UNION INTERNATIONALE DES TÉLÉCOMMUNICATIONS

UIT-T J.191

(07/2002)

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

SÉRIE J: RÉSEAUX CÂBLÉS ET TRANSMISSION DES SIGNAUX RADIOPHONIQUES, TÉLÉVISUELS ET AUTRES SIGNAUX MULTIMÉDIAS

Divers

Paquetage de fonctionnalités IP pour l'amélioration des câblo-modems

Recommandation UIT-T J.191

RECOMMANDATIONS UIT-T DE LA SÉRIE J

RÉSEAUX CÂBLÉS ET TRANSMISSION DES SIGNAUX RADIOPHONIQUES, TÉLÉVISUELS ET AUTRES SIGNAUX MULTIMÉDIAS

Recommandations générales	J.1–J.9
Spécifications générales des transmissions radiophoniques analogiques	J.10–J.19
Caractéristiques de fonctionnement des circuits radiophoniques analogiques	J.20–J.29
Equipements et lignes utilisés pour les circuits radiophoniques analogiques	J.30–J.39
Codeurs numériques pour les signaux radiophoniques analogiques	J.40–J.49
Transmission numérique de signaux radiophoniques	J.50–J.59
Circuits de transmission télévisuelle analogique	J.60–J.69
Transmission télévisuelle analogique sur lignes métalliques et interconnexion avec les faisceaux hertziens	J.70–J.79
Transmission numérique des signaux de télévision	J.80–J.89
Services numériques auxiliaires propres aux transmissions télévisuelles	J.90–J.99
Prescriptions et méthodes opérationnelles de transmission télévisuelle	J.100–J.109
Services interactifs pour la distribution de télévision numérique	J.110–J.129
Transport des signaux MPEG-2 sur les réseaux par paquets	J.130–J.139
Mesure de la qualité de service	J.140–J.149
Distribution de la télévision numérique sur les réseaux locaux d'abonnés	J.150–J.159
IPCablecom	J.160–J.179
Divers	**J.180–J.199**
Application à la télévision numérique interactive	J.200–J.209

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T J.191

Paquetage de fonctionnalités IP pour l'amélioration des câblo-modems

Résumé

La présente Recommandation donne un ensemble des caractéristiques fondées sur IP qui peuvent être ajoutées à un câblo-modem pour permettre aux câblo-opérateurs de fournir un ensemble supplémentaire de services améliorés à leurs clients, comprenant la fourniture de la qualité de service (QS) IPCablecom, une sécurité améliorée, des caractéristiques de gestion et de fourniture supplémentaires, un adressage et un traitement de paquets amélioré.

Source

La Recommandation J.191 de l'UIT-T, élaborée par la Commission d'études 9 (2001-2004) de l'UIT-T, a été approuvée le 29 juillet 2002 selon la procédure définie dans la Résolution 1 de l'AMNT.

AVANT-PROPOS

L'UIT (Union internationale des télécommunications) est une institution spécialisée des Nations Unies dans le domaine des télécommunications. L'UIT-T (Secteur de la normalisation des télécommunications) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un Membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux responsables de la mise en œuvre de consulter la base de données des brevets du TSB.

© UIT 2003

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

Recommandation UIT-T J.191

Paquetage de fonctionnalités IP pour l'amélioration des câblo-modems

1 Domaine d'application

La présente Recommandation donne un ensemble de caractéristiques fondées sur IP qui peuvent être ajoutées à un câblo-modem pour permettre aux câblo-opérateurs de fournir un ensemble supplémentaire de services améliorés à leurs clients, comprenant la fourniture de la qualité de service (QS) IPCablecom, une sécurité améliorée, des caractéristiques de gestion et de fourniture supplémentaires, un adressage et un traitement de paquets amélioré.

2 Références

2.1 Références normatives

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T J.112] Recommandation UIT-T J.112 Annexe B (2001), *Spécifications de l'interface de service pour la transmission de données par câble: Spécification de l'interface radioélectrique*.

[UIT-T J.161] Recommandation UIT-T J.161 (2001), *Caractéristiques des codecs audio destinés au service audio bidirectionnel sur les réseaux de télévision par câble utilisant des câblo-modems*.

[UIT-T J.163] Recommandation UIT-T J.163 (2001), *Qualité de service dynamique pour la fourniture de services en temps réel sur les réseaux de télévision par câble utilisant des câblo-modems*.

[UIT-T J.170] Recommandation UIT-T J.170 (2002), *Spécifications de la sécurité sur IPCablecom*.

[UIT-T X.509] Recommandation UIT-T X.509 (2000) | ISO/CEI 9594-8:2001, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut*.

[UIT-T X.690] Recommandation UIT-T X.690 (2002) | ISO/CEI 8825-1:2002, *Technologies de l'information – Règles de codage ASN.1: spécifications des règles de codage de base, des règles de codage canoniques et des règles de codage distinctives*.

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

[ISO/CEI 10038] ISO/CEI 10038 (ANSI/IEEE Std 802.1D):1993, *Technologies de l'information – Télécommunications et échange d'informations entre systèmes – Réseaux locaux – Contrôle d'accès au milieu (MAC) – Ponts*.

[RFC 768] IETF RFC 768 (1980), *User Datagram Protocol* (Protocole des datagrammes d'usagers).

[RFC 792] IETF RFC 792 (1981), *Internet Control Message Protocol* (Protocole des messages de commande de l'Internet).

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

[RFC 1034] IETF RFC 1034 (1987), *Domain Names – Concepts and Facilities* (Noms de domaines – Concepts et services).

[RFC 1035] IETF RFC 1035 (1987), *Domain Names – Implementation and Specification* (Noms de domaines – Mise en œuvre et spécification).

[RFC 1122] IETF RFC 1122 (1989), *Requirements for Internet Hosts – Communication Layers* (Exigences pour les hôtes Internet – Couches de communication).

[RFC 1123] IETF RFC 1123 (1989), *Requirements for Internet Hosts – Application and Support* (Exigences pour les hôtes Internet – Application et soutien).

[RFC 1157] IETF RFC 1157 (1990), *A Simple Network Management Protocol (SNMP)* (Protocole de gestion de réseau simple).

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

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

[RFC 1905] IETF RFC 1905 (1996), *Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)*.

[RFC 1907] IETF RFC 1907 (1996), *Management Information Base for Version 2 of the Simple Network Management Protocol (SNMPv2)* (Base d'informations de gestion pour la version 2 du Protocole de gestion de réseau simple).

[RFC 2011] IETF RFC 2011 (1996), *SNMPv2 Management Information Base for the Internet Protocol using SMIv2* (Base d'informations de gestion SNMPv2 pour le protocole Internet utilisant SMIv2).

[RFC 2013] IETF RFC 2013 (1996), *SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2* (Base d'informations de gestion SNMPv2 pour le protocole de datagrammes d'usager utilisant SMIv2).

[RFC 2131] IETF RFC 2131 (1997), *Dynamic Host Configuration Protocol* (Protocole de configuration d'hôte dynamique).

[RFC 2132] IETF RFC 2132 (1997), *DHCP Options and BOOTP Vendor Extensions* (Options DHCP et extensions BOOTP des fabricants).

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

[RFC 2349] IETF RFC 2349 (1998), *TFTP Time-out Interval and Transfer Size Options* (Intervalle de temporisation TFTP et options de taille de transfert).

[RFC 2570] IETF RFC 2570 (1999), *Introduction to Version 3 of the Internet-standard Network Management Framework*.

[RFC 2571] IETF RFC 2571 (1999), *An Architecture for Describing SNMP Management Frameworks* (Architecture de description des cadres de la gestion du protocole SNMP).

[RFC 2572] IETF RFC 2572 (1999), *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)* (Traitement et distribution des messages pour le protocole de gestion de réseau simple) (SNMP).

[RFC 2573] IETF RFC 2573 (1999), *SNMP Applications* (Applications du protocole SNMP).

[RFC 2574] IETF RFC 2574 (1999), *User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)* (Modèle de sécurité fondée sur l'utilisateur (USM) pour la version 3 du Protocole de gestion de réseau simple) (SNMPv3).

[RFC 2575] IETF RFC 2575 (1999), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)* (Modèle de commande d'accès fondé sur la vue (VACM) pour le modèle de commande de réseau simple (SNMP)).

[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 2669] IETF RFC 2669 (1999), *DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems* (Base d'informations de gestion d'appareils par câble MIB ou DOCSIS pour les câblo-modems conformes à DOCSIS et les systèmes de terminaison de câblo-modems).

[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), *USM Key Management Information Base and Textual Convention* (Base d'informations de gestion de clés Diffie-Hellman USM et convention textuelle).

[RFC 2863] IETF RFC 2863 (2000), *The Interfaces Group MIB* (Base d'information de gestion de groupe d'interfaces).

[RFC 3022] IETF RFC 3022 (2001), *Traditional IP Network Address Translator (Traditional NAT)* (Traducteur d'adresse réseau IP traditionnel (NAT traditionnel)).

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

2.2 Références informatives

[FIPS 186-2] FIPS PUB 186-2 (2000), *Digital Signature Standard* (Norme de signature numérique), *Department of Commerce, NIST*.

[RFC 347] IETF RFC 347 (1972), *Echo Process* (Traitement de l'écho).

[RFC 2663] IETF RFC 2663 (1999), *IP Network Address Translator (NAT) Terminology and Considerations* (Terminologie et considérations sur le traducteur d'adresse de réseau (NAT) IP).

[DOCSIS2] *Management Information Base for DOCSIS Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus*, draft-ietf-ipcdn-bpiplus-mib-01.txt (work in progress) (Base d'informations de gestion pour les modems-câble DOCSIS et les systèmes de terminaisons de câblo-modems pour la confidentialité de base améliorée) projet-ietf-ipcdn-bpiplus-mib-01.txt (travail en cours).

draft-ietf-ipcdn-bpiplus-mib-06 INTERNET DRAFT – DOCSIS Baseline Privacy Plus MIB – *Management Information Base for DOCSIS Cable Modems and Cable Modem Termination Systems for Baseline Privacy Plus*, Novembre 2001 (Base d'informations de gestion pour la confidentialité de base améliorée DOCSIS – Base d'informations de gestion pour les câblo-modems DOCSIS et les systèmes de terminaison de câblo-modems pour la confidentialité de base améliorée), novembre 2001.

[ID-IGMP] FENNER (W.) et al., *IGMP-based Multicast Forwarding ("IGMP Proxying")*, IETF Internet Draft, http://www.ietf.org/internet-drafts/draft-ietf-magma-igmp-proxy-00.txt (Transmission multidiffusion fondée sur le protocole IGMP ("Mandatement du protocole IGMP"), projet IETF Internet.

3 Termes et définitions

La présente Recommandation définit les termes suivants:

3.1 portail de sécurité de câble (CSP, *cable security portal*): élément fonctionnel qui fournit des fonctions de gestion de la sécurité et de traduction entre le coaxial HFC et l'utilisateur.

3.2 serveur de gestion d'appel (CMS, *call management server*): [IPCablecom] contrôle les connexions audio sur IPCablecom. Appelé aussi un agent d'appel dans la terminologie MGCP/SGCP.

3.3 qualité de service dynamique (DQoS, *dynamic quality of service*): [IPCablecom] allouée au fur et à mesure pour chaque communication selon la qualité de service requise.

3.4 adaptateur de terminal multimédia incorporé (E-MTA, *embedded multimedia terminal adapter*): [IPCablecom] nœud simple qui contient à la fois un adaptateur MTA et un câblo-modem.

3.5 câblo-modem IP amélioré: câblo-modem qui a été amélioré par l'ajout des dispositifs IP de la présente Recommandation.

3.6 service portail (PS, *portal service*): élément fonctionnel qui fournit des fonctions de gestion et de traduction entre le coaxial HFC et l'utilisateur.

3.7 appareil IP de réseau local: un appareil IP local est représentatif d'un appareil IP typique dont on s'attend à ce qu'il réside chez l'utilisateur et qui contient une pile TCP/IP ainsi qu'un DHCP client.

3.8 traverse: sous-fonction du portail CAP, la fonction de traverse fait passer sans changement les paquets du côté WAN-Data du portail CAP au côté LAN-Pass.

3.9 adaptateur de terminal multimédia autonome (S-MTA, *stand-alone multimedia terminal adapter*): nœud unique qui contient un adaptateur MTA et une commande MAC non-DOCSIS (par exemple, Ethernet).

4 Abréviations, acronymes et conventions

4.1 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ASP	mandataire spécifique de l'application (*application-specific proxy*)
CA	autorité de certification (*certificate authority*)
CAP	portail d'adresse câble (*cable address portal*)
CAT	traduction d'adresse câble (*cable address translation*)
CDC	client de protocole DHCP du câble (*cable DHCP client*)
CDP	portail de protocole DHCP du câble (*cable DHCP portal*)
CDS	serveur de protocole DHCP du câble (*cable DHCP server*)
CM	câblo-modem
CMP	portail de gestion du câble (*cable management portal*)
CMS	serveur de gestion d'appels (*call management server*)
CMTS	système de terminaison de câblo-modem (*cable modem termination system*)
C-NAPT	traduction d'adresse et de port de réseau câblé (*cable network address and port translation*)
C-NAT	traduction d'adresse de réseau câblé (*cable network address translation*)
CNP	portail de nommage du câble (*cable naming portal*)
CQoS	qualité de service du câble (*cable quality of service*)
CQP	portail de qualité de service du câble (*cable quality-of-service portal*)
CRL	liste de révocation de certificat (*certificate revocation list*)
CSP	portail de sécurité de câble (*cable security portal*)
CTP	portail d'essai du câble (*cableHome testing portal*)
CVC	certificat de vérification de code
CVS	signature de vérification de code (*code verification signature*)
CxP	sous-fonction de service portail sur le câble (*cable PS sub-function*)
DER	règles de codage distinctives (*distinguished encoding rules*)
DHCP	protocole de configuration de serveur dynamique (*dynamic host configuration protocol*)
DNS	système de nom de domaine (*domain name system*)
DOCSIS	spécification d'interface du service de transmission de données par câble (*data-over-cable service interface specification*)
DQoS	qualité de service dynamique (IPCablecom) (*dynamic quality of service (IPCablecom)*)
E-MTA	adaptateur de terminal multimédia incorporé (*embedded multimedia terminal adapter*)
FTP	protocole de transfert de fichiers (*file transfer protocol*)
FW	pare-feu (*firewall*)

GMT	temps moyen de Greenwich (*Greenwich mean time*)
HA	accès domestique (*home access*)
HEX	hexadécimal
HFC	hybride optique coaxial (*hybrid fiber coax*)
ICMP	protocole de message de commande Internet (*Internet control message protocol*)
IGMP	protocole de gestion de groupe Internet (*Internet group management protocol*)
IP	protocole Internet (*Internet protocol*)
KDC	centre de distribution de clé (*key distribution center*)
LAN-Pass	adresse LAN de traverse (*pass-through LAN address*)
LAN-Trans	adresse LAN traduite (*translated LAN address*)
MAC	commande d'accès au support (*media access control*)
MGCP	protocole de contrôle de passerelle média (*media gateway control protocol*)
MIB	base d'informations de gestion (*management information base*)
MPLS	commutation multiprotocolaire par étiquetage (*multiprotocol label switching*)
MSO	opérateur de services multiples (*multiple service operator*)
MTA	adaptateur de terminal multimédia (*multimedia terminal adapter*)
NAPT	traduction d'adresse et portail réseau (*network address and portal translation*)
NAT	traduction d'adresse de réseau (*network address translation*)
NCS	signalisation d'appel fondée sur le réseau (*network-based call signalling*)
NMS	système de gestion de réseau (*network management system*)
OID	identificateur d'objet (*object identifier*)
OSI	interconnexion des systèmes ouverts (*open system interconnection*)
OSS	système support d'exploitation (*operations support system*)
PDU	unité de données protocolaire (*protocol data unit*)
PING	groupeur interréseau de paquets (*packet inter-network grouper*)
PKI	infrastructure de clé publique (*public key infrastructure*)
PKINIT	authentification initiale par cryptographie à clé publique (*public-key cryptography for initial authentication*)
PS	service portail (*portal service*)
PS WAN-Data	interface de données de réseau WAN d'élément de service portail (*portal service element WAN data interface*)
PS WAN-Man	interface de gestion de réseau WAN d'élément de service portail (*portal service element WAN management interface*)
QS	qualité de service
RFC	demande de commentaires (*request for comments*)
RSA	Rivest, Shamir, Adleman
SHA-1	algorithme de hachage sécurisé n° 1 (*secure hash algorithm 1*)

S-MTA adaptateur autonome de terminal multimédia (*stand-alone multimedia terminal adapter*)

SNMP protocole simple de gestion de réseau (*simple network management protocol*)

SOA début de zone administrative (*start of authority*)

SPF filtrage de paquet d'après l'état (*stateful packet filtering*)

SYSLOG enregistrement système (*system log*)

TCP protocole de commande de transmission (*transmission control protocol*)

TFTP protocole trivial de transfert de fichiers (*trivial file transfer protocol*)

TLV type-longueur-valeur

UDP protocole datagramme d'utilisateur (*user datagram protocol*)

USFS commutation de transmission sélective de sens montant (*upstream selective forwarding switch*)

USM modèle de sécurité d'utilisateur (*user security model*)

UTC temps universel coordonné (*coordinated universal time*)

VACM modèle de commande d'accès fondé sur la vue (*view-based access control model*)

VoIP téléphonie utilisant le protocole Internet (*voice over Internet protocol*)

WAN réseau régional (*wide area network*)

WAN-Data secteur d'adresse de données de réseau régional (*wide area network data address realm*)

WAN-Man secteur d'adresse de gestion de réseau régional (*wide area network management address realm*)

4.2 Conventions

Pour l'implémentation de la présente Recommandation, les mots clés, "DOIT" et "REQUIS" sont à interpréter comme indiquant un aspect obligatoire de la présente Recommandation. Les mots clés, indiquant un certain niveau de signification d'exigences particulières, qui sont utilisés tout au long de la présente Recommandation, sont résumés ci-dessous.

"DOIT" Ce mot ou l'adjectif "REQUIS" signifie que l'élément est une exigence absolue de la présente Recommandation.

"NE DOIT PAS" Cette phrase signifie que l'élément est une interdiction absolue de la présente Recommandation.

"DEVRAIT" Ce mot ou l'adjectif "RECOMMANDÉ" signifie qu'il existe des raisons valables dans des circonstances particulières pour ignorer cet élément, mais il faut en comprendre toutes les implications et peser attentivement les choses avant de choisir une voie différente.

"NE DEVRAIT PAS" Cette phrase signifie qu'il peut exister des raisons valables dans des circonstances particulières, lorsque le comportement indiqué est acceptable ou même utile, mais il faut en comprendre toutes les implications et peser attentivement les choses avant d'implémenter tout comportement décrit avec cette mention.

"PEUT" Ce mot ou l'adjectif "FACULTATIF" signifie que cet élément est véritablement optionnel. Un vendeur peut choisir d'inclure l'élément parce qu'un marché particulier le requiert ou parce qu'il améliore le produit, par exemple, un autre vendeur peut omettre le même élément.

5 Exigences, architecture et aperçu général pour l'ensemble de caractéristiques IP

La présente Recommandation donne un ensemble de caractéristiques fondées sur IP qui peuvent être ajoutées à un câblo-modem qui permettra aux câblo-opérateurs de fournir un ensemble supplémentaire de services améliorés à leurs clients. Ces caractéristiques fondées sur IP résident dans un élément logique appelé service portail (PS ou simplement Portail). Un câblo-modem qui contient ces caractéristiques améliorées est désigné sous le nom de câblo-modem amélioré IP (IPCM, *IP-enhanced cable modem*), qui est une implémentation de la classe d'appareils HA de la Rec. UIT-T J.190. Comme décrit dans la Rec. UIT-T J.190, la classe d'appareils HA inclut à la fois la fonction de câblo-modem et la fonction de service portail.

Les domaines et caractéristiques majeurs sont les suivants:

– *gestion et approvisionnement*
  - gestion à distance et configuration du service portail;
  - mandataire de gestion simple pour les appareils fondés sur IP chez l'usager (par exemple, un ordinateur personnel);
  - approvisionnement automatique pour le service portail;

– *adressage et traitement de paquet*
  - traduction d'adresse une à une pour les appareils chez l'usager;
  - traduction d'une adresse en plusieurs pour les appareils chez l'usager;
  - adressage sans traduction pour les appareils chez l'usager;
  - serveur DNS simple dans le service portail;

– *qualité de service*
  - fonction de transport transparent pour les messages de qualité de service IPCablecom de/vers les applications IPCablecom compatibles;

– *sécurité*
  - authentification d'appareil de service portail;
  - messages de gestion sécurisés;
  - téléchargement sécurisé de fichiers de configuration et de logiciel;
  - qualité de service sécurisée sur la liaison HFC;
  - gestion à distance de pare-feu de service portail.

5.1 Architecture

Voir Figure 1.

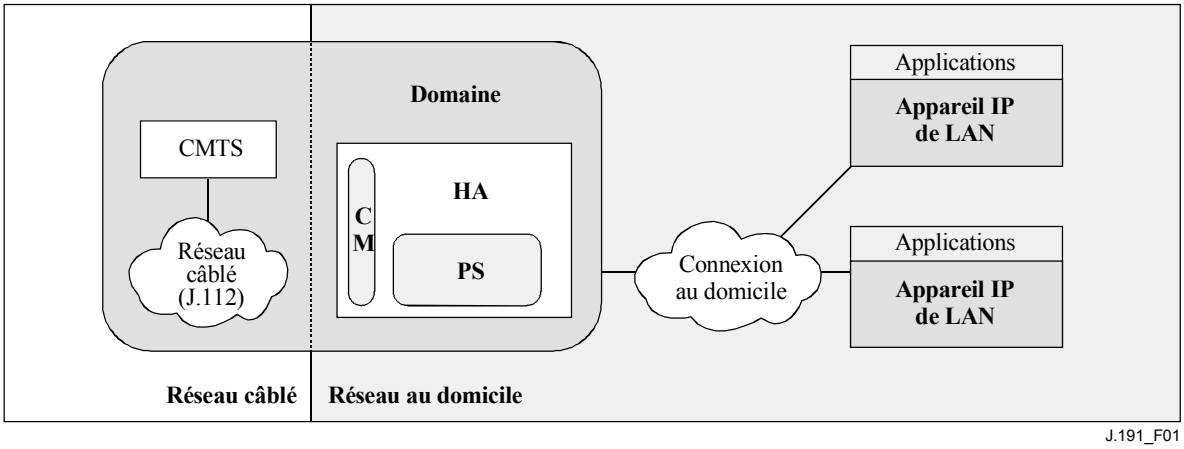

Figure 1/J.191 – Concepts clé

5.1.1 Service portail

Le service portail est un élément logique qui fournit des services de sécurité à l'usager et agrégé, de gestion, d'approvisionnement et d'adressage. Trois ensembles de fonction de service portail sont définis. Ce sont l'ensemble de fonction de gestion, l'ensemble de fonctions de qualité de service (QS) et l'ensemble de fonctions de sécurité. L'élément logique de service portail constitue la base de l'architecture de référence logique.

5.1.2 Secteurs d'adresse

Un secteur d'adresse se définit comme "un domaine réseau dans lequel l'adresse réseau est allouée de façon univoque aux entités de telle sorte que les datagrammes puissent leur être acheminées" [RFC 2663]. Dans la présente Recommandation, les secteurs d'adresse entrent dans les deux catégories de secteurs d'adresse WAN et de secteurs d'adresse LAN (voir Figure 2).

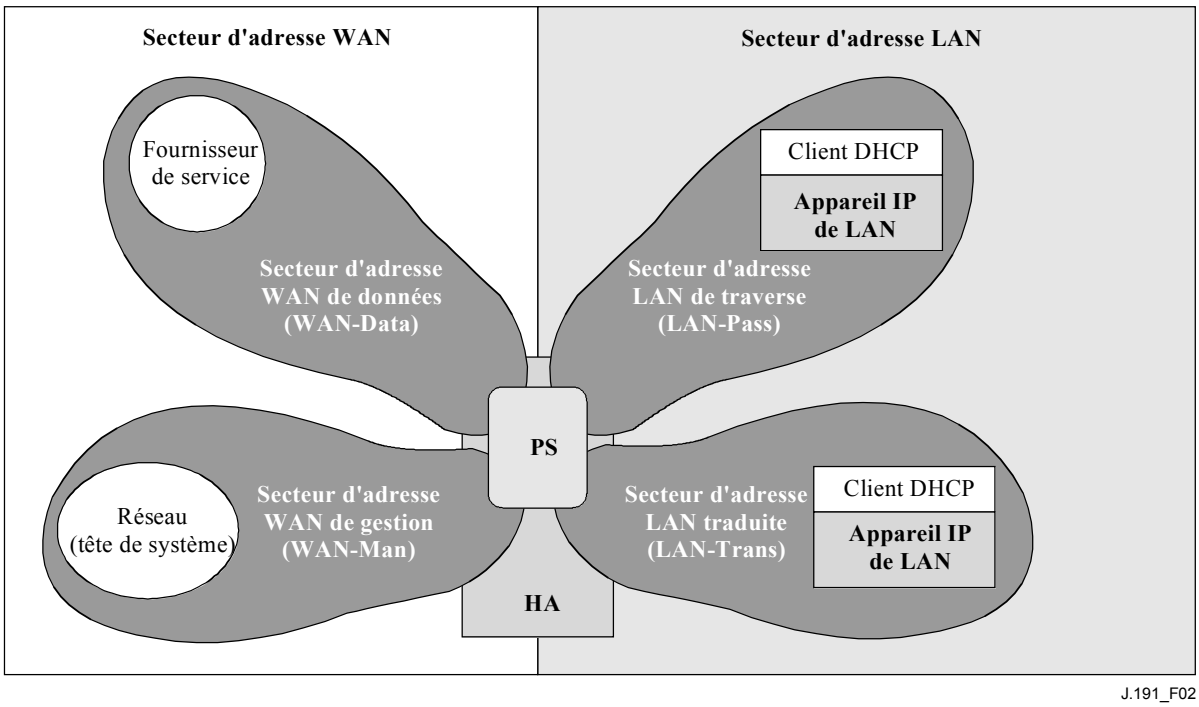

Figure 2/J.191 – Secteurs d'adresses

Les adresses WAN résident dans un des deux secteurs suivants: le secteur d'adresse WAN de gestion (WAN-Man, *wide area network management address realm*) ou le secteur d'adresse WAN de données (WAN-Data, *wide area network data address realm*). Les adresses LAN résident aussi dans l'un des deux secteurs suivants: secteur d'adresse LAN de traverse (LAN-Pass, *pass-through LAN address*) ou secteur d'adresse LAN traduite (LAN-Trans, *translated LAN address*). Les propriétés de ces secteurs d'adressage sont décrites ci-dessous:

- le secteur d'adresse WAN de gestion (WAN-Man) est destiné à transporter du trafic de gestion de réseau sur le réseau câblé entre le système de gestion du réseau et l'élément de service portail. En principe, les adresses de ce secteur résideront dans l'espace privé d'adresse IP;
- le secteur d'adresse WAN de données (WAN-Data) est destiné à transporter du trafic d'application d'usager sur le réseau câblé et au-delà, comme le trafic entre appareils IP de LAN et des hôtes Internet. En principe, les adresses de ce secteur résideront dans l'espace public d'adresse IP;
- le secteur d'adresse LAN traduite (LAN-Trans) est destiné à transporter du trafic d'application d'usager et du trafic de gestion sur le réseau interne entre les appareils IP du LAN et le service portail. En principe, les adresses de ce secteur résideront dans l'espace privé de l'adresse IP, et peuvent en principe être réutilisées par les abonnés;
- le secteur d'adresse LAN de traverse (LAN-Pass) est destiné à transporter du trafic d'application d'usager, comme du trafic entre appareils IP de LAN et hôtes Internet, sur la liaison interne, sur le réseau câblé, et au-delà. En principe, les adresses de ce secteur résideront dans l'espace public d'adresse IP.

Du côté du LAN, les adresses dans le secteur d'adresse LAN de traverse (LAN-Pass) sont directement extraites de l'adresses dans le secteur d'adresse WAN de données. Celles-ci sont utilisées par les appareils IP de LAN et des applications telles que les services IPCablecom qui n'acceptent pas la traduction d'adresse et exigent une adresse IP acheminable globalement. De plus, sur le côté LAN, les appareils IP de LAN peuvent utiliser des adresses traduites venant du secteur d'adresse LAN traduite (LAN-Trans).

5.2 Fonctions de gestion

Trois classes de fonctions de gestion sont définies pour le support de l'approvisionnement et de la gestion des appareils IP de LAN:

- fonctions de gestion serveur;
- fonctions de gestion client;
- fonctions de gestion de service portail.

Plusieurs des fonctions de gestion serveur résident au sein de la tête de système (HE, *headend*). Les fonctions de gestion client se trouvent en principe au sein des appareils IP de LAN. Les fonctions de portail de service de gestion se situent au sein de l'élément logique service portail du câblo-modem et peuvent inclure des fonctionnalités de serveur, de client, et de relais pour agréger les messages traduits entre la tête de système et les appareils IP de LAN. Des exemples de fonctions de serveur de gestion, de service portail et de client introduites dans les Tableaux 1, 2, et 3 sont illustrées à la Figure 3.

Tableau 1/J.191 – Description de la fonction de serveur de gestion

Fonctions de serveur de gestion	Description
Serveur DHCP de tête de système	Le serveur DHCP est un composant de tête de système qui fournit les informations d'adresse pour les secteurs d'adresse WAN-Man et WAN-Data au service portail.
Serveur DNS de tête de système	Le serveur DNS de tête de système est un composant de l'arrière qui sert à assurer le mappage entre les noms de domaine ASCII et les adresses IP.
Serveur de message de gestion de tête de système	Ce sont les serveurs de message de gestion de tête de système, de téléchargement, de notification d'événement, y compris les protocoles tels que SNMP, SYSLOG, et TFTP.

Tableau 2/J.191 – Description de la fonction de service portail de gestion et d'approvisionnement

Fonctions de portail de gestion	Description
Portail d'adresse câble (CAP, *cable address portal*)	Au sein du PS, le portail CAP interconnecte les secteurs d'adresse WAN et LAN pour le trafic de données. (Voir CAT/traverse).
Traduction d'adresse câble (CAT, *cable address translation*)	Sous-fonction du portail CAP, une CAT traduit les adresses sur le côté WAN-Data du CAP en adresses au sein d'un sous-réseau logique unique du côté LAN-Trans.
Traverse	Sous-fonction du portail CAP, la fonction traverse transmet inchangés les paquets du côté WAN-Data du CAP au côté LAN-Pass.

Tableau 2/J.191 – Description de la fonction de service portail de gestion et d'approvisionnement

Fonctions de portail de gestion	Description
Portail de gestion câble (CMP, *cable management portal*)	Fonction qui fournit des interfaces entre la tête de système et la base de données du service portail.
Portail DHCP câble (CDP, *cable DHCP portal*)	Fonctions d'information d'adresse (par exemple, celles transmises via DHCP) incluant un serveur pour le secteur LAN et un client pour les secteurs WAN.
Portail de nommage câble (CNP, *cable naming portal*)	Le portail CNP fournit un service DNS simple pour les appareils IP de LAN qui nécessitent des services de nommage.
Portail d'essai câble (CTP, *cableHome testing portal*)	Le portail CTP fournit des moyens à distance pour initialiser des pings et des bouclages au sein du LAN.

Tableau 3/J.191 – Description de la fonction gestion client

Fonctions de gestion client	Description
Client DHCP d'appareil IP de LAN	La fonction client DHCP sur le câble est un composant chez l'abonné utilisé pendant le processus d'approvisionnement d'appareil IP de LAN pour demander de façon dynamique les adresses IP et les autres informations de configuration d'élément logique.
Répondeur de bouclage d'appareil IP de LAN	Au sein d'un appareil IP de LAN, le répondeur de bouclage renvoie en boucle les données originaires de la fonction de bouclage du portail CTP à la fonction de bouclage du portail CTP.

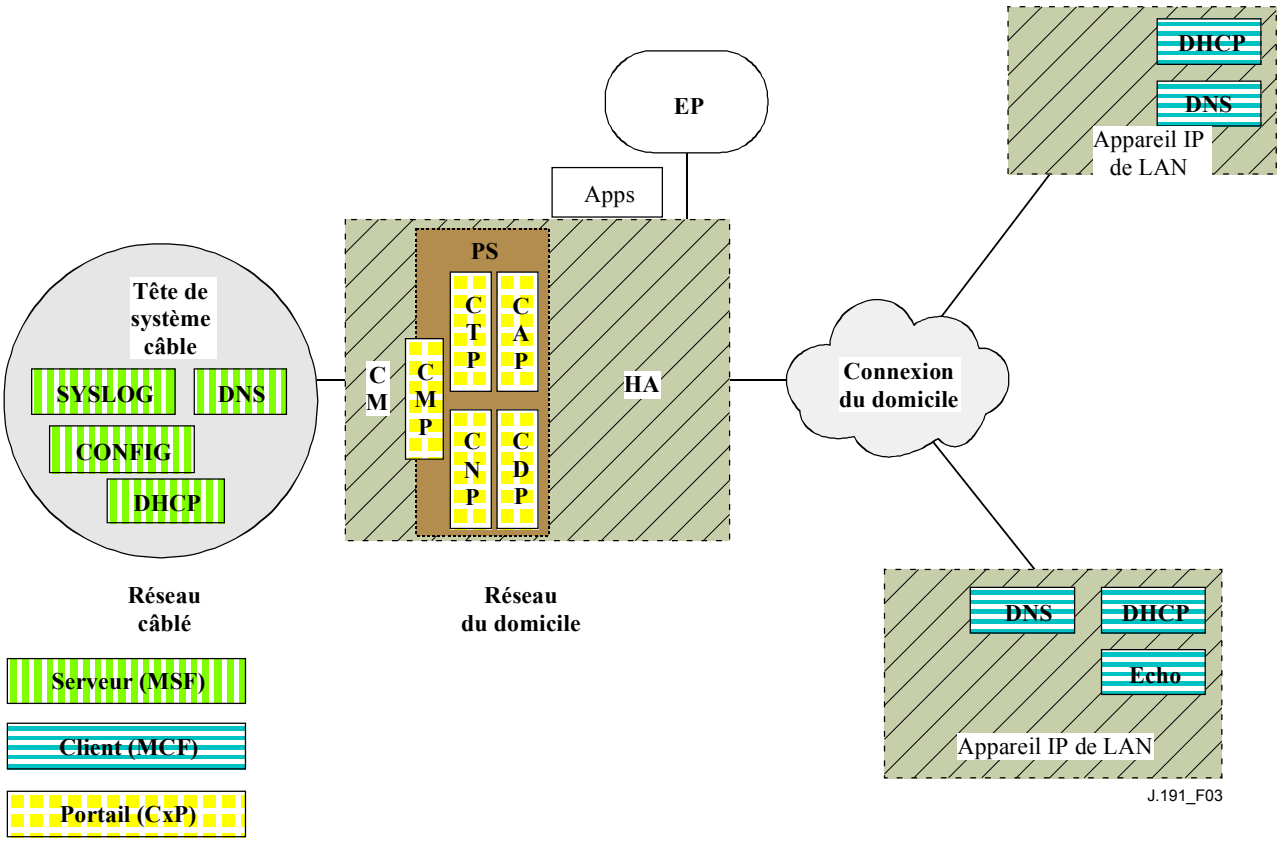

Figure 3/J.191 – Relations de gestion client-serveur

5.3 Fonctions de sécurité

Les fonctions de sécurité rentrent dans les catégories fonctions portail de sécurité ou fonctions serveur de sécurité. Les relations entre les différents éléments de sécurité et leur classification comme fonctions portail ou serveur sont présentées à la Figure 4 et aux Tableaux 4 et 5.

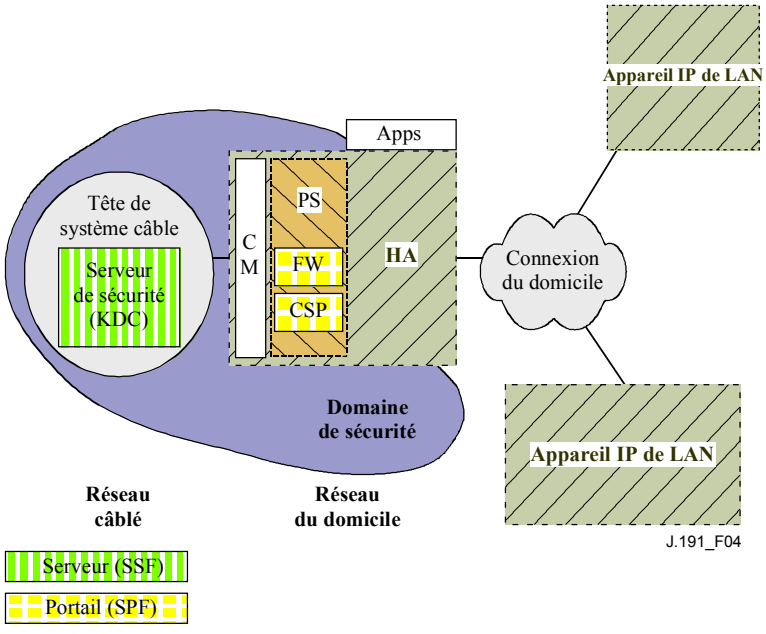

Figure 4/J.191 – Eléments de sécurité

Tableau 4/J.191 – Description de la fonction portail de sécurité

Fonctions portail de sécurité	Description
Portail de sécurité de câble (CSP, *cable security portal*)	Le CSP agit comme un portail pour matériel de sécurité pour toutes les autres fonctions de sécurité au sein du service portail. Le portail CSP communique sur le côté WAN avec le serveur de sécurité (centre de distribution de clé, KDC).
Pare-feu (FW, *firewall*)	Le pare-feu protège l'environnement IP de l'usager contre les attaques malignes.

Tableau 5/J.191 – Description de la fonction serveur de sécurité

Fonctions serveur de sécurité	Description
KDC	Dans la tête de système, les serveurs KDC fournissent les services d'authentification et de distribution de clé pour l'usager. Ils communiquent avec la fonction CSP à l'établissement de ces services.

5.4 Fonctions de qualité de service

L'architecture de qualité de service se compose d'une entité fonctionnelle simple fondée sur le service portail appelée portail de qualité de service du câble (CQP, *cable QoS portal*). Le portail CQP fournit un transport transparent de la messagerie de qualité de service entre les applications IPCablecom et l'infrastructure de qualité de service IPCablecom sur le réseau câblé.

5.5 Modèle d'interface de message

Les communications entre les fonctions dans les éléments de réseau et les appareils IP de LAN se produisent sur les interfaces de messagerie. Les types d'interfaces de messagerie sont différentiés par les éléments impliqués dans la communication. Les interfaces de messagerie sont illustrées à la Figure 5.

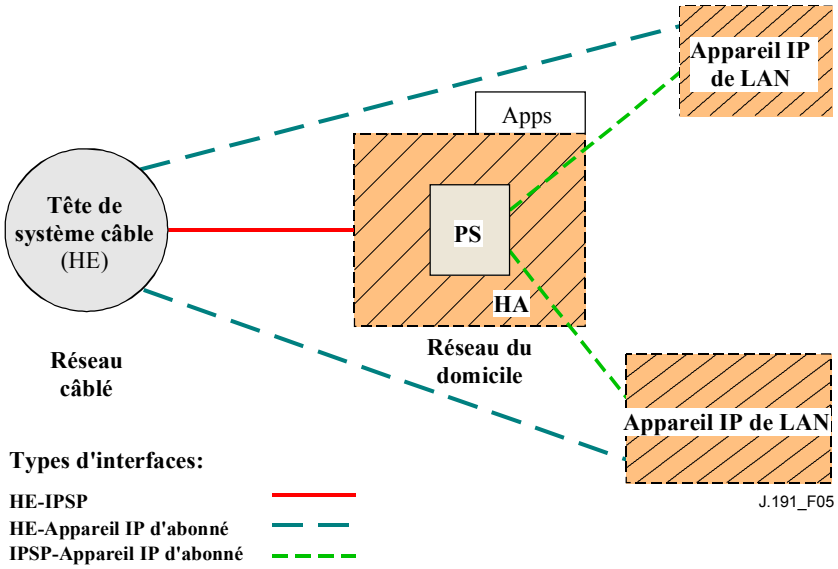

Figure 5/J.191 – Interfaces de référence

Les interfaces de messagerie sont récapitulées au Tableau 6.

Tableau 6/J.191 – Chemins d'interface valables pour chaque fonctionnalité

Fonction	Protocole	Interface		
		HE-PS	HE-LAN IP Dev	PS-LAN IP Dev
Service de nommage	DNS	Non spécifié	Non spécifié	Non spécifié
Téléchargement de logiciel	TFTP	La présente Recommandation	Non spécifié	Non spécifié
Acquisition d'adresse	DHCP	La présente Recommandation	Non spécifié	La présente Recommandation
Gestion			Non spécifié	Non spécifié
(simple)	SNMP	La présente Recommandation		
(en gros)	TFTP	La présente Recommandation		
Notification d'événement	SNMP	La présente Recommandation	Non spécifié	Non spécifié
	SYSLOG	La présente Recommandation		
QS	Protocoles de QS IPCablecom	Non spécifié	IPCablecom	Non spécifié
Sécurité (distribution de clé)	Kerberos	La présente Recommandation	Non spécifié	Non spécifié
Sécurité (authentification)	Kerberos	La présente Recommandation	Non spécifié	Non spécifié
Ping	ICMP	La présente Recommandation	Non spécifié	La présente Recommandation
Bouclage/Echo	UDP/TCP	Non spécifié	Non spécifié	La présente Recommandation

5.6 Modèle de référence d'information

Le fonctionnement du modèle de gestion se fonde sur un stockage de l'information entretenu dans le portail par les diverses fonctions du portail (CAP, CDP, CMP, etc.). Ces fonctions doivent avoir le moyen d'interagir via l'échange d'informations, et la base de données du portail est une entité conceptuelle qui représente le magasin de ces informations. La base de données du portail n'est pas en soi une base de donnée spécifiée réelle, mais plutôt un outil pour aider à comprendre quelles informations sont échangées entre les divers éléments.

La Figure 6 montre les relations entre la base de données et les fonctions de portail, le Tableau 7 décrit les informations typiques associées à chacune de ces fonctions. La Figure 7 donne un exemple détaillé de l'implémentation indiquant l'ensemble des informations, les fonctions d'où découlent les informations, et les relations entre les fonctions et les informations.

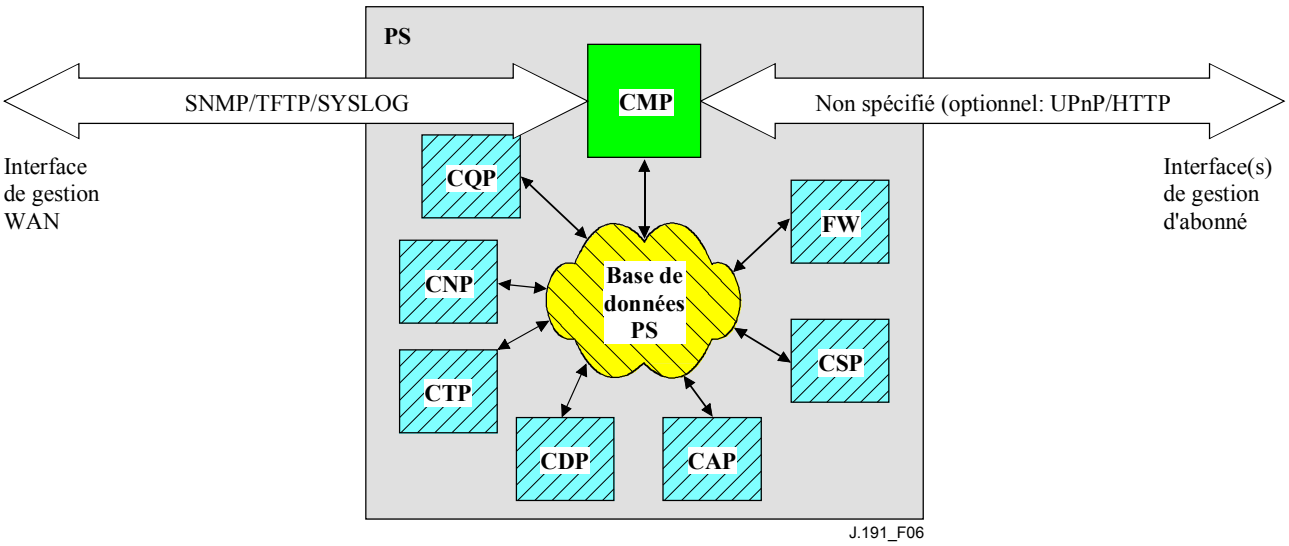

Figure 6/J.191 – Relations entre fonction portail et base de données de service portail

La base de données portail emmagasine une multitude de relations de données. Le CMP fournit l'interface de gestion WAN (SNMP) à la base de données du portail. Les fonctions au sein du portail entrent et révisent les relations des données dans la base de données du portail. De plus, les fonctions au sein du portail peuvent restaurer les informations en provenance de la base de données du portail qui sont entretenues par d'autres fonctions au sein du portail.

Tableau 7/J.191 – Exemples typiques d'informations de base de données de portail

Nom	Usage (en général)
Information CDP	Informations associées aux adresses acquises et allouées via DHCP
Information CAP	Informations associées aux mappages de traduction d'adresses
Information CMP	Informations associées à l'état des fonctions de gestion
Information CTP	Informations associées aux résultats des essais de LAN effectués par le CMP
Information CNP	Informations associées à la résolution de nom d'appareil IP de LAN
Information USFS	Informations associées à la fonction de commutateur de transmission sélective de sens montant
Information CSP	Informations associées à l'authentification, l'échange de clés, etc.
Information de pare-feu	Informations associées au comportement du pare-feu (ensemble de règles) et à la connexion du pare-feu
Information d'événement	Informations associées à la connexion locale pour tous les événements généraux, interruptions, etc.

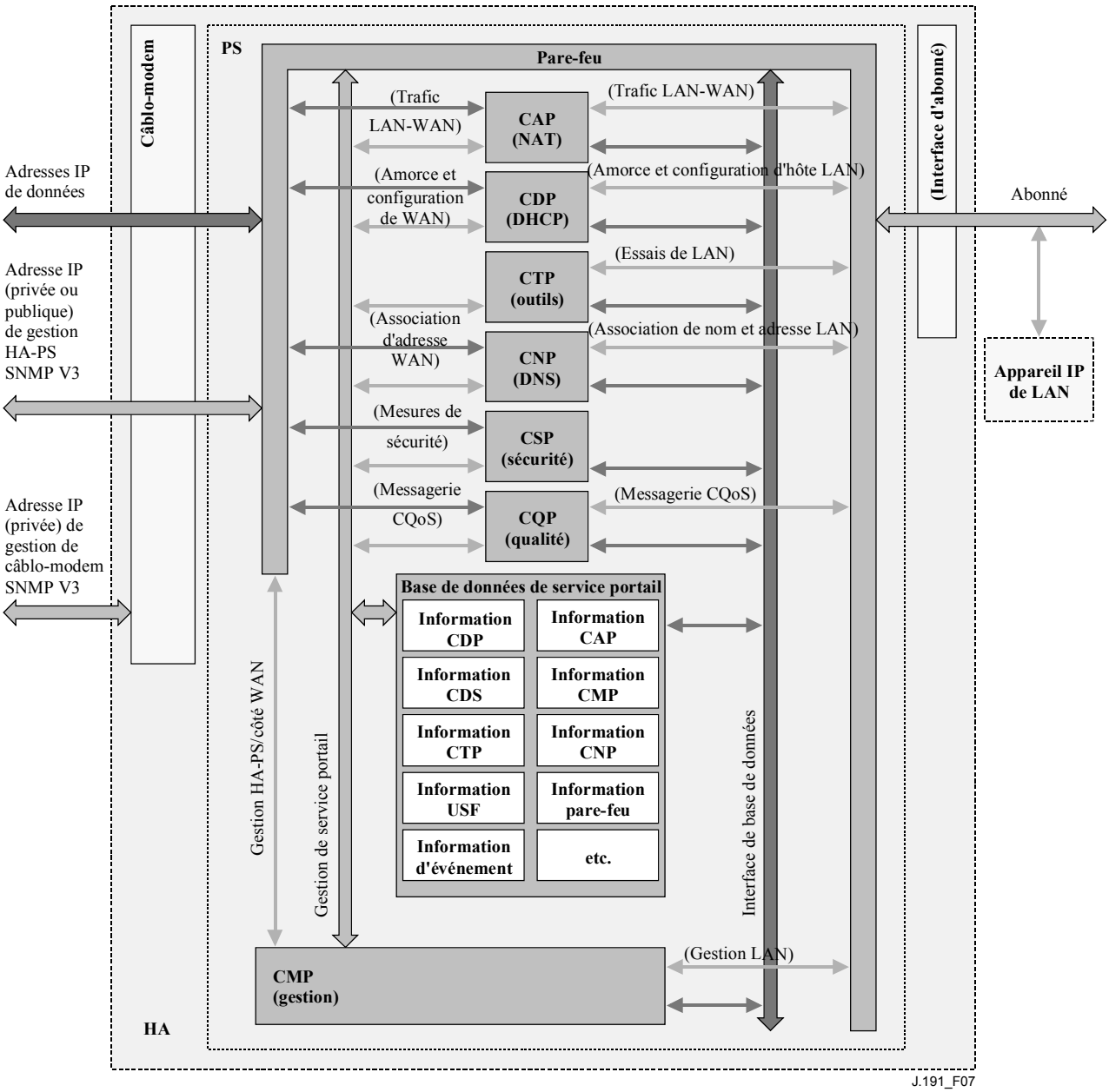

Figure 7/J.191 – Exemple détaillé d'implémentation de base de données de portail

Le portail est géré à partir du WAN via le portail CMP, et dans une large mesure, cela implique l'accès aux informations de la base de données du portail. La gestion sert à l'initialisation et à l'approvisionnement des éléments de réseau du côté du WAN, et aux diagnostics ou aux états du côté LAN. Les diagnostics peuvent s'appuyer sur le portail CTP pour obtenir une meilleure visibilité sur l'état en cours du LAN. On peut mesurer la connectivité et des performances rudimentaires du réseau.

Le portail CNP est le gestionnaire du système de dénomination de domaine (DNS, *domain name system*) du LAN. Tous les appareils IP de LAN LAN-Trans sont configurés par le portail CDP pour qu'ils utilisent le portail CNP comme serveur de nommage primaire. Le portail CNP résout les noms d'hôtes textuels des appareils IP de LAN, retourne leurs adresses IP correspondantes et en plus, renvoie les appareils IP de LAN sur des serveurs DNS externes pour les demandes auxquelles les informations locales ne permettent pas de répondre. Le portail CNP ne répond qu'aux interrogations de serveur DNS sur le secteur du LAN-Trans.

Le portail CDP contient les fonctions d'adresse nécessaires pour servir de support au serveur DHCP dans le secteur LAN-Trans et un client DHCP dans les secteurs de WAN.

Le portail CAP crée des mappages de traduction d'adresse entre les secteurs d'adresse WAN-Data et LAN-Trans. Le portail CAP est aussi responsable des décisions de commutation de transmission sélective de sens montant pour préserver la largeur de bande du canal de sens montant du réseau HFC (WAN) du seul trafic du LAN local. Enfin, le portail CAP contient la fonction de traverse, qui relie le trafic entre les secteurs d'adresse du LAN et du WAN.

Le CSP fournit les capacités d'authentification de portail ainsi que les activités d'échange de clés.

Le portail CQP fait partie d'un système qui permet la qualité de service (QS) IPCablecom à travers le portail. Le portail CQP, agissant comme un pont transparent, transmet les messages de qualité de service conformes à IPCablecom entre applications IPCablecom et l'infrastructure de qualité de service IPCablecom.

L'implémentation du pare-feu est spécifique, et la présente Recommandation ne spécifie pas les détails de l'implémentation du pare-feu.

5.7 Modèles de fonctionnement

Cette infrastructure améliorée se fonde sur une infrastructure de câblo-modem pour permettre les services traditionnels, et incorporer un certain nombre de fonctionnalités qui sont semblables à celles existant au sein d'un système d'approvisionnement IPCablecom.

Pour les besoins de la configuration, le portail peut fonctionner dans l'un des deux modes d'approvisionnement:

- le mode d'approvisionnement DHCP;
- le mode d'approvisionnement SNMP.

Lorsque le service portail fonctionne dans le mode d'approvisionnement DHCP, il peut fonctionner dans l'un des deux sous-modes de gestion de réseau:

- mode NmAccess;
- mode coexistence.

La Figure 8 illustre les divers modes de fonctionnement du service portail ainsi que les déclenchements qui leurs sont associés.

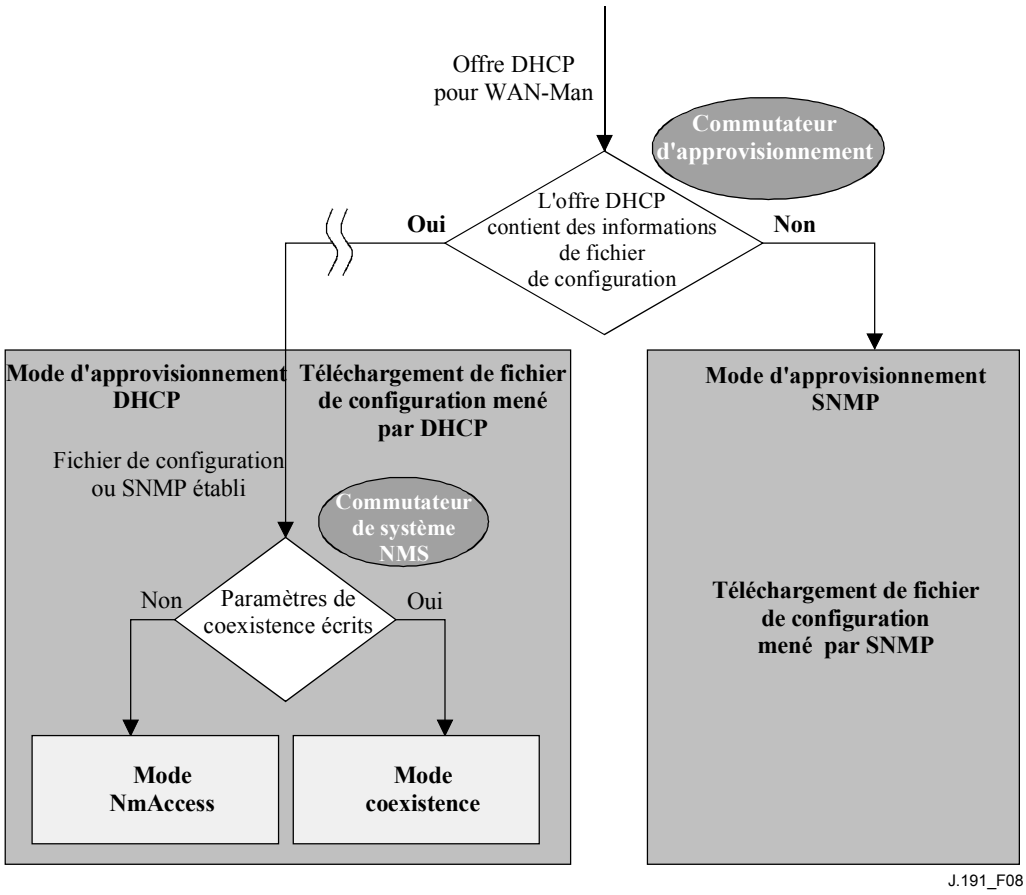

Figure 8/J.191 – Modes de fonctionnement de portail

Si les informations du fichier de configuration du portail (localisation du serveur et nom de fichier) sont fournies au portail dans le DHCP OFFER produit par le serveur DHCP du réseau câblé, le portail fonctionnera en mode d'approvisionnement DHCP. Lorsqu'il est en mode d'approvisionnement DHCP, le portail peut fonctionner dans un des deux modes de gestion de réseau (NmAccess et coexistence). Dans le mode d'approvisionnement DHCP, le portail fonctionnera en mode de gestion de réseau NmAccess par défaut, mais peut être configuré par le système NMS pour fonctionner en mode coexistence.

Si les informations du fichier de configuration du portail ne sont pas fournies au portail dans le DHCP OFFER produit par le serveur DHCP du réseau câblé, le portail fonctionnera en mode d'approvisionnement SNMP. Lors du fonctionnement en mode d'approvisionnement SNMP, les informations et déclenchements pour le téléchargement du fichier de configuration du portail sont fournis par le système NMS via des messages SNMP. A la différence du mode d'approvisionnement DHCP, le comportement de gestion de réseau ne change pas dans ce mode.

Le Tableau 8 décrit les fonctionnalités affectées par chaque mode de fonctionnement décrit ci-dessus.

Tableau 8/J.191 – Infrastructures de portail

Mode	Fonctionnalité directement affectée
Mode d'approvisionnement SNMP	Téléchargement du fichier de configuration
Mode d'approvisionnement DHCP	Téléchargement du fichier de configuration
Mode d'approvisionnement DHCP: mode NmAccess	Version SNMP utilisée entre NMS et PS
Mode d'approvisionnement DHCP: mode coexistence	Version SNMP utilisée entre NMS et PS

Ces divers modes de fonctionnement sont destinés à répondre aux besoins d'infrastructures variées du point de vue du serveur de l'arrière, y compris diverses versions du protocole SNMP, et divers types de serveurs de sécurité. On trouvera des précisions aux § 13.1 à 13.3.

6 Outils de gestion

6.1 Introduction/Aperçu général

Les outils de gestion donnent au câblo-opérateur les fonctionnalités permettant de gérer et configurer le portail IPService, ainsi que d'effectuer les diagnostics à distance sur les appareils IP de LAN. Le présent paragraphe décrit et spécifie les exigences pour ces fonctionnalités.

6.1.1 Objectifs

Les objectifs des outils de gestion comportent:

- fournir aux câblo-opérateurs la visibilité sur les appareils IP de LAN;
- fournir aux câblo-opérateurs un ensemble minimal d'outils de diagnostic qui leur permettront de vérifier la connectivité entre les éléments de service portail et tout outil IP de LAN dans le secteur d'adresse LAN-Trans;
- fournir aux câblo-opérateurs l'accès, via les bases MIB, aux données internes de l'élément de service portail et permettre au câblo-opérateur de surveiller les paramètres spécifiés et de configurer ou reconfigurer les fonctionnalités spécifiées en tant que de besoin;
- fournir les moyens de faire rapport sur les exceptions et autres événements sur la formes des traps du protocole SNMP, des messages à un enregistrement local, ou des messages à un enregistrement système (SYSLOG) dans le réseau câblé.

6.1.2 Hypothèses

Parmi les hypothèses sur l'environnement de gestion de réseau figurent:

- que les appareils compatibles implémentent la suite de protocoles du protocole Internet (IP);
- que SNMP soit utilisé pour l'échange de messages de gestion entre le système NMS du réseau câblé et le portail IPService dans le câblo-modem. SNMP donne la visibilité au système NMS sur les interfaces du portail, via l'accès aux données internes du portail, par l'intermédiaire des bases MIB nécessaires;
- que n'importe laquelle des v1/v2c/v3 du protocole SNMP puisse être utilisée comme protocole de gestion entre le système NMS et le service portail;
- que les appareils IP de LAN implémentent un DHCP client;

- que les informations acquises au travers de l'échange de messages DHCP DISCOVER, DHCP REQUEST, et DHCP OFFER échangés entre le service portail et les appareils IP de LAN, et les informations disponibles en provenance de la base de données du service portail à travers la base MIB de groupe d'interfaces soient suffisantes pour procurer au câblo-opérateur les connaissances nécessaires sur les appareils IP du LAN;
- que l'élément PS et les appareils IP de LAN acceptent le protocole ICMP;
- que l'utilitaire PING fournisse des fonctionnalités suffisantes pour donner au câblo-opérateur les informations nécessaires sur la connectivité entre l'élément PS et les appareils IP de LAN.

6.2 Architecture de gestion

6.2.1 Lignes directrices pour la conception du système

La liste des lignes directrices pour la conception du système d'outils de gestion figure au Tableau 9. Cette liste donne des indications pour le développement des spécifications des outils de gestion.

Tableau 9/J.191 – Lignes directrices pour la conception du système d'outils de gestion

Référence	Lignes directrices pour la conception du système d'outils de gestion
Mgmt 1	Le PS implémentera SNMPv1/v2c/v3 pour fournir l'accès aux données internes du PS.
Mgmt 2	Le PS sera capable de produire une commande Ping du protocole ICMP à tout appareil IP de LAN spécifié dans le secteur LAN-Trans à destination du système NMS du réseau câblé et d'emmagasiner les résultats dans la base de données du PS. Les résultats des essais Ping à distance sont accessibles par les objets de base MIB de CTP cabhCtpPingStatus, cabhCtpPingNumSent, et cabhCtpPingNumRecv.
Mgmt 3	Le PS sera capable d'exécuter un essai de vitesse de connexion avec un appareil IP de LAN spécifié dans le secteur LAN-Trans à destination du système NMS du réseau câblé et d'emmagasiner les résultats dans la base de données du PS.
Mgmt 4	L'élément PS sera capable de faire rapport sur les événements.

6.2.2 Description du système de gestion des outils

Comme indiqué à la Figure 9, l'architecture des outils de gestion comporte les composants suivants:

1) le portail de gestion du câble (CMP, *cable management portal*);
2) le portail d'essai du câble (CTP, *cableHome testing portal*);
3) un mécanisme de rapport d'événements au sein du CMP;
4) un système de gestion réseau (NMS, *network management system*) du protocole SNMP qui fait partie du réseau câblé.

Le système NMS du réseau câblé surveille et configure le service portail en accédant à la base de données du PS à travers les bases MIB spécifiées au § 6.3.7. Le système NMS peut aussi communiquer directement avec les appareils IP de LAN dans le secteur LAN-Pass.

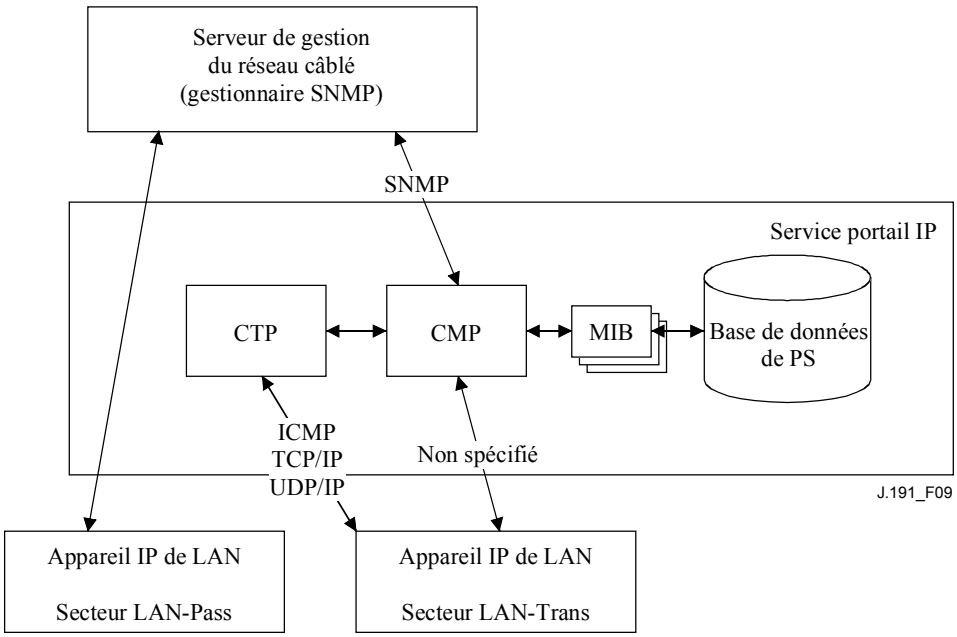

Figure 9/J.191 – Architecture de gestion

Les éléments fonctionnels CMP et CTP résident au sein du service portail.

Le câblo-modem et le PS sont des entités de gestion séparées et indépendantes, et il n'y a pas de partage de données entre câblo-modem et PS, sauf dans le cas de téléchargement de copie de logiciel vers un service portail. On accède aux objets docsDevSoftware du câblo-modem pour établir, initialiser et surveiller le téléchargement d'une copie logicielle en combinaison simple. A cause de cette indépendance de gestion, le câblo-modem et le service portail DOIVENT répondre à des adresses IP de gestion différentes et indépendantes. Les objets de base MIB du câblo-modem ne sont visibles que lorsque le gestionnaire y accède par l'adresse IP de gestion du câblo-modem, et ils ne sont pas visibles via l'adresse IP de gestion du service portail (et vice versa). Les droits d'accès du protocole SNMP aux entités PS et câblo-modem doivent être établies indépendamment. Ceci n'empêche pas d'utiliser un agent SNMP unique.

L'élément de service portail accepte les protocoles SNMPv1, SNMPv2c, et SNMPv3. Le § 5.7 introduit les deux modes d'approvisionnement acceptés par un élément de service portail et le paragraphe 7 donne des détails supplémentaires sur ces modes. Le mode d'approvisionnement dans lequel le service portail fonctionne de façon partielle détermine quelle version du protocole SNMP est utilisée par le service portail. Des détails supplémentaires figurent au § 6.3.3.

6.3 Le portail de gestion câble (CMP)

Le portail de gestion câble (CMP) existe au sein du PS. Il sert de centre d'activité de contrôle de gestion pour les accès de gestion du côté WAN. Le portail CMP agrège et interconnecte les informations de gestion dans les secteurs WAN-Man et LAN-Trans parce qu'ils ne sont pas directement accessibles l'un à l'autre.

6.3.1 Objectifs du CMP

Parmi les objectifs du portail de gestion câble figurent:

- permettre de voir et mettre à jour les informations de configuration du portail d'adresse câble (CAP);
- permettre de voir et mettre à jour les informations de configuration du pare-feu;

- permettre un Ping à distance pour les appareils IP de LAN dans le secteur LAN-Trans, via le portail d'essai du câble (CTP);
- permettre de voir les informations d'appareil IP de LAN obtenues via le portail DHCP câble (CDP);
- permettre de voir les résultats de la surveillance des performances d'appareil IP de LAN effectuée par le portail d'essai câble (CTP);
- permettre l'accès à d'autres paramètres de configuration de service portail;
- traiter en gros les commandes SNMP passées du système NMS de réseau câblé dans un fichier de configuration de service portail;
- faciliter la sécurité en donnant accès aux paramètres de sécurité, et par l'utilisation de SNMPv1/v2c/ v3 dans le mode de gestion approprié;
- donner la capacité de désactiver des segments de LAN.

6.3.2 Lignes directrices de la conception du portail CMP

La liste des lignes directrices de la conception du portail CMP figurent dans le Tableau 10. Cette liste donne des indications pour la spécification des fonctions du CMP.

Tableau 10/J.191 – Lignes directrices de la conception du CMP

Référence	Lignes directrices de la conception du système CMP
CMP 1	Les interfaces devront accepter les caractéristiques et fonctions de gestion et de diagnostic nécessaires pour le traitement des services fondés sur le câble fournis au domicile.
CMP 2	La perte de connexion entre le ou les fournisseurs de service à haut débit et l'appareil IP amélioré ne devra pas causer l'interruption ou la dégradation du fonctionnement d'autres fonctions internes au domicile.
CMP 3	Le service portail se rétablira de lui-même après une coupure de courant, et les appareils connectés au service portail doivent revenir à l'état opérationnel où ils étaient avant la coupure.
CMP 4	Les appareils devront être faciles à installer et à configurer pour le fonctionnement, comme les applications destinées aux particuliers.

6.3.3 Description du système CMP

Comme indiqué auparavant, le portail CMP sert de centre d'activité du contrôle de gestion pour les accès de gestion du côté WAN et il agrège et interconnecte les informations pour la gestion de la gestion WAN et des éléments de réseau de LAN.

Le portail CMP travaille dans les trois modes de gestion du réseau.

Comme décrit au § 5.7, lorsque le service portail se trouve en mode d'approvisionnement SNMP, il fonctionne en utilisant:

1) le protocole SNMPv3;
2) le soutien à USM et VACM;
3) utilise Kerberos pour distribuer le matériel de chiffrement.

Comme décrit au § 5.7, lorsque le service portail se trouve en mode d'approvisionnement DHCP, il peut fonctionner dans l'un des deux autres modes de gestion du réseau, mode NmAccessTable et mode coexistence. En mode NmAccessTable, l'accès de gestion est sous le contrôle de NmAccessTable de la norme [RFC 2669] et les protocoles SNMPv1/v2c sont acceptés. Dans le mode coexistence, l'accès de gestion est commandé comme décrit dans [RFC 2576], les protocoles SNMPv1/v2c/v3 sont acceptés, USM et VACM sont possibles, et le matériel de chiffrement

SNMPv3 est distribué en utilisant [RFC 2786] et les TLV dans le fichier de configuration du service portail.

Le Tableau 11 contient les définitions des termes spécifiques du portail CMP.

Tableau 11/J.191 – Définition des termes

Contrôle de gestion	Accès en lecture ou en écriture à un ensemble de paramètres qui contrôlent ou surveillent le comportement du service portail.
Base de données PS	Ensemble de paramètres qui contrôlent ou surveillent le comportement du service portail par le système de gestion du WAN. Il peut être conçu comme un dépôt d'informations décrivant l'état actuel du service portail.
Utilisateur	Comme défini dans le protocole SNMP [RFC 2574, section 2.1], un utilisateur a un nom associé, des définitions de sécurité associées et l'accès à une vision.
Vision	Une vision est un ensemble d'objets de base MIB et les droits d'accès à ces objets. Chaque vision a un nom et est associée à un utilisateur [RFC 2575, section 2.4].
Autorisation ultime	Autorité unique qui établit, modifie, ou supprime les identifiants d'utilisateur, les clés d'authentification, les clés de chiffrement et les droits d'accès à la base de données du service portail. L'autorisation ultime PEUT être commutée entre un utilisateur dans le système NMS du réseau câblé et un utilisateur à domicile, mais NE DEVRAIT PAS être chez les deux à la fois. Cet utilisateur est responsable de toutes les opérations de gestion de la sécurité.
Utilisateur de maintenance	Utilisateur qui n'effectue en principe que des opérations en lecture seule sur la base de données du service portail. Ceci est surtout utilisé pour effectuer la surveillance et la comptabilité.
Utilisateur administrateur	Utilisateur qui effectue en principe à la fois des opérations de lecture et d'écriture sur la base de données du service portail. Ces opérations servent à la configuration et la gestion des fautes.

Parmi les exemples de types d'informations manipulées via le contrôle de gestion sur le câble figurent l'établissement des politiques de pare-feu, les mappages des traductions NAT configurées selon le système NMS, l'initialisation d'outils de diagnostic à distance et l'accès aux résultats, l'état du service portail, et la configuration du champ des adresses LAN. Ainsi qu'il sera montré plus loin, les diverses interfaces de messages de gestion peuvent avoir des droits d'accès à différents ensembles de paramètres. Il est possible d'accéder à la base de données du service portail aussi bien à partir du WAN que du LAN, cependant l'accès LAN n'est pas spécifié. La Figure 10 indique trois interfaces de messages de gestion possibles:

- NMS – CMP: messages de gestion échangés entre le système NMS du réseau câblé et le portail CMP;
- CMP – appareil IP de LAN: échange de messages de gestion entre le CMP et des appareils IP de LAN dans le secteur LAN-Trans (non spécifié);
- NMS – appareil IP de LAN: échange de messages de gestion entre le système NMS du réseau câblé et des appareils IP de LAN dans le secteur LAN-Pass (non spécifié);
- NMS – appareil IP de LAN: échange de messages de gestion entre le système NMS du réseau câblé et des appareils IP de LAN dans le secteur LAN-Trans (fourni par la configuration du portail CAP – voir § 8.3.2). Ce message n'est pas spécifié.

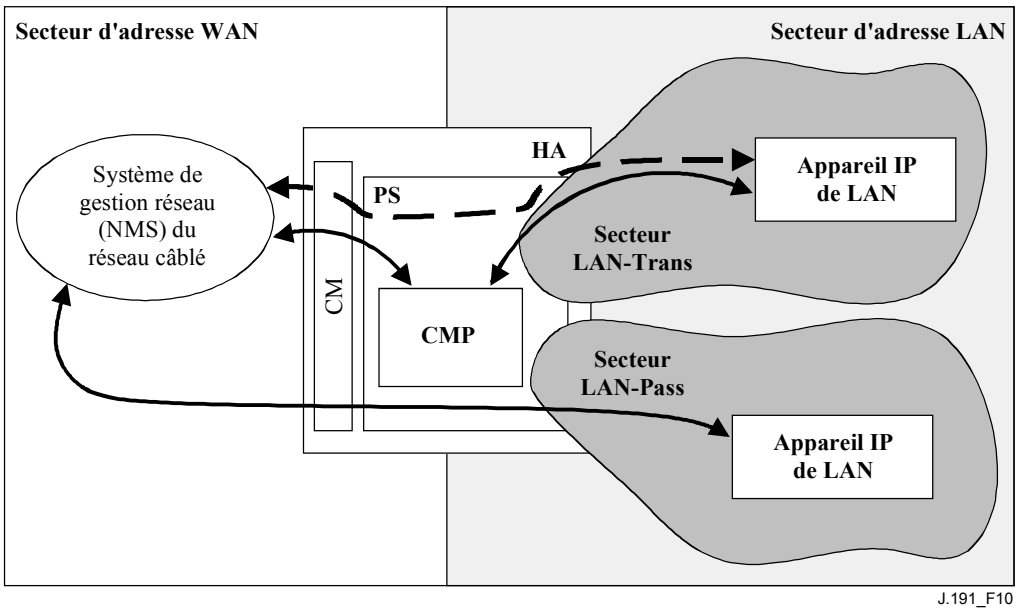

Figure 10/J.191 – Interfaces de messages de gestion

Le portail CMP est essentiellement une entité à laquelle on accède (au moyen du système NMS) par un WAN et qui est contrôlée par un WAN. De plus, on peut faire appel au portail CMP pour informer en tant que de besoin le système NMS du réseau câblé d'événements ou fichiers de connexion de système de transfert. Un exemple d'implémentation de portail CMP est illustré à la Figure 11 pour présenter les concepts des fonctionnalités de portail CMP.

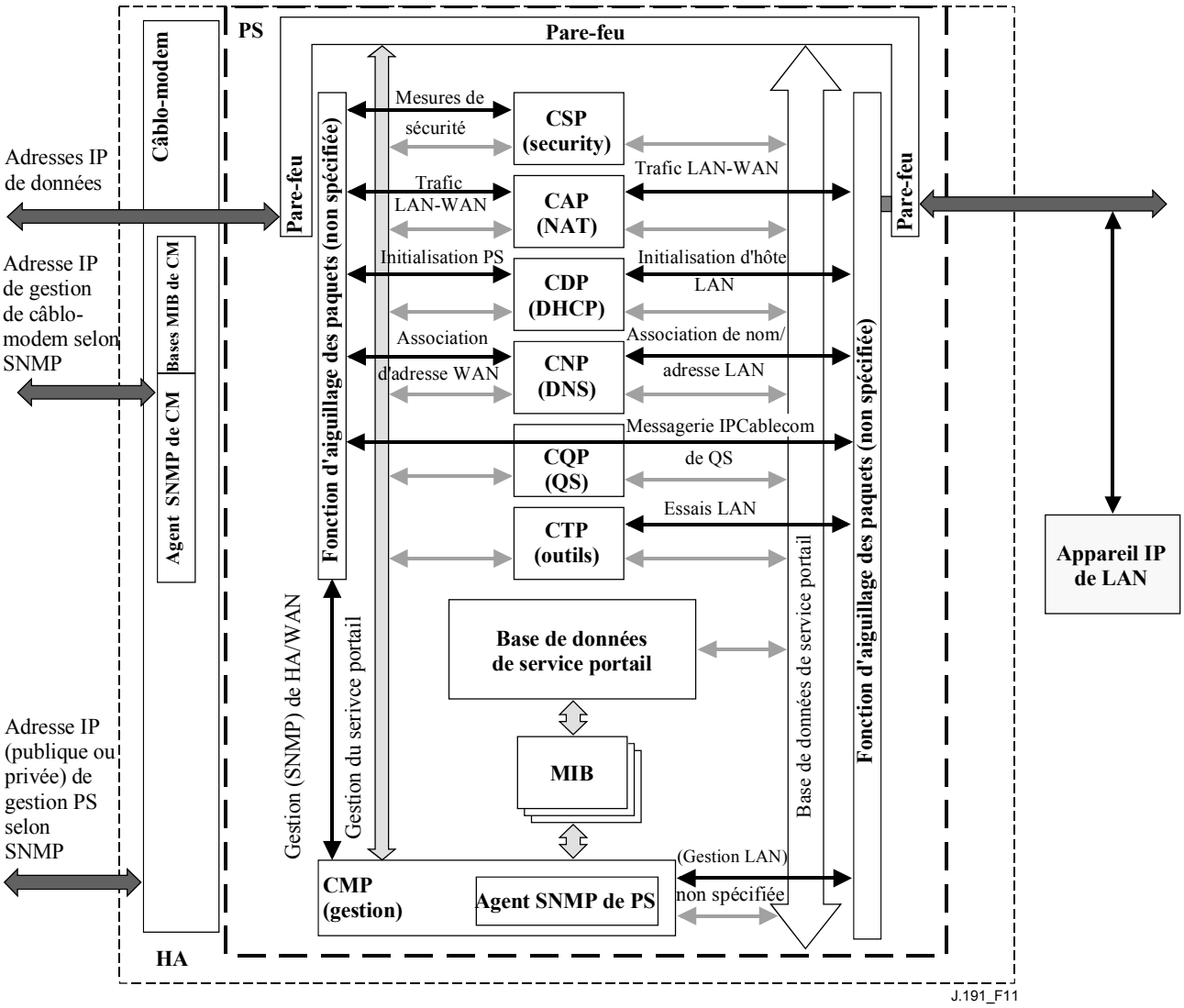

Figure 11/J.191 – Organigramme des services portail

Les outils de gestion du système NMS utilisent le protocole SNMP pour accéder aux objets et les gérer dans le service portail. Le protocole SNMPv3 donne à l'opérateur de système NMS l'authentification de l'utilisateur au service portail, l'accès fondé sur la vision des objets de la base d'informations de gestion (MIB, *management information base*) dans le service portail, et le chiffrement des messages de gestion sur demande.

L'agent de protocole SNMP du service portail est chargé d'établir le mappage de l'identificateur d'objet (OID) et de l'instance de l'OID pour tous les volets des blocs fonctionnels du service portail, tels que le portail CAP ou un stockage local comme la base de données du service portail.

En plus du portail CMP, un opérateur de système NMS peut accéder directement aux appareils IP de LAN ou les "gérer" en utilisant une adresse de raccourci entre la tête de système et l'appareil de LAN à gérer. Cependant, il n'y a pas d'exigences pour les appareils IP de LAN de répondre en particulier à un protocole, gestion ou autre.

6.3.4 Exigences générales pour le portail CMP

Le portail CMP DOIT fournir le contrôle de gestion au WAN au moyen du protocole SNMP v3 [RFC 2571, RFC 2572].

Le portail CMP DOIT implémenter le protocole ICMP [RFC 792] et répondre aux demandes d'écho ICMP venant du système NMS.

Si le service portail fonctionne en mode d'approvisionnement DHCP (indiqué par une valeur de "1"' dans cabhPsDevProvMode) le portail CMP DOIT utiliser par défaut le protocole SNMPv1/v2c pour les messages de gestion avec le système NMS et suivre les règles pour les modes NmAccess et coexistence, décrits au § 6.3.6.1.

Si le service portail fonctionne en mode d'approvisionnement SNMP (indiqué par une valeur de "2" dans cabhPsDevProvMode), le portail CMP DOIT utiliser le protocole SNMPv3 pour les messages de gestion avec le système NM, suivant les règles décrites au § 6.3.6.2.

Le portail CMP DOIT être capable de délivrer l'autorisation ultime à l'administrateur LAN ou à l'administrateur de WAN câble (administrateur de service portail).

Le réglage par défaut de l'autorisation ultime DOIT être l'administrateur WAN. L'autorisation ultime PEUT être modifiée via un accès de protocole SNMP ou un fichier de configuration.

La racine des bases MIB (MIB PSDev, MIB CAP, MIB CDP, MIB CTP, et MIB de sécurité) DOIT être (enterprises.4491.2.4).

L'objet sysDescr du groupe système MIB-2 (MIB-2 1) [RFC 1907] DOIT être implémenté et DOIT persister lors des réinitialisations d'appareil et remises en tension.

L'objet sysDescr DOIT contenir cinq champs dans l'ordre spécifique qui suit: HW_REV: version du matériel; VENDOR: nom du fabricant; BOOTR: version ROM d'amorce; SW_REV: version du logiciel; Model: numéro de modèle.

L'objet sysDesr se compose d'une liste de cinq paires de type/valeur. La séparation entre le type et la valeur est faite de deux points et un espace. La séparation entre une paire de type/valeur et la suivante paire de type/valeur est un point-virgule et un espace. Les cinq paires requises de l'objet SysDescr DOIVENT être contenues entre guillemets. Par exemple, un objet sysDescr pour un service portail du fabricant XYZ, version 5.2 du matériel, version 1.4 de la ROM d'amorce, version 2.2 du logiciel (SW), et modèle numéro ABC, DOIT apparaître comme suit:

> texte quelconque «HW_REV: 5.2; VENDOR: XYZ; BOOTR: 1.4; SW_REV: 2.2; MODEL: ABC» texte quelconque

Le service portail doit faire rapport, au moyen des champs sysDescr, de toutes les informations nécessaires pour déterminer avec quel logiciel le service portail peut être amélioré. Si l'un quelconque des champs sysDescr n'est pas applicable, le SysDescr DOIT indiquer "NONE" comme valeur. Par exemple, un service portail sans BOOTR indiquera BOOTR: NONE (*aucun*).

L'objet sysObjectID du groupe système MIB-2 [RFC 1907] DOIT être implémenté et DOIT persister lors des réinitialisations d'appareil et remises en tension.

L'objet sysUpTime du groupe système MIB-2 [RFC 1907] DOIT être implémenté. SysUpTime est le temps écoulé depuis la réinitialisation du système.

L'objet sysContact du groupe système MIB-2 [RFC 1907] DOIT être implémenté et DOIT persister lors des réinitialisations d'appareil et remises en tension. SysContact retourne le nom de l'utilisateur ou de l'administrateur de système s'il est connu.

L'objet sysLocation du groupe système MIB-2 [RFC 1907] DOIT être implémenté et DOIT persister lors des réinitialisations d'appareil et remises en tension.

L'objet sysServices du groupe système MIB- [RFC 1907] DOIT être implémenté et DOIT persister lors des réinitialisations d'appareil et remises en tension.

L'objet SysServices DOIT retourner la valeur "3" (portail Internet) lorsqu'il est interrogé dans un élément de service portail.

L'objet sysName du groupe système MIB-2 [RFC 1907] DOIT être implémenté et DOIT persister lors des réinitialisations d'appareil et remises en tension. L'interrogation sysName retourne le nom du système.

Les objets du groupe système MIB-2 autres que sysDescr, sysObjectID, sysUpTime, sysContact, sysName, sysLocation, et sysServices NE DEVRAIENT PAS être implémentés.

La base MIB de groupe des interfaces [RFC 2863] DOIT être implémentée.

Le groupe SNMP de MIB-2 [RFC 1907] DOIT être implémenté.

L'objet snmpSetSerialNo du groupe snmpSet [RFC 1907] DOIT être implémenté. SnmpSetSerialNo est un verrou consultatif utilisé pour permettre à plusieurs entités coopératives de protocole SNMPv2, agissant toutes comme gestionnaires, de coordonner leur utilisation du fonctionnement de l'ensemble SNMPv2.

Les objets de groupe SnmpSet autres que snmpSetSerialNo NE DEVRAIENT PAS être implémentés.

6.3.5 Exigences du protocole SNMP

Les appels à commentaires suivants de l'IETF DOIVENT être suivis ou implémentés selon le cas:

1) protocole simple de gestion de réseau [RFC 1157];
2) introduction au protocole SNMPv2 fondé sur la communauté [RFC 1901];
3) fonctionnement du protocole pour SNMPv2 [RFC 1905];
4) mappages de transport pour SNMPv2 [RFC 1906];
5) base d'informations de gestion pour la version 2 du protocole simple de gestion de réseau (SNMPv2) [RFC 1907];
6) introduction à SNMPv3 [RFC 2570];
7) base MIB de la trame du protocole SNMP [RFC 2571];
8) traitement et expédition de message pour SNMP [RFC 2572];
9) base MIB des applications SNMP [RFC 2573];
10) groupe de base MIB SnmpUSM [RFC 2574];
11) groupe de base MIB SnmpVACM [RFC 2575];
12) base MIB de communauté SNMP [RFC 2576];
13) SNMPv2-CONF.

Pour le soutien de SMIv2, les appels à commentaire suivants de l'IETF DOIVENT être implémentés:

1) structure des informations gérées version 2 (SMIv2) [RFC 2578];
2) conventions d'écriture pour SMIv2 [RFC 2579];
3) déclarations de conformité pour SMIv2 [RFC 2580].

6.3.6 Exigences pour le mode de gestion de réseau

Le présent paragraphe décrit les règles pour les modes de gestion du réseau qui sont exigés du service portail. Le § 6.3.6.1 et ses paragraphes décrivent les modes de gestion du réseau pour un service portail fonctionnant en mode d'approvisionnement DHCP. Le § 6.3.6.2 et ses paragraphes décrivent les modes de gestion du réseau pour un service portail fonctionnant en mode d'approvisionnement SNMP.

