Unión Internacional de Telecomunicaciones

# UIT-T J.167

(11/2005)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

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

IPCablecom

## Requisitos del aprovisionamiento de un dispositivo adaptador de terminal de medios para la entrega de servicios en tiempo real por redes de televisión por cable que utilizan módems de cable

Recomendación UIT-T J.167

UIT-T

ITU Unión Internacional de Telecomunicaciones

# Recomendación UIT-T J.167

## Requisitos del aprovisionamiento de un dispositivo adaptador de terminal de medios para la entrega de servicios en tiempo real por redes de televisión por cable que utilizan módems de cable


**Resumen**

En esta Recomendación se describe el proceso de inicialización y aprovisionamiento de un dispositivo adaptador de terminal de medios (MTA) insertado de IPCablecom. Se define además en la presente Recomendación el formato del fichero de configuración utilizado para el aprovisionamiento del dispositivo MTA.



**Orígenes**

La Recomendación UIT-T J.167 fue aprobada el 29 de noviembre de 2005 por la Comisión de Estudio 9 (2005-2008) del UIT-T por el procedimiento de la Recomendación UIT-T A.8.

## PREFACIO

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

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

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

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

## NOTA

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

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

## PROPIEDAD INTELECTUAL

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

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

# ÍNDICE

# Recomendación UIT-T J.167

## Requisitos del aprovisionamiento de un dispositivo adaptador de terminal de medios para la entrega de servicios en tiempo real por redes de televisión por cable que utilizan módems de cable

### 1 Alcance

La presente Recomendación describe el proceso de inicialización y aprovisionamiento de un dispositivo adaptador de terminal de medios (MTA, *media terminal adaptor*) de IPCablecom. Se refiere sólo al aprovisionamiento de un dispositivo MTA incorporado de IPCablecom por un único proveedor de aprovisionamiento y gestión de red.

### 2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

– Recomendación UIT-T J.83 (1997), *Sistemas digitales multiprogramas para servicios de televisión, sonido y datos de distribución por cable.*

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

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

– Recomendación UIT-T J.166 (2005)*, *Marco de las bases de información de gestión IPCablecom.*

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

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

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

– IETF RFC 2475 (1998), *An Architecture for Differentiated Services*.

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

– IETF RFC 2833 (2000), *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*.

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

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

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

---

* Reemplaza las Recs. UIT-T J.166 (2001), J.168 (2001), J.169 (2001) y J.176 (2002).

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

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

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

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

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

– IETF RFC 3495 (2003), *Dynamic Host Configuration Protocol (DHCP) Option for CableLabs Client Configuration*.

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

– IETF RFC 3594 (2003), *PacketCable Security Ticket Control Sub-Option for the DHCP CableLabs Client Configuration (CCC) Option*.

– IETF RFC 3617 (2003), *Uniform Resource Identifier (URI) Scheme and Applicability Statement for the Trivial File Transfer Protocol (TFTP)*.

## 3 Términos y definiciones

En esta Recomendación se definen los términos siguientes.

**3.1 módem de cable**: Un módem de cable es un dispositivo de terminación de dos capas en el que termina el extremo cliente de la conexión J.112.

**3.2 IPCablecom**: Proyecto del UIT-T que incluye una arquitectura y una serie de Recomendaciones para hacer posible la prestación de servicios en tiempo real (por ejemplo, el de telefonía) por redes de televisión por cable que utilizan módems de cable.

## 4 Abreviaturas y convenios

### 4.1 Abreviaturas

En esta Recomendación se utilizan las siguientes siglas.

CM Módem de cable (*cable modem*)

CMS Servidor de gestión de llamada (*call management server*)

CPE Equipo en las instalaciones del cliente (*customer premises equipment*)

DHCP Protocolo dinámico de configuración de anfitrión (*dynamic host configuration protocol*)

DNS Sistema de nombres de dominio (*domain name system*)

FQDN Nombre de dominio completamente cualificado (*fully qualified domain name*)

HTTP Protocolo de transferencia de hipertexto (*hypertext transfer protocol*)

IP Protocolo Internet (*Internet protocol*)

IPSec Seguridad del protocolo Internet (*Internet protocol security*)

MAC Control de acceso a medios (*media access control*)

MTA Adaptador de terminal de medios (*media terminal adaptor*)

RTPC Red telefónica pública conmutada

SNMP Protocolo simple de gestión de red (*simple network management protocol*)

TFTP Protocolo de transferencia de ficheros trivial (*trivial file transfer protocol*)

TGS Servidor que concede tique (*ticket granting server*)

### 4.2 Convenios

Se entiende que la implementación de esta Recomendación es opcional. En caso de implementarse, ha de interpretarse que los tiempos verbales de obligación firme, así como el adjetivo "OBLIGATORIO" indican los aspectos obligatorios de esta Recomendación. A lo largo de esta Recomendación, las palabras utilizadas para señalar la importancia de requisitos particulares son las que se indican a continuación:

"OBLIGACIÓN FIRME" La OBLIGACIÓN FIRME se expresa con el futuro simple del verbo principal (futuro de mandato), el verbo auxiliar "DEBER" (DEBE, DEBERÁ) o el adjetivo "OBLIGATORIO". En algunos casos también pueden utilizarse otras expresiones con significado de OBLIGACIÓN.

"PROHIBICIÓN FIRME" La PROHIBICIÓN FIRME se expresa mediante la negación de la OBLIGACIÓN FIRME

"CONVENIENCIA" La CONVENIENCIA se expresa con el tiempo condicional del verbo modal "DEBER" (DEBERÍA) u otros verbos con significado de CONVENIENCIA (aconsejar, recomendar, ser conveniente) o mediante el adjetivo "RECOMENDADO". Hay que entender plenamente y sopesar las consecuencias que tendría la inobservancia de una determinada disposición, aunque en ciertas circunstancias pueda haber razones fundamentadas para ello.

"OPCIÓN" La OPCIÓN se expresa mediante el verbo "PODER" (PUEDE, PODRÁ), u otras expresiones que indican posibilidad o probabilidad ("ser posible"), o los adjetivos "OPCIONAL" y "FACULTATIVO". La inclusión o no de una determinada opción, bien porque el mercado lo exige o para mejorar un producto, no afectará a la compatibilidad.

## 5 Introducción

### 5.1 Objetivos del servicio

A los operadores de cable les interesa instalar sistemas de comunicaciones de alta velocidad en redes de televisión por cable. Lo que pretenden es prestar servicios de comunicaciones vocales y de vídeo, así como servicios de datos basados en la transferencia bidireccional de tráfico con protocolo Internet (IP), entre la cabecera del sistema de cable y las posiciones de los clientes, por una red de cable totalmente coaxial o híbrida de fibra óptica/cable coaxial (HFC, *hybrid-fiber/coax*), definida por las Recs. UIT-T J.83 y J.112. En la figura 1 se muestra esto de forma simplificada.

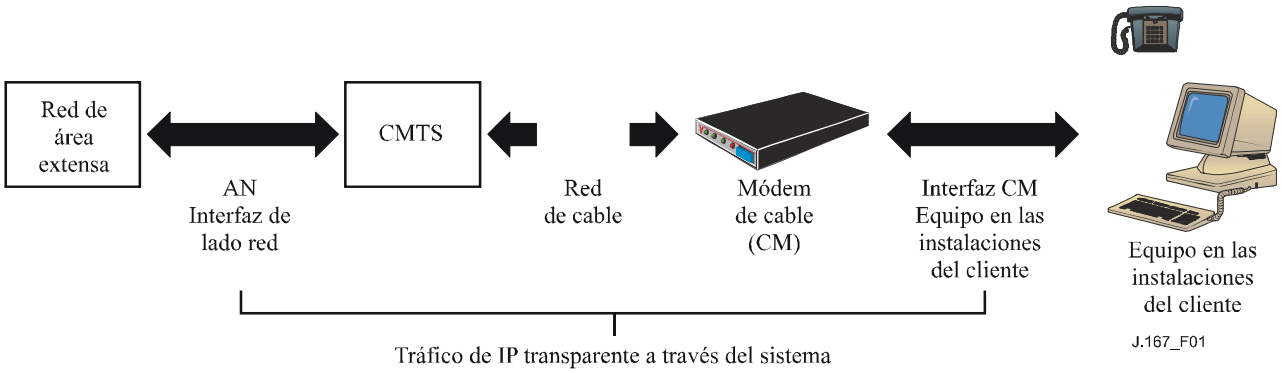


**Figura 1/J.167 – Tráfico de IP transparente a través del sistema de datos por cable**

El trayecto de transmisión por el sistema de cable se realiza en la cabecera por un sistema de terminación de módem de cable (CMTS, *cable modem termination system*), y, en la posición de cada cliente, por un módem de cable (CM, *cable modem*). El objetivo es que los operadores transfieran de manera transparente el tráfico IP entre estas interfaces.

## 5.2 Objetivos de la especificación

Los requisitos aplicables al aprovisionamiento de dispositivos son como sigue:

- Un único dispositivo físico (por ejemplo, un MTA incorporado) deberá ser aprovisionado y gestionado por completo por una entidad empresarial única. Este proveedor puede establecer relaciones empresariales con otros proveedores para servicios tales como los de datos, comunicaciones vocales y servicios de otro tipo.
- Un MTA incorporado es un MTA de IPCablecom combinado con un CM. Se DEBEN efectuar pasos tendentes al aprovisionamiento tanto del CM como del dispositivo IPCablecom para aprovisionar este MTA incorporado. El MTA DEBE tener dos direcciones IP, una de ellas para el componente CM y otra, diferente, para el componente MTA. El MTA incorporado DEBE tener dos direcciones MAC, una para el componente CM y otra, diferente, para el componente MTA. Además, el MTA DEBERÁ funcionar en dos entornos cuando la dirección IP del MTA esté en la misma subred, o en una subred distinta del CM.
- IPCablecom requiere un FQDN único para el componente MTA del MTA incorporado. Ese FQDN DEBE incluirse en la OFERTA de DHCP y en el mensaje ACUSE DE RECIBO del DHCP al componente MTA. IPCablecom no establece ningún otro requisito respecto al FQDN en el componente CM del MTA incorporado distinto de los de la Rec. UIT-T J.112. La correspondencia entre el FQDN y la dirección IP DEBE ser configurada en el servidor DNS de red y ha de estar a disposición del resto de la red.
- El aprovisionamiento del MTA incorporado de IPCablecom DEBE utilizar la opción 12 y la opción 15 de DHCP para entregar el FQDN del MTA al MTA incorporado.
- El aprovisionamiento del MTA incorporado de IPCablecom DEBE soportar dos ficheros de definición de la configuración distintos, a saber, un fichero de definición de la configuración especificado en la Rec. UIT-T J.112 para el componente CM y un fichero de definición de la configuración especificado por IPCablecom para el componente MTA.
- El MTA incorporado queda fuera de la frontera de confianza de la red de IPCablecom J.160 relativa a la arquitectura de IPCablecom.
- IPCablecom DEBE soportar la descarga del software DOCSIS 1.1 (Rec. UIT-T J.112) o DOCSIS 2.0 (Rec. UIT-T J.122), como se define en la Rec. UIT-T J.112. El proceso de descarga de software DOCSIS 1.1 o DOCSIS 2.0 soporta la descarga de un único fichero al

módem de cable o al MTA incorporado. DEBERÁ utilizarse una única descarga de software DOCSIS 1.1 o DOCSIS 2.0 para actualizar el código de ambos DOCSIS y de las funciones de software IPCablecom.

- IPCablecom DEBE soportar la coexistencia de SNMPv2c para las operaciones de gestión de red en los dispositivos aprovisionados con el flujo básico o el flujo híbrido y la coexistencia de SNMPv3/v2 para las operaciones de gestión de red cuando el dispositivo está aprovisionado con el flujo seguro.
- El aprovisionamiento de un MTA incorporado de IPCablecom reduce al mínimo la repercusión en la red de los dispositivos que se atienen a la Rec. UIT-T J.112/J.122 (CM y CMTS).
- Son preferibles las soluciones a base de servidores normalizados (TFTP, SNMP, DNS, etc.). Se sobreentiende que quizá haga falta, además de esos protocolos, una capa de aplicación, para coordinar la configuración de un MTA incorporado de IPCablecom.
- Donde así proceda, se soportarán los protocolos de gestión de J.112/J.122 (SNMP, DHCP, TFTP).

## 5.3 Arquitectura de referencia de IPCablecom

La figura 2 muestra la arquitectura de referencia de la red IPCablecom. Para una información más detallada sobre esta arquitectura de referencia J.160 relativa a la arquitectura de IPCablecom.

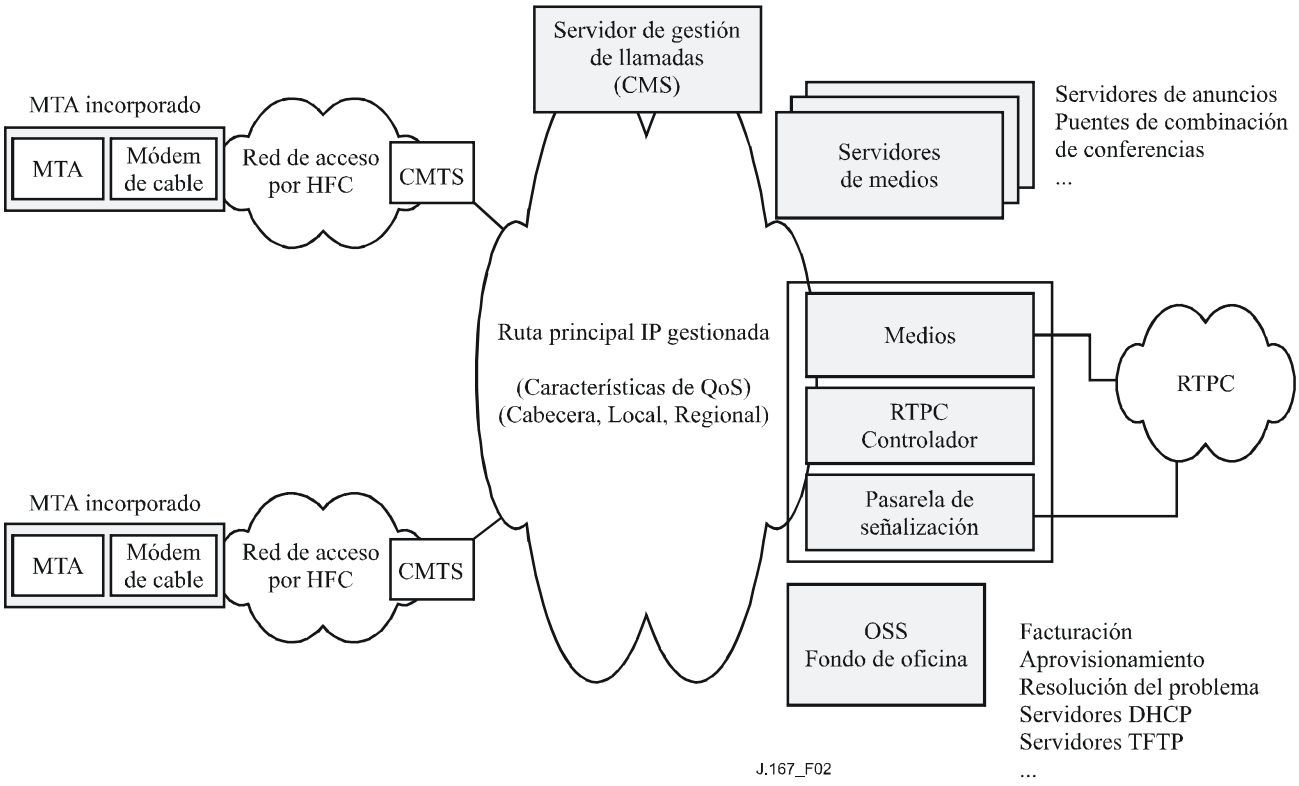


**Figura 2/J.167 – Modelo de referencia de componente de red IPCablecom (parcial)**

## 5.4 Componentes e interfaces

La figura 3 muestra la arquitectura básica de referencia de aprovisionamiento de MTA incorporado de IPCablecom. En dicha figura se representan los componentes y las interfaces a los que se refiere la presente Recomendación.

