Unión Internacional de Telecomunicaciones

UIT-T J.192

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(03/2004)

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

Módems de cable

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

Recomendación UIT-T J.192

Unión Internacional de Telecomunicaciones

Recomendación UIT-T J.192

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

Resumen

En esta Recomendación se presenta un conjunto de características propias del IP, que por lo general se asocian a una pasarela residencial, que puede integrarse a un módem de cable (por ejemplo, conforme a las Recs. UIT-T J.122, J.112) o conectarse al mismo, permitiendo que los operadores del sistema de cable ofrezcan a sus clientes un conjunto de servicios más amplios inherentes a la red doméstica (relacionados a la Rec. UIT-T J.191). Este conjunto incluye el soporte de calidad de servicio (QoS, *quality of service*), determinación del dispositivo y el servicio, seguridad más amplia, gestión de la barrera contrafuego, características de gestión y configuración centrados en la red doméstica, traducción de la dirección de la red gestionada, direccionamiento y tratamiento mejorados de paquetes y diagnóstico de los dispositivos de la red LAN.

Orígenes

La Recomendación UIT-T J.192 fue aprobada el 15 de marzo de 2004 por la Comisión de Estudio 9 (2001-2004) 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.

ÍNDICE

Recomendación UIT-T J.192

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

1 Ámbito de aplicación

La presente Recomendación permite la creación de una pasarela residencial al proponer un conjunto de características propias del IP que podrán añadirse a un módem de cable o incorporarse en un aparato autónomo. Este conjunto permitirá que los operadores de cable ofrezcan a sus clientes un conjunto adicional de servicios ampliado inherentes a la red doméstica, que incluye el manejo de calidad de servicio (QoS), determinación del dispositivo y el servicio, seguridad más amplia, gestión de la barrera contrafuego, 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 los marcos de arquitectura conformes a 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, y se basa sobre la misma para ofrecer características avanzadas adicionales. Un objetivo de diseño esencial de los equipos que habrán de conformarse a esta Recomendación es la interoperabilidad con los que se conformen a 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 red 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 contrafuego;
- funcionalidad de la barrera contrafuego básica normalizada;
- control paternal simple;
- calidad de servicio para la red LAN, que se gestiona en la pasarela residencial.

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.

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

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

[Rec. UIT-T J.161] 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*.

[Rec. UIT-T J.162] Recomendación UIT-T J.162 (2004), *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*.

[Rec. UIT-T J.163] Recomendación UIT-T J.163 (2004), *Calidad de servicio dinámica para la prestación de servicios en tiempo real por las redes de televisión por cable que utilizan módems de cable*.

[Rec. UIT-T J.164] Recomendación UIT-T J.164 (2001), *Requisitos de los mensajes de evento para el soporte de servicios en tiempo real transmitidos mediante redes de televisión por cable que utilizan módems de cable.*

[Rec. UIT-T J.167] Recomendación UIT-T J.167 (2001), *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.*

[Rec. UIT-T J.170] Recomendación UIT-T J.170 (2002), *Especificación de la seguridad de IPCablecom*.

[Rec. UIT-T J.175] Recomendación UIT-T J.175 (2002), *Protocolo de servidor de audio*.

[Rec. UIT-T J.178] Recomendación UIT-T J.178 (2003), *Señalización entre servidores de gestión de llamadas de IPCablecom*.

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

[Rec. UIT-T X.25] Recomendación UIT-T X.25 (1996), *Interfaz entre el equipo terminal de datos y el equipo de terminación del circuito de datos para equipos terminales que funcionan en el modo paquete y están conectados a redes públicas de datos por circuitos especializados.*

[Rec. UIT-T X.509] Recomendación UIT-T X.509 (2000): *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos.*

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

[ANSI/SCTE 23-3] ANSI/SCTE 22-1 2002, *DOCSIS 1.1 Part 3: Operations Support System Interface*.

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

[FIPS 180-1] FIPS PUB 180-1 (1995), *Secure Hash Standard*, Department of Commerce, NIST.

[IANAType] IANAifType MIB Definitions, http://www.iana.org/assignments/ianaiftype-mib.

[ISO/CEI 8825-1] ISO/CEI 8825-1:2002, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*.

[ISO/CEI 10038] ISO/CEI 10038:1993, *Information technology – Telecommunications and information exchange between systems – Local area networks – Media access control (MAC) bridges*.

[RFC 347] IETF RFC 0347 (1972), *Echo Process*.

[RFC 768] IETF RFC 0768 (1980), *User Datagram Protocol (UDP)*.

[RFC 791] IETF RFC 0791 (1981), *Internet Protocol*.

[RFC 792] IETF RFC 0792 (1981), *Internet Control Message Protocol (ICMP)*.

[RFC 868] IETF RFC 0868 (1983), *Time Protocol*.

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

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

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

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

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

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

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

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

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

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

[RFC 1633] IETF RFC 1633 (1994), *Integrated Services in the Internet Architecture: An Overview*.

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

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

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

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

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

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

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

[RFC 2132] IETF RFC-2132 (1997), *DHCP Options and BOOTP Vendor Extensions*.

[RFC 2211] IETF RFC 2211 (1997), *Specification of the Controlled-Load Network Element Service*.

[RFC 2212] IETF RFC 2212 (1997), S*pecification of Guaranteed Quality of Service*.

[RFC 2233] IETF RFC 2233 (1997), *The Interfaces Group MIB using SMIv2*.

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

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

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

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

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

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

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

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

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

[RFC 2576] IETF RFC 2576 (2000), *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*.

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

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

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

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

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

[RFC 2665] IETF RFC 2665 (1999), *Definitions of Managed Objects for Ethernet-like Interface Types*.

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

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

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

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

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

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

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

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

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

[RFC 3411] IETF RFC 3411 (2002), *An Architecture for Describing SNMP Management Frameworks*.

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

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

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

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

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

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

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

[SOAP] W3C Recommendation: *SOAP Version 1.2*, 24 June 2003, http://www.w3.org/TR/2003/REC-soap12-part0-20030624.

[XML] W3C Working Draft: *XML Protocol (XMLP) Requirements*, 26 June 2002, http://www.w3.org/TR/2002/WD-xmlp-reqs-20020626.

2.2 Referencias (informativas)

[ANSI/SCTE 22-3] ANSI/SCTE 22-3 2002, *DOCSIS 1.0 Part 3: Operations Support System Interface*.

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

[FIPS 186-2] FIPS PUB 186-2 (2000), *Digital Signature Standard*. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf.

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

[ID-IGMP] IETF Internet Draft, *IGMP-based Multicast Forwarding ("IGMP Proxying")*. http://www.ietf.org/internet-drafts/draft-ietf-magma-igmp-proxy-01.txt.

[PKCS #1] RSA Laboratories, PKCS #1, v2.0: *RSA Cryptography Standard*, October 1, 1998.

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

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

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

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

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 acceso a 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 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 CM 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*)
CH	Anfitrión de IPCable2Home (*IPCable2Home host*)
CM	Módem de cable (*cable modem*)
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 modem 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*)
DER	Reglas de codificación distinguidas (*distinguished encoding rules*)
DHCP	Protocolo dinámico de configuración de anfitrión (*dynamic host configuration protocol*)
DNS	Servicio de nombres de dominio (*domain name service*)
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 multimedios integrado (*embedded multimedia terminal adapter*)
FTP	Protocolo de transferencia de ficheros (*file transfer protocol*)
FW	Barrera contrafuego (*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 (*multi-protocol label switching*)
MSF	Función de servidor de gestión (*management server function*)
MTA	Adaptador de terminal multimedios (*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 filtering*)
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 WAN-Data	Interfaz de datos entre el elemento de servicios de portal de Cable Home y la red de área extensa (*CableHome portal services element WAN data interface*)
PS WAN-Man	Interfaz de gestión entre el elemento de servicios de portal de CableHome y la red de área extensa (*CableHome portal services element WAN management interface*)
PS	Servicios de portal (*portal services*)

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
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 multimedios autónomo (*stand-alone 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 particulares del sistema de cable a los aparatos instalados en la vivienda, complementando las infraestructuras de CableModem 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 y de los anfitriones conformes (CH, *compliant hosts*) correspondientes. 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 aparatos domésticos que funcionen con el IP (dispositivos IP de la red LAN) bien sean conformes o no. Esto dará al operador de cable la capacidad de controlar la gestión, la configuración, la calidad de servicio y la seguridad de la pasarela residencial. Además, permitirá especificar la mensajería de la red LAN, la QoS con prioridades y los diagnósticos simples a distancia de los aparatos en la vivienda, así como la calidad de servicio de las aplicaciones que funcionan en servidores LAN conformes con IPCable2Home. A continuación se presenta un resumen de las capacidades incluidas en esta Recomendación:

Gestión, determinación y configuración

- gestión y configuración a distancia de la pasarela residencial;
- apoderado simple de diagnósticos de la pasarela residencial para los aparatos domésticos basados en IP;
- configuración automática de la pasarela residencial;
- determinación de los aparatos domésticos basados en el IP y sus aplicaciones correspondientes;
- gestión de la pasarela residencial desde la red LAN.

Direccionamiento y tratamiento de paquetes

- traducción de direcciones de una a varias, para los aparatos en la vivienda;
- traducción de direcciones una a una, para los aparatos en la vivienda;
- direccionamiento sin traducción para los aparatos en la vivienda (en el caso de aplicaciones que no aceptan la traducción de direcciones);
- protección del tráfico HFC contra las comunicaciones entre los aparatos 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 particulares del IP en la vivienda que emplean QoS con traducción de direcciones.

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.

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 contrafuego de la pasarela residencial;
- configuración e informes normalizados de la barrera contrafuego;
- control paternal simple.

La comunicación de IPCable2Home a través de las redes WAN y LAN se fundamenta en el protocolo IPv4 que equilibra los protocolos específicos que se definen en el resto de esta Recomendación . Los dispositivos conformes con IPCable2Home DEBEN aplicar la versión 4 del conjunto de protocolos Internet (IPv4) [RFC 791], [RFC 3280].

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

- lógica (véase 5.1);
- funcional (véase 5.2);

- de interfaz de mensajería (véase 5.3);
- de información (véase 5.4);
- operacional (véase 5.5);
- de interfaz física (véase 5.6).

5.1 Arquitectura de referencia lógica

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

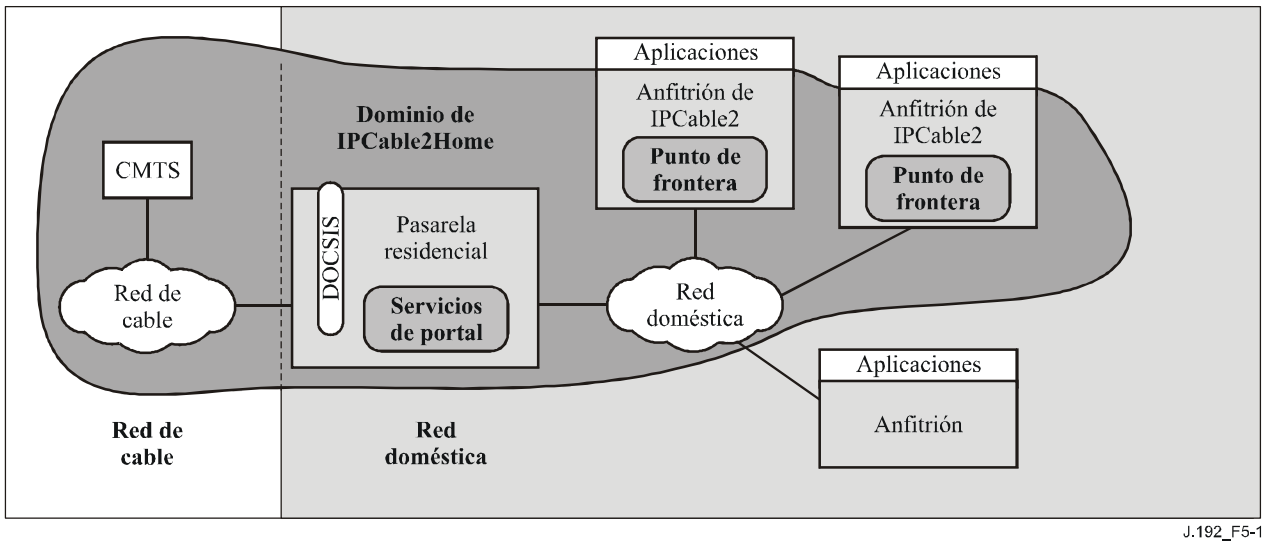


Figura 5-1/J.192 – Conceptos lógicos esenciales de IPCable2Home

5.1.1 Dominio de IPCable2Home

El dominio de IPCable2Home se representa mediante el conjunto de elementos de red que tienen conformidad con esta Recomendación y que se ilustra a manera de diagrama como la zona sombreada en la figura 5-1. Esta zona se utiliza como una herramienta visual para identificar, sin lugar a dudas, los elementos de la red doméstica que son conformes con IPCable2Home. Los elementos que residen en el dominio de IPCable2Home (es decir, elementos conformes) pueden ser gestionados directa o indirectamente por los operadores del sistema de cable. Hay un dominio de IPCable2Home en cada vivienda.

5.1.2 Dispositivos que pertenecen a IPCable2Home

En la arquitectura de IPCable2Home se identifican los dispositivos para asignar un contexto tangible a los elementos lógicos que se describen en 5.1.3. 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 5.1.3.1. La misma 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 dispositivo LAN que tenga una interfaz IP. Un dispositivo de este tipo que se dote con funcionalidad de IPCable2Home, para que sea conforme con la especificación de IPCable2Home, se denomina *dispositivo anfitrión de IPCable2Home* ("HC" en la Rec. UIT-T J.190). Un dispositivo IP de LAN sin funcionalidad de IPCable2Home, se denomina *anfitrión*.

El anfitrión de IPCable2Home representa la ubicación física del punto de frontera (BP, *boundary point*) que se define en 5.1.3.2 y que permite el interfuncionamiento de los anfitriones y las pasarelas particulares de IPCable2Home. El anfitrión de IPCable2Home tiene únicamente una interfaz de LAN en el dominio de IPCable2Home.

IPCable2Home utiliza una topología de conexión en red doméstica con un solo módem de cable (CM) DOCSIS y una pasarela residencial de IPCable2Home en la red 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 LAN se conectan a la red LAN por detrás de la pasarela residencial de IPCable2Home.

5.1.3 Elementos lógicos

El marco de la arquitectura 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 para obtener 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 particulares, y la entidad lógica del BP encapsula la funcionalidad definida para los anfitriones de IPCable2Home (véase 5.1.2 para obtener una descripción de los dispositivos de IPCable2Home).

5.1.3.1 Servicios de portal (PS)

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

5.1.3.1.1 PS autónomo y PS con módem de cable integrado

Las dos entidades funcionales 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. En realidad, la falta de capacidad de uso compartido de recursos entre las funciones del CM y el PS es la que permite distinguir entre el PS autónomo y el 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 pudiera residir en el mismo recinto físico de 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.

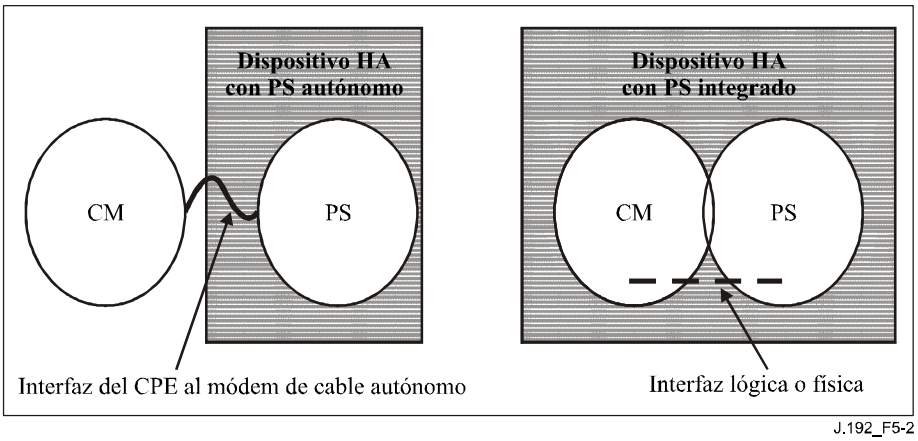


Figura 5-2/J.192 – PS autónomo y PS con CM integrado

5.1.3.2 Punto de frontera (BP)

Se trata de un elemento lógico que encapsula toda la funcionalidad de IPCable2Home definida para un anfitrión de IPCable2Home. Esta funcionalidad incluye la capacidad de mensajería y el comportamiento necesarios para que el operador de cable pueda determinar el dispositivo y la aplicación, así como para facilitar la QoS con prioridades en la red doméstica. El BP interfunciona con el PS a fin de conducir información del dispositivo y de la aplicación, y también para consultar preferencias suministradas por el operador para las prioridades de la aplicación.

5.1.4 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).

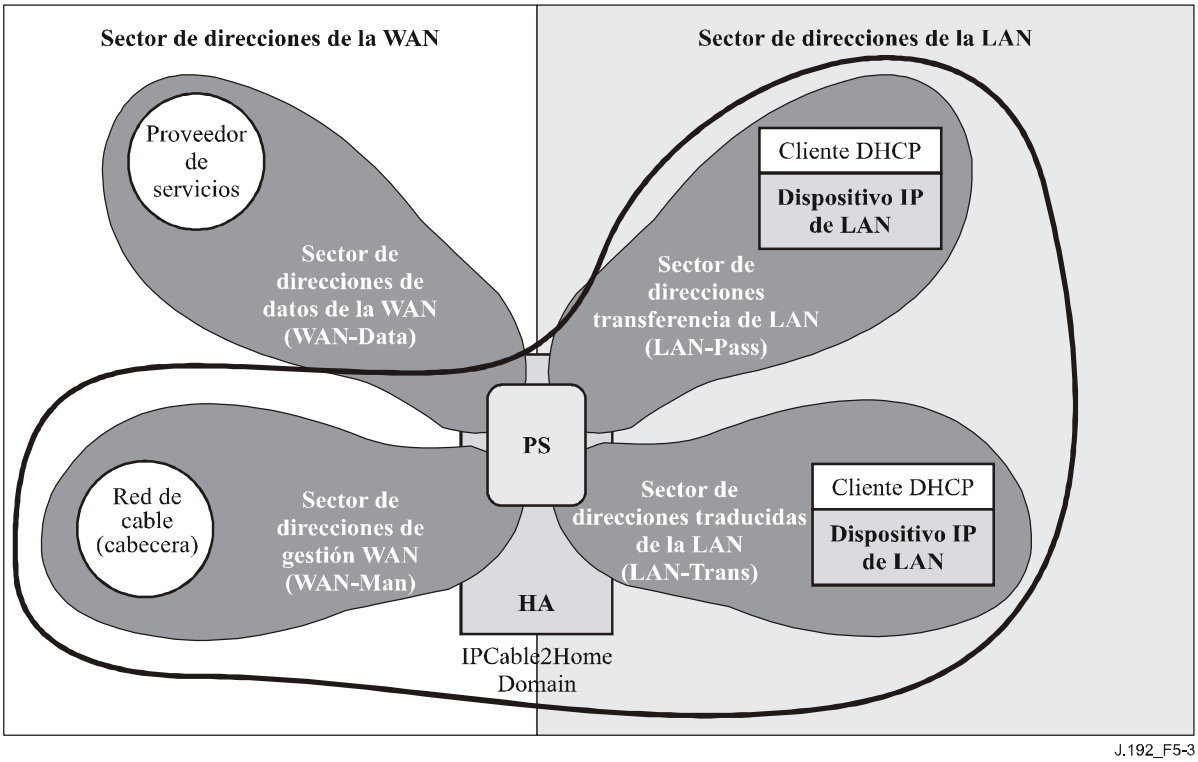


Figura 5-3/J.192 – Sectores de direcciones de IPCable2Home

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 por la red de cable el tráfico de la aplicación del abonado y, más allá de ésta, tráfico tal como el existente entre los anfitriones de IPCable2Home y los servidores 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, *translated LAN address realm*) tiene por objeto transportar tráfico de la aplicación del abonado y de gestión por la red doméstica entre anfitriones de IPCable2Home, los 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 anfitriones de IPCable2Home, los dispositivos IP de LAN y los servidores 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). Hay sectores de direcciones LAN-Pass y LAN-Trans en cada vivienda.

A las interfaces LAN físicas en el PS se les asigna un índice de acuerdo con la MIB del grupo de interfaces [RFC 2233], como se describe en 6.3.3.1.4.8, "MIB del grupo de interfaces". En la misma cláusula se define para el PS una interfaz LAN virtual que permite agregar las interfaces LAN físicas. La dirección IP correspondiente al lado LAN que se definió para el PS se "vincula" a esta interfaz virtual. 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.

5.2 Modelo de referencia funcional de IPCable2Home

Las funciones de IPCable2Home son servicios particulares del IP que se han de implementar mediante el PS, el BP 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 se definen tanto para el PS como para el BP y representan agrupaciones de funcionalidad conexa en ambos. Los elementos lógicos del PS y el BP pueden incluir múltiples subelementos y, a su vez, estos subelementos pueden contener subgrupos de funciones (es decir, subelementos dentro de subelementos).

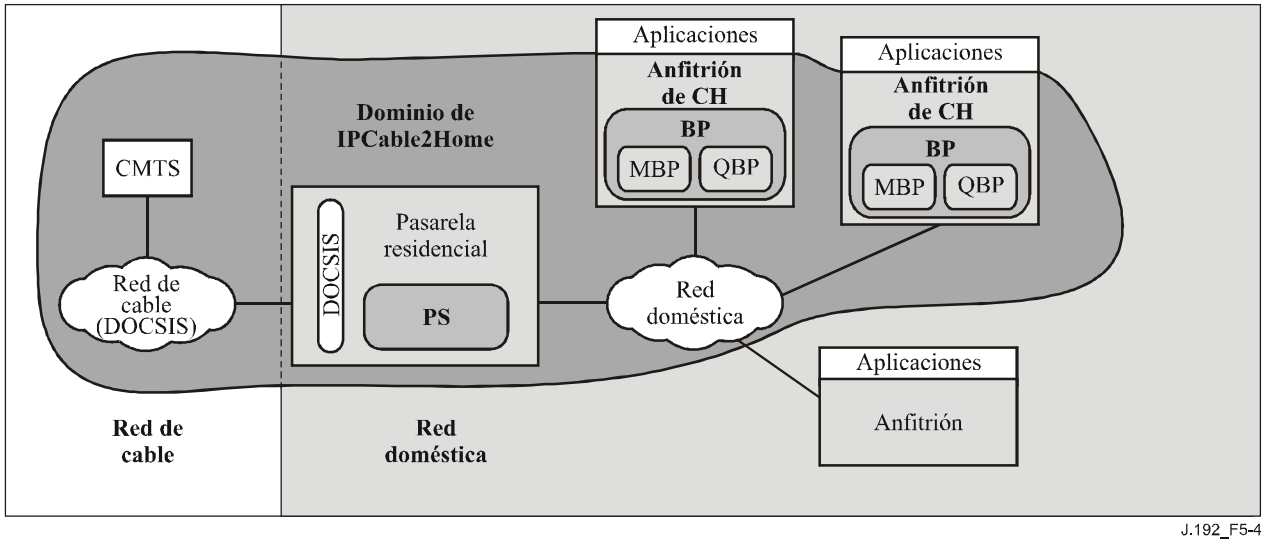


Figura 5-4/J.192 – Subelementos de IPCable2Home

El PS incluye varios subelementos, que se introducen más adelante. En el punto de frontera hay dos subelementos primarios, el punto de frontera de gestión (MBP, *management boundary point*) y el punto de frontera de calidad de servicio (QBP, *quality of service boundary point*), que definen la determinación y la gestión, y la funcionalidad de QoS, respectivamente. El QBP incluye a su vez elementos adicionales propios.

5.2.1 Funciones de gestión y configuración de IPCable2Home

Para soportar los requisitos durante la configuración y la gestión de los anfitriones de IPCable2Home en la red doméstica, IPCable2Home utiliza funciones correspondientes que residen en la red de datos por cable, y define funciones para el PS y el BP. Las funciones de gestión y configuración particulares de 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. Las funciones del punto de frontera se ubican en los anfitriones de IPCable2Home y por lo general incluyen el tipo de funcionalidad de cliente así como otros tipos de funcionalidad. En los cuadros 5-1, 5-2 y 5-3 se muestran ejemplos de las funciones de la red de cable, del PS y del BP y las mismas se ilustran en la figura 5-5.

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.)
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 (passthrough)	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 de servicios múltiples MSO y la base de datos del PS.
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 el sector 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.

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

Funciones del portal de gestión	Descripción
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.

Cuadro 5-3/J.192 – Funciones de gestión y configuración del BP

Funciones de cliente de gestión	Descripción
Cliente DHCP del anfitrión doméstico del sistema de cable	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 así como otro tipo de información de configuración del elemento lógico.
Respondedor de bucle del anfitrión de IPCable2Home	El respondedor de bucle del dispositivo IP de LAN devuelve los datos procedentes de la función de bucle del CTP a esta misma.
Cliente HTTP	Se trata del protocolo de transporte que se emplea para transportar los mensajes SOAP en la red LAN. El BP incluye un cliente HTTP que solicita datos del servidor HTTP alojado en el PS.
Analizadores sintácticos XML y SOAP	Se emplean para los mensajes en la red LAN. El BP incluye ambos analizadores sintácticos.

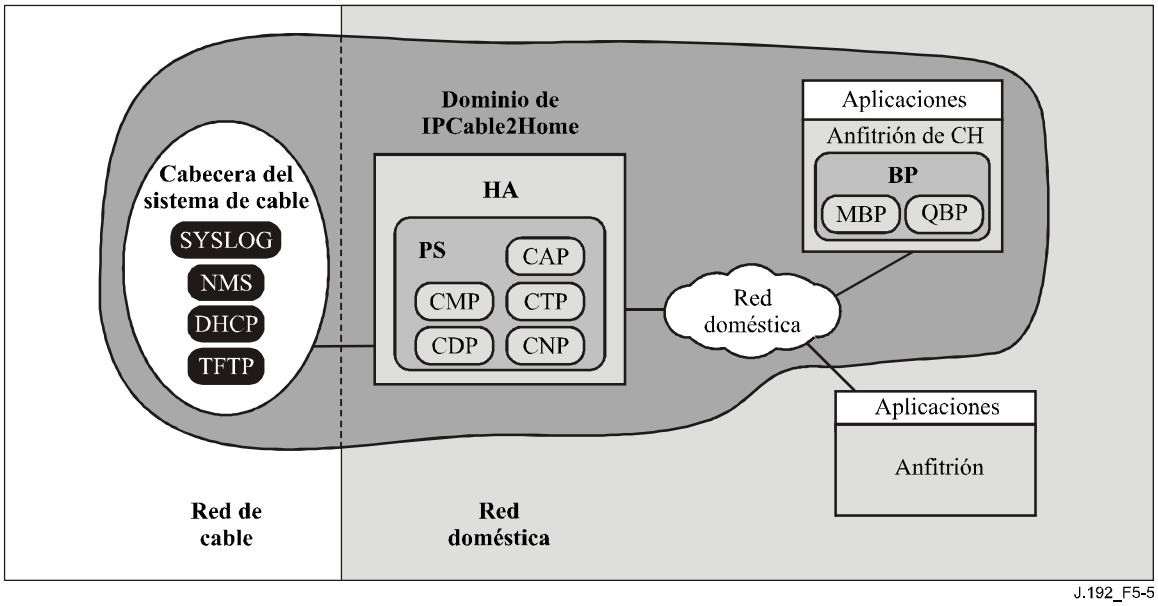


Figura 5-5/J.192 – Elementos de gestión de IPCable2Home

5.2.2 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. Estas funciones residen a su vez en el dominio de seguridad de IPCable2Home, que existe en cada vivienda. Las funciones de seguridad particulares 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 5-6.

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

Funciones	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 contrafuego.
Barrera contrafuego (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

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

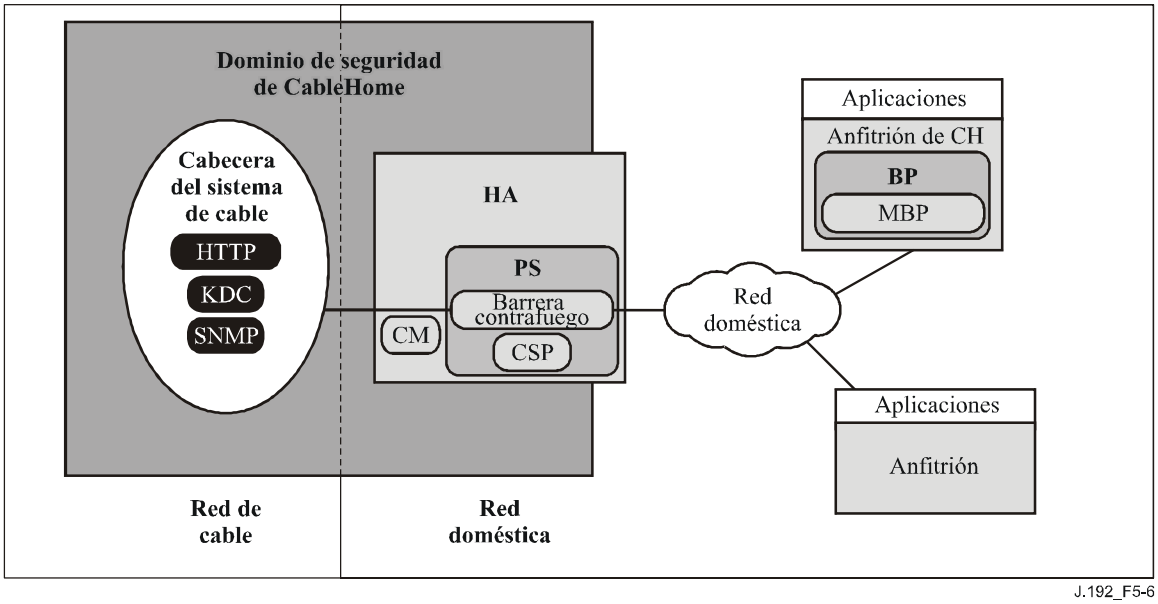


Figura 5-6/J.192 – Elementos de seguridad de IPCable2Home

5.2.3 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 de los servicios de portal se ubican en la pasarela residencial e incluyen una función de servidor y funciones de otros tipos. 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 5-7.

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

Funciones	Descripción
Servidor de características de QoS (QCS)	Obtiene información relativa a las prioridades de QoS para las aplicaciones, desde el sistema de gestión de la red de cable. Obtiene la relación de aplicaciones del BP desde el BP. Proporciona al BP información relativa a las prioridades de las aplicaciones, conforme lo determine el operador del sistema de cable.
Acceso a retransmisión y medios con QoS (QFM)	Ordena los paquetes que se reciben en el PS, procedentes de múltiples interfaces LAN y los retransmite a una interfaz LAN de destino, de acuerdo a sus prioridades. Además, proporciona acceso con prioridad a los medios compartidos durante la transmisión de los paquetes, en función de la prioridad de los mismos.

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

Funciones	Descripción
Cliente con características de QoS (QCC)	Proporciona información al PS relativa a las aplicaciones que residen en el anfitrión de IPCable2Home y también solicita información sobre las prioridades de la aplicación establecidas por el MSO. Además, proporciona acceso con prioridad a los medios compartidos durante la transmisión de los paquetes, en función de la prioridad de los mismos.

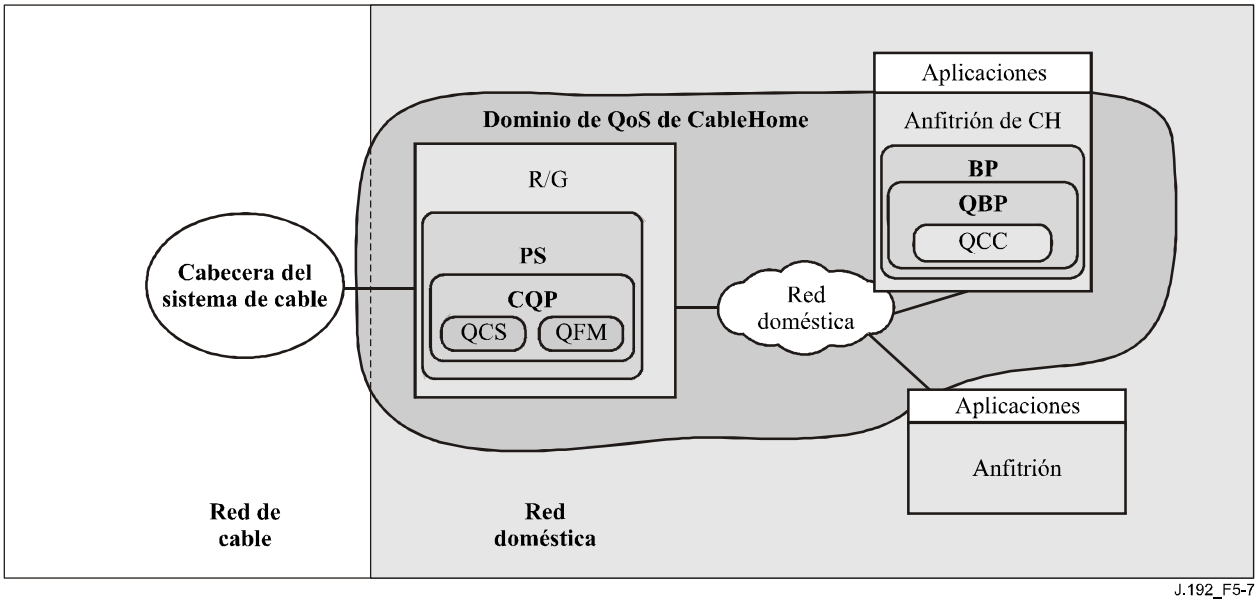


Figura 5-7/J.192 – Elementos de QoS de IPCable2Home

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 5-8. Gracias a los elementos que participan en la comunicación pueden diferenciarse los tipos de esas interfaces.

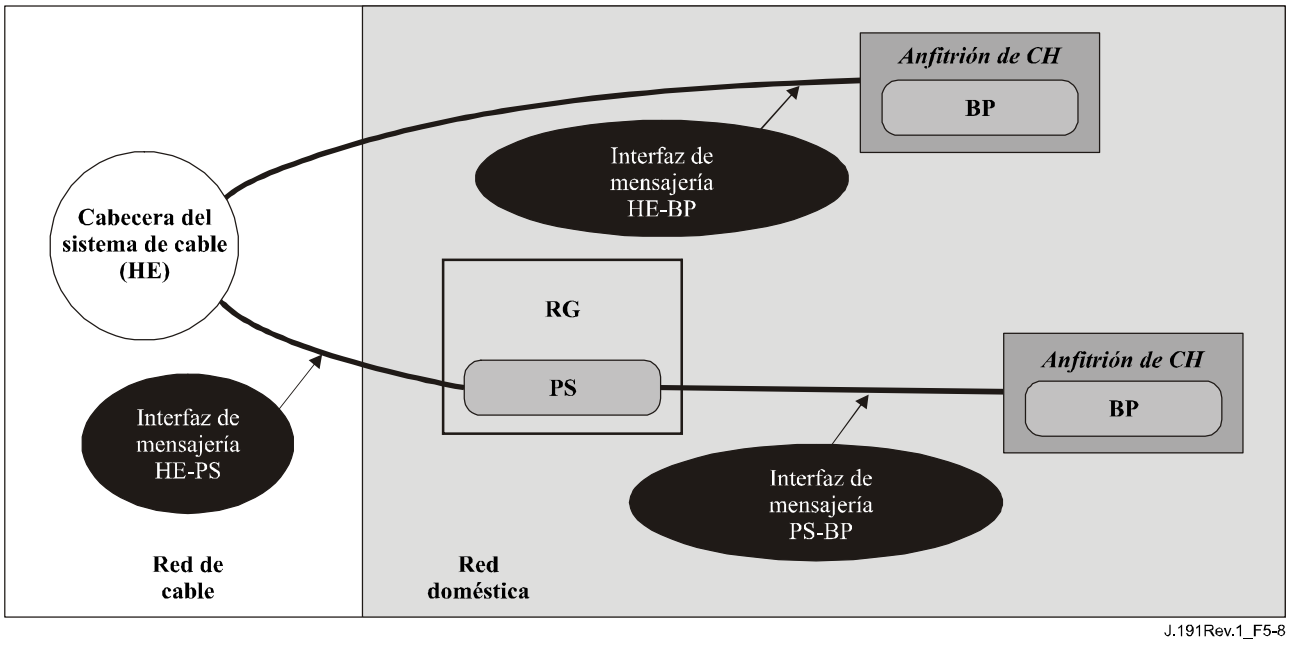


Figura 5-8/J.192 – Interfaces de referencia de IPCable2Home

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-BP	RG-BP
Servicio de nombre	DNS	Sin especificar	Sin especificar	J.192
Descarga de software	TFTP	J.192	Sin especificar	Sin especificar
Obtención de dirección	DHCP	J.192	Sin especificar	J.192
Gestión (simple) (en bloque)	 SNMP TFTP o HTTP	 J.192 J.192	 Sin especificar Sin especificar	 Sin especificar Sin especificar
Notificación de eventos	SNMP SYSLOG	J.192 J.192	Sin especificar	Sin especificar
QoS	Protocolos de QoS de IPCablecom, prioridades SOAP/XML de IPCable2Home	Sin especificar	IPCablecom	J.192
Seguridad (distribución de claves)	Kerberos	J.192	Sin especificar	Sin especificar
Nombre de servicio	DNS	Sin especificar	Sin especificar	J.192
Seguridad (autenticación)	Kerberos o TLS	J.192	Sin especificar	Sin especificar
Ping	ICMP	J.192	Sin especificar	J.192
Bucle/eco	UDP/TCP	Sin especificar	Sin especificar	J.192
Determinación de la aplicación	SNMP SOAP/XML	J.192	Sin especificar	J.192

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 5-9 se indica 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 5-10 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.

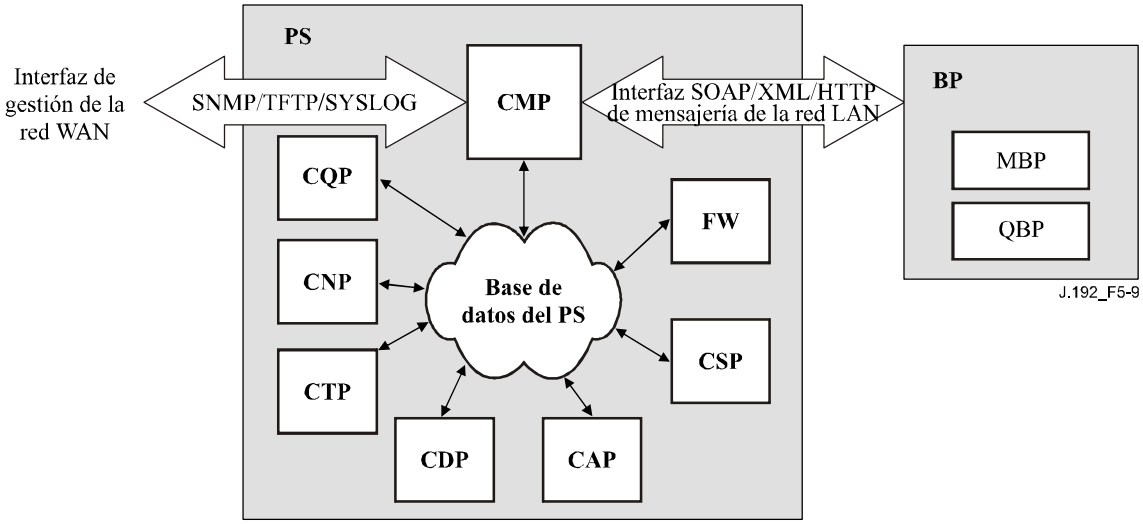


Figura 5-9/J.192 – Relación entre las funciones y la base de datos del PS

En la base de datos del PS se almacena una gran cantidad de relaciones de datos. El CMP aporta la interfaz de la 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 (por lo 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 IPCable2Home.
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 de 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 contrafuego	Información correspondiente al comportamiento de la barrera contrafuego (conjunto de normas), sus eventos y registros históricos.
Información de eventos	Información correspondiente al registro histórico local de todos los eventos, trampas, etc., genéricos.

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

Nombre	Utilización (por lo general)
Información del anfitrión de IPCable2Home	Información del perfil del dispositivo del BP recopilada a través de mensajes BP_Init de los anfitriones de IPCable2Home.
Información relativa a las características de QoS del anfitrión de IPCable2Home	Características de QoS que se reciben del operador del sistema de cable e información del perfil de QoS que se recibe de los anfitriones de IPCable2Home a través de mensajes BP_Init.

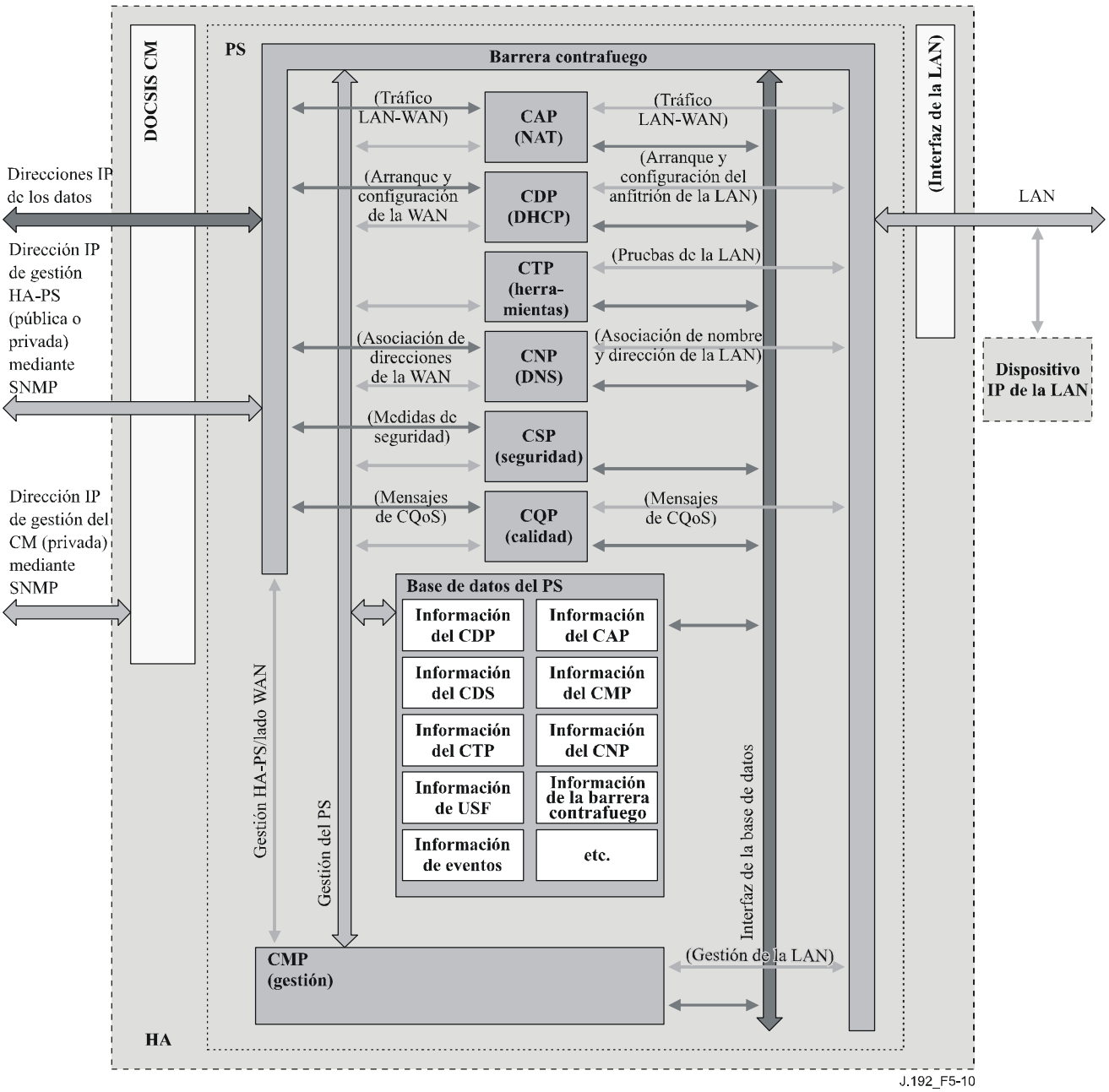


Figura 5-10/J.192 – Ejemplo detallado de implementación de la base de datos del PS

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 service*) 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 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 (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 CableModem para habilitar servicios adicionales, e incorpora diversas capacidades similares a las que existen en un sistema de configuración de IPCable2Home.

A los efectos de la configuración, el PS puede funcionar en cualquiera de dos modos de configuración:

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

Si el PS no se configura para que funcione en cualquiera de estos dos modos, se supondrá que no está disponible el soporte administrativo, 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 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) por HTTP, a fin de proporcionar la descarga asegurada de los ficheros de configuración del PS y de la barrera contrafuego.

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 5-11 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.

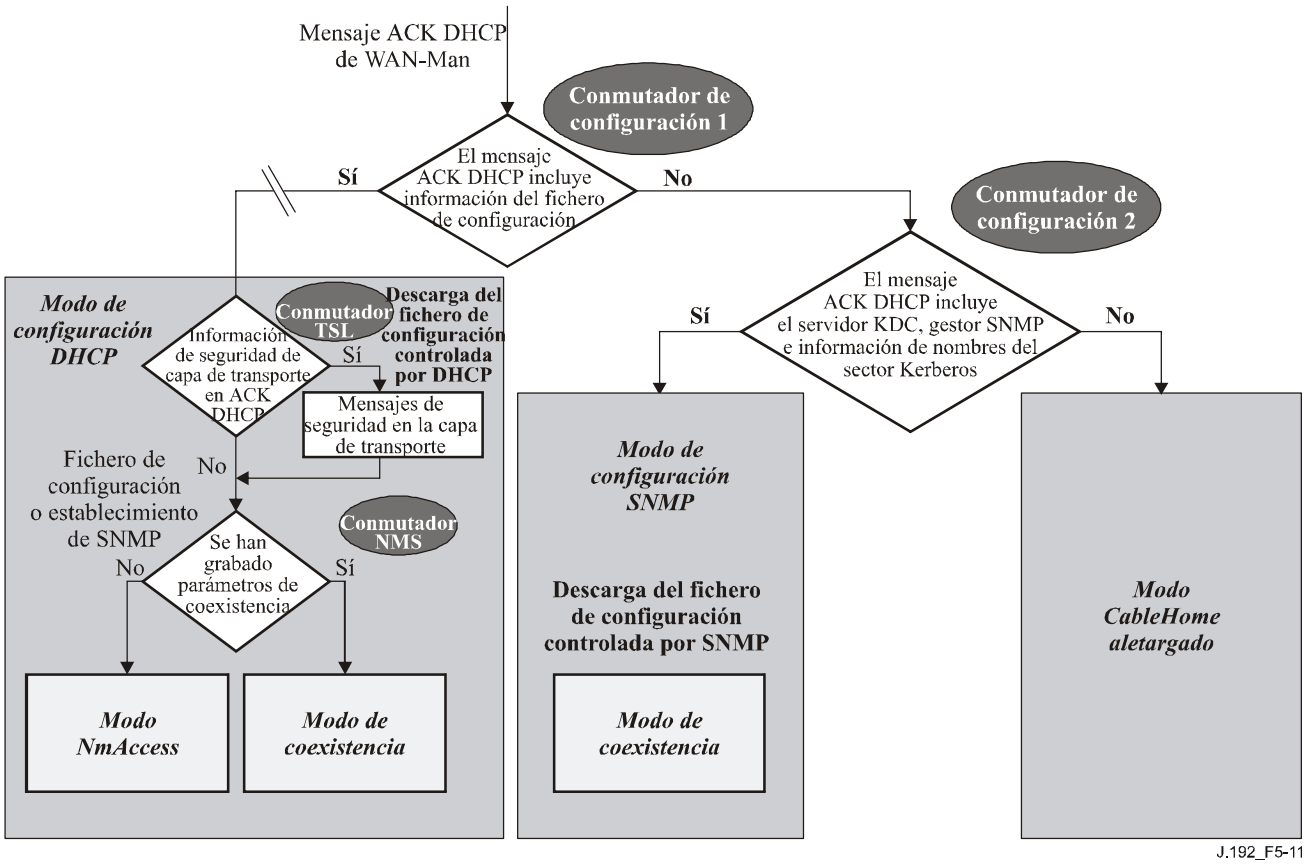


Figura 5-11/J.192 – Modos de funcionamiento del PS

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

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

Modo	Capacidad directamente afectada	Infraestructura deseada
Modo de configuración SNMP	Descarga del fichero de configuración	Infraestructura de configuración de CableModem más IPCablecom
Modo de configuración DHCP	Descarga del fichero de configuración	Infraestructuras de CableModem con soporte de IPCable2Home
Modo de configuración DHCP: con TLS/HTTP	Descarga segura del fichero de configuración	Infraestructuras de CableModem con soporte de IPCable2Home y TLS
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 CableModem más IPCablecom (SNMPv3) con soporte de IPCable2Home
Modo de IPCable2Home aletargado	Configuración y gestión	Sin soporte de IPCable2Home

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 particular 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 podrían 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 acceso (lectura/escritura) de la interfaz de gestión a las funciones del PS NO DEBE permitirse a través del mecanismo que se emplea para configurar las funciones distintas de IPCable2Home.

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), determinar los dispositivos IP de LAN y las aplicaciones que ofrecen, verificar a distancia la conectividad entre los dispositivos de PS y de IP de LAN, proporcionar las políticas de calidad de servicio a los BP en apoyo de la QoS con prioridad entre los anfitriones de IPCable2Home 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.

Más adelante se relacionan las diferencias entre las herramientas de gestión determinadas en la Rec. UIT-T J.191 y las correspondientes a la presente Recomendación. Por consecuencia, en esta Recomendación se añade:

- el requisito necesario para que el PS pueda aceptar gestión SNMP de cualquier interfaz LAN;
- el requisito para que tanto el PS como el BP acepten mensajes PS-BP para el intercambio de las prioridades de QoS;
- el requisito para que el BP implemente un perfil de dispositivo con formato XML;
- los siguientes objetos de MIB al PS:
  - los necesarios para soportar la calidad de servicio con prioridades en la red LAN,
  - los necesarios para soportar una funcionalidad reforzada de la barrera contrafuego,
  - los necesarios para permitir que el operador del sistema de cable determine los atributos de los anfitriones de IPCable2Home.

6.1.1 Objetivos

Los objetivos de las herramientas de gestión de IPCable2Home son:

- Proporcionar un medio para que el operador del sistema de cable determine los dispositivos IP de LAN.
- Dotar a los operadores de sistemas de cable de la visibilidad hacia los dispositivos IP de LAN.
- Dotar a los operadores de sistemas de cable de la visibilidad hacia las aplicaciones en los anfitriones de IPCable2Home.
- Determinar un método para transferir las prioridades de QoS a las aplicaciones en los anfitriones de IPCable2Home.

- Determinar 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 correspondientes al entorno de gestión de la red IPCable2Home son:

- Los dispositivos conformes a IPCable2Home implementan el conjunto de protocolos (IPv4) del protocolo Internet.
- Los anfitriones de IPCable2Home implementan un perfil de dispositivo y un perfil de calidad de servicio en formato XML.
- 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.
- El programa de utilidad PING proporciona la funcionalidad suficiente que permite que el operador de cable obtenga 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 proporciona la orientación 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
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.
Mgmt 5	El elemento PS debe ser capaz de comunicarse con los anfitriones de IPCable2Home 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 las aplicaciones del anfitrión de IPCable2Home.
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);
4) sistema de gestión de red SNMP (NMS) que forma parte de la red de cable, y
5) perfil del dispositivo en formato XML que se implementa para cada anfitrión de IPCable2Home (elemento lógico BP).

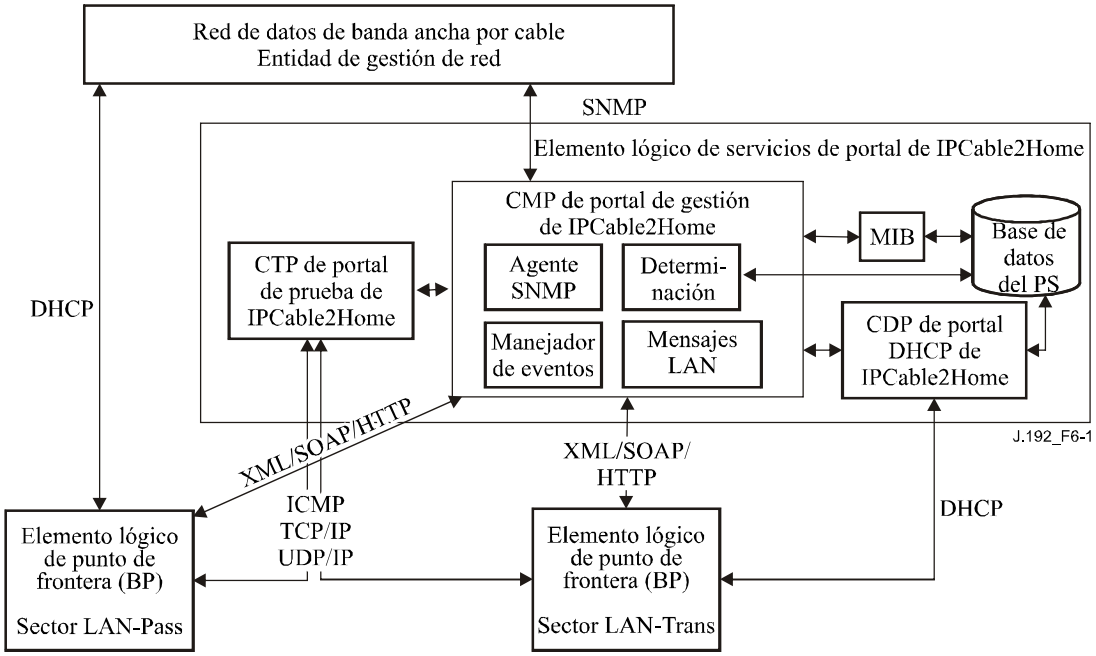


Figura 6-1/J.192 – Arquitectura de gestión de IPCable2Home

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. El operador del sistema de cable accede a los atributos del anfitrión y 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 anfitriones de IPCable2Home con las políticas de QoS (en forma de prioridades de QoS), utilizando el PS como un apoderado.

Cuando el elemento lógico BP en cada anfitrión IPCable2Home recibe el mensaje DHCP ACKNOWLEDGE (DHCPACK) [RFC 2131] de su servidor DHCP, inicia la comunicación con el PS a través de la interfaz de mensajería de la LAN. Estos mensajes, con formato del protocolo simple de acceso a objetos (SOAP, *simple object access protocol*) en el transporte del protocolo de transferencia de hipertexto (HTTP, *hypertext transfer protocol*), se envían para informar al PS con relación a la información de los atributos del dispositivo (perfil de dispositivo) y de una lista de aplicaciones (perfil de QoS) implementadas en el anfitrión de IPCable2Home. Cuando el PS recibe el perfil del dispositivo y el perfil de QoS:

- Almacena la información del perfil del dispositivo del BP en un cuadro MIB de perfil del dispositivo del BP (cabhPsDevBpProfileTable).

  El perfil del dispositivo del BP permite al operador del cable determinar la información relativa a los anfitriones de IPCable2Home en el sector LAN-Pass, y los correspondientes al sector LAN-Trans que se añaden a la información obtenida mediante mensajes DHCP entre el PS y el BP del sector LAN-Trans.
- Almacena la información del perfil de QoS del BP en un cuadro MIB de prioridades de la aplicación del BP (cabhPriorityQosBpTable).

  El perfil de QoS del BP permite al operador del sistema de cable determinar las aplicaciones implementadas en los anfitriones de IPCable2Home. Estas aplicaciones se identifican mediante el número de puerto "bien conocido" de la autoridad de asignación de números Internet (IANA, *Internet assigned number authority*) con el que se han registrado.

Si el operador del sistema de cable configuró el PS con las políticas de QoS rellenando el cuadro maestro de prioridades de las aplicaciones (cabhPriorityQosMasterTable), el PS también proporcionará al BP las prioridades de QoS a partir del cuadro, a través de la misma interfaz de mensajes de la LAN. Ese procedimiento se describe en 10.3.2.4.2, "Intercambio de información de la LAN".

Además, el NMS puede 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 5.1.3.1.1.

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], y 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 acepta 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 6.3.3 se dan mayores detalles.

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 contrafuego.
- Permitir la prueba de la conectividad a distancia entre la pasarela residencial de CableHome 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 la visión de la información del dispositivo IP de LAN que se obtuvo a través del portal DHCP de IPCable2Home (CDP).
- Facilitar el acceso del operador del sistema de cable a los atributos de los anfitriones de IPCable2Home y sus aplicaciones, obtenidos mediante el proceso de determinación de IPCable2Home.
- Soportar el intercambio de atributos de los dispositivos o aparatos, la relación de aplicaciones y las prioridades de QoS de las aplicaciones entre la pasarela residencial de IPCable2Home y los dispositivos del anfitrión de IPCable2Home.
- 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

Estas directrices 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
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	Los anfitriones de IPCable2Home en la red doméstica deberían tener la capacidad de recuperación tras una interrupción de corriente, y regresar a un estado de funcionamiento razonable cuando se normaliza la energía.
CMP 4	Los dispositivos de la red doméstica deben instalarse y configurarse fácilmente para que funcionen como cualquier otro electrodoméstico.
CMP 5	El PS y los dispositivos IP de LAN deben aceptar un protocolo para la determinación de los dispositivos IP de LAN que se conecten a la red LAN doméstica.
CMP 6	El PS proporcionará al operador del sistema de cable, cuando así se solicite, la información relativa a los dispositivos que se añaden a la LAN doméstica.

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

Referencia	Directrices
CMP 7	El PS y el BP deben aceptar un protocolo para el intercambio de los atributos y las aplicaciones del dispositivo del anfitrión de IPCable2Home implementados por los dispositivos del mismo anfitrión, y de las prioridades de QoS para esas aplicaciones.
CMP 8	El PS deberá proporcionar al operador del sistema de cable, cuando así se solicite, la información relativa a los atributos y las aplicaciones del dispositivo del anfitrión de IPCable2Home implementados por los dispositivos del mismo anfitrión.
CMP 9	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 10	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.
- Permitir al gestor la determinación a distancia de los dispositivos conectados a la red LAN doméstica y a las aplicaciones que utilizan.
- Procesar y registrar históricamente los mensajes de eventos.

El CMP consta de las siguientes cuatro 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*

   El CMP envía informes de eventos conforme a los valores del cuadro docsDevEvent. En el anexo B se presenta la relación de los eventos soportados.

3) *Función de determinación*

   El CMP, a través de su funcionalidad de determinación, obtiene la información relativa a cada uno de los dispositivos del anfitrión de IPCable2Home y sus aplicaciones. 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 PSDev (véase E.4) y de la MIB de QoS (véase E.7).

4) *Función de mensajería LAN*

   El CMP intercambia parámetros de QoS y atributos del perfil del dispositivo en formato XML con los anfitriones de IPCable2Home a través de la red LAN, utilizando el protocolo simple de acceso a objetos.

Estas funciones se describen en 6.3.3.1 a 6.3.3.4.

6.3.3.1 Función de agente SNMP del CMP

6.3.3.1.1 Objetivos de la función del 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 (LAN) del PS.
- 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.
- Apegarse a 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 al funcionamiento del agente SNMP

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

Cuadro 6-3/J.192 – Directrices para el diseño del sistema relativo a la funcionalidad del agente SNMP

Referencia	Directrices
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 funcionalidad del agente SNMP

La funcionalidad del 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 funcionalidad 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.

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 2576], 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 6-4 se presentan las definiciones de los términos específicos al CMP.

Cuadro 6-4/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 [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 contrafuego, 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 sus 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.

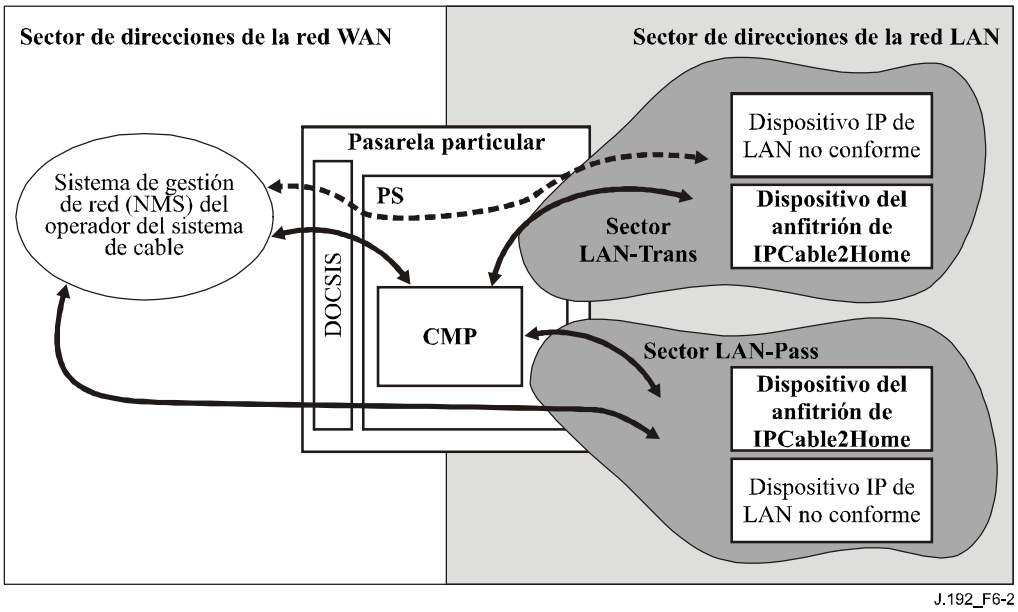


Figura 6-2/J.192 – Interfaces para los mensajes de gestión de CableHome

El CMP es principalmente una entidad a la que se accede por la red WAN (NMS) y que se controla por la misma red, aunque también acepta 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 podrá solicitar al CMP que envíe informes al NMS de la red por cable con relación a los ficheros de registro histórico del sistema de transferencia o de los eventos, 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.

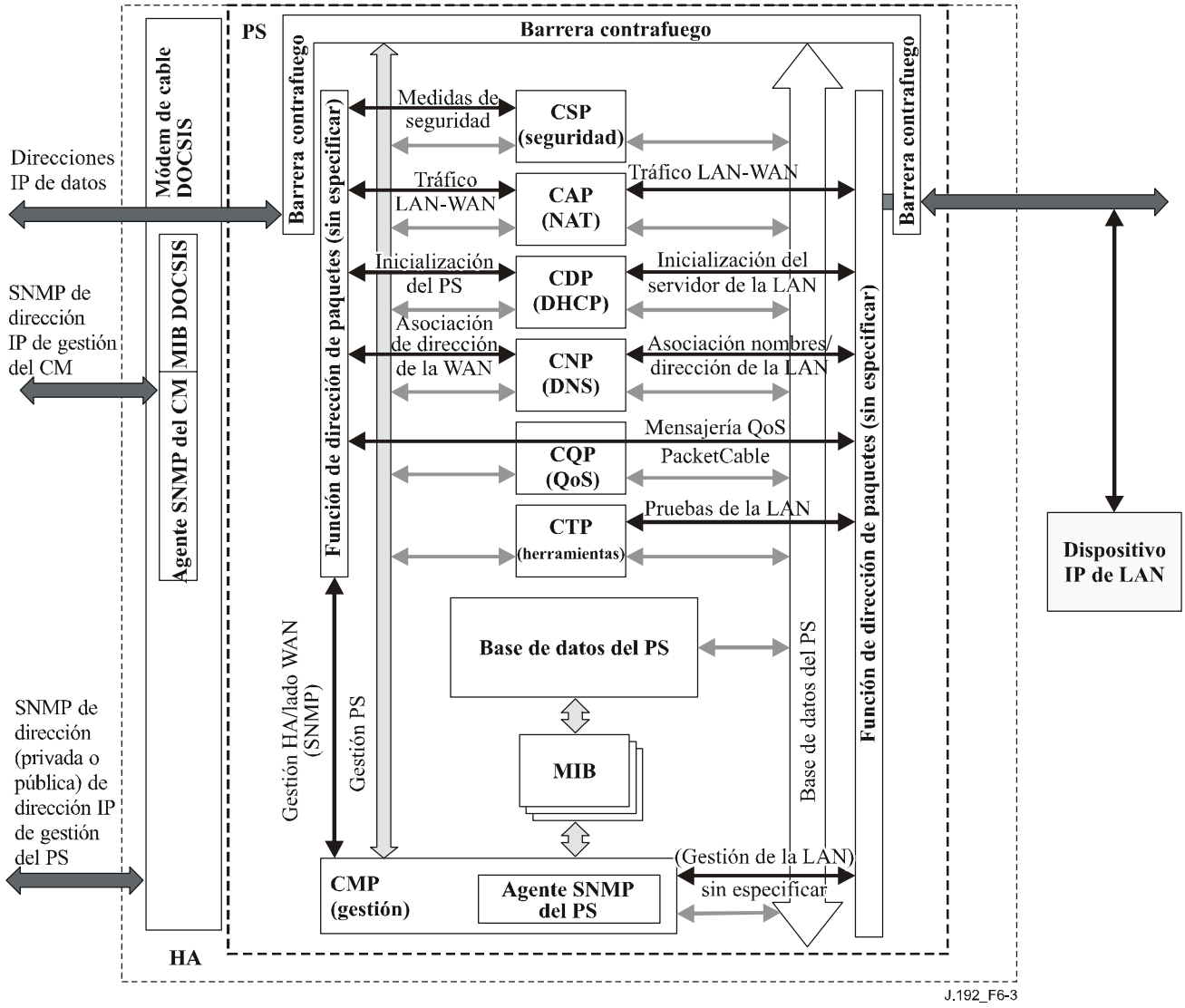


Figura 6-3/J.192 – Diagramas de bloque del PS

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 de CableHome de dos maneras. De un lado, accediendo directamente a los anfitriones de CableHome 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 de CableHome, a través de SNMP.