6.3.6.1 Mode NmAccessTable et mode coexistence pour un PS fonctionnant en mode d'approvisionnement DHCP

Le service portail DOIT accepter les protocoles SNMPv1, SNMPv2c, et SNMPv3 et SNMP Coexistence comme décrit de [RFC 2571] à [RFC 2576]. Le service portail DOIT aussi accepter le mode NmAccessTable comme défini par [RFC 2669]. Le soutien des modes de gestion réseau pour un service portail fonctionnant en mode d'approvisionnement DHCP fait l'objet des lignes directrices suivantes:

6.3.6.1.1 Fonctionnement de base pour un service portail fonctionnant en mode d'approvisionnement DHCP

a) A la suite de la réception d'un accusé de réception DHCP ACK, le service portail fonctionnant en mode d'approvisionnement DHCP [indiqué par une valeur cabhPsDevProvMode de "1" (DHCPmode)] DOIT opérer comme suit:

- l'accès en lecture seule SNMPv1/v2c pour toutes les variables de la base MIB, dont la visibilité est nécessaire pendant le fonctionnement SNMPv1/v2c, est permis à partir du LAN. Le non-accès est permis à partir du WAN, pour empêcher l'accès de gestion non autorisé avant que le service portail ne soit configuré via le fichier de configuration du service portail;
- sont acceptés les paquets SNMPv1/v2c qui contiennent une chaîne communautaire quelconque;
- tous les paquets SNMPv3 sont abandonnés;
- l'accès DEVRAIT être interdit à toute variable de base MIB qui permettrait la détermination de l'adresse IP du service portail WAN-Man, comme l'IpAddrTable de MIB-2;
- aucune des bases MIB du protocole SNMPv3 (base MIB de communauté, MIB cible, MIB VACM, MIB USM, MIB de notification) n'est accessible, sauf qu'elles peuvent être établies à partir du fichier de configuration du service portail;
- aucun des éléments dans la base SNMP-USM-DH-OBJECTS-MIB n'est accessible sauf qu'ils peuvent être établis à partir du fichier de configuration du service portail;
- le traitement réussi de tous les éléments de base MIB dans le fichier de configuration du service portail DOIT être achevé avant le début du calcul des valeurs publiques dans le tableau USMDHKickstart.

b) Si un service portail fonctionne en mode d'approvisionnement DHCP, le contenu du fichier de configuration du service portail détermine le mode de gestion du réseau, comme décrit ci-dessous:

- le service portail est en mode SNMPv1/v2c docsDevNmAccess si le fichier de configuration du service portail ne contient QUE le tableau docsDevNmAccess réglant la commande d'accès SNMP;
- si le fichier de configuration du service portail ne contient pas d'éléments de commande d'accès du protocole SNMP (docsDevNmAccessTable ou snmpCommunityTable ou TLV 34.1/34.2 ou TLV38), le service portail est alors en mode NmAccess;
- si le fichier de configuration du service portail contient le réglage snmpCommunityTable et/ou TLV type 34.1 et 34.2 et/ou TLV type 38, le service portail est alors en mode coexistence SNMP. Dans ce cas, on ignore toutes les entrées faites dans le tableau docsDevNmAccessTable.

c) Après achèvement du processus d'approvisionnement décrit au § 13.2 (indiqué par la valeur "succès" (1) dans cabhPsDevProvState), le service portail fonctionne dans l'un des deux modes de gestion. Le mode de gestion de réseau est déterminé par le contenu du fichier de configuration comme décrit ci-dessus.

Mode NmAccess (utilisant le tableau docsDevNmAccess) avec SNMPv1/v2c.

- Seuls les paquets SNMPv1/v2c sont traités.
- Les paquets SNMPv3 sont abandonnés.
- docsDevNmAccessTable commande les destinations d'accès et les interruptions comme décrit dans [RFC 2669].
- Aucune des bases MIB SNMPv3 (MIB de communauté, MIB cible, MIB VACM, MIB USM, MIB de notification) n'est accessible.

Mode coexistence avec SNMPv1/v2c/v3

Pendant le calcul des valeurs publiques USMDHKickstartTable:

- le service portail NE DOIT PAS permettre d'accès SNMP à partir du WAN;
- le service portail PEUT continuer à permettre l'accès à partir du LAN avec la limitation d'accès telle que configurée par la base MIB USM, la base MIB de communauté et la base MIB VACM.

Après le calcul des valeurs publiques de USMDHKickstartTable:

- le service portail DOIT envoyer le trap de départ à froid ou de départ à chaud pour indiquer que le service portail est maintenant pleinement compatible SNMPv3;
- les paquets SNMPv1/v2c/v3 sont traités comme décrit par les normes [RFC 2571] et [RFC 2576];
- docsDevNmAccessTable n'est pas accessible;
- commande d'accès et destinations de trap sont déterminées par le tableau snmpCommunityTable, la base MIB de notification, la base MIB cible, la base MIB VACM et la base MIB USM;
- la base MIB communautaire commande la traduction de la chaîne communautaire de paquet SNMPv1/v2c en nom de sécurité qui choisit les entrées dans la base MIB USM. La commande d'accès est fournie par la base MIB VACM;
- les bases MIB USM et VACM contrôlent les paquets SNMPv3;
- les destinations de Trap sont spécifiées dans les bases MIB cible et de notification.

En cas d'échec de l'achèvement de l'initialisation SNMPv3 pour un utilisateur (c'est-à-dire, le système NMS ne peut pas accéder au service portail via l'unité PDU SNMPv3), le tableau d'utilisateur USM pour cet utilisateur DOIT être supprimé, le service portail est en mode Coexistence, et le service portail ne permettra l'accès SNMPv1/v2c que si et seulement si les entrées de base MIB communautaire (et les entrées qui s'y rapportent) sont configurées.

6.3.6.1.2 Initialisation du mode SNMPv3 coexistence et changements de clé

Lorsqu'il est en mode coexistence, le service portail DOIT accepter les exigences de "l'initialisation SNMPv3" et les "changements de clé DH" spécifiés aux paragraphes suivants.

6.3.6.1.2.1 Initialisation SNMPv3

Jusqu'à cinq noms de sécurité différents et pour chacun d'eux, l'administrateur du service portail génère une paire de nombres. D'abord, l'administrateur de service portail génère un nombre aléatoire Rm.

Ensuite, l'administrateur IPCable2home utilise l'équation DH pour traduire Rm en un nombre public z. L'équation est comme suit:

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

où g vient de l'ensemble des paramètres Diffie-Hellman, et p est le premier de ces paramètres.

Le fichier de configuration du service portail est créé afin d'inclure la paire (nom de sécurité, nom public). Le service portail DOIT accepter un minimum de 5 paires. Par exemple:

TLV type 34.1 (nom de sécurité de démarrage SNMPv3) = Administrateur de service portail;

TLV type 34.2 (numéro public de démarrage SNMPv3) = z

Le service portail DOIT accepter les entrées VACM définies au § 6.3.6.4. Seules les entrées VACM spécifiées par le nom de sécurité correspondant dans le fichier de configuration du service portail seront (DEVRONT) être actives.

Durant le processus d'amorçage du service portail, les valeurs ci-dessus (nom de sécurité, numéro public) DOIVENT être entrées dans le tableau usmDHKickstartTable.

A ce point:

usmDHKickstartMgrpublic.1 = "z" (chaîne d'octets)

usmDHKickstartSecurityName.1 = "Administrateur du service portail"

Lorsque usmDHKickstartMgrpublic.n est mis avec une valeur valide pendant l'enregistrement, une rangée correspondante est créée dans le tableau usmUserTable avec les valeurs suivantes:

usmUserEngineID: identifiant de moteur local

usmUserName: valeur usmDHKickstartSecurityName.n

usmuserSecurityName: valeur usmDHKickstartSecurityName.n

usmUserCloneFrom: ZéropointZéro

usmUserAuthProtocol: usmHMACMD5AuthProtocol

usmuserAuthKeyChange: (déduit de la valeur de réglage)

usmUserOwnAuthKeyChange: (déduit de la valeur de réglage)

usmUserPrivProtocol: usmDESPrivProtocol

usmUserPrivKeyChange: (déduit de la valeur de réglage)

usmUserOwnPrivKeyChange: (déduit de la valeur de réglage)

usmUserPublic

usmUserStorageType: permanent

usmUserStatus: actif

NOTE – Pour les entrées (de service portail) dhKickstart dans le tableau usmUserTable, Permanent signifie qu'elles DOIVENT être écrites mais non effacées et ne sont pas sauvegardées lors des réamorçages.

Après que le service portail a achevé l'initialisation (indiquée par une valeur de "1" (réussi) pour cabhPsDevProvState):

1) le service portail génère un nombre aléatoire xa pour chaque rangée remplie dans le tableau usmDHKickstartTable qui a un usmDHKickstartSecurityName et usmDHKickstartMgrPublic d'une longueur différente de zéro;

2) le service portail utilise l'équation DH pour traduire xa en numéro public (pour chaque rangée identifiée ci-dessus);

$$c = (g \text{ ^ } xa) \text{ MOD } p$$

où g est tiré de l'ensemble des paramètres Diffie-Hellman, et p est le premier de ces paramètres.

A ce point:

usmDHKickstartMyPublic.1 = "c" (chaîne d'octets)

usmDHKickstartMgrPublic.1 = "z" (chaîne d'octets)

usmDHKickstartSecurityName.1 = "gestionnaire docsis"

3) le service portail calcule la clé secrète partagée sk où sk = z ^xa mod p;

4) le service portail utilise sk pour déduire la clé de confidentialité et la clé d'authentification pour chaque rangée dans le tableau usmDHKickstartTable et établit les valeurs dans le tableau usmUserTable.

Comme spécifié dans la norme [RFC 2786], la clé de confidentialité et la clé d'authentification pour le nom d'utilisateur associé, "Administrateur de service portail" sont dans ce cas déduites de sk en appliquant la fonction de déduction de clé PBKDF2 définie dans PKCS#5 v2.0.

clé de confidentialité ←PBKDF2(salt = 0xd1310ba6,

Compte d'itération = 500,

Longueur de clé = 16,

prf = id-hmacWithSHA1)

clé d'authentification ←PBKDF2(salt = 0x98dfb5ac,

Compte d'itération = 500,

Longueur de clé = 16 (usmHMACMD5AuthProtocol),

prf = id-hmacWithSHA1)

A ce point, le service portail PS (CMP) a achevé son processus d'initialisation SNMPv3 et DOIT permettre le niveau d'accès approprié à un nom de sécurité valide avec la clé d'authentification et/ou clé de confidentialité correcte.

Le service portail DOIT mettre de façon correcte les clés dans les tableaux appropriés comme spécifié par les normes RFC en rapport avec SNMPv3 et la norme [RFC 2786];

5) ce qui suit décrit le processus utilisé par le gestionnaire pour déduire la clé d'authentification unique et la clé de confidentialité du service portail.

Le gestionnaire SNMP accède au contenu du tableau usmDHKickstartTable en utilisant le nom de sécurité de "dhKickstart" sans authentification.

Le service portail DOIT fournir des entrées pré-installées dans le tableau USM et les tableaux VACM pour créer correctement le "dhKickstart" de l'utilisateur du niveau de sécurité noAuthNoPriv qui a un accès en lecture seule au groupe système et au tableau usmDHkickstartTable.

Si le service portail est en mode coexistence et est configuré de façon à utiliser SNMPv3, la spécification de groupe pour la vision dhKickstart DOIT être implémentée comme suit:

dhKickstart Group	
vacmGroupName	'dhKickstart'
vacmAccessContextPrefix	''
vacmAccessSecurityModel	3 (USM)
vacmAccessSecurityLevel	NoAuthNoPriv
vacmAccessContextMatch	exact
vacmAccessReadViewName	'dhKickstartView'

vacmAccessWriteViewName	"
vacmAccessNotifyViewName	"
vacmAccessStorageType	permanent
vacmAccessStatus	actif

La vision VACM pour la vision dhKickstart DOIT être implémentée comme suit:

sous-arbre dhKickstartView 1.3.6.1.2.1.1 (groupe système) et 1.3.6.1.3.101.1.2.1 (usmDHkickstartTable)

Le gestionnaire SNMP obtient la valeur du numéro usmDHKickstartMypublic du service portail associé au nom de sécurité pour lequel le gestionnaire veut déduire les clés d'authentification et de confidentialité. En utilisant le numéro aléatoire privé, le gestionnaire peut calculer le secret partagé DH. A partir de ce secret partagé, le gestionnaire peut déduire les clés opérationnelles d'authentification et de confidentialité pour le nom de sécurité que le gestionnaire va utiliser pour communiquer avec le service portail.

6.3.6.1.2.2 Changements de clés Diffie-Hellman

Le service portail DOIT accepter le mécanisme de changement de clés spécifié dans la norme [RFC 2786].

6.3.6.2 Mode d'approvisionnement SNMP

Si le service portail fonctionne en mode d'approvisionnement SNMP à la suite de l'accusé de réception DHCP (comme indiqué par une valeur "2" (mode SNMP) pour cabhPsDevProvMode), il fonctionne dans le mode de gestion réseau utilisant SNMPv3, USM et VACM, ainsi que Kerberos pour l'échange de matériau de clé (comme décrit au § 6.3.3) en suivant les règles décrites au présent paragraphe.

6.3.6.2.1 Problèmes de gestion

Les commandes de gestion sont dans l'élément de service portail. Les réglages, fondés sur le mode de gestion, définissent les droits d'accès qui sont alloués à un générateur de commandes pour l'accès à la base de données du service portail, à travers des bases MIB spécifiées, via SNMP à partir du système NMS du réseau câblé. Un générateur de commande unique est défini par la présente spécification.

La Figure 12 illustre quelques exemples de vues de la gestion utilisant SNMPv3. On définit une vue de l'administrateur de WAN (vue de l'administrateur de service portail) et un utilisateur d'administrateur WAN (utilisateur d'administrateur de service portail). D'autres vues et utilisateurs, tels que vue de la maintenance WAN, vue de l'administrateur LAN, ou vue de l'utilisateur LAN peuvent être établies par l'autorisation ultime (administrateur du service portail), suivant les règles définies dans les normes [RFC 2574] et [RFC 2575].

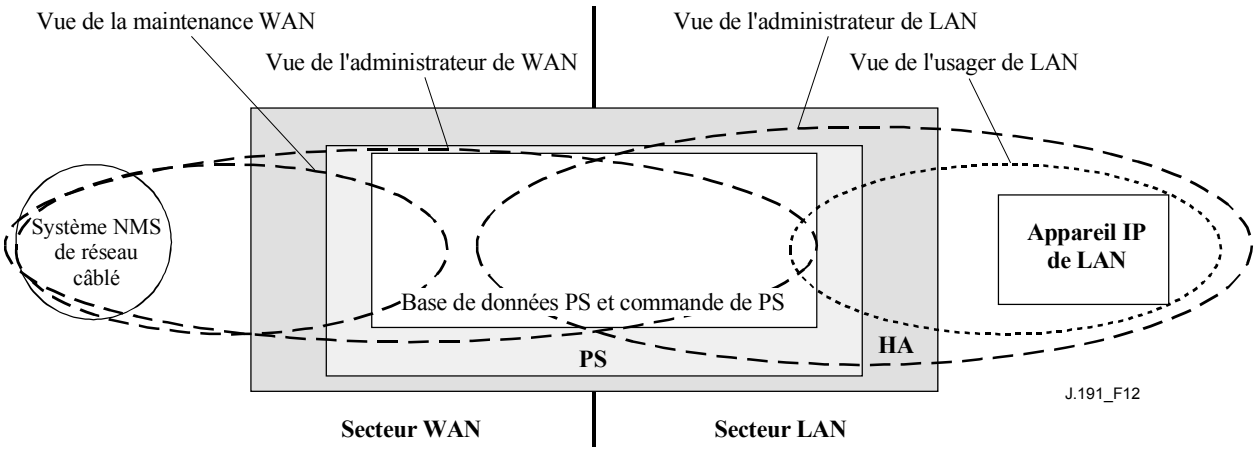

Figure 12/J.191 – Visions de gestion

Les paramètres gérés sont stockés dans la base de données du service portail. Comme indiqué à la Figure 12, il y a dans la base de données PS et dans la commande de service portail une notion de vision d'accès qui permet la gestion simultanée à partir du LAN et du WAN en définissant les vues de gestion dans la base de données et la commande de service portail. Les vues sont un mécanisme de fourniture de la confidentialité et de la sécurité, et la politique peut être réglée séparément par l'utilisateur d'administrateur de service portail.

L'autorisation ultime (utilisateur d'administrateur de service portail) a les responsabilités suivantes:

- établissement de toutes les vues d'accès à la fois sur l'interface de gestion de LAN et de WAN;
- détention de propre identifiant d'utilisateur et ses clés.
- création et gestion de tous les profils d'utilisateur, y compris les identifiants d'utilisateur, les clés et les privilèges d'accès aux bases de données du service portail;
- établissement de la politique pour l'accès du côté LAN comme du côté WAN.

Une implémentation complète du modèle VACM exige un ensemble d'actions qui vont lier un "utilisateur" à un "groupe", et lier le "groupe" à une vue du modèle VACM, qui définit l'accès. Le § 6.3.6.4 décrit la façon de créer ces relations.

Le nom vacmSecurityName est "l'utilisateur". Ce nom de sécurité est lié au nom vacmGroupName. Et donc "l'utilisateur" est lié à un groupe spécifique. Le groupe est alors défini, pour spécifier quel niveau de sécurité est utilisé et aussi quelles vues de lecture, écriture et notification sont disponibles pour ce groupe. Les vues sont alors spécifiées pour montrer exactement quels objets MIB sont accessibles.

Le modèle de commande fondé sur la vue détermine les droits d'accès d'un groupe, représentant zéro ou plus noms de sécurité, qui ont les mêmes droits d'accès. Pour un contexte particulier, identifié par le contextName (*nom de contexte*), auquel un groupe, identifié par le nom de groupe, a accès en utilisant un modèle de sécurité et un niveau de sécurité particulier, ces droits d'accès de groupe sont donnés par une vue de lecture, une vue d'écriture et une vue de notification.

La vue de lecture représente l'ensemble des instances d'objets autorisées pour le groupe lors de la lecture d'objets. La lecture d'objets intervient lors du traitement d'une opération d'écriture (lors du traitement d'unités PDU de classe de lecture).

La vue d'écriture représente l'ensemble des instances d'objets autorisées pour le groupe lors de l'écriture d'objets. Les objets d'écriture interviennent lors du traitement d'une opération d'écriture (lors du traitement d'unités PDU de classe d'écriture).

La vue de notification représente l'ensemble des instances d'objets autorisées pour le groupe lors de l'envoi d'objets dans une notification, comme lors de l'envoi d'une notification (lors de l'envoi d'unités PDU de classe de notification).

La vue d'administrateur PS fournit un accès en lecture et écriture complet à toutes les bases MIB spécifiées.

Les exigences de la vue de gestion sont spécifiées au § 6.3.6.4.

6.3.6.2.2 Commande d'accès WAN

La commande d'accès SNMP, selon la norme [RFC 2575], sera utilisée pour les vues du côté WAN. Le modèle ce commande d'accès fondé sur la vue (VACM, *view-based access control model*) [RFC 2575] définit un ensemble de services qui peuvent être utilisés pour vérifier les droits d'accès. Les groupes du modèle VACM définissent les droits pour accéder au portail CMP.

Comme défini dans la norme [RFC 2575] section 2.4, une "vue MIB " est un ensemble spécifique de types d'objets gérés qui peuvent être définis, et cette notion sert au soutien de la gestion WAN du service portail. L'accès et la vue d'utilisateur d'administrateur de service portail sont spécifiés aux § 11.3.3.2.2 et 6.3.6.4. Le § 12.3.1 donne un exemple de séquence d'accès à une base de donnée de service portail à partir de l'interface WAN.

6.3.6.2.3 Sécurité

La sécurité des messages de gestion est fournie par le protocole SNMPv3. Se reporter au paragraphe 11 pour une description détaillée de la façon dont le protocole SNMPv3 est utilisé. Le portail CMP peut utiliser le protocole SNMP v3 pour contrer les menaces identifiées à l'Annexe C.

Pour se protéger contre les attaques de répétition, une horloge en temps réel est utilisée pour fournir des horodatages pour les messages. Les exigences de sécurité des messages de gestion sont spécifiées au § 11.3.3.

6.3.6.3 Exigences de sécurité

Les exigences de sécurité des messages de gestion sont spécifiées au § 11.3.3.

6.3.6.4 Exigences du modèle de commande d'accès fondée sur la vue (VACM)

Pour fournir le contrôle d'accès aux informations de gestion et créer des secteurs de gestion distincts, le modèle de commande d'accès fondée sur la vue (VACM) DOIT être employé comme défini par la norme [RFC 2575].

La vue de l'administrateur WAN DOIT être implémentée dans l'élément de service portail. Les vues par défaut autres que la vue d'administrateur WAN NE DOIVENT PAS être disponibles sur le service portail. D'autres vues PEUVENT être créées par le système NMS du réseau câblé en configurant la base MIB du modèle VACM.

La spécification d'utilisateur pour la vue d'administrateur WAN DOIT être implémentée comme suit:

vacmSecurityModel	3 (USM)
vacmSecurityName	"Administrateur de service portail"
vacmGroupName	"Administrateur de service portail"
vacmSecurityToGroupStorageType	permanent
vacmSecurityToGroupStatus	actif

La spécification de groupe pour la vue d'administrateur de service portail DOIT être implémentée comme suit:

PS Administrator Group

vacmGroupName	"Administrateur de service portail"
vacmAccessContextPrefix	"
vacmAccessSecurityModel	3 (USM)
vacmAccessSecurityLevel	AuthPriv
vacmAccessContextMatch	exact
vacmAccessReadViewName	"Administrateur de service portail"
vacmAccessWriteViewName	'"Administrateur de service portail"
vacmAccessNotifyViewName	"Administrateur de service portail"
vacmAccessStorageType	permanent
vacmAccessStatus	actif

La vue VACM pour la vue de l'administrateur de service portail DOIT être implémentée comme suit:

sous-arbre de vue d'administrateur de service portail 1.3.6.1 (base MIB entière)

6.3.7 Exigences de la base MIB

Les objets de base MIB dont la liste figure à l'Annexe A DOIVENT être implémentés dans un élément de service portail. Les objets de base MIB requis viennent des documents de base MIB suivants:

base MIB de groupe d'interfaces [RFC 2863]

1) Base MIB d'appareil à câble DOCSIS (*DOCSIS Cable Device MIB*) [RFC 2669];
2) Base MIB DEF CLAB de câble (*Cable CLAB DEF MIB*) [Annexe E.4];
3) Base MIB PSDev de câble (*Cable PSDev MIB*) [Annexe E.1];
4) Base MIB de portail CAP par câble (*Cable CAP MIB*) [Annexe E.6];
5) Base MIB de portail CDP par câble (*Cable CDP MIB*) [Annexe E.5];
6) Base MIB de portail CTP par câble (*Cable CTP MIB*) [Annexe E.2];
7) Base MIB de sécurité par câble (*Cable Security MIB*) [Annexe E.3];
8) draft-ietf-ipcdn-bpiplus-mib-06.txt;
9) Base MIB IP (*IP MIB*) (SNMPv2) [RFC 2011];
10) Base MIB UDP (*UDP MIB*) (SNMPv2) [RFC 2013];
11) Clé USM Diffie-Hellman (*Diffie-Hellman USM Key*) [RFC 2786];
12) Base MIB d'adresse INET (*INET Address MIB*) [RFC 2851];
13) Base MIB IF DOCS (*DOCS IF MIB*) [RFC 2670];
14) Base MIB ifType IANA (*IANA ifType MIB)*.

A l'exception du groupe SNMP de base MIB 2, les bases MIB USM et MIB VACM, auxquelles l'agent SNMP accède directement dans le service portail (CMP), ET la base MIB d'appareil par câble DOCSIS pour le cas de téléchargement de logiciel sur un service portail, le service portail DOIT maintenir des instances de bases MIB spécifiques de service portail séparées du câblo-modem. Les informations auxquelles on a accès à partir de la base de données du service portail au moyen de l'adresse WAN-Man du service portail DOIVENT être séparées et distinctes des informations auxquelles on accède via l'adresse de gestion du câblo-modem.

La hiérarchie générale de base MIB est illustrée à la Figure 13. La liste des identifiants OID spécifiques nécessaires pour les bases MIB individuelles figure à l'Annexe A.

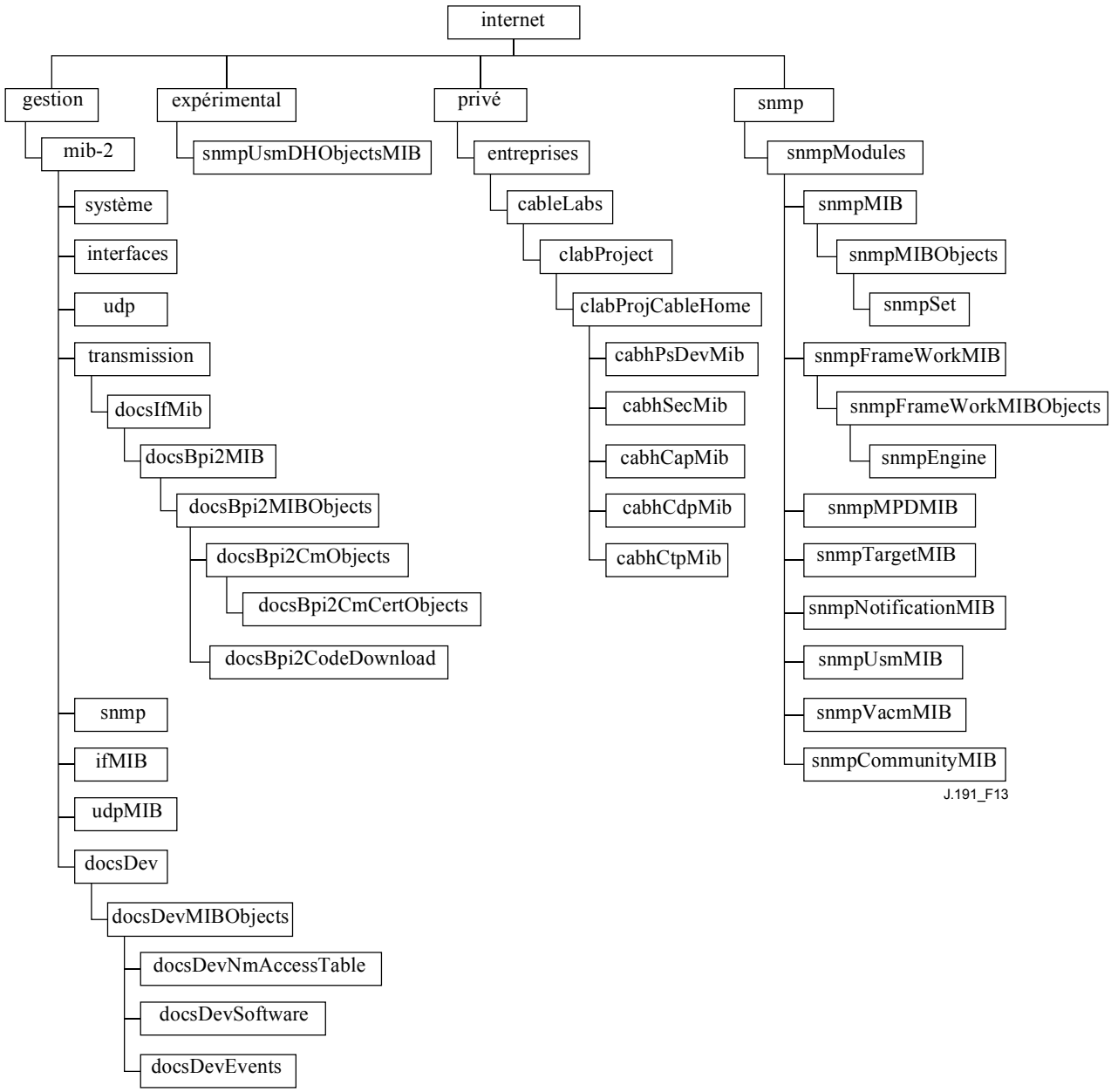

Figure 13/J.191 – Hiérarchie des bases MIB

6.3.8 Exigences pour base MIB de groupe des interfaces

La base MIB de groupe des interfaces fournit un outil puissant pour permettre aux câblo-opérateurs de comprendre l'état et voir les statistiques de toutes les interfaces physiques sur l'élément de service portail. Afin de permettre une utilisation intelligente de cette base MIB, un schéma de numérotation des interfaces est essentiel. Il est donc nécessaire que les éléments de service portail se conforment aux exigences suivantes:

il DOIT exister une instance de IfEntry pour l'interface WAN de l'élément de service portail, même si cet élément WAN est interne – comme cela se produit dans le cas d'un service portail incorporé utilisant une solution de puce intégrée.

Il DOIT exister une instance de IfEntry pour chaque interface LAN physique de cet élément de service portail.

Les interfaces DOIVENT être numérotées comme indiqué au Tableau 12.

Tableau 12/J.191 – Numérotage des interfaces dans le tableau ifTable

Interface	Description
1	Interface WAN
1 + n	Chaque interface LAN

Si l'ifAdminStatus d'une interface donnée = down, cette interface NE DOIT PAS accepter ou transmettre de trafic.

6.3.9 Exigences pour le traitement du fichier de configuration du portail CMP

Le portail CMP est l'entité fonctionnelle dans le service portail qui est responsable du traitement des paramètres passés dans les fichiers de configuration du service portail. Les fichiers de configuration du service portail servent à la reconfiguration du service portail en fournissant des valeurs pour des paramètres gérables dans la base de données du service portail.

Le fichier de configuration PS est d'abord vérifié quant à son intégrité et authentifié, comme décrit au § 11.3.7. Ensuite, les multiples TLV dans les fichiers de configuration PS sont analysés, et les identifiants d'objet SNMP et leurs paramètres sont extraits. Le portail CMP DOIT utiliser les paramètres extraits du fichier de configuration PS pour établir les objets gérés dans la base de données du service portail. Ce processus est fonctionnellement équivalent à une opération SNMP SET, mais il ne repose pas sur les permissions d'accès de l'utilisateur ou fondées sur la vue. Le portail CMP DOIT mettre à jour sans condition les objets correspondants pour les identifiants OID reconnus.

Les réglages de configuration DOIVENT être traités dans le même ordre que celui sous lequel ils apparaissent dans le fichier de configuration PS. Le portail CMP DOIT être capable d'accepter une série de paramètres TLV contenus dans un fichier de configuration PS. Il n'y a pas d'état préconçu du service portail lors de la réception d'un fichier de configuration PS. Le processus de chargement et d'exécution d'un fichier de configuration PS peut interrompre le traitement des données dans le service portail. Le portail CMP NE DOIT PAS tenir compte d'un réglage de configuration quelconque pour lequel n'existent pas de paramètres de base de données valides.

Pour les réglages SNMP dans le fichier de configuration PS, le service portail DOIT traiter toutes les liaisons de variable SNMP (Varibinds) dans le fichier de configuration PS comme s'ils étaient reçus dans une unité PDU SNMP unique. Si des Varibinds sont reçus en double dans le fichier de configuration PS, le service portail DOIT arrêter le processus d'approvisionnement.

Les objets définis par des TLV qui sont passés dans le fichier de configuration PS et ne sont pas acceptés ou ne peuvent être écrits dans l'implémentation particulière de service portail DOIVENT être ignorés. Le portail CMP NE DOIT PAS tenir compte de TLV inconnus, quels qu'ils soient.

La taille du fichier de configuration, le nombre de TLV traités et le nombre de TLV ignorés DOIVENT être mis à jour dans les objets de base MIB: cabhPsDevProvConfigFileSize, cabhPsDevProvConfigTLVProcessed et cabhPsDevProvConfigTLVRejected, respectivement.

Les exigences pour le fichier de configuration PS sont spécifiées au § 7.3.

6.4 Le portail d'essai du câble (CTP, *cableHome testing portal*)

6.4.1 Objectifs du portail CTP

Parmi les objectifs du portail d'essai du câble figurent:

- permettre les diagnostics de faute d'appareil IP de LAN;
- permettre la visibilité sur les appareils IP de LAN, ainsi que l'accès au numéros et types d'appareils IP de LAN;
- permettre la surveillance des performances de l'appareil IP de LAN.

6.4.2 Lignes directrices pour la conception du portail CTP

La liste des lignes directrices du système d'outils de gestion figure dans le Tableau 13. Un certain nombre de ces lignes directrices sont communes avec les lignes directrices de la conception du portail CMP. Cette liste donne des indications pour la spécification des fonctionnalités du portail CTP.

Tableau 13/J.191 – Lignes directrices pour la conception du système de portail CMP

Référence	Lignes directrices pour la conception du système de portail CMP
CTP 1	Il est nécessaire que les interfaces acceptent les caractéristiques de gestion et de diagnostic et les fonctions requises pour le soutien des services fondés sur le câble fournis chez l'utilisateur.
CTP 2	Il est nécessaire que des capacités de surveillance locales et à distance permettent de surveiller le fonctionnement chez l'utilisateur et aident le consommateur et le câblo-opérateur à identifier les zones de problème.
CTP 3	Le système NMS de réseau câblé exige une méthode pour rassembler les informations d'identification sur chaque appareil IP connecté chez l'utilisateur.
CTP 4	Le système NMS de réseau câblé exige une méthode pour détecter si un appareil connecté est en état de fonctionnement.

6.4.3 Description du système de portail CTP

Le portail CTP (portail d'essai du câble) contient les "outils distants" avec lesquels la gestion de système NMS peut collecter d'autres informations d'appareil LAN. Les essais doivent être effectués à distance, dans la mesure où passer derrière une fonction de traduction d'adresse de réseau (NAT, *network address translation*) dans un routeur risque d'être très difficile. Par exemple, un ping de WAN à LAN ne pourra pas passer à travers un PS, à moins que le portail CAP n'ait été préconfiguré pour laisser passer ce trafic. Le portail CTP est un mandataire local qui sert à interpréter et exécuter la classe de faute/diagnostics à distance des messages SNMP qu'il reçoit de l'opérateur de système NMS. Ces essais d'appareil IP de LAN sont définis sur la base des problèmes qu'on peut vraisemblablement rencontrer: diagnostics de connectivité et de débit.

Ces fonctions sont appelées outil de vitesse de connexion de portail CTP et outil de ping à distance de portail CTP. Les outils de vitesse de connexion et de ping à distance permettent au centre de soutien des consommateurs du câblo-opérateur et au centre d'opération réseau d'en savoir plus sur la connexion entre l'élément de service portail et les appareils IP de LAN chez l'utilisateur.

6.4.3.1 Outil de vitesse de connexion de portail CTP

Cette fonction sert à obtenir une mesure grossière de la performance à travers la liaison entre le service portail et l'appareil IP de LAN. Elle envoie une rafale de paquets entre le service portail et l'appareil IP de LAN soumis à l'essai, et le temps d'aller-retour est mesuré pour la rafale. En général, l'opérateur de système NMS entre quelques nouveaux paramètres et déclenche la fonction, et les résultats sont emmagasinés dans la base de données du service portail pour une récupération ultérieure à travers la base MIB du portail CTP.

La fonction de vitesse de connexion repose sur l'incorporation d'une fonction de "bouclage" ou de "service écho" sur les appareils IP de LAN. L'autorité Internet d'allocation des numéros (*Internet assigned numbers authority*) IANA a alloué le port 7 de service écho à la fois au protocole TCP et au protocole UDP [RFC 347]. L'adresse de source IP est toujours celle de la passerelle par défaut du LAN du servie portail (cabhCdpServerRouter). La fonction d'essai ne fonctionne que sur les appareils IP de LAN dans le secteur d'adresse LAN Trans.

Le paragraphe ci-dessous sur les exigences testables pour le portail CTP fait la liste des paramètres et réponses pour l'outil de vitesse de connexion. Le § 12.2.1.1 précise le fonctionnement de l'outil de vitesse de connexion.

6.4.3.2 Outil Ping de portail CTP

On se sert de cette fonction pour tester la connectivité entre le service portail et des appareils IP de LAN individuels. Les résultats de multiples exécutions de l'essai de l'outil ping peuvent être assemblés par le système NMS pour faire un examen réseau des appareils IP de LAN. Le tableau DHCP du portail CDP a un historique des appareils, mais seulement de ceux qui emploient le protocole DHCP. Le ping peut saisir un état actuel qui inclut des clients non DHCP. Pour garder une certaine simplicité au service portail, on suppose que le système NMS incrémente l'adresse et emmagasine les résultats dans l'outil NMS pour effectuer un examen d'un sous-réseau LAN.

L'outil Ping est initialisé par une série de messages établissement-demande du protocole SNMP produits par la console du système NMS du réseau câblé en direction de l'adresse de gestion du service portail.

L'outil Ping du portail CTP DOIT être mis en œuvre en utilisant la fonction "écho" du protocole de message de commande Internet (ICMP, *Internet control message protocol*). Le portail CTP produira une demande d'écho ICMP et on attend de l'appareil IP de LAN qu'il retourne une réponse d'écho ICMP.

Au § 6.4.4 figure la liste des paramètres et réponses pour l'outil Ping. Noter que le délai pour la réponse à la demande n'est pas mémorisé, dans la mesure où le temps de propagation de trame chez l'utilisateur peut être plus rapide que ce que les unités de temps standard (en ms) peuvent effectivement mesurer. Pour les mesures de performance, c'est l'outil de vitesse de connexion qui devrait être utilisé.

Au § 12.2.1.2 figure le détail du fonctionnement de l'outil Ping.

6.4.4 Exigences pour le portail CTP

Le portail CTP DOIT implémenter l'outil de vitesse de connexion avec les paramètres dont la liste figure ci-dessous, où les guillemets simples indiquent l'objet de base MIB du portail CTP. Les numéros entre crochets sont les options ou les limites inférieure et supérieure de la gamme de paramètres, et le numéro entre parenthèses est la valeur par défaut:

– <cabhCtpConnSrcIp> (égal à la valeur de cabhCdpServerRouter) – L'adresse IP de LAN utilisée comme source de l'outil de vitesse de connexion;

– <cabhCtpConnDestIp> – L'adresse IP de LAN utilisée comme destination de l'outil de vitesse de connexion;

  NOTE 1 – Peut être réglé sur n'importe quelle adresse Ipv4 valide, pour trouver les appareils IP de LAN dans le secteur d'adresse LAN-Trans.

– <cabhCtpConnProto> [UDP (1), TCP (2)] (UDP) – Le protocole utilisé pour l'outil de vitesse de connexion;

– <cabhCtpConnPort> [1 à 65535] (7) – Le port utilisé pour l'outil de vitesse de connexion.

  NOTE 2 – IANA réserve le port 7 pour cette utilisation. D'autres ports peuvent être utiles.

– <cabhCtpConnNumPkts> [1 à 255] (1) – Le nombre de paquets à envoyer pour l'outil de vitesse de connexion;

– <cabhCtpConnPktSize> [–64 à 1518] (64) – Taille des trames d'essai en octets pour l'outil de vitesse de connexion;

– <cabhCtpConnTimeOut> [0 à 600 000] (600 000) – Valeur de la temporisation en millisecondes, pour la réponse à l'outil de vitesse de connexion;

NOTE 3 – Une valeur de zéro indique qu'il n'y a pas de temporisation et ne peut être utilisée que pour le protocole TCP.

– <cabhCtpConnControl> [notRun (1), début (2), arrêt (3)] – Commande pour l'essai de vitesse de connexion;

– <cabhCtpConnStatus> [en cours (1), terminé (2), arrêt (3)] – Etat de l'essai de vitesse de connexion;

– <cabhCtpConnPktsSent> [1 à 255] – Nombre de paquets envoyés pendant l'essai de vitesse de connexion;

– <cabhCtpConnPktsRecv> [0 à 255] – Nombre de paquets reçus pendant l'essai de vitesse de connexion;

NOTE 4 – Cette valeur permet à l'opérateur de déterminer si la temporisation est arrivée à expiration (PktsSent > PktsRecv) du fait de la perte de paquets, en supposant que la temporisation a été calculée correctement. Cette paire de paramètres a été incluse pour permettre la détection de perte de paquets UDP. Dans les conditions normales de fonctionnement, PktsRecv est égal à PktsSent.

– <cabhCtpConnAvgRTT> [0 à 600 000] – Temps moyen en millisecondes de l'aller-retour résultant pour accuser réception des paquets;

– <cabhCtpConnMaxRTT> [0 à 600 000] – Temps maximal en millisecondes de l'aller-retour maximal pour accuser réception des paquets;

– <cabhCtpConnMinRTT> [0 à 600 000] – Temps minimal en millisecondes de l'aller-retour maximal pour accuser réception des paquets;

– <cabhCtpConnNumIcmpError> [0 à 255] – Nombre d'erreurs de protocole ICMP;

NOTE 5 – La valeur peut inclure le réseau ou l'hôte "interdit" ou "injoignable". Ce paramètre est nul par défaut, ou lorsque aucune erreur n'est survenue.

– <cabhCtpConnIcmpError> [0 à 255] – Dernière erreur de protocole ICMP.

Le portail CTP DOIT implémenter l'outil Ping de portail CTP avec les paramètres dont la liste figure ci-dessous, où les guillemets simples indiquent l'objet MIB de portail CTP, les nombres entre crochets sont les limites inférieure et supérieure de la gamme du paramètre, et le nombre entre parenthèses est la valeur par défaut:

– <cabhCtpPingSrcIp> (égal à la valeur de cabhCdpServerRouter) – Adresse IP de LAN utilisée comme source de l'outil Ping à distance;

– <cabhCtpPingDestIp> – Adresse IP de LAN utilisée comme destination de l'outil Ping à distance;

– <cabhCtpPingProto> [icmp (1)] (icmp) – Protocole utilisé pour l'outil Ping à distance;

– <cabhCtpPingNumPkts> [1 à 4] (1) – Nombre de paquets à envoyer à chaque hôte pour l'outil Ping à distance;

– <cabhCtpPingPktSize> [−64 à 1518] (64) – Taille des trames d'essai en octets pour l'essai Ping à distance;

– <cabhCtpPingTimeBetween> [0 à 600 000] (1000) – Temps en millisecondes entre l'envoi d'un paquet et le suivant pendant l'essai Ping à distance;

– <cabhCtpPingTimeOut> [0 à 600 000] (5000) – Temporisation en millisecondes pour la réponse à l'envoi d'un seul ping durant l'essai Ping à distance;

– <cabhCtpPingControl> [non en cours (1), début (2), arrêt (3)] – Commande pour l'essai Ping à distance;

– <cabhCtpPingStatus> [en cours (1), terminé (2), arrêté (3)] – Etat de l'essai Ping à distance;

– <cabhCtpPingNumSent> [0 à 254] – Nombre de ping envoyés durant l'essai Ping à distance;

– <cabhCtpPingNumRecv> [0 à 254] – Nombre de ping reçus durant l'essai Ping à distance.

6.5 Rapport d'événement

Les mécanismes de rapport et commande d'événements utilisé est celui de la norme RFC 2669, qui définit un format standard pour les information de rapport d'événement, sans considération du type de message, y compris un tableau d'enregistrement d'événement locaux dans lequel certaines entrées vont persister au long des réamorçages du service portail. Noter que des événements peuvent être générés par toutes parties d'un service portail, mais que le portail CMP enregistre et/ou rapporte les événements soit localement ou sur un serveur Syslog ou Trap.

6.5.1 Notification d'événement

Le service portail DOIT générer des événements asynchrones qui indiquent les événements et situations importants comme spécifié à l'Annexe B. Les événements peuvent être emmagasinés dans un enregistreur d'événements interne, emmagasinés dans une mémoire non volatile, rapportés à d'autres entités du protocole SNMP (comme des messages TRAP ou INFORM du protocole SNMP), ou envoyés en tant que message d'événement SYSLOG à un serveur SYSLOG prédéfini.

Le service portail DOIT accepter le mécanisme de notification d'événement suivant:

- enregistrement d'événements locaux lorsque certaines entrées dans l'enregistrement local peuvent être identifiés comme persistant lors d'un réamorçage du service portail;
- messages TRAP et INFORM du protocole SNMP;
- SYSLOG.

La notification d'événement par le service portail est entièrement configurable. Le service portail DOIT implémenter le tableau docsDevEvControlTable de la norme [RFC 2669] pour le rapport sur la commande des événements. Les valeurs de bits suivantes pour les docsDevEvReporting d'objets de la norme [RFC 2669] DOIVENT être acceptées par le service portail:

- 1: local non volatile (0)
- 2: traps(1)
- 3: syslog(2)
- 4: local volatile(3)
- 5: inform(4)

Les messages de demande SET (*établissement*) du protocole SNMP au docsDevEvReporting d'objets de la norme [RFC 2669] utilisant les valeurs suivantes DOIVENT résulter en une erreur "Valeur erronée" pour les unités PDU du protocole SNMP:

- 0x20 = syslog seulement
- 0x40 = trap seulement
- 0x60 = (trap + syslog) seulement

Un événement rapporté par Trap, Syslog, ou Inform DOIT aussi générer une entrée d'enregistrement local non volatile comme décrit au § 6.5.1.1.

6.5.1.1 Enregistrement d'événement local

Le service portail DOIT maintenir un seul tableau d'événement d'enregistrement local qui contient les événements emmagasinés à la fois volatiles locaux et non volatiles locaux. Les événements emmagasinés comme événements locaux non volatiles DOIVENT persister à travers les réamorçages du service portail. Le tableau d'événements d'enregistrement local DOIT être organisé comme une mémoire tampon cyclique avec un minimum de dix entrées. Le tableau unique d'événements d'enregistrement local DOIT être accessible à travers le tableau docsDevEventTable comme défini dans la norme [RFC 2669].

Les descriptions d'événement DOIVENT apparaître en anglais. Les descriptions d'événement NE DOIVENT PAS dépasser 255 octets, ce qui est le maximum défini pour la chaîne SnmpAdminString.

L'identifiant d'événement (*EventId*) est un entier arithmétique de 32 bits. Les EventId allant de 0 à $(2^{31} - 1)$ sont réservés. L'EventId DOIT être converti à partir des codes d'erreur définis à l'Annexe B. Les EventId allant de 2^{31} à $(2^{32} - 1)$ DOIVENT être utilisés comme des EventId spécifiques du fabricant utilisant le format suivant:

- Bit 31 mis pour indiquer un événement spécifique du fabricant;
- Bits 30-16 contiennent les 15 derniers bits du numéro d'entreprise SNMP du fabricant;
- Bits 15-0 utilisés par le fabricant pour numéroter ses événements.

L'objet docsDevEvIndex de la norme [RFC 2669] sert à ordonner plus ou moins les événements dans l'enregistrement. Le marquage des événements d'enregistrement local comme local volatile et local non volatile nécessite une méthode pour synchroniser les valeurs de docsDevEvIndex entre deux types d'événements après un réamorçage du service portail. Après un réamorçage de service portail, pour synchroniser les valeurs de docsDevEvIndex pour les événements volatiles et non volatiles, on DOIT utiliser la procédure suivante:

- les valeurs de docsDevEvIndex pour les événements d'enregistrement local marqués comme local non volatile DOIVENT être renumérotés en commençant par 1;
- l'enregistrement local DOIT alors être initialisé avec les événements marqués comme local non volatile dans le même ordre que celui qu'ils avaient immédiatement avant le réamorçage;
- les événements suivants mémorisés dans l'enregistrement local, qu'ils soient marqués local volatile ou local non volatile, DOIVENT utiliser les valeurs croissantes de docsDevEvIndex.

Un rétablissement de l'enregistrement local initialisé par le moyen d'un SNMP SET d'objet [RFC 2669] docsDevEvControl DOIT supprimer tous les événements de l'enregistrement local, y compris les événements enregistrés marqués à la fois comme local volatile et local non volatile.

6.5.1.2 TRAP et INFORM du protocole SNMP

Le service portail DOIT accepter l'unité PDU Trap du protocole SNMP comme décrit dans la norme [RFC 2571]. Le service portail DOIT accepter l'unité PDU INFORM du protocole SNMP comme décrit dans la norme [RFC 2571]. INFORM est une variante de trap et exige de hôte de réception qu'il accuse réception de l'arrivée d'une unité PDU de demande InformRequest avec une unité PDU de réponse InformResponse.

Lorsqu'un trap standard du protocole SNMP est activé dans le service portail, il DOIT envoyer des notifications pour chaque événement de cette catégorie dont la priorité est soit "erreur" soit "notice".

Le service portail PEUT accepter des événements spécifiques du fabricant. S'ils sont acceptés, les événements de service portail spécifiques du fabricant rapportables via TRAP du protocole SNMP DOIVENT être décrits dans une base MIB privée qui est distribuée avec le service portail. Lors de la définition d'un trap SNMP spécifique du fabricant, la déclaration OBJECTS de la définition du trap privé DEVRAIT contenir au moins les objets décrits ci-dessous:

- EvLevel;
- EvIdText;
- seuil d'événement (s'il y en a un pour le trap);
- IfPhysAddress (adresse physique associée à l'adresse IP du WAN-Man du service portail).

Plus d'objets peuvent être, selon le besoin, contenus dans la déclaration OBJECTS.

6.5.1.3 Syslog

Les messages SYSLOG produits par le service portail DOIVENT être du format suivant:

<level>PortalServicesElement[vendor]: <eventId> text

où:

level (*niveau*) – Présentation ASCII de la priorité de l'événement, inclus entre des guillemets simples, il est construit comme le "au bit près" OU la fonction par défaut (128) et la priorité d'événement (0-7). Le niveau résultant est compris entre 128 et 135.

vendor (*fabricant*) – C'est le nom du fabricant pour les messages SYSLOG spécifiques du fabricant ou "CABLE" pour les messages standard du câble.

eventId (*Identificateur d'événement*) – Présentation ASCII du nombre ENTIER en format décimal, inclus entre guillemets simples, qui identifie de façon univoque le type d'événement. Cet EventID DOIT être le même nombre que celui qui est emmagasiné dans l'objet docsDevEvId dans le tableau docsDevEventTable. Pour les événement standard du câble, ce nombre est converti à partir du code d'erreur suivant les règles ci-après:

- c'est un nombre décimal à huit chiffres;
- les deux premiers chiffres (les plus à gauche) sont le code ASCII (décimal) pour la lettre dans le code d'erreur;
- les quatre chiffres suivants sont remplis par 2 ou 3 chiffres entre la lettre et le point dans le code d'erreur, et l'espace vide à gauche est rempli avec des zéros;
- les deux derniers chiffres sont remplis avec le numéro après le point dans le code d'erreur, et l'espace vide à gauche est rempli avec des zéros.

Par exemple, l'événement D04.2 est converti en 68000402, et l'événement Event I114.1 est converti en 73011401.

Veuillez noter que cette notion n'utilise qu'une petite partie des espaces de numéros disponibles réservés pour le câble (0 à $2^{31} – 1$). La première lettre d'un code d'erreur est toujours en majuscule.

text – Pour les messages câble standard, cette chaîne DOIT avoir la description textuelle comme défini à l'Annexe B.

Exemple de l'événement syslog pour l'événement D04.2: "Time of the day received in invalid format" (*heure reçue dans un format non valide*):

<132>PS Element[CABLE]: <68000402> Time of the day received in invalid format.

Dans l'exemple de l'événement syslog, le nombre 68000402 est le nombre alloué à cet événement particulier.

6.5.2 Format des événements

Les messages d'événement de gestion PEUVENT contenir les informations suivantes:

- Event Counter (*compteur d'événement*) – Indicateur de la séquence d'événement
- Event Time (*heure de l'événement*) – Heure à laquelle l'événement survient
- Event Priority (*priorité d'événement*) – Sévérité de la condition. La norme [RFC 2669] définit huit niveaux de sévérité. La sévérité d'événement par défaut peut être remplacée par une valeur différente pour chaque événement donné via l'interface de protocole SNMP.
- Event Enterprise Number (*numéro entreprise d'événement*) – Ce numéro identifie les événements soit comme un événement standard soit comme un événement défini par le fabricant.

- Event ID (*identifiant d'événement*) – Identifie l'événement exact lorsqu'il est combiné avec le numéro entreprise d'événement. Les fabricants définissent leurs propres identifiants d'événement. Les événements de gestion standard sont définis à l'Annexe B. Chaque événement de gestion décrit dans l'annexe s'est vu allouer un identifiant d'événement.
- Event Text (*texte de l'événement*) – Décrit l'événement sous une forme lisible par l'homme.
- MAC Address (*adresse MAC*) – Décrit l'adresse de couche MAC de l'appareil.

Le format exact de ces informations pour les trap et inform est défini à l'Annexe B. Le format des messages SYSLOG est défini dans la partie exigences de ce paragraphe.

6.5.2.1 Priorités d'événements

Le document [RFC 2669] définit huit différents niveaux de priorité et les mécanismes de rapport correspondants pour chaque niveau. Les événements standard spécifiés dans ce document utilisent ces niveaux de priorité.

1) Evénement d'urgence (priorité 1)

   Réservé aux erreurs "fatales" de matériel ou de logiciel spécifiques du fabricant qui empêchent le fonctionnement normal du système et causent le réamorçage du système de rapport. Chaque fabricant peut définir son propre ensemble d'événements d'urgence. Des exemples de tels événements pourraient être "pas de mémoire tampon disponible", "échec des essais de mémoire", etc.

2) Evénement d'alerte (priorité 2)

   Echec sérieux qui cause le réamorçage du système mais ce réamorçage n'est pas causé par un dysfonctionnement du matériel ou du logiciel. Après récupération de l'événement, le système DOIT envoyer la notification de démarrage à froid/chaud.

3) Evénement critique (priorité 3)

   Echec sérieux qui empêche l'appareil de transmettre des données mais dont on peut se remettre sans réamorçage du système. Après récupération d'un événement critique, le service portail DOIT envoyer la notification Link up (*liaison active*). Des exemples de tels événements peuvent être des problèmes de fichier de configuration de service portail ou l'incapacité à obtenir une adresse IP par le protocole DHCP.

4) Evénement d'erreur (priorité 4)

   Echec qui pourrait interrompre le flux normal de données mais ne cause pas de réamorçage de l'appareil. Les événements d'erreur peuvent être rapportés en temps réel en utilisant les mécanismes TRAP ou SYSLOG.

5) Evénement avertissement (priorité 5)

   Echec qui pourrait interrompre le flux normal de données. Le rapport Syslog et Trap est désactivé par défaut pour ce niveau.

6) Evénement notice (priorité 6)

   Evénement d'importance qui n'est pas un échec et pourrait être rapporté en temps réel en utilisant le mécanisme TRAP ou SYSLOG. Des exemples des événements NOTICE sont "Démarrage à froid", "Démarrage à chaud', "Liaison active"' et "Mise à jour SW réussie".

7) Evénement d'information (priorité 7)

   Evénement d'importance qui n'est pas un échec, mais qui pourrait être utile pour garder la trace du fonctionnement normal de l'appareil.

8) Evénement déboguage (priorité 8)

   Réservé à des événements non critiques spécifiques du fabricant.

La priorité associée aux événements standard NE DOIT PAS être changée.

Le Tableau 14 indique les types de notification par défaut pour les diverses priorités d'événements. Le service portail DOIT implémenter les types de notification par défaut pour les huit priorités d'événement. Par exemple, le type de notification par défaut pour les événements Urgence et Alerte est de les placer dans l'enregistrement local comme entrées non volatiles.

Tableau 14/J.191 – Types de notification par défaut pour les priorités d'événements pour le service portail

Priorité d'événement	Local non volatile (bit-0)	SNMP Trap (bit-1)	SYSLOG (bit-2)	Local volatile (bit-3)	Note
1) Urgence	Oui	Non	Non	Non	Spécifique du fabricant
2) Alerte	Oui	Non	Non	Non	Standard
3) Critique	Oui	Non	Non	Non	Standard
4) Erreur	Non	Oui	Oui	Oui	Standard
5) Avertissement	Non	Non	Non	Oui	Standard
6) Notice	Non	Oui	Oui	Oui	Standard
7) Information	Non	Non	Non	Non	Standard et Spécifique du fabricant
8) Déboguage	Non	Non	Non	Non	Spécifique du fabricant

Le Tableau 15 indique le niveau minimal d'acceptation requis pour les types de notification pour les diverses priorités d'événements. Par exemple, le service portail doit accepter au minimum les entrées non volatiles dans l'enregistrement local pour les priorités d'événement d'urgence, d'alerte et critique. Le service portail DOIT accepter les exigences minimales pour l'implémentation des priorités d'événement de chaque type de rapport d'événement. Le service portail PEUT choisir de rapporter une priorité d'événement avec plus de types de notification que ne sont exigés au Tableau 15.

Tableau 15/J.191 – Niveau minimal d'acceptation de type de notification par priorité d'événement dans le PS

Priorité d'événement	Local non volatile (bit-0)	SNMP Trap (bit-1)	SYSLOG (bit-2)	Local volatile (bit-3)	Note
1) Urgence	Oui	Oui	Oui	Oui	Spécifique du fabricant
2) Alerte	Oui	Oui	Oui	Oui	Standard
3) Critique	Oui	Oui	Oui	Oui	Standard
4) Erreur		Oui	Oui	Oui	Standard
5) Avertissement		Oui	Oui	Oui	Standard
6) Notice		Oui	Oui	Oui	Standard
7) Information		Oui	Oui	Oui	Standard et Spécifique du fabricant
8) Déboguage		Oui	Oui	Oui	Spécifique du fabricant

6.5.2.2 Evénement standard

Le service portail DOIT envoyer les traps génériques de protocole SNMP suivants, comme défini dans les normes [RFC 1907] et [RFC 2863]:

- coldStart [RFC 1907] (*démarrage à froid*);
- linkUp [RFC 2863] (*liaison active*);
- linkDown [RFC 2863] (*liaison désactivée*);
- SNMP authentication-Failure [RFC 1907] (*échec d'authentification SNMP*).

Le service portail DOIT être capable de générer des notifications d'événement fondées sur la liste d'événements standard de l'Annexe B.

6.5.3 Ralentisseur et limiteur d'événements

Le service portail DOIT accepter le ralentisseur et le limiteur TRAP/INFORM et SYSLOG du protocole SNMP comme décrits dans la norme [RFC 2669].

Le service portail DOIT considérer que les événements sont identiques si leurs identifiants EventId sont identiques.

La norme [RFC 2669] spécifie quatre états de ralentisseurs:

- unconstrained(1) amène la transmission des trap et messages syslog sans considération du réglage des seuils.
- maintainBelowThreshold(2) amène la suppression des trap et messages syslog si le nombre de traps devait excéder le seuil.
- stopAtThreshold(3) amène la cessation de la transmission de trap au niveau du seuil, et elle ne reprend pas avant qu'on ne le lui ordonne.
- inhibited(4) amène la suppression de toute transmission de trap et messages syslog.

Un seul événement DOIT être traité comme événement unique pour le compte du seuil, c'est-à-dire qu'un événement causant à la fois un trap et un message syslog est toujours traité comme événement unique.

7 Outils d'approvisionnement

7.1 Introduction/Aperçu général

L'élément de service portail et les appareils IP de LAN doivent être correctement initialisés et configurés afin d'échanger des informations significatives l'un avec l'autre et avec les éléments connectés au réseau câblé et l'Internet. Les outils d'approvisionnement permettent à cette initialisation et configuration de survenir sans coupure et avec l'intervention minimale de l'utilisateur. Ils permettent aussi aux câblo-opérateurs d'apporter de la valeur ajoutée aux abonnés aux services de données à haut débit en définissant les processus par lesquels le câblo-opérateur peut faciliter et personnaliser l'initialisation et la configuration du service portail et de l'appareil IP de LAN. Les trois outils d'approvisionnement définis pour accomplir cette tâche sont énumérés ci-dessous:

- fonction portail DHCP par câble (CDP, *cable DHCP portal*) dans l'élément de service portail;
- outil de configuration globale de service portail (BPSC, *bulk PS configuration*);
- heure client dans l'élément de service portail.

7.1.1 Modes d'approvisionnement

Deux modes d'approvisionnement sont acceptés. On les appelle mode d'approvisionnement DHCP (mode DHCP) et mode d'approvisionnement SNMP (mode SNMP). Ces deux modes d'approvisionnement sont comparés au Tableau 16.

Tableau 16/J.191 – Modes d'approvisionnement

	Mode DHCP	**Mode SNMP**
Déclenchement du fichier de configuration PS	Déclenché par la présence d'informations du serveur TFTP dans le message DHCP	Déclenché par le système NMS via un message SNMP
Exigences du fichier de configuration PS	Le téléchargement du fichier de configuration PS est exigé	Le téléchargement du fichier de configuration PS n'est pas exigé

Le comportement spécifié des outils d'approvisionnement dépend du mode d'approvisionnement dans lequel fonctionne le service portail.

Le paragraphe 13 Processus d'approvisionnement décrit la séquence des événements pour chacun des deux modes d'approvisionnement.

7.1.2 Architecture d'approvisionnement

La Figure 14 illustre l'architecture d'approvisionnement. Les éléments de service portail vont interagir avec les fonctions de serveur dans le réseau câblé à l'interface HFC, ou avec les appareils IP de LAN pour répondre aux lignes directrices de conception du système énumérées au § 7.2.1.

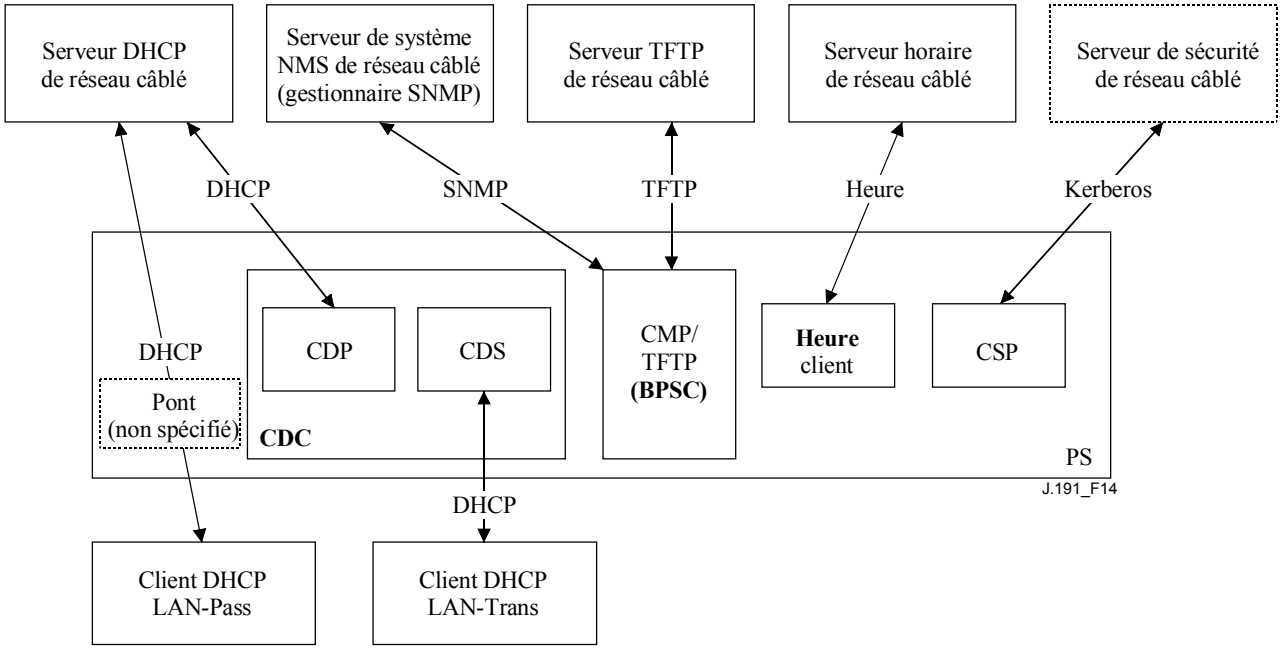

Figure 14/J.191 – Architecture d'approvisionnement

7.1.3 Objectifs

Les objectifs du portail DHCP sur le câble sont:

- allouer, via DHCP, les adresses IP aux appareils IP de LAN conformément aux règles spécifiées dans le présent paragraphe.
- acquérir, via DHCP, les adresses IP pour les interfaces WAN des éléments de service portail conformément aux règles spécifiées dans le présent paragraphe.

Les objectifs de l'outil de configuration globale du service portail sont:

- télécharger et traiter les fichiers de configuration.

Les objectifs de l'heure client sont:

- synchroniser l'horloge dans l'élément de service portail avec celle de la tête de système du réseau.

7.1.4 Hypothèses

Les hypothèses de fonctionnement du portail DHCP sur le câble sont:

1) les appareils IP de LAN implémentent un client DHCP comme défini par la norme [RFC 2131];
2) le système d'approvisionnement du réseau câblé implémente un serveur DHCP comme défini par la norme [RFC 2131];
3) si le système d'approvisionnement du réseau câblé du serveur DHCP accepte l'option 61 (option d'identifiant client) du protocole DHCP, les interfaces IP WAN-Man et toutes les interfaces WAN-Data peuvent partager une adresse MAC commune;
4) les appareils IP de LAN peuvent accepter diverses options DHCP et extensions fabricant BOOTP, permises par la norme [RFC 2132].

Les hypothèses de fonctionnement de l'outil de configuration globale de service portail sont:

– la configuration globale de service portail sera réalisée par le téléchargement d'un fichier de configuration PS contenant un ou plusieurs paramètres.

Les hypothèses de fonctionnement de l'heure client sont:

– le serveur DHCP de tête de système fournira une option DHCP à l'interface de gestion WAN, qui reste en relation avec un serveur horaire, fonctionnant au sein du réseau de tête de système.

7.2 Architecture de portail DHCP de câble

Le portail DHCP de câble (CDP) est un des trois outils d'approvisionnement présentés au § 7.1. Le présent paragraphe décrit les lignes directrices de la conception du système, la description du système et les exigences relatives au portail CDP.

7.2.1 Lignes directrices de conception du système de portail DHCP de câble

Les lignes directrices de conception suivantes dans le Tableau 17 pilotent les fonctionnalités définies pour le portail CDP:

Tableau 17/J.191 – Lignes directrices de conception du système de CDP

Numéro	Lignes directrices de conception du système de CDP
CDP 1	Les mécanismes d'adressage seront sous le contrôle de l'opérateur, et fourniront au câblo-opérateur la connaissance et l'accessibilité au **service portail** et aux appareils IP de LAN.
CDP 2	L'acquisition d'adresse et les processus de gestion n'exigeront pas d'intervention humaine (en supposant qu'un compte d'usager/établissement a déjà été établi).
CDP 3	L'acquisition d'adresse et de gestion seront échelonnables pour supporter l'augmentation attendue du nombre d'appareils IP de LAN.
CDP 4	Il est préférable que les adresses IP de LAN restent les mêmes après des événements tels qu'une interruption d'alimentation ou un changement de fournisseur de service Internet.

Tableau 17/J.191 – Lignes directrices de conception du système de CDP

Numéro	Lignes directrices de conception du système de CDP
CDP 5	On fournira un mécanisme permettant de surveiller et contrôler le nombre d'appareils IP de LAN dans le secteur LAN-Trans.
CDP 6	Au domicile, les communications continueront de fonctionner comme prévu pendant les périodes d'interruption du serveur d'adresses de la tête de système. Le soutien de l'adressage sera fourni pour les appareils IP de LAN nouvellement ajoutés et les adresses expirées pendant les interruptions de serveur d'adresses distant.
CDP 7	Les adresses IP seront conservées si possible à la fois (aussi bien des adresses acheminables globalement que les adresses privées de gestion de réseau câblé).

7.2.2 Description du système de portail DHCP par câble

Le portail DHCP par câble (CDP) est l'entité logique responsable des activités d'adressage. Les responsabilités du portail CDP pour la demande d'adresse et l'allocation d'adresse incluent:

- l'allocation d'adresse IP, la maintenance d'adresse IP et la délivrance des paramètres de configuration (via DHCP) aux appareils IP de LAN dans le secteur d'adresse LAN-Trans;
- l'acquisition d'un WAN-Man et de zéro ou plus adresses IP WAN-Data et les paramètres associés de configuration DHCP pour l'élément de service portail;
- fournir des informations au portail de nommage du câble (CNP) en soutien des services de nom d'hôte d'appareil IP de LAN.

L'élément de service portail exige une adresse IP pour son rôle de routeur de trafic chez l'abonné (voir paragraphe 8, Traitement de paquet et traduction d'adresse), un serveur DHCP (CDS), et un serveur DNS (voir paragraphe 9, Résolution de nom). Pour chacune de ces trois fonctions de serveur d'élément de service portail et de routeur, une adresse IP de LAN est sauvegardée dans la base de données du service portail. Chacune peut être atteinte via un objet MIB différent, dont la liste figure ci-dessous et dans le Tableau 17.

– Adresse de routeur (passerelle par défaut) cabhCdpServerRouter
– Adresse de système de nom de domaine (DNS) cabhCdpServerDnsAddress
– Adresse de serveur de configuration dynamique d'hôte (DHCP) (CDS) cabhCdpServerDhcpAddress

La valeur par défaut de cabhCdpServerRouter est 192.168.0.1. Les valeurs par défaut de cabhCdpServerDnsAddress et cabhCdpServerDhcpAddress sont égales à la valeur de cabhCdpServerRouter.

Comme indiqué à la Figure 15, les fonctionnalités du portail CDP sont incorporées dans deux éléments fonctionnels résidant au sein du CDP: le serveur DHCP câble (CDS) et le client DHCP câble (CDC).

La Figure 15 illustre aussi l'interaction entre les composants du portail CDP et les secteurs d'adresse présentés au paragraphe 5. Le client CDC échange des messages DHCP avec le serveur DHCP dans le réseau câblé (secteur d'adresse de gestion WAN) pour acquérir une adresse IP et des options DHCP pour le service portail, pour les besoins de la gestion. Le client CDC peut aussi échanger des messages DHCP avec le serveur DHCP dans le réseau câblé (secteur d'adresse de données WAN) pour acquérir zéro ou plus adresses IP au nom des appareils IP de LAN dans le secteur LAN-Trans. Le serveur CDS échange des messages DHCP avec les appareils IP de LAN dans le secteur LAN-Trans, et alloue des adresses IP privées, accorde des locations, et pourrait fournir des options DHCP aux clients DHCP dans ces appareils IP de LAN. Les appareils IP de LAN dans le secteur LAN-Pass reçoivent leurs adresses IP, locations, et options DHCP directement du serveur DHCP

dans le réseau câblé. Le portail CDP transmet simplement les messages DHCP entre le serveur DHCP dans le réseau câblé et les appareils IP de LAN dans le secteur LAN-Pass.

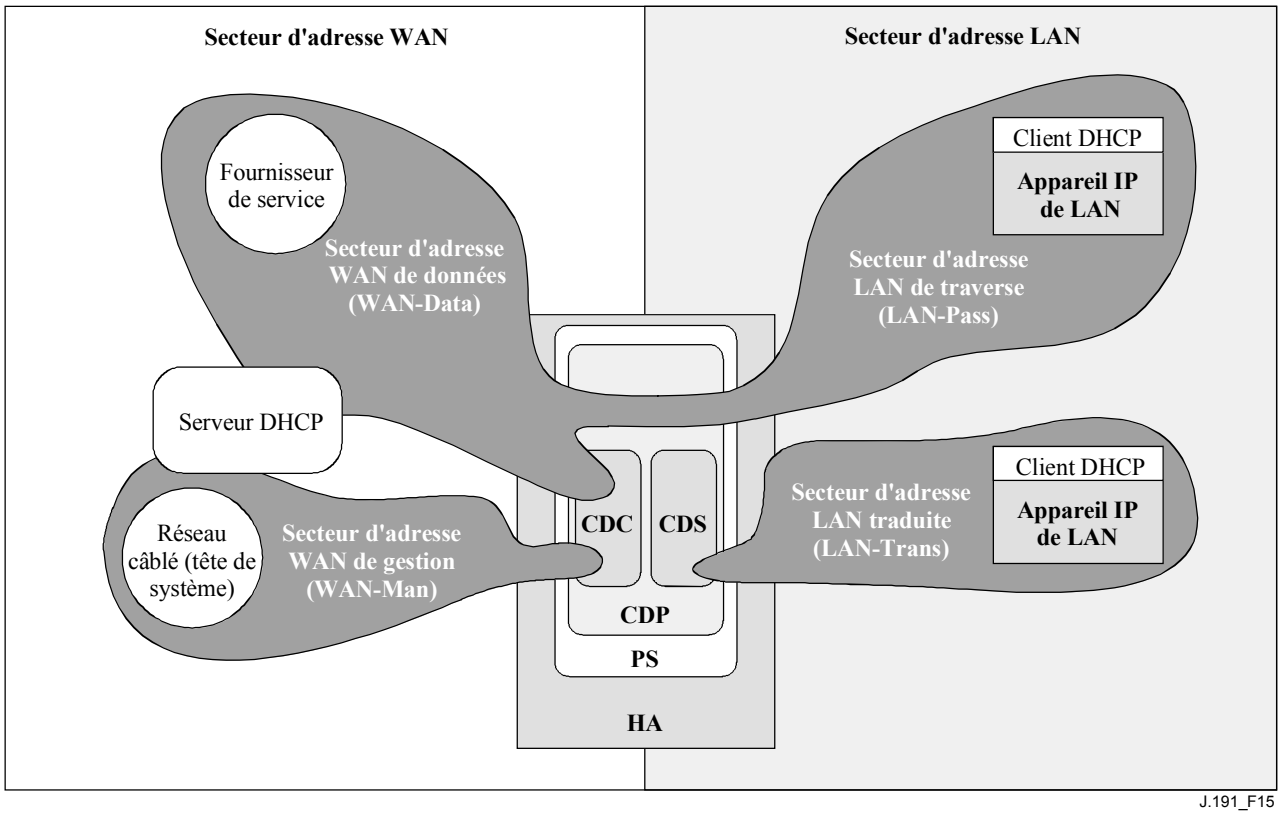

Figure 15/J.191 – Fonctions du portail CDP

7.2.2.1 Description du système de serveur CDS

Le serveur CDS est un serveur DHCP standard comme défini dans la norme [RFC 2131], et ses responsabilités sont:

- le serveur CDS alloue les adresses et délivre les paramètres de configuration DHCP aux appareils IP de LAN recevant une adresse dans le secteur d'adresse LAN-Trans. Le serveur CDS apprend les options DHCP du système NMS et fournit ces options DHCP aux appareils IP de LAN. Si les options DHCP n'ont pas été fournies par le système NMS (par exemple lorsque le service portail s'amorce lors d'une interruption du câble), le serveur CDS s'appuie sur les valeur par défaut par construction (DefVals) pour les options nécessaires;
- le serveur CDS est capable de fournir des services d'adressage aux appareils IP de LAN, indépendamment de l'état de connexion du WAN;
- le nombre d'adresses fournies par le serveur CDS aux appareils IP de LAN est contrôlable par le système NMS. Le comportement du serveur CDS lorsque la limite de réglage d'un câblo-opérateur est dépassée est aussi configurable via le système NMS. Parmi les actions de serveur CDS possibles lorsque la limite est dépassée figurent:
  1) allouer une adresse IP LAN-Trans et traiter l'interconnexion LAN à LAN CAT comme elle devrait normalement se produire si la limite n'avait pas été dépassée;
  2) ne pas allouer d'adresse aux appareils IP de LAN demandeurs;
- en l'absence d'informations sur l'heure de la part du serveur horaire, le serveur CDS utilise la date de départ par défaut du service portail de 0 (1er janvier 1900), met à jour l'heure d'expiration pour toutes locations actives dans le secteur LAN-Trans pour se resynchroniser

avec les clients DHCP dans les appareils IP de LAN, et assure la maintenance des locations sur la base de ce point de départ jusqu'à ce que le service portail se synchronise avec le serveur horaire dans le réseau câblé;

- lors d'un réamorçage ou rétablissement du service portail, le serveur CDS reste inactif jusqu'à son activation par le service portail après le téléchargement réussi du fichier de configuration du service portail ou après cinq échecs par le service portail du téléchargement de son fichier de configuration, quelque soit celui qui intervient le premier. Le serveur CDS est ainsi prémuni contre l'octroi de locations DHCP dans le secteur LAN-Trans jusqu'à ce qu'il y ait eu une opportunité raisonnable pour le câblo-opérateur de mettre à jour les paramètres de location LAN-Trans tels que cabhCdpServerLeaseTime, cabhCdpLanPoolStart, et cabhCdpLanPoolEnd;
- si le mode primaire de traitement de paquet du service portail (cabhCapPrimaryMode) a été réglé à Traverse, le serveur CDS est alors désactivé.

Les appareils IP de LAN peuvent recevoir des adresses qui résident dans le secteur LAN-Pass. Comme indiqué à la Figure 15, les demandes d'adresse LAN-Pass sont servies par l'infrastructure d'adressage du WAN, et non par le service portail. Le processus d'adressage LAN-Pass surviendra lorsque le service portail est configuré pour fonctionner en mode Traverse ou en mode mixte Pontage/Routage (voir au § 8.2.2.2 pour plus de détails). Dans ces cas, les interactions DHCP surviendront directement entre les appareils IP de LAN et les serveurs de tête de système, et la présente Recommandation ne spécifie pas le processus.

Tout au long de la présente Recommandation, les termes allocation automatique, allocation dynamique, et allocation manuelle sont utilisés comme défini dans la norme [RFC 2131]. L'allocation automatique des adresses IP au sein d'un secteur d'adresse LAN-Trans sera permanente, et le serveur CDS peut réutiliser les adresses automatiques si des adresses disponibles ont été allouées. **Options DHCP fournies au serveur CDS**, les objets cabhCdpServer dans la base MIB du portail CDP sont utilisés par le serveur CDS pour indiquer les options DHCP offertes aux appareils IP de LAN affectés à une adresse LAN-Trans. Options DHCP fournies au serveur CDS, les objets cabhCdpServer persistent après une interruption d'alimentation électrique du service portail et le système NMS peut établir, lire, écrire et supprimer ces objets. Options DHCP fournies au serveur CDS, les objets cabhCdpServer sont conservés pendant les périodes d'interruption du câble et ces objets sont proposés aux appareils IP de LAN affectés à une adresse LAN-Trans pendant les périodes d'interruption du câble. Le stockage persistant au client CDC des options DHCP est cohérent avec la section 2.1 de la norme [RFC 2131]. Les valeurs par défaut des options DHCP fournies au serveur CDS, objets cabhCdpServer, sont définies au Tableau 17, et le système NMS peut rétablir les options DHCP fournies au serveur CDS, objets cabhCdpServer, à leurs valeurs par défaut, en écrivant à l'objet MIB cabhCdpSetToFactory.

Les objets **seuil d'adresse de serveur CDS** (cabhCdpLanTrans) contiennent les paramètres de commande d'événement utilisés par le serveur CDS pour signaler au portail CMP de générer une notification au système de gestion de tête de système, lorsque le nombre d'adresses LAN-Trans allouées par le serveur CDS dépasse le seuil préétabli.

L'objet compte d'adresses (cabhCdpLanTransCurCount) est une valeur indiquant le nombre d'adresses LAN-Trans allouées par le serveur CDS qui ont des locations DHCP actives.

L'objet seuil d'adresses (cabhCdpLanTransThreshold) est une valeur qui indique le moment où une notification est générée au système de gestion de tête de système. La notification est générée lorsque le serveur CDS alloue une adresse à l'appareil IP de LAN qui fait que le compte d'adresses (cabhCdpLanTransCurCount) dépasse le seuil d'adresses (cabhCdpLanTransThreshold).

L'action seuil dépassé (cabhCdpLanTransAction) est l'action prise par le serveur CDS lorsque le compte d'adresses (cabhCdpLanTransCurCount) dépasse le seuil d'adresses (cabhCdpLanTransThreshold). Si l'action seuil dépassé (cabhCdpLanTransAction) permet des

allocations d'adresses après que le compte est dépassé, la notification est générée chaque fois qu'une adresse est allouée. Les actions définies sont:

a) allouer une adresse LAN-Trans comme en cas normal;

b) ne pas allouer d'adresse au prochain appareil IP de LAN demandeur.

Le compte d'adresse (cabhCdpLanTransCurCount) continue d'être mis à jour pendant les périodes d'interruption du câble.

La base MIB du serveur CDS contient aussi les paramètres début de groupe d'adresse (cabhCdpLanPoolStart) et fin de groupe d'adresse (cabhCdpLanPoolEnd). Ces paramètres indiquent la gamme d'adresses qui dans le secteur LAN-Trans peuvent être allouées par le serveur CDS aux appareils IP de LAN.

Le tableau d'adresse LAN du portail CDP (cabhCdpLanAddrTable) contient la liste des paramètres associés aux adresses allouées aux appareils IP de LAN avec des adresses LAN-Trans. Ces paramètres comprennent:

1) les identifiants du client, voir la section 9.14 de la norme [RFC 2132] (cabhCdpLanAddrClientID);

2) l'adresse IP de LAN allouée au client (cabhCdpLanAddrIp);

3) une indication disant si l'adresse a été allouée manuellement (via le CMP) ou automatiquement (via le CDP) (cabhCdpLanAddrConfig).

Le serveur CDS utilise l'adresse MAC pour identifier les appareils IP de LAN.

Le serveur CDS crée une entrée de tableau de portail CDP (cabhCdpLanAddrTable) lorsqu'il alloue une adresse IP à un appareil IP de LAN. Le serveur CDS peut créer des entrées de tableau de portail CDP (cabhCdpLanAddrTable) pendant les périodes d'interruption du câble.

Le tableau de portail CDP (cabhCdpLanAddrTable) entretient un temps de location DHCP pour chaque appareil IP de LAN.

Les entrées de tableau de portail CDP approvisionné avec le système NMS (cabhCdpLanAddrTable) sont conservées pendant les périodes d'interruption du câble et persistent à travers une coupure d'alimentation.

7.2.2.2 Description du système de client CDC

Le client CDC est un client DHCP standard, comme défini dans la norme [RFC 2131], et ses responsabilités comprennent:

- faire des demandes aux serveurs DHCP de tête de système pour l'acquisition des adresses dans le WAN-Man et faire des demandes aux serveurs DHCP de tête de système pour l'acquisition des adresses dans les secteurs d'adresse WAN-Data. Le client CDC comprend de nombreux paramètres de configuration DHCP câble et agit sur eux;
- le client CDC accepte l'acquisition d'un seule adresse IP WAN-Man et zéro ou plus d'adresses IP WAN-Data;
- le client CDC accepte l'option d'identifiant de classe du fabricant (option DHCP 60), l'option d'informations spécifiques du fabricant (option DHCP 43), et l'option d'identifiant client (option DHCP 61);
- dans le cas par défaut, le client CDC acquerra une seule adresse IP pour un usage simultané par les interfaces IP WAN-Man et WAN-Data. Afin de minimiser les changements à apporter aux serveurs DHCP de tête de système existants, l'utilisation d'un identifiant de client (option DHCP 61) par le client CDC n'est pas exigée dans ce cas par défaut.

Le portail CDP accepte diverses options DHCP et extensions BOOTP de fabricant, permises par la norme [RFC 2132], comme décrit au § 7.2.2.2.1. Options 60 et 43 du client DHCP par câble.

L'option d'identifiant de classe du fabricant (option DHCP 60) définit une classe d'appareil spécifique. L'option d'identifiant de classe du fabricant contiendra une chaîne spécifique pour identifier un élément logique de service portail, chaque fois que le client CDC demande une adresse WAN-Man ou WAN-Data.

L'option d'informations spécifiques du fabricant (option DHCP 43) pousse plus loin l'identification du type d'appareil et de ses capacités. Elle décrit le type de composant qui fait la demande, les composants qui sont contenus dans l'appareil (CM, MTA, PS, etc.), le numéro de série de l'appareil et elle permet aussi des paramètres spécifiques de l'appareil.

Les Tableaux 19 et 20 contiennent des précisions sur les exigences de l'acceptation des options DHCP 60 et 43.

7.2.2.2.1 Option 61 du client DHCP par câble

L'élément du service portail peut avoir une ou plusieurs adresses IP de WAN IP associées à une ou plusieurs interfaces de couche de liaison (par exemple, MAC). Le client CDC ne peut donc pas se reposer seulement sur une adresse MAC comme unique valeur d'identifiant de client.

La présente Recommandation permet l'utilisation de l'option d'identifiant de client (option DHCP 61), section 9.14 de la norme [RFC 2132], pour identifier de façon univoque l'interface WAN logique associée à une adresse IP particulière.

Pour permettre la compatibilité avec autant de systèmes d'approvisionnement de câblo-opérateurs que possible, le client CDC devra accepter les modes d'adresses WAN configurables suivants:

mode d'adresse WAN 1: l'élément de service portail utilise une seule adresse IP de WAN. L'élément de service portail a une interface IP WAN-Man et une interface IP WAN-Data, qui partagent une adresse MAC commune. Ces deux interfaces partagent une adresse IP commune, unique. C'est la configuration d'usine par défaut de l'élément de service portail. Le serveur DHCP de tête de système du câblo-opérateur n'a pas, en principe, besoin de modifications de logiciel pour accepter ce mode d'approvisionnement;

mode d'adresse WAN 2: l'élément de service portail utilise deux adresses IP de WAN différentes ou plus. L'élément de service portail peut avoir une ou plusieurs interfaces IP WAN-Man et une ou plusieurs interfaces IP WAN-Data, qui partagent une adresse MAC commune. Ces deux ou plus interfaces devraient avoir chacune leur propre adresse IP, non partagée. Le serveur DHCP de tête de système peut avoir besoin de modifications de logiciel pour accepter l'allocation d'adresses IP multiples à une adresse MAC unique. Dans ce mode, le serveur DHCP de tête de système devra accepter l'allocation IP sur la base de l'identifiant client (option 61), ainsi que l'adresse MAC.

Le mode adresse WAN 2 est déclenché en écrivant une chaîne d'identifiant client unique dans l'entrée cabhCdpWanDataAddrClientId du tableau cabhCdpWanDataAddrTable des bases MIB du portail CDP, pour chaque interface WAN-Data à utiliser. Pour accepter ce mode d'approvisionnement, le câblo-opérateur devra fournir (via le système NMS, le fichier de configuration, ou une entrée normale d'usager via une interface propriétaire) à l'élément de service portail une chaîne unique d'identifiant client pour chaque interface IP WAN-Data.

7.2.3 Exigences du portail DHCP de câble

7.2.3.1 Exigences du portail CDP

L'allocation manuelle d'adresse de portail CDP DOIT être acceptée en utilisant les entrées du tableau CDP (cabhCdpLanAddrTable) créées via le système NMS ou le fichier de configuration.

Les entrées du tableau de gestion d'adresse LAN du portail CDP (cabhCdpLanAddrTable) approvisionné DOIVENT être conservées pendant une interruption du câble et DOIVENT persister après une coupure du courant d'alimentation du service portail. Le serveur CDS DOIT être capable

de fournir des services d'adressage DHCP aux appareils IP de LAN, indépendamment de l'état de connexion du WAN.

7.2.3.2 Exigences du serveur CDS

Le comportement du serveur CDS DOIT être conforme aux exigences du serveur figurant à la section 4.3 de la norme [RFC 2131].

Le serveur CDS DOIT accepter l'allocation d'adresse automatique, dynamique, et manuelle, conformément à la section 1 de la norme [RFC 2131].

Lors d'un réamorçage ou rétablissement du service portail, le serveur CDS NE DOIT PAS échanger de messages DHCP avec les appareils IP de LAN jusqu'à ce que le serveur CDS soit activé par le service portail, à la suite du succès du téléchargement du fichier de configuration du service portail ou à la suite de cinq échecs successifs de tentatives de téléchargement du fichier de configuration du service portail, suivant ce qui se produit d'abord.