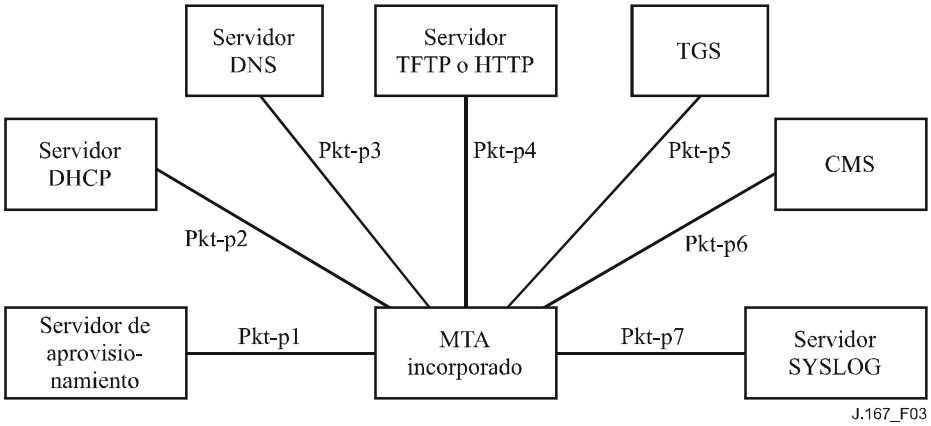


**Figura 3/J.167 – Interfaces de aprovisionamiento de IPCablecom**

### 5.4.1 MTA

El MTA DEBE cumplir, durante la secuencia de aprovisionamiento, los requisitos que se indican a continuación.

#### 5.4.1.1 Requisitos de seguridad del MTA

El MTA DEBE cumplir, durante la secuencia de aprovisionamiento, los requisitos de seguridad que se indican a continuación.

- La base de información de gestión (MIB, *management information base*) del dispositivo MTA se estructura de modo que represente la asignación de un punto extremo MTA a un CMS. Puede encontrarse más información sobre la asociación de seguridad entre un MTA y un CMS en la Rec. UIT-T J.170.
- El nombre principal Kerberos CMS no está explícitamente configurado en los puntos extremos MTA. El MTA DEBE poder determinar el nombre principal Kerberos CMS de acuerdo con la FQDN CMS, como se especifica en la Rec. UIT-T J.170.
- Para cada par único nombre principal/dominio Kerberos del CMS asignado a un punto extremo, el MTA DEBE obtener un solo tique Kerberos de acuerdo con la Rec. UIT-T J.170.
- Si el MTA ya tiene un tique Kerberos válido para ese CMS, el MTA NO DEBE pedir un tique Kerberos adicional para el CMS (a menos que la hora de expiración del tique Kerberos vigente ≤ hora actual + periodo de gracia de PKINIT, en cuyo caso el MTA DEBE obtener un tique nuevo para el mismo CMS).
- Si un FQDN de CMS corresponde a múltiples direcciones IP, el MTA DEBE establecer inicialmente un par de asociaciones de seguridad IPSec con una de las direcciones IP devueltas por el servidor DNS. El MTA PUEDE establecer también inicialmente asociaciones de seguridad IPSec con las direcciones IP de CMS adicionales. Puede encontrarse más información en la Rec. UIT-T J.170.
- Si el MTA ya tiene un par de asociaciones de seguridad activas (de entrada y de salida) con una dirección IP de CMS particular, el MTA NO DEBE tratar de establecer asociaciones de seguridad adicionales con la misma dirección IP.

Durante la secuencia de aprovisionamiento no hay requisitos específicos de seguridad para el flujo básico y el flujo híbrido.

#### 5.4.1.2 Requisitos de SNMP de MTA

El MTA DEBE cumplir, durante la secuencia de aprovisionamiento por flujo seguro, los requisitos del SNMP versión 3 (SNMPv3) que se indican a continuación:

- La seguridad del SNMPv3 del MTA es ajena a la seguridad del SNMPv3 del CM y difiere de la misma. La información de seguridad del USM (clave de autenticación y privacidad, y otras entradas en el cuadro del USM) se establece por separado.
- La inicialización del SNMPv3 se DEBE completar antes de informar sobre el enrolamiento del aprovisionamiento.
- En el flujo seguro, el MTA DEBE soportar la gestión de los dispositivos SNMPv3 y SNMPv2, como se define en RFC 3414 y RFC 3584.

El MTA DEBE ajustarse a los siguientes requisitos SNMPv2c durante la secuencia de aprovisionamiento de flujo híbrido o flujo básico:

- La inicialización del SNMPv2c DEBE completarse inmediatamente después de la fase DHCP.

La gestión del dispositivo SNMPv2c es la definida en RFC 3584.

### 5.4.2 Servidor de aprovisionamiento

El servidor de aprovisionamiento está formado por los componentes siguientes:

- Una aplicación de aprovisionamiento – La aplicación de aprovisionamiento se encarga de coordinar el proceso de aprovisionamiento del MTA incorporado. Esta aplicación tiene una entidad SNMP asociada.
- Una entidad SNMP de aprovisionamiento – La entidad SNMP de aprovisionamiento DEBE incluir un manejador de trampa/informes para el registro de aprovisionamiento y las trampas/informes de situación de aprovisionamiento así como un aparato SNMP para la recuperación de capacidades del dispositivo y la fijación del nombre del fichero Configuración y el método de acceso. Véase una descripción de los atributos de acceso del MTA a la base de información de gestión (MIB) en la Rec. UIT-T J.166 relativa a la MIB de un MTA de IPCablecom.

La interfaz entre la aplicación de aprovisionamiento y la entidad SNMP asociada no se especifica en IPCablecom y se deja a criterio del fabricante. La interfaz y el servidor de aprovisionamiento y el servidor TFTP no se especifica en IPCablecom y se deja a criterio del fabricante.

### 5.4.3 MTA a servidor Syslog de telefonía

Los MTA de IPCablecom DEBEN aplicar el mecanismo de evento de gestión de acuerdo con la Rec. UIT-T J.172 e incorporar la MIB MEM que se define en la Rec. UIT-T J.166, y que incluye el soporte del servidor Syslog.

Del mismo modo, los MTA de IPCablecom DEBEN aplicar los eventos de gestión de aprovisionamiento IPCablecom que se describen en el anexo A/J.172.

### 5.4.4 MTA a servidor DHCP

Esta interfaz identifica requisitos específicos del servidor DHCP y del cliente para la asignación IP durante el proceso de inicialización del MTA:

- Tanto el servidor DHCP como el MTA incorporado DEBEN soportar el código de opción DHCP 6, 7, 12, 15, 43, 60 y el código de opción DHCP 122 (definido en RFC 2132). El código de opción 12 (nombre de anfitrión) y 15 (nombre de dominio) DEBEN formar un nombre de dominio plenamente calificado y DEBEN poder ser resueltos por el servidor DNS.

- El servidor DHCP DEBE aceptar y soportar mensajes radiodifundidos y unidifundidos, de acuerdo con RFC 3396, del cliente DHCP del MTA.
- El servidor DHCP DEBE incluir el FQDN asignado del MTA en los mensajes OFERTA y ACUSE DE RECIBO DHCP al componente MTA del MTA incorporado. Véase en RFC 2131 la descripción detallada del mensaje de OFERTA de DHCP.

### 5.4.5 MTA a aplicación de aprovisionamiento

Esta interfaz identifica requisitos específicos de la aplicación de aprovisionamiento a efectos de inicialización y registro del MTA. Los requisitos de la aplicación de aprovisionamiento son como sigue:

- El MTA DEBE generar un ID de correlación – un valor arbitrario que se intercambiará como parte de los datos de capacidad de dispositivo en la aplicación de aprovisionamiento. Este valor se utiliza como un identificador para correlacionar eventos relacionados en la secuencia de aprovisionamiento del MTA.
- La aplicación de aprovisionamiento DEBE proporcionar al MTA su fichero de datos de configuración de MTA. El fichero de definición de la configuración de MTA es específico del componente MTA del MTA incorporado y difiere del fichero de datos de configuración del componente CM.
- El formato del fichero de datos de configuración consta de datos binarios de tipo/longitud/valor (T/L/V, *type/length/value*) adecuados para el transporte en aplicación del método de acceso TFTP o HTTP especificado.
- La aplicación de aprovisionamiento DEBE tener la capacidad de configurar el MTA con proveedores de servicios de datos y voz diferentes.
- La aplicación de aprovisionamiento DEBE utilizar únicamente el SNMPv3 para aprovisionar dispositivos con el flujo seguro. El soporte de los flujos básico a híbrido es opcional para la aplicación de aprovisionamiento. Si se soportan los flujos básico e híbrido, la aplicación de aprovisionamiento DEBE utilizar únicamente el SNMPv2c para aprovisionar dispositivos con los flujos híbrido o básico.
- La aplicación de aprovisionamiento DEBE tener SNMPv3 y SNMPv2 para realizar la gestión del dispositivo.
- La aplicación de aprovisionamiento DEBE soportar el aprovisionamiento incremental en línea de dispositivos/abonados utilizando el SNMP.
- El MTA DEBE especificar todas sus capacidades en la opción 60 DHCP de conformidad con la cláusula 10.
- La aplicación de aprovisionamiento NO DEBE asumir ningún tipo de capacidad que no tenga valores por defecto. En caso de que las capacidades proporcionadas por el MTA no sean compatibles en formato y/o número y/o valores, la aplicación de aprovisionamiento DEBE utilizar otros medios para identificar las capacidades del MTA (por ejemplo, SNMPv3, de ser posible).

### 5.4.6 MTA a CMS

La principal interfaz entre el MTA y el CMS es la de señalización. En la Rec. UIT-T J.162 sobre señalización de IPCablecom figura una descripción detallada de la interfaz:

- El CMS DEBE aceptar las peticiones de canal de señalización y portador procedentes de un MTA que tenga una asociación de seguridad activa.
- El CMS NO DEBE aceptar las peticiones de canal de señalización y portador procedentes de un MTA, que no tenga una asociación de seguridad activa, a menos que esté aprovisionado para hacerlo con la información correspondiente al objeto MIB "pktcMtaDevCmslpsecCtrl".

### 5.4.7 MTA a servidor de seguridad (KDC)

La interfaz entre el MTA y el centro de distribución de claves (KDC, *key distribution center*) DEBE ser conforme a la Rec. UIT-T J.170, Especificación de seguridad de IPCablecom.

El mecanismo de retroceso y reintento de intercambio AP-REQ/REP de la negociación de claves SNMPv3 kerberizada que se define en la Rec. UIT-T J.170 se controla gracias a los valores que proporciona la subopción 5 de la opción 122 DHCP (véase 8.1.4).

El mecanismo de retroceso y reintento de intercambio AS-REQ/REP de la negociación de claves SNMPv3 kerberizada que se define en la Rec. UIT-T J.170 está controlada por los valores que proporciona la subopción 4 de la opción 122 DHCP (véase 8.1.3) o por los valores por defecto de los objetos MIB correspondientes en el cuadro de sector, de no estar presente en la subopción 4 en la opción 122 DHCP.

### 5.4.8 MTA y acceso a fichero de datos de configuración

Esta Recomendación permite más de un método de acceso para la telecarga del fichero de datos de configuración del MTA:

- El MTA DEBE soportar el método de acceso TFTP para telecargar el fichero de datos de configuración del MTA.
- El MTA PUEDE soportar el método de acceso HTTP para telecargar el fichero de datos de configuración del MTA.
- El servidor de aprovisionamiento DEBE proporcionar al MTA la dirección del servidor TFTP/HTTP con codificación URL y el nombre de fichero de definición de la configuración mediante un mensaje de FIJAR de SNMPv3 en el flujo seguro. El servidor de aprovisionamiento DEBE proporcionar al MTA la dirección del servidor TFTP/HTTP con codificación URL mediante un mensaje FIJAR de SNMPv2c, si se soporta el modo de aprovisionamiento mediante flujo híbrido. El flujo básico no requiere ningún mensaje FIJAR SNMP para obtener el fichero de definición de la configuración. El servidor de aprovisionamiento DEBE proporcionar al MTA la dirección de servidor TFTP/HTTP en los campos "file" y "siaddr" de DHCP, si soporta el modo de aprovisionamiento mediante el flujo básico. Puede encontrarse más información al respecto en 7.3.

### 5.4.9 Extensiones del DOCSIS para aprovisionamiento del MTA

La presente Recomendación requiere que se soporten las adiciones siguientes a los flujos DOCSIS a efectos de autoconfiguración del MTA:

- DEBE aplicarse en DOCSIS un nuevo código de opción 122 de DHCP así como en los procedimientos asociados.

## 6 Visión general del aprovisionamiento

El aprovisionamiento es un subconjunto del control de gestión de la configuración. Entre los aspectos relativos al aprovisionamiento figuran, pero sin ser los únicos, la definición de atributos de datos configurables, la gestión de valores de atributos definidos, la inicialización y el registro del recurso, la gestión del soporte físico del recurso y la notificación de datos de la configuración. El recurso (al que también se alude como recurso gestionado) se refiere siempre al dispositivo MTA. Por otra parte, también al abonado asociado se hace referencia denominándolo recurso gestionado.

### 6.1 Aprovisionamiento del dispositivo

El aprovisionamiento del dispositivo es el proceso por el cual un dispositivo MTA incorporado se configura de modo que soporte los servicios de comunicaciones vocales.

El aprovisionamiento del dispositivo conlleva el que el MTA obtenga su configuración IP, que requiere a efectos de conectividad de red básica, se anuncie a sí mismo a la red y extraiga sus datos de configuración de su servidor de configuración.

Cuando el dispositivo sea aprovisionado utilizando el "flujo seguro", el dispositivo MTA DEBE poder verificar la autenticidad del fichero de definición de la configuración que telecarga del servidor. El "flujo seguro" generado por el fichero de definición de la configuración se "firma" y puede quedar "sellado". Para más información, véase la Rec. UIT-T J.170.

Por lo que se refiere a las reglas de aprovisionamiento relacionadas con las asociaciones de seguridad, véase 5.4.1.

Cuando el dispositivo se aprovisiona utilizando los flujos básico o híbrido, el MTA DEBE realizar una verificación de la integridad del contenido del fichero de definición de la configuración. Pueden encontrarse más detalles al respecto en 9.1.

## 6.2 Aprovisionamiento de punto extremo

El aprovisionamiento de punto extremo se produce cuando un MTA aprovisionado se autentica a sí mismo ante el CMS, y establece una asociación de seguridad con ese servidor. Esto permite proteger la señalización de llamadas subsiguientes en el marco de la asociación de seguridad establecida.

El MTA DEBE ajustarse a los requisitos definidos en la especificación de seguridad IPCablecom (Rec. UIT-T J.170) para la gestión de claves kerberizadas NCS, independientemente del flujo de aprovisionamiento (seguro, híbrido o básico) con el que se haya aprovisionado el MTA.

## 6.3 Transiciones de estado de aprovisionamiento

La figura 4 representa estados lógicos del dispositivo y posibles transiciones a través de esos estados lógicos. Esta representación sólo tiene una finalidad ilustrativa, sin representar, por tanto, ninguna implementación específica. Las transiciones de estado del MTA que siguen no especifican el número de tentativas de reintento ni el valor de la temporización de los reintentos.