6.3.3.1.4 Requisitos de la funcionalidad del 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".

El agente SNMP en el PS DEBE recibir y procesar únicamente mensajes SNMP dirigidos a su dirección IP de la WAN-Man o a su dirección del encaminador del servidor LAN (cabhCdpServerRouter), cuando se encuentra funcionando en el modo de configuración DHCP o SNMP (cabhPsDevProvMode = dhcpmode(1) o snmpmode(2)).

Si el PS no ha sido aún configurado, el agente SNMP en el PS DEBE recibir y procesar todos los mensajes SNMP dirigidos a la dirección del encaminador del servidor de la red LAN del PS (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 reside 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) y tipos de mensajes de indicación de tiempo y de respuesta de indicación de tiempo de ICMP (tipo 13 y tipo 14) 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 6-5:

Cuadro 6-5/J.192 – Formato de los campos sysDescr

Formato de cada uno de los campos	Informar
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:

texto<<HW_REV: 5.2, VENDOR: X; BOOTR: 1.4; SW_REV: 2.2; MODEL: X>>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 contrafuego 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 las reactivaciones y los ciclos de energía del dispositivo.

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

El objeto sysContact del grupo de sistema MIB-2 [RFC 3418] DEBE implementarse y mantenerse durante las reactivaciones y los ciclos de energía eléctrica 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 las reactivaciones y los ciclos de energía eléctrica del dispositivo.

El objeto sysServices del grupo de sistema MIB-2 [RFC 3418] DEBE implementarse y mantenerse durante las reactivaciones y los ciclos de energía eléctrica del dispositivo.

El objeto sysName del grupo del sistema de la MIB-2 [RFC 3418] DEBE implementarse y mantenerse durante las reactivaciones y los ciclos de energía eléctrica 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 de 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 aceptar 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 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 2576]

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 y en sus subcláusulas 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 y en sus subcláusulas 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 2576], [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 2576]. 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:

a) 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:

- Todos los paquetes SNMP se descartan.
- 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.

b) 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 TLV38), 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.

c) 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 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 CableHome, sin tener en cuenta la interfaz 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 2576].
- 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 CableHome, sin tener en cuenta la interfaz 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 ACK DHCP (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 claves 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 CableHome 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 CableHome 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 2576]. 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].

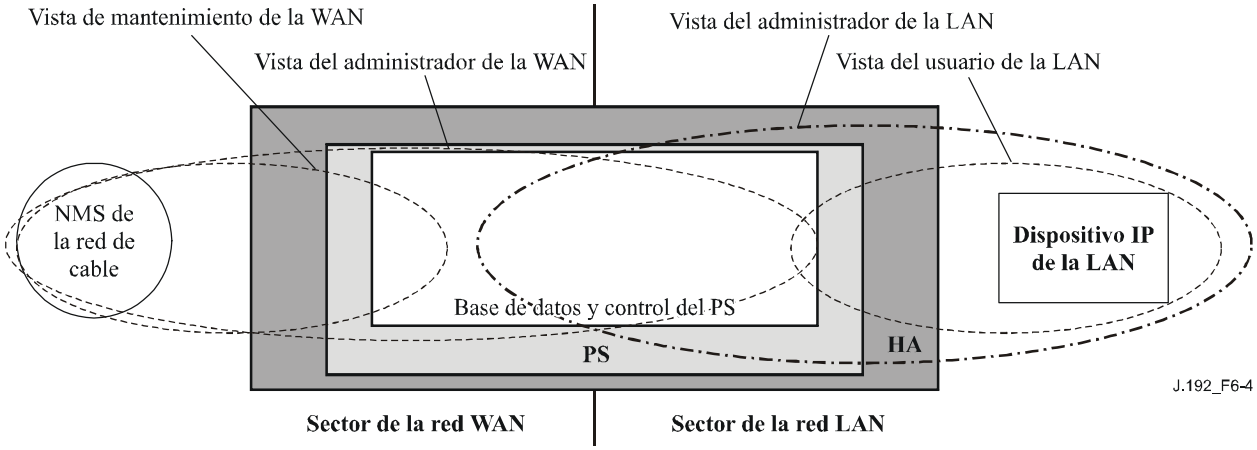


Figura 6-4/J.192 – Vistas de gestión

Los parámetros gestionados que define CableHome 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 CableHome.

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

El control de acceso SNMP, conforme a [RFC 3415], se utilizará para el control del acceso a los objetos de la MIB específicos de CableHome, sin tener en cuenta la interfaz a través de la que se recibe la petición. El modelo de control de acceso basado en vistas (VACM) [RFC 3415] determina un conjunto de servicios que pueden utilizarse para la verificación de los derechos de acceso. Los grupos VACM determinan 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 CableHome 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 es responsable de la seguridad de los mensajes de gestión. Véase la cláusula 11 para obtener 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 indicaciones 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	'CHAdministrator'
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 los campos TLV con las filas del cuadro SNMPv3 creado

En esta cláusula se dan los pormenores de cómo se logra la correspondencia del elemento del fichero de configuración *receptor de notificación del SNMP* (tipo 38 de TLV) con los cuadros funcionales de SNMPv3. Véase 7.4.4.1.9, "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 6-6, "snmpNotifyTable", a 6-15, "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 6-6/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 6-7/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, o 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 6-8/J.192 – snmpTargetAddrExtTable

[RFC 2576] 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 6-9/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 – La correspondencia de los tipos de protocolo SNMP al 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 6-10/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	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 – 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 6-11/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 6-12/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 6-13/J.192 – snmpCommunityTable

[RFC 2576] SNMP-COMMUNITY-MIB	Primera 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 con el valor recién determinado.

Cuadro 6-14/J.192 – usmUserTable

[RFC 3414] SNMP-USER-BASED-SM-MIB	Primera fila
Nombre de columna (* = Parte del índice)	Valor de columna
* usmUserEngineID	0
* usmUserName	"@PSconfig" Cuando se crean otras filas, ésta se sustituye con el campo <Security Name> desde el elemento TLV.
usmUserSecurityName	"@PSconfig" Cuando se crean otras filas, ésta se sustituye con el campo <Security Name> desde el elemento TLV.
usmUserCloneFrom	<don't care> – no es posible clonar esta fila
usmUserAuthProtocol	Ninguna. Cuando se crean otras filas, ésta se sustituye con 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 con 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 6-15/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 de "se conserva" 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:

- Interfaces Group MIB [RFC 2863];
- DOCSIS Cable Device MIB [RFC 2669];
- MIB de definición de CableLabs (véase E.6);
- MIB PSDev de CableHome (véase E.4);
- MIB de CAP de CableHome (véase E.1);
- MIB de CDP de CableHome (véase E.2);
- MIB de CTP de CableHome (véase E.3);
- MIB de seguridad de CableHome (véase E.5);
- MIB de QoS de CableHome (véase E.7);
- [draft-ietf-ipcdn-bpiplus-mib-05];
- IP MIB (SNMPv2) [RFC 2011];
- UDP MIB (SNMPv2) [RFC 2013];
- Diffie-Hellman USM Key [RFC 2786];
- INET Address MIB [RFC 3291];
- DOCS IF MIB [RFC 2670];
- IANA ifType MIB [IANAType].

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.

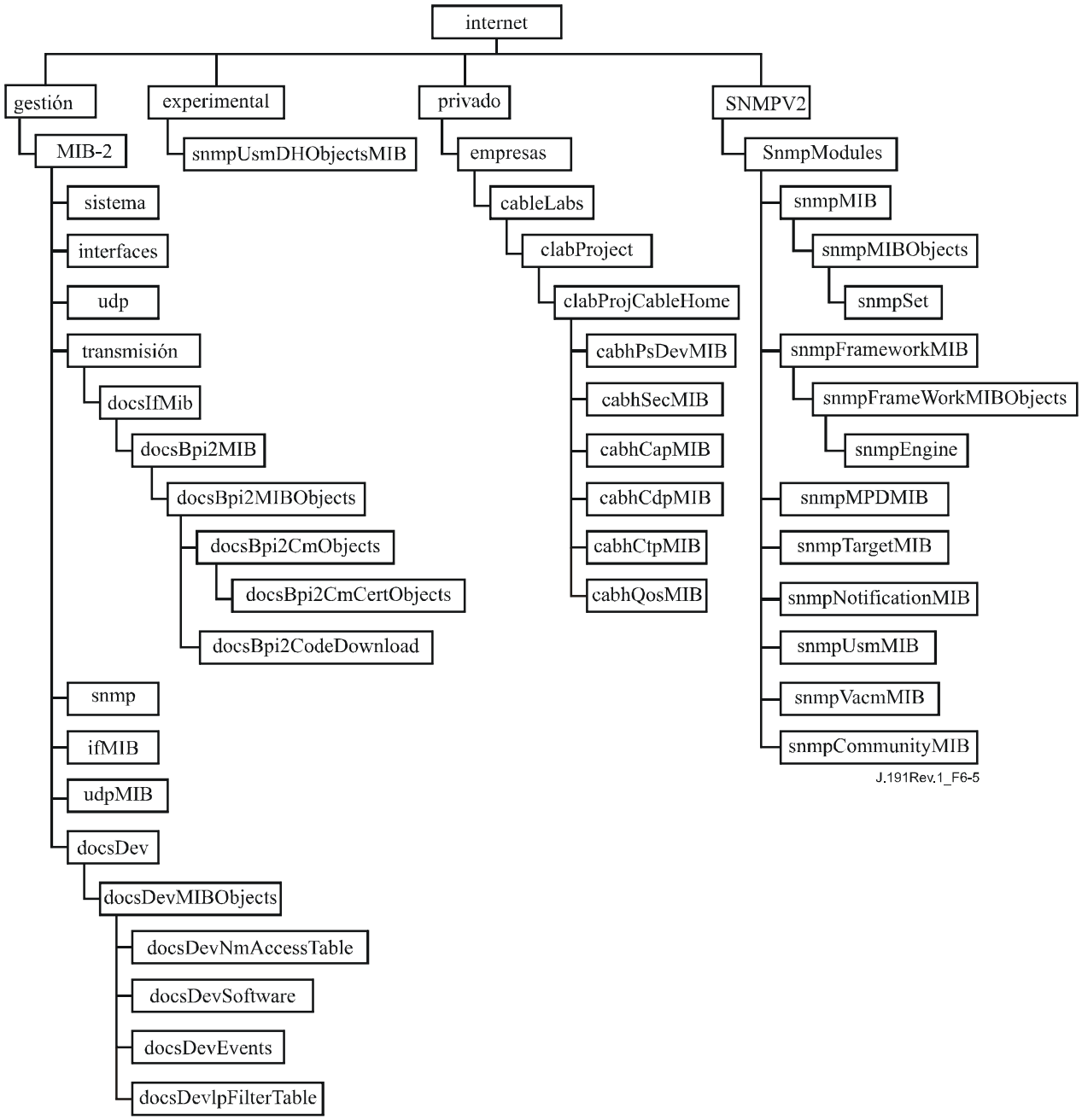


Figura 6-5/J.192 – Jerarquía de la MIB de IPCable2Home

6.3.3.1.4.8 MIB del grupo de interfaces

La MIB del grupo de interfaces [RFC 2863] representa una herramienta fundamental 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:

DEBE existir 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.

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

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

Las interfaces ifTable del PS DEBEN numerarse como se indica en el cuadro 6-16.

Cuadro 6-16/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
255	Interfaz de LAN agregada

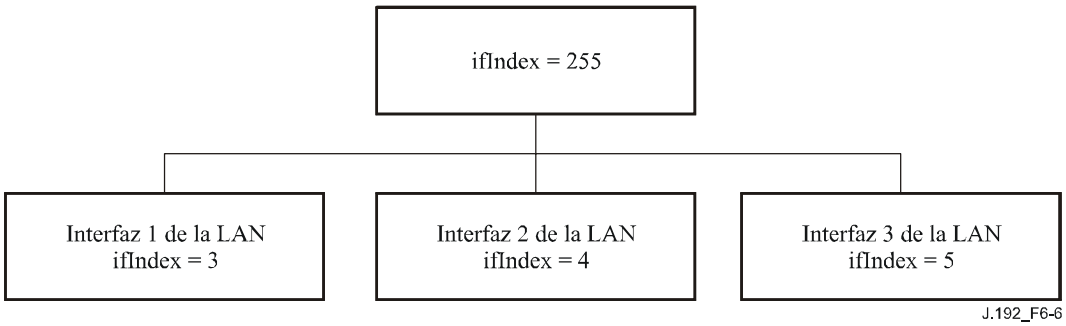
Si un determinado ifAdminStatus = down da la interfaz, esa interfaz NO DEBE aceptar o retransmitir ningún tráfico. El objeto ifAdminStatus correspondiente al valor 255 de ifIndex DEBE proporcionar el control administrativo de todas las interfaces de la LAN y DEBE implementarse como lectura-escritura.

El PS DEBE asignar el valor other(1) a las anotaciones ifTable [RFC 2233] ifType correspondientes al valor 255 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.

Los contadores ifTable de las interfaces de la WAN relativas a los valores 1 y 2 de ifIndex DEBEN compartirse entre las dos interfaces. Los contadores ifTable relativos al valor 255 de ifIndex PODRÁN implementarse.

El grupo de pila de interfaces (ifStack) de [RFC 2233] DEBE implementarse para identificar las relaciones entre la interfaz de "interfaces de la LAN agregadas" de capa superior y las subinterfaces de la LAN de capa inferior. En la figura 6-6 se ilustra la utilización del grupo ifStack en el caso de un PS con tres interfaces de LAN.



Iimplementación de ifStack para este ejemplo:

ifStackHigherLayer	ifStackLowerLayer
255	3
255	4
255	5

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

6.3.3.1.4.9 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 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 6-17:

Cuadro 6-17/J.192 – ipNetToMediaTable del PS

ipNetToMediaAddress	ipNetToMediaPhysAddress	ipNetToMediaIfIndex
Dirección IP de WAN-Man	Dirección de hardware de WAN-Man	1
Dirección IP de WAN-Data	Dirección de hardware de WAN-Data	2
Dirección IP del servidor de DHCP	Cadena de octetos con longitud cero	255
Dirección IP del servidor DNS	Cadena de octetos con longitud cero	255
Dirección IP del encaminador del servidor	Cadena de octetos con longitud cero	255

6.3.3.2 Función de informes de eventos del CMP

El CMP debe soportar el manejo y el informe 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.

Informes 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 de 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 relativo a la funcionalidad de notificación de eventos

Las directrices de diseño del sistema, que se relacionan en el cuadro 6-18, dan la orientación para la especificación de la función de notificación de eventos del CMP.

Cuadro 6-18/J.192 – Directrices de diseño del sistema relativo a la funcionalidad de la 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 funcionalidad relativa a la notificación de eventos

La notificación de eventos es un medio que 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 6-19) 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 funcionalidad relativa a la 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 de 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 trap o inform SNMP), o enviarse como un mensaje de eventos SYSLOG al servidor SYSLOG cuya dirección IP se transfirió en la opción 7 de DHCP del mensaje DHCP OFFER recibido del servidor DHCP de la cabecera a través de la interfaz 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 de 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 = SYSLOG only
- 0x40 = trap only
- 0x60 = (trap + SYSLOG) only

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 6-19, 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 entradas.

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 reactivación 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 descrita en [RFC 3411]. El PS DEBE soportar 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 las trampas del SNMP específicas del fabricante, la declaración de OBJECTS de la definición de la trampa privada DEBERÍA contener como mínimo los objetos indicados a continuación:

- EvLevel;
- EvIdText;
- umbral de 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 Prioridad de los eventos

La norma [RFC 2669] define 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 '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.

El cuadro 6-19 muestra 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 6-19, "Tipos de notificación por defecto de las prioridades de los 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 entradas no volátiles.

Cuadro 6-19/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	CableHome
3) Crítico	Sí	No	No	No	CableHome
4) Error	Sí	Sí	Sí	No	CableHome
5) F	Sí	Sí	Sí	No	CableHome
6) Notificación	No	Sí	Sí	Sí	CableHome
7) Informativo	No	No	No	No	CableHome 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 6-19.

6.3.3.2.4.7 Eventos normales

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 del anexo B, "Formato y contenido de los eventos, SYSLOG y trampas SNMP", se describen los eventos correspondientes a las actualizaciones del software de los servicios de portal, en tres categorías: inicialización de la 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 5.1.3.1, "Servicios de portal (PS)", NO DEBE generar eventos con las categorías indicadas en el cuadro B.1, "Eventos definidos para IPCable2Home", como eventos de "inicialización 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).

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 a los atributos del dispositivo del anfitrión de IPCable2Home y de la pasarela residencial de IPCable2Home.
- Permitir que los operadores del sistema de cable dispongan de la visibilidad necesaria a las aplicaciones implementadas en los dispositivos del anfitrión de IPCable2Home.
- Coexistencia e interoperatividad entre el PS, los anfitriones de IPCable2Home y los dispositivos IP de LAN que NO son conformes a la presente Recomendación.

NOTA – Los objetivos de la función de determinación NO impiden la utilización de otros métodos de determinación, protocolos, etc., en la red LAN sino que tienen la intención exclusiva de especificar los requisitos de los dispositivos conformes. No obstante, los dispositivos del anfitrión de IPCable2Home NO DEBEN interferir con los dispositivos IP de LAN que no pertenecen a IPCable2Home y que funcionan correctamente.

Hipótesis

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

- Los dispositivos del anfitrión de IPCable2Home, los dispositivos IP de LAN, y los dispositivos de la pasarela residencial de IPCable2Home aplican el conjunto de protocolos de Internet (IPv4).

- Los anfitriones de IPCable2Home aplican un perfil de dispositivo con formato XML como se describe en 6.5.3.1.3 y un perfil de QoS con formato XML como se describe en 10.3.2.4.2.1.

6.3.3.3.2 Directrices de diseño del sistema relativo a la funcionalidad de la determinación

Las directrices de diseño del sistema relacionadas en el cuadro 6-20 proporcionan la orientación para la evolución de la especificación de la función de determinación del CMP.

Cuadro 6-20/J.192 – Directrices de diseño del sistema relativo a la determinación del PS

Referencia	Directrices
Determinación 1	El PS y el BP deben soportar un protocolo para la determinación de los dispositivos del anfitrión de IPCable2Home conectados a la red LAN doméstica.
Determinación 2	El PS debe proporcionar al operador del sistema de cable, cuando así se solicite, información relativa a los dispositivos agregados a la red LAN doméstica.
Determinación 3	El PS debe proporcionar al operador del sistema de cable, cuando así se solicite, información relativa a las aplicaciones que se implementan en los dispositivos del anfitrión de IPCable2Home.
Determinación 4	El intercambio de mensajes del protocolo de determinación en la red LAN doméstica no debe degradar sensiblemente la calidad de funcionamiento de la red LAN doméstica.
Determinación 5	Los mensajes del protocolo de determinación de la red LAN doméstica no deberán difundirse a la red WAN.

6.3.3.3.3 Descripción del sistema relativo a la funcionalidad de la 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 y las aplicaciones disponibles en la red LAN del abonado.

La función de determinación especifica que el PS debe fungir como depósito central de información relativa a los dispositivos y las aplicaciones disponibles en la red LAN del abonado. Los elementos lógicos específicos del BP proporcionan información particular del dispositivo relativa al dispositivo en el que residen, así como una lista de las aplicaciones implementadas en el dispositivo en el que residen.

La función de determinación consta de dos etapas:

1) El PS se entera de cada una de las direcciones IP y MAC del anfitrión de IPCable2Home. El PS obtiene esta información directamente de los dispositivos LAN-Trans cuando recibe y responde a las peticiones de DISCOVER DHCP. Véase 7.3.3.1.4, "Requisitos del CDS". Es necesario que el PS reciba esta información de los dispositivos LAN-Pass para que pueda soportar la funcionalidad USFS (véase 8.3.3.4, "Resumen de la conmutación de retransmisión selectiva en sentido ascendente"), aunque en la presente Recomendación no se indica cómo se debe efectuar.

2) El PS obtiene información relativa a los atributos y las aplicaciones del dispositivo de cada BP. Es necesario que cada BP envíe sus perfiles de dispositivo y de QoS al PS. Esto se realiza a través del modelo "BP iniciado", en el que el BP envía la información al CMP. El BP puede iniciar esta transferencia de información en cualquier momento pero debe realizarla cada vez que obtiene o actualiza su licencia de dirección IP. El PS recibe esta información y la almacena, poniéndola a disposición del operador del sistema de cable a través de la MIB PSDev (véase E.4).

El PS mantiene información relativa al dispositivo de la pasarela residencial de IPCable2Home, en la base de datos del PS, de manera análoga al perfil del dispositivo del BP. Esta información, que permite que el operador del sistema de cable determine los atributos de la pasarela residencial de IPCable2Home, está disponible mediante SNMP a través de los objetos sysDescr, sysName, y sysLocation de la MIB-2 [RFC 1213] y a través del grupo de perfiles de los dispositivos del PS de la MIB PSDev (véase E.4).

6.3.3.3.4 Requisitos de la función de determinación

El PS DEBE almacenar en la base de datos del PS, la información del perfil del dispositivo (véase 6.5.3.1, "Perfil del dispositivo del BP") que se recibe en el mensaje BP_Init de cada BP, y ponerla a disposición a través del cuadro (cabhPsDevBpProfileTable) del perfil del dispositivo del anfitrión IPCable2Home/BP de la MIB del dispositivo del PS (véase E.4). Además, es necesario que el PS almacene la información de la aplicación recibida en el perfil de QoS resultante del proceso de determinación de la información de esta aplicación. Véase 10.3.2.4.2.

El PS DEBE almacenar sus atributos de perfil de dispositivo, relacionados más adelante, en la base de datos del PS y ponerlos a disposición de la entidad SNMP a través del grupo de perfiles de la MIB del dispositivo del PS (véase E.4):

- tipo de dispositivo (cabhPsDevPsDeviceType);
- localizador universal de recursos del fabricante (cabhPsDevPsManufacturerUrl);
- localizador universal de recursos del modelo del dispositivo (cabhPsDevPsModelUrl);
- código universal de producto del dispositivo (cabhPsDevPsModelUpc).

6.3.3.4 Función de mensajes de la LAN del CMP

La mensajería de la red LAN se refiere al intercambio de mensajes entre el PS y un BP. Aunque los sistemas SNMP son frecuentes en las redes de datos del operador del sistema de cable para fines de supervisión y configuración de los sistemas de terminación del módem de cable (CMTS, *cable modem termination system*) y de los módems de cable (CM, *cable modem*), el SNMP no es corriente entre los dispositivos que conectan los abonados del servicio de datos por cable a sus redes LAN domésticas. Por consecuencia, IPCable2Home define un protocolo de mensajería dentro de la vivienda para satisfacer las necesidades de los operadores de cable a fin de poder soportar a los abonados al servicio de datos y mantener la compatibilidad con los protocolos de mensajería que se implementan por lo general en los dispositivos de comunicaciones de datos basados en la red LAN. En esta cláusula se describe la solución de la mensajería de la red LAN.

Es esencial observar que un BP podría residir en un dominio LAN-Trans o en un dominio LAN-Pass. Cuando reside en el dominio LAN-Trans puede direccionar paquetes fácilmente hacia el PS, ya que la dirección del encaminador del servidor del PS (cabhCdpServerRouter) es la pasarela por defecto del BP de LAN-Trans, transferida al BP en la opción código 3 del DHCP. No obstante, el BP de LAN-Pass no tiene un conocimiento real de la dirección IP del encaminador del servidor del PS. Los mensajes de LAN enviados al PS desde el BP de LAN-Trans pueden utilizar la dirección IP del encaminador del servidor del PS como la dirección IP de destino. Será necesario definir otro método para el BP de LAN-Pass.

Una manera de garantizar la mensajería de BP a PS de LAN-Pass, y el método que se adopte para tal efecto, es definir en el PS una dirección IP fija "bien conocida" que será utilizada por el BP de LAN-Pass como destino. Ya que el PS es un puente de capa 2 para los dispositivos de LAN-Pass, la función USFS será la encargada de capturar los mensajes enviados por un BP de LAN-Pass a la dirección IP de destino bien conocida. Los paquetes dirigidos a la dirección IP bien conocida del PS que sean capturados por la función USFS serán procesados por el PS. La dirección 192.168.0.1 se define como la dirección IP del PS "bien conocida" que deben utilizar los BP de LAN-Pass como dirección IP de destino para los mensajes de LAN entre el BP y el PS. No se permitirá que esta dirección IP fija bien conocida del PS se asigne mediante el CDS a los dispositivos de LAN-Trans.

La dirección IP bien conocida del PS que se definió anteriormente tiene el mismo valor que el valor *por defecto* de cabhCdpServerRouter, pero la dirección IP bien conocida del PS definida para la mensajería de LAN es fija y no podrá modificarse, mientras que el valor de cabhCdpServerRouter pueda modificarse mediante el fichero de configuración del PS o de la instrucción de establecimiento de SNMP. Se exige que el PS responda a ambas direcciones, si son distintas.

Ya que un BP podría residir en cualquier dominio de direcciones, debe soportar el método de direccionamiento definido para LAN-Trans, así como el método definido para los BP de LAN-Pass. Es decir, los BP deben soportar ambos métodos de direccionamiento LAN-Trans a PS y LAN-Pass a PS, y el PS debe aceptar los mensajes destinados a la dirección IP fija "bien conocida" del PS o a la dirección del encaminador del servidor del PS (que podrían ser iguales o distintas). El BP utilizará la presencia o la ausencia del valor "CableHome1.1LAN-Trans" de la subopción 101 de la opción código 43 del DHCP en el mensaje ACK DHCP que recibió de su servidor DHCP para determinar el método de direccionamiento que debe emplear. Si este valor está presente en la subopción 101 antes referida el BP deberá enviar sus mensajes BP_Init a su pasarela por defecto (del BP), es decir, la dirección del encaminador del servidor del PS. Si por el contrario el valor no está presente en el mensaje ACK DHCP el BP debe enviar sus mensajes BP_Init a la dirección 192.168.0.1.

El PS contestará a un BP utilizando como dirección de destino la dirección BP que recibió como una dirección IP del origen, es decir, el PS contesta transmitiendo a la dirección de la que recibió el mensaje BP-iniciado. Este mensaje aparece ante un BP de LAN-Pass como originado desde un dispositivo en el dominio LANS-Trans.

En la figura 6-7 se resumen los requisitos de direccionamiento del BP al PS de un elemento lógico de BP conforme.

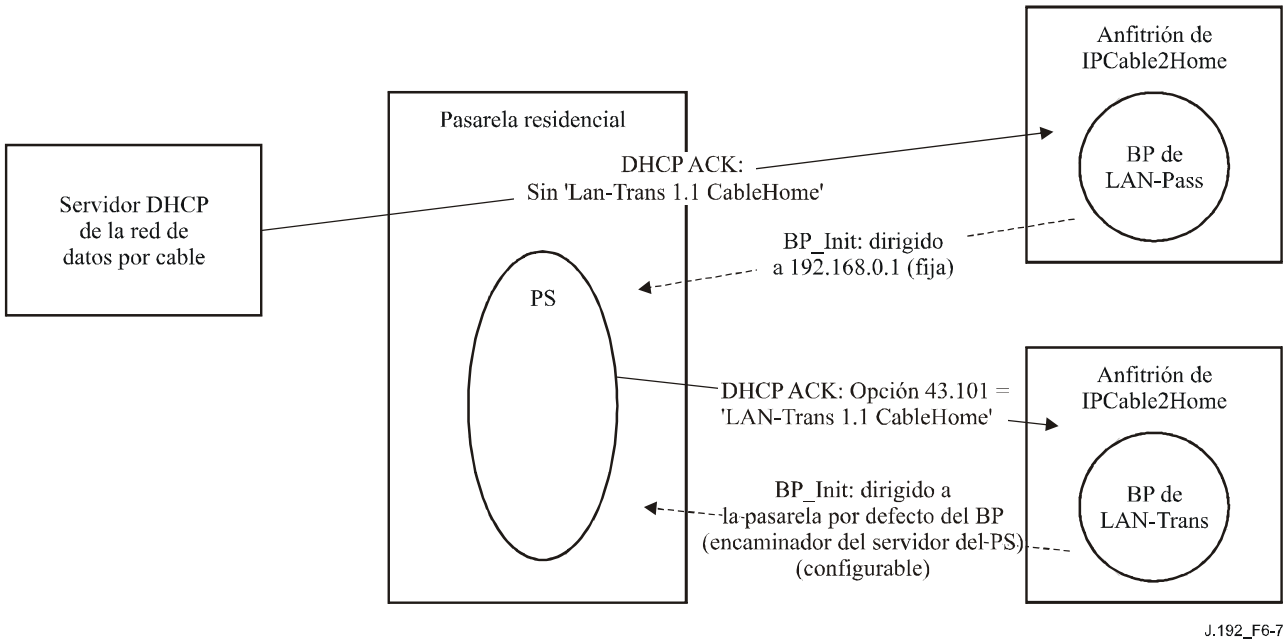


Figura 6-7/J.192 – Direccionamiento del mensaje BP_Init

6.3.3.4.1 Objetivos de la función de mensajería LAN

Los objetivos de la función de mensajería LAN son:

- Soportar los requisitos de la determinación del dispositivo y de la aplicación, al permitir la transferencia de información del perfil del dispositivo desde los elementos lógicos del BP en los dispositivos del anfitrión de IPCable2Home al elemento PS en los dispositivos de las pasarelas particulares conformes.
- Especificar un método abierto y normalizado en la industria para el intercambio del perfil del dispositivo y del perfil de calidad del servicio, con prioridad entre el elemento lógico del BP en cada dispositivo de anfitrión de IPCable2Home y el elemento lógico del PS en un dispositivo de una pasarela residencial conforme.

6.3.3.4.2 Directrices de diseño del sistema relativo a la funcionalidad de mensajería LAN

Las directrices de diseño que se relacionan en el cuadro 6-21 dan la orientación para la especificación de la función de mensajería de la LAN.

Cuadro 6-21/J.192 – Directrices de diseño del sistema relativo a la funcionalidad de mensajería de la LAN

Referencia	Directrices
Mensaje 1 de LAN	El PS y el BP deben soportar un protocolo para el intercambio de información con formato XML.
Mensaje 2 de LAN	El protocolo de mensajería LAN será una norma abierta.
Mensaje 3 de LAN	El protocolo de mensajería LAN tendrá que ser tan compatible como sea posible con los dispositivos IP de LAN y los dispositivos de las pasarelas particulares existentes.

6.3.3.4.3 Descripción del sistema relativo a la funcionalidad de mensajería de la LAN

Debido a su flexibilidad, aceptación por parte de la industria y capacidades para transferir información de configuración y de estado, se seleccionó XML [XML] como el formato de información para los mensajes (BP-PS) de LAN. XML ha recibido la aceptación del público como un protocolo de comunicaciones para la red Internet, y se trata de un formato abierto, no patentado y popular por su capacidad de adaptación a los distintos sistemas. Los beneficios de XML incluyen su capacidad para facilitar la creación, modificación, organización y almacenamiento de información en cualquier forma adaptada a las necesidades de los mensajes de gestión. Las reglas del documento y el soporte de caracteres de XML representan un beneficio adicional. Las capacidades de XML lo recomiendan para el intercambio de mensajes entre los elementos lógicos del PS y del BP.

El protocolo simple de acceso a objetos (SOAP) [SOAP] es un miembro de la familia de los protocolos asociados a XML. Se trata de un protocolo ligero para el intercambio de información en un entorno descentralizado y distribuido. SOAP es un protocolo basado en XML que consta de tres partes:

- un sobre que define un marco para describir lo que contiene un mensaje y cómo procesarlo;
- un conjunto de reglas de codificación para expresar los ejemplares de los tipos de datos definidos por la aplicación; y
- un convenio para representar un procedimiento de llamadas y respuestas a distancia.

SOAP se especifica para el intercambio de perfiles de dispositivos y de QoS entre elementos lógicos del PS y del BP.

6.3.3.4.3.1 Protocolo simple de acceso a objetos (SOAP)

La codificación de un perfil en XML es solamente el primer paso para el intercambio de mensajes entre los dispositivos de la pasarela residencial y de los anfitriones de IPCable2Home. En esta Recomendación también se deben prever convenios para:

- los tipos de información que se han de intercambiar;
- saber cómo se debe expresar la información como XML;
- saber cómo se envía la información entre elementos lógicos.

Sin estos convenios, el PS y el BP no pueden decodificar la información que reciben, aunque esté codificada en XML. Esos convenios son proporcionados por SOAP [SOAP]. Ya que esta Recomendación especifica SOAP únicamente para los mensajes en la red LAN doméstica del abonado, no se requieren todos los formatos de los mensajes de SOAP.

Capa de transporte de SOAP

HTTP es el mecanismo de transporte que se utiliza más comúnmente para los mensajes SOAP. El PS y el BP deben utilizar HTTP como mecanismo de transporte para los mensajes SOAP a fin de garantizar la interoperabilidad entre distintas implementaciones de PS y de BP. Para soportar este método, el PS implementa un servidor HTTP que recibe mensajes (escucha) por el puerto 80 y el BP implementa un cliente HTTP. El PS y el BP también deben tener en funcionamiento una aplicación de procesamiento de SOAP.

Cuando la aplicación de procesamiento de SOAP que funciona en un BP o en un PS recibe un mensaje SOAP, lo procesa realizando las siguientes acciones en el orden que se relaciona más adelante. El BP tiene prohibido realizar modificaciones al perfil del dispositivo o al perfil de QoS como resultado de cualquier mensaje SOAP excepto con la recepción del mensaje BP_Init_Response que reciba del PS:

1) Identificar todas las partes del mensaje SOAP destinado a esa aplicación.
2) Verificar que todas las partes obligatorias identificadas en el paso 1 pueden ser soportadas por la aplicación de este mensaje y que pueden procesarse en consecuencia. Si éste no es el caso el mensaje se descartará. El procesador tiene la opción de ignorar partes facultativas que hayan sido identificadas durante el paso 1 sin afectar el resultado del procesamiento.
3) Enviar un mensaje de respuesta, si procede, como se define en las cláusulas posteriores.

6.3.3.4.3.1.1 Formato de los mensajes SOAP

En esta cláusula se introduce el formato de los mensajes SOAP, necesario para soportar los requisitos de los mensajes de la LAN.

Los mensajes SOAP que se intercambian entre el PS y el BP (a fines de intercambiar los perfiles del dispositivo y de QoS) se inician en el BP. Esta mensajería se denomina "funcionamiento BP_Init".

En esta Recomendación se definen dos rótulos de *código de confirmación* que se utilizan en los mensajes SOAP. Los códigos de confirmación correspondientes a esos rótulos son:

Códigos de confirmación

El código de confirmación en un mensaje indica los detalles de éxito/fracaso relativos al último mensaje en la transacción. Un valor negativo indica una condición de error. Valores no negativos indican la condición de éxito. Un valor positivo distinto de cero indica un mensaje informativo. En el cuadro 6-22 se relacionan los códigos de confirmación definidos para CableHome.

Cuadro 6-22/J.192 – Códigos de confirmación de la mensajería de la red LAN de CableHome

Código de confirmación	Significado
10	Presencia de un atributo no reconocido
0	Éxito
–10	Falta un atributo necesario
–20	Valor no aceptable de un atributo
–30	Se encontraron múltiples errores
–40	Error no clasificado o definido

CableHome define dos rótulos de código de confirmación: código de confirmación de dispositivo y código de confirmación de QoS. El primero es el código de confirmación específico para el perfil del dispositivo y el segundo es el código de confirmación específico para el perfil de QoS. El PS podrá enviar estos códigos en cualquier orden. Los valores del código de confirmación relacionados anteriormente se aplican a ambos tipos de códigos.

6.3.3.4.3.2 Mensajería de SOAP iniciada por el BP (funcionamiento BP_Init)

En la figura 6-8 se muestra el diagrama de flujo de los mensajes que se intercambian entre el BP y el PS durante la mensajería SOAP iniciada por el BP. El mensaje enviado por el BP al PS se denomina mensaje *BP_Init*. La respuesta emitida por un PS al mensaje BP_Init es *BP_Init_Response*. La mensajería mostrada en la figura 6-8 incluye un mensaje BP_Init con la información del perfil emitido por el BP al PS (mensaje *BP_Init*) y la respuesta del PS correspondiente a ese mensaje (mensaje *BP_Init_Response*).

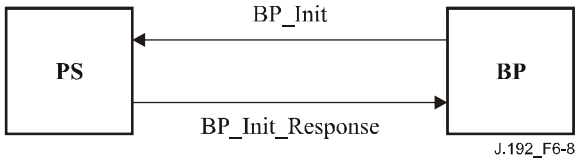


Figura 6-8/J.192 – Mensajería de SOAP iniciada por el BP: funcionamiento BP_Init

6.3.3.4.3.2.1 Formato del mensaje BP_Init

A continuación se presenta el formato del mensaje BP_Init, utilizando como ejemplo la transferencia del perfil del dispositivo del BP y el perfil de QoS hacia el PS:

POST /DevQoSProfileService HTTP/1.1

HOST *IP Address of PS*

Content-Type: text/xml; charset="utf-8"

Content-Length: nnnn

SOAPAction: "/DevQoSProfileService"

<SOAP-ENV:Envelope

xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"

```
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
  <SOAP-ENV:Body>
   <ch:BP_Init xmlns:m= IP Address of PS >
      <ch:BP_IP>
         IP Address of BP
      </ch:BP_IP>
      <ch:DeviceProfile>
         Device Profile from BP
      </ch:DeviceProfile>
      <ch:QoSProfile>
         QoS Profile from BP
       </ch:QoSProfile>
    </ch:BP_Init>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

6.3.3.4.3.2.2 Formato del mensaje BP_Init_Response

A continuación se muestra el formato del mensaje de respuesta al mensaje BP_Init, denominado mensaje BP_Init_Response, utilizando a manera de ejemplo la respuesta al mensaje BP_Init con el perfil del dispositivo y el perfil de QoS que se describió anteriormente.

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset="utf-8"
Content-Length: nnnn

<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
SOAP-ENV:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/"/>
  <SOAP-ENV:Body>
   <ch:BP_Init_Response xmlns:m= IP Address of PS >
      <ch:DeviceConfirmationCode>0</ch:DeviceConfirmationCode >

      <ch:QoSConfirmation Code>0</ch:QoSConfirmationCode>
      <ch:QoSProfile> QoS Profile from PS </ch:QoSProfile>
    </ch: BP_Init_Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

6.3.3.4.4 Requisitos de la función de mensajería de gestión de la LAN

El PS DEBE implementar un servidor HTTP de acuerdo con los requisitos del servidor conforme a [RFC 2616], que recibirá los mensajes en el puerto 80.

El PS DEBE implementar un analizador sintáctico XML conforme a [XML].

El PS DEBE implementar un analizador sintáctico SOAP conforme a las especificaciones descritas en [SOAP].

El PS DEBE utilizar HTTP como mecanismo de transporte de los mensajes SOAP a fin de garantizar la interoperatividad entre distintas implementaciones de PS y BP.

El PS DEBE utilizar el servicio web de SOAP-por-HTTP denominado DevQoSProfileService.

El PS DEBE realizar las siguientes acciones en el orden relacionado cuando recibe el mensaje SOAP BP_Init:

1) Identificar todas las partes del mensaje destinado al PS.
2) Verificar que el mensaje recibido tenga un formato conforme a 6.3.3.4.3.2.1 y procesar el mensaje. Si el mensaje no incluye todos los componentes obligatorios, se descartará. El procesador tiene la opción de ignorar partes facultativas identificadas en el paso 1 sin afectar al resultado del procesamiento.
3) Si el mensaje BP_Init incluye un perfil de dispositivo y/o un perfil de QoS, enviará un mensaje BP_Init_Response conforme a 6.3.3.4.3.1.1, "Formato de los mensajes SOAP".
4) Si el procesamiento del mensaje no puede llevarse a cabo debido a que su formato es incorrecto, incluye un valor no válido o no es conforme a la especificación de CableHome o [SOAP] por cualquier razón, se devolverá un mensaje de estado al emisor con el código de confirmación adecuado como se describe en 6.3.3.4.3.1.1.

El PS DEBE apegarse a las siguientes reglas de sintaxis de SOAP:

- Un mensaje SOAP DEBE codificarse utilizando XML.
- Un mensaje SOAP DEBE tener un sobre SOAP.
- Un mensaje SOAP PUEDE tener un encabezamiento SOAP.
- Un mensaje SOAP DEBE tener un cuerpo SOAP.
- Un mensaje SOAP DEBE utilizar los espacios de nombre del sobre SOAP.
- Un mensaje SOAP DEBE utilizar el espacio de nombre de codificación SOAP.
- Un mensaje SOAP NO DEBE incluir una declaración de tipo de documento (DTD, *document type declaration*).
- Un mensaje SOAP NO DEBE incluir instrucciones de procesamiento XML.
- El PS DEBE utilizar los siguientes espacios de nombre por defecto:
  - en el caso de la sintaxis del sobre SOAP: http://schemas.xmlsoap.org/soap/envelope/;
  - en el caso de codificación y tipos de datos SOAP: http://schemas.xmlsoap.org/soap/encoding/;
  - en el caso de 'BP_Init_Response': dirección IP del PS.

El PS DEBE aceptar y procesar cada uno de los mensajes BP_Init que reciba con una dirección IP de destino 192.168.0.1 o con una dirección IP de destino igual al valor de cabhCdpServerRouter.

El PS DEBE ignorar cualquier mensaje BP_Init que reciba por cualquier interfaz WAN del PS o con una dirección IP de destino *distinta* de 192.168.0.1 o del valor de cabhCdpServerRouter.

El PS DEBE responder con un mensaje BP_Init_Response a cada mensaje BP_Init que reciba por su interfaz LAN y que transporte un perfil de dispositivo, un perfil de QoS o ambos. El PS DEBE

enviar el mensaje BP_Init_Response a la dirección IP que era la dirección IP de origen del mensaje BP_Init. No es necesario que el PS responda a los mensajes BP_Init que no transportan un perfil de dispositivo ni un perfil de QoS.

Si el mensaje BP_Init que recibe el PS incluye un perfil de dispositivo, el mensaje BP_Init_Response emitido por el PS DEBE incluir un código de confirmación de dispositivo válido.

Si el mensaje BP_Init que recibe el PS incluye un perfil de QoS, el mensaje BP_Init_Response emitido por el PS DEBE incluir un código de confirmación de QoS válido y PUEDE incluir un perfil de QoS.

El PS NO DEBE transmitir un mensaje BP_Init_Response a través de ninguna interfaz WAN del PS.

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

6.4.1 Objetivos del CTP

Los objetivos del portal de prueba de CableHome incluyen:

- Facilitar los diagnósticos de fallos de dispositivo IP de LAN y de los anfitriones de CableHome.
- Facilitar la visibilidad a los dispositivos IP de LAN y a los anfitriones de CableHome, 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 CableHome.

6.4.2 Directrices de diseño del CTP

En el cuadro 6-23 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 6-23/J.192 – Directrices de diseño del sistema CTP

Referencia	Directrices de diseño del sistema CTP
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 1.1 de CableHome: 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 de la herramienta de velocidad de la conexión del CTP

6.4.3.1.1 Objetivos de la funcionalidad de la herramienta de la 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 relativo a la herramienta de velocidad de la conexión

Las directrices de diseño relacionadas en el cuadro 6-23, "*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 relativo a la funcionalidad de la 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 de 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) 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 relativos a la funcionalidad de la 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:

- reactivar 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 de 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 el fin del 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 de la 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 kilobits por segundo, redondear el número al entero más próximo y almacenar el resultado en cabhCtpConnThroughput.

El PS DEBE reactivar 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 de 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 de 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 de 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 por la fijación del valor abort(2) del SNMP 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 la herramienta Ping del CTP

6.4.3.2.1 Objetivos de la función de la 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 relativas a la funcionalidad de la herramienta Ping

Las directrices de diseño relacionadas en el cuadro 6-23, "Directrices de diseño del sistema CTP", se utilizaron para orientar la especificación de la función de la herramienta Ping.

6.4.3.2.3 Descripción del sistema relativa a la función de la herramienta Ping

Se invoca la función de la 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 crear una exploración de los dispositivos IP de LAN o de los anfitriones de IPCable2Home de la red. El cuadro de 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 aumentará la dirección y almacenará los resultados en la herramienta NMS para llevar a cabo una exploración de una subred de LAN.

La herramienta PING se inicia mediante una serie de mensajes de petición de establecimiento de 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 la 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 de ICMP y se prevé que el dispositivo IP de LAN devolverá 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 de 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 de 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 su temporizador particular, 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 un temporizador expira durante por lo 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 de la 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 el funcionamiento de la 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 de 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 reactivar 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 desde el último bit de cada paquete de petición de eco de ICMP transmitido por la herramienta Ping del CTP, al momento en que se recibe el último bit del paquete de respuesta de eco de 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).

6.5 Punto de frontera de gestión (MBP) relativo al elemento lógico del BP

En la cláusula 5 se define el punto de frontera (BP) como el elemento lógico definido por IPCable2Home que permite agregar funcionalidad específica de IPCable2Home a un dispositivo del anfitrión de IPCable2Home. El punto de frontera de gestión (MBP) es el elemento lógico del BP encargado de las capacidades del BP para la determinación definida por IPCable2Home.

La determinación de los dispositivos del anfitrión de IPCable2Home es el primer paso de la gestión eventual de la funcionalidad específica de IPCable2Home en esos dispositivos. Con el apoyo de esta Recomendación se habilita la determinación de los dispositivos del anfitrión de CableHome a través del acceso a la información del perfil mediante HTTP, desde el CMP.

6.5.1 Objetivos del MBP

El objetivo del MBP es satisfacer los requisitos de IPCable2Home para la determinación del dispositivo del anfitrión de IPCable2Home y de la mensajería de LAN. El MBP es necesario para proporcionar al operador del sistema de cable el perfil de cada dispositivo del anfitrión de IPCable2Home, a través del PS que desempeña el papel de apoderado.

6.5.2 Directrices de diseño del sistema MBP

El MBP se especificó basándose en las directrices de diseño que se indican en el cuadro 6-24.

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

Referencia	Directrices
MBP 1	El MBP debe mantener información relativa a los atributos del dispositivo del anfitrión de IPCable2Home en el que reside el BP.
MBP 2	El MBP proporcionará información del dispositivo del anfitrión de IPCable2Home y de la aplicación al gestor del sistema IPCable2Home durante el proceso de inicialización del BP.
MBP 3	El MBP proporcionará periódicamente información del dispositivo del anfitrión de IPCable2Home y de la aplicación al gestor del sistema IPCable2Home tras completarse la inicialización del BP.

6.5.3 Descripción del sistema MBP

Se necesita que el BP mantenga un perfil de dispositivo como el descrito en 6.5.3.1.3, "Descripción del perfil del dispositivo", y un perfil de QoS como el descrito en 10.3.2.4.2.1, "Método XML para el perfil de QoS".

Además, el BP debe enviar el perfil del dispositivo al PS, proporcionando de ese modo al gestor del sistema de IPCable2Home el acceso a la información de los atributos de cada uno de los dispositivos del anfitrión de IPCable2Home a través de la MIB del dispositivo del PS (véase E.4), mediante acceso SNMP por la red WAN de datos por cable. Al disponer de acceso a la información de atributos de este modo, el MBP satisface los requisitos de la determinación del dispositivo.

Por otro lado, el BP debe soportar mensajes de LAN utilizando transporte de SOAP por HTTP, como medio para transferir los perfiles de dispositivo y de QoS del BP al PS.

6.5.3.1 Perfil del dispositivo del BP

Los perfiles de dispositivo y de QoS son estructuras con formato XML que contienen información relativa al dispositivo del anfitrión de IPCable2Home y de las aplicaciones que implementa. El perfil del dispositivo se utiliza como medio para mantener y comunicar información relativa al dispositivo del anfitrión de IPCable2Home. El BP debe implementar un perfil de dispositivo y proporcionar la información correspondiente a ese perfil al PS, el cual pone la información a disposición a través de la MIB del dispositivo del PS (véase E.4). El NMS de la red de datos del operador del cable y otros organismos de soporte de abonados pueden obtener información básica relativa al dispositivo del anfitrión de IPCable2Home consultando la MIB del dispositivo del PS por la red de datos por cable, utilizando mensajes de petición SNMP.

6.5.3.1.1 Objetivos del perfil del dispositivo

Los objetivos del perfil del dispositivo del BP son:

- agregar información específica y única para el anfitrión de IPCable2Home aplicando el BP;
- proporcionar al gestor del sistema de IPCable2Home información relativa al dispositivo del anfitrión de IPCable2Home.

6.5.3.1.2 Directrices de diseño del sistema relativo al perfil del dispositivo

En el cuadro 6-25 se presentan las directrices de diseño del sistema que sirven para especificar el perfil del dispositivo MBP.

Cuadro 6-25/J.192 – Directrices de diseño del sistema relativas al perfil del dispositivo MBP

Referencia	Directrices
MBP DevProf 1	El MBP debe mantener un conjunto de información específica del dispositivo del anfitrión de IPCable2Home en el que reside el BP.
MBP DevProf 2	El formato de la información específica del dispositivo deberá apegarse a una norma abierta.
MBP DevProf 3	El formato de la información específica del dispositivo mantenida por un MBP debe ser compatible con los sistemas operativos del dispositivo IP de LAN, debe ser flexible para dar cabida a cualquier clase o cantidad de información específica del dispositivo y debe ser compatible, en la medida posible, con los protocolos y las tendencias de la industria.

6.5.3.1.3 Descripción del perfil del dispositivo

En esta Recomendación se especifica la implementación de un perfil de dispositivo y de un perfil de QoS en elementos lógicos BP para soportar la determinación de los dispositivos del anfitrión de IPCable2Home y la configuración de las prioridades de QoS en los BP. Los perfiles de dispositivo y de QoS tienen estructuras con formato XML. El perfil del dispositivo incluye un conjunto de atributos que describen el dispositivo del anfitrión de IPCable2Home. Un perfil de dispositivo incluye atributos específicos de IPCable2Home y podría incluir igualmente atributos específicos del fabricante. El perfil de QoS contiene una relación de los números de puerto definidos por IANA que determinan las aplicaciones implementadas por cada dispositivo, la prioridad que se asigna a cada aplicación e información facultativa sobre la prioridad de QoS relativa a la dirección IP y el número de puerto de destino. En esta cláusula se describe el perfil del dispositivo. El perfil de QoS se describe en 10.3.2.4.2.1, Método XML para el perfil de QoS.

En el cuadro 6-26 se presenta una descripción general del perfil del dispositivo que necesitan los elementos BP.

Cuadro 6-26/J.192 – Atributos del perfil del dispositivo del BP

Nombre de atributo	Tipo de atributo	Uso
Tipo de dispositivo	Cadena	Necesario
Fabricante	Cadena	Necesario
URL del fabricante	Cadena	Facultativo
Revisión de hardware	Cadena	Necesario
Opciones del hardware	Cadena	Facultativo
Número de serie	Cadena	Necesario
Nombre de modelo	Cadena	Facultativo
Número de modelo	Cadena	Facultativo
URL del modelo	Cadena	Facultativo
UPC del modelo	Cadena	Facultativo
OS software del modelo	Cadena	Necesario
Versión de software del modelo	Cadena	Necesario
Tipo de interfaz de red LAN (IANAifType)	Cadena	Necesario
Número de prioridades de acceso a los medios	Entero	Necesario
Ubicación física	Cadena	Facultativo
Dirección física	Cadena	Necesario

Detalles de los atributos del perfil del dispositivo

El atributo *tipo de dispositivo* puede tomar uno de los siguientes valores: pasarela residencial o anfitrión de IPCable2Home.

El atributo *fabricante* es el nombre del fabricante del dispositivo.

El atributo *URL del fabricante* es el localizador universal de recurso del sitio web del fabricante.

El atributo *revisión de hardware* es una cadena asignada por el fabricante que identifica de manera única la revisión del hardware de un producto particular.

El atributo *opciones de hardware* es una cadena asignada por el fabricante que identifica características facultativas del hardware del producto implementadas a este último.

El atributo *número de serie* es el número de serie de identificación única del dispositivo del anfitrión de IPCable2Home, asignado por el fabricante del dispositivo.

El atributo *nombre de modelo* es el nombre de modelo del dispositivo del anfitrión de IPCable2Home u otro nombre de identificación asignado por el fabricante del dispositivo.

El atributo *número de modelo* es el número de modelo u otro valor de identificación asignado por el fabricante del dispositivo.

El atributo *URL del modelo* es el localizador universal de recursos del sito web del modelo.

El atributo *UPC del modelo* es el valor universal del código de producto asignado al dispositivo.

El atributo *OS software del modelo* es el sistema de operación implementado en el dispositivo.

El atributo *versión de software del modelo* es la versión de software que se emplea actualmente en el dispositivo.

El atributo *tipo de interfaz de red LAN* es una cadena que contiene el valor IANAifType [IANA1] de la tecnología de funcionamiento en red de capa 2 de OSI ISO implementada por el fabricante del producto.

El atributo *número de prioridades de acceso a los medios* se refiere a las prioridades que soporta la interfaz de la red LAN del dispositivo del anfitrión de IPCable2Home. Este atributo y su forma de utilización se describen con detalle en la cláusula 10, ("QoS").

El atributo *ubicación física* es un valor que puede asignar el propietario del dispositivo para indicar su ubicación física, tal como *oficina* o *salón*.

El atributo *dirección física* es la dirección de hardware del dispositivo, tal como la dirección de control de acceso a los medios (MAC, *media access control*) de un dispositivo basado en la Norma 802.3.

6.5.3.1.4 Perfil del dispositivo con formato XML

A continuación se presenta el perfil del dispositivo con formato XML como lo exige IPCable2Home.