Le serveur CDS DOIT allouer les adresses et délivrer les paramètres de configuration DHCP aux seuls appareils IP de LAN qui reçoivent une adresse dans le secteur d'adresse LAN-Trans.

L'allocation automatique d'adresses au sein d'un secteur d'adresse LAN-Trans DOIT être permanente et le serveur CDS PEUT réutiliser les adresses automatiques si toutes les adresses disponibles ont été allouées.

Le serveur CDS DOIT utiliser l'adresse (MAC) de matériel des appareils IP de LAN comme valeur d'identifiant de client.

Le serveur CDS DOIT accepter la base MIB de portail CDP y compris tous les objets dans le tableau cabhCdpLanAddrTable, les objets cabhCdpLanPool, les objets cabhCdpServer, et les objets cabhCdpLanTrans.

Le serveur CDS DOIT accepter les options DHCP indiquées comme obligatoires dans la colonne Soutien du protocole CDS du Tableau 18.

Tableau 18/J.191 – CDS DHCP Options

Numéro d'option	Fonction de l'option	Soutien du protocole CDS (O)bligatoire (F)acultatif	Soutien de la gestion CDS (O)bligatoire (F)acultatif	CDS aux valeurs d'usine	Maintien par le serveur CDS en cas de coupure de câble (O)bligatoire	Persiste au serveur CDS en cas de coupure de courant (O)bligatoire	Nom d'objet MIB
0	Bourrage	O	–	N/A	N/A	N/A	N/A
255	Fin	O	O	N/A	N/A	N/A	N/A
1	Gabarit sous-réseau	O	O	255.255.255.0	O	O	cabhCdpServer SubnetMask
2	Décalage de temps	O	F	F	N/A	N/A	cabhCdpServer TimeOffset
3	Option de routeur	O	O	192.168.0.1	O	O	cabhCdpServer Router
6	Serveur de nom de domaine	O	O	192.168.0.1	O	O	cabhCdpServer DnsAddress
7	Serveur d'enregistre-ment	O	O	0.0.0.0	O	O	cabhCdpServer SyslogAddress
12	Nom d'hôte	O	F	N/A	N/A	N/A	N/A
15	Nom de Domaine	O	O	Chaîne nulle	O	O	cabhCdpServer DomainName

Tableau 18/J.191 – CDS DHCP Options

Numéro d'option	Fonction de l'option	Soutien du protocole CDS (O)bligatoire (F)acultatif	Soutien de la gestion CDS (O)bligatoire (F)acultatif	CDS aux valeurs d'usine	Maintien par le serveur CDS en cas de coupure de câble (O)bligatoire	Persiste au serveur CDS en cas de coupure de courant (O)bligatoire	Nom d'objet MIB
23	Temps d'arrêt par défaut	O	O	255	O	O	cabhCdpServer TTL
26	MTU d'interface	O	O	1520	O	O	cabhCdpServer InterfaceMTU
43	Informations spécifiques fabricant	O	O	Choisi par le fabricant	O	O	cabhCdpServer VendorSpecific
50	Adresse IP demandée	O	N/A	N/A	N/A	N/A	N/A
51	Temps de location d'adresse IP	O	O	60	O	O	cabhCdpServer LeaseTime
54	Identifiant de serveur	O	O	192.168.0.1	O	O	cabhCdpServer DhcpAddress
55	Liste de demande de paramètres	O	N/A	N/A	N/A	N/A	N/A
60	Identifiant de classe de fabricant	O	N/A	N/A	N/A	N/A	N/A
61	identifiant de client	O	N/A	N/A	N/A	N/A	N/A

Le serveur CDS DOIT accepter l'approvisionnement par le système NMS des options indiquées comme obligatoires dans la colonne Soutien de la gestion CDS du Tableau 18.

Les options DHCP du serveur CDS indiquées comme obligatoires dans la colonne Maintien par le serveur CDS en cas de coupure de câble du Tableau 18 DOIVENT être conservées pendant une coupure du service câble.

Les options DHCP du serveur CDS indiquées comme obligatoires dans la colonne Persiste au serveur CDS en cas de coupure de courant du Tableau 18 DOIVENT persister après une coupure de courant au portail CDP.

Le serveur CDS DOIT accepter d'offrir les valeurs par défaut indiquées dans la colonne CDS aux valeurs d'usine du Tableau 18, si l'option DHCP n'a pas été approvisionnée.

Si le mode de traitement de paquet primaire du service portail (cabhCapPrimaryMode) a été mis à traverse, le serveur CDS DOIT alors être désactivé.

Pour traiter l'allocation automatique d'adresse, le serveur CDS DOIT être capable de créer, modifier et supprimer les entrées du tableau de portail CDP pour les appareils alloués à une adresse LAN-Trans.

Le serveur CDS DOIT assurer la maintenance du paramètre compte d'adresse (cabhCdpLanTransCurCount) indiquant le nombre d'adresses LAN-Trans allouées aux appareils IP de LAN.

Le compte d'adresse DOIT s'accroître chaque fois qu'une location d'adresse LAN-Trans est accordée à un appareil IP de LAN et DOIT être diminué chaque fois qu'une adresse LAN-Trans est libérée ou qu'une location d'adresse LAN-Trans arrive à expiration.

Le serveur CDS DOIT comparer le paramètre compte d'adresse (cabhCdpLanTransCurCount) au paramètre seuil d'adresse (cabhCdpLanTransThreshold) après avoir alloué une adresse LAN-Trans. Si le paramètre compte d'adresse (cabhCdpLanTransCurCount) excède le paramètre seuil d'adresse (cabhCdpLanTransThreshold), une notification DOIT être générée en accord avec le mécanisme de rapport d'événement défini au § 6.5. Lorsque le paramètre compte d'adresse (cabhCdpLanTransCurCount) excède le paramètre seuil d'adresse (cabhCdpLanTransThreshold), le serveur CDS DOIT être capable d'effectuer les actions de seuil dépassé suivantes lors du DHCP DISCOVER suivant issu du LAN: allouer une adresse LAN-Trans comme en temps normal ou ne pas allouer d'adresse.

L'action spécifique prise par le serveur CDS DOIT être celle indiquée par le paramètre fourni d'action de seuil dépassé (cabhCdpLanTransAction).

7.2.3.3 Exigences pour le client CDC

Le comportement du client CDC DOIT être conforme aux exigences du client de la norme [RFC 2131].

L'élément de service portail DOIT avoir une adresse de matériel d'interface WAN distincte de celle du câblo-modem.

Si le client CDC reçoit, dans la réponse DHCP [RFC 2131] issue du serveur DHCP dans le réseau câblé, une adresse IP valide dans le champ 'siaddr' ET un nom de fichier valide dans le champ 'fichier' ET ne reçoit pas l'option DHCP 177 sous-option 51, le service portail DOIT mettre cabhPsDevProvMode à '1' (Mode DHCP).

Si le client CDC reçoit, du serveur DHCP dans le réseau câblé, une adresse IP valide pour l'option DHCP 177 sous-option 51 ET ne reçoit pas une adresse IP valide dans le champ 'siaddr' ET ne reçoit pas un nom de fichier valide dans le champ 'fichier', le service portail DOIT mettre cabhPsDevProvMode à '2' (Mode SNMP).

Si le client CDC reçoit, dans le message DHCP [RFC 2131] de la part du serveur DHCP dans le réseau câblé, l'option DHCP 177 sous-option 51 ET une adresse IP valide dans le champ 'siaddr', OU si le client CDC reçoit l'option DHCP 177 sous-option 51 ET un nom de fichier valide dans le champ 'fichier', le service portail DOIT enregistrer une erreur dans l'enregistreur local et rediffuser un message DHCP DISCOVER (c'est-à-dire, redémarrer la séquence d'approvisionnement dans le cas de cette condition d'invalidité).

Si le client CDC ne reçoit pas l'option DHCP 177 sous-option 51 ET ne reçoit pas une adresse IP valide dans le champ 'siaddr' ET ne reçoit pas un nom de fichier valide dans le champ 'fichier', le service portail DOIT enregistrer une erreur dans l'enregistreur local et rediffuser un message DHCP DISCOVER (c'est-à-dire, redémarrer la séquence d'approvisionnement dans le cas de cette condition d'invalidité).

L'option DHCP 43, sous-option 11 est un paramètre spécifique de l'appareil. Il indique si une adresse est demandée dans la gestion WAN du service portail ou dans le secteur WAN Data du service portail. Le Tableau 19 indique comment les valeurs de l'option DHCP 43, sous-option 11 DOIVENT être réglées pour ces interfaces.

Tableau 19/J.191 – Valeurs de l'option DHCP 43, sous-option 11

Identifiant d'élément	Description et commentaires
PS WAN-Man = 0x01	Identifie la demande d'adresse de secteur WAN-Man
PS WAN-Data = 0x02	Identifie la demande d'adresse de secteur WAN-Data

Le client CDC DOIT implémenter l'option identifiant de classe de fabricant (option DHCP 60) comme spécifié au Tableau 20.

Le câblo-modem et l'élément de service portail envoient chacun des demandes DHCP séparées. Le Tableau 20 décrit comment le client CDC DOIT régler le contenu des options 60 et 43 pour le service portail lorsque des adresses séparées de gestion WAN de PS et de données WAN de PS sont demandées.

Tableau 20/J.191 – Options DHCP pour Demandes d'adresse incorporées WAN-Man et WAN-Data

Options de demande DHCP	Valeur	Description
Demande DHCP du PS pour une adresse WAN-Man		
CPE option 60	"PS"	
CPE option 43 sous-option 1	Demande un vecteur sous-option	Liste des sous-options (dans l'option 43) à retourner par le serveur. Aucune n'est définie.
CPE option 43 sous-option 2	"EPS"	PS incorporé
CPE option 43 sous-option 3	"ECM:EPS"	Liste des appareils incorporés (CM incorporés et PS incorporés)
CPE option 43 sous-option 4	Par exemple, "123456"	Numéro de série d'appareil
CPE option 43 sous-option 11	PS WAN-Man (0x01)	Définit qu'une adresse est demandée dans le secteur WAN-Man du PS
Demande DHCP du PS pour une adresse WAN-Data		
CPE option 60	"PS"	
CPE option 43 sous-option 1	Demande un vecteur sous-option	Liste des sous-options (dans l'option 43) à retourner par le serveur. Aucune n'est définie.
CPE option 43 sous-option 2	"EPS"	PS incorporé
CPE option 43 sous-option 3	"ECM:EPS"	Liste des appareils incorporés (CM incorporés et PS incorporés)
CPE option 43 sous-option 4	Par exemple, "123456"	Numéro de série d'appareil
CPE option 43 sous-option 11	PS WAN-Data (0x02)	Définit qu'une adresse est demandée dans le secteur WAN-Data du PS

Le client CDC DOIT accepter les options DHCP indiquées comme obligatoires dans la colonne Soutien du protocole CDC dans le Tableau 21.

Tableau 21/J.191 – Options DHCP du client CDC

Numéro d'option	Fonction de l'option	Soutien du protocole CDC (O)bligatoire
0	Bourrage	O
255	Fin	O
1	Gabarit de sous-réseau	O
2	Option de décalage horaire	O
3	Option de routeur	O
4	Option de serveur horaire	O
6	Serveur de nom de domaine	O
7	Serveur d'enregistrement (syslog)	O
12	Nom d'hôte	O
15	Nom de domaine	O
23	Temps d'arrêt par défaut	O
26	MTU d'interface	O
43	Informations spécifiques du fabricant	O
50	Adresse IP demandées	O
51	Heure de location d'adresse IP	O
54	Identifiant de serveur	O
55	Liste de demande de paramètre	O
60	Identifiant de classe de fabricant	O
61	Identifiant de client	O
177	Sous-option 3 – Adresse d'entité SNMP du fournisseur de service	O
177	Sous-option 51 – Adresse IP de serveur Kerberos	O

Le Tableau 21 représente les options DHCP qu'il est obligatoire ou facultative que le client CDC accepte. Les options DHCP marquées obligatoires dans le Tableau 21 DOIVENT être incluses dans les messages DHCP DISCOVER et DHCP REQUEST envoyés par le client CDC au serveur DHCP du réseau câblé.

Le service portail DOIT accepter une adresse d'entité SNMP de fournisseur de service (option DHCP 177 sous-option 3) configurée comme une adresse IPv4.

Chaque fois que la première interface WAN-Data du service portail n'a pas une location DHCP en cours, cette première interface WAN-Data PS DOIT avoir par défaut les paramètres IP suivants:

(cette adresse IP est utilisée pour le mappage WAN pour le tuple dynamique NAPT. Cette adresse ne peut pas être utilisée pour le mappage NAT parce que le côté WAN du mappage NAT est persistante. Elle ne peut non plus être utilisée pour les adresses de traverse, qui sont allouées à partir du groupe d'adresses IP du fournisseur de service.)

Adresse IP de gestion: 192.168.100.5

Netmask: 255.255.255.0

Passerelle par défaut: 192.168.100.1

Même en utilisant l'adresse IP WAN-Data par défaut 192.168.100.5, le client CDC DOIT continuer à émettre un message DHCP DISCOVER toutes les 10 secondes jusqu'à ce qu'une location DHCP valide soit accordée à cette interface WAN-Data de service portail (ou à l'interface WAN-Man, si le WAN-Man et le WAN-data partagent une seule adresse IP).

Lorsqu'un service portail acquiert une adresse IP de gestion WAN pour son interface WAN-Man, le client CDC DOIT toujours insérer son adresse de matériel WAN dans le champ d'identifiant de client (option DHCP 61) dans le message DHCP Discover.

Lorsqu'un service portail fonctionnant en mode adresse WAN 2 (comme décrit au § 7.2.2.2) acquiert une adresse IP WAN-Data pour une interface WAN-Data qui va utiliser une adresse IP distincte de celle de l'interface WAN-Man, le client CDC DOIT inclure l'option Identifiant client (cabhCdpWanDataAddrClientId) dans le message DHCP Discover. Pour activer ces identifiants client Wan-Data uniques, le client CDC DOIT permettre au système NMS de créer des entrées cabhCdpWanDataAddrClientId dans le tableau cabhCdpWanDataAddrTable.

Si un service portail fonctionne en mode adresse WAN 2 (comme décrit au § 7.2.2.2) le client CDC DOIT essayer d'obtenir une adresse IP, via DHCP, pour chaque identifiant client unique (cabhCdpWanDataAddrClientId) dans le tableau cabhCdpWanDataAddrTable.

Le client CDC DOIT continuer à diffuser son message DHCP DISCOVER (conformément à la norme [RFC 2131]) jusqu'à ce qu'il reçoive une adresse et un accusé de réception DHCP. La temporisation spécifique pour l'accès au serveur DHCP dépend de l'implémentation. Cependant, le client CDC NE DOIT PAS diffuser le message DHCP DISCOVER plus de trois fois dans une période de 30 secondes quelconque. Au minimum, le client CDC DOIT diffuser le message DHCP DISCOVER au moins une fois par intervalle de 30 secondes, jusqu'à ce qu'il réussisse à acquérir une adresse.

Si le client CDC ne reçoit pas un message DHCP OFFER après cinq tentatives de diffusion d'un message DHCP DISCOVER, le service portail DOIT initialiser le fonctionnement du serveur CDS, de telle sorte que les appareils IP de LAN dans le secteur LAN-Trans puissent être servis en adresses IP.

7.3 Architecture de configuration globale de service portail

7.3.1 Lignes directrices pour la conception de système de configuration PS globale

Les lignes directrices de conception de système suivantes dans le Tableau 22 retracent les fonctionnalités définies pour l'outil de configuration globale de service portail:

Tableau 22/J.191 – Lignes directrices pour la conception de système PS globale

Numéro	Lignes directrices pour la conception de système de configuration PS globale (BPSC)
BPSC 1	Il est nécessaire de fournir un mécanisme permettant au PS de télécharger et traiter les fichiers de configuration.

7.3.2 Description du système de configuration globale de service portail

La configuration globale de service portail est typiquement effectuée pendant l'approvisionnement de l'élément de service portail, via le traitement des réglages de configuration contenus au sein d'un fichier de configuration. Cependant, ce processus peut être initialisé à tout moment. L'outil de configuration globale de service portail comporte les composants suivants:

Format du fichier de configuration:

1) modes de déclenchement du processus de téléchargement;
2) moyens d'authentification du fichier;

3) moyens de faire rapport sur l'état du téléchargement du fichier de configuration du service portail et sur d'autres considérations.

La configuration globale de service portail (BPSC, *bulk PS configuration*) est un outil que les opérateurs peuvent utiliser pour changer en bloc les réglages de configuration du service portail, via un fichier de configuration. En principe, le fichier de configuration va contenir de nombreux réglages, dans la mesure où la principale utilité des fichiers de configuration est leur capacité à changer un certain nombre de réglages de configuration avec le minimum d'intervention de la part du câblo-opérateur.

Le processus de configuration globale de service portail peut se comporter de la même façon que des réglages SNMP successifs exécutés manuellement par un opérateur. Le fichier de configuration est un outil destiné à rendre les opérateurs plus productifs et à faire moins d'erreurs dans les grands changements de configuration.

Il est significatif de noter qu'un service portail n'a pas besoin d'avoir un fichier de configuration chargé avant de commencer à fonctionner. On suppose qu'un service portail va s'initialiser lui-même dans un état connu et un service portail pourrait toujours fonctionner sans charger de fichier de configuration. Cependant, un service portail acceptera et traitera un fichier de configuration PS lorsqu'on lui en fournira un.

Le téléchargement du fichier de configuration du pare-feu utilise une procédure analogue à celle du téléchargement de paramètres de configuration globale de service portail. Se reporter au § 11.3.5.2 pour une description de la procédure de téléchargement du fichier de configuration du pare-feu.

7.3.3 Exigences de la configuration globale PS

7.3.3.1 Exigences de format du fichier de configuration

Les données de configuration du service portail DOIVENT être contenues dans un fichier, qui est téléchargé via TFTP. Le fichier de configuration PS DOIT consister en un certain nombre de réglages de configuration (1 par paramètre), chacun étant de la forme "Type Longueur Valeur (TLV)". Les définitions de ces termes sont fournies au Tableau 23.

Tableau 23/J.191 – Définitions des TLV

Type	Identifiant d'un seul octet qui définit le paramètre
Longueur	Un ou plusieurs octets spécifiant la longueur du champ Valeur (non inclus les champs Type et Longueur)
Valeur	Ensemble d'octets de la longueur définie par Longueur, contenant la valeur spécifique pour le paramètre

Les réglages de configuration DOIVENT se suivre l'un l'autre directement dans le fichier, qui est un flux d'octets (pas de marqueurs d'enregistrement). La longueur du fichier DOIT être complétée à un nombre entier de mots de 32 bits. Voir le § 7.3.3.1.1 pour la définition du bourrage. Les réglages de configuration se divisent en trois types:

- réglages de configuration standard qui doivent obligatoirement être présents;
- réglages supplémentaires ou facultatifs de configuration qui PEUVENT être présents;
- réglages de configuration spécifiques du fabricant.

Le fichier de configuration du service portail PEUT contenir de nombreux paramètres différents, mais le seul paramètre qui DOIT être inclus dans tout fichier de configuration PS est le marqueur de fin de données (Type 255).

Pour permettre une gestion uniforme des câblo-modems améliorés IP se conformant à la présente Recommandation, les appareils conformes DOIVENT accepter un fichier de configuration allant jusqu'à 64k octets de long.

Chaque élément de service portail DOIT accepter les types de paramètres de configuration 0, 4, 9, 17, 21, 28, 32, 33, et 255, qui sont décrits dans le présent paragraphe, et un fichier de configuration PEUT les inclure.

La taille de la valeur dans le champ Longueur pour tout paramètre de configuration inclus dans un fichier de configuration de service portail DOIT être 2 octets.

La valeur de Longueur pour chaque type décrit aux § 7.3.3.1.1 à 7.3.3.1.10 est la longueur réelle en octets du champ Valeur.

7.3.3.1.1 Réglage de configuration du bourrage

Il n'a pas de champs Longueur ou Valeur et n'est utilisé qu'à la fin du marqueur de données pour compléter le fichier à un nombre entier de mots de 32 bits.

Type	Longueur	Valeur
0	–	–

7.3.3.1.2 Clé publique RSA

Cet attribut est un attribut chaîné contenant un RSAPublicKey de type ASN.1 codé en DER, comme défini dans la norme de chiffrement RSA PKCS #1 v2.0 [RSA1].

PKCS #1 v2.0 spécifie qu'une clé publique RSA consiste à la fois en un module public RSA et un exposant public RSA; le type RSAPublicKey les inclut tous les deux comme types d'ENTIER codés en DER.

PKCS #1 v2.0 déclare que l'exposant public RSA peut être normalisé dans des applications spécifiques, et le document suggère des valeurs de 3 à 65 537 (F4). La présente Recommandation exige F4 comme exposant public et emploie un module de 2048 bits.

Type	Longueur	Valeur
4	106, 140, ou 270[a)]	RSAPublicKey de type ASN.1 codé en DER
[a)] Longueur du codage DER, utilisant F4 comme exposant public, et un module public de 2048 bits, respectivement.		

7.3.3.1.3 Nom de fichier d'amélioration de logiciel

Le nom de fichier du fichier d'amélioration du logiciel pour le service portail. Le nom de fichier est un nom pleinement qualifié du chemin directeur. Le fichier est supposé résider dans un serveur TFTP identifié dans une option de réglage de configuration.

Type	Longueur	Valeur
9	Variable[a)]	Nom de fichier
[a)] Longueur NE DOIT PAS causer le dépassement de la taille maximale autorisée par le message de gestion MAC résultant.		

7.3.3.1.4 Commande SNMP d'accès en écriture

Cet objet rend possible de désactiver l'accès SNMP "établi" à des objets de base MIB individuels. Chaque instance de cet objet commande l'accès à tous les objets de base MIB inscriptibles dont les préfixes d'identificateur d'objet (OID, *object identifier*) correspondent. Cet objet peut être répété pour désactiver l'accès à un nombre quelconque d'objets MIB.

Type	Longueur	Valeur
10	n	Préfixe d'OID plus fanion de commande

Où n est la taille du codage ASN.1 des règles de base du codage [UIT-T X.690] du préfixe de l'identificateur d'objet plus un octet pour le fanion de commande.

Le fanion de commande peut prendre les valeurs suivantes:

– 0 permet le droit d'accès;

– 1 interdit le droit d'accès.

Tout préfixe d'OID peut être utilisé. L'OID nul 0.0 peut être utilisé pour commander l'accès à tous les objets MIB. (L'OID 1.3.6.1 aura le même effet.)

Lorsque des instances multiples de cet objet sont présentes et se recouvrent, le plus long préfixe (le plus spécifique) l'emporte.

Et donc on peut avoir par exemple:

– someTable interdit l'accès en écriture;

– someTable.1.3 permet l'accès en écriture.

Cet exemple interdit l'accès à tous les objets dans someTable sauf ceux de someTable.1.3.

7.3.3.1.5 Certificat de CA

Cet attribut est un attribut chaîné contenant un certificat de CA X.509, comme défini dans la Rec. UIT-T X.509.

Type	Longueur	Valeur
17	Variable[a)]	Certificat de CA X.509 (ASN.1 codé en DER)
[a)] Longueur NE DOIT PAS causer le dépassement de la taille maximale autorisée par le message de gestion MAC résultant.		

7.3.3.1.6 Serveur TFTP d'amélioration de logiciel

L'adresse IP du serveur TFTP, sur laquelle réside le fichier d'amélioration de logiciel pour le service portail

Type	Longueur	Valeur
21	4	ip1, ip2, ip3, ip4

7.3.3.1.7 Objet de base MIB SNMP avec extension de Longueur

Cet objet permet d'établir des objets de base MIB SNMP arbitraires via le processus TFTP d'enregistrement, lorsque la valeur est une liaison variable (VarBind) du protocole SNMP, comme défini dans la norme [RFC 1157]. Le VarBind est codé en ASN.1 Règles de codage de base, exactement comme s'il faisait partie d'une demande Réglage SNMP.

Type	Longueur	Valeur
28	Variable[a)]	Liaison variable
[a)] Longueur NE DOIT PAS causer le dépassement de la taille maximale autorisée par le message de gestion MAC résultant.		

Le service portail DOIT traiter la liaison variable, dans un TLV de type 28, comme si elle faisait partie d'une demande Réglage SNMP avec les avertissements suivants:

- il DOIT traiter la demande comme étant pleinement autorisée (il ne peut pas refuser la demande pour absence de privilège);
- les dispositions de commande d'écriture SNMP (voir le paragraphe précédent) ne s'appliquent pas;
- une réponse non SNMP est générée par le service portail;
- cet objet PEUT être répété avec différents VarBind pour "Etablir (*Set*)" un certain nombre d'objets de base MIB. Tous les SNMP Set d'un fichier de configuration DOIVENT être traités comme s'ils étaient simultanés. Chaque VarBind DOIT être limité à 65 535 octets.

7.3.3.1.8 Certificat de vérification de code de fabricant

Le certificat de vérification de code de fabricant (M-CVC, *manufacturer's code verification certificate*) sert pour la sécurisation du téléchargement du logiciel. Le fichier de configuration du service portail DOIT contenir un certificat M-CVC et/ou C-CVC afin de permettre à l'appareil de télécharger le fichier de code à partir du serveur TFTP.

Type	Longueur	Valeur
32	Variable	CVC du fabricant (ASN.1 codé en DER)

Si la longueur du M-CVC dépasse 65 535 octets, le M-CVC DOIT être fragmenté en deux ou plus éléments de type 32 successifs. Chaque fragment, sauf le dernier, DOIVENT avoir une longueur de 65 535 octets. Le service portail reconstruit le M-CVC en enchaînant le contenu (valeur du TLV) des éléments de type 32 successifs dans l'ordre dans lequel ils apparaissent dans le fichier de configuration. Par exemple, le premier octet suivant le champ Longueur du second élément de type 32 est traité comme s'il suivait immédiatement le dernier octet du premier élément de type 32.

7.3.3.1.9 Certificat de vérification de code de cosignataire

Le certificat de vérification de code de cosignataire (C-CVC, *co-signer's code verification certificate*) sert pour la sécurisation du téléchargement du logiciel. Le fichier de configuration du service portail DOIT contenir un C-CVC et/ou un M-CVC afin de permettre à l'appareil de télécharger le fichier de code à partir du serveur TFTP.

Type	Longueur	Valeur
33	Variable	CVC de cosignataire (ASN.1 codé en DER)

Si la longueur du C-CVC dépasse 65 535 octets, le C-CVC DOIT être fragmenté en deux ou plus éléments de type 33 successifs. Chaque fragment, sauf le dernier, DOIVENT avoir une longueur de 65 535 octets. Le service portail reconstruit le C-CVC en enchaînant le contenu (valeur du TLV) des éléments de type 33 successifs dans l'ordre dans lequel ils apparaissent dans le fichier de configuration. Par exemple, le premier octet suivant le champ Longueur du second élément de type 33 est traité comme s'il suivait immédiatement le dernier octet du premier élément de type 33.

7.3.3.1.10 Valeur de démarrage SNMPv3

Les éléments de service portail conformes DOIVENT comprendre le TLV suivant et ses sous-éléments et être capable de démarrer l'accès SNMPv3 au service portail sans considération de savoir si le service portail fonctionne en mode NmAccess ou en mode coexistence (voir les § 6.3.3 et 6.3.6).

Type	Longueur	Valeur
34	n	Composite

Jusqu'à 5 de ces objets peuvent être inclus dans le fichier de configuration. Chaque résultat dans une rangée additionnelle étant ajouté aux tableaux usmDHKickstartTable et usmUserTable et résultant en un numéro public d'agent qui est généré pour ces rangées.

7.3.3.1.10.1 Nom de sécurité de démarrage SNMPv3

Type	Longueur	Valeur
34.1	2-16	Nom de sécurité codé en UTF8

Pour le jeu de caractères ASCII, les codages UTF8 et ASCII sont identiques. Normalement, ceci est spécifié comme étant incorporé dans un manuel d'utilisateur DOCSIS, par exemple, "docsisManager," "docsisOperator," "docsisMonitor," "docsisUser."

Le nom de sécurité N'EST PAS terminé par zéro. Ceci est rapporté dans le tableau usmDHKickStartTable comme nom usmDHKickStartSecurityName et dans le tableau usmUserTable comme noms usmUserName et usmUserSecurityName.

7.3.3.1.10.2 Numéro public de gestionnaire de démarrage SNMPv3

Type	Longueur	Valeur
34.2	n	Numéro public Diffie-Hellman du gestionnaire exprimé comme une chaîne d'octets

Ce numéro est le numéro public Diffie-Hellman déduit d'un nombre aléatoire généré de façon privée (par le gestionnaire ou par l'opérateur) et transformé conformément à la norme [RFC 2786]. Ceci est rapporté dans le tableau usmDHKickStartTable comme usmKickstartMgrPublic. Lorsqu'il est combiné avec l'objet rapporté dans la même rangée comme usmKickstartMyPublic, il peut être utilisé pour déduire les clés dans la rangée correspondante du tableau usmUserTable.

7.3.3.1.11 Elément de fichier de configuration – Récepteur de notification docsisV3

Type	Longueur	Valeur
38	Variable	(Voir ci-dessous.)

Cet élément de fichier de configuration spécifie une station de gestion de réseau qui va recevoir des notifications de la part du service portail lorsqu'il est en mode de gestion de réseau coexistence. Jusqu'à 10 de ces éléments peuvent être inclus dans le fichier de configuration du service portail.

Format de cet élément:

définition des champs de l'élément docsisV3NotificationReceiver;

Tous les champs multi-octet ont les octets de plus fort poids en premier dans le champ.

Ce TLV (38) consiste en plusieurs sous-TLV à l'intérieur du TLV élément de fichier de configuration:

sous-TLV 38.1 – adresse IP du receveur de trap, en binaire

Adresse IP 4 octets Adresse IP du receveur de trap, en binaire;

sous-TLV 38.2 – numéro de port UDP du receveur de trap, en binaire

Port UDP 2 octets Numéro de port UDP du receveur de trap, in binaire.

(s'il est absent, on utilise la valeur par défaut 162);

sous-TLV 38.3 – type de trap envoyé par le PS (Note 2)

Type de trap 2 octets

1 = trap SNMP v1 dans un paquet SNMP v1;

2 = trap SNMP v2c dans un paquet SNMP v2c;

3 = inform SNMP dans un paquet SNMP v2c;

4 = trap SNMP v2c dans un paquet SNMP v3;

5 = inform SNMP dans un paquet SNMP v3;

sous-TLV 38.4 – temporisation, en millisecondes, utilisée pour envoyer inform

temporisation 2 octets 0-65 535;

sous-TLV 38.5 – nombre d'essais lors de l'envoi d'un inform, après avoir envoyé le inform la première fois;

essais 2 octets 0-65 535;

sous-TLV 38.6 – paramètres de filtrage de notification

si ce sous-TLV est absent, le receveur de notification recevra toutes les notifications générées par l'agent SNMP.

Identificateur d'objet formaté en ASN.1 pour OID de filtre de la valeur snmpTrapOID qui identifie les notifications à envoyer au receveur de notification. Cette notification et tout ce qu'elle recouvre sera envoyé. <z> est la longueur, en octet du codage ASN.1. Ce champ commence avec l'octet de type 6 (Identificateur d'objet) Universl ASN.1, puis le champ longueur ASN.1, puis les composants d'identificateur d'objet codé en ASN.1;

sous-TLV 38.7 – nom de sécurité à utiliser lors de l'envoi d'une notification SNMP V3

ce sous-TLV n'est pas exigé pour le type Trap = 1, 2, ou 3 ci-dessus. S'il n'est pas approvisionné avec un type 4 ou 5 de Trap, la notification V3 sera alors envoyée avec le niveau de sécurité noAuthNoPriv en utilisant le nom de sécurité "@config" (Note 2).

Nom de sécurité

le nom V3 de sécurité à utiliser lors de l'envoi d'une notification V3. Il n'est utilisé que si le type de Trap est réglé à 4 ou 5. Le nom doit être un nom spécifié dans un TLV de type 34 de fichier de configuration en tant que partie de la procédure de démarrage DH. Les notifications seront envoyées en utilisant les clés d'authentification et de confidentialité calculées par le service portail pendant la procédure de démarrage Diffie-Hellman.

NOTE 1 – A réception de l'un de ces éléments de TLV, le service portail DOIT faire des entrées dans les tableaux suivants afin de provoquer la transmission de trap désirée: snmpNotifyTable, snmpTargetAddrTable, snmpTargetParamsTable, snmpNotifyFilterProfileTable, snmpNotifyFilterTable, snmpCommunityTable, usmUserTable, vacmSecurityToGroupTable, vacmAccessTable, et vacmViewTreeFamilyTable.

NOTE 2 – Type de trap: la chaîne communautaire pour les trap dans les paquets SNMP V1 et V2 DOIT être "public". Le nom de sécurité dans les trap et inform dans les paquets SNMP V3 où il n'a pas été spécifié de nom de sécurité DOIT être "@config et dans ce cas, le niveau de sécurité DOIT être noAuthNoPriv.

NOTE 3 – OID filtre: SNMP V3 permet la spécification des OID de Trap qui sont à envoyer à un receveur de trap. L'OID filtre dans l'élément de fichier de configuration spécifie l'OID de la racine d'un sous-arbre de filtre de trap. Tous les Trap avec un OID de Trap contenu dans ce sous-arbre de filtre de trap DOIVENT être envoyés au receveur de trap.

NOTE 4 – Numéro de TLV de fichier de configuration: le champ Type de ce TLV DOIT être (38).

NOTE 5 – Le fichier de configuration du service portail PEUT aussi contenir des éléments MIB de TLV qui font des entrées dans n'importe lequel des 10 tableaux dont la liste figure dans la Note 1. Ces éléments MIB de TLV NE DOIVENT PAS utiliser les colonnes d'index qui commencent par les caractères "@config".

NOTE 6 – Cet élément de TLV NE DOIT être traité que si le service portail est passé en mode coexistence SNMP V3 pendant le traitement du fichier de configuration du service portail.

7.3.3.1.12 Marqueur de fin de données

C'est un marqueur spécial pour la fin des données. Il ne comporte pas de champs Longueur ou Valeur.

Type	Longueur	Valeur
255	–	–

7.3.3.2 Mode de déclenchement

Le transfert du fichier de configuration, du serveur TFTP dans le système de tête de réseau à l'élément de service portail, est initialisé par un événement qu'on désigne par le terme de déclencheur. Les exigences pour le déclenchement du transfert d'un fichier de configuration PS du serveur TFTP au service portail sont données ci-après.

Le mode de déclenchement du téléchargement du fichier de configuration PS dépend du mode d'approvisionnement dans lequel fonctionne le service portail. Le portail CMP DOIT lire la valeur du mode cabhPsDevProvMode (voir § 7.2.3.3) avant d'initialiser un téléchargement de fichier de configuration PS.

Déclenchement du téléchargement de fichier de configuration PS pour le mode d'approvisionnement DHCP:

si le service portail reçoit l'adresse du serveur TFTP dans le champ "siaddr" et le nom de fichier de configuration PS dans le champ "fichier" du message DHCP OFFER, le service portail DOIT combiner l'adresse du serveur TFTP et le nom de fichier de configuration PS pour former une valeur codée en URL et écrire cette valeur dans cabhPsDevProvConfigFile. Le hachage de configuration PS accolé au nom de fichier de configuration PS NE DOIT PAS être inclus dans la valeur codée en URL.

Le téléchargement du fichier de configuration du service portail, par un service portail fonctionnant en mode d'approvisionnement DHCP, est déclenché par la présence de la localisation du fichier de configuration PS (adresse IP de serveur TFTP) et de son nom dans le message DHCP présenté au service portail (CDC) par le serveur DHCP dans le réseau câblé. Se reporter au § 7.2.3.3.

Si le service portail fonctionne en mode d'approvisionnement DHCP (comme indiqué par la valeur de cabhPsDevProvMode), après réception par le service portail (CDC) d'un message DHCPACK (*accusé de réception DHCP*) du serveur DHCP dans le réseau câblé, le service portail DOIT envoyer une demande TFTP Get (*Obtenu*) au serveur identifié dans le champ "siaddr" du message DHCP pour télécharger le fichier identifié dans le champ "fichier" du message DHCP.

Déclenchement du téléchargement de fichier de configuration PS pour le mode d'approvisionnement SNMP:

si le service portail fonctionne en mode d'approvisionnement SNMP (comme indiqué par la valeur de cabhPsDevProvMode), le téléchargement du fichier de configuration NE DOIT PAS survenir avant l'achèvement du processus d'authentification SNMP v3 (se reporter au paragraphe 11 Sécurité pour des précisions sur le processus d'authentification SNMP).

Si le service portail fonctionne en mode d'approvisionnement SNMP (comme indiqué par la valeur de cabhPsDevProvMode), l'élément de service portail NE DOIT PAS initialiser un téléchargement de fichier de configuration si une valeur valide pour cabhPsDevProvConfigHash (base MIB PSDev) n'a pas été approvisionnée par le système NMS.

Si le service portail fonctionne en mode d'approvisionnement SNMP (comme indiqué par la valeur de cabhPsDevProvMode) ET que l'objet cabhPsDevProvConfigHash issu de la base MIB PSDev a une valeur valide, le téléchargement du fichier de configuration DOIT être déclenché lorsqu'un message de demande SNMP-set (*établi*), adressé à l'interface WAN-Man du service portail, contient une valeur valide pour l'objet de base MIB PSDev cabhPsDevProvConfigFile. Le format de cabhPsDevProvConfigFile DOIT être une adresse IP de serveur TFTP codée en URL et un nom de fichier de configuration.

Fonctionnement après déclenchement:

une fois déclenché, le service portail DOIT utiliser un client TFTP conforme à la norme [RFC 1350] pour télécharger les fichiers de configuration de service portail.

Si le fichier de configuration PS est authentifié correctement, lorsque le téléchargement du fichier de configuration PS est terminé, le service portail DOIT traiter les TLV contenus dans le fichier. Se reporter au § 6.3.9 pour une description de la façon dont le portail CMP traite le fichier de configuration.

7.3.3.3 Moyens d'authentification du fichier de configuration PS

Le présent paragraphe définit la procédure d'authentification du fichier de configuration PS.

On utilise un calcul de hachage pour authentifier le fichier de configuration PS. Le système NMS calcule le hachage du fichier de configuration PS puis envoie la valeur de hachage résultante à l'élément de service portail. L'identité du système NMS qui a généré le fichier de configuration PS est authentifiée en comparant le hachage du fichier de configuration PS qui a été généré par le système NMS et transporté à l'élément de service portail avec le hachage (calculé par le PS) sur le fichier de configuration PS téléchargé depuis le serveur TFTP. L'identité de l'élément de service portail demandant le fichier n'est pas exigée..

L'algorithme de sécurité utilisé pour authentifier le fichier de configuration du service portail dépend du mode d'approvisionnement de l'élément de service portail (voir § 5.7). Il y a deux types de modes d'approvisionnement: le mode d'approvisionnement DHCP et le mode d'approvisionnement SNMP. Les paragraphes suivants décrivent les algorithmes de sécurité et les exigences nécessaires pour authentifier le fichier de configuration PS sur la base du mode d'approvisionnement de l'élément de service portail. L'élément de service portail DOIT accepter les deux algorithmes de sécurité spécifiés aux § 7.3.3.3.1 et 7.3.3.3.2.

7.3.3.3.1 Algorithme d'authentification de fichier de configuration PS pour le mode d'approvisionnement DHCP

Procédure pour l'authentification du fichier de configuration PS par l'élément de service portail en mode d'approvisionnement DHCP:

1) lorsque le système NMS crée un nouveau fichier de configuration PS ou modifie un fichier existant, le système NMS va créer un hachage SHA-1 du contenu complet du fichier de configuration PS, pris comme une chaîne binaire;
2) le système NMS ajoute la valeur du hachage au nom du fichier de configuration PS qui est envoyé à l'élément de service portail dans l'Offre DHCP (voir § 7.2.3.3 et 13.2). Le séparateur utilisé entre le nom du fichier de configuration PS et la valeur de hachage est le caractère "@" (par exemple, "configfile1.txt@23423487987345"). L'élément de service portail met à jour l'objet de base MIB cabhPsDevProvConfigHash avec la valeur du hachage reçu;
3) l'élément de service portail télécharge le fichier nommé à partir du serveur TFTP configuré;
4) l'élément de service portail DOIT calculer un hachage SHA-1 sur le contenu complet du fichier de configuration PS et comparer le hachage calculé avec le hachage dans l'objet de base MIB cabhPsDevProvConfigHash. Si les valeurs des hachages calculées et configurées sont identiques, le fichier de configuration PS est authentifié; autrement, le fichier DOIT être rejeté;
5) lorsque l'authentification est réussie, l'élément de service portail DOIT utiliser le contenu du fichier de configuration PS pour sa configuration.

7.3.3.3.2 Algorithme d'authentification de fichier de configuration PS pour le mode d'approvisionnement SNMP

Procédure pour l'authentification du fichier de configuration PS par l'élément de service portail en mode d'approvisionnement SNMP:

1) lorsque le système NMS crée un nouveau fichier de configuration PS ou modifie un fichier existant, le système NMS va créer un hachage SHA-1 du contenu complet du fichier de configuration PS, pris comme une chaîne binaire;
2) le système NMS envoie la valeur du hachage calculé à l'étape 1 à l'élément de service portail via le message SNMP SET et met à jour l'objet de base MIB cabhPsDevProvConfigHash;
3) le système NMS envoie le nom et la localisation du fichier de configuration PS via le message SNMP SET et met à jour l'objet MIB cabhPsDevProvConfigFile (ceci déclenche le téléchargement TFTP, voir § 7.3.3.2);
4) l'élément de service portail télécharge le fichier nommé à partir du serveur TFTP configuré;
5) l'élément de service portail DOIT calculer un hachage SHA-1 sur le contenu complet du fichier de configuration PS et comparer le hachage calculé au hachage dans l'objet de base MIB cabhPsDevProvConfigHash MIB. Si les valeurs de hachage calculées et configurées sont les mêmes, le fichier de configuration PS est authentifié, autrement, le fichier DOIT être rejeté;
6) lorsque l'authentification est réussie, l'élément de service portail DOIT utiliser le contenu du fichier de configuration PS pour sa configuration.

Le téléchargement réussi du fichier de configuration PS est défini comme la réception complète et correcte par l'élément de service portail du contenu du fichier de configuration PS dans les limites de la période de temporisation TFTP ET le calcul par le service portail des valeurs de hachage pour le fichier de configuration PS sans erreurs résultant du calcul.

7.3.3.4 Etat des moyens de rapport

Le service portail DOIT faire rapport sur l'état et les conditions d'erreur du téléchargement du fichier de configuration en utilisant le processus de rapport d'événement décrit au § 6.5.

Le Tableau 24 identifie les modes de traitement qui DOIVENT être utilisés et l'action qui DOIT être entreprise lorsque ces modes de traitement sont détectés.

Tableau 24/J.191 – Mode de traitement de fichier de configuration PS

Mode d'échec	Action
Le champ Type n'est pas valide	Ne pas tenir compte du TLV en question et rapporter un événement. Continuer de traiter le fichier.
Le fichier échoue à l'essai d'intégrité (l'intégrité de fichier reste encore à définir)	Rapporter un événement. Ne pas essayer de traiter le fichier.
Le fichier est trop gros	Rapporter un événement. Ne pas essayer de traiter le fichier.
On ne trouve pas le fichier de configuration	Rapporter un événement. Ne pas essayer de traiter le fichier.
Le bourrage du fichier n'est pas correct	Rapporter un événement. Ne pas essayer de traiter le fichier.
Pas de marqueur de fin de fichier	Rapporter un événement. Ne pas essayer de traiter le fichier.
Incapable d'établir la valeur	Rapporter un événement, refuser le fichier de configuration et réinitialiser. Rétablir toutes les valeurs (valeurs d'avant l'établissement SNMP) qui étaient sauvegardées dans une mémoire non volatile.
Rencontre une valeur alors que l'OID SNMP n'est pas reconnaissable	Ne pas tenir compte du TLV en question et rapporter un événement. Continuer de traiter le fichier.

Se reporter à l'Annexe B pour une liste des événements y compris ceux qui figurent au Tableau 24, et des informations sur la façon dont les événements sont rapportés.

Si des réglages de configuration sont traités, un événement DOIT être généré lorsque la fin du fichier est détectée, et cet événement DOIT inclure le nombre de TLV traités avec succès et le nombre de TLV passés.

Une fois déclenché le téléchargement d'un fichier de configuration PS, l'élément de service portail DOIT continuer à essayer de télécharger le fichier de configuration PS spécifié de la localisation spécifiée jusqu'à ce que le fichier de configuration PS soit téléchargé avec succès et que le hachage soit bien calculé comme décrit au § 7.3.3.3. La temporisation spécifique pour l'accès du serveur TFTP dépend de l'implémentation. Cependant, le service portail NE DOIT PAS tenter d'accéder au serveur TFTP plus de trois fois dans toute période de cinq minutes. Au minimum, le PS DOIT tenter au moins une fois par intervalle de 5 minutes de télécharger le fichier de configuration PS, jusqu'à ce que le téléchargement du fichier de configuration PS soit réussi.

Le service portail DOIT générer l'événement approprié identifié dans l'Annexe B indiquant l'échec de téléchargement de fichier de configuration PS chaque fois que le service portail ne réussit pas à télécharger le fichier de configuration PS.

Si le service portail réussit à télécharger le fichier de configuration PS, le service portail DOIT remettre le compteur de téléchargement de fichier de configuration PS à zéro et générer l'événement approprié identifié dans l'Annexe B pour indiquer la réussite du téléchargement du fichier de configuration PS.

Si le service portail fonctionne en mode DHCP (comme indiqué par la valeur de cabhPsDevProvMode) ET interrompt le processus de téléchargement du fichier de configuration

PS, le service portail DOIT générer un événement identifié à l'Annexe B pour indiquer l'échec du processus de téléchargement du fichier de configuration PS ET libérer son adresse IP WAN-Man de PS conformément à la norme [RFC 2131] ET produire à nouveau un message DHCP DISCOVER conformément à la norme [RFC 2131], c'est-à-dire que le service portail doit recommencer le processus d'initialisation.

Le service portail DOIT utiliser une temporisation adaptative pour TFTP, fondée sur un dégagement exponentiel binaire comme décrit dans les normes [RFC 1123] et [RFC 2349].

7.4 Architecture de l'heure client

7.4.1 Lignes directrices pour la conception du système d'heure du client

Les lignes directrices de conception de système suivantes dans le Tableau 25 décrivent les fonctionnalités définies pour l'heure client du service portail.

Tableau 25/J.191 – Lignes directrices pour la conception du système d'heure du client

Numéro	Lignes directrices pour la conception du système d'heure du client
TOD 1	Il est nécessaire de fournir un mécanisme permettant au service portail de réaliser la synchronisation horaire avec la tête de système du réseau.

7.4.2 Description du système d'heure du client

L'élément de service portail utilise une heure client compatible avec la norme [RFC 868], afin de réaliser la synchronisation horaire avec un serveur horaire sur la tête de système du réseau. La synchronisation horaire est essentielle pour les fonctions de sécurité du service portail ainsi que pour les messages d'événement.

Lorsque le client DHCP du CDC demande une adresse IP – au serveur DHCP de tête de système – pour l'interface WAN-Man, le client DHCP va recevoir l'adresse IP du serveur horaire de tête de système au sein de l'option 4 DHCP. Le client DHCP recevra aussi le décalage de temps (par rapport à l'UTC), au sein de l'option 2 DHCP.

Un fois que la pile IP de WAN-Man commence à utiliser l'adresse IP qu'elle a reçue du DHCP, elle devrait envoyer une demande d'heure [RFC 868] au serveur horaire. Si le serveur horaire répond avec une réponse valide, le service portail commencera à utiliser cette heure pour les messages d'événement et les fonctions de sécurité.

Exigences pour l'heure client

L'élément de service portail DOIT implémenter l'heure client.

L'heure client du service portail DOIT être conforme au protocole horaire de la norme [RFC 868] et ne doit utiliser que le protocole UDP.

Lors d'un rétablissement, l'élément de service portail DOIT initialiser sa date à 0 (0:0.0 1er janvier 1900) conformément à [RFC 868].

L'élément de service portail DOIT tenter la synchronisation horaire avec le serveur horaire indiqué par l'option 4 de DHCP, qui est reçue dans le message OFFRE DHCP faite à l'interface WAN-Man.

Le service portail DOIT combiner l'heure récupérée auprès du serveur horaire avec le décalage d'heure fourni par l'option 2 de DHCP, pour créer l'heure local actuelle.

L'élément de service portail DOIT utiliser l'heure locale actuelle calculée à partir de l'heure récupérée auprès du serveur horaire et du décalage d'heure reçu de l'option 2 de DHCP pour les messages d'événement et les fonctions de sécurité et doit seulement être exact à la seconde près.

L'élément de service portail DOIT continuer d'essayer de communiquer avec le serveur horaire, jusqu'à établissement de l'heure locale. La temporisation spécifique pour les demandes d'heure dépend de l'implémentation. Cependant, le client d'heure du service portail NE DOIT PAS dépasser trois demandes d'heure dans toute période de cinq minutes. Au minimum, le client d'heure du service portail DOIT produire au moins une demande d'heure par période de cinq minutes, jusqu'à ce que l'heure locale soit établie.

Si le serveur horaire ne répond pas avec une réponse valide, le service portail DOIT faire ce qui suit, pas nécessairement dans cet ordre:

- établir la valeur de cabhPsDevTodSyncStatus à "2" (échec de l'accès à l'heure);
- s'il y a des locations actives dans le secteur LAN-Trans comme indiqué par une valeur différente de zéro pour cabhCdpLanTransCurCount, mettre cabhCdpLanAddrCreateTime à l'heure actuelle et mettre cabhCdpLanAddrExpireTime à la valeur de cabhCdpLanAddrCreateTime plus la valeur de cabhCdpServerLeaseTime pour chaque location active (heure d'expiration = heure de création + temps de location);
- enregistrer l'échec et générer un événement standard défini en Annexe B;
- continuer de réessayer les communications avec le serveur horaire jusqu'à l'établissement de l'heure locale.

Si le service portail réussit à synchroniser son heure de référence avec le serveur horaire dans le réseau câblé, le service portail DOIT mettre la valeur de cabhPsDevTodSyncStatus à "1" (synchronisation horaire réussie).

Si la valeur de cabhPsDevTodSyncStatus est "1", c'est-à-dire, si l'heure locale a déjà été établie, il n'est pas nécessaire que le client de l'heure de produire une demande d'heure.

8 Traitement de paquet et traduction d'adresse

8.1 Introduction/Aperçu général

8.1.1 Objectifs

Les objectifs clés qui conduisent les fonctionnalités de traitement de paquet comportent:

- fournir une fonction de traduction d'adresse facile sur le câble, permettant au câblo-opérateur la visibilité et la facilité de gestion des appareils de l'utilisateur tout en préservant les architectures d'acheminement fondées sur une origine réseau câblé;
- empêcher le trafic non nécessaire sur le réseau câblé et local;
- la conservation des adresses IP acheminables mondialement ainsi que les adresses de gestion privée de réseau câblé;
- faciliter l'acheminement de trafic IP chez l'utilisateur en allouant des adresses réseau aux appareils IP de LAN de telle sorte qu'ils résident sur le même sous-réseau logique.

8.1.2 Hypothèses

- on suppose que lorsque les serveurs d'approvisionnement de câblo-opérateur fournissent des adresses IP multiples acheminables mondialement aux appareils du domicile des utilisateurs, ces adresses ne résideront pas nécessairement sur le même sous-réseau;
- le changement de fournisseurs de service Internet est supposé ne survenir qu'assez rarement, à un rythme similaire à celui du changement de transporteur longue distance par un abonné résidentiel;

- la fonction de traitement de paquet de service portail peut transmettre du trafic de diffusion à toutes les interfaces de LAN et de WAN-Data de façon transparente. Le ralentissement du trafic de diffusion n'est pas exigé. On suppose que le câblo-modem DOCSIS a la capacité de filtrer le trafic IP de diffusion.

8.2 Architecture

Le présent paragraphe décrit les concepts clés de la fonction de traitement de paquet et de traduction d'adresse.

8.2.1 Lignes directrices pour la conception du système

Voir Tableau 26.

Tableau 26/J.191 – Lignes directrices pour la conception du système de traitement de paquet et traduction d'adresse

Numéro	Lignes directrices pour la conception du système
Pckt Handling 1	Les mécanismes d'adressage seront sous le contrôle de l'opérateur et donneront à l'opérateur connaissance et accès au service portail.
Pckt Handling 2	L'adressage ne fera rien qui puisse compromettre les architectures d'acheminement du réseau câblé actuel (par exemple, l'acheminement fondé sur la source, MPLS).
Pckt Handling 3	Les mécanismes de gestion du trafic isoleront le réseau câblé du trafic généré par les communications domestiques d'homologues à homologues, s'il y a lieu.
Pckt Handling 4	Les adresses IP seront conservée lorsque c'est possible (à la fois les adresses acheminables mondialement et les adresses de gestion privée du réseau câblé).

8.2.2 Description du système de traitement de paquet

Le présent paragraphe donne un aperçu général sur les concepts de traitement de paquet et de traduction d'adresse.

8.2.2.1 Aperçu général sur la fonction de traitement de paquet

La fonction de traduction d'adresse et de traitement de paquet est fournie par l'entité fonctionnelle connue sous le nom de portail d'adresse câble (CAP, *cable address portal*). Le CAP englobe les éléments suivants de traduction d'adresse et de transmission de paquet:

- traduction d'adresse câble (CAT, *cable address translation*);
- fonction traverse;
- commutation de transmission sélective de sens montant (USFS, *upstream selective forwarding switch*).

Comme indiqué à la Figure 16, la fonction CAT fournit un mécanisme d'interconnexion des secteurs d'adresse WAN-Data et LAN-Trans (via la traduction d'adresse), tandis que la fonction traverse fournit un mécanisme d'interconnexion des secteurs d'adresse WAN-Data et LAN-Pass (via le pontage). La fonction CAT est conforme à la traduction d'adresse de réseau (NAT, *network address translation*) traditionnelle de la section 2 de la norme [RFC 3022]. Comme avec la traduction NAT traditionnelle, il y a deux variantes de traduction CAT, qu'on appelle acheminement transparent de traduction d'adresse de réseau câblé (C-NAT, *cable network address translation*) et acheminement transparent de traduction d'adresse et de port de réseau câblé (C-NAPT, *cable network address and port translation*). L'acheminement transparent C-NAT est la version compatible câble de la traduction NAT de base de la section 2.1 de la norme [RFC 3022] et

l'acheminement transparent C-NAPT est la version compatible câble de la traduction NAPT de la section 2.2 de la norme [RFC 3022].

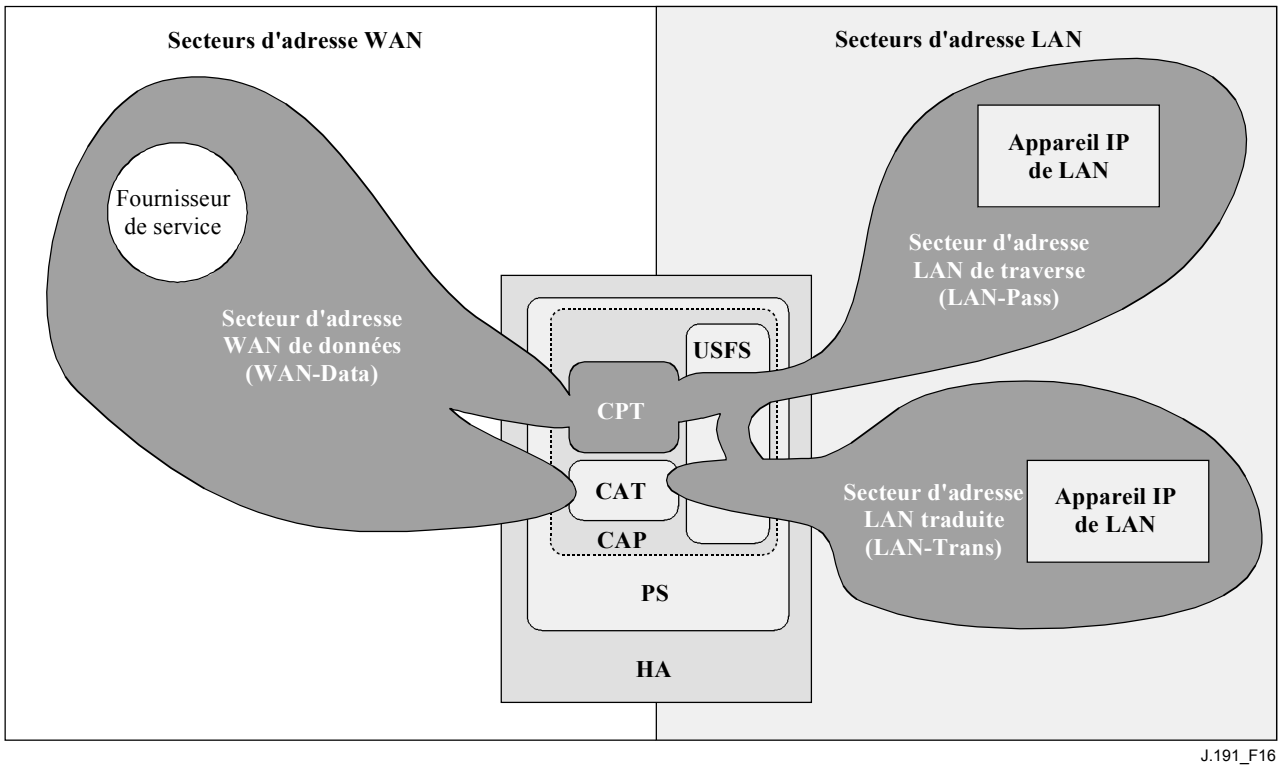

Figure 16/J.191 – Fonctions du portail d'adresse câble (CAP)

Selon la norme [RFC 3022], l'acheminement transparent C-NAT est "une méthode de mappage des adresses IP d'un groupe à un autre, de façon transparente pour les utilisateurs finaux", et l'acheminement transparent C-NAPT est "une méthode par laquelle de nombreuses adresses réseau et leurs ports TCP/UDP (protocole de commande de transmission/protocole datagramme d'utilisateur) sont traduites en une seule adresse réseau et ses ports TCP/UDP." Aussi, selon la norme [RFC 3022], l'objet des fonctions C-NAT et C-NAPT est de "fournir un mécanisme de connexion d'un secteur d'adresses privées à un secteur externe ayant des adresses mondiales enregistrées de façon unique".

La fonction traverse de câble à domicile (CPT, *cableHome pass-through*) est un processus de pontage spécifié qui interconnecte les secteur d'adresse WAN-Data et LAN-Pass sans traduction d'adresse.

La commutation de transmission sélective de sens montant (USFS) définit au sein du portail CAP une fonction qui a la capacité de confiner le trafic du domicile au domicile, même dans lorsque les appareils d'usager qui génèrent de trafic résident sur des sous réseaux logiques IP différents. Spécifiquement, cette fonction transmet du trafic qui trouve la source d'une adresse dans un des secteurs d'adresse du LAN, destiné à des secteurs d'adresse IP de LAN, directement à sa destination. Cette fonction de transmission directe empêche le trafic de traverser le réseau HFC, et interconnecte les secteurs d'adresse LAN-Trans et LAN-Pass.

Tout au long de la présente Recommandation, les termes liaison d'adresse, non-liaison d'adresse, traduction d'adresse et session sont utilisés selon les définitions de la norme [RFC 2663]. De plus, le terme "mappage"est défini comme étant l'information nécessaire pour effectuer l'acheminement transparent C-NAT et l'acheminement transparent C-NAPT.

En particulier, un mappage C-NAT est défini comme un couple de la forme (adresse IP WAN-Data, adresse IP LAN-Trans) fournissant un mappage bi-univoque entre les adresses WAN-Data et les adresses LAN-Trans. De même, un mappage C-NAPT est défini comme un couple de la forme (adresse IP WAN-Data et port TCP/UDP, adresse IP LAN-Trans et port TCP/UDP) fournissant un mappage multivoque entre une adresse WAN-Data unique et des adresses LAN-Trans multiples. Pour le trafic ICMP (comme un ping), on utilise un numéro de séquence ICMP à la place du numéro de port TCP/UDP.

Le trafic de LAN à WAN est défini comme étant d'origine paquet par les appareils IP de LAN et destiné à des appareils situés du côté WAN du service portail. Le trafic de WAN à LAN est défini comme d'origine paquet par les hôtes WAN et destiné à des appareils IP de LAN. Le trafic LAN à LAN est défini comme étant d'origine paquet par les appareils IP de LAN et destiné à des appareils IP de LAN sur le même sous-réseau ou sur un sous-réseau différent.

8.2.2.2 Modes de traitement des paquets

L'élément de service portail est configurable, via l'objet de base MIB cabhCapPrimaryMode, pour fonctionner dans un des trois modes primaires de traitement de paquet lors du traitement de trafic LAN à WAN et WAN à LAN:

1) mode traverse;
2) mode d'acheminement transparent C-NAT;
3) mode d'acheminement transparent C-NAPT.

De plus, les modes primaires C-NAT ou C-NAPT peuvent aussi fonctionner dans un mode mixte décrit ci-dessous.

En mode traverse, le portail CAP agit comme un pontage transparent [ISO DIS 10038 MAC Bridges] entre le secteur WAN-Data et le secteur LAN-Pass. En mode traverse, les décisions de transmission sont d'abord faites à la couche 2 OSI (couche Liaison de données). Dans ce mode, le portail CAP n'accompli aucune fonction d'acheminement transparent C-NAT ou C-NAPT.

Le portail CAP accepte la transmission de couche 3 OSI (couche Réseau) à la fois dans le mode d'acheminement transparent C-NAT et dans le mode d'acheminement transparent C-NAPT, décrits ci-dessous.

En mode C-NAT, l'élément de service portail (CDC) acquiert une ou plusieurs adresses IP utilisées pour le trafic WAN-Data pendant le processus d'amorce du service portail. Après l'acquisition, via DHCP, ces adresses IP sont utilisées comme portion d'adresse IP WAN-Data des couples de mappage C-NAT créée dynamiquement. S'il existe des adresses IP disponibles dans le groupe d'adresses IP WAN-Data, le portail CAP crée un mappage dynamique C-NAT lorsqu'il voit pour la première fois du trafic IP de LAN à WAN qui n'a pas de mappage existant. S'il n'existe pas d'adresses IP disponibles dans le groupe d'adresses IP WAN-Data, le mappage dynamique C-NAT ne peut pas être créé, ce trafic est abandonné, et un événement est généré (voir Annexe B).

Les mappages dynamiques C-NAT pour le trafic UDP sont détruits lorsqu'une temporisation de période d'inactivité, cabhCapUdpTimeWait, arrive à expiration. Les mappages dynamiques C-NAT pour le trafic TCP sont détruits lorsqu'une temporisation de période d'inactivité, cabhCapTcpTimeWait, arrive à expiration ou qu'une session TCP se termine. Les mappages dynamiques C-NAT pour le trafic ICMP sont détruits lorsqu'une temporisation de période d'inactivité, cabhCapIcmpTimeWait, arrive à expiration. De plus, les mappages statiques C-NAT peuvent être créés ou détruits lorsque le système NMS écrit ou supprime sur le tableau de base MIB cabhCapMappingTable.

En mode C-NAPT (mode de construction par défaut pour le système) l'élément de service portail (CDC) acquiert une adresse IP, utilisée pour le trafic WAN-Data. Après acquisition, via DHCP, cette adresse IP est utilisée comme portion d'adresse IP WAN-Data des couples de mappage

C-NAPT créé dynamiquement. Si l'adresse IP WAN-Data a été acquise, les mappages dynamiques C-NAPT sont créés lorsque le portail CAP voit pour la première fois du trafic LAN à WAN IP qui n'a pas de mappage existant. Si l'adresse IP WAN-Data n'a pas été acquise (c'est-à-dire qu'il n'y a pas de location DHCP active), le mappage dynamique C-NAPT ne peut pas être créé, ce trafic est abandonné, et un événement standard est généré (voir Annexe B).

Les mappages dynamiques C-NAPT pour le trafic UDP sont détruits lorsqu'une temporisation de période d'inactivité, cabhCapUdpTimeWait, arrive à expiration. Les mappages dynamiques C-NAPT pour le trafic TCP sont détruits lorsqu'une temporisation de période d'inactivité, cabhCapTcpTimeWait, arrive à expiration ou qu'une session TCP se termine. Les mappages dynamiques C-NAPT pour le trafic ICMP sont détruits lorsqu'une temporisation de période d'inactivité, cabhCapIcmpTimeWait, arrive à expiration. De plus, les mappages statiques C-NAPT peuvent être créés ou détruits lorsque le système NMS écrit ou supprime sur le tableau de base MIB cabhCapMappingTable.

La Figure 17 montre un processus typique de mappage dynamique C-NAPT avec un paquet TCP. Dans cet exemple, le service portail est configuré pour fonctionner en mode NAPT et a déjà obtenu une adresse IP de WAN, et l'appareil IP de LAN a déjà obtenu une adresse IP dans le secteur LAN-Trans.

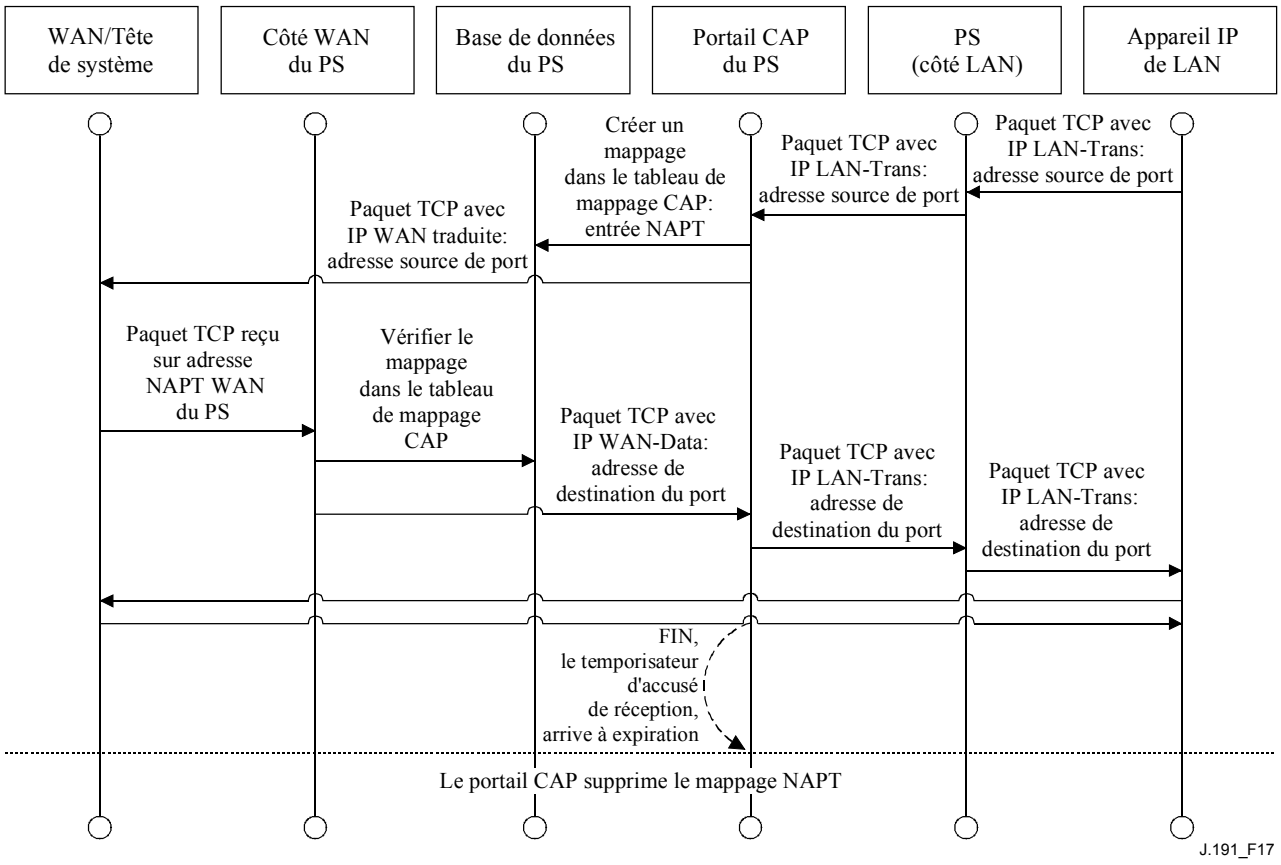

Figure 17/J.191 – Diagramme de séquence de configuration de service portail (Tableau de mappage CAP – NAPT)

Il est aussi possible au service portail de fonctionner en mode mixte pontage/acheminement. Dans ce cas, le système NMS établit le mode primaire à acheminement transparent C-NAT ou C-NAPT, et le système NMS écrit une ou plusieurs adresses MAC appartenant aux appareils IP de LAN, dont le trafic doit être ponté, dans le tableau (cabhCapPassthroughTable). Dans ce mode mixte, le service portail examine les adresses MAC des trames reçues pour déterminer si il faut faire un pontage

transparent de la trame ou effectuer des fonctions d'acheminement transparent C-NAT ou C-NAPT à la couche IP. Dans le cas de trafic de LAN à WAN, le service portail examine l'adresse MAC source, et si cette adresse MAC existe dans le tableau cabhCapPassthroughTable, la trame est pontée de façon transparente à l'interface WAN-Data. Dans le cas de trafic WAN à LAN, le service portail examine l'adresse MAC de destination et si cette adresse MAC existe dans le tableau cabhCapPassthroughTable, la trame est pontée de façon transparente à l'interface LAN appropriée. Si l'adresse MAC n'existe pas dans le tableau cabhCapPassthroughTable, le paquet est traité par des fonctions de couches supérieures, y compris la fonction d'acheminement transparent C-NAT/C-NAPT.

Il faut noter que la fonctionnalité USFS (voir § 8.2.2.3) est appliquée dans chacun des trois modes primaires de traitement de paquet, et sans que l'utilisation ou non du mode mixte entre en considération. Les décisions de transmission USFS prendront le pas sur les autres décisions de transmission qui pourraient éventuellement transmettre du trafic du LAN vers le WAN.

8.2.2.3 Généralités sur la commutation de transmission sélective de sens montant

Dans certains cas, un appareil IP de secteur d'adresse LAN-Pass résidera sur un sous-réseau IP logique différent de celui des autres appareils IP de LAN connectés au même élément de service portail. Il est important d'empêcher le trafic entre ces appareils IP de LAN de traverser le réseau HFC. Empêcher ce trafic HFC non désiré est la fonction qui est fournie par la commutation de transmission sélective de sens montant (USFS).

Spécifiquement, la fonction USFS achemine du trafic – qui a son origine chez l'utilisateur et est destiné à l'utilisateur – directement à sa destination. Le trafic ayant son origine dans un appareil IP de LAN dont l'adresse IP de destination est en dehors du secteur d'adresse du LAN est passé sans altération à la fonction pontage/acheminement du portail CAP.

La fonctionnalité USFS utilise le tableau de traduction d'adresse IP (comme défini dans la norme [RFC 2011]) au sein de l'élément de service portail. Ce tableau, le tableau ipNetToMediaTable de la norme [RFC 2011], contient une liste d'adresses MAC, leurs adresses IP correspondantes, et les numéros d'indice d'interface de service portail auxquels ces adresses sont associées. La fonction USFS va se référer à ce tableau afin de prendre des décisions sur la façon de diriger le flux de trafic de LAN vers WAN. Pour remplir le tableau ipNetToMediaTable, le service portail apprend les adresses IP et MAC et leurs associations. Pour chaque interface physique associée, le service portail apprend toutes les adresses IP LAN-Trans et LAN-Pass avec leurs liaisons MAC associées, et cet apprentissage peut se faire via différentes méthodes. Des méthodes d'apprentissage d'adresse IP/MAC spécifiques du fabricant peuvent inclure: espionnage du portail ARP, surveillance du trafic, et consultation des entrées de portail CDP. Les entrées sont purgées du tableau ipNetToMediaTable après l'expiration d'une période raisonnable de temporisation d'inactivité.

La fonctionnalité USFS inspecte tout le trafic IP reçu sur les interfaces LAN du service portail. Si l'adresse IP de destination se trouve (via le tableau ipNetToMediaTable) résider sur une interface LAN de service portail, l'adresse de destination de couche de liaison de données de la trame originale est changée de celle de l'adresse de la passerelle par défaut à celle de l'appareil IP de LAN de destination, et le trafic est retransmis sur l'interface LAN de service portail appropriée. Si on ne trouve pas de correspondance avec l'adresse IP de destination dans le tableau ipNetToMediaTable, le paquet est passé, dans sa forme originale, à la fonction d'acheminement transparent du C-NAT/C-NAPT ou à la fonction de pontage de traverse (selon le mode de traitement de paquet activé).

8.2.2.4 Multidiffusion

Le portail CAP accepte le trafic en multidiffusion par le pontage transparent des messages IGMP [RFC 2236] et des paquets en multidiffusion. Le portail CAP transmet le trafic IGMP originaire du WAN au LAN pour permettre aux annonces d'atteindre les appareils IP de LAN. Un appareil IP de LAN va déterminer à quelle multidiffusion il souhaite se joindre et enverra un message

multidiffusion "join" (*joindre*). La source multidiffusion sera alors capable de transmettre des données à l'appareil IP de LAN. Lorsque le service multidiffusion n'est plus désiré, l'appareil IP de LAN peut soit ignorer le serveur et le flux s'arrêtera en fin de temporisation, ou bien l'appareil IP de LAN peut envoyer un message IGMP "leave" (*quitter*) à la chaîne pour couper le flux de trafic. La Figure 18 donne un exemple détaillé des processus IGMP et multidiffusion passant à travers un service portail.

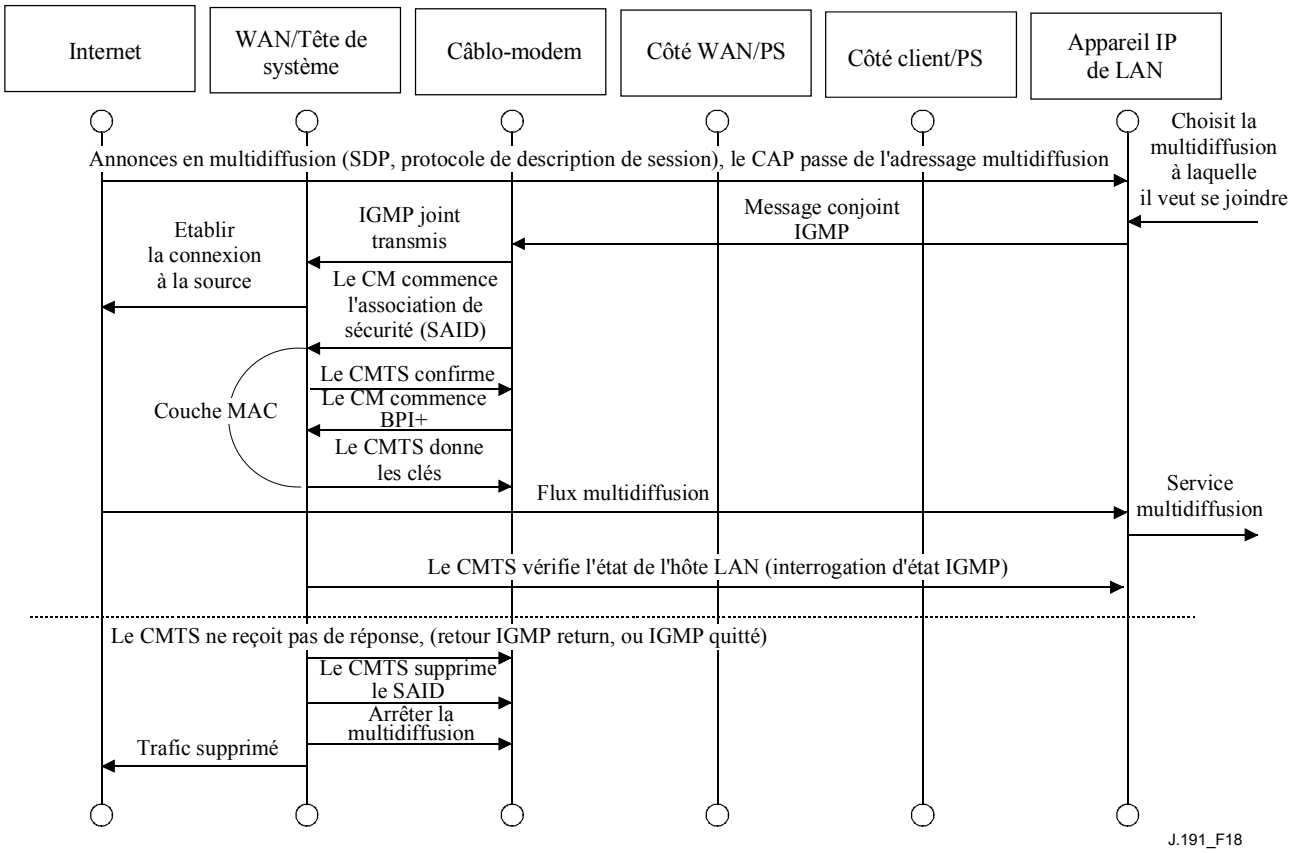

Figure 18/J.191 – Multidiffusion via une séquence IGMP

8.2.2.5 Exemples de traitement de paquet

Le présent paragraphe donne quelques informations sur les processus impliqués dans le traitement de paquet. La Figure 19 donne un exemple d'étapes possibles de traitement de paquet pour le trafic monodiffusion de LAN à WAN, et la Figure 20 donne un exemple d'étapes possibles de traitement de paquet pour du trafic monodiffusion de WAN à LAN. Ces exemples ne sont qu'informatifs et n'impliquent aucune obligation quant à l'implémentation.

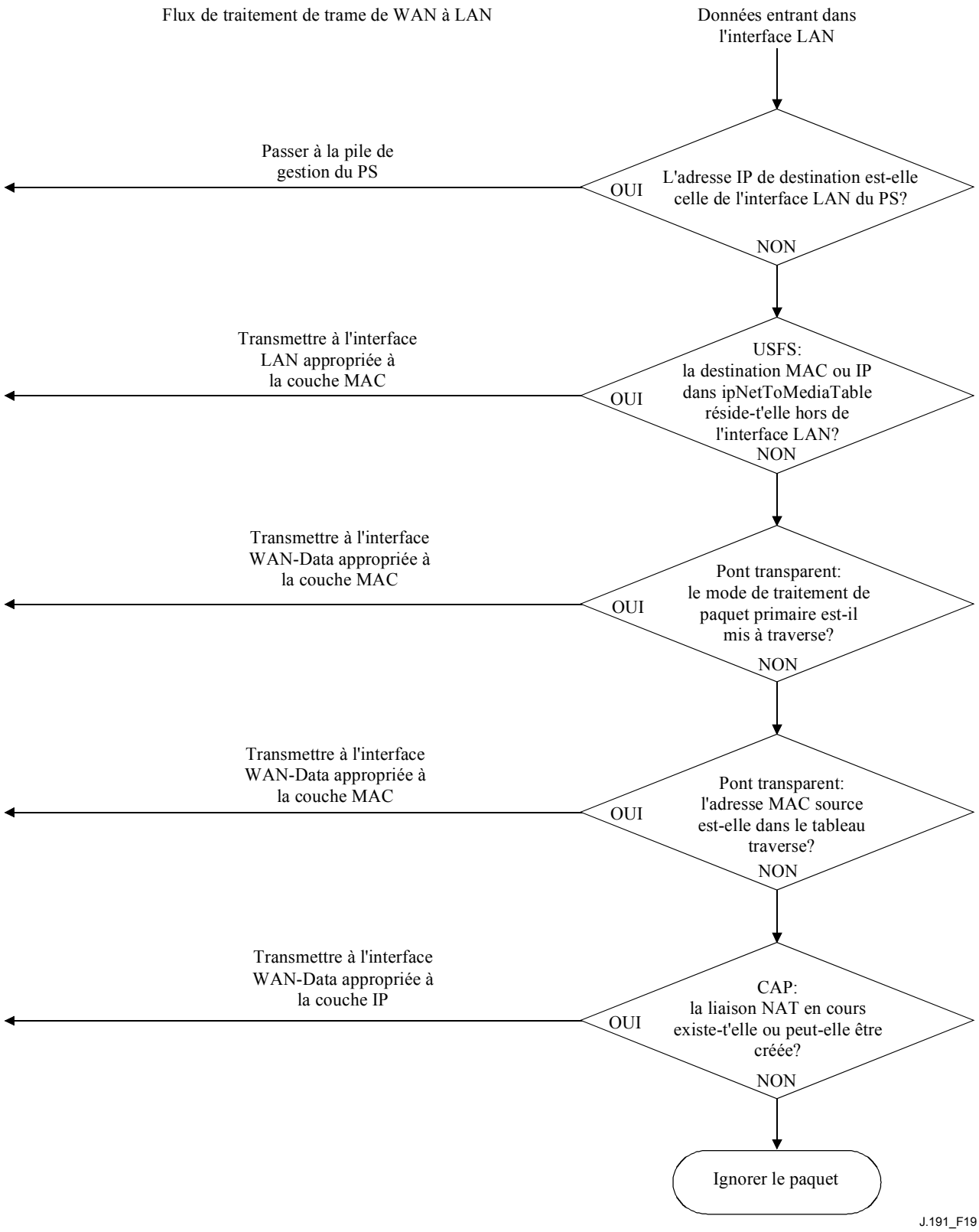

Figure 19/J.191 – Exemple de traitement de paquet de LAN à WAN

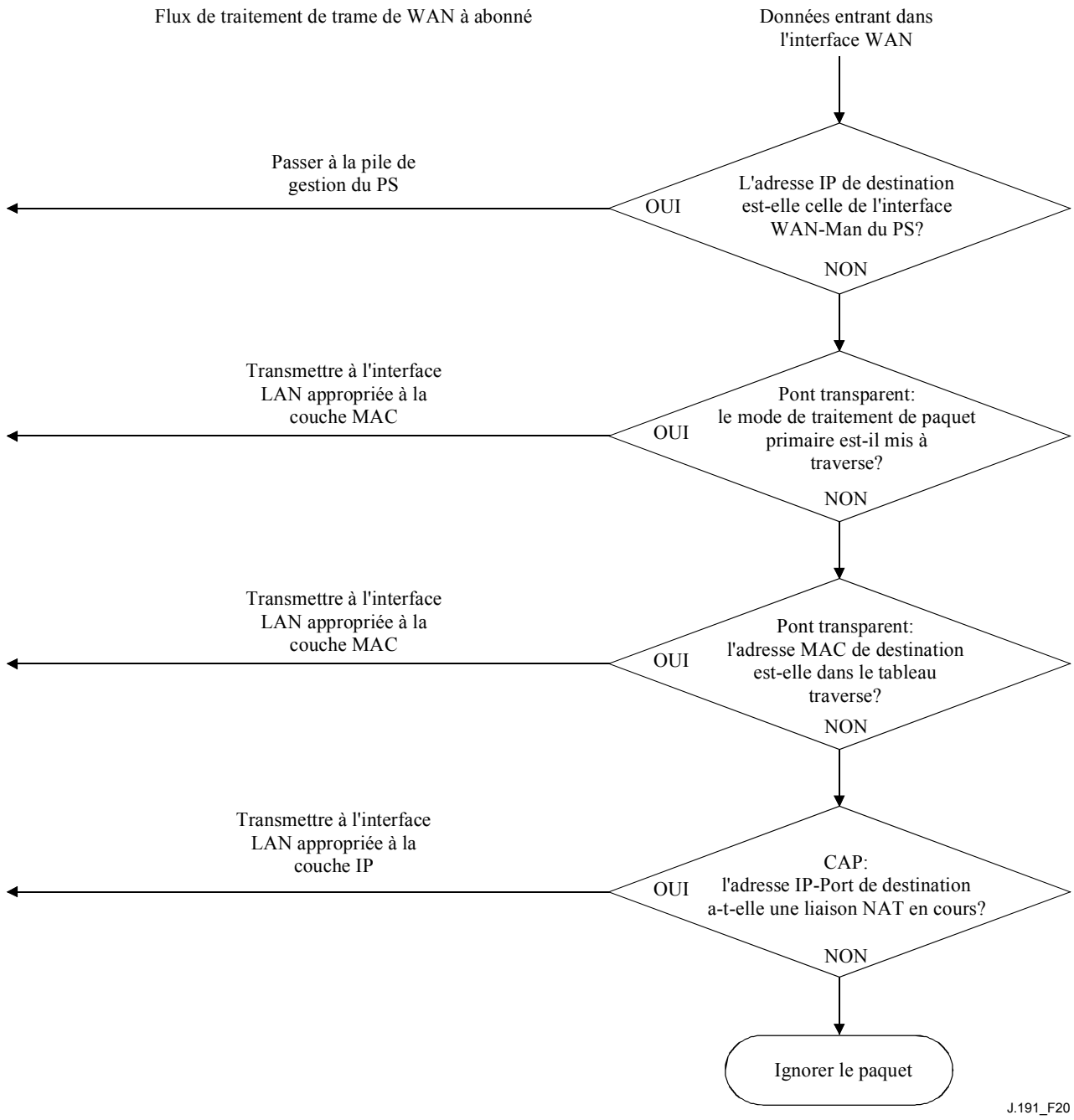

Figure 20/J.191 – Exemple de traitement de paquet de WAN à LAN

8.3 Exigences pour le portail CAP

8.3.1 Exigences générales

Toutes les interfaces IP logiques sur l'élément de service portail DOIVENT être conformes aux sections 3 et 4 de la norme [RFC 1122], pour permettre les communications standard avec les hôtes Internet.

Le portail CAP DOIT accepter le trafic multidiffusion, au moyen du pontage transparent de messages IGMP et de paquets mutidiffusion IP comme défini dans la norme [RFC 2236].

8.3.2 Exigences pour le traitement des paquets

Le portail CAP DOIT accepter le mode traverse, le mode d'acheminement transparent C-NAT, et le mode d'acheminement transparent C-NAPT, et le portail CAP DOIT accepter la sélection de ce mode primaire de traitement de paquet, via l'objet de base MIB cabhCapPrimaryMode.