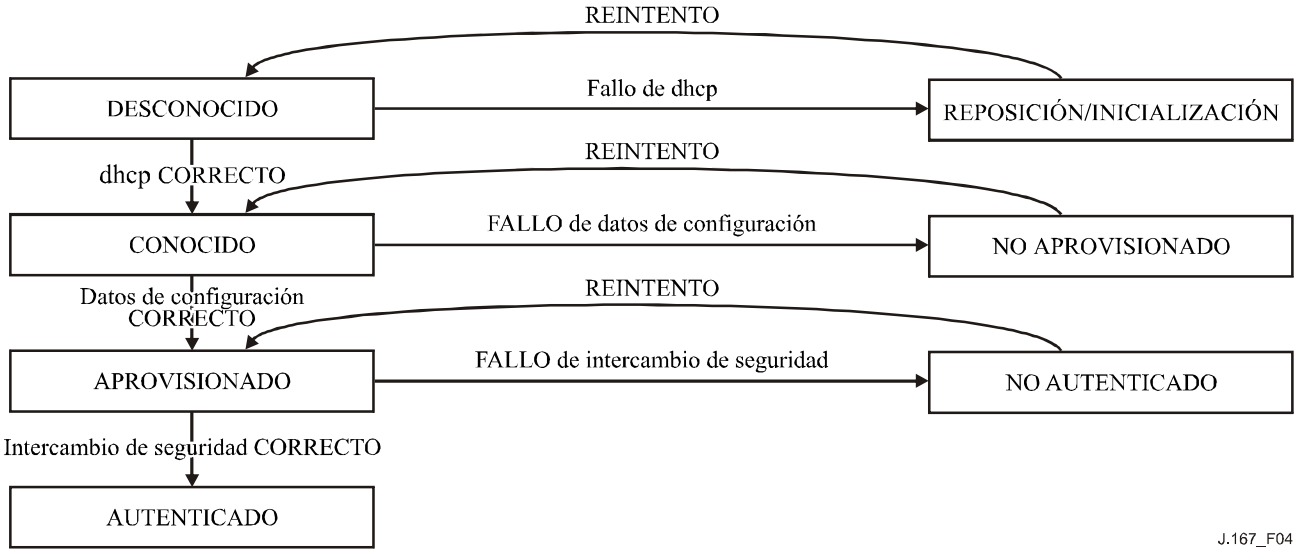


**Figura 4/J.167 – Estados del dispositivo y transiciones de estado en el aprovisionamiento por flujo seguro**

## 6.4 Transiciones de estado de aprovisionamiento por flujos básico e híbrido

La figura 5 representa estados lógicos del dispositivo y posibles transiciones a través de estos estados lógicos. Esta representación sólo tiene una finalidad ilustrativa, sin representar, por tanto, ninguna implementación específica. Las transiciones de estado del MTA que siguen no especifican el número de tentativas de reintento ni el valor de la temporización de los reintentos.

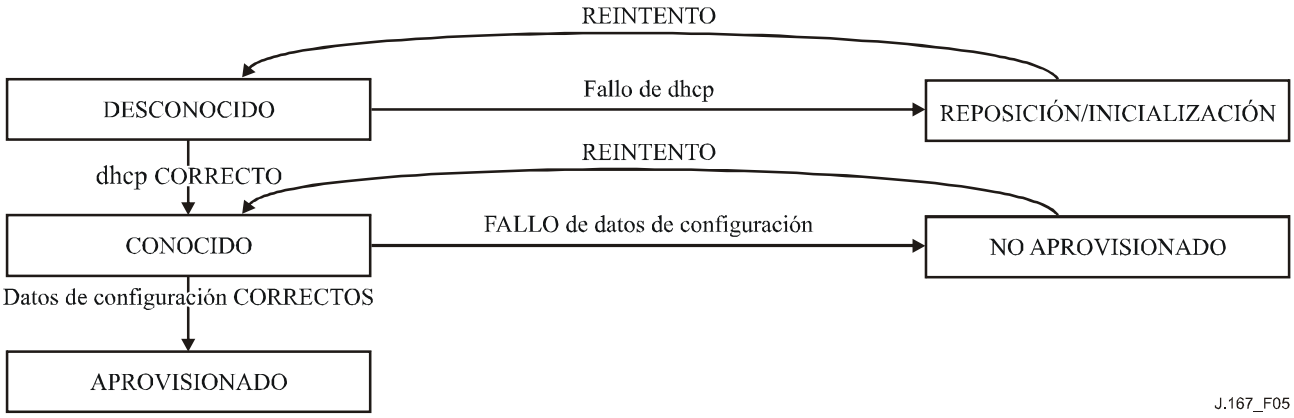


**Figura 5/J.167 – Estados del dispositivo y transiciones de estado en el aprovisionamiento de flujos básico e híbrido**

## 7 Flujos de aprovisionamiento

Un MTA IPCablecom se aprovisiona mediante uno de los tres flujos de aprovisionamiento.

- El flujo seguro soporta la autenticación mutua Kerberos entre el MTA y el sistema de aprovisionamiento, así como la mensajería SNMPv3 kerberizada. Los MTA IPCablecom y las aplicaciones de aprovisionamiento DEBEN soportar el flujo seguro.
- Los flujos básicos son flujos de aprovisionamiento semejantes a DOCSIS simplificados sin Kerberos ni seguridad SNMPv3, ni enrolamiento SNMP mediante mensajes INFORME SNMP. Los MTA IPCablecom y las aplicaciones de aprovisionamiento DEBERÍAN soportar los flujos básicos.
- Los flujos híbridos son básicamente flujos seguros de los que se ha eliminado el intercambio de mensajes Kerberos y donde el SNMPv2c ha sustituido al SNMPv3. Los MTA IPCablecom y las aplicaciones de aprovisionamiento DEBERÍAN soportar los flujos híbridos.

Toda mención al SNMP que se hace en esta Recomendación sin hacer referencia específica a la versión de protocolo SNMP debe interpretarse de la siguiente manera:

- En el caso del flujo seguro, el MTA DEBE soportar 'únicamente el SNMPv3' para el aprovisionamiento y coexistencia SNMPv3/v2c para la gestión de red y/o las operaciones de supervisión. La coexistencia SNMPv3/v2c DEBE soportarse y configurarse utilizando los valores de TLV-38 o TLV-11 y TLV-64 del fichero de definición de la configuración del MTA.
- En el caso de los flujos híbrido y básico, el MTA DEBE soportar el SNMPv2c para el aprovisionamiento, la gestión de red y/o las operaciones de supervisión. El nivel de acceso SNMPv2c DEBE soportarse de acuerdo con los valores de TLV-38 o TLV-11 y TLV-64 del fichero de definición de la configuración del MTA.

Un MTA también puede configurarse con objetivos SNMPv2c adicionales mediante su fichero de definición de la configuración utilizando TLV-38 o TLV-11 y TLV-64.

Un MTA recibe las instrucciones de ejecutar un flujo específico mediante los contenidos de las subopción 6 de la opción 122 de DHCP, como se describe en 8.1.5. Todos estos flujos comienzan con un conjunto común de fases de flujo.

## 7.1 Retroceso, reintentos y temporizaciones

Los mecanismos de retroceso ayudan a la red a estrangular el registro del dispositivo en condiciones de registro típicas o de registro en masa cuando las peticiones del cliente MTA no son atendidas dentro de los plazos de temporización especificados por el protocolo. Los detalles respecto a cómo se produce el aprovisionamiento en condiciones de registro en masa quedan fuera del alcance de IPCablecom, no obstante lo cual, en la presente cláusula se hacen las recomendaciones y se establecen los requisitos que se indican a continuación:

- El estrangulamiento de registros PUEDE basarse en el registro DOCSIS CM.
- El MTA DEBE atenerse a los mecanismos de temporización y reintento de la especificación de DHCP (RFC 2131) y HTTP. Se recomienda ajustarse a IETF RFC 3413 en cuanto a los mecanismos de temporización y reintento de SNMP.
- El MTA DEBE utilizar temporización adaptable para TFTP, como se especifica en DOCSIS (Rec. UIT-T J.112/J.122).
- El MTA DEBE seguir las recomendaciones sobre retroceso y reintento definidas en la Rec. UIT-T J.170, especificación de seguridad, por lo que se refiere a flujos de mensajes de seguridad.
- En todos los flujos de aprovisionamiento (seguro, híbrido y básico) que se describen en 7.2, 7.3 y 7.4.
  - El temporizador de configuración DEBE ponerse en marcha inmediatamente después de recibir el mensaje ACUSE DE RECIBO DHCP y DEBE pararse cuando se complete la respuesta del fichero de definición de la configuración TFTP/HTTP.
  - En caso de que el temporizador de aprovisionamiento expire antes de que se complete la respuesta del fichero de definición de la configuración TFTP/HTTP, el MTA DEBE volver a MTA1.
  - El MTA no DEBE esperar a que expire el temporizador de aprovisionamiento antes de reaccionar a las condiciones de fallo en cada una de las etapas del aprovisionamiento. Por ejemplo, en el caso de flujo seguro, si ocurre un fallo en MTA19, el MTA no debe esperar a que expire el temporizador de aprovisionamiento, sino volver inmediatamente a MTA1 cuando se constate la condición de fallo.
- Cuando se utiliza el flujo de aprovisionamiento seguro, si ocurre un fallo en cualquiera de las fases relacionadas con PROV_SNMP_ENTITY (MTA13, MTA14, MTA15, MTA19) antes de que el MTA obtenga el fichero de definición de la configuración del dispositivo y el MTA resuelva múltiples direcciones IP para PROV_SNMP_ENTITY (FQDN recibido en la subopción 3 de la opción 122), entonces DEBE reintentar cada paso con las direcciones IP resueltas antes de volver a MTA1, a menos que la Rec. UIT-T J.170 dicte lo contrario. No obstante, cabe señalar que una vez que el MTA selecciona una dirección IP resuelta para utilizarla en MTA13, DEBE utilizar la misma dirección IP en MTA15 y MTA25.
- En el flujo de aprovisionamiento híbrido, de ocurrir un fallo en cualquiera de las fases relacionadas con PROV_SNMP_ENTITY (H- MTA15, H-MTA19), antes de que el MTA obtenga el fichero de definición de la configuración del dispositivo y resuelva múltiples direcciones IP para PROV_SNMP_ENTITY (FQDN recibido en las subopción 3 de la opción 122), entonces DEBE reintentar cada paso con las direcciones IP resueltas antes de volver a MTA1. No obstante, cabe señalar que una vez que el MTA selecciona una

dirección IP resuelta para utilizarla en H-MTA15, DEBE utilizar la misma dirección IP en H-MTA25.

## 7.2 Flujos de inicialización de la activación de potencia del MTA incorporado

El cuadro 1 muestra el flujo de mensajes obligatorios a que DEBE atenerse el dispositivo MTA incorporado durante la inicialización de la activación de potencia (a menos que se indique explícitamente lo contrario). Se da por supuesto que no implican implementación ni limitan funcionalidad alguna.

Aunque estos flujos muestran la telecarga del fichero de definición de la configuración de MTA desde un servidor TFTP, el texto descriptivo detalla los requisitos para el soporte de la telecarga del fichero de definición de la configuración de MTA desde un servidor HTTP.

Obsérvese, en los detalles de los flujos que se exponen a continuación, que determinados pasos pueden dar la impresión de que constituirían un bucle si se produjera un fallo. En otras palabras, lo que hay que hacer si falla un paso es reintentar ese paso de nuevo. Se recomienda, no obstante, que si el número deseado de tentativas de retroceso y reintento no permite completar el paso de manera satisfactoria, el dispositivo que detecte el fallo genere una notificación de evento de fallo.

En los detalles del flujo que se muestran a continuación (véanse figura 6 y cuadro 1), el cálculo del valor generado y la criptación/descriptación del fichero de definición de la configuración del MTA DEBE ajustarse a los requisitos de la Rec. UIT-T J.170.

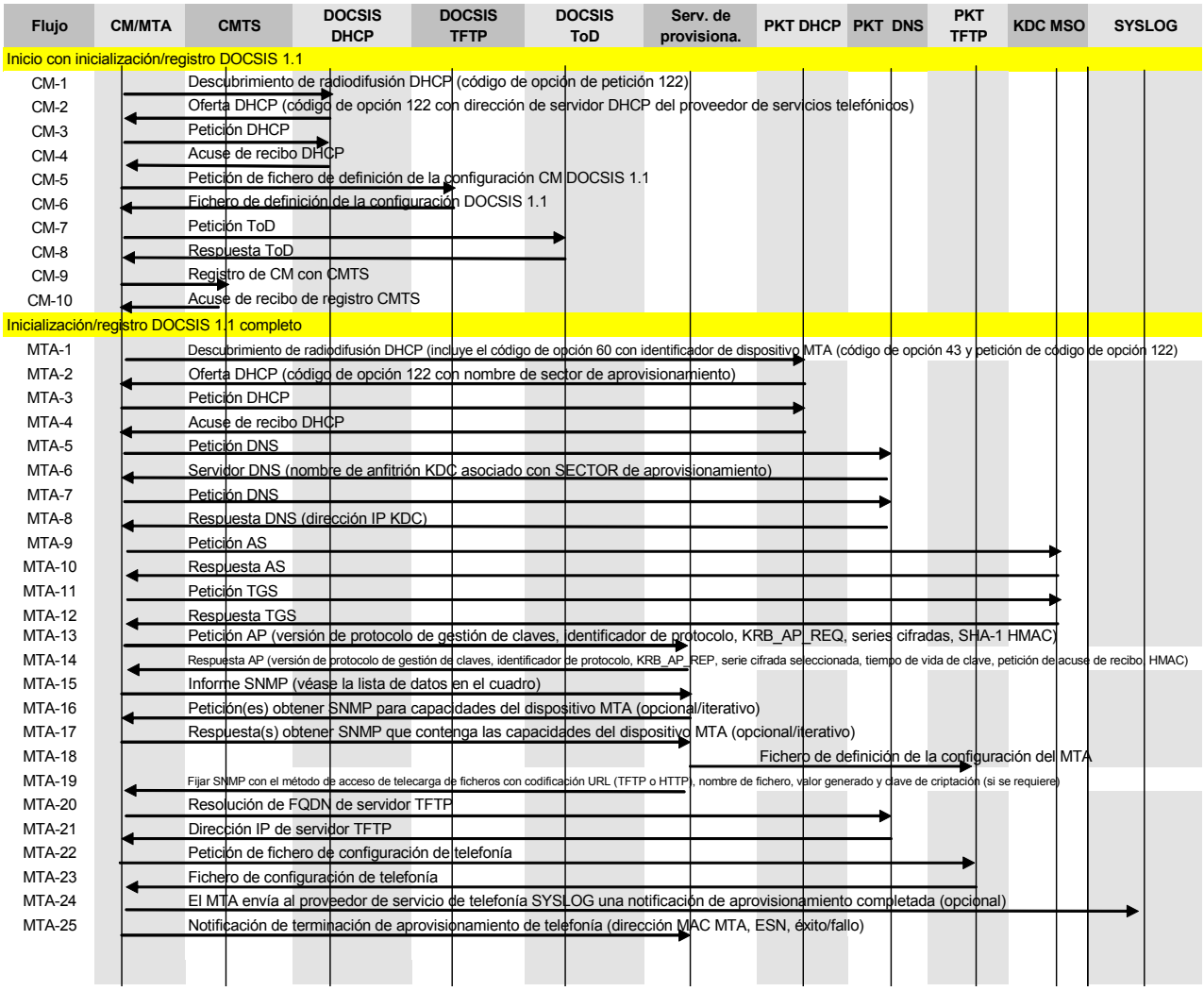


**Figura 6/J.167 – Flujo de inicialización de activación de potencia seguro del MTA incorporado**

## Cuadro 1/J.167 – Descripción de los flujos de inicialización de la activación de potencia del MTA incorporado

| Flujo | Descripción de los flujos de inicialización de la activación de potencia del MTA incorporado | Secuenciación del flujo normal | DEBE avanzar hasta aquí si falla este paso |
|---|---|---|---|
| CM1 | El dispositivo cliente empieza el registro del dispositivo haciendo que el componente CM envíe un mensaje de descubrimiento de DHCP radiodifundido.<br>En dicho mensaje se incluye un código de opción 60 (opción específica del vendedor) en formato "docsis1.1:xxxxxxx". Este mensaje DEBE pedir la opción 122 en la opción 55, que es la lista de parámetros de petición. El resto de este mensaje DEBE ser conforme a los datos de descubrimiento de DHCP definidos en la Rec. UIT-T J.112. | Inicial<br>DEBE avanzar en secuencia | De acuerdo con DOCSIS |
| CM2 | El servidor DHCP DOCSIS, si se ha configurado para soportar los dispositivos MTA, DEBE incluir el código de opción 122 con la subopción 1 y, posiblemente, la subopción 2, de conformidad con 8.1. Si se ha configurado para evitar la configuración de la porción MTA del dispositivo, la subopción 1 del código de opción 122 DEBE contener una dirección de servidor DHCP cuyo valor sea 0.0.0.0.<br>Los servidores DHCP DOCSIS sin conocimiento previo de los dispositivos MTA PUEDEN responder con OFERTAS DHCP que no incluyan la opción 122. | CM2 DEBE ocurrir una vez terminado CM1 | De acuerdo con el DOCSIS |
| CM3 | Una vez que se reciba la OFERTA DHCP, el CM DEBE verificar la opción 122 solicitada. De no estar presente, DEBE reintentar el proceso DESCUBRIMIENTO DHCP (CM1) exponencialmente en 3 intentos (por ejemplo, a intervalos de 2, 4 y 8 segundos). Si no logra recibir una OFERTA DHCP con la opción 122 tras haber aplicado el mecanismo de reintento exponencial, DEBE considerar las OFERTAS sin el código de opción 122 y aceptar una de ellas de conformidad con la especificación RFC 2131 de DHCP. El dispositivo de cliente (CM) DEBE enviar entonces un mensaje PETICIÓN DHCP radiodifundido al servidor DHCP cuya OFERTA se ha aceptado, como se especifica en la especificación DHCP de RFC 2131. | CM3 DEBE ocurrir una vez terminado CM2 | De acuerdo con DOCSIS |
| CM4 | El servidor DHCP envía al componente CM del dispositivo cliente un mensaje de ACUSE DE RECIBO de DHCP para confirmar la aceptación de los datos ofrecidos. Una vez recibido el mensaje ACUSE DE RECIBO DHCP, el CM debe verificar nuevamente la opción 122. La ausencia de opción 122 en el mensaje ACUSE DE RECIBO de DHCP aceptado por el CM implica que éste NO DEBE inicializar el MTA incorporado. La presencia de la opción 122 implica que DEBE inicializar el MTA y pasar la subopción 1 y, posiblemente la subopción 2.<br>Si el contenido de la opción de este mensaje ACUSE DE RECIBO de DHCP difiere de la de la OFERTA de DHCP anterior, el contenido de opción de este mensaje ACUSE DE RECIBO de DHCP DEBE considerarse prioritario (de acuerdo con RFC 2131). | CM4 DEBE ocurrir una vez terminado CM3 | De acuerdo con DOCSIS |

