allow the value of cabhCtpPingSrcIp
            to be changed if cabhCtpPingTimeOut = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpPingSrcIp when the
            value of cabhCtpPingTimeOut is running(2)."
    REFERENCE
            "CableHome Specification, Management Tools - PS
            Logical Element CableHome Test Portal (CTP) section."
    DEFVAL { 'c0a80001'h } --192.168.0.1
    ::= { cabhCtpPing 2 }

cabhCtpPingDestIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The IP Address Type for the CTP Ping Tool destination
            address.
            The PS MUST NOT allow the value of cabhCtpPingDestIpType
            to be changed if cabhCtpPingStatus = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpPingDestIpType when the
            value of cabhCtpPingStatus is running(2)."
    DEFVAL { ipv4 }
    ::={ cabhCtpPing 3 }

cabhCtpPingDestIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Destination IP Address used as the destination
            address for the Ping Test. The type of this address
            is specified by cabhCtpPingDestIpType. The PS MUST NOT
            allow the value of cabhCtpPingDestIp to be changed if
            cabhCtpPingStatus = running(2). The PS MUST return
            inconsistentValue error to a manager that attempts
            to set the value of cabhCtpPingDestIp when the value of
            cabhCtpPingStatus is running(2)."
    ::= { cabhCtpPing 4 }

cabhCtpPingNumPkts OBJECT-TYPE
    SYNTAX      INTEGER (1..4)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The number of ICMP Echo Request messages to send to
            the destination defined by cabhCtpPingDestIp. The PS
            MUST NOT allow the value of cabhCtpPingNumPkts to be
            changed if cabhCtpPingStatus = running(2).  The PS MUST
            return inconsistentValue error to a manager that attempts
            to set the value of cabhCtpPingNumPkts when the value of
            cabhCtpPingStatus is running(2)."
    DEFVAL { 1 }
    ::= { cabhCtpPing 5 }
```

```
cabhCtpPingPktSize OBJECT-TYPE
    SYNTAX      INTEGER (64..1518)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The size of the ICMP Echo Request packets to send to
            the destination defined by cabhCtpPingDestIp. The PS
            MUST NOT allow the value of cabhCtpPingPktSize to be
            changed if cabhCtpPingStatus = running(2).  The PS MUST
            return inconsistentValue error to a manager that attempts
            to set the value of cabhCtpPingPktSize when the value of
            cabhCtpPingStatus is running(2)."
    DEFVAL { 64 }
    ::= { cabhCtpPing 6 }

cabhCtpPingTimeBetween OBJECT-TYPE
    SYNTAX      INTEGER (0..600000)
    UNITS       "milliseconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The time between sending one ping and the next.
            The PS MUST NOT allow the value of cabhCtpPingTimeBetween
            to be changed if the value of cabhCtpPingStatus is
            running(2).  The PS MUST return inconsistentValue error
            to a manager that attempts to set the value of
            cabhCtpPingTimeBetween when the value of
            cabhCtpPingStatus is running(2)."
    DEFVAL { 1000 }
    ::= { cabhCtpPing 7 }

cabhCtpPingTimeOut OBJECT-TYPE
    SYNTAX      INTEGER (1..600000)
    UNITS       "milliseconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The time out for ping response (ICMP reply) for a
            single transmitted ping message (ICMP request).
            The PS MUST NOT allow the value of cabhCtpPingTimeOut
            to be changed if cabhCtpPingStatus = running(2). The PS
            MUST return inconsistentValue error to a manager that
            attempts to set the value of cabhCtpPingTimeOut when the
            value of cabhCtpPingStatus is running(2)."
    DEFVAL { 1000 } -- 1 second
    ::={ cabhCtpPing 8 }

cabhCtpPingControl OBJECT-TYPE
    SYNTAX      INTEGER {
                    start(1),
                    abort(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The control for the Ping Tool. Setting this object
            to start(1) causes the Ping Tool to execute. Setting
            this object to abort(2) causes the Ping Tool to stop
            running. This parameter should only be set via SNMP."
    DEFVAL {abort }
    ::={ cabhCtpPing 9 }
```

```
cabhCtpPingStatus OBJECT-TYPE
    SYNTAX      INTEGER {
                    notRun(1),
                    running(2),
                    complete(3),
                    aborted(4),
                    timedOut(5)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object returns the status of the Ping Tool.

            The value notRun(1) indicates that the Ping Tool
            has not been run since the Portal Services element of the
            CableHome residential gateway was initialized or reset.

            The value running(2) indicates that the Ping Tool
            was initiated by a manager (cabhCtpPingControl = start(1))
            and the test has not timed out and the PS has not yet
            completed sending all the packets it was configured to
            send or it has not received all responses.

            The value complete(3) indicates that the Ping Tool
            was initiated by a manager, successfully sent all the
            packets it was configured to send, received all responses,
            and is no longer sending packets or waiting for responses.

            The value aborted(4) indicates that the Ping Tool was
            initiated by a manager then was terminated by the manager
            by setting cabhCtpPingControl = abort(2). The Ping Tool
            is no longer sending packets or waiting for responses.

            The value timedOut(5) indicates that the Ping Tool was
            initiated by a manager and had not received all responses
            from the client but the amount of time allowed for the
            Ping Tool to execute, defined by the value of
            cabhCtpPingTimeOut, has transpired. The Ping Tool is no
            longer sending packets or waiting for responses."
    DEFVAL { notRun }
    ::={ cabhCtpPing 10 }

cabhCtpPingNumSent OBJECT-TYPE
    SYNTAX      INTEGER (0..4)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of Pings sent."
    ::={ cabhCtpPing 11 }

cabhCtpPingNumRecv OBJECT-TYPE
    SYNTAX      INTEGER (0..255)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of pings received."
    ::= { cabhCtpPing 12 }

cabhCtpPingAvgRTT OBJECT-TYPE
    SYNTAX      INTEGER (0..600000)
    UNITS       "millisec"
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
            "The resulting average of round trip times for
            acknowledged packets."
    ::= { cabhCtpPing 13 }

cabhCtpPingMaxRTT OBJECT-TYPE
    SYNTAX      INTEGER (0..600000)
    UNITS       "millisec"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The resulting maximum of round trip times for
            acknowledged packets."
    ::= { cabhCtpPing 14 }

cabhCtpPingMinRTT OBJECT-TYPE
    SYNTAX      INTEGER (0..600000)
    UNITS       "millisec"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The resulting minimum of round trip times for
            acknowledged packets."
    ::= { cabhCtpPing 15 }

cabhCtpPingNumIcmpError OBJECT-TYPE
    SYNTAX      INTEGER (0..255)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Number of ICMP errors."
    ::= { cabhCtpPing 16 }

cabhCtpPingIcmpError OBJECT-TYPE
    SYNTAX      INTEGER (0..255)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The last ICMP error."
    ::= { cabhCtpPing 17 }

--=====================================================================

--
-- notification group is for future extension.
--

cabhCtpNotification  OBJECT IDENTIFIER ::= { cabhCtpMib 2 }
cabhCtpNotifications OBJECT IDENTIFIER ::= { cabhCtpNotification 0 }
cabhCtpConformance   OBJECT IDENTIFIER ::= { cabhCtpMib 3 }
cabhCtpCompliances   OBJECT IDENTIFIER ::= { cabhCtpConformance 1 }
cabhCtpGroups        OBJECT IDENTIFIER ::= { cabhCtpConformance 2 }

--
--    Notification Group
--

-- compliance statements

cabhCtpBasicCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
            "The compliance statement for devices that implement
            Portal Service feature."
    MODULE   --cabhCtpMib
```

```
-- unconditionally mandatory groups

    MANDATORY-GROUPS {
          cabhCtpGroup
    }

    ::= { cabhCtpCompliances 3 }


cabhCtpGroup OBJECT-GROUP
    OBJECTS {

        cabhCtpSetToFactory,
        cabhCtpLastSetToFactory,
        cabhCtpConnSrcIpType,
        cabhCtpConnSrcIp,
        cabhCtpConnDestIpType,
        cabhCtpConnDestIp,
        cabhCtpConnProto,
        cabhCtpConnNumPkts,
        cabhCtpConnPktSize,
        cabhCtpConnTimeOut,
        cabhCtpConnControl,
        cabhCtpConnStatus,
        cabhCtpConnPktsSent,
        cabhCtpConnPktsRecv,
        cabhCtpConnRTT,
        cabhCtpConnThroughput,

        cabhCtpPingSrcIpType,
        cabhCtpPingSrcIp,
        cabhCtpPingDestIpType,
        cabhCtpPingDestIp,
        cabhCtpPingNumPkts,
        cabhCtpPingPktSize,
        cabhCtpPingTimeBetween,
        cabhCtpPingTimeOut,
        cabhCtpPingControl,
        cabhCtpPingStatus,
        cabhCtpPingNumSent,
        cabhCtpPingNumRecv,
        cabhCtpPingAvgRTT,
        cabhCtpPingMinRTT,
        cabhCtpPingMaxRTT,
        cabhCtpPingNumIcmpError,
        cabhCtpPingIcmpError
        }
    STATUS      current
    DESCRIPTION
            "Group of objects for CableHome CTP MIB."
    ::= { cabhCtpGroups 1 }

END
```

E.4 Requisitos de la MIB dispositivo de servicios de portal IPCable2Home (PSDev)

La MIB PSDev IPCable2Home DEBE implementarse tal como se define a continuación.

```
CABH-PS-DEV-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    Integer32,
    Unsigned32,
    TimeTicks,
    NOTIFICATION-TYPE            FROM SNMPv2-SMI

    TruthValue,
    PhysAddress,
    DateAndTime,
    TimeStamp,
    RowStatus                    FROM SNMPv2-TC

    SnmpAdminString              FROM SNMP-FRAMEWORK-MIB

    OBJECT-GROUP,
    MODULE-COMPLIANCE,
    NOTIFICATION-GROUP           FROM SNMPv2-CONF

    ifIndex                      FROM IF-MIB

    InetAddressType,
    InetAddress                  FROM INET-ADDRESS-MIB

    IANAifType                   FROM IANAifType-MIB

    docsDevSwCurrentVers,
    docsDevEvLevel,
    docsDevEvId,
    docsDevEvText,
    docsDevSwFilename,
    docsDevSwServer              FROM DOCS-CABLE-DEVICE-MIB -- RFC 2669

    cabhCdpServerDhcpAddress,
    cabhCdpWanDataAddrClientId,
    cabhCdpLanTransThreshold,
    cabhCdpLanTransCurCount      FROM CABH-CDP-MIB

    ZeroBasedCounter32           FROM RMON2-MIB

    cabhQos2NumActivePolicyHolder,
    cabhQos2PolicyHolderEnabled,
    cabhQos2PolicyAdmissionControl FROM CABH-QOS2-MIB

    clabProjCableHome            FROM CLAB-DEF-MIB;

cabhPsDevMib MODULE-IDENTITY
    LAST-UPDATED    "200504080000Z" -- April 8, 2005
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
            858 Coal Creek Circle
            Louisville, Colorado 80027
            U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com; mibs@cablelabs.com"
```

```
    DESCRIPTION
            "This MIB module supplies the basic management objects for
            the Portal Services logical element of a CableHome
            compliant Residential Gateway device. The PS device
            parameters describe general PS Device attributes and
            behaviour characteristics.
            Most the PS Device MIB is needed for configuration
            download."
    ::= { clabProjCableHome 1 }

-- Textual Conventions

cabhPsDevMibObjects     OBJECT IDENTIFIER ::= { cabhPsDevMib 1 }
cabhPsDevBase           OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 1 }
cabhPsDevProv           OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 2 }
cabhPsDevAttrib         OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 3 }
cabhPsDevPsAttrib       OBJECT IDENTIFIER ::= { cabhPsDevAttrib 1 }
cabhPsDevBpAttrib       OBJECT IDENTIFIER ::= { cabhPsDevAttrib 2 }
cabhPsDevStats          OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 4 }
cabhPsDevAccessControl  OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 5 }
cabhPsDevMisc           OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 6 }
cabhPsDevUI             OBJECT IDENTIFIER ::= { cabhPsDevMisc 1 }
cabhPsDev802dot11       OBJECT IDENTIFIER ::= { cabhPsDevMisc 2 }
cabhPsDevUpnp           OBJECT IDENTIFIER ::= { cabhPsDevMisc 3 }
cabhPsDevUpnpBase       OBJECT IDENTIFIER ::= { cabhPsDevUpnp 1 }
cabhPsDevUpnpCommands   OBJECT IDENTIFIER ::= { cabhPsDevUpnp 2 }

--
-- The following group describes the base objects in the PS.
-- These are device-based parameters.
--

cabhPsDevDateTime OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The date and time, with optional timezone information."
    ::= { cabhPsDevBase 1 }

cabhPsDevResetNow OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Setting this object to true(1) causes the standalone or
            embedded PS device to reboot. Device code initializes as if
            starting from a power-on reset. The CMP ensures that MIB
            object values persist as specified in Annex A. Reading this
            object always returns false(2)."
    ::= { cabhPsDevBase 2 }

cabhPsDevSerialNumber OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..128))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The manufacturer's serial number for this PS. This
            parameter is manufacturer provided and is stored in
            non-volatile memory."
    ::= { cabhPsDevBase 3 }
```

```
cabhPsDevHardwareVersion OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..48))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The manufacturer's hardware version for this PS. This parameter is
            manufacturer provided and is stored in non-volatile memory."
    ::= { cabhPsDevBase 4 }

cabhPsDevWanManMacAddress OBJECT-TYPE
    SYNTAX      PhysAddress (SIZE (0..16))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The PS WAN-Man MAC address. This is the PS hardware
            address to be used by the CDC to uniquely identify
            the PS to the cable data network DHCP server for
            the acquisition of an IP address to be used for
            management messaging between the cable network
            NMS and the CMP."
    ::= { cabhPsDevBase 5 }

cabhPsDevWanDataMacAddress OBJECT-TYPE
    SYNTAX      PhysAddress (SIZE (0..16))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The PS WAN-Data MAC address. The PS could have multiple
            WAN-Data Interfaces, which share the same hardware address.
            The client identifiers will be unique so that each may be
            assigned a different, unique IP address."
    ::= { cabhPsDevBase 6 }

cabhPsDevTypeIdentifier OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This is a copy of the device type identifier used in the
            DHCP option 60 exchanged between the PS and the DHCP
            server."
    REFERENCE
            "CableHome Specification, CDC Function System
            Description section."
    ::= { cabhPsDevBase 7 }

cabhPsDevSetToFactory OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Setting this object to true(1) sets all PsDev MIB objects
            to the factory default values. Reading this object always
            returns false(2)."
    ::= { cabhPsDevBase 8 }

cabhPsDevWanManClientId OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE (1..80))
    MAX-ACCESS  read-write
    STATUS      deprecated
    DESCRIPTION
            "This is the client ID used for WAN-MAN DHCP requests.
            The default value is the 6 byte MAC address."
    ::= { cabhPsDevBase 9 }
```

```
cabhPsDevTodSyncStatus OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object indicates whether the PS was able to successfully
            synchronize with the Time of Day (ToD) Server in the cable
            network. The PS sets this object to true(1) if the PS
            successfully synchronizes its time with the ToD server.
            The PS sets this object to false(2) if the PS does not
            successfully synchronize with the ToD server."
    DEFVAL { false }
    ::= { cabhPsDevBase 10 }

cabhPsDevProvMode OBJECT-TYPE
    SYNTAX      INTEGER
    {
        dhcpmode(1),
        snmpmode(2),
        dormantCHmode(3)
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION

            "This object indicates the provisioning mode in which the PS is
            operating. If the PS is operating in DHCP Provisioning Mode as
            described in the CableHome specification, the PS sets this object
            to dhcpmode(1). If the PS is operating in SNMP Provisioning Mode,
            the PS sets this object to snmpmode(2). If the PS is not configured
            to operate in either dhcpmode or snmpmode, it will fall back to
            Dormant CableHome Mode and set the value of cabhPsDevProvMode
            to dormantCHmode(3)."
    ::= { cabhPsDevBase 11 }

cabhPsDevLastSetToFactory OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The value of sysUpTime when cabhPsDevSetToFactory was
            last set to true. Zero if never reset."
    ::= { cabhPsDevBase 12 }

cabhPsDevTrapControl OBJECT-TYPE
    SYNTAX BITS {
        cabhPsDevInitTLVUnknownTrap(0),
        cabhPsDevInitTrap(1),
        cabhPsDevInitRetryTrap(2),
        cabhPsDevDHCPFailTrap(3),
        cabhPsDevSwUpgradeInitTrap(4),
        cabhPsDevSwUpgradeFailTrap(5),
        cabhPsDevSwUpgradeSuccessTrap(6),
        cabhPsDevSwUpgradeCVCFailTrap(7),
        cabhPsDevTODFailTrap(8),
        cabhPsDevCdpWanDataIpTrap(9),
        cabhPsDevCdpThresholdTrap(10),
        cabhPsDevCspTrap(11),
        cabhPsDevCapTrap(12),
        cabhPsDevCtpTrap(13),
        cabhPsDevProvEnrollTrap(14),
        cabhPsDevCdpLanIpPoolTrap(15),
        cabhPsDevUpnpMultiplePHTrap(16)
    }
```

```
    MAX-ACCESS read-write
    STATUS current
    DESCRIPTION
            "The object is used to enable PS notifications.
            From left to right, the set bit indicates
            the corresponding PS notification is enabled.
            For example, if the first bit is set, then
            cabhPsDevInitTLVUnknownTrap is enabled.
            If the bit is zero, the trap is disabled."
    DEFVAL { '0000'h }
    ::= { cabhPsDevBase 13 }

--
--    The following group defines Provisioning Specific parameters
--

cabhPsDevProvisioningTimer OBJECT-TYPE
    SYNTAX      INTEGER (0..16383)
    UNITS       "minutes"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This object enables the user to set the duration of the
            provisioning timeout timer. The value is in minutes.
            Setting the timer to 0 disables it. The default value
            for the timer is 5."
    DEFVAL { 5 }
    ::= { cabhPsDevProv 1 }

cabhPsDevProvConfigFile OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..128))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The URL of the TFTP host for downloading provisioning and
            configuration parameters to this device. Returns NULL if
            the server address is unknown."
    ::= { cabhPsDevProv 2 }

cabhPsDevProvConfigHash OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0|20))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Hash of the contents of the PS config file, which is
            calculated by the NMS and sent to the PS. For the SHA-1
            authentication algorithm, the hash length is 160 bits.
            This hash value is encoded in binary format."
    ::= { cabhPsDevProv 3 }

cabhPsDevProvConfigFileSize OBJECT-TYPE
    SYNTAX      Integer32
    UNITS       "bytes"
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Size of the configuration file."
    ::= { cabhPsDevProv 4 }

cabhPsDevProvConfigFileStatus OBJECT-TYPE
    SYNTAX      INTEGER
    {
        idle(1),
        busy(2)
    }
```

```
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object indicates the current status of the
            configuration file download process. It is provided to
            indicate to the management entity that the PS will reject
            PS Configuration File triggers (set request to
            cabhPsDevProvConfigFile) when busy."
    ::= { cabhPsDevProv 5 }

cabhPsDevProvConfigTLVProcessed OBJECT-TYPE
    SYNTAX      INTEGER (0..16383)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Number of TLVs processed in config file."
    ::= { cabhPsDevProv 6 }

cabhPsDevProvConfigTLVRejected OBJECT-TYPE
    SYNTAX      INTEGER (0..16383)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Number of TLVs rejected in config file."
    ::= { cabhPsDevProv 7 }

cabhPsDevProvSolicitedKeyTimeout OBJECT-TYPE
    SYNTAX      Integer32 (15..600)
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This timeout applies only when the Provisioning Server
            initiated key management (with a Wake Up message) for
            SNMPv3.  It is the period during which the PS will save
            a number (inside the sequence number field) from the sent
            out AP Request and wait for the matching AP Reply from the
            Provisioning Server."
    DEFVAL { 120 }
    ::= { cabhPsDevProv 8 }

cabhPsDevProvState OBJECT-TYPE
    SYNTAX      INTEGER
    {
        pass(1),
        inProgress(2),
        fail(3)
    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object indicates the completion state of the
            initialization process. Pass or Fail states occur after
            completion of the initialization flow. InProgress occurs
            from PS initialization start to PS initialization end."
    ::= { cabhPsDevProv 9 }

cabhPsDevProvAuthState OBJECT-TYPE
    SYNTAX      INTEGER
    {
        accepted(1),
        rejected(2)
    }
```

```
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This object indicates the authentication state of the
            configuration file."
    ::= { cabhPsDevProv 10 }

cabhPsDevProvCorrelationId OBJECT-TYPE
    SYNTAX      Integer32
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
            "Random value generated by the PS for use in registration
            authorization. It is for use only in the PS initialization
            messages and for PS configuration file download. This value
            appears in both cabhPsDevProvisioningStatus and
            cabhPsDevProvisioningEnrollmentReport informs to verify the
            instance of loading the configuration file."
    ::= { cabhPsDevProv 11 }

cabhPsDevTimeServerAddrType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The IP address type of the Time server (RFC 868).
            IP version 4 is typically used."
    ::= { cabhPsDevProv 12 }

cabhPsDevTimeServerAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The IP address of the Time server (RFC 868). Returns
            0.0.0.0 if the time server IP address is unknown."
    ::= { cabhPsDevProv 13 }

--============================================================
--
--   PS Device Profile Group
--
--  The cabhPsDevPsProfile contains the Residential Gateway's
--  device attributes. This set of attributes is analogous to
--  some attributes of the BP Device profile.
--
--============================================================

cabhPsDevPsDeviceType OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(1..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The type of device, as defined in the CableHome
            specifications (Residential Gateway Device or CableHome
            Host Device), that implements this OID."
    DEFVAL { "CableHome Residential Gateway" }
    ::= { cabhPsDevPsAttrib 1 }

cabhPsDevPsManufacturerUrl OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
            "Universal Resource Locator to the Residential Gateway
            device manufacturer's web site."
    ::= { cabhPsDevPsAttrib 3 }

cabhPsDevPsModelUrl OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Universal Resource Locator to the web site describing this
            CableHome compliant residential gateway device."
    ::= { cabhPsDevPsAttrib 7 }

cabhPsDevPsModelUpc OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Universal Product Code of the CableHome compliant
            residential gateway device.
            See: Uniform Code Council  www.uc-council.org"
    ::= { cabhPsDevPsAttrib 8 }