Si le mode primaire de traitement de paquet, cabhCapPrimaryMode, est réglé à C-NAT, le portail CAP DOIT s'assurer qu'il existe une adresse IP disponible fournie par la tête de système dans le groupe d'adresses IP WAN-Data (avec une location DHCP en cours) avant d'essayer d'utiliser cette adresse IP comme partie d'un mappage C-NAT. Si le portail CAP n'est pas capable de créer un mappage C-NAT, du fait de la réduction du groupe d'adresses IP WAN-Data, il doit générer un événement standard (comme défini à l'Annexe B).

Si le mode primaire de traitement de paquet, cabhCapPrimaryMode, est réglé à C-NAPT, le portail CAP DOIT s'assurer qu'il existe une adresse IP de WAN en cours (avec une location DHCP en cours venant de l'approvisionnement de la tête de système) avant d'essayer d'utiliser cette adresse IP comme partie d'un mappage C-NAPT. Si le portail CAP est incapable de créer un mappage C-NAPT, du fait qu'il n'a pas d'adresse IP de WAN en cours ou du fait de la réduction du nombre de ports, il doit générer un événement standard (comme défini à l'Annexe B).

Le trafic de LAN à LAN NE DOIT jamais être acheminé ou ponté hors d'une interface de WAN.

8.3.2.1 Exigences de traverse

Lorsque le mode primaire de traitement de paquet du portail CAP, cabhCapPrimaryMode, est réglé au mode traverse, le portail CAP DOIT agir comme un pont transparent, comme défini dans la norme [ISO/CEI 10038], entre le secteur WAN-Data et le secteur LAN-Pass, et NE DOIT PAS effectuer de fonctions d'acheminement transparent C-NAT ou C-NAPT. Même lorsque le mode primaire de traitement de paquet est réglé à traverse, le traitement de fonction USFS DOIT prendre le pas sur les décisions de pontage de LAN à WAN.

8.3.2.2 Exigences d'acheminement transparent C-NAT et C-NAPT

Lorsque le mode primaire de traitement de paquet (cabhCapPrimaryMode) est réglé à C-NAT le portail CAP DOIT accepter le processus de traduction d'adresse C-NAT conformément aux exigences de base NAT définies dans la norme [RFC 3022].

Lorsque le mode primaire de traitement de paquet (cabhCapPrimaryMode) est réglé à C-NAPT le portail CAP DOIT accepter le processus de traduction d'adresse C-NAPT conformément aux exigences de base NAT définies dans la norme [RFC 3022].

Sans considération du mode primaire de traitement de paquet, le portail CAP DOIT accepter la création et la suppression des correspondances statiques C-NAT et C-NAPT, en permettant au système NMS de lire, créer et supprimer (via le portail CMP) les entrées de mappage statique de portail CAP (cabhCapMappingTable).

Les mappages statiques C-NAT et C-NAPT créés par le système DOIVENT persister à travers les réamorçages du service portail.

Le portail CAP DOIT accepter la création de mappages statiques C-NAT et C-NAPT, initialisés par le trafic TCP, UDP ou ICMP de LAN à WAN. Le portail CAP DOIT permettre au système NMS de lire (via le portail CMP) les entrées de mappage dynamique du portail CAP (cabhCapMappingTable).

Le portail CAP DOIT accepter la suppression de mappages dynamiques C-NAT et C-NAPT si un mappage donné est associé à une session TCP ET que cette session TCP se termine OU que la temporisation d'inactivité TCP, cabhCapTcpTimeWait, pour ce mappage, arrive à expiration.

Le portail CAP DOIT accepter la suppression de mappages dynamiques C-NAT et C-NAPT si un mappage donné est associé à une session UDP ET que la temporisation d'inactivité UDP, cabhCapUdpTimeWait, pour ce mappage, arrive à expiration.

Le portail CAP DOIT accepter la suppression de mappages dynamiques C-NAT et C-NAPT si un mappage donné est associé à une session ICMP ET que la temporisation d'inactivité ICMP, cabhCapIcmpTimeWait, pour ce mappage, arrive à expiration.

Les mappages dynamiques C-NAT et C-NAPT NE DOIVENT PAS persister à travers les réamorçages de service portail.

8.3.2.3 Exigences du mode mixte pontage/acheminement

Le portail CAP DOIT accepter le mode mixte de pontage/acheminement comme décrit au § 8.2.2, où le mode primaire de traitement de paquet au portail CAP, cabhCapPrimaryMode, est réglé à "acheminement transparent C-NAT ou C-NAPT" et où le portail CAP va aussi ponter de façon transparente du trafic pour des adresses MAC particulières. Si le mode primaire de traitement de paquet du portail CAP, cabhCapPrimaryMode, est réglé sur l'acheminement transparent C-NAT ou C-NAPT ET que le système NMS a écrit une adresse MAC appartenant à un appareil IP de LAN dans le tableau cabhCapPassthroughTable, le portail CAP DOIT ponter de façon transparente le trafic de LAN à WAN originaire de cette adresse MAC et le trafic de WAN à LAN destiné à cette adresse MAC.

En mode mixte de pontage/acheminement, comme décrit au § 8.2.2, la fonction USFS DOIT être appliquée à tout le trafic d'origine LAN reçu.

8.3.3 Exigences USFS

La fonctionnalité de commutation de transmission sélective de sens montant (USFS) DOIT être appliquée au traitement de paquet, sans considération du mode de traitement de paquet du portail CAP (traverse, C-NAT, C-NAPT, ou pontage/acheminement mixte).

L'élément de service portail DOIT apprendre toutes les adresses IP de LAN-Trans, IP de LAN-Pass, et MAC des appareils IP de LAN, associées à chacune de ses interfaces de réseau physique actives. Les adresses IP et MAC apprises par l'élément de service portail et les numéros d'index d'interface physique de service portail DOIVENT être accessible au système NMS (à travers le portail CMP) via le tableau ipNetToMediaTable [RFC 2011]. L'élément de service portail DOIT supprimer les entrées du tableau ipNetToMediaTable, lorsqu'une temporisation d'inactivité arrive à expiration.

La fonction USFS DOIT inspecter tout le trafic IP prenant son origine sur les interfaces de LAN du service portail, pour déterminer si l'adresse IP de destination d'un paquet est celle d'un appareil résidant sur une interface IP de LAN. Si l'adresse IP de destination dans un paquet inspecté par la fonction USFS est celle d'un appareil IP de LAN résidant hors d'une interface LAN du service portail, la fonction USFS DOIT remplacer l'adresse de destination de la couche MAC, au sein de l'en-tête de couche 2 du paquet, par l'adresse MAC de l'appareil IP de LAN de cette destination et transmettre la trame à l'interface LAN physique appropriée.

9 Résolution de nom

9.1 Introduction/Aperçu général

9.1.1 Objectifs

Parmi les objectifs de la résolution de nom figurent:

- fournir le système de nom de domaine (DNS, *domain name system*) à partir d'un serveur dans le service portail aux clients DNS au sein des appareils IP de LAN, même pendant les coupures de connexion du câble;

- permettre aux abonnés de se référer aux appareils locaux au moyen de noms d'appareils ayant une signification intuitive plutôt que d'une adresse IP;
- soumettre les clients DNS de LAN aux serveurs DNS de tête de système, pour la résolution des noms d'hôtes non locaux;
- fournir une récupération de service DNS facile lors du rétablissement de la connexion câble après une coupure.

9.1.2 Hypothèses

Parmi les hypothèses de fonctionnement des services de nommage figurent que:

- le serveur DNS dans l'élément de service portail est le seul serveur DNS qui fait foi pour les appareils IP de LAN dans le secteur LAN-Trans;
- l'élément de service portail ne fournira pas le service DNS aux appareils IP de LAN dans le secteur LAN-Pass;
- si l'élément de service portail utilise des adresses WAN-Data multiples, les informations de serveur DNS de WAN obtenues pendant le processus (DHCP) d'acquisition d'adresse WAN-Data le plus récent seront utilisées.

9.2 Architecture

9.2.1 Lignes directrices pour la conception du système

Voir Tableau 27.

Tableau 27/J.191 – Lignes directrices pour la conception du système de résolution de nom

Référence	Lignes directrices pour la conception du système
Name Rsln 1	Fournir le service de nom de domaine (DNS) à partir d'un serveur dans le service portail aux clients DNS dans les appareils IP de LAN, pour la résolution de nom des appareils IP de LAN (indépendamment de l'état de la connexion WAN).
Name Rsln 2	Fournir l'arbitrage DNS aux serveurs DNS de tête de système, pour les clients DNS au sein des appareils IP de LAN, pour la résolution des noms d'hôtes non locaux.

9.2.2 Description du système

Le présent paragraphe donne un aperçu général sur les services de résolution de nom au sein de l'élément de service portail.

9.2.2.1 Aperçu général sur le fonctionnement de la résolution de nom

Le portail de nommage du câble (CNP, *cable naming portal*) est un service fonctionnant dans le service portail qui fournit un serveur DNS simple aux appareils IP de LAN dans le secteur d'adresse LAN-Trans. Le portail CNP n'est pas utilisé par les appareils IP de LAN dans le secteur d'adresse LAN-Pass, parce qu'ils seront servis directement par les serveurs DNS extérieurs au domicile.

Tous les appareils IP de LAN dans le secteur LAN-Trans sont configurés par le portail CDP pour utiliser le portail CNP comme leur serveur de nom de domaine. Le service de portail CNP dans le secteur LAN-Trans ne dépend pas de l'état de la connexion WAN. Le portail CNP effectue les tâches suivantes:

- résoudre les noms d'hôte pour les appareils IP de LAN, en retournant leurs adresses IP correspondantes;
- renvoyer les appareils IP de LAN à des serveurs DNS extérieurs pour les questions qui ne peuvent être résolues via les informations de service portail locales. Cette action ne survient que lorsque des informations de serveur DNS de WAN sont disponibles dans le service

portail. Autrement, le portail CNP retourne une erreur indiquant que le nom ne peut être résolu à ce moment.

Faire du portail CNP le serveur DNS primaire dans les locaux de l'utilisateur évite d'avoir à reconfigurer les appareils IP de LAN lorsque change l'état de la connexion WAN. Cela permet aussi de changer l'allocation de serveur DNS extérieur sans reconfigurer l'appareil IP de LAN.

9.2.2.2 Fonctionnement de la résolution de nom

Lorsqu'il est interrogé pour résoudre un nom d'hôte, le portail CNP effectue un processus d'examen indiqué à la Figure 21. Le portail CNP répond aux questions initiales DNS standard [RFC 1035], dirigées sur l'adresse cabhCdpServerDnsAddress, pour toutes les consultations de noms. Si le portail CNP répond avec un renvoi à des serveurs DNS extérieurs, on supposera qu'il est de la responsabilité de l'appareil IP de LAN d'envoyer une question directement au serveur mentionné.

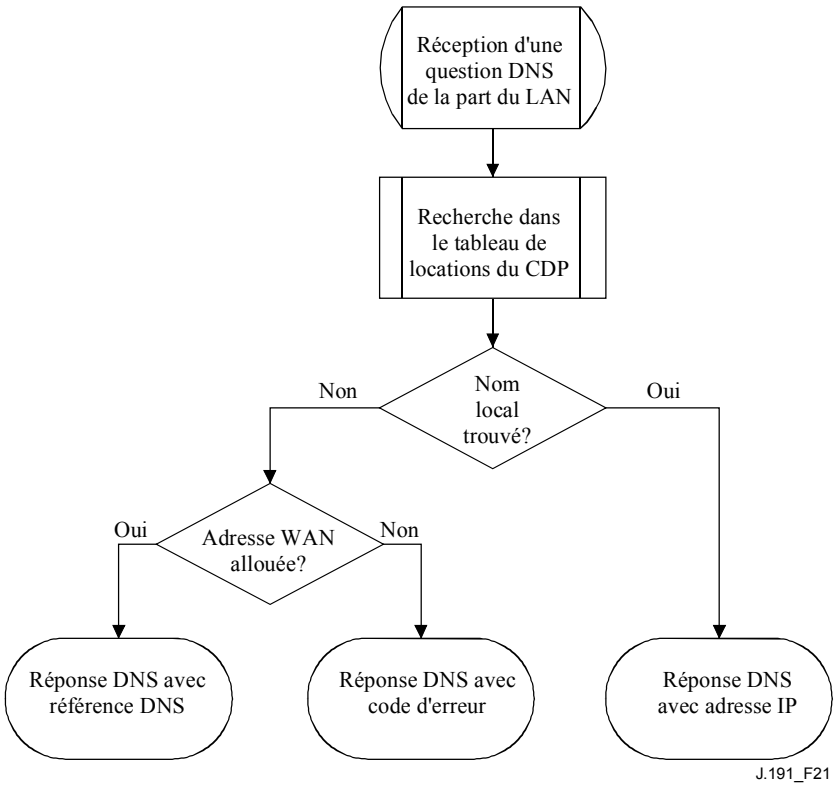

Figure 21/J.191 – Traitement de paquet au portail CNP

Le portail CNP s'appuie sur le tableau cabhCdpLanAddrTable du portail CDP, pour apprendre les noms d'hôte associés aux adresses IP actuelles des appareils IP de LAN actifs. Tant que l'appareil IP de LAN maintient une location DHCP active avec le portail CDP et a fourni un nom d'hôte au portail CDP (au titre du processus d'acquisition d'adresse IP) son nom peut être résolu par le portail CNP. Si le nom d'hôte dont la résolution est demandée ne peut être trouvé dans le tableau cabhCdpLanAddrTable, le portail CNP retourne un avis de serveur DNS qui indique un serveur DNS extérieur (qui le client CDC apprend via les options DHCP). L'adresse IP du serveur DNS extérieur est la dernière entrée cabhCdpWanDataAddrDnsIp dans le tableau cabhCdpWanDataAddrServerTable du portail CDP.

Une interrogation de serveur DNS standard spécifie un nom de domaine cible (QNAME), un type d'interrogation (QTYPE, *query type*), et une classe d'interrogation (QCLASS, *query class*), et demande des enregistrements de ressources qui correspondent. Le portail CNP va répondre aux interrogations de serveur DNS avec QCLASS = IN, et QTYPE = A, NS, SOA ou PTR comme

défini dans la norme [RFC 1035]. L'acceptation de transferts de zone et de serveur DNS au protocole TCP n'est pas exigée.

Dans la mesure où le portail CNP est un serveur DNS de confiance dans le secteur LAN-Trans, il va fournir les enregistrements de début d'autorisation (SOA, *start of authority*) et de serveur de nom (NS, *nameserver*) de confiance sur demande. Le Tableau 28 est un exemple des champs d'enregistrement SOA (voir la section 3.3.13 de la norme [RFC 1035]):

Tableau 28/J.191 – Champs d'enregistrement SOA

Champ RDATA de RFC 1035	Objet MIB de CDP
MNAME	cabhCdpServerDomainName
RNAME	Non spécifié
SERIAL	Non spécifié
REFRESH	Non spécifié
RETRY	Non spécifié
EXPIRE	Non spécifié
MINIMUM	Non spécifié

Le champ MNAME est le nom de domaine du secteur d'adresse LAN-Trans. Le portail CNP utilise la valeur conservée dans cabhCdpServerDomainName comme nom de domaine de secteur d'adresse LAN-Trans.

La champ RNAME est la boîte à lettre de la personne responsable du domaine. Si le service portail conserve une adresse e-mail pour un administrateur, ces informations pourraient être spécifiées dans ce champ.

La champ SERIAL est un nombre arithmétique de 32 bits, utilisé pour identifier la version des informations de zone. Mais dans la mesure où les transferts de zone ne sont pas spécifiés, la valeur de ce champ n'est pas spécifiée.

9.3 Exigences pour la résolution des noms

Le portail CNP DOIT être conforme au format de message DNS standard et accepter les interrogations DNS standard, comme décrit dans les normes [RFC 1034, RFC 1035].

Le portail CNP est un serveur sans état qui DOIT être capable de recevoir des interrogations et d'envoyer des réponses en paquets UDP [RFC 768].

Le portail CNP DOIT fonctionner au moins en mode non récursif, comme défini dans [RFC 1034].

Le portail CNP répond aux interrogations de noms, en n'utilisant que des informations locales au sein du service portail, et ses messages de réponse DOIVENT contenir une erreur, une réponse, ou une soumission à un serveur DNS extérieur.

Le portail CNP DOIT répondre aux interrogations DNS adressées à cabhCdpServerDnsAddress.

Le portail CNP NE DOIT PAS répondre à des interrogations DNS adressées aux adresses IP WAN-Man et WAN-Data du service portail.

A réception d'une demande initiale de résolution de nom d'hôte de la part d'un appareil IP de LAN, le portail CNP DOIT accéder au tableau cabhCdpLanAddrTable du portail CDP pour examiner les noms d'hôte associés aux adresses IP qui sont louées aux appareils IP de LAN.

Sans considération de l'état de l'entrée cabhCdpWanDataAddrDnsIp dans le tableau cabhCdpWanDataAddrServerTable du portail CDP, si le nom d'hôte peut être résolu par le portail

CNP à partir de données locales, le portail CNP DOIT répondre à l'interrogation de résolution de nom d'hôte par l'adresse IP de l'appareil IP de LAN nommé.

Lorsqu'il fonctionne comme un serveur DNS non récursif: si le nom d'hôte ne peut être résolu par le portail CNP à partir des données locales ET que la dernière entrée cabhCdpWanDataAddrDnsIP dans le tableau cabhCdpWanDataAddrServerTable du portail CDP est remplie, le portail CNP DOIT répondre à l'interrogation de résolution de nom par une soumission à un serveur DNS extérieur, représentée par l'adresse IP contenue dans l'objet cabhCdpWanDataAddrDnsIp.

Si le nom d'hôte ne peut pas être résolu par le portail CNP à partir de données locales ET que l'objet cabhCdpWanDataAddrDnsIp n'est pas rempli, le portail CNP DOIT répondre à l'interrogation de résolution de nom d'hôte avec l'erreur appropriée spécifiée par [RFC 1035].

Lors qu'arrive à expiration la dernière location DHCP WAN-Data restante, le client CDC DOIT effacer toutes les entrées cabhCdpWanDataAddrDnsIp du tableau cabhCdpWanDataAddrServerTable.

Le portail CNP DOIT répondre aux interrogations DNS du type QCLASS = IN, et QTYPE = A, NS, SOA ou PTR.

Les réponses du portail CNP aux interrogations DNS DOIVENT être conformes à la section 3.3 de la norme [RFC 1035], avec le bit Authoritative Answer (*réponse d'autorisation*) mis à "1" dans la section d'en-tête (voir la section 4.1.1 de la norme [RFC 1035]).

Dans la mesure où le portail CNP est un serveur DNS de confiance au sein du secteur LAN-Trans, il DOIT fournit les enregistrements de début d'autorisation (SOA, *start of authority*) et de serveur de nom (NS) de confiance sur demande. Les champs d'enregistrement de SOA (voir la section 3.3.13 de la norme [RFC 1035]) DOIVENT contenir une entrée pour le champ MNAME qui soit égal à la valeur de l'objet de base MIB cabhCdpServerDomainName du portail CDP.

Si le nom cabhCdpServerDomainName n'est pas réglé, le portail CNP DOIT encore fournir le service d'arbitrage de serveur DNS aux appareils IP de LAN.

10 Qualité de service

10.1 Introduction

Le présent paragraphe décrit le rôle du câblo-modem amélioré IP pour permettre aux applications d'abonné d'utiliser les ressources de qualité de service IPCablecom et DOCSIS. Ces ressources fournissent un mécanisme de gestion qui donne des priorités aux flux de sessions de données pour accepter le trafic d'applications en temps réel, tels que voix sur le protocole Internet, répartition A/V, et jeux vidéo, en réduisant la latence des paquets et les délais de gigue. Les mécanismes de qualité de service IPCablecom et DOCSIS permettent aussi une gestion plus efficace du trafic sur le réseau HFC.

La qualité de service définit les exigences d'élément de service portail nécessaires pour permettre aux applications IPCablecom d'établir les différents niveaux de qualité de service à travers le réseau HFC.

10.1.1 Objectifs

Les objectifs de qualité de service comportent:

- permettre aux applications d'abonné d'établir des priorités dans les sessions de données entre le système CMTS et l'appareil de service portail en utilisant le système de messages conforme à IPCablecom;
- faciliter la conception et les essais de terrain qui conduisent à la fabrication et l'interfonctionnement des matériels et logiciels des différents fabricants.

10.1.2 Hypothèses

Les hypothèses suivantes sont faites pour la qualité de service:

- la qualité de service suppose que les systèmes IPCablecom existent sur le réseau câblé;
- pour éviter des problèmes avec les fonctions NAT dans l'élément de portail CAP, les applications conformes à IPCablecom utiliseront l'adressage LAN-Pass comme défini aux paragraphes 7 et 8.

10.2 Architecture de qualité de service

L'architecture de qualité de service (CQoS) se compose d'éléments fonctionnels et de la classe d'appareils HA. Les développeurs d'équipements de réseau (par exemple, de matériel et de logiciel) implémentent un ou plusieurs de ces éléments selon l'ensemble de caractéristiques désirées. Les ensembles minimaux de capacités spécifiés doivent obligatoirement participer du domaine CQoS. Les éléments de base CQoS sont présentés au § 10.2.2.

10.2.1 Lignes directrices pour la conception du système

La liste des lignes directrices pour la conception du système de qualité de service figure dans le Tableau 29.

Tableau 29/J.191 – Lignes directrices pour la conception du système de qualité de service

Numéro	Lignes directrices pour la conception du système de qualité de service
QS 1	Il existera un mécanisme standard de signalisation de qualité de service permettant aux câblo-modems améliorés IP d'accepter l'établissement de priorités de sessions de service à travers le réseau DOCSIS pour les applications multimédia.
QS 2	Les applications multimédia peuvent être incorporées dans l'appareil HA ou sur un appareil externe connecté à l'appareil HA.
QS 4	Les applications multimédia peuvent inclure des services IPCablecom (E-MTA/S-MTA).

10.2.2 Description du système de qualité de service

L'architecture CQoS se compose des entités suivantes:

- domaine CQoS;
- fonction de service portail (PS);
- fonction portail de qualité de service câble (CQP);
- appareil HA;
- système CMTS.

Le domaine CQoS définit la sphère d'influence directe de la fonctionnalité CQoS, qui est étendue à l'appareil HA à partir de la tête de système du réseau câblé. Le service portail et les éléments de portail CQP sont pleinement à l'intérieur du domaine CQoS et sont spécifiés. Le domaine CQoS existe pour fournir des services aux applications conformes à IPCablecom.

L'architecture de référence décrit aussi l'appareil HA. Voir le paragraphe 5.

Le système de terminaison de câblo-modem (CMTS, *cable modem termination system*) est situé à la tête de système du réseau câblé et gère les fonctions DOCSIS de qualité de service.

10.2.2.1 Elément des services portail

L'élément des services portail (PS) est un élément logique qui contient des composants de portail d'adressage réseau, de gestion, de sécurité et de qualité de service qui fournissent des fonctions de traduction entre le réseau HFC et l'abonné. Le service portail ne réside que dans les appareils HA (voir le paragraphe 5). Le composant de qualité de service est appelé portail de qualité de service du câble (CQP). Le portail CQP agit comme un portail CQoS pour les applications compatibles IPCablecom. Sa fonction primaire est de transmettre la messagerie de qualité de service entre le système CMTS et les applications IPCablecom.

10.2.2.2 Domaine CQoS

Le domaine CQoS existe sur une base d'utilisateur individuel. Les domiciles individuels sont séparés et ont des domaines CQoS indépendants. L'élément de portail CQP fait la limite du domaine CQoS au sein d'un domicile donné.

10.2.2.3 Classes d'appareils physiques et éléments fonctionnels de CQoS

Les appareils HA contiennent l'élément logique de service portail et l'élément fonctionnel de portail CQP. Le portail CQP agit comme un pont transparent pour la messagerie de qualité de service des applications IPCablecom (APP). Un exemple des relations entre les éléments fonctionnels de CQoS et la classe d'appareils HA est présenté à la Figure 22.

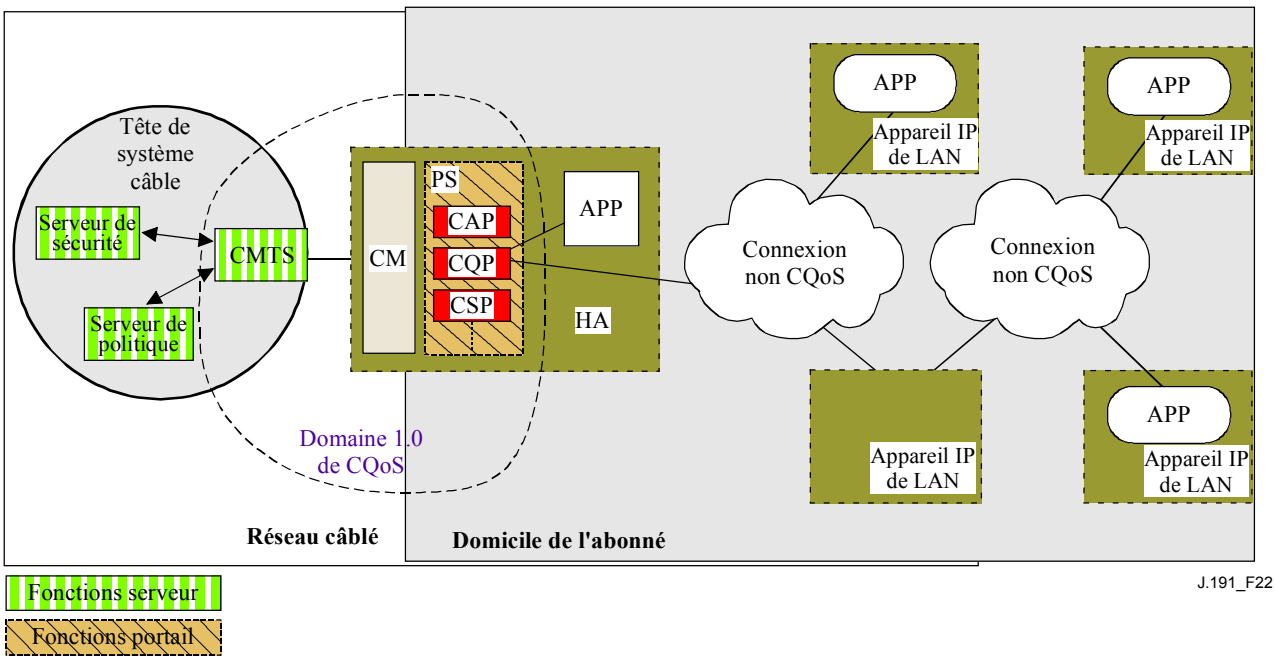

Figure 22/J.191 – Exemple d'éléments fonctionnels de CQoS

10.3 Exigences de la messagerie QS câble

L'architecture de qualité de service (CQoS) se compose de l'élément fonctionnel de portail CQP dans le domaine CQoS. Le portail CQP existe dans le service portail et soutient la livraison de la messagerie de qualité de service à travers le réseau HFC pour les applications IPCablecom. La messagerie conforme à IPCablecom inclut la messagerie de qualité de service et d'autres messages en rapport avec les questions d'un service spécifique comme les décisions de politique et d'application de modèles de réservation à deux phases.

Les exigences fonctionnelles pour le portail CQP et d'autres éléments de CQoS sont définis dans les paragraphes ci-dessous.

10.3.1 Exigences du portail CQP

Le portail CQP DOIT agir comme un pont transparent et transmettre la messagerie de qualité de service IPCablecom (Recommandations UIT-T J.161 et J.163) entre le système CMTS et les applications IPCablecom. Les données d'application sont associées à un flux de service DOCSIS en fonction d'un classificateur qui est créé dans l'interface du câblo-modem sur la base des informations incluses dans les messages IPCablecom (tels que RSVP PATH).

Dans la mesure où les exigences de portail CQP sont simplement de transmettre la messagerie de qualité de service IPCablecom, il n'y a pas de dépendance du système NMS pour assurer cette fonction. Donc, cette fonction CQP reste la même à la fois pour le mode d'approvisionnement DHCP et pour le mode d'approvisionnement SNMP (voir § 5.7).

10.3.2 Gestion de la politique de qualité de service et commande d'admission

La messagerie de qualité de service IPCablecom est définie par les Recommandations UIT-T J.161 et J.163. Comme telles, les fonctions de gestion de la politique de qualité de service et de commande d'admission sont également définies par les Recommandation IPCablecom.

11 Sécurité

11.1 Introduction/Aperçu général

Le présent paragraphe définit les interfaces de sécurité, protocoles et exigences fonctionnelles nécessaires pour fournir sur une base fiable les services IP fondés sur le câble au service portail dans un environnement sécurisé.

Assurer la livraison de services IP multimédia aux appareils clients chez l'utilisateur exige un mécanisme sécurisé pour protéger ces services des accès illégaux, de l'espionnage et de l'interruption. L'objet de toute technologie de sécurité est de protéger la valeur, qu'elle soit un flux de revenu ou un capital d'informations commercialisables d'un certain type. Les menaces contre ce revenu existent lorsqu'un utilisateur du réseau perçoit la valeur, dépense des efforts et de l'argent, et invente une technique pour échapper aux payements nécessaires (voir l'Annexe C). Certains utilisateurs du réseau vont jusqu'à des extrémités pour voler lorsqu'ils perçoivent une valeur extrême. L'ajout des techniques de sécurité pour protéger la valeur a un coût associé; plus on dépense d'argent, plus grande est la sécurité (l'efficacité de la sécurité est donc de l'économie de base).

11.1.1 Objectifs

Parmi les objectifs du modèle de sécurité figurent:

- employer une technique de sécurité répondant à son coût pour forcer tout utilisateur ayant l'intention de voler ou interrompre des services réseau à dépenser une quantité déraisonnable de ressources en argent ou en temps;
- sécuriser les connexions domestiques utilisées pour offrir des services câblés à grande valeur de sorte qu'elles soient au moins aussi sécurisées que les technologies DOCSIS et IPCablecom sur le réseau hybride optique coaxial (HFC, *hybrid fiber-coax*);
- fournir des mécanismes de sécurité flexibles pour qu'ils soient compatibles avec les mécanismes de sécurité DOCSIS et IPCablecom utilisés sur le réseau HFC.

11.1.2 Hypothèses

Parmi les hypothèses pour l'environnement de sécurité figurent:

- que la fonction service portail et câblo-modem résident dans un seul appareil physique;
- que des niveaux de sécurité inférieurs puissent exister au domicile lorsque les services fournis sont considérés comme étant de faible valeur.

11.2 Architecture de sécurité

L'architecture de sécurité est fondée sur l'architecture générale définie au paragraphe 5. L'architecture définit un élément IP de service portail (PS), qui inclut des fonctions de gestion/approvisionnement, sécurité et qualité de service.

L'architecture inclut aussi un ensemble d'éléments de tête de système comme le système de terminaison de câblo-modem (CMTS), le serveur de protocole de configuration dynamique d'hôte (DHCP), le serveur de gestion de réseau, le serveur de sécurité, etc.

La spécification de sécurité se concentre sur la définition, les fonctionnalités et interfaces des fonctions de sécurité et sur la sécurité qui se rapporte aux serveurs de tête de système.

11.2.1 Lignes directrices pour la conception du système

La liste des exigences pour la conception de la sécurité figure au Tableau 30. Cette liste donne des directives pour le développement de la spécification de sécurité.

Tableau 30/J.191 – Lignes directrices pour la conception du système de sécurité

Référence	Lignes directrices pour la conception du système de sécurité
SEC1	L'opérateur aura la capacité de gérer à distance des pare-feu conformes.
SEC2	La conception du système de sécurité comprendra une interface d'enregistrement/messagerie d'événements de pare-feu permettant à l'opérateur de surveiller et corriger l'activité du pare-feu.
SEC3	Les messages de gestion du pare-feu entre la tête de système du câble et le service portail seront authentifiés et facultativement cryptés pour les protéger contre toute surveillance et commandes non autorisées.
SEC4	La conception du système de sécurité comprendra l'authentification mutuelle des éléments.
SEC5	Le niveau de sécurité à domicile sera tel qu'il ne soit pas facile pour l'abonné moyen d'obtenir un accès illégal au réseau HFC et aux services du câble.
SEC6	Une fois le compte d'un abonné ouvert, l'authentification du service portail avec le système d'approvisionnement de l'opérateur devra être automatique.
SEC7	L'opérateur aura la capacité de télécharger de façon sécurisée des copies de logiciel, des fichiers de configuration et les règles de comportement vis-à-vis du pare-feu sur l'élément de service portail.
SEC8	La sécurité apportera à travers le pare-feu le soutien nécessaire pour la DQoS sécurisée IPCablecom.
SEC9	Les messages de gestion réseau entre la tête de système câble et le service portail seront authentifiés et facultativement cryptés pour les protéger contre toute surveillance et commandes non autorisées.

Le présent paragraphe limite sa portée à ces exigences primaires de sécurité du système, mais tient compte de ce que dans certains cas, il peut être souhaitable d'ajouter à la sécurité. Les problèmes d'opérateurs ou fabricants individuels peuvent avoir pour résultat des protections de sécurité accrues. La présente Recommandation n'interdit pas l'utilisation de protections supplémentaires, dans la mesure où elles n'entrent pas en conflit avec les intentions et les lignes directrices de la présente Recommandation.

11.2.2 Description du système

Le paragraphe suivant donne un aperçu général de tous les éléments qui font partie de l'architecture de sécurité.

L'architecture de sécurité inclut les éléments de sécurité suivants:

- domaine de sécurité;
- fonction de service portail (PS) IP;
- fonction de portail de sécurité de câble (CSP);
- pare-feu (FW);
- serveur de sécurité.

Le domaine de sécurité définit les frontières de la sphère d'influence directe dans laquelle la fonction de sécurité est étendue au service portail à partir de la tête de système du réseau câblé. Les éléments de service portail, de portail CSP et de pare-feu sont pleinement à l'intérieur du domaine de sécurité. L'élément de service portail contient des fonctions d'adressage réseau, de portail de gestion et de sécurité. Le portail CSP agit comme l'élément frontière entre le domaine de sécurité et le domaine non sécurisé. Le domaine de sécurité existe afin de fournir des services de sécurité aux appareils conformes.

Ces éléments contiennent des fonctionnalités spécifiques du client, du serveur ou du portail et peuvent exister dans différents types d'appareils physiques. L'architecture définit la classe d'appareil HA. Un exemple des relations entre les différents éléments de sécurité et les classes d'appareils HA est présenté à la Figure 23. Dans cette figure, les applications domestiques sont représentées sous le nom de APP et le serveur OSS est le serveur du système NMS.

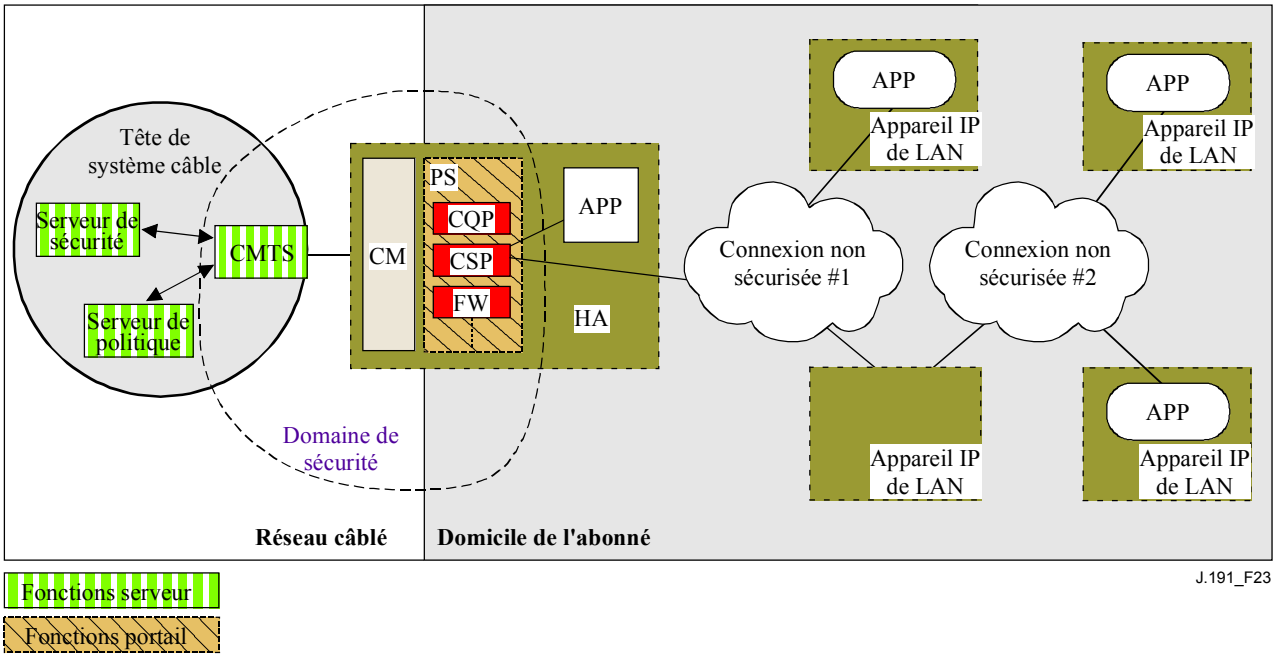

Figure 23/J.191 – Eléments de sécurité

11.2.2.1 Domaine de sécurité

Le domaine de sécurité est défini dans la Figure 23 et englobe l'élément de service portail dans le HA et les serveurs de tête de système illustrés.

11.2.2.2 Fonction de service portail

Le service portail (PS) est un élément logique qui contient des fonctions d'adressage réseau, de gestion et de portail de sécurité. Il ne réside que dans les appareils HA. Le service portail PS inclut les éléments suivants:

- portail de sécurité de câble (CSP);
- pare-feu (FW).

Le portail CSP agit comme un portail de sécurité pour les autres éléments de service portail. Une de ses fonctions primaires est de transmettre la messagerie de sécurité entre les serveurs OSS de tête de système (y compris le serveur de sécurité) et les applications IPCablecom. Les portails CSP fournit aussi des services de sécurité, tels que l'authentification et la gestion de clés, pour l'élément de service portail.

Le service portail inclut aussi une fonction de pare-feu. Le pare-feu assure la protection de l'utilisateur, aussi bien que du réseau HFC, contre le trafic indésirable provenant des domaines WAN ou LAN. Un tel trafic peut inclure des attaques délibérées sur le réseau domestique aussi bien que de la limitation de trafic pour des applications de contrôle parental.

La spécification de la sécurité ne définira pas en détail la spécification de l'implémentation d'un pare-feu, mais définira à la place un ensemble d'exigences pour permettre la gestion à distance par l'opérateur.

Typiquement, les pare-feu sont construits à l'aide d'une combinaison de deux composants différents: un filtrage de paquets et un serveur mandataire. Un module de filtrage de paquets est probablement le composant de pare-feu le plus commun parce qu'il détermine quels flux de paquets sont bloqués et lesquels sont autorisés à franchir le pare-feu. Chaque décision individuelle d'abandonner un paquet est fondée sur des informations de configuration statique qui commandent l'inspection des champs d'en-tête de paquet incluant: les adresses IP de source et de destination, les numéros de port de protocole de source et de destination, le type de protocole, etc. Selon le niveau de sécurité désiré, il peut être nécessaire de configurer un grand nombre de filtres sur un pare-feu, ce qui peut être très difficile et requérir une bonne compréhension du type de services (protocoles) à filtrer.

Un mandataire spécifique d'application (ASP, *application-specific proxy*), autre composant typique de pare-feu, crée un point de terminaison et relais de protocole en implémentant les parties nécessaires de client et de serveur d'un protocole client-serveur spécifique. La sécurité bénéficie de l'utilisation des mandataires ASP. Pour l'un, il est possible d'ajouter des listes de contrôle d'accès aux protocoles, en exigeant des utilisateurs ou des systèmes qu'il produisent un certain niveau d'authentification avant de se voir accorder l'accès. De plus, étant spécifique du protocole, un mandataire ASP comprend le protocole et peut être configuré pour bloquer seulement des sous-parties du protocole. Par exemple, un mandataire ASP du protocole FTP peut être configuré pour bloquer le trafic en provenance d'utilisateurs non authentifiés, tandis que les utilisateurs authentifiés se verront attribuer un accès sélectif aux commandes "put" (*mettre*) et "get" (*obtenir*), selon, disons, vers quelle direction ces commandes sont dirigées.

La combinaison particulière de classeurs de paquets et de mandataires ASP sur un pare-feu donné constitue un compromis entre la performance et le niveau de sécurité qu'accorde le pare-feu. Etant typiquement un mécanisme de couche Réseau, les filtres de paquets tendent à donner de meilleures performances que les mandataires ASP qui sont des mécanismes de couche Application. Une solution de compromis qui devient très populaire consiste à utiliser un filtrage de paquet d'après l'état (SPF, *stateful packet filtering*) où les informations d'état accumulées à partir des paquets appartenant à la même connexion sont conservées et utilisées dans la prise de décision sur l'abandon de paquet.

En dernier ressort, dans un pare-feu les filtrages statiques ou SPF et les mandataires ASP sont les nœuds de contrôle qui servent à implémenter le niveau de sécurité désiré sur un site. Cependant, tandis que la politique de sécurité détermine les services autorisés et la façon dont ils sont utilisés à travers le pare-feu, la politique de sécurité n'explicite pas la configuration spécifique pour le pare-feu. C'est l'ensemble de règles dérivées de la politique de sécurité qui définit la collection de règles de contrôle d'accès (règles d'action des filtres et mandataires) qui détermine ensuite quels paquets le pare-feu transmet ou rejette. Déduire l'ensemble de règles des déclarations de la politique de sécurité est un vrai défi car ces dernières sont habituellement exprimées dans un langage humain très distingué.

Parce qu'un pare-feu n'a besoin que de l'ensemble de règles pour configurer ses composants de filtrage SPF et de mandataire ASP, la définition de la politique de sécurité et la déduction d'un ensemble de règles correspondant sont considérées comme en dehors du domaine d'application du pare-feu. Un ensemble de règles approprié doit être configuré dans un pare-feu via un téléchargement de fichier de configuration de pare-feu authentifié. Le format réel du fichier contenant l'ensemble de règles applicables à un pare-feu particulier et la façon dont ce fichier est utilisé dans le pare-feu pour configurer les composants de filtrage SPF et de mandataire ASP est spécifique de l'implémentation. La présente Recommandation ne vise que le mécanisme d'authentification utilisé pour télécharger l'ensemble de règles d'un pare-feu sur un élément de service portail.

La Figure 24 illustre les relations entre les composants du pare-feu. En particulier, la figure suggère qu'un ensemble de règles (RS, *rule set*) doit être utilisé pour la configuration interne des composants du pare-feu. Ces composants sont les fonctions de filtre de paquet interne (IPF, *inbound packet filter*), de filtre de paquet externe (OPF, *outbound packet filter*), et de mandataire spécifique d'application (ASP) ou de filtre de paquet d'après l'état (SPF). La Figure 24 donne aussi une vision plus détaillée du service portail et de ses relations avec les fonctions de pare-feu et autres composants dans l'appareil HA. En particulier, la figure suggère que les fonctions de mandataire spécifique de l'application/filtrage de paquet d'après l'état (ASF/SPF) du pare-feu sont intimement associées dans la fonction de traduction d'adresse réseau (NAT) du portail CAP. Parce que la fonction de traduction NAT casse certaines applications, le traitement spécifique d'application est exigé en tant que partie de l'implémentation de la traduction NAT et donc, l'implémentation du service portail PEUT combiner les fonctions ASP/SPF et NAT.

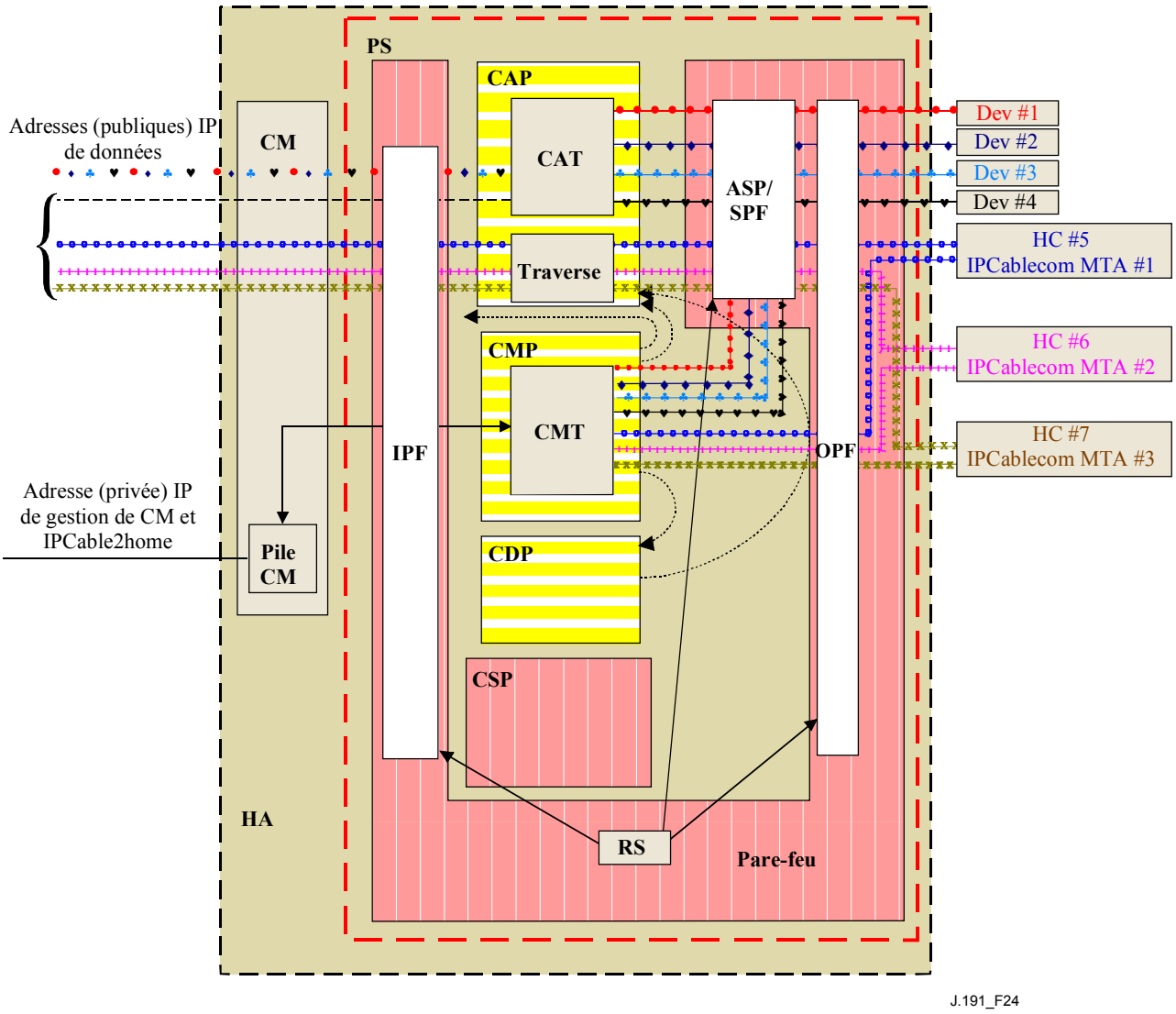

Figure 24/J.191 – Exemple d'élément de service portail dans un appareil HA

11.2.3 Serveur de centre de distribution de clé (KDC)

Le serveur de sécurité qui est accepté est le serveur centre de distribution de clé (KDC, *key distribution center*). Si un serveur KDC de soutien est disponible à la tête de système, il sera utilisé pour assurer les services d'authentification et de distribution de clés en utilisant le protocole Kerberos. S'il est disponible, le centre KDC communiquera avec la fonction de portail CSP pour établir ces services.

11.2.4 Autres éléments et fonctions concernés

Les éléments suivants ne sont pas considérés comme éléments de sécurité, mais utilisent ou prennent part à la gestion de ces services de sécurité.

- OSS;
- CMP.

L'OSS représente un ensemble de serveurs de tête de système qui permettent la gestion des éléments au domicile. Les serveurs OSS communiquent avec le portail CMP pour gérer les fonctions et services de sécurité. La liaison entre l'OSS et le portail CMP est sécurisée au moyen des services d'authentification et de confidentialité définis dans la présente Recommandation.

Le portail CMP est la fonction de gestion au sein du service portail. L'architecture de sécurité fournit l'authentification et d'autres services de sécurité pour ses communications avec les serveurs OSS à la tête de système. Le portail CMP permet la gestion des fonctions de service portail, y compris la gestion des services de sécurité.

On trouvera des détails complémentaires sur ces éléments et leurs fonctions aux paragraphes 12 et 13, et au paragraphe 10 sur la qualité de service.

11.3 Exigences

Pour toutes les références à la sécurité IPCablecom, on est prié de se reporter à la Rec. UIT-T J.170.

11.3.1 Authentification d'élément

Pour les besoins de la sécurité, il est important de savoir avec qui on est en communication avant d'échanger des informations significatives. L'authentification fournit un moyen d'identifier de façon sûre des parties qui ne se connaissent pas et veulent communiquer. Il y a trois parties dans l'identification: les pièces justificatives de l'identité, la vérification de la validité des pièces justificatives d'identité et les moyens communs de communiquer l'information d'identité. La présente Recommandation spécifie une pièce justificative d'identification standard pour l'industrie, l'utilisation de certificats X.509 en conjonction avec la norme [RFC 2459]. Le certificat d'élément de service portail fournit l'identité de l'élément de service portail associé en liant cryptographiquement l'adresse MAC de l'élément de service portail au certificat de clé publique produit pour cet élément de service portail. De plus, les certificats de clé publique fournissent un moyen sécurisé de communiquer les informations d'identité.

Lorsqu'un centre KDC qui accepte cette application est disponible dans la tête de système, l'authentification est acceptée. Si un centre KDC est disponible, il est recommandé que le câblo-opérateur fournisse l'élément de service portail en mode d'approvisionnement SNMP (comme décrit au § 5.1) pour tirer parti du protocole d'authentification mutuelle spécifié en se servant de Kerberos avec l'extension PKINIT. Kerberos donne un protocole pour une authentification mutuelle sécurisée afin de fournir du matériau de clé et n'établir les communications qu'entre les parties authentifiées. Parce que ce modèle d'authentification a déjà été spécifié par IPCablecom, la présente Recommandation se réfère en tant que de besoin au modèle IPCablecom.

11.3.1.1 Kerberos/PKINIT

Lorsque l'élément de service portail est approvisionné en mode d'approvisionnement SNMP, la présente Recommandation spécifie l'utilisation de Kerberos avec l'extension de clé publique PKINIT pour authentifier les éléments et pour soutenir les exigences de gestion de clé. Les éléments (les clients) s'authentifient eux-même auprès de centre KDC avec le protocole PKINIT. Une fois authentifiés auprès du centre KDC, les clients peuvent recevoir un ticket Kerberos pour s'identifier eux-mêmes auprès d'un serveur particulier.

L'authentification activée par le centre KDC DOIT suivre la spécification pour Kerberos/PKINIT comme défini dans la Rec. UIT-T J.170. Le centre KDC est équivalent à, ou le même que le centre KDC d'opérateur IPCablecom (IPCablecom spécifie l'utilisation de plusieurs centres KDC). L'élément de service portail DOIT agir comme le client envers le centre KDC. Dans la Recommandation sur la sécurité IPCablecom l'adaptateur MTA est le client. On suppose que les implémentations vont utiliser la fonctionnalité client spécifiée pour l'adaptateur MTA pour l'élément de service portail. L'élément de service portail utilise Kerberos pour le protocole SNMP. Les certificats utilisés dans PKINIT sont spécifiés au § 11.3.2. Lorsque IPCablecom spécifie un certificat d'appareil pour un adaptateur MTA, la présente Recommandation fournit un certificat pour l'élément de service portail (certificat d'élément de service portail), et les implémentations des éléments de service portail DOIVENT inclure le certificat d'élément de service portail.

La sécurité IPCablecom pour les fonctionnalités Kerberos suivantes ne s'applique pas à la présente Recommandation:

1) suivi des versions de service de clé (voir § 6.4.10/J.170);
2) fonctionnement Kerberos de secteurs croisés (voir § 6.4.11/J.170);
3) message de répétition de clé (voir § 6.5.4/J.170);
4) IPsec kerbérisé (voir § 6.5.6/J.170);
5) localisation des serveurs et conventions de nommage Kerberos (voir § 6.4.6.3, CMS).

11.3.1.2 Variables d'authentification spécifiques

Le modèle IPCablecom spécifies certains noms de variables spécifiques pour Kerberos dans l'architecture de réseau IPCablecom. Afin que la présente Recommandation utilise le modèle IPCablecom, les noms de variables suivants doivent être changés:

- remplacer pktcKdcToMtaMaxClockSkew comme défini dans la spécification IPCablecom de sécurité par KdcToClientMaxClockSkew;
- remplacer pktcSrvrToMtaMaxClockSkew comme défini dans la spécification IPCablecom de sécurité par SrvrToClientMaxClockSkew;
- remplacer MTAProvSrvr comme défini dans la spécification IPCablecom de sécurité par ProvSrvr;
- remplacer MTA-FQDN-Map comme défini dans la spécification IPCablecom de sécurité par FQDN-Map.

Les implémentations Kerberos DOIVENT ignorer la portion de champ Identificateur d'objet (OID), qui se lit clabProjPacketCable (2) dans AppSpecificTypedData au sein des messages KRB-ERROR.

11.3.2 Infrastructure de clé publique (PKI)

La présente Recommandation utilise les certificats de clé publique, qui sont conformes à la Rec. UIT-T X.509 et à la norme [RFC 3280] de l'IETF.

11.3.2.1 Structure générique

11.3.2.1.1 Version

La version des certificats DOIT être X.509 v3, qui est noté comme v2 dans le certificat présent (parce que v1 n'a pas eu de numéro de version associé). Tous les certificats DOIVENT être conformes à la norme [RFC 3280] excepté lorsque la non-conformité avec la norme RFC est explicitement déclarée dans le présent paragraphe. Toute demande de non-conformité de la part de la présente Recommandation quant au contenu n'implique pas non-conformité quant au format. Toute demande spécifique de non-conformité quant au format sera décrite explicitement.

11.3.2.1.2 Type de clé publique

Les clés publiques RSA sont utilisées dans toute la hiérarchie des certificats décrite au § 11.3.2.2. L'identificateur d'objet subjectPublicKeyInfo.algorithm utilisé DOIT être 1.2.840.113549.1.1.1 (rsaEncryption).

L'exposant public pour toutes les clés RSA DOIT être F4 – 65537.

11.3.2.1.3 Extensions

Les extensions (subjectKeyIdentifier, authorityKeyIdentifier, KeyUsage, BasicContraints, Signature Algorithm, SubjectName et IssuerName) DOIVENT suivre la norme [RFC 3280]. Toute autre extension de certificat PEUT aussi être incluse comme non critique. Les marques de codage sont [c:critique, n:non critique; m:obligatoire, o:facultatif] et elles sont identifiées dans le tableau pour chaque certificat.

11.3.2.1.3.1 subjectKeyIdentifier

L'extension subjectKeyIdentifier incluse dans tous les certificats comme l'exige la norme [RFC 3280] (par exemple, tous les certificats excepté les certificats d'appareil et auxiliaires) DOIT inclure la valeur keyIdentifier composée du hachage SHA-1 de 160 bits de la valeur de la CHAINE BINAIRE subjectPublicKey (excluant la marque, la longueur et le nombre de bits inutilisés du codage ASN.1) (voir la norme [RFC 3280]).

11.3.2.1.3.2 authorityKeyIdentifier

L'extension authorityKeyIdentifier incluse dans tous les certificats comme l'exige la norme [RFC 3280] DOIT inclure l'identificateur subjectKeyIdentifier tiré du certificat de celui qui le produit (voir la norme [RFC 3280]).

11.3.2.1.3.3 KeyUsage

L'extension keyUsage DOIT être utilisée pour tous les certificats d'autorité de certification (CA, *certification authority*) et les certificats de vérification de code (CVC). Pour les certificats d'autorité CA, l'extension keyUsage DOIT être marquée comme critique avec une valeur de keyCertSign et cRLSign. Pour les certificats de code CVC, l'extension keyUsage DOIT être marquée comme critique avec une valeur de digitalSignature et keyEncipherment. Les certificats d'entité de terminaison peuvent utiliser l'extension keyUsage comme indiqué dans la norme [RFC 3280].

11.3.2.1.3.4 BasicConstraints

L'extension basicConstraints DOIT être utilisée pour tous les certificats d'autorité CA et de code CVC et DOIT être marquée comme critique. Les valeurs propres à chaque certificat pour basicConstraints DOIVENT être marquées comme spécifié dans les Tableaux 31 à 42 de description de certificat.

11.3.2.1.4 Algorithme de signature

Le mécanisme de signature utilisé DOIT être SHA-1 avec codage RSA. L'identificateur OID spécifique est 1.2.840.113549.1.1.5.

11.3.2.1.5 SubjectName et IssuerName

Si une chaîne ne peut pas être codée comme une chaîne PrintableString, elle DOIT être codée comme une chaîne UTF8String (marque [UNIVERSAL 12]).

Lors du codage d'un nom X.500:

- chaque RelativeDistinguishedName (RDN, *nom distinctif relatif*) DOIT contenir un élément seulement dans l'ensemble des attributs X.500;
- l'ordre des noms RDN dans un nom X.500 DOIT être le même que l'ordre dans lequel ils sont présentés dans la présente Recommandation.

11.3.2.2 Hiérarchies des certificats

Trois hiérarchies de certificats distinctes sont utilisées. La chaîne de fabricant sert à identifier les fabricants autorisés, la chaîne de code de vérification sert à identifier les copies de logiciel conformes; la chaîne de fournisseur de service sert à identifier les appareils sur le réseau du fournisseur de service pour l'authentification mutuelle sur les appareils de l'abonné.

Les hiérarchies de certificat sont de nature générique et applicables à toutes les applications qui ont besoin de certificats. Ceci signifie que l'infrastructure de base peut être réutilisée pour chaque application (DOCSIS, IPCablecom, PS). Il peut y avoir des différences dans les certificats d'entité terminale exigés pour chaque projet, mais dans les cas où les certificats d'entité terminale se recouvrent, un certificat d'entité terminale pourrait être utilisé pour accepter le recouvrement. Par exemple, IPCablecom exige un centre KDC pour le fournisseur de service et la présente

Recommandation tire parti d'un centre KDC acceptant IPCablecom pour fournir l'authentification mutuelle. Si le fournisseur de service fait tourner les deux architectures de réseau sur ses systèmes, il peut utiliser le même centre KDC et le même certificat de centre KDC pour les communications sur les deux systèmes, c'est-à-dire, IPCablecom et cette application. Dans ce cas, le centre KDC de cette application est équivalent au centre KDC de l'opérateur IPCablecom ou le même que lui (IPCablecom spécifie l'utilisation de plusieurs centres KDC).

Dans la Figure 25, le terme "autorité de certification" est abrégé en CA et "certificat de vérification de code" est abrégé en CVC.

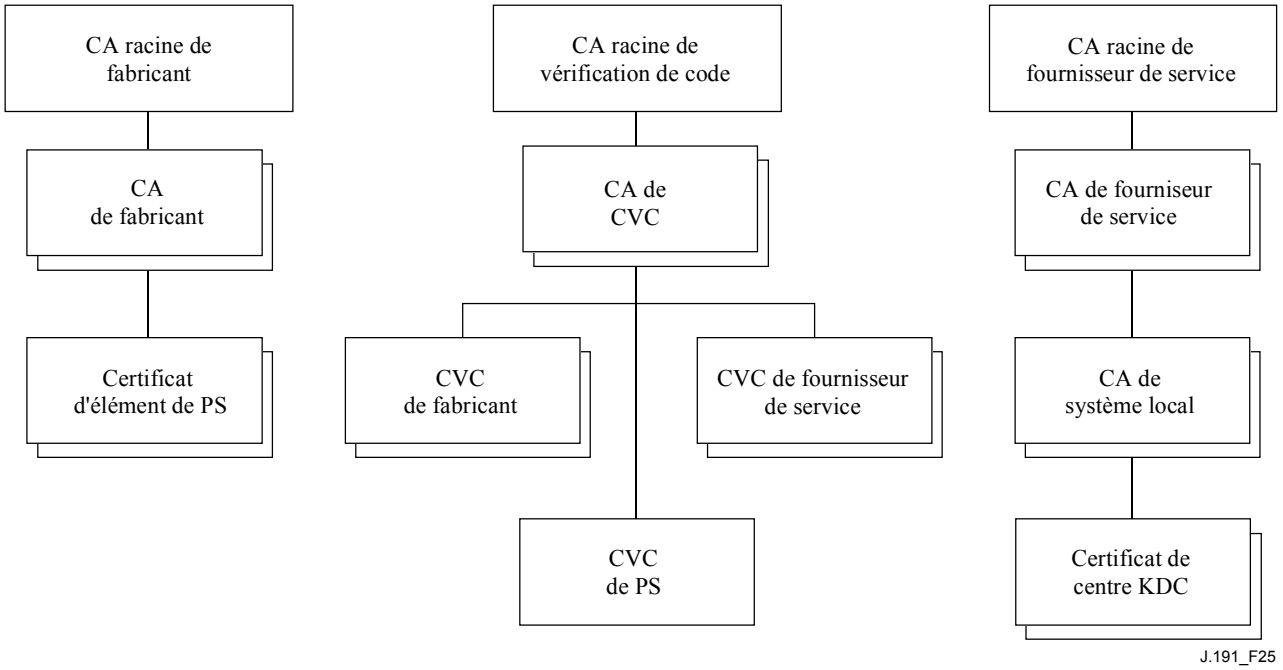

Figure 25/J.191 – Hiérarchie des certificats

11.3.2.2.1 Hiérarchie des certificats de fabricant

La hiérarchie de certificats de fabricant ou chaîne des fabricants est construite comme une autorité racine de fabricant, qui est utilisée pour produire des certificats d'autorité de certification (CA) de fabricant pour un ensemble de fabricants autorisés. Les fabricants utilisent leur autorité CA pour produire des certificats individuels d'éléments de service portail. Cette chaîne sert à l'authentification des appareils d'abonné.

Les informations contenues dans les tableaux ci-après sont les valeurs spécifiques pour les champs exigés conformément à la norme [RFC 3280]. Ces valeurs spécifiques de la hiérarchie de certificat de fabricant DOIVENT être suivies conformément aux Tableaux 31 à 33. Si un champ exigé n'est pas spécifiquement inscrit dans les tableaux, les lignes directrices de la norme [RFC 3280] DOIVENT alors être suivies. Les extensions génériques DOIVENT aussi être incluses comme spécifié au § 11.3.2 (PKI).

11.3.2.2.1.1 Certificat CA racine de fabricant

Le certificat CA racine de fabricant (voir Tableau 31) DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat CA racine de fabricant, le certificat CA de fabricant et le certificat d'élément de service portail.

Tableau 31/J.191 – Certificat CA racine de fabricant

Forme du nom du sujet	C = <pays>, O =, CN = autorité CA racine de fabricant
Usage de destination	Ce certificat sert à produire les certificats CA de fabricant.
Signé par	Autosigné
Période de validité	20 ans et plus. Il est souhaité que la période de validité soit assez longue pour que ce certificat n'ait pas à être renouvelé.
Module de longueur	2048
Extensions	keyusage [c, m] (keyCertSign, cRL Sign), subjectkeyidentifier, basicConstraints [c, m](cA = true)

11.3.2.2.1.2 Certificat CA de fabricant

Le certificat CA de fabricant (voir Tableau 32) DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat CA racine de fabricant, le certificat CA de fabricant et le certificat d'élément de service portail.

Tableau 32/J.191 – Certificat CA de fabricant

Forme du nom de sujet	C = <pays>, O = <Nom de la compagnie>, [S = <état/région>,] [L = <ville>,] OU =, [OU = <Usine du fabricant>,] CN = <Nom de la compagnie> Mfg CA
Usage de destination	Ce certificat est produit pour chaque fabricant par l'autorité CA racine de fabricant et peut être fourni à chaque élément de service portail soit au moment de la fabrication, soit pendant une mise à jour de code de champ. Ce certificat apparaît comme un paramètre en lecture seule dans la base MIB d'élément de service portail. Ce certificat produit des certificats d'élément de service portail. Ce certificat, avec le certificat CA racine de fabricant et le certificat d'élément de service portail, sert à authentifier l'identité de l'élément de service portail.
Signé par	L'autorité CA racine de fabricant
Période de validité	20 ans
Longueur du module	2048
Extensions	keyUsage[c, m](keyCertSign, cRLSign), subjectKeyIdentifier, authorityKeyIdentifier basicConstraints[c, m](cA = true, pathLenConstraint = 0)

Le pays/région, ville et usine du fabricant sont des attributs facultatifs. Un fabricant PEUT avoir plus d'un certificat CA de fabricant. Si un fabricant utilise plus d'un certificat CA de fabricant, l'élément de service portail DOIT avoir accès au certificat approprié comme il sera vérifié en faisant correspondre le nom du producteur dans le certificat d'élément de service portail au nom de sujet

dans le certificat CA de fabricant. S'il est présent, le authorityKeyIdentifier du certificat d'élément de service portail DOIT être mis en correspondance avec le subjectKeyIdentifier du certificat de fabricant, comme décrit dans la norme [RFC 3280].

11.3.2.2.1.3 Certificat d'élément de service portail

Le certificat d'élément de service portail DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat CA racine de fabricant, le certificat CA de fabricant et le certificat d'élément de service portail.

Le pays/région, ville et usine du fabricant sont des attributs facultatifs.

L'adresse MAC de l'élément de service portail DOIT être exprimée par six paires de chiffres hexadécimaux séparés par deux points, par exemple, "00:60:21:A5:0A:23". Les caractères hexadécimaux (A-F) DOIVENT être exprimés en lettres majuscules.

Un certificat d'élément de service portail est installé de façon permanente, non renouvelable et non remplaçable. Donc, le certificat d'élément de service portail DOIT avoir une période de validité plus grande que la durée de vie de fonctionnement de l'appareil spécifique (voir Tableau 33).

Tableau 33/J.191 – Certificat d'appareil

Forme du nom de sujet	C = <pays>, O = <Nom de la compagnie>, [S = <état/région>,] [L = <ville>], OU = [OU = <Nom de produit>,] [OU = <Usine du fabricant>,] CN = <Adresse MAC>
Usage de destination	Ce certificat est produit par l'autorité CA de fabricant et installé en usine. Le serveur de système NMS ne peut pas mettre à jour ce certificat. Ce certificat apparaît comme un paramètre en lecture seule dans la base MIB d'élément de service portail. Ce certificat sert à authentifier l'identité de l'élément de service portail.
Signé par	Autorité CA de fabricant
Période de validité	20 ans
Longueur du module	2048
Extensions	keyUsage[n, o](digitalSignature, keyEncipherment), authorityKeyIdentifier, L'extension keyUsage est facultative. Lorsque l'extension keyUsage est utilisée elle DEVRAIT être marquée comme non critique.

11.3.2.2.2 Hiérarchie de certificat de vérification de code

La hiérarchie de certificat de vérification de code (CVC), ou chaîne de vérification de code prend sa racine dans une autorité CA racine de vérification de code, qui produit le certificat CA de vérification de code. L'autorité CA de vérification de code sert à produire des certificats CVC pour un ensemble de fabricants et fournisseurs de service autorisés. L'autorité CA de vérification de code produit aussi les certificats CVC. Cette chaîne sert spécifiquement à authentifier les téléchargements de logiciels. L'infrastructure PKI permet les certificats CVC de fabricant, un certificat CVC et les certificats CVC de fournisseur de service.

Les informations contenues dans les tableaux ci-après sont les valeurs spécifiques pour les champs exigés, conformément à la norme [RFC 3280]. Ces valeurs spécifiques pour la hiérarchie de certificat de vérification de code DOIVENT être suivies conformément aux Tableaux 34 à 38. Si un champ exigé ne figure pas spécifiquement dans la liste des tableaux, on DOIT alors suivre les lignes directrices de la norme [RFC 3280]. Les extensions génériques DOIVENT être aussi incluses comme spécifié au § 11.3.2 (PKI).

11.3.2.2.2.1 Certificat CA racine de vérification de code

Ce certificat (voir Tableau 34) DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat CA de vérification de code, l'autorité CA de vérification de code et les certificats de vérification de code.

Tableau 34/J.191 – Certificat CA racine de vérification de code

Forme du nom de sujet	C = <pays>, O =, CN = Autorité CA racine de certificat CVC
Usage de destination	Ce certificat sert à signer les certificats CA de vérification de code.
Signé par	Autosigné
Période de validité	20 ans et plus. Il est supposé que la période de validité sera assez longue pour que ce certificat ne soit jamais renouvelé.
Longueur du module	2048
Extensions	keyUsage [c, m] (keyCertSign, cRL Sign), subjectkeyidentifier, basicConstraints [c, m](cA = true, pathLenConstraint = 0)

11.3.2.2.2.2 Certificat CA de vérification de code

Le certificat CA de vérification de code (voir Tableau 35) DOIT être vérifié en tant que partie d'une chaîne de certificats contenant le certificat CA racine de vérification de code, le certificat CA de vérification de code et le certificat de vérification de code. Il PEUT y avoir plus d'une autorité CA de vérification de code.

Tableau 35/J.191 – Certificat CA de vérification de code

Forme du nom de sujet	C = <pays>, O =, CN = Autorité CA de certificat CVC
Usage de destination	Ce certificat est produit par l'autorité CA racine de vérification de code. Ce certificat produit les certificats de vérification de code.
Signé par	Autorité CA racine de vérification de code.
Période de validité	20 ans
Longueur du module	2048
Extensions	keyUsage [c, m] (keyCertSign, cRL Sign), subjectKeyIdentifier, authorityKeyIdentifier, basicConstraints [c, m](cA = true, pathLenConstraint = 0)

11.3.2.2.2.3 Certificat de vérification de code fabricant

Ce certificat (voir Tableau 36) DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat CA racine de vérification de code, le certificat CA de vérification de code, et les certificats de vérification de code.

Tableau 36/J.191 – Certificat de vérification de code fabricant

Forme du nom de sujet	C = <pays>, O = <Nom de la compagnie>, [S = <état/région>], [L = <ville>], CN = <Nom de la compagnie> Mfg CVC
Usage de destination	L'autorité CA de vérification de code produit ce certificat pour chaque fabricant autorisé. Il sert à la politique établie par le câblo-opérateur pour le téléchargement de logiciel sécurisé.
Signé par	Autorité CA de vérification de code
Période de validité	2 ans
Longueur du module	2048
Extensions	keyUsage[c, m](digitalSignature, keyEncipherment), authorityKeyIdentifier

11.3.2.2.2.4 Certificat de vérification de code

Le certificat de vérification de code (voir Tableau 37) DOIT être vérifié en tant que partie d'une chaîne de certificats contenant le certificat CA racine de vérification de code, le certificat CA de vérification de code et le certificat de vérification de code.

Tableau 37/J.191 – Certificat de vérification de code

Forme du nom de sujet	C = <pays>, O =, CN = certificat CVC
Usage de destination	L'autorité CA de vérification de code produit ce certificat. Il sert à authentifier le code certifié. Il est utilisé dans la politique établie par le câblo-opérateur pour le téléchargement de logiciel sécurisé.
Signé par	Autorité CA de vérification de code
Période de validité	2 ans
Longueur du module	2048
Extensions	keyUsage[c, m](digitalSignature, keyEncipherment), authorityKeyIdentifier

11.3.2.2.2.5 Certificat de vérification de code de fournisseur de service

Le certificat de vérification de code de fournisseur de service (voir Tableau 38) DOIT être vérifié en tant que partie d'une chaîne de certificats contenant le certificat CA racine de vérification de code, le certificat CA de vérification de code et le certificat de vérification de code de fournisseur de service.

Tableau 38/J.191 – Certificat de vérification de code de fournisseur de service

Forme du nom de sujet	C = <pays>, O = <Nom de la compagnie>, [S = <état/région>,][L=<ville>,] CN = <Nom de la compagnie> Certificat CVC de fournisseur de service
Usage de destination	L'autorité CA de vérification de code produit ce certificat pour chaque fournisseur de service autorisé. Il sert à la politique établie par le câblo-opérateur pour le téléchargement de logiciel sécurisé.
Signé par	Autorité CA racine de vérification de code
Période de validité	2 ans
Longueur du module	2048
Extensions	keyUsage[c, m](digitalSignature, keyEncipherment), authorityKeyIdentifier

11.3.2.2.3 Hiérarchie de certificat de fournisseur de service

La hiérarchie de certificat de fournisseur de service, ou chaîne de fournisseur de service prend sa racine dans l'autorité CA racine de fournisseur de service, qui est utilisée pour produire des certificats pour un ensemble de fournisseurs de service autorisés. L'autorité CA de fournisseur de service peut être utilisée pour produire des certificats facultatifs de système local ou des certificats auxiliaires. Si l'autorité CA de fournisseur de service ne produit pas les certificats auxiliaires, cela sera alors fait par l'autorité CA de système local. Les certificats auxiliaires sont les certificats d'entité terminale sur le réseau du câblo-opérateur.

Les informations contenues dans les tableaux suivants sont les valeurs spécifiques pour les champs exigés, conformément à la norme [RFC 3280]. Ces valeurs spécifiques pour la hiérarchie de certificat de fournisseur de service DOIVENT être suivis conformément aux Tableaux 39 à 42. Si un champ exigé ne figure pas spécifiquement dans la liste des tableaux, les lignes directrices de la norme [RFC 3280] DOIVENT alors être suivies. Les extensions génériques DOIVENT aussi être incluses comme spécifié au § 11.3.2 (PKI).

11.3.2.2.3.1 Certificat CA racine de fournisseur de service

Ce certificat (voir Tableau 39) DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat CA racine de fournisseur de service, le certificat CA de fournisseur de service, le certificat facultatif de système local et les certificats auxiliaires.

Tableau 39/J.191 – Certificat CA racine de fournisseur de service

Forme du nom de sujet	C = <pays>, O =, CN = Autorité CA racine de fournisseur de service
Usage de destination	Ce certificat est utilisé pour produire les certificats CA de fournisseur de service.
Signé par	Autosigné
Période de validité	20 ans et plus. Il est supposé que la période de validité sera assez longue pour que ce certificat ne soit jamais renouvelé.
Longueur du module	2048
Extensions	keyUsage [c, m] (keyCertSign, cRL Sign), subjectkeyidentifier, basicConstraints [c, m](cA = true)

11.3.2.2.3.2 Certificat CA de fournisseur de service

Le certificat CA de fournisseur de service (voir Tableau 40) DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat CA racine de fournisseur de service, le certificat CA de fournisseur de service, le certificat facultatif de système local et les certificats auxiliaires.

Tableau 40/J.191 – Certificat CA de fournisseur de service

Forme du nom de sujet	C = <pays>, O = <Nom de la compagnie>, CN = <Nom de la compagnie> Autorité CA de fournisseur de service
Usage de destination	L'autorité CA racine de fournisseur de service produit ce certificat pour chaque fournisseur de service. Afin de faciliter la mise à jour de ce certificat, chaque élément de réseau est configuré avec l'attribut OrganizationName du SubjectName du certificat CA de fournisseur de service. C'est le seul attribut qui doit rester constant dans le certificat. Ce certificat apparaît comme un paramètre en lecture seule dans l'objet de base MIB qui identifie l'attribut OrganizationName pour le secteur Kerberos. L'élément n'accepte pas les certificats de fournisseur de service qui ne correspondent pas à cette valeur de l'attribut OrganizationName dans le SubjectName. Si la tête de système contient un centre KDC qui accepte cette application, l'élément de service portail doit alors effectuer le premier échange PKINIT avec le centre KDC juste après un réamorçage, et à ce moment les tableaux de la base MIB ne sont pas encore configurés. A ce moment, le client Kerberos DOIT accepter tout attribut OrganizationalName de fournisseur de service, mais il DOIT ultérieurement vérifier que la valeur ajoutée dans la base MIB pour ce secteur est le même que celle de la réponse PKINIT initiale. Cette autorité CA produit les certificats CA de système local ou les certificats auxiliaires.
Signé par	Autorité CA racine de fournisseur de service.
Période de validité	20 ans
Longueur du module	2048
Extensions	keyUsage[c, m](keyCertSign, cRLSign), subjectKeyIdentifier, authorityKeyIdentifier, basicConstraints[c, m](cA = true, pathLenConstraint = 1)

11.3.2.2.3.3 Certificat CA de système local

Ce certificat (voir Tableau 41) est facultatif pour le fournisseur de service. Si ce certificat existe il DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat CA racine de fournisseur de service, le certificat CA de fournisseur de service, le certificat facultatif de système local et les certificats auxiliaires.

Tableau 41/J.191 – Certificat CA de système local

Forme du nom de sujet	C = <pays>, O = <Nom de la compagnie>, CN = <Nom de la compagnie> Autorité CA de système local
Usage de destination	Ce certificat est facultatif, et s'il existe il est produit par l'autorité CA de fournisseur de service. Cette autorité CA produit des certificats auxiliaires. Les serveurs de réseau sont autorisés à se déplacer librement entre autorités CA régionales du même fournisseur de service.
Signé par	Autorité CA de fournisseur de service
Période de validité	20 ans
Longueur du module	2048
Extensions	keyUsage[c, m](keyCertSign, cRLSign), subjectKeyIdentifier, authorityKeyIdentifier, basicConstraints[c, m](cA = true, pathLenConstraint = 0)

11.3.2.2.3.4 Certificat de centre KDC

Ce certificat (voir Tableau 42) DOIT être vérifié en tant que partie de la chaîne de certificats contenant le certificat CA racine de fournisseur de service, le certificat CA de fournisseur de service, le certificat facultatif de système local et les certificats auxiliaires (par exemple, les certificats de centre KDC).

Le certificat de centre KDC DOIT inclure le subjectAltName PKINIT de Kerberos comme spécifié dans la spécification IPCablecom sur la sécurité, sous "certificat de centre de distribution de clés".

Tableau 42/J.191 – Certificat de centre KDC

Forme du nom de sujet	C = <pays>, O = <Nom de la compagnie>, [OU = <Nom de système local>,] OU = <KDC>, CN = <Adresse IP du serveur KDC>
Usage de destination	Ce certificat est produit soit par l'autorité CA de fournisseur de service soit par l'autorité CA de système local. Il sert à authentifier l'identité du centre KDC auprès des clients Kerberos pendant les échanges PKINIT. Ce certificat est passé à l'élément de service portail dans la réponse PKINIT.
Signé par	Autorité CA de fournisseur de service ou de système local
Période de validité	20 ans
Longueur du module	2048
Extensions	keyUsage[n, o](digitalSignature, keyEncipherment), authorityKeyIdentifier. The keyUsage extension is optional. When it is used it SHOULD be marked as non-critical. subjectAltName [n, m] (see IPCablecom Security specification).

11.3.2.3 Validation de certificat

La validation de certificat implique la validation d'une chaîne de certificats liés depuis les certificats d'entité terminale jusqu'à la racine valide. Par exemple, la signature sur le certificat d'élément de service portail est vérifiée avec le certificat CA de fabricant et ensuite la signature sur le certificat CA de fabricant est vérifiée avec le certificat CA racine de fabricant. Le certificat CA racine de

fabricant est auto-signé et ce certificat est reçu d'une source de confiance d'une façon sécurisée. La clé publique présente dans le certificat CA racine de fabricant sert à valider la signature sur le même certificat.

Les règles exactes pour la validation de la chaîne de certificat DOIVENT se conformer pleinement à la norme [RFC 3280], où elles sont désignées sous le nom de "Chemin de validation de certificat" En général, les certificats X.509 acceptent un ensemble de règles souples pour déterminer si le nom du producteur d'un certificat correspond au nom de sujet d'un autre. Les règles sont telles que deux champs de nom peuvent être déclarés correspondre même si une comparaison binaire des deux champs de nom n'indique pas la correspondance. La norme [RFC 3280] recommande que les autorités de certificat interdisent le codage des champs de nom de telle sorte qu'une implémentation puisse déclarer une correspondance ou une non correspondance en utilisant une simple comparaison binaire. Cette spécification de sécurité suit cette recommandation. En conséquence, le champ tbsCertificate.issuer codé en DER d'un certificat DOIT être une correspondance exacte du champ tbsCertificate.subject codé en DER du certificat de son producteur. Une implémentation PEUT comparer le nom du producteur avec son nom de sujet en effectuant une comparaison binaire des champs tbsCertificate.issuer et tbsCertificate.subject codés en DER.

La validation des périodes de validité pour l'emboîtement n'est pas vérifiée et n'est pas mise en œuvre intentionnellement, ce qui est conforme aux normes en vigueur. Au moment de leur production, la date de départ de validité pour tout certificat d'entité terminale DOIT être la même ou plus tardive que la date de départ de la période de validité du certificat de l'autorité CA qui le produit. Après le renouvellement d'un certificat d'autorité CA, les dates de départ des certificats des entités terminales PEUVENT être plus tôt que la date de départ du certificat d'autorité CA de production. La date de fin de validité pour les entités peut être avant, la même ou après la date de fin de validité pour l'autorité CA, comme spécifié dans les tableaux de certificats.

11.3.2.3.1 Validation pour la chaîne de fabricant et la vérification de racine

Le centre KDC DOIT valider la chaîne de certificats de fabricant liée. Habituellement, le premier certificat dans la chaîne n'est pas explicitement inclus dans la chaîne de certificats qui est envoyée sur le câble. Dans le cas où le certificat CA racine de fabricant est explicitement inclus dans la transmission, il DOIT déjà être connu du vérificateur avant le moment de cette vérification du certificat. Le certificat CA racine de fabricant transmis NE DOIT contenir aucun changement du certificat avec l'exception possible du numéro de série du certificat, de la période de validité et de la valeur de la signature. Si des changements, autres que le numéro de série du certificat, sa période de validité et la valeur de la signature, existent dans le certificat CA racine de fabricant transmis par rapport au certificat CA racine de fabricant connu, le centre KDC faisant la comparaison DOIT déclarer que la vérification du certificat est un échec.

11.3.2.3.2 Validation pour la chaîne de vérification de code et la vérification de racine

Un serveur de l'arrière peut vérifier la validité de la chaîne de vérification de code avant de commencer le processus de téléchargement de logiciel. Pour des précisions, voir le téléchargement de logiciel sécurisé au § 11.3.7.

11.3.2.3.3 Validation pour la chaîne de fournisseur de service et la vérification de racine

L'élément de service portail DOIT valider la chaîne de certificats de fournisseur de service liée. Habituellement, le premier certificat dans la chaîne n'est pas explicitement inclus dans la chaîne de certificats envoyée sur le câble. Dans les cas où le certificat CA racine de fournisseur de service est explicitement inclus dans la transmission, il DOIT être déjà connu du vérificateur avant le moment de la vérification de ce certificat. Le certificat CA racine de fournisseur de service NE DOIT contenir aucun changement dans le certificat avec l'exception possible du numéro de série du certificat, de la période de validité et de la valeur de la signature. Si des changements, autres que le numéro de série du certificat, sa période de validité et la valeur de la signature, existent dans le

certificat CA racine de fournisseur de service transmis par rapport au certificat CA racine de fournisseur de service connu, l'élément PS faisant la comparaison DOIT déclarer que la vérification du certificat est un échec.

11.3.2.4 Révocation de certificat

La révocation de certificat est en dehors du domaine d'application de la présente Recommandation.

11.3.3 Messagerie de gestion sécurisée

L'algorithme de sécurité utilisé pour initialiser la messagerie de gestion SNMP dépend du mode d'approvisionnement de l'élément de service portail (voir § 5.7). Il y a deux types de mode d'approvisionnement, le mode d'approvisionnement DHCP et le mode d'approvisionnement SNMP. Le mode d'approvisionnement DHCP a des sous-modes supplémentaires qui permettent de savoir s'il est configuré pour le mode NmAccess ou le mode coexistence. Le mode d'approvisionnement SNMP exige SNMPv3 pour la messagerie de gestion.

Les paragraphes suivants décrivent les algorithmes et exigences de sécurité nécessaires pour initialiser la messagerie de gestion SNMP fondée sur le mode d'approvisionnement de l'élément de service portail. L'élément de service portail DOIT accepter les algorithmes de sécurité SNMPv3 spécifiés aux § 11.3.3.1.2 et 11.3.3.2.

11.3.3.1 Algorithmes de sécurité pour SNMP en mode d'approvisionnement DHCP

En mode d'approvisionnement DHCP, l'élément de service portail peut être configuré pour le mode NmAccess ou le mode coexistence. En mode coexistence l'élément de service portail peut être configuré pour la messagerie de gestion SNMPv1, SNMPv2, et/ou SNMPv3.

11.3.3.1.1 Mode NmAccess

Si l'élément de service portail est fourni en mode d'approvisionnement DHCP avec le mode NmAccess, la gestion de réseau fondée sur SNMP au sein de l'élément de service portail n'utilise pas SNMPv3 et n'a donc pas besoin d'initialiser les fonctions de sécurité SNMPv3. L'initialisation de la liaison de gestion SNMPv1/v2 est définie au § 6.3.6.1.

11.3.3.1.2 Mode coexistence

Si l'élément de service portail est fourni en mode d'approvisionnement DHCP avec le mode coexistence et que le protocole de messagerie de gestion se révèle être SNMPv3 (voir § 6.3.6.1), l'élément de service portail DOIT alors utiliser la sécurité SNMPv3 spécifiée par la norme [RFC 2574]. L'authentification SNMPv3 DOIT toujours être activée et la confidentialité SNMPv3 PEUT aussi être utilisée.

Pour l'établissement des clés SNMPv3, le câblo-modem conforme au service portail DOIT accepter "l'initialisation SNMPv3" décrite ci-dessous.

NOTE – La conception du câblo-modem lui donne une attitude de sécurité "très sécurisée" dans le contexte de l'Appendice A de la norme RFC 2574 et de l'Appendice A de la norme RFC 2575. Ceci signifie que les entrées usmUser et vacmAccess par défaut définies dans l'Appendice A de la norme RFC 2574 et de l'Appendice A de la norme RFC 2575 NE DOIVENT PAS être présentes.

1) Pour chacun des différents noms de sécurité, pouvant aller jusqu'à cinq, le gestionnaire génère une paire de nombres:

   a) le gestionnaire génère un nombre aléatoire Rm;

   b) le gestionnaire utilise l'équation DH pour traduire Rm en un numéro public z:

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

      où g est tiré de l'ensemble des paramètres Diffie-Hellman, p est le premier de ces paramètres;

2) Le fichier de configuration du câblo-modem inclut dès sa création la paire (nom de sécurité, numéro public) et le câblo-modem DOIT accepter un minimum de 5 paires. Par exemple:

TLV type 34.1 (SnmpV3 Kickstart Security Name) = docsisManager

TLV type 34.2 (SnmpV3 Kickstart Public Number) = z

Durant le processus d'amorçage du câblo-modem, les valeurs ci-dessus (nom de sécurité, numéro public) vont (DOIVENT) être remplies dans le tableau usmDHKickstartTable.