## Cuadro 1/J.167 – Descripción de los flujos de inicialización de la activación de potencia del MTA incorporado

| Flujo | Descripción de los flujos de inicialización de la activación de potencia del MTA incorporado | Secuenciación del flujo normal | DEBE avanzar hasta aquí si falla este paso |
|---|---|---|---|
| CM5-CM10 | El componente CM del dispositivo cliente completa el resto de la secuencia de registro especificada del CM. Se incluye aquí la telecarga del fichero de definición de la configuración de CM, la petición de registro de la hora del día y el registro en el CMTS. | CM5-CM10 DEBE ocurrir una vez terminado CM4 | De acuerdo con DOCSIS |
| MTA1 | Descubrimiento de radiodifusión DHCP. El MTA DEBE enviar un mensaje DESCUBRIMIENTO de DHCP radiodifundido. Este mensaje DEBE incluir un código de opción 60 (opción específica del vendedor) en formato "pktc1.0:xxxxxx". El MTA DEBE incluir el código de opción 43 de DHCP en el mensaje DESCUBRIMIENTO de DHCP, como se define en 8.5. El MTA DEBE pedir en la opción 55 de DHCP las opciones 1, 3, 6, 7, 12, 15 y 122. Si la subopción 1 del código de opción 122 de DHCP del CM (pasado por CM al MTA) contiene un servidor DHCP de valor 0.0.0.0, el MTA no DEBE intentar la configuración y DEBE mantenerse a la espera hasta que el CM lo reinicialice. | El MTA1 NO DEBE ocurrir hasta que haya terminado CM4 | Si falla el protocolo DHCP, repítase MTA1 |
| MTA2 | OFERTA de DHCP<br>El MTA puede recibir múltiples OFERTAS DHCP (durante el periodo de espera, de acuerdo con RFC 2131).<br>Los siguientes requisitos se aplican al MTA y/o a las aplicaciones de aprovisionamiento.<br>1) El MTA DEBE aceptar únicamente un mensaje OFERTA DHCP válido. Una OFERTA DHCP válida DEBE ser enviada por los servidores DHCP primarios o secundarios de vuelta en las subopciones 1 y 2 del código de opción 122 de DHCP tal y como lo haya obtenido el E-MTA en la fase CM-4 de aprovisionamiento del CM. Una OFERTA DHCP válida DEBE asimismo incluir las siguientes opciones: 1, 3, 6, 7, 12, 15, 122 con las subopciones 3 y 6 de la opción 122 DHCP. La opción 122 DHCP PUEDE contener además las subopciones 4, 5, 7, 8 y 9.<br>2) Si un servidor DHCP válido devuelve la subopción 6 de la opción 122 DHCP, quiere indicar que ha de aplicarse el flujo básico o híbrido, y el MTA DEBE ignorar las subopciones 4, 5, 7 y 9 de la opción 122 DHCP, de estar presentes.<br>3) Si un servidor DHCP válido devuelve la subopción 6 de la opción 122 DHCP, lo que indica que ha de utilizarse el flujo básico, el servidor de aprovisionamiento DEBE incluir la ubicación del fichero de configuración en los campos 'siaddr' y 'file' de las respuestas DHCP. | MTA2 DEBE ocurrir una vez terminado MTA1 | En caso de fallo de acuerdo con el protocolo DHCP, vuélvase a MTA1 |

## Cuadro 1/J.167 – Descripción de los flujos de inicialización de la activación de potencia del MTA incorporado

| Flujo | Descripción de los flujos de inicialización de la activación de potencia del MTA incorporado | Secuenciación del flujo normal | DEBE avanzar hasta aquí si falla este paso |
|---|---|---|---|
| MTA2 | 4) Si un servidor DHCP válido devuelve la subopción 6 de la opción 122 DHCP, indicando que ha de aplicarse el flujo seguro, el MTA DEBE procesar las subopciones 4, 5, 7 y 9 de la opción 122 DHCP.<br>A continuación el MTA aplica las siguientes normas al conjunto de OFERTAS DHCP válidas:<br>a) El MTA DEBE comprobar el valor de la subopción 3 de la opción 122 DHCP. Si todas las OFERTAS válidas contienen 0.0.0.0 en la subopción 3 de la opción 122 DHCP, el MTA no DEBE seguir procesando el DHCP y DEBE cerrarse hasta que se reinicialice. En caso contrario, el MTA DEBE seguir restringiendo el conjunto de OFERTAS válidas a aquellas que contengan un valor distinto de 0 en la subopción 3 de la opción 122 DHCP.<br>b) El MTA DEBE comprobar el valor de la subopción 6 de la opción 122 DHCP para ver si se encuentra una indicación de flujo seguro. Si ninguno de los mensajes de OFERTA DHCP del MTA hacia un flujo seguro, el MTA DEBE reintentar el proceso DESCUBRIMIENTO DHCP (MTA1) exponencialmente por 3 intentos (por ejemplo, a intervalos de 2, 4 y 8 segundos). Si no se recibe ninguna OFERTA DHCP válida que indique un flujo seguro, el MTA DEBE seleccionar una OFERTA DHCP de flujo híbrido válida o una OFERTA de flujo básico válida, por ese orden.<br>Si no se recibe ninguna OFERTA DHCP válida, el MTA DEBE dar un resultado de fallo para esa etapa del flujo de aprovisionamiento.<br>NOTA – En el caso del flujo seguro, si un MTA soporta el TGT y recibe un subopción 7 de opción 122 de DHCP puesta a FALSO, NO DEBE pedir el TGT. Si un MTA soporta el TGT y recibe una subopción 7 de opción 122 de DHCP con un valor de VERDADERO, debe pedir el TGT. Los MTA que no soportan los TGT DEBEN ignorar la subopción 7 de la opción 122 de DHCP. | | |
| MTA3 | PETICIÓN de radiodifusión de DHCP<br>Una vez que el MTA ha seleccionado una OFERTA de DHCP, DEBE enviar un mensaje PETICIÓN de DHCP radiodifundido para aceptar la OFERTA DHCP, de conformidad con RFC 2131. | MTA3 DEBE ocurrir una vez terminado MTA2 | En caso de fallo de acuerdo con el protocolo DHCP, vuélvase a MTA1 |

## Cuadro 1/J.167 – Descripción de los flujos de inicialización de la activación de potencia del MTA incorporado

| Flujo | Descripción de los flujos de inicialización de la activación de potencia del MTA incorporado | Secuenciación del flujo normal | DEBE avanzar hasta aquí si falla este paso |
|---|---|---|---|
| MTA4 | ACUSE DE RECIBO de DHCP<br>El servidor DHCP envía un mensaje ACUSE DE RECIBO de DHCP al MTA. El mensaje ACUSE DE RECIBO de DHCP DEBE incluir todas las opciones y subopciones que se han enviado en MTA2 (OFERTA de DHCP). Si los valores de opción y subopción de este mensaje ACUSE DE RECIBO de DHCP difieren de la anterior OFERTA DHCP (MTA2), DEBEN primar los valores de opción y subopción del mensaje ACUSE DE RECIBO de DHCP (de acuerdo con RFC 2131).<br>Si el ACUSE DE RECIBO de DHCP no es válido de acuerdo con los criterios establecidos en MTA2, el MTA DEBE considerar que hay fallo en esta etapa.<br>NOTA – El flujo de aprovisionamiento bifurca en una de las direcciones siguientes:<br>Si el mensaje ACUSE de RECIBO de DHCP de MTA4 indica un flujo básico, el MTA DEBE proceder a la fase B-MTA-22 que se describe en 7.3.<br>Si el mensaje ACUSE DE RECIBO de DHCP de MTA4 indica un flujo híbrido, el MTA DEBE proceder a la etapa H-MTA-15 que se describe en 7.4.<br>En cualquier otro caso, se considera que se indica el flujo seguro y el MTA DEBE proceder a la fase MTA5 siguiente. | MTA4 DEBE ocurrir una vez terminado MTA3 | En caso de fallo de acuerdo con el protocolo DHCP, vuélvase a MTA1 |
| MTA5 | Petición de servidor DNS<br>El MTA solicita el nombre de anfitrión KDC MSO para el sector Kerberos. | MTA5 DEBE ocurrir una vez terminado MTA4 | MTA1 |
| MTA6 | Respuesta de servidor DNS<br>Se devuelve el nombre de anfitrión KDC MSO asociado con el SECTOR de configuración. | MTA6 DEBE ocurrir una vez terminado MTA5 | MTA1 |
| MTA7 | Petición DNS<br>El MTA pide la dirección IP del KDC MSO. | MTA7 DEBE ocurrir una vez terminado MTA6 | MTA1 |
| MTA8 | Respuesta DNS<br>El servidor DNS devuelve la dirección IP del KDC MSO | MTA8 DEBE ocurrir una vez terminado MTA7 | MTA1 |
| MTA9 | Petición AS<br>El mensaje petición AS se envía al KDC MSO para solicitar un tique Kerberos. | MTA9 DEBE ocurrir, de ser el caso, una vez terminado MTA8 | MTA1<br>Las condiciones de fallo son las definidas por la Especificación de seguridad J.170 |

## Cuadro 1/J.167 – Descripción de los flujos de inicialización de la activación de potencia del MTA incorporado

| Flujo | Descripción de los flujos de inicialización de la activación de potencia del MTA incorporado | Secuenciación del flujo normal | DEBE avanzar hasta aquí si falla este paso |
|---|---|---|---|
| MTA10 | Respuesta AS<br>Se recibe el mensaje de respuesta AS del KDC MSO con el tique Kerberos.<br>NOTA 1 – El KDC debe establecer la correspondencia entre la dirección MAC del MTA y el FQDN antes de enviar la respuesta AS.<br>NOTA 2 – Los flujos MTA11-MTA12 son opcionales en algunos casos. Véase la especificación de seguridad (J.170).<br>NOTA 3 – La entidad SNMPv3 (FQDN) DEBE corresponder con cualquier dirección IP durante los flujos MTA5 a MTA12.<br>NOTA 4 – Si se proporciona en el campo información adicional de la respuesta DNS-SRV (MTA6), una dirección IP, el MTA PUEDE utilizar la misma dirección y saltarse los flujos MTA7 y MTA8.<br>NOTA 5 – Si el MTA tiene un tique de servidor de aplicación de aprovisionamiento válido guardado en NVRAM, DEBE saltarse los flujos MTA5 a MTA12 en sucesivas puestas a cero del MTA (flujos MTA1 a MTA25). | MTA10 DEBE ocurrir, una vez terminado MTA9 | MTA1 |
| MTA11 | Petición TGS<br>Si el MTA obtiene el TGT en MTA10, se envía el mensaje de petición TGS al KDC MSO. | MTA11 DEBE ocurrir, de ser el caso, una vez terminado MTA10 | MTA1 |
| MTA12 | Respuesta TGS<br>Se recibe el mensaje de respuesta TGS del KDC MSO. | MTA12 DEBE ocurrir, una vez terminado MTA11 | MTA1 |
| MTA13 | Petición AP<br>Se envía el mensaje de petición AP al servidor de configuración para solicitar la información de claves necesaria para SNMPv3. | MTA13 DEBE ocurrir una vez terminados MTA12 o MTA10 | MTA1<br>Las condiciones de fallos se definen en la Especificación de seguridad de J.170 |
| MTA14 | Respuesta AP<br>Se recibe del servidor de configuración el mensaje de respuesta AP que contiene la información de claves para SNMPv3.<br>NOTA – Deben fijarse las claves SNMPv3 antes de la siguiente etapa y utilizando la información de la respuesta AP. | MT14 DEBE ocurrir una vez terminado MTA13 | MTA1 |

## Cuadro 1/J.167 – Descripción de los flujos de inicialización de la activación de potencia del MTA incorporado

| Flujo | Descripción de los flujos de inicialización de la activación de potencia del MTA incorporado | Secuenciación del flujo normal | DEBE avanzar hasta aquí si falla este paso |
|---|---|---|---|
| MTA15 | INFORME enrolamiento de SNMP<br>El MTA DEBE enviar un mensaje INFORME enrolamiento SNMPv3 la PROV_SNMP_ENTITY (especificada en la subopción 3 de la opción 122 DHCP). El mensaje INFORME de SNMP DEBE contener un objeto "PktcMtaDevProvisioningEnrollment" como se define en la Rec. UIT-T J.166.<br>La PROV_SNMP_ENTITY notifica a la aplicación de aprovisionamiento que el MTA ha entrado en el dominio de gestión.<br>NOTA – Llegado a este punto el servidor de aprovisionamiento puede poner a cero el MTA en los flujos. El MTA forma parte del dominio de seguridad y DEBE responder a las peticiones de gestión, de las que el mensaje INFORME de SNMP de MTA15 es el indicador, véase 5.4.1.2. | MTA15 DEBE ocurrir después de terminado MTA14 | En caso de fallo de acuerdo con el protocolo SNMP, vuélvase a MTA1. El servidor de SNMP DEBE enviar una respuesta al mensaje INFORME de SNMP. |
| MTA16 | Petición OBTENER de SNMPv3 (opcional). Si PROV_APP necesita capacidades del dispositivo MTA adicionales, las pedirá al MTA vía peticiones obtener SNMPv3. Esto se realiza cuando el PROV_APP hace que la PROV_SNMP_ENTITY envíe iterativamente una "petición obtener". La PROV_SNMP_ENTITY envía al MTA una o más peticiones OBTENER de SNMPv3 para obtener toda la información de capacidades del MTA necesarias. La aplicación de aprovisionamiento puede utilizar una petición OBTENER en bloque para percibir diversos elementos de información en un único mensaje. | MTA16 es opcional y puede ocurrir una vez terminado MTA15 | No aplicable |
| MTA17 | Respuesta OBTENER SNMPv3<br>Iterativo:<br>El MTA envía a PROV_SNMP_ENTITY una respuesta para cada petición OBTENER. Una vez terminado el procedimiento obtener u obtener todo, la PROV_SNMP_ENTITY envía los datos solicitados a PROV_APP. | MTA17 DEBE ocurrir una vez terminado MTA16, si se realiza MTA16 | No aplicable |
| MTA18 | Este protocolo no está definido por IPCablecom. El PROV_APP PUEDE utilizar la información de MTA16 y MTA17 para determinar los contenidos del fichero de datos de configuración MTA. Los mecanismos de envío, almacenamiento y, posiblemente, creación del fichero de definición de la configuración se esbozan en MTA19. | MTA18 DEBERÍA ocurrir una vez terminado MTA15, a menos que se realice MTA16, en cuyo caso, DEBERÍA realizarse una vez terminado MTA17 | No aplicable |