```
<xs: complexType name="ch:device">
        <xs:element name="ch:deviceType"                type="xs:string"/>
        <xs:element name="ch:manufacturer"              type="xs:string"/>
        <xs:element name="ch:manufacturerURL"           type="xs:string"/>
        <xs:element name="ch:hardwareRevision"          type="xs:string"/>
        <xs:element name="ch:hardwareOptions"           type="xs:string"/>
        <xs:element name="ch:serialNumber"              type="xs:string"/>
```

```
        <xs:element name="ch:modelName"                          type="xs:string"/>
        <xs:element name="ch:modelNumber"                        type="xs:string"/>
        <xs:element name="ch:modelURL"                           type="xs:string"/>
        <xs:element name="ch:modelUPC"                           type="xs:string"/>
        <xs:element name="ch:modelSoftwareOS"                    type="xs:string"/>
        <xs:element name="ch:modelSoftwareVersion"               type="xs:string"/>
        <xs:element name="ch:lanInterfaceType"                   type="xs:string"/>
        <xs:element name="ch:numberMediaAccessPriorities"        type="xs:int"/>
        <xs:element name="ch:physicalLocation"                   type="xs:string"/>
        <xs:element name="ch:physicalAddress"                    type="xs:string"/>
    </xs:complexType>
```

6.5.3.1.5 Requisitos del perfil del dispositivo

El BP DEBE implementar un perfil de dispositivo conforme a 6.5.3.1.4, que sea congruente con las reglas del formato XML que se describen en [XML].

El BP DEBE rellenar el atributo tipo de dispositivo del perfil del dispositivo del BP (véase 6.5.3.1.4, "Perfil del dispositivo con formato XML") con la cadena "CableHome Host" (sin comillas).

El BP DEBE rellenar el atributo fabricante del perfil del dispositivo del BP (véase 6.5.3.1.4, "Perfil del dispositivo con formato XML") con una cadena cuyo valor identifique al fabricante del dispositivo del anfitrión de IPCable2Home donde reside el BP.

El BP DEBE rellenar el atributo revisión de hardware del perfil del dispositivo del BP (véase 6.5.3.1.4, "Perfil del dispositivo con formato XML") con una cadena cuyo valor represente de manera precisa el número de revisión del hardware del fabricante para el dispositivo del anfitrión de IPCable2Home donde reside el BP.

El BP DEBE rellenar el atributo número de serie del perfil del dispositivo del BP (véase 6.5.3.1.4, "Perfil del dispositivo con formato XML") con una cadena cuyo valor será igual al número de serie que identifique de manera única el dispositivo del anfitrión de IPCable2Home donde reside el BP.

El BP DEBE rellenar el atributo software OS del modelo del perfil del dispositivo del BP (véase 6.5.3.1.4, "Perfil del dispositivo con formato XML") con una cadena cuyo valor represente de manera precisa el sistema de operación del software implementado en el dispositivo del anfitrión de IPCable2Home donde reside el BP.

El BP DEBE rellenar el atributo versión de software del modelo del perfil del dispositivo del BP (véase 6.5.3.1.4, "Perfil del dispositivo con formato XML") con una cadena cuyo valor represente de manera precisa la versión del software del BP implementado en el dispositivo del anfitrión de IPCable2Home donde reside el BP.

El BP DEBE rellenar el atributo tipo de interfaz de red LAN del perfil del dispositivo del BP (véase 6.5.3.1.4, "Perfil del dispositivo con formato XML") con una cadena cuyo valor sea igual al IANAifType [IANAType] que representa la tecnología de la red LAN que soporta el dispositivo del anfitrión de IPCable2Home donde reside el BP.

El BP DEBE rellenar el atributo número de prioridades de acceso a los medios del perfil del dispositivo del BP (véase 6.5.3.1.4, "Perfil del dispositivo con formato XML") con un entero en la gama de 1 a 8 cuyo valor sea igual al número de prioridades de la interfaz de red LAN que soporte el dispositivo del anfitrión de IPCable2Home donde reside el BP.

El BP PUEDE rellenar el atributo URL del fabricante del perfil del dispositivo del BP (véase 6.5.3.1.4, "Perfil del dispositivo con formato XML") con una cadena cuyo valor identifique de manera precisa y única un localizador universal de recursos para el fabricante del dispositivo del anfitrión de IPCable2Home donde reside el BP.

El BP PUEDE rellenar el atributo opciones de hardware del perfil del dispositivo del BP (véase 6.5.3.1.4, "Perfil del dispositivo con formato XML") con una cadena cuyo valor represente las opciones de hardware del dispositivo del anfitrión de IPCable2Home donde reside el BP.

El BP PUEDE rellenar el atributo nombre de modelo del perfil del dispositivo del BP (véase 6.5.3.1.4, "Perfil del dispositivo con formato XML") con una cadena cuyo valor identifique de manera precisa y única el nombre del modelo del fabricante del dispositivo del anfitrión de IPCable2Home donde reside el BP.

El BP PUEDE rellenar el atributo número de modelo del perfil del dispositivo del BP (véase 6.5.3.1.4, "Perfil del dispositivo con formato XML") con una cadena cuyo valor identifique de manera precisa y única del número del modelo del fabricante correspondiente al dispositivo del anfitrión de IPCable2Home donde reside el BP.

El BP PUEDE rellenar el atributo URL del modelo del perfil del dispositivo del BP (véase 6.5.3.1.4, "Perfil del dispositivo con formato XML") con una cadena cuyo valor identifique de manera precisa y única un localizador universal de recursos para el modelo del dispositivo del anfitrión de IPCable2Home donde reside el BP.

El BP PUEDE rellenar el atributo UPC de modelo del perfil del dispositivo del BP (véase 6.5.3.1.4, "Perfil del dispositivo con formato XML") con una cadena cuyo valor identifique de manera precisa y única el código universal del producto del dispositivo del anfitrión de IPCable2Home donde reside el BP.

El BP PUEDE rellenar el atributo ubicación física del perfil del dispositivo del BP (véase 6.5.3.1.4, "Perfil del dispositivo con formato XML") con una cadena cuyo valor identifique la ubicación física del dispositivo del anfitrión de IPCable2Home donde reside el BP.

6.5.3.2 Función de mensajería de la LAN del MBP

6.5.3.2.1 Objetivos de la función de mensajería de LAN del MBP

Estos objetivos se relacionan en 6.3.3.4.1, "Objetivos de la función de mensajería de la red LAN".

6.5.3.2.2 Directrices de diseño del sistema relativas a la función de mensajería de LAN del MBP

Estas directrices se relacionan en el cuadro 6-21, "Directrices de diseño del sistema relativas a la función de mensajería de LAN".

6.5.3.2.3 Descripción del sistema relativa a la función de mensajería de LAN del MBP

Esta función se describe en 6.3.3.4.3, "Descripción del sistema relativa a la función de mensajería de LAN".

6.5.3.2.4 Requisitos de la función de mensajería de LAN de MBP

El BP DEBE implementar un respondedor de servicio de eco, de manera que el BP devuelva inmediatamente (aplique el servicio de eco) al emisor cualquier paquete IP que reciba por el puerto 7, bit a bit, modificando únicamente el puerto y la dirección IP de origen al puerto y la dirección IP de destino, y viceversa.

El BP DEBE implementar tipos de mensajes de eco y de respuesta de eco de ICMP (tipo 8 y tipo 0) y tipos de mensajes de indicación de tiempo y de respuesta de indicación de tiempo de ICMP (tipo 13 y tipo 14), como se describe en [RFC 792], y contestar adecuadamente a las peticiones Ping que se reciben por cualquier interfaz.

El BP DEBE implementar un cliente HTTP conforme a los requisitos del cliente que figuran en [RFC 2616].

El BP DEBE implementar un analizador sintáctico XML conforme a [XML].

El BP DEBE implementar un analizador sintáctico SOAP conforme a [SOAP].

El BP DEBE utilizar HTTP como mecanismo de transporte para la mensajería de SOAP para garantizar la interoperatividad entre distintas implementaciones de PS y BP.

Si el BP recibe la subopción 101 de la opción código 43 de DHCP que incluye la cadena 'CableHome 1.1 LAN-Trans' en el mensaje ACK DHCP, DEBE dirigir cada mensaje BP_Init a su pasarela por defecto (valor de la opción 3 de DHCP recibida en ACK DHCP).

Si el BP no recibe la subopción 101 de la opción código 43 de DHCP incluyendo la cadena 'CableHom 1.1 LAN-Trans', DEBE dirigir cada mensaje BP_Init a la dirección IP 192.168.0.1.

El BP NO DEBE transmitir un mensaje BP_Init con una frecuencia mayor a uno cada 20 segundos.

El BP NO DEBE transmitir un mensaje BP_Init cuando no se trate de las ocasiones específicas relacionadas en 10.4.1.4.1.1, "Información del BP al PS utilizando el mensaje BP_Init".

El BP NO DEBE transmitir un mensaje BP_Init a ninguna dirección distinta de la dirección de la pasarela por defecto del BP o de 192.168.0.1.

El BP DEBE observar las siguientes reglas de sintaxis de SOAP:

- Un mensaje SOAP DEBE codificarse utilizando XML.
- Un mensaje SOAP DEBE tener un sobre SOAP.
- Un mensaje SOAP PUEDE tener un encabezamiento SOAP.
- Un mensaje SOAP DEBE tener un cuerpo SOAP.
- Un mensaje SOAP DEBE utilizar los espacios de nombre del sobre SOAP.
- Un mensaje SOAP DEBE utilizar el espacio de nombre de codificación SOAP.
- Un mensaje SOAP NO DEBE incluir una declaración de tipo de documento (DTD, *document type declaration*).
- Un mensaje SOAP NO DEBE incluir instrucciones de procesamiento XML.
- El BP DEBE utilizar los siguientes espacios de nombre por defecto:
  - en el caso de la sintaxis del sobre SOAP: http://schemas.xmlsoap.org/soap/envelope/;
  - en el caso de la codificación y los tipos de datos SOAP: http://schemas.xmlsoap.org/soap/encoding/;
  - en el caso de 'BP_Init': dirección IP del PS.

El BP DEBE realizar las siguientes acciones, en el orden relacionado cuando recibe un mensaje SOAP:

1) Identificar todas las partes del mensaje SOAP destinado al BP.
2) Verificar que el mensaje recibido utiliza el formato especificado en 6.3.3.4.3.2.1 y procesarlo. Si el mensaje no incluye todos los componentes obligatorios, deberá descartarse. El procesador tiene la opción de no tener en cuenta las partes facultativas identificadas en el paso 1 sin afectar el resultado del proceso.
3) Si el mensaje no puede procesarse debido a que su formato es incorrecto, incluye un valor no válido o no es conforme a la presente Recomendación o de alguna manera a [SOAP], el BP DEBE retransmitir el mensaje BP_Init, hasta en tres ocasiones, durante un periodo de tres minutos. Si el BP no recibe un mensaje BP_Init_Response válido tras emitir los tres mensajes BP_Init en el periodo indicado, DEBE dejar de reintentarlo hasta que renueve o consiga su licencia de dirección IP.

6.5.3.3 Función de determinación del MBP

6.5.3.3.1 Objetivos de la función de determinación del MBP

El objetivo de la funcionalidad de determinación del MBP de IPCable2Home es ofrecer al gestor del sistema IPCable2Home la información relativa al dispositivo del anfitrión de IPCable2Home donde reside el BP.

6.5.3.3.2 Directrices del diseño del sistema relativas a la función de determinación del MBP

En el cuadro 6-27 se indican las directrices para especificar esta función.

Cuadro 6-27/J.192 – Directrices de diseño del sistema relativas a la función de determinación del MBP

Referencia	Directrices
Disco 1 de MBP	El MBP debe proporcionar al operador del sistema de cable información específica de dispositivo relativa al anfitrión de IPCable2Home en el que reside, a través del PS que desempeña el papel de apoderado.
Disco 2 de MBP	El MBP debe proporcionar información al operador del sistema de cable relativa a las aplicaciones implementadas por un dispositivo del anfitrión de IPCable2Home, a través del PS que desempeña el papel de apoderado.

6.5.3.3.3 Descripción del sistema relativa a la función de determinación del MBP

Resulta necesario que cada BP implemente un perfil de dispositivo con formato XML como se describe en 6.5.3.1.4, "Perfil del dispositivo con formato XML". Además, se requiere que cada BP implemente un perfil de QoS como se describe en 10.3.2.4.2.1, "Método XML de perfil de QoS". Cuando el BP está funcionando y ha completado la inicialización, debe enviar al PS información de los perfiles de dispositivo y de QoS utilizando mensajes de LAN como se describe en 6.3.3.4, "Función de mensajería de LAN del CMP". Al proporcionar al PS la información de los perfiles de dispositivo y de QoS, el BP habilita al operador del sistema de cable para que determine los atributos del dispositivo del anfitrión de IPCable2Home donde reside el BP y las aplicaciones que funcionan en el mismo, a través del PS que desempeña el papel de apoderado para el sistema de gestión de la red del operador del cable.

6.5.3.3.4 Requisitos de la función de determinación

Cuando el BP recibe cualquier mensaje ACK DHCP [RFC 2131] dirigido a él mismo, DEBE transmitir un mensaje BP_Init como se describe en 6.3.3.4.3.2, incluyendo sus perfiles de dispositivo y de QoS en el cuerpo del mensaje. Hay en otros momentos en el que el BP envía el mensaje BP_Init, incluyendo el caso cuando se refresca su perfil de QoS como se describe en 10.4.1.4.1, "Intercambio de información de LAN".

Si el BP no recibe un mensaje BP_Init_Response válido un minuto después que generó un mensaje BP_Init, DEBE retransmitir inmediatamente el mismo mensaje BP_Init con los perfiles de dispositivo y de QoS del BP en el cuerpo del mensaje, repitiendo el proceso hasta en tres ocasiones o hasta que el BP reciba un mensaje BP_Init_Response válido, si no hubiera ocurrido lo anterior.

Si el BP no recibe un mensaje BP_Init_Response válido tras haber transmitido una secuencia de tres mensajes BP_Init, DEBE esperar hasta que reciba el siguiente mensaje ACK DHCP [RFC 2131] y repetir el proceso.

7 Herramientas de configuración

7.1 Introducción y síntesis

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 PS 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 de DHCP como se define en RFC 2131.
- Si el servidor de DHCP del sistema de configuración de la red de cable soporta la opción 61 de 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 por 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) [RFC 1350] o el protocolo de transferencia de hipertexto (HTTP) [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 177.	No recibe información del fichero de configuración. Recibe valores válidos de las subopciones 3, 6 y 51 de la opción 177.	No recibe información del fichero de configuración ni de la opción 177, o recibe una combinación no válida de información del fichero de configuración y de las subopciones de la opción 177.
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.

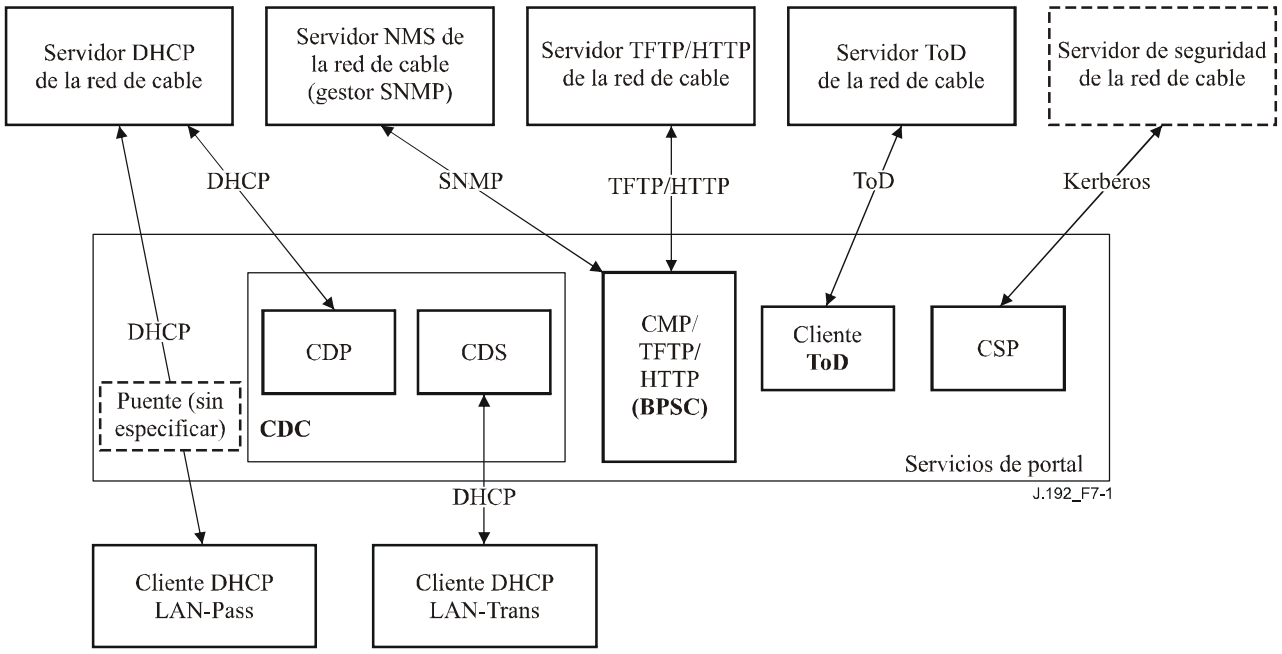


Figura 7-1/J.192 – Arquitectura de configuración

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 controlan las capacidades definidas para el CDP:

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

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

Número	Directrices
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, "Determinación de nombres"). Para cada una de estas funciones de servidor y encaminador del elemento de los servicios de portal, se almacena una dirección IP de LAN en la base de datos del PS. Podrá accederse a cada una de ellas a través de un objeto MIB distinto, que se relacionan más adelante en el cuadro 7-2.

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

El valor por defecto de cabhCdpServerRouter es 192.168.0.1. Los valores por defecto de cabhCdpServerDnsAddress y cabhCdpServerDhcpAddress son también 192.168.0.1. Cualquiera de estos tres objetos MIB de CDP podrán modificarse sin afectar a los otros dos.

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 de DHCP para el PS, a efectos de gestión. El CDC podría intercambiar asimismo mensajes de DHCP con el servidor de 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.

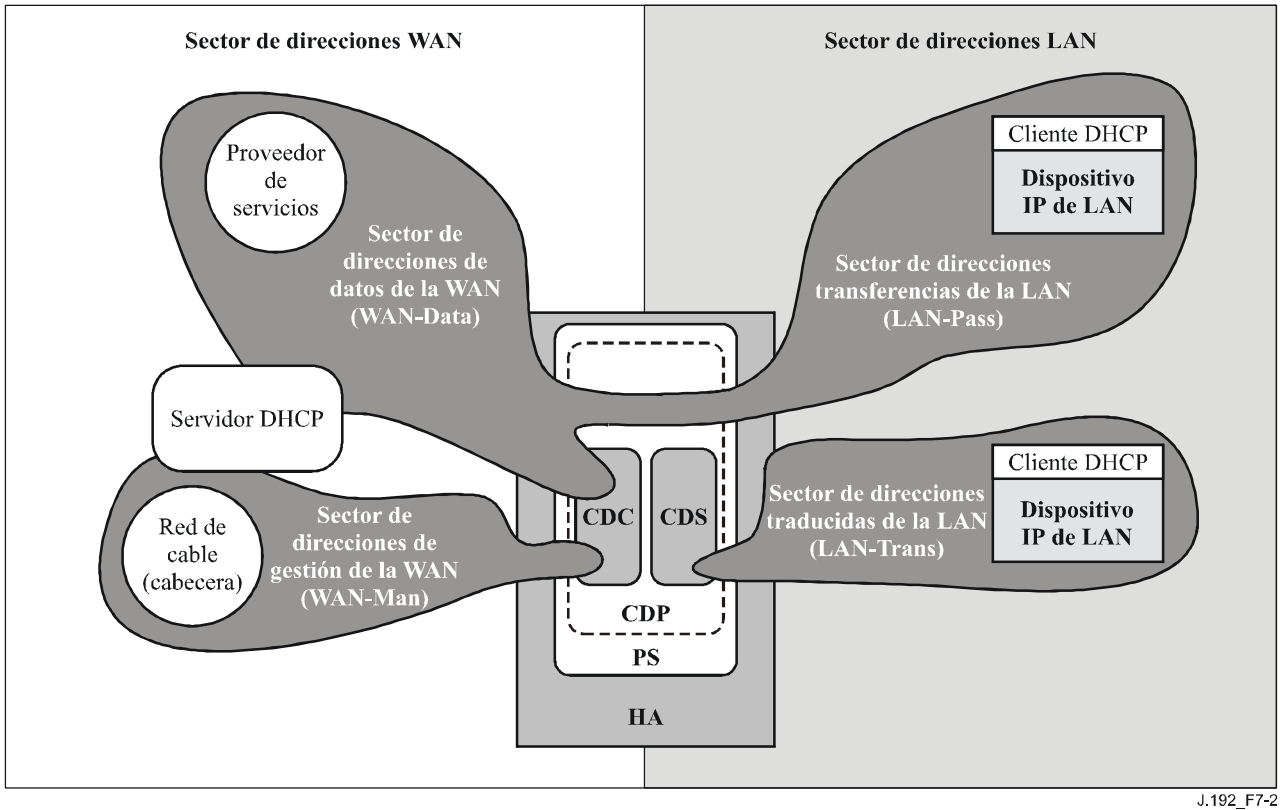


Figura 7-2/J.192 – Funciones del CDP

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 de 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 del CDS

Los objetivos de la función del 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 relativas a la función del 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 relativo a la función del 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 relativa a la función del 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), 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 de 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 CDC es congruente con la sección 2.1 de RFC 2132. Los valores por defecto de dichas opciones de DHCP se definen en el cuadro 7-4 pudiendo el NMS reactivar 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 REQUEST DHCP 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 del 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 reactivación o 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 y REQUEST DHCP 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"):

- 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 DISCOVER DHCP de la LAN: asignar una dirección LAN-Trans como normal o no asignar ninguna dirección.

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

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

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 Ack DHCP con el valor 192.168.0.1 en el campo yiaddr.

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

Número de la opción	Función de la opción	Soporte del protocolo CDS	Datos por defecto de fábrica del CDS	Nombre del objeto de la 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"	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

M Obligatorio (*mandatory*)

O Opcional (*optional*)

NOTA – El CDS debe incluir la subopción 101 de la opción código 43 de DHCP *únicamente* en los mensajes OFFER DHCP y ACK DHCP que envía a los dispositivos IP de LAN conformes a CableHome. La conformidad de los dispositivos IP de LAN a CableHome se indica por la presencia de la cadena *CableHome1.1BP* en los mensajes DISCOVER DHCP y REQUEST DHCP.

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 del cable y el PS;
- obtener información de configuración del servidor DHCP de la red del operador del 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 relativas a la función del 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 relativas a la función 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 relativa a 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 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 ACKNOWLEDGE DHCP 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 CDP soporta diversas opciones DHCP y extensiones BOOTP del fabricante, contempladas en la norma 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 ACK DHCP, como se describe en 5.5, "Modelos de funcionamiento de IPCable2Home".

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 ACK DHCP, y *no* recibe las subopciones 3, 6 ó 51 de la opción 177 de 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;
- pasa por defecto a la utilización de SNMPv1 y SNMPv2c para los mensajes de gestión;
- pasa por defecto a la utilización de 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, *transport layer security*) [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 configuración SNMP

El PS funciona en el modo de configuración SNMP si recibe la opción 177 de DHCP con los campos de subopción 3, 6 y 51, y *no* recibe un nombre de fichero válido en el campo *file* ni una dirección IP válida en el campo *siaddr* del mensaje ACK DHCP.

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.
- Pasa a funcionar por defecto en el modo de coexistencia SNMPv3 con el soporte de SNMPv1 y SNMPv2 *inhabilitado* (véase 11.4, "Mensajería de gestión de seguridad al 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).
- 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 de 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").
- 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 177 de 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.

Cuando el PS se encuentra funcionando en el modo CableHome aletargado, es necesario que su comportamiento sea 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 CableHome:

- 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 de DHCP en los mensajes DISCOVER DHCP y REQUEST DHCP que emite a los servidores DHCP de la red de cable. La opción de identificador de clase de fabricante (opción 60 de 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 de DHCP) identifica con mayor detalles 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.

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

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 de DHCP), sección 9.14 de [RFC 2132], para identificar de manera singular la interfaz WAN lógica asociada a una dirección IP particular.

Es necesario que el PS disponga de dos direcciones de hardware: una que se empleará para identificar singularmente la interfaz WAN lógica asociada con la dirección IP de WAN-Man (dirección de hardware de WAN-Man) y la otra para identificar de manera singular 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 del 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 varias 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 de 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 del sistema de cable podría tener que modificar el software para incluir el soporte de los ID de cliente (opción 61 de 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 MSO 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 MSO como el valor de cabhCdpWanDataIpAddrCount, es decir, el MSO 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 MSO que el valor de cabhCdpWanDataIpAddrCount, es decir, el MSO 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 de 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 de 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 de 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=<0'x'FF).

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 DISCOVER DHCP 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 de 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.

El PS DEBE implementar una función de cliente TFTP conforme a los requisitos de cliente de RFC 1350.

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 el 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 DISCOVER DHCP 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 DISCOVER DHCP por primera vez, a continuación del rearranque del dispositivo o de la reactivación del PS. No es necesario que el PS fije cabhPsDevProvState a inProgress (2) cuando efectúa la renovación de su licencia de dirección IP a través de DHCP.

El PS DEBE utilizar la dirección de hardware de WAN-Man del PS en el campo *chaddr* y en la opción 61 de DHCP, en los mensajes DISCOVER DHCP y REQUEST DHCP, 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 (CDC) solicita direcciones IP de WAN-Data del servidor DHCP de la cabecera, el PS DEBE utilizar anotaciones cabhCdpWanDataAddrClientId para la opción 61 de 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 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 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.

La subopción 11 de la opción 43 de DHCP es un parámetro específico de dispositivo, que se define en la presente Recomendación. Este parámetro indica si se está solicitando una dirección del sector WAN-Man o WAN-Data del PS. En el cuadro 7-6 se indica cómo DEBE el PS fijar los valores de la subopción 11 de la opción 43 de DHCP para sus interfaces WAN.

Cuadro 7-6/J.192 – Valores de la subopción 11 de la opción 43 de DHCP

Identificador (Id) del elemento	Descripción y comentarios
PS WAN-Man = 0x01	Identifica la petición de una dirección del sector WAN-Man.
PS WAN-Data = 0x02	Identifica la petición de una dirección del sector WAN-Data.

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 DEBE el PS fijar el contenido de sus opciones 60 y 43 cuando el elemento PS está integrado con un módem de cable, y se solicitan direcciones de WAN-Man y de WAN-Data del PS.

Cuadro 7-7/J.192 – Opciones de DHCP para las peticiones de direcciones de WAN-Man y de WAN-Data del 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 contrafuego a partir de cabhSecFwPolicyFileCurrentVersion
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 el PS es un dispositivo autónomo.

Cuadro 7-8/J.192 – Opciones de DHCP para peticiones de direcciones de WAN-Man y de WAN-Data del 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 contrafuego a partir de cabhSecFwPolicyFileCurrentVersion
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 función del agente SNMP".

El PS DEBE soportar las opciones de DHCP señaladas como obligatorias en la columna de soporte del protocolo CDC del cuadro 7-9. En el mismo cuadro se relacionan las opciones de 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
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
60	Identificador de clase de fabricante	M
61	Identificador de cliente	M
177	Subopción 3 – Dirección de la entidad SNMP del proveedor de servicio	M
177	Subopción 6 – Nombre del sector de configuración del sector Kerberos	M
177	Subopción 51 – 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 DISCOVER DHCP y REQUEST DHCP 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
255	Fin	M
43	Información específica de fabricante	M
50	Dirección IP solicitada	M
55	Lista de solicitudes de parámetros	M
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 de DHCP (Lista de peticiones de parámetros) [RFC 2132] que se envía en los mensajes DISCOVER DHCP y REQUEST DHCP.

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
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
177	Opción de configuración de cliente compatible con PacketCable	M

El PS DEBE soportar una dirección de la entidad SNMP del proveedor de servicio (subopción 3 de la opción 177 de DHCP) configurada como una dirección IPv4. El formato de la subopción 3 de la opción 177 de DHCP se describe más adelante:

La longitud de la subopción DEBE ser de 5 octetos, después de los cuales HABRÁ un solo octeto que indica el tipo de dirección particular que sigue y que DEBE fijarse a 1 para indicar una dirección IPv4. Después del octeto de tipo DEBE haber 4 octetos correspondientes a la dirección IPv4.

Código	Longitud	Tipo	Dirección			
3	5	1	a1	a2	a3	a4

El PS DEBE soportar un nombre del sector Kerberos (subopción 6 de la opción 177 de 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 177 del DHCP es:

El nombre del sector DEBE codificarse conforme al nombre de sector de estilo de dominio que se describe en RFC 1510. El nombre del sector DEBE indicarse con letras mayúsculas y ser conforme a la sintaxis descrita en la sección 3.1 de RFC 1035. La subopción se codifica como se indica a continuación:

Código	Longitud	Nombre del sector Kerberos			
6	n	k1	k2	. . .	k_n

El PS DEBE soportar una dirección IP de servidor Kerberos (subopción 51 de la opción 177 del DHCP). La subopción de la dirección IP del servidor Kerberos 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 debe apegarse al formato de una dirección IPv4 utilizando el puerto por defecto. La longitud mínima de esta opción es de 4 octetos, y DEBE ser siempre un múltiplo de 4. Si se relacionan múltiples servidores de KDC DEBE ser en orden de prioridad decreciente. La subopción de dirección de servidor KDC se codifica como se indica a continuación:

Código	**Longitud**	**Dirección 1**				**Dirección 2**		
51	n	a1	a2	a3	a4	a1	a2	. . .

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. La dirección 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. Si el PS se encuentra funcionando en el modo 2 de direccionamiento WAN y es necesario que trate de obtener múltiples licencias de dirección IP de WAN-Data y no puede conseguirlas después de haber enviado tres mensajes DISCOVER DHCP (de acuerdo con los procedimientos de reintento DHCP especificados en 7.3.3.2.4, "Requisitos del CDC"), el PS DEBE utilizar la dirección IP de WAN-Data de "repliegue" como la porción WAN de cada tupla NAT dinámica, hasta que obtenga las licencias de dirección IP de WAN-Data necesarias del servidor DHCP a través de una interfaz WAN del PS.

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 un DISCOVER DHCP 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 de DHCP) en el mensaje de DISCOVER DHCP.

Si durante ese intento, el CDC no recibe OFFER DHCP, el PS DEBE registrar el ID de evento 68000100 en el registro histórico local y volver a difundir un mensaje DISCOVER DHCP (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 OFFER DHCP, 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 DISCOVER DHCP por su interfaz WAN cada 10 segundos hasta que se otorgue la licencia DHCP válida para la dirección IP de WAN-Man.

Si durante el proceso de obtención de una licencia para la dirección IP de WAN-Man del PS el CDC recibe, en el mensaje ACK DHCP [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 51 (combinación 1 válida) de la opción 177 de DHCP, el PS DEBE fijar cabhPsDevProvMode a dhcpmode(1) y tratar de sincronizar la hora del día con el servidor ToD, como se describe en 7.5.4, "Requisitos de la función cliente de hora del día".

Si durante el proceso de obtención de una licencia para la dirección IP de WAN-Man del PS el CDC recibe un mensaje ACK DHCP del servidor DHCP en la red de cable que incluya la opción 177 de DHCP con una dirección IP válida (dirección de la entidad 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 51, 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".

Si durante el proceso de obtención de una licencia para la dirección IP de WAN-Man del PS el CDC recibe, en el mensaje ACK DHCP del servidor DHCP en la red de cable, cualquier combinación de las subopciones 3, 6 y 51 de la opción 177 de 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 correspondiente y redifundir un mensaje DISCOVER DHCP (es decir, reactivar la secuencia de configuración en el caso de esta condición que no es válida, repitiendo todo el proceso de obtención de la licencia DHCP hasta en cinco ocasiones.

Si después del quinto intento para obtener una licencia para la dirección IP de WAN-Man del PS el CDC recibe, en el mensaje ACK DHCP del servidor DHCP en la red de cable, cualquier combinación de las subopciones 3, 6 y 51 de la opción 177 de DHCP, el campo 'siaddr' y el campo 'file' distinta de las dos combinaciones válidas que se describieron anteriormente, el PS DEBE 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 IPCable2Home (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 contrafuego.

- 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 reactivar sus objetos MIB a los valores por defecto de fábrica.

Cuando un PS que está funcionando en el modo 2 de direccionamiento WAN (como se describió en 7.3.3.2) trata de obtener una dirección IP de WAN-Data para una interfaz de WAN-Data que utilizará una dirección IP distinta de la correspondiente a la interfaz de WAN-Man, el PS DEBE incluir la opción de identificador de cliente (cabhCdpWanDataAddrClientId) en el mensaje de DISCOVER DHCP. A fin de habilitar estos ID de cliente de WAN-Data únicos, el CDC DEBE habilitar el sistema NMS para crear anotaciones cabhCdpWanDataAddrClientId en cabhCdpWanDataAddrTable.

Si un PS se encuentra funcionando en el modo 2 de direccionamiento WAN (como se describió en 7.3.3.2) DEBE tratar de obtener una dirección IP, a través de DHCP, para cada ID de cliente único (cabhCdpWanDataAddrClientId) en cabhCdpWanDataAddrTable, hasta el límite definido por cabhCdpWanDataIpAddrCount.

El PS DEBE continuar difundiendo el mensaje DISCOVER DHCP mediante la implementación de un algoritmo de reducción exponencial aleatorizado, congruente con el descrito en RFC 2131, hasta que consiga una licencia de dirección IP de WAN-Man y/o de WAN-Data del PS, según proceda.

Si el PS (CDC) tiene éxito para conseguir la dirección IP de WAN-Man (es decir, si recibe un mensaje ACK DHCP del servidor DHCP a través de la interfaz WAN-Man del PS) en el primer intento, y si se encuentra funcionando en el modo de configuración DHCP, DEBE intentar la sincronización de la hora del día con el servidor ToD, emitiendo una petición ToD como se describe en 7.5.4, antes de tratar de descargar el fichero de configuración del PS.

Si el PS (CDC) no obtiene la dirección IP de WAN-Man (es decir, la petición del DHCP alcanza su límite temporal conforme a RFC 2131) después de su primer intento, DEBE activar el CDS (es decir, iniciar su funcionamiento), de modo que el CDS pueda atender las peticiones de DHCP de los dispositivos IP de LAN en el sector LAN-Trans.

La función CDC del PS DEBE responder únicamente a los mensajes DHCP que se reciban a través de una interfaz WAN o enviar mensajes DHCP a través de la misma interfaz.

Cuando expira la licencia DHCP de WAN-Man, el PS DEBE despejar todas las anotaciones de la fila en cabhCdpWanDnsServerTable.

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 contrafuego.

7.4.2 Directrices de diseño del sistema relativas a la función de configuración de los servicios de portal en bloque

Las directrices indicadas en el cuadro 7-12 permiten orientar la especificación de las capacidades de la función de configuración del PS en bloque:

Cuadro 7-12/J.192 – Directrices de diseño del sistema relativas a 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 contrafuego.

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, a través del 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 contrafuego. 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 contrafuego. 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 MSO para modificar los valores de configuración del PS y de la barrera contrafuego 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 contrafuego se utilizará únicamente para valores específicos de la barrera contrafuego.

El proceso de configuración del PS en bloque podrá tener el mismo comportamiento de peticiones sucesivas de ESTABLECIMIENTO de SNMP realizadas 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 contrafuego 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 contrafuego 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)". En el cuadro 7-13 se proporcionan las definiciones de estos términos.

Cuadro 7-13/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 7.3.3.1.1 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 o de la barrera contrafuego PUEDE incluir distintos parámetros, pero los únicos parámetros que DEBEN incluirse en cualquier fichero de configuración son la verificación de integridad del mensaje (MIC, *message integrity check*) del PS (tipo 53) y el marcador de fin de datos (tipo 255).

Para facilitar la gestión uniforme del PS, éste DEBE soportar un fichero de configuración que tenga hasta 64K-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 contrafuego describe un atributo de esta última. Ya que la barrera contrafuego de IPCable2Home se configura accediendo a la MIB de seguridad de IPCable2Home (véase 11.6.4, "Requisitos de la barrera contrafuego"), por lo general un fichero de configuración de la barrera contrafuego incluye valores de configuración TLV tipo 28, que a su vez incluyen objetos MIB de SNMP. La información de configuración de la barrera contrafuego específica de fabricante podrá transferirse al PS en el fichero de configuración de la barrera contrafuego 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 dato 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 de 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 grabables, 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 [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 transladan, 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 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 de SNMP.

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 de 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 de SNMP en un fichero de configuración DEBEN tratarse simultáneamente. Cada VarBinds debe limitarse a 65535 bytes.

7.4.4.1.6 Certificado de verificación de código de 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)

7.4.4.1.7 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)

7.4.4.1.8 Valor de arranque (Kickstart) de SNMPv3

(Véase la sección 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.

7.4.4.1.8.1 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.

7.4.4.1.8.2 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.

7.4.4.1.9 Receptor de notificaciones SNMP

Tipo	Longitud	Valor
34.2	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.

7.4.4.1.9.1 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

7.4.4.1.9.2 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.

7.4.4.1.9.3 Sub-TLV 38.3 – Tipo de trampa enviada por el PS (véase la 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

7.4.4.1.9.4 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 a 65535

7.4.4.1.9.5 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 a 65535

7.4.4.1.9.6 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.

7.4.4.1.9.7 Sub-TLV 38.7 – Nombre de seguridad que debe utilizarse cuando se envía la notificación SNMP V3

Tipo	Longitud	Valor
38.7	2 a 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".

NOTA 5 – Si el PS entra al modo de coexistencia SNMPv3 durante el procesamiento del fichero de configuración del PS, el PS DEBE procesar únicamente TLV-38.

7.4.4.1.10 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 ID del fabricante DEBE ser el primer sub-TLV integrado en VSIF. Si el primer TLV en VSIF no es un ID de fabricante, el fichero de configuración del PS DEBE ignorarse.

Este valor de configuración puede aparecer en múltiples ocasiones en un fichero de configuración y el mismo ID de fabricante puede aparecer también varias veces. El PS DEBE rechazar el fichero de configuración si dentro de un solo VSIF hay más de un sub-TLV de ID de fabricante.

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

7.4.4.1.11 Verificación de integridad del mensaje del PS (PS MIC, PS *message integrity check*)

Tipo	Longitud	Valor
53	20	Troceo SHA de 160 bits (20 octetos)

Este parámetro incluye un troceo (PS MIC) que se calcula mediante un algoritmo *hash* seguro (SHA-1), definido en NIST, FIPS PUB 180-1: Secure Hash Standard, abril de 1995 [FIPS 180-1]. Este TLV se utiliza únicamente en el fichero de configuración justo antes del marcador de fin de datos.

7.4.4.1.12 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 contrafuego 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 contrafuego 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, 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, el PS DEBE emitir una petición Get TFTP 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 '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 Get HTTP 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 Get HTTP 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).

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 de 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 de 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 contrafuego

La descarga del fichero de configuración de la barrera contrafuego se activa cuando el valor utilizado para ESTABLECER (SET) el objeto de la MIB cabhSecFwPolicyFileURL, mediante el fichero de configuración del PS o la instrucción SNMP SET, difiere del valor de la MIB cabhSecFwPolicySuccessfulFileURL. Si el valor utilizado para ESTABLECER (SET) el objeto de la MIB cabhSecFwPolicyFileURL, mediante el fichero de configuración del PS o una instrucción SNMP SET, es el mismo del valor de la MIB cabhSecFwPolicySuccessfulFileURL, NO DEBE activarse la descarga del fichero de configuración de la barrera contrafuego.

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 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 = [0, 1, 2, 3, 4 ó 5] para el contador de reintentos del fichero de configuración del PS o de la barrera contrafuego;
- n = 0 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 0 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 contrafuego solicitado después del intento con n = 5, n debe reiniciar en 0 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-28 del fichero de configuración a una sola PDU de SNMP que contenga(n) OID/ejemplar y componentes de valor de la MIB (varbinds de SNMP). Conforme a RFC 3416, la PDU de SNMP única generada por el fichero de configuración 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-28 en el fichero de configuración o en la PDU de SNMP. El requisito de la PDU de SNMP única generada por el fichero de configuración es congruente con el comportamiento de los paquetes PDU de SNMP recibidos de un gestor de SNMP: el orden de las varbind de la PDU de SNMP no tiene importancia, y no existe un límite definido para la PDU de SNMP MAX. Una vez construida una PDU de SNMP simple, 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 de 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 acepta 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 cláusulas se describen los algoritmos y los requisitos de seguridad necesarios para verificar el troceo (*hash*) 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 del 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 SHA-1 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 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 adecuado.

---

[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 generado también que se creó en los pasos 1 y 2.

5) El elemento PS DEBE calcular un 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 SHA-1 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 dicha generación calculado en el paso 1 al elemento PS a través de SET SNMP. 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 a través de SNMP SET. 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 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 contrafuego

El PS debe utilizar la verificación del fichero de configuración de la barrera contrafuego en el fichero de configuración de la barrera contrafuego 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 contrafuego 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 contrafuego 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 contrafuego 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 un troceo SHA-1 de todo el contenido del fichero de configuración de la barrera contrafuego 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 contrafuego y el PS DEBE utilizar ese fichero para configurar la barrera contrafuego, 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 que se describe en 6.3.3.2, "Función de notificación de eventos del CMP".

En el cuadro 7-14 se identifican los modos de éxito y de fracaso que podrían encontrarse durante la descarga y el procesamiento del fichero de configuración del PS, y las medidas que DEBE tomar el PS cuando detecta estos modos.

Cuadro 7-14/J.192 – Modos de éxito y fracaso del procesamiento del fichero de configuración

Modo de fracaso	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 TFTP – no se encontró el fichero de configuración	Notificar un evento (ID de evento 68000600) y reintentar TFTP.
Fracaso de TFTP – paquetes en desorden	Notificar un evento (ID de evento 68000700) y reintentar TFTP.
Fracaso de la descarga de TFTP – se excedió el número máximo de reintentos	Notificar un evento (ID de evento 68000900) y reactivar.
Descarga satisfactoria de TFTP	Notificar un evento (ID de evento 68001000 si no se utilizó TLS o ID de evento 68003200 si se utilizó 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 reactivar. No se debe tratar de procesar el fichero.
El fichero de configuración es demasiado largo	Notificar un evento (ID de evento 73040102) y reactivar. No se debe tratar de procesar el fichero.
No hay marcador de fin de datos	Notificar un evento (ID de evento 7340102) y reactivar. No se debe tratar de procesar el fichero.

Cuadro 7-14/J.192 – Modos de éxito y fracaso del procesamiento del fichero de configuración

Modo de fracaso	Medida
OID de TLV-28 duplicado	Notificar un evento (ID de evento 73040102), rechazar el fichero de configuración y reactivar. Mantener todos los valores de objeto que existían antes de tratar de procesar este fichero de configuración erróneo.
Tipo reconocido pero valor erróneo u OID de TLV-28 válido pero valor de MIB erróneo	Notificar un evento (ID de evento 73040102), rechazar el fichero de configuración y reactivar. Conservar todos los valores de objeto que existían antes de tratar de procesar este fichero de configuración erróneo.
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 7-14 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 GET TFTP o HTTPS, el fichero de configuración del PS no se encontró en el servidor, o fracasó la petición GET TFTP o HTTPS 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 contrafuego es menor que 5 y se alcanza el fin de temporización de la petición GET TFTP o HTTP, el fichero en cuestión no se encuentra en el servidor o fracasa el GET TFTP o HTTP, 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 contrafuego, 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 7-14, "Modos de éxito y fracaso 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 la norma 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 contrafuego 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 7-14, "Modos de procesamiento del fichero de configuración", para señalar el fallo del proceso de descarga del fichero de configuración de la barrera contrafuego y continuar su funcionamiento normal. Si el fichero de configuración de la barrera contrafuego 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 7-14, "Modos 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-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 28 válido pero 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 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.

7.4.4.4.5 Descarga satisfactoria del fichero de configuración de la barrera contrafuego

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 contrafuego, 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 contrafuego, DEBE reiniciar el contador de reintentos de dicho fichero a cero y notificar el ID de evento 68003200 (véase el cuadro B.1, "Eventos definidos para IPCable2Home"). Tras la descarga y el proceso satisfactorio del fichero de configuración de la barrera contrafuego por parte del PS, la barrera contrafuego 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 contrafuego