A ce point:

```
usmDHKickstartMgrpublic.1 = "z"  (chaîne d'octets)
usmDHKickstartSecurityName.1 = "docsisManager"
```

Lorsque usmDHKickstartMgrpublic.n est établit avec une valeur valide pendant l'enregistrement, une rangée correspondante est créée dans le tableau usmUserTable avec les valeurs suivantes:

```
usmUserEngineID: localEngineID
usmUserName: usmDHKickstartSecurityName.n value
usmuserSecurityName: usmDHKickstartSecurityName.n value
usmUserCloneForm: ZeroDotZero
usmUserAuthProtocol: usmHMACMD5AuthProtocol
usmuserAuthKeyChange: déduit de la valeur établie
usmUserOwnAuthKeyChange: déduit de la valeur établie
usmUserPrivProtocol: usmDESPrivProtocol
usmUserPrivKeyChange: déduit de la valeur établie
usmUserOwnPrivKeyChange: déduit de la valeur établie
usmUserPublic: ""
usmUserStorageType: permanent
usmUserStatus: actif
```

NOTE – Pour les entrées (de CM) dhKickstart dans le tableau usmUserTable, "permanent" signifie qu'elles DOIVENT être écrites mais non supprimées et ne sont pas sauvegardées à travers les réamorçages.

Après que le câblo-modem s'est enregistré auprès du nœud d'accès:

– le câblo-modem génère un nombre aléatoire xa pour chaque rangée remplie du tableau usmDHKickstartTable qui a un usmDHKickstartSecurityName et un usmDHKickstartMgrPublic d'une longueur différente de zéro;

– le câblo-modem utilise l'équation DH pour traduire xa en un numéro public c (pour chaque rangée identifiée ci-dessus):

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

où g est tiré de l'ensemble des paramètres Diffie-Hellman, p est le premier de ces paramètres.

A ce point:

```
usmDHKickstartMyPublic.1 = "c" (chaîne d'octets)
usmDHKickstartMgrPublic.1 = "z" (chaîne d'octets)
usmDHKickstartSecurityName.1 = "docsisManager"
```

3) le câblo-modem calcule un secret partagé sk où sk = z ^ xa mod p;

4) le câblo-modem utilise sk pour déduire la clé de confidentialité et la clé d'authentification pour chaque rangée dans le tableau usmDHKickstartTable et établit les valeurs dans le tableau usmUserTable.

Comme spécifié dans la norme RFC 2786, la clé de confidentialité et la clé d'authentification pour le nom d'utilisateur associé, "docsisManager" dans ce cas, sont déduites de sk en appliquant la fonction de déduction de clé PBKDF2 définie dans PKCS#5v2.0.

```
privacy key <---        PBKDF2( salt = 0xd1310ba6,
            iterationCount = 500,
            keyLength = 16,
            prf = id-hmacWithSHA1)
authentication key <---- PBKDF2( salt = 0x98dfb5ac,
                  iterationCount = 500,
                  keyLength = 16 (usmHMACMD5AuthProtocol),
                  prf = id-hmacWithSHA1)
```

A ce point le câblo-modem a terminé son processus d'initialisation SNMPv3 et DOIT permettra un niveau d'accès approprié à un nom de sécurité valide avec la clé d'authentification et/ou clé de confidentialité correcte.

Le câblo-modem conforme DOIT remplir correctement les bons tableaux avec les bonnes clés comme spécifié par les normes RFC se rapportant à SNMPv3 et la norme RFC 2786;

5) ce qui suit décrit le processus qu'utilise le gestionnaire pour déduire la clé d'authentification et la clé de confidentialité unique du câblo-modem.

Le gestionnaire SNMP accède au contenu du tableau usmDHKickstartTable en utilisant le nom de sécurité de "dhKickstart" sans authentification.

Le câblo-modem conforme DOIT fournir des entrées préinstallées dans le tableau USM et les tableaux VACM pour créer correctement le "dhKickstart" d'utilisateur du niveau de sécurité noAuthnoPriv qui a l'accès en lecture seule au groupe système et au tableau usmDHkickstartTable.

Le gestionnaire SNMP obtient la valeur du numéro usmDHKickstartMypublic du câblo-modem associé au nom de sécurité que le gestionnaire veut pour déduire les clés d'authentification et de confidentialité. Le gestionnaire connaissant le numéro aléatoire privé, il peut calculer le secret partagé DH. A partir de ce secret partagé, le gestionnaire peut déduire les clés de fonctionnement d'authentification et de confidentialité pour le nom de sécurité que le gestionnaire va utiliser pour communiquer avec le câblo-modem.

Pour les besoins de l'initialisation SNMPv3 et les changements de clés, l'élément de service portail DOIT aussi être capable de recevoir des TLV des types 34, 34.1, et 34.2 comme défini au § B.C.1.2.8/J.112 dans la spécification d'interface radio-fréquence DOCSIS, et implémenter le mécanisme de changement de clé spécifié dans la norme [RFC 2786] qui inclut l'objet de base MIB usmDHKickstartTable.

11.3.3.2 Algorithmes de sécurité pour SNMPv3 en mode d'approvisionnement SNMP

Si l'élément de service portail est approvisionné en mode d'approvisionnement SNMP, la gestion de réseau fondée sur SNMP au sein de l'élément de service portail DOIT fonctionner sur SNMPv3 avec la sécurité spécifiée par la norme [RFC 2574]. L'authentification SNMPv3 DOIT être toujours activée et la confidentialité SNMPv3 PEUT aussi être utilisée. Pour établir les clés SNMPv3, toutes les interfaces SNMP DOIVENT utiliser la gestion de clé SNMPv3 kerbérisée comme spécifié au § 11.3.3.2.3.

11.3.3.2.1 Algorithmes de chiffrement SNMPv3

Les identifiants de transformation de codage, utilisés par la gestion de clé kerbérisée pour négocier un algorithme de codage que doit utiliser SNMPv3, sont les mêmes que ceux définis au § 6.3.1/J.170.

11.3.3.2.2 Algorithmes d'authentification SNMPv3

Les identifiants de transformation d'authentification que la gestion de clé kerbérisée doit utiliser pour négocier un algorithme d'authentification de message que va utiliser SNMPv3 sont les mêmes que ceux définis au § 6.3.2/J.170.

11.3.3.2.3 SNMPv3 kerbérisé

Le profil de gestion de clé kerbérisée spécifique pour SNMPv3 est le même profil que défini au § 6.5.7/J.170.

11.3.3.2.4 Identifiants de moteur SNMPv3

Parce que le gestionnaire et le client SNMP DOIVENT vérifier que l'identifiant de moteur SNMPv3 dans les messages de demande et de réponse AP sont fondés sur le nom principal Kerberos approprié dans le ticket [UIT-T J.170], ce qui suit définit la règle à utiliser en générant ces identifiants de moteur SNMPv3 à utiliser dans la présente application:

- l'identifiant de moteur SNMPv3 suit le format définit dans la norme [RFC 2571], c'est-à-dire, le premier bit est mis à 1 (un) et la valeur appropriée est utilisée pour les quatre premiers octets [RFC 2571];
- le cinquième octet porte la valeur 4 (quatre) pour indiquer que les octets suivants, jusqu'à 27, sont à considérer comme du texte. Ces octets jusqu'au 27^{e} sont définis comme suit:
  - les premiers caractères du nom principal Kerberos jusqu'au 25^{e} sont utilisés pour les octets d'identifiant de moteur commençant au sixième octet;
  - la séquence d'octets ci-dessus, indiquant le nom principal Kerberos, est suivie par un octet à considérer comme une valeur hexadécimale de 8 bits. Chaque valeur différente identifie un moteur SNMP particulier dans l'appareil (élément ou serveur de système NMS). La valeur 0 (zéro) NE DOIT PAS être utilisée;
  - la chaîne de texte qui débute au sixième octet se termine par un caractère Nul.

Noter que d'autres formats sont possibles en suivant l'approche de la norme [RFC 2571]. Le choix ci-dessus cependant, est destiné à réduire la complexité d'implémentation qui serait nécessaire si toutes les approches de la norme [RFC 2571] étaient permises.

11.3.3.2.5 Remplissage du tableau usmUserTable

Les paramètres msgSecurityParameters dans les messages SNMPv3 portent un champ msgUserName qui spécifie l'utilisateur au nom duquel le message est échangé et dont les informations de sécurité produisent les champs msgAuthenticationParameters et msgPrivacyParameters. Pour que le moteur SNMP d'un élément traite ces messages, les informations d'utilisateur nécessaires DOIVENT être entrées dans le tableau usmUserTable [RFC 2574] pour le moteur de l'élément. Le tableau usmUserTable DOIT être rempli dans l'élément de service portail juste après la réception du message Réponse AP avec les informations suivantes:

- usmUserEngineID: l'identifiant de moteur SNMP local comme défini au § 11.3.3.2.4;
- usmUserName: administrateur de service portail-XXXXXX;
- usmUserSecurityName: administrateur de service portail-XXXXXX;
- usmUserCloneFrom: 0.0;
- usmUserAuthProtocol: indique le protocole d'authentification choisi pour l'utilisateur, à partir du message Réponse AP;
- usmUserAuthKeyChange: valeur par défaut "";
- usmUserOwnAuthKeyChange: valeur par défaut "";
- usmUserPrivProtocol: indique le protocole de codage choisi pour l'utilisateur, à partir du message Réponse AP;
- usmUserPrivKeyChange: valeur par défaut "";
- usmUserOwnPrivKeyChange: valeur par défaut "";
- usmUserPublic: valeur par défaut "";

- usmUserStorageType: permanent;
- usmUserStatus: actif.

La valeur XXXXXX sera l'adresse MAC d'élément pour cet élément de service portail.

De nouveaux utilisateurs du protocole SNMPv3 PEUVENT être créés avec le clonage standard SNMPv3 comme défini dans la norme [RFC 2475]. Pour des informations supplémentaires, se référer au § 7.1.1.3.1/J.170.

11.3.4 CQoS sécurisée

La CQoS fournit la qualité de service aux applications IPCablecom qui ont besoin d'une adresse de traverse. Les messages DQoS IPCablecom entre l'adaptateur MTA et le système CMTS, le serveur CMS ou le câblo-modem sont sécurisés par la spécification de sécurité IPCablecom. Pour la sécurité, il est nécessaire de s'assurer que ces messages IPCablecom, déjà sécurisés par IPCablecom, peuvent passer à travers le pare-feu dans le service portail. Il n'est pas dans le domaine d'application de la présente Recommandation d'ajouter à la sécurité pour les messages IPCablecom. Parce que les exigences de sécurité CQoS de l'élément de service portail sont simplement de transmettre la messagerie de sécurité IPCablecom, il ne dépend pas du système NMS de traiter cette fonction. En conséquence, la fonction de sécurité CQoS reste la même à la fois pour le mode d'approvisionnement DHCP et le mode d'approvisionnement SNMP (voir § 5.7).

L'exigence de sécurisation de CQoS est de fournir une sécurité qui ne soit pas un fardeau insupportable pour le système. Le point clé de la sécurisation de la qualité de service est de s'assurer que le vol de service et les interruptions du réseau soient réduits à une perte insignifiante. Il est aussi important de comprendre que la CQoS est la passerelle de qualité de service vers le domicile et donc va vraisemblablement commander ou soutenir toutes les applications et dispositifs du domicile qui requièrent de la qualité de service sur le réseau câblé, de et vers le service portail. Donc, il est particulièrement critique de s'assurer que ce point d'entrée unique n'est pas le maillon faible dans le système de qualité de service.

11.3.4.1 Architecture CQoS

L'architecture de CQoS consiste en un élément fonctionnel de portail CQP qui facilite l'établissement des flux de qualité de service à travers le réseau HFC pour les applications IP. L'élément de portail CQP existe dans le service portail. Voir le paragraphe 10. L'élément de portail CQP agit comme un pont transparent pour la messagerie CQoS entre les applications conformes à IPCablecom et le système CMTS. Le pare-feu devra être capable de passer la messagerie de sécurité et de qualité de service conforme à IPCablecom.

Voir le paragraphe 10 pour des détails complémentaires sur la CQoS.

11.3.4.2 Architecture IPCablecom de DQoS sécurisée

Le présent paragraphe décrit l'architecture IPCablecom de DQoS sécurisée pour discuter comment des messages interagissent avec le pare-feu dans le service portail. Au sein de DQoS, l'adaptateur de terminal multimédia (MTA) communique avec le système CMTS et le serveur de gestion d'appel (CMS) pour établir la qualité de service nécessaire pour ses services IPCablecom. L'adaptateur MTA est incorporé dans le câblo-modem DOCSIS. Ci-dessous figurent un tableau (Tableau 43) et un diagramme (Figure 26) des appareils, le protocole de communication et le protocole de sécurité pour la DQoS.

Tableau 43/J.191 – Architecture DQoS sécurisée

E-MTA		
Liaison avec le MTA à domicile	**Protocole**	**Protocole de sécurité**
E-MTA/CM – CMS	NCS	IPsec
E-MTA/CM – CMTS	DOCSIS	BPI+

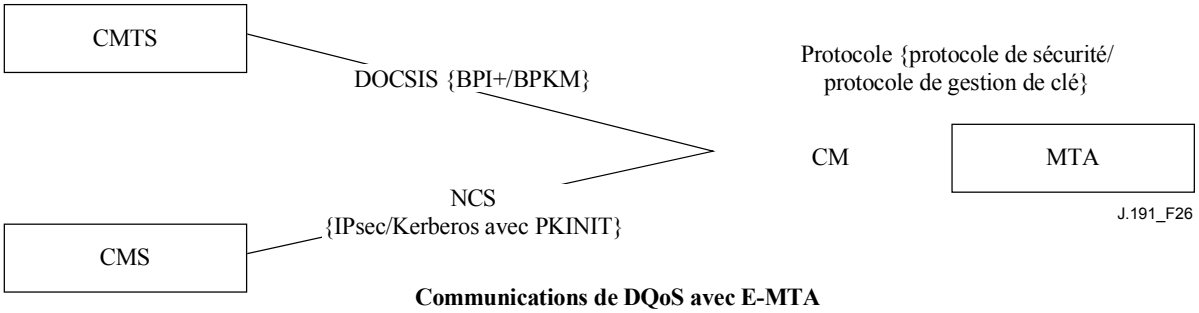

Figure 26/J.191 – Architecture DQoS sécurisée pour l'adaptateur MTA

11.3.4.3 Architecture CQoS de sécurité

La CQoS requiert la messagerie DQoS d'IPCablecom [UIT-T J.163]. Toute la messagerie CQoS DOIT être sécurisée comme décrit dans la spécification de sécurité IPCablecom. La Figure 27 indique les protocoles nécessaires pour accepter le E-MTA pour la DQoS. La seule différence entre l'architecture CQoS sécurisée et l'architecture DQoS d'IPCablecom est que le service portail est logiquement entre le câblo-modem et l'adaptateur MTA. Cependant, dans la mesure où le service portail agit comme un pont transparent, il n'y a pas de changement dans les protocoles ou les liaisons de communication.

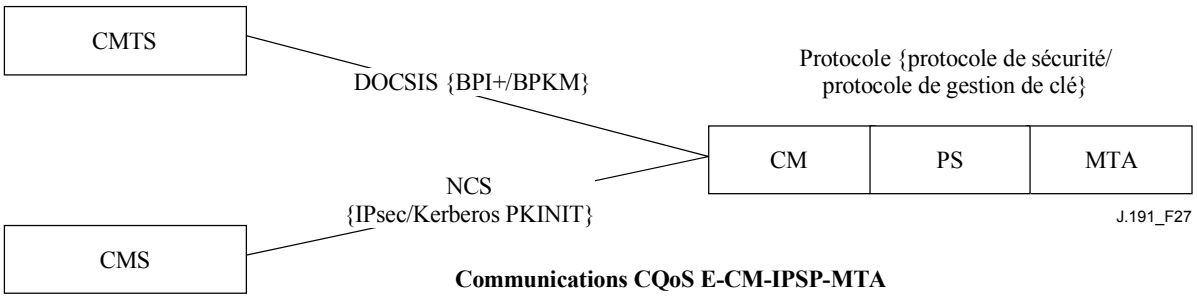

Figure 27/J.191 – Architecture CQoS sécurisée pour l'adaptateur MTA

11.3.4.4 Rôle du portail CSP en CQoS

Le portail de sécurité de câble (CSP) est le point unique de contrôle de la sécurité au sein de la fonction de service portail dans l'architecture; et donc le portail CSP fournit la sécurité dans l'architecture CQoS. Le portail CQP agit comme un pont transparent pour les messages de DQoS qu'il accepte, et donc le portail CSP ne fournit aucun service pour la CQoS.

11.3.5 Gestion du pare-feu

Tandis que les questions de sécurité ont longtemps été un problème majeur pour les réseaux, l'ubiquité croissante de la connectabilité permanente sur Internet au moyen du câblo-modem (CM) transporte les problèmes de sécurité jusqu'au domicile. Parce que l'abonné moyen manque de connaissances techniques, de la compréhension des questions de sécurité et du temps pour garder ses ordinateurs personnels dans le créneau supérieur du fonctionnement sécurisé, un pare-feu devient une première ligne de défense nécessaire pour protéger les ordinateurs non sécurisés du domicile.

Il y a de nombreuses définitions du pare-feu, parmi lesquelles:

– "un pare-feu est une approche de la sécurité; il aide à implémenter une plus grande politique de sécurité qui définit les services et les accès à permettre";

– "un pare-feu est un agent qui fait écran au trafic réseau d'une certaine façon, bloquant le trafic qu'il croit être inapproprié, dangereux, ou les deux".

Et donc, un pare-feu implémente une politique de sécurité en se servant de certains mécanismes pour bloquer du trafic que la politique de sécurité stipule être indésirable.

Les exigences de traitement du trafic par le pare-feu comportent:

• IPCablecom (voir Tableau 44) et les protocoles définis dans la présente Recommandation NE DOIVENT pas être arrêtés par le pare-feu. Par exemple, un pare-feu devrait avoir un mandataire spécifique d'application approprié ou un support de filtrage de paquets de plein droit pour ouvrir les ports UDP qui sont définis en application de la signalisation IPCablecom.

Tableau 44/J.191 – Recommandations IPCablecom pertinentes pour le pare-feu

Description	Recommandation
Spécification des codecs audio/vidéo	J.161
Spécification de la qualité de service dynamique	J.163
Spécification du protocole de signalisation d'appel fondé sur le réseau	J.162
Spécification de l'approvisionnement d'appareil MTA	J.167
Spécification de sécurité	J.170
Spécification du mécanisme d'événement de gestion	J.172
Spécification du protocole de serveur audio	J.175
Spécification de la signalisation du serveur de gestion d'appel	J.cmss

Les protocoles définis par IPCablecom comportent ce qui suit:

• approvisionnement SNMPv3, DHCP, DNS, TFTP, SYSLOG

• flux média RTP, RTCP

• qualité de service RSVP

• signalisation d'appel réseau MGCP, SDP

• sécurité Messagerie Kerberos, IPSec

Les protocoles définis par cette application comportent ce qui suit:

- approvisionnement SNMPv3, DHCP, DNS, TFTP, SYSLOG
- gestion ICMP
- sécurité Kerberos

Le pare-feu DEVRAIT protéger contre l'examen du port ou du réseau lancé de l'intérieur ou de l'extérieur du domicile. Il DEVRAIT aussi protéger contre la liste suivante d'attaques de déni de service: "Ping of Death", "Teardrop", "Bonk", "Nestea", "SYN Flood", "LAND Attack", "IP Spoofing", "Smurf Attack" and "WinNuke".

Le pare-feu DOIT être capable de permettre l'accès des mêmes protocoles d'application Internet populaires que ceux qui sont définis à l'Annexe D. Un simple filtre de traducteur NAT ou de paquet n'est pas suffisant pour notre objet. Pour fournir une solution souple et sécurisée, le pare-feu DOIT mettre en œuvre soit un pare-feu avec un mandataire spécifique d'application (ASP) soit avec un filtrage de paquet d'après l'état (SPF).

11.3.5.1 Téléchargement à distance de l'ensemble des règles de pare-feu

Les caractéristiques de l'élément de service portail qui permettent à l'opérateur de gérer à distance les fonctions de pare-feu seront activées. Le gros de cette gestion est accompli via le téléchargement d'un fichier de configuration. Le fichier de configuration du pare-feu contient l'ensemble de règles d'une politique de sécurité particulière. La gestion de pare-feu est achevée par l'accès aux objets de gestion de la base MIB de sécurité.

La politique de sécurité définit le niveau de sécurité/fonctionnalité désiré pour le pare-feu d'un abonné. Il peut en exister plus d'un parmi lesquels faire un choix. Les fichiers contenant l'ensemble de règles correspondant à ces politiques de sécurité sont conservés sur un serveur de fichiers d'un opérateur. Le service portail DOIT utiliser un client TFTP conforme à la norme [RFC 1350] pour télécharger le fichier de configuration de l'ensemble des règles de pare-feu. Pour authentifier le téléchargement de fichier d'ensemble de règles, l'algorithme d'authentification défini au § 7.3.3.3.2 DOIT être utilisé avec les paramètres correspondants de hachage et de gestion de nom de fichier défini au § 11.3.5.2.

En utilisant l'interface de gestion de la base MIB de sécurité, l'opérateur configure les paramètres de fichier d'ensemble de règles de politique de sécurité dont la liste figure au § 11.3.5.2 et suit ensuite la procédure définie au § 7.3.3.3.2 pour télécharger et authentifier le fichier. Si le téléchargement réussit, le fichier d'ensemble de règles de politique de sécurité DOIT être "activé" sur le pare-feu. Si l'authentification échoue, l'ensemble de règles de politique DOIT être détruit.

11.3.5.2 Paramètres de gestion de l'ensemble de règles du pare-feu

Les paramètres de gestion suivants DOIVENT être implémentés dans le service portail comme défini par la base MIB de sécurité pour soutenir le fichier d'ensemble de règles de pare-feu:

- **cabhSecFwPolicyFileURL** – Contient le nom du fichier de l'ensemble de règles de politique et l'adresse IP du serveur TFTP contenant le fichier de l'ensemble de règles de politique, en format d'URL TFTP. Une fois que l'objet cabhSecFwPolicyFileURL a été mis à jour, il DOIT déclencher le téléchargement du fichier. Le service portail DOIT utiliser un client TFTP conforme à la norme [RFC 1350] pour télécharger le fichier de configuration du pare-feu.
- **cabhSecFwPolicyFileHash** – Définit le résumé SHA-1 pour le fichier d'ensemble de règles correspondant.

- **cabhSecFwPolicyFileOperStatus** – InProgress(1) indique qu'un téléchargement de fichier d'ensemble de règles est en cours, soit par suite d'une non-concordance de version à l'approvisionnement soit par suite d'une demande de upgradeFromMgt. CompleteFromProvisioning(2) indique que la dernière amélioration de fichier d'ensemble de règles était le résultat d'une non-concordance de version à l'approvisionnement. CompleteFromMgt(3) indique que la dernière amélioration de fichier d'ensemble de règles était le résultat du réglage de l'objet FirewallPolicyFileAdminStatus à upgradeFromMgt. Failed(4) indique que la dernière tentative de téléchargement a échoué, habituellement à cause de l'expiration de la temporisation TFTP.
- **cabhSecFwPolicyFileCurrentVersion** – Version du fichier d'ensemble de règles fonctionnant actuellement dans l'élément de service portail. Cet objet devrait être dans la syntaxe utilisée par le vendeur individuel pour identifier les versions de fichier d'ensemble de règles. Tout élément de service portail DOIT retourner une chaîne décrivant le chargement du fichier d'ensemble de règles actuel. Si cela n'est pas applicable, cet objet DOIT contenir une chaîne vide.
- **cabhSecFwPolicyFileEnable** – Permet l'activation et la désactivation de la politique de sécurité du pare-feu.

11.3.5.3 Enregistrement d'événement au pare-feu

Le pare-feu DOIT être capable d'enregistrer les types d'événements suivants:

- TYPE 1: tentatives de clients aussi bien publics que privés de traverser le pare-feu en violation de la politique de sécurité.
- TYPE 2: tentatives identifiée d'attaques de déni de service.
- TYPE 3: changements faits à la politique de pare-feu active ou des paramètres de configuration du pare-feu.

Le choix des types d'événements de pare-feu qui sont réellement enregistrés est configuré à travers l'interface de base MIB de sécurité, comme décrit au § 11.3.5.2.

Les opérateurs peuvent surveiller les événements de pare-feu en utilisant le mécanisme de messagerie d'événement défini au § 6.5. L'accès aux paramètres de gestion d'enregistrement d'événement se fait via la base MIB de sécurité et est défini au § 6.5.

L'enregistrement de messages d'événement de pare-feu permet à un opérateur d'accéder au niveau d'activité des pirates à travers le réseau de l'opérateur et de surveiller les changements apportés à la politique de sécurité du pare-feu. Lorsque les types de message d'événement ont été activés via les paramètres de gestion de la base MIB de sécurité, ces événements de pare-feu DOIVENT être enregistrés avec une entrée de message d'événement utilisant le mécanisme d'enregistrement d'événement défini au § 6.5.

Une entrée de message d'événement de pare-feu contiendra les informations suivantes:

- priorité d'événement;
- date et heure – lorsque l'événement est survenu;
- protocole – indiqué par le champ En-tête IP (TCP, UDP, ICMP);
- adresse source IP;
- adresse de destination IP;
- port de destination (TCP et UDP) ou type de message (ICMP);
- règle de politique pertinente;
- description de l'événement (facultatif).

Le § 6.5.2.1 définit un champ Priorité d'événement qui décrit différents niveaux de priorité pour les événements enregistrés. Ce champ Priorité d'événement DOIT être mis à la priorité 6 pour les événements de pare-feu de type 1, 2, et 3. Si le champ n'est pas applicable, il doit être laissé blanc. L'élément de service portail DOIT formater les messages d'événement de pare-feu comme défini à l'Annexe B.

Pour aider à la surveillance des activités de piratage sur un pare-feu d'abonné, les objets de gestion d'alerte au piratage ont été définis dans la base MIB de sécurité. Ce dispositif alerte l'opérateur lorsque le nombre d'événements de pare-feu de type 1 et 2 excède un seuil d'alerte pour une période d'alerte donnée (en jours). Le seuil d'alerte et la période d'alerte sont configurables par l'opérateur. L'élément de service portail accumule le nombre d'événements de pare-feu de type 1 et 2 qui sont survenus pendant le nombre de jours écoulés défini par la période d'alerte. Si ce nombre excède le seuil d'alerte, un message d'alerte au piratage est enregistré pour informer l'opérateur.

11.3.5.4 Paramètres de gestion pour l'enregistrement d'événement

Les paramètres de gestion suivants DOIVENT être implémentés dans le service portail comme défini par la base MIB de sécurité pour surveiller/configurer l'enregistrement d'événement de pare-feu:

- **cabhSecFwEventType1Enable** – active ou désactive l'enregistrement de messages d'événement de pare-feu de type 1;
- **cabhSecFwEventType2Enable** – active ou désactive l'enregistrement de messages d'événement de pare-feu de type 2;
- **cabhSecFwEventType3Enable** – active ou désactive l'enregistrement de messages d'événement de pare-feu de type 3;
- **cabhSecFwEventAttackAlertThreshold** – si le nombre d'attaques pirates de type 1 ou 2 excède ce seuil dans la période définie par l'objet cabhSecFwEventAttackAlertPeriod, un message d'événement de pare-feu DOIT être enregistré avec le niveau de priorité 4;
- **cabhSecFwEventAttackAlertPeriod** – indique la période à utiliser en jours passés pour l'objet cabhSecFwEventAttackAlertThreshold.

11.3.6 Bases MIB

Le service portail DOIT accepter les bases MIB de soutien au téléchargement de logiciel suivantes définies dans la norme [RFC 2669]:

- **docsDevSwAdminStatus** – s'il est réglé à upgradeFromMgt(1), l'appareil initialisera un téléchargement de copie de logiciel TFTP en utilisant le nom docsDevSwFilename;
- **docsDevSwFilename** – le nom du fichier de la copie de logiciel à charger dans l'appareil;
- **docsDevSwCurrentVers** – la version de logiciel fonctionnant actuellement dans l'appareil;
- **docsDevSwServer** – l'adresse du serveur TFTP utilisé pour les améliorations de logiciel;
- **docsDevSwOperStatus** – état du téléchargement de logiciel.

Le service portail DOIT accepter les bases MIB de soutien au téléchargement de logiciel suivantes définies dans la Rec. UIT-T J.112, Annexe B.O:

- **docsBpi2CodeDownloadGroup** – collection d'objets qui servent au téléchargement de logiciels authentifiés. Le groupe docsBpi2CodeDownloadGroup inclut:
  - **docsBpi2CodeDownloadStatusCode** – indique le résultat de la dernière vérification de certificat CVC de fichier de configuration, de la vérification de certificat CVC SNMP, ou de vérification de fichier de code;
  - **docsBpi2CodeDownloadStatusString** – informations supplémentaires au code d'état;
  - **docsBpi2CodeMfgOrgName** – nom d'organisation du fabricant d'appareil;

- **docsBpi2CodeMfgCodeAccessStart** – valeur actuelle du codeAccessStart du fabricant de l'appareil se référant au temps moyen de Greenwich (GMT, *Greenwich mean time*).
- **docsBpi2CodeMfgCvcAccessStart** – valeur actuelle du cvcAccessStart du fabricant de l'appareil se référant au temps moyen de Greenwich (GMT);
  - **docsBpi2CodeCoSignerOrgName** – nom d'organisation du cosignataire;
- **docsBpi2CodeCoSignerCodeAccessStart** – valeur actuelle du codeAccessStart du cosignataire se référant au temps moyen de Greenwich (GMT);
- **docsBpi2CodeCoSignerCvcAccessStart** – valeur actuelle du cvcAccessStart du cosignataire se référant au temps moyen de Greenwich (GMT);
  - **docsBpi2CodeCvcUpdate** – déclenche la vérification par l'appareil du certificat CVC et la mise à jour de la valeur cvcAccessStart;
  - **docsBpi2CmPublicKey** – chaîne RSAPublicKey de type ASN.1 codée en DER, comme défini dans la norme de codage RSA [RSA1];
  - **docsBpi2CmDeviceCmCert** – certificat X.509 d'appareil, codé en DER;
  - **docsBpi2CmDeviceManufCert** – certificat CA X.509 de fabricant, codé en DER, qui signe le certificat d'appareil.

Le service portail DOIT accepter la base MIB de soutien au téléchargement de configuration suivant:

- **cabhPsDevProvConfigHash** – hachage SHA-1 du contenu entier du fichier de configuration, pris comme une chaîne d'octets.

11.3.7 Téléchargement de logiciel sécurisé

L'élément de service portail dans un appareil DOIT être capable de télécharger à distance une copie de logiciel sur le réseau. La nouvelle copie du logiciel permettra à l'opérateur d'améliorer les performances, de fournir de nouvelles fonctions et caractéristiques, de corriger des déficiences de conception, et de permettre un chemin de migration pour les appareils lors des évolutions de la présente Recommandation. La faculté de télécharger des logiciels DOIT permettre de changer les fonctionnalités de l'élément de service portail sans qu'il soit besoin que le personnel du système câblé visite physiquement et reconfigure chaque unité. Le processus de téléchargement de logiciel sécurisé vise les exigences primaires de système suivantes:

- le mécanisme utilisé pour télécharger des logiciels DOIT être le transfert de fichier TFTP;
- le téléchargement de logiciel DOIT être initialisé de l'une des deux façons suivantes:
  1) une demande d'ensemble SNMP produite par le système NMS au docsDevSwAdminStatus;
  2) via le fichier de configuration de l'élément de service portail.

  Si le nom de fichier d'amélioration de logiciel dans le fichier de configuration ne correspond pas à la copie actuelle du logiciel de l'appareil, l'élément de service portail DOIT demander le fichier spécifié via TFTP auprès du serveur de logiciel;
- l'élément de service portail DOIT vérifier que la copie de logiciel téléchargée est appropriée pour lui-même. Si la copie de logiciel téléchargée est appropriée, l'élément de service portail DOIT écrire la nouvelle copie de logiciel dans une mémoire non volatile. Une fois que le transfert du fichier est terminé et réussi, l'appareil DOIT se redémarrer avec la nouvelle configuration.
  - Si l'élément de service portail est incapable de terminer le transfert de fichier pour une raison quelconque, l'élément de service portail DOIT rester capable d'accepter de nouveaux téléchargements de logiciel (sans interaction avec l'opérateur ou avec l'utilisateur), même si l'alimentation ou la connexion sont interrompues entre les essais.

- L'élément de service portail DOIT enregistrer les échecs de téléchargement et PEUT faire rapport de ces échecs en asynchrone au gestionnaire de réseau.
- Lorsque le logiciel a été amélioré pour satisfaire à une nouvelle version de la présente Recommandation, le logiciel DOIT impérativement alors travailler avec la version précédente afin de permettre une transition graduelle des unités sur le réseau.
- L'élément de service portail DOIT authentifier celui qui est à l'origine du téléchargement de logiciel.
- L'élément de service portail DOIT vérifier que le code téléchargé n'a pas été altéré par rapport à la forme originale dans laquelle il a été fourni par la source de confiance.
- Le processus de téléchargement de logiciel DOIT fournir à un opérateur les mécanismes d'amélioration ou de dégradation de la version de code des éléments.
- Le processus de téléchargement de logiciel DOIT fournir des options permettant à un opérateur de définir sa propre politique de téléchargement.
- Le fabricant de fichier de code DOIT appliquer une signature de vérification de code (CVS, *code verification signature*) sur la copie du code et sur tout autres attributs authentifiés, comme défini dans la présente Recommandation pour la signature numérique de la structure PKCS#7 au fichier de code; la clé privée utilisée pour appliquer la signature DOIT être liée à un certificat de clé publique qui permet de suivre la chaîne jusqu'au certificat CVC racine. La signature du fabricant authentifie la source et l'intégrité du fichier code.
- Un cosignataire (opérateur ou service portail) PEUT contresigner le fichier de code en plus de la signature du fabricant.
- L'élément de service portail DOIT être capable de traiter une signature numérique PKCS#7 et un certificat X.509 comme défini aux § 11.3.7.2.1.1 et 11.3.7.3 respectivement.
- (Facultatif): l'élément de service portail DEVRAIT être capable de mettre à jour la clé publique CA racine de certificat CVC mémorisée dans l'appareil.
- (Facultatif): l'élément de service portail DEVRAIT être capable de remplacer le ou les certificats CA de fabricant mémorisés dans l'appareil.
- (Facultatif): l'élément de service portail DEVRAIT être capable de mettre à jour le certificat CA de CVC mémorisé dans l'appareil.

Le téléchargement facultatif de la clé publique CA racine de CVC, du certificat CA de CVC, et/ou du certificat CA de fabricant en tant que partie du fichier de code permet de distinguer clairement la copie de code des autres paramètres dans le fichier de téléchargement de code. Il permet aussi de changer la clé publique CVC racine, le certificat CA de CVC, les certificats CA de fabricant ou les paramètres SignedData dans le fichier de téléchargement de code sans désorganiser ou changer la copie de code que l'élément de service portail va recevoir. Ceci permet à l'élément de service portail de vérifier que la copie de code n'a pas été altérée même si le fichier de téléchargement de code a changé du fait des modifications de la clé publique CA racine de CVC, du certificat CA de CVC, des certificats CA de fabricant ou des paramètres SignedData.

11.3.7.1 Téléchargement de logiciel vers les éléments de service portail

Dans la mesure où l'élément de service portail est incorporé dans un câblo-modem, la copie PS/CM DOIT être une copie unique, et le téléchargement de logiciel ne DOIT être effectué que par le câblo-modem.

11.3.7.2 Exigences pour le fichier de code

11.3.7.2.1 Structure du fichier de téléchargement de code pour le téléchargement de logiciel sécurisé

Pour un téléchargement de logiciel sécurisé, le fichier de téléchargement de code est un fichier construit en utilisant une structure conforme à PKCS#7 qui a été définie dans un format spécifique de l'utilisation avec des éléments de service portail. Le fichier de code DOIT se conformer à [PKCS#7] et DOIT être codé en DER. Le fichier de code DOIT correspondre à la structure indiquée au Tableau 45.

Lors du téléchargement de la clé publique de CA racine de CVC et/ou de certificats CA (par exemple, un certificat CA de CVC et/ou un certificat CA de fabricant) en tant que partie du fichier de code, les certificats PEUVENT être contenus dans le champ RootCAPublicKey et/ou les champs CACerts respectivement comme spécifié respectivement dans le Tableau 45, et séparé de la copie de code réelle contenue dans le champ CodeImage.

Tableau 45/J.191 – Structure du fichier de code

Fichier code	Description
Signature numérique PKCS#7 {	
ContentInfo	
ContentType	SignedData
SignedData ()	Valeur EXPLICITE du contenu des données signées: y compris la signature CVS et les certificats conformes à X.509
} *fin de signature numérique PKCS#7*	
SignedContent {	
DownloadParameters {	Format de TLV obligatoire (type 28). (La longueur est zéro s'il n'y a pas de sous-TLV.)
RootCAPublicKey ()	TLV facultatif pour la clé publique CA racine de CVC CL formattée conformément au format de clé publique RSA (type 4).
CACerts ()	TLV facultatif pour un ou plusieurs certificats CA codés en DER formatés chacun conformément au format de TLV de certificat CA (type 17).
}	
CodeImage ()	Met à niveau la copie de code
} *fin de SignedContent*	

11.3.7.2.1.1 Données signées

Le fichier de téléchargement de code contiendra les informations dans un type de contenu données signées PKCS#7 comme indiqué dans le Tableau 46. Tout en maintenant la conformité à [PKCS#7], la structure utilisée a été réduite en format pour faciliter le traitement effectué par le service portail pour valider la signature. Les données signées PKCS#7 DOIVENT être codées en DER et correspondre exactement à la structure indiquée ci-dessous sauf pour les changements d'ordre requis par le codage DER (par exemple, l'ordre des attributs SET OF). L'élément de service portail DEVRAIT rejeter la signature PKCS#7 si les données signées PKCS#7 ne correspondent pas à la structure codée en DER.

Tableau 46/J.191 – Données signées PKCS#7

Champ PKCS#7	Description
Données signées {	
version	Version = 1
DigestAlgorithmIdentifiers	SHA-1
ContentInfo	
ContentType	Données (SignedContent est enchaîné à la fin de la structure PKCS#7)
certificates {	(Certificat de vérification de code (CVC) CableLabs)
mfgCVC	(EXIGÉ pour tous les fichiers de code)
co-signerCVC	(FACULTATIF; exigé pour les cosignatures)
} *fin des certificats*	
SignerInfo {	
MfgSignerInfo {	(EXIGÉ pour tous les fichiers de code)
version	Version = 1
issuerAndSerialNumber	
issuerName	
CountryName	US
organizationName	CableLabs
CommonName	CA racine de CVC CableLabs
certificateSerialNumber	<Numéro de série de CVC Mfg>
digestAlgorithm	SHA-1
AuthenticatedAttributes	
contentType	Données (type de contenu de signedContent)
signing Time	Temps UTC (GMT), AAMMJJhhmmssZ
messageDigest	(Résumé du contenu comme défini dans [PKCS#7]
digestEncryptionAlgorithm	rsaEncryption
EncryptedDigest	
} *fin d'infos signataire mfg*	
CoSignerInfo {	(FACULTATIF; exigé pour les cosignatures)
version	Version = 1
issuerandserialnumber	
issuername	
CountryName	US
organizationName	CableLabs
CommonName	CA racine de CVC CableLabs
certificateSerialNumber	<Numéro de série de CVC de cosignataire>
digestAlgorithm	SHA-1
AuthenticatedAttributes	
contentType	Données (type de contenu de signedContent)
signing Time	Temps UTC (GMT), AAMMJJhhmmssZ

Tableau 46/J.191 – Données signées PKCS#7

Champ PKCS#7	Description
messageDigest	(Résumé du contenu comme défini dans [PKCS#7]
digestEncryptionAlgorithm	rsaEncryption
EncryptedDigest	
} *fin d'infos signataire mso*	
} *fin d'infos de signataire*	
} *fin de données signées*	

11.3.7.2.1.2 Contenu signé

Le champ Contenu signé du fichier de code contient la copie du code et le champ paramètres téléchargés, qui peuvent contenir d'autres éléments facultatifs supplémentaires – une clé publique CA racine de CVC et des certificats CA (par exemple un certificat CA de CVC et/ou un certificat CA de fabricant).

La copie de code finale est dans un format compatible avec l'élément de service portail de destination. Pour accepter les exigences de la signature PKCS#7, le contenu du code est caractérisé comme données, c'est-à-dire une simple chaîne d'octets. Le format de la copie de code finale n'est pas spécifié ici et sera défini par chaque fabricant en fonction de ses exigences.

Chaque fabricant DEVRAIT construire son code avec des mécanismes supplémentaires qui vérifient qu'une copie de code améliorée est compatible avec l'élément de service portail de destination.

Si elle est incluse dans le champ Contenu signé, la clé publique CA racine de CVC est destinée à remplacer la clé publique CA de CVC actuellement mémorisée dans l'élément de service portail. Si le téléchargement du code et l'installation sont réussis, l'élément de service portail DOIT alors remplacer sa clé publique CA racine de CVC actuellement mémorisée par la clé publique CA racine de CVC reçue dans le champ Contenu signé. Cette nouvelle clé publique CA racine de CVC sera alors utilisée pour les vérifications de CVC suivantes.

S'ils sont inclus dans le champ Contenu signé, le ou les certificats CA sont destinés à remplacer le ou les certificats CA actuellement mémorisés dans l'élément de service portail. Par exemple, si le téléchargement du code et l'installation sont réussis et si le CACert contenait un certificat CA de fabricant, l'élément de service portail DOIT alors remplacer son ou ses certificats de fabricant mémorisés par le ou les certificats de fabricant reçus dans le champ Contenu signé.

11.3.7.2.1.3 Clés de signature de code

La signature numérique PKCS#7 utilise l'algorithme de cryptage RSA avec SHA-1 [FIPS 186]. Le module clé RSA pour la signature de code est long de 2048 bits. L'élément de service portail DOIT être capable de vérifier les signatures de fichier de code qui sont signées en utilisant cette taille de module. L'exposant public est F4 (65 537 en décimal).

11.3.7.3 Format de certificat de vérification de code (CVC)

11.3.7.3.1 Format de CVC pour le téléchargement de logiciel sécurisé

Pour le téléchargement de logiciel sécurisé, le format utilisé pour le certificat CVC est conforme à X.509. Cependant, la structure X.509 a été réduite pour faciliter le traitement effectué par un élément de service portail pour valider le certificat et extraire la clé publique utilisée pour vérifier la signature CVS. Le certificat CVC DOIT être codé en DER et correspondre exactement à la structure indiquée au Tableau 47 sauf pour les changements d'ordre requis par le codage DER (par exemple

l'ordre des attributs SET OF). L'élément de service portail DEVRAIT rejeter le certificat CVC s'il ne correspond pas à la structure codée en DER représentée au Tableau 47.

Tableau 47/J.191 – Certificat de vérification de code conforme à X.509

Certificat X.509	Description
Certificate {	
version	2 (c'est-à-dire X.509 version 3)
serialNumber	Entier, 8 octets (c'est-à-dire, nombre unique alloué par l'autorité CA racine)
signature	RSA SHA-1, paramètres nuls
issuer	
countryName	US
organizationName	CableLabs
commonName	CA racine de certificat CableLabs
validity	
notBefore	Temps UTC (GMT), AAMMJJhhmmssZ (c'est-à-dire l'heure de la production)
notAfter	Temps UTC (GMT), AAMMJJhhmmssZ
subject	
countryName	<Nom du pays>
organizationName	<Nom de la compagnie>
commonName	<Nom usuel>
subjectPublicKeyInfo	
algorithm	Chiffrement RSA, paramètres nuls
subjectPublicKey	Module de 2048 bits
extensions	
KeyUsage	<Utilisation de la clé>
authorityKeyIdentifier	<Identifiant de la clé d'autorité>
signatureAlgorithm	RSA SHA-1, paramètres nuls
signature Value	<Valeur de la signature>
} *fin de certificat*	

11.3.7.3.2 Révocation de certificat

La présente Recommandation n'exige pas ou ne définit pas l'utilisation de listes de révocation de certificat (CRL). Il n'est pas demandé à l'élément de service portail de traiter les listes CRL. Les opérateurs peuvent vouloir définir et utiliser les listes CRL en dehors du réseau HFC pour aider à la gestion des fichiers de code qui leurs sont fournis par les fabricants. Cependant, il existe une méthode de révocation des certificats fondée sur la date de début de validité du certificat. Cette méthode exige qu'un certificat CVC mis à jour soit délivré à l'élément de service portail avec une heure de début de validité mise à jour. Une fois que la validation du certificat CVC a réussi, l'heure de début de validité X.509 va mettre à jour la valeur actuelle de cvcAccessStart de l'élément de service portail.

11.3.7.4 Contrôles d'accès de fichier de code

Pour le téléchargement de logiciel sécurisé, des valeurs de contrôle spéciales sont incluses dans le fichier de code pour que l'élément de service portail les vérifie avant qu'il ne valide une copie de code. Les conditions mises sur les valeurs de ces paramètres de contrôle DOIVENT être satisfaites avant que l'élément de service portail ne valide le certificat CVC ou la signature CVS, et n'accepte la copie de code.

11.3.7.4.1 Noms d'organisation sujet

L'élément de service portail va reconnaître jusqu'à deux noms, à tout instant donné, qu'il considère comme un agent signataire de code de confiance dans le champ Sujet d'un certificat CVC de fichier de code. Ceci inclut:

- le fabricant de l'appareil: le nom du fabricant dans le champ Sujet du certificat CVC du fabricant DOIT correspondre exactement au nom du fabricant mémorisé dans une mémoire non volatile de l'élément de service portail par le fabricant. Un certificat CVC de fabricant DOIT toujours être inclus dans le fichier de code;
- un agent cosignataire: il est permis qu'une autre organisation de confiance co-signe les fichiers de code destinés à l'appareil. Dans la plupart des cas, c'est l'opérateur qui contrôle le domaine de fonctionnement actuel de l'appareil. Le nom d'organisation du cosignataire est communiqué à l'élément de service portail via un certificat CVC du cosignataire dans le fichier de configuration lors de l'initialisation du processus de vérification de code de l'élément de service portail. Le nom d'organisation du cosignataire dans le champ Sujet CVC du cosignataire DOIT correspondre exactement au nom d'organisation du cosignataire reçu précédemment dans le certificat CVC d'initialisation du cosignataire et mémorisé par l'élément de service portail.

L'élément de service portail PEUT comparer les noms d'organisation au moyen d'une comparaison binaire.

11.3.7.4.2 Contrôles des variations de temps

Pour atténuer la possibilité qu'un élément de service portail reçoive un vieux fichier de code via une attaque en répétition, les fichiers de code incluent une valeur d'heure signée dans la structure PKCS#7 qui peut servir à indiquer l'heure de signature de la copie de code. L'élément de service portail DOIT conserver deux valeurs de temps UTC associées à chaque agent de signature de code. Un ensemble DOIT toujours être mémorisé et entretenu pour le fabricant de l'appareil. De plus, si le fichier de code est co-signé, l'élément de service portail DOIT aussi mémoriser et entretenir un jeu séparé de valeurs d'heure pour le cosignataire.

Ces valeurs servent à contrôler l'accès du fichier de code à l'élément de service portail en contrôlant individuellement la validité de la signature CVS et le certificat CVC. Ces valeurs sont:

- codeAccessStart: une valeur de temps UTC de 12 octets se rapportant au temps moyen de Greenwich (GMT).
- cvcAccessStart: une valeur de temps UTC de 12 octets se rapportant au temps moyen de Greenwich (GMT).

Les valeurs du temps UTC dans le certificat CVC DOIVENT être exprimées en GMT et DOIVENT inclure les secondes. C'est-à-dire qu'elles DOIVENT être exprimées dans le format suivant: AAMMJJhhmmssZ. Le champ an (AA) DOIT être interprété comme suit:

- lorsque AA est supérieur ou égal à 50, l'année doit être interprétée comme 19AA;
- lorsque AA est inférieur à 50, l'année doit être interprétée comme 20AA.

Ces valeurs feront toujours référence au temps moyen de Greenwich, et ainsi le caractère ASCII (Z) final peut être supprimé lorsqu'elles sont mémorisées par l'élément de service portail comme codeAccessStart et cvcAccessStart.

L'élément de service portail DOIT entretenir chacune de ces valeurs de temps dans un format qui contienne les informations de temps équivalentes et pertinentes pour le format UTV à 12 caractères (c'est-à-dire, AAMMJJhhmmss). L'élément de service portail DOIT comparer précisément ces valeurs mémorisées avec les valeurs de temps UTC délivrées par l'élément de service portail dans un certificat CVC. Ces exigences sont présentées plus loin dans la présente Recommandation.

Les valeurs de codeAccessStart et cvcAccessStart correspondant au fabricant de l'élément de service portail NE DOIVENT PAS décroître. La valeur de codeAccessStart et cvcAccessStart correspondant au cosignataire NE DOIT PAS décroître tant que le cosignataire ne change pas et que l'élément de service portail maintient les valeurs de contrôle de variations de temps du cosignataire.

11.3.7.5 Initialisation de mise à niveau de code

11.3.7.5.1 Initialisation du fabricant

Il est de la responsabilité du fabricant d'installer correctement la version initiale de code dans l'élément de service portail.

Pour le soutien du téléchargement de logiciel sécurisé, les valeurs des contrôles de variation de temps DOIVENT être chargées dans une mémoire non volatile de l'élément de service portail:

- nom d'organisation du fabricant de l'élément de service portail;
- valeurs des contrôles de variation de temps du fabricant:
  a) valeur d'initialisation codeAccessStart;
  b) valeur d'initialisation cvcAccessStart.

Le nom d'organisation du fabricant de l'élément de service portail DOIT toujours être présent dans l'appareil. Le nom d'organisation du fabricant de l'élément de service portail PEUT être mémorisé dans la copie de code de l'appareil. Le nom du fabricant utilisé pour la mise à niveau du code n'est pas nécessairement le même que celui qui est utilisé dans le certificat CA de fabricant.

Les valeurs de contrôle de variation de temps, codeAccessStart et cvcAccessStart, DOIVENT être initialisées à un temps UTC compatible avec l'heure de début de validité du dernier certificat CVC du fabricant. Ces valeurs de variation de temps seront mises à jour périodiquement en période de fonctionnement normal au moyen des certificats CVC du fabricant qui sont reçus et vérifiés par l'élément de service portail.

11.3.7.5.2 Initialisation réseau

Pour les besoins de la vérification de code, le fichier de configuration du service portail est utilisé comme moyen authentifié dans lequel on initialise le processus de vérification de code. Dans le fichier de configuration de l'élément de service portail, l'élément de service portail reçoit les réglages de configuration pertinents pour la vérification de mise à niveau de code.

Le fichier de configuration DEVRAIT toujours inclure le certificat CVC le plus à jour applicable pour l'élément de service portail de destination; mais lorsque le fichier de configuration sert à initialiser une mise à niveau de code, il DOIT inclure un certificat de vérification de code (CVC) pour initialiser l'acceptation des fichiers de code par l'élément de service portail conformément à la présente Recommandation. Sans s'occuper de savoir si une mise à niveau de code est nécessaire, un certificat CVC dans le fichier de configuration DOIT être traité par l'élément de service portail. Un fichier de configuration PEUT contenir:

- pas de certificat CVC – l'élément de service portail NE DOIT PAS accepter un fichier de code;

- seulement un certificat CVC de fabricant – l'élément de service portail DOIT vérifier que le certificat CVC de fabricant s'articule bien à la racine de certificat CVC avant d'accepter un fichier de code. Lorsque le fichier de configuration de l'élément de service portail ne contient qu'un certificat CVC de fabricant valide, l'appareil ne demandera alors qu'une signature de fabricant sur les fichiers de code. Dans ce cas, l'élément de service portail NE DOIT PAS accepter les fichiers de code qui n'ont pas été cosignés;
- seulement un certificat CVC de cosignataire – l'élément de service portail DOIT vérifier que le certificat CVC du cosignataire s'articule bien jusqu'à la racine de certificat CVC avant d'accepter un fichier de code. Lorsque le fichier de configuration de l'élément de service portail contient un certificat CVC de cosignataire valide, il est utilisé pour initialiser l'appareil avec un cosignataire. Une fois validé, le nom organizationName du sujet du certificat CVC deviendra le cosignataire de code alloué à l'élément de service portail. Pour qu'un élément de service portail accepte ultérieurement une copie de code, le cosignataire DOIT avoir signé le fichier de code en plus du fabricant de l'appareil;
- à la fois un certificat CVC de fabricant et un de cosignataire. L'élément de service portail DOIT vérifier que les deux certificats CVC s'articulent bien jusqu'à la racine de certificats CVC avant d'accepter un fichier de code.

Avant que l'élément de service portail n'active sa capacité de mise à niveau des fichiers de code sur le réseau, il DOIT recevoir un certificat CVC valide dans un fichier de configuration. De plus, lorsque le fichier de configuration de l'élément de service portail ne contient pas de certificat CVC valide et que sa capacité à mettre à niveau les fichiers de code a été désactivée, l'élément de service portail DOIT rejeter toute information contenue dans un certificat CVC délivré ultérieurement via SNMP.

Le nom d'organisation du fabricant de l'élément de service portail et les valeurs de contrôle des variations de temps du fabricant DOIVENT toujours être présents dans l'élément de service portail. Si l'élément de service portail est initialisé pour accepter un code cosigné par un cosignataire supplémentaire, le nom de l'organisation et leurs valeurs correspondantes de contrôle de variations de temps DOIVENT être mémorisées et entretenues pendant qu'elles sont en fonctionnement. De l'espace DOIT être alloué dans la mémoire des éléments de service portail pour les valeurs de contrôle de cosignataires suivantes:

1) nom d'organisation de l'agent cosignataire;
2) valeurs de contrôle de variation de temps du cosignataire:
    a) cvcAccessStart
    b) codeAccessStart

L'ensemble de ces valeurs du fabricant DOIT être mémorisé dans la mémoire non volatile de l'élément de service portail et ne doit pas être perdu lorsque la source d'alimentation principale de l'appareil est retirée ou lors d'un réamorçage.

Lorsqu'un cosignataire est alloué à l'élément de service portail, l'ensemble de valeurs de certificat CVC du cosignataire DOIT être mémorisé dans la mémoire de l'élément de service portail. L'élément de service portail PEUT retenir ces valeurs dans une mémoire non volatile qui ne doit pas être perdue lorsque la source d'alimentation principale de l'appareil est retirée ou lors d'un réamorçage. Cependant, lors de l'allocation d'un cosignataire à un élément de service portail, le certificat CVC est toujours dans le fichier de configuration. L'élément de service portail recevra donc toujours les valeurs de contrôle du cosignataire pendant la phase d'initialisation et il ne lui est donc pas imposé de mémoriser les valeurs de contrôle de variation de temps lorsque l'alimentation du secteur est perdue ou pendant un processus de réamorçage.

11.3.7.6 Traitement de certificat CVC

Pour accélérer la livraison d'un certificat CVC mis à jour sans demander au service portail de procéder à la mise à niveau de code, le certificat CVC PEUT être livré en fichier de configuration ou en base MIB SNMP. Le format du certificat CVC est le même qu'il soit un fichier de code, un fichier de configuration ou une base MIB SNMP.

11.3.7.6.1 Traitement du certificat CVC du fichier de configuration

Lorsqu'un certificat CVC est inclus dans le fichier de configuration, l'élément de service portail DOIT vérifier le certificat CVC avant d'accepter quelques réglages de mise à niveau de code qu'il contienne. A réception du certificat CVC dans le fichier de configuration, l'élément de service portail DOIT effectuer les étapes de validation et de procédure suivantes. Si l'un des essais de vérification suivant échoue, l'élément de service portail DOIT immédiatement arrêter le processus de vérification du certificat CVC et enregistrer l'erreur s'il y a lieu. Si le fichier de configuration de l'élément de service portail n'inclut pas un certificat CVC qui valide de façon appropriée, l'élément de service portail NE DOIT PAS télécharger de fichiers de mise à niveau de code, qu'ils soient déclenchés par le fichier de configuration de l'élément de service portail ou via une base MIB SNMP. De plus, si les fichiers de configuration de l'élément de service portail n'incluent pas un certificat CVC qui valide correctement, l'élément de service portail n'est pas tenu de traiter les certificats CVC délivrés ultérieurement via une base MIB SNMP et NE DOIT PAS accepter d'informations d'un certificat CVC ultérieurement délivré via une base MIB SNMP.

A réception du certificat CVC dans un fichier de configuration, l'élément de service portail DOIT:

1) vérifier que l'extension d'utilisation de clé étendue est dans le certificat CVC comme défini au § 11.3.2.2.2;
2) vérifier le nom d'organisation de sujet de certificat.
   a) Si le certificat CVC est un certificat CVC de fabricant (Type 32) alors:
      i) SI le nom d'organisation est identique au nom de fabricant de l'appareil, ALORS, c'est le certificat CVC du fabricant. Dans ce cas, l'élément de service portail DOIT vérifier que la date de départ de validité du certificat CVC de fabricant est supérieure ou égale à la valeur cvcAccessStart du fabricant actuellement détenue dans l'élément de service portail;
      ii) SI le nom d'organisation n'est pas identique au nom de fabricant de l'appareil, ce certificat CVC DOIT ALORS être rejeté et l'erreur doit être enregistrée.
   b) Si le certificat CVC est un certificat CVC de cosignataire (Type 33) alors:
      i) SI le nom d'organisation est identique au cosignataire de code actuel de l'élément de service portail, ALORS c'est le certificat CVC du cosignataire actuel et l'élément de service portail DOIT vérifier que la date de début de validité est supérieure ou égale à la valeur cvcAccessStart du cosignataire actuellement détenue dans l'élément de service portail;
      ii) SI le nom d'organisation n'est pas identique au nom de cosignataire actuel, ALORS, après que le certificat CVC a été validé (et que l'enregistrement est terminé) ce nom d'organisation sujet deviendra le nouveau cosignataire de code de l'élément de service portail. L'élément de service portail NE DOIT PAS accepter un fichier tant qu'il n'a pas été signé par le fabricant, et cosigné par le cosignataire de code;
3) valider la signature du producteur de certificat CVC en utilisant la clé publique CA de certificat CVC par l'élément de service portail;
4) valider la signature CA de certificat CVC en utilisant la clé publique CA racine de CVC détenue par l'élément de service portail. La vérification de la signature authentifiera la source et validera la confiance dans les paramètres de certificat CVC;

5) mettre à jour la valeur actuelle cvcAccessStart de l'élément de service portail correspondant au nom d'organisation du certificat CVC (c'est-à-dire du fabricant ou du cosignataire) avec la valeur de date de début de validité venant du certificat CVC validé. Si la valeur de date de début de validité est supérieure à la valeur actuelle de l'élément de service portail codeAccessStart, mettre à jour la valeur codeAccessStart de l'élément de service portail avec la valeur de date de début de validité. L'élément de service portail DEVRAIT mettre à l'écart tous les restes du certificat CVC.

11.3.7.6.2 Traitement du certificat CVC SNMP

L'élément de service portail DOIT traiter les certificats livrés par le protocole SNMP lorsqu'il a la capacité de mettre à niveau les fichiers de code, autrement, tous les certificats CVC livrés via le protocole SNMP DOIVENT être rejetés. Lorsqu'il valide le certificat CVC livré via SNMP, l'élément de service portail DOIT effectuer les étapes de validation et de procédure suivantes. Si un seul des essais de vérification suivants échoue, l'élément de service portail DOIT immédiatement arrêter le processus de vérification de certification CVC, enregistrer s'il y a lieu l'erreur, et retirer tous les restes du processus de cette étape.

L'élément de service portail DOIT:

1) vérifier que l'extension d'utilisation de clé étendue est dans ce certificat CVC comme défini au § 11.3.2.2.2;
2) vérifier le nom d'organisation sujet du certificat CVC;
   a) SI le nom d'organisation est identique au nom de fabricant de l'appareil, PUIS c'est le certificat CVC du fabricant. Dans ce cas, l'élément de service portail DOIT vérifier que la date de début de validité su certificat CVC du fabricant est supérieure à la valeur cvcAccessStart du fabricant actuellement détenue dans l'élément de service portail;
   b) SI le nom d'organisation est identique au cosignataire de code actuel de l'élément de service portail, ALORS c'est un certificat CVC actuel de cosignataire, et la date de début de validité DOIT être supérieure à la valeur cvcAccessStart du cosignataire actuellement détenue dans l'élément de service portail;
   c) SI le nom d'organisation n'est pas identique au nom du fabricant d'appareil ou du cosignataire actuel, ALORS l'élément de service portail DOIT immédiatement rejeter ce certificat CVC;
3) valider la signature du producteur du certificat CVC en utilisant la clé publique CA de CVC détenue par l'élément de service portail;
4) valider la signature du producteur de certificat CVC en utilisant la clé publique CA racine de certificat CVC détenue par l'élément de service portail. La vérification de la signature authentifiera le certificat et confirmera la confiance dans la date de départ de validité du certificat CVC;
5) mettre à jour la valeur actuelle des valeurs cvcAccessStart du sujet avec la valeur de date de début de validité du certificat CVC. Si la valeur de date de début de validité est supérieure à la valeur actuelle de codeAccessStart de l'élément de service portail, mettre à jour la valeur de codeAccessStart de l'élément de service portail avec la valeur de début de validité. Tous les paramètres de certificat EXCEPTÉ la date de début de validité ne sont plus nécessaires et DEVRAIENT être mis à l'écart.

11.3.7.7 Exigences de signature de code

11.3.7.7.1 Exigences d'autorité de certification (CA)

Les certificats de vérification de code (CVC) sont signés et produits par l'autorité CA de certificat CVC. Le certificat CVC DOIT être exactement comme spécifié au § 11.3.7.3. L'autorité CA de CVC NE DOIT PAS signer de certificat CVC à moins qu'il ne soit identique au format spécifié dans

le présent paragraphe. Avant de signer un certificat CVC, l'autorité CA de CVC DOIT vérifier que la demande de certificat est authentique.

L'autorité CA de CVC sera responsable de l'enregistrement des noms des abonnés autorisés de certificat CVC. Les abonnés de certificat CVC incluent les fabricants d'élément de service portail et les fabricants et opérateurs qui vont co-signer les copies de code. Il est de la responsabilité de l'autorité CA de CVC de garantir que le nom d'organisation de chaque abonné CVC est différent. Les lignes directrices suivantes DOIVENT être appliquées lors de l'allocation de noms d'organisation aux cosignataires de fichiers de code:

- le nom d'organisation utilisé pour s'identifier comme agent cosignataire de code dans un certificat CVC DOIT être alloué par l'organisation qui a produit le certificat racine;
- le nom DOIT être une chaîne imprimable de huit chiffres hexadécimaux qui distingue de façon non équivoque un agent signataire de code de tous les autres;
- chaque chiffre hexadécimal dans le nom DOIT être choisi parmi l'ensemble de caractères 0-9 (0x30-0x39) ou A-F (0x41-0x46);
- la chaîne consistant en huit chiffres 0 n'est pas admise et NE DOIT PAS être utilisée dans un certificat CVC.

Pour conserver de l'espace de mémorisation, l'élément de service portail PEUT représenter en interne le nom du cosignataire de code dans un format alternatif dans la mesure où toutes les informations sont conservées et que le format d'origine peut être reproduit, par exemple, comme un entier de 32 bits différents de zéro, avec une valeur entière de 0 représentant l'absence de signataire de code.

11.3.7.7.1.1 Exigences pour le certificat CVC de fabricant

Pour signer leurs fichiers de code, les fabricants DOIVENT obtenir un certificat CVC valide de l'autorité CA de CVC. Toutes les copies de code de fabricant fournies à un opérateur pour la mise à niveau à distance d'un appareil DOIVENT être signées conformément aux exigences définies dans la présente Recommandation. Lorsqu'il signe un fichier de code, un fabricant PEUT choisir de ne pas mettre à jour la valeur signingTime PKCS#7 dans les informations de signature du fabricant. La présente Recommandation exige que la valeur signingTime PKCS#7 soit égale ou supérieure à la date de début de validité du certificat CVC. Si le fabricant utilise une valeur de signingTime égale à la date de début de validité du certificat CVC lorsqu'il signe une série de fichiers de code, ces fichiers de code peuvent être utilisés et réutilisés. Ceci permet à un opérateur d'utiliser le fichier de code pour mettre à niveau ou dégrader la version de code pour les appareils de ce fabricant. Ces fichiers de code seront valides jusqu'à ce qu'un nouveau certificat CVC soit généré et reçu par l'élément de service portail.

11.3.7.7.1.2 Exigences pour l'opérateur

Lorsqu'un opérateur reçoit des fichiers de code mis à niveau de la part d'un fabricant, l'opérateur DEVRAIT valider la copie de code en utilisant la clé publique CA de certificat CVC. Ceci permettra à l'opérateur de vérifier que la copie de code est comme lorsqu'elle a été construite par le fabricant de confiance. L'opérateur peut vérifier à nouveau le fichier code à tout moment en répétant le processus.

Si un opérateur veut exercer l'option de cosignature de la copie de code destinée à un appareil de son réseau, l'opérateur DOIT obtenir un certificat CVC valide de l'autorité CA de CVC.

Lorsqu'il signe un fichier de code, l'opérateur DOIT cosigner le contenu du fichier conformément à la norme de signature PKCS#7, et inclure son certificat CVC d'opérateur comme défini au § 11.3.7.2.1.1. La présente application n'exige pas d'un opérateur qu'il cosigne les fichiers de code, mais lorsque l'opérateur suit toutes les règles définies dans la présente Recommandation pour la préparation d'un fichier de code, l'élément de service portail DOIT l'accepter.

11.3.7.8 Processus de déclenchement

Les téléchargements de code, sans considération du mode d'approvisionnement, peuvent être initialisés pendant le processus d'approvisionnement et d'enregistrement via un téléchargement initialisé par le fichier de configuration, ou pendant le fonctionnement normal en utilisant la commande de téléchargement initialisée par le protocole SNMP. L'élément de service portail DOIT accepter les deux méthodes.

NOTE – Avant de déclencher un téléchargement sécurisé de logiciel, les informations appropriées de certificat CVC DOIVENT être incluses dans le fichier de configuration. Si l'opérateur décide d'utiliser le téléchargement initialisé par le protocole SNMP comme méthode pour déclencher un téléchargement sécurisé de logiciel, il est recommandé que les informations de certificat CVC soient toujours présentes dans le fichier de configuration, de sorte que l'élément de service portail ait toujours les informations de CVC initialisées lorsqu'il en a besoin. Si l'opérateur décide d'utiliser le téléchargement initialisé par le fichier de configuration comme méthode de déclenchement du téléchargement sécurisé de logiciel, les informations de CVC doivent nécessairement être présentes dans le fichier de configuration au moment où l'appareil est réamorcé pour obtenir le fichier de configuration qui déclenchera la mise à niveau.

11.3.7.8.1 Téléchargement de logiciel à l'initiative du protocole SNMP

A partir d'une station de gestion de réseau:

- mettre docsDevSwServer à l'adresse du serveur TFTP de mise à niveau de logiciels;
- mettre docsDevSwFilename au nom de chemin de fichier de la copie de mise à niveau de logiciel;
- mettre docsDevSwAdminStatus à Upgrade-from-mgt (*mise à niveau venant de la gestion*). L'état docsDevSwAdminStatus DOIT persister à travers les rétablissements/réamorçages jusqu'à ce qu'il soit modifié par un gestionnaire SNMP ou via le fichier de configuration de l'élément de service portail.

L'état par défaut de docsDevSwAdminStatus DOIT être allowProvisioningUpgrade{2} jusqu'à ce qu'il soit recouvert par ignoreProvisioningUpgrade{3} à la suite d'une mise à niveau réussie de logiciel initialisée par le protocole SNMP ou autrement modifié par la station de gestion. L'état docsDevSwOperStatus DOIT persister à travers les réinitialisations pour rapporter le résultat de la dernière tentative de mise à niveau de logiciel.

Si un élément de service subit une perte d'alimentation ou une réinitialisation pendant une mise à niveau à l'initiative du protocole SNMP, l'élément de service portail DOIT arrêter la mise à niveau sans exiger d'intervention manuelle, et lorsque l'élément de service portail arrête le processus de mise à niveau:

- docsDevSwAdminStatus DOIT être Upgrade-from-mgt{1};
- docsDevSwFilename DOIT être le nom de fichier de la copie de logiciel à mettre à niveau;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant la copie mise à niveau du logiciel à mettre à niveau;
- docsDevSwOperStatus DOIT être inProgress{1};
- docsDevSwCurrentVers DOIT être la version actuelle du logiciel qui fonctionne sur l'appareil.

Dans le cas où l'élément de service portail atteint le nombre maximal d'essais (maximum d'essais = 3) à la suite de multiples pertes d'alimentation ou de réinitialisations pendant une mise à niveau à l'initiative du protocole SNMP, l'état de l'élément de service portail DOIT adhérer aux exigences suivantes après qu'il s'est enregistré:

- docsDevSwAdminStatus DOIT être allowProvisioningUpgrade{2};
- docsDevSwFilename DOIT être le nom de fichier qui a échoué au processus de mise à niveau;

- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué au processus de mise à niveau;
- docsDevSwOperStatus DOIT être other{5};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui fonctionne sur l'appareil.

Si un élément de service portail épuise le nombre exigé d'essais TFTP en alignant un total de 16 essais consécutifs, l'élément de service portail DOIT retourner à la dernière copie connue qui fonctionnait et repasser en état opérationnel tout en suivant les exigences suivantes:

- docDevSwAdminStatus DOIT être allowProvisioningUpgrade{2};
- docDevSwFilename DOIT être le nom de fichier du logiciel qui a échoué au processus de mise à niveau;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué au processus de mise à niveau;
- docsDevSwOperStatus DOIT être failed{4};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui fonctionne sur l'appareil.

Après que l'élément de service portail a terminé le téléchargement sécurisé de logiciel à l'initiative du protocole SNMP, l'élément de service portail DOIT réamorcer et devenir opérationnel avec la copie correcte du logiciel, et une fois que l'appareil est opérationnel, il DOIT suivre les exigences suivantes:

- mettre son état docsDevSwAdminStatus à ignoreProvisioningUpgrade{3};
- mettre son état docsDevOperStatus à completeFromMgt{3};
- réamorcer.

L'élément de service portail DOIT utiliser de façon appropriée l'état ignoreProvisioningUpgrade pour ignorer la valeur de mise à niveau de logiciel qui peut être incluse dans le fichier de configuration de l'élément de service portail et devenir opérationnel avec la copie de logiciel correcte et après que l'appareil est repassé en fonctionnement, il DOIT adhérer aux exigences suivantes:

- docsDevSwAdminStatus DOIT être ignoreProvisioningUpgrade{3};
- docsDevSwFilename PEUT être le nom de fichier du logiciel fonctionnant actuellement sur l'élément de service portail;
- docsDevSwServer PEUT être l'adresse du serveur TFTP contenant le logiciel qui fonctionne actuellement sur l'élément de service portail;
- docsDevSwOperStatus DOIT être completeFromMgt{3};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui fonctionne sur l'élément de service portail.

Dans le cas où l'élément de service portail réussit à télécharger (ou à détecter pendant le téléchargement) une copie qui n'est pas destinée à l'appareil, le:

- docsDevSwAdminStatus DOIT être allowProvisioningUpgrade{2};
- docsDevSwFilename DOIT être le nom de fichier du logiciel qui a échoué à la mise à niveau;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué au processus de mise à niveau;

- docsDevSwOperStatus DOIT être other{5};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui fonctionne sur l'appareil.

Dans le cas où l'élément de service portail détermine que la copie téléchargée a subi des dommages ou des lésions, l'élément de service portail DOIT rejeter la copie nouvellement faite. L'élément de service portail PEUT réessayer de télécharger si le nombre MAX de la séquence d'essais TFTP n'a pas été atteint. Si l'élément de service portail choisit de ne pas réessayer et que le nombre MAX de la séquence d'essais TFTP n'a pas été atteint, l'élément de service portail DOIT repasser à la dernière copie connue qui fonctionnait, passer à un état opérationnel, générer les notifications d'événement appropriées comme spécifié au § 11.3.7.10, et adhérer aux exigences suivantes:

- docsDevSwAdminStatus DOIT être allowProvisioningUpgrade{2};
- docsDevSwFilename DOIT être le nom de fichier du logiciel qui a échoué à la mise à niveau;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué à la mise à niveau;
- docsDevSwOperStatus DOIT être other{5};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui fonctionne sur l'appareil.

Dans le cas où l'élément de service portail détermine que la copie est endommagée ou corrompue, l'élément de service portail DOIT rejeter la copie nouvellement téléchargée. L'élément de service portail PEUT tenter de télécharger une nouvelle copie si le nombre MAX d'essais de séquence TFTP n'a pas été atteint. A la 16ième tentative de téléchargement de logiciel consécutive qui échoue, l'élément de service portail DOIT repasser à la dernière copie connue qui fonctionnait et passer à un état opérationnel. Dans ce cas, il est demandé à l'élément de service portail d'envoyer deux notifications, une pour notifier que la limite d'essais TFTP MAX a été atteinte, et l'autre pour notifier que la copie est endommagée. Immédiatement après que l'élément de service portail a atteint l'état opérationnel, l'élément de service portail DOIT adhérer aux exigences suivantes:

- docsDevSwAdminStatus DOIT être allowProvisioningUpgrade{2};
- docsDevSwFilename DOIT être le nom de fichier du logiciel qui a échoué à la mise à niveau;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué à la mise à niveau;
- docsDevSwOperStatus DOIT être other{5};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui fonctionne sur l'appareil.

11.3.7.8.2 Téléchargement de logiciel à l'initiative du fichier de configuration

Le téléchargement de logiciel à l'initiative du fichier de configuration est initialisé par l'envoi du nom de fichier de mise à jour de logiciel dans le fichier de configuration de l'élément de service portail. Si le nom de fichier de mise à jour de logiciel dans le fichier de configuration de l'élément de service portail ne correspond pas à la copie de logiciel actuelle de l'appareil, l'élément de service portail DOIT demander le fichier spécifié au serveur de logiciels via TFTP.

NOTE – L'adresse IP du serveur de logiciels est un paramètre distinct. S'il est présent, l'élément de service portail DOIT essayer de télécharge le fichier spécifié à partir de ce serveur. S'il n'est pas présent, l'élément de service portail DOIT essayer de télécharger le fichier spécifié du serveur de fichiers de configuration.

Dans le cas où l'élément de service portail atteint le nombre maximal d'essais (maximum d'essais = 3) résultant de pertes d'alimentation ou réinitialisations multiples pendant une mise à

niveau à l'initiative du fichier de configuration, l'état de l'élément de service portail DOIT adhérer aux exigences suivantes après son enregistrement:

- docsDevSwAdminStatus DOIT être allowProvisioningUpgrade{2};
- docsDevSwFilename DOIT être le nom de fichier du logiciel qui a échoué à la mise à niveau;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué à la mise à niveau;
- docsDevSwOperStatus DOIT être other{5};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui fonctionne sur l'appareil.

Si un élément de service portail dépasse le nombre d'essais TFTP requis en produisant un total de 16 essais consécutifs, l'élément de service portail DOIT repasser à la dernière copie connue qui fonctionnait, passer à un état opérationnel, et adhérer aux exigences suivantes:

- docDevSwAdminStatus DOIT être allowProvisioningUpgrade{2};
- docDevSwFilename DOIT être le nom de fichier du logiciel qui a échoué au processus de mise à niveau;
- docsDevSwServer DOIT être l'adresse du serveur TFTP contenant le logiciel qui a échoué au processus de mise à niveau;
- docsDevSwOperStatus DOIT être failed{4};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel qui fonctionne sur l'appareil.

Après que l'élément de service portail a terminé le téléchargement de logiciel initialisé par le fichier de configuration, l'élément de service portail DOIT réamorcer et devenir opérationnel avec la copie de logiciel correcte. Après que l'élément de service portail est enregistré, le:

- docsDevSwAdminStatus DOIT être allowProvisioningUpgrade{2};
- docsDevSwFilename PEUT être le nom de fichier du logiciel fonctionnant actuellement sur l'appareil;
- docsDevSwServer PEUT être l'adresse su serveur TFTP contenant le logiciel fonctionnant actuellement sur l'appareil;
- docsDevSwOperStatus DOIT être completeFromProvisioning{2};
- docsDevSwCurrentVer DOIT être la version actuelle du logiciel fonctionnant sur l'appareil.

11.3.7.9 Vérification de code

Pour un téléchargement sécurisé de logiciel, l'élément de service portail DOIT effectuer les essais de vérification présentés dans ce paragraphe. Si l'un des essais de vérification échoue, ou si une portion quelconque du fichier de code est rejetée à cause d'un format non valide, l'élément de service portail DOIT immédiatement arrêter le processus de téléchargement, enregistrer l'erreur s'il y a lieu, retirer tous les restes du processus jusqu'à cette étape et continuer de fonctionner avec son code existant. Les essais de vérification peuvent être effectués dans n'importe quel ordre, pourvu que tous les essais applicables présentés dans ce paragraphe soient effectués.

1) L'élément de service portail DOIT valider les informations de signature du fabricant en vérifiant que la valeur signingTime (*date de signature*) de PKCS#7 est:
   a) égale ou supérieure à la valeur de codeAccessStart du fabricant actuellement détenue dans l'élément de service portail;
   b) égale ou supérieure à la valeur de date de début de validité du certificat CVC du fabricant;

c) inférieure ou égale à la date de fin de validité du certificat CVC du fabricant.

2) L'élément de service portail DOIT valider le certificat CVC du fabricant en vérifiant que:

a) le nom d'organisation sujet du CVC est identique au nom de fabricant actuellement mémorisé dans la mémoire de l'élément de service portail;

b) la date de début de validité de certificat CVC est égale ou supérieure à la valeur cvcAccessStart du fabricant actuellement détenue dans l'élément de service portail;

c) l'extension d'utilisation de clé étendue est dans le certificat CVC comme défini au § 11.3.2.2.2.

3) L'élément de service portail DOIT valider la signature du certificat en utilisant la clé publique CA de CVC détenue par l'élément de service portail. A son tour, la signature du certificat CA de CVC est validée par la clé publique CA racine de CVC détenue par l'élément de service portail. La vérification de la signature authentifiera la source de la clé de vérification de code (CVK, *code verification key*) publique et confirmera que la clé est de confiance. Une fois que la confiance a été établie dans la clé CVK du fabricant, les paramètres restants du certificat, EXCEPTÉ la date de début de validité, ne sont plus nécessaires et DEVRAIENT être mis à l'écart.

4) L'élément de service portail DOIT vérifier la signature du fichier de code du fabricant.

a) L'élément de service portail DOIT effectuer un nouveau hachage SHA-1 sur le contenu SignedContent. Si la valeur du résumé de message ne correspond pas au nouveau hachage, l'élément de service portail DOIT considérer la signature sur le fichier de code comme non valide.

b) Si la signature n'est pas vérifiée, tous les composants du fichier de code (y compris la copie de code), et toutes valeurs déduites du processus de vérification DOIVENT être rejetés et DEVRAIENT être immédiatement mis à l'écart.

5) Si la signature du fabricant est vérifiée et que la signature d'un agent cosignataire est requise:

a) l'élément de service portail DOIT valider les informations de signature du cosignataire en vérifiant que:

i) les informations de signature du cosignataire sont incluses dans le fichier de code;

ii) la valeur signingTime de PKCS#7 est égale ou supérieure à celle de la valeur correspondante de codeAccessStart actuellement détenue dans l'élément de service portail;

iii) la valeur PKCS#7 de signingTime est égale ou supérieure à celle de la date de début de validité de CVC correspondante;

iv) la valeur signingTime de PKCS#7 est inférieure ou égale à la date de fin de validité du certificat CVC correspondant;

b) l'élément de service portail DOIT valider le certificat CVC du cosignataire en vérifiant que:

i) le nom d'organisation sujet du certificat CVC est identique au nom d'organisation du cosignataire actuellement mémorisé dans la mémoire de l'élément de service portail;

ii) la date de début de validité du certificat CVC est égale ou supérieure à la valeur cvcAccessStart actuellement détenue dans l'élément de service portail pour le nom d'organisation sujet correspondant;

iii) l'extension d'usage de clé étendue est dans le certificat CVC comme défini au § 11.3.2.2.2;

c) l'élément de service portail DOIT valider la signature du certificat en utilisant la clé publique CA de CVC détenue par l'élément de service portail. A son tour, la signature de certificat CA de CVC est validée par la clé publique CA racine de CVC détenue dans l'élément de service portail. La vérification de la signature va authentifier la source de la clé de vérification de code (CVK) du cosignataire et confirmer que la clé est de confiance. Une fois que la confiance a été établie à l'égard de la clé CVK du cosignataire, les paramètres de certificat restants, EXCEPTÉ la date de début de validité, ne sont plus nécessaires et DEVRAIENT être mis à l'écart;

d) l'élément de service portail DOIT vérifier la signature de fichier de code du cosignataire;

e) l'élément de service portail DOIT effectuer un nouveau hachage SHA-1 sur le SignedContent. Si la valeur du résumé de message ne correspond pas au nouveau hachage, l'élément de service portail DOIT considérer que la signature sur le fichier de code est non valide;

f) si la signature n'est pas vérifiée, tous les composants du fichier de code (y compris la copie de code), et toutes les valeurs déduites du processus de vérification DOIVENT être rejetés et DEVRAIENT être immédiatement mis à l'écart;

6) si la signature du fabricant, et facultativement du cosignataire, est vérifiée, la copie de code peut être de confiance et l'installation peut se poursuivre. Avant d'installer la copie de code, tous les autres composants du fichier de code et toutes les valeurs déduites du processus de vérification à l'exception des valeurs de signingTime PKCS#7 et de début de validité du certificat CVC DEVRAIENT être immédiatement mis à l'écart;

7) si l'installation de code est un échec, l'élément de service portail DOIT rejeter les valeurs de signingTime PKCS#7 et de début de validité du certificat CVC qu'il vient de recevoir dans le fichier de code;

8) lorsque l'installation de code est réussie, l'élément de service portail DOIT mettre à jour les commandes du fabricant qui sont dépendantes du temps avec les valeurs provenant des informations de signature et du certificat CVC du fabricant:

a) mettre à jour la valeur actuelle de codeAccessStart avec la valeur signingTime PKCS#7;

b) mettre à jour la valeur actuelle de cvcAccessStart avec la valeur de début de validité de certificat CVC;

9) lorsque l'installation de code est réussie, SI le fichier de code était cosigné, l'élément de service portail DOIT mettre à jour les commandes du cosignataire qui varient selon le temps avec les valeurs provenant des informations de signature et du CVC du cosignataire:

a) mettre à jour la valeur actuelle de codeAccessStart avec la valeur signingTime PKCS#7;

b) mettre à jour la valeur actuelle de cvcAccessStart avec la valeur de début de validité de certificat CVC.

11.3.7.10 Codes d'erreur

Des codes d'erreur sont définis pour indiquer les états d'échec possibles pendant le processus de vérification de code de téléchargement de logiciel sécurisé.

1) commandes de fichier code inappropriées:

a) le nom d'organisation sujet de CVC pour le fabricant ne correspond pas au nom de fabricant de l'élément de service portail;

b) le nom d'organisation sujet de CVC pour l'agent cosignataire ne correspond pas à l'agent cosignataire de code actuel de l'élément de service portail;

c) la valeur signingTime PKCS#7 est inférieure à la valeur de codeAccessStart actuellement détenue dans l'élément de service portail;

d) la valeur de date de début de validité PKCS#7 du fabricant est inférieure à la valeur de cvcAccessStart actuellement détenue dans l'élément de service portail;

e) la date de début de validité du certificat CVC du fabricant est inférieure à la valeur de cvcAccessStart actuellement détenue dans l'élément de service portail;

f) la valeur signingTime PKCS#7 du fabricant est inférieure à la date de début de validité du certificat CVC;

g) l'extension d'usage de clé étendu manque ou est inappropriée dans le certificat CVC du fabricant;

h) la valeur signingTime PKCS#7 du cosignataire est inférieure à la valeur de codeAccessStart actuellement détenue dans l'élément de service portail;

i) la valeur de date de début de validité PKCS#7 du cosignataire est inférieure à la valeur de cvcAccessStart actuellement détenue dans l'élément de service portail;

j) la date de début de validité du certificat CVC du cosignataire est inférieure à la valeur de cvcAccessStart actuellement détenue dans l'élément de service portail;

k) la valeur signingTime PKCS#7 du cosignataire est inférieure à la date de début de validité du certificat CVC;

l) l'extension d'usage de clé étendu manque ou est inappropriée dans le certificat CVC du cosignataire.

2) échec de la validation du certificat CVC du fabricant du fichier de code;

3) échec de la validation de la signature CVS du fabricant du fichier de code;

4) échec de la validation du certificat CVC du cosignataire du fichier de code;

5) échec de la validation de la signature CVS du cosignataire du fichier de code;

6) format de certificat CVC de fichier de configuration inapproprié (par exemple, attribut d'usage de clé manquant ou impropre);

7) échec de la validation du certificat CVC du fichier de configuration;

8) format du certificat CVC de protocole SNMP inapproprié:

a) le nom d'organisation sujet de certificat CVC pour le fabricant ne correspond pas au nom de fabricant de l'appareil;

b) le nom d'organisation sujet de certificat CVC pour l'agent cosignataire de code ne correspond pas à l'agent cosignataire de code actuel de l'élément de service portail;

c) la date de début de validité du certificat CVC est inférieure ou égale à la valeur de cvcAccessStart du sujet actuellement détenue dans l'élément de service portail;

d) Attribut d'usage de clé manquant ou impropre;

9) échec de la validation du certificat CVC de protocole SNMP.

11.3.7.11 Dégradation du logiciel

La dégradation du logiciel définit le processus de retrait de la version mise à niveau du téléchargement de la copie de logiciel, et donc du retour de l'appareil à l'exact état antérieur.

Lorsque l'élément de service portail reçoit un fichier de code avec une date de signature postérieure à celle de la valeur mémorisée, le dispositif actualisera sa mémoire interne avec la valeur reçue.