## Cuadro 1/J.167 – Descripción de los flujos de inicialización de la activación de potencia del MTA incorporado

| Flujo | Descripción de los flujos de inicialización de la activación de potencia del MTA incorporado | Secuenciación del flujo normal | DEBE avanzar hasta aquí si falla este paso |
|---|---|---|---|
| MTA19 | FIJAR SNMPv3<br>El PROV_APP PUEDE crear en este momento un fichero de definición de la configuración o enviar uno predefinido. DEBE aplicarse un valor generado a todos los contenidos del fichero de definición de la configuración. El fichero de configuración PUEDE estar criptado. El valor generado y la clave de criptación (de estar criptado el fichero de definición de la configuración) DEBE enviarse al MTA. El PROV_APP DEBE almacenar el fichero de configuración en el servidor TFTP adecuado.<br>El PROV_APP indica a la PROV_SNMP_ENTITY que envíe el mensaje FIJAR de SNMP al MTA con las siguientes variables (definidas en la Rec. UIT-T J.166)<br>pktcMtaDevConfigFilepktcMtaDevProvConfigHash<br>y<br>pktcMtaDevProvConfigKey (esto NO DEBE incluirse y el fichero de configuración MTA no está criptado)<br>NOTA 1 – En caso de descarga de fichero utilizando el método de acceso HTTP, el nombre del fichero DEBE tener una codificación URL en un formato URL compatible con RFC 2616, a excepción de lo que se indica en la nota 3.<br>NOTA 2 – En caso de descarga de fichero utilizando un método de acceso TFTP, el nombre de fichero DEBE estar en codificación URL con un formato URL compatible con RFC 3617, a excepción de lo que se indica en la nota 3.<br>NOTA 3 – El MTA DEBE aceptar las direcciones IPv4 incorporadas en el formato de codificación URL con o sin corchetes. | MTA19 DEBE ocurrir una vez terminado el MTA18 | En caso de fallo de acuerdo con el protocolo de SNMP vuélvase a MTA1. |
| MTA20 | Petición DNS<br>Si el método de acceso con codificación URL contiene un FQDN en vez de una dirección IPv4, el MTA DEBE utilizar el servidor DNS de la red de proveedor de servicio para transformar el FQDN en una dirección IPv4 del servidor TFTP o HTTP. | MTA20 DEBE ocurrir una vez terminado MTA19, si se utiliza FQDN | En caso de fallo de acuerdo con el protocolo DNS, vuélvase a MTA1. |
| MTA21 | Respuesta DNS<br>Respuesta DNS: El servidor DNS devuelve a la dirección IP que solicita la petición DNS de MTA20. | MTA21 DEBE ocurrir una vez terminado MTA20, si se utiliza FQDN | En caso de fallo de acuerdo con el protocolo DNS, vuélvase a MTA1. |
| MTA22 | Petición de fichero de definición de la configuración TFTP/HTTP<br>El MTA DEBE realizar en un intercambio de protocolo TFTP o HTTP, como se especifica en la fase S-MTA-19, para descargar su propio fichero de definición de la configuración. Pueden encontrarse los detalles específicos de este protocolo en la RFC 3415 y RFC 3412. | MTA22 DEBE ocurrir después de MTA-19, si no se requiere una resolución DNS; después de MTA-21, si se requiere una resolución DNS | En caso de fallo de acuerdo con los protocolos TFTP o HTTP, vuélvase a MTA1. |

## Cuadro 1/J.167 – Descripción de los flujos de inicialización de la activación de potencia del MTA incorporado

| Flujo | Descripción de los flujos de inicialización de la activación de potencia del MTA incorporado | Secuenciación del flujo normal | DEBE avanzar hasta aquí si falla este paso |
|---|---|---|---|
| MTA23 | Peticiones de fichero de definición de la configuración TFTP/HTTP<br>El servidor TFTP/HTTP DEBE enviar el fichero de definición de la configuración solicitado al MTA. Pueden encontrarse detalles específicos de cada protocolo en RFC 3415 y RFC 3412. El MTA calcula el valor generado del fichero de configuración descargado y lo compara con el valor recibido en MTA19. Si los valores generados no concuerdan, el MTA DEBE declarar el fallo de esta etapa. Si está criptado, el fichero de definición de la configuración DEBE descriptarse.<br>Véase en 9.1 el contenido de fichero de configuración MTA. | MTA23 DEBE ocurrir una vez terminado MTA22 | Si en la descarga del fichero de definición de la configuración falla de acuerdo con los protocolos TFTP o HTTP, vuélvase a MTA1. En cualquier otro caso, procédase a MTA24 o MTA25, y envíese la respuesta de fallo si el propio fichero de definición de la configuración MTA es erróneo. |
| MTA24 | Notificación SYSLOG<br>Si un servidor SYSLOG está configurado y activado como parte del proceso de aprovisionamiento (véanse la fase MTA2 para las opciones DHCP y las Recs. UIT-T J.172, UIT-T J.166 para la configuración utilizando la MIB MEM), el MTA DEBE enviar al SYSLOG del proveedor de servicios vocales un evento "aprovisionamiento completo" indicando el estado del proceso de aprovisionamiento. Esta notificación incluirá el resultado paso-fallo del procedimiento de aprovisionamiento. El formato general de esta notificación es el definido en 5.4.3. | MTA24 DEBE ocurrir una vez terminado MTA23, si se configura SYSLOG | El MTA PUEDE reintentar esta fase antes de proceder a MTA25. |
| MTA25 | INFORME de SNMP<br>El MTA DEBE enviar a la PROV_SNMP_ENTITY (especificada en la subopción 3 de la opción 122 de DHCP) un INFORME de SNMP que contenga una notificación de "aprovisionamiento completo". Se acusa recibo de la recepción del INFORME mediante un mensaje de respuesta definido en RFC 3414.<br>El mensaje INFORME de SNMP DEBE contener un objeto "PktcMtaDevProvisioningStatus", como se define en la Rec. UIT-T J.166.<br>NOTA 1 – En esta fase, los datos de aprovisionamiento de dispositivo MTA bastan para proporcionar los servicios mínimos, según determina el proveedor de servicios (por ejemplo, 611).<br>NOTA 2 – Dependiendo del aprovisionamiento TLV-38, es posible que se envíen múltiples mensajes INFORME de SNMP a las estaciones de gestión SNMP configuradas. | MTA25 DEBE ocurrir después de MTA24, si se utiliza SYSLOG, en cualquier otro caso, DEBE ocurrir una vez terminado MTA23 | El MTA PUEDE generar una notificación de evento de fallo de aprovisionamiento al servidor de gestión de fallo del proveedor de servicios.<br>Se detiene el proceso de aprovisionamiento, y se requiere una interacción manual. El servidor SNMP DEBE enviar una respuesta al mensaje INFORME SNMP. |

## 7.3 Flujos de inicialización de la activación de potencia del MTA incorporado (flujo básico)

El flujo de aprovisionamiento del MTA básico es muy similar al flujo de configuración de CM DOCSIS.

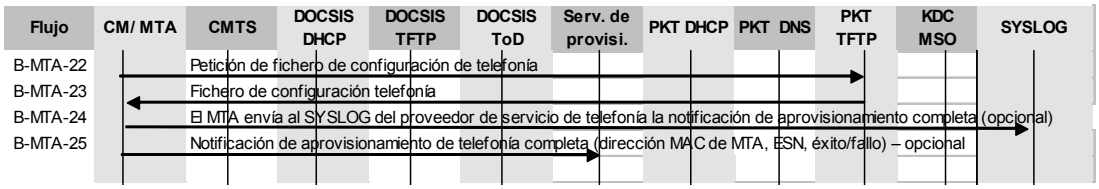


**Figura 7/J.167 – Flujo básico de inicialización de la activación de potencia del MTA incorporado**

**Cuadro 2/J.167 – Flujo básico de inicialización de la activación de potencia del MTA incorporado**

| Flujo | Descripción de los flujos de inicialización de la activación de potencia del MTA incorporado | Secuenciación del flujo normal | DEBE avanzar hasta aquí si falla este paso |
|---|---|---|---|
| | NOTA – El FQDN proporcionado en el mensaje ACUSE DE RECIBO de DHCP en la subopción 3 de la opción 122 de DHCP (Dirección de Entidad de configuración) DEBE corresponder a una dirección IP antes del paso B-MTA-22. | | |
| B-MTA-22 | Petición de fichero de definición de la configuración TFTP<br>El MTA DEBE realizar un intercambio de protocolo TFTP para descargar su fichero de definición de la configuración. Los campos 'siaddr' y 'file' del mensaje ACUSE DE RECIBO de DHCP se utilizan para ubicar el fichero de configuración. Pueden encontrarse los detalles específicos del protocolo TFTP en RFC 3415. | B-MTA-22 DEBE ocurrir después de MTA-4. | En caso de fallo de acuerdo con el protocolo TFTP, vuélvase a MTA1. |
| B-MTA-23 | Respuesta de fichero de definición de la configuración TFTP<br>El fichero TFTP DEBE enviar el fichero de definición de la configuración solicitado al MTA. Pueden encontrarse los detalles específicos del protocolo TFTP en RFC 3415.<br>El fichero de definición de la configuración descargado DEBE comprender el objeto 'pktcMtaDevConfigHash' de MIB. El MTA DEBE calcular el valor generado del fichero de configuración descargado, de conformidad con 9.1, y compara este valor con el del objeto 'pktcMtaDevConfigHash'. Si estos valores no concuerdan DEBE considerarse que ha fallado este paso.<br>Véase en 9.1 el contenido del fichero de configuración MTA. | B-MTA-23 DEBE ocurrir después de B-MTA-22 | Si la descarga del fichero de configuración falla de acuerdo con los protocolos de TFTP, vuélvase a MTA1.<br>En caso contrario, procédase a B-MTA-24 y envíese la respuesta de fallo si el fichero de configuración de MTA mismo es erróneo. |

**Cuadro 2/J.167 – Flujo básico de inicialización de la activación de potencia del MTA incorporado**

| Flujo | Descripción de los flujos de inicialización de la activación de potencia del MTA incorporado | Secuenciación del flujo normal | DEBE avanzar hasta aquí si falla este paso |
|---|---|---|---|
| B-MTA-24 | Notificación SYSLOG.<br>Si un servidor SYSLOG está configurado y activado como parte del proceso de aprovisionamiento (véanse en el paso MTA2 las opciones de DHCP y las Recs. UIT-T J.172, J.166 para la configuración utilizando MIB-MEM), el MTA DEBE enviar al SYSLOG del proveedor de servicio vocal un evento "aprovisionamiento completo" indicando el estado del proceso de aprovisionamiento. El formato general de esta notificación es el que se define en 5.4.3. | B-MTA-24 DEBE ocurrir una vez terminado B-MTA-23, si SYSLOG está configurado | El MTA PUEDE reintentar este paso antes de proceder a B-MTA-25 |
| B-MTA-25 | INFORME de estado de aprovisionamiento SNMPv2C (opcional).<br>Si recibe la instrucción de la subopción 6 de la opción 122 de DHCP, el MTA DEBE enviar a la PROV_SNMP_ENTITY (especificada en la subopción 3 de la opción 122 de DHCP) un mensaje INFORME de SNMP que contenga la notificación "configuración completa". Se acusa recibo del mensaje INFORME SNMP.<br>El mensaje INFORME de SNMP DEBE contener el objeto "PktcMtaDevProvisioningStatus", definido en la Rec. UIT-T J.166.<br>El nombre comunitario SNMPv2c utilizado en el mensaje INFORME de SNMP de estado DEBE tener un valor "público" (sin las comillas).<br>NOTA 1 – En esta fase los datos de aprovisionamiento del dispositivo MTA bastan para proporcionar servicios mínimos, según determine el proveedor de servicios (por ejemplo, 611).<br>NOTA 2 – Dependiendo de los pares de valores de configuración TLV-38, es posible que se envíen múltiples mensajes de INFORME de SNMP a las estaciones de gestión SNMP configuradas. | B-MTA-25 es opcional y PUEDE ocurrir después de B-MTA-24, si se utiliza SYSLOG. En caso contrario PUEDE ocurrir una vez terminado B-MTA-23 | Se detiene el proceso de aprovisionamiento y se requiere una interacción manual. El servidor SNMP DEBE enviar una respuesta al INFORME de SNMP |

## 7.4 Flujo de inicialización de la activación de potencia del MTA incorporado (flujo híbrido)

El flujo de aprovisionamiento híbrido (flujo híbrido) consiste básicamente en el flujo seguro sin los intercambios Kerberos y sustituyendo SNMPv2c por SNMPv3. El nombre comunitario de SNMPv2c, utilizado en los mensajes INFORME de SNMP que envía el MTA en los pasos H-MTA15 y H-MTA25 DEBE tener un valor "público" (sin las comillas). Véanse la figura 8 y el cuadro 3.

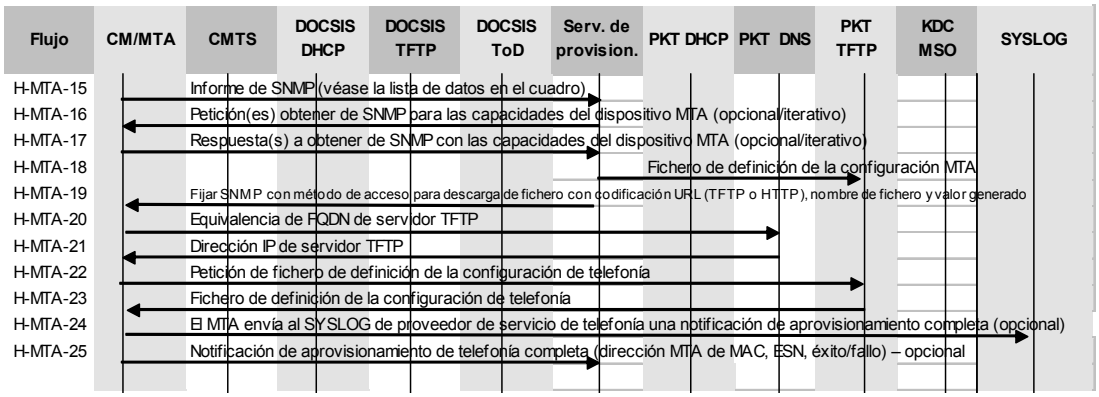


**Figura 8/J.167 – Flujo de inicialización de la activación de potencia del MTA incorporado**

**Cuadro 3/J.167 – Flujo de inicialización de la activación de potencia del MTA incorporado**

| Flujo | Descripción de los flujos de inicialización de activación de potencia del MTA incorporado | Secuenciación de flujo normal | DEBE avanzar hasta aquí si falla este paso |
|---|---|---|---|
| | NOTA – El FQDN proporcionado en el mensaje ACUSE DE RECIBO de DHCP en la subopción 3 de la opción 122 de DHCP (dirección de entidad de aprovisionamiento) DEBE corresponderse con una dirección IP antes del paso H-MTA-15. | | |
| H-MTA-15 | INFORME de enrolamiento de SNMPv2c<br>El MTA DEBE enviar un mensaje INFORME de enrolamiento de SNMPv2c a la PROV_SNMP_ENTITY (especificada en la subopción 3 de la opción 122 de DHCP). El mensaje INFORME de SNMP DEBE contener un objeto 'PktcMtaDevProvisioningEnrollment', como se define en la Rec. UIT-T J.166.<br>La PROV_SNMP_ENTITY notifica al PROV_APP que el MTA ha entrado en el dominio de gestión. | H-MTA-15 DEBE ocurrir una vez terminado MTA4 | En caso de fallo de acuerdo con el protocolo SNMP, vuélvase a MTA1. El servidor SNMP DEBE enviar una respuesta al mensaje INFORME de SNMP |
| H-MTA-16 | Petición OBTENER de SNMPv2c (opcional)<br>La aplicación de aprovisionamiento puede solicitar capacidades del dispositivo MTA adicionales al MTA mediante peticiones OBTENER de SNMPv2c. Esto se consigue cuando la aplicación de aprovisionamiento envía a la PROV_SNMP_ENTITY una petición OBTENER de SNMP.<br>Iterativo:<br>La PROV_SNMP_ENTITY envía al MTA una o más peticiones OBTENER de SNMPv2c para obtener toda la información de capacidades de MTA que necesita. La aplicación de aprovisionamiento puede utilizar una petición OBTENER en bloque para recibir diversas informaciones en un único mensaje. | H-MTA-16 es opcional y puede ocurrir una vez terminado H-MTA-15 | No aplicable |