--================================================================
--
--   CableHome Host/BP Device Profile Table
--
--  The cabhPsDevBpProfile contains the list of the CableHome Host
--  device attributes provided to the PS by BPs passing their Device
--  Profile XML schema via SOAP/HTTP.
--
--================================================================

cabhPsDevBpProfileTable OBJECT-TYPE
    SYNTAX SEQUENCE OF CabhPsDevBpProfileEntry
    MAX-ACCESS  not-accessible
    STATUS      obsolete
    DESCRIPTION
            "This table contains the information for the CableHome Host Device
            Profiles. Attributes of a device make up a Device Profile."
    ::= { cabhPsDevBpAttrib 1 }


cabhPsDevBpProfileEntry OBJECT-TYPE
    SYNTAX      CabhPsDevBpProfileEntry
    MAX-ACCESS  not-accessible
    STATUS      obsolete
    DESCRIPTION
            "The table that describes the CableHome Host Device
            Profile."
    INDEX { cabhPsDevBpIndex }
    ::= { cabhPsDevBpProfileTable 1 }

CabhPsDevBpProfileEntry ::= SEQUENCE {
        cabhPsDevBpIndex                    INTEGER,
        cabhPsDevBpDeviceType               SnmpAdminString,
        cabhPsDevBpManufacturer             SnmpAdminString,
        cabhPsDevBpManufacturerUrl          SnmpAdminString,
        cabhPsDevBpSerialNumber             SnmpAdminString,
        cabhPsDevBpHardwareVersion          SnmpAdminString,
        cabhPsDevBpHardwareOptions          SnmpAdminString,
        cabhPsDevBpModelName                SnmpAdminString,
        cabhPsDevBpModelNumber              SnmpAdminString,
```

```
        cabhPsDevBpModelUrl                   SnmpAdminString,
        cabhPsDevBpModelUpc                   SnmpAdminString,
        cabhPsDevBpModelSoftwareOs            SnmpAdminString,
        cabhPsDevBpModelSoftwareVersion       SnmpAdminString,
        cabhPsDevBpLanInterfaceType           IANAifType,
        cabhPsDevBpNumberInterfacePriorities INTEGER,
        cabhPsDevBpPhysicalLocation           SnmpAdminString,
        cabhPsDevBpPhysicalAddress            PhysAddress
        }

cabhPsDevBpIndex OBJECT-TYPE
    SYNTAX      INTEGER (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      obsolete
    DESCRIPTION
            "Integer index into the CableHome Host Device Profile
            Table."
    ::= { cabhPsDevBpProfileEntry 1 }

cabhPsDevBpDeviceType OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "The type of device, as defined by the CableHome
            specifications (CableHome Residential Gateway or CableHome
            Host Device), that passed the Device Profile whose
            information is made available through this table row."
    DEFVAL { "CableHome Host" }
    ::= { cabhPsDevBpProfileEntry 2 }

cabhPsDevBpManufacturer OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "The name of the CableHome Host Device's manufacturer."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 3 }

cabhPsDevBpManufacturerUrl OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "Universal Resource Locator to the CableHome Host device
            manufacturer's web site."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 4 }

cabhPsDevBpSerialNumber OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "The serial number assigned by the manufacturer for this
            CableHome Host Device."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 5 }

cabhPsDevBpHardwareVersion OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
```

```
    DESCRIPTION
            "The hardware version number assigned by the manufacturer
            for this CableHome Host Device."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 6 }

cabhPsDevBpHardwareOptions OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "The hardware options implemented on this CableHome Host
            Device."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 7 }

cabhPsDevBpModelName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "The model name assigned by the manufacturer for this
            CableHome Host Device."
    DEFVAL  { "" }
    ::= { cabhPsDevBpProfileEntry 8 }

cabhPsDevBpModelNumber OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "The model number assigned by the manufacturer for this
            CableHome Host Device."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 9 }

cabhPsDevBpModelUrl OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "The Universal Resource Locator to the web site describing
            this CableHome Host Device model."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 10 }

cabhPsDevBpModelUpc OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "Universal Product Code of the CableHome Host Device."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 11 }

cabhPsDevBpModelSoftwareOs OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "Software operating system implemented on the CableHome
            Host Device."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 12 }
```

```
cabhPsDevBpModelSoftwareVersion OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "Version of the operating system implemented on the
            CableHome Host Device."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 13 }

cabhPsDevBpLanInterfaceType OBJECT-TYPE
    SYNTAX      IANAifType
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "The ifType for the LAN Interface implemented on the
            CableHome Host Device."
    REFERENCE
            "http://www.iana.org/assignments/ianaiftype-mib."
    DEFVAL { other }
    ::= { cabhPsDevBpProfileEntry 14 }

cabhPsDevBpNumberInterfacePriorities OBJECT-TYPE
    SYNTAX      INTEGER (1..8)
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "Number of QoS priorities supported by the LAN technology
            (Data Link Layer) implemented in the CableHome Host
            Device."
    DEFVAL { 1 }
    ::= { cabhPsDevBpProfileEntry 15 }

cabhPsDevBpPhysicalLocation OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "Physical location of the CableHome Host Device."
    DEFVAL { "" }
    ::= { cabhPsDevBpProfileEntry 16 }

cabhPsDevBpPhysicalAddress OBJECT-TYPE
    SYNTAX      PhysAddress (SIZE (0..16))
    MAX-ACCESS  read-only
    STATUS      obsolete
    DESCRIPTION
            "The CableHome Host Device's hardware address."
    DEFVAL { ''h }
    ::= { cabhPsDevBpProfileEntry 17 }
```

```
--================================================================
--
--  LAN IP Traffic Statistics Table
--
--  The cabhPsDevLanIpTrafficTable contains the Traffic Statistics
--  for all LAN IP Devices connected to the PS. When the PS learns a
--  new LAN IP address, an entry is added to this table.
--
--================================================================

cabhPsDevLanIpTrafficCountersReset OBJECT-TYPE
    SYNTAX      INTEGER
    {
        clearCounters(1),
        clearTable(2)
    }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Setting this object to clearCounters(1) resets all the
            traffic statistic counter entries to zero in the
            cabhPsDevLanIpTrafficTable. Setting this object to
            clearTable(2) removes all entries in the
            cabhPsDevLanIpTrafficTable. Reading this object always
            returns clearCounters(1)."
    DEFVAL { clearCounters }
    -- Default read value
    ::= { cabhPsDevStats 1 }

cabhPsDevLanIpTrafficCountersLastReset OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The value of sysUpTime when
            cabhPsDevLanIpTrafficCountersReset was last written to.
            Zero if never written to."
    ::= { cabhPsDevStats 2 }

cabhPsDevLanIpTrafficEnabled OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Setting this object to true(1) turns on the IP traffic
            counters. Setting this object to false(2) turns off the IP
            traffic counters."
    DEFVAL { false } -- IP traffic counters are off by default
    ::= { cabhPsDevStats 3 }

cabhPsDevLanIpTrafficTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhPsDevLanIpTrafficEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains IP-layer Traffic Statistics for all
            LAN IP Devices connected to the PS."
    ::= { cabhPsDevStats 4 }

cabhPsDevLanIpTrafficEntry OBJECT-TYPE
    SYNTAX      CabhPsDevLanIpTrafficEntry
    MAX-ACCESS  not-accessible
    STATUS      current
```

```
    DESCRIPTION
            "List of Traffic Statistics for LAN IP Devices."
    INDEX { cabhPsDevLanIpTrafficIndex }
    ::= { cabhPsDevLanIpTrafficTable 1 }

CabhPsDevLanIpTrafficEntry ::= SEQUENCE {
    cabhPsDevLanIpTrafficIndex              INTEGER,
    cabhPsDevLanIpTrafficInetAddressType    InetAddressType,
    cabhPsDevLanIpTrafficInetAddress        InetAddress,
    cabhPsDevLanIpTrafficInOctets           ZeroBasedCounter32,
    cabhPsDevLanIpTrafficOutOctets          ZeroBasedCounter32
    }

cabhPsDevLanIpTrafficIndex OBJECT-TYPE
    SYNTAX      INTEGER   (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The Index into the LAN IP Traffic Statistics Table."
    ::= { cabhPsDevLanIpTrafficEntry 1 }

cabhPsDevLanIpTrafficInetAddressType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The type of IP address assigned to the LAN IP device to
            which the statistics in this table row apply.  IP version
            4 is typically used."
    DEFVAL { ipv4 }
    ::= { cabhPsDevLanIpTrafficEntry 2 }

cabhPsDevLanIpTrafficInetAddress OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The IP address of the LAN IP device to which the
            statistics in this table row apply.  An IPv4 IP
            address is typically used."
    ::= { cabhPsDevLanIpTrafficEntry 3 }

cabhPsDevLanIpTrafficInOctets OBJECT-TYPE
    SYNTAX      ZeroBasedCounter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The total number of octets the PS forwarded from the WAN
            interfaces to the LAN IP device associated with the value
            of cabhPsDevLanIpTrafficInetAddress. This counter object
            does not include LAN-to-LAN traffic."
    ::= { cabhPsDevLanIpTrafficEntry 4 }

cabhPsDevLanIpTrafficOutOctets OBJECT-TYPE
    SYNTAX      ZeroBasedCounter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The total number of octets the PS forwarded from the LAN
            IP device associated with the value of
            cabhPsDevLanIpTrafficInetAddress, to the WAN interfaces.
            This counter object does not include LAN-to-LAN traffic."
    ::= { cabhPsDevLanIpTrafficEntry 5 }
```

```
--=================================================================
--
--    CableHome Interface Access Control Table
--
--  The cabhPsDevAccessControlTable lists the physical addresses
--  of all LAN IP Devices for which the PS will forward traffic to
--  or from an interface type for which the Table is enabled.
--  If an interface type is enabled, the PS will not forward traffic
--  to or from any device on that interface whose physical address
--  is not listed in the Access Control Table. If an interface type
--  is disabled, the PS does apply forwarding restrictions based on
--  entires of the Access Control Table.
--
--=================================================================

cabhPsDevAccessControlEnable OBJECT-TYPE
    SYNTAX      BITS {
        hpna(0),  -- most significant bit
        ieee80211(1),
        ieee8023(2),
        homeplug(3),
        usb(4),
        ieee1394(5),
        scsi(6),
        other(7)
        }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This object specifies the interface type(s) for which the
            PSDev Access Control Table access rules are enabled. If a
            bit field is set to 1, the PS MUST only forward traffic
            received through that interface type if the source physical
            address is an entry in the cabhPsDevAccessControlTable. If
            a bit field is set to 1, the PS MUST only forward traffic
            destined to a device on that interface type if the
            destination physical address is an entry in the
            cabhPsDevAccessControlTable. If the bit field for an
            interface type is not set, i.e., if it is equal to 0, the
            PS MUST NOT apply forwarding restrictions for that
            interface type based on the Access Control Table. The PS
            MUST implement cabhPsDevAccessControlEnable for bit 1
            (wireless LAN) and for bit 3 (HomePlug). If the PS does not
            implement cabhPsDevAccessControlEnable for any of the other
            defined bits, the PS MUST return inconsistent value error,
            and not allow the bit to be set, if an attempt is made to
            set a bit that is not implemented.

            If the PS implements a HomePNA interface and implements the
            PSDev Access Control Table enable functionality for the
            HomePNA interface, then if bit 0 is set, the PS MUST apply
            PSDev Access Control Table access rules to any PS interface
            of  IANAifType 220 (Home Phoneline Networking Alliance). If
            the PS does not implement PSDev Access Control Table enable
            functionality for the HomePNA interface, and an attempt is
            made to set bit 0 to value '1', the PS MUST return
            'Inconsistent Value' error and MUST NOT set bit 0 to
            value '1'.

            If bit 1 (ieee80211) is set, the PS MUST apply PSDev
            Access Control Table access rules to any PS interface of
            IANAifType 71 (radio spread spectrum).
```

```
            If the PS implements an IEEE 802.3/CSMA-CD interface and
            implements the PSDev Access Control Table enable
            functionality for the IEEE 802.3/CSMA-CD interface, then
            if bit 2 is set, the PS MUST apply PSDev Access Control
            Table access rules to any PS interface of  IANAifType 6
            (ethernetCsmacd). If the PS does not implement PSDev
            Access Control Table enable functionality for a
            IEEE 802.3/CSMA-CD interface, and an attempt is made to set
            bit 2 to value '1', the PS MUST return 'Inconsistent
            Value' error and MUST NOT set bit 2 to value '1'.

            If bit 3 (homeplug) is set, the PS MUST apply PSDev
            Access Control Table access rules to any PS HomePlug
            Powerline Alliance (HomePlug) interface as defined by
            HomePlug Powerline Alliance (www.homeplug.org).

            If the PS implements a USB interface and implements the
            PSDev Access Control Table enable functionality for the
            USB interface, then if bit 4 is set, the PS MUST apply
            PSDev Access Control Table access rules to any PS
            interface of  IANAifType 160 (USB). If the PS does not
            implement PSDev Access Control Table enable functionality
            for the USB interface, and an attempt is made to set
            bit 4 to value '1', the PS MUST return 'Inconsistent Value'
            error and MUST NOT set bit 4 to value '1'.

            If the PS implements an IEEE 1394 interface and
            implements the PSDev Access Control Table enable
            functionality for the IEEE 1394 interface, then if bit 5
            is set, the PS MUST apply PSDev Access Control Table
            access rules to any PS interface of  IANAifType 144
            (IEEE 1394 High Performance Serial Bus). If the PS does
            not implement PSDev Access Control Table enable
            functionality for the IEEE 1394 interface, and an attempt
            is made to set bit 5 to value '1', the PS MUST return
            'Inconsistent Value' error and MUST NOT set bit 5 to
            value '1'.

            If the PS implements a SCSI interface and implements the
            PSDev Access Control Table enable functionality for the
            SCSI interface, then if bit 6 is set, the PS MUST apply
            PSDev Access Control Table access rules to any PS SCSI-2
            or SCSI-3 interface. If the PS does not implement PSDev
            Access Control Table enable functionality for the SCSI
            interface, and an attempt is made to set bit 6 to value
            '1', the PS MUST return 'Inconsistent Value' error and
            MUST NOT set bit 6 to value '1'.

            If bit 7 (other) is set, the PS MAY apply PSDev Access
            Control Table filter access to any PS interface of a type
            other than the types defined by bits 0 - 6."
    DEFVAL { '00'h }  -- null, all interface types disabled
    ::= { cabhPsDevAccessControl 1 }

cabhPsDevAccessControlTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhPsDevAccessControlEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains a list of the physical addresses of
            LAN IP Devices to and from which the PS will forward
            traffic through a LAN interface if
            cabhPsDevAccessControlEnable is enabled(1) for that
            interface type."
```

```
    REFERENCE
            "CableHome specification, Packet Handling & Address
            Translation section."
    ::= { cabhPsDevAccessControl 2 }

cabhPsDevAccessControlEntry OBJECT-TYPE
    SYNTAX      CabhPsDevAccessControlEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "List of the physical addresses for LAN IP Devices
            to and from which the PS will forward traffic when
            the PSDev Access Control Table is enabled."
    INDEX { cabhPsDevAccessControlIndex }
    ::= { cabhPsDevAccessControlTable 1 }

CabhPsDevAccessControlEntry ::= SEQUENCE {
    cabhPsDevAccessControlIndex     INTEGER,
    cabhPsDevAccessControlPhysAddr  PhysAddress,
    cabhPsDevAccessControlRowStatus RowStatus
    }

cabhPsDevAccessControlIndex OBJECT-TYPE
    SYNTAX      INTEGER (1..65535)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Integer index into the CableHome PSDev Access Control
            Table."
    ::= { cabhPsDevAccessControlEntry 1 }

cabhPsDevAccessControlPhysAddr OBJECT-TYPE
    SYNTAX      PhysAddress (SIZE (1..16))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The physical address of the LAN IP Device for which the PS
            will forward traffic when the PSDev Access Control
            Table is enabled. The PS will not forward traffic
            from any LAN IP Device whose physical address is
            not an entry of the PSDev Access Control Table when the
            PSDev Access Control Table is enabled for the
            corresponding interface."
    ::= { cabhPsDevAccessControlEntry 2 }

cabhPsDevAccessControlRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The RowStatus interlock for the creation and deletion
            of a cabhPsDevAccessControlTable entry. Any writable
            object in each row of the cabhPsDevAccessControlTable
            can be modified at any time while the row is active(1)."
    ::= { cabhPsDevAccessControlEntry 3 }
```

```
--=========================================================================
--
--    CableHome Miscellaneous MIB
--
--  This branch of cabhPsDevMib contains extensions related to
--  functionalities defined for other standards bodies or outside
--  of CableHome fully defined features.
--
--=========================================================================

--=========================================================================
--
--    CableHome User Interface Miscellaneous MIB
--
--  PS MIB objects for controlling features of the CableHome compliant
--  residential gateways User Interface (UI) if present.
--
--=========================================================================

cabhPsDevUILogin OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0..32))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This parameter specifies the value of the user login name
            required for access to the CableHome compliant residential
            gateway device's user interface."
    ::= { cabhPsDevUI 1 }

cabhPsDevUIPassword OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(4..32))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This parameter specifies the value of the user password
            required for access to the CableHome compliant residential
            gateway device's user interface."
    ::= { cabhPsDevUI 2 }

cabhPsDevUISelection OBJECT-TYPE
    SYNTAX      INTEGER {
                    manufacturerLocal(1),
                    cableOperatorLocal(2),
                    cableOperatorServer(3),
                    disabledUI(4)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Indicates the type of Web user interface (UI)
            to present to the user if Web interface is supported:
            manufacturerLocal:
              PS uses the vendor UI shipped with the device.
            cableOperatorLocal:
              PS uses a cable operator defined UI interface.
              To operate properly, it should require a special code
              image downloaded into the PS.  By default, if no cable
              operator UI is being defined, selecting this option
              points to 'manufacturerLocal' selection.
            cableOperatorServer:
              PS redirects HTTP requests to its UI to the URL specified
              in cabhPsDevUIServerUrl.
```

```
            disabledUI:
              PS responds to HTTP requests to its UI with an HTTP page
              containing the value of
              cabhPsDevUISelectionDisabledBodyText as the body tag;
              or with a vendor specific message or HTTP error if that
              value is null."
    DEFVAL { manufacturerLocal }
    ::= { cabhPsDevUI 3 }

cabhPsDevUIServerUrl OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..255))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Uniform Resource Locator (URL) provisioned by the cable
            operator to which the PS re-directs the subscriber's LAN IP Device
            for presentation of the PS User Interface when the value of
            cabhPsDevUISelection is cableOperatorServer(3). This object is valid
            and applicable only when the value of cabhPsDevUISelection is
            cableOperatorServer(3)."
    DEFVAL { "" }
    ::= { cabhPsDevUI 4 }

cabhPsDevUISelectionDisabledBodyText OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..255))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Default text for the HTTP body tag to include in the
            response to UI requests when the object
            cabhPsDevUISelection is set to 'disabledUI'.
            An example of a body tag is below:
            <body>Feature currently disabled by Cable Operator</body>."
    ::= { cabhPsDevUI 5 }

-- ========================================================
-- IEEE802dot11-MIB CableHome extension
-- ========================================================

cabhPsDev802dot11BaseTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhPsDev802dot11BaseEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "CableHome specifics controls for 80211 wireless
            interfaces."
    ::= { cabhPsDev802dot11 1 }

cabhPsDev802dot11BaseEntry OBJECT-TYPE
    SYNTAX      CabhPsDev802dot11BaseEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "An entry in cabhPsDev802dot11BaseTable associated to a
            wireless interface of IANAifType ieee80211.(71)"
    INDEX { ifIndex }
    ::= { cabhPsDev802dot11BaseTable 1 }
```

```
CabhPsDev802dot11BaseEntry ::=
    SEQUENCE {
              cabhPsDev802dot11BaseSetToDefault     TruthValue,
              cabhPsDev802dot11BaseLastSetToDefault TimeStamp,
              cabhPsDev802dot11BaseAdvertiseSSID    TruthValue,
              cabhPsDev802dot11BasePhyCapabilities  BITS,
              cabhPsDev802dot11BasePhyOperMode      INTEGER
             }

cabhPsDev802dot11BaseSetToDefault OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "When set  to true(1), the PS MUST reset to default values
            the MIB objects of IEEE802dot11-MIB module and others under
            cabhPsDev802dot11 for this entry related IfIndex.
            Reading this object always return false(2)."
    DEFVAL { false }
    ::= { cabhPsDev802dot11BaseEntry 1 }

cabhPsDev802dot11BaseLastSetToDefault OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The value of sysUpTime when
            cabhPsDev802dot11MIBSetToDefault was last set to true.
            Zero if never reset."
    ::= { cabhPsDev802dot11BaseEntry 2 }

cabhPsDev802dot11BaseAdvertiseSSID OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "When set to false(2) the PS does not advertise the BSS SSID
            in a proprietary manner. To avoid interoperability problems and
            service disruption, it is RECOMMENDED to set this object always
            to true. This feature does not provide any security, and does not
            prevent Wireless Stations to obtain the SSID by sniffing frames
            from other stations in the ESS. If the device does not support
            the feature of turning on/off the SSID advertisement, this object
            always reports 'true(1)' and reports the error 'wrongValue' when
            set to 'false(2)."
    DEFVAL { true }
    ::= { cabhPsDev802dot11BaseEntry 3 }

cabhPsDev802dot11BasePhyCapabilities OBJECT-TYPE
    SYNTAX      BITS {
                    --ieee80211DSSS(0) , not interest
                      ieee80211a(0),
                      ieee80211b(1),
                      ieee80211g(2)
                    --ieee80211FHSS(8),
                    --ieee80211IR(16)
                    --values with comments are not requirements
                    --included for completeness of 80211 spec.
                    }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Indicates the PHY capabilities of the wireless interface."
    ::= { cabhPsDev802dot11BaseEntry 4 }
```

```
cabhPsDev802dot11BasePhyOperMode OBJECT-TYPE
    SYNTAX      INTEGER {
                         ieee80211a(1),
                         ieee80211b(2),
                         ieee80211g(4),
                         ieee80211bg(24)
                        }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Indicates the PHY mode of operation being set for the
            wireless interface. Setting this object will update the
            value of dot11PhyType. Accordingly (if implemented), as
            well as the object dot11OperationalRateSet to the 80211
            mandatory rates for dot11PhyType.

            It is left to vendors the option to update the values of
            PS optional dot11SupportedDataRatesTxEntry and
            dot11SupportedDataRatesRxEntry tables based on the
            operational mode.