Comme l'élément PS n'acceptera pas de fichiers de code avec une date de signature antérieure à celle de la valeur mémorisée, le signataire peut choisir de ne pas mettre à jour la date de signature lorsqu'il met à niveau un dispositif avec un nouveau fichier de code et qu'il veut éviter d'interdire

l'accès aux anciens fichiers de code. De cette façon, de multiples fichiers de code avec la même date de signature de code permettent à un opérateur de dégrader librement une copie de code d'un appareil avec une version ancienne (c'est-à-dire, jusqu'à ce que le certificat CVC soit mis à jour). Cela présente un certain nombre d'avantages pour l'opérateur, mais ces avantages devraient être soigneusement pesés au regard des risques d'attaque en répétition du fichier de code.

Une autre approche serait de signer le fichier de code précédent avec une date de signature égale ou supérieure à la date de signature de la dernière mise à niveau.

11.3.8 Sécurité physique

La présente application exige que le service portail assure la maintenance, dans sa mémoire, des clés et autres variables cryptographiques se rapportant à la sécurité du réseau. Tous les éléments et appareils DOIVENT empêcher l'accès physique non autorisé à ce matériel cryptographique.

Le niveau de protection physique du matériau de clé exigé pour les éléments de réseau et appareils est spécifié en termes de niveaux de sécurité dans le document FIPS PUBS 140-2, exigences de sécurité pour les modules cryptographiques, norme [FIPS 140-2]. En particulier, les éléments DOIVENT satisfaire les exigences du niveau 1 de sécurité de la norme FIPS PUBS 140-2.

Le niveau 1 de sécurité de la norme FIPS PUBS 140-2 exige une protection physique minimale par l'utilisation d'enceintes de qualité de production et de bonnes pratiques de logiciel.

12 Traitement de la gestion

12.1 Introduction/Aperçu général

Le présent paragraphe donne des exemples de traitements associés à l'utilisation des outils décrits au paragraphe 6 (Outils de gestion) et des traitements supplémentaires qui facilitent d'autres fonctions obligatoires de gestion définies dans la présente Recommandation. L'accès à la base de données des services portail et d'autres opérations des services portail du portail de gestion câble (CMP) sont décrites au paragraphe 6. Les règles types d'accès à une base MIB figurent au § 6.3.6.

Les processus relatifs à la gestion et d'autres processus descriptifs sont fournis pour les scénarios suivants:

- traitement des outils de gestion;
- fonctionnement du portail CTP:
  - essai à distance de vitesse de connexion;
  - essai Ping à distance;
- fonctionnement des services portail;
- accès à la base de données des services portail;
- reconfiguration:
  - téléchargement de logiciel de service portail;
  - téléchargement de fichier de configuration de service portail;
- accès à la base MIB;
- configuration du modèle VACM;
- configuration de messagerie d'événements de gestion:
  - fonctionnement de la notification d'événement de portail CMP;
  - fonctionnement du ralentissement et de la limitation d'événements de portail CMP.

12.1.1 Objectifs

Le présent paragraphe est d'abord composé d'un texte informatif, destiné à aider le lecteur à comprendre, et il ne contient aucune exigence. Les exemples décrivent l'utilisation des outils de gestion pour l'accomplissement des fonctions de gestion typiques. Des tableaux de séquences des processus supplémentaires se rapportant à la gestion (c'est-à-dire, ceux qui ne sont pas définis au paragraphe 6) sont également fournis, y compris les processus de gestion ou les étapes des processus associés à l'utilisation des outils de gestion obligatoires. Tous les processus indiqués impliquent l'interaction de l'élément de service portail avec les têtes de systèmes.

12.2 Processus d'outils de gestion

Les processus d'outils de gestion sont ceux qui sont associés aux outils de gestion obligatoires définis au paragraphe 6.

12.2.1 Fonctionnement du portail CTP

Le portail d'essai câble (CTP) fournit des fonctions d'essai à distance de vitesse de connexion et d'essai Ping à distance, décrites respectivement au § 6.4.3.1 et au § 6.4.3.2.

12.2.1.1 Essai à distance de vitesse de connexion

L'essai à distance de vitesse de connexion peut être utile pour valider les niveaux de performance, identifier les erreurs possibles de configuration, et déterminer d'autres caractéristiques tournant autour des performances (voir Figure 28).

- Le système de gestion de réseau (NMS) débute l'essai en initialisant les paramètres d'essai et en mettant le fanion de début d'essai, via la demande SET du protocole SNMP.
- L'agent SNMP de portail CMP met à jour la base de données de service portail avec les paramètres d'essai et notifie au portail CTP de commencer l'essai.
- Le portail CTP interroge la base de données de service portail pour les paramètres d'essai.
- Le portail CTP produit une rafale de paquets UDP au port 7 de l'appareil IP de LAN spécifié. Le port 7 est réservé pour le service d'écho.
- L'appareil IP de LAN cible fait simplement écho en retour au portail CTP de la charge utile de paquet UDP.
- Une fois que tous les paquets ont été reçus, ou que la période de temporisation de l'essai est arrivée à expiration, le portail CTP met à jour la base de données du service portail avec les résultats de l'essai et met le fanion Essai terminé.
- Le système NMS vérifie que la commande est terminée en vérifiant que Etat = terminé.
- Le système NMS demande les résultats des essais via la demande GET du protocole SNMP.
- L'agent SNMP de portail CMP interroge la base de données du service portail sur les résultats d'essai et en fait rapport dans la réponse GET du protocole SNMP. Si l'essai ne s'est pas terminé, les données de l'essai indiqueront que l'essai est toujours en cours. Le système NMS doit répéter la demande GET de SNMP jusqu'à ce que les résultats de l'essai indiquent que l'essai est terminé.

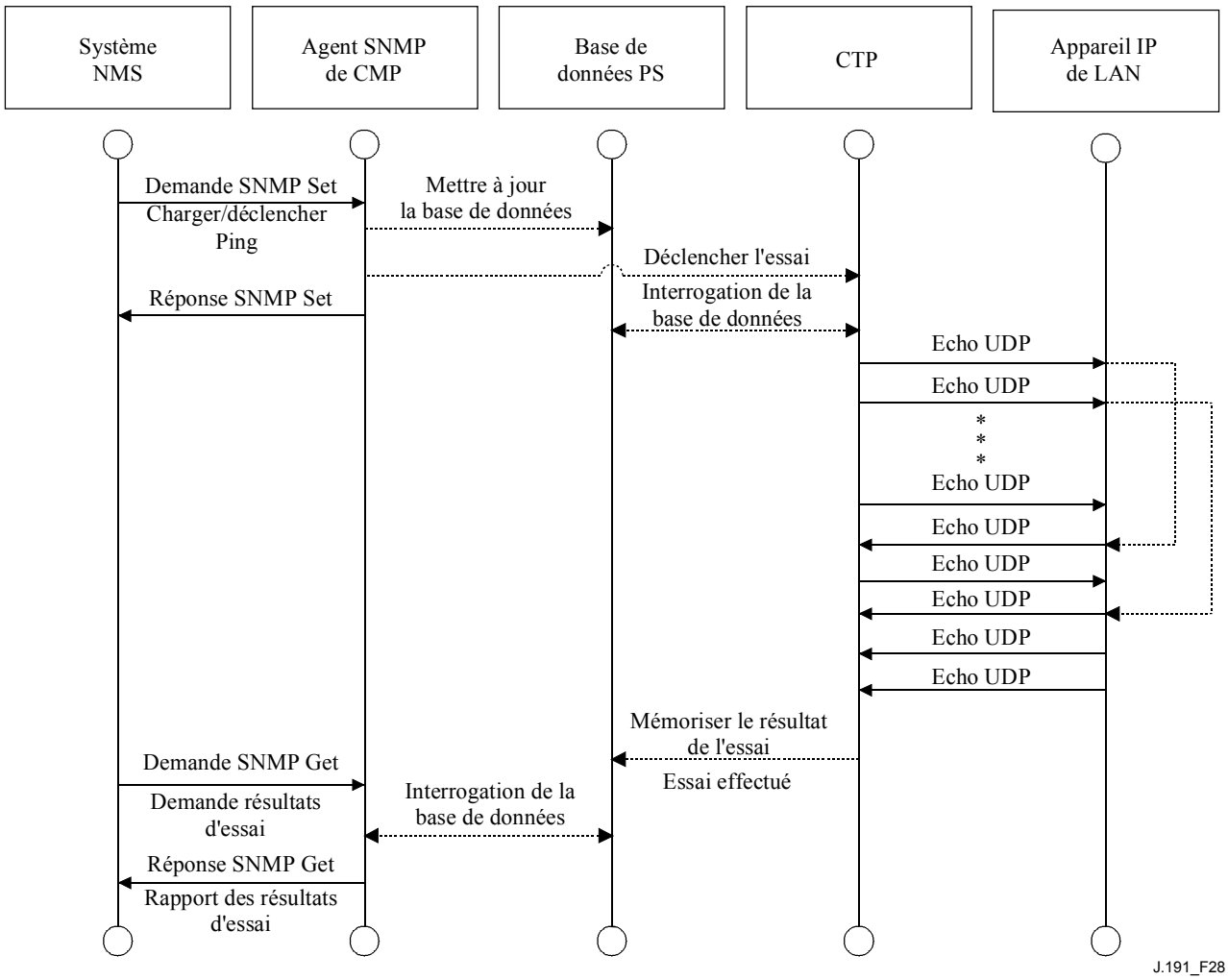

Figure 28/J.191 – Diagramme de la séquence d'essai de vitesse de connexion

12.2.1.2 Essai Ping à distance

L'essai Ping à distance peut être utile pour la validation de l'état de connectivité, les niveaux de performance, et l'identification d'erreurs de configuration possibles (voir Figure 29).

- Le système NMS débute l'essai en initialisant les paramètres d'essai et en mettant le fanion début d'essai, via la demande SET du protocole SNMP.
- L'agent SNMP de portail CMP met à jour la base de données du service portail avec les paramètres d'essai et notifie au portail CTP de commencer l'essai.
- Le portail CTP interroge la base de données du service portail sur les paramètres d'essai.
- Le portail CTP produit un paquet demande d'écho ICMP auprès de l'appareil IP de LAN spécifié.
- L'appareil IP de LAN cible répond avec une réponse d'écho ICMP.
- Le portail CTP met à jour la base de données du service portail avec les résultats de l'essai et met le fanion Essai terminé.
- Le système NMS vérifie que la command est exécutée en vérifiant que Etat = terminé.
- Le système NMS demande les résultats de l'essai via la demande GET du protocole SNMP.

- L'agent SNMP du portail CMP interroge la base de données du service portail sur les résultats de l'essai et en fait rapport dans la réponse GET du protocole SNMP. Si l'essai n'est pas terminé, les données d'essai indiqueront que l'essai est toujours en cours. Le système NMS doit répéter la demande GET de SNMP jusqu'à ce que les résultats d'essai indiquent que l'essai est terminé.

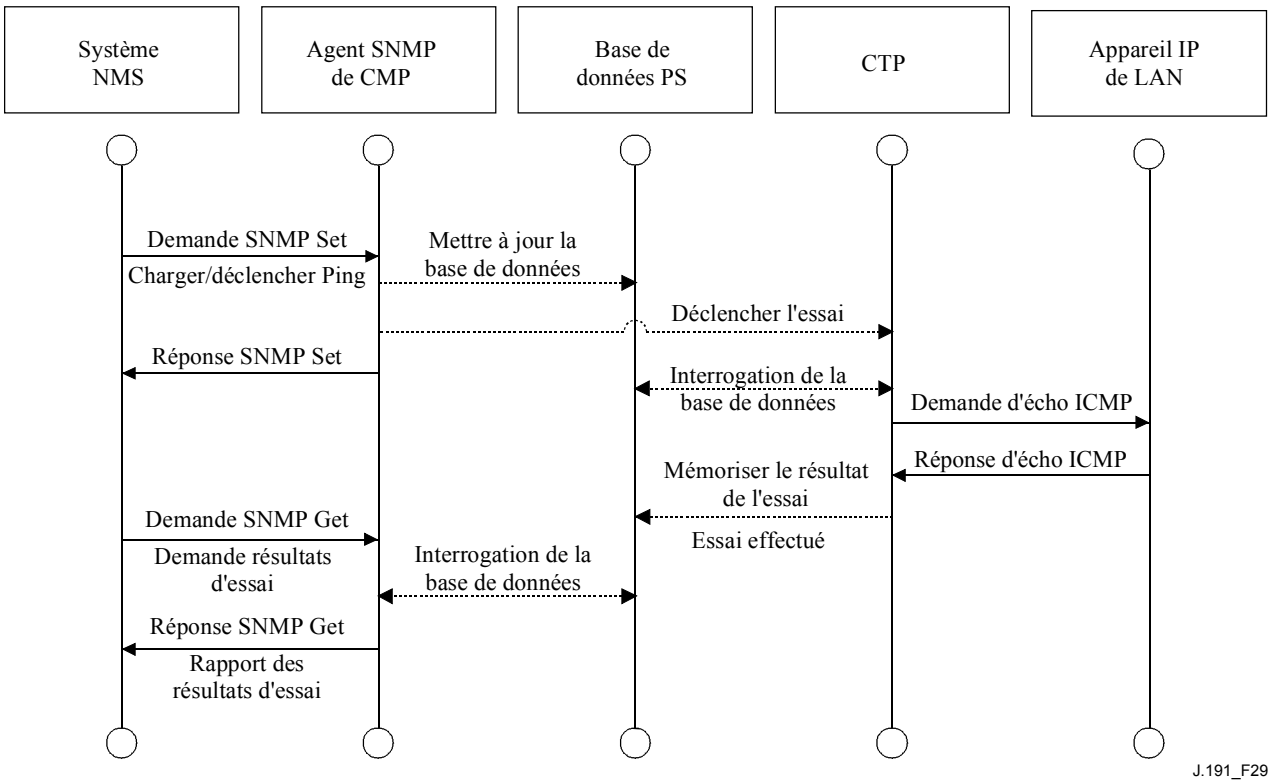

Figure 29/J.191 – Diagramme de la séquence d'essai Ping à distance

12.3 Fonctionnement du service portail

Le portail de gestion câble (CMP) donne accès à la base de données du service portail via l'interface WAN-Man du service portail, comme décrit au paragraphe 6. La séquence de messages pour un fonctionnement à distance d'accès à une base de donnée de service portail à partir de l'interface WAN-Man de service portail est décrite ci-dessous.

12.3.1 Accès à une base de données de service portail

Le système NMS accède aux paramètres de configuration et de gestion mémorisés dans la base de données du service portail via les bases MIB SNMP. Les paramètres sont récupérés en utilisant les messages Get Request, Get Next Request, et Get Bulk du protocole SNMP produits par le système NMS avec l'adresse WAN-Man du service portail comme adresse de destination. Des paramètres peuvent être modifiés et des actions (comme les essais de vitesse de connexion et le Ping à distance) exécutées par le système NMS en produisant des messages Set Request du protocole SNMP avec les paramètres appropriés, à l'adresse WAN-Man du service portail.

La Figure 30 décrit les séquences de messages de gestion pour un accès de base de données de service portail typique à partir d'une interface WAN-Man de service portail. Les séquences de messages supposent qu'une liaison SNMPv3 sécurisée a été établie.

- Le système NMS lit les données sur la base de données du service portail en utilisant la demande GET du protocole SNMP. La demande fait la liste des objets spécifiques que le système NMS veut dans la base de données.
- L'agent SNMP du portail CMP interroge la base de données du service portail sur les paramètres spécifiés.
- Le portail CMP SNMP rapporte les données au système NMS avec la réponse GET du protocole SNMP.

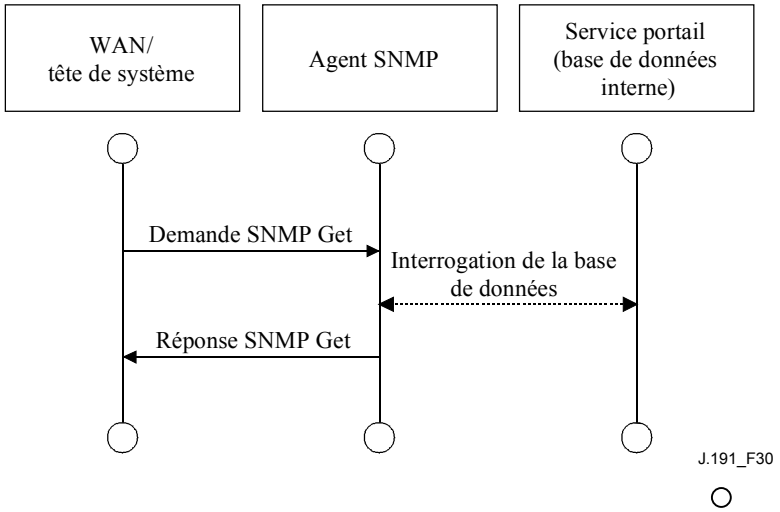

Figure 30/J.191 – Diagramme de séquences de l'accès de base de données de service portail à partir de l'interface WAN-Man PS

12.3.2 Reconfiguration

12.3.2.1 Téléchargement de logiciel au service portail

L'exemple dans la Figure 31 illustre un processus de téléchargement de logiciel/microprogramme pour un service portail en mode d'approvisionnement SNMP. Ce processus est déclenché par le système NMS. Il est indiqué au service portail où obtenir le nouveau logiciel de fichier de code. Une fois le téléchargement du fichier de code achevé, le service portail va tester la copie pour chercher toute altération qui aurait pu survenir pendant le téléchargement. L'authentification est effectuée pour vérifier que le fichier de code est de confiance. Après cette étape, un réamorçage du système est effectué.

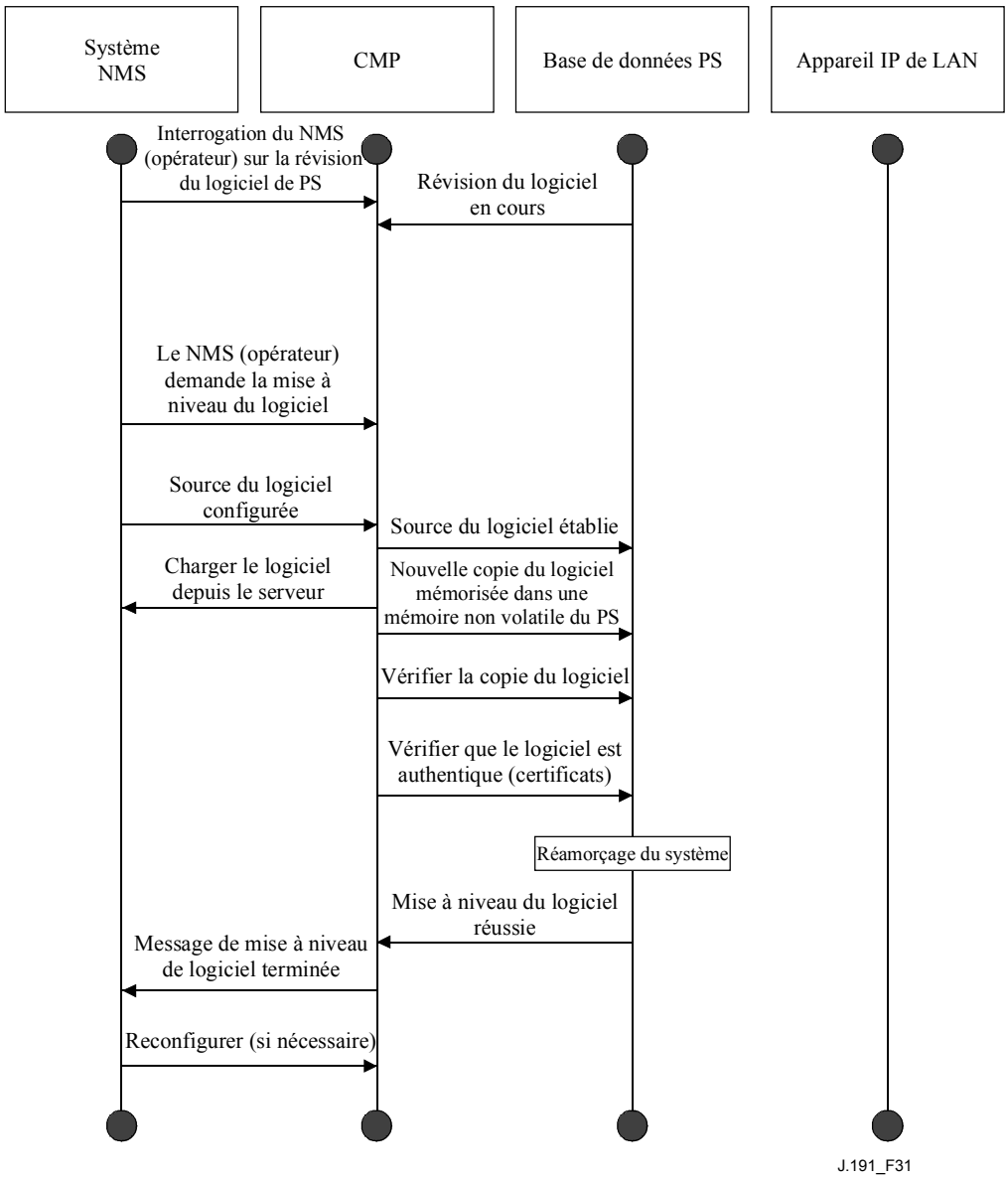

Figure 31/J.191 – Diagramme de séquence de téléchargement de logiciel au service portail

Après ce réamorçage, le service portail arrête de fonctionner sur la nouvelle copie de logiciel. Le service portail peut avoir besoin d'être reconfiguré après la mise à niveau de logiciel, et les interfaces WAN peuvent avoir besoin d'être approvisionnées à nouveau (non montré dans l'exemple). Si le service portail n'accepte pas la nouvelle copie du logiciel, il va revenir à la précédente version de logiciel (sauvegarde) et faire rapport au système NMS de ce qui est arrivé.

12.3.2.2 Téléchargement de fichier de configuration au service portail

L'exemple dans la Figure 32 illustre une reconfiguration de service portail en mode d'approvisionnement SNMP, via le téléchargement d'un fichier de configuration. Ce processus est déclenché par le système NMS. Le fichier de configuration est donné au service portail en écrivant le serveur de fichier et le nom de fichier dans le service portail, et en déclenchant le téléchargement du fichier par le service portail. Une fois chargé le fichier de configuration, les commandes contenues sont interprétées. Si l'une des commandes n'est pas comprise ou n'est pas applicable, elle est sautée et un événement est généré. Lorsque le service portail a terminé de traiter le fichier de configuration, il va enregistrer le nombre de couples de TLV traités et sautés dans les objets de base MIB appropriés.

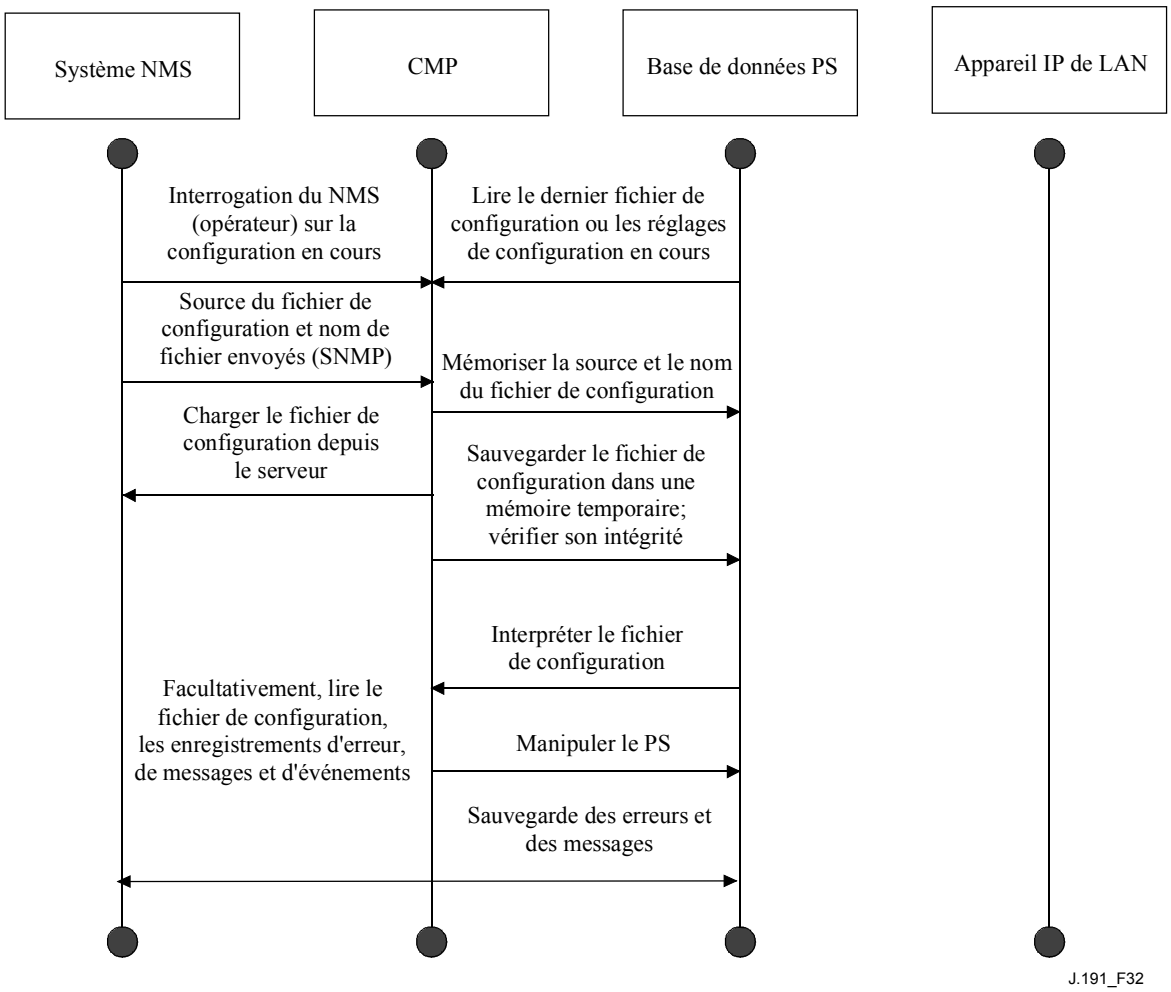

Figure 32/J.191 – Diagramme de séquence de reconfiguration de service portail (téléchargement de fichier de configuration)

12.4 Accès de base MIB

12.4.1 Configuration du modèle VACM

Le câblo-opérateur a le contrôle du domaine de gestion. Un exemple de la configuration des paramètres du modèle VACM est donné dans la Figure 33.

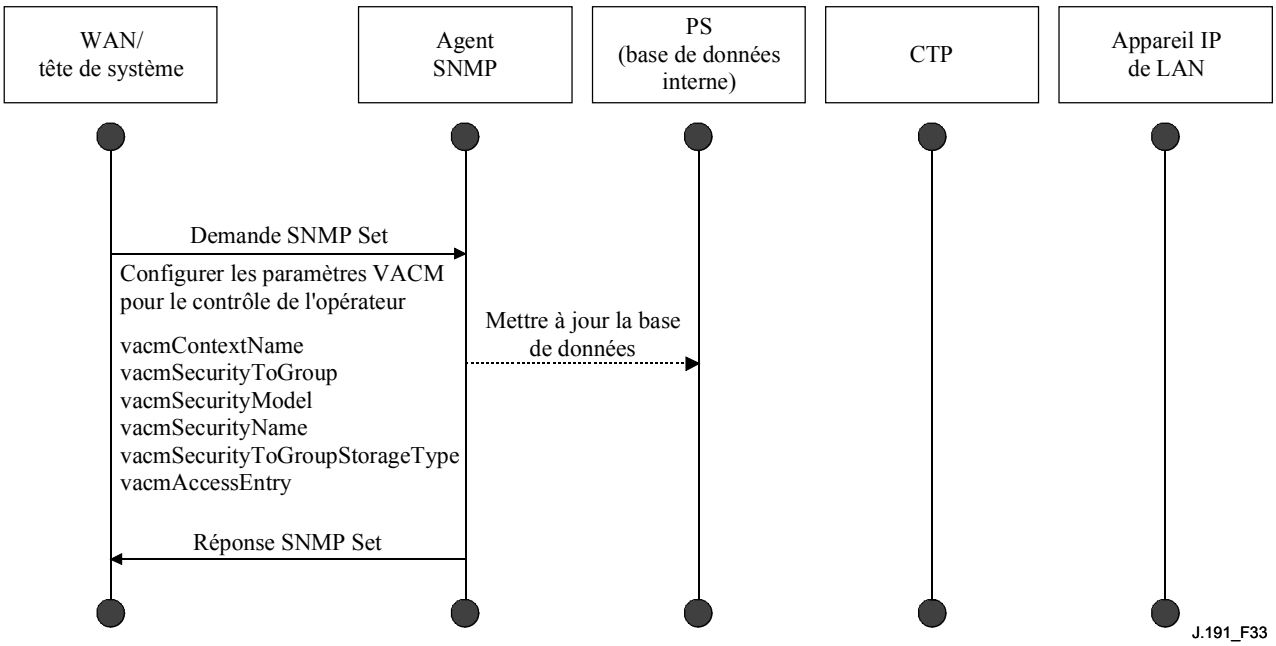

Figure 33/J.191 – Séquence de configuration de service portail (paramètres VACM)

12.4.2 Configuration de messagerie d'événement de gestion

12.4.2.1 Fonctionnement de la notification d'événement au portail CMP

Les événements sont rapportés au moyen d'enregistrements d'événements locaux, de messages SNMP TRAP, SNMP INFORM, et de SYSLOG. Le mécanisme de notification d'événement peut être établi ou modifié par le système NMS, en produisant un message de demande SET du protocole SNMP à l'adresse WAN-Man du service portail.

L'exemple dans la Figure 34 illustre la façon de configurer la base de données du service portail pour mémoriser les événements dans les fichiers d'enregistrement locaux. Les événements d'enregistrement local sont de deux types: local non volatile et local volatile. Le système NMS lira le contenu de l'enregistrement local et écrira ce contenu sur le système d'enregistrement d'événements de la tête de système. Un réamorçage du service portail ne provoque l'effacement que des événements volatiles de la base de données du service portail. Les événements non volatiles persistent à travers les réamorçages.

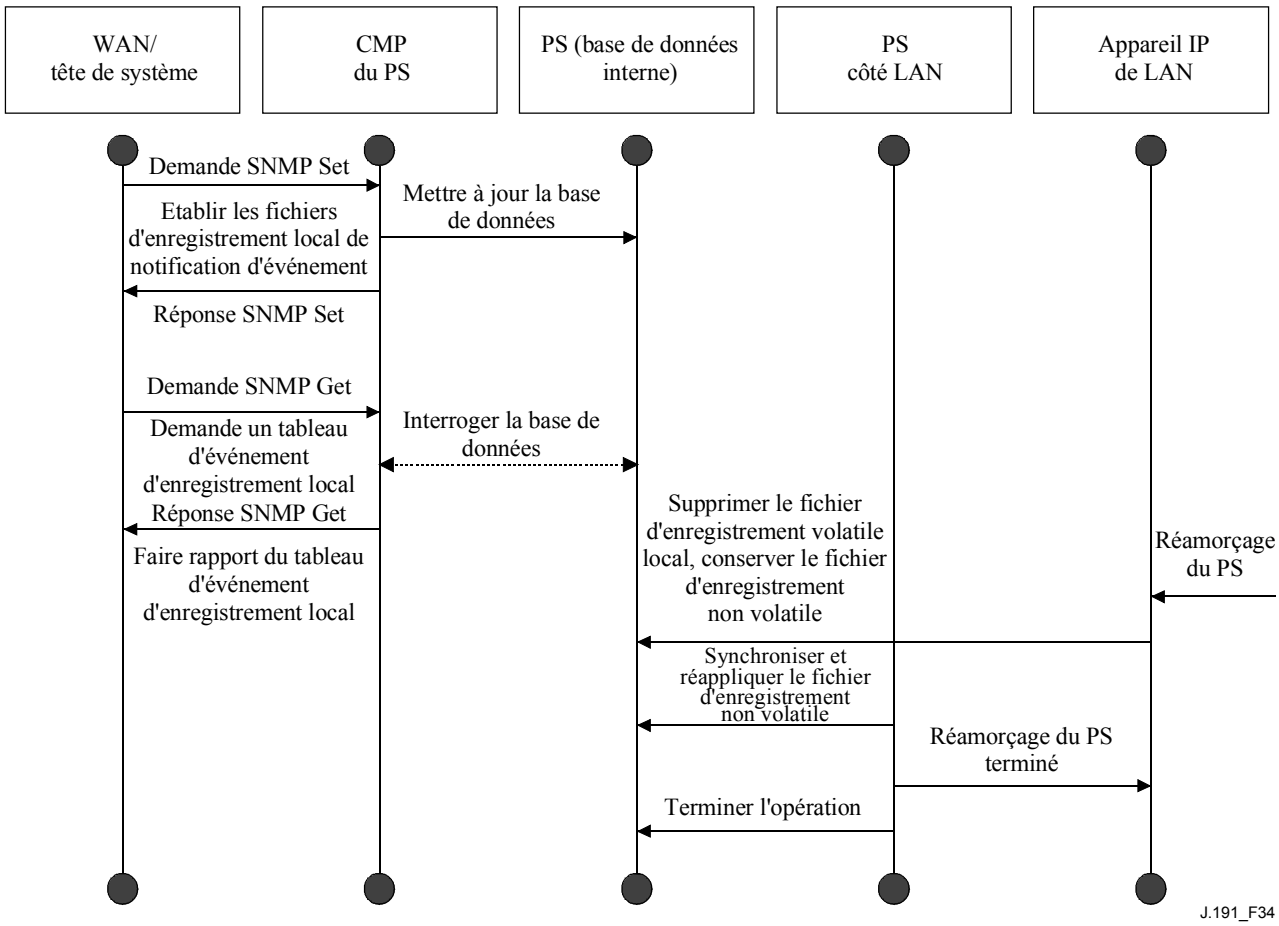

Figure 34/J.191 – Séquence de configuration de service portail (contrôle d'événement)

Le scénario dans la Figure 35 illustre le téléchargement d'un fichier de configuration pour un service portail en mode d'approvisionnement SNMP. Ce processus est déclenché via une demande SET du protocole SNMP. Le service portail doit vérifier ce fichier avant de l'accepter. Dans l'exemple, il existe une erreur de TLV dont il est fait rapport. Dans la mesure où la notification d'événement est mise au mode TRAP du protocole SNMP, l'adresse du serveur TRAP est récupérée sur la base de données du service portail et l'événement est envoyé au serveur TRAP.

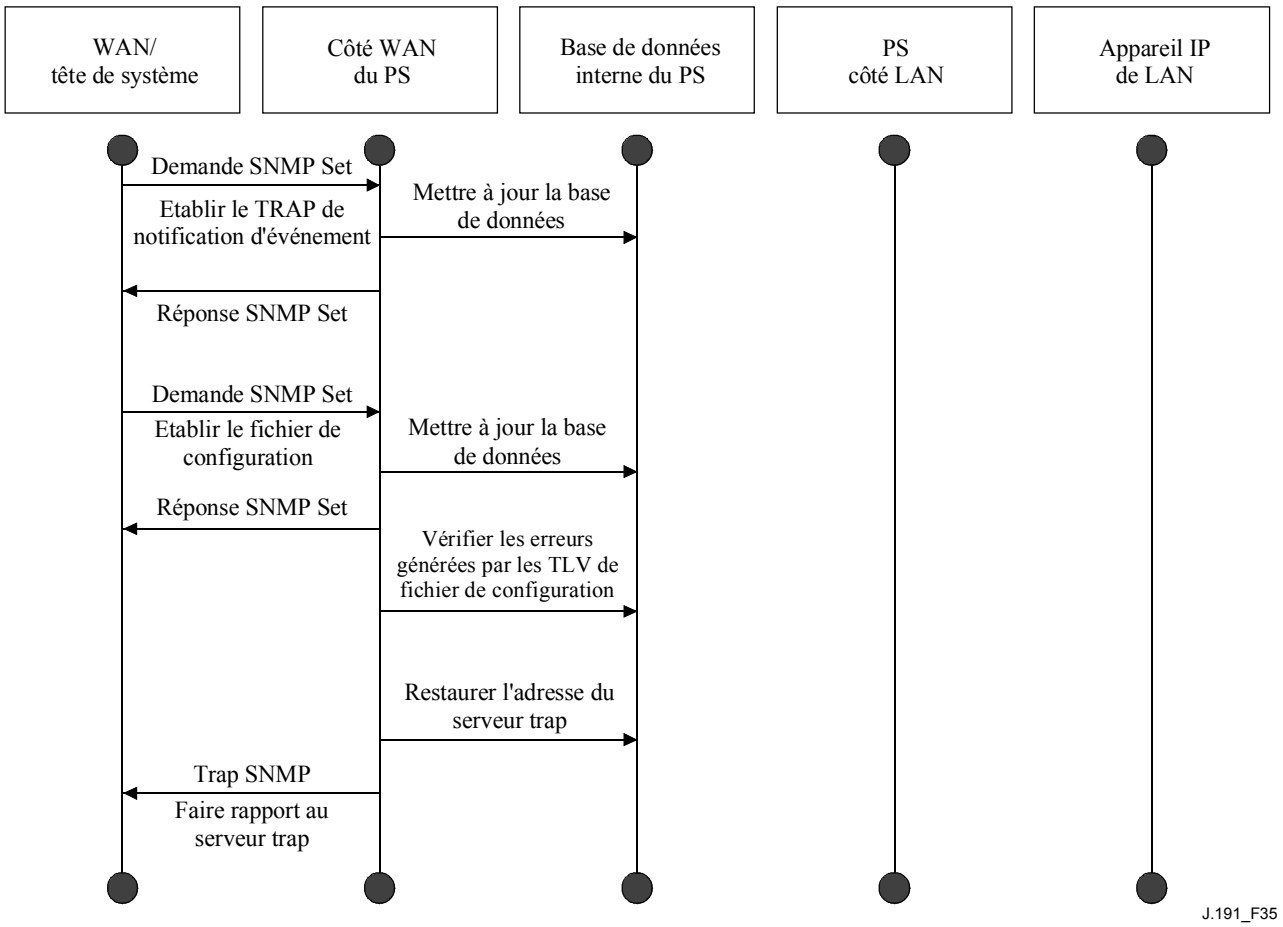

Figure 35/J.191 – Séquence de téléchargement de fichier de configuration de service portail (avec des TLV non valides)

L'exemple dans la Figure 36 illustre le processus d'un appareil IP de LAN essayant d'obtenir une adresse IP du serveur DHCP (CDS). La fonction de serveur CDS vérifie la base de données du service portail pour trouver une adresse IP disponible. Dans ce cas, le serveur CDS détecte qu'il n'y a pas d'adresse IP disponible dans le groupe d'adressage, et il génère un événement à SYSLOG.

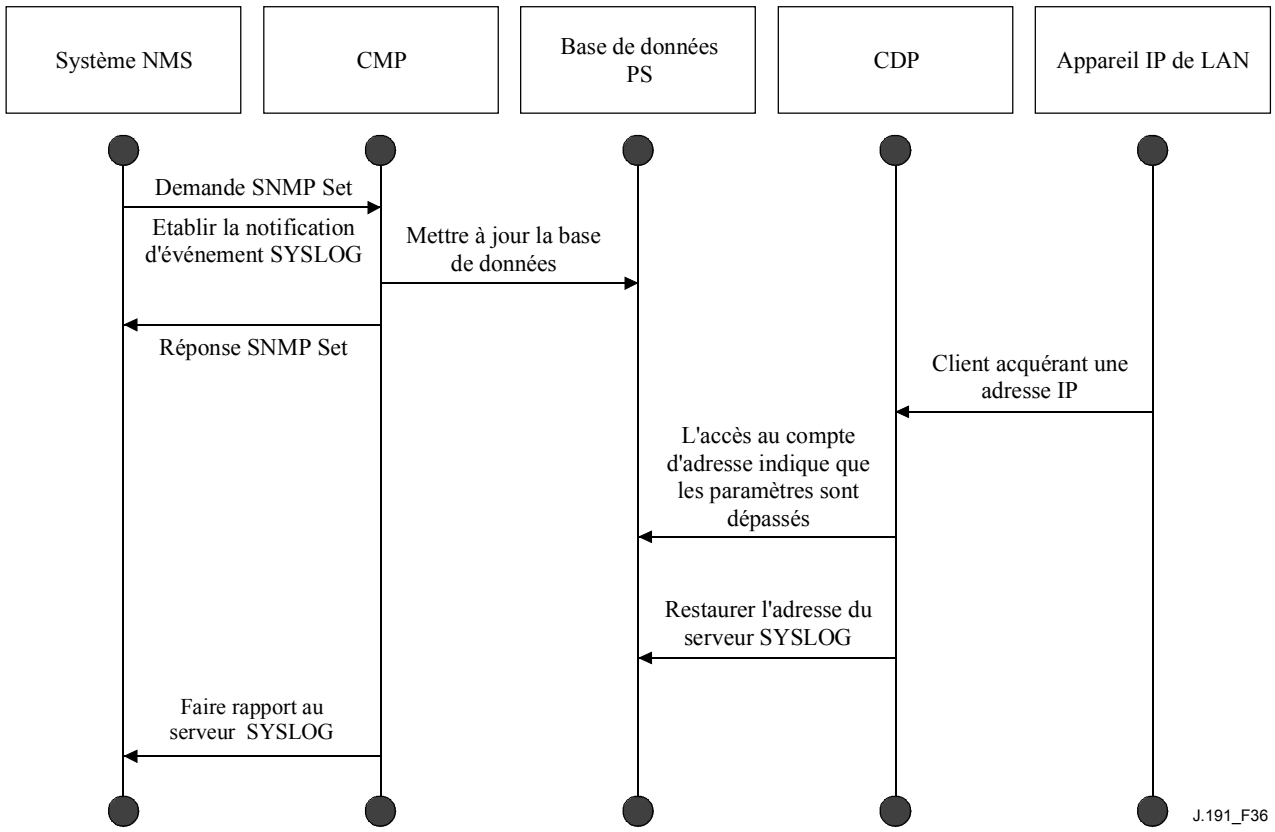

Figure 36/J.191 – Séquence d'acquisition d'adresse d'appareil IP de LAN (demande excédant le compte prévu)

12.4.2.2 Exemple de fonctionnement de ralentissement et de limitation d'événements au portail CMP

Un mécanisme de ralentissement d'événement est fourni via la fonctionnalité de portail CMP du service portail. Le ralentissement et la limitation d'événement est très souple et peut inclure des cas dans lesquels les événements sont rapportés et des cas dans lesquels aucun événement n'est rapporté au système NMS. Se reporter à la Figure 37 pour une description du mécanisme de ralentissement et de limitation d'événements au portail CMP.

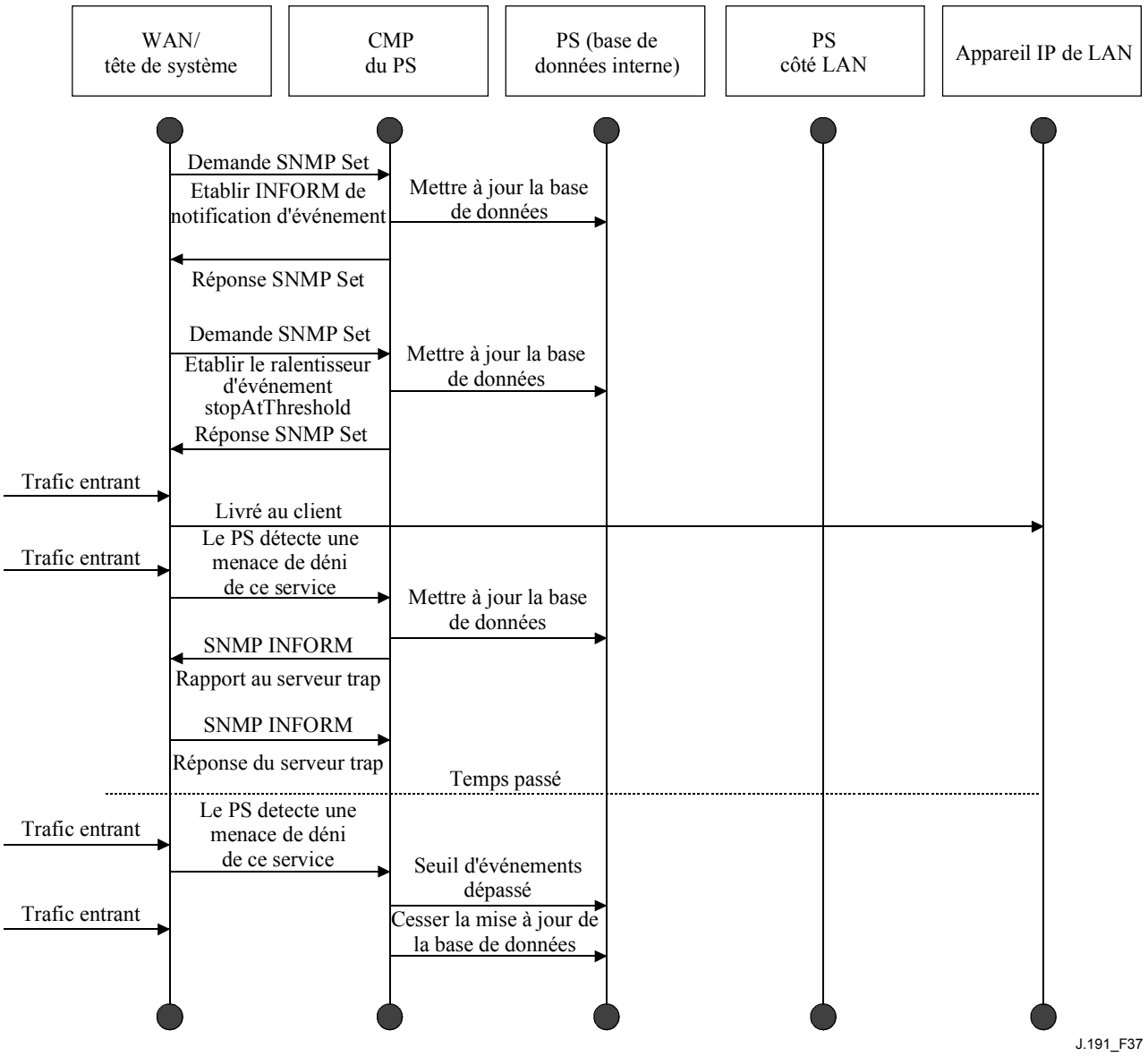

Figure 37/J.191 – Fonctionnement du ralentissement et limitation d'événements au portail CMP

L'exemple fourni dans la Figure 37 illustre la configuration de la base de données du service portail pour retourner des événements via la méthode INFORM du protocole SNMP. Au départ, plusieurs messages INFORM sont écrits au fichier d'enregistrement local et livrés au système NMS. Le mécanisme de ralentissement d'événements fixe la limite du nombre d'événements qui peuvent être envoyés au système NMS dans un laps de temps donné. Lorsque cette limite est atteinte, le service portail arrêtera d'envoyer des messages INFORM au système NMS. Pour redémarrer la notification d'événements, le système NMS devra réactiver le rapport d'événements.

13 Processus d'approvisionnement

Le présent paragraphe décrit les processus impliqués lors de l'utilisation des outils d'approvisionnement, décrits au paragraphe 7, pour l'approvisionnement initial de l'appareil IP de LAN et de l'élément de service portail. L'approvisionnement recouvre les trois tâches suivantes:

1) acquisition des adresses réseau;

2) acquisition des informations de serveur;

3) téléchargement sécurisé et traitement du fichier de configuration du service portail.

Les processus d'approvisionnement sont décrits dans le présent paragraphe pour chacun des cas pertinents suivants:

- WAN-Man de service portail – Approvisionnement de la fonctionnalité de gestion fondée sur le WAN du service portail.
- WAN-Data de service portail – Approvisionnement des adresses IP WAN-Data de service portail à utiliser pour la création des mappages de traduction CAT avec les appareil IP de LAN dans le secteur d'adresse LAN-Trans.
- Appareil IP de LAN dans le secteur LAN-Trans – Approvisionnement d'appareil IP de LAN avec une adresse IP traduite.
- Appareil IP de LAN IP dans le secteur LAN-Pass – Approvisionnement d'appareil IP de LAN avec une adresse IP qui est passée à travers le WAN.

L'approvisionnement de la fonctionnalité de câblo-modem est séparée et distincte de l'approvisionnement de service portail et est en dehors du domaine d'application de la présente Recommandation. Le lecteur est prié de se reporter aux spécifications DOCSIS pour les descriptions de l'approvisionnement des câblo-modems.

Les éléments fonctionnels dont la liste figure ci-dessus avec lesquels interagit l'élément de service portail pendant les processus d'approvisionnement sont identifiés dans la Figure 38. L'élément fonctionnel de centre de distribution de clés (KDC, *key distribution center*) est indiqué en pointillés dans la mesure où il est utilisé dans le mode d'approvisionnement SNMP mais pas en mode d'approvisionnement DHCP. Les autres éléments fonctionnels sont utilisés dans les deux modes d'approvisionnement.

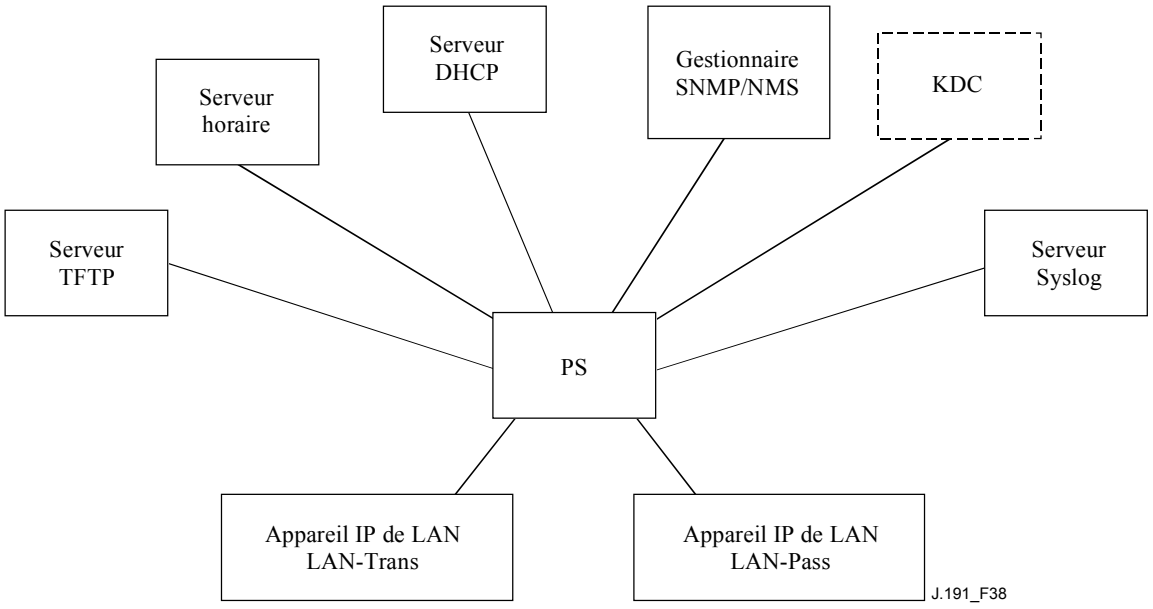

Figure 38/J.191 – Eléments fonctionnels d'approvisionnement

Le serveur du protocole trivial de transfert de fichier (TFTP, *trivial file transfer protocol*) donne accès au fichier de configuration du service portail pour le service portail et suit les règles décrites dans la norme [RFC 1350]. Le serveur horaire (TOD) fournit au service portail les moyens d'acquérir l'heure courante en format UTC, comme décrit dans la norme [RFC 868]. Le serveur de protocole de configuration de serveur dynamique (DHCP, *dynamic host configuration protocol*) fournit au service portail les adresses IP privées et/ou mondiales selon la norme [RFC 2131] et fournit également d'autres informations via des options du protocole DHCP conformément à la norme [RFC 2132]. Le système de gestion de réseau (NMS)/gestionnaire du protocole simple de gestion de réseau (SNMP) se conforme à la norme [RFC 1157] et éventuellement avec les versions les plus courantes du protocole SNMP, par exemple [RFC 2571], [RFC 2572], [RFC 2574], et [RFC 2575]. Le centre de distribution de clés (KDC) gère les clés d'autorisation et de chiffrement pour l'établissement de la confiance entre les éléments de réseau et implémente les règles définies dans la norme [RFC 1949]. Le serveur d'enregistrement système (SYSLOG) traite les messages d'événement générés par le service portail et les appareils IP de LAN au domicile. Le service portail implémente les clients de ces serveurs de tête de système, et utilise ces fonctions client pendant les processus d'approvisionnement décrits dans le présent paragraphe pour accomplir les tâches dont la liste figure au début de ce paragraphe.

13.1 Modes d'approvisionnement

Les § 5.7 et 7.1.1 introduisent deux modes d'approvisionnement acceptés par l'élément de service portail: le mode d'approvisionnement DHCP et le mode d'approvisionnement SNMP. Dans le présent paragraphe, chacun des deux modes est présenté plus en détails. La Figure 39 illustre un flux d'événements possible pour les deux modes d'approvisionnement. Le point clé de la Figure 39 est le commutateur utilisé par le service portail pour déterminer le mode d'approvisionnement dans lequel il doit fonctionner.

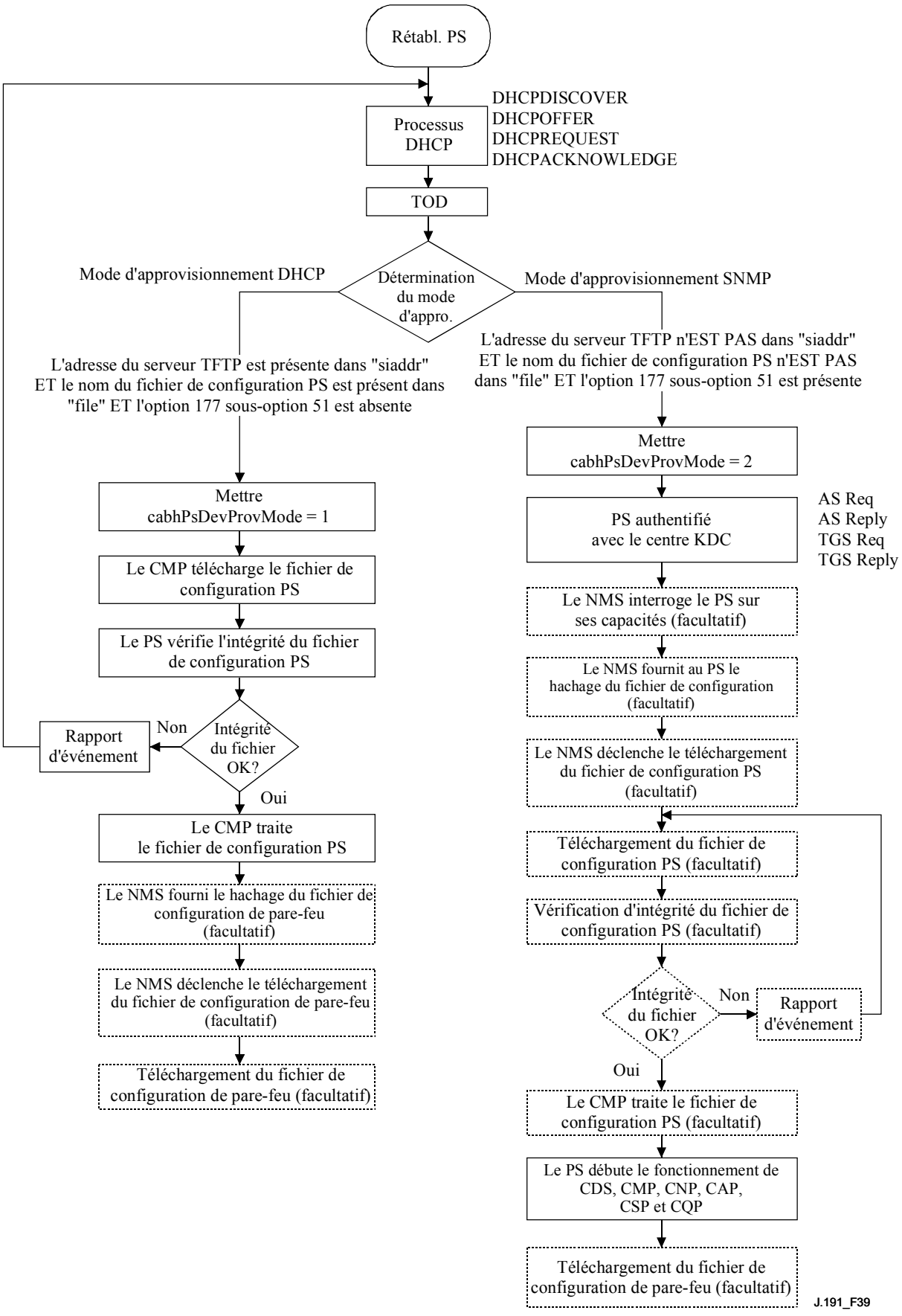

Figure 39/J.191 – Modes d'approvisionnement

Le service portail fonctionne en mode d'approvisionnement DHCP (mode DHCP) si le serveur DHCP dans le réseau câblé fournit une adresse IP valide pour le serveur TFTP dans le champ "siaddr" du message DHCP, s'il fournit un nom de fichier valide pour le fichier de configuration du service portail dans le champ "file" du message DHCP, et s'il NE fournit PAS l'option 177 sous-option 51 du protocole DHCP au client CDC du service portail, pendant la phase DHCPOFFER du processus d'initialisation. Le mode d'approvisionnement DHCP est conçu pour permettre au service portail de fonctionner sur une infrastructure qui ne comporte pas de caractéristiques IPCablecom évoluées.

Le mode d'approvisionnement SNMP dans le service portail est déclenché lorsque le serveur DHCP du réseau câblé NE fournit PAS de valeurs pour les champs "siaddr" et "file", et lorsque le serveur DHCP du réseau câblé NE fournit PAS l'option 177 sous-option 51 du protocole DHCP. Le mode d'approvisionnement SNMP est conçu pour permettre au service portail de tirer parti des caractéristiques évoluées d'une architecture IPCablecom.

13.2 Processus d'approvisionnement du PS pour la gestion: mode d'approvisionnement DHCP

Le service portail demande au système d'approvisionnement de la tête de système une adresse IP à utiliser pour l'échange de messages de gestion entre le système NMS et le service portail. Le service portail fait une analyse grammaticale du message DHCP retourné dans le DHCP OFFER et prend une décision quant au mode d'approvisionnement dans lequel il doit fonctionner (voir § 7.2.3.3). Le § 7.2.2.2.1 décrit deux modes d'adresse WAN acceptés pour l'acquisition d'adresses IP par le service portail de la part du serveur DHCP dans le réseau câblé.

Si le service portail prend la décision de fonctionner en mode d'approvisionnement DHCP, il utilisera les informations du fichier de configuration du service portail passées dans le message DHCP comme déclenchement du téléchargement du fichier de configuration du service portail, comme décrit au § 7.2. Le téléchargement de fichier de configuration est une exigence pour le service portail fonctionnant en mode d'approvisionnement DHCP mais il est facultatif pour le service portail fonctionnant en mode d'approvisionnement SNMP. Après le téléchargement initial du fichier de configuration du service portail déclenché par les champs de messages DHCP, le système NMS peut initialiser une configuration d'après approvisionnement en produisant une demande Set du protocole DHCP pour les objets de base MIB cabhPsDevProvConfigHash et cabhPsDevProvConfigFile comme décrit au § 7.3.

En mode d'approvisionnement DHCP, le service portail (CMP) utilise par défaut le mode NmAccess pour l'échange de messages de gestion avec le système NMS, mais le système NMS a la faculté de configurer le portail CMP pour le mode coexistence. Ces modes de messagerie de gestion sont décrits au § 6.3.3.

La Figure 40 et le Tableau 48 décrivent la séquence des messages nécessaires pour initialiser un service portail fonctionnant en mode d'approvisionnement DHCP. L'approvisionnement du service portail NE DOIT PAS survenir avant le processus d'approvisionnement du câblo-modem.

Le processus facultatif de téléchargement d'un fichier de configuration de pare-feu est montré en grisé sur la Figure 40.

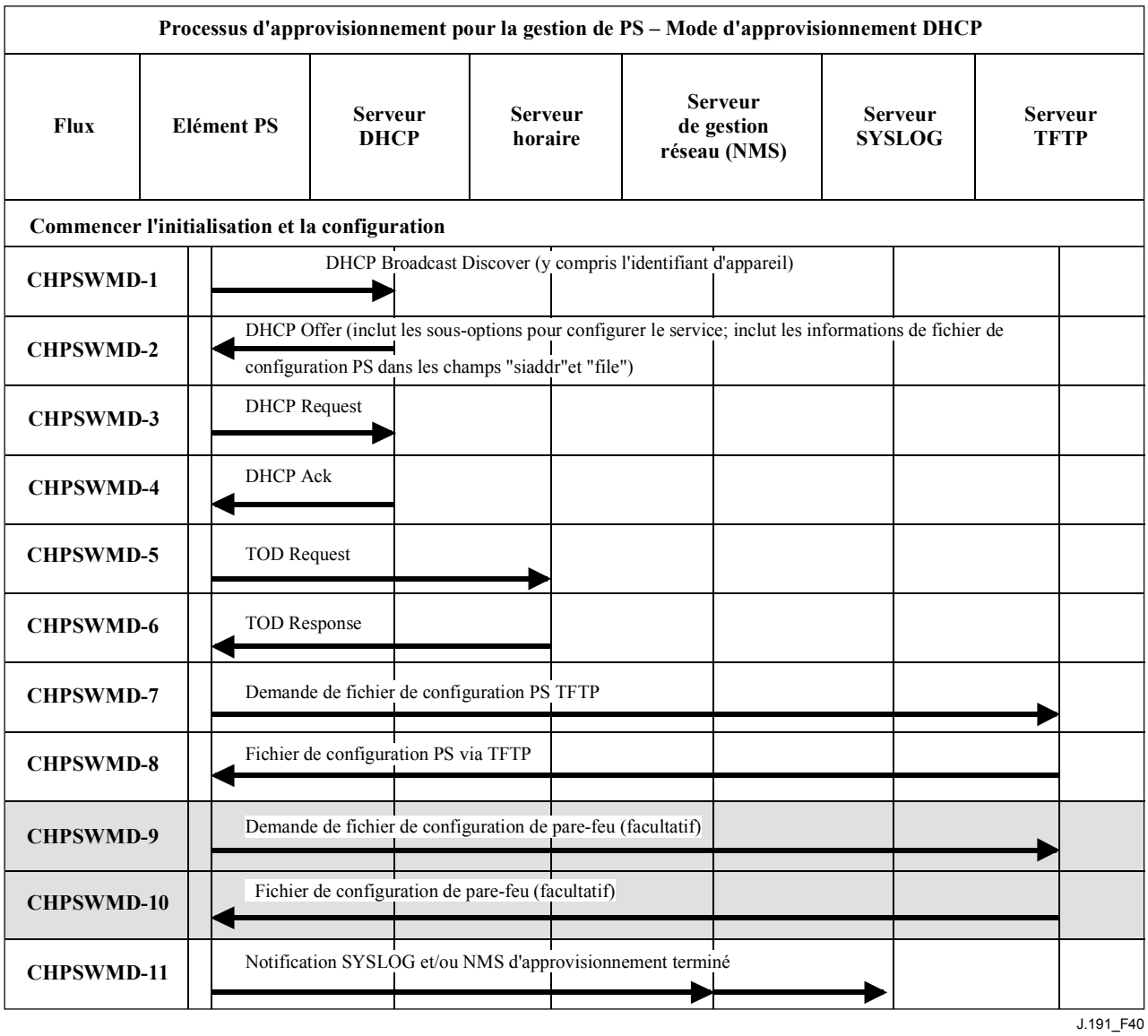

Figure 40/J.191 – Processus d'approvisionnement pour la gestion de PS – Mode d'approvisionnement DHCP

Le Tableau 48 décrit les messages individuels CHPSWMD-1 à CHPSWMD-11 montrés à la Figure 40.

Tableau 48/J.191 – Description des flux pour le processus d'approvisionnement WAN-Man du service portail pour le mode d'approvisionnement DHCP

Etape du flux	Approvisionnement WAN-Man du PS: mode d'approvisionnement DHCP	Séquence normale	Séquence d'échec
CHPSWMD-1	*DHCP Broadcast Discover* Le CDP (CDC) DOIT envoyer un message DHCP DISCOVER en diffusion. La diffusion du DHCP DISCOVER par le CDP (CDC) DOIT inclure les options obligatoires dont la liste figure au Tableau 21. Le service portail DOIT lancer le temporisateur d'approvisionnement en utilisant la valeur de début accessible via cabhPsDevProvTimer ET mettre cabhPsDevProvState à l'état "inProgress" (2) lorsque le CDC envoie un DHCP DISCOVER en diffusion.	Commencer la séquence d'approvisionnement.	En cas d'échec selon le protocole DHCP, rapporter une erreur et continuer d'essayer DHCP Broadcast Discover jusqu'à réussite (retourner à l'étape CHPSWMD-1). Après 5 essais le PS initialise le fonctionnement du serveur CDS comme précisé au § 7.2.3.3.
CHPSWMD-2	*DHCP OFFER (offre DHCP)* Le message DHCP OFFER produit par le serveur DHCP dans les réseaux câblés est censé ne pas inclure l'option de code 177 avec la sous-option 51 ET est censé inclure les informations de fichier de configuration dans les champs "siaddr" et "file" du message DHCP. Le PS modifie cabhPsDevProvMode sur la base des informations reçues dans DHCP OFFER (voir § 7.2.3.3).	CHPSWMD-2 DOIT survenir après achèvement de CHPSWMD-1.	En cas d'échec selon le protocole DHCP, retourner à CHPSWMD-1 et faire rapport d'une erreur.
CHPSWMD-3	*DHCP REQUEST (demande DHCP)* Le CDP DOIT envoyer au serveur DHCP approprié un message DHCP REQUEST pour accepter la DHCP OFFER.	CHPSWMD-3 DOIT survenir après achèvement de CHPSWMD-2.	En cas d'échec selon le protocole DHCP, retourner à CHPSWMD-1 et faire rapport d'une erreur.
CHPSWMD-4	*DHCP ACK (accusé de réception DHCP)* Le serveur DHCP envoie au CDP un message DHCP ACK qui contient l'adresse IPv4 du PS. Le PS DOIT mémoriser l'adresse du serveur d'horaire dans cabhPsDevTimeServerAddr.	CHPSWMD-4 DOIT survenir après achèvement de CHPSWMD-3.	En cas d'échec selon le protocole DHCP, retourner à CHPSWMD-1 et faire rapport d'une erreur.
CHPSWMD-5	*Demande d'heure (TOD) selon [RFC 868]* Le PS DOIT produire une demande d'heure au serveur horaire identifié dans la DHCP OFFER.	CHPSWMD-5 DOIT survenir après achèvement de CHPSWMD-4.	Continuer avec CHPSWMD-6.

Tableau 48/J.191 – Description des flux pour le processus d'approvisionnement WAN-Man du service portail pour le mode d'approvisionnement DHCP

Etape du flux	Approvisionnement WAN-Man du PS: mode d'approvisionnement DHCP	Séquence normale	Séquence d'échec
CHPSWMD-6	*Réponse d'heure* Le serveur horaire est censé répondre avec l'heure courante en format UTC.	CHPSWMD-6 DOIT survenir après achèvement de CHPSWMD-5.	Continuer avec CHPSWMD-7, faire rapport d'une erreur, et retourner à CHPSWMD-5 (continuer d'essayer l'heure jusqu'à réussite).
CHPSWMD-7	*Demande TFTP* Le PS fonctionnant en mode d'approvisionnement DHCP DOIT envoyer au serveur TFTP une demande TFTP Get pour demander le fichier de données de configuration spécifié comme décrit au § 7.3.3.	CHPSWMD-7 DOIT survenir après achèvement de CHPSWMD-5. CHPSWMD-7 PEUT survenir avant l'achèvement de CHPSWMD-6.	Continuer avec CHPSWMD-8.
CHPSWMD-8	*Le serveur TFTP envoie un fichier de configuration de PS* Après réception du fichier de configuration, le hachage du fichier de configuration est calculé et comparé à la valeur annexée au nom du fichier de configuration du PS (se reporter au § 7.3.3.3). Le fichier de configuration du PS est alors traité. Se reporter au § 7.3.3 pour le contenu du fichier de configuration du PS. Facultativement, l'adresse/FQDN IP du serveur TFTP de fichier de configuration de pare-feu, le nom de fichier du fichier de configuration du pare-feu, le hachage du fichier de configuration du pare-feu, et la clé de chiffrement (si le fichier de configuration du pare-feu est crypté) sont inclus dans le fichier de configuration du PS s'il y a un fichier de configuration de pare-feu à charger, et ceci est la méthode choisie pour le spécifier.	CHPSWM-8 DOIT survenir après achèvement de CHPSWM-7.	Si le téléchargement TFTP échoue, faire rapport d'une erreur et retourner à CHPSWMD-7 (continuer d'essayer de télécharger le fichier de configuration PS). Si le traitement du fichier de configuration produit une erreur, continuer CHPSWMD-9 et rapporter l'erreur comme événement. Si le temporisateur d'approvisionnement arrive à expiration avant que le fichier de configuration PS soit bien téléchargé, le PSD DOIT rapporter une erreur et retourner à CHPSWMD-1.

Tableau 48/J.191 – Description des flux pour le processus d'approvisionnement WAN-Man du service portail pour le mode d'approvisionnement DHCP

Etape du flux	Approvisionnement WAN-Man du PS: mode d'approvisionnement DHCP	Séquence normale	Séquence d'échec
CHPSWMD-9	*Demande TFTP – Fichier de configuration de pare-feu (facultatif)* Si le PS reçoit des informations de fichier de configuration de pare-feu (serveur TFTP de pare-feu et nom de fichier de configuration de pare-feu) dans le fichier de configuration PS, le PS envoie au serveur TFTP de configuration de pare-feu une demande TFTP Get pour demander un fichier de configuration de pare-feu (voir le § 11.3.5.1). Si le PS ne reçoit pas d'information de fichier de configuration de pare-feu dans le fichier de configuration PS, le processus d'approvisionnement du PS (mode d'approvisionnement DHCP) DOIT sauter les étapes CHPSWMD-9 et CHPSMWD-10 et continuer avec étape CHPSWMD-11.	Si CHPSWMD-9 survient, il DOIT survenir après achèvement de CHPSWMD-8.	Si TFTP échoue, continuer le fonctionnement du PS mais faire rapport d'une erreur et continuer d'essayer CHPSWMD-9.
CHPSWMD-10	*Le serveur TFTP envoie un fichier de configuration de pare-feu (facultatif)* Si l'étape CHPSWMD-9 survient, le serveur TFTP envoie au PS une réponse TFTP contenant le fichier demandé. Après réception du fichier de configuration de pare-feu, le hachage du fichier de configuration est calculé et comparé à la valeur reçue dans le fichier de configuration du PS. S'il est chiffré, le fichier est déchiffré. Le fichier est alors traité. Se reporter au § 11.3.5.	CHPSWMD-10 DOIT survenir après achèvement de CHPSWMD-9.	Si le TFTP échoue, continuer le fonctionnement du PS mais faire rapport d'une erreur et continuer d'essayer CHPSWMD-9. Si le traitement du fichier de configuration de pare-feu produit une erreur, continuer et rapporter l'erreur comme événement.
CHPSWMD-11	*Approvisionnement terminé* Sur demande du système d'approvisionnement, le PS est tenu d'informer le système d'approvisionnement de l'état de l'approvisionnement du PS. Le système d'approvisionnement peut demander au PS d'envoyer un message SYSLOG ou un trap SNMP, ou les deux. Si le PS mène à bien toutes les étapes requises de CHPSWMD-1 à CHPSWMD-10 ET qu'il reçoit une adresse de serveur SYSLOG dans DHCP OFFER, le PS DOIT envoyer un message d'approvisionnement terminé au serveur SYSLOG avec l'état d'approvisionnement mis à PASS (*réussi*).	CHPSWMD-11 DOIT survenir après achèvement de CHPSWMD-10.	Si le trap SNMP échoue, le serveur d'approvisionnement peut ignorer que le processus d'approvisionnement est terminé à moins qu'il n'interroge l'objet cabhPsProvState.

Tableau 48/J.191 – Description des flux pour le processus d'approvisionnement WAN-Man du service portail pour le mode d'approvisionnement DHCP

Etape du flux	Approvisionnement WAN-Man du PS: mode d'approvisionnement DHCP	Séquence normale	Séquence d'échec
CHPSWMD-11	Si le PS mène à bien toutes les étapes d'approvisionnement requises de CHPSWMD-1 à CHPSWMD-10 ET qu'il reçoit des paramètres valides pour docsDevNmAccessGroup identifiant le récepteur Trap (docsDevNmAccessIP) et configurant le trap d'achèvement d'approvisionnement (cabhPsDevInitTrap) pour "lecture seule avec les Trap" (commande docsDevNmAccess mise à "4". Voir la norme [RFC 2669]), le PS DOIT envoyer un trap d'approvisionnement terminé (cabhPsDevInitTrap) avec les paramètres appropriés au récepteur de Trap. Si le temporisateur d'approvisionnement PS arrive à expiration avant l'achèvement de toutes les étapes requises de CHPSWMD-1 à CHPSWMD-10 ET si le PS reçoit une adresse de serveur SYSLOG dans le message DHCP OFFER, le PS DOIT envoyer un message approvisionnement terminé au serveur SYSLOG avec l'état d'approvisionnement mis à FAIL. Si le temporisateur d'approvisionnement PS arrive à expiration avant l'achèvement de toutes les étapes requises de CHPSWMD-1 à CHPSWMD-10 ET si le PS reçoit des paramètres valides pour docsDevNmAccessGroup identifiant le récepteur de Trap (docsDevNmAccessIP) et configurant le trap approvisionnement terminé (cabhPsDevInitTrap) pour "lecture seule avec des Trap" (mettre la commande docsDevNmAccess à "4". Voir la norme [RFC 2669].), le PS DOIT envoyer un trap d'approvisionnement échoué (cabhPsDevInitRetryTrap) au récepteur de trap. Le PS DOIT mettre à jour la valeur de cabhPsDevProvState avec l'état 'pass' (1) lorsque les étapes de flux d'approvisionnement CHPSWMD-1 à CHPSWMD-11 ont été menées à bien. Le PS DOIT mettre à jour la valeur de cabhPsDevProvState avec l'état 'fail' (3) ET faire rapport d'un événement indiquant l'échec du processus d'approvisionnement si le temporisateur d'approvisionnement PS arrive à expiration avant que la valeur de cabhPsDevProvState ne soit mise à jour avec l'état "pass".		

Le temporisateur d'approvisionnement du service portail NE DOIT PAS être remis à la valeur de départ de cabhPsDevProvTimer avant l'expiration du temporisateur d'approvisionnement du service portail ET tant que la valeur de l'état cabhPsDevProvState est toujours inProgress (2) OU que le service portail n'est pas rétabli.

13.3 Processus d'approvisionnement du PS pour la gestion: mode d'approvisionnement SNMP

Le service portail demande au serveur DHCP de tête de système une adresse réseau WAN-Man destinée aux échanges de messages de gestion entre les fonctions de gestion de service portail et le système NMS du réseau câblé. Si le service portail détermine sur la base de la procédure décrite au § 7.2.3.3 qu'il doit fonctionner en mode d'approvisionnement SNMP, le service portail sécurisera ses messages de gestion en utilisant SNMPv3, en suivant la procédure d'authentification décrite au § 11.3.3.

Le système NMS du réseau câblé peut facultativement donner pour instruction au service portail (CMP) fonctionnant en mode d'approvisionnement SNMP de télécharger un fichier de configuration de service portail du serveur TFTP. La notification d'achèvement du processus d'approvisionnement est fournie au moyen du processus de rapport d'événement décrit au § 6.5.

La Figure 41 illustre les flux de messages qui sont utilisés pour réaliser l'approvisionnement du service portail lorsqu'il fonctionne en mode d'approvisionnement SNMP.

Le processus d'approvisionnement pour l'interface WAN-Man d'un service portail fonctionnant en mode d'approvisionnement SNMP DOIT se faire via la séquence décrite à la Figure 41 et précisée de façon détaillée au Tableau 49. Des étapes facultatives sont indiquées en grisé dans la Figure 41. Ces étapes facultatives peuvent être faites immédiatement à la suite de l'étape CHPSWMS-15, plus tard, ou pas du tout.

Le Tableau 49 décrit les étapes individuelles du processus d'approvisionnement montré à la Figure 41.

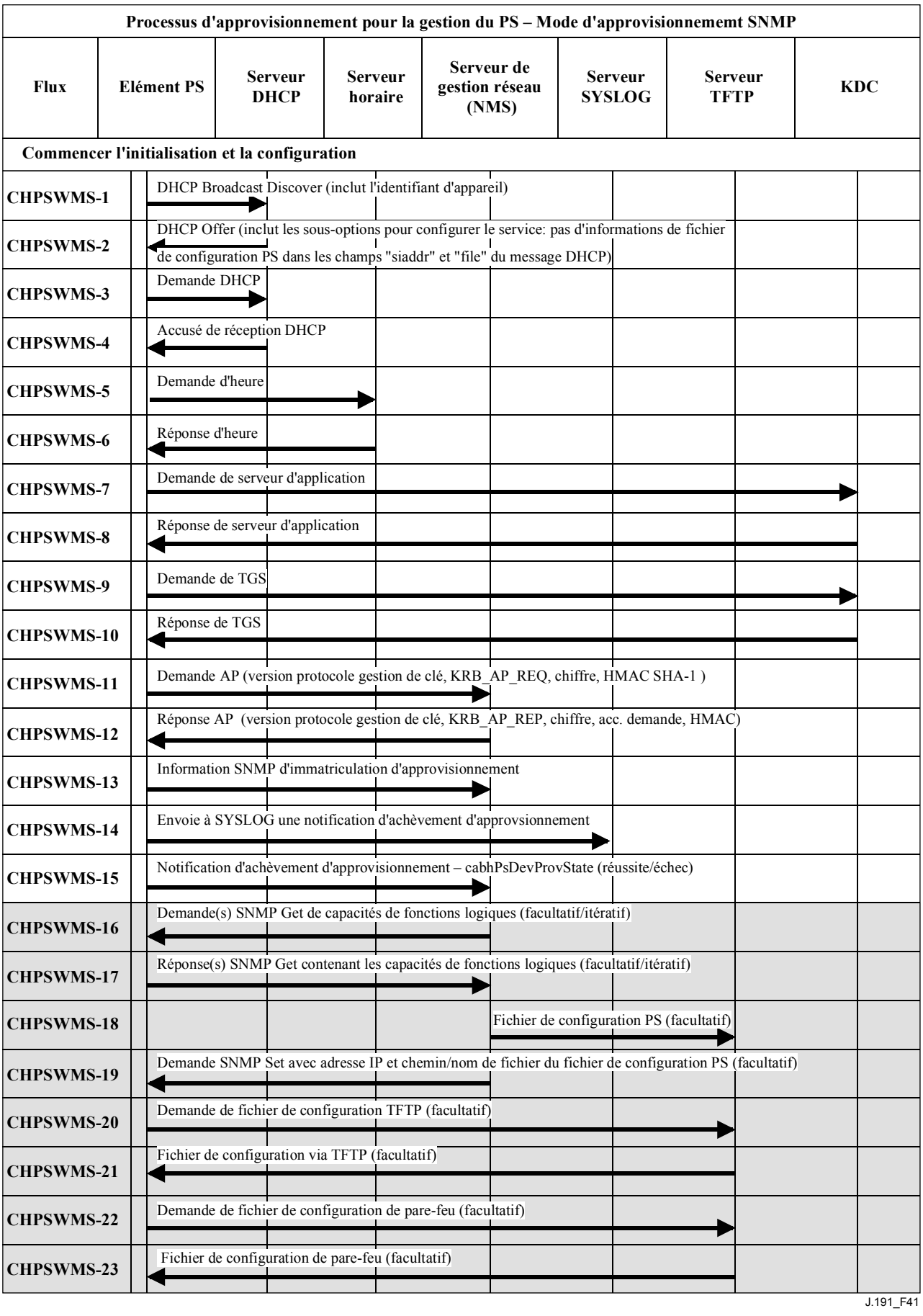

Figure 41/J.191 – Processus d'approvisionnement pour la gestion de PS – Mode d'approvisionnement SNMP

Tableau 49/J.191 – Descriptions des flux pour le processus d'approvisionnement WAN-Man de PS pour le mode d'approvisionnement SNMP

Etape de flux	Approvisionnement WAN-Man de PS: mode d'approvisionnement SNMP	Séquence normale	Séquence d'échec
CHPSWMS-1	*DHCP Broadcast Discover* Le CDP (CDC) DOIT envoyer un message DHCP DISCOVER en diffusion. La diffusion de DHCP DISCOVER par le CDP (CDC) DOIT inclure les options obligatoires dont la liste figure au Tableau 21. Le PS DOIT débuter le temporisateur d'approvisionnement en utilisant la valeur de début accessible via cabhPsDevProvTimer ET mettre cabhPsDevProvState à l'état "inProgress"(2) lorsque le CDC envoie un message DHCP DISCOVER en diffusion.	Commencer la séquence d'approvisionnement	S'il y a échec selon le protocole DHCP, faire rapport de l'erreur et continuer a essayer DHCP Broadcast Discover jusqu'à réussite (retourner à CHPSWMS-1). Après 5 essais le PS initialise le fonctionnement du CDS comme spécifié au § 7.2.3.3.
CHPSWMS-2	*DHCP OFFER* Le DHCP OFFER produit par le serveur DHCP dans le réseau câblé est censé inclure l'option de code facultatif 177 avec la sous-option 51 ET pas d'informations de fichier de configuration PS dans les champs "siaddr" et "file" du message DHCP. Le PS modifie cabhPsDevProvMode sur la base des informations reçues dans le DHCP OFFER (voir § 7.2.3.3).	CHPSWMS-2 DOIT survenir après achèvement de CHPSWMS-1.	S'il y a échec selon le protocole DHCP, retourner à CHPSWMS-1 et faire rapport de l'erreur.
CHPSWMS-3	*DHCP REQUEST* Le CDP DOIT envoyer au serveur DHCP approprié un message DHCP REQUEST pour accepter l'offre DHCP OFFER.	CHPSWMS-3 DOIT survenir après achèvement de CHPSWMS-2.	S'il y a échec selon le protocole DHCP, retourner à CHPSWMS-1.
CHPSWMS-4	*DHCP ACK* Le serveur DHCP envoie au CDP un message d'accusé de réception DHCP ACK qui contient l'adresse IPv4 du PS. Le PS DOIT mémoriser l'adresse du serveur horaire dans cabhPsDevTimeServerAddr.	CHPSWMS-4 DOIT survenir après achèvement de CHPSWMS-3.	S'il y a échec selon le protocole DHCP, retourner à CHPSWMS-1 et faire rapport de l'erreur.
CHPSWMS-5	*Demande d'heure (TOD) selon [RFC 868]* Le PS envoie une demande d'heure à l'adresse mémorisée dans cabhPsDevServerTime comme exigé au § 7.4.2.	CHPSWMS-5 DOIT survenir après achèvement de CHPSWMS-4.	Continuer avec CHPSWMS-6.

Tableau 49/J.191 – Descriptions des flux pour le processus d'approvisionnement WAN-Man de PS pour le mode d'approvisionnement SNMP

Etape de flux	Approvisionnement WAN-Man de PS: mode d'approvisionnement SNMP	Séquence normale	Séquence d'échec
CHPSWMS-6	*Réponse d'heure* Le serveur horaire est censé répondre avec l'heure actuelle en format UTC.	CHPSWMS-6 DOIT survenir après achèvement de CHPSWMS-5.	Continuer avec CHPSWMS-7, faire rapport de l'erreur, et retourner à CHPSWMS-5 (continuer à essayer l'heure jusqu'à réussite).
CHPSWMS-7	*Demande de serveur d'application*[a)] Le PS DOIT envoyer le message demande de serveur d'application au centre KDC de l'opérateur pour demander un ticket Kerberos.	CHPSWMS-7 DOIT survenir après achèvement de CHPSWMS-5. CHPSWMS-7 PEUT survenir après achèvement de CHPSWMS-6.	Retourner à CHPSWMS-1.
CHPSWMS-8	*Réponse de serveur d'application* Le message réponse de serveur d'application est reçu du centre KDC de l'opérateur qui contient le ticket Kerberos.	CHPSWMS-8 DOIT survenir après achèvement de CHPSWMS-7.	Retourner à CHPSWMS-1.
CHPSWMS-9	*Demande de serveur TGS* Si le PS a obtenu un ticket d'allocation de ticket (TGT, *ticket granting ticket*) dans l'étape CHPSWMS-10 du processus d'approvisionnement de l'interface WAN-Man du PS, le message demande de serveur TGS DOIT être envoyée au centre KDC de l'opérateur.	CHPSWMS-9 DOIT survenir après achèvement de CHPSWMS-8.	Retourner à CHPSWMS-1.
CHPSWMS-10	*Réponse de serveur TGS* Le message réponse de serveur TGS contenant le ticket est reçu du centre KDC de l'opérateur.	CHPSWMS-10 DOIT survenir après achèvement de CHPSWMS-9.	Retourner à CHPSWMS-1.

Tableau 49/J.191 – Descriptions des flux pour le processus d'approvisionnement WAN-Man de PS pour le mode d'approvisionnement SNMP

Etape de flux	Approvisionnement WAN-Man de PS: mode d'approvisionnement SNMP	Séquence normale	Séquence d'échec
CHPSWMS-11	*Demande de point d'accès* Le message demande de point d'accès DOIT être envoyé au serveur d'approvisionnement pour demander les informations sur les clés pour SNMPv3.	CHPSWMS-11 DOIT survenir après achèvement de CHPSWMS-10.	Retourner à CHPSWMS-1.
CHPSWMS-12	*Réponse de point d'accès* Le message réponse de point d'accès est reçu du serveur d'approvisionnement contenant les informations sur les clés pour SNMPv3. NOTE – Les clés SNMPv3 DOIVENT être établies et les tableaux SNMPv3 associés remplis avant l'étape suivante. Les clés et tableaux sont établis en utilisant les informations de la réponse AP.	CHPSWMS-12 DOIT survenir après achèvement de CHPSWMS-11.	Retourner à CHPSWMS-1.
CHPSWMS-13	*SNMP Inform* Le PS DOIT envoyer au système NMS un message SNMPv3 INFORM (cabhPsDevProvEnrollTrap) demandant l'immatriculation. L'adresse IP de cette entité SNMP d'approvisionnement est contenue dans le message DHCP OFFER.	CHPSWMS-13 DOIT survenir après achèvement de CHPSWMS-12.	Retourner à CHPSWMS-1.
CHPSWMS-14	*Notification SYSLOG* Si le PS a reçu une adresse de serveur SYSLOG dans le message DHCP OFFER, le PS DOIT envoyer au SYSLOG une notification "approvisionnement terminé". Cette notification comportera le résultat réussite/échec de l'opération d'approvisionnement. Le format général de cette notification est comme défini au § 6.5.1.	CHPSWMS-14 DOIT survenir après achèvement de CHPSWMS-13.	
CHPSWMS-15	*SNMP Inform* Le PS DOIT envoyer au système NMS un message SNMP INFORM (cabhPsDevInitTrap) contenant une notification "approvisionnement terminé". FAIL (*échec*) survient lorsque le traitement du fichier de configuration échoue. Autrement, l'état d'approvisionnement est PASS (*réussi*).	CHPSWMS-15 DOIT survenir après achèvement de CHPSWMS-14.	Si SNMP Inform échoue, le serveur d'approvision-nement peut ne pas savoir que le processus d'approvision-nement s'est terminé à moins qu'il n'interroge l'objet cabhPsProvisioningState.