Si fracasa la verificación del fichero de configuración de la barrera contrafuego 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 contrafuego 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 contrafuego contiene elementos 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 contrafuego 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 contrafuego contiene un campo de tipo reconocido pero un campo valor erróneo, o un valor de OID de TLV-28 pero un valor de MIB erróneo, el PS DEBE continuar su funcionamiento normal, rechazar el fichero de configuración de la barrera contrafuego 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 contrafuego contiene un campo tipo no reconocido o un elemento 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 contrafuego.

Si la descarga del fichero de configuración de la barrera contrafuego fracasa por cualquier razón, la barrera contrafuego DEBE funcionar de acuerdo con la configuración anterior al intento de descarga fallido.

7.5 Función del PS – Cliente de hora del día

7.5.1 Objetivos de la función del cliente de hora del día

El objetivo de la función del cliente de 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 relativo a la función de cliente de hora del día

La directriz que se presenta en el cuadro 7-15 da la orientación para la especificación de las capacidades determinadas para la función de cliente de hora del día del PS.

Cuadro 7-15/J.192 – Directrices de diseño del sistema relativo al cliente de hora del día

Número	Directrices
ToD1	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 relativo a la función de cliente de hora del día

El elemento de servicios de portal utiliza un cliente de hora del día conforme a [RFC 868], a fin de lograr la sincronización de tiempo con un servidor de tiempo en la red de la cabecera. 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 cabecera) para la interfaz WAN-Man, el cliente DHCP recibirá la dirección IP del servidor ToD de la cabecera en la opción 4 de DCHP. El cliente de DHCP también recibirá el desplazamiento de tiempo (con relación a UTC), en la opción 2 de DHCP.

Una vez que la pila de protocolos de IP de WAN-Man comienza a utilizar la dirección IP recibida del DHCP, debería enviar una consulta de tiempo conforme a [RFC 868] al servidor de ToD. Si éste ofrece una respuesta válida, el PS comenzará 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 de hora del día

El elemento de servicios de portal DEBE implementar un cliente de hora del día.

El cliente de 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, el elemento de servicios de portal DEBE inicializar su tiempo a 00:00.0 (medianoche) GMT, 1 de enero de 1970.

El elemento de servicios de portal DEBE tratar de sincronizar la hora del día con los servidores de tiempo propuestos en la opción 4 de DHCP del mensaje ACK DHCP, recibido por la interfaz de WAN-Man durante el proceso de obtención de la licencia DHCP de WAN-Man.

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.

El PS DEBE combinar el tiempo recuperado del servidor de tiempo con el desplazamiento de tiempo proporcionado por la opción 2 de DHCP, para producir la hora local actual.

El elemento de servicios de portal DEBE utilizar la hora local actual calculada a partir del tiempo recuperado del servidor ToD y del desplazamiento de tiempo recibido en la opción 2 de DHCP para cualquier función que demande la hora del día, y que necesita sólo una precisión al segundo más próximo.

La prioridad del reloj de hora del día del sistema para un PS integrado es la siguiente:

- primera prioridad: hora del día obtenida del servidor de ToD;
- segunda prioridad: hora del día obtenida del módem de cable;
- tercera prioridad: hora inicializada al 1 de enero de 1970.

Un PS integrado DEBE utilizar la hora del día válida más reciente obtenida del servidor de ToD para el reloj de hora del día del sistema, aun en el caso que esto signifique suprimir la hora del sistema obtenida del CM.

Si un PS integrado no tiene la capacidad para obtener la hora del día del servidor de ToD, DEBE utilizar la hora del día obtenida del módem de cable para el reloj de hora de día del sistema.

Si un PS integrado no tiene la capacidad para obtener la hora del día del servidor de ToD, ni tampoco para obtener la hora del día válida del módem de cable, DEBE utilizar la hora del día inicializada en el proceso de arranque al 1 de enero de 1970 para el reloj de hora del día del sistema.

La prioridad del reloj de hora del día del sistema para un PS autónomo es la siguiente:

- primera prioridad: hora del día obtenida del servidor de ToD;
- segunda prioridad: hora inicializada al 1 de enero de 1970.

Un PS autónomo DEBE utilizar la hora del día válida más reciente obtenida del servidor de ToD para el reloj de hora del día del sistema.

Si el PS autónomo no tiene la capacidad para obtener la hora del día del servidor de ToD, DEBE utilizar la hora del día inicializada en el proceso de arranque al 1 de enero de 1970, para el reloj de hora del día del sistema.

El elemento PS DEBE seguir tratando de comunicarse con el servidor de hora del día hasta que se establezca la hora local. La temporización específica para las peticiones de hora del día depende de

la implementación, no obstante, el cliente de hora del día del PS NO DEBE exceder más de 3 peticiones de ToD en un periodo de 5 minutos. El cliente de hora del día del PS DEBE, como mínimo, emitir una petición de ToD por cada periodo de 5 minutos, hasta que se establezca la hora local.

Si el servidor de ToD no envía una respuesta válida el PS DEBE efectuar lo siguiente, no necesariamente en el orden indicado:

- fijar el valor de cabhPsDevTodSyncStatus a '2' (el acceso al ToD fracasó);
- si hay licencias activas en el sector LAN-Trans indicadas por un valor distinto de cero para cabhCdpLanTransCurCount, se debe fijar cabhCdpLanAddrCreateTime a la hora actual y cabhCdpSLanAddrExpireTime al valor de cabhCdpLanAddrCreateTime más el valor de cabhCdpServerLeaseTime para cada licencia activa (Tiempo de expiración = CreateTime + LeaseTime);
- registrar el fallo y generar un evento normal definido en el anexo B; y
- seguir reintentando la comunicación con el servidor de ToD hasta que se establezca la hora local; y
- si se recibe la instrucción de activación correspondiente, tratar de descargar el fichero de configuración del PS conforme a 7.4.4.2.4, "Funcionamiento posterior a la activación".

Si el servidor de ToD no envía una respuesta válida, el PS DEBE efectuar lo siguiente, y no necesariamente en el orden indicado:

- fijar el valor de cabhPsDevTodSyncStatus a '1' (acceso satisfactorio al ToD);
- si hay licencias activas en el sector LAN-Trans indicadas por un valor distinto de cero para cabhCdpLanTransCurCount, se debe fijar cabhCdpLanAddrCreateTime a la hora actual y cabhCdpLanAddrExpireTime al valor de cabhCdpLanAddrCreateTime más el valor de cabhCdpServerLeaseTime para cada licencia activa (Tiempo de expiración = CreateTime + LeaseTime);
- si se recibe la instrucción para la activación correspondiente, tratar de descargar el fichero de configuración del PS conforme a 7.4.4.2.4, "Funcionamiento posterior a la activación".

Si el valor de cabhPsDevTodSyncStatus es '1', es decir, si ya se estableció la hora local, no será necesario que el cliente de hora del día emita una petición de ToD.

El PS DEBE enviar y recibir mensajes de ToD sólo a través de una interfaz de WAN-Man.

7.6 Función del BP – Cliente de 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 relativo a la función de cliente DHCP del BP

Las directrices relacionadas en el cuadro 7-16 orientan la especificación de la función de cliente DHCP del BP.

Cuadro 7-16/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 del 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 reactivación 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 7-17.

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";
- código 255 de opción DHCP, Fin.

Cuadro 7-17/J.192 – Opciones de DHCP necesarias para el cliente DHCP del BP

Número de opción	Función de la opción	Soporte obligatorio (M) 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 del 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) 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 relativo a 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).

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 la misma norma.

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, *upstream selective forwarding switch*) 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.

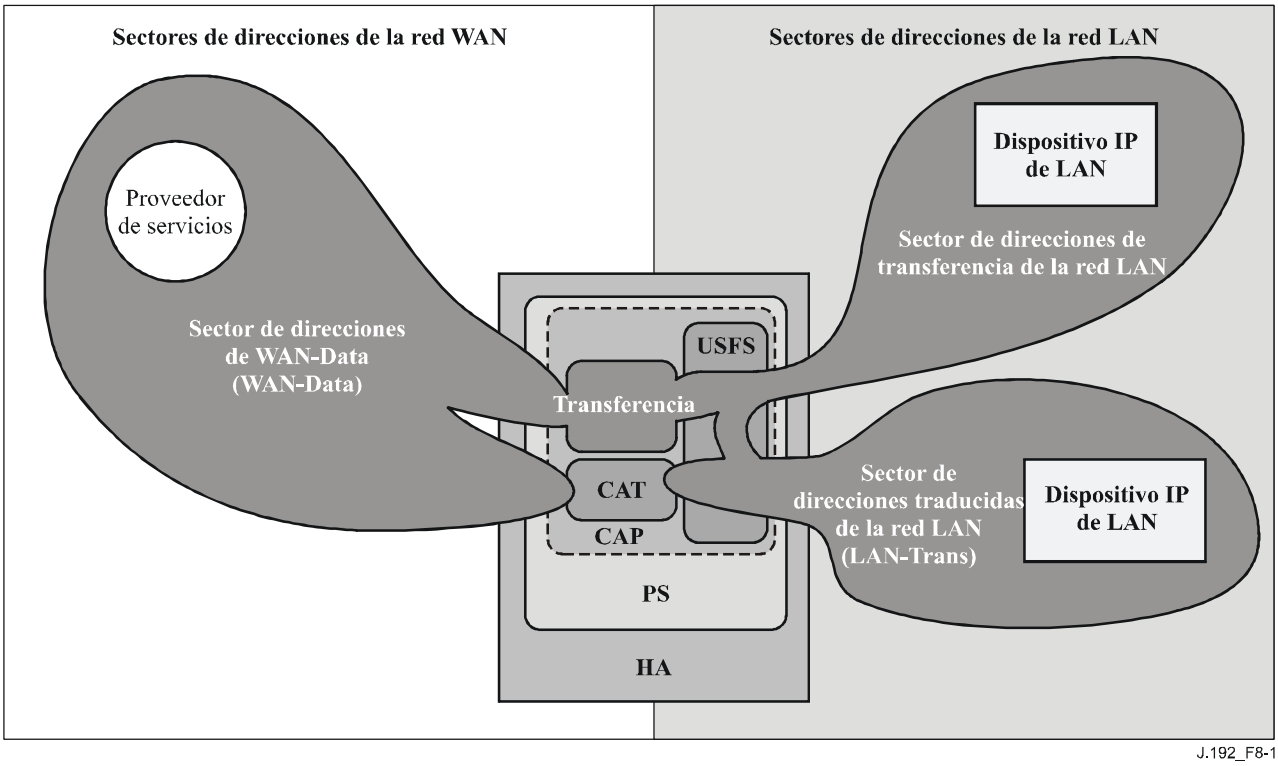


Figura 8-1/J.192 – Funciones del portal de direcciones de IPCable2Home (CAP)

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" (Mapping) 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 número de secuencia 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 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 del 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 la cabecera 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, "Comodines de retransmisión de puerto estático", 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.

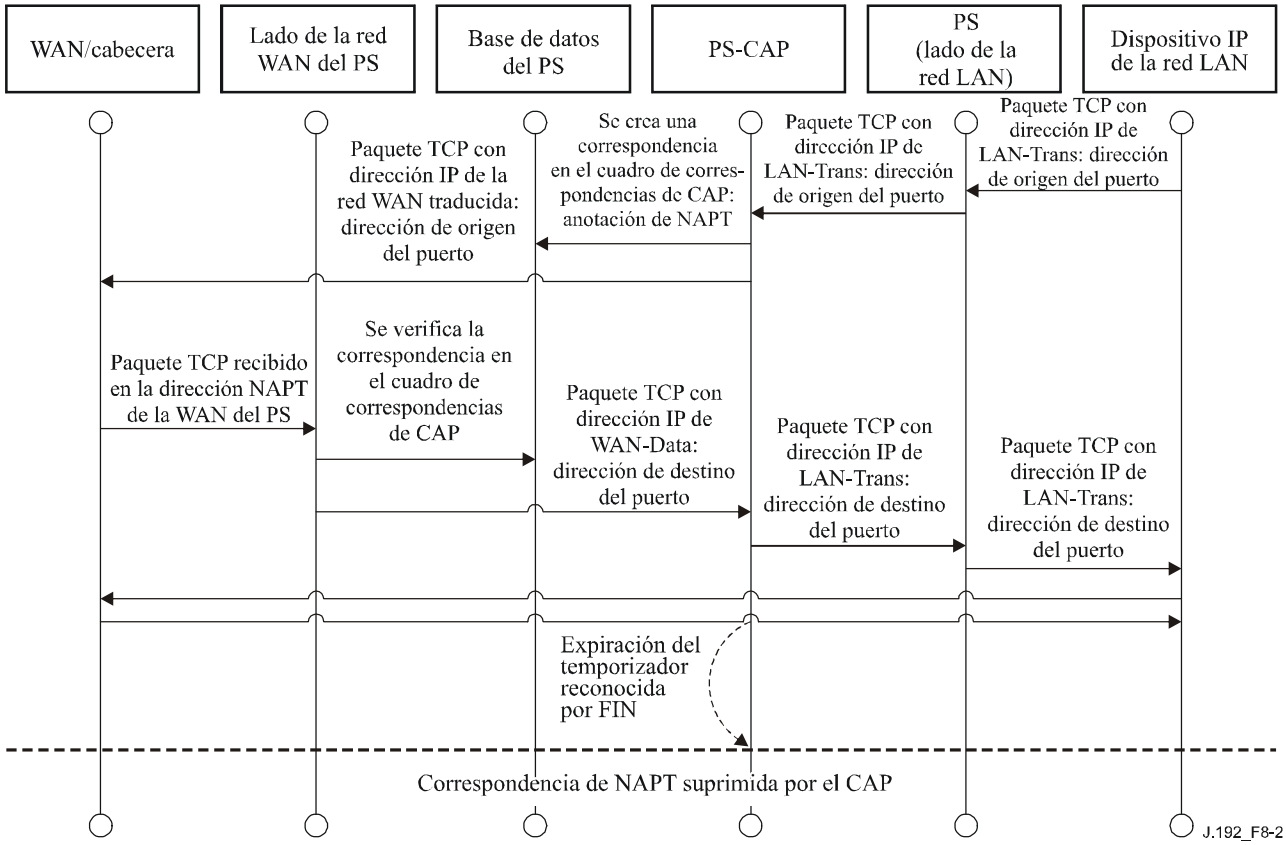


Figura 8-2/J.192 – Diagrama de la secuencia de configuración del PS (cuadro de correspondencias de CAP-NAPT)

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 (Passthrough), 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 Comodines de retransmisión de puerto estático

Cuando el PS se configura para funcionar en el modo de tratamiento de paquetes primario de C-NAPT y se crea estáticamente una vinculación de C-NAPT con el número de puerto fijado a cero, el CAP tratará el tráfico entrante de un modo especial, retransmitiendo todo el tráfico entrante no asociado con una sesión C-NAPT existente, o una vinculación estática de C-NAPT existente, a la dirección IP de LAN especificada en este tipo especial de vinculación de C-NAPT.

El CAP procesará los paquetes de la siguiente manera:

1) Verifica todos los paquetes entrantes para examinar si están asociados con una sesión existente especificada por una vinculación dinámica de C-NAPT. Si éste es el caso, el paquete se traduce como se especifica y a continuación se retransmite.
2) Si no existe la asociación antes referida el CAP verifica si hay una vinculación de C-NAPT estática asociada con el paquete. Si éste es el caso, el paquete se traduce como se especifica y a continuación se retransmite.
3) De no tratarse del caso indicado en el punto anterior, el CAP verifica si hay una vinculación 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 vinculación 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.

8.3.3.3 Soporte de red privada virtual (RPV) en el CAP

El PS debe implementar una característica de *transferencia* (*Passthrough*) *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 contrafuego 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 contrafuego 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 entradas del CDP. Las entradas 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 de QoS y del acceso a los medios (QFM) (véase 10.3, CQP del elemento lógico del PS) 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 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 [ID-IGMP] 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.

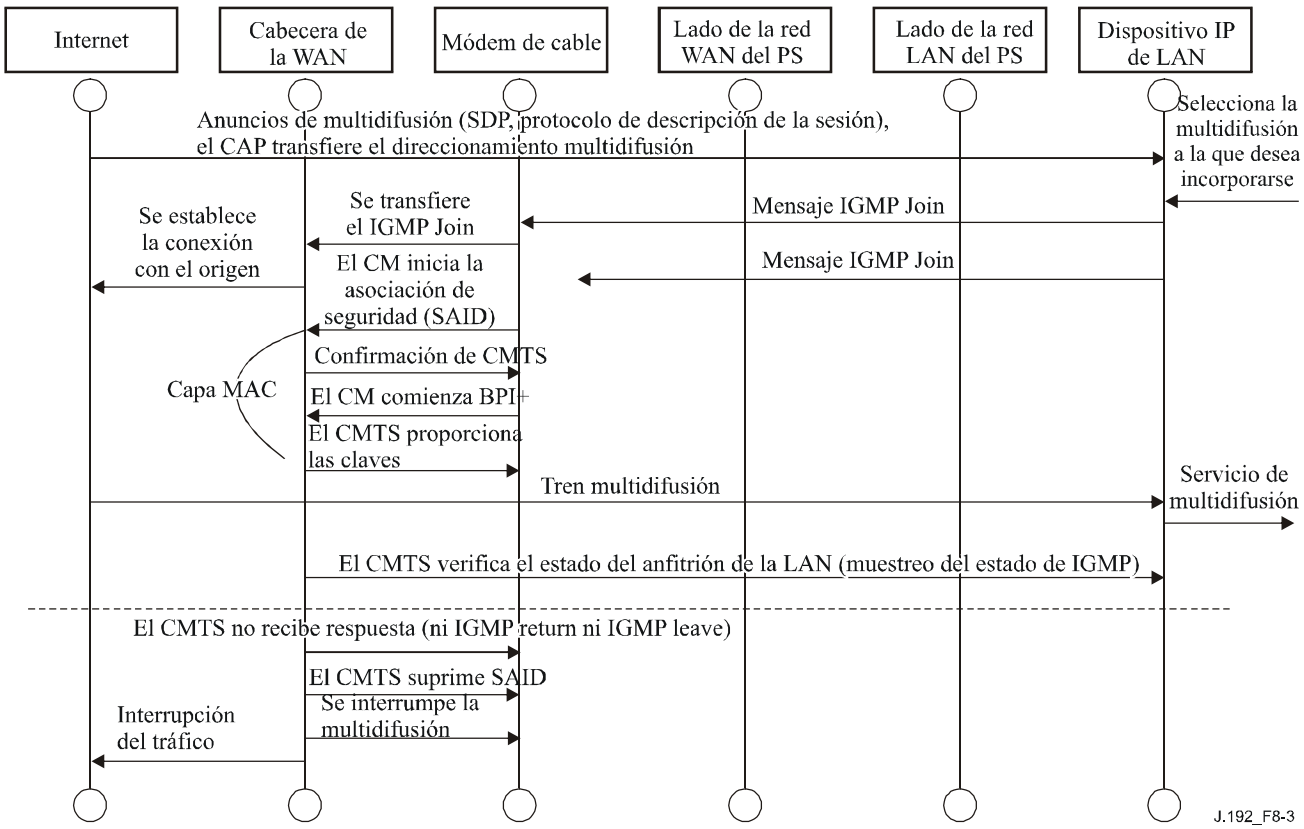


Figura 8-3/J.192 – Multidifusión a través de la secuencia de IGMP

8.3.3.6 Ejemplos de tratamiento de los paquetes de IPCable2Home

Esta cláusula pretende informar sobre 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.

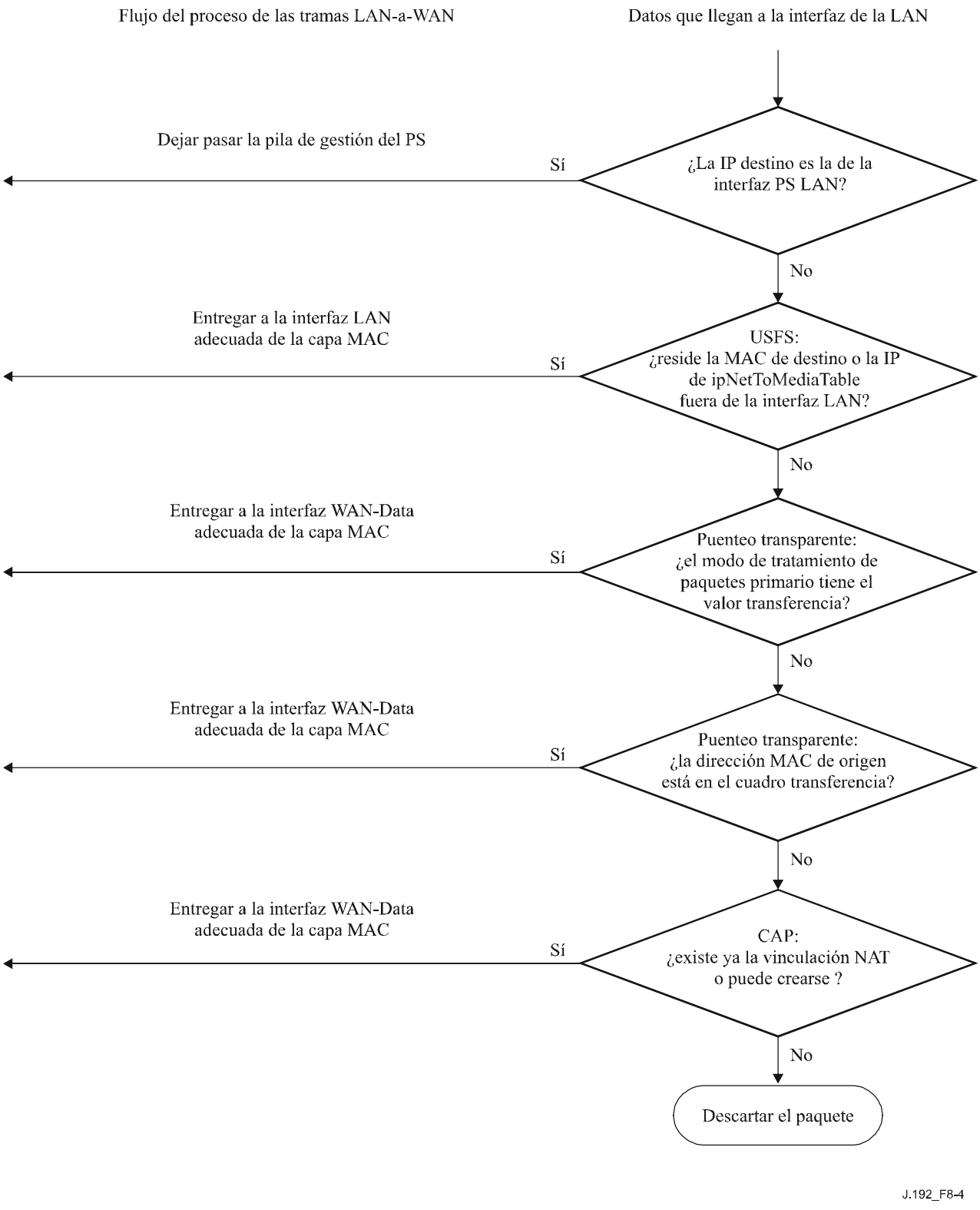


Figura 8-4/J.192 – Ejemplo de procesamiento de paquetes LAN-a-WAN

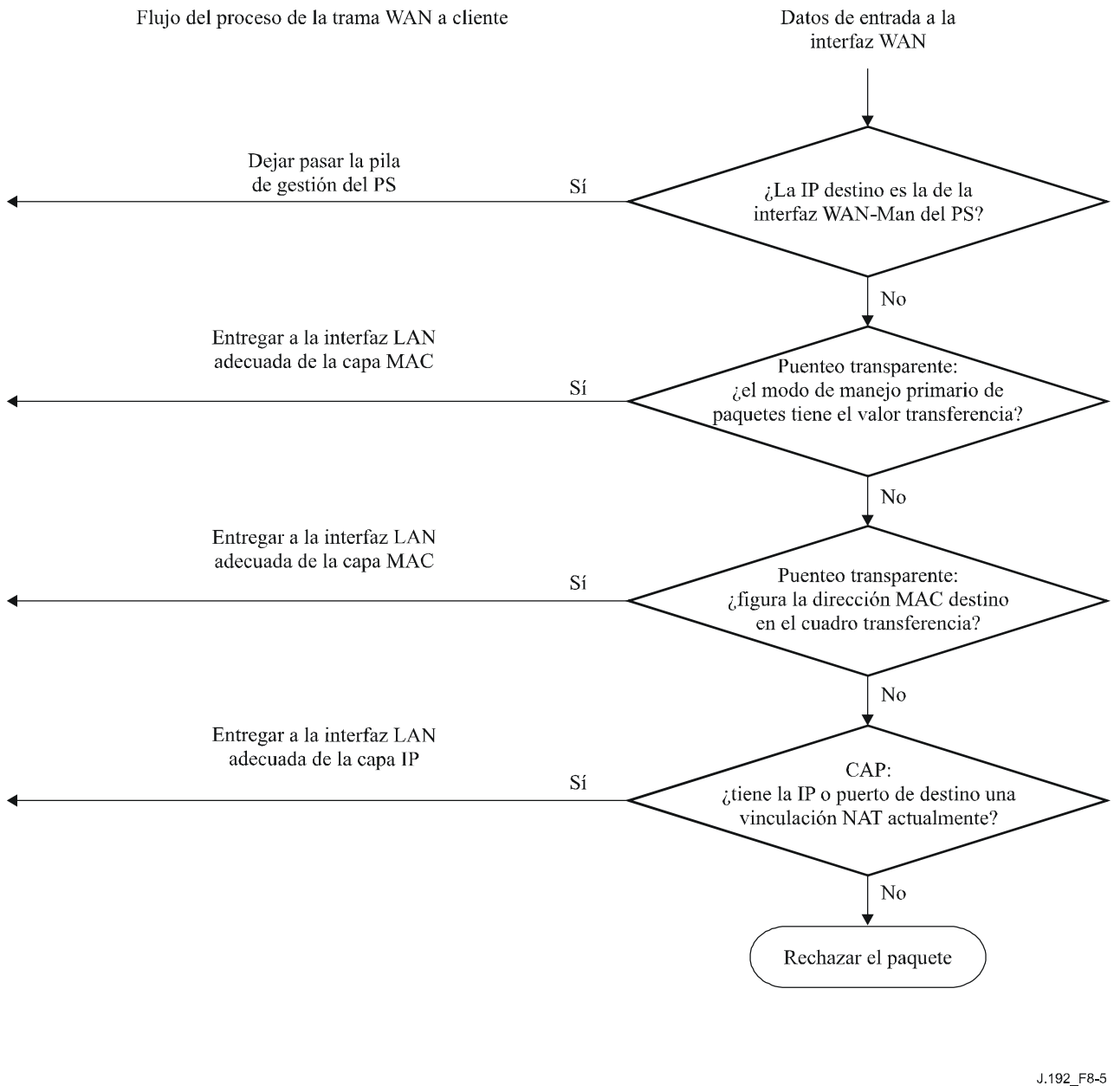


Figura 8-5/J.192 – Ejemplo de procesamiento de paquetes WAN-a-LAN

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. 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) entradas 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 entradas 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.

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 relativo al 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 soporte de la retransmisión de puerto estático

Cuando el modo primario de tratamiento de paquetes (cabhCapPrimaryMode) se fija a C-NAPT y hay una vinculación estática de C-NAPT con el número de puerto de la red WAN fijado a 0, en ese caso el PS DEBE traducir las direcciones IP especificadas en la vinculación de los paquetes que no estén asociados con una vinculación de C-NAPT dinámica o estática existente.

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).

El elemento PS DEBE obtener todas las direcciones IP LAN-Trans, IP LAN-Pass y MAC de los dispositivos IP de LAN asociados a cada una de sus interfaces de red físicas activas. Las direcciones IP y las direcciones MAC obtenidas por el elemento PS y los números de índice de la interfaz física del PS DEBEN ser accesibles al sistema NMS (a través del CMP) mediante ipNetToMediaTable [RFC 2011]. El elemento PS DEBE suprimir entradas de ipNetToMediaTable, cuando se alcance el límite temporal de inactividad.

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 de QoS y de acceso a los medios (QMA) (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.

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 sistema 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

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) 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. 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.

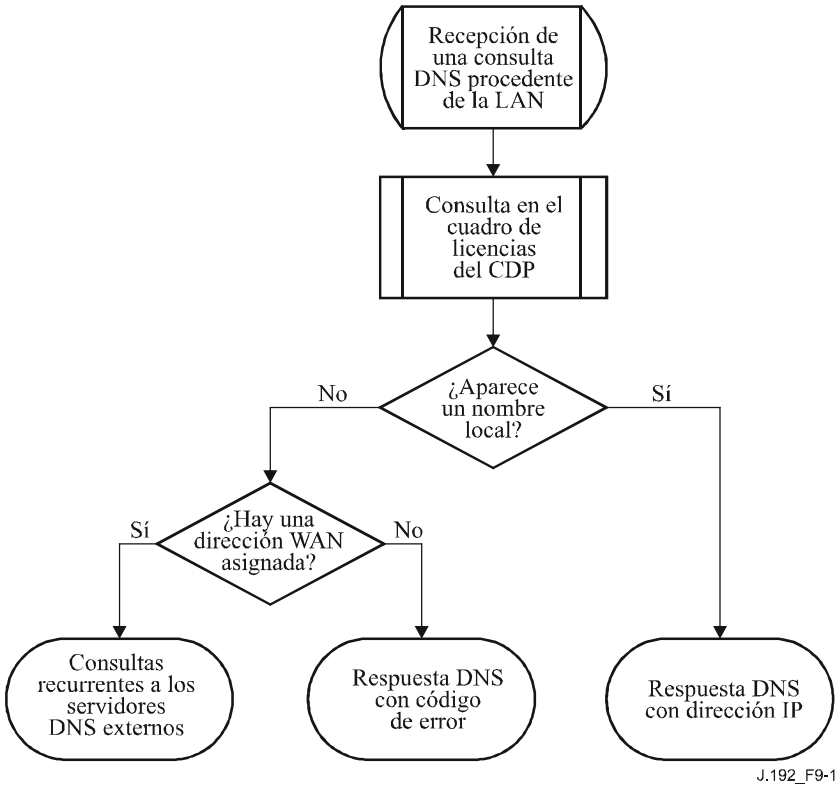


Figura 9-1/J.192 – Procesamiento de los paquetes del CNP

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).

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 cabhCdpServerDnsAddress.

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.

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.

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 entrada 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 de referencia DNS a los dispositivos IP de LAN.

10 Calidad de servicio

10.1 Introducción

En esta cláusula se describe el entorno de IPCable2Home que facilita las aplicaciones de funcionamiento en red doméstica utilizando recursos de QoS. Estos recursos representan 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.

En esta Recomendación se definen los requisitos de QoS necesarios para los elementos y subelementos del PS y del BP, que permiten a las aplicaciones establecer distintos niveles de QoS en la red doméstica y los operadores comunicar el tratamiento de prioridad deseado a las aplicaciones habilitadas con IPCable2Home en la red doméstica.

10.1.1 Objetivos

Los objetivos de la QoS de IPCable2Home son:

- Habilitar aplicaciones de funcionamiento en red doméstica que permitan establecer transmisión de datos con prioridades entre anfitriones, así como entre éstos y la pasarela residencial utilizando mensajería conforme.
- Habilitar aplicaciones de funcionamiento en red doméstica para establecer sesiones de datos con prioridades entre el CMTS y la pasarela residencial, utilizando mensajes conformes con IPCablecom.

10.1.2 Hipótesis

Se efectúan las siguientes hipótesis para la QoS de IPCable2Home:

- Para evitar problemas con las funciones de NAT del elemento CAP, las aplicaciones conformes con IPCablecom 1.0 deben utilizar direcciones de LAN-Pass de IPCable2Home conforme a las cláusulas 7 y 9.
- Las aplicaciones que podrían beneficiarse con la QoS podrán integrarse en los dispositivos del anfitrión de IPCable2Home conectados con la tecnología de funcionamiento en red doméstica.
- Las aplicaciones del anfitrión de IPCable2Home podrían incluir servicios de IPCablecom.

NOTA – Cualquier dispositivo que necesite recibir QoS para los servicios del operador habrá de cumplir con esta Recomendación 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 de elementos funcionales de IPCable2Home (PS y BP) y de subelementos en el PS y en los BP. Los desarrolladores de equipo de funcionamiento en red de IPCable2Home (por ejemplo, hardware y software) implementan uno o varios de estos elementos en función del conjunto de características deseadas para estos productos. Se requiere especificar conjuntos de capacidades mínimas para poder participar en el dominio Q. Los elementos básicos de CqoS se presentan en 10.2.2.

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.

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 un mecanismo que controle el acceso a la transmisión utilizando prioridades en los medios compartidos para los elementos lógicos PS y BP. 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 y que habrán de retransmitirse/reenviarse a través de las interfaces de LAN.
QoS 3	Gestión de las características de QoS: IPCable2Home especificará un mecanismo de señalización y gestión para la comunicación de las características de QoS entre el PS y los BP que necesiten QoS en una red doméstica. Este mecanismo se agregará y gestionará en el PS.

10.2.2 Descripción del sistema de QoS de IPCable2Home

La arquitectura de CqoS consta de las siguientes entidades:

- Dominio Q.
- Elemento de servicios de portal (PS).
- Elemento de punto de frontera (BP).
- Subelemento de portal de calidad de servicio de IPCable2Home (CQP).
- Subelemento de punto de frontera de calidad de servicio de IPCable2Home (QBP).

El equipo de la red de datos por cable gestiona las funciones de QoS de IPCable2Home pero no dentro del dominio Q.

10.2.2.1 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 las aplicaciones conformes con IPCable2Home. 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 características de QoS a distintos dispositivos en la red.

El CQP soporta además la distribución de mensajes de QoS a través de la red HFC para las aplicaciones de IPCablecom. Los mensajes conformes con IPCablecom incluyen mensajes de QoS y otros mensajes relativos a los aspectos de un servicio específico como es el caso de las decisiones de política y la aplicación de modelos de reservación de dos fases. (A partir de CH 1.0.)

10.2.2.2 Subelemento QBP

El elemento BP incluye un subelemento de punto de frontera de calidad de servicio de IPCable2Home (QBP). Éste asigna el acceso a los medios basado en las prioridades para el tráfico que origina el BP. Además, se encarga de la recepción de las características de QoS del PS.

10.2.2.3 Funcionalidad de QoS en CQP y QBP

Los subelementos CQP y QBP consisten en una o varias de las siguientes funcionalidades:

- **Retransmisión y acceso a los medios con prioridades de QoS (QFM)**: Especifica colas y retransmisión de paquetes con prioridades y acceso a medios compartidos con prioridades en el PS. Esta funcionalidad es parte sólo del PS.
- **Servidor de características de QoS (QCS)**: Esta funcionalidad se encarga de mantener un depósito de características de QoS para múltiples dispositivos y aplicaciones en la red doméstica y también de la comunicación de dichas características a esos dispositivos y aplicaciones. Esta funcionalidad forma parte sólo del PS.
- **Cliente de características de QoS (QCC)**: Esta funcionalidad, con el apoyo de QCS, determina las características de QoS que debe utilizar una aplicación/dispositivo particular. Reside sólo en el BP.

10.2.2.4 Dominio Q

El dominio Q define el ámbito de influencia directa de la funcionalidad de CQoS. Hay un dominio Q por cada vivienda y es independiente de los sectores de direccionamiento. Las viviendas particulares están separadas y tienen dominios Q independientes. Los elementos CQP y QBP delimitan el dominio Q en una vivienda determinada.

10.2.2.5 Clases de dispositivos físicos y elementos funcionalidades 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.

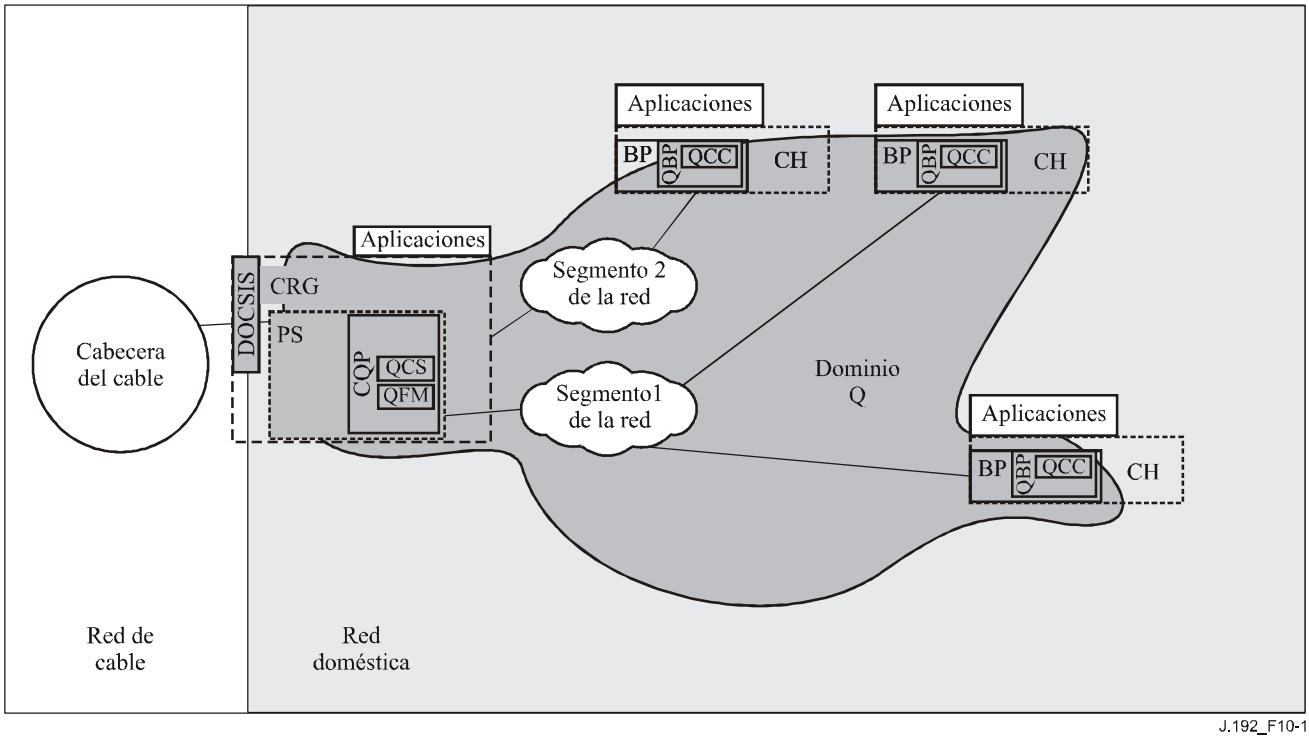


Figura 10-1/J.192 – Ejemplo de elementos funcionales de CqoS

10.2.2.6 Prioridades de IPCable2Home y sus correspondencias

10.2.2.6.1 Prioridades de IPCable2Home

En la presente Recomendación se definen tres prioridades de QoS distintas de IPCable2Home:

- prioridades genéricas;
- prioridades de las colas;
- prioridades de acceso a los medios.

10.2.2.6.1.1 Prioridades genéricas de IPCable2Home

En esta Recomendación se definen ocho niveles de prioridades genéricas de IPCable2Home, 0 a 7, siendo 7 el nivel más alto y 0 el más bajo. Los operadores de cable pueden asignar una de estas ocho prioridades a una aplicación. De los tres tipos de prioridades que se definen, el operador del sistema de cable puede establecer únicamente el valor de la prioridad genérica de IPCable2Home para una aplicación. Las otras dos prioridades, relativas a las colas y al acceso a los medios de IPCable2Home, se deducen a partir de la prioridad genérica de IPCable2Home, en función de las capacidades de hardware y de software en el dispositivo. Mientras más alta sea la prioridad genérica de IPCable2Home asignada a una aplicación, mayor será la preferencia asignada a los paquetes de esa aplicación para su retransmisión y para las funcionalidades de acceso a los medios.

10.2.2.6.1.2 Prioridades relativas a las colas de IPCable2Home

En el PS, los paquetes pueden provenir de múltiples interfaces y estar destinados a una sola interfaz. Por consiguiente, cada interfaz debe implementar una función de colas. 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 las colas 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 las colas de IPCable2Home. Esta prioridad debe identificarse por cada paquete que habrá de transmitirse por cada interfaz del PS, de manera que el paquete pueda colocarse en una cola adecuada. Esta prioridad orientada a colas se deduce de la prioridad genérica de

IPCable2Home asignada a la aplicación que envía el paquete, utilizando el número de colas soportadas por una interfaz del PS. Esta correspondencia se especifica en 10.2.2.6.2.

10.2.2.6.1.3 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 recibe una prioridad basándose en la prioridad asignada al paquete. Por consiguiente, una tecnología de medios compartidos debe soportar la QoS con prioridades de modo 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, HomePNA soporta ocho prioridades de acceso a los medios, HomePlug soporta cuatro prioridades). La prioridad de acceso a los medios de IPCable2Home relativa a los paquetes se deduce de su prioridad genérica en IPCable2Home basándose en el número de prioridades de acceso a los medios soportadas por la tecnología de medios compartidos de capa 2 de la interfaz. Esta correspondencia se determina en 10.2.2.6.3. Los valores de la prioridad de acceso a los medios de IPCable2Home son niveles lógicos que representan un nivel de preferencia que debería obtener un paquete de aplicación para el acceso a los medios. La correspondencia de las prioridades de acceso a los medios de IPCable2Home es independiente y distinta de las correspondencias de las prioridades de acceso a los medios nativas definidas por las tecnologías de medios compartidos de capa 2, para mantener la correspondencia de la prioridad de acceso a los medios de IPCable2Home independiente de las tecnologías de capa 2.

10.2.2.6.2 Correspondencia de las prioridades genérica de IPCable2Home a las prioridades de las colas de IPCable2Home

Como se explicó en 10.2.2.6.1.2, el PS aplica colas con prioridades a cada una de sus interfaces. Hay 8 prioridades genéricas de IPCable2Home definidas, por lo que el caso ideal sería que una interfaz tuviera 8 colas y a cada una se le asignara una prioridad de cola de 0 a 7. No obstante, el número de colas implementadas para una interfaz en el PS varía en función de la implementación. El número de colas soportadas por una interfaz se almacenará en la base de datos del PS y podrá leerse a través de un objeto cabhPriorityQosPsIfAttribIfNumQueues de la MIB. Si en una interfaz se implementan N ($1 \leq N \leq 8$) colas, las distintas colas en una interfaz se designarán con las prioridades de colas de IPCable2Home de 0 (la más baja) a N – 1 (la más alta). Cuando llega un paquete al PS, la prioridad de cola de IPCable2Home del paquete debe determinarse basándose en su prioridad genérica de manera que un paquete pueda colocarse en una cola adecuada. Esta correspondencia entre las dos prioridades se especifica en el cuadro 10-2.

En el cuadro 10-2, se expresan ocho prioridades genéricas en la primera columna. En las columnas adyacentes del cuadro, se presenta el número de colas soportadas por la interfaz como una gama de 8 a 1. Las anotaciones en el cuadro representan prioridades de las colas de IPCable2Home para los paquetes que van de 0 a N – 1.

Una vez determinada la prioridad de la cola de IPCable2Home de un paquete a partir de la prioridad genérica empleando el cuadro 10-2, el paquete se coloca en una cola designada para esa prioridad de cola de IPCable2Home particular.

Cuadro 10-2/J.192 – Correspondencia de las prioridades de las colas de IPCable2Home

Prioridad genérica de IPCable2Home	Número de colas soportadas por la interfaz (N)							
	8	7	6	5	4	3	2	1
7	7	6	5	4	3	2	1	0
6	6	5	4	3	3	2	1	0
5	5	4	3	2	2	1	1	0
4	4	3	2	2	2	1	1	0
3	3	2	1	1	1	1	0	0
2	2	1	1	1	1	0	0	0
1	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

NOTA – n el siguiente párrafo se ilustra cómo debería utilizarse la correspondencia de las prioridades de las colas de IPCable2Home.

Si un paquete de datos entrante tiene una prioridad genérica igual a 7, y se destina a una interfaz saliente que soporta únicamente tres colas (N = 3), en ese caso la prioridad de la cola de IPCable2Home para ese paquete sería 2. Las tres colas para esa interfaz particular se designarían con las prioridades '0' (inferior), '1' y '2' (superiores). Este paquete particular se colocaría en la cola con la designación de prioridad igual a dos para esa interfaz.

10.2.2.6.3 Correspondencia de las prioridades genéricas de IPCable2Home a las prioridades de acceso a los medios de IPCable2Home

Tal y como se analizó en 10.2.2.6.1.3, distintas tecnologías de capa 2 soportan un número variable de prioridades de acceso a los medios. Por consiguiente, las ocho prioridades genéricas de IPCable2Home definidas para las aplicaciones deben hacerse corresponder al número adecuado de prioridades de acceso a los medios de IPCable2Home, basándose en el número de prioridades de acceso a los medios ($1 \leq M \leq 8$) soportadas por una interfaz con tecnología de capa 2. El número de prioridades nativas de acceso a los medios (M) soportadas por la tecnología de medios compartidos de capa 2 particular de cada interfaz en el PS y en el BP se almacena en el PS y en el BP respectivamente. El número de prioridades de acceso a los medios soportadas por las interfaces del PS está disponible a través del objeto cabhPriorityQosPsIfAttribIfNumPriorities de la MIB en el PS. El número de prioridades de acceso a los medios soportadas por la interfaz BP está disponible en el PS a través del objeto cabhPsDevBpNumberInterfacesPriorties de la MIB. La correspondencia entre estas dos prioridades se indica en el cuadro 10-3.

El cuadro 10-3 es muy similar al cuadro 10-2, excepto que la correspondencia de los valores de la prioridad genérica de IPCable2Home se realiza utilizando el número de las prioridades de acceso a los medios (M) soportadas por una tecnología de medios compartidos de capa 2 particular. Las anotaciones en el cuadro representan las prioridades de acceso a los medios de IPCable2Home. Por consiguiente, si una tecnología de capa 2 soporta M prioridades de acceso a los medios, en ese caso las prioridades de acceso a los medios de IPCable2Home para esa tecnología irán de 0 (la más baja) a $M - 1$ (la más alta). Estos valores de prioridad de acceso a los medios de IPCable2Home representan niveles lógicos relativos. Mientras más alto sea el valor de la prioridad de acceso a los medios de IPCable2Home para el paquete, mayor será la preferencia que se debería conceder para el acceso a los medios compartidos. Los implementadores de esta Recomendación deberían asegurarse que a los paquetes se les otorgue el acceso preferencial relativo necesario a los medios compartidos, conforme a la correspondencia de las prioridades de acceso a los medios de IPCable2Home.

NOTA – En el siguiente párrafo se ilustra cómo debería utilizarse la correspondencia de las prioridades de acceso a los medios de IPCable2Home:

Si un valor de prioridad genérica de IPCable2Home para un paquete de aplicación es 7 (el más alto), y la tecnología de capa 2 con la que se ha de transmitir el paquete soporta 4 prioridades de acceso a los medios, haciendo referencia al cuadro 10-3, el valor de la prioridad de acceso a los medios de IPCable2Home para el paquete sería 3 (el más alto). No obstante, si un valor de prioridad genérica de un paquete es 2, el valor de la prioridad de acceso a los medios de IPCable2Home para la tecnología antes mencionada sería 1 (segundo valor más bajo). Anteriormente, la correspondencia de IPCable2Home necesaria podía ser distinta de las correspondencias nativas utilizadas por las tecnologías de medios compartidos.

Véase el apéndice I para encontrar ejemplos de las diferencias entre la correspondencia de la prioridad de acceso a los medios de IPCable2Home y las correspondencias de la tecnología de capa 2 nativa.

Cuadro 10-3/J.192 – Correspondencias de las prioridades de acceso a los medios de IPCable2Home

Prioridad genérica de IPCable2Home	Número de prioridades de acceso a los medios soportadas en la red LAN (N)							
	8	7	6	5	4	3	2	1
7	7	6	5	4	3	2	1	0
6	6	5	4	3	3	2	1	0
5	5	4	3	2	2	1	1	0
4	4	3	2	2	2	1	1	0
3	3	2	1	1	1	1	0	0
2	2	1	1	1	1	0	0	0
1	1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

10.3 CQP del subelemento lógico del PS

El CQP incluye las funcionalidades QFM y QCS que se muestran en la figura 10-1. La funcionalidad de QFM se describe en 10.3.1. Mientras que la correspondiente a QCS se describe en 10.3.2.

10.3.1 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 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 LAN para el 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 basándose en su prioridad y en las capacidades de los medios compartidos para el acceso mediante prioridades.

10.3.1.2 Directrices de diseño de la retransmisión y acceso a los medios con QoS

Cuadro 10-4/J.192 – Directrices de diseño del sistema QFM

Número	Directrices
QFM.1	La QFM debería aplicarse a los paquetes hacia y desde los sectores de direcciones de LAN-Trans y de LAN-Pass.
QFM.2	La QFM debe determinar la prioridad de los paquetes utilizando la información disponible en la MIB del PS que conserva el QCS.
QFM.3	La QFM debe 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	La QFM debe proporcionar acceso a los medios compartidos en cada interfaz, mediante prioridades, conforme a la prioridad de los paquetes.
QFM.6	La QFM debería traducir la prioridad genérica de IPCable2Home del paquete a la prioridad de acceso a los medios de IPCable2Home conforme a la correspondencia definida.
QFM.7	La QFM debería poder utilizar interfaces que acepten distintos números de prioridades para el acceso a los medios.

10.3.1.3 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.

10.3.1.4 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 desde el PS a un anfitrión de la red LAN 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 por la red LAN doméstica pueden disponer de acceso con prioridad a las interfaces de transmisión del anfitrión y a los medios compartidos de la red LAN. Cualquier paquete que sale del PS por una interfaz de LAN debería ser procesado por la QFM sin tener en cuenta su origen.

Una vez que la QFM recibe un paquete destinado a una interfaz LAN particular, realiza las siguientes tres acciones antes de que el paquete se transmita a la interfaz LAN de destino:

1) proceso de clasificación para identificar la prioridad genérica del paquete;
2) establecimiento de una cola con prioridad;
3) acceso a los medios con prioridad.

10.3.1.4.1 Clasificación de los paquetes para identificar la prioridad genérica de IPCable2Home

Cuando el PS tiene necesidad de transmitir un paquete por la interfaz LAN, primero lo examina para poder identificar su prioridad genérica de IPCable2Home. El PS lee la dirección IP y el puerto de destino del paquete. La base de datos del PS tiene un cuadro clasificador (cabhPriorityQosDestPriorityListTable) que utiliza valores de la dirección IP y del puerto de destino que permiten determinar la prioridad genérica del paquete. El comodín (0) podrá utilizarse en el campo puerto de destino pero no en la dirección IP de destino. Por consiguiente, el PS intenta

encontrar en primer lugar una anotación particular que haga concordar la dirección IP y el puerto de destino para determinar la prioridad. Si la anotación específica no se encuentra, el PS trata de determinar la prioridad utilizando únicamente la dirección IP de destino. Si no se encuentra una anotación en el cuadro clasificador de la dirección IP y el puerto de destino del paquete, en ese caso el PS asigna un valor 0 como prioridad genérica del paquete. El PS utiliza el valor de prioridad genérica de IPCable2Home asignado para determinar la prioridad de la cola de IPCable2Home del paquete y la prioridad de acceso a los medios de IPCable2Home.

10.3.1.4.2 Colas 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 valores de la prioridad genérica de IPCable2Home que se definen en esta Recomendación. Por lo tanto, el PS hace corresponder el valor de la prioridad genérica de IPCable2Home del paquete al valor de la prioridad de la cola de IPCable2Home como se define en 10.2.2.6.1.2. A continuación el PS coloca el paquete en una cola adecuada de la interfaz de destino que corresponde a este valor de prioridad de cola de IPCable2Home para el que se estableció una correspondencia.

El QFM interroga a todas las colas de cada interfaz saliente conforme a sus prioridades para 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.

10.3.1.4.3 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 de la prioridad genérica de IPCable2Home del paquete al valor de la prioridad de acceso a los medios de IPCable2Home como se explicó en 10.2.2.6.3, utilizando el cuadro 10-3. 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.

10.3.1.4.4 Soporte de las aplicaciones de IPCablecom

Como el objetivo de la QoS es ofrecer calidad de servicio únicamente en la red doméstica, esta Recomendación no da ninguna consideración especial a la QoS de la red de acceso. No obstante, un dispositivo IP de LAN puede contener una aplicación de IPCablecom [J.161], [J.163], en cuyo caso el PS podrá configurarse para el tratamiento de paquetes en modo de transferencia para puentear los mensajes de QoS entre la aplicación de IPCablecom en la red doméstica y el sistema CMTS.

Como el PS simplemente retransmitirá los mensajes de QoS de IPCablecom durante el modo de transferencia, no habrá dependencia del NMS para soportar esa función. Por consiguiente, esta función CQP se mantiene idéntica para ambos modos de configuración DHCP y SNMP (véase 5.5).

10.3.1.5 Requisitos de la retransmisión y el acceso a los medios con QoS

10.3.1.5.1 Requisitos de clasificación de los paquetes

Cuando el PS tenga necesidad de transmitir un paquete por una interfaz de LAN, el PS DEBE determinar la prioridad genérica de IPCable2Home de ese paquete a partir de sus valores de

dirección IP y puerto de destino utilizando el cuadro clasificador del PS, (cabhPriorityQosBpDestTable) almacenado en la base de datos del PS (véase E.7). En todos los casos el PS DEBE tratar de encontrar una anotación particular en la base de datos del PS que concuerde con la dirección de IP y el puerto de destino del paquete para determinar la prioridad. Si no se encuentra una anotación específica el PS DEBE tratar de encontrar otra que concuerde únicamente con la dirección IP de destino del paquete. Si no existe tal anotación el PS DEBE asignar el valor 0 a la prioridad genérica de IPCable2Home del paquete.

10.3.1.5.2 Requisitos de las colas con prioridad

El PS DEBE almacenar en la base de datos del PS el número de colas implementadas por cada una de sus interfaces, información a la que podrá accederse a través de una MIB cabhPriorityQosPsIfAttribIfNumQueues (véase E.7).

El PS DEBE hacer corresponder el valor de la prioridad genérica de IPCable2Home del paquete identificado durante el proceso de clasificación al valor de la prioridad de la cola de IPCable2Home que se define en 10.2.2.6.1.2 utilizando el número de colas (cabhPriorityQosPsIfAttribIfNumQueues) implementadas en la interfaz por la que se transmitirá el paquete. El PS DEBE poner el paquete de manera adecuada en la cola de interfaz de destino de acuerdo con el valor de prioridad de cola de IPCable2Home para el que se haya establecido una 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.

10.3.1.5.3 Requisitos de acceso a los medios 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 cabhPriorityQosPsIfAttribIfNumPriorities (véase E.7).

Después de que el paquete se extrae de las colas de una interfaz particular PS DEBE hacer corresponder la prioridad genérica del paquete a la prioridad de acceso a los medios de IPCable2Home, como se describe en 10.2.2.6.1.3, utilizando el número de prioridades de acceso a los medios (cabhPriorityQosPsIfAttribIfNumPriorities) que soporta esa interfaz. El PS DEBE transmitir el paquete mediante la tecnología de medios compartidos de modo que se mantenga el acceso preferencial relativo a los medios, como lo exige el valor de la prioridad de acceso a los medios de IPCable2Home.

10.3.1.5.4 Requisitos del soporte de aplicaciones de IPCablecom

El PS DEBE comportarse como un puente transparente y retransmitir los mensajes de QoS de IPCablecom [J.161], [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).

10.3.2 Servidor de características de QoS del PS (QCS)

La funcionalidad de este servidor en el PS se encarga de la gestión de las prioridades de la aplicación en la red doméstica en representación del operador del sistema de cable. En esta cláusula se presenta la descripción de la funcionalidad de QCS y de los requisitos del PS asociados.

10.3.2.1 Objetivos del servidor de características de QoS

- Establecer un conjunto de criterios mediante los cuales las aplicaciones y las pilas de protocolos de la red puedan asignar y utilizar características de QoS para el tráfico en la red doméstica.
- Ofrecer un mecanismo para que la cabecera comunique las características de QoS deseadas al PS y a continuación a los anfitriones de IPCable2Home (BPs). En forma particular, la asignación de las características de QoS se relaciona a la información de las prioridades por tipo de aplicación.

10.3.2.2 Directrices de diseño del servidor de características de QoS

Cuadro 10-5/J.192 – Directrices de diseño del QCS

Número	Directrices
QCS.1	El servidor de gestión de red (NMS) en el encabezamiento debe proporcionar la información de las prioridades de cada aplicación al QCS
QCS.2	Los operadores del sistema de cable deben controlar la información de las prioridades suministrada al QCS (PS particular o control de actualización de mass PS)
QCS.3	La cabecera podrá actualizar la información de las prioridades suministrada al QCS y los BP (QCC) obtendrán esta información actualizada del QCS
QCS.4	El QCS utilizará un protocolo de contenido de mensaje definido (XML) y un protocolo de transporte de mensajes (SOAP) para la distribución de la información de las prioridades a los BP
QCS.5	El QCS debe utilizar una interfaz de contenido de mensaje definida (MIB) para proporcionar información de las prioridades de diversas aplicaciones en la red LAN doméstica al servidor de gestión de la red (NMS) en el encabezamiento
QCS.6	El QCS complementa la funcionalidad de retransmisión y acceso a los medios con QoS (QFM) para determinar una prioridad del paquete de la aplicación

10.3.2.3 Hipótesis relativas al servidor de características de QoS

- IPCable2Home define un formato para el intercambio de mensajes entre el PS y el BP.
- IPCable2Home define un protocolo para el intercambio de información entre el PS y el BP.
- Los anfitriones de IPCable2Home pueden tener más de un servicio/aplicación.

10.3.2.4 Descripción del sistema relativo al servidor de características de QoS

El QCS mantiene una "base de datos" de la información en la base de datos del PS como se describe en 5.4. El QCS recibe información de prioridades de la aplicación desde el encabezamiento, a través de la configuración inicial del PS, o a través de una interfaz MIB en el CMP. Además, el QCS recoge información de la aplicación de diversos BP en la red LAN doméstica y les asigna prioridades. El QCS comunica esta información a los BP (QCC) que se utilizará para que los BP puedan acceder a los medios mediante prioridades. La información mantenida por el QCS la emplea la funcionalidad de QFM en el PS para el acceso a los medios y la retransmisión con prioridades de los paquetes que pasan por ella.

El resto de 10.3.2.4 se dedica a la descripción del intercambio de información que se produce entre el encabezamiento y el PS por la red WAN y entre el PS y los BP por la red LAN.

10.3.2.4.1 Intercambio de información de WAN

Desde el lado de la red WAN, la cabecera del operador del sistema de cable proporciona al PS la correspondencia de distintas aplicaciones y las prioridades que deberían utilizarse en un fichero de configuración o empleando SNMP SET. El NMS, en el encabezamiento, puede leer y actualizar (cambiar/modificar/suprimir) estas prioridades de la aplicación en la base de datos del PS utilizando SNMP a través de la interfaz de la MIB.

10.3.2.4.1.1 Envío de la correspondencia del ID de aplicación a la prioridad genérica de IPCable2Home entre la cabecera y el PS

El encabezamiento proporciona al PS una lista de los ID de aplicación y sus prioridades genéricas de IPCable2Home que el operador del cable desea que se utilicen en estas aplicaciones. 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 el encabezamiento. El PS almacena esta información en su base de datos a la que puede accederse a través de un cuadro de la MIB, cabhPriorityQosMasterTable (véase E.7). El PS lo utiliza como un cuadro maestro para identificar las prioridades de distintas aplicaciones en los BP de la red LAN doméstica.

El PS también puede recibir peticiones del NMS para actualizar (añadir/modificar/suprimir) estas prioridades genéricas de IPCable2Home para las aplicaciones en su cuadro maestro utilizando SNMP. En respuesta a esas peticiones, el PS actualiza (añade/modifica/suprime) el cuadro maestro de prioridades (cabhPriorityQosMasterTable). Dichas actualizaciones a las prioridades de la aplicación se comunican a los BP durante intercambios de información de LAN subsiguientes, lo que se describe en 10.3.2.4.2.

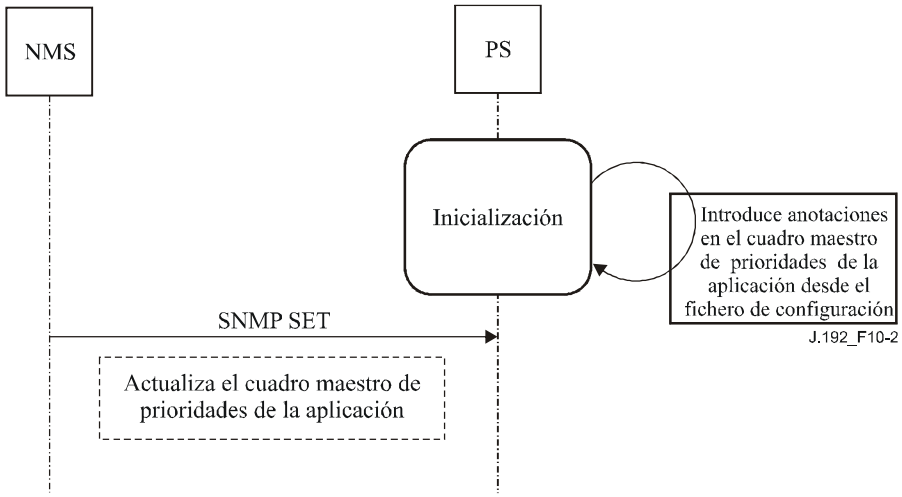


Figura 10-2/J.192 – Intercambio y procesamiento de información de la WAN en el PS

10.3.2.4.2 Intercambio de información de LAN

En el lado de la LAN, un BP comunica al PS su información relativa a las aplicaciones y sesiones (dirección IP y puerto de destino) a fin de obtener sus prioridades. Cuando el PS recibe esta información, determina las prioridades apropiadas consultándolas en el cuadro maestro de prioridades y enviándoselas al BP. Esta información se intercambia entre el PS y el BP utilizando el método QoSProfile XML (que se describe en 10.3.2.4.2.1) y los mensajes de SOAP iniciados por el BP (operación BP_Init) como se describe en 6.3.3.4.3.2.

10.3.2.4.2.1 Esquema de QoSProfile XML

Este método incluye dos secuencias complejas de XML: QoSApplicationList y DesPriorityList. La primera incluye cuatro elementos: BpIpAddress, ApplicationId, DefaultCHpriority y una secuencia de DestPriorityList. El tipo complejo DestPriorityList, el cual está considerado como una secuencia secundaria de QoSApplicationList, incluye tres elementos: DestIp, DestPort e IpPortPriority. Cada uno de los elementos tiene un tipo definido como se indicó en el cuadro 10-6. Los tipos definidos son referencias de las definiciones del esquema de W3C XML [XML].

El elemento ApplicationId es el número de puerto del servidor de aplicaciones de cada aplicación BP asignada por el organismo de asignación de números Internet (IANA) [IANAPort]. No obstante que las aplicaciones se identifican mediante el número de puerto asignado por IANA, también es posible que la comunicación tenga lugar por otros números de puerto. El BP comunica al PS una relación de los ApplicationIds de todas las aplicaciones instaladas en él mediante el mensaje BP_Init (que se describe en 10.4.1.4.1.1).

El elemento DefaultCHpriority es la prioridad de IPCable2Home por defecto de una aplicación. El BP puede asignar un valor para este elemento en QoSProfile. Ese valor será suprimido por el valor que suministre el PS, mediante el mensaje BP_Init_Response (que se describe posteriormente en 10.3.2.4.2.3), tras consultar el cuadro maestro de prioridades de las aplicaciones en la base de datos del PS (cabhPriorityQosMasterTable).

El BP incluye las secuencias DestPriorityListEntry en el QoSProfile de una sesión de aplicación con otro dispositivo. Estas secuencias se asocian al elemento ApplicationId en el esquema de QoSProfile XML. Los elementos DestIP y DestPort, respectivamente, corresponden a la dirección IP y el número de puerto de destino de la sesión de la aplicación (conexión socket) que ha sido establecida por el BP. Estas anotaciones se utilizan para determinar la prioridad (IpPortPriority) del tráfico, que pasa a través del PS, basándose en la dirección IP y el número de puerto de destino específicos según se especifique en la anotación. El comodín (0) se permite únicamente para DestPort, pero no para DestIP. El BP puede proporcionar un valor para el elemento IpPortPriority en el QoSProfile. El PS sustituye ese valor con DefaultCHpriority, suministrado en el mensaje BP_Init_Response, después de consultar el cuadro maestro de prioridades de la aplicación en la base de datos del PS (cabhPriorityQosMasterTable).

En todos los casos es necesario que un BP transmita todo el esquema de QoSProfile XML al PS cuando envíe el mensaje BP_Init.

Cuadro 10-6/J.192 – Esquema de QoSProfile XML