            In the case of selecting ieee80211bg(14), dot11PhyType
            reports erp(6) and dot11OperationalRateSet should report
            HRDSSS and ERP mandatory rates and in addition 54 Mbit/s rate
            if supported by PS. e.g. : (this example assumes 54 Mbit/s
            OFDM is supported.
            HR-DSSS :
              Mandatory:
                     1 Mbit/s '80'H + '01'H
                     2 Mbit/s '80'H + '02'H
                     5.5 Mbit/s '80'H + '0B'H
                    11 Mbit/s '80'H + '16'H
            ERP :
              Mandatory:
                     6 Mbit/s '80'H + '0C'H
                    12 Mbit/s '80'H + '18'H
                    24 Mbit/s '80'H + '30'H
     (if supported) 54 Mbit/s '80'H + '6C'
              Optional:
                    22 Mbit/s '00'H + '2C'H
                    33 Mbit/s '00'H + '42'H
                    18 Mbit/s '00'H + '24'H
                    36 Mbit/s '00'H + '48'H
                    48 Mbit/s '00'H + '60'H

          Combined operational rates in :

            dot11OperationalRateSet value in rate order regardless
            of '80'H flag and using dots for clarity :
            + means flagged '80'H, - not flagged.
          Rates Mbit/s: +1,+2,+5.5,+6,+11,+12,-18,-22,+24,-33,-36,-48,+54
                Hex:  '81.82.8B.8C.96.98. 24.2C.B0.48.42. 60.EC'H

            The default value of this object is left to the vendor to
            accommodate the factory defaults for the device."
    REFERENCE
            "IEEE Std 802.11, 1999 Edition,
            IEEE Std 802.11a-1999,
            IEEE Std 802.11b-1999/Cor 1-2001,
            IEEE Std 802.11g-2003."
    ::= { cabhPsDev802dot11BaseEntry 5 }
```

```
-- ================================================================
-- IEEE802dot11MIB CableHome extension for security configuration
-- ================================================================

cabhPsDev802dot11SecTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhPsDev802dot11SecEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "CableHome specifics controls for configuring the
            security mechanisms of 80211 wireless interfaces."
    ::= { cabhPsDev802dot11 2 }

cabhPsDev802dot11SecEntry OBJECT-TYPE
    SYNTAX      CabhPsDev802dot11SecEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "An entry in cabhPsDev802dot11SecTable associated to a
            wireless interface of IANAifType ieee80211(71)."
    INDEX { ifIndex }
    ::= { cabhPsDev802dot11SecTable 1 }

CabhPsDev802dot11SecEntry ::=
    SEQUENCE {
              cabhPsDev802dot11SecCapabilities              BITS,
              cabhPsDev802dot11SecOperMode                  BITS,
              cabhPsDev802dot11SecPassPhraseToWEPKey        OCTET STRING,
              cabhPsDev802dot11SecUsePassPhraseToWEPKeyAlg  TruthValue,
              cabhPsDev802dot11SecPSKPassPhraseToKey        OCTET STRING,
              cabhPsDev802dot11SecWPAPreSharedKey           OCTET STRING,
              cabhPsDev802dot11SecWPARekeyTime              Unsigned32,
              cabhPsDev802dot11SecControl                   INTEGER,
              cabhPsDev802dot11SecCommitStatus              INTEGER
             }

cabhPsDev802dot11SecCapabilities OBJECT-TYPE
    SYNTAX      BITS {
                      wep64(0),
                      wep128(1),
                      wpaPSK(2)
                    --wpa2PSK(3)
                     }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The PS capabilities for Authentication and encryption used
            to authenticate 802.11 clients."
    ::= { cabhPsDev802dot11SecEntry 1 }

cabhPsDev802dot11SecOperMode OBJECT-TYPE
    SYNTAX      BITS {
                      wep64(0),
                      wep128(1),
                      wpaPSK(2)
                   -- wpa2PSK(3)
                     }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Indicates the Authentication and encryption mechanism to
            be enabled for the users and advertised in Beacon messages.
            Bits set to this object and not supported by the PS in
            cabhPsDev802dot11SecCapabilities are set to '0' without
```

```
            failing the SNMP set. Setting two bits that the PS does not
            support in combination returns an error 'wrongValue'.
            In particular:
              Setting to '1' both wep64(0)and wep128(1) bits returns an
                error'wrongValue'.
              Setting a combination of WEP bits (wep64(0) or wep128(1))
                and wpaPSK bit returns is not a mandatory requirement,
                therefore an error 'wrongValue' may be reported.

            Setting any bit to '1' must not affect the value of object
            dot11PrivacyInvoked.

            If dot11PrivacyInvoked is set to 'false', the 80211 WEP
            security mechanism is disabled (see dot11PrivacyInvoked
            description) and the value of this object is not used.

            Setting the wpaPSK(2) bit to '1' indicates the usage of
            WPA-PSK TKIP.

            Note that to enable the PSK security mechanism, the value
            of cabhPsDev802dot11SecWPAPreSharedKey must be a non-zero
            length string."
    ::= { cabhPsDev802dot11SecEntry 2 }

cabhPsDev802dot11SecPassPhraseToWEPKey OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0|5..63))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Password used for PS to derive WEP encryption keys.
            After a successful set, the values of
            dot11WEPDefaultKeyValue are populated as described below:

            For wep64:
              If cabhPsDev802dot11SecOperMode wep64 bit is set to '1'
              This object value (x) is used as a generator of a 4-octet
              seed.

              seed[i%4] = XOR(seed[i%4],x[i]); i from 1 to len(x) -1

            The values of the four dot11WEPDefaultKeyValue are
            calculated as indicated below :
              loop j 1..4
              loop k 0..4
              seed = seed * (((26*8+1)*256-1)*4+1) + 2531011
              The value is always truncated at 32 bits.
              OCTETk = (seed >> 16 )& 0xFF  -lowest octet-
              end loop
              dot11WEPDefaultKeyValue(j) = OCTET0,OCTET1, ... OCTET4
              end loop

              Note that seed value is constantly re-computed when
              calculating each octet of each default WEP key.

            For wep128:
              If cabhPsDev802dot11SecOperMode wep128 bit is set to '1'
              This object value (x) fills a 64-octet buffer y :
              y = x,x,x...up to 64 octets.
              Calculate the 128-bit MD5 digest of y
              the values of all dot11WEPDefaultKeyValue (1..4)
              are calculated by truncating the first 13 octets
              of MD5y.

            dot11WEPDefaultKeyValue = MD5y0,MD5y1, .. MD5y12
```

```
   This object value is normally read by issuing SNMP
   request PDUs. This object can be cleared with an SNMP
   SET to an empty string Value and the PS MUST not update
   the type of keys being set to '1' in
   cabhPsDev802dot11SecOperMode.

 If cabhPsDev802dot11SecUsePassPhraseToKeyAlg is set to
 false(2), the behaviour of a SET to this object depends
 on the bits set for cabhPsDev802dot11SecOperMode as
 follows:


   If cabhPsDev802dot11SecOperMode bit wep64 is set to '1'
   and this object value length is 5 octets, the MIB object
   dot11WEPDefaultKeyValue.1 (WEP key 0) is populated with
   this object value, otherwise an error 'inconsistentValue'
   is reported.

   If cabhPsDev802dot11SecOperMode bit wep128 is set to '1'
   and this object value length is 13 octets, the MIB object
   dot11WEPDefaultKeyValue.1 (WEP key 0) is populated with
   this object value, otherwise an error 'inconsistentValue'
   is reported.

 Vector examples for wep64 and wep128 key derivation:

   Note:
   % refers to the module operation (reminder of the
   quotient of i and 4); XOR is the OR exclusive boolean
   operation.

For wep64:
passphrase:
        'ABCD4321' ( hex code 0x41.42.43.44.34.33.32.31 )


First loop: (octets 0..3)
   XOR (0x00,A) -> XOR(0x00,0x41) -> 0x41
   XOR (0x00,B) -> XOR(0x00,0x42) -> 0x42
   XOR (0x00,C) -> XOR(0x00,0x43) -> 0x43
   XOR (0x00,D) -> XOR(0x00,0x44) -> 0x44

Second loop: (octets 4..7)
   XOR (A,4) -> XOR(0x41,0x34) -> 0x75
   XOR (B,3) -> XOR(0x42,0x33) -> 0x71
   XOR (C,2) -> XOR(0x43,0x32) -> 0x71
   XOR (D,1) -> XOR(0x44,0x31) -> 0x75

 initial seed 0x75717175 -> 1970368885

 DefaultKeys calculation

 key1
 seed : 0x16545E64 -> 2nd MSB byte : 0x54
 seed : 0x41681397 -> 2nd MSB byte : 0x68
 seed : 0x1BE77FFE -> 2nd MSB byte : 0xE7
 seed : 0xAA6996C9 -> 2nd MSB byte : 0x69
 seed : 0xD1523E68 -> 2nd MSB byte : 0x52
 dot11WEPDefaultKeyValue.1 = 0x5468E76952
```

```
            key2
            seed : 0x1FFB838B -> 2nd MSB byte : 0xFb
            seed : 0xF9C60022 -> 2nd MSB byte : 0xC6
            seed : 0xAB43A65D -> 2nd MSB byte : 0x43
            seed : 0xE9A35FAC -> 2nd MSB byte : 0xA3
            seed : 0xE7AA2FBF -> 2nd MSB byte : 0xAA
            dot11WEPDefaultKeyValue.2 = 0xFBC643A3AA

            key3
            seed : 0x6D13CB86 -> 2nd MSB byte : 0x13
            seed : 0x5D8CD431 -> 2nd MSB byte : 0x8C
            seed : 0xCC702630 -> 2nd MSB byte : 0x70
            seed : 0xD78AEC33 -> 2nd MSB byte : 0x8A
            seed : 0x24DC662A -> 2nd MSB byte : 0xDC
            dot11WEPDefaultKeyValue.3 = 0x138C708ADC

            key4
            seed : 0x4F329445 -> 2nd MSB byte : 0x32
            seed : 0x3EC035F4 -> 2nd MSB byte : 0xC0
            seed : 0xF416CCE7 -> 2nd MSB byte : 0x16
            seed : 0x9904940E -> 2nd MSB byte : 0x04
            seed : 0x28969A99 -> 2nd MSB byte : 0x96
            dot11WEPDefaultKeyValue.4 = 0x32C0160496

            For wep128:
            passphrase:
                   'ABCD4321' ( hex code 0x41.42.43.44.34.33.32.31 )
            128-bit MD-5 digest 0xFECBACF05B42F7A138A5F3928E
            dot11WEPDefaultKeyValue.1..4 = 0xFECBACF05B42F7A138A5"
    ::= { cabhPsDev802dot11SecEntry 3 }

cabhPsDev802dot11SecUsePassPhraseToWEPKeyAlg OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "When this object value is true(1), the WEP Pass Phrase to
            key mechanism described in
            cabhPsDev802dot11SecPassPhraseToWEPKey applies. When this
            object is set to false(2), the Pass Phrase to WEP Key
            mechanism is ignored and the password is used as WEP key
            to populate the MIB object keydot11WEPDefaultKeyValue
            object as indicated in
            cabhPsDev802dot11SecPassPhraseToWEPKey description."
    DEFVAL { true }
    ::= { cabhPsDev802dot11SecEntry 4 }

cabhPsDev802dot11SecPSKPassPhraseToKey OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(8..63))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Password used for PS to derive WPA PSK encryption key.
            After a successful set, the values of
            cabhPsDev802dot11SecWPAPreSharedKey are updated as described
            below:

            For wpaPSK:
            If cabhPsDev802dot11SecOperMode wpaPSK bit is set to '1',
            the value of cabhPsDev802dot11SecWPAPreSharedKey is updated
            with the Password Base Key Derivation Function from  the
            Password-based Cryptographic Specification PKCS #5 v2.0
            RFC 2898 (PBKDF2) with the following specific parameters:
```

```
            PSK = PBKDF2(PassPhrase, ssid, ssidLength, 4096, 256);
            PassPhrase is the value of this object;
            ssid is the PS SSID value used as the function salt;
            ssidLength is the number of octets of ssid;
            the iterations count is 4096 and the key generation length
            is 256 bits (32 octets).

            This object value is normally read by issuing SNMP request
            PDUs. This object can be cleared with an SNMP SET to an
            empty string Value and the PS MUST not update the type of
            keys being set to '1' in cabhPsDev802dot11SecOperMode.

            Vector examples for wpaPSK:

            for wpaPSK:
            passphrase:
                   'ABCD4321' ( hex code 0x41.42.43.44.34.33.32.31 )
            SSID: 'ABCD4321' ( hex code 0x41.42.43.44.34.33.32.31 )

            256 bit PBKDF2('ABCD4321', 'ABCD4321', 8, 4096, 32)
            cabhPsDev802dot11SecWPAPreSharedKey =
            0x7C199CF2FEF9AF206C8EE0E9703920C2
              3517068B3F96B011E0F975C9131BDB58"
    ::= { cabhPsDev802dot11SecEntry 5 }

cabhPsDev802dot11SecWPAPreSharedKey OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0|32))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The Pre-shared key used for the PS when the bit 'wpaPSK' is set
            to '1'. This object can be set directly or derived from the password
            phrase set in cabhPsDev802dot11SecPSKPassPhraseToKey. This object is
            meaningful when the bit wpaPSK is set to '1'.

            If the value of this object is the zero-length string, the PS
            must not activate the PSK security mechanism."
    DEFVAL { ''H }
    ::= { cabhPsDev802dot11SecEntry 6 }

cabhPsDev802dot11SecWPARekeyTime OBJECT-TYPE
    SYNTAX      Unsigned32 (1..4294967295)
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Time interval to initiate WPA Group Keys (GTK) updates."
    DEFVAL { 86400 }
    ::= { cabhPsDev802dot11SecEntry 7 }

cabhPsDev802dot11SecControl OBJECT-TYPE
    SYNTAX INTEGER {
        restoreConfig(1),
        commitConfig(2)
        }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The control for the indexed 80211 device configuration. All changes
            to the cabhPsDev802dot11SecEntry MIB objects are reflected when
            reading the value of the MIB objects; however, those changes
            are NOT applied to the running configuration of the indexed 80211
            device until they are successfully committed via use of the
            cabhPsDev802dot11SecControl object.
```

```
            If changes are made to the cabhPsDev802dot11SecEntry MIB
            objects which are not yet successfully committed to the
            indexed 80211 device, the cabhPsDev802dot11SecControl
            object can be used to roll back all changes to the last
            valid 80211 device configuration and discard all
            intermediate changes.

            restoreConfig - Setting cabhPsDev802dot11SecControl to this
            value will cause any changes to the
            cabhPsDev802dot11SecEntry objects not yet committed be
            reset to the values from the current running
            configuration of the indexed 80211 device.

            commitConfig - Setting cabhPsDev802dot11SecControl to this value
            will cause the indexed 80211 device to validate and apply the valid
            cabhPsDev802dot11SecEntry MIB settings to its running configuration.
            The cabhPsDev802dot11SecCommitStatus object will detail the
            status of this operation."
    DEFVAL { restoreConfig }
    ::= { cabhPsDev802dot11SecEntry 8 }

cabhPsDev802dot11SecCommitStatus OBJECT-TYPE
    SYNTAX INTEGER {
        commitSucceeded(1),
        commitNeeded(2),
        commitFailed(3)
        }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Indicates the status of committing the current
            cabhPsDev802dot11SecEntry MIB object values to the running
            configuration of the indexed 80211 device.

            commitSucceeded - indicates the current
            cabhPsDev802dot11SecEntry MIB object values are valid
            and have been successfully committed to the running
            configuration of the indexed 80211 device.

            commitNeeded - indicates that the value of one or more
            objects in cabhPsDev802dot11SecEntry MIB group have been
            changed but not yet committed to the running configuration
            of the indexed 80211 device.

            commitFailed - indicates the PS was unable to commit the
            cabhPsDev802dot11SecEntry MIB object values to the running
            configuration of the indexed 80211 device due to conflicts
            in those values."
    DEFVAL { commitSucceeded }
    ::= { cabhPsDev802dot11SecEntry 9 }

-- ============================================================
--
-- UPnP Services
-- Contains CableHome Portal Server UPnP information of LAN hosts
--
-- ============================================================

cabhPsDevUpnpEnabled OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
```

```
    DESCRIPTION
            "Setting this object to false(1) disables PS UPnP
            services and UPnP MIB objects related functionality.
            When this object reports 'false', any set to
            UPnP read-write or read-create objects returns error
            'InconsistentValue'.  Transitions of this object from
            'true' to 'false' and vice versa does not alter the content
            of persistent MIB objects and may clear dynamically UPnP
            created entries. This object value persists upon system
            reinitialization."
    DEFVAL { true }
    ::= { cabhPsDevUpnpBase 1 }

cabhPsDevUpnpCommandIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The type of InetAddress for cabhPsDevUpnpCommandIp."
    DEFVAL { ipv4 }
    ::= { cabhPsDevUpnpCommands 1 }

cabhPsDevUpnpCommandIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The IP address of the device for which the UPnP
            information is being requested. This may be an IPv4 or
            IPv6 prefix. When quering specific information about the
            PS itself, the PS router IP address 192.168.0.1
            should be specified ."
    DEFVAL { 'C0A80001'h } -- 192.168.0.1
    ::= { cabhPsDevUpnpCommands 2 }

cabhPsDevUpnpCommand OBJECT-TYPE
    SYNTAX      INTEGER {
        discoveryInfo(1),
        qosDeviceCapabilities(2),
        qosDeviceState(3)
        }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The type of information to be retrieved from the Upnp
            Devices in the LAN side and stored in
            cabhPsDevUpnpInfoTable.
            The following selections are supported:

            - discoveryInfo:
            PS retrieves the Discovery information of UPnP devices.
            If the Ip address specified in
            cabhPsDevUpnpCommandIp is 255.255.255.255,
            the PS executes an M-search command and then
            retrieves the discovery information of the
            responding devices. The data stored in
            cabhPsDevUpnpInfoTable also contain UPnP
            discovery data of the PS itself.

            - qosDeviceCapabilities:
            This command is executed for unicast address only
            and will trigger the PS to retrieve the QoS device
            information pertaining to QoS capabilities.
```

```
            - qosDeviceState:
            This command is executed for unicast address only
            and will trigger the PS to retrieve the QoS device
            information pertaining to QoS Device state."
    DEFVAL { discoveryInfo }
    ::= { cabhPsDevUpnpCommands 3 }

cabhPsDevUpnpCommandUpdate OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "If set to 'true' triggers the execution of the command
            indicated in cabhPsDevUpnpCommand for the host(s) in
            cabhPsDevUpnpCommandIp. Setting to true this object will
            return error 'wrongValue'  if host IP corresponds to
            255.255.255.255 and cabhPsDevUpnpCommand value is not
            'discoveryInfo'. Reading this value always returns 'false'."
    ::= { cabhPsDevUpnpCommands 4 }

cabhPsDevUpnpLastCommandUpdate OBJECT-TYPE
    SYNTAX      TimeTicks
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The sysUpTime value of the last time the object
            cabhPsDevUpnpLastCommandUpdate was set to 'true'."
    ::= { cabhPsDevUpnpCommands 5 }

cabhPsDevUpnpCommandStatus OBJECT-TYPE
    SYNTAX      INTEGER {
        none(1),
        inProgress(2),
        complete(3),
        failed(4)
        }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The status of cabhPsDevUpnpCommandUpdate trigger
            none(1)
            initial state.
            inProgress(2)
            the information is being acquired by the
            device, PS does not change from 'inProgress'
            to the final state (complete, failed)
            until the execution has finished.
            complete(3) The overall execution is finished with
            no error conditions.
            failed(4).
            The UPnP Device has experienced a timeout. In the
            case of multiple devices query
            (cabhPsDevUpnpCommand set to 'discoveryInfo')
            The failed devices are stored with content information
            empty. At system initialization this object returns
            'none'."
    DEFVAL { none }
    ::= { cabhPsDevUpnpCommands 6}

cabhPsDevUpnpInfoTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhPsDevUpnpInfoEntry
    MAX-ACCESS  not-accessible
    STATUS      current
```

```
    DESCRIPTION
            "This table contains QoS related information of LAN
            UPnP devices or the PS itself."
    ::= { cabhPsDevUpnpCommands 7 }

cabhPsDevUpnpInfoEntry OBJECT-TYPE
    SYNTAX      CabhPsDevUpnpInfoEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The Indexes for this entries
            Entries are created after setting to 'true' the
            value of cabhPsDevUpnpCommand."
    INDEX { cabhPsDevUpnpInfoIpType, cabhPsDevUpnpInfoIp,
            cabhPsDevUpnpInfoXmlFragmentIndex }
    ::= { cabhPsDevUpnpInfoTable 1 }

CabhPsDevUpnpInfoEntry::= SEQUENCE {
    cabhPsDevUpnpInfoIpType            InetAddressType,
    cabhPsDevUpnpInfoIp                InetAddress,
    cabhPsDevUpnpInfoXmlFragmentIndex  Unsigned32,
    cabhPsDevUpnpInfoXmlFragment       OCTET STRING
    }

cabhPsDevUpnpInfoIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The type of InetAddress for cabhPsDevUpnpInfoIp."
    ::= { cabhPsDevUpnpInfoEntry 1 }

cabhPsDevUpnpInfoIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The IP address of the device for which the UPnP
            information is being stored. This may be a DNS name
            (LAN Host name), an IPv4 or IPv6 prefix. Information
            pertaining to the PS itself is indicated by the PS
            well-known LAN IP address interface 192.168.0.1."
    ::= { cabhPsDevUpnpInfoEntry 2 }

cabhPsDevUpnpInfoXmlFragmentIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (1..4294967295)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The index of the sequence of entries of
            cabhPsDevUpnpInfoXmlFragment for a specific
            cabhPsDevUpnpInfoIp IP address starting with '1'."
    ::= { cabhPsDevUpnpInfoEntry 3 }

cabhPsDevUpnpInfoXmlFragment OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0..400))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The UPnP Device information being requested by
            cabhPsDevUpnpCommand for the IP addresses specified in
            cabhPsDevUpnpInfoIp for LAN host(s). If the information is
            greater than 400 bytes, cabhPsDevUpnpInfoXmlFragmentIndex
```

```
            indicates the sequence of the consecutive portions per host
            identified in the table."
    ::= { cabhPsDevUpnpInfoEntry 4 }

--

cabhPsNotification     OBJECT IDENTIFIER ::= { cabhPsDevMib 2 }
cabhPsDevNotifications OBJECT IDENTIFIER ::= { cabhPsNotification 0 }
cabhPsConformance      OBJECT IDENTIFIER ::= { cabhPsDevMib 3 }
cabhPsCompliances      OBJECT IDENTIFIER ::= { cabhPsConformance 1 }
cabhPsGroups           OBJECT IDENTIFIER ::= { cabhPsConformance 2 }