Tableau 49/J.191 – Descriptions des flux pour le processus d'approvisionnement WAN-Man de PS pour le mode d'approvisionnement SNMP

Etape de flux	Approvisionnement WAN-Man de PS: mode d'approvisionnement SNMP	Séquence normale	Séquence d'échec
CHPSWMS-15	Le PS DOIT mettre à jour la valeur de cabhPsDevProvState avec l'état 'pass' (1) lorsque les étapes de flux d'approvisionnement CHPSWMS-1 à CHPSWMS-23 sont menées à bien. Le PS DOIT mettre à jour la valeur de cabhPsDevProvState avec l'état 'fail' (3) ET faire rapport d'un événement indiquant l'échec du processus d'approvisionnement si le temporisateur d'approvisionnement du PS arrive à expiration avant que la valeur de cabhPsDevProvState soit mise à jour avec l'état 'pass'.		
Etapes facultatives			
CHPSWMS-16	*SNMP Get*[b)] Si des capacités supplémentaires quelconques de l'appareil sont nécessaires pour le système d'approvisionnement, celui-ci les demande au PS via des demandes SNMPv3 Get. (Itératif:) le système NMS envoie au PS une ou plusieurs demandes SNMPv3 GET pour obtenir toutes informations sur les capacités de PS nécessaires. L'application d'approvisionnement peut utiliser une demande GETBulk pour obtenir plusieurs éléments d'information dans un seul message.	CHPSWMS-16 n'est pas supposé survenir avant achèvement de CHPSWMS-15.	Retourner à CHPSWMS-1.
CHPSWMS-17	*Réponse à SNMP Get* (Itératif:) le PS DOIT répondre aux messages de demande NMS Get ou Get Bulk par une réponse Get pour chaque demande Get. Après que tous les Get, ou GetBulk, sont terminés, le système NMS envoie les données demandées à l'application d'approvisionnement.	CHPSWMS-17 DOIT survenir après achèvement de CHPSWMS-16.	N/A

Tableau 49/J.191 – Descriptions des flux pour le processus d'approvisionnement WAN-Man de PS pour le mode d'approvisionnement SNMP

Etape de flux	Approvisionnement WAN-Man de PS: mode d'approvisionnement SNMP	Séquence normale	Séquence d'échec
CHPSWMS-18	*Créer un fichier de configuration* (Facultatif:) le système d'approvisionnement utilise les informations des étapes d'approvisionnement de PS CHPSWMS-14 et CHPSWMS-15 pour créer un fichier de configuration PS. Le système d'approvisionnement effectue un hachage sur le contenu du fichier de configuration. Le hachage est envoyé au PS dans l'étape suivante.	CHPSWMS-18 DOIT survenir après achèvement de CHPSWMS-17.	N/A
CHPSWMS-19	*SNMP Set* Le système d'approvisionnement peut donner pour instruction au système NMS d'envoyer un message SNMP Set au PS, contenant l'adresse IP du serveur TFTP, le nom de fichier du fichier de configuration et le hachage du fichier de configuration comme décrit au § 7.3.3.2 (mode d'approvisionnement SNMP). Facultativement, l'adresse IP du serveur TFTP du fichier de configuration du pare-feu, le nom de fichier du fichier de configuration du pare-feu, le hachage du fichier de configuration du pare-feu, et la clé de chiffrement (si le fichier de configuration du pare-feu est chiffré) sont inclus dans l'ensemble SNMP s'il y a un fichier de configuration de pare-feu à charger, et cette méthode est choisie pour le spécifier.	CHPSWMS-19 DOIT survenir après achèvement de CHPSWMS-18.	Retourner à CHPSWMS-1 si l'ensemble a été reçu mais qu'il y a eu une erreur de traitement.
CHPSWMS-20	*Demande TFTP* Si le système NMS déclenche le téléchargement par le PS d'un fichier de configuration PS comme décrit au § 7.3.3.2, le PS DOIT envoyer au serveur TFTP une demande TFTP Get pour demander le fichier de configuration PS demandé.	CHPSWMS-20 DOIT survenir après achèvement de CHPSWMS-19.	Continuer avec CHPSWMS-21.

Tableau 49/J.191 – Descriptions des flux pour le processus d'approvisionnement WAN-Man de PS pour le mode d'approvisionnement SNMP

Etape de flux	Approvisionnement WAN-Man de PS: mode d'approvisionnement SNMP	Séquence normale	Séquence d'échec
CHPSWMS-21	*Le serveur TFTP envoie le fichier de configuration* Après avoir reçu le fichier de configuration PS, le PS calcule le hachage du fichier de configuration PS et le compare à la valeur reçue dans l'étape CHPSWMS-19. Le PS traite alors le fichier de configuration PS. Voir au § 7.3.3 le contenu du fichier de configuration PS. Facultativement, l'adresse IP/FQDN du serveur TFTP du fichier de configuration du pare-feu, le nom de fichier du fichier de configuration du pare-feu, le hachage du fichier de configuration du pare-feu et la clé de chiffrement (si le fichier de configuration du pare-feu est chiffré) sont inclus dans le fichier de configuration PS s'il y a un fichier de configuration de pare-feu à charger, et ceci est la méthode choisie pour le spécifier.	CHPSWMS-21 DOIT survenir après achèvement de CHPSWMS-20.	Si le téléchargement TFTP échoue, faire rapport d'une erreur, passer à CHPSWMS-23, et continuer d'essayer CHPSWMS-20 (continuer d'essayer le téléchargement du fichier de configuration PS). Si le traitement du fichier de configuration produit une erreur, continuer et faire rapport de l'erreur comme d'un événement.
CHPSWMS-22	*Demande TFTP – Fichier de configuration de pare-feu* (Facultatif:) Le PS envoie au serveur TFTP de configuration de pare-feu une demande TFTP Get pour demander le fichier de données de configuration de pare-feu spécifié.	Si CHPSWMS-22 survient, il DOIT survenir après achèvement de CHPSWMS-21.	Retourner à CHPSWMS-1.
CHPSWMS-23	*Le serveur TFTP envoie le fichier de configuration de pare-feu* Le serveur TFTP envoie au PS une réponse TFTP contenant le fichier demandé. Après réception du fichier de configuration de pare-feu par le PS, celui-ci calcule le hachage du fichier de configuration du pare-feu et le compare à la valeur reçue à l'étape CHPSWMS-21. S'il est chiffré, le fichier est déchiffré. Le fichier est alors traité. Se reporter au § 7.3.3 pour la description du contenu du fichier de configuration PS.	CHPSWMS-23 DOIT survenir après achèvement de CHPSWMS-22.	Si le téléchargement TFTP échoue, continuer le fonctionnement du PS mais faire rapport d'une erreur et continuer d'essayer CHPSWMS-22. Si le traitement du fichier de configuration de pare-feu produit une erreur, continuer et faire rapport de l'erreur comme d'un événement.

[a] Les étapes CHPSWMS-7-CHPSWMS-10 sont facultatives dans certains cas. Voir les détails au paragraphe 11.

[b] Les opérations SNMP Get et la réponse à SNMP Get suivante sont facultatives, selon que des informations supplémentaires sont nécessaires pour former un fichier de configuration PS, et aussi selon qu'un fichier de configuration PS est nécessaire.

13.3.1 Téléchargement de fichier de configuration WAN-Man de service portail

Le service portail fonctionnant en mode d'approvisionnement SNMP contient suffisamment d'informations d'usine par défaut pour permettre le fonctionnement des côtés soit LAN ou WAN soit les deux sans téléchargement de fichier de configuration. Si le service portail fonctionne en mode d'approvisionnement SNMP, le fichier de configuration PS PEUT être téléchargé pour l'approvisionnement initial pour remplacer les valeurs d'usine par défaut ou pour fournir des informations complémentaires.

Le fichier de configuration de pare-feu contient les informations fournissant la fonction pare-feu. L'indication de téléchargement du fichier de configuration viendra soit dans le fichier de configuration PS soit via un SNMP Set pendant l'initialisation.

13.3.2 Temporisateur d'approvisionnement de service portail

Il est fourni un temporisateur d'approvisionnement destiné à garantir que le service portail continuera de poursuivre le processus d'approvisionnement même si une opération ne se termine pas. L'objet de temporisation, cabhPsDevProvTimer, a une initialisation par défaut de 5 minutes.

Mode d'approvisionnement DHCP

Le temporisateur d'approvisionnement DOIT commencer son décompte lorsque commence l'étape CHPSWMD-1. Si le temporisateur d'approvisionnement PS arrive à expiration avant l'exécution de l'étape CHPSWMD-12, le centre CDC DOIT mettre cabhPsDevProvState à l'état "3" (échec), le processus d'approvisionnement DOIT retourner à l'étape CHPSWMD-1, ET le service portail doit générer l'événement approprié et remettre le temporisateur d'approvisionnement PS à la valeur de cabhPsDevProvTimer.

Mode d'approvisionnement SNMP

Le temporisateur d'approvisionnement DOIT commencer son décompte lorsque commence l'étape CHPSWMS-1. Si le temporisateur d'approvisionnement PS arrive à expiration avant l'exécution de l'étape CHPSWMS-23, le centre CDC DOIT mettre cabhPsDevProvState à l'état "3" (échec), le processus d'approvisionnement DOIT retourner à l'étape CHPSWMS-1, le service portail DOIT faire rapport de l'événement approprié ET le service portail DOIT remettre le temporisateur d'approvisionnement PS à la valeur de cabhPsDevProvTimer.

13.3.3 Information d'immatriculation d'approvisionnement/approvisionnement terminé

Pour le service portail fonctionnant seulement en mode d'approvisionnement SNMP, l'information d'immatriculation d'approvisionnement, définie à l'Annexe B, permet au serveur d'approvisionnement de déterminer si le service portail est prêt pour le fichier de configuration PS.

Aussi bien en mode d'approvisionnement DHCP qu'en mode d'approvisionnement SNMP, le trap d'approvisionnement achevé (cabhPsDevInitTrap), défini à l'Annexe B, indique si la séquence d'approvisionnement a été ou non menée à bien.

13.4 Approvisionnement SYSLOG

L'adresse IP du serveur syslog DOIT être approvisionnée à travers le processus DHCP. L'événement syslog ne sera pas envoyé si l'adresse IP du serveur syslog n'est pas configurée.

13.4.1 Etat d'approvisionnement et rapport d'erreur

Comme indiqué aux Tableaux 48 et 49, l'échec d'une des étapes du processus d'approvisionnement provoque généralement le redémarrage du processus à la première étape, CHPSWMD-1 ou CHPSWMS-1.

13.5 Processus d'approvisionnement WAN-Data du service portail

Le service portail demande zéro ou plus adresses réseau WAN-Data au serveur DHCP dans le réseau câblé, destinées à être utilisées pour l'échange des données entre les éléments connectés à l'Internet et aux appareils IP de LAN.

Il n'y a pas de différence dans le fonctionnement WAN-Data du service portail entre les modes d'approvisionnement DHCP et SNMP.

Les diagrammes ci-après illustrent les flux de messages qui doivent être utilisés pour réaliser l'approvisionnement des adresses WAN-Data de service portail.

Si le processus d'approvisionnement pour la ou les adresses WAN-Data de service portail survient, il DOIT suivre la séquence décrite à la Figure 42 qui est détaillée dans le Tableau 50.

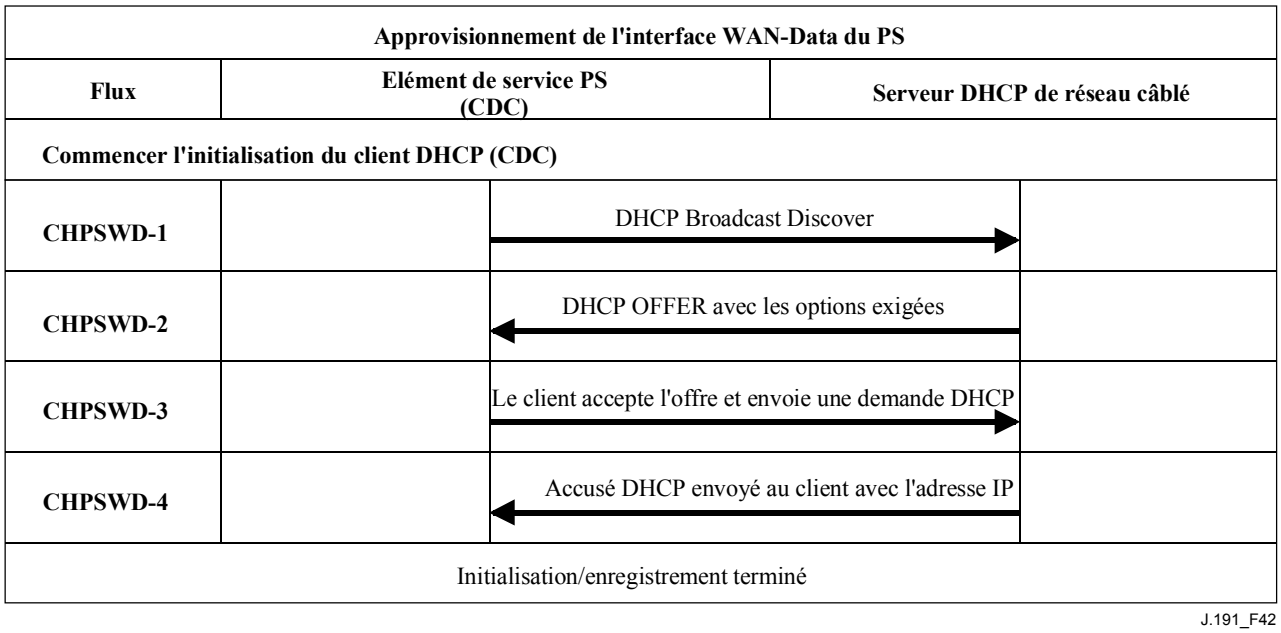

Figure 42/J.191 – Processus d'approvisionnement WAN-Data du service portail

Tableau 50/J.191 – Descriptions de flux pour le processus d'approvisionnement WAN-Data de service portail

Etape de flux	Approvisionnement d'adresse WAN-Data PS	Séquence normale	Séquence d'échec
CHPSWD-1	*DHCP Discover en diffusion* Le PS DOIT envoyer un message DHCP DISCOVER en diffusion incluant les options obligatoires listées au Tableau 21.	Passer à CHPSWD-2.	En cas d'échec selon le protocole DHCP, répéter CHPSWD-1.
CHPSWD-2	*DHCP OFFER* Le serveur DHCP à la tête de système reçoit le paquet DHCP DISCOVER, alloue une adresse IP du groupe WAN-Data, construit un paquet DHCP OFFER, et transmet l'offre DHCP OFFER à l'agent de relais DHCP dans le système CMTS.	Passer à CHPSWD-3.	En cas d'échec, le client dépassera la temporisation selon le protocole DHCP et l'étape CHPSWD-1 sera répétée.

Tableau 50/J.191 – Descriptions de flux pour le processus d'approvisionnement WAN-Data de service portail

Etape de flux	Approvisionnement d'adresse WAN-Data PS	Séquence normale	Séquence d'échec
CHPSWD-3	*DHCP REQUEST* Le portail CDP DOIT envoyer au serveur DHCP approprié un message DHCP REQUEST pour accepter l'offre DHCP OFFER.	CHPSWD-3 DOIT survenir après achèvement de CHPSWD-2.	En cas d'échec selon le protocole DHCP, retourner à CHPSWD-1.
CHPSWD-4	*DHCP ACK* Le serveur DHCP envoie au portail CDP un message d'accusé de réception DHCP ACK qui contient l'adresse IPv4 pour l'interface WAN Data du PS.	CHPSWD-4 DOIT survenir après achèvement de CHPSWD-3. L'approvision-nement se termine avec l'achèvement de CHPSWD-4.	En cas d'échec selon le protocole DHCP, retourner à CHPSWD-1.

13.6 Processus d'approvisionnement: client DHCP dans le secteur LAN-Trans

Les appareils IP de LAN demandent des adresses IP via les processus DHCP. L'élément de service portail traite ces messages conformément aux paramètres d'approvisionnement alloués par le système NMS du réseau câblé (voir § 7.2.3.2).

Le présent paragraphe décrit le processus d'approvisionnement pour le cas où le système NMS a approvisionné le service portail pour fonctionner en mode de traitement de paquet primaire C-NAT ou C-NAPT (voir paragraphe 8). Il n'y a pas de différence dans le processus d'approvisionnement d'appareil IP de secteur LAN-Trans entre les modes d'approvisionnement DHCP et SNMP.

Les flux de messages du processus d'approvisionnement pour un appareil IP de LAN dans le secteur d'adresse LAN-Trans sont décrits à la Figure 43. Des détails supplémentaires sur le processus sont fournis au Tableau 51.

Le processus d'approvisionnement pour l'appareil IP de LAN dans le secteur LAN-Trans DOIT survenir via la séquence décrite à la Figure 43 et détaillée au Tableau 51.

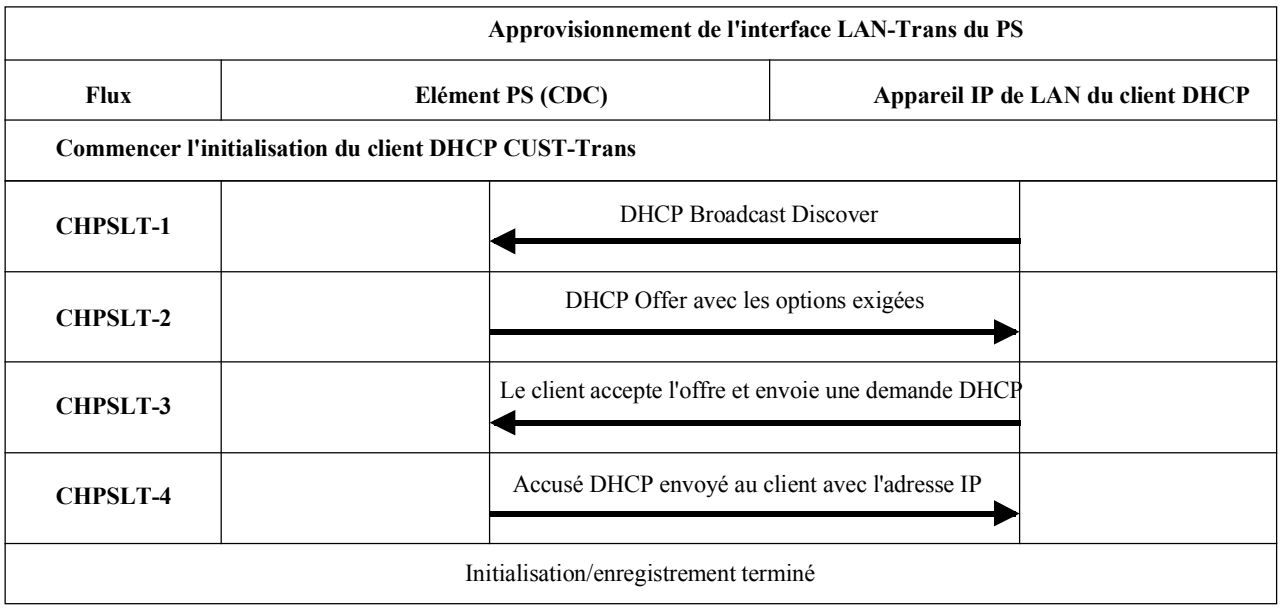

Figure 43/J.191 – Processus d'approvisionnement pour appareil IP de LAN dans le secteur LAN-Trans

Tableau 51/J.191 – Descriptions de flux pour le processus d'approvisionnement LAN-Trans de PS

Etape de flux	Approvisionnement d'adresse LAN-Trans de client	Séquence normale	Séquence d'échec
CHPSLT-1	*DHCP Discover en diffusion* Le client[a)] envoie un message DHCP DISCOVER en diffusion sur son LAN[b)] local.	Passer à CHPSLT-2.	En cas d'échec selon le protocole DHCP répéter CHPSLT-1.
CHPSLT-2	*DHCP OFFER* Le PS reçoit le message DHCP DISCOVER sur son interface LAN et examine le champ chaddr. Si: – il y a une adresse LAN-Trans disponible, et – il n'y a pas de considérations administratives justifiant le rejet de l'adresse LAN-Trans pour le client, le PS DOIT alors envoyer un message DHCP OFFER au client pour lui offrir l'adresse LAN-Trans soit en monodiffusion soit en diffusion spécifique de la liaison (conformément au bit BROADCAST du champ fanions du message DHCP DISCOVER).	Passer à CHPSLT-3.	En cas d'échec, le client dépassera la temporisation selon le protocole DHCP et CHPSLT-1 sera répétée.
CHPSLT-3	*DHCP REQUEST* Le client DHCP de l'appareil IP de LAN reçoit le message DHCP OFFER. Lorsqu'un client DHCP d'appareil IP de LAN souhaite accepter une DCHP OFFER, il est censé formater et envoyer un paquet DHCP REQUEST en utilisant la diffusion spécifique de la liaison[c)].	Passer à CHPSLT-4.	En cas d'échec, le client dépassera la temporisation selon le protocole DHCP et CHPSLT-1 sera répétée.

Tableau 51/J.191 – Descriptions de flux pour le processus d'approvisionnement LAN-Trans de PS

Etape de flux	Approvisionnement d'adresse LAN-Trans de client	Séquence normale	Séquence d'échec
CHPSLT-4	*DHCP ACK* Le PS reçoit la DHCP REQUEST sur son interface LAN. Si l'adresse LAN-Trans indiquée est toujours allouable, le PS DOIT alors envoyer DHCP ACK au client soit en monodiffusion soit comme diffusion spécifique de la liaison (conformément au bit BROADCAST du champ fanions de la demande DHCP REQUEST).	Approvision-nement terminé.	En cas d'échec, le client dépassera la temporisation selon le protocole DHCP et CHPSLT-1 sera répétée.

[a] Si le client connaît l'adresse IP précédente (par exemple, à la suite d'un réamorçage), il peut omettre DHCP DISCOVER et passer à l'étape 3.

[b] Si le client est situé sur un réseau qui ne fait pas de diffusion, il est censé envoyer le message en monodiffusion au serveur DHCP.

[c] Si le client est situé sur un réseau qui ne fait pas de diffusion, il est censé envoyer le message en monodiffusion au service portail.

13.6.1 Choix d'adresse LAN-Trans et des options DHCP

Le PS DOIT choisir l'adresse LAN-Trans qu'il offre à partir de la gamme indiquée par les variables de base MIB cabhCdpLanPoolStart et cabhCdpLanPoolEnd.

Le serveur CDS de service portail DOIT inclure dans DHCP OFFER les options obligatoires listées au Tableau 18.

13.7 Processus d'approvisionnement: client DHCP dans le secteur LAN-Pass

Certaines applications d'usager ne fonctionnent pas correctement avec une adresse réseau traduite. Pour s'accommoder de ces applications, le service portail active sa capacité à fonctionner en mode traverse (pontage transparent). Comme décrit au § 8.2.2.2, le pontage survient lorsque le système NMS du réseau câblé met le mode de traitement de paquet primaire (cabhCapPrimaryMode) à traverse, ou en écrivant les adresses MAC d'appareils IP de LAN individuels dans le tableau de traverse (*Pass-through*) (cabhCapPassthroughTable). La Figure 44 décrit le processus pour la demande et l'allocation d'une adresse IP aux appareils IP de LAN pour lesquels le service portail a été préprovisionné pour ponter le trafic. Lorsque le service portail a été configuré pour ponter du trafic pour un appareil IP de LAN, les messages DHCP DISCOVER et DHCP REQUEST produits par cet appareil IP de LAN seront servis par le serveur DHCP du réseau câblé et non par le serveur CDS.

Le processus d'approvisionnement pour l'appareil IP de LAN dans le secteur LAN-Pass DOIT survenir via la séquence décrite à la Figure 44 et détaillé au Tableau 52.

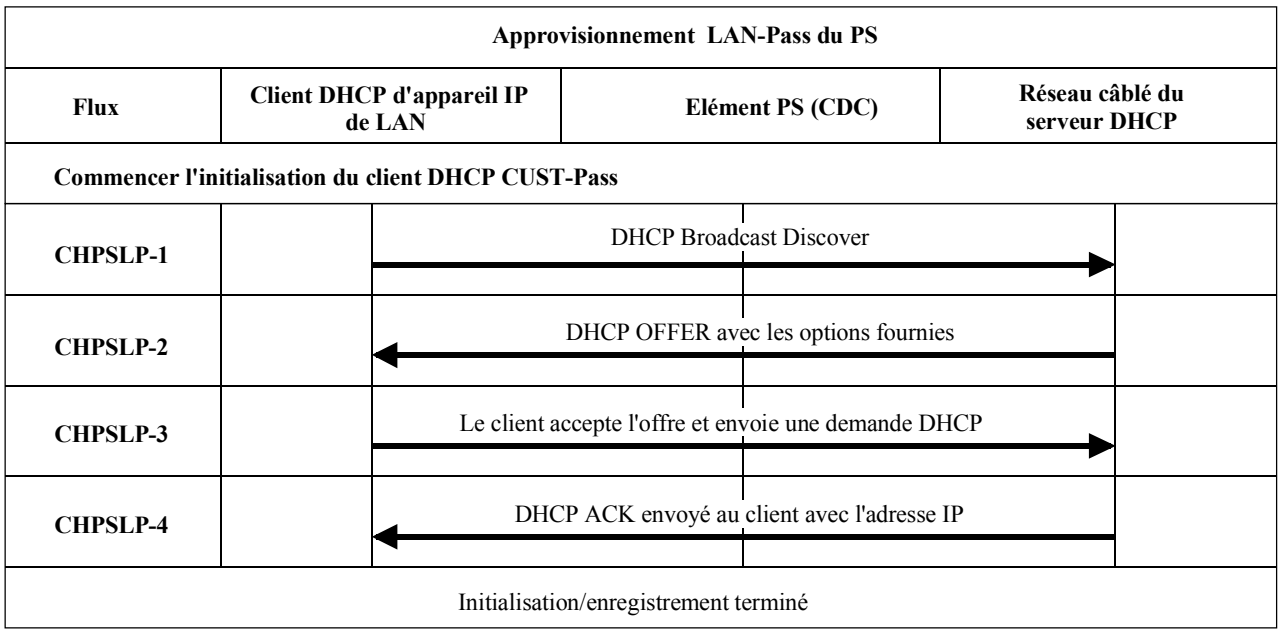

Figure 44/J.191 – Processus d'approvisionnement pour appareil IP de LAN dans le secteur LAN-Pass

Tableau 52/J.191 – Descriptions des flux pour le processus d'approvisionnement LAN-Pass

Etape de flux	Approvisionnement d'adresse de traverse client	Séquence normale	Séquence d'échec
CHPSLP-1	*DHCP Broadcast Discover* L'appareil IP de LAN diffuse un message DHCP DISCOVER sur son LAN local[a)]. Le PS reçoit le paquet DHCP DISCOVER en diffusion sur son interface LAN et DOIT ponter le paquet de façon transparente à l'interface WAN sans changer le contenu du paquet.	Passer à CHPSLP-2.	En cas d'échec selon le protocole DHCP répéter CHPSLP-1.
CHPSLP-2	*DHCP OFFER* Le serveur DHCP à la tête de système reçoit le paquet DHCP DISCOVER et alloue une adresse IP lisible en externe et les autres options, construit un paquet DHCP OFFER, et transmet la DHCP OFFER à l'appareil IP de LAN. Le PS DOIT ponter de façon transparente l'offre DHCP OFFER à partir de son interface WAN jusqu'à son interface LAN sans changer le contenu du paquet IP.	Passer à CHPSLP-3.	En cas d'échec, l'appareil IP de LAN dépassera la temporisation selon le protocole DHCP et CHPSLP-1 sera répétée.

Tableau 52/J.191 – Descriptions des flux pour le processus d'approvisionnement LAN-Pass

Etape de flux	Approvisionnement d'adresse de traverse client	Séquence normale	Séquence d'échec
CHPSLP-3	*DHCP REQUEST* L'appareil IP de LAN reçoit la DHCP OFFER et produit un message DHCP REQUEST. Le PS DOIT ponter de façon transparente la DHCP REQUEST à partir de son interface LAN jusqu'à son interface WAN sans changer le contenu du paquet IP.	Passer à CHPSLP-4.	En cas d'échec selon le protocole DHCP, répéter CHPSLP-1.
CHPSLP-4	*DHCP ACK* Le serveur DHCP de tête de système reçoit la DHCP REQUEST et envoie le DHCP ACK à l'appareil IP de LAN IP avec l'adresse IPv4 de l'appareil IP de LAN. Le PS DOIT ponter de façon transparente le DHCP ACK de son interface WAN à son interface LAN sans changer le contenu du paquet IP.	Approvision-nement terminé	En cas d'échec, l'appareil IP de LAN dépassera la temporisation selon le protocole DHCP et CHPSLP-1 sera répétée.
[a] Si le client est situé sur un réseau sans diffusion, il doit transmettre le message en monodiffusion au serveur DHCP ou à l'agent relais DHCP dans le réseau câblé.			

Annexe A

Objets MIB

La présente annexe donne la liste de tous les objets de base MIB exigés, comme indiqué au § 6.3.7.

NOM/Paramètre MIB	Max-Access	Persistant
mib-2		
système		
sysDescr	en lecture seule	Oui
sysObjectID	en lecture seule	Oui
sysUpTime	en lecture seule	Non
sysContact	en lecture seule	Oui
sysName	en lecture seule	Oui
sysLocation	en lecture seule	Oui
sysServices	en lecture seule	Oui
interfaces [RFC 2863]		
ifNumber	en lecture seule	Non
ifTable/ifEntry		
ifIndex	en lecture seule	Non
ifDescr	en lecture seule	Non
ifType	en lecture seule	Non

ifMtu	en lecture seule	Non
ifSpeed	en lecture seule	Non
ifPhysAddress	en lecture seule	Non
ifAdminStatus	en lecture-écriture	Non
ifOperStatus	en lecture seule	Non
ifLastChange	en lecture seule	Non
ifInOctets	en lecture seule	Non
ifInUcastPkts	en lecture seule	Non
ifInNUcastPkts	en lecture seule	Non
ifInDiscards	en lecture seule	Non
ifInErrors	en lecture seule	Non
ifInUnknownProtos	en lecture seule	Non
ifOutOctets	en lecture seule	Non
ifOutUcastPkts	en lecture seule	Non
ifOutNUcastPkts	en lecture seule	Non
ifOutDiscards	en lecture seule	Non
ifOutErrors	en lecture seule	Non
ifOutQLen	en lecture seule	Non
ifSpecifc	en lecture seule	Non
ip [RFC 2011]		
ipForwarding	en lecture-écriture	Non
ipDefaultTTL	en lecture-écriture	Non
ipInReceives	en lecture seule	Non
ipInHdrErrors	en lecture seule	Non
ipInAddrErrors	en lecture seule	Non
ipForwDatagrams	en lecture seule	Non
ipInUnknownProtos	en lecture seule	Non
ipInDiscards	en lecture seule	Non
ipInDelivers	en lecture seule	Non
ipOutRequests	en lecture seule	Non
ipOutDiscards	en lecture seule	Non
ipOutNoRoutes	en lecture seule	Non
ipReasmTimeout	en lecture seule	Non
ipReasmReqds	en lecture seule	Non
ipReasmOKs	en lecture seule	Non
ipReasmFails	en lecture seule	Non
ipFragOKs	en lecture seule	Non
ipFragFails	en lecture seule	Non
ipFragCreates	en lecture seule	Non
ipNetToMediaTable/ipNetToMediaEntry		
ipNetToMediaIfIndex	en lecture-création	Non

ipNetToMediaPhyAddress	en lecture-création	Non
ipNetToMediaNetAddress	en lecture-création	Non
ipNetToMediaType	en lecture-création	Non
icmp		
icmpInMsgs	en lecture seule	Non
icmpInErrors	en lecture seule	Non
icmpInDestUnreachs	en lecture seule	Non
icmpInTimeExcds	en lecture seule	Non
icmpInParmProbs	en lecture seule	Non
icmpInSrcQuenchs	en lecture seule	Non
icmpInRedirects	en lecture seule	Non
icmpInEchos	en lecture seule	Non
icmpInEchosReps	en lecture seule	Non
icmpInTimestamps	en lecture seule	Non
icmpInTimestampsReps	en lecture seule	Non
icmpInAddrMasks	en lecture seule	Non
icmpInAddrMaskReps	en lecture seule	Non
icmpOutMsgs	en lecture seule	Non
icmpOutErrors	en lecture seule	Non
icmpOutDestUnreachs	en lecture seule	Non
icmpOutTimeExcds	en lecture seule	Non
icmpOutParmProbs	en lecture seule	Non
icmpOutSrcQuenchs	en lecture seule	Non
icmpOutRedirects	en lecture seule	Non
icmpOutEchos	en lecture seule	Non
icmpOutEchosReps	en lecture seule	Non
icmpOutTimestamps	en lecture seule	Non
icmpOutTimestampReps	en lecture seule	Non
icmpOutAddrMasks	en lecture seule	Non
icmpOutAddrMaskReps	en lecture seule	Non
udp [RFC 2013]		
udpInDatagrams	en lecture seule	Non
udpNoPorts	en lecture seule	Non
udpInErrors	en lecture seule	Non
udpOutDatagrams	en lecture seule	Non
udpTable/udpEntry		
udpLocalAddress	en lecture seule	Non
udpLocalPort	en lecture seule	Non
transmission [RFC draft-ietf-ipcdn-bpiplus-mib-06.txt]		
docsIfMib		
docsBpi2MIB		

docsBpi2MIBObjects		
docsBpi2CmObjects		
docsBpi2CmCertObjects		
docsBpi2CmDeviceCertTable/docsBpi2CmDeviceCertEntry		
docsBpi2CmDeviceCmCert	en lecture-écriture	Oui
docsBpi2CmDeviceManufCert	en lecture seule	Oui
docsBpi2CodeDownloadControl		
docsBpi2CodeDownloadStatusCode	en lecture seule	Oui
docsBpi2CodeDownloadStatusString	en lecture seule	Oui
docsBpi2CodeMfgOrgName	en lecture seule	Oui
docsBpi2CodeMfgCodeAccessStart	en lecture seule	Oui
docsBpi2CodeMfgCvcAccessStart	en lecture seule	Oui
docsBpi2CodeCoSignerOrgName	en lecture seule	Oui
docsBpi2CodeCoSignerCodeAccessStart	en lecture seule	Oui
docsBpi2CodeCoSignerCvcAccessStart	en lecture seule	Oui
docsBpi2CodeCvcUpdate	en lecture-écriture	Oui
snmp [RFC 1907]		
snmpInPkts	en lecture seule	Non
snmpOutPkts	en lecture seule	Non
snmpInBadVersions	en lecture seule	Non
snmpInBadCommunityNames	en lecture seule	Non
snmpInBadCommunityUses	en lecture seule	Non
snmpInASNParseErrs	en lecture seule	Non
snmpInTooBigs	en lecture seule	Non
snmpInNoSuchNames	en lecture seule	Non
snmpInBadValues	en lecture seule	Non
snmpInReadOnlys	en lecture seule	Non
snmpInGenErrs	en lecture seule	Non
snmpInTotalReqVars	en lecture seule	Non
snmpInTotalSetVars	en lecture seule	Non
snmpInGetRequests	en lecture seule	Non
snmpInGetNexts	en lecture seule	Non
snmpInSetRequests	en lecture seule	Non
snmpInGetResponses	en lecture seule	Non
snmpInTraps	en lecture seule	Non
snmpOutTooBigs	en lecture seule	Non
snmpOutNoSuchNames	en lecture seule	Non
snmpOutBadValues	en lecture seule	Non
snmpOutGenErrs	en lecture seule	Non
snmpOutGetRequests	en lecture seule	Non
snmpOutGetNexts	en lecture seule	Non

snmpOutSetRequests	en lecture seule	Non
snmpOutGetResponses	en lecture seule	Non
snmpOutTraps	en lecture seule	Non
snmpEnableAuthenTraps	en lecture-écriture	Non
snmpSilentDrops	en lecture seule	Non
snmpProxyDrops	en lecture seule	Non
ifMIB [RFC 2863]		
ifMIBOjects		
ifXTable/ifXEntry		
ifName	en lecture seule	Non
ifInMulticastPkts	en lecture seule	Non
ifInBroadcastPkts	en lecture seule	Non
ifOutMulticastPkts	en lecture seule	Non
ifOutBroadcastPkts	en lecture seule	Non
ifHCInOctets	en lecture seule	Non
ifHCInUcastPkts	en lecture seule	Non
ifHCInMulticastPkts	en lecture seule	Non
ifHCInBroadcastPkts	en lecture seule	Non
ifHCOutOctets	en lecture seule	Non
ifHCOutUcastPkts	en lecture seule	Non
ifHCOutMulticastPkts	en lecture seule	Non
ifHCOutBroadcastPkts	en lecture seule	Non
ifLinkUpDownTrapEnable	en lecture-écriture	Non
ifHighSpeed	en lecture seule	Non
ifPromiscuousMode	en lecture-écriture	Non
ifConnectorPresent	en lecture seule	Non
ifAlias	en lecture-écriture	Non
ifCounterDiscontinuitityTime	en lecture seule	Non
docsDev [RFC 2669]		
docsDevMIBObjects		
docsDevNmAccessTable/docsDevNmAccessEntry		
docsDevNmAccessIndex	non accessible	Non
docsDevNmAccessIp	en lecture-création	Non
docsDevNmAccessIpMask	en lecture-création	Non
docsDevNmAccessCommunity	en lecture-création	Non
docsDevNmAccessControl	en lecture-création	Non
docsDevNmAccessInterfaces	en lecture-création	Non
docsDevNmAccessStatus	en lecture-création	Non
docsDevSoftware		
docsDevSwServer	en lecture-écriture	Oui
docsDevSwFilename	en lecture-écriture	Oui

docsDevSwAdminStatus	en lecture-écriture	Oui
docsDevSwOperStatus	en lecture seule	Oui
docsDevSwCurrentVers	en lecture seule	Oui
docsDevEvent		
docsDevEvControl	en lecture-écriture	Non
docsDevEvSyslog	en lecture-écriture	Non
docsDevEvThrottleAdminStatus	en lecture-écriture	Non
docsDevEvThrottleInhibited	en lecture seule	Non
docsDevEvThrottleThreshold	en lecture-écriture	Non
docsDevEvThrottleInterval	en lecture-écriture	Non
docsDevEvControlTable/docsDevEvControlEntry		
docsDevEvPriority	non accessible	Non
docsDevEvReporting	en lecture-écriture	Non
docsDevEventTable/docsDevEventEntry		
docsDevEvIndex	non accessible	Oui
docsDevEvFirstTime	en lecture seule	Oui
docsDevEvLastTime	en lecture seule	Oui
docsDevEvCounts	en lecture seule	Oui
docsDevEvLevel	en lecture seule	Oui
docsDevEvId	en lecture seule	Oui
docsDevEvText	en lecture seule	Oui
private		
enterprises		
cableLabs		
clabProject		
clabProjCableHome		
cabhPsDevMib		
cabhPsDevBase		
cabhPsDevDateTime	en lecture-écriture	Non
cabhPsDevResetNow	en lecture-écriture	Non
cabhPsDevSerialNumber	en lecture seule	Oui
cabhPsDevHardwareVersion	en lecture seule	Oui
cabhPsdevMacAddress	en lecture seule	Oui
cabhPsDevTypeIdentifier	en lecture seule	Oui
cabhPsDevResetDefaults	en lecture-écriture	Non
cabhPsDevWanManClientId	en lecture-écriture	Oui
cabhPsDevTodSyncStatus	en lecture seule	Non
cabhPsDevProvMode	en lecture seule	Non
cabhPsDevDwnldMode	en lecture seule	Non
cabhPsDevProv		
cabhPsDevProvisioningTimer	en lecture-écriture	Oui

cabhPsDevProvConfigFile	en lecture-écriture	Non
cabhPsDevProvConfigHash	en lecture-écriture	Non
cabhPsDevProvConfigFileSize	en lecture seule	Non
cabhPsDevProvConfigTLVProcessed	en lecture seule	Non
cabhPsDevProvConfigTLVRejected	en lecture seule	Non
cabhPsDevProvSolicitedKeyTimeout	en lecture-écriture	Oui
cabhPsDevProvState	en lecture seule	Non
cabhPsDevProvAuthState	en lecture seule	Non
cabhPsDevProvCorrelationId	en lecture seule	Non
cabhPsDevServerType	en lecture seule	Non
cabhPsDevServerTime	en lecture seule	Non
cabhSecMib		
cabhSecFwObjects		
cabhSecFwBase		
cabhSecFwPolicyFileEnable	en lecture-écriture	Oui
cabhSecFwPolicyFileURL	en lecture-écriture	Non
cabhSecFwPolicyFileHash	en lecture-écriture	Non
cabhSecFwPolicyFileOperStatus	en lecture seule	Non
cabhSecFwPolicyFileCurrentVersion	en lecture-écriture	Oui
cabhSecFwLogCtl		
cabhSecFwEventType1Enable	en lecture-écriture	Oui
cabhSecFwEventType2Enable	en lecture-écriture	Oui
cabhSecFwEventType3Enable	en lecture-écriture	Oui
cabhSecFwEventAttachAlertThreshold	en lecture-écriture	Oui
cabhSecFwEventAttackAlertPeriod	en lecture-écriture	Oui
cabhCapMib		
cabhCapObjects		
cabhCapBase		
cabhCapTcpTimeWait	en lecture-écriture	Oui
cabhCapUdpTimeWait	en lecture-écriture	Oui
cabhCapIcmpTimeWait	en lecture-écriture	Oui
cabhCapPrimaryMode	en lecture-écriture	Oui
cabhCapSetToFactory	en lecture-écriture	Non
cabhCapMap		
cabhCapMappingTable/cabhCapMappingEntry		
cabhCapMappingWanAddrType	non accessible	Oui[1]
cabhCapMappingWanAddrType	non accessible	Oui[1]
cabhCapMappingWanPort	non accessible	Oui[1]

[1] Les objets cabhCapMappingEntry sont persistants s'ils sont approvisionnés par le système NMS et non persistants s'ils sont créés de façon dynamique sur la base du trafic sortant. Voir au § 8.3.2.2.

cabhCapMappingLanAddrType	non accessible	Oui[1]
cabhCapMappingLanAddrType	non accessible	Oui[1]
cabhCapMappingLanPort	non accessible	Oui[1]
cabhCapMappingMode	en lecture seule	Oui[1]
cabhCapMappingMethod	en lecture seule	Oui[1]
cabhCapMappingProtocol	en lecture seule	Oui[1]
cabhCapPassthroughTable/cabhCapPassthroughEntry		
cabhCapPassthroughMACAddr	non accessible	Oui
cabhCapPassthroughRowStatus	en lecture-création	Non
cabhCdpMib		
cabhCdpObjects		
cabhCdpBase		
cabhCdpSetToFactory	en lecture-écriture	Non
cabhCdpLanTransCurCount	en lecture seule	Non
cabhCdpLanTransThreshold	en lecture-écriture	Oui
cabhCdpLanTransAction	en lecture-écriture	Oui
cabhCdpAddr		
cabhCdpLanAddrTable/cabhCdpLanAddrEntry		
cabhCdpLanAddrIpType	non accessible	Oui
cabhCdpLanAddrIp	non accessible	Oui
cabhCdpLanAddrClientID	en lecture seule	Oui
cabhCdpLanAddrCreateTime	en lecture seule	Oui
cabhCdpLanAddrExpireTime	en lecture seule	Oui
cabhCdpLanAddrMethod	en lecture seule	Oui
cabhCdpLanAddrHostName	en lecture seule	Oui
cabhCdpLanAddrRowStatus	en lecture-création	Non
cabhCdpWanDataAddrTable/cabhCdpWanDataAddrEntry		
cabhCdpWanDataAddrIndex	non accessible	Oui
cabhCdpWanDataAddrClientId	en lecture-création	Oui
cabhCdpWanDataAddrIpType	en lecture-création	Non
cabhCdpWanDataAddrIp	en lecture-création	Non
cabhCdpWanDataAddrAddrRenewalTime	en lecture-création	Non
cabhCdpWanDataAddrRowStatus	en lecture-création	Non
cabhCdpWanDataAddrSeverTable/cabhCdpWanDataAddrSeverEntry		
cabhCdpWanDataAddrDnsIpType	non accessible	Non
cabhCdpWanDataAddrDnsIp	non accessible	Non
cabhCdpWanDataAddrDnsRowStatus	en lecture-création	Non
cabhCdpServer		
cabhCdpLanPoolStartType	en lecture-écriture	Oui
cabhCdpLanPoolStart	en lecture-écriture	Oui
cabhCdpLanPoolEndType	en lecture-écriture	Oui

cabhCdpLanPoolEnd	en lecture-écriture	Oui
cabhCdpServerSubnetMaskType	en lecture-écriture	Oui
cabhCdpServerSubnetMask	en lecture-écriture	Oui
cabhCdpServerTimeOffset	en lecture-écriture	Oui
cabhCdpServerRouterType	en lecture-écriture	Oui
cabhCdpServerRouter	en lecture-écriture	Oui
cabhCdpServerDnsAddressType	en lecture-écriture	Oui
cabhCdpServerDnsAddress	en lecture-écriture	Oui
cabhCdpServerSyslogAddressType	en lecture-écriture	Oui
cabhCdpServerSyslogAddress	en lecture-écriture	Oui
cabhCdpServerDomainName	en lecture-écriture	Oui
cabhCdpServerTTL	en lecture-écriture	Oui
cabhCdpServerInterfaceMTU	en lecture-écriture	Oui
cabhCdpServerVendorSpecific	en lecture-écriture	Oui
cabhCdpServerLeaseTime	en lecture-écriture	Oui
cabhCdpServerDhcpAddressType	en lecture-écriture	Oui
cabhCdpServerDhcpAddress	en lecture-écriture	Oui
cabhCtpMib		
cabhCtpObjects		
cabhCtpBase		
cabhCtpReset	en lecture-écriture	Non
cabpCtpConnSpeed		
cabhCtpConnSrcIpType	en lecture-écriture	Non
cabhCtpConnSrcIp	en lecture-écriture	Non
cabhCtpConnDestIpType	en lecture-écriture	Non
cabhCtpConnDestIp	en lecture-écriture	Non
cabhCtpConnProto	en lecture-écriture	Non
cabhCtpConnPort	en lecture-écriture	Non
cabhCtpConnNumPkts	en lecture-écriture	Non
cabhCtpConnPktSize	en lecture-écriture	Non
cabhCtpConnTimeOut	en lecture-écriture	Non
cabhCtpConnControl	en lecture-écriture	Non
cabhCtpConnStatus	en lecture seule	Non
cabhCtpConnPktsSent	en lecture seule	Non
cabhCtpConnPktsRecv	en lecture seule	Non
cabhCtpConnAvgRTT	en lecture seule	Non
cabhCtpConnMaxRTT	en lecture seule	Non
cabhCtpConnMinRTT	en lecture seule	Non
cabhCtpConnNumIcmpError	en lecture seule	Non
cabhCtpConnIcmpError	en lecture seule	Non
cabhCtpPing		

cabhCtpPingSrcIpType	en lecture-écriture	Non
cabhCtpPingSrcIp	en lecture-écriture	Non
cabhCtpPingDestIpType	en lecture-écriture	Non
cabhCtpPingDestIp	en lecture-écriture	Non
cabhCtpPingProto	en lecture-écriture	Non
cabhCtpPingNumPkts	en lecture-écriture	Non
cabhCtpPingPktSize	en lecture-écriture	Non
cabhCtpPingTimeBetween	en lecture-écriture	Non
cabhCtpPingTimeOut	en lecture-écriture	Non
cabhCtpPingControl	en lecture-écriture	Non
cabhCtpPingStatus	en lecture seule	Non
cabhCtpPingNumSent	en lecture seule	Non
cabhCtpPingNumRecv	en lecture seule	Non
expérimental		
snmpUSMDHObjectsMIB [RFC 2786]		
usmDHKeyObjects		
usmDHPublicObjects		
usmDHPParameters	en lecture-écriture	Non
usmDHUserKeyTable/usmDHUserKeyEntry		
usmDHUserAuthKeyChange	en lecture-création	Non
usmDHUserOwnAuthKeyChange	en lecture-création	Non
usmDHUserPrivKeyChange	en lecture-création	Non
usmDHUserOwnPrivKeyChange	en lecture-création	Non
usmDHKickstartGroup		
usmDHKickstartTable/usmDHKickstartEntry		
usmDHKickstartIndex	non accessible	Non
usmDHKickstartMyPublic	en lecture seule	Non
usmDHKickstartMgrPublic	en lecture seule	Non
usmDHKickstartSecurityName	en lecture seule	Non
snmpV2		
snmpModules		
snmpMIB		
snmpMIBObjects		
snmpSet		
snmpSetSerialNo	en lecture-écriture	Non
snmpFrameworkMIB [RFC 2571]		
snmpEngine		
snmpEngineID	en lecture seule	Oui
snmpEngineBoots	en lecture seule	Oui
snmpEngineTime	en lecture seule	Non
snmpEngineMaxMessageSize	en lecture seule	Oui

snmpMPDMIB [RFC 2572]		
snmpMPDObjects		
snmpMPDStats		
snmpUnknownSecurityModels	en lecture seule	Non
snmpInvalidMsgs	en lecture seule	Non
snmpUnknownPDUHandlers	en lecture seule	Non
snmpTargetMIB [RFC 2573]		
snmpTargetObjects		
snmpTargetSpinLock	en lecture-écriture	Non
snmpTargetAddrTable/snmpTargetAddrEntry		
snmpTargetAddrName	non accessible	Non
snmpTargetAddrTDomain	en lecture-création	Non
snmpTargetAddrTAddress	en lecture-création	Non
snmpTargetAddrTimeout	en lecture-création	Non
snmpTargetAddrRetryCount	en lecture-création	Non
snmpTargetAddrTagList	en lecture-création	Non
snmpTargetAddrParams	en lecture-création	Non
snmpTargetAddrStorageType	en lecture-création	Non
snmpTargetAddrRowStatus	en lecture-création	Non
snmpTargetParamsTable/snmpTargetParamsEntry		
snmpTargetParamsName	non accessible	Non
snmpTargetParamsMPModel	en lecture-création	Non
snmpTargetParamsSecurityModel	en lecture-création	Non
snmpTargetParamsSecurityName	en lecture-création	Non
snmpTargetParamsSecurityLevel	en lecture-création	Non
snmpTargetParamsStorageType	en lecture-création	Non
snmpTargetParamsRowStatus	en lecture-création	Non
snmpUnavailableContexts	en lecture seule	Non
snmpUnknownContexts	en lecture seule	Non
snmpNotificationMIB [RFC 2573]		
snmpNotifyObjects		
snmpNotifyTable/snmpNotifyEntry		
snmpNotifyName	non accessible	Non
snmpNotifyTag	en lecture-création	Non
snmpNotifyType	en lecture-création	Non
snmpNotifyStorageType	en lecture-création	Non
snmpNotifyRowStatus	en lecture-création	Non
snmpNotifyFilterProfileTable/snmpNotifyFilterProfileEntry		
snmpNotifyFilterProfileName	en lecture-création	Non
snmpNotifyFilterProfileStorType	en lecture-création	Non
snmpNotifyFilterProfileRowStatus	en lecture-création	Non

snmpNotifyFilterTable/snmpNotifyFilterEntry		
snmpNotifyFilterSubtree	non accessible	Non
snmpNotifyFilterMask	en lecture-création	Non
snmpNotifyFilterType	en lecture-création	Non
snmpNotifyFilterStorageType	en lecture-création	Non
snmpNotifyFilterRowStatus	en lecture-création	Non
snmpUsmMIB [RFC 2574]		
usmStats		
usmStatsUnsupportedSecLevels	en lecture seule	Non
usmStatsNotInTimeWindows	en lecture seule	Non
usmStatsUnknownUserNames	en lecture seule	Non
usmStatsUnknownEngineIDs	en lecture seule	Non
usmStatsWrongDigests	en lecture seule	Non
usmStatsDecryptionErrors	en lecture seule	Non
usmUser		
usmUserSpinLock	en lecture-écriture	Non
usmUserTable/usmUserEntry		
usmUserEngineID	non accessible	Non
usmUserName	non accessible	Non
usmUserSecurityName	en lecture seule	Non
usmUserCloneFrom	en lecture-création	Non
usmUserAuthProtocol	en lecture-création	Non
usmUserAuthKeyChange	en lecture-création	Non
usmUserOwnAuthKeyChange	en lecture-création	Non
usmUserPrivProtocol	en lecture-création	Non
usmUserPrivKeyChange	en lecture-création	Non
usmUserOwnPrivKeyChange	en lecture-création	Non
usmUserPublic	en lecture-création	Non
usmUserStorageType	en lecture-création	Non
usmUserStatus	en lecture-création	Non
SNMP-VIEW-BASED-ACM-MIB [RFC 2575]		
snmpVacmMIB		
vacmMIBObjects		
vacmContextTable/vacmContextEntry		
vacmContextName	en lecture seule	Non
vacmSecurityToGroupTable/vacmSecurityToGroupEntry		
vacmSecurityModel	non accessible	Non
vacmSecurityName	non accessible	Non
vacmGroupName	en lecture-création	Non
vacmSecurityToGroupStorageType	en lecture-création	Non
vacmSecurityToGroupStatus	en lecture-création	Non

vacmAccessTable/vacmAccessEntry		
vacmAccessContextPrefix	non accessible	Non
vacmAccessSecurityModel	non accessible	Non
vacmAccessSecurityLevel	non accessible	Non
vacmAccessContextMatch	en lecture-création	Non
vacmAccessReadViewName	en lecture-création	Non
vacmAccessWriteViewName	en lecture-création	Non
vacmAccessNotifyViewName	en lecture-création	Non
vacmAccessStorageType	en lecture-création	Non
vacmAccessStatus	en lecture-création	Non
vacmMIBViews		
vacmViewSpinLock	en lecture-écriture	Non
vacmViewTreeFamilyTable/vacmViewTreeFamilyEntry		
vacmViewTreeFamilyViewName	non accessible	Non
vacmViewTreeFamilySubtree	non accessible	Non
vacmViewTreeFamilyMask	en lecture-création	Non
vacmViewTreeFamilyType	en lecture-création	Non
vacmViewTreeFamilyStorageType	en lecture-création	Non
vacmViewTreeFamilyStatus	en lecture-création	Non
snmpCommunityMIB [RFC 2576]		
snmpCommunityMIBObjects		
snmpCommunityTable/snmpCommunityEntry		
snmpCommunityIndex	non accessible	Non
snmpCommunityName	en lecture-création	Non
snmpCommunitySecurityName	en lecture-création	Non
snmpCommunityContextEngineID	en lecture-création	Non
snmpCommunityContextName	en lecture-création	Non
snmpCommunityTransportTag	en lecture-création	Non
snmpCommunityStorageType	en lecture-création	Non
snmpCommunityStatus	en lecture-création	Non
snmpTargetAddrExtTable/snmpTargetAddrExtEntry		
snmpTargetAddrTMask	en lecture-création	Non
snmpTargetAddrMMS	en lecture-création	Non
snmpTrapAddress	accessible pour notifier	Non
snmpTrapCommunity	accessible pour notifier	Non

Annexe B

Format et contenu des événements, SYSLOG et trap SNMP

Le Tableau B.1 résume les formats et contenus des entrées d'événements d'enregistrement local, les messages syslog et les trap SNMP.

Chaque rangée du Tableau B.1 spécifie un événement que le service portail doit être capable de générer. Le service portail doit faire rapport sur ces événements par l'un, ou tous, des trois moyens suivants: enregistrement d'événement local comme effectué par le tableau d'événement local de la norme [RFC 2669], SYSLOG, et trap SNMP. Le format SYSLOG est spécifié au § 6.5.1.3 et le format de trap SNMP est défini dans la présente annexe, à la suite du Tableau B.1.

Les deux premières colonnes indiquent à quel stade surviennent les événements. La troisième colonne indique la priorité allouée à l'événement. Ces priorités sont les mêmes que celles rapportées dans l'objet docsDevEvLevel dans la norme [RFC 2669] et dans le champ LEVEL (*niveau*) d'un message syslog.

La quatrième colonne spécifie le texte de l'événement, qui est rapporté dans l'objet docsDevEvText de la norme [RFC 2669] et dans le champ texte d'un message syslog. La cinquième colonne donne des informations supplémentaires sur le texte de l'événement de la quatrième colonne. Par exemple, certains des champs de texte d'événement sont constants et certains autres incluent des informations variables. Certaines des variables ne sont exigées que dans l'enregistrement SYSLOG, comme décrit dans la cinquième colonne. La sixième colonne spécifie l'ensemble de code d'erreur.

La septième colonne indique un numéro d'identification unique pour l'événement, qui est alloué à l'objet docsDevEvId et au champ <eventId> d'un message syslog. La huitième colonne spécifie le trap SNMP, qui notifie cet événement à un récepteur d'événement SNMP.

Les règles pour générer de façon univoque un identifiant d'événement à partir du code d'erreur sont décrites au § 6.5.1.3. Les identifiants d'événement dans le Tableau B.1 sont en format décimal.

Pour mieux illustrer le Tableau B.1, voici un exemple utilisant la première rangée dans la section événements de mise à niveau de logiciels.

Les deux premières colonnes sont "Mise à niveau de logiciel" et "Initialisation de mise à niveau de logiciel". La priorité d'événement est "Remarque" (*Notice*). Le texte de l'événement est "Initialiser le téléchargement de logiciel – Via NMS". La cinquième colonne dit "Pour SYSLOG seulement, ajouter: MAC addr: <P1> P1 = Adresse Mac du PS". Il s'agit d'une note sur le SYSLOG. C'est-à-dire que le corps du texte syslog sera quelque chose comme "Initialiser le téléchargement du logiciel – Via NMS – MAC addr: x1 x2 x3 x4 x5 x6".

La dernière colonne "nom trap" est cabhPsDevSwUpgradeInitTrap, dont le format est donné à la fin de la présente annexe.

Tableau B.1/J.191 – Evénements définis

Processus	Sous-processus	Priorité PS	Texte d'événement	Notes et détails du message	Ensemble de code d'erreur	Identifiant d'événement	Nom trap
Erreurs DHCP avant l'achèvement de l'approvisionnement							
Initialiser	DHCP	Critique	Echec DHCP – Discover envoyé, pas d'offre reçue		D01.0	68000100	
Initialiser	DHCP	Critique	Echec DHCP – Demande envoyée, pas de réponse		D02.0	68000200	
Initialiser	DHCP	Critique	Echec DHCP – Info demandée non acceptée		D03.0	68000300	
Initialiser	DHCP	Critique	Echec DHCP – La réponse ne contient pas TOUS les champs valides décrits dans la Recom-mandation.		D03.1	68000301	
Erreurs d'heure avant l'achèvement de l'approvisionnement							
Initialiser	HEURE	Avertis-sement	Demande d'heure envoyée – Pas de réponse reçue		D04.1	68000401	
Initialiser	HEURE	Avertis-sement	Réponse d'heure reçue – Format de données non valide		D04.2	68000402	
Erreurs TFTP avant l'achèvement de l'approvisionnement							
Initialiser	TFTP	Critique	Echec TFTP – Demande envoyée – Pas de réponse		D05.0	68000500	
Initialiser	TFTP	Critique	Echec TFTP – Fichier de configuration INTROUVABLE	Pour SYSLOG seul, ajouter: nom de fichier = <P1> P1 = nom de fichier demandé	D06.0	68000600	
Initialiser	TFTP	Critique	Echec TFTP – Paquet HORS SERVICE		D07.0	68000700	
Initialiser	TFTP	Critique	Fichier TFTP terminé – Mais échec de la vérification d'intégrité du message MIC	Pour SYSLOG seul, ajouter: nom de fichier = <P1> P1 = nom de fichier du fichier TFTP	D08.0	68000800	
Initialiser	TFTP	Critique	Echec TFTP – Nombre maximal d'essais dépassé	Pour SYSLOG seul, ajouter: limite d'essais = <P1> P1 = nombre maximal d'essais	D09.0	68000900	
TFTP réussi							
Initialiser	TFTP	Remarque	TFTP réussi		D10.0	68001000	

Tableau B.1/J.191 – Evénements définis

Processus	Sous-processus	Priorité PS	Texte d'événement	Notes et détails du message	Ensemble de code d'erreur	Identifiant d'événement	Nom trap
Analyse grammaticale de TLV							
Initialiser	Analyse de TLV	Remarque	TLV-28 – OID non reconnu		I401.0	73040100	cabhPsDev InitTLVUnknownTrap
Initialiser	Analyse de TLV	Remarque	TLV inconnu <P1>	Pour SYSLOG seul: <P1> = le TLV complet en hexa-décimal	I401.1	73040101	cabhPsDev InitTLVUnknownTrap
Initialiser	Analyse de TLV	Remarque	Format/ contenu de TLV non valide <P1>	Pour SYSLOG seul, <P1> = le TLV complet en hexa-décimal	I401.2	73040102	
Approvisionnement							
Initialiser	SNMP Inform	Remarque	SNMP Inform a envoyé le signal de fin d'appro. (réussite/ échec)	Pour SYSLOG seul, ajouter MAC Addr: <P1>. P1 = adresse MAC du PS	I11.0	73001100	cabhPsDev InitTrap
Initialiser	Retrans-mission de SNMP Inform	Critique	SNMP Inform a envoyé le signal de fin d'appro. (réussite/ échec), pas de réponse. SNMP Inform renvoyé	Pour SYSLOG seul, ajouter: MAC Addr: <P1>. P1 = adresse MAC du PS	I11.1	73001101	cabhPsDev InitRetryTrap
SW upgrade init (initialisation de mise à niveau de logiciel)							
Mise à niveau de logiciel	Initialisa-tion de mise à niveau de logiciel	Remarque	Initialiser le téléchargement du logiciel – Via NMS	Pour SYSLOG seul, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E101.0	69010100	cabhPsDev SwUpgrade InitTrap
Mise à niveau de logiciel	Initialisa-tion de mise à niveau de logiciel	Remarque	Initialiser le téléchargement du logiciel – Via fichier de configuration <P1>	P1 = nom du fichier de configuration du câblo-modem Pour SYSLOG seul, ajouter: fichier logiciel: <P2> – serveur logiciel: < P3>. P2 = nom de fichier logiciel et P3 = adresse IP de serveur TFTP	E102.0	69010200	cabhPsDev SwUpgrade InitTrap

Tableau B.1/J.191 – Evénements définis

Processus	Sous-processus	Priorité PS	Texte d'événement	Notes et détails du message	Ensemble de code d'erreur	Identifiant d'événement	Nom trap
Echec général de mise à niveau de logiciel							
Mise à niveau de logiciel	Echec général de mise à niveau de logiciel	Erreur	La mise à niveau de logiciel a échoué pendant le téléchargement – Maximum d'essais dépassé (3)	Pour SYSLOG seul, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E103.0	69010300	cabhPsDev SwUpgrade FailTrap
Mise à niveau de logiciel	Echec général de mise à niveau de logiciel	Erreur	La mise à niveau de logiciel a échoué avant le téléchargement – Pas de serveur présent	Pour SYSLOG seul, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E104.0	69010400	cabhPsDev SwUpgrade FailTrap
Mise à niveau de logiciel	Echec général de mise à niveau de logiciel	Erreur	La mise à niveau de logiciel a échoué avant le téléchargement – Pas de fichier présent	Pour SYSLOG seul, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E105.0	69010500	cabhPsDev SwUpgrade FailTrap
Mise à niveau de logiciel	Echec général de mise à niveau de logiciel	Erreur	La mise à niveau de logiciel a échoué avant le téléchargement – Nombre maximal d'essais TFTP dépassé	Pour SYSLOG seul, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E106.0	69010600	cabhPsDev SwUpgrade FailTrap
Mise à niveau de logiciel	Echec général de mise à niveau de logiciel	Erreur	La mise à niveau de logiciel a échoué après le téléchargement – Fichier logiciel incompatible	Pour SYSLOG seul, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E107.0	69010700	cabhPsDev SwUpgrade FailTrap

Tableau B.1/J.191 – Evénements définis

Processus	Sous-processus	Priorité PS	Texte d'événement	Notes et détails du message	Ensemble de code d'erreur	Identifiant d'événe-ment	Nom trap
Mise à niveau de logiciel	Echec général de mise à niveau de logiciel	Erreur	La mise à niveau de logiciel a échoué après le téléchargement – Fichier logiciel endommagé	Pour SYSLOG seul, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E108.0	69010800	cabhPsDev SwUpgrade FailTrap
Mise à niveau de logiciel	Echec général de mise à niveau de logiciel	Erreur	Interruption pendant le téléchargement du logiciel – Panne de courant	Pour SYSLOG seul, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E109.0	69010900	cabhPsDev SwUpgrade FailTrap
Mise à niveau de logiciel	Echec général de mise a niveau de logiciel	Erreur	Interruption pendant le téléchargement du logiciel – Panne radio-fréquence	Pour SYSLOG seul, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E110.0	69011000	cabhPsDev SwUpgrade FailTrap
Réussite de mise à niveau de logiciel							
Mise à niveau de logiciel	Réussite de mise à niveau de logiciel	Remarque	Téléchargement du logiciel réussi – Via le système NMS	Pour SYSLOG seul, ajouter: fichier logiciel: <P1> – serveur logiciel: <P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E111.0	69011100	cabhPsDev SwUpgrade SuccessTrap
Mise à niveau de logiciel	Réussite de mise à niveau de logiciel	Remarque	Téléchargement du logiciel réussi – Via le fichier de configuration	Pour SYSLOG seul, ajouter: fichier logiciel: <P1> – serveur logiciel: < P2>. P1 = nom de fichier logiciel et P2 = adresse IP du serveur TFTP	E112.0	69011200	cabhPsDev SwUpgrade SuccessTrap

Tableau B.1/J.191 – Evénements définis

Processus	Sous-processus	Priorité PS	Texte d'événement	Notes et détails du message	Ensemble de code d'erreur	Identifiant d'événement	Nom trap
Echec DHCP après l'achèvement de l'approvisionnement					D100.0	68010000	
DHCP		Erreur	DHCP RENEW envoyé – Non réponse		D101.0	68010100	cabhPsDev DHCPFailTrap
DHCP		Erreur	DHCP REBIND envoyé – Non réponse		D102.0	68010200	cabhPsDev DHCPFailTrap
DHCP		Erreur	DHCP RENEW envoyé – Option DHCP non valide		D103.0	68010300	cabhPsDev DHCPFailTrap
DHCP		Erreur	DHCP REBIND envoyé – Option DHCP non valide		D104.0	68010400	cabhPsDev DHCPFailTrap
Echec de l'heure après achèvement de l'approvisionnement							
Heure	Heure	Avertis-sement	Demande d'heure envoyée – Pas de réponse reçue		D04.3	68000403	cabhPsDev TODFailTrap
Heure	Heure	Avertis-sement	Réponse d'heure reçue – Format de données non valide		D04.4	68000404	cabhPsDev TODFailTrap
Vérification de fichier code					E200		
Mise à niveau de logiciel	Echec général de mise à niveau de logiciel	Erreur	Contrôles de fichier code impropres	Pour SYSLOG seul, ajouter: fichier code: <P1> – serveur de fichier code: <P2>. P1 = nom de fichier code, P2 = adresse IP du serveur de fichier code	E201.0	69020100	cabhPsDev SwUpgrade FailTrap
Mise à niveau de logiciel	Echec général de mise à niveau de logiciel	Erreur	Echec de validation de certificat CVC de fabricant	Pour SYSLOG seul, ajouter: fichier code: <P1> – serveur de fichier code: <P2>. P1 = nom de fichier code, P2 = adresse IP du serveur de fichier code	E202.0	69020200	cabhPsDev SwUpgrade FailTrap
Mise à niveau de logiciel	Echec général de mise à niveau de logiciel	Erreur	Echec de validation de signature CVS de fabricant de fichier code	Pour SYSLOG seul, ajouter: fichier code: <P1> – serveur de fichier code: <P2>. P1 = nom de fichier code, P2 = adresse IP du serveur de fichier code	E203.0	69020300	cabhPsDev SwUpgrade FailTrap

Tableau B.1/J.191 – Evénements définis

Processus	Sous-processus	Priorité PS	Texte d'événement	Notes et détails du message	Ensemble de code d'erreur	Identifiant d'événement	Nom trap
Mise à niveau de logiciel	Echec général de mise a niveau de logiciel	Erreur	Echec de validation de certificat CVC de cosignataire de fichier code	Pour SYSLOG seul, ajouter: fichier code: <P1> – serveur de fichier code: <P2>. P1 = nom de fichier code, P2 = adresse IP du serveur de fichier code	E204.0	69020400	cabhPsDev SwUpgrade FailTrap
Mise à niveau de logiciel	Echec général de mise a niveau de logiciel	Erreur	Echec de validation de signature CVS de cosignataire de fichier code	Pour SYSLOG seul, ajouter: fichier code: <P1> – serveur de fichier code: <P2>. P1 = nom de fichier code, P2 = adresse IP du serveur de fichier code	E205.0	69020500	cabhPsDev SwUpgrade FailTrap
Vérification de CVC							
Mise à niveau de logiciel	Vérifica-tion de CVC	Erreur	Format de certificat CVC de fichier de configuration impropre – Serveur TFTP: <P1> – Fichier de configuration: <P2>	P1 = adresse IP de serveur TFTP P2 = Nom de fichier de configuration	E206.0	69020600	cabhPsDev SwUpgrade CVCFailTrap
Mise à niveau de logiciel	Vérifica-tion de CVC	Erreur	Echec de validation de certificat CVC de fichier de configuration – Serveur TFTP: <P1> – Fichier de configuration: <P2>	P1 = adresse IP de serveur TFTP P2 = Nom de fichier de configuration	E207.0	69020700	cabhPsDev SwUpgrade CVCFailTrap
Mise à niveau de logiciel	Vérifica-tion de CVC	Erreur	Format de certificat CVC SNMP impropre – Gestionnaire SNMP: <P1>	P1 = adresse IP du gestionnaire SNMP	E208.0	69020800	cabhPsDev SwUpgrade CVCFailTrap
Mise à niveau de logiciel	Vérifica-tion de CVC	Erreur	Echec de validation de certificat CVC SNMP – Gestionnaire SNMP: <P1>	P1=Adresse IP du gestionnaire SNMP	E209.0	69020900	cabhPsDev SwUpgrade CVCFailTrap

Tableau B.1/J.191 – Evénements définis

Processus	Sous-processus	Priorité PS	Texte d'événement	Notes et détails du message	Ensemble de code d'erreur	Identifiant d'événe-ment	Nom trap
Evénements de portail CDP					P		
CDP	CDS	Remarque	Tentative d'allocation de plus d'adresses IP LAN TRANS qu'autorisé		P01.0	80000100	cabhPsDev CDPTrap
Evénements de portail CSP							
CSP	Pare-feu	Remarque	Seuil de piratage de pare-feu de type 1 et type 2 dépassé		P101.0	80010100	cabhPsDev CSPTrap
CSP	Pare-feu	Remarque	Evénement de pare-feu de type 1 détecté	P1 = adresse IP de source, P2 = adresse IP de destination, P3 = type de protocole, P4 = nom de fichier d'ensemble actif de règles, P5 = description d'événe-ment	P102.0	80010200	cabhPsDev CSPTrap
CSP	Pare-feu	Remarque	Evénement de pare-feu de type 2 détecté	P1 = adresse IP de source, P2 = adresse IP de destination, P3 = type de protocole, P4 = nom de fichier d'ensemble actif de règles, P5 = description d'événe-ment	P103.0	80010300	cabhPsDev CSPTrap
CSP	Pare-feu	Remarque	La configuration de pare-feu a changé	P1 = description du changement dans les paramètres de configuration du pare-feu	P120.0	80012000	cabhPsDev CSPTrap
Evénements de portail CAP							
CAP	C-NAT	Remarque	CAP incapable de faire le mappage C-NAT. Pas d'adresse IP WAN-data disponible		P201.0	800201.00	cabhPsDev CAPTrap
CAP	C-NAPT	Remarque	CAP incapable de faire le mappage C-NAPT. Pas d'adresse IP WAN-data disponible		P250.0	800250.00	cabhPsDev CAPTrap

B.1 Descriptions de Trap

```
cabhPsDevInitTLVUnknownTrap  TYPE DE NOTIFICATION
      OBJETS { docsDevEvLevel,
                     docsDevEvId,
                     docsDevEvText,
                     ifPhysAddress }
      ETAT en cours
      DESCRIPTION
            "Evénement dû à la détection d'un TLV inconnu pendant le processus
            d'analyse grammaticale de TLV. Les valeurs de docsDevEvLevel,
            docsDevId, et DocsDevEvText sont tirées de l'entrée qui enregistre
            cet événement dans le tableau docsDevEventTable. La valeur de
            ifPhysAddress est l'adresse MAC du service portail. Cette partie des
            informations est uniformisée à travers tous les trap du service
            portail."
      := { cabhPsDevTraps 1 }

cabhPsDevInitTrap TYPE DE NOTIFICATION
      OBJETS { docsDevEvLevel,
                     docsDevEvId,
                     docsDevEvText,
                     ifPhysAddress,
                     docsDevServerConfigFile,
                     nombre de TLV,
                     nombre de TLV sautés }
      ETAT en cours
      DESCRIPTION
            " Un événement pour faire rapport du processus d'initialisation est
            achevé comme il est détecté dans le service portail. Les valeurs de
            docsDevEvLevel, docsDevId, et docsDevEvText sont tirées de l'entrée
            qui enregistre cet événement dans le tableau docsDevEventTable. La
            valeur de ifPhysAddress indique l'adresse MAC du service portail.
            DocsDevServerConfigFils est le nom du fichier de configuration
            utilisé. De même que le nombre de TLV dans le fichier de
            configuration et le nombre de TLV sautés. Si aucun fichier de
            configuration n'était utilisé, tous trois sont mis à 'none' (aucun).
            Cette partie des informations est uniformisée à travers tous les
            trap du service portail."
      ::= { cabhPsDevTraps 2 }

cabhPsDevInitRetryTrap TYPE DE NOTIFICATION
      OBJETS { docsDevEvLevel,
                     docsDevEvId,
                     docsDevEvText,
                     ifPhysAddress }
      ETAT en cours
      DESCRIPTION
            "Un événement pour faire rapport d'un échec survenu pendant le
            processus d'initialisation et détecté dans le service portail. Les
            valeurs de docsDevEvLevel, docsDevId, et docsDevEvText sont tirées
            de l'entrée qui enregistre cet événement dans le tableau
            docsDevEventTable. La valeur de ifPhysAddress indique l'adresse MAC
            du service portail. La valeur de ifPhysAddress indique l'adresse MAC
            du service portail.
            Cette partie des informations est uniformisée à travers tous les
            trap du service portail."
      ::= { cabhPsDevTraps 3 }
cabhPsDevDHCPFailTrap TYPE DE NOTIFICATION
```

```
      OBJETS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  docsDevServerDhcp }
      ETAT en cours
      DESCRIPTION
            " Un événement pour faire rapport sur l'échec d'un serveur DHCP. La
            valeur de docsDevServerDhcp est l'adresse IP du serveur DHCP."
      ::= { cabhPsDevTraps 4 }

cabhPsDevSwUpgradeInitTrap TYPE DE NOTIFICATION
      OBJETS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  docsDevSwFilename,
                  docsDevSwServer }
      ETAT en cours
      DESCRIPTION
            " Un événement pour faire rapport d'un événement généré par la mise
            à niveau du logiciel. Les valeurs de docsDevSwFilename, et
            docsDevSwServer indiquent le nom de la copie de logiciel et
            l'adresse IP du serveur d'où vient la copie."
      ::= { cabhPsDevTraps 5 }

cabhPsDevSwUpgradeFailTrap TYPE DE NOTIFICATION
      OBJETS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  docsDevSwFilename,
                  docsDevSwServer }
      ETAT en cours
      DESCRIPTION
            "Un événement pour faire rapport de l'échec d'une tentative de mise
            à niveau de logiciel. Les valeurs de docsDevSwFilename, et
            docsDevSwServer indiquent le nom de la copie de logiciel et
            l'adresse IP de serveur d'où vient la copie."
      ::= { cabhPsDevTraps 6 }

cabhPsDevSwUpgradeSuccessTrap TYPE DE NOTIFICATION
      OBJETS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  docsDevSwFilename,
                  docsDevSwServer }
      ETAT en cours
      DESCRIPTION
            "Un événement pour faire rapport de l'événement réussi de mise à
            niveau de logiciel. Les valeurs de docsDevSwFilename, et
            docsDevSwServer indiquent le nom de la copie de logiciel et
            l'adresse IP de serveur d'où vient la copie."
      ::= { cabhPsDevTraps 7 }

cabhPsDevSwUpgradeCVCFailTrap TYPE DE NOTIFICATION
      OBJETS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress }
```

```
      ETAT en cours
      DESCRIPTION
            "Un événement pour faire rapport de l'échec de la vérification du
            fichier code survenu pendant une tentative de mise à niveau de
            logiciel sécurisée."
      ::= { cabhPsDevTraps 8 }

cabhPsDevTODFailTrap TYPE DE NOTIFICATION
      OBJETS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  docsDevServerTime }
      ETAT en cours
      DESCRIPTION
            "Un événement pour faire rapport de l'échec d'un serveur horaire. La
            valeur de docsDevServerTime indique l'adresse IP du serveur."
      ::= { cabhPsDevTraps 9 }

cabhPsDevCDPTrap TYPE DE NOTIFICATION
      OBJETS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress,
                  addressThreshold }
      ETAT en cours
      DESCRIPTION
            "Pour faire rapport d'un événement avec le portail DHCP."
      ::= { cabhPsDevTraps 10 }

cabhPsDevCSPTrap   TYPE DE NOTIFICATION
      OBJETS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress }
      ETAT en cours
      DESCRIPTION
            "Pour faire rapport d'un événement avec le portail Sécurité."
      ::= { cabhPsDevTraps 11 }

cabhPsDevCAPTrap   TYPE DE NOTIFICATION
      OBJETS { docsDevEvLevel,
                  docsDevEvId,
                  docsDevEvText,
                  ifPhysAddress }
      ETAT en cours
      DESCRIPTION
            "Pour faire rapport d'un événement avec le portail Sécurité."
      ::= { cabhPsDevTraps 12 }
```

Annexe C

Menaces sur la sécurité et mesures préventives

Lors du développement d'une technique de sécurité, il est important de comprendre ce que sont les principales menaces pour une application ou environnement donné. Ces informations peuvent alors être utilisées pour choisir les outils de sécurité et les technologies les plus efficaces pour la protection et la prévention contre les attaques hostiles.

On a identifié les menaces principales contre la sécurité suivantes pour les abonnés et les opérateurs:

– **vol de service**: le vol de service survient sous deux formes: l'accès non autorisé aux services par câble et la copie non autorisée du contenu des services.

  L'accès non autorisé implique un abonné ou une tierce partie (comme un voisin) ayant accès aux services par câble pour lesquels ils n'ont pas payé. Les appareils peuvent être "clonés" ou modifiés pour apparaître comme des appareils qualifiés au domicile de l'abonné. Cela peut aussi dégrader les performances de fourniture du service car ces appareils consomment des ressources de transport supplémentaires sur le câble HFC et les liaisons au domicile.

  La duplication non autorisée implique habituellement un abonné ou une tierce partie (comme un voisin) qui fait des copies illégales du contenu du service. Dans certains cas, ces copies sont distribuées à d'autres consommateurs sans l'aval de l'opérateur ou du fournisseur du contenu;

– **attaques de déni de service (DOS, *denial of service*)**: les attaques de déni de service peuvent survenir lorsqu'une entité tierce (attaquant, consommateur mécontent, etc.) interrompt les communications normales et la fourniture de services entre les opérateurs et leurs abonnés. Des transmissions de données dolosives venant de ce qui semble être un appareil/source valide, peuvent être injectées dans la liaison locale et dégrader sévèrement les fonctions normales. Ces transmissions de données dolosives peuvent s'étendre au réseau de câble HFC de l'opérateur et y causer des problèmes de performances;

– **confidentialité du service**: la menace sur la confidentialité du service implique une tierce partie (voisins, attaquant, etc.) surveillant/recevant les informations sur un abonné et les services qu'il utilise. Ceci peut provoquer le vol de mots de passe ou d'informations sur la configuration des appareils, ce qui permet aux attaquants d'obtenir ultérieurement accès aux ressources réseau et fichiers/données confidentiels de l'abonné.

Un certain nombre de méthodes différentes peuvent être utilisées pour prévenir les menaces contre la sécurité mentionnées ci-dessus. Malheureusement, une seule méthode ne peut les empêcher toutes, mais leur combinaison peut être la meilleure ligne de défense. On peut utiliser les mesures préventives suivantes:

– **authentification**: l'authentification implique la vérification que les entités expéditrice et réceptrice sont bien ce qu'elles prétendent être. Ceci inclut la source du service, l'appareil récepteur et l'abonné.

  L'authentification aide à prévenir le vol de service en validant les appareils et les utilisateurs d'extrémité, mais n'empêche pas la copie illégale des contenus ni ne prévient l'accès non autorisé de tierces parties qui surveilleraient la liaison. Elle est efficace dans la prévention des attaques de déni de service parce que le trafic peut être rejeté s'il ne vient pas d'une source valide. Par elle-même, l'authentification ne fournit aucun support de confidentialité de service et il faut utiliser le chiffrement;

– **protection contre la copie**: ces méthodes de protection contre la copie limitent la capacité d'un appareil récepteur à faire des copies non autorisées du contenu du service.

  La protection contre la copie aide à prévenir le vol de service en limitant le nombre de copies qui peuvent être faites, mais ne protège pas contre l'accès non autorisé aux services. Elle ne protège pas non plus contre le déni de service et n'assure pas la protection de la confidentialité du service. En général, cette mesure préventive est implémentée à des couches d'application plus élevées;

– **chiffrement des données**: le chiffrement des données empêche la découverte et l'accès non autorisés aux données.

  Le chiffrement des données est efficace pour la confidentialité des données et la protection contre le vol de service. Le chiffrement empêche de lire les données en l'absence de la clé de déchiffrement correcte, cependant, il ne valide pas les entités source ou de réception et il ne donne pas de protection contre la copie après le déchiffrement des données. Il ne protège pas non plus contre les attaques de déni de service;

– **pare-feu**: les applications de pare-feu empêchent le trafic réseau de passer d'un domaine à l'autre à moins qu'il ne satisfasse à certains critères établis par l'abonné ou l'opérateur. Dans les applications à domicile, les pare-feu sont typiquement situés sur les appareils de passerelle résidentielle qui connectent le réseau de câble HFC au domicile.

  Une application de pare-feu aide à prévenir les attaques de déni de service et les attaques contre la confidentialité à partir du côté réseau régional (WAN) du pare-feu, mais elle n'empêche pas ce type d'attaques venant du côté domicile du pare-feu. Elle ne protège pas non plus contre le vol de service;

– **sécurité des messages de gestion**: cette méthode de prévention implique l'authentification et le chiffrement des seuls messages de gestion du réseau. Les messages de gestion du réseau sont utilisés pour la configuration des appareils, la commande/surveillance du réseau, l'approvisionnement en service, et les réservations de qualité de service (QS).

  La sécurité des messages de gestion est un bon mécanisme de prévention des attaques de déni de service grâce à l'authentification et au chiffrement des messages de gestion. Les informations de configuration réseau et personnelles de l'abonné sont aussi protégées contre les attaques contre la confidentialité, mais le contenu du service ne l'est pas. Aussi la sécurité des messages de gestion n'empêche pas le vol du contenu du service par des entités non autorisées.

Annexe D

Applications par traduction CAT et pare-feu

L'existence des fonctions de traduction NAT et de pare-feu est connue pour interrompre un certain nombre de protocoles et d'applications. Les protocoles et applications dont la liste figure ci-après DOIVENT fonctionner à travers les implémentations de traduction CAT et de pare-feu. Cette liste ne donne pas un ordre de priorité.

1) FTP;
2) application d'homologue à homologue (c'est-à-dire, Gnutella, LimeWire, BearShare, Morpheus, etc.);
3) IPsec;
4) IGMP et IP Multidiffusion;
5) H.323 (Utilisé dans Windows® pour diverses applications);
6) applications de messagerie instantanée (c'est-à-dire, AOL, Microsoft, Yahoo, etc.);
7) E-mail (SMTP et POP);
8) applications de répartition de média (c'est-à-dire, Real, MediaPlayer, etc.).

De plus, les fabricants DEVRAIENT faire tout leur possible pour accepter les applications de jeu en ligne au moyen de l'implémentation de la traduction CAT et du pare-feu.