```
<xs:complexType name= "ch:QoSProfile"/>
      <xs:element name ="ch:QoSApplicationList"   type="ch:QoSApplicationListEntry minOccurs="1"
maxOccurs="4"/>"
</xs:complexType>


<xs:complexType name= "ch:QoSApplicationListEntry>
   <xs:sequence>
        <xs:element name="ch:BpIpAddress"              type="xs:string"/>
        <xs:element name="ch:ApplicationId"             type="xs:int"/>
        <xs:element name="ch:DefaultCHPriority"        type="xs:int"/>
        <xs:element name="ch:DestPriorityList"   type="ch:DestPriorityListEntry minOccurs="0"
maxOccurs="4"/>"
    </xs:sequence>
</xs:complexType>
```

Cuadro 10-6/J.192 – Esquema de QoSProfile XML

```
<xs:complexType name= "ch:DestPriorityListEntry>
   <xs:sequence>
        <xs:element name="ch:DestIp"            type="xs:string"/>
        <xs:element name="ch:DestPort"          type="xs:int"/>
        <xs:element name="ch:IpPortPriority"    type="xs:int"/>
    </xs:sequence>
</xs:complexType>
```

10.3.2.4.2.2 Intercambio de información del BP al PS utilizando el mensaje BP_Init

Un BP debe enviar información de sus aplicaciones y sus sesiones al PS en el formato del esquema QoSProfile XML utilizando el mensaje BP_Init, según se describe en 6.3.3.4.3.2.1, en los siguientes tres casos distintos:

- obtención o renovación de una licencia DHCP;
- actualización de la aplicación (adición o supresión) en un BP;
- establecimiento y terminación de la sesión de aplicación con otro dispositivo mediante un BP.

Véase 10.4.1.4.1.1.1 para obtener una descripción detallada del intercambio de información del BP en cada uno de los tres casos antes referidos.

10.3.2.4.2.3 Intercambio de información relativa a la prioridad del PS y al BP utilizando BP_Init_Response

El procesamiento del esquema QoSProfile XML mediante el PS es exactamente el mismo en los tres casos distintos (mencionados anteriormente en 10.3.2.4.2.2), cuando se recibe el mensaje BP_Init. A continuación se describe el procesamiento del esquema QoSProfile XML:

Cuando se recibe el esquema QoSProfile XML del BP en el mensaje BP_Init, el PS determina los valores para los elementos DefaultCHPriority (parte de QoSApplicationListEntry) e IpPortPriority (parte de DestPriorityListEntry) de todas las aplicaciones en el QoSProfile consultando el cuadro maestro de prioridades en la base de datos del PS (cabhPriorityQosMasterTable). El PS actualiza el QoSProfile del BP con esas prioridades suprimiendo los valores que el BP haya proporcionado en su QoSProfile original.

A continuación, el PS almacena esta información de prioridades de la aplicación del BP, representada por el QoSProfile actualizado, en la base de datos del PS a la que puede accederse a través de los cuadros de la MIB, cabhPriorityQosBpTable y cabhPriorityQosBpDestTable (véase E.7). El PS sustituye completamente la información antigua de prioridad de la aplicación del BP que pueda haberse almacenado en su base de datos con la nueva información representada por el QoSProfile actualizado. Dicha sustitución incluye el procesamiento de la adición así como de la supresión de una nueva aplicación o de una sesión en el BP y mantiene la complejidad del procesamiento en el PS a un nivel mínimo.

El cuadro cabhPriorityQosBpTable representa la información relativa a las distintas aplicaciones y sus prioridades en un BP particular en la red doméstica. El cuadro cabhPriorityQosBpDestTable representa las prioridades particulares de la dirección IP y el puerto de destino para las distintas sesiones de aplicación del BP. La funcionalidad de la QFM en el PS utiliza la información representada por cabhPriorityQosBpDestTable para el acceso con prioridad a los medios y las colas en el PS.

Tras haber actualizado la base de datos con la información de la prioridad de la aplicación del BP, el PS envía al BP el QoSProfile del BP, actualizado con la información de la prioridad, utilizando el mensaje BP_Init_Response como se describe en 6.3.3.4.3.2.2. El QoSProfile actualizado lleva al BP la información de prioridad apropiada necesaria para que sea utilizada por sus aplicaciones.

10.3.2.5 Requisitos del servidor de características de QoS

10.3.2.5.1 Requisitos del intercambio de información de la WAN

El PS DEBE almacenar una relación de los Id de aplicación y de sus prioridades genéricas de IPCable2Home, proporcionadas por el operador del sistema de cable, en la base de datos del PS, a la que puede accederse a través de un cuadro maestro de la MIB relativa a las prioridades de la aplicación, cabhPriorityQosMasterTable (véase E.7). El PS DEBE soportar actualizaciones (añadir/modificar/suprimir) de su cuadro maestro de prioridades (cabhPriorityQosMasterTable) a través de un fichero de configuración en el momento de la inicialización del PS, o a través de instrucciones SNMP SET desde el encabezamiento.

10.3.2.5.2 Requisitos de intercambio de información de la LAN

El procesamiento del esquema QoSProfile XML mediante el PS es idéntico en los tres casos distintos (mencionados en 10.3.2.4.2.2), cuando se recibe el mensaje BP_Init.

El PS DEBE ser capaz de procesar el esquema QoSProfile XML del BP (como se describe en 10.3.2.4.2.1) que incluye la información de sus aplicaciones y sesiones (dirección IP y puerto de destino) recibida en el mensaje BP_Init (como se describe en 6.3.3.4.3.2). Cuando el PS recibe el esquema QoSProfile XML del BP (en cualquiera de los tres casos descritos en 10.3.2.4.2.2) en el mensaje BP_Init, el PS DEBE determinar valores para los elementos DefaultCHPriority (parte de QoSApplicationListEntry) e IpPortPriority (parte de DestPriorityListEntry) de todas las aplicaciones en el QoSProfile consultando el cuadro maestro de prioridades en la base de datos del PS (cabhPriorityQosMasterTable). El PS DEBE actualizar el QoSProfile del BP con estos valores de prioridad sustituyendo los valores que el BP pudiera haber proporcionado en su QoSProfile original.

A continuación PS DEBE almacenar esta información de prioridad de la aplicación del BP, representada por el QoSProfile actualizado, en la base de datos del PS a la que puede accederse a través de los cuadros de la MIB, cabhPriorityQosBpTable y cabhPriorityQosBpDestTable (véase E.7). El PS DEBE sustituir completamente la información antigua de prioridad de la aplicación del BP que pueda haber sido almacenada en su base de datos, con la nueva información representada por el QoSProfile actualizado.

Tras haber actualizado la base de datos del PS con la información de prioridad de la aplicación del BP, el PS DEBE enviar el BP todo el QoSProfile del BP, actualizado con la información de prioridad, utilizando el mensaje BP_Init_Response, como se describe en 6.3.3.4.3.2.2.

10.4 QBP del subelemento lógico del BP

10.4.1 Cliente de características de QoS (QCC)

10.4.1.1 Objetivos del cliente de características de QoS

- Ofrecer un mecanismo para que un anfitrión de IPCable2Home reciba las características de QoS deseadas del PS. Estas características de QoS las comunica el encabezamiento al PS.
- Establecer un conjunto de criterios en un anfitrión de IPCable2Home mediante los cuales sus aplicaciones y pilas de protocolos de red puedan asignar y utilizar características de QoS para su tráfico de aplicación.

10.4.1.2 Hipótesis del sistema relativo al cliente de características de QoS

Un anfitrión conforme a IPCable2Home (BP) puede tener más de un servicio o aplicación.

10.4.1.3 Directrices del sistema relativo al cliente de características de QoS

Cuadro 10-7/J.192 – Directrices de diseño de QCC

Número	Directrices
QCC.1	El QCS debe proporcionar información relativa a las prioridades de la aplicación al QCC.
QCC.2	Las prioridades controladas por el QCS se actualizan de modo dinámico y el QCC debe solicitar información relativa a las prioridades actualizadas del QCS.
QCC.3	El QCC debe utilizar un protocolo de contenido de mensaje definido (XML) y un protocolo de transporte de mensajes (SOAP) para comunicar la información de las prioridades al PS.
QCC.4	El QCC debe ofrecer acceso con prioridades a los medios compartidos de su interfaz LAN conforme a la prioridad del paquete.

10.4.1.4 Descripción del sistema del cliente de características de QoS

En esta cláusula se presenta una síntesis de los conceptos esenciales del cliente de características de QoS (QCC) en el BP.

Los mensajes del QCC están estrechamente relacionados con los mensajes del QCS que se describieron en 10.3.2.4.2. El QCC en el BP es la contraparte del QCS en el PS. El QCC realiza todos los intercambios de mensajes de QoSProfile con el PS (como se describe en 10.3.2.4.2) en representación del BP, utilizando mensajes SOAP iniciados por el BP (véase 6.3.3.4.3.2). De esta manera, el QCC obtiene información relativa a las prioridades de diversas aplicaciones y sesiones de aplicación en el BP. El QCC dispone de una base de datos interna para almacenar la información de la prioridad de la aplicación que recibe del QCS, y la emplea para asignar prioridades a los trenes de su aplicación.

Además, el QCC se encarga de establecer la correspondencia entre la prioridad genérica de IPCable2Home del paquete de aplicación y la prioridad de acceso a los medios de IPCable2Home, utilizando el número de prioridades de acceso a los medios que soporta la interfaz del BP, como se especifica en 10.2.2.6.3.

El QCC se encarga de las dos funciones principales del BP que son:

- Intercambio de información de LAN.
- Acceso a los medios con prioridad para las aplicaciones del BP.

NOTA – El resto de 10.4.1.4 se centra en la descripción de estas dos funciones esenciales del QCC.

10.4.1.4.1 Intercambio de información de LAN

Como se describió en 10.3.2.4.2, el BP necesita comunicar al PS la información relativa a sus aplicaciones y sesiones (dirección IP y puerto de destino) a fin de obtener sus prioridades. Después de que el PS envía la información de las prioridades al BP, almacena esta información en su base de datos y la utiliza para el acceso a los medios con prioridades. Es necesario que el BP envíe su información al PS, utilizando el esquema QoSProfile XML (descrito en 10.3.2.4.2.1) y los mensajes de SOAP iniciados por el BP (funcionamiento BP_Init), como se describe en 6.3.3.4.3.2.

10.4.1.4.1.1 Envío de información del BP al PS utilizando mensajes BP_Init

En todos los casos es necesario que un BP envíe su información al PS en el formato del esquema QoSProfile XML (cuadro 10-6), utilizando mensajes BP_Init, como se describe en 6.3.3.4.3.2.1. Un BP siempre envía todo su esquema QoSProfile al PS. Como se describe en 10.3.2.4.2.2, es

necesario que un BP envíe al PS un mensaje BP_Init con todo su esquema QoSProfile en los siguientes tres casos distintos:

- obtención o renovación de licencia de DHCP;
- actualización de aplicación (adición o supresión) en un BP;
- establecimiento o terminación de la sesión de aplicación con otro dispositivo mediante un BP.

10.4.1.4.1.1.1 Envío de información del dispositivo y la aplicación del BP al PS durante la obtención o renovación de la licencia de DHCP del BP

Cuando un BP recibe un mensaje DHCPACK [RFC 2131] dirigido a él mismo, en el momento de obtención o renovación de la licencia DHCP, debe enviar la información de prioridad de su dispositivo y de su aplicación al PS, utilizando mensajes BP_Init. La información relativa al dispositivo del BP se envía utilizando el esquema XML del perfil del dispositivo (definido en 6.5.3.1.4), y la información relativa a la prioridad de la aplicación se envía utilizando el método QoSProfile XML.

El perfil del dispositivo del BP que se envía al PS incluye ciertas prioridades de acceso a los medios (elemento XML: numberMedia AccessPriorities) soportadas por una interfaz en un BP. Este intercambio y procesamiento de información se describe en 6.5.3.3, "Función de determinación de MBP". Utilizando esta información, el PS rellena la MIB cabhPsDevBpNumberInterfacePriorities (véase E.4), que forma parte de la MIB cabhPsDevBpProfileTable (véase E.4).

El QoSProfile del BP enviado al PS tras la obtención o renovación de la licencia DHCP del BP, incluye una relación de las aplicaciones en el BP (QoSApplicationListEntry). También puede contener facultativamente anotaciones específicas de la dirección IP y el puerto de destino (DestPriorityListEntry) asociadas a una aplicación. Esta información utiliza el formato conforme al esquema QoSProfile XML, que se describe en el cuadro 10-6. Facultativamente, el BP puede proporcionar valores para los elementos XML DefaultCHPriority e IpPortPriority.

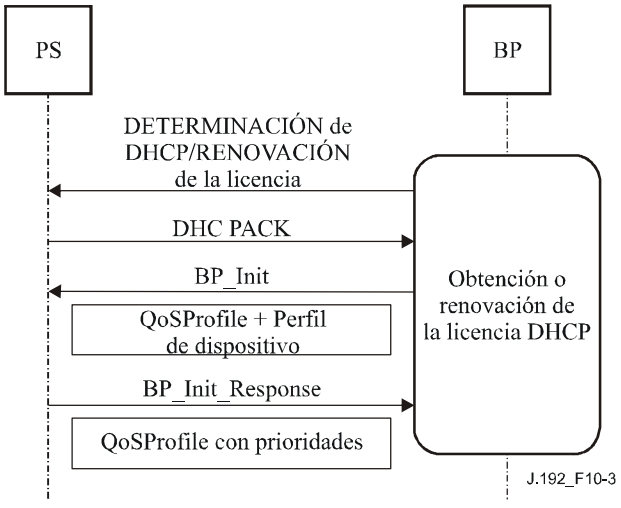


Figura 10-3/J.192 – Intercambio de información durante la obtención o renovación de la licencia del BP

10.4.1.4.1.1.2 Envío de información de aplicación del BP al PS durante la actualización de la aplicación en el BP

Cuando se añade una nueva aplicación al BP, éste inserta una anotación para su aplicación (QoSApplicationListEntry) a su esquema QoSProfile XML existente. El BP también puede rellenar facultativamente el elemento DefaultCHPriority asociado con este ApplicationId en el QoSProfile.

También puede incluir la secuencia DestPriorityListEntry para este ApplicationId. El BP tiene que enviar este nuevo esquema QoSProfile XML al PS usando un mensaje BP_Init.

Cuando se suprime una aplicación del BP, éste necesita suprimir a su vez todas las anotaciones (QoSApplicationListEntry así como DestPriorityListEntry) relativas a esa aplicación particular de su QoSProfile. En ese caso el BP necesita enviar el QoSProfile modificado al PS utilizando mensajes BP_Init.

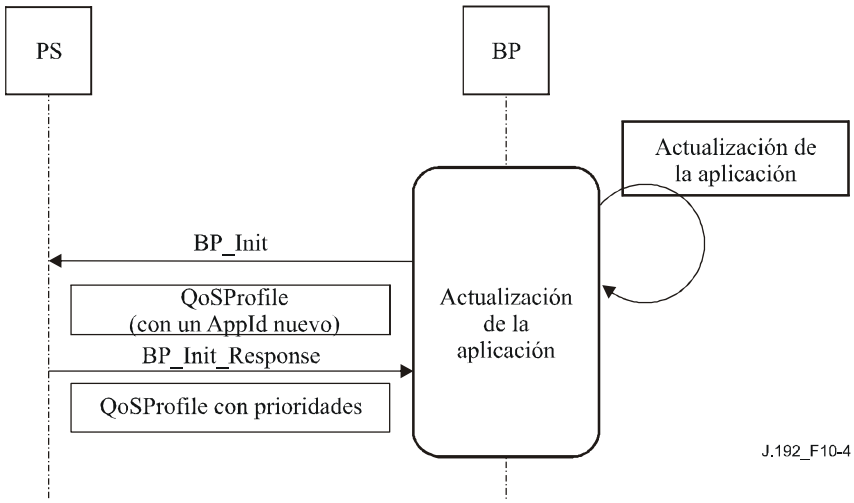


Figura 10-4/J.192 – Intercambio de información durante la actualización de la aplicación del BP

10.4.1.4.1.1.3 Envío de información de la aplicación del BP al PS durante el establecimiento o terminación de la sesión de la aplicación

Después de que una aplicación de un BP establece una sesión con otro dispositivo, el BP añade la información de la dirección IP y del puerto de destino de la sesión, (DestPriorityListEntry) asociada a esa aplicación (ID de la aplicación) en su esquema QoSProfile XML (cuadro 10-6). El BP puede rellenar facultativamente el elemento IpPortPriority en DestPriorityListEntry. A continuación, el BP envía este esquema QoSProfile XML al PS utilizando mensajes BP_Init para que el PS pueda introducir anotaciones en su cuadro clasificador (cabhPriorityQosBpDestTable), tras identificar una prioridad (IpPortPriority) para la anotación utilizando el cuadro maestro de prioridades. Estas anotaciones del clasificador las utiliza la funcionalidad de QFM en el PS para determinar las prioridades de los paquetes examinando su dirección IP y puerto de destino (si se da el caso de que pasen a través del PS). Utilizando estas anotaciones en el cuadro del clasificador, la QFM ejecuta el acceso a los medios y las colas con prioridad como se describe en 10.3.1.4.

Cuando el BP da por terminada una sesión, suprime la anotación particular de la dirección IP y del puerto de destino correspondiente, DestPriorityListEntry, de su esquema QoSProfile XML y envía este QoSProfile actualizado al PS utilizando mensajes BP_Init de modo que el PS pueda suprimir las anotaciones en su cuadro clasificador.

Estas anotaciones particulares de dirección IP y de puerto de destino en el cuadro clasificador del PS (cabhPriorityQosBpDestTable) pueden utilizarse para ofrecer la retransmisión de los paquetes y el acceso a los medios con prioridad para el tráfico que va del PS a un dispositivo de sólo recepción no conforme.

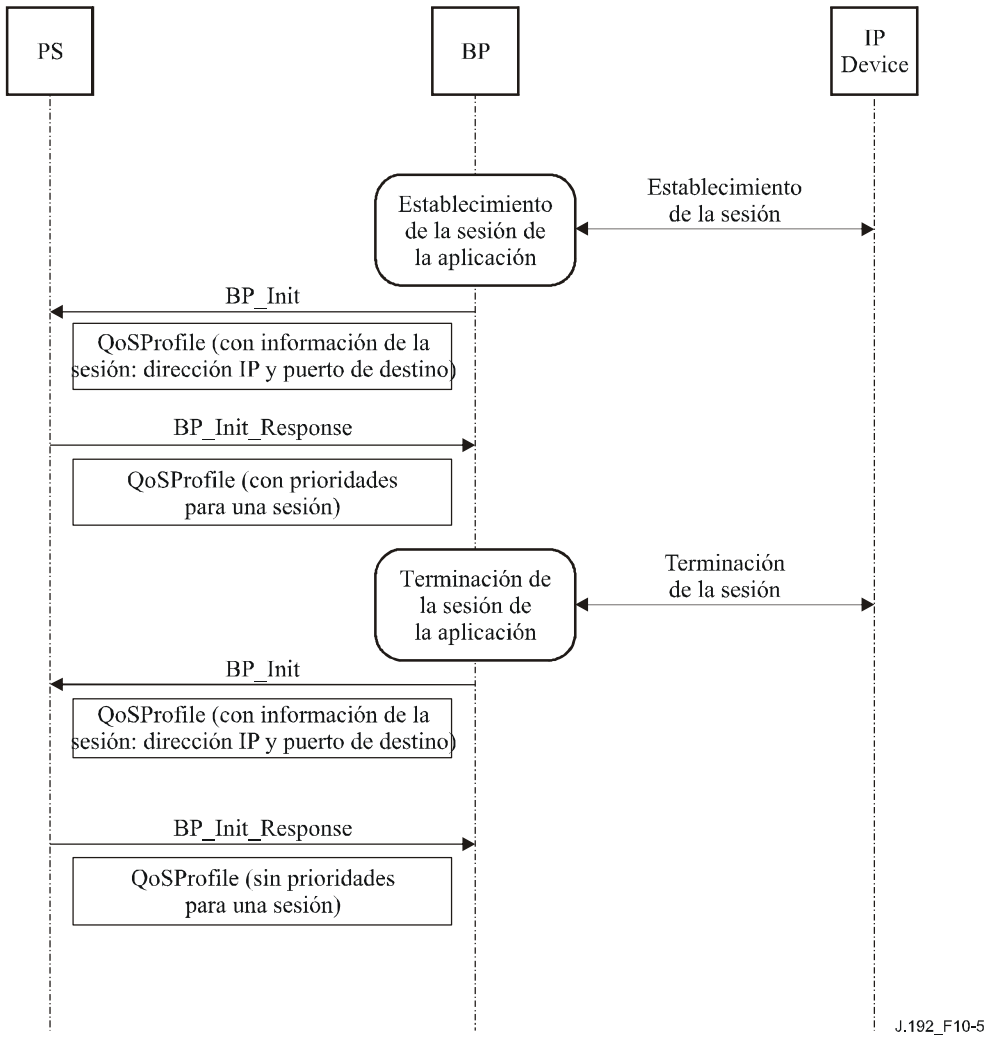


Figura 10-5/J.192 – Intercambio de información durante el establecimiento y terminación de una sesión del BP

10.4.1.4.1.2 Recepción de información de las prioridades del PS en el mensaje BP_Init_Response

Un BP recibe información de prioridades para sus aplicaciones (DefaultCHPriority) y las sesiones de la aplicación (IpPortPriority) en el mensaje BP_Init_ Response desde el PS en el formato del esquema QoSProfile XML. Desde el punto de vista de un BP, el proceso de recepción y procesamiento del esquema QoSProfile XML, después de recibir el mensaje BP_Init_Response del PS, es exactamente el mismo para los tres casos (mencionados en 10.4.1.4.1.1), cuando se envía un mensaje BP_Init.

Cuando se recibe esta información, el BP sustituye completamente su esquema QoSProfile XML almacenado previamente con el QoSProfile recién recibido, en su base de datos. El BP utiliza la información de prioridad suministrada en este esquema QoSProfile XML para determinar las prioridades de sus aplicaciones (Id de aplicación) y las sesiones de la aplicación (identificadas por la dirección IP y el puerto de destino).

10.4.1.4.2 Acceso a los medios con prioridades

El BP utiliza la información de la prioridad de la aplicación que recibe del PS en el esquema QoSProfile XML (cuadro 10-6) para identificar una prioridad genérica de IPCable2Home para todos los paquetes que han de transmitirse por su interfaz LAN. Si la dirección IP y el número de puerto de destino de un paquete de la aplicación concuerda con DestIP y DestPort de cualquiera de

las secuencias DestPriorityListEntry en el esquema QoSProfile XML, el BP utiliza un valor de prioridad especificado por IpPortPriority de esa secuencia DestPriorityListEntry como la prioridad genérica de IPCable2Home para ese paquete. De lo contrario, el BP utiliza DefaultCHpriority que corresponde a CHApplicationId como una prioridad genérica de IPCable2Home para el paquete. El BP hace corresponder esta prioridad genérica de IPCable2Home del paquete a una prioridad de acceso a los medios de IPCable2Home como se describe en 10.2.2.6.3, utilizando el elemento numberMediaAccessPriorities del esquema XML del perfil del dispositivo del BP (véase 6.5.3.1). A continuación, el BP transmite el paquete por su tecnología de medios compartidos de tal manera que se conserve el acceso preferencial relativo del paquete a los medios compartidos como lo exige el valor de la prioridad de acceso a los medios de IPCable2Home.

10.4.1.5 Requisitos del cliente de características de QoS

10.4.1.5.1 Requisitos de intercambio de información de LAN

En esta cláusula se especifican los requisitos del BP para el intercambio de información que debe realizar a fin de obtener la información de las prioridades desde el PS para sus aplicaciones y sesiones.

10.4.1.5.1.1 Envío de información del BP al PS utilizando el mensaje BP_Init

Para que un BP pueda recibir la información de sus prioridades, DEBE comunicar la información de sus aplicaciones y sesiones (dirección IP y número de puerto de destino) al PS en el formato del esquema QoSProfile XML (cuadro 10-6) utilizando mensajes BP_Init, como se describe en 6.3.3.4.3.2.1. Un BP DEBE enviar un mensaje BP_Init con todo su esquema QoSProfile al PS en los tres distintos casos que se indican a continuación:

- obtención o renovación de la licencia DHCP;
- actualización de la aplicación (adición o supresión) en un BP;
- establecimiento o terminación de la sesión de la aplicación con otro dispositivo, mediante un BP.

10.4.1.5.1.1.1 Envío de información del dispositivo y de la aplicación del BP al PS durante la obtención o renovación de la licencia de DHCP del BP

Después de que BP recibe un mensaje DHCPACK [RFC 2131] dirigido a él mismo, en el momento de la obtención o de la renovación de la licencia DHCP, el BP debe enviar la información relativa a sus prioridades del dispositivo y la aplicación al PS utilizando mensajes BP_Init como se describe en 6.5.3.3.4.

El BP DEBE incluir su relación de aplicaciones (QoSApplicationListEntry) en el QoSProfile enviado al PS tras la obtención o renovación de la licencia DHCP. El BP PUEDE incluir anotaciones particulares de la dirección IP y del puerto de destino (DestPriorityListEntry) asociadas a una aplicación en este QoSProfile. Además, el BP PUEDE proporcionar valores para los elementos XML DefaultCHPriority e IpPortPriority en este QoSProfile.

10.4.1.5.1.1.2 Envío de información de la aplicación del BP al PS durante la actualización de la aplicación en el BP

Cuando se añade una nueva aplicación en el BP, éste DEBE añadir una anotación para su aplicación (QoSApplicationListEntry) en su esquema QoSProfile XML existente. Facultativamente, el BP PUEDE rellenar el elemento DefaultCHPriority asociado con su ApplicationId en el QoSProfile. Además, el BP PUEDE incluir la secuencia DestPriorityListEntry para este ApplicationId.

Cuando se suprime una aplicación del BP, éste DEBE suprimir todas las anotaciones (QoSApplicationListEntry así como DestPriorityListEntry) relacionadas a esa aplicación particular a partir de su QoSProfile.

Tras efectuar dicha actualización al esquema QoSProfile XML, el BP envía este nuevo esquema QoSProfile XML al PS utilizando mensajes BP_Init.

10.4.1.5.1.1.3 Envío de información de la aplicación del BP al PS durante el establecimiento o terminación de una sesión de la aplicación

Cuando una aplicación de un BP establece una sesión con otro dispositivo, el BP DEBE añadir la información de la dirección IP y el puerto de destino de la sesión (DestPriorityListEntry) asociada a esa aplicación (ID de aplicación) en su esquema QoSProfile XML (cuadro 10-6). El BP PUEDE utilizar un "comodín" (0) para el elemento DestPort. El BP NO DEBE utilizar "un comodín" para el elemento DestIP. Facultativamente, el BP PUEDE rellenar el elemento IpPortPriority en DestPriorityListEntry.

Cuando una aplicación en un BP da por terminada una sesión, el BP DEBE suprimir la anotación particular de la dirección IP y el puerto de destino correspondiente, DestPriorityListEntry, de su esquema QoSProfile XML.

Una vez efectuada esa actualización al esquema QoSProfile XML, el BP debe enviar este nuevo esquema al PS utilizando un mensaje BP_Init de modo que el PS pueda actualizar (añadir/suprimir) las anotaciones en su cuadro clasificador (cabhPriorityQosBpDestTable).

Esas anotaciones particulares de dirección IP y puerto de destino en el cuadro clasificador del PS (cabhPriorityQosBpDestTable) PUEDEN utilizarse para ofrecer acceso a los medios y retransmisión de paquetes con prioridad al tráfico que va del PS a un dispositivo de sólo recepción no conforme.

10.4.1.5.1.2 Envío de información relativo a prioridades del PS a un BP en el mensaje BP_Init_Response

Un BP DEBE ser capaz de procesar la información de las prioridades de sus aplicaciones (DefaultCHPriority) y de las sesiones de la aplicación (IpPortPriority) que recibe del PS en el formato del esquema QoSProfile XML (cuadro 10-6) utilizando mensajes BP_Init_ Response. Cuando el BP recibe esta información, DEBE sustituir completamente su esquema QoSProfile XML almacenado anteriormente con el método del mismo tipo recién recibido.

10.4.1.5.2 Requisitos de acceso a los medios con prioridades

El BP DEBE utilizar información de la prioridad de la aplicación (DefaultCHPriority o IpPortPriority) que recibe del PS en el esquema QoSProfile XML (cuadro 10-6) para identificar una prioridad genérica de IPCable2Home para todos los paquetes que han de transmitirse por su interfaz LAN. Si la dirección IP y el número de puerto de destino de un paquete de la aplicación concuerda con la DestIP y el DestPort de cualquiera de las secuencias DestPriorityListEntry en el esquema QoSProfile XML, en ese caso el BP DEBE utilizar un valor de prioridad especificado por IpPortPriority de esa secuencia DestPriorityListEntry como la prioridad genérica de IPCable2Home para ese paquete. De lo contrario, el BP DEBE utilizar la DefaultCHpriority correspondiente al CHApplicationId como una prioridad genérica de IPCable2Home para el paquete. El BP DEBE hacer corresponder esta prioridad genérica de IPCable2Home del paquete a una prioridad de acceso a los medios de IPCable2Home como se describe en 10.2.2.6.3, utilizando el elemento numberMediaAccessPriorities del método XML del perfil del dispositivo del BP (véase 6.5.3.1). A continuación, el BP DEBE transmitir el paquete mediante su tecnología de medios compartidos de modo que se mantenga el acceso preferencial relativo del paquete a los medios compartidos, como exige el valor de la prioridad de acceso a los medios de IPCable2Home.

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 encabezamiento. Gracias a la funcionalidad del PS, es posible establecer la base para la utilización de otras aplicaciones y servicios prestados por el operador del 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 [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 CableModem e IPCablecom en la red HFC.
- Lograr la compatibilidad de los mecanismos de seguridad, siempre que sea posible, con las Recomendaciones de seguridad de CableModem 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", de esta Recomendación. 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 de encabezamiento: sistema de terminación de módem de cable (CMTS), servidor de protocolo dinámico de configuración de anfitrión (DHCP) [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 encabezamiento.

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 el encabezamiento de cable y el PS y, facultativamente, encriptarlos para protegerlos contra supervisión y control no autorizados.
SEC4	La barrera contrafuego aceptará ficheros de configuración que tengan un lenguaje y formato (nota) normalizados.
SEC5	El operador del cable podrá gestionar a distancia barreras contrafuego conformes mediante el fichero de configuración o instrucciones SNMP.
SEC6	La barrera contrafuego 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 contrafuego.
SEC8	Se establecerá un conjunto mínimo de requisitos en las capacidades de filtrado de la barrera contrafuego para paquetes, puertos, direcciones IP y hora del día.
SEC9	El operador de cable podrá, gracias a una interfaz de registro detallado de eventos, supervisar y revisar la actividad de la barrera contrafuego, tal como ha sido configurada.
SEC10	La barrera contrafuego soportará las aplicaciones de uso común en casos específicos.
SEC11	La barrera contrafuego 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 contrafuego 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 contrafuego.
NOTA – En 7.4, Función PS – Configuración de los servicios de portal en bloque (BPSC), se definen los requisitos de fichero de configuración de la barrera contrafuego.	

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);
- barrera contrafuego (FW, *firewall*);
- centros 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.

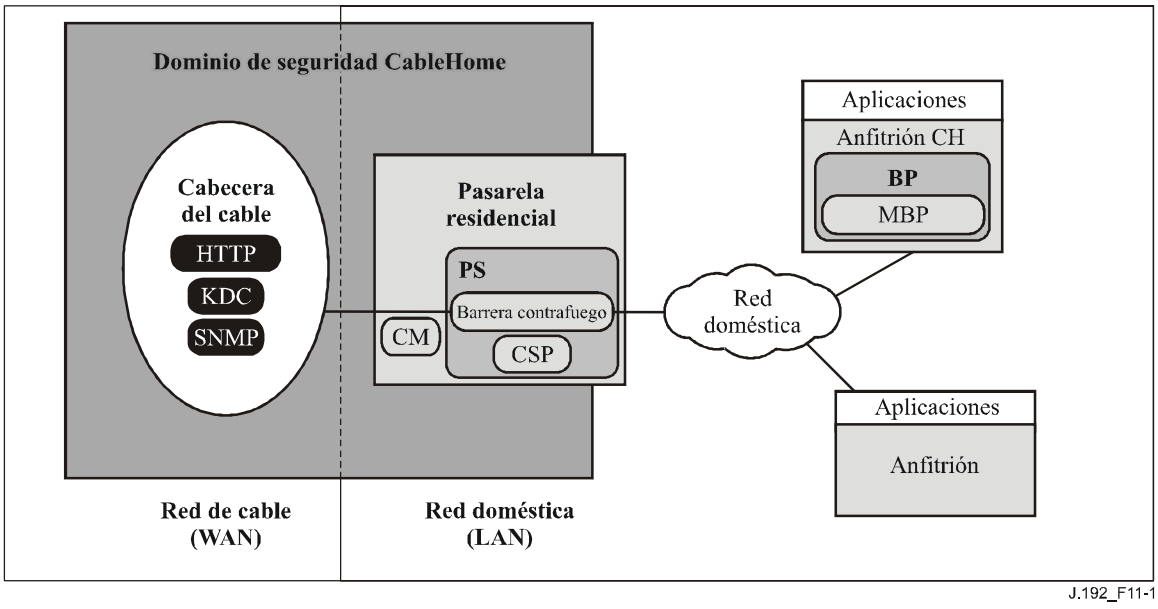


Figura 11-1/J.192 – Elementos de seguridad de IPCable2Home

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 encabezamiento 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 el encabezamiento 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 contrafuego 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, *cable security portal*)
- barrera contrafuego (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 contrafuego.

La funcionalidad de barrera contrafuego 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 de 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 el encabezamiento, 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

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 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 corresponda.

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 la cláusula 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 opción 177, subopción 51, 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 autentificación 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 las cláusulas 6.4 y 6.5 de [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 de esta Recomendación 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 [J.170]:

- cláusula 6.4.8.4, Preautenticador para la ubicación de servidor de configuración;
- cláusula 6.4.7, Nombres principales de MTA;
- cláusula 6.4.8, Correspondencia de dirección MAC MTA con FQDN MTA;
- cláusula 6.4.10, Versiones de claves de servicio;
- cláusula 6.4.11, Funcionamiento entre sectores Kerberos;
- cláusula 6.5.4, Mensajes Rekey;
- cláusula 6.5.6, IPSec "Kerberizado";
- cláusula 6.4.6, Ubicaciones de servidor Kerberos y convenios de denominación.

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 las ubicaciones de servidor Kerberos y los convenios de denominación

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 6.4.6.2/J.170 tienen carácter informativo, y se prevé que el KDC ejecutará las funciones necesarias en el interior, 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 " PSElement" (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 entity address> DEBE ser la dirección IP de la entidad SNMP del proveedor de servicio (Opción 177, subopción 3, de DHCP CDC) escrita con notación separada por puntos y dentro de paréntesis cuadrados (por ejemplo [12.34.56.78]).

11.3.4.2 In fraestructura 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 [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) y en todos los certificados de verificación de código (CVC). 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 11-2 a 11-13, descripción de certificado.
- **Algoritmo de firma –** El mecanismo de firma que se utiliza DEBE ser el SHA-1 [FIPS 186-2] con criptación RSA. El OID específico es 1.2.840.113549.1.1.5.
- **subjectName e 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.

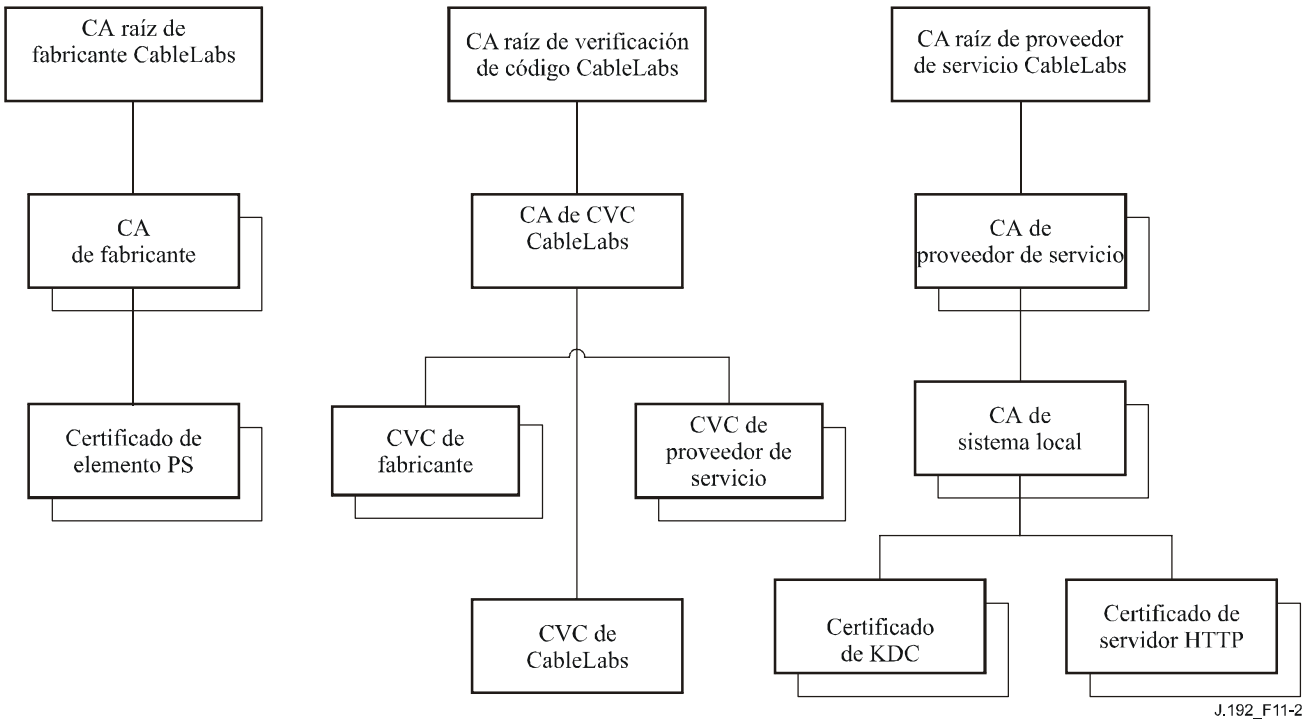


Figura 11-2/J.192 – Jerarquía de certificados de IPCable2Home

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 utilizan sus CA para emitir certificados de elemento PS particulares. 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 y 11-5. 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, "Infraestructura de clase pública (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	Más de 20 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

Este 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. Ese certificado emite certificados de elemento PS y, 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, *commom name*).

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 y el certificado del elemento PS.

Los atributos estado/provincia, ciudad, nombre de producto y local de 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 11-5/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, dataEncipherment), anyExtendedKeyUsage[n,m] (id-kp-clientAuth), 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.

En los cuadros a continuación 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 11-6, 11-7, 11-8, 11-9 y 11-10. De no haber 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 11-6/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	Más de 20 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 11-7/J.192 – Certificado de CA de verificación de código

Formato de nombre de sujeto	C=<country> O=<Company Name> 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 11-8/J.192 – Certificado de verificación de código del fabricante

Formato de nombre del sujeto	C=<country> O=<CompanyName> [ST=<state/province>] [L=<city>] CN=<CompanyName> CVC de fabricante
Utilización prevista	La CA de verificación de código emite este certificado a cada fabricante autorizado. El operador del 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

Se DEBE verificar este certificado 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 11-9/J.192 – Certificado de verificación de código

Formato de nombre del sujeto	C=<country> O=<Company Name> 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 del 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

Se DEBE verificar este certificado 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 11-10/J.192 – Certificado de verificación de código del proveedor de servicio

Formato de nombre del sujeto	C=<country> O=<CompanyName> [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 del 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 del 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 11-11 a 11-14. 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.

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 11-11/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	Más de 20 años

Cuadro 11-11/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 11-12/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. Cuando el encabezamiento contenga un KDC que soporte IPCable2Home, el elemento PS deberá realizar el primer intercambio PKINIT con el KDC inmediatamente después de un rearranque, cuando los cuadros MIB no hayan 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 11-13/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 8.2.4.1/J.170, "Certificado de centro de distribución de claves".

Cuadro 11-14/J.192 – Certificados 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

Cuadro 11-14/J.192 – Certificados de KDC

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 11-15/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), anyExtendedKeyUsage[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 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 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. En 11.8 se presentan más detalles acerca de 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 encriptar 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 diseños de sistema de mensajería de gestión segura

Referencia	Directrices de diseño de sistema de seguridad
SEC3	Los mensajes de gestión de red entre el encabezamiento del cable y el PS se pueden autenticar y, facultativamente, criptar, para protegerlos contra la supervisión y el control no autorizados.

11.4.3 Descripción de 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 del 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 2576], 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 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 del 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 la sección 2.2 de DOCSIS 1.1 *Operations Support Systems Interface specification*, [ANSI/SCTE 23-3 de 2003] (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 la sección C.1.2.8 de la especificación de la interfaz de radiofrecuencia DOCSIS 1.1, [anexo B/J.112] 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:

$$z = g \wedge Rm \text{ MOD } p$$

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).

$$C = g \text{ ^ } xa \text{ MOD } p$$

donde g pertenece al conjunto de parámetros Diffie-Hellman, y p es el número primo de dichos parámetros.

Hasta aquí:

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 del 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 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 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], a continuación se definen las reglas que se han de utilizar al generar dicha máquina:

- El ID de máquina SNMPv3 sigue 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].
- El quinto byte transporta 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. Estos últimos bytes se definen así:
  - Los primeros 25 caracteres del nombre principal Kerberos se utilizan para los bytes de ID de máquina, empezando por el 6º byte.
- La anterior secuencia de bytes, que indica el nombre principal Kerberos, va seguida de un byte que se debe considerar como un valor hexadecimal de 8 bits. Cada valor distinto 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 termina con un carácter Nulo.

Obsérvese que, 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 la 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 del cable. El CHAdministrator es la autoridad suprema 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 13-2, "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 13.4.3, "Informe 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 contrafuego 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 modem de cable 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 contrafuego 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 contrafuego de IPCable2Home

Objetivos

- Facilitar al operador del cable una configuración normalizada e interoperable para la barrera contrafuego.
- Facilitar al operador del cable un conjunto mínimo de funcionalidades requeridas para la barrera contrafuego.
- Activar la supervisión de los eventos en la barrera contrafuego 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 del cable.
- Garantizar que la barrera contrafuego 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 contrafuego en casos específicos.
- Facilitar al operador del cable la capacidad para supervisar y cambiar las reglas utilizadas por la barrera contrafuego.
- Garantizar que existan las configuraciones de seguridad adecuadas en el sistema de la barrera contrafuego (por ejemplo, reglas y políticas de filtrado).
- Identificar los tipos de ataques que han de ser registrados por la barrera contrafuego y especificar el tipo de registro de tal modo que el operador pueda consultarlo cuando sea necesario.
- Soportar IPCablecom a través de la barrera contrafuego.
- Informar al administrador, en tiempo real, de los eventos definidos como importantes.
- Proporcionar un conjunto de reglas por defecto definidas por el fabricante a fin de garantizar la coherencia cuando se reinicialice la barrera contrafuego.

Hipótesis

- La barrera contrafuego 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 contrafuego 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 contrafuego de IPCable2Home. Es decir, este conjunto se representa externamente como una colección de objetos MIB.
- Los objetos MIB de política controlan las acciones de registro emprendidas por el filtro de paquetes de la barrera contrafuego.
- La barrera contrafuego 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 de sistema de barrera contrafuego

En el cuadro 11-16 figuran las directrices de diseño de sistema de la barrera contrafuego que dieron origen a las especificaciones de la barrera contrafuego de IPCable2Home.

Cuadro 11-16/J.192 – Directrices de diseño de sistemas de seguridad IPCable2Home

Referencia	Directrices
SEC4	La barrera contrafuego aceptará los ficheros de configuración que se reciban en lenguaje y formato normalizados (nota).
SEC5	El operador del cable podrá gestionar a distancia las barreras contrafuego conformes a la norma, a través del fichero de configuración o de instrucciones SNMP.
SEC6	La barrera contrafuego 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 contrafuego.
SEC8	Se atribuirá un conjunto mínimo de requisitos en las capacidades de filtrado de la barrera contrafuego para paquetes, puertos, direcciones IP, TOD, etc.
SEC9	Gracias a una interfaz de registro detallado de eventos en la barrera contrafuego, el operador del cable podrá supervisar y revisar la actividad de ésta, conforme a su configuración.
SEC10	La barrera contrafuego soportará las aplicaciones comúnmente utilizadas en casos específicos.
SEC11	La barrera contrafuego 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 contrafuego 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 contrafuego.	

11.6.3 Descripción de sistema de barrera contrafuego

En general, las barreras contrafuego se componen de una combinación de: filtrado de paquetes (PF, *packet filtering*), filtrado dinámico de paquetes (SPF, *stateful packet filtering*), pasarela de capa aplicación (ALG, *application level gateway*) y apoderado específico de aplicación (ASP, *application-specific proxy*). El componente más comúnmente utilizado en estas barreras es el módulo de filtrado de paquetes, ya que permite establecer a cuáles trenes de paquetes se les autoriza cruzar la barrera 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, 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 contrafuego una gran cantidad de filtros. Es tarea del operador del 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, siempre que se decida descartar un paquete. 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 específico de aplicación (ASP), otra de las barreras contrafuego más comunes, puede filtrar basándose en las características únicas del protocolo de capa de aplicación o en 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 determinada barrera contrafuego depende de un 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 contrafuego vienen determinados por la política de seguridad, en ésta no se explica detalladamente la configuración específica de la barrera. El conjunto de reglas se pone en términos lisibles para una persona, que son entonces interpretados por la barrera 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 contrafuego y cuáles no.

En la figura 11-3 se presenta un diagrama general de la barrera 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.

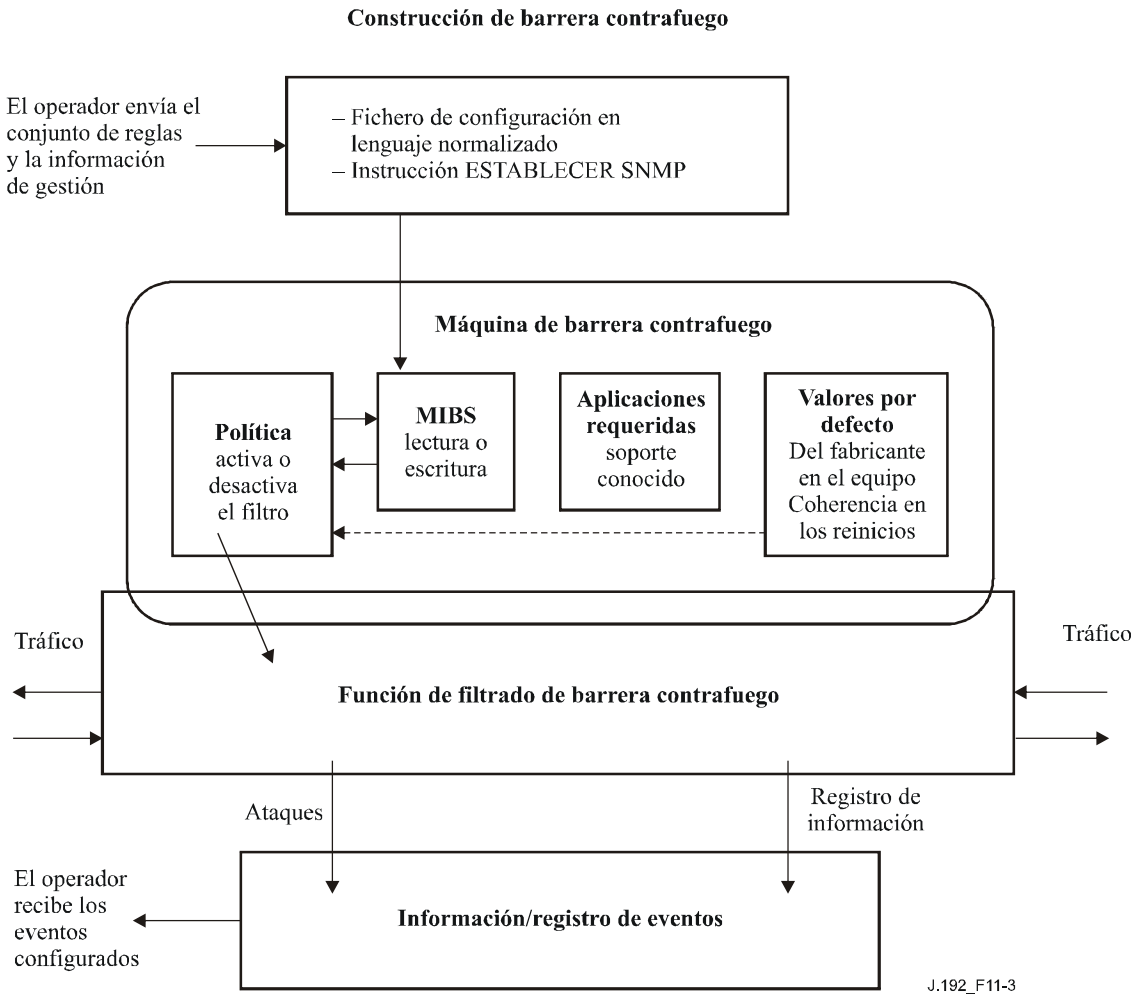


Figura 11-3/J.192 – Referencia lógica de barrera contrafuego

11.6.4 Requisitos de la barrera contrafuego

11.6.4.1 Lenguaje del fichero de configuración para la barrera contrafuego

Se puede configurar el conjunto de reglas escogido por el operador del cable en la barrera contrafuego, a través de un fichero de configuración PS o descargando un fichero de configuración de barrera contrafuego. En esta cláusula, fichero de configuración significa bien el del PS o el de la barrera. No sólo se definen el lenguaje y formato del fichero de configuración, que contienen el conjunto de reglas que se aplica a determinado producto de barrera contrafuego, sino también la utilización de dicho fichero en la barrera para configurar los componentes SPF y ASP que dependerá del tipo de implementación.

El PS DEBE poder recibir e interpretar ficheros de configuración de barrera contrafuego construidos utilizando los TLV con formato ASN.1 y codificación BER [ISO/CEI 8025-1]. Dentro de la barrera, 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 contrafuego. El lenguaje de los ficheros de configuración del PS y de barrera contrafuego 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 contrafuego.

11.6.4.2 Configuración de barrera contrafuego

En el PS se permite, aunque no sea obligatorio, que el operador del cable gestione a distancia las funciones de la barrera contrafuego. Ésta DEBE aceptar los conjuntos de reglas configurados en bloque, a través de los ficheros de configuración especificados del PS o de la barrera contrafuego. Siempre que haya reglas de filtrado de la barrera contrafuego en el fichero de configuración, se les puede procesar bien como un conjunto de reglas que se incrementa o como uno totalmente configurado, tal como lo establezca el objeto cabhSec2FwClearPreviousRuleset. Cuando se concluye la descarga y el proceso del fichero de configuración, se DEBEN aplicar inmediatamente las reglas para la barrera contrafuego del fichero de configuración, y se usarán una vez que el objeto MIB cabhPsDevProvState tenga un valor pass(1), sin necesidad de rearrancar el PS. Si el objeto cabhSec2FwPolicySelection se fija a configuredRuleset, se DEBEN aplicar inmediatamente las nuevas reglas al procesamiento. Cuando el PS procese un fichero de configuración utilizando un conjunto de reglas de barrera contrafuego, NO DEBE perder las reglas incrementales enviadas a través de la instrucción SET SNMP, o las enviadas en ficheros de configuración anteriores, a menos que el objeto cabhSec2FwClearPreviousRuleset esté puesto a complete(2) o incrementDefault(3). Cuando se trata de reglas enviadas a través del SNMP, la regla o el valor del objeto MIB DEBEN estar activados (o disponible adecuadamente cuando no se permita la activación) inmediatamente después del procesamiento del mensaje SET SNMP sin necesidad de rearrancar el PS. Por ejemplo, cuando se actualice uno de los filtros de la barrera contrafuego a través de SET SNMP, y siempre que el objeto cabhSec2FwPolicySelection esté fijado a factoryDefault, el PS actualizará entonces el conjunto de reglas configurado incluyendo la regla modificada, aunque funcionará utilizando la política por defecto del fabricante hasta que el operador del cable modifique el objeto a configuredRuleset, que ya incluye la regla recién configurada.

La barrera DEBE verificar y aplicar las reglas configuradas en el docsDevFilterIpTable, como se describe en [RFC 2669], a menos que se indique lo contrario en esta Recomendación.

Si por algún motivo el PS no puede procesar el fichero de configuración, DEBE enviar el evento adecuado para el fallo de procesamiento, y la barrera DEBE utilizar el conjunto de reglas escogido por el objeto cabhSec2FwPolicySelection y habilitado por el objeto cabhSec2FwEnable.

11.6.4.3 Política de barrera contrafuego

Es la que indica a la barrera cómo filtrar el tráfico sobre la base de ciertas reglas. En ella se acepta aplicar el conjunto de reglas mediante la función de filtrado, puesto que ésta no tiene ningún significado como ente independiente, ya que es solamente un conjunto de capacidades. Las capacidades de filtrado de la barrera contrafuego, junto con su política, proporcionan a la LAN protección de barrera contrafuego. Los filtros de barrera contrafuego inspeccionan constantemente cada paquete o conexión utilizando la política a fin de permitir su paso o negarlo. De haber un conflicto de reglas en la política, la barrera lo DEBE resolver, tal como se describe para el caso de docsDevFilterIpTable en [RFC 2669], a menos que se indique lo contrario en la presente Recomendación.

Se diseña la barrera con el fin de proteger los sistemas informáticos en la vivienda de ataques y tráfico no deseado. El tráfico se clasifica según su origen, a saber, WAN, LAN y PS. Cuando no exista una regla para el tráfico que haya sido iniciado en direcciones IP que no pertenecen a la LAN (las direcciones IP LAN se definen como direcciones LAN-Trans y LAN-Pass), la barrera DEBE rechazarlo por defecto. De igual manera, de no haber reglas configuradas respecto al tráfico proveniente de direcciones IP de LAN y destinado a direcciones IP de WAN, la barrera DEBE permitirlo por defecto. Se DEBEN verificar todos los paquetes que no pertenezcan a una de las categorías explícitamente permitidas por una de las reglas configuradas, a fin de observar si se DEBE permitir su paso como resultado del estado.

Se especifican una manera estándar para comunicar las políticas, a la barrera contrafuego una política por defecto, y el soporte de IPCablecom. La política por defecto se puede utilizar como configuración estándar de fábrica por defecto; el operador puede decidir en cualquier momento si reinicia el equipo para que tenga estos valores. Gracias a la política de fábrica por defecto, es posible gestionar el PS y habilitarlo para procesar la mayor parte del tráfico que va de la LAN a la WAN. Los operadores del cable pueden crear todo tipo de configuraciones necesarias para soportar cualquier aplicación destinada a cada cliente a través de la barrera contrafuego. Es posible establecer la política a través del fichero de configuración PS, el fichero de configuración de barrera contrafuego o los mensajes SET SNMP.

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 11.6.4.3.3 se describe el soporte de IPCableCom, que consiste en políticas de fábrica por defecto para IPCable2Home más los protocolos necesarios a fin de permitir que la mensajería IPCablecom atraviese la barrera. 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.

La política por defecto de fábrica, que se define en el cuadro 11-17, debe instalarse durante la fabricación y estar siempre disponible en el equipo a fin de poderlo reiniciar en un nivel básico de filtrado. El operador del cable provee todos los conjuntos de reglas configurados. La política de fábrica por defecto no se denomina "conjunto de reglas", puesto que no se especifica en el lenguaje y formato requeridos para un fichero de configuración, sino que sus requisitos se enumeran y su implementación depende del fabricante, pues se lleva a cabo durante la fabricación.

Actualmente, en IPCable2Home se especifica una política de fábrica por defecto para la barrera contrafuego que se incorpora en el PS durante la fabricación, así como un método para que el operador del cable pueda configurar los conjuntos de reglas que se necesite en el PS según proceda. En esta cláusula se describe el concepto general de política de barrera contrafuego, en lo que respecta a sectores de direcciones, la política de fábrica por defecto, la información de los conjuntos de reglas de IPCablecom y el conjunto de reglas configurado por el operador del cable.

11.6.4.3.1 Política de barrera contrafuego y sectores de direcciones

La barrera contrafuego filtra políticas a través de la configuración de un conjunto particular de reglas. Si el operador del cable no ha configurado la barrera contrafuego, ésta empleará la política de fábrica por defecto. La política incluye reglas de filtrado de las direcciones IP de origen y destino, y puesto que el concepto de sentido se infiere de las palabras origen y destino, no se especifica aquí.

En esta Recomendación se define el concepto de sectores de direccionamiento IP para direcciones IP de WAN y LAN. Aunque el PS esté en la LAN, los paquetes que se originan en él o que están destinados al mismo no se denominan como tráfico LAN a efectos del filtrado de la barrera contrafuego. 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 misma dirección IP de encaminador de servidor PS). Siendo así, la barrera contrafuego distinguirá el tráfico saliente y entrante del PS en la política de fábrica por defecto. No se distingue en los modos de direccionamiento las direcciones IP LAN puesto que la barrera no filtra basándose en modos de direccionamiento IP de IPCable2Home. Se DEBE considerar la dirección IP de WAN-Data del PS como parte del sector de direcciones IP LAN, puesto que esa dirección sólo actúa como apoderada para paquetes que tengan direcciones IP traducidas por la CAT (por ejemplo, direcciones IP de LAN-Trans).

11.6.4.3.2 Política de fábrica por defecto

La política de fábrica por defecto se ocupa tanto de la funcionalidad normal del PS como de la mayoría del tráfico que se inicia en los anfitriones. Ésta DEBE programarse en el PS durante la fabricación, y el PS DEBE utilizarla siempre que el objeto cabhSec2FwPolicySelection esté puesto a factoryDefault(1).

La política de fábrica por defecto DEBE soportar los protocolos requeridos por IPCable2Home, salvo el protocolo ToD que no se especifica más allá de los procesos de configuración y que por tanto no se incluye, ya que la barrera contrafuego no se activa antes de que haya pasado el estado de configuración. Si el objeto cabhSec2FwPolicySelection se pone a factoryDefault durante el proceso de configuración (por ejemplo, en el rearranque), el PS DEBE activar la política de fábrica por defecto justo después de que el objeto MIB cabhPsDevProvState tenga un valor pass(1), sin necesidad de rearrancar el PS. Cuando el objeto cabhSec2FwPolicySelection se ponga a factoryDefault a través de SNMP, el PS DEBE activar la política de fábrica por defecto inmediatamente, sin necesidad de rearrancar el PS. La política de fábrica por defecto NO DEBE incluir ninguna restricción de la hora ni límites de la cantidad de sesiones o conexiones que se puedan soportar simultáneamente, a menos que se especifique lo contrario en el anexo D, "Aplicaciones mediante traducción de direcciones IPCable2Home y la barrera contrafuego".

En el cuadro 11-17 se especifica la política de fábrica por defecto. Ambos sectores de direcciones LAN, LAN-Trans y LAN-Pass, son tratados de igual manera por la política de fábrica por defecto y etiquetados como direcciones IP LAN. La barrera contrafuego 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. Las direcciones del PS NO DEBEN incluir ninguna dirección IP de WAN-Data del PS. Las direcciones WAN-Data del PS pertenecen al tráfico IP de LAN y por consiguiente se tratan como direcciones IP LAN. La información del cuadro se basa en el inicio de sesión, más no en el tráfico permitido. Por tanto, la política de fábrica por defecto de la barrera contrafuego se DEBE implementar para el inicio de sesión y no para el tráfico permitido. El tráfico que retorne a petición de quién lo inicia se interpreta como información de estado para una sesión y por tanto la barrera verificará el estado de sesión tras haber verificado las políticas, a fin de garantizar que no se rechace un paquete que forma parte de la sesión en curso. Se DEBE implementar el cuadro 11-17 como política de fábrica por defecto de la barrera contrafuego.

Cuadro 11-17/J.192 – Política de fábrica por defecto de barrera contrafuego en IPCable2Home

Las cabeceras de columna identifican el inicio de la sesión	Fuente: Dirección IP de WAN Destino: Dirección IP de WAN-Man del PS	Fuente: Dirección IP de WAN Destino: Dirección IP de LAN	Fuente: Dirección IP de WAN-Man del PS Destino: Dirección IP de WAN	Fuente: Dirección IP de WAN-Man del PS Destino: Dirección IP de LAN	Fuente: Dirección IP de LAN Destino: Dirección IP de encaminador de servidor del PS	Fuente: Dirección IP de LAN Destino: 192.168.0.1 del PS	Fuente: Dirección IP de LAN Destino: Dirección IP de WAN-Man del PS	Fuente: Dirección IP de LAN Destino: Dirección IP de WAN	Casos de relación requeridos
IM AOL	Prohibido	Permitido	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Permitido	Todos
DHCP	Prohibido	Prohibido	Permitido	Prohibido	Permitido	Permitido	Prohibido	Permitido	Todos
DNS	Prohibido	Prohibido	Permitido	Prohibido	Permitido	Permitido	Prohibido	Permitido	Todos
FTP	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Permitido	Todos
HTTP	Prohibido	Prohibido	Prohibido	Prohibido	Permitido	Permitido	Prohibido	Permitido	Todos
HTTP (HTTPS por TLS)	Prohibido	Prohibido	Permitido	Prohibido	Permitido	Permitido	Prohibido	Permitido	Todos
Petición de eco e indicación de tiempo ICMP (Ping y Traceroute)	Permitido	Permitido	Prohibido	Permitido	Permitido	Permitido	Prohibido	Permitido	Todos
IPSec	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Permitido	Uno a uno, único
Kerberos	Prohibido	Prohibido	Permitido	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Todos
Microsoft Messenger	Prohibido	Permitido	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Permitido	Todos
MSN Messenger	Prohibido	Permitido	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Permitido	Todos
POP3	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Permitido	Todos
SMTP	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Permitido	Todos
SNMP	Permitido	Prohibido	Permitido	Prohibido	Permitido	Permitido	Prohibido	Prohibido	Todos
SNMP trap	Prohibido	Prohibido	Permitido	Prohibido	Permitido	Permitido	Prohibido	Prohibido	Todos
SYSLOG	Prohibido	Prohibido	Permitido	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Todos
Telnet	Prohibido	Prohibido	Prohibido	Prohibido	Permitido	Permitido	Prohibido	Permitido	Todos
TFTP	Prohibido	Prohibido	Permitido	Prohibido	Prohibido	Prohibido	Prohibido	Permitido	Todos
Yahoo Messenger	Prohibido	Permitido	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Permitido	Todos
Windows Messenger	Prohibido	Permitido	Prohibido	Prohibido	Prohibido	Prohibido	Prohibido	Permitido	Uno a uno, uno a varios

11.6.4.3.3 Conjunto de reglas de IPCablecom

Cuando el operador utilice IPCablecom, es posible que la barrera contrafuego 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 contrafuego NO DEBE contradecir los protocolos definidos por el conjunto de Recomendaciones IPCablecom. Puede ocurrir que el operador del cable deba configurar la barrera con otras reglas adicionales a fin de garantizar que IPCablecom pueda funcionar a través de ésta. En el cuadro 11-18 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 11-18/J.192 – Especificaciones IPCablecom 1.x pertinentes para la barrera contrafuego de IPCable2Home