--
--    Notification Group
--

cabhPsDevInitTLVUnknownTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress
        }
    STATUS      current
    DESCRIPTION
            "Event due to detection of unknown TLV during the TLV
            parsing process. The values of docsDevEvLevel, docsDevId,
            and docsDevEvText are from the entry which logs this event
            in the docsDevEventTable.  The value of
            cabhPsDevWanManMacAddress indicates the WAN-Man MAC address
            of the PS. This part of the information is uniform across
            all PS Traps."
    ::= { cabhPsDevNotifications 1 }

cabhPsDevInitTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress,
        cabhPsDevProvConfigFile,
        cabhPsDevProvConfigTLVProcessed,
        cabhPsDevProvConfigTLVRejected
    }
    STATUS      current
    DESCRIPTION
            "This inform is issued to confirm the successful completion
            of the CableHome provisioning process."
    ::= { cabhPsDevNotifications 2 }

cabhPsDevInitRetryTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
            "An event to report a failure happened during the
            initialization process and was detected in the PS."
    ::= { cabhPsDevNotifications 3 }
```

```
cabhPsDevDHCPFailTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress,
        cabhCdpServerDhcpAddress
    }
    STATUS      current
    DESCRIPTION
            "An event to report the failure of a DHCP server. The value of
            cabhCdpServerDhcpAddress is the IP address of the DHCP server."
    ::= { cabhPsDevNotifications 4 }

cabhPsDevSwUpgradeInitTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress,
        docsDevSwFilename,
        docsDevSwServer
    }
    STATUS      current
    DESCRIPTION
            "An event to report a software upgrade initiated event. The values
            of docsDevSwFilename, and docsDevSwServer indicate the software
            image name and the IP address of the server from which the image
            was downloaded."
    ::= { cabhPsDevNotifications 5 }

cabhPsDevSwUpgradeFailTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress,
        docsDevSwFilename,
        docsDevSwServer
    }
    STATUS      current
    DESCRIPTION
            "An event to report the failure of a software upgrade attempt.
            The values of docsDevSwFilename, and docsDevSwServer indicate
            the software image name and the IP address of the server from
            which the image was downloaded."
    ::= { cabhPsDevNotifications 6 }

cabhPsDevSwUpgradeSuccessTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress,
        docsDevSwFilename,
        docsDevSwServer
    }
    STATUS      current
    DESCRIPTION
            "An event to report the Software upgrade success event.
            The values of docsDevSwFilename, and docsDevSwServer
            indicate the software image name and the IP address of the
            server from which the image was downloaded."
    ::= { cabhPsDevNotifications 7 }
```

```
cabhPsDevSwUpgradeCVCFailTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
            "An event to report the failure of the verification of code
            file happened during a secure software upgrade attempt."
    ::= { cabhPsDevNotifications 8 }

cabhPsDevTODFailTrap NOTIFICATION-TYPE
    OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevTimeServerAddr,
       cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
            "An event to report the failure of a time of day server.
            The value of cabhPsDevTimeServerAddr indicates the server
            IP address."
    ::= { cabhPsDevNotifications 9 }

cabhPsDevCdpWanDataIpTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhCdpWanDataAddrClientId,
        cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
            "An event to report the failure of PS to obtain all
            needed WAN-Data Ip Addresses.
            cabhCdpWanDataAddrClientId indicates the ClientId for
            which the failure occurred."
    ::= { cabhPsDevNotifications 10 }

cabhPsDevCdpThresholdTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress,
        cabhCdpLanTransThreshold
    }
    STATUS      current
    DESCRIPTION
            "An event to report that the LAN-Trans address assignment
            threshold has been exceeded."
    ::= { cabhPsDevNotifications 11 }
```

```
cabhPsDevCspTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
            "To report an event with the CableHome Security Portal."
    ::= { cabhPsDevNotifications 12 }

cabhPsDevCapTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
            "To report an event with the CableHome Address Portal."
    ::= { cabhPsDevNotifications 13 }

cabhPsDevCtpTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
            "To report an event with the CableHome Test Portal."
    ::= { cabhPsDevNotifications 14 }

cabhPsDevProvEnrollTrap NOTIFICATION-TYPE
    OBJECTS {
        cabhPsDevHardwareVersion,
        docsDevSwCurrentVers,
        cabhPsDevTypeIdentifier,
        cabhPsDevWanManMacAddress
    }
    STATUS      current
    DESCRIPTION
            "This notification is issued to initiate the CableHome
            provisioning process for SNMP Provisioning Mode."
    ::= { cabhPsDevNotifications 15 }

cabhPsDevCdpLanIpPoolTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhPsDevWanManMacAddress,
        cabhCdpLanTransCurCount
    }
    STATUS      current
    DESCRIPTION
            "An event to report that the pool of IP addresses for LAN
            clients, as defined by cabh CdpLanPoolStart and
            cabhCdpLanPoolEnd, is exhausted."
    ::= { cabhPsDevNotifications 16 }
```

```
cabhPsDevUpnpMultiplePHTrap NOTIFICATION-TYPE
    OBJECTS {
        docsDevEvLevel,
        docsDevEvId,
        docsDevEvText,
        cabhQos2NumActivePolicyHolder,
        cabhQos2PolicyHolderEnabled,
        cabhQos2PolicyAdmissionControl
    }
    STATUS      current
    DESCRIPTION
            "To report that more than one active UPnP Policy Holders
            have been detected.
            This notification is triggered in the case the PS
            has cabhPsDevUpnpEnabled true."
    ::= { cabhPsDevNotifications 17 }

-- compliance statements

cabhPsBasicCompliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
            "The compliance statement for devices that implement the
            CableHome Portal Services logical element."
    MODULE   -- cabhPsMib

-- unconditionally mandatory groups

MANDATORY-GROUPS {
        cabhPsDevBaseGroup,
        cabhPsDevProvGroup,
        cabhPsNotificationGroup,
        cabhPsDevAttribGroup,
        cabhPsDevStatsGroup,
        cabhPsDevAccessControlGroup,
        cabhPsDevUpnpGroup
        }

--  conditionally mandatory groups

GROUP cabhPsDev802dot11Group
    DESCRIPTION
            "This group is implemented only if PS
            supports interfaces of ifType ieee80211(71)."

GROUP cabhPsDevUIGroup
    DESCRIPTION
            "This group is implemented only in CableHome compliant
            residential gateways that implement a User Interface (UI)."

OBJECT cabhPsDevTimeServerAddrType
    SYNTAX      InetAddressType { ipv4(1) }
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses. "

OBJECT cabhPsDevTimeServerAddr
    SYNTAX      InetAddress (SIZE(4))
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."
```

```
OBJECT cabhPsDevLanIpTrafficInetAddress
    SYNTAX      InetAddress (SIZE(4))
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."

OBJECT cabhPsDevUpnpCommandIpType
    SYNTAX      InetAddressType { ipv4(1) }
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."

OBJECT cabhPsDevUpnpCommandIp
    SYNTAX      InetAddress (SIZE(4))
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."


OBJECT cabhPsDevUpnpInfoIpType
    SYNTAX      InetAddressType { ipv4(1) }
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses. "

OBJECT cabhPsDevUpnpInfoIp
    SYNTAX      InetAddress (SIZE(4))
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."

    ::= { cabhPsCompliances 1 }

cabhPsDeprecatedCompliance MODULE-COMPLIANCE
    STATUS      deprecated
    DESCRIPTION
            "The compliance statement for deprecated MIB objects."
    MODULE   -- cabhPsMib

-- deprecated groups

GROUP cabhPsDevDeprecatedGroup
    DESCRIPTION
            "Group containing deprecated MIB objects."
    ::= { cabhPsCompliances 2 }

cabhPsObsoleteCompliance MODULE-COMPLIANCE
    STATUS      obsolete
    DESCRIPTION
            "The compliance statement for obsolete MIB objects."
    MODULE   -- cabhPsMib

GROUP cabhPsDevObsoleteGroup
    DESCRIPTION
            "Group containing obsolete MIB objects."

    ::= { cabhPsCompliances 3 }

cabhPsDevBaseGroup OBJECT-GROUP
    OBJECTS {
        cabhPsDevDateTime,
        cabhPsDevResetNow,
        cabhPsDevSerialNumber,
        cabhPsDevHardwareVersion,
```

```
        cabhPsDevWanManMacAddress,
        cabhPsDevWanDataMacAddress,
        cabhPsDevTypeIdentifier,
        cabhPsDevSetToFactory,
        cabhPsDevTodSyncStatus,
        cabhPsDevProvMode,
        cabhPsDevLastSetToFactory,
        cabhPsDevTrapControl
    }
    STATUS      current
    DESCRIPTION
            "A collection of objects for providing device status and
            control."
    ::= { cabhPsGroups 1 }

cabhPsDevProvGroup OBJECT-GROUP
    OBJECTS {
        cabhPsDevProvisioningTimer,
        cabhPsDevProvConfigFile,
        cabhPsDevProvConfigHash,
        cabhPsDevProvConfigFileSize,
        cabhPsDevProvConfigFileStatus,
        cabhPsDevProvConfigTLVProcessed,
        cabhPsDevProvConfigTLVRejected,
        cabhPsDevProvSolicitedKeyTimeout,
        cabhPsDevProvState,
        cabhPsDevProvAuthState,
        cabhPsDevTimeServerAddrType,
        cabhPsDevTimeServerAddr
    }
    STATUS      current
    DESCRIPTION
            "A collection of objects for controlling and providing
            status on provisioning."
    ::= { cabhPsGroups 2 }

cabhPsDevAttribGroup OBJECT-GROUP
    OBJECTS {
        cabhPsDevPsDeviceType,
        cabhPsDevPsManufacturerUrl,
        cabhPsDevPsModelUrl,
        cabhPsDevPsModelUpc
    }
    STATUS      current
    DESCRIPTION
            "A collection of objects for providing information on
            LAN IP devices known to the PS."
    ::= { cabhPsGroups 3 }

cabhPsDevStatsGroup OBJECT-GROUP
    OBJECTS {
        cabhPsDevLanIpTrafficCountersReset,
        cabhPsDevLanIpTrafficCountersLastReset,
        cabhPsDevLanIpTrafficEnabled,
        cabhPsDevLanIpTrafficInetAddressType,
        cabhPsDevLanIpTrafficInetAddress,
        cabhPsDevLanIpTrafficInOctets,
        cabhPsDevLanIpTrafficOutOctets
    }
    STATUS      current
    DESCRIPTION
            "A collection of objects for providing information
            on LAN IP traffic."
    ::= { cabhPsGroups 4 }
```

```
cabhPsDevDeprecatedGroup OBJECT-GROUP
    OBJECTS {
        cabhPsDevWanManClientId,
        cabhPsDevProvCorrelationId
    }
    STATUS      deprecated
    DESCRIPTION
            "Group of deprecated PSDev MIB objects."
    ::= { cabhPsGroups 5 }

cabhPsNotificationGroup NOTIFICATION-GROUP
    NOTIFICATIONS {
        cabhPsDevInitTLVUnknownTrap,
        cabhPsDevInitTrap,
        cabhPsDevInitRetryTrap,
        cabhPsDevDHCPFailTrap,
        cabhPsDevSwUpgradeInitTrap,
        cabhPsDevSwUpgradeFailTrap,
        cabhPsDevSwUpgradeSuccessTrap,
        cabhPsDevSwUpgradeCVCFailTrap,
        cabhPsDevTODFailTrap,
        cabhPsDevCdpWanDataIpTrap,
        cabhPsDevCdpThresholdTrap,
        cabhPsDevCspTrap,
        cabhPsDevCapTrap,
        cabhPsDevCtpTrap,
        cabhPsDevProvEnrollTrap,
        cabhPsDevCdpLanIpPoolTrap,
        cabhPsDevUpnpMultiplePHTrap
    }
    STATUS      current
    DESCRIPTION
            "These notifications indicate change in status of the
            Portal Services set of functions in a device complying
            with ITU-T Rec. J.192."
    ::= { cabhPsGroups 6 }

cabhPsDevAccessControlGroup OBJECT-GROUP
    OBJECTS {
        cabhPsDevAccessControlEnable,
        cabhPsDevAccessControlPhysAddr,
        cabhPsDevAccessControlRowStatus
    }
    STATUS      current
    DESCRIPTION
            "Group of Access Control objects for the CableHome PSDev
            MIB."
    ::= { cabhPsGroups 7 }

cabhPsDevUIGroup OBJECT-GROUP
    OBJECTS {
        cabhPsDevUILogin,
        cabhPsDevUIPassword,
        cabhPsDevUISelection,
        cabhPsDevUIServerUrl,
        cabhPsDevUISelectionDisabledBodyText
    }
    STATUS      current
    DESCRIPTION
            "A collection of objects for configuring the selection and
            operation of the User Interface displayed to an HTTP
            client, if a UI is implemented."
    ::= { cabhPsGroups 8 }
```

```
cabhPsDev802dot11Group OBJECT-GROUP
    OBJECTS {
                cabhPsDev802dot11BaseSetToDefault,
                cabhPsDev802dot11BaseLastSetToDefault,
                cabhPsDev802dot11BaseAdvertiseSSID,
                cabhPsDev802dot11BasePhyCapabilities,
                cabhPsDev802dot11BasePhyOperMode,
                cabhPsDev802dot11SecCapabilities,
                cabhPsDev802dot11SecOperMode,
                cabhPsDev802dot11SecPassPhraseToWEPKey,
                cabhPsDev802dot11SecUsePassPhraseToWEPKeyAlg,
                cabhPsDev802dot11SecPSKPassPhraseToKey,
                cabhPsDev802dot11SecWPAPreSharedKey,
                cabhPsDev802dot11SecWPARekeyTime,
                cabhPsDev802dot11SecControl,
                cabhPsDev802dot11SecCommitStatus
            }
    STATUS      current
    DESCRIPTION
            "Group of CableHome proprietary objects for the management
            of IEEE 80211 interfaces."
    ::= { cabhPsGroups 9 }

cabhPsDevUpnpGroup OBJECT-GROUP
    OBJECTS {
                cabhPsDevUpnpEnabled,
                cabhPsDevUpnpCommandIpType,
                cabhPsDevUpnpCommandIp,
                cabhPsDevUpnpCommand,
                cabhPsDevUpnpCommandUpdate,
                cabhPsDevUpnpLastCommandUpdate,
                cabhPsDevUpnpCommandStatus,
                cabhPsDevUpnpInfoXmlFragment
              }
    STATUS      current
    DESCRIPTION
            "Group of MIB objects for the management interface
            of UPnP Services."
    ::= { cabhPsGroups 10 }

cabhPsDevObsoleteGroup OBJECT-GROUP
    OBJECTS {
        cabhPsDevBpDeviceType,
        cabhPsDevBpManufacturer,
        cabhPsDevBpManufacturerUrl,
        cabhPsDevBpSerialNumber,
        cabhPsDevBpHardwareVersion,
        cabhPsDevBpHardwareOptions,
        cabhPsDevBpModelName,
        cabhPsDevBpModelNumber,
        cabhPsDevBpModelUrl,
        cabhPsDevBpModelUpc,
        cabhPsDevBpModelSoftwareOs,
        cabhPsDevBpModelSoftwareVersion,
        cabhPsDevBpLanInterfaceType,
        cabhPsDevBpNumberInterfacePriorities,
        cabhPsDevBpPhysicalLocation,
        cabhPsDevBpPhysicalAddress
    }
    STATUS      obsolete
    DESCRIPTION
            "Group of BP related objects with obsoleted status."
    ::= { cabhPsGroups 11 }

END
```

E.5 Requisitos de la MIB seguridad IPCable2Home (SEC, IPCable2Home Security)

La SEC MIB CableHome™ DEBE implementarse tal como se define a continuación.

```
CABH-SEC-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    Unsigned32,
    zeroDotZero,
    Counter32,
    OBJECT-TYPE                FROM SNMPv2-SMI  -- RFC 2578

    DateAndTime,
    TruthValue,
    TimeStamp,
    RowStatus,
    VariablePointer            FROM SNMPv2-TC  -- RFC 2579

    OBJECT-GROUP,
    MODULE-COMPLIANCE          FROM SNMPv2-CONF -- RFC 2580
    InetPortNumber,
    InetAddress                FROM INET-ADDRESS-MIB -- RFC 3291

    SnmpAdminString            FROM SNMP-FRAMEWORK-MIB -- RFC 2571

    X509Certificate            FROM DOCS-BPI2-MIB

    ZeroBasedCounter32         FROM RMON2-MIB
    docsDevFilterIpEntry       FROM DOCS-CABLE-DEVICE-MIB
    InterfaceIndexOrZero       FROM IF-MIB

    clabProjCableHome          FROM CLAB-DEF-MIB;

    cabhSecMib MODULE-IDENTITY
    LAST-UPDATED    "200408060000Z" -- August 6, 2004
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
            858 Coal Creek Circle
            Louisville, Colorado 80027
            U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com; mibs@cablelabs.com"
    DESCRIPTION
            "This MIB module supplies the basic management
            objects for the Security Portal Services."
    ::=  { clabProjCableHome 2 }


-- Textual conventions

   cabhSecMibObjects  OBJECT IDENTIFIER ::= { cabhSecMib 5 }
   cabhSecFwObjects   OBJECT IDENTIFIER ::= { cabhSecMib 1 }
   cabhSecFwBase      OBJECT IDENTIFIER ::= { cabhSecFwObjects 1 }
   cabhSecFwLogCtl    OBJECT IDENTIFIER ::= { cabhSecFwObjects 2 }

   cabhSecCertObjects OBJECT IDENTIFIER ::= { cabhSecMib 2 }
   cabhSecKerbObjects OBJECT IDENTIFIER ::= { cabhSecMibObjects 3 }
   cabhSecKerbBase    OBJECT IDENTIFIER ::= { cabhSecKerbObjects 1 }
```

```
   cabhSec2FwObjects  OBJECT IDENTIFIER ::= { cabhSecMibObjects 4 }
   cabhSec2FwBase     OBJECT IDENTIFIER ::= { cabhSec2FwObjects 1 }
   cabhSec2FwEvent    OBJECT IDENTIFIER ::= { cabhSec2FwObjects 2 }
   cabhSec2FwLog      OBJECT IDENTIFIER ::= { cabhSec2FwObjects 3 }
   cabhSec2FwFilter   OBJECT IDENTIFIER ::= { cabhSec2FwObjects 4 }

--
--    CableHome 1.0 Base Firewall Functions
--

cabhSecFwPolicyFileEnable OBJECT-TYPE
    SYNTAX      INTEGER {
                    enable (1),
                    disable(2)
                }
    MAX-ACCESS  read-write
    STATUS      deprecated
    DESCRIPTION
            "This parameter indicates whether or not to enable
            the firewall functionality."
    DEFVAL { enable }
    ::= { cabhSecFwBase 1 }

cabhSecFwPolicyFileURL OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-write
    STATUS      deprecated
    DESCRIPTION
            "A policy rule set file download is triggered when the
            value used to set this object is different than the value
            in the cabhSecFwPolicySuccessfulFileURL object."
    REFERENCE
            "CableHome 1.0 Specification, CH-SP-CH1.0-I05-030801,
            11.3.5.2 of ITU-T Rec. J.191, Firewall Rule Set Management
            Parameters."
    DEFVAL { "" }
    ::= { cabhSecFwBase 2 }

cabhSecFwPolicyFileHash OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0|20))
    MAX-ACCESS  read-write
    STATUS      deprecated
    DESCRIPTION
            "Hash of the contents of the rules set file,
            calculated and sent to the PS prior to sending
            the rules set file. For the SHA-1 authentication
            algorithm, the length of the hash is 160 bits.
            This hash value is encoded in binary format."
    DEFVAL { ''h }
    ::= { cabhSecFwBase 3 }

cabhSecFwPolicyFileOperStatus OBJECT-TYPE
    SYNTAX      INTEGER {
                    inProgress(1),
                    complete(2),
                 -- completeFromMgt(3), deprecated
                    failed(4)
                }
    MAX-ACCESS  read-only
    STATUS      deprecated
```

```
    DESCRIPTION
            "inProgress(1) indicates a firewall configuration
            file download is under way.
            complete (2) indicates the firewall configuration
            file downloaded and configured successfully.
            completeFromMgt(3). This state is deprecated.
            failed(4) indicates the last attempted firewall
            configuration file download or processing
            failed ordinarily due to TFTP timeout."
    ::= { cabhSecFwBase 4 }

cabhSecFwPolicyFileCurrentVersion OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
            "The rule set version currently operating in the
            PS device. This object should be in the syntax
            used by the individual vendor to identify software
            versions. Any PS element MUST return a string
            descriptive of the current rule set file load.
            If this is not applicable, this object MUST
            contain an empty string."
    ::= { cabhSecFwBase 5 }

cabhSecFwPolicySuccessfulFileURL OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-only
    STATUS      deprecated
    DESCRIPTION
            "Contains the location of the last successful downloaded
            policy rule set file in the format pointed in the
            reference. If a successful download has never occurred,
            this MIB object MUST report empty string."
    REFERENCE
            "CableHome 1.0 Specification, CH-SP-CH1.0-I05-030801,
            11.3.5.2 of ITU-T Rec. J.191, Firewall Rule Set Management
            Parameters."
    DEFVAL { "" }
    ::= { cabhSecFwBase 6 }

--
-- CableHome 1.0 Firewall Event MIBs
--

cabhSecFwEventType1Enable OBJECT-TYPE
    SYNTAX      INTEGER {
                    enable(1), -- log event
                    disable(2) -- do not log event
                }
    MAX-ACCESS  read-write
    STATUS      deprecated
    DESCRIPTION
            "This object enables or disables logging of type 1
            firewall event messages. Type 1 event messages report
            attempts from both private and public clients to
            traverse the firewall that violate the Security
            Policy."
    DEFVAL { disable }
    ::= { cabhSecFwLogCtl 1 }
```

```
cabhSecFwEventType2Enable OBJECT-TYPE
    SYNTAX      INTEGER {
                    enable(1), -- log event
                    disable(2) -- do not log event
                }
    MAX-ACCESS  read-write
    STATUS      deprecated
    DESCRIPTION
            "This object enables or disables logging of
            type 2 firewall event messages. Type 2 event
            messages report identified Denial of Service
            attack attempts."
    DEFVAL { disable }
    ::= { cabhSecFwLogCtl 2 }

cabhSecFwEventType3Enable OBJECT-TYPE
    SYNTAX      INTEGER {
                    enable(1), -- log event
                    disable(2) -- do not log event
                }
    MAX-ACCESS  read-write
    STATUS      deprecated
    DESCRIPTION
            "Enables or disables logging of type 3 firewall
            event messages. Type 3 event messages report
            changes made to the following firewall management
            parameters: cabhSecFwPolicyFileURL,
            cabhSecFwPolicyFileCurrentVersion,
            cabhSecFwPolicyFileEnable"
    DEFVAL { disable }
    ::= { cabhSecFwLogCtl 3 }

cabhSecFwEventAttackAlertThreshold OBJECT-TYPE
    SYNTAX      INTEGER (0..65535)
    MAX-ACCESS  read-write
    STATUS      deprecated
    DESCRIPTION
            "If the number of type 1 or 2 hacker attacks
            exceeds this threshold in the period defined
            by cabhSecFwEventAttackAlertPeriod, a firewall
            message event MUST be logged with priority
            level 4."
    DEFVAL { 65535 }
    ::= { cabhSecFwLogCtl 4 }

cabhSecFwEventAttackAlertPeriod OBJECT-TYPE
    SYNTAX      INTEGER (0..65535)
    MAX-ACCESS  read-write
    STATUS      deprecated
    DESCRIPTION
            "Indicates the period to be used (in hours) for
            the cabhSecFwEventAttackAlertThreshold. This MIB
            variable should always keep track of the last x
            hours of events meaning that if the variable is
            set to track events for 10 hours then, when the
            11th hour is reached, the 1st hour of events is
            deleted from the tracking log. A default value
            is set to zero, meaning zero time, so that this
            MIB variable will not track any events unless
            configured."
    DEFVAL { 0 }
    ::= { cabhSecFwLogCtl 5 }
```