**Cuadro 3/J.167 – Flujo de inicialización de la activación de potencia del MTA incorporado**

| Flujo | Descripción de los flujos de inicialización de activación de potencia del MTA incorporado | Secuenciación de flujo normal | DEBE avanzar hasta aquí si falla este paso |
|---|---|---|---|
| H-MTA-17 | Respuesta OBTENER de SNMPv2c (opcional)<br>Iterativo:<br>El MTA envía a PROV_SNMP_ENTITY una respuesta obtener para cada petición obtener. Una vez terminados todos los procedimientos obtener u obtener en bloque, la PROV_SNMP_ENTITY envía los datos solicitados a la aplicación de aprovisionamiento. | H-MTA-17 DEBE ocurrir una vez terminado H-MTA-16, de realizarse dicha etapa | No aplicable |
| H-MTA-18 | Este protocolo no está definido por IPCablecom<br>La aplicación de aprovisionamiento PUEDE utilizar la información de H-MTA-15, -16 y -17 para determinar el contenido del fichero de datos de configuración MTA. En H-MTA-19 se esbozan los mecanismos para enviar, almacenar y, posiblemente, crear el fichero de definición de la configuración. | H-MTA-18 DEBERÍA ocurrir una vez terminado H-MTA-15, a menos que se ejecute H_MTA-16, en cuyo caso DEBERÍA ocurrir una vez terminado H-MTA-17 | No aplicable |
| H-MTA-19 | Fijar fichero de definición de la configuración de SNMPv2c<br>La aplicación de aprovisionamiento PUEDE crear el fichero de definición de la configuración en este momento o enviar uno predefinido. La aplicación de aprovisionamiento DEBE calcular el valor generado SHA-1 del contenido del fichero de definición de la configuración. La aplicación de configuración DEBE almacenar el fichero de definición de la configuración en el fichero del servidor TFTP adecuado.<br>A continuación, la aplicación de aprovisionamiento ordena a PROV_SNMP_ENTITY que envíe un mensaje fijar SNMPv2c al MTA con las siguientes vinculaciones variables (definidas en la Rec. UIT-T J.166):<br>pktcMtaDevConfigFile<br>pktcMtaDevProvConfigHash<br>A diferencia de lo que ocurre en el flujo, el objeto MIB pktcMtaDevProvConfigKey NO DEBE incluirse. Si se incluye el objeto MIB pktcMtaDevProvConfigKey, el MTA DEBE devolver un error 'valor incompatible' (puede encontrarse más información sobre las respuestas a FIJAR de SNMP en RFC 3413). | H-MTA-19 DEBE ocurrir una vez terminado H-MTA-18 | En caso de fallo de acuerdo con el protocolo SNMP, vuélvase a MTA1 |

**Cuadro 3/J.167 – Flujo de inicialización de la activación de potencia del MTA incorporado**

| Flujo | Descripción de los flujos de inicialización de activación de potencia del MTA incorporado | Secuenciación de flujo normal | DEBE avanzar hasta aquí si falla este paso |
|---|---|---|---|
| | NOTA 1 – En caso de que para la descarga de ficheros se utilice el método de acceso HTTP, el nombre de fichero DEBE tener una codificación URL y un formato URL compatible con RFC 2616, a excepción de lo que se indica en la nota 3.<br>NOTA 2 – En caso de que la descarga de fichero se realice utilizando el método de acceso TFTP, el nombre de fichero DEBE tener una codificación URL y un formato URL compatible con RFC 3617, a excepción de lo que se indica en la nota 3.<br>NOTA 3 – El MTA DEBE aceptar las direcciones IPv4 incorporadas en formato de codificación URL con o sin corchetes. | | |
| H-MTA-20 | Petición de DNS (opcional)<br>Si el método de acceso con codificación URL contiene un FQDN en vez de una dirección IPv4, el MTA DEBE utilizar el servidor DNS de la red del proveedor de servicio para transformar el FQDN en una dirección IPv4 del servidor TFTP o del servidor HTTP. | H-MTA-20 DEBE ocurrir una vez terminado H-MTA-19, si se utiliza un FQDN | En caso de fallo de acuerdo con el protocolo DNS, vuélvase a MTA1 |
| H-MTA-21 | Respuesta de DNS (opcional)<br>Respuesta de DNS: el servidor DNS devuelve una dirección IP a la petición de DNS de H-MTA-20. | H-MTA-21 DEBE ocurrir una vez terminado H-MTA-20, si se utiliza un FQDN | En caso de fallo de acuerdo con el protocolo DNS, vuélvase a MTA1 |
| H-MTA-22 | Petición de fichero de definición de la configuración TFTP/HTTP<br>El MTA DEBE realizar un intercambio de protocolo TFTP o HTTP, según se especifique en H-MTA-19, para descargar su fichero de configuración. Pueden encontrarse los detalles específicos de cada uno de los protocolos en las RFC 3415 y RFC 3412. | H-MTA-22 DEBE ocurrir después de H-MTA-19, a menos que se especifique el FQDN, en cuyo caso DEBE ocurrir después de H-MTA-21 | En caso de fallo según los protocolos TFTP o HTTP, vuélvase a MTA1 |

**Cuadro 3/J.167 – Flujo de inicialización de la activación de potencia del MTA incorporado**

| Flujo | Descripción de los flujos de inicialización de activación de potencia del MTA incorporado | Secuenciación de flujo normal | DEBE avanzar hasta aquí si falla este paso |
|---|---|---|---|
| H-MTA-23 | Respuesta de fichero de definición de la configuración TFTP/HTTP<br>El servidor TFTP/HTTP DEBE enviar el fichero de definición de la configuración solicitado al MTA. Pueden encontrarse detalles de cada uno de los protocolos en las RFC 3415 y RFC 3412.<br>El MTA calcula el valor generado del fichero de definición de la configuración telecargado y lo compara al valor recibido en H-MTA-19. Si los valores no concuerdan, DEBE considerarse que este paso falla.<br>Véase en 9.1 el contenido del fichero de configuración MTA. | H-MTA-23 DEBE ocurrir después de H-MTA-22 | Si la descarga del fichero de configuración falla de acuerdo con los protocolos TFTP o HTTP, vuélvase a MTA1.<br>En cualquier otro caso, procédase a MTA24 o MTA25 y envíese la respuesta de fallo, en caso de que el fichero de definición de la configuración del MTA mismo sea erróneo. |
| H-MTA-24 | Notificación SYSLOG<br>Si un servidor SYSLOG está configurado y activado como parte del proceso de aprovisionamiento (véanse en el paso MTA2 las opciones de DHCP y las Recs. UIT-T J.172, UIT-T J.166 para la configuración utilizando la MIB-MEM), el MTA DEBE enviar al SYSLOG del proveedor de servicios vocales un evento "aprovisionamiento completo" indicando el estado del proceso de configuración. Esta notificación incluirá el resultado de paso-fallo del proceso de aprovisionamiento. El formato general de esta notificación es el definido en 5.4.3. | H-MTA-24 DEBE ocurrir una vez terminado H-MTA-23, si SYSLOG está configurado | El MTA PUEDE reintentar este paso antes de proceder a H-MTA-25 |

**Cuadro 3/J.167 – Flujo de inicialización de la activación de potencia del MTA incorporado**

| Flujo | Descripción de los flujos de inicialización de activación de potencia del MTA incorporado | Secuenciación de flujo normal | DEBE avanzar hasta aquí si falla este paso |
|---|---|---|---|
| H-MTA-25 | Informe de estado de aprovisionamiento de SNMPv2c (opcional)<br>Si así lo indica la instrucción de la subopción 6 de la opción 122 de DHCP, el MTA DEBE enviar a PROV_SNMP_ENTITY (especificada en la subopción 3 de la opción 122 de DHCP) un mensaje INFORME de estado de aprovisionamiento de SNMPv2c con una notificación "aprovisionamiento completo". Se acusa recibo del informe.<br>El informe DEBE contener un objeto 'PktcMtaDevProvisioningStatus', como se define en la Rec. UIT-T J.166.<br>NOTA 1 – En esta etapa, los datos de aprovisionamiento del dispositivo MTA bastan para proporcionar servicios mínimos, según determine el proveedor de servicios (por ejemplo, 611).<br>NOTA 2 – Dependiendo de la configuración TLV38, es posible que se envíen múltiples INFORMES de SNMPv2C a las estaciones de gestión de SNMP. | H-MTA-25 es opcional. PUEDE ocurrir después de H-MTA-24, si se utiliza SYSLOG, o una vez terminado H-MTA-23 | Se detiene el proceso de configuración y se requiere interacción manual. El servidor SNMP DEBE enviar una respuesta a INFORME de SNMP |

## 7.5 Notificaciones de aprovisionamiento completa del punto extremo

Una vez aprovisionado satisfactoriamente el MTA, independientemente del flujo de aprovisionamiento que se haya seleccionado, el MTA creará las asociaciones de seguridad necesarias con los sectores configurados del CMS correspondientes (KDC). El software de señalización NCS del MTA iniciará el establecimiento de la asociación de seguridad IPSec con los sectores CMS configurados. Se desencadenan notificaciones de eventos si no pueden establecerse asociaciones de seguridad (de acuerdo con la Rec. UIT-T J.170).

Una vez completado el flujo básico, híbrido o seguro seleccionado, y creadas las asociaciones de seguridad requeridas, el software de señalización NCS del MTA determina si puede establecerse un trayecto de señalización con un mensaje de red RSIP y su ACUSE DE RECIBO asociado. A partir de un enlace inactivo, el MTA enviará una trampa de enlace activo SNMP cuando se haya recibido el debido acuse de recibo al RSIP, lo que indica que el punto extremo está configurado. Si se utiliza el mismo CMS para múltiples puntos extremos, se enviará el mensaje de enlace activo de SNMP a cada uno de ellos. Si no todos los puntos extremos utilizan el mismo CMS, ha de repetirse el mismo proceso para cada punto extremo que utilice un CMS configurado distinto.

## 7.6 Aprovisionamiento incremental posterior a la inicialización

En esta cláusula se describen los flujos que permiten a la aplicación de aprovisionamiento efectuar el aprovisionamiento incremental de puntos extremos de comunicaciones vocales individuales una vez que el MTA ha sido inicializado. El aprovisionamiento incremental posterior a la inicialización PUEDE implicar la comunicación con un representante del servicio del cliente (CSR, *customer service representative*).

### 7.6.1 Sincronización de atributos de aprovisionamiento con fichero de definición de la configuración

El aprovisionamiento incremental incluye la adición, la supresión y la modificación de servicios de abonado en uno o más puntos extremos MTA incorporado. Los servicios en un punto extremo MTA DEBEN ser modificados utilizando SMNP por conducto de la base de información de gestión (MIB) del adaptador de terminal de medios (MTA) (Rec. UIT-T J.166). Las aplicaciones de fondo de oficina DEBERÍAN soportar un mecanismo de aprovisionamiento "mediante flujos" que sincronice toda la información de aprovisionamiento del dispositivo en el MTA incorporado con las bases de datos y los servidores de fondo de oficina apropiados. La sincronización se necesita en caso de que la información de aprovisionamiento tenga que ser recuperada para reinicializar el dispositivo. Aunque los detalles de la sincronización de fondo de oficina quedan fuera del alcance de la presente Recomendación, se prevé que, como mínimo, se actualizará la información siguiente: los registros de clientes y el fichero de definición de la configuración de MTA en el servidor TFTP o el servidor HTTP.

### 7.6.2 Habilitación/adición de servicios telefónicos en un punto extremo MTA

Pueden añadirse y/o habilitarse en un punto extremo MTA servicios de telefonía. Pueden añadirse servicios telefónicos a puntos extremos MTA que no hayan sido configurados anteriormente.

Siempre que se añada/habilite un punto extremo de este tipo:

- El MTA DEBE haberse configurado con los datos de configuración de 'nivel de dispositivo' gracias al fichero de definición de la configuración (como se indica en 9.1.1).
- La estación de gestión SNMP autorizada DEBE proporcionar todos los atributos de configuración necesarios, como se indica en 9.1.3, 9.1.4 y 9.1.5, utilizando los mensajes FIJAR de SNMP para actualizar los atributos de aprovisionamiento del dispositivo con el objetivo de habilitar el puerto telefónico específico.

Pueden habilitarse servicios de telefonía en puntos extremos MTA con servicios aprovisionados, pero inhabilitados (véanse más detalles en 7.6.3 y 9.1.1). Para habilitar servicios telefónicos previamente inhabilitados en el punto extremo MTA, una estación de gestión SNMP autorizada DEBE utilizar los mensajes FIJAR de SNMP adecuados para lograr los dos siguientes objetivos:

- Garantizar que el objeto MIB de estado de fila (pktcNcsEndPntConfigStatus) para la fila correspondiente al punto extremo se pone al valor "active (1)" (modifíquese convenientemente si se pone otro valor).
- Garantizar que el valor de "ifAdminStatus" correspondiente al punto extremo que se habilita tiene el valor "up(2)" (modifíquese convenientemente si se pone cualquier otro valor).

Cuando el punto extremo está configurado o habilitado, el MTA DEBE seguir los siguientes pasos (no necesariamente en este orden):

- Seguir los procedimientos descritos en 7.1.1.2.5 de la Especificación de seguridad (J.170).
- Modificar el objeto MIB "ifOperStatus" de conformidad con 7.7.

Si el objeto MIB "pktcMtaDevEnabled" está puesto a "true (1)", el MTA DEBE seguir los pasos antedichos para todos los puntos extremos configurados.

Cabe señalar que, dada la naturaleza del objeto MIB que controla la ausencia o presencia de asociaciones de seguridad IPSec con un servidor de gestión de llamadas, el aprovisionamiento del punto extremo no puede utilizarse para modificar el estado IPSec (puede encontrarse más información al respecto en el anexo B/J.166). Por consiguiente, la habilitación de nuevos servicios con un servidor de gestión de llamadas cuyo estado no se ha indicado anteriormente (mediante el fichero de definición de la configuración) hará que se habilite el IPSec en el momento de asignación al punto extremo.

Como ejemplo de habilitación de servicios de telefonía en un punto extremo, considérese el caso en que un abonado ha solicitado un servicio en un punto extremo no aprovisionado anteriormente.

NOTA – En el ejemplo se supone que se ha completado el proceso de creación de la cuenta del proveedor de servicio, y se muestran sólo los componentes que son fundamentales para los flujos. Se supone, por ejemplo, que es posible crear cuentas y bases de datos de facturación, y que éstas se hallan integradas en la serie de aplicaciones de fondo de oficina.