Descripción	Recomendación UIT-T
Especificación de códec de audio/vídeo	[J.161]
Especificación de la calidad de servicio dinámica	[J.163]
Especificación de protocolo de señalización de llamada basada en la red	[J.162]
Especificación de configuración de dispositivo MTA	[J.167]
Especificación de seguridad	[J.170]
Especificación de mecanismo de evento de gestión	[J.164]
Especificación de protocolo de servidor de audio	[J.175]
Especificación de señalización de servidor de gestión de llamada	[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 contrafuego", 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. 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.)

11.6.4.3.4 Conjunto de reglas configurado y versión actual

El operador del cable puede enviar cualquier conjunto de reglas de barrera contrafuego que necesite el PS a través del fichero de configuración o de la instrucción SET SNMP. Cuando un operador del cable envía reglas al PS, éstas se conocen como el conjunto de reglas configurado o la versión actual. Este conjunto se DEBE almacenar en una memoria permanente (es decir, que se conserve durante los rearranques). Siendo así, se garantiza que el PS pueda rehabilitar dicho conjunto siempre y cuando la barrera contrafuego esté activa y se ponga la selección de política a configuredRuleset. Los filtros definidos de la barrera contrafuego se activan con el conjunto de reglas configurado. En [RFC 2669] se especifica el conjunto global de objetos MIB de filtrado de la barrera, y se añade un cuadro de programación adicional en la MIB de seguridad. Los objetos MIB se agrupan en un cuadro de filtros que representa el conjunto de reglas configurado.

El procesamiento y la aplicación a cargo del PS, del conjunto de reglas configurado enviado por el operador del cable depende del contenido del fichero de configuración y del valor del objeto cabhSec2FwClearPreviousRuleset. Puede ser que el conjunto de reglas configurado sea el conjunto de reglas configurado existente con un algún incremento o que se trate de un reemplazo completo de éste. De igual manera, es posible aumentar la política de fábrica por defecto. Cuando el operador del cable aumente un conjunto de reglas de barrera contrafuego tomando como base la política de fábrica por defecto, el PS DEBE rellenar el cuadro de filtros con las reglas de fábrica por defecto antes de hacer lo mismo con las reglas configuradas por el operador del cable. De esta manera, el operador del cable podrá ver todas las reglas de filtrado. En 11.6.4.7.1, y en particular en la descripción de objeto MIB cabhSec2FwClearPreviousRuleset se indican los detalles funcionales y requisitos de esta característica.

11.6.4.4 Filtrado de barrera contrafuego

En esta cláusula se especifican los requisitos del componente de filtrado de paquetes de la barrera contrafuego. El filtro de paquetes especificado examina cada paquete y determina si debe permitir o impedir su paso a través de la barrera. 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.

11.6.4.4.1 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 contrafuego DEBE implementar un ASP o una barrera 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 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. 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 todo, sin importar el tipo de barrera contrafuego 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. Esta petición incluye su 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 se especifican filtros y PS separados en el sentido entrante (WAN-a-LAN) y saliente (LAN-a-WAN). El filtro de paquetes entrante examina los paquetes que llegan a la interfaz WAN del PS. El otro, examina aquellos que llegan a la interfaz LAN del PS. Es posible aplicar reglas diferentes a cada uno de estos filtros. En la barrera se filtran los paquetes destinados al PS que provienen de la WAN o de la LAN, antes de reenviarlos a cualquiera de los componentes del PS sin barrera contrafuego (CAP, CDP, CNP, CSP, CQP, y CPM).

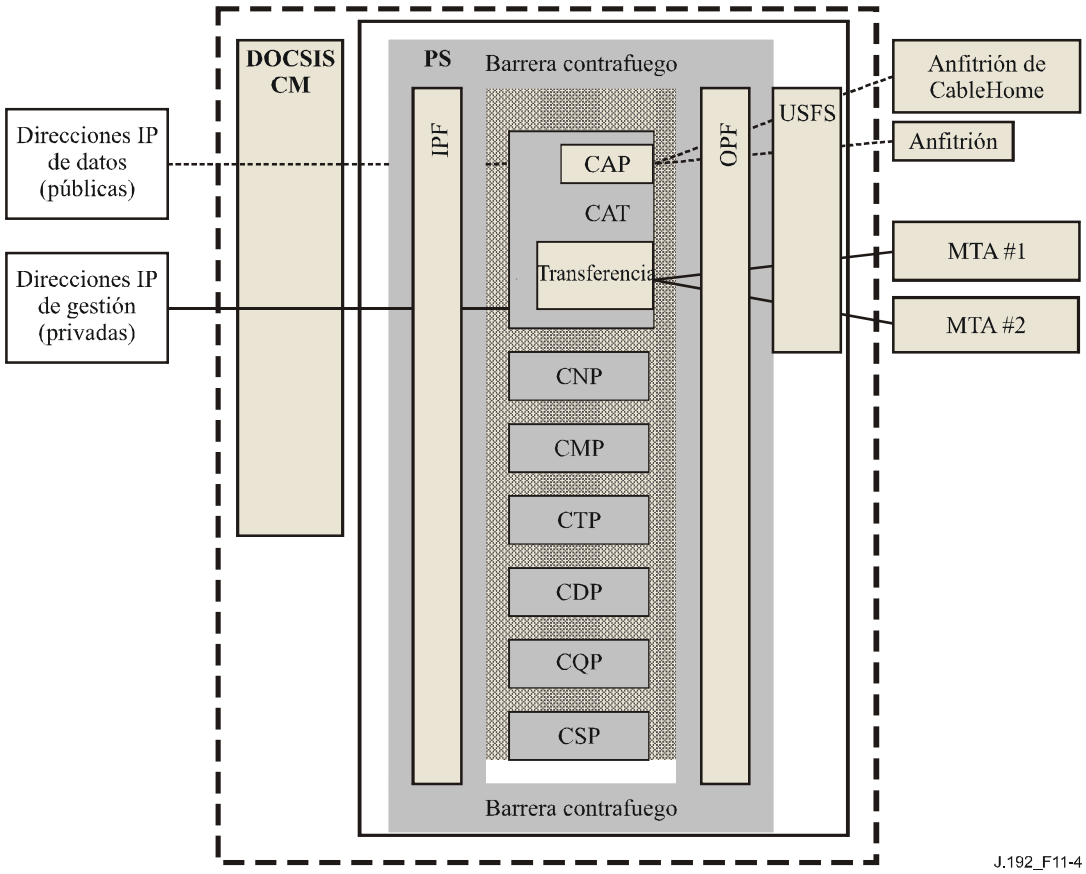


Figura 11-4/J.192 – Funcionalidad de barrera contrafuego dentro del PS

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 paquetes NAT/NAPT (CAT CH) se traducirán desde la LAN, mientras que aquellos que retornen de la WAN a esta última se reconocerán como tales y serán sometidos a la operación inversa de NAT/NAPT. Se aplicarán los filtros de barrera contrafuego junto con la dirección correcta de origen o destino en la LAN.

Los filtros de paquetes entrantes y salientes de la barrera contrafuego DEBEN comportarse de la siguiente manera:

- La barrera DEBE prohibir todo tráfico iniciado por direcciones IP que no provengan de la LAN, a menos que exista una regla explícita que lo permita. Las direcciones IP no LAN son aquellas que no figuran en la lista de direcciones LAN-Trans o en la de LAN-Pass.
- La barrera DEBE permitir el paso de todo el tráfico iniciado por direcciones IP de LAN (que excluye las direcciones IP de encaminador de servidor PS o de WAN-Man del PS), a menos que una regla explícita ordene lo contrario.
- La barrera DEBE prohibir el paso de paquetes reproducidos bien sea desde la LAN o desde la WAN.
- La barrera 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.

- El PS 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 fuente (LSRR, *loose-source-route*), ruta estricta de fuente (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 contrafuego. 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 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 DISCOVER de DHCP.

11.6.4.4.2 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 y la política por defecto 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 ("próximo nivel"); por ejemplo, TCP, UDP, ICMP, IPsec AH e 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 contrafuego 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 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.

11.6.4.4.3 Arquitectura de filtrado

El filtro de paquetes de la barrera contrafuego DEBE poder filtrar el tráfico en la entrada del PS, salvo cuando se utilice la función USFS de la LAN, y disponer de filtros diferentes para los paquetes entrantes (WAN-a-LAN), salientes (LAN-a-WAN), y del PS. Los atributos que DEBE tener una barrera contrafuego son:

- filtrar paquetes recibidos de la interfaz WAN del PS, por ejemplo, IfIndex = 1, (se conoce como filtrado al ingreso);
- filtrar paquetes recibidos de la interfaz LAN del PS, por ejemplo, IfIndex = 255, (conocido como filtrado al egreso o saliente);
- filtrar paquetes que se originan dentro del PS y que van hacia la LAN o la WAN;
- aplicar sólo los filtros actualmente habilitados;
- el filtrado de paquetes entrantes y salientes antecede la entrega de paquetes a cualquier componente del PS sin protección de la barrera, salvo el USFS para los paquetes que provienen de la LAN;
- el filtrado de paquetes salientes antecede cualquier procesamiento ASP/SPF.

El filtro de paquetes entrantes de WAN DEBE exhibir el siguiente comportamiento:

- Prohibición de paquetes por defecto; lo que quiere decir que el comportamiento por defecto de la barrera respecto a los paquetes entrantes, cuando no haya reglas explícitas de filtrado que les permita pasar, es descartarlos.
- Prohibir todos los paquetes cuya dirección de origen esté en el dominio de direcciones LAN-Pass o LAN-Trans y se reciba de la interfaz WAN del PS, por ejemplo, IfIndex = 1.
- Prohibir todos los paquetes que tengan direcciones de origen de difusión o multidifusión.

El filtro de paquetes salientes de LAN DEBE tener el siguiente comportamiento:

- Permitir el paso de paquetes por defecto; lo que quiere decir que la barrera permite por defecto el paso de los paquetes salientes, a menos que haya reglas explícitas que indiquen lo contrario.
- Rechazar todos los paquetes que tengan direcciones de origen de difusión o multidifusión.

11.6.4.5 Informe de eventos en la barrera contrafuego

La información que proviene de la barrera contrafuego 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 contrafuego. Cuando hay grandes cantidades de datos, el análisis y clasificación de los registros puede ser bastante dispendioso. Asimismo, de enviarse demasiados eventos al operador del cable, puede haber un consumo exagerado de ancho de banda (muchas barreras contrafuego enviando al mismo tiempo eventos a su NMS). El operador habrá de decidir cuáles elementos se han de activar para supervisar la barrera 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 contrafuego. Una vez se hayan puesto los objetos MIB que habilitan eventos de tal manera que se permita a la barrera 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 del 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 Set SNMP. Conviene utilizar el SNMPv3 para asegurar los mensajes SNMP que contengan información relativa a la barrera contrafuego.

11.6.4.5.1 Eventos de barrera contrafuego

Gracias a estos eventos, el operador del cable puede evaluar a distancia el nivel de actividad de intrusos y de las modificaciones a la barrera contrafuego 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 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 contrafuego, se DEBEN enviar con arreglo al anexo B.

La barrera contrafuego 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 contrafuego 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 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 exceda 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 contrafuego otorga al operador del cable un conocimiento valioso y eficaz, a efectos de corregir errores. Cuando esté habilitado este tipo y se sobrepase 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 excede 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 del 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 excede 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 del 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 superarse 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 del cable evaluar y ejecutar la respuesta necesaria a los eventos detectados e informados por la barrera contrafuego.

11.6.4.5.2 Registros de barrera contrafuego

Se DEBE almacenar la información de registro de la barrera contrafuego en el PS por cada tipo de registro habilitado, conforme a 11.6.4.5.1. El PS DEBE registrar la información especificada, a menos que se haya puesto a cero el cabhSec2FwEventThreshold, que se haya puesto a inhabilitar el cabhSec2FwEventEnable, que se haya puesto a cero el cabhSec2FwEventInterval o que el registro esté lleno. Cuando el cabhSec2FwEventThreshold no sea cero, el cabhSec2FwEventEnable esté habilitado, el cabhSec2FwEventInterval no sea cero y el registro no esté lleno, el PS DEBE seguir registrando eventos del tipo habilitado. Una vez se haya puesto a 1 el cabhSec2FwEventLogReset, a fin de limpiar el registro, y si el cabhSec2FwEventEnable está habilitado, el cabhSec2FwEventCount DEBE iniciar su cuenta desde cero.

El PS, como mínimo DEBE soportar el registro de 1 kilobyte de datos por cada registro en la memoria que no es permanente, de tal modo que sea posible almacenar cerca de 40 eventos sin necesidad de comprimir los datos. Cuando se habilita un tipo de evento, el PS DEBE registrar la información requerida por él a una velocidad mínima de 1 evento cada 5 segundos, aun si está 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.

11.6.4.5.2.1 Datos de registro

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 del 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 encriptados. 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 contrafuego 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 contrafuego 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.

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.
- Declaración de fallo – En los eventos de tipo 4 se DEBE establecer el fallo y su razón.

11.6.4.6 Aplicaciones a través de la barrera contrafuego

Como parte del conjunto mínimo de capacidades, la barrera DEBE poder permitir que aplicaciones especificadas, como se define en el anexo D, atraviesen el PS y lleguen al destino previsto. Se permiten dichas aplicaciones, más no por defecto sino que el operador del cable debe activarlas. La barrera contrafuego 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.

La política de la barrera contrafuego se aplica al tráfico a medida que éste intenta atravesarla. Se procesan primero los paquetes en la barrera 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.

11.6.4.7 Objetos MIB de barrera contrafuego

Los objetos MIB de barrera contrafuego constan de tres partes principales, a saber:

1) un conjunto para gestionar la configuración de la barrera;

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 contrafuego junto con el documento MIB de seguridad (véase E.5).

11.6.4.7.1 Objetos MIB de gestión de conjunto de reglas de barrera contrafuego

Se DEBEN implementar en el PS los siguientes objetos de gestión de barrera contrafuego:

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 contrafuego".

Cuando falle la descarga del fichero de configuración de barrera contrafuego, 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 y DEBE incluir los tres estados siguientes:

- inProgress (1) – hay una descarga de fichero de configuración de barrera contrafuego en curso.
- complete (2) – la descarga del fichero de configuración de barrera contrafuego ha sido completada con éxito.
- failed (3) – el último intento de descarga de fichero de configuración de barrera contrafuego fracasó.

cabhSec2FwPolicyFileCurrentVersion – Etiqueta puesta por el operador del cable que se utiliza para rastrear las diversas versiones de conjuntos de regla configurados. Cuando esta etiqueta está establecida por SNMP o un fichero de configuración, su valor está modificado y las reglas de filtro de barrera contrafuego configurado son modificadas. Sin embargo, como las reglas de filtro de barreras contrafuego se pueden modificar utilizando SNMP después de la configuración inicial por el fichero de política (fichero de configuración de barrera contrafuego), el valor de esta etiqueta (por ejemplo, la versión vigente del fichero de política), puede no corresponder correctamente a la configuración de barrera contrafuego actualmente vigente. Si no ha sido configurado antes, este objeto DEBE contener la cadena "null".

cabhSec2FwEnable – Permite activar y desactivar la barrera. Cuando este objeto se ponga a inhabilitado, la barrera DEBE desactivarse completamente. Cuando se ponga a habilitado, la barrera DEBE activarse inmediatamente sin que sea necesario rearrancar el PS.

cabhSec2FwClearPreviousRuleset – Este objeto permite que el fichero de configuración de barrera contrafuego o del PS contenga un conjunto completo de reglas configurado de la barrera, o un aumento al ya configurado, dependiendo de que exista en el fichero de configuración. Cuando el PS reciba un fichero de configuración que contenga la configuración de una barrera contrafuego, y que incluya una configuración de objeto cabhSec2FwClearPreviousRuleset etiquetada como increment(1), o si no se incluye la configuración de dicho objeto en un fichero de configuración que contenga la configuración del filtro para la barrera contrafuego, el PS DEBE considerar la configuración de filtro de la barrera contrafuego como un incremento al conjunto de reglas configurado. Si el PS recibe un fichero de configuración que tenga una configuración de barrera contrafuego en donde se incluye la configuración del objeto cabhSec2FwClearPreviousRuleset etiquetada como incrementDefault(3), el PS DEBE suprimir todas las reglas previamente configuradas de dicho conjunto configurado, incluyendo las del cuadro de programación de filtros, e incrementar las reglas que acaba de descargar por encima (es decir, subsiguiente a) de la política de fábrica por defecto. Si el PS recibe un fichero de configuración con los valores de barrera contrafuego que incluya la configuración del objeto cabhSec2FwClearPreviousRuleset etiquetado como complete(2), el PS DEBE suprimir todas las reglas previamente configuradas del conjunto de reglas configurado, incluyendo las del cuadro de programación de filtros, antes de aplicar la configuración del filtro de la barrera contrafuego que se incluye en el fichero de configuración.

Si se pone cabhSec2FwClearPreviousRuleset a increment(1) a través del SNMP, el PS DEBE tratar todas las configuraciones siguientes de filtro de la barrera contrafuego que usan el SNMP, como un incremento del conjunto de reglas configurado. Si cabhSec2FwClearPreviousRuleset se pone a incrementDefault(3) mediante el SNMP, el PS DEBE suprimir todas las reglas previamente configuradas del conjunto de reglas configurado, incluidas las reglas en el cuadro de programación de filtros, y tratar todas las configuraciones siguientes de filtro de barrera que utilizan el SNMP, como un incremento por encima de la política de fábrica por defecto. Si cabhSec2FwClearPreviousRuleset se pone a complete(2), utilizando el SNMP, el PS DEBE suprimir todas las reglas del conjunto configurado, incluidas aquéllas en el cuadro de programación de filtros. En este caso, el PS funciona sin reglas configuradas (por ejemplo, si bien no habrá reglas de filtrado definidas la barrera continuará suministrando el conjunto mínimo de capacidades y arquitectura que se define en 11.6.4.4.1 y 11.6.4.4.3). Valor por defecto = increment (1).

cabhSec2FwPolicySelection – Permite la selección de la política de filtrado de fábrica por defecto, o del conjunto de reglas configuradas:

- factoryDefault (1) – Indica que la barrera contrafuego está utilizando la configuración de fábrica por defecto. Si este objeto está puesto a factoryDefault (1), la barrera contrafuego DEBE filtrar teniendo en cuenta la política de fábrica por defecto especificada.
- configuredRuleset (2) – Indica que la barrera contrafuego está utilizando el conjunto de reglas configurado por el operador del cable. Si este objeto se pone a configuredRuleset (2), la barrera contrafuego DEBE utilizar el conjunto de reglas configurado del que se tenga conocimiento más recientemente.

cabhSec2FwEventSetToFactory – Permite al operador del 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.

11.6.4.7.2 Objetos MIB para eventos de barrera contrafuego

Se DEBEN implementar en el PS los siguientes objetos de eventos de barrera contrafuego, 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 11.6.4.5.1 se definen los tipos de eventos.

cabhSec2FwEventEnable – Activa o desactiva el conteo y registro de los eventos de barrera contrafuego según su tipo, como se indica en cabhSec2FwEventType. Los requisitos de registro se definen en la cláusula sobre datos de registro de la presente Recomendación. 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 contrafuego DEBE registrar los eventos en el cabhSec2FwLog. La barrera 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 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, tal como lo indica cabhSec2FwEventType. Este intervalo tiene valor en tanto que no se supere 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 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, se borra el cuadro de registro del tipo de evento especificado. La lectura de este objeto siempre produce un resultado "False". Valor por defecto = False.

cabhSec2FwEventLogLastReset – Indica cuándo fue la última vez que se borró el registro.

11.6.4.7.3 Objetos MIB de política de barrera contrafuego

Proporcionan al operador del cable una forma de configurar las reglas que ha de utilizar la barrera contrafuego 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 política de filtrado de barrera contrafuego se basan en el conjunto mínimo de requisitos de filtrado. La capacidad de filtrado de la barrera 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 se utilizan algunos de los objetos de filtrado que ya han sido definidos en dicha referencia y se añaden algunos objetos MIB particulares de la barrera, 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 contrafuego. 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. Constituye el núcleo de la implementación de política, pues ésta se define y construye en este cuadro MIB. Cada paquete, entrante o saliente, se ha de comparar con la política habilitada.

En IPCable2Home se define una extensión docsDevFilterIPTable, el cabhSec2FwFilterScheduleTable donde figuran atributos de filtro para el instante de arranque, instante de fin y día de la semana que aparecen en la configuración de filtrado en las anotaciones del docsDevFilterIPTable. Gracias a este cuadro se introduce una regla o filtro que se puede activar a través 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. 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 p.m. a 7 a.m. y sábados y domingos de 10 p.m. a 8 a.m. La barrera contrafuego NO DEBE asociar restricciones de tiempo con ninguna política de filtrado, a menos que exista una regla explícita que defina dichas restricciones y que esté asociada claramente con direcciones IP conocidas.

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, DEBE aplicar el conjunto mínimo de capacidades y arquitectura de la barrera contrafuego, tal como se define en 11.6.4.4.1 y 11.6.4.4.3. 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 el FilterIpTable para las reglas de filtrado de la barrera. 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**
  - para filtrar el tráfico proveniente de la WAN, docsDevFilterIpIfIndex DEBE ponerse a 1;
  - para filtrar el tráfico proveniente de la LAN, docsDevFilterIpIfIndex DEBE ponerse a 255.
- **docsDevFilterIpDirection**

  Esta variable no tiene ningún valor para la barrera contrafuego. Por tanto, no importa cuál valor se le asigne en este objeto. No obstante, puesto que, docsDevFilterIpDirection se DEBE poner a un valor de 1, 2 ó 3, se debe fijar este objeto MIB a both(3), ya que [RFC 2669] no incluye un valor permitido para poder ignorar este objeto.

- **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**
- **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 contrafuego DEBE soportar los siguientes objetos MIB, como se especifica en el documento MIB de seguridad:

- **cabhSec2FwFilterScheduleStartTime –** El momento de inicio de las restricciones de tráfico, como se define en el conjunto de reglas.
- **cabhSec2FwFilterScheduleEndTime –** El momento para finalizar las restricciones de tráfico, como se define en el conjunto de reglas.
- **cabhSec2FwFilterScheduleDOW –** El día de la semana en que se aplican las restricciones de tráfico.

Las reglas del cabhSec2FwFilterScheduleTable para las restricciones de hora y día se asocian con políticas, con arreglo al docsDevFilterIPTable. Un paquete procesado con fecha e indicación de tiempo dentro del rango restringido de día y hora, conforme a este cuadro, se DEBE rechazar.

11.7 Objetos adicionales de MIB de seguridad en el PS

En la cláusula relativa a la barrera contrafuego en esta Recomendación se describen los objetos MIB de dicha barrera, 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 de 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.
- **clabMfgCVCCert –** Certificado de verificación de código de fabricante utilizado para almacenar el Cert CVC 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 respecto al tiempo medio de Greenwich (GMT, *greenwich mean time*).
  - **docsBpi2CodeMfgCvcAccessStart –** El valor actual del cvcAccessStart del fabricante de dispositivo respecto al GMT.
  - **docsBpi2CodeCoSignerOrgName –** El organizationName del cofirmante.
  - **docsBpi2CodeCoSignerCodeAccessStart –** El valor actual del codeAccessStart del cofirmante respecto 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 generadora SHA-1 [FIPS 186-2] de todo el contenido del fichero de configuración, considerado como una cadena de bytes.

11.7.3 Objetos MIB de 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 de certificado de PS

El PS DEBE soportar el siguiente objeto MIB de 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 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

Cuadro 11-19/J.192 – Directrices de diseño de 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 se activa esa función a través del fichero de configuración o de la instrucción SET SNMP.

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 incorporado viene controlada por el módem de cable. Gracias a la nueva copia imagen de software el operador de cable podrá 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 DEBERÁ permitir que se cambie la funcionalidad del elemento PS sin que sea necesario que el personal del operador de cable 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 bien:

  1) A través de una petición set SNMP del NMS al docsDevSwAdminStatus; o bien

  2) a través del fichero de configuración del elemento PS.

  Cuando el nombre de fichero de actualización de software que aparece en el fichero de configuración no corresponda con la copia imagen de software actual del dispositivo, el elemento PS DEBE solicitar el fichero especificado del 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 asincrónicamente 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.
- Con el proceso de descarga de software se DEBE suministrar al operador de cable un mecanismo para actualizar o disminuir la versión de código de los elementos IPCable2Home.
- Con el proceso de descarga de software se DEBEN 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 especificación 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.
- (Facultativo): El elemento PS DEBERÍA poder actualizar el certificado CA raíz de CVC almacenado en el dispositivo.
- (Facultativo): El elemento PS DEBERÍA poder reemplazar el o los certificados CA de fabricante almacenados en el dispositivo.
- (Facultativo): El elemento PS DEBERÍA poder actualizar el certificado de CA de CVC almacenado en el dispositivo.
- (Facultativo): El elemento PS DEBERÍA poder actualizar el certificado de CA raíz de proveedor de servicio almacenado en el dispositivo.

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 en esta Recomendación.

- Si el elemento PS se incorpora con un módem de cable, la imagen de PS/CM DEBE ser única, y sólo el módem de cable debe descargar el software.
- Cuando el elemento PS se componga de entidades autónomas separadas, DEBE ser el elemento PS el que efectúe la descarga de software para los elementos IPCable2Home, como se describe más adelante.

11.8.4.1 Estructura de 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 11-20.

Siempre que se descarguen certificados como parte del fichero de código, éstos PUEDEN incluirse en los campos que se especifican en el cuadro 11-20, y separados de la imagen de código real contenida en el campo CodeImage.

Cuadro 11-20/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 razíz 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 11-21. 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 11-21/J.192 – Datos firmados PKCS#7

Campo PKCS #7	Descripción
Signed Data {	
version	versión = 1
DigestAlgorithmIdentifiers	SHA-1
ContentInfo	
ContentType	datos (SignedContent concatenado al final de la estructura PKCS #7)
certificates {	(Certificación de verificación de código (CVC) de CableLabs)
mfgCVC	(REQUERIDO para todos los ficheros de código)

Cuadro 11-21/J.192 – Datos firmados PKCS#7

Campo PKCS #7	Descripción
co-signerCVC	(FACULTATIVO; requerido para las cofirmas)
} *end certificates*	
SignerInfo{	
MfgSignerInfo {	(REQUERIDO para todos los ficheros de código)
version	versión = 1
issuerAndSerialNumber	
issuerName	
CountryName	US
organizationName	CableLabs
CommonName	La raíz de CVC de CableLabs
certificateSerialNumber	<número de serie de CVC de fabricante>
digestAlgorithm	SHA-1
AuthenticatedAttributes	
contentType	datos (contentType de signedContent)
signingTime	UTCTime (GMT), YYMMDDhhmmssZ
messageDigest	(resumen del contenido como se define en [PKCS #7])
digestEncryptionAlgorithm	rsaEncryption
EncryptedDigest	
} *end mfg signer info*	
CoSignerInfo {	(FACULTATIVO; requerido para las cofirmas)
version	versión = 1
issuerAndSerialNumber	
issuerName	
CountryName	US
organizationName	CableLabs
CommonName	CableLabs CVC Root CA
certificateSerialNumber	<número de serie de CVC de cofirmante>
digestAlgorithm	SHA-1
AuthenticatedAttributes	
contentType	datos (contentType de signedContent)
signingTime	UTCTime (GMT), YYMMDDhhmmssZ
messageDigest	(resumen del contenido como se define en [PKCS #7])
digestEncryptionAlgorithm	rsaEncryption
EncryptedDigest	
} *end mso signer info*	
} *end signer info*	
} *end signed data*	

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);
- 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. 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 186-2]. 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 la 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 la 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 la 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 la 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 la 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 corresponder exactamente con la estructura mostrada en el cuadro 11-22, salvo por los cambios en el orden necesarios para codificar en DER (por ejemplo, el orden de los atributos SET OF). El elemento PS DEBERÍA rechazar el CVC si no corresponde con la estructura codificada en DER indicada en el cuadro 11-22. La codificación en DER DEBE cumplir con los requisitos de 11.3.4.2, "Infraestructura de clave pública (PKI)".

Cuadro 11-22/J.192 – Certificado de verificación de código conforme a X.509

Certificado X.509	Descripción
Certificate {	
version	2 (es decir, versión 3 de [UIT-T X.509])
serialNumber	entero, menor o igual a 20 octetos (es decir, número único atribuido por la CA raíz)
signature	RSA SHA-1, parámetros nulos
issuer	
countryName	US
organizationName	
commonName	CA raíz de CVC
validity	
notBefore	utcTime (GMT), YYMMDDhhmmssZ (es decir, hora de emisión)
notAfter	utcTime (GMT), YYMMDDhhmmssZ
subject	
countryName	<Nombre de país>
organizationName	<Nombre de empresa>
commonName	<Nombre común>
subjectPublicKeyInfo	
algorithm	Criptación RSA, parámetros nulos
subjectPublicKey	Módulo de 2048 bit
extensions	
KeyUsage	<Utilización de clave>
authorityKeyIdentifier	<Identificador de clave de autoridad>
signatureAlgorithm	RSA SHA-1, parámetros nulos
signatureValue	<Valor de firma>
} end certificate	

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). 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 Sujeto nombre de organización

El elemento PS podrá reconocer hasta dos nombres a la vez, que considere como un agente de confianza que firma 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 a través 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 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 PS incorporado:

- 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 del 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 la habilitación del elemento PS para 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, y su capacidad para actualizar ficheros de código haya sido inhabilitada, el elemento PS DEBE rechazar toda información contenida en un CVC subsiguiente que se reciba a través de SNMP.

El nombre de organización del fabricante del elemento PS y los valores de control dependientes del tiempo del fabricante DEBEN estar incluídos 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 Set SNMP. 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 de SNMP. Además, si el fichero de configuración del PS no incluye un CVC que se convalide adecuadamente, el elemento PS no necesita procesar los CVC que se reciban posteriormente, a través de un SET SNMP, y NO DEBE aceptar información proveniente de éstos, a través de un SET SNMP.

Al recibir el CVC en un fichero de configuración, el elemento PS DEBE:

1) Verificar que el CVC incluya la extensión de utilización de claves ampliada, como se define en 11.3.4.2.2.2.
2) Verificar el sujeto nombre de organización 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 de 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.

iii) Validar la firma de quien emite el CVC utilizando la clave pública de CA de CVC de CTL en poder del elemento PS.

iv) 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.

v) 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 en el CVC haya la extensión de utilización de clave ampliada, que se define en 11.3.4.2.2.2.

2) Verificar el sujeto nombre de organización de CVC, para:

   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 firmar el código

11.8.4.5.1 Requisitos de autoridad certificado (CA)

La CA de CVC de laboratorio de prueba de certificación firma y emite los certificados de verificación de código (CVC). El CVC DEBE ser exactamente como se especifica en 11.8.4.1.7. La CA de CVC de CTL NO DEBE firmar ningún CVC a menos que tenga el formato especificado en dicha cláusula. Antes de firmarlo, la CA de CVC de CTL DEBE verificar que la petición de certificado es auténtica.

Corresponde a la CA de CVC de CTL registrar los nombres de los abonados CVC autorizados, entre los que se encuentran los fabricantes de elemento PS y los operadores de cable que cofirmarán las imágenes de código. Corresponde a la CA de CVC de CTL garantizar que el nombre de organización de cada abonado CVC sea diferente. Al atribuir nombres de organización a los cofirmantes de ficheros de código se DEBE procurar cumplir las directrices que se especifican a continuación:

- El nombre de organización que se utiliza para autoidentificarse como agente cofirmante de código en un CVC DEBE ser atribuido por un CTL.
- El nombre DEBE consistir en una cadena que se pueda imprimir de ocho cifras hexadecimales que distingan unívocamente a un agente cofirmante de los demás.
- Cada cifra hexadecimal en el nombre se DEBE escoger del conjunto 0-9 (0x30-0x39) o A-F (0x41-0x46).
- No se permite y NO DEBE utilizarse en un CVC la cadena que consta de ocho cifras 0.

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 por 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 entre las reactivaciones/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 mediante el 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 una reactivación que afecta a un elemento PS durante la actualización iniciada a través de SNMP, dicho elemento DEBE reiniciar 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}.
- docsDevSwCurrentVers DEBE ser la versión actual del software que está funcionando en el dispositivo.

Cuando el elemento PS alcance el número máximo de reensayos (max retries = 3) que resultan de varias pérdidas de alimentación eléctrica o reinicios 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}.
- docsDevSwCurrentVers 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}.
- docsDevSwCurrentVers 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}.
- docsDevSwCurrentVers 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}.
- 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 de la nueva imagen si no se ha alcanzado aún el número MAX de reintentos de secuencia TFTP. Tras el sexagésimo 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}.
- docsDevSwCurrentVers DEBE ser la versión actual del software que funciona en el dispositivo.

11.8.4.6.2 Descarga de software iniciada a través de fichero de configuración

Empieza tras el envío del nombre de fichero de actualización de software en el fichero de configuración del elemento PS. Si este nombre no coincide con la imagen de software actual del dispositivo, el elemento PS DEBE solicitar al servidor de software el fichero especificado a través de TFTP.

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 reensayos (max retries = 3) por causa de varias interrupciones de alimentación eléctrica, o de reactivaciones durante la actualización iniciada a través de fichero de configuración, tras haber sido registrado el estado de dicho elemento DEBE cumplir con 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 other{5}.
- docsDevSwCurrentVers 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}.
- docsDevSwCurrentVers 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}.
- docsDevSwCurrentVers 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 sujeto organizationName del CVC sea idéntico al nombre de fabricante almacenado actualmente en la memoria del elemento PS;

b) la hora de inicio de validez del CVC sea mayor o igual que el valor de cvcAccessStart de fabricante presente en el elemento PS;

c) la extensión de utilización de clave ampliada esté presente en el CVC, como se define en 11.3.4.2.2.2.

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 hash SHA-1 a SignedContent. Cuando el valor del messageDigest no corresponda con dicha función, el elemento PS DEBE considerar inválida 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 suprimírse 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) 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.

iii) La extensión de utilización de clave ampliada esté presente en el CVC, como se define en 11.3.4.2.2.2.

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 hasta SHA-1, al SignedContent. Cuando el valor del messageDigest no corresponda a la nueva función hash, 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 versión de software

Proceso que consiste en suprimir la versión actualizada de la imagen de software descargada, y que hace retornar el dispositivo doméstico de cable a su estado anterior exacto.

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 contrafuego 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 de sistema de seguridad de fichero de configuración

Cuadro 11-23/J.192 – Directrices de diseño de sistema de seguridad

Referencia	Directrices
SEC14	El operador de cable podrá autenticar y, facultativamente, criptar el transporte de los ficheros de configuración hacia el PS o la barrera contrafuego.

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 contrafuego. Gracias al establecimiento de una sesión TLS entre el PS y el servidor HTTPS, se obtiene la seguridad. 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 contrafuego de una manera segura. El protocolo TLS permite autenticar y criptar la sesión, de conformidad con la configuración activada por el operador del 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 de el 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.

Cuadro 11-24/J.192 – Criptación de TLS

Datos de 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 utilizarlas, el PS DEBE rechazar los mensajes.

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 Ack de DHCP deberá incluir la dirección IP del servidor HTTPS en el campo siaddr. El Ack DHCP 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, 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 corresponda a la dirección IP en siaddr, del mensaje Ack de DHCP. Si el PS no recibe dicha correspondencia, 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, en el fichero de configuración de PS, la información necesaria para iniciar un fichero independiente de configuración de barrera contrafuego, como se especifica en la cláusula 6, DEBE establecer si es necesario seguir con la sesión TLS al servidor HTTPS, que aportó el fichero de configuración PS, o crear una nueva sesión TLS a otro servidor HTTPS para la descarga del fichero de configuración de barrera contrafuego. Cuando se ordene al PS descargar un fichero de configuración de barrera contrafuego a otro servidor HTTPS el mismo que se empleó para descargar el fichero de configuración del PS, DEBE establecer una sesión TLS, como se especifica en esta Recomendación, antes de solicitar el fichero de configuración de barrera contrafuego.

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 al 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 tras cinco intentos infructuosos, cada uno con una tolerancia de 30 segundos, no ha sido posible establecer la conexión TCP/IP, el PS DEBE enviar el evento 68002000.

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 de los mensajes de servidor en el PS

El PS DEBE poder procesar los mensajes de 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)

El PS DEBE enviar su certificado de elemento PS al servidor HTTPS dentro del mensaje ClientCertificate. Se espera que dicho servidor validará y verificará el certificado de cliente PS antes de efectuar la toma de contacto. Cuando el servidor no pueda autenticar el certificado PS, el cliente PS DEBE tratar el mensaje recibido como una alerta fatal y enviar el evento 68002200, con el código de error apropiado según [RFC 2246].

11.9.4.4 Series de conjunto de cifrado y compresión de TLS

Se DEBE enumerar la serie de 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 de 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. En esta Recomendación se requieren las series del conjunto de cifrado que son subconjunto de aquéllas disponibles y además el PS puede soportar otras más.

El PS DEBE soportar los siguientes algoritmos criptográficos:

- TLS_NULL_WITH_NULL_NULL;
- 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 contrafuego 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 contrafuego del mismo servidor HTTPS, inmediatamente después de haber procesado el fichero de configuración PS.

– El fichero de configuración de barrera contrafuego 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]. Los errores que tengan que ver con certificados se DEBEN tratar como graves, puesto que tanto el PS como el HTTP dependen de la autenticación de cliente y 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 contrafuego. 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 contrafuego 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 set SNMP.

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 y enviar el evento 68003000, utilizando el código de error adecuado proveniente de [RFC 2616]. De no poderse completar la descarga tras cinco intentos, cada uno con una tolerancia máxima de 240 segundos, el PS DEBE interrumpir la sesión y enviar el evento 68003100.

NOTA – Se concede un intervalo suficientemente largo para incluir la descarga del fichero de configuración, puesto que ésta puede ser bastante lenta. 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 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", norma [FIPS 140-2]. En particular, el PS DEBE cumplir con los requisitos de nivel 1 de seguridad FIPS PUBS 140-2.

Dicho nivel 1 requiere protección física mínima a través de la utilización de recintos de calidad 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 está integrada principalmente por texto informativo, destinada a facilitar la comprensión del mismo 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 de proceso asociadas al uso de las herramientas de gestión. Todos los procesos mostrados implican la interacción del elemento PS con los sistemas de 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 prueba 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 remota

La prueba de velocidad de conexión remota 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 SET SNMP.

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 GET SNMP.

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 GET SNMP. Si no se hubiera completado la prueba, los datos de prueba indicarían que la prueba continúa efectuándose. El NMS debe repetir la petición GET SNMP hasta que los resultados de la prueba indiquen la terminación de la misma.

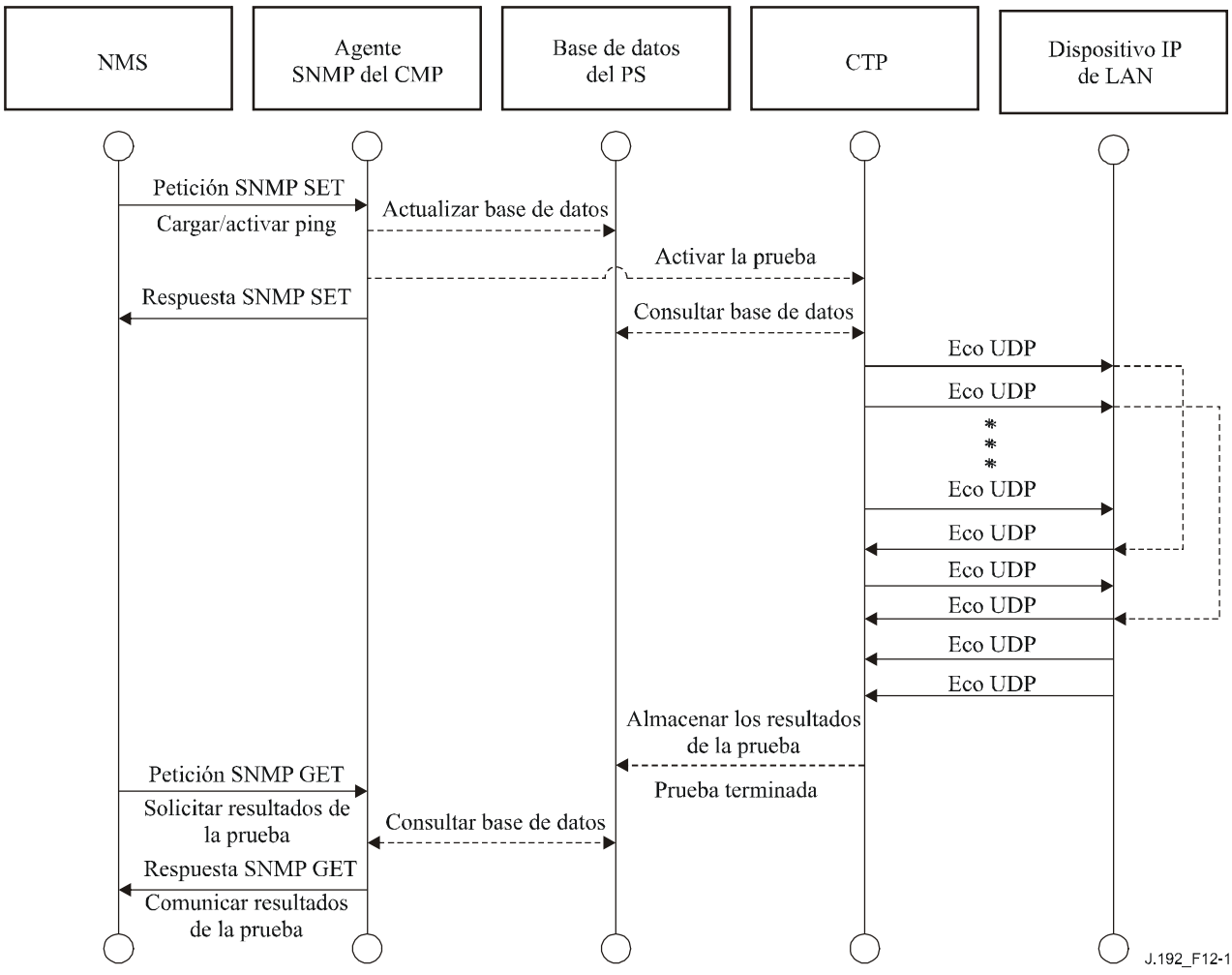


Figura 12-1/J.192 – Diagrama secuencial del proceso de prueba de la velocidad de conexión

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.

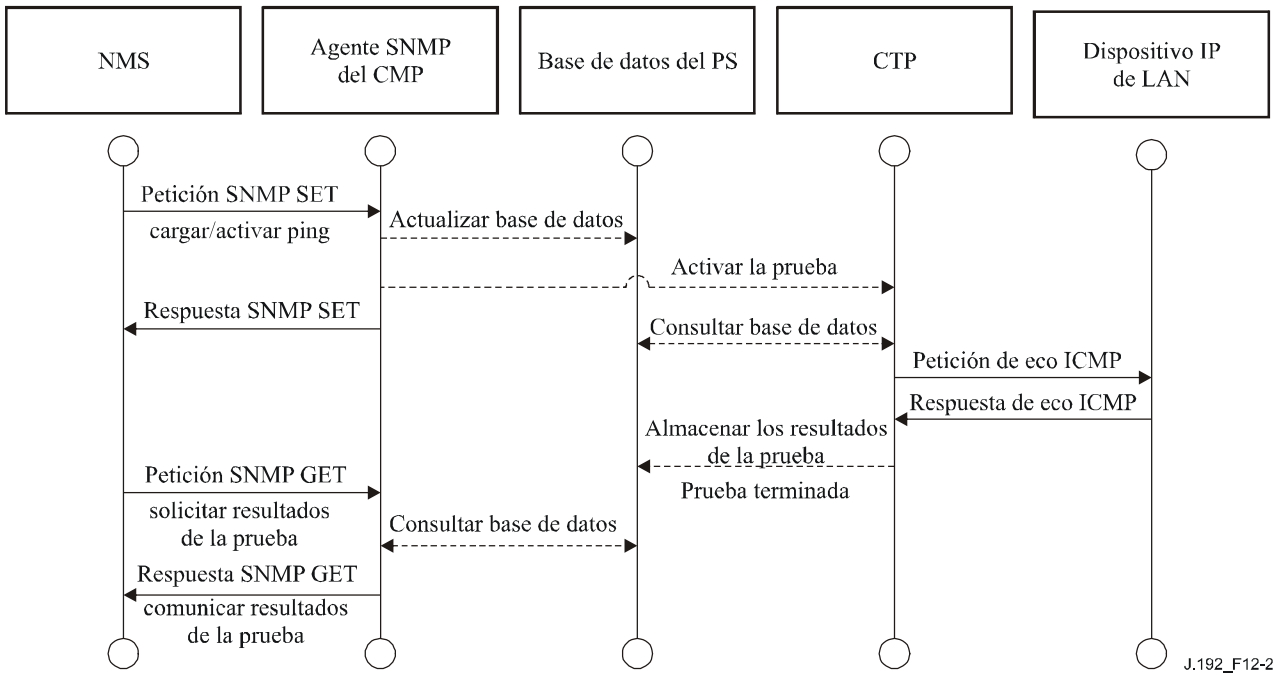


Figura 12-2/J.192 – Diagrama secuencial del proceso de la herramienta ping

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 SNMP GET-Request, SNMP GET-Next-Request y SNPM GET-Bulk 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".

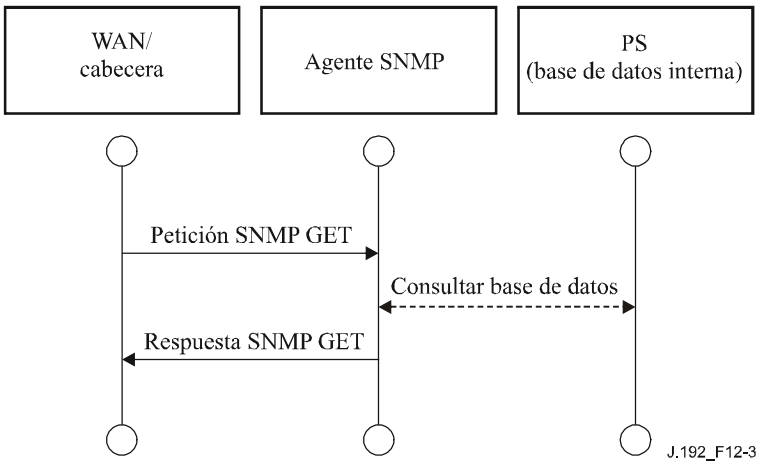


Figura 12-3/J.192 – Diagrama secuencial del acceso a la base de datos del PS desde la interfaz WAN-Man del PS

12.3.2 Reconfiguración

12.3.2.1 Descarga de software del PS

El ejemplo siguiente en la figura 12-4 ilustra el proceso de descarga de software y de microprogramas 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.

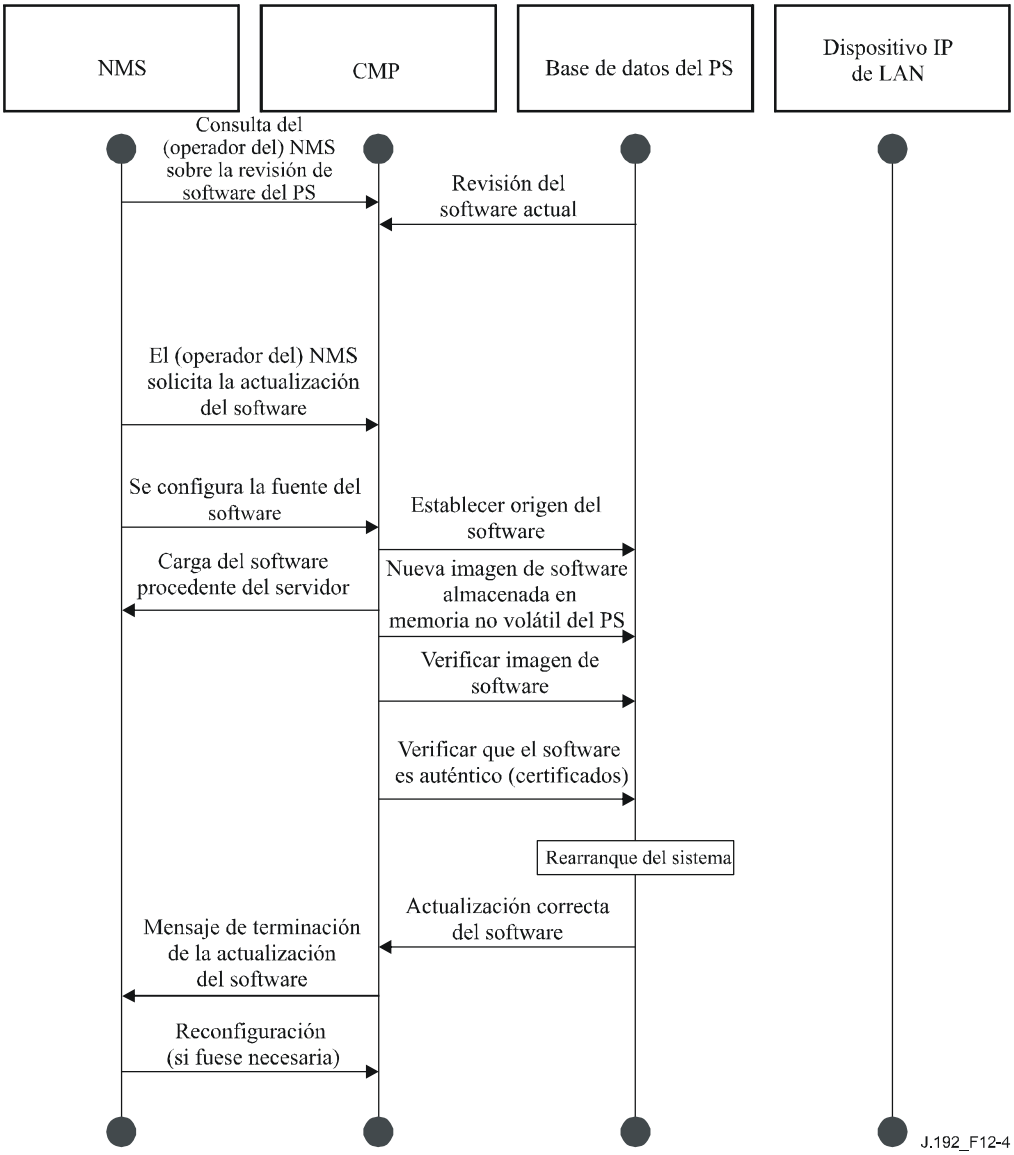


Figura 12-4/J.192 – Diagrama secuencial de la descarga de software del PS

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.

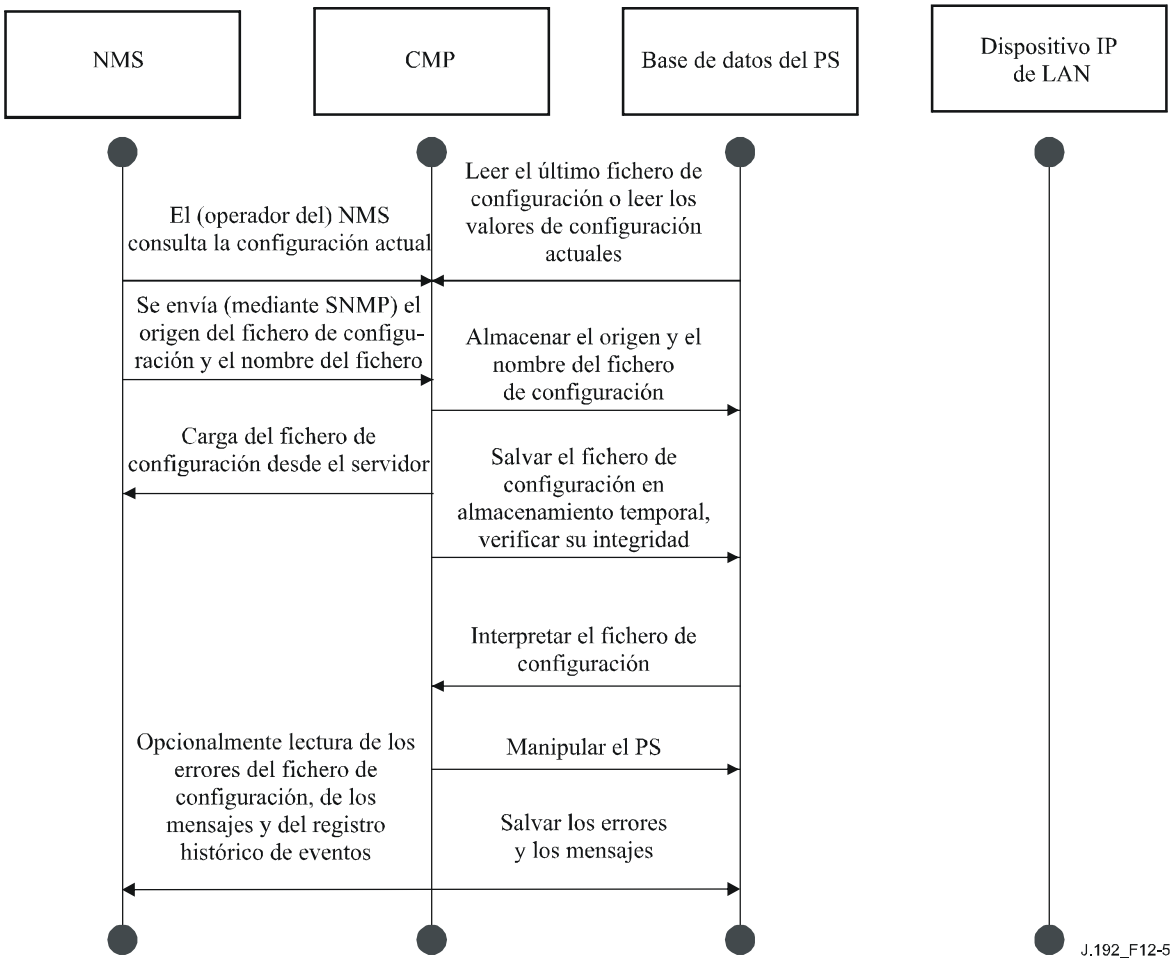


Figura 12-5/J.192 – Diagrama secuencial de la reconfiguración del PS (descarga del fichero de configuración)

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.

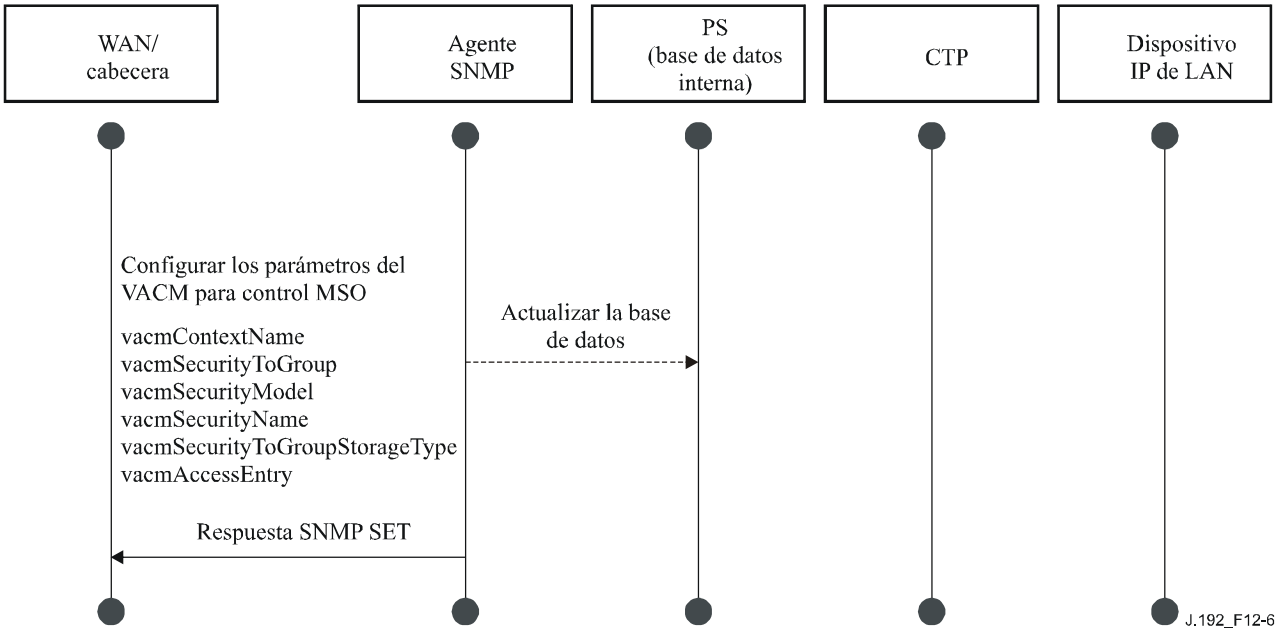


Figura 12-6/J.192 – Secuencia de configuración del PS (parámetros del VACM)

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.

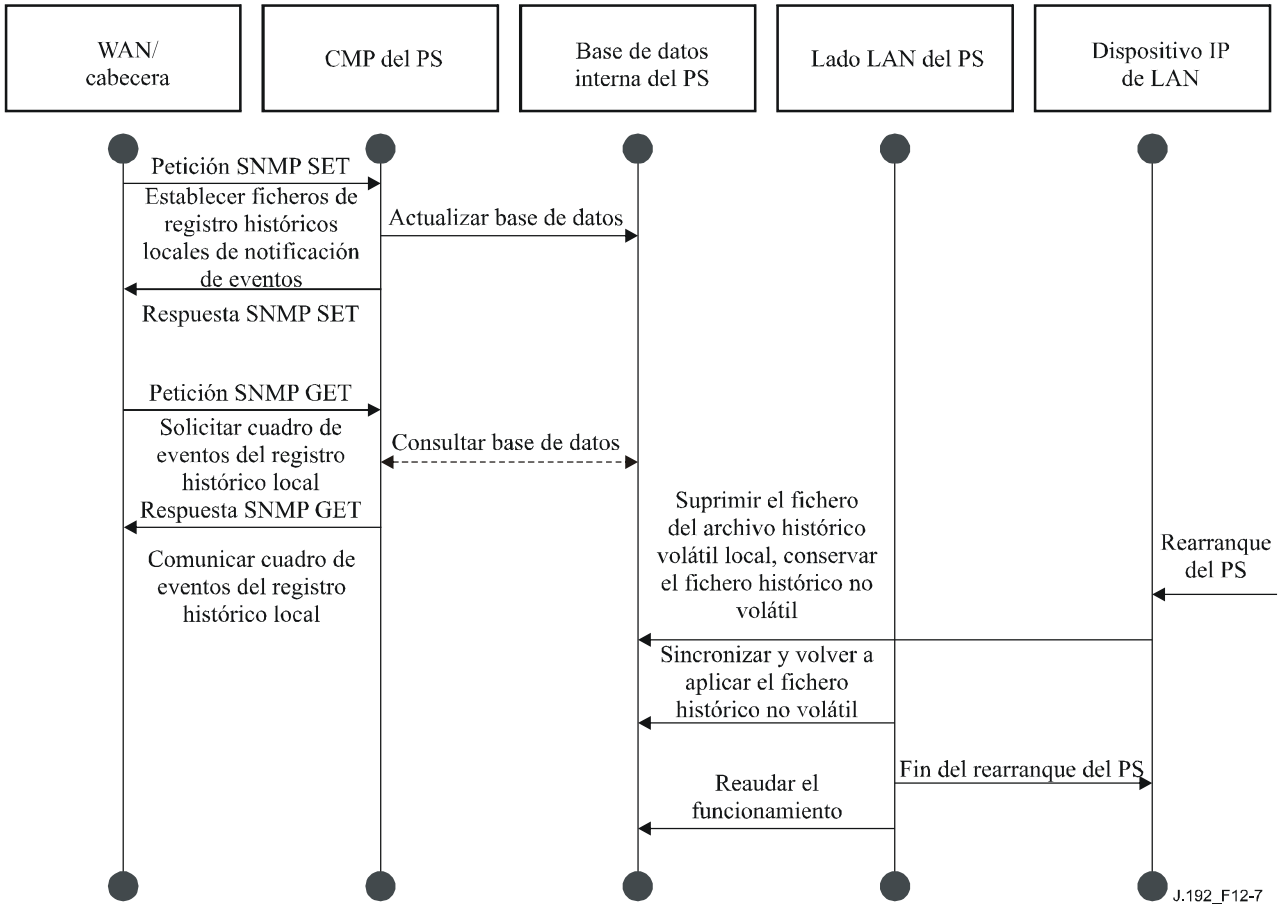


Figura 12-7/J.192 – Secuencia de la configuración del PS (control de eventos)

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, existe un error TLV que se comunica. 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.

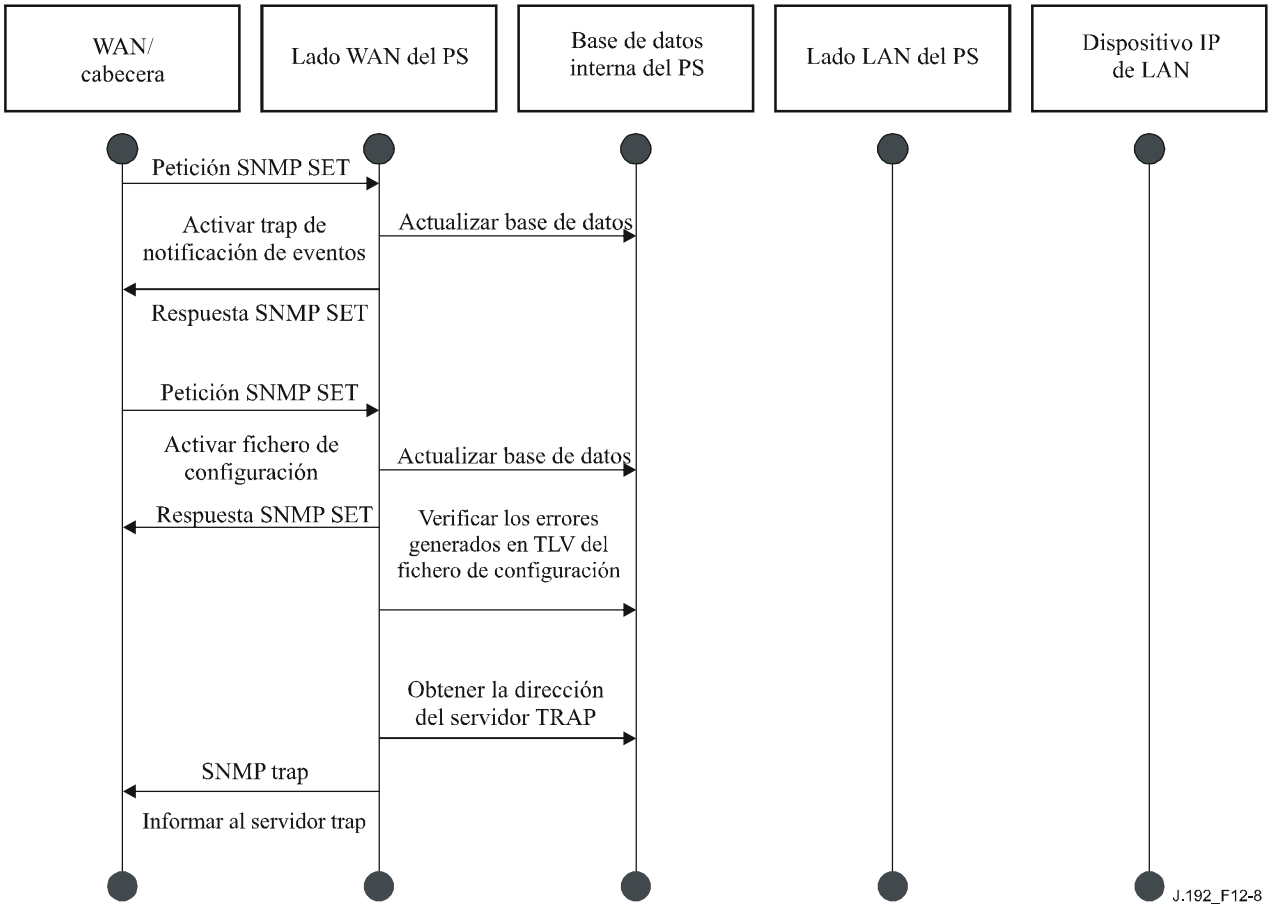


Figura 12-8/J.192 – Secuencia de descarga del fichero de configuración del PS (con TLV no válidos)

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 el SYSLOG.

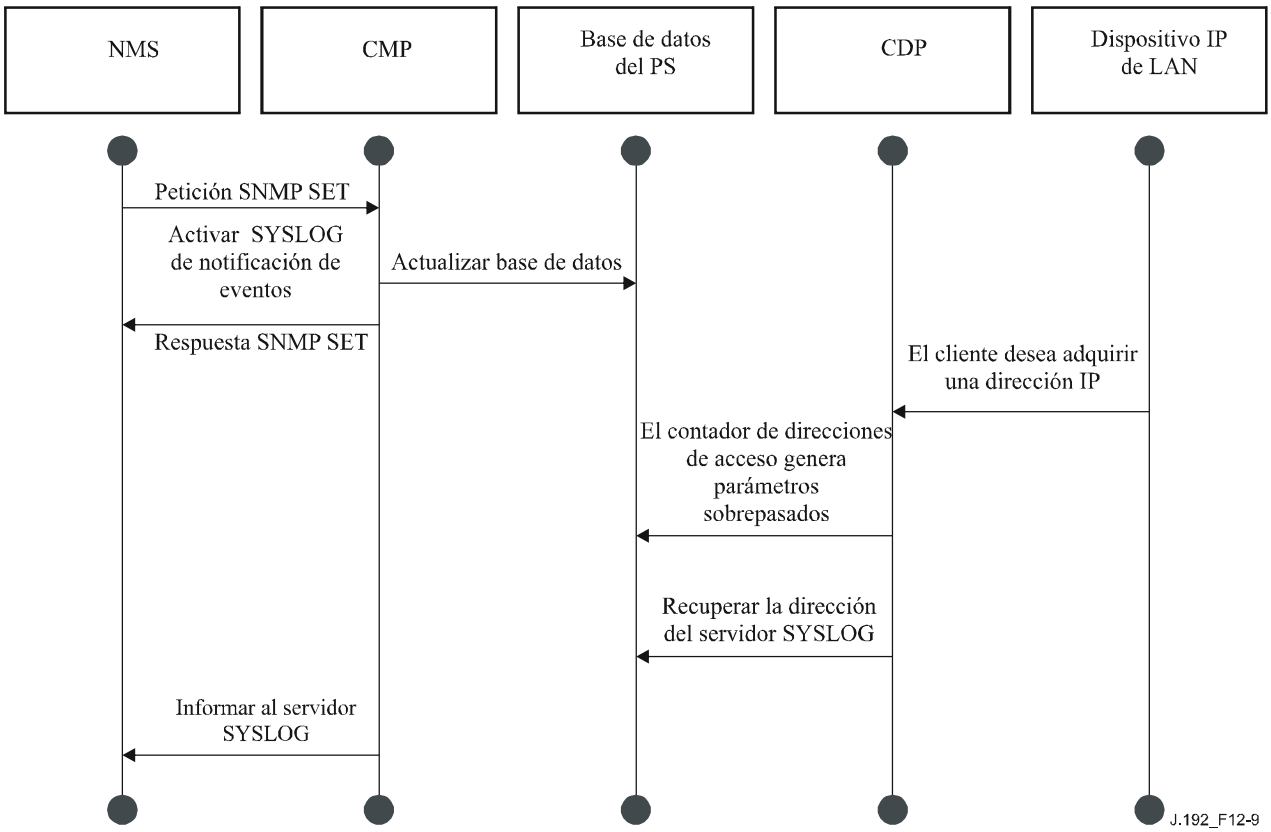


Figura 12-9/J.192 – Secuencia de adquisición de direcciones (la petición sobrepasa el contador suministrado)

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 la limitación de eventos son muy flexibles 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 en 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 reactivar la comunicación de eventos.

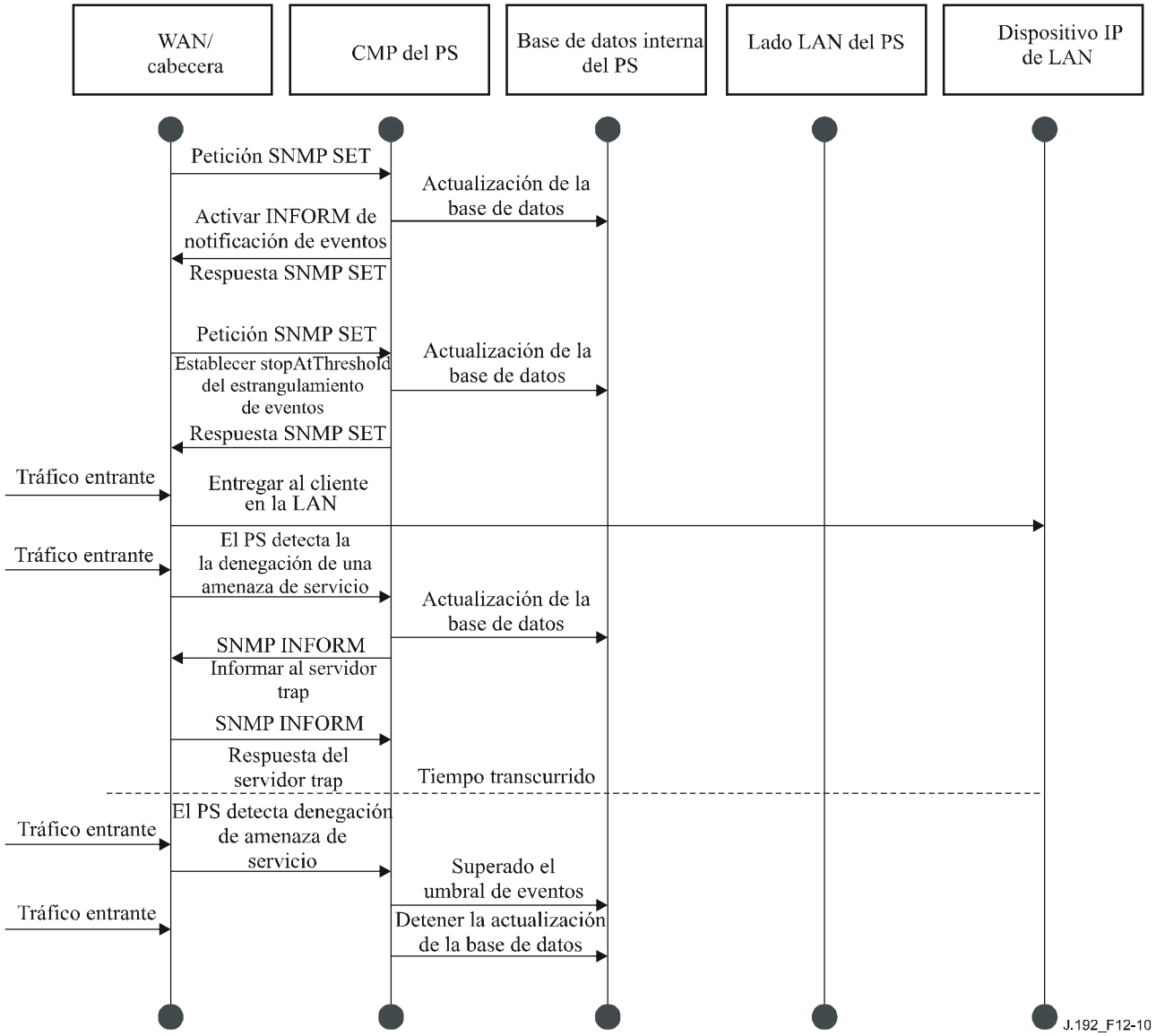


Figura 12-10/J.192 – Operación de estrangulamiento y limitación de eventos del CMP

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.

Los procesos de configuración descritos en esta cláusula corresponden a cada uno de los siguientes casos de interés:

- configuración WAN-Man del PS de la funcionalidad de gestión basada en la WAN del PS;
- configuración WAN-Data del PS 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;

- configuración de dispositivo IP de LAN en el sector LAN-Trans correspondiente a un dispositivo IP de LAN con una dirección IP traducida;
- configuración de dispositivo IP de LAN en el sector LAN-Pass correspondiente un dispositivo IP de LAN con dirección IP que se hace llegar 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 CableModem 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 un perfil discontinuo 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.

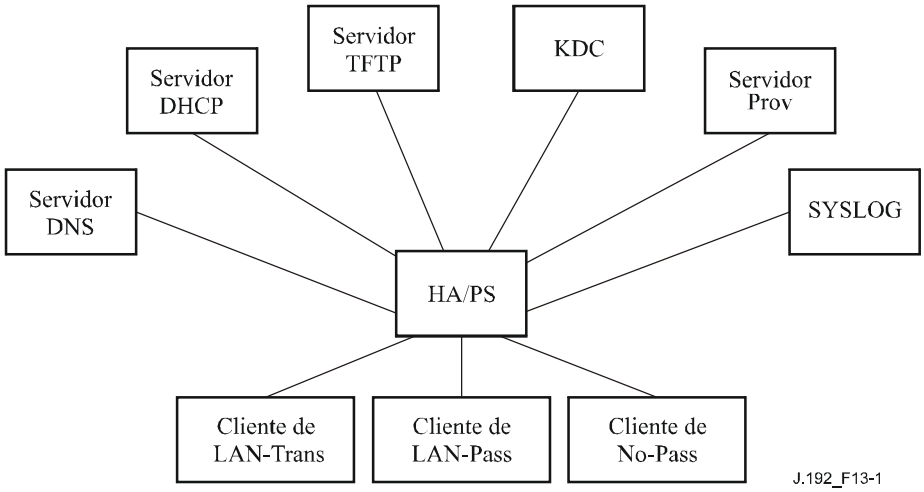


Figura 13-1/J.192 – Elementos funcionales de la configuración IPCable2Home

El servidor del protocolo de transferencia de fichero trivial (TFTP, *trivial file transfer protocol*) o el servidor del protocolo de transferencia de hipertexto (HTTP, *hypertext transfer protocol*) 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, *time of day*) 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, *dynamic host configuration protocol*) 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, *network management system*) cumple con las versiones SNMPv1, SNMPv2 y SNMPv3 del protocolo simple de gestión de red (SNMP, *simple network management protocol*) como se describe en la norma [RFC 2576]. El centro de distribución de claves (KDC) gestiona las claves de autorización y encriptación que permiten establecer la confianza entre los elementos en red y las reglas implementadas definidas en [RFC 1949]. El servidor del registro de 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 esta cláusula.

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.

En la figura 13-2 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.

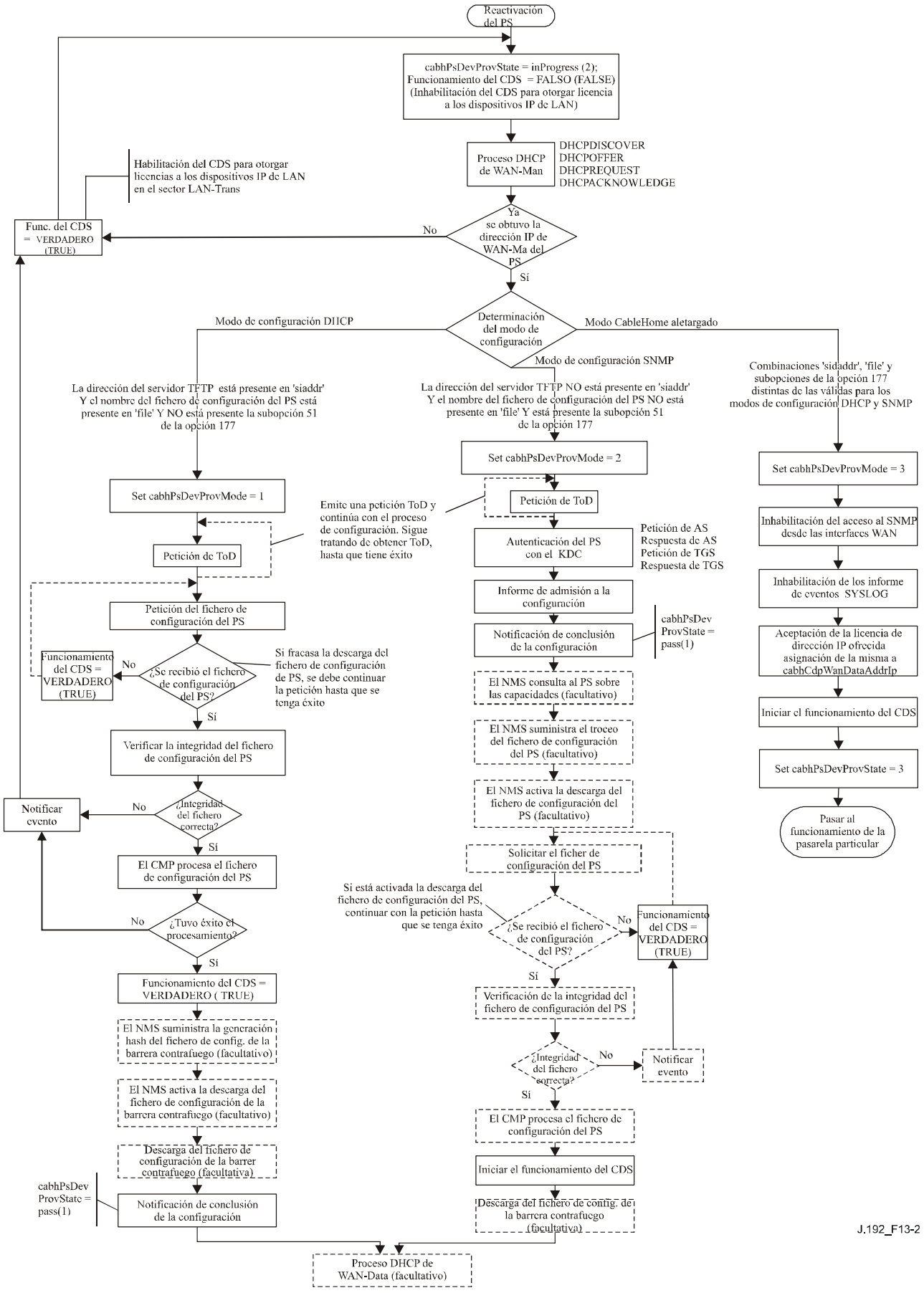


Figura 13-2/J.192 – Modos de configuración de IPCable2Home

13.2 Proceso de configuración de la gestión del PS: modo de configuración DHCP

El PS solicita del sistema de configuración de 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 13-3 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/reactivación.

El proceso opcional de descarga del fichero de configuración de la barrera contrafuego se muestra sombreado en la figura 13-3.

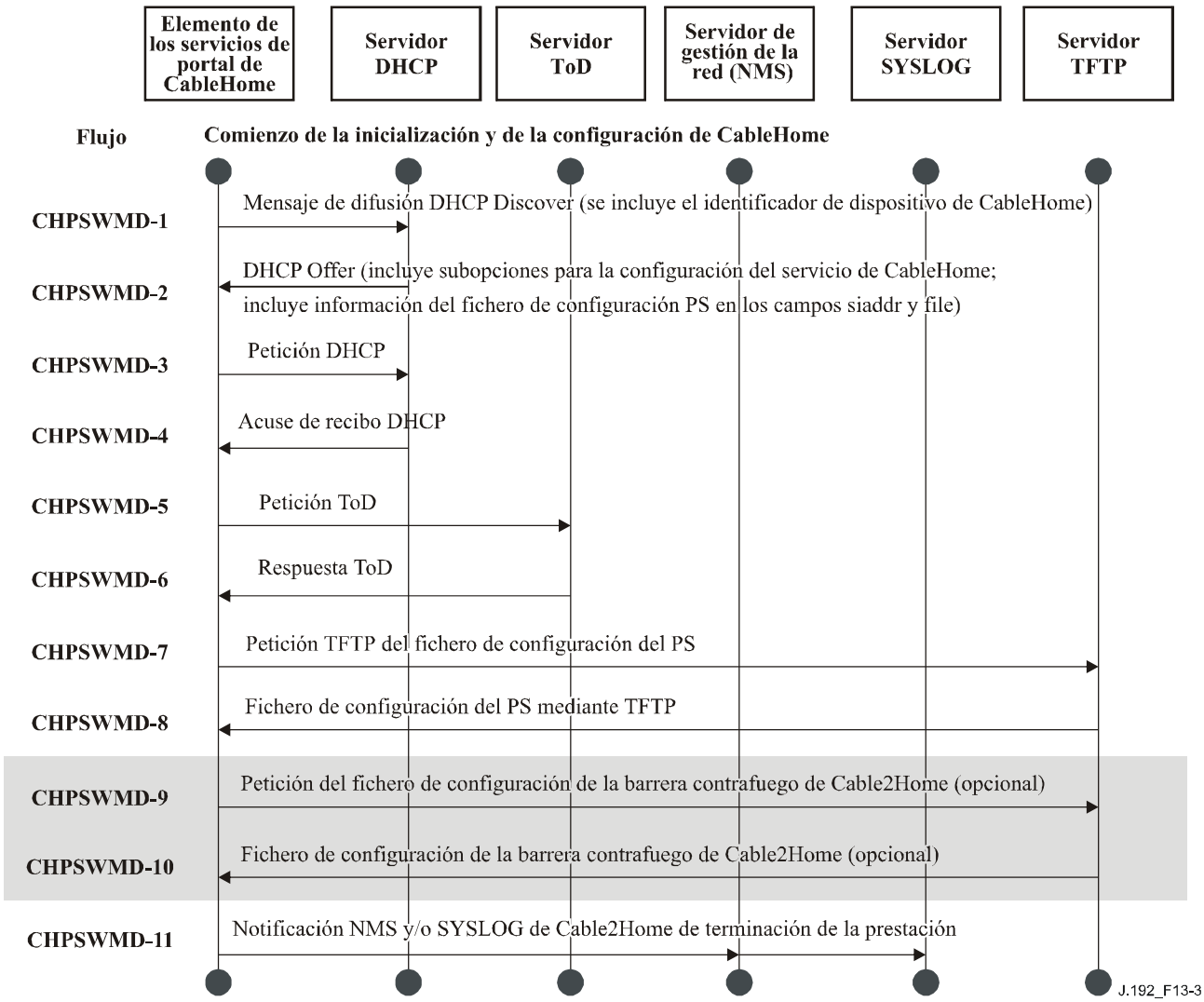


Figura 13-3/J.192 – Proceso de configuración de la gestión del PS – Modo de configuración DHCP

El cuadro 13-1 describe los mensajes CHPSWMD-1 a CHPSWMD-11 mostrados en la figura 13-3.

Cuadro 13-1/J.192 – Descripciones del flujo del proceso de configuración PS WAN-Man en el modo de configuración DHCP

Fase	Configuración WAN-Man del PS: modo de configuración DHCP	Secuencia normal	Secuencia de fallo
CHPSWMD-1	Mensaje de difusión DHCP discover El CDP (CDC) envía un mensaje DISCOVER DHCP de difusión para obtener la dirección IP de WAN-Man como se describe en 7.3.3.2.4. Esta difusión incluye opciones obligatorias relacionadas en el cuadro 7-10, "Opciones DHCP del CDC", en los mensajes DISCOVER y REQUEST. El PS fija cabhPsDevProvState a estado 'inProgress' (2) cuando el CDC envía un mensaje DISCOVER DHCP de difusión.	Comenzar la secuencia de configuración.	Si ha fallado de acuerdo con 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	DHCP OFFER	CHPSWMD-2 DEBE tener lugar una vez completada CHPSWMD-1.	Si se falla respecto al protocolo DHCP volver a CHPSWMD-1 y comunicar el error.
CHPSWMD-3	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 se falla respecto al protocolo DHCP volver a CHPSWMD-1 y comunicar el error.
CHPSWMD-4	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 se falla respecto al protocolo DHCP volver a CHPSWMD-1 y comunicar el error.

Cuadro 13-1/J.192 – Descripciones del flujo del proceso de configuración PS WAN-Man en el modo de configuración DHCP

Fase	Configuración WAN-Man del PS: modo de configuración DHCP	Secuencia normal	Secuencia de fallo
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.
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.	Continuar en CHPSWMD-7, comunicar el error y volver a CHPSWMD-5 (continuar reintentando ToD hasta que tenga éxito).
CHPSWMD-7	Petición TFTP El PS funcionando en el modo de configuración DHCP envía al servidor TFTP un TFTP GET Request 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. Véase 7.4.4 con relación al contenido del fichero de configuración del PS. Facultativamente, se incluyen la dirección IP del servidor TFTP del fichero de configuración de la barrera contrafuego, el nombre de dicho fichero y su troceo en el fichero de configuración del PS si hay un fichero de configuración de la barrera contrafuego que tenga que cargarse, y éste es el método seleccionado para especificarlo.	CHPSWM-8 DEBE tener lugar una vez completada CHPSWM-7.	Si falla la descarga TFTP, comunicar un error y volver a CHPSWMD-7 (continuar reintentando la descarga del fichero de configuración del PS). Si el proceso del fichero de configuración del PS provoca un error continuar en CHPSWMD-9 y comunicar el error como evento. Si expira el temporizador de configuración antes de la descarga con éxito del fichero de configuración del PS, el PS DEBE comunicar un error y volver a CHPSWMD-1.

Cuadro 13-1/J.192 – Descripciones del flujo del proceso de configuración PS WAN-Man 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 contrafuego (opcional) Si el PS recibe información del fichero de configuración de la barrera contrafuego (servidor TFTP de la barrera contrafuego y nombre del fichero de configuración de la barrera contrafuego) en el fichero de configuración del PS, el PS envía al servidor TFTP de configuración de la barrera contrafuego un TFTP GET Request solicitando un fichero de configuración de la barrera contrafuego (véase 11.6.4.2). Si el PS no recibe información de un fichero de configuración de la barrera contrafuego 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 terminada 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 contrafuego (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 contrafuego 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. Consúltese 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 contrafuego provoca un error, continuar y comunicar el error como evento.
CHPSWMD-11	Fin de la configuración Si lo solicita el sistema de configuración, se requiere al PS que informe al sistema de configuración del estado de configuración del PS. El sistema de configuración podría solicitar al PS que enviase un mensaje SYSLOG, una trampa SNMP, o ambos.	CHPSWMD-11 DEBE tener lugar una vez completada CHPSWMD-10.	Si falla la trampa SNMP, el servidor de configuración puede desconocer que se ha completado el proceso de configuración salvo que consulte el objeto cabhPsProvState.

Cuadro 13-1/J.192 – Descripciones del flujo del proceso de configuración PS WAN-Man en el modo de configuración DHCP

Fase	Configuración WAN-Man del PS: modo de configuración DHCP	Secuencia normal	Secuencia de fallo
	Si el PS completa con éxito todas las fases requeridas desde CHPSWMD-1 hasta CHPSWMD-10 y el PS recibió 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 PASS. Si el PS completa con éxito todas las fases de configuración desde CHPSWMD-1 a CHPSWMD-10 y el PS recibió parámetros válidos del receptor de notificaciones, el PS DEBE enviar una notificación de configuración completa (cabhPsDevInitTrap) con los parámetros adecuados al receptor de notificaciones. Si el temporizador de configuración del PS expira antes de completar las fases necesarias desde CHPSWMD-1 a CHPSWMD-10 y el PS recibió 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 fijado en FAIL. Si el temporizador de configuración del PS expira antes de completar todos los pasos necesarios desde CHPSWMD-1 a CHPSWMD-10 y el PS recibió parámetros válidos para el receptor de notificaciones, el PS DEBE enviar una notificación de configuración fallida (cabhPsDevInitTrap) 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. El PS DEBE actualizar el valor de cabhPsDevProvState con el estado 'fail' (3) y comunicar un evento que indique el fallo del proceso de configuración si el temporizador de configuración del PS expira antes de actualizar el valor de cabhPsDevProvState con el estado 'pass1.		

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 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 ACK DHCP, 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 13-4 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/reactivación.

En la figura 13-4 se muestra sombreado el proceso facultativo de descarga de un fichero de configuración de la barrera contrafuego.

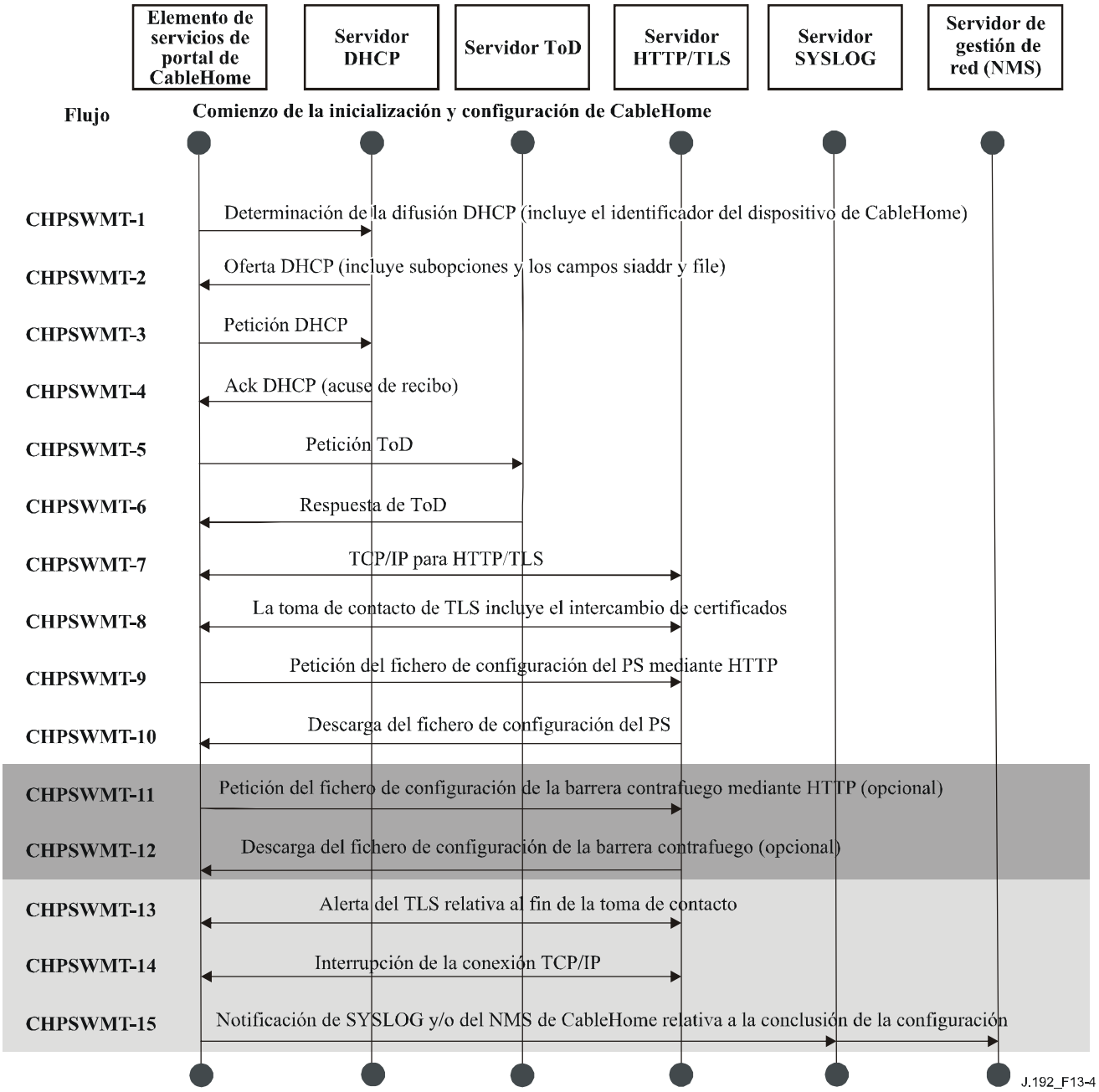


Figura 13-4/J.192 – Modo de configuración DHCP del proceso de configuración utilizando HTTP/TLS

En el cuadro 13-2 se describen los mensajes individuales CHPSWMT-1 – CHPSWMT-15 indicados en la figura 13-4. Véase 11.9, "Seguridad del fichero de configuración del PS en el modo de configuración DHCP" si se requiere mayor información.