```
--
-- CableHome PS device certificate
--

    cabhSecCertPsCert OBJECT-TYPE
    SYNTAX      X509Certificate
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The X509 DER-encoded PS certificate."
    ::= { cabhSecCertObjects 1 }

--
--  CableHome 1.1 Firewall Management MIBs
--

cabhSec2FwEnable OBJECT-TYPE
    SYNTAX      INTEGER    {
                    enabled(1),
                    disabled(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This parameter indicates whether to enable or disable the
            firewall."
    DEFVAL { enabled }
    ::= { cabhSec2FwBase 1 }

cabhSec2FwPolicyFileURL OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "A policy rule set file download is triggered when the
            value used to set this object is different than the value
            in the cabhSec2FwPolicySuccessfulFileURL object."
    REFERENCE
            "CableHome 1.1 Specification, CH-SP-CH1.1-I05-040806,
            11.6.4.9.1 of ITU-T Rec. J.192, Firewall Rule Set Management
            MIB Objects."
    DEFVAL { "" }
    ::= { cabhSec2FwBase 2 }

cabhSec2FwPolicyFileHash OBJECT-TYPE
    SYNTAX      OCTET STRING (SIZE(0|20))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Hash of the contents of the firewall
            configuration file. For the SHA-1 authentication
            algorithm, the length of the hash is 160 bits.
            This hash value is encoded in binary format."
    DEFVAL { ''h }
    ::= { cabhSec2FwBase 3 }

cabhSec2FwPolicyFileOperStatus OBJECT-TYPE
    SYNTAX      INTEGER {
                    inProgress(1),
                    complete(2),
                    failed(3)
                }
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
            "InProgress(1) indicates a firewall configuration file download
            is under way. Complete(2) indicates the firewall configuration
            file was downloaded and processed successfully. Failed(3)
            indicates that the last attempted firewall configuration
            file download or processing failed."
    ::= { cabhSec2FwBase 4 }

cabhSec2FwPolicyFileCurrentVersion OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "A label set by the cable operator that can be used to track
            various versions of configured rulesets. Once the label is
            set and configured rules are changed, it may not accurately
            reflect the version of configured rules running on the box.
            If this object has never been configured, it MUST contain
            an empty string."
    DEFVAL { "" }
    ::= { cabhSec2FwBase 5 }

cabhSec2FwClearPreviousRuleset OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "If set to 'true', the PS MUST clear all entries in the
            docsDevFilterIpTable. Reading this value always returns
            false."
    REFERENCE
            "CableHome specification - Security section"
    DEFVAL { false }
    ::= { cabhSec2FwBase 6 }

cabhSec2FwPolicySelection OBJECT-TYPE
    SYNTAX      INTEGER {
                    factoryDefault(1),
                    configuredRulesetBoth(2),
                    factoryDefaultAndConfiguredRulesetBoth(3),
                    configuredRulesetDocsDevFilterIpTable(4),
                    configuredRulesetCabhSec2FwLocalFilterIpTable (5),
                    factoryDefaultAndDocsDevFilterIpTable (6),
                    factoryDefaultAndCabhSec2FwLocalFilterIpTable (7)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This object allows for selection of the filtering policy
            as defined by the following options:

            factoryDefault (1) The firewall filters against the Factory
            Default Ruleset in the cabhSec2FwFactoryDefaultFilterTable.

            configuredRulesetBoth (2) The firewall filters against the
            Configured Ruleset defined by both the
            docsDevFilterIpTable and the cabhSec2FwLocalFilterIpTable.

            factoryDefaultAndConfiguredRulesetBoth (3) The firewall
            filters against the CableHome specified Factory Default
            Ruleset in the cabhSec2FwFactoryDefaultFilterTable and
            the Configured Ruleset in the docsDevFilterIpTable and
            the cabhSec2FwLocalFilterIpTable.
```

```
            configuredRulesetDocsDevFilterIpTable(4) The firewall
            filters against the Configured Ruleset defined by the
            docsDevFilterIpTable.

            configuredRulesetCabhSec2FwLocalFilterIpTable (5) The
            firewall filters against the Configured Ruleset defined
            by the cabhSec2FwLocalFilterIpTable.

            factoryDefaultAndDocsDevFilterIpTable (6) The firewall
            filters against the Factory Default Ruleset and the
            Configured Ruleset defined by the DocsDevFilterIpTable.

            factoryDefaultAndCabhSec2FwLocalFilterIpTable (7) The
            firewall filters against the Factory Default Ruleset
            and the Configured Ruleset defined by the
            cabhSec2FwLocalFilterIpTable."
    REFERENCE
            "CableHome specification - Security section."
    DEFVAL { factoryDefault }
    ::= { cabhSec2FwBase 7 }

cabhSec2FwEventSetToFactory OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "If set to 'true', entries in cabhSec2FwEventControlEntry
            are set to their default values.
            Reading this value always returns false."
    DEFVAL { false }
    ::= { cabhSec2FwBase 8 }

cabhSec2FwEventLastSetToFactory OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The value of sysUpTime when cabhSec2FwEventSetToFactory
            was Last set to true. Zero if never reset."
    ::= { cabhSec2FwBase 9 }

cabhSec2FwPolicySuccessfulFileURL OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Contains the location of the last successful downloaded
            policy rule set file in the format pointed in the
            reference. If a successful download has not yet
            occurred, this MIB object should report empty string."
    REFERENCE
            "CableHome 1.1 Specification, CH-SP-CH1.1-I05-040806,
            11.6.4.9.1 of ITU-T Rec. J.192, Firewall Rule Set Management MIB
Objects."
    DEFVAL { "" }
    ::= { cabhSec2FwBase 10 }

cabhSec2FwConfiguredRulesetPriority OBJECT-TYPE
    SYNTAX      INTEGER {
                    docsDevFilterIpTable (1),
                    cabhSec2FwLocalFilterIpTable (2)
                }
    MAX-ACCESS  read-write
    STATUS      current
```

```
    DESCRIPTION
            "This object defines which Configured Ruleset filter rule
             has priority when a conflict exists between a filter rule
             in the docsDevFilterIpTable and a filter rule in the
             cabhSec2FwLocalFilterIpTable as indicated by the following
             options:

             docsDevFilterIpTable (1) - indicates that filter rules in
             the docsDevFilterIpTable have priority over any
             conflicting filters that may exist in the
             cabhSec2FwLocalFilterIpTable.

             cabhSec2FwLocalFilterIpTable (2) - indicates that filter
             rules in the cabhSec2FwLocalFilterIpTable have priority
             over any conflicting filters that may exist in the
             docsDevFilterIpTable."
    REFERENCE
             "CableHome specification - Security section."
    DEFVAL { cabhSec2FwLocalFilterIpTable }
    ::= { cabhSec2FwBase 11 }

cabhSec2FwClearLocalRuleset OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "If set to 'true', the PS MUST clear all entries in the
            cabhSec2FwLocalFilterIpTable. Reading this value always
            returns false."
    REFERENCE
            "CableHome specification - Security section"
    DEFVAL { false }
    ::= { cabhSec2FwBase 12 }

-- ++++++++++

--
-- CableHome 1.1 Firewall Event MIBs
--


cabhSec2FwEventControlTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhSec2FwEventControlEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table controls the reporting of the
            Firewall Attacks events"
    ::= { cabhSec2FwEvent 1 }

cabhSec2FwEventControlEntry OBJECT-TYPE
    SYNTAX      CabhSec2FwEventControlEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Allows configuration of the reporting mechanisms
            for a particular type of attack."
    INDEX { cabhSec2FwEventType }
    ::= { cabhSec2FwEventControlTable 1 }
```

```
CabhSec2FwEventControlEntry ::= SEQUENCE {
    cabhSec2FwEventType          INTEGER,
    cabhSec2FwEventEnable        INTEGER,
    cabhSec2FwEventThreshold     Unsigned32,
    cabhSec2FwEventInterval      Unsigned32,
    cabhSec2FwEventCount         ZeroBasedCounter32,
    cabhSec2FwEventLogReset      TruthValue,
    cabhSec2FwEventLogLastReset TimeStamp
    }

cabhSec2FwEventType OBJECT-TYPE
    SYNTAX      INTEGER     {
                    type1(1),
                    type2(2),
                    type3(3),
                    type4(4),
                    type5(5),
                    type6(6)
                }
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Classification of the different types of
            attacks.
            Type 1  logs all attempts from both LAN and WAN
            clients to traverse the Firewall that violate the
            Security Policy.
            Type 2 logs identified Denial of Service attack
            attempts.
            Type 3 logs all changes made to the
            cabhSec2FwPolicyFileURL,
            cabhSec2FwPolicyFileCurrentVersion or
            cabhSec2FwPolicyFileEnable objects.
            Type 4 logs all failed attempts to modify
            cabhSec2FwPolicyFileURL and
            cabhSec2FwPolicyFileEnable objects.
            Type 5 logs allowed inbound packets from the WAN.
            Type 6 logs allowed outbound packets from the
            LAN."
    ::= { cabhSec2FwEventControlEntry 1 }

cabhSec2FwEventEnable OBJECT-TYPE
    SYNTAX      INTEGER    {
                    enabled(1),
                    disabled(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Enables or disables counting and logging of
            firewall events by type as assigned by
            cabhSec2FwEventType."
    DEFVAL { disabled }
    ::= { cabhSec2FwEventControlEntry 2 }

cabhSec2FwEventThreshold OBJECT-TYPE
    SYNTAX       Unsigned32 (0..65535)
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
            "Number of attacks to count before sending the appropriate
            event by type as assigned by cabhSec2FwEventType."
    DEFVAL { 0 }
    ::= { cabhSec2FwEventControlEntry 3 }
```

```
cabhSec2FwEventInterval OBJECT-TYPE
    SYNTAX      Unsigned32 (0..744)
    UNITS       "hours"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Indicates the time interval in hours to count and log
            occurrences of a firewall event type as assigned in
            cabhSec2FwEventType. If this MIB has a value of zero,
            then there is no interval assigned and the PS will not
            count or log events."
    DEFVAL { 0 }
    ::= { cabhSec2FwEventControlEntry 4 }

cabhSec2FwEventCount OBJECT-TYPE
    SYNTAX       ZeroBasedCounter32
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
           "Indicates the current count up to the
            cabhSec2FwEventThreshold value by type as
            assigned by cabhSec2FwEventType."
    ::= { cabhSec2FwEventControlEntry 5 }

cabhSec2FwEventLogReset OBJECT-TYPE
    SYNTAX       TruthValue
    MAX-ACCESS   read-write
    STATUS       current
    DESCRIPTION
            "Setting this object to true clears the log table
            for the specified event type. Reading this object
            always returns false."
    DEFVAL { false }
    ::= { cabhSec2FwEventControlEntry 6 }

cabhSec2FwEventLogLastReset OBJECT-TYPE
    SYNTAX       TimeStamp
    MAX-ACCESS   read-only
    STATUS       current
    DESCRIPTION
            "The value of sysUpTime when cabhSec2FwEventLogReset was
            last set to true. Zero if never reset."
    ::= { cabhSec2FwEventControlEntry 7 }

--
-- CableHome 1.1 Firewall Log Tables
--

cabhSec2FwLogTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhSec2FwLogEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Contains a log of packet information as related
            to events enabled by the cable operator. The types
            are defined in the CableHome 1.1 specification and
            require various objects to be included in the log.
            The following is a description for what is
            expected in the log for each type Type 1, Type 2,
            Type 5 and Type 6 table MUST include
            cabhSec2FwEventType, cabhSec2FwEventPriority,
            cabhSec2FwEventId, cabhSec2FwLogTime,
            cabhSec2FwIpProtocol, cabhSec2FwIpSourceAddr,
```

```
            cabhSec2FwIpDestAddr, cabhSec2FwIpSourcePort,
            cabhSec2FwIpDestPort, cabhSec2Fw,
            cabhSec2FwReplayCount. The other values not used
            by Types 1, 2, 5 and 6 are default values. Type 3
            and Type 4 MUST include cabhSec2FwEventType,
            cabhSec2FwEventPriority, cabhSec2FwEventId,
            cabhSec2FwLogTime, cabhSec2FwIpSourceAddr,
            cabhSec2FwLogMIBPointer. The other values not used
            by type 3 and 4 are default values. When applicable,
            Type 1, Type 5,and Type 6 MUST also include
            cabhSec2FwLogMatchingFilterTableName,
            cabhSec2FwLogMatchingFilterTableIndex,
            cabhSec2FwLogMatchingFilterDescr."
    ::= { cabhSec2FwLog 1 }

cabhSec2FwLogEntry OBJECT-TYPE
    SYNTAX      CabhSec2FwLogEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Each entry contains the log of firewall events"
    INDEX {cabhSec2FwLogIndex}
    ::= { cabhSec2FwLogTable 1 }

CabhSec2FwLogEntry ::= SEQUENCE {
    cabhSec2FwLogIndex                    Unsigned32,
    cabhSec2FwLogEventType                INTEGER,
    cabhSec2FwLogEventPriority            INTEGER,
    cabhSec2FwLogEventId                  Unsigned32,
    cabhSec2FwLogTime                     DateAndTime,
    cabhSec2FwLogIpProtocol               Unsigned32,
    cabhSec2FwLogIpSourceAddr             InetAddress,
    cabhSec2FwLogIpDestAddr               InetAddress,
    cabhSec2FwLogIpSourcePort             InetPortNumber,
    cabhSec2FwLogIpDestPort               InetPortNumber,
    cabhSec2FwLogMessageType              Unsigned32,
    cabhSec2FwLogReplayCount              Unsigned32,
    cabhSec2FwLogMIBPointer               VariablePointer,
    cabhSec2FwLogMatchingFilterTableName  INTEGER,
    cabhSec2FwLogMatchingFilterTableIndex Unsigned32,
    cabhSec2FwLogMatchingFilterDescr      SnmpAdminString
    }

cabhSec2FwLogIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (1..2147483647)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "A sequence number for the specific events
            under a cabhSec2FwEventType."
    ::= { cabhSec2FwLogEntry 1 }

cabhSec2FwLogEventType OBJECT-TYPE
    SYNTAX INTEGER     {
               type1(1),
               type2(2),
               type3(3),
               type4(4),
               type5(5),
               type6(6)
           }
    MAX-ACCESS  read-only
    STATUS      current
```

```
    DESCRIPTION
            "Classification of the different types of
            attacks.
            Type 1 logs all attempts from both LAN and WAN
            clients to traverse the Firewall that violate
            the Security Policy.
            Type 2 logs identified Denial of Service attack
            attempts.
            Type 3 logs all changes made to the
            cabhSec2FwPolicyFileURL,
            cabhSec2FwPolicyFileCurrentVersion or
            cabhSec2FwPolicyFileEnable objects.
            Type 4 logs all failed attempts to modify
            cabhSec2FwPolicyFileURL and
            cabhSec2FwPolicyFileEnable objects.
            Type 5 logs allowed inbound packets from the WAN.
            Type 6 logs allowed outbound packets from the
            LAN."
    ::= { cabhSec2FwLogEntry 2 }

cabhSec2FwLogEventPriority OBJECT-TYPE
    SYNTAX     INTEGER     {
                   emergency(1),
                   alert(2),
                   critical(3),
                   error(4),
                   warning(5),
                   notice(6),
                   information(7),
                   debug(8)
               }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The priority level of this event as defined by CableHome
            Specification. If a priority is not assigned in the CableHome
            specification for a particular event, then the vendor or cable
            operator may assign priorities. These are ordered from most serious
            (emergency)to least serious (debug)."
    ::= { cabhSec2FwLogEntry 3 }

cabhSec2FwLogEventId  OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The assigned event ID."
    ::= { cabhSec2FwLogEntry 4 }

cabhSec2FwLogTime OBJECT-TYPE
    SYNTAX      DateAndTime
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The time that this entry was created by the PS."
    ::= { cabhSec2FwLogEntry 5 }

cabhSec2FwLogIpProtocol OBJECT-TYPE
    SYNTAX      Unsigned32 (0..256)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The IP Protocol."
    ::= { cabhSec2FwLogEntry 6 }
```

```
cabhSec2FwLogIpSourceAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The Source IP Address of the packet logged."
    ::= { cabhSec2FwLogEntry 7 }

cabhSec2FwLogIpDestAddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The Destination IP Address of the packet logged."
    ::= { cabhSec2FwLogEntry 8 }

cabhSec2FwLogIpSourcePort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The Source IP Port of the packet logged."
    ::= { cabhSec2FwLogEntry 9 }

cabhSec2FwLogIpDestPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The Source IP Port of the packet logged."
    ::= { cabhSec2FwLogEntry 10 }

cabhSec2FwLogMessageType OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The ICMP defined types."
    ::= { cabhSec2FwLogEntry 11}

cabhSec2FwLogReplayCount OBJECT-TYPE
    SYNTAX      Unsigned32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of identical attack packets that
            were seen by the firewall based on
            cabhSec2FwLogIpProtocol, cabhSec2FwLogIpSourceAddr,
            cabhSec2FwLogIpDestAddr, cabhSec2FwLogIpSourcePort,
            cabhSec2FwLogIpDestPort and cabhSec2FwLogMessageType."
    DEFVAL { 0 }
    ::= { cabhSec2FwLogEntry 12 }

cabhSec2FwLogMIBPointer OBJECT-TYPE
    SYNTAX      VariablePointer
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Identifies if the cabhSec2FwPolicyFileURL or the
            cabhSec2FwEnable MIB object changed or an attempt
            was made to change it."
    DEFVAL { zeroDotZero }
    ::= { cabhSec2FwLogEntry 13 }
```

```
cabhSec2FwLogMatchingFilterTableName OBJECT-TYPE
    SYNTAX      INTEGER     {
                   cabhSec2FwFactoryDefaultFilterTable(1),
                   docsDevFilterIpTable(2),
                   cabhSec2FwLocalFilterIpTable(3),
                   none(4)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "When applicable, cabhSec2FwLogMatchingFilterTableName
            indicates the filter table name containing the last filter
            rule matched that caused the event to be generated."
    DEFVAL { none }
    ::= { cabhSec2FwLogEntry 14 }

cabhSec2FwLogMatchingFilterTableIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (0..2147483647)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "When applicable, cabhSec2FwLogMatchingFilterTableIndex
            indicates the filter table index if the last filter
            rule matched that caused the event to be generated. If
            the value is 0, the event was not caused by a filter
            rule match. "
    DEFVAL { 0 }
    ::= { cabhSec2FwLogEntry 15 }

cabhSec2FwLogMatchingFilterDescr OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "When applicable, cabhSec2FwLogMatchingFilterDesc
            contains the description value found in the
            cabhSec2FwFilterScheduleDesc MIB object or the
            cabhSec2FwLocalFilterIpDesc MIB object of the last
            filter rule matched that caused the event to be
            generated."
    DEFVAL { "" }
    ::= { cabhSec2FwLogEntry 16 }

-- ============================================================
--
--  CableHome 1.1 PS IP Filter Scheduling Table
--
--  The cabhSec2FwFilterScheduleTable contains the firewall
--  policy identification and links that policy as defined
--  in RFC 2669 to specific time of day restrictions.
--
-- ============================================================

cabhSec2FwFilterScheduleTable OBJECT-TYPE
    SYNTAX SEQUENCE OF CabhSec2FwFilterScheduleEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Extends the filtering matching parameters of
            docsDevFilterIpTable defined in RFC 2669 for CableHome
            Residential Gateways to include time day intervals and days
            of the week."
    ::= { cabhSec2FwFilter 1 }
```

```
cabhSec2FwFilterScheduleEntry OBJECT-TYPE
    SYNTAX      CabhSec2FwFilterScheduleEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Extended values for entries of docsDevFilterIpTable.
            If the PS has not acquired ToD, the entire
            docsDevFilterIpEntry rule set is ignored.
            Note - A filter time period may include two days
            (e.g., from 10 PM to 4 AM).  A filter time period that
            includes two days is identified by the absolute value
            of the cabhSec2FwFilterScheduleEndTime being less than the
            absolute value of the cabhSec2FwFilterScheduleStartTime.
            The cabhSec2FwFilterScheduleDOW setting and the
            cabhSec2FwFilterScheduleStartTime value indicate what day
            and time the filter becomes active. The
            cabhSec2FwFilterScheduleEndTime indicates when the filter
            becomes inactive on the second day. The maximum filter
            time period that includes two days is 24 hours.
            If cabhSec2FwFilterScheduleStartTime is less than or
            equal to the cabhSec2FwFilterScheduleEndTime, the time
            period of the filter falls in the same day."
    AUGMENTS { docsDevFilterIpEntry }
    ::= { cabhSec2FwFilterScheduleTable 1 }

CabhSec2FwFilterScheduleEntry ::= SEQUENCE {
    cabhSec2FwFilterScheduleStartTime    Unsigned32,
    cabhSec2FwFilterScheduleEndTime      Unsigned32,
    cabhSec2FwFilterScheduleDOW          BITS,
    cabhSec2FwFilterScheduleDescr        SnmpAdminString
    }

cabhSec2FwFilterScheduleStartTime OBJECT-TYPE
    SYNTAX      Unsigned32 (0..2359)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The start time for matching the filter ruleset in the
            specified days indicated in cabhSec2FwFilterScheduleDOW.
            Time is represented in Military Time, e.g., 8:30 AM is
            represented as 830 and 11:45 PM as 2345. An attempt to set
            this object to an invalid military time value, e.g., 1182,
            returns 'wrongValue' error."
    DEFVAL { 0 }
    ::= { cabhSec2FwFilterScheduleEntry 1 }

cabhSec2FwFilterScheduleEndTime OBJECT-TYPE
    SYNTAX      Unsigned32 (0..2359)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The end time for matching the filter rule for the
            days indicated in cabhSec2FwFilterScheduleDOW. The filter
            rule associated with this end time MUST not be disabled
            until the minute following the time indicated by this
            MIB object. If the time period is for two days,
            identified by cabhSec2FwFilterScheduleEndTime being
            less than cabhSec2FwFilterScheduleStartTime, then
            the cabhSec2FwFilterScheduleDOW settings
            do not apply to this MIB object.
```