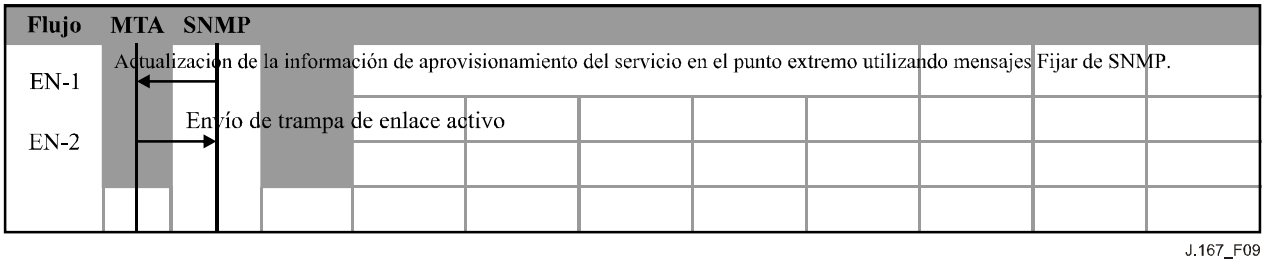


**Figura 9/J.167 – Habilitación de servicios en un punto extremo MTA**

**Cuadro 4/J.167 – Descripción de los flujos de habilitación de servicios en punto extremo MTA**

| Flujo | Descripción de los flujos de habilitación de servicios en un punto extremo MTA | Secuenciación de flujo normal |
|---|---|---|
| EN-1 | La estación de gestión SNMP autorizada realiza las operaciones FIJAR de SNMP necesarias para añadir servicios en el punto extremo MTA. | Si se desea la configuración del punto extremo, EN-1 DEBE ocurrir una vez completado satisfactoriamente el flujo de inicialización de potencia. |
| EN-2 | El MTA DEBE enviar una trampa de enlace activo a las estaciones de gestión SNMP configuradas. Puede encontrarse más información en 7.7 y la MIB-IF (RFC 2863). | EN-2 DEBE ocurrir después de EN-1. |

### 7.6.3 Eliminación/inhabilitación de servicios de telefonía en un punto extremo MTA

Pueden inhabilitarse (dejarse fuera de servicio) o eliminarse, si así se requiere, los servicios de telefonía habilitados y configurados utilizando el SNMP mediante la MIB MTA (Rec. UIT-T J.166) y la MIB de señalización (Rec. UIT-T J.166) para cada punto extremo.

Cuando se desea eliminar un servicio de telefonía en un punto extremo, la estación de gestión SNMP DEBE eliminar los correspondientes atributos de configuración descritos en 9.1.3, 9.1.4 y 9.1.5 utilizando las operaciones FIJAR de SNMP para el punto extremo correspondiente.

Para inhabilitar los servicios en un punto extremo MTA, la estación de gestión SNMP DEBE utilizar las operaciones FIJAR SNMP para lograr ajustarse a una o más de las siguientes condiciones:

- Para dicho punto extremo, modificar el objeto de estado de fila a un valor distinto de "active (1)" en "pktcNcsEndPntConfigTable".
- Modificar el valor de "ifAdminStatus" a "down (2)" para ese punto extremo en concreto.

Si el punto extremo se elimina o inhabilita cuando hay una llamada en curso, el MTA DEBE:

- Cerrar todas las sesiones de medios, de haberlas.
- Cortar la señalización NCS siguiendo los procedimientos de reinicio en curso de la especificación inicial IPCablecom (Rec. UIT-T J.162).

- Poner el objeto de MIB pktcNcsEndPntStatusError para dicho punto extremo al estado "disconnected (3)".

Si el objeto MIB "pktcMtaDevEnabled" está puesto a "false (2)", el MTA DEBE seguir el procedimiento antedicho para todos los puntos extremos configurados.

Como ejemplo de inhabilitación de servicios telefónicos en un punto extremo, puede considerase el caso en que un abonado ha solicitado la inhabilitación de los servicios telefónicos en un punto extremo configurado anteriormente.

NOTA 1 – Se supone que el proceso de actualización de la cuenta del proveedor de servicio se ha completado y se muestran únicamente las operaciones fundamentales para el funcionamiento del MTA.

NOTA 2 – En el ejemplo se supone que se ha completado el proceso de actualización de la cuenta del proveedor de servicio y se muestran sólo las aplicaciones que son fundamentales para el funcionamiento del MTA.

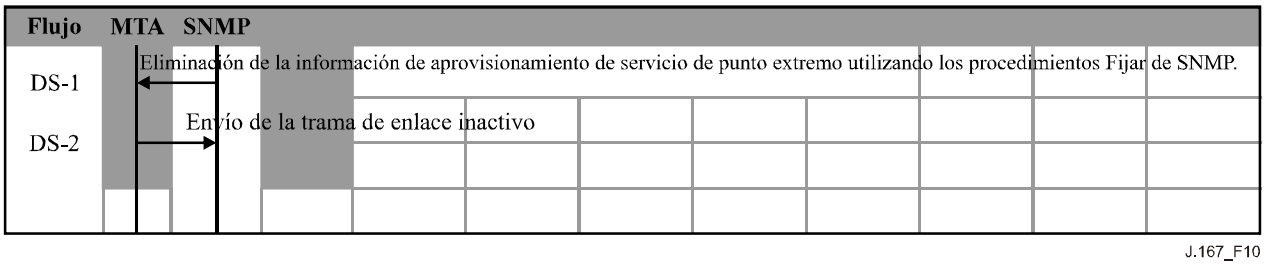


**Figura 10/J.167 – Inhabilitación de servicios en un punto extremo MTA**

**Cuadro 5/J.167 – Descripción de los flujos de inhabilitación de servicios en un punto extremo MTA**

| Flujo | Descripción de los flujos de inhabilitación de servicios en un punto extremo MTA | Secuenciación de flujo normal |
|---|---|---|
| DS-1 | La estación de gestión SNMP autorizada realiza las operaciones FIJAR de SNMP para inhabilitar los servicios en el punto extremo MTA. | DS-1 DEBE ocurrir una vez que el punto extremo se ha habilitado, ya sea inmediatamente después del aprovisionamiento inicial o después del aprovisionamiento incremental por puntos extremos. |
| DS-2 | El MTA DEBE enviar una trampa de enlace inactivo a las estaciones de gestión SNMP configuradas. Puede encontrarse más información al respecto en 7.7 y en MIB IF (RFC 2863). | DS-2 DEBE ocurrir después de DS-1. |

### 7.6.4 Modificación de servicios telefónicos en un punto extremo MTA

Pueden modificarse servicios telefónicos en un "punto extremo MTA" ya configurado utilizando SNMP a través de la MIB MTA (Rec. UIT-T J.166) y la MIB de señalización (Rec. UIT-T J.166) para cada punto extremo. Si esta modificación en un punto extremo cambia la asociación CMS (pktcNcsEndPntConfigCallAgentId) y/o el puerto (pktcNcsEndPntConfigCallAgentUdpPort), el punto extremo se considera fuera de servicio (de conformidad con 7.6.3), y a continuación se vuelve a poner el punto extremo en servicio (de acuerdo con 7.6.2).

El MTA DEBE asimismo seguir los procedimientos descritos en 7.1.1.2.5 de la Especificación de seguridad (Rec. UIT-T J.170).

Cabe señalar que:

- La modificación de las características del servicio de llamada requieren modificaciones en el CMS y no en el MTA.
- La modificación de los parámetros nivel de servicio relacionados con el componente eCM del eMTA puede requerir un rearranque del MTA incorporado.

### 7.7 Reflejo del estado de la interfaz del punto extremo en el ifTable

El estado operativo de cada "punto extremo MTA" se refleja en el objeto MIB "ifOperStatus" del MTA, que estará influido por las siguientes condiciones:

- El estado administrativo correspondiente al punto extremo, que se refleja en el cuadro "ifAdminStatus".
- El estado de servicio telefónico asignado al punto extremo correspondiente.
- La presencia o ausencia de asociaciones de seguridad IPSec en dicho punto extremo, siempre y cuando IPSec esté habilitado (es decir, el objeto MIB "pktcMtaDevCmsIpsecCtrl" está puesto al valor "true(1)" para dicho punto extremo).

Siempre que un MTA se reinicie (después de un rearranque o una puesta a cero), DEBE inmediatamente poner las entradas "ifAdminStatus" correspondientes a todos los puntos extremos físicos disponibles al valor 'up (1)'. No obstante, las entradas del fichero de definición de la configuración o la estación de gestión SNMP pueden modificar este estado. El MTA DEBE además reflejar las condiciones anteriores en el estado operativo de cada punto extremo como se indica a continuación.

Para cada entrada correspondiendo a un punto extremo en el MIB "ifTable" de la MIB, el MTA DEBE poner el objeto "ifOperStatus" a un valor de:

- "down(2)", si el punto extremo correspondiente está inhabilitado o eliminado, o poner el correspondiente "ifAdminStatus" a un valor de "down(2)";
- "up(1)", si el correspondiente "ifAdminStatus" tiene un valor de "up(1)", los servicios telefónicos se han añadido/habilitado para dicho punto extremo e IPSec está deshabilitado en el servidor de gestión de llamadas asignado;
- "up(1)" si el correspondiente "ifAdminStatus" tiene un valor de "up(1)", los servicios telefónicos se han añadido/habilitado para dicho punto extremo, IPSec está habilitado en el servidor de gestión de llamadas asignado y la asociación de seguridad IPSec se ha establecido;
- "dormant(3)", si el correspondiente "ifAdminStatus" tiene un valor de "up(1)", los servicios telefónicos se han añadido/habilitado para dicho punto extremo, IPSec está habilitado en el servidor de gestión de llamadas asignado, pero la asociación de seguridad IPSec no se ha establecido.

Además, el MTA no DEBE fijar "ifOperStatus" a un valor de "dormant(3)" para los puntos extremos en que IPSec esté inhabilitado. Pueden verse más detalles sobre la habilitación/deshabilitación de IPSec en la Rec. UIT-T J.166; la adición/habilitación de puntos extremos en 7.6.2; y la eliminación/inhabilitación de puntos extremos en 7.6.3.

El MTA DEBE poder habilitar o inhabilitar la 'trampa de enlace activo' y la 'trampa de enlace inactivo' utilizando el objeto MIB "ifLinkUpDownTrapEnable" (véase más detalles al respecto en la MIB IF).

## 7.8 Aprovisionamiento del trayecto de comunicación de señalización entre el MTA y el CMS

Todas las cuestiones relacionadas con la creación y tratamiento de los flujos de servicio NCS se consideran resueltas por DOCSIS, por lo que quedan fuera de alcance de esta Recomendación.

## 7.9 Sustitución del MTA

IPCablecom no requiere que se especifiquen los procedimientos de sustitución del MTA. No obstante, los flujos de secuencia de aprovisionamiento que se detallan en la presente Recomendación proporcionan suficiente cobertura y flexibilidad para soportar la sustitución. De hecho, la secuencia de inicialización de sustitución del MTA puede ser idéntica a la de la primera inicialización del MTA. Los procedimientos de fondo de oficina relacionados con la transferencia de perfiles de abonado de un MTA a otro dependen específicamente del funcionamiento de la red de cada proveedor de servicios. Como resultado de esta amplia diversidad, los procedimientos de fondo de oficina quedan fuera del alcance de esta Recomendación.

## 7.10 Pérdida temporal de la señal

Si el eCM (en un MTA incorporado) se pone a cero debido a cualquier condición Rf (por ejemplo, pérdida temporal de Rf), el eMTA IPCablecom asociado DEBE igualmente ponerse a cero.

NOTA – Esto tendrá repercusiones para las llamadas en curso.

## 7.11 Reinicio/rearranque de MTA

El rearranque se define como un 'ciclo de potencia' de todo el dispositivo eMTA. El reinicio se define como un 'reinicio SNMP' de la parte MTA del eMTA, un reinicio SNMP del eCM (lo que da lugar a un reinicio del eMTA correspondiente) o a una condición Rf que da como resultado un reinicio del eCM (que resulta en un reinicio del MTA correspondiente).

La parte MTA de un eMTA NO DEBE establecer diferencias entre un 'rearranque' y un 'reinicio'. Para ser más específico, el MTA DEBE tener los mismos parámetros de inicialización (por ejemplo, cuadros SNMP) y seguir todos los requisitos relativos a la información persistente (por ejemplo, almacenamiento de tique NVRAM) del mismo modo en ambos casos.

# 8 Opciones de DHCP

El DHCP se utiliza para obtener direcciones del protocolo Internet de versión 4 (IPv4) tanto para el CM como para el MTA. Los requisitos de CM y MTA para los códigos de opción 122 y 60 de DHCP se detallan en 8.1 y 8.2. Si el número total de octetos en cualquier opción DHCP supera los 255 octetos, el MTA DEBE ajustarse a RFC 3396 para dividir el mensaje DHCP en múltiples submensajes.

## 8.1 Opción 122 de DHCP: Opción de configuración de cliente

El código de opción 122 de DHCP es el sustituto RFCed de la antigua opción 177 (que era en realidad un código temporal). El CM y el MTA NO DEBEN solicitar la opción 177 en sus mensajes DESCUBRIMIENTO o PETICIÓN de DHCP en la opción 55 (lista de petición de parámetros). En caso de que un CM o un MTA pidan ambas opciones 122 y 177:

- El servidor de aprovisionamiento DEBE responder con la opción 122 de DHCP.
- El servidor de aprovisionamiento NO DEBE responder con la opción 177 de DHCP.
- El CM y el MTA DEBEN considerar preeminente la opción 122 de DHCP.

El código de opción de DHCP 122 se utiliza en los mensajes OFERTA/ACUSE DE RECIBO de DHCP tanto del CM como del MTA para proporcionar las direcciones de servidores de red de IPCablecom válidos y los datos de configuración de distintos dispositivos.

Pueden encontrarse todos los detalles de la codificación de la opción 122 de DHCP en RFC 3495 y RFC 3594.

En las siguientes cláusulas se presentan más detalles semánticos de cada subopción de la opción 122 de DHCP.

**Cuadro 6/J.167 – Opciones de servidor**

| Opción | Sub-opción | Descripción y comentarios | Subopción requerida u opcional | Valor por defecto |
|---|---|---|---|---|
| 122 | 1 | Dirección de servidor DHCP primario del proveedor de servicio. Requerido únicamente por el CM. | Requerido | No aplicable |
| | 2 | Dirección de servidor DHCP secundario del proveedor de servicio.<br>Requisito opcional para el CM. | Opcional | Cadena vacía |
| | 3 | Dirección de entidad de aprovisionamiento del proveedor de servicio. | Requerido | No aplicable |
| | 4 | Retroceso y reintento de intercambio AS-REQ/REP para gestión de claves SNMPv3. | Opcional | De acuerdo con los siguientes objetos de MIB:<br>"pktcMtaDevRealmUnsolicitedKeyNomTimeout",<br>"pktcMtaDevRealmUnsolicitedKeyMaxTimeout",<br>"pktcMtaDevRealmUnsolicitedKeyMaxRetries" |
| | 5 | Retroceso y reintento de aprovisionamiento kerberizado AP-REQ/REP. | Opcional | De conformidad con los siguientes objetos MIB:<br>"pktcMtaDevProvUnsolicitedKeyNomTimeout"<br>"pktcMtaDevProvUnsolicitedKeyMaxTimeout"<br>"pktcMtaDevProvUnsolicitedKeyMaxRetries" |
| | 6 | Sector Kerberos de la entidad SNMP. | Requerido | No aplicable |
| | 7 | Utilización del servidor que concede tique. | Opcional | No aplicable – Si el MTA no implementa TGT.0 – de otra manera. |
| | 8 | Temporizador de aprovisionamiento. | Opcional | De conformidad con el objeto MIB "pktcMtaDevProvisioningTimer" MIB (10 minutos) |
| | 9 | Invalidación del tique de seguridad. | Opcional | 0 – Se aplican las normas de invalidación de tique habituales, de conformidad con J.170 |

El MTA DEBE poder extraer y procesar los datos de todas las subopciones del cuadro anterior. El servidor de configuración DEBE proporcionar al MTA toda las subopciones "requeridas" y PUEDE proporcionar todas las subopciones "opcionales".

Si el servidor de aprovisionamiento no proporciona una subopción "opcional", el MTA DEBE utilizar el valor por defecto de tal subopción.

Si el servidor de aprovisionamiento no proporciona una subopción "requerida", el MTA DEBE rechazar la OFERTA/ACUSE DE RECIBO de DHCP correspondiente.