Cuadro 13-2/J.192 – Descripciones de los flujos durante el 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	Determinación de la difusión de DHCP. El CDP (CDC) envía un mensaje DISCOVER DHCP de difusión para 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. El PS fija cabhPsDevProvState a estado 'in Progress' (2) cuando el CDC envía un mensaje DISCOVER DHCP de difusión.	Comienzo de la secuencia de configuración.	Si ha fallado por causa del protocolo DHCP notificar el error y continuar reintentando la determinación de la difusión 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	OFFER DHCP (oferta de DHCP)	CHPSWMT-2 DEBE tener lugar una vez completada CHPSWMT-1.	Si ha fallado por causa del protocolo DHCP volver a CHPSWMT-1 y notificar el error.
CHPSWMT-3	REQUEST DHCP (petición de DHCP) 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 ha fallado por causa del protocolo DHCP volver a CHPSWMT-1 y notificar el error.
CHPSWMT-4	ACK DHCP 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 ACK DHCP 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 ACK DHCP. Véase el cuadro 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 ha fallado por causa del protocolo DHCP volver a CHPSWMT-1 y notificar el error.

Cuadro 13-2/J.192 – Descripciones de los flujos durante el 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 de 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.	Notificar el error y volver a CHPSWMT-5 (continuar reintentando ToD hasta que se tenga éxito).
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 ha fallado por causa de 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 ha fallado por causa de 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 ha fallado por causa de HTTP, reintentar conforme a la especificación. Si fallan todos los reintentos, volver a CHPSWMT-1 y notificar el error.

Cuadro 13-2/J.192 – Descripciones de los flujos durante el 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 contrafuego y el nombre de ese fichero en el fichero de configuración del PS.	CHPSWMT-10 DEBE tener lugar una vez completada CHPSWMT-9.	Si ha fallado 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. Si el temporizador de configuración expira antes de que se descargue con éxito el fichero de configuración del PS, éste DEBE notificar el error y volver a CHPSWMT-1.
CHPSWMT-11	Petición HTTP – Fichero de configuración de la barrera contrafuego (opcional) Si el PS recibe información del fichero de configuración de la barrera contrafuego (servidor TFTP y nombre del fichero de configuración de la barrera contrafuego) en el fichero de configuración del PS, éste solicita el fichero de configuración de la barrera contrafuego 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 contrafuego (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 contrafuego 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 contrafuego produce un error, continuar y notificar el error como un evento.

Cuadro 13-2/J.192 – Descripciones de los flujos durante el 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-13	Alerta del TLS relativa al fin de la toma de contacto El PS DEBE desconectar 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.
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 CHPSWMT-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 una dirección del servidor SYSLOG en el mensaje OFFER DHCP, DEBE enviar un mensaje de conclusión de la 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 – Descripciones de los flujos durante el 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 OFFER DHCP, 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 DEBE actualizar el valor de cabhPsDevProvState al estado 'pass' (1) cuando se completan satisfactoriamente las fases del flujo de configuración CHPSWMT-1 a CHPSWMT-14. El PS DEBE actualizar el valor de cabhPsDevProvState al estado 'fail' (3) y notificar el evento indicando el fallo del proceso de configuración si el temporizador de configuración del PS expira antes de que el valor de cabhPsDevProvState se actualice al estado 'pass'.		

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.

La figura 13.5 ilustra 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/reactivación.

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 13-5 y definida en detalle en el cuadro 13-3. Los pasos opcionales se muestran sombreados en la figura 13-5. Estos pasos opcionales pueden tener lugar inmediatamente después de la fase CHPSWMS-15 con posterioridad a ésta o no tener lugar en absoluto.

El cuadro 13-3 describe las fases particulares del proceso de configuración ilustrado en la figura 13.5.

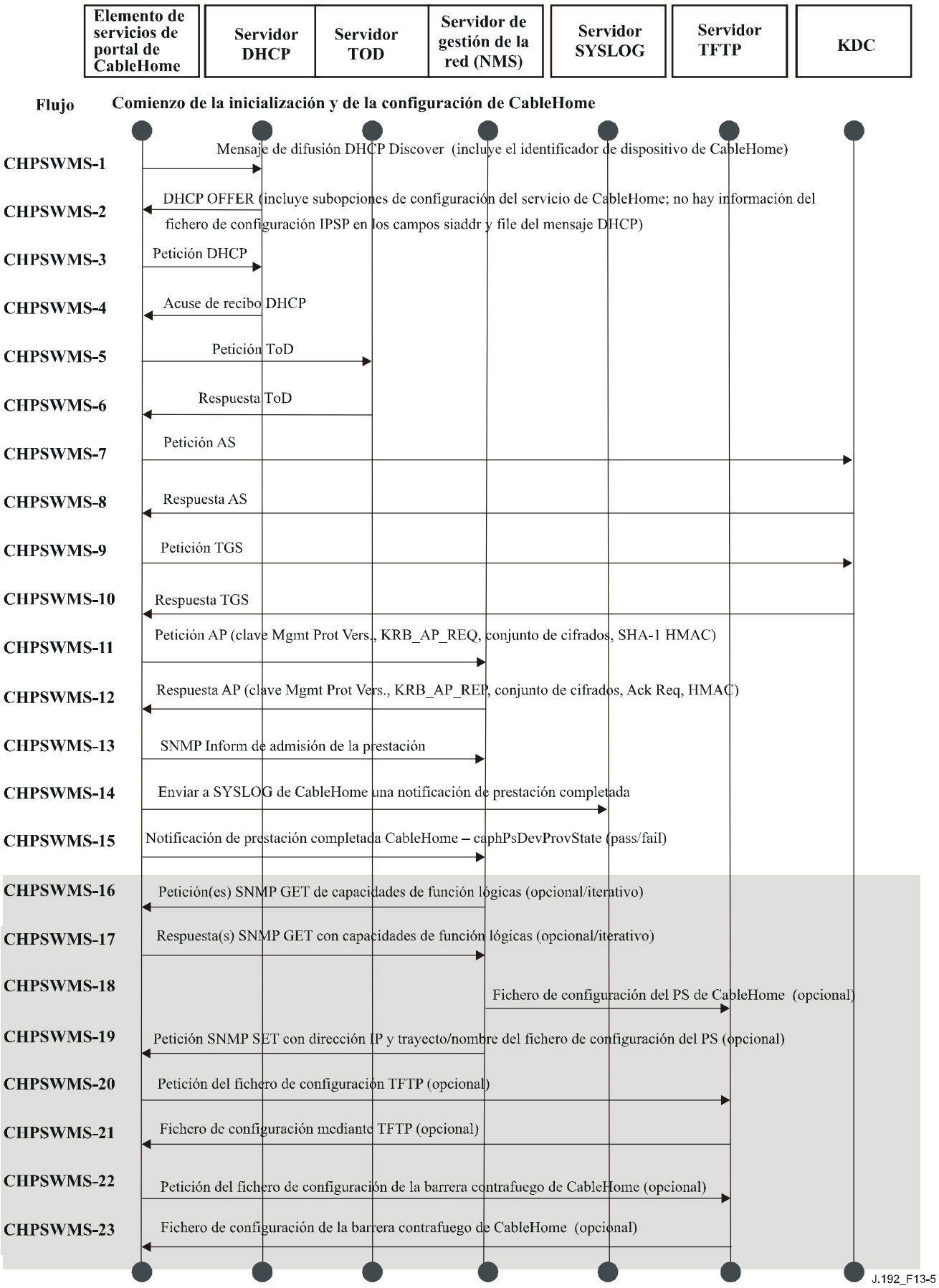


Figura 13-5/J.192 – Proceso de configuración de la gestión del PS – Modo de configuración SNMP

Cuadro 13-3/J.192 – Descripciones del flujo 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 ordinaria	Secuencia de fallo
CHPSWMS-1	Mensaje de difusión DHCP Discover El CDP (CDC) difunde un mensaje DISCOVER DHCP 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 DISCOVER DHCP.	Comenzar la secuencia de configuración.	Si el fallo ocurre por causa del protocolo DHCP comunicar un error y continuar reintentando el mensaje de difusión DHCP Discover hasta tener éxito (volver a CHPSWMS-1). Si falla el primer intento para obtener una licencia de dirección del servidor DHCP del operador del cable, se debe iniciar el funcionamiento del CDS como se describe en 7.3.3.2.4, "Requisitos del CDC".
CHPSWMS-2	DHCP OFFER	CHPSWMS-2 DEBE tener lugar tras completarse CHPSWMS-1.	Si el fallo ocurre en virtud del protocolo DHCP volver a CHPSWMS-1 y comunicar un error.
CHPSWMS-3	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 el fallo ocurre en virtud del protocolo DHCP volver a CHPSWMS-1.
CHPSWMS-4	DHCP ACK El servidor DHCP envía un mensaje ACK DHCP al CDC que incluye la dirección IPv4 de la interfaz WAN-Man del PS que se supone que contiene la opción código 177 de IPCable2Home, con las subopciones 3, 6 y 51 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 ACK DHCP (véase 7.2.3.3). El PS almacena la dirección del servidor de hora del día en cabhPsDevTimeServerAddr.	CHPSWMS-4 DEBE tener lugar tras completarse CHPSWMS-3.	Si el fallo ocurre en virtud del protocolo DHCP volver a CHPSWMS-1 y comunicar un error.

Cuadro 13-3/J.192 – Descripciones del flujo 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 ordinaria	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.	Comunicar un error y volver a CHPSWMS-5 (continuar reintentando ToD hasta tener éxito).
CHPSWMS-7	Petición AS (nota 1) El PS envía el mensaje de petición AS al KDC de IPCable2Home del MSO suministrado en la subopción 51 de la opción 177 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 de 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 Si el PS obtuvo el tique de concesión de tique (TGT, *ticket granting ticket*) en la fase CHPSWMS-8, envía el mensaje de petición de TGS al servidor KDC del MSO cuya dirección fue transferida al PS (CDC) en la subopción 51 de la opción 177 de DHCP.	CHPSWMS-9 DEBE tener lugar tras completarse CHPSWMS-8.	Volver a CHPSWMS-1. El PS inicia el funcionamiento del CDS.
CHPSWMS-10	Respuesta TGS Se recibe el mensaje de respuesta TGS con el tique procedente del KDC de IPCable2Home de MSO.	CHPSWMS-10 DEBE tener lugar tras completarse CHPSWMS-9.	Volver a CHPSWMS-1. El PS inicia el funcionamiento del CDS.

Cuadro 13-3/J.192 – Descripciones del flujo 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 ordinaria	Secuencia de fallo
CHPSWMS-11	Petición AP El PS envía el mensaje de 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 de 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	SNMP Inform Después de que el PS que funciona en el modo de configuración SNMP establece las claves de SNMPv3, DEBE enviar un INFORME de SNMPv3 (cabhPsDevProvEnrollTrap) solicitando la admisión a SNMP ENTITY cuya dirección IP fue transferida en la subopción 3 de la opción 177, en el mensaje DHCP ACK.	CHPSWMS-13 DEBE tener lugar tras completarse CHPSWMS-12.	Volver a CHPSWMS-1.
CHPSWMS-14	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 de 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-14 DEBE tener lugar tras completarse CHPSWMS-13.	

Cuadro 13-3/J.192 – Descripciones del flujo 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 ordinaria	Secuencia de fallo
CHPSWMS-15	SNMP Inform El PS DEBE enviar al NMS un SNMP INFORM (cabhPsDevInitTrap) con una notificación "configuración completada". Se presenta FAIL cuando fracasa el proceso del fichero de configuración. De lo contrario el estado de configuración es PASS. El PS DEBE actualizar el valor cabhPsDevProvState con el estado 'pass' (1) cuando las fases de configuración CHPSWMS-1 a CHPSWMS-15 se completan con éxito. El PS DEBE actualizar el valor de cabhPsDevProvState con el estado 'fail' (3) y comunicar un evento indicando el fallo del proceso de configuración si el temporizador de configuración del PS expira antes de la actualización del valor de cabhPsDevProvState con el estado 'pass'.	CHPSWMS-15 DEBE tener lugar tras completarse CHPSWMS-14.	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.
Fases opcionales			
CHPSWMS-16	SNMP GET 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 petición GET-Bulk para obtener varias informaciones en un único mensaje.	CHPSWMS-16 no debe tener lugar antes de completarse CHPSWMS-15.	Volver a CHPSWMS-1.
CHPSWMS-17	Respuesta SNMP GET Iterativo: El PS responde a NMS los mensajes de petición GET Request o GET-bulk con una respuesta GET para cada una de las peticiones GET. Una vez terminados todos los GET y los GetBulk, el NMS envía el dato solicitado a la aplicación de configuración.	Si CHPSWMS-16 tiene lugar, CHPSWMS-17 DEBE suceder tras completarse CHPSWMS-16.	N/A

Cuadro 13-3/J.192 – Descripciones del flujo 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 ordinaria	Secuencia de fallo
CHPSWMS-18	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-17 tiene lugar, CHPSWMS-18 DEBE suceder tras completarse CHPSWMS-17.	N/A
CHPSWMS-19	SNMP SET 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 7.4.4.1, "Requisitos del formato del fichero de configuración" (modo de configuración SNMP). Opcionalmente, la dirección IP del servidor TFTP del fichero de configuración de la barrera contrafuego, el nombre del fichero de configuración de la barrera contrafuego, el troceo del fichero de configuración de la barrera contrafuego y la clave de criptación (si se cripta el fichero de configuración de la barrera contrafuego, se incluyen en el SNMP Set si ha de cargarse un fichero de configuración de la barrera contrafuego y se selecciona este método para especificarlo.	Si CHPSWMS-18 tiene lugar, CHPSWMS-19 DEBE suceder tras completarse CHPSWMS-18.	Volver a CHPSWMS-1 si se recibió el Set pero tuvo lugar un error de proceso.
CHPSWMS- 20	Petición TFTP Si el NMS activa la descarga por parte del PS del fichero de configuración del PS descrito en 7.4.4.1, el PS DEBE enviar al servidor TFTP una petición TFTP GET para solicitar el fichero de configuración del PS especificado.	Si CHPSWMS-19 tiene lugar, CHPSWMS-20 DEBE suceder tras completarse CHPSWMS-19.	Continuar en CHPSWMS-19.

Cuadro 13-3/J.192 – Descripciones del flujo 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 ordinaria	Secuencia de fallo
CHPSWMS-21	El servidor TFTP envía el fichero de configuración Una vez recibido por el PS el fichero de configuración del PS, calcula el troceo de éste y lo compara con el valor recibido en la fase CHPSWMS-19. A continuación el PS procesa el fichero de configuración del PS. Opcionalmente, la dirección IP del servidor TFTP del fichero de configuración de la barrera contrafuego, el nombre del fichero de configuración de la barrera contrafuego y el troceo del fichero de configuración de la barrera contrafuego se incluyen en el fichero de configuración del PS cuando hay que cargar un fichero de configuración de la barrera contrafuego, y éste es el método seleccionado para especificarlo.	Si CHPSWMS-20 tiene lugar, CHPSWMS-21 sucede tras completarse CHPSWMS-20.	Si falla la descarga TFTP, comunicar el error, continuar en CHPSWMS-22, y continuar reintentando CHPSWMS-20 (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.
CHPSWMS-22	TFTP Request – Fichero de configuración de la barrera contrafuego (opcional) El PS envía al servidor TFTP de configuración de la barrera contrafuego una petición TFTP GET para solicitar el fichero de datos de configuración de la barrera contrafuego 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 contrafuego 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 contrafuego, 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 contrafuego provoca un error, continuar y comunicar el error como evento.
NOTA 1 – Las fases CHPSWMS-5 a CHIPSWMS-8 son opcionales en ciertos casos. Pueden consultarse los detalles en 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, del 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 contrafuego contiene información para proveer la función de barrera contrafuego. La indicación de descarga del fichero de configuración de la barrera contrafuego 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 que el PS continúe los ciclos del proceso de configuración cuando queda incompleta alguna operación. El objeto temporizador, cabhPsDevProvTimer, tiene un valor de inicialización por defecto de cinco minutos.

13.4.3 Informe de terminación de la admisión a configuración y de la 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 terminación 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 proveerse mediante el proceso DHCP. El evento SYSLOG no se enviará si no se configura 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.

Los siguientes diagramas ilustran 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 13-6 y describe el cuadro 13-4 detalladamente.

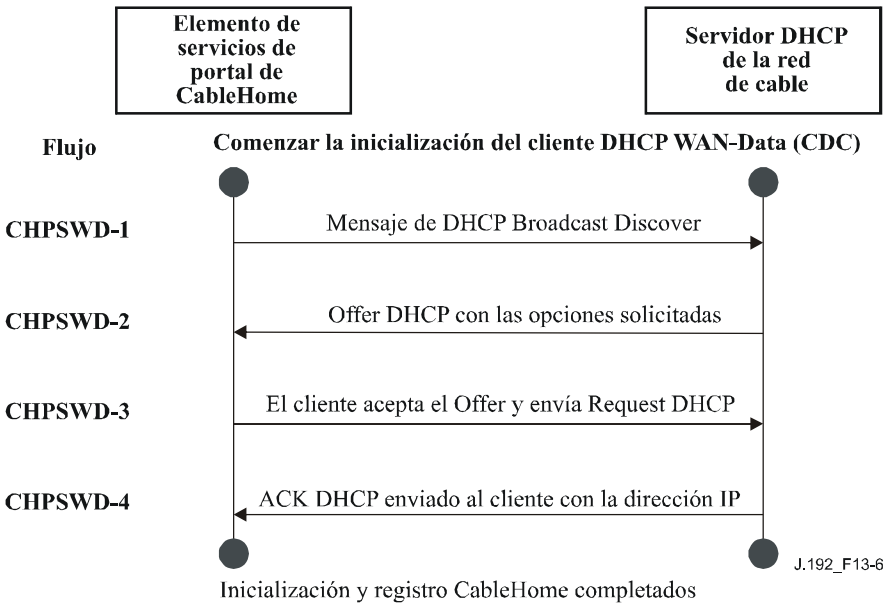


Figura 13-6/J.192 – Proceso de configuración WAN-Data del PS

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 ordinaria	Secuencia de fallo
CHPSWD-1	Mensaje de difusión DHCP Discover El PS envía un mensaje de difusión DHCP DISCOVER 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 en virtud del protocolo DHCP repetir CHPSWD-1.
CHPSWD-2	DHCP OFFER El servidor DHCP de 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 agotará el tiempo en virtud del protocolo DHCP y se repetirá la fase CHPSWD-1.
CHPSWD-3	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 hay fallo en virtud del protocolo DHCP volver a CHPSWD-1.
CHPSWD-4	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 en virtud del protocolo DHCP volver a CHPSWD-1.

13.6 Proceso de configuración: BP en el sector LAN-Trans

Los elementos lógicos de punto de frontera (BP) son necesarios para implementar dos protocolos que se emplean durante su proceso de configuración: mensajería DHCP [RFC 2131] y BP_Init, que se describen en 6.5.3.2, "Función de los mensajes de LAN de MBP".

La función CDP (CDS) del elemento PS responde a los mensajes DHCP emitidos por los BP en el sector LAN-Pass, de acuerdo a los requisitos determinados en 7.3.3.1.4, "Requisitos de la función del CDS". La función CMP del PS responde a los mensajes BP_Init que se reciben de los BP. Esto se describe en 6.3.3.4, "Función de los mensajes LAN del CMP".

En esta cláusula se describe el proceso de configuración para el caso en el que el NMS ha configurado el PS para que funcione en el modo de tratamiento de paquetes primario C-NAT o C-NAPT (véase la cláusula 8). No hay diferencia en el proceso de configuración del BP del sector LAN-Trans entre los modos de configuración DHCP y SNMP.

El proceso de configuración de un BP en el sector LAN-Trans DEBE tener lugar mediante la secuencia ilustrada en la figura 13-7 y descrita con detalle en el cuadro 13-5.

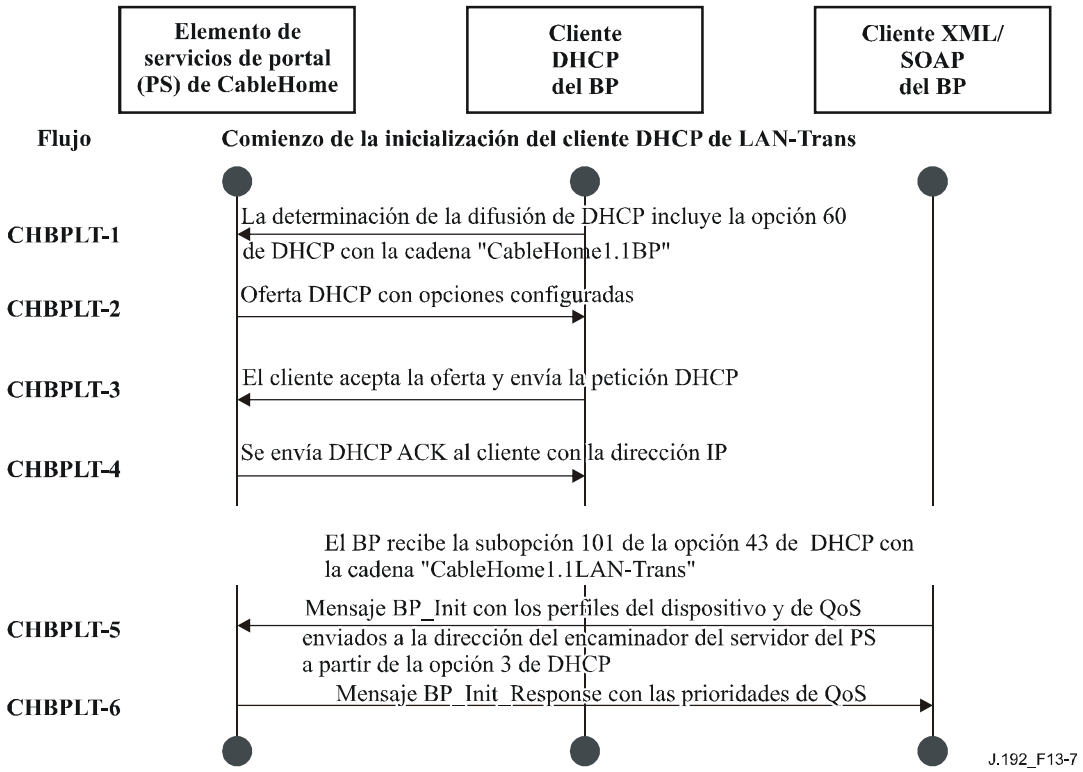


Figura 13-7/J.192 – Proceso de configuración de un BP en el sector LAN-Trans

Cuadro 13-5/J.192 – Descripciones de los flujos del proceso de configuración del BP en el sector LAN-Trans

Fase del flujo	Configuración de la dirección LAN-Trans del cliente	Secuencia normal	Secuencia en caso de fallo
CHBPLT-1	Determinación de la difusión DHCP El cliente DHCP (nota 1) envía un mensaje de difusión DHCP DISCOVER por su red LAN local (nota 2) . El BP debe incluir la opción 60 de DHCP con la cadena "CableHome1.1BP".	Continuar en CHBPLT-2.	Si falla por causa del protocolo DHCP repetir CHBPLT-1.
CHBPLT-2	Oferta DHCP El PS recibe el mensaje DISCOVER DHCP por su interfaz LAN y examina el campo chaddr. Si: – hay una dirección LAN-Trans disponible; y – no hay impedimentos administrativos para denegar la dirección LAN-Trans al cliente; el PS DEBE enviar un mensaje OFFER DHCP al cliente para ofrecerle la dirección de LAN-Trans ya sea para unidifusión o para difusión específica del enlace (conforme al bit BROADCAST del campo banderas en el mensaje DISCOVER DHCP). Si la determinación de DHCP incluye la opción 60 de DHCP con la cadena "CableHome1.1BP" el PS debe incluir la subopción 101 de la opción 43 de DHCP con la cadena "CableHome1.1LANTrans" en el mensaje DHCP Offer.	Continuar en CHBPLT-3.	Si falla, el cliente alcanzará su límite temporal conforme al protocolo DHCP y se repetirá CHBPLT-1.
CHBPLT-3	Petición de DHCP El cliente DHCP del dispositivo IP de LAN recibe el mensaje OFFER DCHP. Cuando un cliente de este tipo desea aceptar OFFER DCHP, se prevé que formateará y enviará un paquete REQUEST DHCP utilizando difusión específica del enlace (nota 3).	Continuar en CHBPLT-4.	Si falla, el cliente cancelará el temporizador del protocolo DHCP y se repetirá CHBPLT-1.

Fase del flujo	Configuración de la dirección LAN-Trans del cliente	Secuencia normal	Secuencia en caso de fallo
CHBPLT-4	Mensaje DHCP ACK El PS recibe el mensaje REQUEST DHCP por su interfaz LAN. Si la dirección LAN-Trans indicada aún puede asignarse, el PS DEBE enviar el mensaje ACK DHCP al cliente como unidifusión o difusión específica del enlace (de acuerdo con el bit BROADCAST del campo banderas en el mensaje REQUEST DHCP). El mensaje ACK DHCP incluye la subopción 101 de la opción 43 de DHCP con la cadena "CableHome1.1LAN-Trans". Esto indica al BP que se encuentra en el sector de direcciones de LAN-Trans y que recibió la dirección IP del encaminador del servidor del PS en la opción 3 de DHCP. Por consiguiente, el BP debe enviar mensajes BP_Init a la dirección IP del encaminador del servidor del PS.	Continuar en CHBPLT-5.	Si falla, el cliente alcanzará su límite temporal conforme al protocolo DHCP y se repetirá CHBPLT-1.
CHBPLT-5	Mensaje BP_Init El BP envía un mensaje BP_Init SOAP/XML con sus perfiles de dispositivo y de QoS a la dirección IP del encaminador del servidor del PS.	Continuar en CHBPLT-6.	Si el BP no recibe BP_Init_Response, reintentará BP_Init hasta en tres ocasiones como máximo.
CHBPLT-6	Mensaje BP_Init_Response El PS envía un mensaje a BP_Init_Response SOAP/XML al BP.	Configuración completada.	
NOTA 1 – Si el cliente tiene conocimiento de su dirección IP anterior (por ejemplo, tras un rearranque), puede omitir el mensaje DISCOVER DHCP y continuar en la fase 3. NOTA 2 – Si el cliente está ubicado en una red que no admite difusión se prevé que enviará el mensaje mediante unidifusión al servidor DHCP. NOTA 3 – Si el cliente está ubicado en una red que no admite difusión se prevé que enviará el mensaje al PS mediante unidifusión.			

13.7 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 introduce el modo de tratamiento de paquetes primario (cabhCapPrimaryMode) de transferencia, o escribiendo direcciones MAC particulares del dispositivo IP de LAN en el cuadro de transferencia (cabhCapPassthroughTable). En la figura 13-8 se describe el proceso para la petición y asignación de una dirección de red a los dispositivos IP de LAN para los cuales el PS se preconfiguró a modo de puentear el tráfico. Cuando el PS se ha configurado para este propósito, los mensajes DISCOVER DHCP y REQUEST DHCP 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 Recomendación, debe implementar un cliente DHCP y solicitar una licencia de dirección IP mediante DHCP. El elemento lógico del BP de un dispositivo IP de LAN conforme a IPCable2Home también debe intercambiar mensajes BP_Init con el PS, como se describe en 6.5.3.2, "Función de los mensajes de LAN de MBP". En esta cláusula se describen los mensajes necesarios para el BP. Los mensajes de DHCP que se supone que tienen lugar entre un dispositivo IP de LAN no conforme y un servidor DHCP por lo general seguirán las primeras cuatro fases de los mensajes DHCP del BP necesarios. No obstante, es posible que un dispositivo IP de LAN no conforme no incluya la cadena "CableHome 1.1 BP <*hardware address*>" de la opción 61 de DHCP.

El proceso de configuración de un dispositivo IP de LAN en el sector LAN-Pass debe tener lugar mediante la secuencia ilustrada en la figura 13-8 y descrita con detalle en el cuadro 13-6.

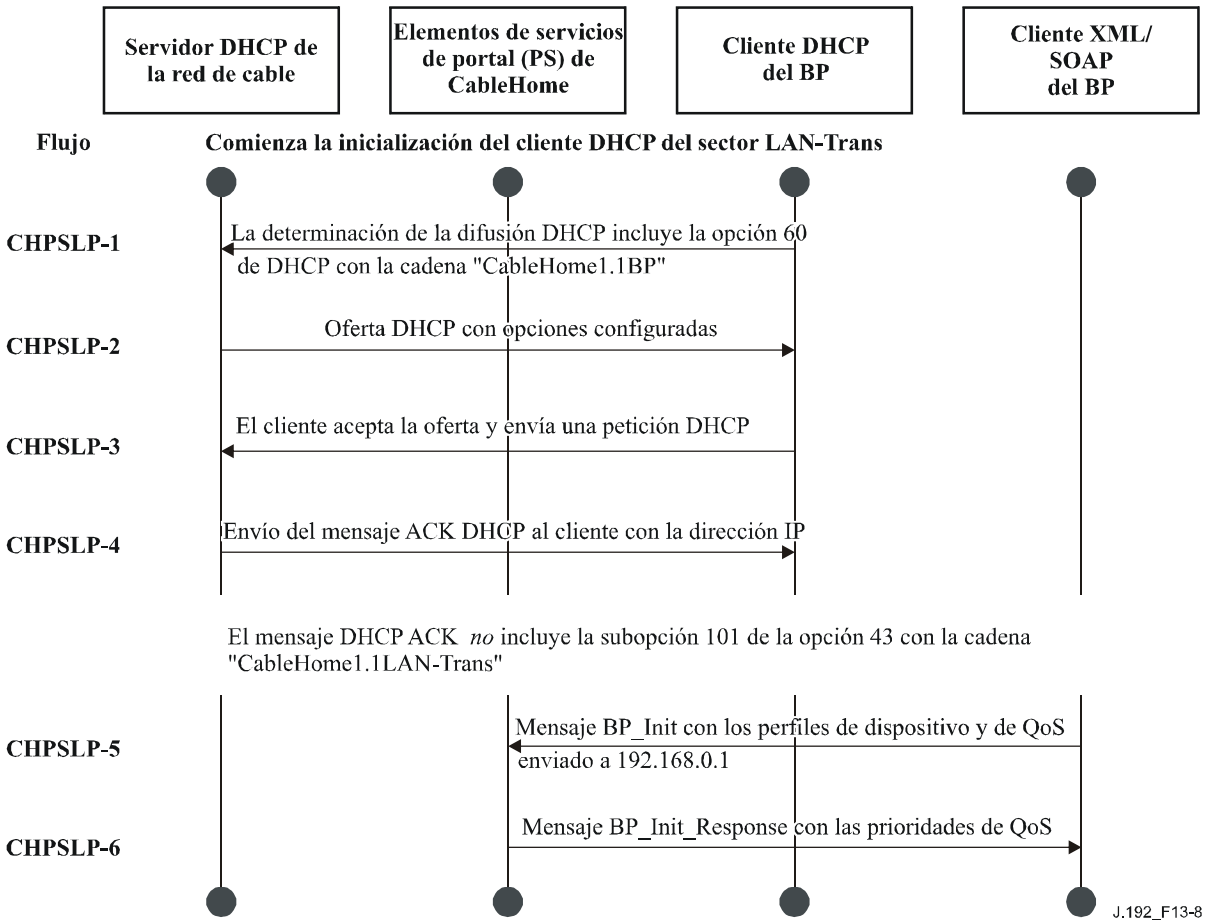


Figura 13-8/J.192 – Proceso de configuración de un dispositivo IP de LAN en el sector LAN-Pass

Cuadro 13-6/J.192 – Descripciones de los flujos durante el proceso de configuración de un dispositivo IP de LAN en el sector LAN-Pass

Fase del flujo	Configuración de la dirección de LAN-Pass del cliente	Secuencia normal	Secuencia en caso de fallo
CHPSLP-1	Determinación de la difusión de DHCP El BP o el dispositivo de IP de LAN no conforme a IPCable2Home difunde un mensaje DISCOVER DHCP por su red LAN local (nota). El PS recibe dicho paquete de difusión por su interfaz LAN y debe puentearlo de modo transparente a la interfaz WAN sin modificar su contenido. Véase 8.3.4, "Requisitos del CAP".	Continuar en CHPSLP-2.	Si falla por causa del protocolo DHCP repetir CHPSLP-1.
CHPSLP-2	OFFER DHCP El servidor DHCP en la red del operador del cable recibe el paquete DISCOVER DHCP y asigna una dirección IP direccionable externamente y otras opciones, construye un paquete OFFER DHCP y lo transmite al dispositivo IP de LAN. El PS debe puentear de modo transparente el paquete DHCP OFFER entre su interfaz WAN y su interfaz LAN sin modificar el contenido del paquete IP. Véase 8.3.4, "Requisitos del CAP".	Continuar en CHPSLP-3.	Si falla, el dispositivo IP de LAN alcanzará su límite temporal conforme al protocolo DHCP y se repetirá CHPSLP-1.
CHPSLP-3	Mensaje REQUEST DHCP El dispositivo IP de LAN recibe el paquete OFFER DHCP y emite un mensaje REQUEST DHCP. El PS debe puentear de modo transparente el mensaje REQUEST DHCP entre su interfaz LAN y su interfaz WAN sin modificar el contenido del paquete IP. Véase 8.3.4, "Requisitos del CAP".	Continuar en CHPSLP-4.	Si falla por causa del protocolo DHCP repetir CHPSLP-1.

Cuadro 13-6/J.192 – Descripciones de los flujos durante el proceso de configuración de un dispositivo IP de LAN en el sector LAN-Pass

Fase del flujo	Configuración de la dirección de LAN-Pass del cliente	Secuencia normal	Secuencia en caso de fallo
CHPSLP-4	ACK DHCP El servidor DHCP en la red del operador del cable recibe el mensaje REQUEST DHCP y envía el mensaje ACK DHCP al dispositivo IP de LAN con la dirección IPv4 del dispositivo IP de LAN. El PS debe puentear de modo transparente el mensaje ACK DHCP entre su interfaz WAN y su interfaz LAN sin modificar el contenido del paquete IP. Véase 8.3.4, "Requisitos del CAP". Se prevé que el mensaje ACK DHCP no incluirá la subopción 101 de la opción 43 de DHCP con la cadena "CableHome 1.1 LAN-Trans". Esto indica al BP que se encuentra en el sector de direcciones de LAN-Pass y que no recibió la dirección del encaminador del servidor del PS en la opción 3 de DHCP, de manera que debe enviar sus mensajes BP_Init a la dirección IP "bien conocida" del PS 192.168.0.1. Véase 6.5.3.2, "Función de los mensajes de LAN del MBP".	Continuar en CHPSLP-5.	Si falla, el dispositivo IP de LAN alcanzará su límite temporal conforme al protocolo DHCP y repetirá CHPSLP-1.
CHPSLP-5	Mensaje BP_Init El BP envía un mensaje SOAP/XML BP_Init con sus perfiles del dispositivo y de QoS al PS.	Continuar en CHPSLP-6.	Si el BP no recibe BP_Init_Response, reintentará BP_Init hasta en tres ocasiones como máximo.
CHPSLP-6	Mensaje BP_Init_Response El PS envía un mensaje SOAP/XML BP_Init_Response al BP.	Configuración completada.	
NOTA – Si el cliente está ubicado en una red que no admite difusión debe transmitir el mensaje mediante unidifusión al servidor DHCP o al agente de enlace DHCP [RFC 3046] en la red de cable.			

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", y señala el requisito de la persistencia de cada uno de los objetos relacionados.

A continuación se define el término 'persistente' como se aplica en este anexo:

Persistente: La necesidad 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 reactivación 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 reactivación del PS, DEBE ser el mismo que su valor justo antes del rearranque o reactivación.

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 a cero o a ninguno según proceda, inmediatamente a continuación de un rearranque o reactivación del PS.

En los casos de los 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 reactivación del PS se deja a la implementación del 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 reactivación del PS.)

NOMBRE/parámetro de la MIB	Acceso máximo	Persistencia	N.º de anotaciones persistentes
mib-2[RFC 1213] sistema			
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
ifPhysAddress	sólo lectura	–	N/A
ifAdminStatus	lectura-escritura	No	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
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	lectura-creación	No	N/A
ipNetToMediaPhyAddress	lectura-creación	No	N/A
ipNetToMediaNetAddress	lectura-creación	No	N/A
ipNetToMediaType	lectura-creación	No	N/A

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

transmisión [draft-ietf-ipcdn-bpiplus-mib-05] **docsIfMib** **docsBpi2MIB** **docsBpi2MIBObjects** **docsBpi2CmObjects** **docsBpi2CmCertObjects**			
docsBpi2CmDeviceCertTable/docsBpi2CmDeviceCertEntry			
docsBpi2CmDeviceCmCert	sólo lectura	–	N/A
docsBpi2CmDeviceManufCert	sólo lectura	–	N/A
docsBpi2CodeDownloadGroup			
docsBpi2CodeDownloadStatusCode	sólo lectura	–	N/A
docsBpi2CodeDownloadStatusString	sólo lectura	–	N/A
docsBpi2CodeMfgOrgName	sólo lectura	–	N/A
docsBpi2CodeMfgCodeAccessStart	sólo lectura	–	N/A
docsBpi2CodeMfgCvcAccessStart	sólo lectura	–	N/A
docsBpi2CodeCoSignerOrgName	sólo lectura	–	N/A
docsBpi2CodeCoSignerCodeAccessStart	sólo lectura	–	N/A
docsBpi2CodeCoSignerCvcAccessStart	sólo lectura	–	N/A
docsBpi2CodeCvcUpdate	lectura-escritura	Sí	1
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] **ifMIBObjects**			
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

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
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	20
docsDevFilterIpControl	lectura-creación	Sí	20
docsDevFilterIpIfIndex	lectura-creación	Sí	20
docsDevFilterIpDirection	lectura-creación	No	N/A
docsDevFilterIpBroadcast	lectura-creación	No	N/A
docsDevFilterIpSaddr	lectura-creación	Sí	20
docsDevFilterIpSmask	lectura-creación	Sí	20
docsDevFilterIpDaddr	lectura-creación	Sí	20
docsDevFilterIpDmask	lectura-creación	Sí	20
docsDevFilterIpProtocol	lectura-creación	Sí	20
docsDevFilterIpSourcePortLow	lectura-creación	Sí	20
docsDevFilterIpSourcePortHigh	lectura-creación	Sí	20
docsDevFilterIpDestPortLow	lectura-creación	Sí	20
docsDevFilterIpDestPortHigh	lectura-creación	Sí	20
docsDevFilterIpMatches	sólo lectura	–	N/A
docsDevFilterIpTos	lectura-creación	No	N/A
docsDevFilterIpTosMask	lectura-creación	No	N/A
docsDevFilterIpContinue	lectura-creación	No	N/A
docsDevFilterIpPolicyId	lectura-creación	Sí	20
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
cabhlsDevProvConfFileSize	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

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
cabhPsDevAttrib cabhPsDevBpAttrib			
cabhPsDevBpProfileTable/cabhPsDevBpProfileEntry			
cabhPsDevBpIndex	inaccesible	–	N/A
cabhPsDevBpDeviceType	sólo lectura	–	N/A
cabhPsDevBpManufacturer	sólo lectura	–	N/A
cabhPsDevBpManufacturerURL	sólo lectura	–	N/A
cabhPsDevBpSerialNumber	sólo lectura	–	N/A
cabhPsDevBpHardwareVersion	sólo lectura	–	N/A
cabhPsDevBpHardwareOptions	sólo lectura	–	N/A
cabhPsDevBpModelName	sólo lectura	–	N/A
cabhPsDevBpModelNumber	sólo lectura	–	N/A
cabhPsDevBpModelURL	sólo lectura	–	N/A
cabhPsDevBpModelUPC	sólo lectura	–	N/A
cabhPsDevBpModelSoftwareOs	sólo lectura	–	N/A
cabhPsDevBpModelSoftwareVersion	sólo lectura	–	N/A
cabhPsDevBpLanInterface	sólo lectura	–	N/A
cabhPsDevBpNumberInterfacePriorities	sólo lectura	–	N/A
cabhPsDevBpPhysicalLocation	sólo lectura	–	N/A
cabhPsDevBpPhysicalAddress	sólo lectura	–	N/A

cabhPsDevPsStats			
cabhPsDevLanIpTrafficResetCounters	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
cabhPsDevLanIpTrafficIpOutOctets	sólo lectura	–	N/A
cabhSecMib **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	Sí	N/A
cabhSec2FwEventLastSetToFactory	sólo lectura	Sí	N/A
cabhSec2FwPolicySuccessfulFileURL	sólo lectura	Sí	1
cabhSec2FwEvent			
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
cabhSec2FwLogEntry			
cabhSec2FwLogIndex	inaccesible	–	N/A
cabhSec2FwLogEventType	sólo lectura	–	N/A
cabhSec2FwLogEventPriority	sólo lectura	–	N/A
cabhSec2FwLogEventId	sólo lectura	–	N/A
cabhSec2FwLogTime	sólo lectura	–	N/A
cabhSec2FwLogIpProtocol	sólo lectura	–	N/A
cabhSec2FwLogIpSourceAddr	sólo lectura	–	N/A

cabhSec2FwLogIpDestAddr	sólo lectura	–	N/A
cabhSec2FwLogIpSourcePort	sólo lectura	–	N/A
cabhSec2FwLogIpDestPort	sólo lectura	–	N/A
cabhSec2FwLogMessageType	sólo lectura	–	N/A
cabhSec2FwLogReplayCount	sólo lectura	–	N/A
cabhSec2FwLogMIBPointer	sólo lectura	–	N/A
cabhSec2FwFilter **cabhSec2FwFilterScheduleTable** **cabhSec2FwFilterScheduleEntry**			
cabhSec2FwFilterScheduleIndex	inaccesible	–	N/A
cabhSec2FwFilterScheduleRowStatus	lectura-creación	Sí	1
cabhSec2FwFilterScheduleStartTime	lectura-creación	Sí	1
cabhSec2FwFilterScheduleEndTime	lectura-creación	Sí	1
cabhSec2FwFilterScheduleDOW	lectura-creación	Sí	1
cabhSecCertObjects			
cabhSecCertPsCert	sólo lectura	–	1
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
cabhCapMap			
cabhCapMappingTable/cabhCapMappingEntry			
cabhCapMappingIndex	inaccesible	–	N/A
cabhCapMappingWanAddrType	lectura-creación	Sí[2]	16
cabhCapMappingWanAddr	lectura-creación	Sí[2]	16
cabhCapMappingWanPort	lectura-creación	Sí[2]	16
cabhCapMappingLanAddrType	lectura-creación	Sí[2]	16

[2] Los objetos cabhCapMappingEntry son persistentes si son suministrados por el NMS y no persistentes si se crean dinámicamente basándose en el tráfico saliente. Véase 8.3.4.4.

cabhCapMappingLanAddr	lectura-creación	Sí[2]	16
cabhCapMappingLanPort	lectura-creación	Sí[2]	16
cabhCapMappingMethod	sólo lectura	–	N/A
cabhCapMappingProtocol	lectura-creación	Sí[2]	16
cabhCapMappingRowStatus	lectura-creación	Sí	16
cabhCapPassthroughTable/cabhCapPassthroughEntry			
cabhCapPassthroughIndex	inaccesible	–	N/A
cabhCapPassthroughMACAddr	lectura-creación	Sí	16
cabhCapPassthroughRowStatus	lectura-creación	Sí	16

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

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
cabhCdpWanDataAddrRenewalTime	sólo lectura	–	N/A
cabhCdpWanDataAddrRowStatus	lectura-creación	No	N/A
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
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	lectura-escritura	Sí	1
cabhCdpServerDhcpAddress	lectura-escritura	Sí	1
cabhCtpMib **cabhCtpObjects** **cabhCtpBase**			
cabhCtpSetToFactory	lectura-escritura	No	N/A
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
cabhCtpPingMinRTT	sólo lectura	–	N/A
cabhCtpPingMaxRTT	sólo lectura	–	N/A
cabhCtpPingNumIcmpError	sólo lectura	–	N/A
cabhCtpPingIcmpError	sólo lectura	–	N/A
cabhQosMib **cabhPriorityQosMibObjects** **cabhPriorityQosBase**			
cabhPriorityQosSetToFactory	lectura-escritura	No	N/A
cabhPriorityQosLastReset	sólo lectura	No	N/A
cabhPriorityQosMasterTable/cabhPriorityQosMasterEntry			
cabhPriorityQosMasterApplicationId	inaccesible	–	N/A
cabhPriorityQosMasterDefaultCHPriority	lectura-creación	Sí	16
cabhPriorityQosMasterRowStatus	lectura-creación	Sí	16
cabhPriorityQosBp			
cabhPriorityQosBpTable/cabhPriorityQosBpEntry			
cabhPriorityQosBpIndex	inaccesible	–	N/A
cabhPriorityQosBpIpAddrType	sólo lectura	–	N/A
cabhPriorityQosBpIpAddr	sólo lectura	–	N/A
cabhPriorityQosBpApplicationId	sólo lectura	–	N/A
cabhPriorityQosBpDefaultCHPriority	sólo lectura	–	N/A
cabhPriorityQosBpDestTable/cabhPriorityQosBpDestEntry			
cabhPriorityQosBpDestIndex	inaccesible	–	N/A
cabhPriorityQosBpDestIpAddrType	sólo lectura	–	N/A
cabhPriorityQosBpDestIpAddr	sólo lectura	–	N/A
cabhPriorityQosBpDestPort	sólo lectura	–	N/A
cabhPriorityQosBpDestIpPortPriority	sólo lectura	–	N/A
cabhPriorityQosPs			

cabhPriorityQosPsIfAttribTable/cabhPriority QosPsIfAttribEntry			
cabhPriorityQosPsIfAttribIfNumPriorities	sólo lectura	–	N/A
cabhPriorityQosPsIfAttribIfNumQueues	sólo lectura	–	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

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
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
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 2576] **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
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
clabMfgCVCCert	sólo lectura	–	N/A

Anexo B

Formato y contenido de los eventos, SYSLOG y trap SNMP

El cuadro B.1 resume el formato y el contenido de las anotaciones históricas de eventos, de los mensajes SYSLOG y SNMP trap.

Cada fila en el cuadro especifica los eventos que el PS puede generar. Estos eventos ha de comunicarlos el PS por cualquier medio de los tres 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 a continuación del cuadro.

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 campos de texto del evento contienen información variable. Algunas de las variables sólo son necesarias en el SYSLOG 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 para el 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 sección de eventos de actualización de software.

La primera y segunda columnas son "Actualización del SW" e "Inicialización de actualización de software". La prioridad del evento es "Notificación". El texto del evento es "INIT de descarga de 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 "INIT de descarga del software – Mediante NMS – dirección MAC: x1 x2 x3 x4 x5 x6".

La última columna "Trap name" es cabhPsDevSwUpgradeInitTrap, cuyo formato se proporciona al final del presente anexo.

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 errores	ID del evento	Nombre de la trampa
Errores DHCP antes de completar la configuración							
Inicialización	CDC	Crítica	Falló DHCP – Enviado Discover, no se recibe offer		D01.0	68000100	
Inicialización	CDC	Crítica	Falló DHCP – Enviado Request, no hay respuesta		D02.0	68000200	
Inicialización	CDC	Crítica	Falló DHCP – Información solicitada no soportada		D03.0	68000300	
Inicialización	CDC	Error	Falló DHCP – La respuesta no contiene TODOS los campos válidos O el PS no tiene la capacidad para determinar el modo de configuración		D03.1	68000301	
Inicialización	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	cabhPsDevCdp WanDataIpTrap
Errores de ToD antes de completar la configuración							
Inicialización	ToD	Alarma	Enviada petición ToD – No se recibe respuesta		D04.1	68000401	cabhPsDevInitTrap
Inicialización	ToD	Alarma	Recibida respuesta ToD – Formato de datos no válido		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 errores	ID del evento	Nombre de la trampa
Errores TFTP antes de completar la configuración							
Inicialización	TFTP	Error	Falló TFTP – Enviada petición – No hay respuesta		D05.0	68000500	cabhPsDevInitTrap (La trampa es importante sólo para el modo de configuración SNMP.)
Inicialización	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	cabhPsDevInit Trap (La trampa es importante sólo para el modo de configuración SNMP.)
Inicialización	TFTP	Error	Falló TFTP – Paquetes DESORDENADOS		D07.0	68000700	cabhPsDevInit Trap (La trampa es importante sólo para el modo de configuración SNMP.)
Inicialización	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.)
Inicialización	TFTP	Error	Falló TFTP – Sobrepasado el máximo número de reintentos	Únicamente para SYSLOG: añadir: límite de reintentos = <P1> P1 = número máximo de reintentos	D09.0	68000900	cabhPsDevInitTrap (La trampa es importante sólo para el modo de configuración SNMP.)
TFTP conseguido							
Inicialización	TFTP	Notificación	TFTP conseguido		D10.0	68001000	

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 errores	ID del evento	Nombre de la trampa
TLS							
Inicialización	TCP/IP	Crítica	Fallo del PS al tratar de conectarse al servidor HTTP/TLS		D20.0	68002000	
Inicialización	TLS	Crítica	Expira el temporizador de la conexión TLS y se excede el número máximo de reintentos		D21.0	68002100	
Inicialización	TLS	Crítica	Error grave del TLS <P1>	P1 = Código de Error conforme a [RFC 2246]	D22.0	68002200	
HTTP							
Inicialización	HTTP	Crítica	Fallo de la descarga del fichero de configuración, pero se efectúan reintentos. Error de HTTP. <P1>	P1 = Códigos de estado conformes a [RFC 2616]	D30.0	68003000	
Inicialización	HTTP	Crítica	Fallo de la descarga del fichero de configuración. Debido a la expiración del temporizador de la conexión y al número máximo de reintentos. Se abortó la operación.		D31.0	68003100	
Inicialización	HTTP	Crítica	Se completó con éxito la descarga segura del fichero de configuración		D32.0	68003200	

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 errores	ID del evento	Nombre de la trampa
Análisis sintáctico TLV							
Inicialización	TLV Parsing	Alarma	TLV-28 – OID no reconocido		I401.0	73040100	cabhPsDev InitTLVUnknownTrap
Inicialización	TLV Parsing	Alarma	TLV desconocida <P1>	Únicamente para SYSLOG: <P1> = el TLV completo en hexadecimal	I401.1	73040101	cabhPsDev InitTLVUnknownTrap
Inicialización	TLV Parsing	Error	Formato o contenido TLV no válido <P1>	Únicamente para SYSLOG: <P1> = el TLV completo en hexadecimal	I401.2	73040102	
Configuración							
Inicialización	Configuración completa	Notificación	Conclusión de configuración	Únicamente para SYSLOG, añadir dirección MAC: <P1>. P1 = dirección MAC del PS	I11.0	73001100	cabhPsDev InitRetryTrap
Inicialización de actualización del SW*							
Actualización del SW	Inicialización de actualización del SW	Notificación	Inicialización de descarga de 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	cabhPsDev SwUpgradeInitTrap

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 errores	ID del evento	Nombre de la trampa
Actualización del SW	Inicialización de actualización del SW	Notificación	Inicialización de descarga de software – Mediante fichero de configuración <P1>	P1 = nombre del fichero de configuración 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
Fallo general* de la actualización del SW							
Actualización del SW	Fallo general de la actualización 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	cabhPsDev SwUpgrade FailTrap
Actualización del SW	Fallo general de la actualización 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	cabhPsDev SwUpgrade 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 errores	ID del evento	Nombre de la trampa
Actualización del SW	Fallo general de la actualización 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	cabhPsDev SwUpgrade FailTrap
Actualización del SW	Fallo general de la actualización 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	cabhPsDev SwUpgrade FailTrap
Actualización del SW	Fallo general de la actualización 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	cabhPsDev SwUpgrade FailTrap
Actualización del SW	Fallo general de la actualización 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	cabhPsDev SwUpgrade 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 errores	ID del evento	Nombre de la trampa
Actualización del SW	Fallo general de la actualización 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	cabhPsDev SwUpgrade FailTrap
Éxito de la actualización del SW*							
Actualización del SW	Éxito de la actualización 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	cabhPsDev SwUpgrade SuccessTrap
Actualización del SW	Éxito de la actualización 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	cabhPsDev SwUpgrade SuccessTrap
Fallo del DHCP tras completarse la configuración							
DHCP	CDC	Error	Enviado DHCP RENEW – Sin respuesta		D101.0	68010100	cabhPsDev DHCPFail Trap
DHCP	CDC	Error	Enviado DHCP REBIND – Sin respuesta		D102.0	68010200	cabhPsDev DHCPFail 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 errores	ID del evento	Nombre de la trampa
DHCP	CDC	Error	Enviado DHCP RENEW – Opción DHCP no válida		D103.0	68010300	cabhPsDev DHCPFail Trap
DHCP	CDC	Error	Enviado DHCP REBIND – Opción DHCP no válida		D104.0	68010400	cabhPsDev DHCPFail Trap
Fallo de ToD tras completarse la configuración							
ToD	ToD	Alarma	Petición ToD enviada – No se recibe respuesta		D04.3	68000403	cabhPsDev TODFail Trap
ToD	ToD	Alarma	Respuesta ToD recibida – Formato de datos no válido		D04.4	68000404	cabhPsDev TODFail Trap
Verificación del fichero de código							
Actualización del SW	Fallo general de la actualización 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	cabhPsDev SwUpgrade FailTrap
Actualización del SW	Fallo general de la actualización 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	cabhPsDev SwUpgrade 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 errores	ID del evento	Nombre de la trampa
Actualización del SW	Fallo general de la actualización 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	cabhPsDev SwUpgrade FailTrap
Actualización del SW	Fallo general de la actualización 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	cabhPsDev SwUpgrade FailTrap
Actualización del SW	Fallo general de la actualización 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	cabhPsDev SwUpgrade 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 errores	ID del evento	Nombre de la trampa
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	cabhPsDev SwUpgrade 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	cabhPsDev SwUpgrade CVCFailTrap
Actualización del SW	Verificación del CVC	Error	Formato SNMP CVC inadecuado – Gestor SNMP: <P1>	P1 = dirección IP del gestor SNMP	E208.0	69020800	cabhPsDev SwUpgrade CVCFailTrap
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	cabhPsDev SwUpgrade CVCFailTrap
Eventos del CDP							
CDP	CDS	Notificación	Intento de asignar más direcciones IP LAN-Trans de las permitidas		P01.0	80000100	cabhPsDev CDPThreshold Trap
CDP	CDS	Notificación	No pudo suministrar el cliente de LAN DHCP – Se agotó el conjunto de direcciones IP		P03.0	80000300	cabhPsDev CdpLanIpPoolTrap

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 errores	ID del evento	Nombre de la trampa
Eventos del CSP							
CSP	Barrera contrafuego	Notificación	Barrera contrafuego tipo 1 habilitada Valor de la MIB <P1>	P1 = valor de cabhSecFwEvent Type1 habilitado	P101.1	80010101	cabhPsDevCSPTrap
CSP	Barrera contrafuego	Notificación	Barrera contrafuego tipo 2 habilitada Valor de la MIB <P1>	P1 = valor de cabhSecFwEventType2 habilitado	P101.2	80010102	cabhPsDevCSPTrap
CSP	Barrera contrafuego	Notificación	Barrera contrafuego tipo 3 habilitada Valor de la MIB <P1>	P1 = valor de cabhSecFwEventType3 habilitado	P101.3	80010103	cabhPsDevCSPTrap
CSP	Barrera contrafuego	Notificación	Barrera contrafuego tipo 4 habilitada Valor de la MIB <P1>	P1 = valor de cabhSecFwEventType4 habilitado	P101.4	80010104	cabhPsDevCSPTrap
CSP	Barrera contrafuego	Notificación	Barrera contrafuego tipo 5 habilitada Valor de la MIB <P1>	P1 = valor de cabhSecFwEventType5 habilitado	P101.5	80010105	cabhPsDevCSPTrap
CSP	Barrera contrafuego	Notificación	Barrera contrafuego tipo 6 habilitada Valor de la MIB <P1>	P1 = valor de cabhSecFwEventType6 habilitado	P101.6	80010106	cabhPsDevCSPTrap
CSP	Barrera contrafuego	Alarma	Se rebasó el umbral de los eventos de la barrera contrafuego tipo 1		P102.1	80010201	cabhPsDevCSPTrap
CSP	Barrera contrafuego	Alarma	Se rebasó el umbral de los eventos de la barrera contrafuego tipo 2		P102.2	80010202	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 errores	ID del evento	Nombre de la trampa
CSP	Barrera contrafuego	Alarma	Se rebasó el umbral de los eventos de la barrera contrafuego tipo 3		P102.3	80010203	cabhPsDevCSPTrap
CSP	Barrera contrafuego	Alarma	Se rebasó el umbral de los eventos de la barrera contrafuego tipo 4		P102.4	80010204	cabhPsDevCSPTrap
CSP	Barrera contrafuego	Alarma	Se rebasó el umbral de los eventos de la barrera contrafuego tipo 5		P102.5	80010205	cabhPsDevCSPTrap
CSP	Barrera contrafuego	Alarma	Se rebasó el umbral de los eventos de la barrera contrafuego tipo 6		P102.6	80010206	cabhPsDevCSPTrap
CSP	TFTP de la barrera contrafuego	Crítica	Fracasó la descarga TFTP del fichero de políticas de la barrera contrafuego: Se envió la petición y no se recibió respuesta	P1 = se solicitó el URL del fichero de políticas de la barrera contrafuego	P130.0	80013000	cabhPsDevCSPTrap
CSP	TFTP de la barrera contrafuego	Crítica	Fracaso de TFTP – No se encontró el fichero de políticas de barrera contrafuego	P1 = se solicitó el URL del fichero de políticas de la barrera contrafuego	P131.0	80013100	cabhPsDevCSPTrap
CSP	TFTP de la barrera contrafuego	Crítica	Fracaso de TFTP – Fichero de políticas de la barrera contrafuego no válido	P1 = se solicitó el URL de políticas de la barrera contrafuego	P132.0	80013200	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 errores	ID del evento	Nombre de la trampa
CSP	TFTP de la barrera contrafuego	Crítica	Se completó la descarga del fichero de políticas de barrera contrafuego pero fracasó la verificación de la generación SHA-1	P1 = se solicitó el URL del fichero de políticas de la barrera contrafuego, P2 = valor del fichero de políticas de la barrera contrafuego	P133.0	80013300	cabhPsDevCSPTrap
CSP	TFTP de la barrera contrafuego	Crítica	La descarga del fichero de políticas de la barrera contrafuego excedió el número máximo permitido de reintentos de TFTP	P1 = se solicitó el URL del fichero de políticas de la barrera contrafuego	P134.0	80013400	cabhPsDevCSPTrap
CSP	TFTP de la barrera contrafuego	Notificación	La descarga TFTP del fichero de políticas de la barrera contrafuego se completó con éxito	P1 = se solicitó el URL del fichero de políticas de la barrera contrafuego Únicamente para SYSLOG: añadir: Límite 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

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 errores	ID del evento	Nombre de la trampa
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
CTP	Herramienta de la velocidad de la conexión	Notificación	La prueba de la herramienta de velocidad de la conexión se completó satisfactoriamente	P1 = dirección IP del origen P2 = dirección IP del destino P3 = protocolo P4 = caudal	P301.0	80030100	cabhPsDevCtpTrap
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	P1 = dirección IP del origen P2 = dirección IP del destino P3 = protocolo P4 = valor del temporizador (ms)	P302.0	80030200	cabhPsDevCtpTrap
CTP	Herramienta de velocidad de la conexión	Notificación	Se abortó la prueba de la herramienta de velocidad de la conexión	P1 = dirección IP del origen P2 = dirección IP del destino P3 = protocolo P4 = valor del temporizador (ms)	P303.0	80030300	cabhPsDevCtpTrap
CTP	Herramienta Ping	Notificación	Se completó satisfactoriamente la prueba de la herramienta Ping	P1 = dirección IP del origen P2 = dirección IP del destino P3 = tiempo promedio de ida y vuelta	P320.0	80032000	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 errores	ID del evento	Nombre de la trampa
CTP	Herramienta Ping	Notificación	La prueba de la herramienta Ping alcanzó el fin de temporización	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	P1 = dirección IP del origen P2 = dirección IP del destino P3 = número de peticiones enviadas P4 = número de respuestas recibidas	P322.0	80032200	cabhPsDevCtpTrap
NOTA – Los eventos de actualización del software (descarga segura de software) se aplican únicamente a los servicios de portal 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. Si se requiere mayor información véase 11.8, "Descarga de software en elementos PS integrados o autónomos".							

B.1 Descripción de las trampas

Todas las trampas se describen en la especificación de la MIB DEV del PS, (véase E.4).

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 tecnología 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:

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 (tal como un negocio) tenga acceso a los servicios del cable que no ha pagado. Los dispositivos pueden "clonarse" o modificarse para que parezcan dispositivos calificados 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 HFC y de las redes domésticas.

La reproducción no autorizada supone que un abonado o tercero (tal como 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.

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.

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 los 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:

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.

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.

Criptación de datos: La criptación de datos evita la divulgación o acceso no autorizado a los datos.

La encriptación 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.

Barrera contrafuego: Las aplicaciones de barrera contrafuego 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 contrafuego se suelen ubicar en los dispositivos domésticos de pasarela que conectan la red HFC a la red doméstica.

Una aplicación barrera contrafuego contribuye a evitar los ataques DoS y los de confidencialidad procedentes del lado de red de área extensa (WAN) de la barrera contrafuego, aunque no evita el tipo de ataques procedente del lado de la red doméstica de la barrera contrafuego. Tampoco protege del robo del servicio.

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 contrafuego

Durante la operación normal de la funcionalidad de la traducción de la dirección y la barrera contrafuego, es posible que varios de los protocolos y las aplicaciones tengan impedimentos para funcionar como se tenía previsto. Las barreras contrafuego podrán filtrar deliberadamente ciertas aplicaciones y protocolos con fines de seguridad. La política de la barrera contrafuego 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 contrafuego 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 la norma [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 apeguen en la medida posible a dichas directrices.

Se sabe que la utilización de la funcionalidad de NAT y la barrera contrafuego afecta 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 contrafuego de modo que puentee los sectores. En muchos casos, la CAT y la barrera contrafuego no puede proporcionar la transparencia deseada de la aplicación y el protocolo sin la ayuda de una pasarela de nivel de aplicación (ALG). 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 contrafuego 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 mediante la política únicamente y se etiqueta como "aplicaciones que necesitan exclusivamente la política de la barrera contrafuego"; 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 contrafuego y una ALG".

De acuerdo con la política establecida en la cláusula 11, los cuadros incluyen información para que el lector pueda 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 contrafuego 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 permitir IPCablecom a través de la barrera contrafuego. Los valores de la barrera contrafuego que permiten 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 contrafuego. 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 contrafuego 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 caso;
- relación "uno a uno" para múltiples casos (es posible identificar el número de casos necesarios);
- relación "uno a varios" para un solo caso;
- relación "uno a varios" para múltiples casos (es posible identificar el número de casos necesarios);
- relación "varios a uno" para un solo caso;
- relación "varios a uno" para múltiples casos (si es necesario se identificará el número de casos 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.

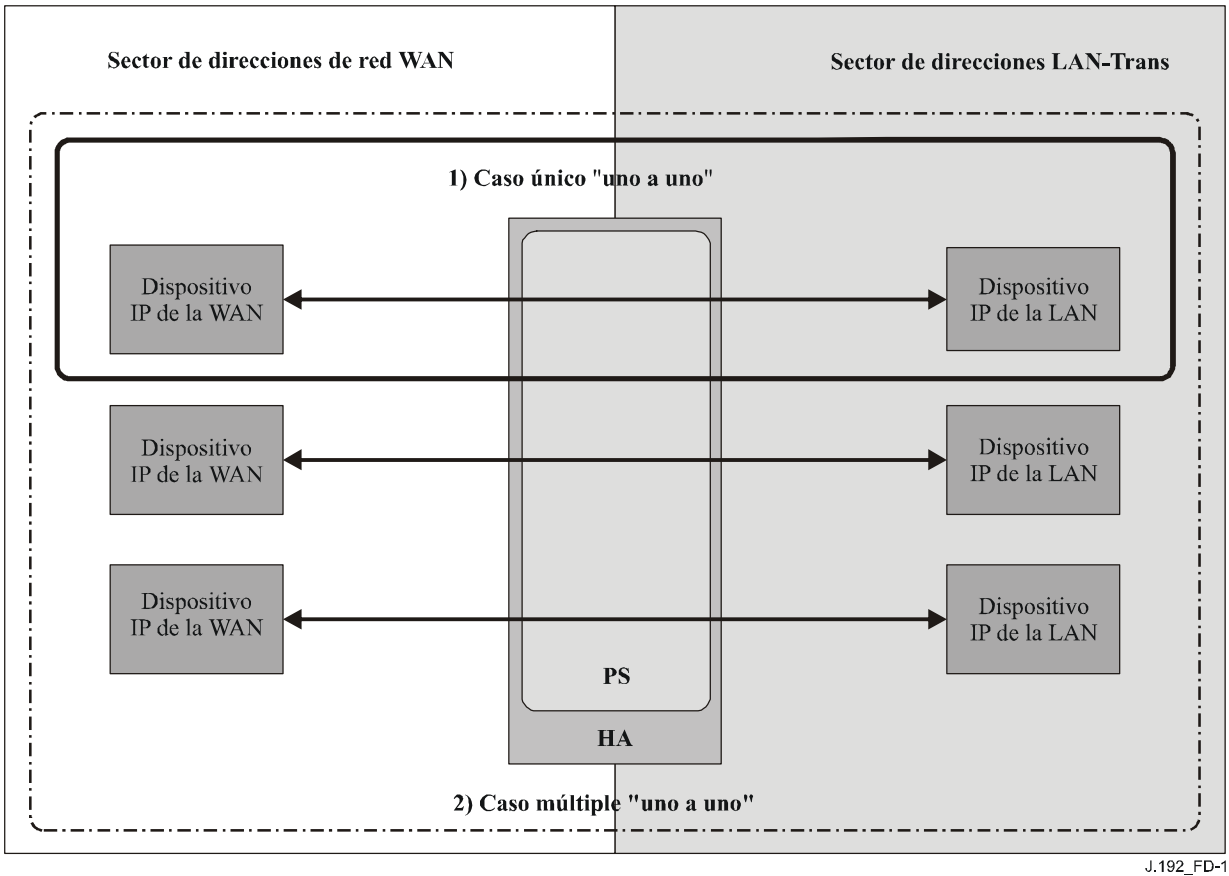


Figura D.1/J.192 – Casos de "uno a uno"

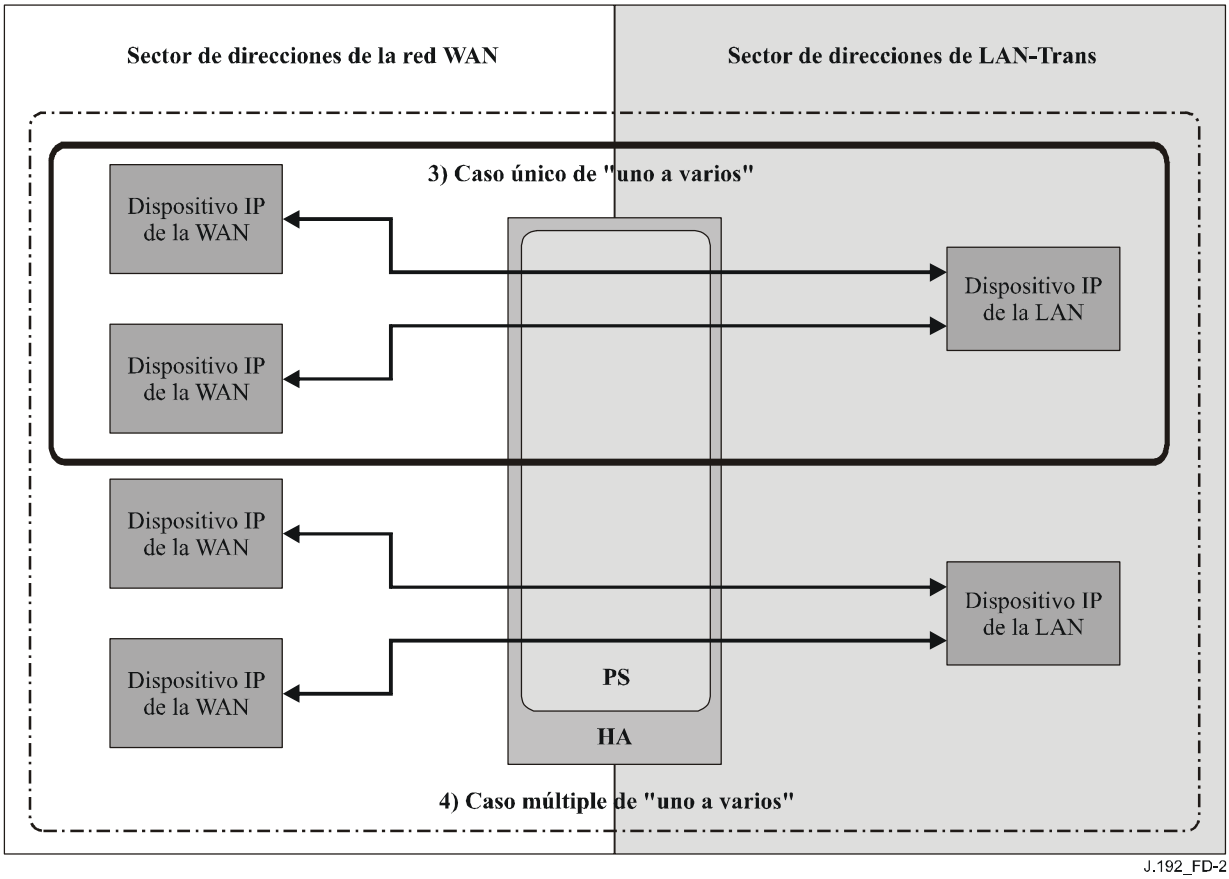


Figura D.2/J.192 – Casos de "uno a varios"

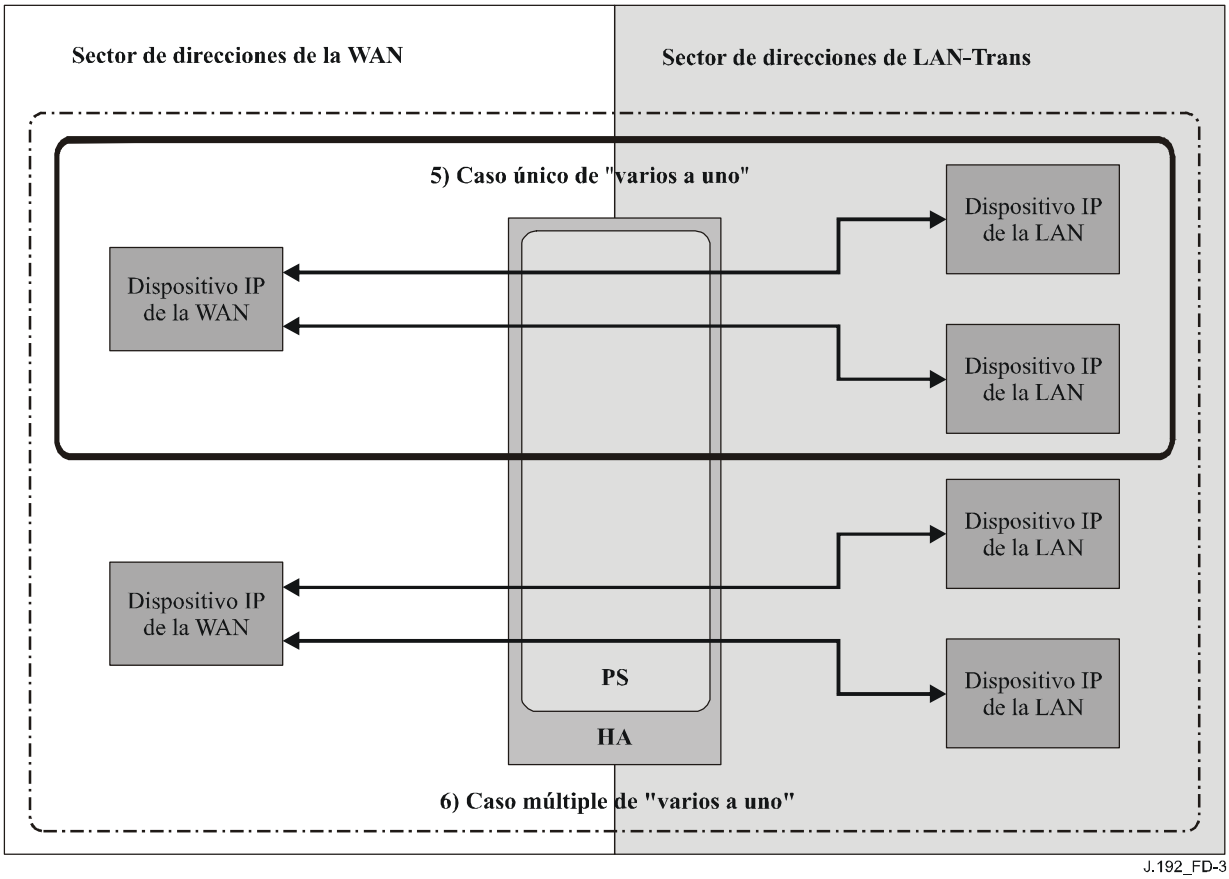


Figura D.3/J.192 – Casos de "varios a uno"

D.2 Aplicaciones que necesitan sólo la política de la barrera contrafuego

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 contrafuego. Esto no impide el soporte de aplicaciones y protocolos adicionales. Una CAT/barrera contrafuego 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 contrafuego. La barrera contrafuego NO DEBE iniciar operaciones antes de que el PS envíe el mensaje de conclusión de la configuración, por 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 contrafuego DEBEN soportarse en los seis casos 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 contrafuego del CH

Aplicación/Protocolo	Puertos	Comentarios
AOL IM	TCP/5190, 5191, 5192, 5193 & 13784	Valor por defecto en la red Internet
CU-SeeMe	TCP/7648, 7649; UDP/7648, 7649, 24032	
DHCP		Valor por defecto en la red Internet
DNS	UDP/53	IPCablecom e IPCable2Home
FTPS	989 & 990	
HTTP	TCP/80	Valor por defecto en la red Internet
HTTPS	TCP/443	Valor por defecto en la red 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 a 3332	Valor por defecto en la red Internet mcs-calypsoicf 3330 mcs-messaging 3331 mcs-mailsvr 3332

Cuadro D.1/J.192 – Protocolos necesarios para el funcionamiento a través de la CAT y de la barrera contrafuego del CH

Aplicación/Protocolo	Puertos	Comentarios
MGCP	2427, 2727	IPCablecom
Par a par (eDonkey)	TCP/4662 UDP/4665	eDonkey
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 la red 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 la red 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 la red 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 la red 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 la red Internet

NOTA – IANA canceló anteriormente la asignación de algunos números de puertos relacionados en esta cláusula, aunque 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 contrafuego y una ALG

En muchos casos la CAT y la barrera contrafuego no pueden proporcionar la transparencia deseada para la aplicación y el protocolo. Como la CAT modifica las direcciones del nodo de 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 en conjunto con la CAT y la política de la barrera contrafuego adecuada para proporcionar la transparencia al nivel deseado de la aplicación. La función de una ALG depende de la aplicación, y por consiguiente en el cuadro D.2 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 contrafuego 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 1024-65535 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 dos 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			

Cuadro D.2/J.192 – Aplicaciones que necesitan la política de la barrera contrafuego 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
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

MIB

E.1 Requisitos de la MIB del portal de direccionamiento de IPCable2Home (CAP)

Requisitos

The CableHome™ CAP MIB MUST be implemented as defined below.