```
            Time is represented in the same manner as in
            cabhSec2FwFilterScheduleStartTime. An attempt to set
            this object to an invalid military time value, e.g., 1182,
            returns 'wrongValue' error."
    DEFVAL { 2359 }
    ::= { cabhSec2FwFilterScheduleEntry 2 }

cabhSec2FwFilterScheduleDOW OBJECT-TYPE
    SYNTAX BITS {
                    sunday(0),
                    monday(1),
                    tuesday(2),
                    wednesday(3),
                    thursday(4),
                    friday(5),
                    saturday(6)
                }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "If the day of week bit associated with the PS given day
            is '1', this object criteria matches."
    DEFVAL { 'fe'h }  -- 11111110 Sun-Sat
    ::= { cabhSec2FwFilterScheduleEntry 3 }

cabhSec2FwFilterScheduleDescr OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "A filter rule description configured by the
            cable operator or subscriber."
    DEFVAL { "" }
    ::= { cabhSec2FwFilterScheduleEntry 4 }

-- ============================================================
--
--  CableHome 1.1 PS Firewall Factory Default Filter Table
--
--  The cabhSec2FwFactoryDefaultFilterTable contains the
--  firewall factory default ruleset in a read only table as
--  defined by the CableLabs CableHome 1.1 Specification.
--
-- ============================================================

cabhSec2FwFactoryDefaultFilterTable OBJECT-TYPE
    SYNTAX SEQUENCE OF CabhSec2FwFactoryDefaultFilterEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Contains the firewall factory default ruleset as
            defined by the CableLabs CableHome 1.1 Specification."
    ::= { cabhSec2FwFilter 2 }

cabhSec2FwFactoryDefaultFilterEntry OBJECT-TYPE
    SYNTAX      CabhSec2FwFactoryDefaultFilterEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Contains the firewall factory default ruleset."
    INDEX {cabhSec2FwFactoryDefaultFilterIndex }
    ::= { cabhSec2FwFactoryDefaultFilterTable 1 }
```

```
CabhSec2FwFactoryDefaultFilterEntry ::= SEQUENCE {
    cabhSec2FwFactoryDefaultFilterIndex          Unsigned32,
    cabhSec2FwFactoryDefaultFilterControl        INTEGER,
    cabhSec2FwFactoryDefaultFilterIfIndex        InterfaceIndexOrZero,
    cabhSec2FwFactoryDefaultFilterDirection      INTEGER,
    cabhSec2FwFactoryDefaultFilterSaddr          InetAddress,
    cabhSec2FwFactoryDefaultFilterSmask          InetAddress,
    cabhSec2FwFactoryDefaultFilterDaddr          InetAddress,
    cabhSec2FwFactoryDefaultFilterDmask          InetAddress,
    cabhSec2FwFactoryDefaultFilterProtocol       Unsigned32,
    cabhSec2FwFactoryDefaultFilterSourcePortLow  Unsigned32,
    cabhSec2FwFactoryDefaultFilterSourcePortHigh Unsigned32,
    cabhSec2FwFactoryDefaultFilterDestPortLow    Unsigned32,
    cabhSec2FwFactoryDefaultFilterDestPortHigh   Unsigned32,
    cabhSec2FwFactoryDefaultFilterContinue       TruthValue
}

cabhSec2FwFactoryDefaultFilterIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (1..2147483647)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Index used to order the application of filters.
            The filter with the lowest index is always applied
            first."
    ::= { cabhSec2FwFactoryDefaultFilterEntry 1 }

cabhSec2FwFactoryDefaultFilterControl OBJECT-TYPE
    SYNTAX      INTEGER {
                    deny(1),
                    allow(2)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "If set to deny(1), all packets matching this filter
            will be discarded. If set to allow(2), all
            packets matching this filter will be accepted.
            The cabhSec2FwFactoryDefaultFilterContinue object is
            set to true, and therefore the PS MUST continue to
            scan the table for other matches to apply the match
            with the highest cabhSec2FwFactoryDefaultFilterIndex
            value."
    ::= { cabhSec2FwFactoryDefaultFilterEntry 2 }

cabhSec2FwFactoryDefaultFilterIfIndex OBJECT-TYPE
    SYNTAX      InterfaceIndexOrZero
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The index number assigned to this object MUST
            match the IfIndex numbering assigned in the
            ifTable from the Interfaces Group MIB [RFC 2863],
            and as specified in CH 1.1 Spec, Table 6-17 of
            ITU-T Rec. J.192, Numbering Interfaces in the
            ifTable. If the value is zero, the filter applies
            to all interfaces. This object MUST be specified
            to create a row in this table."
    ::= { cabhSec2FwFactoryDefaultFilterEntry 3 }
```

```
cabhSec2FwFactoryDefaultFilterDirection OBJECT-TYPE
    SYNTAX      INTEGER {
                    inbound(1),
                    outbound(2),
                    both(3)
                }
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This value represents direction in relationship
            to the assigned
            cabhSec2FwFactoryDefaultFilterIfIndex
            in this particular rule, meaning that the PS
            MUST represent traffic direction as follows:
            inbound(1)traffic, outbound(2) traffic, or
            both(3)inbound and outbound traffic."
    ::= { cabhSec2FwFactoryDefaultFilterEntry 4 }

cabhSec2FwFactoryDefaultFilterSaddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The source IP address, or portion thereof, that is
            to be matched for this filter. The source address
            is first masked (and'ed) against
            cabhSec2FwFactoryDefaultFilterSmask
            before being compared  to this value. A value of 0
            for this object and 0 for the mask matches all IP
            addresses."
    DEFVAL { '00000000'h }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 5 }

cabhSec2FwFactoryDefaultFilterSmask OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "A bit mask that is to be applied to the source
            address prior to matching. This mask is not
            necessarily the same as a subnet mask, but 1's
            bits must be leftmost and contiguous."
    DEFVAL { '00000000'h }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 6 }

cabhSec2FwFactoryDefaultFilterDaddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The destination IP address, or portion thereof, that
            is to be matched for this filter. The destination
            address is first masked (and'ed) against
            cabhSec2FwFactoryDefaultFilterDmask
            before being compared  to this value. A value of 0
            for this object and 0 for the mask matches all
            IP addresses."
    DEFVAL { '00000000'h }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 7 }
```

```
cabhSec2FwFactoryDefaultFilterDmask OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "A bit mask that is to be applied to the destination
            address prior to matching. This mask is not necessarily
            the same as a subnet mask, but 1's bits must be leftmost
            and contiguous."
    DEFVAL { '00000000'h }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 8 }

cabhSec2FwFactoryDefaultFilterProtocol OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The protocol value that is to be matched. For example:
            icmp is 1, tcp is 6, udp is 17. A value of 65535 matches
            ANY protocol."
    DEFVAL { 65535 }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 9 }

cabhSec2FwFactoryDefaultFilterSourcePortLow OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "If cabhSec2FwFactoryDefaultFilterProtocol is udp
            or tcp, this is the inclusive lower bound of the
            transport-layer source port range that is to be
            matched, otherwise it is ignored during matching."
    DEFVAL { 0 }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 10 }

cabhSec2FwFactoryDefaultFilterSourcePortHigh OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "If cabhSec2FwFactoryDefaultFilterProtocol is
            udp or tcp, this is the inclusive upper bound
            of the transport-layer source port range that
            is to be matched, otherwise it is ignored
            during matching."
    DEFVAL { 65535 }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 11 }

cabhSec2FwFactoryDefaultFilterDestPortLow OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "If cabhSec2FwFactoryDefaultFilterProtocol is
            udp or tcp, this is the inclusive lower bound
            of the transport-layer destination port range
            that is to be matched, otherwise it is ignored
            during matching."
    DEFVAL { 0 }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 12 }
```

```
cabhSec2FwFactoryDefaultFilterDestPortHigh OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "If cabhSec2FwFactoryDefaultFilterProtocol is udp or tcp,
            this is the inclusive upper bound of the transport-layer
            destination port range that is to be matched, otherwise
            it is ignored during matching."
    DEFVAL { 65535 }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 13 }

cabhSec2FwFactoryDefaultFilterContinue OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This value is always set to true so the PS MUST continue
            scanning and applying rules."
    DEFVAL { true }
    ::= { cabhSec2FwFactoryDefaultFilterEntry 14 }

-- ============================================================
--
--  CableHome 1.1 PS Firewall Local Filter Table
--
--  The cabhSec2FwLocalFilterIpTable can be configured to contain
--  a filtering Ruleset for the PS firewall.  It can be used to
--  support subscriber specific or local filtering rules that
--  are separate from general filtering rules that may be
--  be configured in the docsDevFilterIpTable.
-- ============================================================

cabhSec2FwLocalFilterIpTable OBJECT-TYPE
    SYNTAX SEQUENCE OF CabhSec2FwLocalFilterIpEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Contains a configured filtering Ruleset for the PS firewall."
    ::= { cabhSec2FwFilter 3 }

cabhSec2FwLocalFilterIpEntry OBJECT-TYPE
    SYNTAX      CabhSec2FwLocalFilterIpEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Contains a configured filter rule for the PS firewall.

            If the PS has not acquired ToD, entries that do not have
            default time settings are ignored.

            Note that a filter time period may include two days
            (e.g., from 10 PM to 4 AM).  A filter time period that
            includes two days is identified by the absolute value of
            the cabhSec2FwLocalFilterIpEndTime being less than the
            absolute value of the cabhSec2FwLocalFilterIpStartTime.
            The cabhSec2FwLocalFilterIpDOW setting and the
            cabhSec2FwLocalFilterIpStartTime value indicate what day
            and time the filter becomes active.  The
            cabhSec2FwLocalFilterIpEndTime indicates when the filter
            becomes inactive on the second day. The maximum filter time
            period that includes two days is 24 hours.
```

```
            If cabhSec2FwLocalFilterIpStartTime is less than or equal
            to the cabhSec2FwLocalFilterIpEndTime, the time period
            of the filter falls in the same day."

    INDEX { cabhSec2FwLocalFilterIpIndex }
    ::= { cabhSec2FwLocalFilterIpTable 1 }

CabhSec2FwLocalFilterIpEntry ::= SEQUENCE {
    cabhSec2FwLocalFilterIpIndex           Unsigned32,
    cabhSec2FwLocalFilterIpStatus          RowStatus,
    cabhSec2FwLocalFilterIpControl         INTEGER,
    cabhSec2FwLocalFilterIpIfIndex         InterfaceIndexOrZero,
    cabhSec2FwLocalFilterIpDirection       INTEGER,
    cabhSec2FwLocalFilterIpSaddr           InetAddress,
    cabhSec2FwLocalFilterIpSmask           InetAddress,
    cabhSec2FwLocalFilterIpDaddr           InetAddress,
    cabhSec2FwLocalFilterIpDmask           InetAddress,
    cabhSec2FwLocalFilterIpProtocol        Unsigned32,
    cabhSec2FwLocalFilterIpSourcePortLow   Unsigned32,
    cabhSec2FwLocalFilterIpSourcePortHigh  Unsigned32,
    cabhSec2FwLocalFilterIpDestPortLow     Unsigned32,
    cabhSec2FwLocalFilterIpDestPortHigh    Unsigned32,
    cabhSec2FwLocalFilterIpMatches         Counter32,
    cabhSec2FwLocalFilterIpContinue        TruthValue,
    cabhSec2FwLocalFilterIpStartTime       Unsigned32,
    cabhSec2FwLocalFilterIpEndTime         Unsigned32,
    cabhSec2FwLocalFilterIpDOW             BITS,
    cabhSec2FwLocalFilterIpDescr           SnmpAdminString
}

cabhSec2FwLocalFilterIpIndex OBJECT-TYPE
    SYNTAX      Unsigned32 (1..2147483647)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Index used to order the application of filters.
            The filter with the lowest index is always applied
            first."
    ::= { cabhSec2FwLocalFilterIpEntry 1 }

cabhSec2FwLocalFilterIpStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "Controls and reflects the status of rows in this
             table.  Creation of the
             rows may be done via either create-and-wait or
             create-and-go, but the filter is not applied until this
             object is set to (or changes to) active. There is no
             restriction in changing any object in a row while this
             object is set to active."
    ::= { cabhSec2FwLocalFilterIpEntry 2 }

cabhSec2FwLocalFilterIpControl OBJECT-TYPE
    SYNTAX      INTEGER {
                    deny(1),
                    allow(2)
                }
    MAX-ACCESS  read-create
    STATUS      current
```

```
    DESCRIPTION
            "If set to deny(1), all packets matching this filter
            will be discarded. If set to allow(2), all
            packets matching this filter will be accepted.
            The cabhSec2FwLocalFilterIpContinue object is
            set to true, and therefore the PS MUST continue to
            scan the table for other matches to apply the match
            with the highest cabhSec2FwLocalFilterIpIndex
            value."
    ::= { cabhSec2FwLocalFilterIpEntry 3 }

cabhSec2FwLocalFilterIpIfIndex OBJECT-TYPE
    SYNTAX      InterfaceIndexOrZero
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The index number assigned to this object MUST
            match the IfIndex numbering assigned in the
            ifTable from the Interfaces Group MIB [RFC 2863],
            and as specified in CH 1.1 Spec, Table 6-17 of
            ITU-T Rec. J.192, Numbering Interfaces in the ifTable."
    DEFVAL { 255 }
    ::= { cabhSec2FwLocalFilterIpEntry 4 }

cabhSec2FwLocalFilterIpDirection OBJECT-TYPE
    SYNTAX      INTEGER {
                    inbound(1),
                    outbound(2),
                    both(3)
                }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "This value represents direction in relationship
            to the assigned cabhSec2FwLocalFilterIpIfIndex
            in this particular rule, meaning that the PS
            MUST represent traffic direction as follows:
            inbound(1)traffic, outbound(2) traffic, or
            both(3)inbound and outbound traffic."
    ::= { cabhSec2FwLocalFilterIpEntry 5 }

cabhSec2FwLocalFilterIpSaddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The source IP address, or portion thereof, that is to be matched
            for this filter. The source address is first masked (and'ed)
            against cabhSec2FwLocalFilterIpSmask before being compared
            to this value. A value of 0 for this object and 0 for the mask
            matches all IP addresses."
    DEFVAL { '00000000'h }
    ::= { cabhSec2FwLocalFilterIpEntry 6 }

cabhSec2FwLocalFilterIpSmask OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "A bit mask that is to be applied to the source address prior
            to matching. This mask is not necessarily the same as a subnet
            mask,but 1's bits must be leftmost and contiguous."
    DEFVAL { '00000000'h }
    ::= { cabhSec2FwLocalFilterIpEntry 7 }
```

```
cabhSec2FwLocalFilterIpDaddr OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The destination IP address, or portion thereof, that
            is to be matched for this filter. The destination
            address is first masked (and'ed) against
            cabhSec2FwLocalFilterIpDmask
            before being compared  to this value. A value of 0
            for this object and 0 for the mask matches all
            IP addresses."
    DEFVAL { '00000000'h }
    ::= { cabhSec2FwLocalFilterIpEntry 8 }

cabhSec2FwLocalFilterIpDmask OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "A bit mask that is to be applied to the destination
            address prior to matching. This mask is not necessarily
            the same as a subnet mask, but 1's bits must be leftmost
            and contiguous."
    DEFVAL { '00000000'h }
    ::= { cabhSec2FwLocalFilterIpEntry 9 }

cabhSec2FwLocalFilterIpProtocol OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The protocol value that is to be matched. For example:
            icmp is 1, tcp is 6, udp is 17. A value of 65535 matches
            ANY protocol."
    DEFVAL { 65535 }
    ::= { cabhSec2FwLocalFilterIpEntry 10 }

cabhSec2FwLocalFilterIpSourcePortLow OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "If cabhSec2FwLocalFilterIpProtocol is udp
            or tcp, this is the inclusive lower bound of the
            transport-layer source port range that is to be
            matched, otherwise it is ignored during matching."
    DEFVAL { 0 }
    ::= { cabhSec2FwLocalFilterIpEntry 11 }

cabhSec2FwLocalFilterIpSourcePortHigh OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "If cabhSec2FwLocalFilterIpProtocol is
            udp or tcp, this is the inclusive upper bound
            of the transport-layer source port range that
            is to be matched, otherwise it is ignored
            during matching."
    DEFVAL { 65535 }
    ::= { cabhSec2FwLocalFilterIpEntry 12 }
```

```
cabhSec2FwLocalFilterIpDestPortLow OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "If cabhSec2FwLocalFilterIpProtocol is
            udp or tcp, this is the inclusive lower bound
            of the transport-layer destination port range
            that is to be matched, otherwise it is ignored
            during matching."
    DEFVAL { 0 }
    ::= { cabhSec2FwLocalFilterIpEntry 13 }

cabhSec2FwLocalFilterIpDestPortHigh OBJECT-TYPE
    SYNTAX      Unsigned32 (0..65535)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "If cabhSec2FwLocalFilterIpProtocol is
            udp or tcp, this is the inclusive upper bound
            of the transport-layer destination port range
            that is to be matched, otherwise it is ignored
            during matching."
    DEFVAL { 65535 }
    ::= { cabhSec2FwLocalFilterIpEntry 14 }

cabhSec2FwLocalFilterIpMatches OBJECT-TYPE
    SYNTAX      Counter32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Counts the number of times this filter was matched.
             This object is initialized to 0 at boot, or at row
             creation, and is reset only upon reboot."
    ::= { cabhSec2FwLocalFilterIpEntry 15 }

cabhSec2FwLocalFilterIpContinue OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "This value is always set to true so the PS MUST continue
            scanning and applying rules."
    DEFVAL { true }
    ::= { cabhSec2FwLocalFilterIpEntry 16 }

cabhSec2FwLocalFilterIpStartTime OBJECT-TYPE
    SYNTAX      Unsigned32 (0..2359)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The start time for matching the filter ruleset in the
            specified days indicated in cabhSec2FwLocalFilterIpDOW.
            Time is represented in Military Time, e.g., 8:30 AM is
            represented as 830 and 11:45 PM as 2345. An attempt to set
            this object to an invalid military time value, e.g., 1182,
            returns 'wrongValue' error."
    DEFVAL { 0 }
    ::= { cabhSec2FwLocalFilterIpEntry 17 }

cabhSec2FwLocalFilterIpEndTime OBJECT-TYPE
    SYNTAX      Unsigned32 (0..2359)
    MAX-ACCESS  read-create
    STATUS      current
```

```
    DESCRIPTION
            "The end time for matching the filter ruleset for the
            days indicated in cabhSec2FwLocalFilterIpDOW.  The filter
            rule associated with this end time MUST not be disabled
            until the minute following the time indicated by this
            MIB object.  If the time period is for two days, identified
            by cabhSec2FwLocalFilterIpEndTime being less than
            cabhSec2FwLocalFilterIpStartTime, then the
            cabhSec2FwLocalFilterIpDOW settings do not apply to this
            MIB object. Time is represented in the same manner as in
            cabhSec2FwLocalFilterIpStartTime. An attempt to set
            this object to an invalid military time value, e.g., 1182,
            returns 'wrongValue' error."
    DEFVAL { 2359 }
    ::= { cabhSec2FwLocalFilterIpEntry 18 }

cabhSec2FwLocalFilterIpDOW OBJECT-TYPE
    SYNTAX BITS {
                    sunday(0),
                    monday(1),
                    tuesday(2),
                    wednesday(3),
                    thursday(4),
                    friday(5),
                    saturday(6)
                }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "If the day of week bit associated with the PS given day
            is '1', this object criteria matches."
    DEFVAL { 'fe'h }  -- 11111110 Sun-Sat
    ::= { cabhSec2FwLocalFilterIpEntry 19 }

cabhSec2FwLocalFilterIpDescr OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE(0..32))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "A filter rule description configured by the
            cable operator or subscriber."
    DEFVAL { "" }
    ::= { cabhSec2FwLocalFilterIpEntry 20 }

--
-- Kerberos MIBs
--

cabhSecKerbPKINITGracePeriod OBJECT-TYPE
    SYNTAX      Unsigned32 (15..600)
    UNITS       "minutes"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The PKINIT Grace Period is needed by the PS
            to know when it should start retrying to get
            a new ticket. The PS MUST obtain a new Kerberos
            ticket (with a PKINIT exchange),this, many minutes
            before the old ticket expires."
    DEFVAL { 30 }
    ::= { cabhSecKerbBase 1}
```

```
cabhSecKerbTGSGracePeriod OBJECT-TYPE
    SYNTAX      Unsigned32 (1..600)
    UNITS       "minutes"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The TGS Grace Period is needed by the PS to
            know when it should start retrying to get a new
            ticket. The PS MUST obtain a new Kerberos ticket
            (with a TGS Request), this, many minutes before the
            old ticket expires."
    DEFVAL { 10 }
    ::= { cabhSecKerbBase 2 }

cabhSecKerbUnsolicitedKeyMaxTimeout OBJECT-TYPE
    SYNTAX      Unsigned32 (15..600)
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "This timeout applies to PS initiated AP-REQ/REP
            key management exchange with NMS. The maximum
            timeout is the value which may not be exceeded in
            the exponential backoff algorithm."
    DEFVAL { 600 }
    ::= { cabhSecKerbBase 3 }

cabhSecKerbUnsolicitedKeyMaxRetries OBJECT-TYPE
    SYNTAX      Unsigned32 (1..32)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The number of retries the PS is allowed for
            AP-REQ/REP key management exchange initiation
            with the NMS. This is the maximum number of
            retries before the PS gives up attempting to
            establish an SNMPv3 security association
            with NMS."
    DEFVAL { 8 }
    ::= { cabhSecKerbBase 4 }

cabhSecNotification OBJECT IDENTIFIER ::= { cabhSecMib 3 }
cabhSecConformance  OBJECT IDENTIFIER ::= { cabhSecMib 4 }
cabhSecCompliances  OBJECT IDENTIFIER ::= { cabhSecConformance 1 }
cabhSecGroups       OBJECT IDENTIFIER ::= { cabhSecConformance 2 }

--
--    Notification Group for future extension
--

-- compliance statements

cabhSecCompliance MODULE-COMPLIANCE
    STATUS      deprecated
    DESCRIPTION
            "The compliance statement for CableHome Security."
    MODULE   --cabhSecMib

-- unconditionally mandatory groups

    MANDATORY-GROUPS {
        cabhSecCertGroup,
        cabhSecKerbGroup
        }
```

```
-- conditional mandatory groups

    GROUP cabhSecGroup
    DESCRIPTION
            "This group is implemented only for CH 1.0 gateways."
    ::= { cabhSecCompliances 1 }

    cabhSec2Compliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
            "The compliance statement for CableHome 1.1 Security."
    MODULE   --cabhSecMib