Annexe E

Bases MIB

E.1 Base MIB de service portail (PS)

La base MIB de service portail DOIT être implémentée comme défini ci-dessous.

```
CABH-PS-DEV-MIB DEFINITIONS ::= BEGIN
IMPORTS
     MODULE-IDENTITY,
     OBJECT-TYPE,
     Integer32,
     NOTIFICATION-TYPE
                                    FROM SNMPv2-SMI
     TruthValue,
     DisplayString,
     PhysAddress,
     DateAndTime,
     TEXTUAL-CONVENTION
                                    FROM SNMPv2-TC
     OBJECT-GROUP,
     MODULE-COMPLIANCE,
     NOTIFICATION-GROUP
                                    FROM SNMPv2-CONF

     InetAddressType,
     InetAddress,
     InetAddressIPv4,
     InetAddressIPv6
                                    FROM INET-ADDRESS-MIB
```

```
     docsDevSwCurrentVers,
     docsDevEvLevel,
     docsDevEvId,
     docsDevEvText,
     docsDevSwFilename,
     docsDevSwServer,
                FROM DOCS-CABLE-DEVICE-MIB -- RFC 2669

     cabhCdpServerDhcpAddress,
     cabhCdpWanDataAddrClientId
                       FROM CABH-CDP-MIB

     clabProjCableHome
                                      FROM CLAB-DEF-MIB;

--================================================================================
--
--   Historique:
--================================================================================

cabhPsDevMib MODULE-IDENTITY
     DERNIÈRE MISE À JOUR    "0112190000Z" -- 19 décembre 2001
     ORGANISATION  "Cable    NMP Group"
     CONTACT-INFO
     "Kevin Luehrs
     Adresse postale: Cable Television Laboratories, Inc.
                400 Centennial Parkway
                Louisville, Colorado 80027-1266
       U.S.A.
       Téléphone: +1 303-661-9100
       Fax: +1 303-661-9199
       E-mail: k.luehrs@cablelabs.com"
     DESCRIPTION
       "Le présent module de base MIB fournit les objets de gestion de base pour
       l'appareil de service portail. Le paramètre de service portail décrit les
       attributs généraux d'appareil de service portail et leurs
       caractéristiques de comportement. La plus grande partie de la base MIB
       d'appareil de service portail est nécessaire pour le téléchargement de la
       configuration."

-- Conventions textuelles
     X509Certificate ::= TEXTUAL-CONVENTION
       ETAT en cours
       DESCRIPTION
          "Un certificat numérique X.509 codé comme un objet DER en ASN.1."
       CHAINE D'OCTETS DE SYNTAXE (TAILLE (0..4096))

--
-- suppose SNMPv3
-- la gestion du chargement est uniquement selon DOCSIS 1.1 --
--

IDENTIFICATEUR D'OBJET cabhPsDevMibObjects ::= { cabhPsDevMib 1 }
IDENTIFICATEUR D'OBJET cabhPsDevBase ::= { cabhPsDevMibObjects 1 }
IDENTIFICATEUR D'OBJET cabhPsDevProv ::= { cabhPsDevMibObjects 2 }

--
-- Le groupe suivant décrit les objets de base dans le service portail.
-- Ces paramètres sont fondés sur l'appareil.
--

TYPE D'OBJET cabhPsDevDateTime
     SYNTAXE       DateAndTime
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
```

```
     DESCRIPTION
       "La date et l'heure, avec des informations facultatives sur l'heure
       locale."
     ::= { cabhPsDevBase 1 }

TYPE D'OBJET cabhPsDevResetNow
     SYNTAXE       TruthValue
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "Mettre cet objet à true(1) provoque le réamorçage de l'appareil. La
       lecture de cet objet envoie toujours le retour false(2). Lorsque
       cabhPsDevResetNow est mis à Vrai (true), les actions suivantes
       surviennent:
       1) vide toutes les statistiques dans le service portail.
       2) vide les enregistrements d'historique
       3) vide toutes les associations de sécurité.
       4) initialise tous les paramètres de configuration.
       5) supprime toutes les traductions d'adresse
       6) supprime tous les mappages de noms FQDN à IP.
       7) supprime toutes les traductions d'ARP mémorisées.
       8) le flux d'approvisionnement débute à l'étape PS – 1."
     ::= { cabhPsDevBase 2 }

TYPE D'OBJET cabhPsDevSerialNumber
     SYNTAXE       DisplayString (TAILLE (0..128))
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "Numéro de série du fabricant pour ce service portail. Ce paramètre est
       fourni par le fabricant et est mémorisé dans une mémoire non volatile."
     ::= { cabhPsDevBase 3 }

TYPE D'OBJET cabhPsDevHardwareVersion
     SYNTAXE       DisplayString (TAILLE (0..48))
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "Version de matériel du fabricant pour ce service portail. Ce
       paramètre est fourni par le fabricant et est mémorisé dans une mémoire
       non volatile."
     ::= { cabhPsDevBase 4 }

TYPE D'OBJET cabhPsDevMacAddress
     SYNTAXE       PhysAddress
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "Adresse MAC WAN-MAN du service portail. Typiquement, les adresses
       WAN-MAN et WAN-DATA du service portail seront identiques. Les
       identifiants du client ne seront pas les mêmes de façon que chacune
       puisse être allouée à une adresse IP différente."
     ::= { cabhPsDevBase 5 }

TYPE D'OBJET cabhPsDevTypeIdentifier
     SYNTAXE       DisplayString
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "C'est une copie de l'identifiant de type d'appareil utilisé dans
       l'option 60 de DHCP échangée entre le service portail et le serveur
       dhcp."
     ::= { cabhPsDevBase 6 }
```

```
TYPE D'OBJET cabhPsDevResetDefaults
     SYNTAXE       TruthValue
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "Mettre cet objet à True (Vrai) met tous les paramètres à leurs valeurs
       par défaut d'usine."
     ::= { cabhPsDevBase 7 }

TYPE D'OBJET cabhPsDevWanManClientId
     SYNTAXE       CHAINE D'OCTET (TAILLE (1..80))
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "C'est l'identifiant de client utilisé pour les demandes WAN-MAN DHCP.
       La valeur par défaut est l'adresse MAC à 6 octets."
     ::= { cabhPsDevBase 8 }

TYPE D'OBJET cabhPsDevTodSyncStatus
     SYNTAXE       TruthValue
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "Cet objet indique si le service portail a été capable de réussir à
       se synchroniser avec le serveur horaire du réseau câblé. Le service
       portail met cet objet à true(1) s'il a réussi à synchroniser son
       heure avec celle du serveur horaire. Le service portail met cet
       objet à false(2) (Faux) s'il n'a pas réussi à se synchroniser avec
       le serveur horaire."
     REFERENCE
       " "
     VALEUR PAR DEFAUT { false }
     ::= { cabhPsDevBase 9 }

TYPE D'OBJET cabhPsDevProvMode
     SYNTAXE  ENTIER
     {
          dhcpmode (1),
          snmpmode (2)
     }
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "Cet objet indique le mode d'approvisionnement dans lequel opère le
       service portail. Si le service portail reçoit des informations de
       fichier de configuration de PS (adresse de serveur et nom de
       fichier) dans le message DHCP produit par le serveur DHCP dans le
       réseau câblé, le service portail met cet objet en mode DHCP(1). Si
       le service portail reçoit l'option DHCP 177 sous-option 51 ET ne
       reçoit pas d'information de fichier de configuration PS dans le
       message DHCP qu'il reçoit du serveur DHCP dans le réseau câblé, le
       service portail met cet objet à mode SNMP(2)."
     ::= { cabhPsDevBase 10 }

TYPE D'OBJET cabhPsDevDwnldMode
     SYNTAXE  ENTIER
     {
       standard     (1),
       enhanced     (2)
     }
     MAX-ACCESS    en lecture seule
     ETAT     en cours
```

```
     DESCRIPTION
       "C'est le mode de téléchargement qu'utilisera le service portail."
       ::= { cabhPsDevBase 11 }

--
--   Le groupe suivant définit les paramètres spécifiques d'approvisionnement--
--

TYPE D'OBJET cabhPsDevProvisioningTimer
     SYNTAXE       ENTIER (0..16383)
     UNITÉS        "minutes"
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "Cet objet permet à l'usager de régler la durée du temporisateur
       d'approvisionnement. La valeur est en minutes. Régler le temporisateur à
       0 le désactive. La valeur par défaut pour le temporisateur est 5."
     VALEUR PAR DEFAUT {5}
     ::= {cabhPsDevProv 1}

TYPE D'OBJET cabhPsDevProvConfigFile
     SYNTAXE       DisplayString(TAILLE(1..128))
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "C'est l'URL de l'hôte TFTP pour télécharger les paramètres
       d'approvisionnement et de configuration sur cet appareil. Le retour
       est NULL si l'adresse du serveur est inconnue."
     ::= { cabhPsDevProv 2 }

TYPE D'OBJET cabhPsDevProvConfigHash
     SYNTAXE       CHAINE D'OCTET (TAILLE(20))
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "Hachage du contenu du fichier de configuration, calculé et envoyé au
       service portail avant d'envoyer le fichier de configuration. Pour
       l'algorithme d'authentification SHA-1 le hachage a une longueur de
       160 bits."
     ::= { cabhPsDevProv 3 }

TYPE D'OBJET cabhPsDevProvConfigFileSize
     SYNTAXE       Integer32
     UNITÉS        "octets"
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "Taille du fichier de configuration."
     ::={ cabhPsDevProv 4 }

TYPE D'OBJET cabhPsDevProvConfigTLVProcessed
     SYNTAXE       ENTIER (0..16383)
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "Nombre de TLV traités dans le fichier de configuration."
     ::={ cabhPsDevProv 5 }

TYPE D'OBJET cabhPsDevProvConfigTLVRejected
     SYNTAXE       ENTIER (0..16383)
     MAX-ACCESS    en lecture seule
     ETAT          en cours
```

```
     DESCRIPTION
       "Nombre de TLV rejetés dans le fichier de configuration."
     ::={ cabhPsDevProv 6 }

TYPE D'OBJET cabhPsDevProvSolicitedKeyTimeout
     SYNTAXE       Integer32 (15..600)
     UNITÉS        "secondes"
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "Cette temporisation ne s'applique que lorsque le serveur
       d'approvisionnement a débuté la gestion de clés (avec un message Wake Up
       (réveil)) pour SNMPv3. C'est la période pendant laquelle le service
       portail va sauvegarder un numéro (à l'intérieur du champ Numéro de
       séquence) tiré de la Demande de point d'accès et attendre la Réponse de
       point d'accès correspondante venant du serveur d'approvisionnement."
     VALEUR PAR DEFAUT { 120 }
     ::= { cabhPsDevProv 7 }

TYPE D'OBJET cabhPsDevProvState
     SYNTAXE  ENTIER
     {
          pass          (1),
          inProgress    (2),
          fail          (3)
     }
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "Cet objet indique l'état d'achèvement du processus
       d'initialisation. Les états de réussite ou d'échec surviennent après
       achèvement du flux d'initialisation. InProgress (en cours)
       intervient depuis le début de l'initialisation du service portail
       jusqu'à la fin de l'initialisation du service portail."
       ::= { cabhPsDevProv 8 }

TYPE D'OBJET cabhPsDevProvAuthState
     SYNTAXE   ENTIER
     {
          accepted      (1),
           rejected     (2)
     }
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "Cet objet indique l'état d'authentification du fichier de
       configuration."
     ::= { cabhPsDevProv 9 }

TYPE D'OBJET cabhPsDevProvCorrelationId
     SYNTAXE       Integer32
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "Valeur aléatoire générée par le service portail et destinée à être
       utilisée dans l'autorisation d'enregistrement. Elle n'est destinée à
       être utilisée que dans les messages d'initialisation du service
       portail et pour le téléchargement du fichier de configuration PS.
       Cette valeur apparaît à la fois dans les informations
       cabhPsDevProvisioningStatus et cabhPsDevProvisioningEnrollmentReport
       pour vérifier que le chargement du fichier de configuration est bien
       en cours."
     ::= { cabhPsDevProv 10 }
```

```
TYPE D'OBJET cabhPsDevTimeServerAddrType
     SYNTAXE       InetAddressType
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "Type d'adresse IP du serveur horaire (RFC 868). IP version 4 est
       utilisée en principe."
     ::= { cabhPsDevProv 11 }

TYPE D'OBJET cabhPsDevTimeServerAddr
     SYNTAXE       InetAddress
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "Adresse IP du serveur horaire (RFC 868). Retourne 0.0.0.0 si
       l'adresse IP du serveur horaire est inconnue."
     ::= { cabhPsDevProv 12 }

--
--   groupe de notification est destiné à des extensions futures.
--

IDENTIFICATEUR D'OBJET cabhPsNotification  ::= { cabhPsDevMib 2 0 }
IDENTIFICATEUR D'OBJET cabhPsConformance   ::= { cabhPsDevMib 3 }
IDENTIFICATEUR D'OBJET cabhPsCompliances   ::= { cabhPsConformance 1 }
IDENTIFICATEUR D'OBJET cabhPsGroups ::= { cabhPsConformance 2 }

--
--   Groupe de notification
--

TYPE DE NOTIFICATION cabhPsDevInitTLVUnknownTrap
     OBJETS   {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevMacAddress
     }
     ETAT en cours
     DESCRIPTION
       "Evénement dû à la détection d'un TLV inconnu pendant le processus
       d'analyse grammaticale de TLV. Les valeurs de docsDevEvLevel,
       docsDevId, et docsDevEvText sont tirées de l'entrée qui enregistre
       cet événement dans le tableau docsDevEventTable. La valeur de
       cabhPsDevMacAddress indique l'adresse MAC du service portail. Cette
       partie des informations est uniforme sur tous les Trap du service
       portail."
     ::= { cabhPsNotification 1 }

TYPE DE NOTIFICATION cabhPsDevInitTrap
     OBJETS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevMacAddress,
       cabhPsDevProvConfigFile,
       cabhPsDevProvConfigTLVProcessed,
       cabhPsDevProvConfigTLVRejected
     }
     ETAT      en cours
     DESCRIPTION
       "Cette information est produite pour confirmer la réussite de
       l'achèvement du processus d'approvisionnement."
     ::= { cabhPsNotification 2 }
```

```
TYPE DE NOTIFICATION cabhPsDevInitRetryTrap
     OBJETS  {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
     cabhPsDevMacAddress
     }
     ETAT      en cours
     DESCRIPTION
       "Un événement pour faire rapport de l'échec survenu pendant le
       processus d'initialisation est détecté dans le PS."
     ::= { cabhPsNotification 3 }

TYPE DE NOTIFICATION cabhPsDevDHCPFailTrap
     OBJETS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevMacAddress,
       cabhCdpServerDhcpAddress
     }
     ETAT      en cours
     DESCRIPTION
       "Un événement pour faire rapport de l'échec d'un serveur DHCP. La
       valeur de cabhCdpServerDhcpAddress est l'adresse IP du serveur DHCP."
     ::= { cabhPsNotification 4 }

TYPE DE NOTIFICATION cabhPsDevSwUpgradeInitTrap
     OBJETS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevMacAddress,
       docsDevSwFilename,
       docsDevSwServer
     }
     ETAT      en cours
     DESCRIPTION
       "Un événement pour faire rapport d'un événement initialisé par la
       mise à niveau de logiciel. Les valeurs de docsDevSwFilename, et
       docsDevSwServer indiquent le nom de la copie de logiciel et
       l'adresse IP du serveur dont la copie est issue."
     ::= { cabhPsNotification 5 }

TYPE DE NOTIFICATION cabhPsDevSwUpgradeFailTrap
     OBJETS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevMacAddress,
       docsDevSwFilename,
       docsDevSwServer
     }
     ETAT      en cours
     DESCRIPTION
       "Un événement pour faire rapport de l'échec d'une tentative de mise à
       niveau de logiciel. Les valeurs de docsDevSwFilename, et
       docsDevSwServer indiquent le nom de la copie de logiciel et
       l'adresse IP du serveur dont la copie est issue."
     ::= { cabhPsNotification 6 }
```

```
TYPE DE NOTIFICATION cabhPsDevSwUpgradeSuccessTrap
     OBJETS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevMacAddress,
       docsDevSwFilename,
       docsDevSwServer
     }
     ETAT      en cours
     DESCRIPTION
       "Un événement pour faire rapport d'un événement de réussite de la
       mise à niveau de logiciel. Les valeurs de docsDevSwFilename, et
       docsDevSwServer indiquent le nom de la copie de logiciel et
       l'adresse IP du serveur dont la copie est issue."
     ::= { cabhPsNotification 7 }

TYPE DE NOTIFICATION cabhPsDevSwUpgradeCVCFailTrap
     OBJETS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevMacAddress
     }
     ETAT      en cours
     DESCRIPTION
       "Un événement pour faire rapport de l'échec de la vérification du
       fichier code survenu durant une tentative de mise à niveau sécurisée
       de logiciel."
     ::= { cabhPsNotification 8 }

TYPE DE NOTIFICATION cabhPsDevTODFailTrap
     OBJETS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevTimeServerAddr
     }
     ETAT en cours
     DESCRIPTION
       "Un événement pour faire rapport de l'échec d'un serveur horaire. La
       valeur de cabhPsDevTimeServerAddr indique l'adresse IP du serveur."
     ::= { cabhPsNotification 9 }

TYPE DE NOTIFICATION cabhPsDevCdpWanDataIpTrap
     OBJETS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhCdpWanDataAddrClientId
     }
     ETAT en cours
     DESCRIPTION
       "Un événement pour faire rapport de l'échec du service portail à
       obtenir toutes les adresses IP WAN-Data nécessaires.
       cabhCdpWanDataAddrClientId indique l'identifiant de client pour
       lequel l'échec est intervenu."
     ::= { cabhPsNotification 10 }
```

```
TYPE DE NOTIFICATION cabhPsDevCdpThresholdTrap
     OBJETS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevMacAddress,
       cabhCdpLanTransThreshold
     }
     ETAT en cours
     DESCRIPTION
       "Un événement pour faire rapport du dépassement du seuil de LAN-Trans."
     ::= { cabhPsNotification 11 }

TYPE DE NOTIFICATION cabhPsDevCspTrap
     OBJETS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevMacAddress
     }
     ETAT en cours
     DESCRIPTION
       "Pour faire rapport d'un événement avec le portail de sécurité câble."
     ::= { cabhPsNotification 12 }

TYPE DE NOTIFICATION cabhPsDevCapTrap
     OBJETS {
       docsDevEvLevel,
       docsDevEvId,
       docsDevEvText,
       cabhPsDevMacAddress
     }
     ETAT en cours
     DESCRIPTION
       "Pour faire rapport d'un événement avec le portail d'adresse câble."
     ::= { cabhPsNotification 13 }

TYPE DE NOTIFICATION cabhPsDevProvEnrollTrap
     OBJETS {
       cabhPsDevHardwareVersion,
       docsDevSwCurrentVers,
       cabhPsDevTypeIdentifier,
       cabhPsDevMacAddress,
       cabhPsDevProvCorrelationId
     }
     ETAT en cours
     DESCRIPTION
       "Cette information est produite pour initialiser la processus
       d'approvisionnement."
     REFERENCE
       "Information comme définie dans la norme RFC 1902."
     ::= { cabhPsNotification 14 }

-- déclarations de conformité

MODULE DE CONFORMITÉ cabhPsBasicCompliance
     ETAT     en cours
     DESCRIPTION
       "Déclaration de conformité pour les appareils qui mettent en œuvre
       la caractéristique de service portail."
     MODULE   --cabhPsMib

-- groupes obligatoires inconditionnels
```

```
     GROUPES OBLIGATOIRES {
       cabhPsGroup
     }

::= { cabhPsCompliances 3 }

GROUPE D'OBJET cabhPsGroup
     OBJETS {
       cabhPsDevDateTime,
       cabhPsDevResetNow,
       cabhPsDevSerialNumber,
       cabhPsDevHardwareVersion,
       cabhPsDevMacAddress,
       cabhPsDevTypeIdentifier,
          cabhPsDevResetDefaults,
          cabhPsDevWanManClientId,
          cabhPsDevTodSyncStatus,
       cabhPsDevProvMode,
       cabhPsDevDwnldMode,

       cabhPsDevProvisioningTimer,
          cabhPsDevProvConfigFile,
          cabhPsDevProvConfigHash,
          cabhPsDevProvConfigFileSize,
          cabhPsDevProvConfigTLVProcessed,
          cabhPsDevProvConfigTLVRejected,
          cabhPsDevProvSolicitedKeyTimeout,
          cabhPsDevProvState,
          cabhPsDevProvAuthState,
       cabhPsDevProvCorrelationId,
       cabhPsDevTimeServerAddrType,
       cabhPsDevTimeServerAddr

     }
     ETAT      en cours
     DESCRIPTION
       "Groupe d'objets pour base MIB de service portail."
     ::= { cabhPsGroups 1 }

GROUPE DE NOTIFICATION cabhPsNotificationGroup
     NOTIFICATIONS { cabhPsDevInitTLVUnknownTrap, cabhPsDevInitTrap,
cabhPsDevInitRetryTrap,
          cabhPsDevDHCPFailTrap, cabhPsDevSwUpgradeInitTrap,
cabhPsDevSwUpgradeFailTrap,
          cabhPsDevSwUpgradeSuccessTrap, cabhPsDevSwUpgradeCVCFailTrap,
cabhPsDevTODFailTrap,
          cabhPsDevCdpWanDataIpTrap, cabhPsDevCdpThresholdTrap,
cabhPsDevCspTrap,
          cabhPsDevCapTrap, cabhPsDevProvEnrollTrap }
     ETAT      en cours
     DESCRIPTION
          "Ces notifications traitent du changement d'état de l'appareil de
          service portail."
     ::= { cabhPsGroups 2 }

FIN
```

E.2 Base MIB de portail d'essai câble

La base MIB de portail CTP DOIT être implémentée comme défini ci-dessous.

```
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;

--============================================================================
--
--   Historique:
--
--============================================================================

UNITÉ DE MODULE cabhCtpMib
     DERNIÈRE MISE À JOUR    "0112190000Z" -- 19 décembre 2001
     ORGANISATION       "Cable NMP Group"
     CONTACT-INFO
       "Kevin Luehrs
       Adresse postale: Cable Television Laboratories, Inc.
          400 Centennial Parkway
          Louisville, Colorado 80027-1266
          U.S.A.
          Téléphone: +1 303-661-9100
          Fax: +1 303-661-9199
          E-mail: k.luehrs@cablelabs.com"
     DESCRIPTION
       "Ce module de base MIB définit les commandes de diagnostic proposées
       par le portail d'essai câble (CTP).
       Accusés de réception:
       "
     ::= { clabProjCableHome 5 }

-- Conventions textuelles

--
-- suppose SNMPv3
-- la gestion de chargement de logiciel est seulement selon DOCSIS 1.1.
--

IDENTIFICATEUR D'OBJET cabhCtpObjects ::= { cabhCtpMib 1 }
IDENTIFICATEUR D'OBJET cabhCtpBase ::= { cabhCtpObjects 1 }
IDENTIFICATEUR D'OBJET cabhCtpConnSpeed ::= { cabhCtpObjects 2 }
IDENTIFICATEUR D'OBJET cabhCtpPing ::= { cabhCtpObjects 3 }

--
-- Le groupe suivant décrit les objets de base dans le portail de gestion
-- câble.
--
```

```
TYPE D'OBJET cabhCtpReset
       SYNTAXE          TruthValue
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Mettre cet objet à true(1) provoque la fin de tous les essais. La
       lecture de cet objet donne toujours en retour false(2). Lorsque
       cabhCtpReset est mis à true, les actions suivantes surviennent:
       1) termine tous les essais de diagnostic en cours.
       2) efface toutes les statistiques de diagnostic."
     ::= { cabhCtpBase 1 }

--
--   Paramètres et résultats de la commande de vitesse de connexion
--

TYPE D'OBJET cabhCtpConnSrcIpType
       SYNTAXE          InetAddressType
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Type d'adresse IP utilisée comme adresse source pour l'essai de
       vitesse de connexion."
     VALEUR PAR DEFAUT { ipv4 }
     ::= { cabhCtpConnSpeed 1 }

TYPE D'OBJET cabhCtpConnSrcIp
       SYNTAXE          InetAddress
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Adresse IP utilisée comme adresse source pour l'essai de vitesse de
       connexion. Typiquement, l'adresse sera la valeur dans
       cabhCdpServerRouter. L'adresse par défaut est 192.168.0.1."
       REFERENCE
          "Paragraphe 6.4.3.2 de la spécification"
       VALEUR PAR DEFAUT { 'c0a80001'h }   -- 192.168.0.1
       ::= { cabhCtpConnSpeed 2 }

TYPE D'OBJET cabhCtpConnDestIpType
       SYNTAXE          InetAddressType
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Type d'adresse IP utilisée comme adresse de destination pour
       l'essai de vitesse de connexion."
       ::= { cabhCtpConnSpeed 3 }

TYPE D'OBJET cabhCtpConnDestIp
       SYNTAXE          InetAddress
       MAX-ACCESS  en lecture-écriture
     ETAT     en cours
     DESCRIPTION
       "Adresse IP utilisée comme adresse de destination pour l'essai de
       vitesse de connexion."
       ::= { cabhCtpConnSpeed 4 }

TYPE D'OBJET cabhCtpConnProto
       SYNTAXE          ENTIER {
                  udp         (1),
                  tcp         (2)
                  }
       MAX-ACCESS  en lecture-écriture
```

```
     ETAT      en cours
     DESCRIPTION
       "Protocole utilisé dans l'essai de vitesse de connexion. L'essai de
       TCP est facultatif."
       VALEUR PAR DEFAUT { udp }
       ::= { cabhCtpConnSpeed 5 }

TYPE D'OBJET cabhCtpConnPort
       SYNTAXE          ENTIER (1..65535)
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Port utilisé pour l'essai de vitesse de connexion."
     VALEUR PAR DEFAUT {7}
     ::= { cabhCtpConnSpeed 6 }

TYPE D'OBJET cabhCtpConnNumPkts
     SYNTAXE       ENTIER (1..255)
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "Nombre de paquets à envoyer."
       VALEUR PAR DEFAUT {1}
       ::= { cabhCtpConnSpeed 7 }

TYPE D'OBJET cabhCtpConnPktSize
       SYNTAXE          ENTIER (64..1518)
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Taille des trames d'essai."
       REFERENCE
       ""
       ::= { cabhCtpConnSpeed 8 }

TYPE D'OBJET cabhCtpConnTimeOut
       SYNTAXE          ENTIER (0..600000)      -- Max 10 minutes
       UNITÉS           "millisecondes"
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Valeur de temporisation pour la réponse. Une valeur de zéro indique
       l'absence de temporisation et ne peut être utilisée que pour TCP."
       VALEUR PAR DEFAUT {600000}
     ::= { cabhCtpConnSpeed 9 }

TYPE D'OBJET cabhCtpConnControl
          SYNTAXE  ENTIER {
                        notRun        (1),
                        start         (2),
                        abort         (3)
                        }
       MAX-ACCESS  en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "Commande pour l'essai de vitesse de connexion. La valeur notRun est
       utilisée pour indiquer qu'il n'a jamais été exécuté. Ce paramètre
       ne devrait être établi que via SNMP."
       VALEUR PAR DEFAUT { notRun(1) }
     ::= { cabhCtpConnSpeed 10 }
```

```
TYPE D'OBJET cabhCtpConnStatus
      SYNTAXE          ENTIER {
                       running       (1),
                       complete      (2),
                       aborted       (3)
                       }
      MAX-ACCESS       en lecture seule
    ETAT               en cours
    DESCRIPTION
      "Etat de l'essai en cours d'exécution ou dernièrement exécuté."
      VALEUR PAR DEFAUT { complete(2) }
      ::= { cabhCtpConnSpeed 11 }

TYPE D'OBJET cabhCtpConnPktsSent
      SYNTAXE          ENTIER (0..255)
    MAX-ACCESS         en lecture seule
    ETAT               en cours
    DESCRIPTION
      "Nombre de paquets envoyés."
      ::= { cabhCtpConnSpeed 12 }

TYPE D'OBJET cabhCtpConnPktsRecv
      SYNTAXE          ENTIER (0..255)
      MAX-ACCESS       en lecture seule
    ETAT               en cours
    DESCRIPTION
      "Nombre de paquets reçus."
    ::= { cabhCtpConnSpeed 13 }

TYPE D'OBJET cabhCtpConnAvgRTT
    SYNTAXE        ENTIER (0..600000)
    UNITÉS         "milliseconds"
    MAX-ACCESS     en lecture seule
    ETAT           en cours
    DESCRIPTION
      "La moyenne résultante des temps d'aller-retour pour les paquets
      d'accusé de réception."
      ::= { cabhCtpConnSpeed 14 }

TYPE D'OBJET cabhCtpConnMaxRTT
      SYNTAXE          ENTIER (0..600000)
      UNITÉS           "milliseconds"
      MAX-ACCESS       en lecture seule
    ETAT               en cours
    DESCRIPTION
      "Le maximum résultant des temps d'aller -retour des paquets d'accusé
      de réception."
      ::= { cabhCtpConnSpeed 15 }

TYPE D'OBJET cabhCtpConnMinRTT
      SYNTAXE          ENTIER (0..600000)
      UNITÉS           "millisecondes"
      MAX-ACCESS       en lecture seule
    ETAT               en cours
    DESCRIPTION
      "Temps minimal constaté d'aller-retour des paquets d'accusé de
      réception."
      ::= { cabhCtpConnSpeed 16 }

TYPE D'OBJET cabhCtpConnNumIcmpError
      SYNTAXE          ENTIER (0..255)
      MAX-ACCESS       en lecture seule
    ETAT               en cours
```

```
     DESCRIPTION
       "Nombre d'erreurs ICMP."
       ::= { cabhCtpConnSpeed 17 }

TYPE D'OBJET cabhCtpConnIcmpError
       SYNTAXE          ENTIER (0..255)
       MAX-ACCESS       en lecture seule
     ETAT               en cours
     DESCRIPTION
       "Dernière erreur ICMP."
     ::= { cabhCtpConnSpeed 18 }

--
--   Paramètres et résultats pour la commande Ping
--

TYPE D'OBJET cabhCtpPingSrcIpType
       SYNTAXE          InetAddressType
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Type d'adresse IP utilisé comme adresse source pour l'essai de Ping."
       ::= { cabhCtpPing 1 }

TYPE D'OBJET cabhCtpPingSrcIp
       SYNTAXE          InetAddress
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Adresse IP utilisée comme adresse source pour l'essai de Ping.
       Typiquement, l'adresse sera la valeur de l'adresse IP WAN-Man du service
       portail. L'adresse 192.168.0.x est utilisée."
       ::= { cabhCtpPing 2 }

TYPE D'OBJET cabhCtpPingDestIpType
       SYNTAXE          InetAddressType
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Type d'adresse IP de destination utilisé comme adresse de destination
       pour l'essai de Ping."
       ::= { cabhCtpPing 3 }

TYPE D'OBJET cabhCtpPingDestIp
       SYNTAXE          InetAddress
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Adresse IP de destination utilisée comme adresse de destination pour
       l'essai de Ping."
     ::= { cabhCtpPing 4 }

TYPE D'OBJET cabhCtpPingProto
       SYNTAXE          ENTIER {
                        icmp (1),
                        }
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Protocole utilisé pour rassembler les informations de topologie."
       VALEUR PAR DEFAUT { icmp }
     ::= { cabhCtpPing 5 }
```

```
TYPE D'OBJET cabhCtpPingNumPkts
       SYNTAXE          ENTIER (1..4)
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Nombre de paquets à envoyer à chaque hôte."
       VALEUR PAR DEFAUT {1}
       ::= { cabhCtpPing 6 }

TYPE D'OBJET cabhCtpPingPktSize
       SYNTAXE          ENTIER (64..1518)
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Taille des trames d'essai."
       VALEUR PAR DEFAUT {64}
       ::= { cabhCtpPing 7 }

TYPE D'OBJET cabhCtpPingTimeBetween
       SYNTAXE          ENTIER (0..600000)
       UNITÉS           "milliseconds"
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Le temps séparant l'envoi d'un ping et le suivant."
       VALEUR PAR DEFAUT { 1000 }
       ::= { cabhCtpPing 8 }

TYPE D'OBJET cabhCtpPingTimeOut
       SYNTAXE          ENTIER (0..600000)
       UNITÉS           "milliseconds"
       MAX-ACCESS       en lecture-écriture
       ETAT             en cours
     DESCRIPTION
       "Temporisation pour la réponse ping d'envoi d'un seul ping."
       VALEUR PAR DEFAUT { 5000 } -- 5 secondes
       ::= { cabhCtpPing 9 }

TYPE D'OBJET cabhCtpPingControl
       SYNTAXE          ENTIER {
                             notRun        (1),
                             start         (2),
                             abort         (3)
                        }
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Commande du Ping d'essai. La valeur notRun est utilisée pour indiquer
       qu'il n'a pas été exécuté."
       VALEUR PAR DEFAUT { notRun(1) }
       ::= { cabhCtpPing 10 }

TYPE D'OBJET cabhCtpPingStatus
       SYNTAXE          ENTIER {
                             running       (1),
                             complete      (2),
                             aborted       (3)
                        }
       MAX-ACCESS       en lecture seule
     ETAT               en cours
```

```
     DESCRIPTION
       "Etat de l'essai en cours ou exécuté en dernier."
       ::= { cabhCtpPing 11 }

TYPE D'OBJET cabhCtpPingNumSent
       SYNTAXE          ENTIER (0..255)
       MAX-ACCESS       en lecture seule
     ETAT               en cours
     DESCRIPTION
       "Nombre de pings envoyés."
       VALEUR PAR DEFAUT { complete(2) }
       ::= { cabhCtpPing 12 }

TYPE D'OBJET cabhCtpPingNumRecv
       SYNTAXE          ENTIER (0..255)
       MAX-ACCESS       en lecture seule
     ETAT               en cours
     DESCRIPTION
       "Nombre de ping reçus."
       ::= { cabhCtpPing 13 }

--============================================================================

--
-- le groupe de notification est pour une extension future.
--

IDENTIFICATEUR D'OBJET cabhCtpNotification ::= { cabhCtpMib 2 0 }
IDENTIFICATEUR D'OBJET cabhCtpConformance ::= { cabhCtpMib 3 }
IDENTIFICATEUR D'OBJET cabhCtpCompliances ::= { cabhCtpConformance 1 }
IDENTIFICATEUR D'OBJET cabhCtpGroups ::= { cabhCtpConformance 2 }

--
--   Groupe de notification
--

-- déclarations de conformité

CONFORMITÉ DE MODULE cabhCtpBasicCompliance
     ETAT en cours
     DESCRIPTION
       "Déclaration de conformité pour les appareils qui implémentent la
       caractéristique de service portail."
     MODULE   -- cabhCtpMib

-- groupes obligatoires inconditionnellement

     GROUPES OBLIGATOIRES {
       cabhCtpGroup
     }

::= { cabhCtpCompliances 3 }

GROUPE D'OBJET cabhCtpGroup
     OBJETS {
       cabhCtpReset,
          cabhCtpConnSrcIpType,
          cabhCtpConnSrcIp,
          cabhCtpConnDestIpType,
          cabhCtpConnDestIp,
          cabhCtpConnProto,
          cabhCtpConnPort,
          cabhCtpConnNumPkts,
          cabhCtpConnPktSize,
```

```
          cabhCtpConnTimeOut,
          cabhCtpConnControl,
          cabhCtpConnStatus,
          cabhCtpConnPktsSent,
          cabhCtpConnPktsRecv,
          cabhCtpConnAvgRTT,
          cabhCtpConnMinRTT,
          cabhCtpConnMaxRTT,
          cabhCtpConnNumIcmpError,
          cabhCtpConnIcmpError,

          cabhCtpPingSrcIpType,
          cabhCtpPingSrcIp,
          cabhCtpPingDestIpType,
          cabhCtpPingDestIp,
          cabhCtpPingProto,
          cabhCtpPingNumPkts,
          cabhCtpPingPktSize,
          cabhCtpPingTimeBetween,
          cabhCtpPingTimeOut,
          cabhCtpPingControl,
          cabhCtpPingStatus,
          cabhCtpPingNumSent,
          cabhCtpPingNumRecv
        }
    ETAT en cours
    DESCRIPTION
      "Groupe d'objets pour base MIB de portail CTP de câble."
      ::= { cabhCtpGroups 1 }

FIN
```

E.3 Base MIB de sécurité

La base MIB de sécurité DOIT être implémentée comme défini ci-dessous.

```
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 -- RFC 2571
      X509Certificate       FROM DOCS-BPI2MIB
      clabProjCableHome     FROM CLAB-DEF-MIB;
```

```
--=============================================================================
--
--   Historique:
--
--
--
--=============================================================================

IDENTITÉ DE MODULE cabhSecMib
     DERNIÈRE MISE À JOUR    "0112200000Z" -- 20 décembre 2001
     ORGANISATION       "Cable NMP Group"
     CONTACT-INFO
       "Kevin Luehrs
       Adresse postale: Cable Television Laboratories, Inc.
              400 Centennial Parkway
              Louisville, Colorado 80027-1266
       U.S.A.
       Téléphone: +1 303-661-9100
       Fax: +1 303-661-9199
       E-mail: k.luehrs@cablelabs.com"
     DESCRIPTION
       "Ce module de base MIB fournit les objets de gestion de base pour les
       services de portail de sécurité."

       Accusés de réception:
       "
     ::= { clabProjCableHome 2 }

-- Conventions textuelles

--
-- suppose SNMPv3
-- la gestion du chargement de logiciel est uniquement selon DOCSIS 1.1
--

IDENTIFICATEUR D'OBJET cabhSecFwObjects ::= { cabhSecMib 1 }
IDENTIFICATEUR D'OBJET cabhSecFwBase ::= { cabhSecFwObjects 1 }
IDENTIFICATEUR D'OBJET cabhSecFwLogCtl ::= { cabhSecFwObjects 2 }
IDENTIFICATEUR D'OBJET cabhSecCertObjects ::= { cabhSecMib 2 }
--
--   Le groupe ci-dessous décrit les objets de base dans le pare-feu de câble.
--

TYPE D'OBJET cabhSecFwPolicyFileEnable
     SYNTAXE     ENTIER {
                        enable        (1),
                        disable       (2)
                        }
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "Ce paramètre indique d'activer ou non la fonctionnalité de pare-feu."
       VALEUR PAR DEFAUT {enable}
     ::= { cabhSecFwBase 1 }

TYPE D'OBJET cabhSecFwPolicyFileURL
     SYNTAXE       DisplayString
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "Contient le nom et l'adresse IP du fichier d'ensemble de règles de
       politique en format d'URL TFTP. Une fois que cet objet a été mis à jour,
       il va déclencher le téléchargement du fichier."
     ::= { cabhSecFwBase 2 }
```

```
TYPE D'OBJET cabhSecFwPolicyFileHash
     SYNTAXE       CHAINE D'OCTETS (TAILLE(20))
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "Hachage du contenu du fichier d'ensemble de règles, calculé et envoyé au
       service portail avant d'envoyer le fichier d'ensemble de règles. Pour
       l'algorithme SHA-1 d'authentification, la longueur du hachage est de
       160 bits."
     ::= { cabhSecFwBase 3 }

TYPE D'OBJET cabhSecFwPolicyFileOperStatus
     SYNTAXE ENTIER    {
     inProgress(1),
     completeFromProvisioning(2),
     completeFromMgt(3),
     failed(4)
     }
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "InProgress(1) indique qu'un téléchargement TFTP est en cours, soit comme
       résultat d'une non-concordance de version à l'approvisionnement, soit par
       suite d'une demande upgradeFromMgt. CompleteFromProvisioning(2) indique
       que la dernière mise à niveau de logiciel résultait d'une non-concordance
       de version à l'approvisionnement. CompleteFromMgt(3) indique que la
       dernière mise à niveau de logiciel résultait du réglage
       docsDevSwAdminStatus pour upgradeFromMgt. Failed(4) indique que la
       dernière tentative de téléchargement a échoué, habituellement à cause de
       l'expiration de la temporisation TFTP."

     ::= { cabhSecFwBase 4 }

TYPE D'OBJET cabhSecFwPolicyFileCurrentVersion
     SYNTAXE       SnmpAdminString
     -- MAX-ACCESS en lecture seule
     -- L'accès en écriture est ajouté pour permettre la configuration d'usine
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "Version d'ensemble de règles en cours de fonctionnement dans l'appareil
       de service portail. Cet objet devrait être dans la syntaxe utilisée par
       le vendeur individuel pour identifier les versions de logiciel. Tout
       élément de service portail DOIT retourner une chaîne descriptive du
       chargement de fichier d'ensemble de règles en cours. Si ce n'est pas
       applicable, cet objet DOIT contenir une chaîne vide."
       ::= { cabhSecFwBase 5 }

--
--   Paramètres d'enregistrement de pare-feu
--

TYPE D'OBJET cabhSecFwEventType1Enable
     SYNTAXE  ENTIER         {
       enable                (1), -- enregistrer l'événement
       disable               (2), -- ne pas enregistrer l'événement
       }
     MAX-ACCESS  en lecture-écriture
     ETAT        en cours
     DESCRIPTION
       "Active ou désactive l'enregistrement des messages d'événement de
       pare-feu de type 1."
     ::= { cabhSecFwLogCtl 1 }
```

```
TYPE D'OBJET cabhSecFwEventType2Enable
     SYNTAXE  ENTIER         {
       enable                (1), -- enregistrer l'événement
       disable               (2), -- ne pas enregistrer l'événement
       }
     MAX-ACCESS  en lecture-écriture
     ETAT        en cours
     DESCRIPTION
       "Active ou désactive l'enregistrement des messages d'événement de
       pare-feu de type 2."
     ::= { cabhSecFwLogCtl 2 }

TYPE D'OBJET cabhSecFwEventType3Enable
     SYNTAXE   ENTIER        {
       enable                (1), -- enregistrer l'événement
       disable               (2), -- ne pas enregistrer l'événement
       }
     MAX-ACCESS  en lecture-écriture
     ETAT        en cours
     DESCRIPTION
       "Active ou désactive l'enregistrement des messages d'événement de
       pare-feu de type 3."
     ::= { cabhSecFwLogCtl 3 }

TYPE D'OBJET cabhSecFwEventAttackAlertThreshold
     SYNTAXE     ENTIER                (0..65535)
     MAX-ACCESS  en lecture-écriture
     ETAT        en cours
     DESCRIPTION
       "Si le nombre d'attaques de pirate de type 1 ou 2 dépasse ce seuil sur la
       période définie par cabhSecFwEventAttackAlertPeriod, un événement de
       message de pare-feu DOIT être enregistré avec le niveau de priorité 4."
     ::= { cabhSecFwLogCtl 4 }

TYPE D'OBJET cabhSecFwEventAttackAlertPeriod
     SYNTAXE     ENTIER                (0..65535)
     MAX-ACCESS  en lecture-écriture
     ETAT        en cours
     DESCRIPTION
       "Indique la période à utiliser (en jours) pour le seuil
       cabhSecFwEventAttackAlertThreshold."
     ::= { cabhSecFwLogCtl 5 }
TYPE D'OBJET cabhSecCertPsCert
     SYNTAXE     X509Certificate
     MAX-ACCESS  en lecture seule
     ETAT     en cours
     DESCRIPTION
       "Certificat de service portail X.509 codé en DER."
     REFERENCE
       "Section 11.3.2.2 de la spécification de sécurité"
     ::= { cabhSecCertObjects 1 }

--
-- le groupe de notification fera l'objet de développements dans l'avenir.
--

IDENTIFICATEUR D'OBJET cabhSecNotification ::= { cabhSecMib 3 0 }
IDENTIFICATEUR D'OBJET cabhSecConformance ::= { cabhSecMib 4 }
IDENTIFICATEUR D'OBJET cabhSecCompliances ::= { cabhSecConformance 1 }
IDENTIFICATEUR D'OBJET cabhSecGroups ::= { cabhSecConformance 2 }

--
--   Groupe de notification
--
```

```
-- déclaration de conformité

CONFORMITÉ DE MODULE cabhSecBasicCompliance
     ETAT      en cours
     DESCRIPTION
       "Déclaration de conformité pour fonction pare-feu de câble."
     MODULE   --cabhSecMib

-- groupes obligatoires inconditionnellement

     GROUPES OBLIGATOIRES {
       cabhSecFwGroup
     }

::= { cabhSecCompliances 3 }

GROUPE D'OBJET cabhSecGroup
     OBJETS {
       cabhSecFwPolicyFileEnable,
       cabhSecFwPolicyFileURL,
       cabhSecFwPolicyFileHash,
       cabhSecFwPolicyFileOperStatus,
       cabhSecFwPolicyFileCurrentVersion,

       cabhSecFwEventType1Enable,
       cabhSecFwEventType2Enable,
       cabhSecFwEventType3Enable,
       cabhSecFwEventAttackAlertThreshold,
       cabhSecFwEventAttackAlertPeriod,
       cabhSecCertPsCert
     }
     ETAT en cours
     DESCRIPTION
       "Groupe d'objets dans la base MIB du pare-feu câble."
     ::= { cabhSecGroups 1 }

FIN
```

E.4 Base MIB de définition

La base MIB de définition DOIT être implémentée comme défini ci-dessous.

```
CLAB-DEF-MIB DEFINITIONS ::= BEGIN
IMPORTS
     MODULE-IDENTITY,
     enterprises
                                  FROM SNMPv2-SMI;

IDENTITÉ DE MODULE cableLabs
     DERNIÈRE MISE À JOUR   "0201310000Z" -- 31 janvier 2002
     ORGANISATION       "CableLabs"
     CONTACT-INFO
       "Ralph Brown
       Adresse postale: Cable Television Laboratories, Inc.
          400 Centennial Parkway
          Louisville, Colorado 80027-1266
       U.S.A.
       Téléphone: +1 303-661-9100
       Fax: +1 303-661-9199
       E-mail: r.brown@cablelabs.com"
```

```
     DESCRIPTION
       "Ce module de base MIB fournit les catégories d'objets de gestion de base
       pour Cable Labs.

     ::= { enterprises 4491 }

IDENTIFICATEUR D'OBJET clabFunction        ::= { cableLabs 1 }
IDENTIFICATEUR D'OBJET clabFuncMib2        ::= { clabFunction 1 }
IDENTIFICATEUR D'OBJET clabFuncProprietary ::= { clabFunction 2 }
IDENTIFICATEUR D'OBJET clabProject         ::= { cableLabs 2 }
IDENTIFICATEUR D'OBJET clabProjDocsis      ::= { clabProject 1 }
IDENTIFICATEUR D'OBJET clabProjPacketCable ::= { clabProject 2 }
IDENTIFICATEUR D'OBJET clabProjOpenCable   ::= { clabProject 3 }
IDENTIFICATEUR D'OBJET clabProjCableHome   ::= { clabProject 4 }

FIN
```

E.5 Base MIB de portail DHCP câble (CDP) MIB

La base MIB de portail CDP DOIT être implémentée comme défini ci-dessous.

```
CABH-CDP-MIB DEFINITIONS ::= BEGIN
IMPORTS
     MODULE-IDENTITY,
     OBJECT-TYPE,
       Integer32,
       Unsigned32
                                FROM SNMPv2-SMI
     TruthValue,
       TimeStamp,
       DisplayString,
     RowStatus,
     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;

--=============================================================================
--
--   Historique:
--
--
--
--=============================================================================

IDENTITÉ DE MODULE cabhCdpMib
     DERNIÈRE MISE À JOUR    "0112190000Z" -- 19 décembre 2001
     ORGANISATION  "Cable NMP Group"
     CONTACT-INFO
       "Kevin Luehrs
       Adresse postale: Cable Television Laboratories, Inc.
          400 Centennial Parkway
          Louisville, Colorado 80027-1266
       U.S.A.
       Téléphone: +1 303-661-9100
```

```
      Fax: +1 303-661-9199
      E-mail: k.luehrs@cablelabs.com"
    DESCRIPTION
      "Ce module de base MIB fournit les objets de gestion de base pour les
      portions CDP et CAP de la base de données de service portail."

      Accusés de réception:
      "
    ::= { clabProjCableHome 4 }

-- Conventions textuelles
CabhCdpLanTransDhcpClientId ::= TEXTUAL-CONVENTION
    ETAT     en cours
    DESCRIPTION
      "Informations sur l'option 61 de DHCP pour LAN-Trans."
    SYNTAXE   CHAINE D'OCTET (TAILLE (1..80))

--
-- suppose SNMPv3
-- la gestion du chargement de logiciel est uniquement selon DOCSIS 1.1
--

IDENTIFICATEUR D'OBJET cabhCdpObjects ::= { cabhCdpMib 1 }
IDENTIFICATEUR D'OBJET cabhCdpBase    ::= { cabhCdpObjects 1 }
IDENTIFICATEUR D'OBJET cabhCdpAddr    ::= { cabhCdpObjects 2 }
IDENTIFICATEUR D'OBJET cabhCdpServer  ::= { cabhCdpObjects 3 }
--
--   Le groupe suivant décrit les objets de base dans le portail DHCP câble.
--   Le reste de ce groupe traite des adresses définies sur le côté LAN.
--

TYPE D'OBJET cabhCdpSetToFactory
      SYNTAXE          TruthValue
    MAX-ACCESS         en lecture-écriture
    ETAT               en cours
    DESCRIPTION
      "Mettre cet objet à true(1) provoque le retour des options DHCP par
      défaut aux valeurs d'usine par défaut et l'utilisation des réglages
      d'usine par défaut par les mappages en cours à la période de
      renouvellement de location suivante. La lecture de cet objet donne
      toujours false(2) en retour. Lorsque cabhCdpDhcpReset est mis à Vrai, les
      actions suivantes surviennent:
      1) remettre toutes les options DHCP de CDS par défaut aux valeurs d'usine
      par défaut.
      2) le serveur CDS offrira les options DHCP d'usine par défaut à la
      prochaine période de renouvellement de location.

      Les objets mis aux valeurs d'usine par défaut sont:
         cabhCdpLanTransThreshold,
         cabhCdpLanTransAction,

         cabhCdpLanPoolStart,
         cabhCdpLanPoolEnd,
         cabhCdpServerSubnetMask,
         cabhCdpServerTimeOffset,
         cabhCdpServerRouter,
         cabhCdpServerDnsAddress,
         cabhCdpServerSyslogAddress,
         cabhCdpServerDomainName,
         cabhCdpServerTTL,
         cabhCdpServerInterfaceMTU,
         cabhCdpServerVendorSpecific,
         cabhCdpServerLeaseTime,
         cabhCdpServerDhcpAddress"
```

```
     REFERENCE
       ""
     ::= { cabhCdpBase 1 }

TYPE D'OBJET cabhCdpLanTransCurCount
     SYNTAXE     Unsigned32
     MAX-ACCESS  en lecture seule
     ETAT        en cours
     DESCRIPTION
       "Nombre d'adresses IP LAN-Trans en cours pour les adresses traduites
       (interconnexions NAT et NAPT). C'est un compte d'adresse du côté WAN."
       REFERENCE
          ""
     ::= { cabhCdpBase 2 }

TYPE D'OBJET cabhCdpLanTransThreshold
     SYNTAXE       ENTIER (1..65533)
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "Nombre seuil des adresses IP LAN-Trans allouées ou assignées, au-dessus
       duquel une condition d'alarme DOIT être générée. Chaque fois qu'il y a
       une tentative d'allocation d'une adresse IP LAN-Trans lorsque
       cabhCdpLanTransCurCount est supérieur ou égal au seuil
       cabhCdpLanTransThreshold, un événement est généré. Pour les adresses de
       classe C, 253 est utilisé comme valeur par défaut. Pour les adresses de
       classe B, 65533 est utilisé comme valeur par défaut. Dans l'un ou l'autre
       cas, ce réglage désactive la caractéristique."
       REFERENCE
          ""
       VALEUR PAR DEFAUT { 65533 }
     ::= { cabhCdpBase 3 }

TYPE D'OBJET cabhCdpLanTransAction
     SYNTAXE     ENTIER {
                            normal             (1),
                       noAssignment            (2)
                            }
     MAX-ACCESS  en lecture-écriture
     ETAT        en cours
     DESCRIPTION
       "Action prise lorsque le serveur CDS alloue une adresse LAN-Trans et que
       le nombre d'adresses LAN-Trans allouées (cabhCdpLanTransCurCount) est
       supérieur au seuil (cabhCdpLanTransThreshold). Les actions sont les
       suivantes:

          normal -           allouer une adresse IP LAN-Trans et traiter
                             l'interconnexion entre le LAN et le WAN comme
                             normalement si le seuil n'était pas dépassé.

          noAssignment -     ne pas allouer d'adresse IP LAN-Trans et ne pas
                             créer d'interconnexion."
     REFERENCE
       ""
     VALEUR PAR DEFAUT { normal }
     ::= { cabhCdpBase 4 }

--
--   Tableaux de gestion d'adresse de portail CDP
--
--============================================================================
--
--   cabhCdpLanAddrTable (tableau d'adresse LAN de portail CDP)
--
```

```
--   Le tableau cabhCdpLanAddrTable contient les paramètres DHCP pour chaque
--   adresse IP servie au secteur LAN-Trans.
--
--   Ce tableau contient une liste d'entrées pour les paramètres de portail CDP
--   côté LAN.
--
--================================================================================

TYPE D'OBJET cabhCdpLanAddrTable
     SYNTAXE  SEQUENCE DE CabhCdpLanAddrEntry
     MAX-ACCESS  non accessible
     ETAT en cours
     DESCRIPTION
       "Ce tableau est une liste de paramètres du secteur LAN-Trans. Cette liste
       a une entrée pour chaque adresse IP LAN-Trans allouée."
     ::= { cabhCdpAddr 1 }

TYPE D'OBJET cabhCdpLanAddrEntry
     SYNTAXE     CabhCdpLanAddrEntry
     MAX-ACCESS    non accessible
     ETAT    en cours
     DESCRIPTION
       "Liste des paramètres généraux pour les mappages de portail CDP."
     INDEX { cabhCdpLanAddrIpType, cabhCdpLanAddrIp }
     ::= { cabhCdpLanAddrTable 1 }

CabhCdpLanAddrEntry ::= SEQUENCE {
     cabhCdpLanAddrIpType         InetAddressType,
       cabhCdpLanAddrIp               InetAddress,
       cabhCdpLanAddrClientId              CabhCdpLanTransDhcpClientId,
       cabhCdpLanAddrCreateTime   TimeStamp,
       cabhCdpLanAddrExpireTime   TimeStamp,
       cabhCdpLanAddrMethod           ENTIER,
       cabhCdpLanAddrHostName         DisplayString,
       cabhCdpLanAddrRowStatus        RowStatus
     }

TYPE D'OBJET cabhCdpLanAddrIpType
     SYNTAXE       InetAddressType
     MAX-ACCESS    non accessible
     ETAT          en cours
     DESCRIPTION
       "Type d'adresse allouée du côté LAN pour le tableau d'adresse de portail
       CDP."
     ::= { cabhCdpLanAddrEntry 1 }

TYPE D'OBJET cabhCdpLanAddrIp
     SYNTAXE       InetAddress
     MAX-ACCESS    non accessible
     ETAT          en cours
     DESCRIPTION
       "Adresse allouée du côté LAN pour le tableau d'adresse de portail CDP."
     ::= { cabhCdpLanAddrEntry 2 }

TYPE D'OBJET cabhCdpLanAddrClientID
     SYNTAXE       CabhCdpLanTransDhcpClientId
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "Identifiant de client comme indiqué dans l'option 61 du DHCP Discover.
       Il y a une relation biunivoque entre l'identifiant de client et l'adresse
       LAN allouée."
     ::= { cabhCdpLanAddrEntry 3 }
```

```
TYPE D'OBJET cabhCdpLanAddrCreateTime
     SYNTAXE       Horodatage
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "Heure à laquelle le côté LAN du tableau LAN de CDP a été créé. Cette
       entrée n'est faite que lors de la création du tableau cabhCdpLanAddrTable
       et que l'entrée n'existe pas déjà. En d'autres termes, cette valeur n'est
       pas remplacée au moment du renouvellement de location."
     ::= { cabhCdpLanAddrEntry 4 }

TYPE D'OBJET cabhCdpLanAddrExpireTime
     SYNTAXE       Horodatage
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "Heure d'expiration de la location du côté LAN. Lorsque la location
       arrive à expiration, cette entrée sera supprimée du tableau."
     ::= { cabhCdpLanAddrEntry 5 }

TYPE D'OBJET cabhCdpLanAddrMethod
     SYNTAXE  ENTIER {
                   cmp           (1),
                   cdp           (2)
                   }
       MAX-ACCESS  en lecture seule
     ETAT     en cours
     DESCRIPTION
       "Méthode de création de cette entrée d'adresse.  cmp indique que cette
       rangée (entrée) a été établie par configuration à travers le portail CMP.
       cdp indique que cette rangée (entrée) a été établie par un DHCP
       discover."
     ::= { cabhCdpLanAddrEntry 6 }

TYPE D'OBJET cabhCdpLanAddrHostName
     SYNTAXE       DisplayString (TAILLE(0..80))
     MAX-ACCESS    en lecture seule
     ETAT     en cours
     DESCRIPTION
       "Nom d'hôte de l'adresse IP de LAN, sur la base de l'option DCHP 12."
     ::= { cabhCdpLanAddrEntry 7 }

TYPE D'OBJET cabhCdpLanAddrRowStatus
     SYNTAXE       RowStatus
     MAX-ACCESS    en lecture-création
     ETAT          en cours
     DESCRIPTION
       "Emboîtage des rangées pour la création et la suppression."
     ::= { cabhCdpLanAddrEntry 8 }
--=============================================================================
--
--   cabhCdpWanDataAddrTable (Tableau d'adresse WAN-Data de portail CDP)
--
--   Le tableau cabhCdpWanDataAddrTable contient les paramètres de configuration
--   ou DHCP pour chaque mappage d'adresse IP selon l'adresse IP WAN-Data.
--
--=============================================================================

TYPE D'OBJET cabhCdpWanDataAddrTable
     SYNTAXE       SEQUENCE DE CabhCdpWanDataAddrEntry
     MAX-ACCESS    non accessible
     ETAT          en cours
```

```
     DESCRIPTION
       "Ce tableau contient les informations de secteur d'adresse WAN-Data."
     ::= { cabhCdpAddr 2 }

TYPE D'OBJET cabhCdpWanDataAddrEntry
     SYNTAXE       CabhCdpWanDataAddrEntry
     MAX-ACCESS    non accessible
     ETAT          en cours
     DESCRIPTION
       "Liste des paramètres généraux pour le secteur d'adresse WAN-Data du
       portail CDP."
     INDEX { cabhCdpWanDataAddrIndex }
     ::= { cabhCdpWanDataAddrTable 1 }

CabhCdpWanDataAddrEntry ::= SEQUENCE {
       cabhCdpWanDataAddrIndex                ENTIER,
       cabhCdpWanDataAddrClientId             CHAINE D'OCTET,
       cabhCdpWanDataAddrIpType               InetAddressType,
       cabhCdpWanDataAddrIp                   InetAddress,
       cabhCdpWanDataAddrRenewalTime          Integer32,
       cabhCdpWanDataAddrRowStatus            RowStatus
     }

TYPE D'OBJET cabhCdpWanDataAddrIndex
     SYNTAXE       ENTIER (1..65535)
     MAX-ACCESS    non accessible
     ETAT          en cours
     DESCRIPTION
       "Indice dans le tableau"
     ::= { cabhCdpWanDataAddrEntry 1 }

TYPE D'OBJET cabhCdpWanDataAddrClientId
     SYNTAXE CHAINE D'OCTETS (TAILLE (1..80))
     MAX-ACCESS    en lecture-création
     ETAT          en cours
     DESCRIPTION
       "Identifiant client WAN-Data unique utilisé lorsque demandant une adresse
       IP WAN-Data via DHCP."
     ::= { cabhCdpWanDataAddrEntry 2 }

TYPE D'OBJET cabhCdpWanDataAddrIpType
     SYNTAXE       InetAddressType
     MAX-ACCESS    en lecture-création
     ETAT          en cours
     DESCRIPTION
       "Type d'adresse allouée du côté WAN-Data."
     ::= { cabhCdpWanDataAddrEntry 3 }

TYPE D'OBJET cabhCdpWanDataAddrIp
     SYNTAXE       InetAddress
     MAX-ACCESS    en lecture-création
     ETAT          en cours
     DESCRIPTION
       "Adresse allouée du côté WAN-Data."
     ::= { cabhCdpWanDataAddrEntry 4 }

TYPE D'OBJET cabhCdpWanDataAddrRenewalTime
     SYNTAXE       Integer32
     MAX-ACCESS    en lecture-création
     ETAT          en cours
     DESCRIPTION
       "Temps restant avant l'expiration de la location. Ceci se fonde sur
       l'option DHCP 51."
     ::= { cabhCdpWanDataAddrEntry 5 }
```

```
TYPE D'OBJET cabhCdpWanDataAddrRowStatus
     SYNTAXE       RowStatus
     MAX-ACCESS    en lecture-création
     ETAT          en cours
     DESCRIPTION
       "Emboîtage des rangées pour la création et la suppression."
     ::= { cabhCdpWanDataAddrEntry 6 }

--============================================================================
--
--   cabhCdpWanDataAddrServerTable (tableau de serveur DNS WAN-Data de portail
--   CDP)
--
--   Le tableau cabhCdpWanDataAddrServerTable contient un tableau de
--   rattachement des serveurs DNS.
--
--============================================================================

TYPE D'OBJET cabhCdpWanDataAddrServerTable
     SYNTAXE       SEQUENCE DE CabhCdpWanDataAddrServerEntry
       MAX-ACCESS  non accessible
     ETAT          en cours
     DESCRIPTION
       "Ceci contient les adresses IP utilisées pour les hôtes DNS WAN-Data
       obtenus via l'option 6 DHCP pendant le processus WAN-Data."
     ::= { cabhCdpAddr 3 }

TYPE D'OBJET cabhCdpWanDataAddrServerEntry
     SYNTAXE       CabhCdpWanDataAddrServerEntry
     MAX-ACCESS    non accessible
     ETAT          en cours
     DESCRIPTION
       "Liste des hôtes DNS WAN-Data."
     INDEX { cabhCdpWanDataAddrDnsIpType, cabhCdpWanDataAddrDnsIp }
     ::= { cabhCdpWanDataAddrServerTable 1 }

CabhCdpWanDataAddrServerEntry ::= SEQUENCE {
     cabhCdpWanDataAddrDnsIpType      InetAddressType,
     cabhCdpWanDataAddrDnsIp          InetAddress,
     cabhCdpWanDataAddrDnsRowStatus        RowStatus
     }

TYPE D'OBJET cabhCdpWanDataAddrDnsIpType
     SYNTAXE       InetAddressType
       MAX-ACCESS  non accessible
     ETAT          en cours
     DESCRIPTION
       "Ce paramètre indique le type d'adresse IP d'un serveur DNS."
       ::= { cabhCdpWanDataAddrServerEntry 1 }

TYPE D'OBJET cabhCdpWanDataAddrDnsIp
     SYNTAXE       InetAddress
       MAX-ACCESS  non accessible
     ETAT          en cours
     DESCRIPTION
       "Ce paramètre indique l'adresse IP d'un serveur DNS."
       ::= { cabhCdpWanDataAddrServerEntry 2 }

TYPE D'OBJET cabhCdpWanDataAddrDnsRowStatus
     SYNTAXE       RowStatus
     MAX-ACCESS    en lecture-création
     ETAT          en cours
```

```
     DESCRIPTION
       "Emboîtement des rangées pour la création et la suppression."
          ::= { cabhCdpWanDataAddrServerEntry 3 }

--
--   Valeurs d'option DHCP côté serveur (CDS) pour le secteur LAN-Trans
--
TYPE D'OBJET cabhCdpLanPoolStartType
     SYNTAXE       InetAddressType
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "Type d'adresse des adresses IP LAN-Trans de début de gamme."
          VALEUR PAR DEFAUT { ipv4 }
     ::= { cabhCdpServer 1 }

TYPE D'OBJET cabhCdpLanPoolStart
     SYNTAXE       InetAddress
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "Adresses IP LAN-Trans de début de gamme."
          VALEUR PAR DEFAUT { 'c0a8000a'h } -- 192.168.0.10
                                -- 192.168.0.0 est le numéro de réseau
                                -- 192.168.0.255 est l'adresse de diffusion, et
                                -- 192.168.0.1 est réservé pour le routeur.
     ::= { cabhCdpServer 2 }

TYPE D'OBJET cabhCdpLanPoolEndType
     SYNTAXE       InetAddressType
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "Type d'adresse des adresses IP LAN-Trans de fin de gamme."
          VALEUR PAR DEFAUT { ipv4 }
     ::= { cabhCdpServer 3 }

TYPE D'OBJET cabhCdpLanPoolEnd
     SYNTAXE       InetAddress
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "Fin de gamme des adresses IP LAN-Trans."
          VALEUR PAR DEFAUT { 'c0a800fe'h }-- 192.168.0.254
     ::= { cabhCdpServer 4 }

TYPE D'OBJET cabhCdpServerSubnetMaskType
       SYNTAXE     InetAddressType
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "Type de gabarit de sous-réseau LAN-Trans."
     VALEUR PAR DEFAUT { ipv4 }
     ::= { cabhCdpServer 5 }

TYPE D'OBJET cabhCdpServerSubnetMask
       SYNTAXE     InetAddress
     MAX-ACCESS    en lecture-écriture
     ETAT          en cours
     DESCRIPTION
       "Valeur d'option 1 – Valeur du gabarit de sous-réseau LAN-Trans."
       VALEUR PAR DEFAUT { 'ffffff00'h }   -- 255.255.255.0
     ::= { cabhCdpServer 6 }
```

```
TYPE D'OBJET cabhCdpServerTimeOffset
       SYNTAXE          Integer32 (-86400..86400) -- 0 à 24 heures (en secondes)
       UNITÉS           "secondes"
     MAX-ACCESS     en lecture-écriture
     ETAT           en cours
     DESCRIPTION
       "Valeur d'option 2 – Valeur du décalage de temps du LAN-Trans par rapport
au Temps coordonné universel (UTC)."
       VALEUR PAR DEFAUT { 0 }        -- UTC
     ::= { cabhCdpServer 7 }

TYPE D'OBJET cabhCdpServerRouterType
       SYNTAXE      InetAddressType
     MAX-ACCESS     en lecture-écriture
     ETAT           en cours
     DESCRIPTION
       "Type d'adresse, Routeur pour le secteur d'adresse LAN-Trans."
       VALEUR PAR DEFAUT { ipv4 }
     ::= { cabhCdpServer 8 }

TYPE D'OBJET cabhCdpServerRouter
       SYNTAXE      InetAddress
     MAX-ACCESS     en lecture-écriture
     ETAT           en cours
     DESCRIPTION
       "Valeur d'option 3 – Routeur pour le secteur d'adresse LAN-Trans."
          VALEUR PAR DEFAUT { 'c0a80001'h }-- 192.168.0.1
     ::= { cabhCdpServer 9 }

TYPE D'OBJET cabhCdpServerDnsAddressType
     SYNTAXE        InetAddressType
     MAX-ACCESS     en lecture-écriture
     ETAT           en cours
     DESCRIPTION
       "Type d'adresses IP des serveurs DNS du secteur d'adresse LAN-Trans."
          VALEUR PAR DEFAUT { ipv4 }
     ::= { cabhCdpServer 10 }

TYPE D'OBJET cabhCdpServerDnsAddress
     SYNTAXE        InetAddress
     MAX-ACCESS     en lecture-écriture
     ETAT           en cours
     DESCRIPTION
       "Adresses IP des serveurs DNS de secteur d'adresse LAN-Trans. Par défaut,
       il y a seulement un serveur DNS et c'est l'adresse spécifiée dans la
       valeur d'option 3 – cabhCdpServerRouter. Seule une adresse est
       spécifiée."
          VALEUR PAR DEFAUT { 'c0a80001'h } -- 192.168.0.1
     ::= { cabhCdpServer 11 }

TYPE D'OBJET cabhCdpServerSyslogAddressType
     SYNTAXE        InetAddressType
     MAX-ACCESS     en lecture-écriture
     ETAT           en cours
     DESCRIPTION
       "Type d'adresse IP des serveurs SYSLOG de LAN-Trans."
          VALEUR PAR DEFAUT { ipv4 }
     ::= { cabhCdpServer 12 }

TYPE D'OBJET cabhCdpServerSyslogAddress
     SYNTAXE        InetAddress
     MAX-ACCESS     en lecture-écriture
     ETAT           en cours
```

```
     DESCRIPTION
       "Adresses IP des serveurs SYSLOG de LAN-Trans. Par défaut il n'y a pas de
       serveur SYSLOG. La valeur d'usine par défaut contient l'indication qu'il
       n'y a pas de valeur de serveur Syslog égale (0.0.0.0)."
          VALEUR PAR DEFAUT { '00000000'h }-- 0.0.0.0
     ::= { cabhCdpServer 13 }

TYPE D'OBJET cabhCdpServerDomainName
       SYNTAXE          DisplayString(TAILLE(0..128))
     MAX-ACCESS         en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Valeur d'option 15 – Nom de domaine du secteur d'adresse LAN-Trans."
       VALEUR PAR DEFAUT {""}
       ::= { cabhCdpServer 14 }

TYPE D'OBJET cabhCdpServerTTL
       SYNTAXE          ENTIER (0..255)
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Valeur d'option 23 – Temps de vie LAN-Trans."
       VALEUR PAR DEFAUT { 64 }
       ::= { cabhCdpServer 15 }

TYPE D'OBJET cabhCdpServerInterfaceMTU
       SYNTAXE          ENTIER (68..4096)
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Valeur d'option 26 – Interface MTU LAN-Trans."
       VALEUR PAR DEFAUT { 1500 }
       ::= { cabhCdpServer 16 }

TYPE D'OBJET cabhCdpServerVendorSpecific
       SYNTAXE          CHAINE D'OCTET (TAILLE(0..255))
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Valeur d'option 43 – Options spécifiques du vendeur."
       VALEUR PAR DEFAUT { ''h }
       ::= { cabhCdpServer 17 }

TYPE D'OBJET cabhCdpServerLeaseTime
       SYNTAXE          Unsigned32
       UNITÉS           "secondes"
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Valeur d'option 51 – Durée de location LAN-Trans par défaut (en
       secondes)."
       VALEUR PAR DEFAUT { 60 }
       ::= { cabhCdpServer 18 }

TYPE D'OBJET cabhCdpServerDhcpAddressType
       SYNTAXE          InetAddressType
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Valeur d'option 54 – Type d'adresse IP de serveur DHCP LAN-Trans."
       VALEUR PAR DEFAUT { ipv4 }
       ::= { cabhCdpServer 19 }
```

```
TYPE D'OBJET cabhCdpServerDhcpAddress
       SYNTAXE          InetAddress
       MAX-ACCESS       en lecture-écriture
     ETAT               en cours
     DESCRIPTION
       "Valeur d'option 54 – Adresse IP de serveur DHCP LAN-Trans. Elle prend
       par défaut l'adresse du routeur comme spécifié dans cabhCdpServerRouter.
       Autrement, un fabricant peut vouloir des adresses CDS séparées des
       adresses de routeur."
       VALEUR PAR DEFAUT { 'c0a80001'h }        --     192.168.0.1
       ::= { cabhCdpServer 20 }

--
-- le groupe de notification est pour un développement futur.
--

IDENTIFICATEUR D'OBJET cabhCdpNotification ::= { cabhCdpMib 2 0 }
IDENTIFICATEUR D'OBJET cabhCdpConformance      ::= { cabhCdpMib 3 }
IDENTIFICATEUR D'OBJET cabhCdpCompliances      ::= { cabhCdpConformance 1 }
IDENTIFICATEUR D'OBJET cabhCdpGroups           ::= { cabhCdpConformance 2 }

--
--   Groupe de notification
--

-- déclarations de conformité

CONFORMITÉ DE MODULE cabhCdpBasicCompliance
     ETAT en cours
     DESCRIPTION
       "Déclaration de conformité pour les appareils qui implémentent la
       caractéristique d'adaptateur MTA."
     MODULE -- cabhCdpMib

-- groupes obligatoires inconditionnellement

     GROUPES OBLIGATOIRES {
       cabhCdpGroup
     }

::= { cabhCdpCompliances 3 }

GROUPE D'OBJET cabhCdpGroup
     OBJETS {
       cabhCdpSetToFactory,
          cabhCdpLanTransCurCount,
       cabhCdpLanTransThreshold,
       cabhCdpLanTransAction,

          cabhCdpLanAddrIpType,
          cabhCdpLanAddrIp,
          cabhCdpLanAddrClientID,
          cabhCdpLanAddrCreateTime,
          cabhCdpLanAddrExpireTime,
          cabhCdpLanAddrMethod,
          cabhCdpLanAddrHostName,
          cabhCdpLanAddrRowStatus,

          cabhCdpWanDataAddrIndex,
          cabhCdpWanDataAddrClientId,
          cabhCdpLanAddrIpType,
          cabhCdpWanDataAddrIp,
          cabhCdpWanDataAddrRenewalTime,
          cabhCdpWanDataAddrRowStatus,
```

```
          cabhCdpWanDataAddrDnsIpType,
          cabhCdpWanDataAddrDnsIp,
          cabhCdpWanDataAddrDnsRowStatus,

          cabhCdpLanPoolStartType,
          cabhCdpLanPoolStart,
          cabhCdpLanPoolEndType,
          cabhCdpLanPoolEnd,
          cabhCdpServerSubnetMaskType,
          cabhCdpServerSubnetMask,
          cabhCdpServerTimeOffset,
          cabhCdpServerRouterType,
          cabhCdpServerRouterType,
          cabhCdpServerRouter,
          cabhCdpServerDnsAddressType,
          cabhCdpServerDnsAddress,
          cabhCdpServerSyslogAddressType,
          cabhCdpServerSyslogAddress,
          cabhCdpServerDomainName,
          cabhCdpServerTTL,
          cabhCdpServerInterfaceMTU,
          cabhCdpServerVendorSpecific,
          cabhCdpServerLeaseTime,
          cabhCdpServerDhcpAddressType,
          cabhCdpServerDhcpAddress
              }
     ETAT     en cours
     DESCRIPTION
       "Groupe d'objets pour base MIB CDB de câble."
     ::= { cabhCdpGroups 1 }

FIN
```

E.6 Portail d'adresse câble

La base MIB du portail CAP DOIT être implémentée comme défini ci-dessous.

```
CABH-CAP-MIB DEFINITIONS ::= BEGIN
IMPORTS
     MODULE-IDENTITY,
     OBJECT-TYPE,
       Unsigned32
                              FROM SNMPv2-SMI
       TimeStamp,
       TruthValue,
       RowStatus,
       PhysAddress
                              FROM SNMPv2-TC
     OBJECT-GROUP,
     MODULE-COMPLIANCE
                              FROM SNMPv2-CONF
     InetAddressType,
     InetAddress,
     InetAddressIPv4,
     InetAddressIPv6
                              FROM INET-ADDRESS-MIB

     clabProjCableHome
                              FROM CLAB-DEF-MIB;
```

```
--=============================================================================
--
--   Historique:
--
--
--=============================================================================

MODULE D'IDENTITÉ cabhCapMib
     DERNIÈRE MISE À JOUR    "0112190000Z" -- 19 décembre 2001
     ORGANISATION  "Cable NMP Group"
     CONTACT-INFO
       "Kevin Luehrs
       Adresse postale: Cable Television Laboratories, Inc.
          400 Centennial Parkway
          Louisville, Colorado 80027-1266
       U.S.A.
       Téléphone: +1 303-661-9100
       Fax: +1 303-661-9199
       E-mail: k.luehrs@cablelabs.com"
     DESCRIPTION
       "Ce module de base MIB fournit les objets de gestion de base pour les
       portions CDP et CAP de la base de données du service portail.

       Accusés de réception:
       "
     ::= { clabProjCableHome 3 }

-- Conventions textuelles

CabhCapPacketMode ::= TEXTUAL-CONVENTION
     ETAT en cours
     DESCRIPTION
       "Type de données établies lorsqu'une liaison/mappage est établie."
     SYNTAXE  ENTIER {
                   napt          (1), -- NAT avec traduction de port
                   nat           (2), -- NAT de base
                   passthrough   (3), -- Adresse externe de traverse
                   }

--
-- suppose SNMPv3
-- la gestion du chargement de logiciel est selon DOCSIS 1.1 seulement
--

IDENTIFICATEUR D'OBJET cabhCapObjects      ::= { cabhCapMib 1 }
IDENTIFICATEUR D'OBJET cabhCapBase         ::= { cabhCapObjects 1 }
IDENTIFICATEUR D'OBJET cabhCapMap          ::= { cabhCapObjects 2 }
--=============================================================================
--
-- Paramètres généraux de portail CAP
--
--=============================================================================

TYPE D'OBJET cabhCapTcpTimeWait
     SYNTAXE     Unsigned32
       UNITÉS    "secondes"
     MAX-ACCESS  en lecture-écriture
     ETAT        en cours
     DESCRIPTION
       "Temps maximal d'attente avant de supposer que la session TCP est
       terminée."
```

```
      REFERENCE
         ""
      VALEUR PAR DEFAUT { 240 }      -- 4 minutes
    ::= { cabhCapBase 1 }

TYPE D'OBJET cabhCapUdpTimeWait
    SYNTAXE     Unsigned32
      UNITÉS    "secondes"
    MAX-ACCESS  en lecture-écriture
    ETAT        en cours
    DESCRIPTION
      "Temps maximal d'attente avant de supposer que la session UDP est
      terminée."
      REFERENCE
         ""
      VALEUR PAR DEFAUT { 86400 }    -- 1 jour
    ::= { cabhCapBase 2 }

TYPE D'OBJET cabhCapIcmpTimeWait
    SYNTAXE     Unsigned32
      UNITÉS    "secondes"
    MAX-ACCESS  en lecture-écriture
    ETAT        en cours
    DESCRIPTION
      "Temps maximal d'attente avant de supposer que la session Icmp est
      terminée."
      REFERENCE
         ""
      VALEUR PAR DEFAUT { 86400 }    -- 1 jour
    ::= { cabhCapBase 3 }

TYPE D'OBJET cabhCapPrimaryMode
    SYNTAXE       CabhCapPacketMode
    MAX-ACCESS    en lecture-écriture
    ETAT          en cours
    DESCRIPTION
      "Mode primaire de traitement de paquet à utiliser."
      VALEUR PAR DEFAUT { napt }
    ::= { cabhCapBase 4 }

TYPE D'OBJET cabhCapSetToFactory
    SYNTAXE       TruthValue
    MAX-ACCESS    en lecture-écriture
    ETAT          en cours
    DESCRIPTION
      "Mettre cet objet à true(1) provoque la suppression de tous les tableaux
      dans le CAP, et tous les objets CAP avec des valeurs par défaut sont
      rétablis à leurs valeurs par défaut."
    ::= { cabhCapBase 5 }
--============================================================================
--
--   cabhCapMappingTable (Tableau de mappage de CAP)
--
--   Le tableau cabhCapMappingTable contient les mappages pour tous les
--   mappages de CAP.
--
--============================================================================

TYPE D'OBJET cabhCapMappingTable
      SYNTAXE          SEQUENCE DE CabhCapMappingEntry
    MAX-ACCESS  non accessible
    ETAT en cours
```

```
     DESCRIPTION
       "Ce tableau contient le mappage des adresses IP pour tous les mappages
       de CAP."
     ::= { cabhCapMap 1 }

TYPE D'OBJET cabhCapMappingEntry
     SYNTAXE       CabhCapMappingEntry
     MAX-ACCESS    non accessible
     ETAT          en cours
     DESCRIPTION
       "Liste des mappages IP de CAP."
     INDEX { cabhCapMappingWanAddrType, cabhCapMappingWanAddr,
     cabhCapMappingWanPort,
       cabhCapMappingLanAddrType, cabhCapMappingLanAddr, cabhCapMappingLanPort}
     ::= { cabhCapMappingTable 1 }

CabhCapMappingEntry ::= SEQUENCE {
     cabhCapMappingWanAddrType   InetAddressType,
       cabhCapMappingWanAddr          InetAddress,
       cabhCapMappingWanPort          ENTIER,
       cabhCapMappingLanAddrType      InetAddressType,
       cabhCapMappingLanAddr          InetAddress,
       cabhCapMappingLanPort          ENTIER,
       cabhCapMappingMode         CabhCapPacketMode,
       cabhCapMappingMethod           ENTIER,
       cabhCapMappingProtocol         ENTIER
       }

TYPE D'OBJET cabhCapMappingWanAddrType
     SYNTAXE       InetAddressType
     MAX-ACCESS    non accessible
     ETAT          en cours
     DESCRIPTION
       "Type d'adresse IP allouée du côté WAN. IP version 4 est utilisé en
       principe."
     ::= { cabhCapMappingEntry 1 }

TYPE D'OBJET cabhCapMappingWanAddr
     SYNTAXE       InetAddress
     MAX-ACCESS    non accessible
     ETAT          en cours
     DESCRIPTION
       "Adresse IP allouée du côté WAN. IP version 4 est utilisé en principe."
     ::= { cabhCapMappingEntry 2 }

TYPE D'OBJET cabhCapMappingWanPort
     SYNTAXE       ENTIER (1..65535)
     MAX-ACCESS    non accessible
     ETAT          en cours
     DESCRIPTION
       "Numéro de port TCP/UDP sur le côté WAN."
     ::= { cabhCapMappingEntry 3 }

TYPE D'OBJET cabhCapMappingLanAddrType
     SYNTAXE       InetAddressType
     MAX-ACCESS    non accessible
     ETAT          en cours
     DESCRIPTION
       "Type d'adresse IP allouée sur le côté LAN. IP version 4 est utilisé en
       principe."
     ::= { cabhCapMappingEntry 4 }
```

```
TYPE D'OBJET cabhCapMappingLanAddr
     SYNTAXE       InetAddress
     MAX-ACCESS    non accessible
     ETAT          en cours
     DESCRIPTION
       "Adresse IP allouée sur le côté LAN. IP version 4 est utilisé en
       principe."
     ::= { cabhCapMappingEntry 5 }

TYPE D'OBJET cabhCapMappingLanPort
     SYNTAXE       ENTIER (1..65535)
     MAX-ACCESS    non accessible
     ETAT          en cours
     DESCRIPTION
       "Numéro de port TCP/UDP sur le côté LAN."
     ::= { cabhCapMappingEntry 6 }

TYPE D'OBJET cabhCapMappingMode
     SYNTAXE       CabhCapPacketMode
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "Type de mode de traitement de paquet pour ce mappage. Noter que cette
       information pourrait être collectée à partir de l'adresse IP et des
       informations de port pour ce mappage"
     ::= { cabhCapMappingEntry 7 }

TYPE D'OBJET cabhCapMappingMethod
     SYNTAXE       ENTIER {
                                 static    (1),
                                 dynamic   (2),
                                 }
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "Indique comment le mappage a été créé. Statique signifie qu'il a été
       approvisionné et dynamique signifie qu'il a été traité par le service
       portail lui-même."
     ::= { cabhCapMappingEntry 8 }

TYPE D'OBJET cabhCapMappingProtocol
     SYNTAXE       ENTIER {
                                 autre     (1), -- non spécifié
                                 icmp      (2),
                                 udp       (3),
                                 tcp       (4)
                                 }
     MAX-ACCESS    en lecture seule
     ETAT          en cours
     DESCRIPTION
       "Protocole pour ce mappage."
     ::= { cabhCapMappingEntry 9 }

--============================================================================
--
--   cabhCapPassthroughTable (Tableau de traverse de CAP)
--
--   Le tableau cabhCapPassthroughTable contient les adresses MAC pour tous
--   les appareils IP de LAN qui seront configurés en mode Traverse.
--
--============================================================================

TYPE D'OBJET cabhCapPassthroughTable
     SYNTAXE       SEQUENCE DE CabhCapPassthroughEntry
```

```
     MAX-ACCESS    non accessible
     ETAT          en cours
     DESCRIPTION
       "Ce tableau contient les adresses MAC des appareils IP de LAN qui sont
       configurés en mode Traverse."
     ::= { cabhCapMap 2 }

TYPE D'OBJET cabhCapPassthroughEntry
     SYNTAXE       CabhCapPassthroughEntry
     MAX-ACCESS    non accessible
     ETAT          en cours
     DESCRIPTION
       "Liste des adresses MAC pour les appareils IP de LAN qui sont configurés
       en mode Traverse."
     INDEX {cabhCapPassthroughMACAddr }
     ::= { cabhCapPassthroughTable 1 }

CabhCapPassthroughEntry ::= SEQUENCE {
     cabhCapPassthroughMACAddr        PhysAddress,
     cabhCapPassthroughRowStatus      RowStatus
     }

TYPE D'OBJET cabhCapPassthroughMACAddr
     SYNTAXE       PhysAddress
     MAX-ACCESS    non accessible
     ETAT          en cours
     DESCRIPTION
       "Adresse MAC de l'appareil IP de LAN à configurer en mode Traverse."
     ::= {cabhCapPassthroughEntry 1 }

TYPE D'OBJET cabhCapPassthroughRowStatus
     SYNTAXE       RowStatus
     MAX-ACCESS    en lecture-création
     ETAT          en cours
     DESCRIPTION
       "Emboîtement de l'état de la rangée pour la création et la suppression de
       l'entrée cabhCapPassthroughTable."
     ::= { cabhCapPassthroughEntry 2 }

--
-- Le groupe de notification est destiné à des extensions ultérieures.
--

IDENTIFICATEUR D'OBJET cabhCapNotification ::= { cabhCapMib 2 0 }
IDENTIFICATEUR D'OBJET cabhCapConformance ::= { cabhCapMib 3 }
IDENTIFICATEUR D'OBJET cabhCapCompliances ::= { cabhCapConformance 1 }
IDENTIFICATEUR D'OBJET cabhCapGroups ::= { cabhCapConformance 2 }

--
-- Groupe de notification
--

-- Déclarations de conformité

CONFORMITÉ DE MODULE cabhCapBasicCompliance
     ETAT en cours
     DESCRIPTION
       "Déclaration de conformité pour les appareils qui implémentent la
       fonction d'adaptateur MTA."
     MODULE -- cabhCapMib

-- groupes obligatoires inconditionnels
```

```
     GROUPES OBLIGATOIRES {
       cabhCapGroup
     }

::= { cabhCapCompliances 3 }

GROUPE D'OBJET cabhCapGroup
     OBJETS {
       cabhCapTcpTimeWait,
       cabhCapUdpTimeWait,
       cabhCapIcmpTimeWait,
       cabhCapPrimaryMode,

--     cabhCapMappingWanAddrType,
--     cabhCapMappingWanAddr,
--     cabhCapMappingWanPort,
--     cabhCapMappingLanAddrType,
--     cabhCapMappingLanAddr,
--     cabhCapMappingLanPort,
       cabhCapMappingMode,
     cabhCapMappingMethod,
       cabhCapMappingProtocol,

--     cabhCapPassthroughMacAddr
       cabhCapPassthroughRowStatus
       }
     ETAT en cours
     DESCRIPTION
       "Groupe d'objets pour base MIB CDB."
     ::= { cabhCapGroups 1 }

FIN
```

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série B	Moyens d'expression: définitions, symboles, classification
Série C	Statistiques générales des télécommunications
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	**Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias**
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	RGT et maintenance des réseaux: systèmes de transmission, circuits téléphoniques, télégraphie, télécopie et circuits loués internationaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données et communication entre systèmes ouverts
Série Y	Infrastructure mondiale de l'information et protocole Internet
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2003