```
CABH-CAP-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
    OBJECT-TYPE,
    Unsigned32          FROM SNMPv2-SMI
    TEXTUAL-CONVENTION,
    TruthValue,
    RowStatus,
    PhysAddress         FROM SNMPv2-TC
    OBJECT-GROUP,
    MODULE-COMPLIANCE   FROM SNMPv2-CONF
    InetAddressType,
    InetAddress,
    InetPortNumber      FROM INET-ADDRESS-MIB
    clabProjCableHome   FROM CLAB-DEF-MIB;

--============================================================================
--
--    History:
--
--    Date        Modified by       Reason
--    04/05/02                      Issued I01
--    09/20/02                      Issued I02
--    04/11/03                      Issued I03
--
--============================================================================

cabhCapMib MODULE-IDENTITY
    LAST-UPDATED    "200304110000Z"--April 11, 2003
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
                  400 Centennial Parkway
                  Louisville, Colorado 80027-1266
                              U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
    DESCRIPTION
           "This MIB module supplies the basic management objects
           for the CableHome Addressing Portal (CAP) portion of
           the PS database.


        Acknowledgements:
        Roy Spitzer           -     Consultant to CableLabs
        Mike Mannette         -     Consultant to Cable Labs
        Randy Dunton          -     Intel
```

```
        Dmitrii Loukianov     -     Intel
        Itay Sherman          -     Texas Instruments
        Chris Zacker          -     Broadcom
        Rick Vetter           -     Consultant to Cable Labs
        John Bevilacqua       -     YAS"
    ::=  { clabProjCableHome 3 }

-- Textual conventions

CabhCapPacketMode ::= TEXTUAL-CONVENTION
      STATUS      current
      DESCRIPTION
            "The data type established when
            a binding/mapping is established."
      SYNTAX      INTEGER {
            napt        (1),  -- NAT with port translation
            nat         (2),  -- Basic NAT
            passthrough (3)   -- Pass Through External Address
            }


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 [RFC793]."
    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."
      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."
      DEFVAL { 300 }  --  5 minutes
      ::= { cabhCapBase 3 }


cabhCapPrimaryMode OBJECT-TYPE
    SYNTAX      CabhCapPacketMode
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
    "The Primary Packet Handling Mode to be used."
    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."

     ::= { cabhCapBase 5 }

--========================================================================
--
--    cabhCapMappingTable (CAP Mapping Table)
--
--    The cabhCapMappingTable contains the info for all CAP mappings.
--
--========================================================================

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 sequence numbers,
assigned to devices on the subscriber's home LAN, and network
addresses, or network addresses and port numbers/ICMP sequence number,
assigned by the cable operator, 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."
    ::= {  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
      }

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 sequence number on the WAN
       side.  A port number of 0 indicates a NAT mapping.  A
       non-zero port number indicates an NAPT mapping."
        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 assigned by the DHCP server function of the
        PS (CableHome DHCP Server, CDS), and comprising the
        LAN-side IP address of the CAP Mapping tuple.
        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 sequence number on the LAN
    side. A port number/sequence number of 0 indicates a NAT mapping.
    A non-zero port number/sequence number indicates an NAPT mapping."
    DEFVAL { 0 }
    ::= { cabhCapMappingEntry 7 }

cabhCapMappingMethod OBJECT-TYPE
    SYNTAX      INTEGER {
            static   (1),
            dynamic  (2)
            }
    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."
    ::= { cabhCapMappingEntry 8 }

cabhCapMappingProtocol OBJECT-TYPE
    SYNTAX      INTEGER {
            other       (1),  -- any other protocol; e.g. IGMP
            icmp        (2),
            udp         (3),
            tcp         (4)
                        }
    MAX-ACCESS  read-create
    STATUS      current
    DESCRIPTION
       "The protocol for this mapping."
    ::= { 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
cabhCapMappingWanAddrType, cabhCapMappingWanAddr,
cabhCapMappingLanAddrType, cabhCapMappingLanAddr, and
cabhCapMappingProtocol have been set.  If Primary Packet-handling
Mode is NAPT (cabhCapPrimaryMode is napt(1)), a newly created row
cannot be set to active(1) until a non-zero value of
cabhCapMappingWanPort and cabhCapMappingLanPort have been set.
If 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 of
cabhCapMappingWanPort and cabhCapMappingLanPort have been set."
    ::={ cabhCapMappingEntry 10 }

--====================================================================
--
--    cabhCapPassthroughTable (CAP Passthrough Table)
--
--    The cabhCapPassthroughTable contains the MAC Addresses for all
--    LAN-IP Devices which will be configured as passthrough.
--
--====================================================================

cabhCapPassthroughTable OBJECT-TYPE
    SYNTAX      SEQUENCE OF CabhCapPassthroughEntry
    MAX-ACCESS  not-accessible
    STATUS      current
    DESCRIPTION
    "This table contains MAC addresses for LAN-IP Devices which are
    configured as passthrough mode."
    ::= {  cabhCapMap 2 }

cabhCapPassthroughEntry OBJECT-TYPE
    SYNTAX        CabhCapPassthroughEntry
    MAX-ACCESS    not-accessible
    STATUS        current
    DESCRIPTION
    "List of hardware addresses of LAN IP Devices which are configured
    for passthrough mode."
    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
    MAX-ACCESS    read-create
    STATUS        current
    DESCRIPTION
    "Hardware address of the LAN-IP Device to be configured as
    passthrough mode."
    ::={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
    MTA feature."
    MODULE   --cabhCapMib


-- unconditionally mandatory groups

MANDATORY-GROUPS {
    cabhCapGroup
    }

::= { cabhCapCompliances 1 }


cabhCapGroup OBJECT-GROUP
    OBJECTS {
            cabhCapTcpTimeWait,
            cabhCapUdpTimeWait,
            cabhCapIcmpTimeWait,
            cabhCapPrimaryMode,
            cabhCapSetToFactory,
            cabhCapMappingWanAddrType,
            cabhCapMappingWanAddr,
            cabhCapMappingWanPort,
            cabhCapMappingLanAddrType,
            cabhCapMappingLanAddr,
            cabhCapMappingLanPort,
            cabhCapMappingMethod,
            cabhCapMappingProtocol,
            cabhCapMappingRowStatus,
            cabhCapPassthroughMacAddr,
            cabhCapPassthroughRowStatus
            }
```

```
    STATUS    current
    DESCRIPTION
        "Group of objects for CableHome CAP MIB."
    ::= { cabhCapGroups 1 }

END
```

E.2 Requisitos de la MIB del portal DHCP de IPCable2Home (CDP)

Requisitos

The CableHome™ CDP MIB MUST be implemented as defined below.

```
CABH-CDP-MIB DEFINITIONS ::= BEGIN
IMPORTS
   MODULE-IDENTITY,
   OBJECT-TYPE,
   Integer32,
   Unsigned32                  FROM SNMPv2-SMI
   MacAddress,
   TruthValue,
   DateAndTime,
   RowStatus                   FROM SNMPv2-TC
   OBJECT-GROUP,
   MODULE-COMPLIANCE           FROM SNMPv2-CONF
   InetAddressType,
   InetAddress                 FROM INET-ADDRESS-MIB
   SnmpAdminString             FROM SNMP-FRAMEWORK-MIB
   clabProjCableHome           FROM CLAB-DEF-MIB;

   --================================================================
   --
   -- History:
   --
   --      Date         Modified by         Reason
   --      04/05/02                         Issued I01
   --      09/20/02                         Issued I02
   --      10/25/02                         IETF I-D revisions
   --      04/11/03                         Issued I03
   --
   --================================================================

   cabhCdpMib MODULE-IDENTITY
       LAST-UPDATED    "200304110000Z" -- April 11, 2003
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal:     Cable Television Laboratories, Inc.
                  400 Centennial Parkway
                  Louisville, Colorado 80027-1266
                  U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
    DESCRIPTION
      "This MIB module supplies the basic management objects
    for the CableHome DHCP Portal (CDP) portion of the PS database.


            Acknowledgements:
            Roy Spitzer             -     Consultant to CableLabs
            Mike Mannette           -     Consultant to CableLabs
            Randy Dunton            -     Intel
```

```
            Dmitrii Loukianov       -     Intel
            Itay Sherman            -     Texas Instruments
            Chris Zacker            -     Broadcom
            Rick Vetter             -     Consultant to CableLabs
            John Bevilacqua         -     YAS"
    ::=  { 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 Cable Home
--    DHCP Portal.  The rest of this group deals 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,
            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."
DEFVAL {0 }
::= { cabhCdpBase 5 }
--
--    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              MacAddress,
      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           MacAddress
       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 that the LAN-Trans lease was
           created (if it has not yet been renewed) or last renewed."
       ::= { cabhCdpLanAddrEntry 4 }

   cabhCdpLanAddrLeaseExpireTime OBJECT-TYPE
       SYNTAX      DateAndTime
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIPTION
          "This is the date and time that the LAN-trans lease expired
           or will expire."
       ::= { cabhCdpLanAddrEntry 5 }

   cabhCdpLanAddrMethod OBJECT-TYPE
       SYNTAX      INTEGER {
      reservationInactive (1),
      reservationActive (2),
      dynamicInactive (3),
      dynamicActive (4)
      }
      MAX-ACCESS  read-only
       STATUS     current
       DESCRIPTION
          "The IP allocation method indicated by this row.
           reservationInactive(1) indicates a reserved IP that has
           not yet been leased or that has an expired lease.
           reservationActive(2) indicates a reserved IP that has an
           active lease.  dynamicInactive(3) indicates an IP that was
           once dynamically assigned to a LAN-Trans device but
           currently has an expired lease.  dynamicActive(4)
           indicates an IP that was dynamically assigned to a
           LAN-Trans device that has a current 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
    }


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 the 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      current
    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 }
--====================================================================
--
-- 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 2 valid IP addresses, the PS must update
         the rows with cabhCdpWanDnsServerOrder values of 1 and 2.
         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."
      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."
      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."
      DEFVAL  { 'c0a80000'h }
    ::= { 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
         "Option value 1 - Value of LAN-Trans Subnet Mask."
      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
       "Option value 2 - Value of LAN-Trans Time Offset from
        Coordinated Universal Time (UTC)."
      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
            "Option value 3 - Router for the LAN-Trans
            address realm."
      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 IP Addresses of the LAN-Trans address realm
       DNS servers.  As a default there is only one DNS
       server and it is the address specified in Option
       Value 3 - cabhCdpServerRouter.  Only one address
       is specified."
      DEFVAL { 'c0a80001'h }  -- 192.168.0.1
    ::= { 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
       "The IP Addresses of the LAN-Trans SYSLOG servers.
       As a default there are no SYSLOG Servers.
       The factory defaults contains the indication of
       no Syslog Server value equals (0.0.0.0)."
      DEFVAL { '00000000'h }  -- 0.0.0.0
    ::= { cabhCdpServer 15 }

cabhCdpServerDomainName OBJECT-TYPE
    SYNTAX      SnmpAdminString(SIZE(0..128))
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
     "Option value 15 - Domain name of LAN-Trans address realm."
      DEFVAL {""}
    ::= { cabhCdpServer 16 }

cabhCdpServerTTL  OBJECT-TYPE
    SYNTAX      INTEGER (0..255)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Option value 23 - LAN-Trans Time to Live."
      DEFVAL  { 64 }
    ::= { cabhCdpServer 17 }

cabhCdpServerInterfaceMTU       OBJECT-TYPE
    SYNTAX      Integer32 (0 | 68..4096)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "Option value 26 - LAN-Trans Interface MTU.  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
            "Option value 43 - Vendor Specific Options."
      DEFVAL  { ''h }
    ::= { cabhCdpServer 19 }

cabhCdpServerLeaseTime  OBJECT-TYPE
    SYNTAX      Unsigned32
    UNITS       "seconds"
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
    "Option value 51 –Lease Time for LAN IP Devices in the LAN-Trans realm
    (seconds)."
      DEFVAL  { 3600 }
    ::= { cabhCdpServer 20 }

cabhCdpServerDhcpAddressType  OBJECT-TYPE
    SYNTAX      InetAddressType
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
    "Option value 54 - Type of LAN-Trans DHCP server IP address."
      DEFVAL { ipv4 }
      ::= { cabhCdpServer 21 }

cabhCdpServerDhcpAddress      OBJECT-TYPE
    SYNTAX      InetAddress
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "Option value 54 - LAN-Trans DHCP server IP
            address. It defaults to the router address as
            specified in cabhCdpServerRouter.  Alternatively
            a vendor may want to separate CDS address from
            router address."
      DEFVAL { 'c0a80001'h }        --    192.168.0.1
      ::= { 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 rollback 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 }


--
-- notification group is for future extension.
--

cabhCdpNotification OBJECT IDENTIFIER ::= { cabhCdpMib 2 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
             MTA feature."
    MODULE   -- cabhCdpMib
```

```
-- unconditionally mandatory groups

    MANDATORY-GROUPS {
            cabhCdpGroup
    }

::= { cabhCdpCompliances 3 }

cabhCdpGroup   OBJECT-GROUP

   OBJECTS {
   cabhCdpSetToFactory,
   cabhCdpLanTransCurCount,
   cabhCdpLanTransThreshold,
   cabhCdpLanTransAction,
   cabhCdpWanDataIpAddrCount,

   cabhCdpLanAddrClientID,
   cabhCdpLanAddrLeaseCreateTime,
   cabhCdpLanAddrLeaseExpireTime,
   cabhCdpLanAddrMethod,
   cabhCdpLanAddrHostName,
   cabhCdpLanAddrRowStatus,

   cabhCdpWanDataAddrClientId,
   cabhCdpWanDataAddrIpType,
   cabhCdpWanDataAddrIp,
   cabhCdpWanDataAddrRenewalTime,
   cabhCdpWanDataAddrRowStatus,

   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
}
STATUS current
DESCRIPTION
"Group of objects for CableHome CDP MIB."
::= { cabhCdpGroups 1 }

END
```

E.3 Requisitos de la MIB del portal de prueba de IPCable2Home (CTP)

Requisitos

The CableHome™ CTP MIB MUST be implemented as defined below.

```
CABH-CTP-MIB DEFINITIONS ::= BEGIN
IMPORTS
   MODULE-IDENTITY,
   OBJECT-TYPE          FROM SNMPv2-SMI
   TruthValue,
   TEXTUAL-CONVENTION   FROM SNMPv2-TC
   OBJECT-GROUP,
   MODULE-COMPLIANCE    FROM SNMPv2-CONF
   InetAddressType,
   InetAddress,
   InetAddressIPv4,
   InetAddressIPv6      FROM INET-ADDRESS-MIB
   clabProjCableHome    FROM CLAB-DEF-MIB;

--=================================================================
--
--    History:
--
--    Date        Modified by       Reason
--    04/05/02                      Issued I01
--    09/20/02                      Issued I02
--    04/11/03                      Issued I03
--
--=================================================================

cabhCtpMib MODULE-IDENTITY
    LAST-UPDATED  "200304110000Z"-- April 11, 2003
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
                  400 Centennial Parkway
                  Louisville, Colorado 80027-1266
            U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
    DESCRIPTION
            "This MIB module defines the diagnostic controls
            offered by the CableHome Test Portal (CTP).

      Acknowledgements:
      Roy Spitzer             -     Consultant to CableLabs
      Mike Mannette           -     Consultant to CableLabs
      Randy Dunton            -     Intel
      Dmitrii Loukianov       -     Intel
      Wes Peters              -     DoBox, Inc.
      Chris Zacker                  Broadcom"
    ::=  { 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 Cable Home
--    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}

--
--    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."
      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)."
      REFERENCE
            "CableHome Specification Section 6.4.4"
      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."
      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."
    ::= { 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."
      DEFVAL { udp }
    ::= { cabhCtpConnSpeed 5 }


cabhCtpConnNumPkts      OBJECT-TYPE
    SYNTAX        INTEGER (1..65535)
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
        "The number of packets the CTP is to send when triggered to
 execute the Connection Speed Tool."
      DEFVAL { 100 }
      ::= { cabhCtpConnSpeed 6 }

cabhCtpConnPktSize      OBJECT-TYPE
      SYNTAX            INTEGER (64..1518)
      MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The size of the test frames."
      REFERENCE
            ""
      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."
      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
   "The status of the Connection Speed Tool."
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."
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)."
    REFERENCE
             "CableHome 1.0 Specification Section 6.4.4"
    DEFVAL { 'c0a80001'h }
      ::= { 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."
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."
      ::= { cabhCtpPing 4 }

cabhCtpPingNumPkts      OBJECT-TYPE
      SYNTAX            INTEGER (1..4)
      MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The number of packets to send to each host."
      DEFVAL {1}
      ::= { cabhCtpPing 5 }

cabhCtpPingPktSize      OBJECT-TYPE
      SYNTAX            INTEGER (64..1518)
      MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
            "The size of the test frames."
      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."
      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)."
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
   "The status of the Ping Tool."
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 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,
         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 del dispositivo de servicios de portal de IPCable2Home (PSDev)

Requisitos

The CableHome™ PSDev MIB MUST be implemented as defined below.

```
CABH-PS-DEV-MIB DEFINITIONS ::= BEGIN
IMPORTS
   MODULE-IDENTITY,
   OBJECT-TYPE,
   Integer32,
   NOTIFICATION-TYPE          FROM SNMPv2-SMI
   TruthValue,
   PhysAddress,
   DateAndTime,
   TEXTUAL-CONVENTION         FROM SNMPv2-TC
   SnmpAdminString            FROM SNMP-FRAMEWORK-MIB
   OBJECT-GROUP,
   MODULE-COMPLIANCE,
   NOTIFICATION-GROUP         FROM SNMPv2-CONF

   InetAddressType,
   InetAddress                FROM INET-ADDRESS-MIB

   docsDevSwCurrentVers,
   docsDevEvLevel,
   docsDevEvId,
   docsDevEvText,
   docsDevSwFilename,
   docsDevSwServer            FROM DOCS-CABLE-DEVICE-MIB -- RFC2669

   cabhCdpServerDhcpAddress,
   cabhCdpWanDataAddrClientId,
   cabhCdpLanTransThreshold,
   cabhCdpLanTransCurCount    FROM CABH-CDP-MIB

   clabProjCableHome          FROM CLAB-DEF-MIB;

--================================================================
--
--    History:
--
--    Date        Modified by       Reason
--    04/05/02                      Issued I01
--    09/20/02                      Issued I02
--    04/11/03                      Issued I03
--
--================================================================


cabhPsDevMib MODULE-IDENTITY
    LAST-UPDATED    "200304110000Z"-- April 11, 2003
    ORGANIZATION    "CableLabs Broadband Access Department"
    CONTACT-INFO
            "Kevin Luehrs
            Postal: Cable Television Laboratories, Inc.
                  400 Centennial Parkway
                  Louisville, Colorado 80027-1266
                        U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
```

```
    DESCRIPTION
            "This MIB module supplies the basic management objects
             for the PS Device.  The PS device parameter describe
      general PS Device attributes and behaviour characteristics.
      Most the PS Device MIB is need for configuration download.

            Acknowledgements:
            Roy Spitzer     - Consultant to CableLabs
            Mike Mannette   - Consultant to CableLabs
            Itay Sherman    - Texas Instruments
            Chris Zacker    - Broadcom
            Rick Vetter     - Consultant to CableLabs "
    ::=  { clabProjCableHome 1 }

-- Textual conventions
      X509Certificate ::= TEXTUAL-CONVENTION
            STATUS current
            DESCRIPTION
"An X509 digital certificate encoded as an ASN.1 DER object."
            SYNTAX OCTET STRING (SIZE (0..4096))


cabhPsDevMibObjects    OBJECT IDENTIFIER ::= { cabhPsDevMib 1 }
cabhPsDevBase       OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 1 }
cabhPsDevProv    OBJECT IDENTIFIER ::= { cabhPsDevMibObjects 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 stand-alone 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 Appendix I of the CableHome 1.0 specification. 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
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
      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."
      ::= { 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 1.0 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
dormantCHmode(3)."
::={ cabhPsDevBase 11 }


--
--    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(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
    cabhPsDevProvisioningEnrolmentReport 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 }

--
-- notification group is for future extension.
--

cabhPsNotification OBJECT IDENTIFIER ::= { cabhPsDevMib 2 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."
   ::= { cabhPsNotification 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."
   ::= { cabhPsNotification 2 }

cabhPsDevInitRetryTrap  NOTIFICATION-TYPE
   OBJECTS  {
         docsDevEvLevel,
         docsDevEvId,
         docsDevEvText,
      cabhPsDevWanManMacAddress
   }
   STATUS      current
   DESCRIPTION
"An event to report a failure happened during the initialization
process and detected in the PS. "
   ::= { cabhPsNotification 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."
   ::= { cabhPsNotification 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 server IP address the image is from."
   ::= { cabhPsNotification 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 server IP address the image is from."
   ::= { cabhPsNotification 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 server IP address the image is from."
   ::= { cabhPsNotification 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."
   ::= { cabhPsNotification 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."
   ::= { cabhPsNotification 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."
   ::= { cabhPsNotification 10 }


cabhPsDevCdpThresholdTrap  NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress,
       cabhCdpLanTransThreshold
   }
```

```
   STATUS      current
   DESCRIPTION
"An event to report that the Lan-Trans threshold has been exceeded."
   ::= { cabhPsNotification 11 }

cabhPsDevCspTrap  NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress
   }
   STATUS      current
   DESCRIPTION
           "To report an event with the CableHome Security Portal."
   ::= { cabhPsNotification 12 }

cabhPsDevCapTrap  NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress
   }
   STATUS      current
   DESCRIPTION
           "To report an event with the CableHome Address Portal."
   ::= { cabhPsNotification 13 }

cabhPsDevCtpTrap  NOTIFICATION-TYPE
   OBJECTS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevWanManMacAddress
   }
   STATUS      current
   DESCRIPTION
           "To report an event with the CableHome Test Portal."
   ::= { cabhPsNotification 14 }

cabhPsDevProvEnrollTrap  NOTIFICATION-TYPE
   OBJECTS {
       cabhPsDevHardwareVersion,
       docsDevSwCurrentVers,
       cabhPsDevTypeIdentifier,
       cabhPsDevWanManMacAddress,
       cabhPsDevProvCorrelationId
   }
   STATUS      current
   DESCRIPTION
           "This inform is issued to initiate the CableHome
              process provisioning."
   REFERENCE
         "Inform as defined in RFC 1902"
   ::= { cabhPsNotification 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 cabhCdpLanPoolStart and cabhCdpLanPoolEnd, is exhausted "

      ::= { cabhPsNotification 16}

-- compliance statements

cabhPsBasicCompliance MODULE-COMPLIANCE
    STATUS     current
    DESCRIPTION
            "The compliance statement for devices that implement
             PS feature."
    MODULE   --cabhPsMib


-- unconditionally mandatory groups

    MANDATORY-GROUPS {
            cabhPsGroup
    }

::= { cabhPsCompliances 1}


cabhPsGroup OBJECT-GROUP
    OBJECTS {
         cabhPsDevDateTime,
         cabhPsDevResetNow,
         cabhPsDevSerialNumber,
         cabhPsDevHardwareVersion,
         cabhPsDevWanManMacAddress,
         cabhPsDevWanDataMacAddress,
         cabhPsDevTypeIdentifier,
       cabhPsDevSetToFactory,
         cabhPsDevWanManClientId,
       cabhPsDevTodSyncStatus,
         cabhPsDevProvMode,
         cabhPsDevProvisioningTimer,
       cabhPsDevProvConfigFile,
       cabhPsDevProvConfigHash,
       cabhPsDevProvConfigFileSize,
       cabhPsDevProvConfigFileStatus,
       cabhPsDevProvConfigTLVProcessed,
       cabhPsDevProvConfigTLVRejected,
       cabhPsDevProvSolicitedKeyTimeout,
       cabhPsDevProvState,
       cabhPsDevProvAuthState,
         cabhPsDevProvCorrelationId,
         cabhPsDevTimeServerAddrType,
         cabhPsDevTimeServerAddr

    }
    STATUS    current
    DESCRIPTION
        "Group of objects for CableHome PS MIB."
    ::= { cabhPsGroups 1 }
```

```
cabhPsNotificationGroup       NOTIFICATION-GROUP
      NOTIFICATIONS {
        cabhPsDevInitTLVUnknownTrap,
        cabhPsDevInitTrap,
        cabhPsDevInitRetryTrap,
        cabhPsDevDHCPFailTrap,
        cabhPsDevSwUpgradeInitTrap,
        cabhPsDevSwUpgradeFailTrap,
        cabhPsDevSwUpgradeSuccessTrap,
        cabhPsDevSwUpgradeCVCFailTrap,
        cabhPsDevTODFailTrap,
        cabhPsDevCdpWanDataIpTrap,
        cabhPsDevCdpThresholdTrap,
        cabhPsDevCspTrap,
        cabhPsDevCapTrap,
        cabhPsDevCtpTrap,
        cabhPsDevProvEnrollTrap,
        cabhPsDevCdpLanIpPoolTrap
      }
      STATUS      current
      DESCRIPTION
         "These notifications indicate change in status of the Portal
         Services set of functions in a device complying with
         CableLabs CableHome(tm) specifications."
      ::= { cabhPsGroups 2 }
END
```

E.5 Requisitos de la MIB de seguridad de IPCable2Home (SEC)

Requisitos

The CableHome™ sec MIB MUST be implemented as defined below.

```
CABH-SEC-MIB DEFINITIONS ::= BEGIN
IMPORTS
    MODULE-IDENTITY,
      Unsigned32,
      BITS,
      OBJECT-TYPE       FROM SNMPv2-SMI
      TruthValue,
      DisplayString,
      TimeStamp         FROM SNMPv2-TC
      OBJECT-GROUP,
      MODULE-COMPLIANCE FROM SNMPv2-CONF
      InetAddressIPv4   FROM INET-ADDRESS-MIB
      SnmpAdminString   FROM SNMP-FRAMEWORK-MIB -- RFC2571
      X509Certificate   FROM DOCS-BPI2-MIB
      clabProjCableHome FROM CLAB-DEF-MIB;

--=================================================================
--
--    History:
--
--    Date        Modified by       Reason
--    04/05/02                      Issued I01
--    09/20/02                      Issued I02
--    04/11/03                      Issued I03
--
--=================================================================

cabhSecMib MODULE-IDENTITY
    LAST-UPDATED    "200304110000Z"--April 11, 2003
    ORGANIZATION    "CableLabs Broadband Access Department"
```

```
    CONTACT-INFO
            "Kevin Luehrs
            Postal:     Cable Television Laboratories, Inc.
                  400 Centennial Parkway
                  Louisville, Colorado 80027-1266
                        U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: k.luehrs@cablelabs.com"
    DESCRIPTION
            "This MIB module supplies the basic management objects
            for the Security Portal Services.

            Acknowledgements:
            Roy Spitzer       -  Consultant to CableLabs
            Chris Zacker      -  Broadcom Visiting Engineer"
    ::=  { clabProjCableHome 2 }

-- Textual conventions

cabhSecFwObjects  OBJECT IDENTIFIER ::= { cabhSecMib 1 }
cabhSecFwBase           OBJECT IDENTIFIER ::= { cabhSecFwObjects 1 }
cabhSecFwLogCtl   OBJECT IDENTIFIER ::= { cabhSecFwObjects 2 }
cabhSecCertObjects      OBJECT IDENTIFIER ::= { cabhSecMib 2 }
--
-- The following group describes the base objects in the Cable Home
-- Firewall.
--

cabhSecFwPolicyFileEnable OBJECT-TYPE
      SYNTAX      INTEGER {
            enable            (1),
            disable           (2)
            }
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
      "This parameter indicates whether or not to enable the firewall
      functionality."
      DEFVAL {enable}
    ::= { cabhSecFwBase 1 }

cabhSecFwPolicyFileURL OBJECT-TYPE
    SYNTAX      DisplayString
    MAX-ACCESS  read-write
    STATUS      current
    DESCRIPTION
"This object contains the name and IP address of the policy rule set
file in a TFTP URL format. Once this object has been updated, it will
trigger the file download."

::= { cabhSecFwBase 2 }


cabhSecFwPolicyFileHash OBJECT-TYPE
    SYNTAX OCTET STRING (SIZE(20))
    MAX-ACCESS read-write
    STATUS current
    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."
```

```
::= { cabhSecFwBase 3 }


cabhSecFwPolicyFileOperStatus OBJECT-TYPE
SYNTAX      INTEGER {
inProgress(1),
complete (2),
completeFromMgt(3)  --- deprecated,
failed(4)
}
MAX-ACCESS read-only
STATUS current
DESCRIPTION
"inProgress(1) indicates that a TFTP download is underway,
complete (2) indicates that the firewall
configuration file downloaded and configured successfully,
completeFromMgt(3) This state is deprecated.
failed(4) indicates that the last attempted download failed
ordinarily due to TFTP timeout."
::= { cabhSecFwBase 4 }


cabhSecFwPolicyFileCurrentVersion OBJECT-TYPE
    SYNTAX      SnmpAdminString
    MAX-ACCESS  read-only
    STATUS      current
    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 }

--
--    Firewall log parameters
--


cabhSecFwEventType1Enable OBJECT-TYPE
SYNTAX      INTEGER {
            enable (1), -- log event
            disable (2) -- do not log event
            }
MAX-ACCESS read-write
STATUS      current
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 current
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 current
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 current
      DESCRIPTION
"If the number of type 1 or 2 hacker attacks exceeds this
threshold in the period define 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 current
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 }


cabhSecCertPsCert OBJECT-TYPE
SYNTAX            X509Certificate
MAX-ACCESS  read-only
STATUS            current
DESCRIPTION
"The X509 DER-encoded PS certificate."
REFERENCE
"CableLabs CableHome 1.0 Specification version I01 (CH-SP-I01-020405)
 Section 11.3 Requirements (security requirements)"
::= { cabhSecCertObjects 1 }
```

```
--
-- notification group is for future extension.
--

cabhSecNotification OBJECT IDENTIFIER ::= { cabhSecMib 3 0 }
cabhSecConformance  OBJECT IDENTIFIER ::= { cabhSecMib 4 }
cabhSecCompliances  OBJECT IDENTIFIER ::= { cabhSecConformance 1 }
cabhSecGroups       OBJECT IDENTIFIER ::= { cabhSecConformance 2 }

--
--    Notification Group
--


-- compliance statements

cabhSecBasicCompliance MODULE-COMPLIANCE
    STATUS     current
    DESCRIPTION
       "The compliance statement for CableHome Firewall feature."
    MODULE   -- cabhSecMib


-- unconditionally mandatory groups

    MANDATORY-GROUPS {
            cabhSecGroup
    }

::= { cabhSecCompliances 3 }


cabhSecGroup OBJECT-GROUP
    OBJECTS {
            cabhSecFwPolicyFileEnable,
            cabhSecFwPolicyFileURL,
            cabhSecFwPolicyFileHash,
            cabhSecFwPolicyFileOperStatus,
            cabhSecFwPolicyFileCurrentVersion,

            cabhSecFwEventType1Enable,
            cabhSecFwEventType2Enable,
            cabhSecFwEventType3Enable,
            cabhSecFwEventAttackAlertThreshold,
            cabhSecFwEventAttackAlertPeriod,
            cabhSecCertPsCert
    }
    STATUS    current
    DESCRIPTION
      "Group of object in CableHome Firewall MIB"
    ::= { cabhSecGroups 1 }

END
```

E.6 Requisitos de la MIB de definición (DEF) IPCable2Home

```
CLAB-DEF-MIB DEFINITIONS ::= BEGIN
IMPORTS
      X509Certificate         FROM DOCS-BPI2-MIB
 -- DocsX509ASN1DEREncodedCertificate   FROM DOCS-BPI2-MIB
      MODULE-IDENTITY,
      enterprises             FROM SNMPv2-SMI;
```

```
cableLabs MODULE-IDENTITY
      LAST-UPDATED    "0209200000Z"-- September 20, 2002
    ORGANIZATION    "CableLabs"
    CONTACT-INFO
            "Ralph Brown
            Postal: Cable Television Laboratories, Inc.
                400 Centennial Parkway
                Louisville, Colorado 80027-1266
                U.S.A.
            Phone:  +1 303-661-9100
            Fax:    +1 303-661-9199
            E-mail: r.brown@cablelabs.com"
    DESCRIPTION
            "This MIB module supplies the basic management object categories for
CableLabs."

    ::= { enterprises 4491 }

clabFunction            OBJECT IDENTIFIER ::= { cableLabs 1 }
clabFuncMib2            OBJECT IDENTIFIER ::= { clabFunction 1 }
clabFuncProprietary     OBJECT IDENTIFIER ::= { clabFunction 2 }
clabProject             OBJECT IDENTIFIER ::= { cableLabs 2 }
clabProjDocsis          OBJECT IDENTIFIER ::= { clabProject 1 }
clabProjPacketCable     OBJECT IDENTIFIER ::= { clabProject 2 }
clabProjCableHome       OBJECT IDENTIFIER ::= { clabProject 4 }
clabSecurity            OBJECT IDENTIFIER ::= { cableLabs 3}

clabSecCertObject OBJECT IDENTIFIER ::= { clabSecurity 1 }

clabSrvcPrvdrRootCACert       OBJECT-TYPE
    SYNTAX        X509Certificate
    MAX-ACCESS          read-only
    STATUS        current
    DESCRIPTION
            "The X509 DER-encoded CableLabs Service Provider Root CA
Certificate."
    REFERENCE
    "CableLabs CableHome Specification Section 11"
    ::= { clabSecCertObject 1 }

clabCVCRootCACert             OBJECT-TYPE
    SYNTAX        X509Certificate
    MAX-ACCESS          read-only
    STATUS        current
    DESCRIPTION
            "The X509 DER-encoded CableLabs CVC Root CA Certificate."
    REFERENCE
    "CableLabs CableHome Specification Section 11 for Standalone PS Elements
only"
    ::= { clabSecCertObject 2 }

clabCVCCACert           OBJECT-TYPE
    SYNTAX        X509Certificate
    MAX-ACCESS          read-only
    STATUS        current
    DESCRIPTION
            "The X509 DER-encoded CableLabs CVC CA Certificate."
    REFERENCE
    "CableLabs CableHome Specification Section 11 for Standalone PS Elements
only"
    ::= { clabSecCertObject 3 }
```

```
clabMfgCVCCert          OBJECT-TYPE
    SYNTAX        X509Certificate
    MAX-ACCESS          read-only
    STATUS        current
    DESCRIPTION
            "The X509 DER-encoded Manufacturer CVC Certificate."
    REFERENCE
    "CableLabs CableHome Specification Section 11 for Standalone PS Elements
only"
    ::= { clabSecCertObject 4 }

END
```

E.7 Requisitos de la MIB del portal de QoS de IPCable2Home (CQP)

Requisitos

The CableHome™ CQP MIBs MUST be implemented as defined below.

```
CABH-QOS-MIB DEFINITIONS ::= BEGIN
   IMPORTS
      MODULE-IDENTITY,
      OBJECT-TYPE,
      Unsigned32
                              FROM SNMPv2-SMI

      TruthValue,
      RowStatus               FROM SNMPv2-TC

      OBJECT-GROUP,
      MODULE-COMPLIANCE       FROM SNMPv2-CONF

      InetPortNumber,
      InetAddressType,
      InetAddress             FROM INET-ADDRESS-MIB

      ifIndex                 FROM IF-MIB

-- CL specs releases before RFC
      clabProjCableHome      FROM CLAB-DEF-MIB;

   cabhQosMib MODULE-IDENTITY
       LAST-UPDATED    "200303010000Z"-- March 1, 2003
       ORGANIZATION    "CableLabs Broadband Access Department"
       CONTACT-INFO
            "Kevin Luehrs
             Postal: Cable Television Laboratories, Inc.
             400 Centennial Parkway
             Louisville, Colorado 80027-1266
             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
                prioritized QoS capability."
       REVISION "200303010000Z"-- March 1, 2003
       DESCRIPTION
               "Initial version, published as RFC xxxx."
                -- RFC editor to assign xxxx
```

```
--    ::= { mib-2 xx }
-- xx to be assigned by IANA
-- CL specs releases before RFC
    ::=  { clabProjCableHome 6 }

   -- Textual conventions

   cabhQosMibObjects         OBJECT IDENTIFIER ::= { cabhQosMib 1}
   cabhPriorityQosMibObjects OBJECT IDENTIFIER ::= { cabhQosMibObjects 1 }
   cabhPriorityQosBase       OBJECT IDENTIFIER ::= { cabhPriorityQosMibObjects 1
}
   cabhPriorityQosBp         OBJECT IDENTIFIER ::= { cabhPriorityQosMibObjects 2
}
   cabhPriorityQosPs         OBJECT IDENTIFIER ::= { cabhPriorityQosMibObjects 3
}

   -- future parametric QOS
   -- cabhParamQosMibObjects  OBJECT IDENTIFIER ::= { cabhQosMibObjects 2 }

   --================================================================
   --
   --  Application Priority Master Table
   --
   --  The cabhPriorityQosMasterTable contains the list of
   --  application priorities provisioned by the cable operator.
   --  Applications are identified by the IANA "well-known" port
   --  numbers  assigned to them.
   --
   --================================================================
   cabhPriorityQosMasterTable  OBJECT-TYPE
         SYNTAX SEQUENCE OF CabhPriorityQosMasterEntry
         MAX-ACCESS  not-accessible
         STATUS      current
         DESCRIPTION
           "This table contains a list of mappings for Application
            IDs to Default CableHome Priorities."
         ::= { cabhPriorityQosBase 1  }

   cabhPriorityQosMasterEntry OBJECT-TYPE
           SYNTAX CabhPriorityQosMasterEntry
           MAX-ACCESS   not-accessible
           STATUS    current
           DESCRIPTION
             "An entry for mapping Application IDs to
             Default CableHome Priorities."
      INDEX { cabhPriorityQosMasterApplicationId }
      ::= { cabhPriorityQosMasterTable 1 }


   CabhPriorityQosMasterEntry ::= SEQUENCE {
         cabhPriorityQosMasterApplicationId       Unsigned32,
         cabhPriorityQosMasterDefaultCHPriority   Unsigned32,
         cabhPriorityQosMasterRowStatus           RowStatus
        }

   cabhPriorityQosMasterApplicationId       OBJECT-TYPE
       SYNTAX                  Unsigned32 (1..65535)
       MAX-ACCESS              not-accessible
       STATUS                  current
       DESCRIPTION
        "The IANA well-known port number identifying an application."
       ::= { cabhPriorityQosMasterEntry 1 }
```

```
   cabhPriorityQosMasterDefaultCHPriority       OBJECT-TYPE
       SYNTAX                  Unsigned32 (0..7)
       MAX-ACCESS              read-create
       STATUS                  current
       DESCRIPTION
        "The Qos priority assigned to the application."
       ::= { cabhPriorityQosMasterEntry 2 }

   cabhPriorityQosMasterRowStatus  OBJECT-TYPE
       SYNTAX                  RowStatus
       MAX-ACCESS              read-create
       STATUS                  current
       DESCRIPTION
         "The Row Status 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 notReady(3) to any new row created
          without a valid value for both entries. The PS will
          prevent modification of this table's columns and return
          an inconsistentValue error if the NMS attempts to make
          such modifications while RowStatus is active(1)."
       ::= { cabhPriorityQosMasterEntry 3 }



   -- ================================================================
   --
   --  SetToFactory Object
   --
   -- This object is used to clear some of the QoS MIB tables
   --
   -- ================================================================

cabhPriorityQosSetToFactory OBJECT-TYPE
       SYNTAX TruthValue
       MAX-ACCESS read-write
       STATUS current
       DESCRIPTION
         "Reading this object alwyas returns false(2). When this object is
          set to true(1), the PS MUST clear all the entries in the
          cabhPriorityQosBpTable and cabhPriorityQosBpDestTable."

       ::= { cabhPriorityQosBase 2 }


   --================================================================
   --
   --  BP Application Priority Table
   --
   --  The cabhPriorityQosBpTable contains the list of
   --  BPs, the applications implemented on each, and the priority
   --  assigned to each application.
   --
   --================================================================

   cabhPriorityQosBpTable OBJECT-TYPE
      SYNTAX SEQUENCE OF CabhPriorityQosBpEntry
      MAX-ACCESS not-accessible
      STATUS current
      DESCRIPTION
         "This table contains the priorities for each of the
          discovered CableHome Host (BP) applications
          and related data."
            ::= {cabhPriorityQosBp 1}
```

```
cabhPriorityQosBpEntry OBJECT-TYPE
   SYNTAX      CabhPriorityQosBpEntry
   MAX-ACCESS     not-accessible
   STATUS      current
   DESCRIPTION
      "List of all the discovered applications on a BP
       and their priorities identified by the PS."
   INDEX { cabhPriorityQosMasterApplicationId,
           cabhPriorityQosBpIpAddrType, cabhPriorityQosBpIpAddr }
   ::= { cabhPriorityQosBpTable 1 }

CabhPriorityQosBpEntry ::= SEQUENCE {
      cabhPriorityQosBpIpAddrType         InetAddressType,
      cabhPriorityQosBpIpAddr             InetAddress,
      cabhPriorityQosBpApplicationId      Unsigned32,
      cabhPriorityQosBpDefaultCHPriority  Unsigned32,
      cabhPriorityQosBpIndex              Unsigned32
      }

cabhPriorityQosBpIpAddrType   OBJECT-TYPE
   SYNTAX      InetAddressType
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
      "The type of the IP address assigned to a particular
       BP element."
   ::= { cabhPriorityQosBpEntry 1 }


cabhPriorityQosBpIpAddr    OBJECT-TYPE
   SYNTAX      InetAddress
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
      "The IP address assigned to a particular BP element."
   ::= { cabhPriorityQosBpEntry 2 }

cabhPriorityQosBpApplicationId   OBJECT-TYPE
   SYNTAX      Unsigned32 (1..65535)
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
      "The IANA well-known port number assigned to a
       particular application implemented on the
       CableHome Host device in which this BP resides."
   ::= { cabhPriorityQosBpEntry 3 }


cabhPriorityQosBpDefaultCHPriority  OBJECT-TYPE
   SYNTAX      Unsigned32 (0..7)
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
      "The priority assigned to a particular application
       implemented on CableHome Host device in which this
       BP resides. The PS populates this entry according
       to the Application Priority Master Table."
   ::= { cabhPriorityQosBpEntry 4 }
```

```
cabhPriorityQosBpIndex  OBJECT-TYPE
   SYNTAX      Unsigned32 (1..65535)
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
     "The unique identifier for a particular row in the
      BP Application Priority Table. This identifier is
      used as an index into the 'nested' Destination
      Priority Table."
        ::= { cabhPriorityQosBpEntry 5 }


--================================================================
--
--  Destination Priority Table
--
--  The cabhPriorityQosDestListTable contains the list of
--  provisioned destinations (IP address and port number) to
--  which a BP can send traffic with a special Qos
--  priority. Any application listed in the BP Application
--  Priority Table can be provisioned with a destination specific
--  priority in this table.
--
--================================================================

cabhPriorityQosBpDestTable OBJECT-TYPE
   SYNTAX SEQUENCE OF CabhPriorityQosBpDestEntry
   MAX-ACCESS     not-accessible
   STATUS      current
   DESCRIPTION
      "This table contains the priorities based on
       sessions established by a BP, identified by
       destination IP address and port number. It
       is indexed with a unique identifier for rows
       in the BP Application Priority Table
       (cabhPriorityQoSBpTable."
       ::= {cabhPriorityQosBp 2}

cabhPriorityQosBpDestEntry OBJECT-TYPE
   SYNTAX      CabhPriorityQosBpDestEntry
   MAX-ACCESS  not-accessible
   STATUS      current
   DESCRIPTION
      "List of Destination IP addresses and port numbers
       for an application to which special Qos
       priority is provisioned."
   INDEX { cabhPriorityQosBpIndex, cabhPriorityQosBpDestIndex }
   ::= { cabhPriorityQosBpDestTable 1 }

CabhPriorityQosBpDestEntry ::= SEQUENCE {
    cabhPriorityQosBpDestIndex            Unsigned32,
    cabhPriorityQosBpDestIpAddrType       InetAddressType,
    cabhPriorityQosBpDestIpAddr           InetAddress,
    cabhPriorityQosBpDestPort             InetPortNumber,
    cabhPriorityQosBpDestIpPortPriority   Unsigned32
      }


cabhPriorityQosBpDestIndex OBJECT-TYPE
   SYNTAX      Unsigned32 (1..65535)
   MAX-ACCESS  not-accessible
   STATUS      current
```

```
   DESCRIPTION
     "The locally unique index into the Destination
      Priority Table."
   ::= { cabhPriorityQosBpDestEntry 1 }

cabhPriorityQosBpDestIpAddrType     OBJECT-TYPE
   SYNTAX      InetAddressType
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
      "The type of the Destination IP Address."
   ::= { cabhPriorityQosBpDestEntry 2 }

cabhPriorityQosBpDestIpAddr   OBJECT-TYPE
   SYNTAX      InetAddress
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
     "The Destination IP address of the device to which
      an application-session is established by a BP and
      a special Qos priority is provisioned."
   ::= { cabhPriorityQosBpDestEntry 3 }

cabhPriorityQosBpDestPort     OBJECT-TYPE
   SYNTAX      InetPortNumber
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
     "The port number on a IP device to which
      an application-session is established by a BP and
      a special Qos priority is provisioned."
   ::= { cabhPriorityQosBpDestEntry 4 }

cabhPriorityQosBpDestIpPortPriority    OBJECT-TYPE
   SYNTAX      Unsigned32 (0..7)
   MAX-ACCESS  read-only
   STATUS      current
   DESCRIPTION
     "The Qos priority assigned to a particular
      application-session (identified by destination IP
      and Port) on a BP."
   ::= { cabhPriorityQosBpDestEntry 5 }


--================================================================
--
--  PS Interface Attributes Table
--
--  The cabhPriorityQosPsIfAttribTable contains the number of
--  media access priorities and number of queues associated with
--  each LAN interface in the Residential Gateway.
--
--================================================================

cabhPriorityQosPsIfAttribTable   OBJECT-TYPE
        SYNTAX SEQUENCE OF CabhPriorityQosPsIfAttribEntry
        MAX-ACCESS   not-accessible
        STATUS    current
        DESCRIPTION
         "This table contains the number of media
          access priorities and number of queues associated
          with each LAN interface in the Residential Gateway."
        ::= { cabhPriorityQosPs 1  }
```

```
cabhPriorityQosPsIfAttribEntry      OBJECT-TYPE
        SYNTAX    CabhPriorityQosPsIfAttribEntry
        MAX-ACCESS   not-accessible
        STATUS    current
        DESCRIPTION
          "Number of media access priorities and number
           of queues for each LAN interface in the
           Residential Gateway. This table applies only
           to interfaces through which data flows."
        INDEX { ifIndex }
        ::= { cabhPriorityQosPsIfAttribTable 1 }

CabhPriorityQosPsIfAttribEntry ::= SEQUENCE {
   cabhPriorityQosPsIfAttribIfNumPriorities   Unsigned32,
        cabhPriorityQosPsIfAttribIfNumQueues   Unsigned32
}

cabhPriorityQosPsIfAttribIfNumPriorities OBJECT-TYPE
       SYNTAX     Unsigned32 (1..8)
       MAX-ACCESS read-only
       STATUS     current
       DESCRIPTION
        "The number of media access priorities supported
         by this LAN interface."
::= { cabhPriorityQosPsIfAttribEntry 1 }

cabhPriorityQosPsIfAttribIfNumQueues OBJECT-TYPE
       SYNTAX     Unsigned32 (1..8)
       MAX-ACCESS read-only
       STATUS     current
       DESCRIPTION
        "The number of queues associated with this LAN
         interface."
::= { cabhPriorityQosPsIfAttribEntry 2 }


-- Placeholder for notifications/traps.
--

cabhQosNotification         OBJECT IDENTIFIER  ::= { cabhQosMib 2 }
cabhPriorityQosNotification OBJECT IDENTIFIER  ::= {
cabhQosNotification 1 }

    --
-- Conformance definitions
--
cabhQosConformance          OBJECT IDENTIFIER  ::= { cabhQosMib 3 }
cabhPriorityQosConformance  OBJECT IDENTIFIER  ::= {
cabhQosConformance 1 }
cabhPriorityQosGroups       OBJECT IDENTIFIER  ::= {
cabhPriorityQosConformance 1 }
cabhPriorityQosCompliances  OBJECT IDENTIFIER  ::= {
cabhPriorityQosConformance 2 }


-- ==================

-- compliance statements

cabhPriorityQosCompliance MODULE-COMPLIANCE
    STATUS     current
    DESCRIPTION
      "The compliance statement for devices that implement
       CableHome 1.1 PriorityQos capability."
```

```
    MODULE   --cabhPriorityQosMib

-- unconditionally mandatory groups

    MANDATORY-GROUPS {
            cabhPriorityQosGroup
    }

::= { cabhPriorityQosCompliances 1}


cabhPriorityQosGroup OBJECT-GROUP
    OBJECTS {
    cabhPriorityQosMasterDefaultCHPriority,
    cabhPriorityQosMasterRowStatus,
    cabhPriorityQosSetToFactory,
    cabhPriorityQosBpIpAddrType,
    cabhPriorityQosBpIpAddr,
    cabhPriorityQosBpApplicationId,
    cabhPriorityQosBpDefaultCHPriority,
    cabhPriorityQosBpIndex,
    cabhPriorityQosBpDestIpAddrType,
    cabhPriorityQosBpDestIpAddr,
    cabhPriorityQosBpDestPort,
    cabhPriorityQosBpDestIpPortPriority,
    cabhPriorityQosPsIfAttribIfNumPriorities,
    cabhPriorityQosPsIfAttribIfNumQueues
    }
    STATUS    current
    DESCRIPTION
        "Group of objects for CableHome Application
         Priority MIB."
    ::= { cabhPriorityQosGroups 1 }

END
```

Apéndice I

Ejemplos de correspondencia de la prioridad de acceso a los medios

En esta Recomendación se define un sistema de QoS basado en prioridades, que se asignan al tráfico que pasa por los medios compartidos, en función de la prioridad atribuida a cada uno de los paquetes. Como las distintas tecnologías de medios compartidos soportan diversas prioridades de acceso a los medios, IPCable2Home define un método de correspondencia para traducir las prioridades de IPCable2Home genéricas a un conjunto de valores denominados prioridades de acceso a los medios de IPCable2Home. Los valores de estas prioridades describen el nivel de preferencia que debería recibir un paquete cuando accede a los medios compartidos. El número de los niveles de preferencia corresponde a la cantidad disponible de las prioridades de acceso a los medios, soportadas por una determinada tecnología de medios. Mientras más alto sea el valor de la prioridad de acceso a los medios de IPCable2Home para el paquete, mayor debería ser la preferencia obtenida para acceder a los medios compartidos. La correspondencia de la prioridad de acceso a los medios de IPCable2Home es independiente y distinta de las correspondencias de la prioridad de acceso a los medios nativa definida para las tecnologías de los medios compartidos. Estas correspondencias nativas se realizan en la capa 2 de cada dispositivo. Por consiguiente, sin tener en cuenta la tecnología de los medios compartidos, se debe asignar a los paquetes el acceso preferencial relativo deseado a los medios compartidos, como exige la correspondencia de la prioridad de acceso a los medios de IPCable2Home. En los cuadros I.2 y I.3 se dan ejemplos de correspondencia para algunas de las tecnologías de acceso a los medios compartidos.

I.1 Ethernet

Ethernet no establece una diferencia entre los paquetes y por consiguiente soporta únicamente una prioridad.

Como se muestra en el cuadro I.1, no se necesitan ajustes de correspondencia especiales.

Cuadro I.1/J.192 – Correspondencias de Ethernet

Prioridad genérica de IPCable2Home	Correspondencia de la prioridad de acceso a los medios de IPCable2Home	Correspondencia de la prioridad nativa del acceso a los medios de Ethernet
0	0	0
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0

I.2 HomePlug

HomePlug soporta 4 prioridades de acceso a los medios.

Como se muestra en el cuadro I.2, la correspondencia de HomePlug asigna una preferencia de acceso al canal a la prioridad 0 genérica de IPCable2Home, con relación a las prioridades 1 y 2 genéricas de IPCable2Home. Sin embargo, la correspondencia de la prioridad de acceso a los medios de IPCable2Home exige que a la prioridad 2 genérica de IPCable2Home se le asigne un

acceso de nivel superior con relación a las prioridades 0 y 1 genéricas de IPCable2Home, y que las prioridades 0 y 1 genéricas de IPCable2Home dispongan de derechos de acceso idénticos. Por consiguiente, el fabricante debe garantizar que a los paquetes se les asigne el acceso preferencial relativo deseado a los medios compartidos como exige la correspondencia de la prioridad de acceso a los medios de IPCable2Home.

Cuadro I.2/J.192 – Correspondencias de HomePlug

Prioridad genérica de IPCable2Home	Correspondencia de la prioridad de acceso a los medios de IPCable2Home	Correspondencia de la prioridad nativa de acceso a los medios de HomePlug
0	0	1
1	0	0
2	1	0
3	1	1
4	2	2
5	2	2
6	3	3
7	3	3

I.3 HomePNA

HomePNA soporta 8 prioridades de acceso a los medios.

Como se muestra en el cuadro I.3, la correspondencia de HomePNA asigna una preferencia de acceso al canal a la prioridad 0 genérica de IPCable2Home con relación a las prioridades 1 y 2 genéricas de IPCable2Home. No obstante, la correspondencia de la prioridad de acceso a los medios de IPCable2Home exige que la prioridad 2 genérica de IPCable2Home reciba un acceso de nivel superior con relación a las prioridades 0 y 1 genéricas de IPCable2Home, y que a la prioridad 1 genérica de IPCable2Home se le asigne un acceso de nivel superior con relación a la prioridad 0 genérica de IPCable2Home. Por consiguiente, el fabricante debe garantizar que a los paquetes se les asigne el acceso preferencial relativo deseado a los medios compartidos como lo exige la correspondencia de la prioridad de acceso a los medios de IPCable2Home.

Cuadro I.3/J.192 – Correspondencia de HomePNA

Prioridad genérica de IPCable2Home	Correspondencia de la prioridad de acceso a los medios de IPCable2Home	Correspondencia de la prioridad nativa de acceso a los medios de HomePNA
0	0	2
1	1	0
2	2	1
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7

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 multimedios
Serie I	Red digital de servicios integrados
Serie J	**Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios**
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, 2005