-- unconditionally mandatory groups

    MANDATORY-GROUPS {
        cabhSecCertGroup,
        cabhSecKerbGroup,
        cabhSec2Group
        }
    ::= { cabhSecCompliances 2 }

cabhSecGroup OBJECT-GROUP
    OBJECTS {
        cabhSecFwPolicyFileEnable,
        cabhSecFwPolicyFileURL,
        cabhSecFwPolicyFileHash,
        cabhSecFwPolicyFileOperStatus,
        cabhSecFwPolicyFileCurrentVersion,
        cabhSecFwPolicySuccessfulFileURL,
        cabhSecFwEventType1Enable,
        cabhSecFwEventType2Enable,
        cabhSecFwEventType3Enable,
        cabhSecFwEventAttackAlertThreshold,
        cabhSecFwEventAttackAlertPeriod
        }
    STATUS      deprecated
    DESCRIPTION
            "Group of objects in CableHome 1.0 Firewall MIB."
    ::= { cabhSecGroups 1 }

cabhSecCertGroup OBJECT-GROUP
    OBJECTS {
        cabhSecCertPsCert
        }
    STATUS      current
    DESCRIPTION
            "Group of objects in CableHome gateway for PS
            Certificate."
    ::= { cabhSecGroups 2 }

cabhSecKerbGroup OBJECT-GROUP
    OBJECTS {
        cabhSecKerbPKINITGracePeriod,
        cabhSecKerbTGSGracePeriod,
        cabhSecKerbUnsolicitedKeyMaxTimeout,
        cabhSecKerbUnsolicitedKeyMaxRetries
        }
    STATUS      current
    DESCRIPTION
            "Group of objects in CableHome gateway for Kerberos."
    ::= { cabhSecGroups 3 }
```

```
cabhSec2Group OBJECT-GROUP
    OBJECTS {
        cabhSec2FwEnable,
        cabhSec2FwPolicyFileURL,
        cabhSec2FwPolicyFileHash,
        cabhSec2FwPolicyFileOperStatus,
        cabhSec2FwPolicyFileCurrentVersion,
        cabhSec2FwClearPreviousRuleset,
        cabhSec2FwPolicySelection,
        cabhSec2FwEventSetToFactory,
        cabhSec2FwEventLastSetToFactory,
        cabhSec2FwPolicySuccessfulFileURL,
        cabhSec2FwEventEnable,
        cabhSec2FwEventThreshold,
        cabhSec2FwEventInterval,
        cabhSec2FwEventCount,
        cabhSec2FwEventLogReset,
        cabhSec2FwEventLogLastReset,
        cabhSec2FwLogEventType,
        cabhSec2FwLogEventPriority,
        cabhSec2FwLogEventId,
        cabhSec2FwLogTime,
        cabhSec2FwLogIpProtocol,
        cabhSec2FwLogIpSourceAddr,
        cabhSec2FwLogIpDestAddr,
        cabhSec2FwLogIpSourcePort,
        cabhSec2FwLogIpDestPort,
        cabhSec2FwLogMessageType,
        cabhSec2FwLogReplayCount,
        cabhSec2FwLogMIBPointer,
        cabhSec2FwFilterScheduleStartTime,
        cabhSec2FwFilterScheduleEndTime,
        cabhSec2FwFilterScheduleDOW,
        cabhSec2FwFactoryDefaultFilterControl,
        cabhSec2FwFactoryDefaultFilterIfIndex,
        cabhSec2FwFactoryDefaultFilterDirection,
        cabhSec2FwFactoryDefaultFilterSaddr,
        cabhSec2FwFactoryDefaultFilterSmask,
        cabhSec2FwFactoryDefaultFilterDaddr,
        cabhSec2FwFactoryDefaultFilterDmask,
        cabhSec2FwFactoryDefaultFilterProtocol,
        cabhSec2FwFactoryDefaultFilterSourcePortLow,
        cabhSec2FwFactoryDefaultFilterSourcePortHigh,
        cabhSec2FwFactoryDefaultFilterDestPortLow,
        cabhSec2FwFactoryDefaultFilterDestPortHigh,
        cabhSec2FwFactoryDefaultFilterContinue
        }
    STATUS      current
    DESCRIPTION
            "Group of objects in CableHome 1.1 Firewall MIB."
    ::= { cabhSecGroups 4 }

END
```

E.6 Requisitos de la MIB Definición

La MIB definición CableLabs DEBE implementarse tal como se define a continuación.

```
CLAB-DEF-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    enterprises
                    FROM SNMPv2-SMI
    DocsX509ASN1DEREncodedCertificate
                    FROM DOCS-IETF-BPI2-MIB;

cableLabs MODULE-IDENTITY
    LAST-UPDATED "200504081700Z" -- April 8, 2005
    ORGANIZATION "Cable Television Laboratories, Inc."
    CONTACT-INFO
           "Editor: Jean-Francois Mule
            Postal: Cable Television Laboratories, Inc.
                    858 Coal Creek Circle
                    Louisville, Colorado 80027-9750
                    U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: jfm@cablelabs.com
                    mibs@cablelabs.com"
    DESCRIPTION
            "This MIB module defines the namespace organization for the
            CableLabs enterprise OID registry.

            Copyright 1999-2005 Cable Television Laboratories, Inc.
            All rights reserved."

    REVISION "200504081700Z" -- April 8, 2005
    DESCRIPTION
            "This revision, published as CL-SP-MIB-CLABDEF-I05."
    ::= { enterprises 4491 }

-- Sub-tree for Registrations
clabFunction            OBJECT IDENTIFIER ::= { cableLabs 1 }
clabFuncMib2            OBJECT IDENTIFIER ::= { clabFunction 1 }
clabFuncProprietary     OBJECT IDENTIFIER ::= { clabFunction 2 }

-- Sub-tree for Project Definitions
clabProject             OBJECT IDENTIFIER ::= { cableLabs 2 }
clabProjDocsis          OBJECT IDENTIFIER ::= { clabProject 1 }
clabProjPacketCable     OBJECT IDENTIFIER ::= { clabProject 2 }
clabProjOpenCable       OBJECT IDENTIFIER ::= { clabProject 3 }
clabProjCableHome       OBJECT IDENTIFIER ::= { clabProject 4 }

-- Sub-tree for Global Security Definitions
clabSecurity            OBJECT IDENTIFIER ::= { cableLabs 3 }
clabSecCertObject       OBJECT IDENTIFIER ::= { clabSecurity 1 }

-- Sub tree for CableLabs cross project common MIB definitions
clabCommonMibs          OBJECT IDENTIFIER ::= { cableLabs 4 }

--
-- CableLabs DOCSIS Project Sub-tree Definitions
--
```

```
dsgMIB OBJECT IDENTIFIER
    -- DOCSIS Set-top Gateway (DSG) MIB module
    -- This object identifier points to the MIB module
    -- DOCSIS-SETTOP-GATEWAY-MIB, which is being deprecated by
    -- DSG-IF-MIB MIB module (dsgIfMib).
    -- Reference:
    -- CableLabs DOCSIS Set-top Gateway (DSG) Interface Specification
    ::= { clabProjDocsis 1 }

docsLoadBalMib OBJECT IDENTIFIER
    -- DOCSIS MIB module defining the CMTS configuration parameters to
    -- support Load Balancing requirements."
    ::= { clabProjDocsis 2 }

dsgIfMIB OBJECT IDENTIFIER
    -- DOCSIS Set-top Gateway (DSG) MIB module
    -- Obsoletes DOCSIS-SETTOP-GATEWAY-MIB Module (dsgMib)
    -- defined initially in DOCSIS Set-top Gateway (DSG) Interface
    -- Specification SP-DSG-I01-020228.
    -- Reference:
    -- CableLabs DOCSIS Set-top Gateway (DSG) Interface Specification
    ::= { clabProjDocsis 3 }

dsgIfStdMib OBJECT IDENTIFIER
    -- DOCSIS Set-top Device (DSG) MIB module.
    -- Reference:
    -- CableLabs DOCSIS Set-top Gateway (DSG) Interface Specification
    ::= { clabProjDocsis 4 }

docsIfExt2Mib OBJECT IDENTIFIER
    -- This MIB module contains the management objects that enhance
    -- DOCSIS RFI Interface Extensions. Contains Enhancements to
    -- DOCSIS RFI interface MIB module.
    -- Reference:
    -- CableLabs DOCSIS RFI Interface Specification.
    ::= { clabProjDocsis 5 }

docsTestMIB OBJECT IDENTIFIER
    -- DOCSIS Test MIB module supporting programmable test features
    -- for DOCSIS 2.0 compliant Cable Modems (CM) and Cable Modems
    -- Termination Systems (CMTS).
    -- Reference:
    -- CableLabs DOCSIS 2.0 Testing MIB Specification
    ::= { clabProjDocsis 12 }

sledMib OBJECT IDENTIFIER
    -- eDOCSIS MIB module supporting the Software Loopback Application
    -- for eDOCSIS (SLED).
    -- Reference:
    -- CableLabs eDOCSIS Specification
    ::= { clabProjDocsis 13 }

--
-- CableLabs CableHome Project Sub-tree Definitions
-- Reference
-- CableLabs CableHome Specification
--
cabhPsDevMib OBJECT IDENTIFIER
    -- CableHome MIB module defining the basic management objects for
    -- the Portal Services logical element of a CableHome compliant
    -- Residential Gateway device. The PS device parameters describe
    -- general PS Device attributes and behaviour characteristics
    ::= { clabProjCableHome 1 }
```

```
cabhSecMib OBJECT IDENTIFIER
    -- CableHome MIB module defining the basic management objects for
    -- the firewall and other security features of the Portal Services
    -- element.
    ::= { clabProjCableHome 2 }

cabhCapMib OBJECT IDENTIFIER
    -- CableHome MIB module defining the basic management objects for
    -- the CableHome Address Portal (CAP) function of the Portal
    -- Services element.
    ::= { clabProjCableHome 3 }

cabhCdpMib OBJECT IDENTIFIER
    -- This MIB module supplies the basic management objects for the
    -- CableHome DHCP Portal (CDP) function of the Portal Services
    -- element.
    ::= { clabProjCableHome 4 }

cabhCtpMib OBJECT IDENTIFIER
    -- CableHome MIB module supporting the remote LAN diagnostic
    -- features provided by the CableHome Test Portal (CTP) function
    -- of the Portal Services element.
    ::= { clabProjCableHome 5 }

cabhQosMib OBJECT IDENTIFIER
    -- CABLEHOME QOS MIB Module (cabhQosMib).
    -- This object identifier points to the MIB module
    -- CABH-QOS-MIB, which is being deprecated by
    -- CABH-QOS2-MIB module (cabhQos2Mib).
    -- Reference:
    -- CableLabs CableHome 1.1 Specification
    ::= { clabProjCableHome 6 }

cabhCsaMib OBJECT IDENTIFIER
    -- CableHome MIB module defining management objects for the
    -- configuration and monitoring of CableHome Commercial Services
    -- Annex.
    -- Reference:
    -- CableLabs CableOffice Commercial Services Annex MIB
    -- Specification
    ::= { clabProjCableHome 7 }

cabhQos2Mib OBJECT IDENTIFIER
    -- Obsoletes CABH-QOS-MIB module (cabhQosMib)
    -- defined initially in CABLEHOME 1.1 Interface Specification.
    -- This MIB module defines the Quality of Service Management
    -- Information Base (MIUB) for CableHome UPnP QOS-compliant
    -- devices.
    -- Reference:
    -- CableLabs CableHome 1.1 Specification
    ::= { clabProjCableHome 8 }

--
-- CableLabs PacketCable Project Sub-tree Definitions
--
pktcMtaMib OBJECT IDENTIFIER
    -- PacketCable MIB module defining the basic management object for
    -- the Multimedia Terminal Adapter (MTA) devices compliant with
    -- PacketCable requirements.
    -- Reference
    -- CableLabs PacketCable MTA Device Provisioning Specification
    ::= { clabProjPacketCable 1 }
```

```
pktcSigMib OBJECT IDENTIFIER
    -- PacketCable MIB module defining the basic management object for
    -- the PacketCable MTA Signalling protocols. This version of the MIB
    -- includes common signalling and Network Call Signalling (NCS)
    -- related signalling objects.
    -- Reference
    -- CableLabs PacketCable MTA Device Provisioning Specification
    ::= { clabProjPacketCable 2 }

pktcEventMib OBJECT IDENTIFIER
    -- PacketCable MIB module defining the basic management objects for
    -- event reporting.
    -- Reference
    -- CableLabs PacketCable Management Event Specification
    ::= { clabProjPacketCable 3 }

pktcSecurity OBJECT IDENTIFIER
    -- CableLabs OID reserved for security and used to specify errors
    -- that can be returned for the Kerberos KDC - Provisioning
    -- Server interface, or the MTA-CMS Kerberized IPSec interface, or
    -- the MTA-Provisioning Server Kerberized SNMPv3 interface.
    -- CableLabs PacketCable Security Specification
    ::= { clabProjPacketCable 4 }

pktcLawfulIntercept OBJECT IDENTIFIER
    -- CableLabs OID reserved for the PacketCable Electronic
    -- Surveillance Protocol (PCESP) between the Delivery Function
    -- and Collection Function. This OID is used to define the ASN.1
    -- PCESP messages.
    -- CableLabs PacketCable Electronic Surveillance Protocol
    -- Specification
    ::= { clabProjPacketCable 5 }

--
-- Sub-tree for PacketCable MIB Enhancements
--

pktcEnhancements OBJECT IDENTIFIER ::= { clabProjPacketCable 6 }


-- The following MIB OBJECTS are being introduced for
-- incorporation of new MIB objects (MIB enhancements)
-- proposed to the PacketCable MIB group.
-- This includes new MIB objects being introduced
-- as part of the PacketCable MIB Enhancement efforts
-- and as a place holder for future revisions.
-- This sub-division would facilitate easier incorporation
-- of proposed IETF Drafts/RFCs by keeping enhancements
-- independent of RFC/Draft changes.
-- For new MIB tables that use previously used indices, it is
-- recommended that the AUGMENT CLAUSE be used to aid SNMP Operations,
-- as deemed necessary.


pktcEnMtaMib OBJECT IDENTIFIER
    -- PacketCable MIB module enhancements to the basic management
    -- objects defined by the MIB group pktcMtaMib for the Multimedia
    -- Terminal Adapter (MTA) devices compliant with PacketCable
    -- requirements.
    -- Reference:
    -- CableLabs PacketCable MTA Device Provisioning Specification.
    ::= { pktcEnhancements 1 }
```

```
pktcEnSigMib OBJECT IDENTIFIER
    -- PacketCable MIB module enhancements to the basic management
    -- objects defined by the MIB group pktcSigMib for the
    -- PacketCable MTA Signalling protocols.
    -- Reference:
    -- CableLabs PacketCable MTA Device Provisioning Specification.
    ::= { pktcEnhancements 2 }

pktcEnEventMib OBJECT IDENTIFIER
    -- PacketCable MIB module enhancements to the basic management
    -- objects defined by the MIB group pktcEventMib for event reporting.
    -- Reference:
    -- CableLabs PacketCable Management Event Specification.
    ::= { pktcEnhancements 3 }

pktcEnSecurityMib OBJECT IDENTIFIER
    -- PacketCable MIB module enhancements to the basic management
    -- objects defined by the reserved MIB group pktcSecurity.
    -- Reference:
    -- CableLabs PacketCable Security Specification.
    ::= { pktcEnhancements 4 }

--
--
-- Definition of CableLabs Security Certificate Objects
--
clabSrvcPrvdrRootCACert OBJECT-TYPE
    SYNTAX      DocsX509ASN1DEREncodedCertificate
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The X509 DER-encoded CableLabs Service Provider Root CA
            Certificate."
    REFERENCE
            "CableLabs CableHome Specification;
            CableLabs PacketCable Security Specification."
    ::= { clabSecCertObject 1 }

clabCVCRootCACert OBJECT-TYPE
    SYNTAX      DocsX509ASN1DEREncodedCertificate
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The X509 DER-encoded CableLabs CVC Root CA Certificate."
    REFERENCE
            "CableLabs CableHome Specification;
            CableLabs PacketCable Security Specification."
    ::= { clabSecCertObject 2 }

clabCVCCACert OBJECT-TYPE
    SYNTAX      DocsX509ASN1DEREncodedCertificate
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The X509 DER-encoded CableLabs CVC CA Certificate."
    REFERENCE
            "CableLabs CableHome Specification;
            CableLabs PacketCable Security Specification."
    ::= { clabSecCertObject 3 }
```

```
clabMfgCVCCert OBJECT-TYPE
    SYNTAX      DocsX509ASN1DEREncodedCertificate
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The X509 DER-encoded Manufacturer CVC Certificate."
    REFERENCE
            "CableLabs CableHome Specification;
            CableLabs PacketCable Security Specification."
    ::= { clabSecCertObject 4 }

clabMfgCACert OBJECT-TYPE
    SYNTAX      DocsX509ASN1DEREncodedCertificate
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The X509 DER-encoded Manufacturer CA Certificate."
    REFERENCE
            "CableLabs CableHome Specification;
            CableLabs PacketCable Security Specification."
    ::= { clabSecCertObject 5 }

--
-- CableLabs cross project common MIB sub-tree definitions
--

clabUpsMib OBJECT IDENTIFIER
    -- CableLabs cross project MIB module defining the basic management
    -- objects for the configuration and monitoring of the battery
    -- backup and UPS functionality for CableLabs compliant devices.
    ::= { clabCommonMibs 1 }

END
```

E.7 Requisitos de la MIB portal con QoS IPCable2Home (CQP, IPCable2Home QoS Portal)

La MIB CQP IPCable2Home DEBE implementarse tal como se define a continuación.

```
CABH-QOS2-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    Unsigned32,
    Gauge32                 FROM SNMPv2-SMI

    TruthValue,
    TimeStamp,
    RowStatus               FROM SNMPv2-TC

    SnmpAdminString         FROM SNMP-FRAMEWORK-MIB

    OBJECT-GROUP,
    MODULE-COMPLIANCE       FROM SNMPv2-CONF

    InetPortNumber,
    InetAddressType,
    InetAddress             FROM INET-ADDRESS-MIB

    ifIndex                 FROM IF-MIB

    clabProjCableHome       FROM CLAB-DEF-MIB;
```

```
cabhQos2Mib MODULE-IDENTITY
    LAST-UPDATED    "200504080000Z" -- April 8, 2005
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
            858 Coal Creek Circle
            Louisville, Colorado 80027
            U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com; mibs@cablelabs.com"
    DESCRIPTION
            "This MIB module supplies parameters for the
            configuration and monitoring of CableHome
            QoS capabilities."
    ::= { clabProjCableHome 8 }

   -- Textual conventions

-- Notifications
cabhQos2Mib2Notifications   OBJECT IDENTIFIER ::= { cabhQos2Mib 0 }

-- Objects definitions

cabhQos2MibObjects          OBJECT IDENTIFIER ::= { cabhQos2Mib 1 }
cabhQos2Base                OBJECT IDENTIFIER ::= {
                                                    cabhQos2MibObjects 1 }
cabhQos2PsIfAttributes      OBJECT IDENTIFIER ::= {
                                                    cabhQos2MibObjects 2 }
cabhQos2PolicyHolderObjects OBJECT IDENTIFIER ::= {
                                                    cabhQos2MibObjects 3 }
cabhQos2DeviceObjects       OBJECT IDENTIFIER ::= {
                                                    cabhQos2MibObjects 4 }

   --================================================================
   --
   -- PS QoS basic control and configuration
   --
   --
   --================================================================

cabhQos2SetToFactory OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "When this object is set to true(1), the PS MUST clear
            all the entries in cabhQos2PolicyTable and
            cabhQos2TrafficClassTable. Reading this object always
            returns false(2)."
    ::= { cabhQos2Base 1 }

cabhQos2LastSetToFactory OBJECT-TYPE
    SYNTAX      TimeStamp
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The value of sysUpTime when cabhQos2SetToFactory
            was last set to true. Zero if never reset."
    ::= { cabhQos2Base 2 }
```

```
   --================================================================
   --
   --  PS Interface Attributes Table
   --
   --  The cabhQos2PsIfAttribTable replaces the deprecated
   --  cabhPriorityQosPsIfAttribTable and contains the number of
   --  media access priorities and number of queues associated with
   --  each PS interface.
   --
   --================================================================

cabhQos2PsIfAttribTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhQos2PsIfAttribEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains interface attributes. It includes
            the number of media access priorities and number of
            queues associated with each PS interface in the
            Residential Gateway."
    ::= { cabhQos2PsIfAttributes 1 }

cabhQos2PsIfAttribEntry OBJECT-TYPE
    SYNTAX      CabhQos2PsIfAttribEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Number of media access priorities and number
            of queues for each PS interface in the Residential
            Gateway. PS does not need to provide support for entries
            associated with Aggregated LAN interfaces (ifIndex 255 and
            254). The PS WAN interfaces are assigned as ifIndex 1 for
            Wan Management and ifIndex 2 for Wan Data; both interfaces
            are indicated in this table as 'WAN interface' with
            ifIndex 1 as the entry identifier."
    INDEX { ifIndex }
    ::= { cabhQos2PsIfAttribTable 1 }

CabhQos2PsIfAttribEntry::= SEQUENCE {
    cabhQos2PsIfAttribNumPriorities   Unsigned32,
    cabhQos2PsIfAttribNumQueues       Unsigned32
    }

cabhQos2PsIfAttribNumPriorities OBJECT-TYPE
    SYNTAX      Unsigned32 (1..8)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of media access priorities supported
            by this interface."
    ::= { cabhQos2PsIfAttribEntry 1 }

cabhQos2PsIfAttribNumQueues OBJECT-TYPE
    SYNTAX      Unsigned32 (1..8)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "The number of queues associated with this interface."
    ::= { cabhQos2PsIfAttribEntry 2 }
```

```
   --================================================================
   --
   --  PS UPnP Policy Holder Information
   --
   --  Provides the UPnP Qos admission control and Upnp Policy Holder
   -- control and information to be used by the policy manager.
   --
   --================================================================

cabhQos2PolicyHolderEnabled OBJECT-TYPE
    SYNTAX      TruthValue
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The value true indicates that the Policy Holder entity is
            active and advertised in PS UPnP standard discovery
            mechanisms; false indicates it is disabled."
    DEFVAL { true }
    ::= { cabhQos2PolicyHolderObjects 1 }

cabhQos2PolicyAdmissionControl OBJECT-TYPE
    SYNTAX      INTEGER {
                enabled(1),
                disabled(2)
                }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Indicates if the QoS Policy Admission Control
            is enabled or disabled for all the traffic requests."
    DEFVAL { disabled }
    ::= { cabhQos2PolicyHolderObjects 2 }

cabhQos2NumActivePolicyHolder OBJECT-TYPE
    SYNTAX      Gauge32 (0..4294967295)
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
            "Indicates the number of active policy holders the PS
            have discovered in the LAN. This object includes the PS
            Policy Holder if active."
    ::= { cabhQos2PolicyHolderObjects 3 }

cabhQos2PolicyTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhQos2PolicyEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains the operator and user created
            policies for the management of QoS for applications.
            PS creates non-persistent entries (of type 'upnp') for
            the QoS-aware applications and services discovered
            through UPnP actions in the user part of this table which
            could be converted to persistent entries by user (of type
            'user' or by cable operator of type
            'operatorForHomeUserOnly)."
    ::= { cabhQos2PolicyHolderObjects 4 }

cabhQos2PolicyEntry OBJECT-TYPE
    SYNTAX      CabhQos2PolicyEntry
    MAX-ACCESS  not-accessible
    STATUS      current
```

```
    DESCRIPTION
            "The indices for these entries."
    INDEX { cabhQos2PolicyOwner, cabhQos2PolicyOwnerRuleId }
    ::= { cabhQos2PolicyTable 1 }

CabhQos2PolicyEntry ::= SEQUENCE {
    cabhQos2PolicyOwner             INTEGER,
    cabhQos2PolicyOwnerRuleId       Unsigned32,
    cabhQos2PolicyRuleOrder         Unsigned32,
    cabhQos2PolicyAppDomain         SnmpAdminString,
    cabhQos2PolicyAppName           SnmpAdminString,
    cabhQos2PolicyServiceProvDomain SnmpAdminString,
    cabhQos2PolicyServiceName       SnmpAdminString,
    cabhQos2PolicyPortDomain        SnmpAdminString,
    cabhQos2PolicyPortNumber        InetPortNumber,
    cabhQos2PolicyIpType            InetAddressType,
    cabhQos2PolicyIpProtocol        Unsigned32,
    cabhQos2PolicySrcIp             InetAddress,
    cabhQos2PolicyDestIp            InetAddress,
    cabhQos2PolicySrcPort           InetPortNumber,
    cabhQos2PolicyDestPort          InetPortNumber,
    cabhQos2PolicyTraffImpNum       Unsigned32,
    cabhQos2PolicyUserImportance    Unsigned32,
    cabhQos2PolicyRowStatus         RowStatus
    }

cabhQos2PolicyOwner OBJECT-TYPE
    SYNTAX      INTEGER {
                operatorOnly(1),
                homeUser(2),
                operatorForHomeUser(3),
                upnp(4)
                }
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This Index defines the policy creation owner. The entries
            of type 'upnp' are dynamically created by the PS for
            the applications, services and devices that it discovers
            on the LAN with UPnP QoS actions."
    ::= { cabhQos2PolicyEntry 1 }

cabhQos2PolicyOwnerRuleId OBJECT-TYPE
    SYNTAX      Unsigned32 (1..4294967295)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Index for the set of rules related to an
            owner index."
    ::= { cabhQos2PolicyEntry 2 }

cabhQos2PolicyRuleOrder OBJECT-TYPE
    SYNTAX      Unsigned32 (0..4294967295)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The order in which the policy rules are processed within
             An owner."
    DEFVAL { 0 }
    ::= { cabhQos2PolicyEntry 3 }
```

```
cabhQos2PolicyAppDomain OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "Vendor domain name from the Vendor application name URN."
    DEFVAL { "" }
    ::= { cabhQos2PolicyEntry 4 }

cabhQos2PolicyAppName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "Text description of the application."
    DEFVAL { "" }
    ::= { cabhQos2PolicyEntry 5 }

cabhQos2PolicyServiceProvDomain OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The service Provider Service Domain Name from the
            service Provider URN."
    DEFVAL { "" }
    ::= { cabhQos2PolicyEntry 6 }

cabhQos2PolicyServiceName OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "Text description of the Service."
    DEFVAL { "" }
    ::= { cabhQos2PolicyEntry 7 }

cabhQos2PolicyPortDomain OBJECT-TYPE
    SYNTAX      SnmpAdminString (SIZE (0..32))
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "Domain name from the Port URN."
    DEFVAL { "" }
    ::= { cabhQos2PolicyEntry 8 }

cabhQos2PolicyPortNumber OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "Well known IP transport port of the application."
    DEFVAL { 0 }
    ::= { cabhQos2PolicyEntry 9 }

cabhQos2PolicyIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The type of InetAddress for cabhQos2PolicySrcIp,
            and cabhQos2PolicyDestIp."
    DEFVAL { ipv4 }
    ::= { cabhQos2PolicyEntry 10 }
```

```
cabhQos2PolicyIpProtocol OBJECT-TYPE
    SYNTAX         Unsigned32 (0..255)
    MAX-ACCESS     read-create
    STATUS         current
    DESCRIPTION
            "The IANA-defined IP protocol number representing
            the IP protocol to match against the IPv4 protocol
            number or the IPv6 Next-Header number in the packet.
            '0' means no protocol is specified as matching criteria
            for policy determination, i.e., QoS policy is
            irrespective of IP protocol."
    REFERENCE
            "http://www.iana.org/assignments/protocol-numbers"
    DEFVAL { 0 }
    ::= { cabhQos2PolicyEntry 11 }

cabhQos2PolicySrcIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The IP address to match against the packet's source IP
            address. This may not be a DNS name, but may be an IPv4 or
            IPv6 prefix."
    DEFVAL { '00000000'h }
    ::= { cabhQos2PolicyEntry 12 }

cabhQos2PolicyDestIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The IP address to match against the packet's source IP
            address. This may not be a DNS name, but may be an IPv4 or
            IPv6 prefix."
    DEFVAL { '00000000'h }
    ::= { cabhQos2PolicyEntry 13 }

cabhQos2PolicySrcPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The value that the layer-4 source port number in the
            packet must have in order to match this policy entry."
    DEFVAL { 0 }
    ::= { cabhQos2PolicyEntry 14 }

cabhQos2PolicyDestPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The value that the layer-4 destination port number in the
             packet must have in order to match this policy entry."
    DEFVAL { 0 }
    ::= { cabhQos2PolicyEntry 15 }

cabhQos2PolicyTraffImpNum OBJECT-TYPE
    SYNTAX      Unsigned32 (0..7)
    MAX-ACCESS  read-create
    STATUS      current
```

```
    DESCRIPTION
            "The Traffic priority being assigned to this policy. The
            final packet tagging is determined by 802.1D rules with
            the priority hierarchy order (highest to lowest priority)
            as defined in 802.1D-2004 table G-2:
            7, 6, 5, 4, 3, 0, 2, 1.
            Note that traffic type '1' and '2' has lower priority than
            '0' (best effort)."
    DEFVAL { 0 }
    ::= { cabhQos2PolicyEntry 16 }

cabhQos2PolicyUserImportance OBJECT-TYPE
    SYNTAX      Unsigned32 (0..255)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The UPnP relative value to determine the allocation or
            reallocation of resources to multiple streams."
    DEFVAL { 0 }
    ::= { cabhQos2PolicyEntry 17 }

cabhQos2PolicyRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The status of this conceptual row. All writable objects
            in this row may be modified at any time. The PS MUST
            NOT allow creation of new entry or modification to an
            existing active entry such that the resulting entry is a
            duplicate entry with respect to the following MIBs
            in an entry:
            cabhQos2PolicyAppDomain,
            cabhQos2PolicyAppNameSnmpAdminString,
            cabhQos2PolicyServiceProvDomainSnmpAdminString,
            cabhQos2PolicyServiceName SnmpAdminString,
            cabhQos2PolicyPortDomain SnmpAdminString,
            cabhQos2PolicyPortNumber InetPortNumber,
            cabhQos2PolicyIpType InetAddressType,
            cabhQos2PolicyIpProtocol Unsigned32,
            cabhQos2PolicySrcIp InetAddress,
            cabhQos2PolicyDestIp InetAddress,
            cabhQos2PolicySrcPort InetPortNumber,
            cabhQos2PolicyDestPort InetPortNumber,

            The entries of type 'upnp' are not persistent while others
            are persistent. The user or the operator can change the
            'upnp' entries and in that case the PS MUST change the
            entry to either 'homeUser' or 'operatorForHomeUser',
            respectively. The PS MUST NOT change the entries of type
            'upnp' to 'operatorOnly'."
    ::= { cabhQos2PolicyEntry 18 }
```

```
   --================================================================
   --
   --  PS UPnP QoS Device Information
   --
   --  Contains PS QoS device traffic descriptors as classifiers when
   --  acting as an intermediate device for traffic flows
   --  Qos Device information retrieval from the SNMP WAN interface is
   --  defined in PSDEV-MIB module
   --
   --================================================================

cabhQos2TrafficClassTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhQos2TrafficClassEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "This table contains the Classifiers being configured
            in the PS as an intermediate QoS device.
            For matching classifiers the PS processes entries
            in a sorted manner, first entries with
            cabhQos2TrafficClassMethod 'static' and then
            'dynamic' entries."
    ::= { cabhQos2DeviceObjects 1 }

cabhQos2TrafficClassEntry OBJECT-TYPE
    SYNTAX      CabhQos2TrafficClassEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The conceptual row definition of this table.
            Only entries with cabhQos2TrafficClassMethod
            'static' do persist after PS reboot."
    INDEX { cabhQos2TrafficClassMethod, cabhQos2TrafficClassIdx }
    ::= { cabhQos2TrafficClassTable 1 }

CabhQos2TrafficClassEntry::= SEQUENCE {
    cabhQos2TrafficClassMethod         INTEGER,
    cabhQos2TrafficClassIdx            Unsigned32,
    cabhQos2TrafficClassProtocol       Unsigned32,
    cabhQos2TrafficClassIpType         InetAddressType,
    cabhQos2TrafficClassSrcIp          InetAddress,
    cabhQos2TrafficClassDestIp         InetAddress,
    cabhQos2TrafficClassSrcPort        InetPortNumber,
    cabhQos2TrafficClassDestPort       InetPortNumber,
    cabhQos2TrafficClassImpNum         Unsigned32,
    cabhQos2TrafficClassRowStatus      RowStatus
    }

cabhQos2TrafficClassMethod OBJECT-TYPE
    SYNTAX      INTEGER {
                static(1),
                upnp(2)
                }
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "Indicates how this entry has been created.
            'static' indicates that the entry has been
             provisioned via SNMP or related mechanisms
             like a config file.
            'upnp' indicates that the entry was created via UPnP
            Qos actions."
    ::= { cabhQos2TrafficClassEntry 1 }
```

```
cabhQos2TrafficClassIdx OBJECT-TYPE
    SYNTAX      Unsigned32 (1..4294967295)
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
            "The index of this conceptual row entry."
    ::= { cabhQos2TrafficClassEntry 2 }

cabhQos2TrafficClassProtocol OBJECT-TYPE
    SYNTAX      Unsigned32 (0..256)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The IANA IP transport protocol designated for this
            classifier. '0' means no protocol is specified as
            matching criteria."
    DEFVAL { 0 }
    ::= { cabhQos2TrafficClassEntry 3 }

cabhQos2TrafficClassIpType OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The type of InetAddress for cabhQos2TrafficClassSrcIp,
            and cabhQos2TrafficClassDestIp."
    DEFVAL { ipv4 }
    ::= { cabhQos2TrafficClassEntry 4 }

cabhQos2TrafficClassSrcIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The IP address to match against the packet's source IP
            address for this classifier. This may not be a DNS name,
            but may be an IPv4 or IPv6 prefix."
    DEFVAL { '00000000'h }
    ::= { cabhQos2TrafficClassEntry 5 }

cabhQos2TrafficClassDestIp OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The IP address to match against the packet's source IP
            address for this classifier. This may not be a DNS name,
            but may be an IPv4 or IPv6 prefix."
    DEFVAL { '00000000'h }
    ::= { cabhQos2TrafficClassEntry 6 }

cabhQos2TrafficClassSrcPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The value that the layer-4 source port number in the
            packet must have in order to match this classifier entry."
    DEFVAL { 0 }
    ::= { cabhQos2TrafficClassEntry 7 }
```

```
cabhQos2TrafficClassDestPort OBJECT-TYPE
    SYNTAX      InetPortNumber
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The value that the layer-4 destination port number in the
            packet must have in order to match this classifier entry."
    DEFVAL { 0 }
    ::= { cabhQos2TrafficClassEntry 8 }

cabhQos2TrafficClassImpNum OBJECT-TYPE
    SYNTAX      Unsigned32 (0..7)
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The traffic priority assigned to this classifier and used
            for the tagging of the packet streams."
    DEFVAL { 0 }
    ::= { cabhQos2TrafficClassEntry 9 }

cabhQos2TrafficClassRowStatus OBJECT-TYPE
    SYNTAX      RowStatus
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
            "The status of this conceptual row. All writable objects
            in rows with cabhQosTrafficMethod 'static' may be
            modified at any time. An SNMP Set to Entries with
            cabhQosTrafficMethod 'upnp' returns an error
            'wrongValue'with the exception of the RowStatus
            object when set to 'destroy'.
            An attempt to create an entry via SNMP with
            cabhQosTrafficMethod UPnP returns error 'wrongValue'."
    ::= { cabhQos2TrafficClassEntry 10 }

   -- Placeholder for notifications.
   --
   --
   -- Conformance definitions
   --
cabhQos2Conformance    OBJECT IDENTIFIER  ::= { cabhQos2Mib 2 }
cabhQos2Compliances    OBJECT IDENTIFIER  ::= { cabhQos2Conformance 1 }
cabhQos2Groups         OBJECT IDENTIFIER  ::= { cabhQos2Conformance 2 }

   -- ==================

   -- compliance statements

cabhQos2Compliance MODULE-COMPLIANCE
    STATUS      current
    DESCRIPTION
            "The compliance statement for devices that implement
            CableHome QoS UPnP capabilities."
    MODULE   --cabhQos2Mib

   -- unconditionally mandatory groups

    MANDATORY-GROUPS {
          cabhQos2Group
          }

 -- conditionally groups
```

```
GROUP cabhQos2ClassifierGroup
    DESCRIPTION
            "This group is optional and implemented only for
             traffic between LAN and WAN."

OBJECT cabhQos2PolicyIpType
    SYNTAX InetAddressType { ipv4(1) }
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."

OBJECT cabhQos2PolicySrcIp
    SYNTAX InetAddress (SIZE(4))
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."

OBJECT cabhQos2PolicyDestIp
    SYNTAX InetAddress (SIZE(4))
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."

OBJECT cabhQos2TrafficClassIpType
    SYNTAX InetAddressType { ipv4(1) }
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses. "

OBJECT cabhQos2TrafficClassSrcIp
    SYNTAX InetAddress (SIZE(4))
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."

OBJECT cabhQos2TrafficClassDestIp
    SYNTAX InetAddress (SIZE(4))
    DESCRIPTION
            "An implementation is only required to support IPv4
            addresses."
    ::= { cabhQos2Compliances 1 }

cabhQos2Group OBJECT-GROUP
    OBJECTS {
    cabhQos2SetToFactory,
    cabhQos2LastSetToFactory,
    cabhQos2PsIfAttribNumPriorities,
    cabhQos2PsIfAttribNumQueues,
    cabhQos2PolicyHolderEnabled,
    cabhQos2PolicyAdmissionControl,
    cabhQos2NumActivePolicyHolder,
    cabhQos2PolicyRuleOrder,
    cabhQos2PolicyAppDomain,
    cabhQos2PolicyAppName,
    cabhQos2PolicyServiceProvDomain,
    cabhQos2PolicyServiceName,
    cabhQos2PolicyPortDomain,
    cabhQos2PolicyPortNumber,
    cabhQos2PolicyIpProtocol,
    cabhQos2PolicyIpType,
    cabhQos2PolicySrcIp,
    cabhQos2PolicyDestIp,
```

```
    cabhQos2PolicySrcPort,
    cabhQos2PolicyDestPort,
    cabhQos2PolicyTraffImpNum,
    cabhQos2PolicyUserImportance,
    cabhQos2PolicyRowStatus,
    cabhQos2TrafficClassProtocol,
    cabhQos2TrafficClassIpType,
    cabhQos2PolicySrcIp,
    cabhQos2PolicyDestIp,
    cabhQos2PolicySrcPort,
    cabhQos2PolicyDestPort,
    cabhQos2PolicyTraffImpNum,
    cabhQos2PolicyUserImportance,
    cabhQos2PolicyRowStatus
    }
    STATUS      current
    DESCRIPTION
            "Group of objects for CableHome QoS management."
    ::= { cabhQos2Groups 1 }

cabhQos2ClassifierGroup OBJECT-GROUP
    OBJECTS {
    cabhQos2TrafficClassProtocol,
    cabhQos2TrafficClassIpType,
    cabhQos2TrafficClassSrcIp,
    cabhQos2TrafficClassDestIp,
    cabhQos2TrafficClassSrcPort,
    cabhQos2TrafficClassDestPort,
    cabhQos2TrafficClassImpNum,
    cabhQos2TrafficClassRowStatus
    }
    STATUS      current
    DESCRIPTION
            "Group of objects for cableHome QoS Packet
            classification."
    ::= { cabhQos2Groups 2 }
END
```

Apéndice I

Ejemplo de descripción del dispositivo raíz UPnP del PS IPCable2Home

El siguiente documento en lenguaje XML proporciona un ejemplo de descripción del dispositivo raíz UPnP del PS IPCable2Home.

```
<?xml version="1.0" encoding="utf-8" ?>
- <root xmlns="urn:schemas-upnp-org:device-1-0">
  - <specVersion>
      <major>1</major>
      <minor>0</minor>
    </specVersion>
    <URLBase>URLBase</URLBase>
  - <device>
      <deviceType>urn:schemas-cablelabs-com:device:CableHomePSDevice:1</deviceType>
      <friendlyName>friendlyName</friendlyName>
      <manufacturer>manufacturer</manufacturer>
      <manufacturerURL>manufacturerURL</manufacturerURL>
      <modelDescription>modelDescription</modelDescription>
      <modelName>modelName</modelName>
      <modelNumber>modelNumber</modelNumber>
      <modelURL>modelURL</modelURL>
      <serialNumber>serialNumber</serialNumber>
      <UDN>uuid:CableHomePSDevice-1_0-00AABBCCDDEE</UDN>
      <UPC>upc</UPC>
    - <serviceList>
      - <service>
          <serviceType>urn:schemas-upnp-org:service:QosManager:1</serviceType>
          <serviceId>urn:upnp-org:serviceId:QosManager</serviceId>
          <SCPDURL>/QosManager.xml</SCPDURL>
          <controlURL>/QosManager</controlURL>
          <eventSubURL>/QosManager</eventSubURL>
        </service>
      - <service>
          <serviceType>urn:schemas-upnp-org:service:QosPolicyHolder:1</serviceType>
          <serviceId>urn:upnp-org:serviceId:QosPolicyHolder</serviceId>
          <SCPDURL>/QosPolicyHolder.xml</SCPDURL>
          <controlURL>/QosPolicyHolder</controlURL>
          <eventSubURL>/QosPolicyHolder</eventSubURL>
        </service>
      - <service>
          <serviceType>urn:schemas-upnp-org:service:QosDevice:1</serviceType>
          <serviceId>urn:upnp-org:serviceId:QosDevice</serviceId>
          <SCPDURL>/QosDevice.xml</SCPDURL>
          <controlURL>/QosDevice</controlURL>
          <eventSubURL>/QosDevice</eventSubURL>
        </service>
      </serviceList>
    - <deviceList>
      - <device>
          <deviceType>urn:schemas-upnp-org:device:InternetGatewayDevice:1</deviceType>
          <friendlyName>friendlyName</friendlyName>
          <manufacturer>manufacturer</manufacturer>
          <manufacturerURL>manufacturerURL</manufacturerURL>
          <modelDescription>modelDescription</modelDescription>
          <modelName>modelName</modelName>
          <modelNumber>modelNumber</modelNumber>
          <modelURL>modelURL</modelURL>
          <serialNumber>serialNumber</serialNumber>
          <UDN>uuid:InternetGatewayDevice-1_0-00AABBCCDDEE</UDN>
          <UPC>upc</UPC>
```

```
            - <deviceList>
                - <device>
                    <deviceType>urn:schemas-upnp-org:device:WANDevice:1</deviceType>
                    <friendlyName>friendlyName</friendlyName>
                    <manufacturer>manufacturer</manufacturer>
                    <manufacturerURL>manufacturerURL</manufacturerURL>
                    <modelDescription>modelDescription</modelDescription>
                    <modelName>modelName</modelName>
                    <modelNumber>modelNumber</modelNumber>
                    <modelURL>modelURL</modelURL>
                    <serialNumber>serialNumber</serialNumber>
                    <UDN>uuid:upnp-WANDevice-1_0-XXXX</UDN>
                    <UPC>upc</UPC>
                  - <serviceList>
                      - <service>
                          <serviceType>urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1</serviceType>
                          <serviceId>urn:upnp-org:serviceId:WANCommonInterfaceConfig</serviceId>
                          <SCPDURL>/WANCommonInterfaceConfig.xml</SCPDURL>
                          <controlURL>/WANCommonInterfaceConfig</controlURL>
                          <eventSubURL>/WANCommonInterfaceConfig</eventSubURL>
                        </service>
                    </serviceList>
                  - <deviceList>
                      - <device>
                          <deviceType>urn:schemas-upnp-org:device:WANConnectionDevice:1</deviceType>
                          <friendlyName>friendlyName</friendlyName>
                          <manufacturer>manufacturer</manufacturer>
                          <manufacturerURL>manufacturerURL</manufacturerURL>
                          <modelDescription>modelDescription</modelDescription>
                          <modelName>modelName</modelName>
                          <modelNumber>modelNumber</modelNumber>
                          <modelURL>modelURL</modelURL>
                          <serialNumber>serialNumber</serialNumber>
                          <UDN>uuid:upnp-WANConnectionDevice-1_0-XXXX</UDN>
                          <UPC>upc</UPC>
                        - <serviceList>
                            - <service>
                                <serviceType>urn:schemas-upnp-org:service:WANIPConnection:1</serviceType>
                                <serviceId>urn:upnp-org:serviceId:WANIPConnection</serviceId>
                                <SCPDURL>/WANIPConnection.xml</SCPDURL>
                                <controlURL>/WANIPConnection</controlURL>
                                <eventSubURL>/WANIPConnection</eventSubURL>
                              </service>
                          </serviceList>
                        </device>
                    </deviceList>
                </device>
              </deviceList>
              <presentationURL>/index.htm</presentationURL>
            </device>
        </deviceList>
        <presentationURL>/index.htm</presentationURL>
    </device>
</root>
```

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	**Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia**
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de transmisión telefónica, instalaciones telefónicas y redes locales
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos, comunicaciones de sistemas abiertos y seguridad
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2007