Si la subopción contiene un valor erróneo (no válido), el MTA DEBE:

- rechazar la correspondiente OFERTA/ACUSE DE RECIBO de DHCP en el caso de una subopción "requerida";
- utilizar el valor por defecto en el caso de una subopción "opcional". Para una subopción con múltiples parámetros (por ejemplo, subopción 4 de la opción 122 o subopción 5 de la opción 122), el MTA DEBE aplicar el correspondiente valor por defecto únicamente al parámetro (o parámetros) que contienen el valor erróneo.

El MTA DEBE ignorar cualquier otra subopción de la opción 122, a excepción de las enumeradas en el cuadro anterior.

### 8.1.1 Dirección DHCP de proveedor de servicio (subopción 2)

Las direcciones de servidor DHCP de proveedor de servicio identifican a los servidores DHCP de los que se aceptará una OFERTA de DHCP para obtener una dirección IP de MTA única para un dominio administrativo de red de un determinado proveedor de servicio.

La codificación de estas subopciones está definida en RFC 3495.

La subopción 1 DEBE estar incluida en la OFERTA/ACUSE DE RECIBO de DHCP al CM e indicar la dirección IP del servidor DHCP primaria. El valor contenido en la subopción 1 DEBE ser una dirección IP válida, un valor 255.255.255.255 o un valor de 0.0.0.0. El valor de la subopción 2 DEBE ser una dirección IP válida.

El MTA DEBE seguir la lógica del cuadro 7 al definir su estrategia DHCP, independientemente del flujo de aprovisionamiento que utilice:

**Cuadro 7/J.167 – Dirección DHCP de proveedor de servicio (subopción 2**

| **Valor de la subopción 1** | **Valor de la subopción 2** | |
|---|---|---|
| | IP válido – el servidor DHCP responde | IP válido – DHCP no responde |
| IP válido – el servidor DHCP responde | El MTA DEBE aceptar las OFERTAS de DHCP procedentes únicamente de direcciones IP de la subopción 1. | MTA DEBE aceptar OFERTAS de DHCP procedentes únicamente de direcciones IP de la subopción 1. |
| IP válido – DHCP NO responde | El MTA DEBE intentar exponencialmente al menos tres veces antes de aceptar la OFERTA de DHCP procedente del servidor DHCP indicado por la subopción 2. | EL MTA DEBE volver al paso MTA1. |
| 255.255.255.255 | El MTA DEBE seleccionar las OFERTAS de acuerdo con la lógica de RFC 2131. DEBE ignorarse el valor de la subopción 2. | El MTA DEBE seleccionar las OFERTAS de acuerdo con la lógica de RFC 2131. DEBE ignorarse el valor de la subopción 2. |
| 0.0.0.0 | El MTA DEBE detener todos los intentos de aprovisionamiento así como otras actividades. | El MTA DEBE detener todos los intentos de aprovisionamiento así como otras actividades. |

### 8.1.2 Dirección de entidad de aprovisionamiento de proveedor de servicio (subopción 3)

La dirección de entidad de aprovisionamiento de proveedor de servicio es la dirección de red del servidor de aprovisionamiento para el dominio administrativo de red de un determinado proveedor de servicio vocal.

La codificación de esta subopción está definida en RFC 3495. Esta dirección DEBE estar configurada únicamente como un FQDN.

Un valor de FQDN de 0.0.0.0 en la subopción 3 de una OFERTA/ACUSE DE RECIBO de DHCP de MTA especifica que el MTA DEBE apagarse y no intentar la aprovisión, a menos que el CM lo reinicialice. Esto queda explicado en el paso MTA2 del proceso de flujo de aprovisionamiento de 7.2.

El componente dirección de entidad de aprovisionamiento del proveedor de servicio DEBE ser capaz de aceptar las trampas SNMP.

La subopción 3 DEBE estar incluida en la OFERTA de DHCP al MTA.

### 8.1.3 Retroceso y reintento de intercambio AS-REQ/REP para la gestión de claves SNMPv3 (subopción 4)

El MTA DEBE utilizar la subopción 4 de la opción 122 de DHCP únicamente si la proporciona el flujo seguro. El mecanismo de retroceso y reintento de intercambio AS-REQ/REP de la negociación de claves SNMPv3 kerberizada que se define en la Rec. UIT-T J.170 está controlado por valores proporcionados en esta subopción o por valores por defecto de los correspondientes objetos MIB en el cuadro de sector, si esta subopción no está presente en la opción 122 de DHCP.

La codificación de esta subopción está definida en RFC 3495.

El valor nominal de expiración del temporizador de la subopción corresponde al objeto MIB pktcMtaDevRealmUnsolicitedKeyNomTimeout del pktcMtaDevRealmTable.

El valor máximo de expiración de temporizador de la subopción corresponde al objeto MIB pktcMtaDevRealmUnsolicitedKeyNomTimeout del pktcMtaDevRealmTable.

El cómputo máximo de reintentos de la subopción corresponde al objeto MIB pktcMtaDevRealmUnsolicitedKeyMaxRetries del pktcMtaDevRealmTable.

Un MTA DEBE poder extraer los antedichos parámetros de esa subopción, si se los proporciona el servidor de configuración.

El servidor de configuración PUEDE configurar un MTA con estos parámetros utilizando esta subopción.

Si cualquiera de los valores definidos en esta subopción es "FFFFFFFF" (hexadecimal), DEBE utilizarse el valor por defecto de la correspondiente columna del cuadro de sector.

### 8.1.4 Retroceso y reintento de aprovisionamiento kerberizado AP-REQ/REP (subopción 5)

El MTA DEBE utilizar la subopción 5 de la opción 122 de DHCP únicamente si se la proporciona el flujo seguro. El mecanismo de retroceso y reintento AP-REQ/REP de la negociación de claves SNMPv3 kerberizada definida en especificación de seguridad J.170 está controlado por los valores proporcionados en esta subopción.

La codificación de esta subopción está definida en RFC 3495.

El valor nominal de expiración del temporizador de la subopción corresponde al objeto MIB pktcMtaDevProvUnsolicitedKeyNomTimeout.

El valor máximo de expiración del temporizador de subopción corresponde al objeto MIB pktcMtaDevProvUnsolicitedKeyMaxTimeout.

El cómputo máximo de reintentos de la subopción corresponde al objeto de MIB pktcMtaDevProvUnsolicitedKeyMaxRetries.

Un MTA DEBE poder extraer los parámetros anteriores de la subopción, si se los proporciona el servidor de aprovisionamiento.

El servidor de aprovisionamiento PUEDE aprovisionar un MTA con estos parámetros utilizando esta subopción.

Si cualquiera de los valores definidos en esta subopción es "FFFFFFFF" (hexadecimal), DEBE utilizarse el valor por defecto del correspondiente objeto de MIB.

### 8.1.5 Sector Kerberos de la entidad SNMP (subopción 6)

Junto con la dirección de entidad de aprovisionamiento, el sector Kerberos se utiliza como medio de contactar con una entidad SNMP en el sector de aprovisionamiento. El nombre de sector se utiliza para realizar una comprobación SRV DNS del KDC del sector.

La subopción 6 de la opción 122 de DHCP DEBE estar incluida en la OFERTA de DHCP al MTA. Cuando se utiliza el flujo seguro, la subopción 6 de la opción 122 de DHCP DEBE contener únicamente el nombre de sector en el formato del FQDN (tipo=0, de conformidad con el RFC 3495).

El MTA DEBE seleccionar el correspondiente flujo de aprovisionamiento de conformidad con el cuadro 8 que se muestra a continuación (la comparación del contenido en la subopción 6 de la opción 122 de DHCP tiene en cuenta las mayúsculas y las minúsculas y DEBE figurar íntegramente en letras mayúsculas).

**Cuadro 8/J.167 – Selección del flujo de aprovisionamiento del dispositivo MTA**

| Contenido de la subopción 6 de la opción 122 de DHCP | Selección del flujo de aprovisionamiento del dispositivo MTA |
|---|---|
| BASIC.1 | Si el valor de la subopción 6 de la opción 122 de DHCP es BASIC.1 (BÁSICO.1), el MTA DEBE ejecutar el flujo básico sin el mensaje INFORME de SNMP de configuración completa. |
| BASIC.2 | Si el valor de la subopción 6 de la opción 122 es BASIC.2 (BÁSICO.2), el MTA DEBE ejecutar el flujo básico con el mensaje INFORME de SNMP del aprovisionamiento completo. |
| HYBRID.1 | Si el valor de la subopción 6 de la opción 122 de DHCP es HYBRID.1 (HÍBRIDO.1), el MTA DEBE ejecutar el flujo híbridos sin el mensaje INFORME de SNMP de aprovisionamiento completo. |
| HYBRID.2 | Si el valor de la subopción 6 de la opción 122 de DHCP es HYBRID.2 (HÍBRIDO.2), el MTA DEBE ejecutar el flujo híbrido con el mensaje INFORME de SNMP de aprovisionamiento completo. |

El MTA DEBE utilizar el flujo seguro si en la subopción 6 de la opción 122 de DHCP se proporciona cualquier otro valor. Para el flujo seguro, la codificación de la subopción 6 de la opción 122 de DHCP está definida en RFC 3495.

#### 8.1.5.1 Establecimiento de claves SNMPv3

El establecimiento de claves SNMPv3 es aplicable únicamente al flujo seguro. La petición AP/respuesta AP que se describe en la figura 6, la correspondiente descripción de flujos y la especificación de seguridad son utilizadas por el MTA en la fase inicial de aprovisionamiento para establecer claves según el "MTA-Prov-xx:xx:xx:xx:xx:xx" de usuario USM de SNMPv3. En este caso, xx:xx:xx:xx:xx:xx representa la dirección MAC del MTA y DEBE ir en mayúsculas. El MTA DEBE ejemplificar a este usuario en la MIB USM que se describe en el RFC 3414, siempre con la

posibilidad de crear claves utilizando el método de gestión de claves kerberizada IPCablecom que se describe en la especificación de seguridad. Se requiere de la autenticación SNMPv3 y la privacidad es opcional. Puede consultarse en la Rec. UIT-T J.170 la lista de algoritmos de autenticación y privacidad SNMPv3.

Además, el usmUserSecurityName DEBE estar puesto a la cadena "MTA-Prov-xx:xx:xx:xx:xx:xx" (comillas no incluidas), donde xx:xx:xx:xx:xx:xx representa la dirección MAC del MTA y DEBE ir en mayúsculas. Se garantiza así la creación de un usmUserSecurityName único para cada MTA.

El MTA debe, en primer lugar, obtener un tique de servicio para el sector de aprovisionamiento, como se describe en el paso MTA9. La gestión de claves USM se realiza en todo el UDP, como se especifica en la Rec. UIT-T J.170. Las claves SNMPv3 se crean antes de que exista cualquier comunicación SNMPv3, por lo que los mensajes SNMPv3 DEBEN autenticarse en todo momento (siendo la privacidad opcional). El MTA DEBE utilizar el usuario USM creado anteriormente en su INFORME inicial.

### 8.1.6 Utilización del servidor que concede tique (subopción 7)

El MTA DEBE utilizar la subopción 7 de la opción 122 de DHCP, únicamente si se proporciona para la gestión de claves kerberizada de aprovisionamiento. Esta subopción contiene un valor booleano que, cuando es verdadero, indica que el MTA DEBERÍA obtener su TGT (tique de concesión de tique).

La subopción 7 PUEDE estar incluida en los mensajes OFERTA/ACUSE DE RECIBO de DHCP al MTA.

La codificación de esta subopción está definida en RFC 3495.

### 8.1.7 Temporizador de aprovisionamiento (subopción 8)

La subopción 8 define el valor que se ha de utilizar para el temporizador de aprovisionamiento. La subopción 8 PUEDE estar incluida en los mensajes OFERTA/ACUSE DE RECIBO de DHCP al MTA.

La codificación de esta subopción se define en RFC 3495.

### 8.1.8 Invalidación de tique de seguridad (subopción 9)

La subopción 9 contiene una máscara de bits que dirige el MTA a invalidar algunos tiques de seguridad del servidor de aplicación específicos. La subopción 9 PUEDE estar incluida en los mensajes OFERTA/ACUSE DE RECIBO de DHCP al MTA. La codificación de esta subopción está definida en el RFC 3594.

## 8.2 Opción 60 de DHCP: Identificador de cliente fabricante

El código de opción 60 contiene una cadena que identifica las capacidades del MTA. El MTA DEBE enviar la siguiente cadena con codificación ASCII en el código de opción 60 de DHCP: "pktc1.0:xxxxxx". En este caso, xxxxxx DEBE tener una representación ASCII de la codificación hexadecimal de las capacidades con codificación TLV del MTA, como se define en la cláusula 10.

## 8.3 Opciones 12 y 15 de DHCP

El FQDN del MTA DEBE enviarse al MTA incorporado en las opciones 12 y 15. La opción 12 DEBE contener la parte "nombre anfitrión" del FQDN, y la opción 15 DEBE contener la parte "nombre de dominio" del FQDN.

Por ejemplo, si el FQDN del MTA es "mta1.pclab.com", la opción 12 contendrá "mta1" y la opción 15 contendrá "pclab.com".

## 8.4 Opción 6 de DHCP

La opción 6 de DHCP DEBE utilizarse para proporcionar al MTA su lista de direcciones de servidor DNS. La opción 6 DEBE contener, como mínimo, una dirección de servidor DNS. La opción 6 PUEDE contener una dirección DNS secundaria. Si esta opción contiene más de dos servidores DNS, el MTA DEBE utilizar las dos primeras direcciones.

## 8.5 Opción 43 de DHCP

El MTA DEBE enviar la opción 43 de DHCP en los mensajes DESCUBRIMIENTO y PETICIÓN de DHCP en los flujos seguro, híbrido y básico.

La opción 43 de DHCP contiene el número de subopciones definido para proporcionar información específica del dispositivo MTA a los sistemas de fondo de oficina. Las subopciones 1, 10, 31 y 32 de la opción 43 de DHCP están especificadas por IPCablecom Las subopciones 11 a 30 están reservadas para las recomendaciones relativas a IPCable2Home (serie J.19x); las subopciones 33 a 50 están reservadas para IPCablecom; las subopciones 51 a 127 están reservadas a la normalización futura; y las subopciones 128 y siguientes están reservadas para uso privado. Las subopciones de la opción 43 de DHCP IPCablecom DEBEN estar presentes en formato "extensión específica del vendedor encapsulada" (RFC 2132).

En el cuadro 9 se muestran las subopciones de la opción 43 de DHCP que DEBE utilizar el MTA. El MTA DEBE enviar todas las subopciones requeridas enumeradas en el siguiente cuadro, a menos que se indique explícitamente lo contrario. Si el número total de octetos en todas las subopciones de la opción 43 de DHCP supera los 255, el MTA DEBE ajustarse a RFC 3396 para dividir la opción en múltiples opciones más pequeñas.

**Cuadro 9/J.167 – Sintaxis de la opción 43 de DHCP**

| Subopciones de la opción 43 de DHCP para el MTA | Requerido/ no utilizado en la opción 43 | Valor | Descripción |
|---|---|---|---|
| Subopción 1 | No utilizado | | El vector de la subopción requerida es una lista de subopciones (dentro de la opción 43) que ha de devolver el servidor al cliente en una respuesta a una petición. No se define ninguna. La subopción 1 de la opción 43 de DHCP NO DEBE ser utilizada por el MTA, y, de estar presente, DEBE ser ignorada por el servidor de aprovisionamiento. |
| Subopción 2 | Requerido | <DevType> | La subopción 2 contiene el tipo de dispositivo del componente que envía la petición DHCP. El MTA DEBE enviar la subopción 2 de la opción 43 de DHCP.<br>Para los MTA de IPCablecom, los tipos de dispositivos permitidos son:<br>– "EMTA" para los MTA incorporados<br>– "SMTA" para los MTA autónomos |
| Subopción 3 | No utilizado | | La subopción 3 contiene una lista separada por comas de todos los componentes del dispositivo eDOCSIS. La utiliza el dispositivo eCM de eDOCSIS.<br>El MTA NO DEBE enviar la subopción 3 de la opción 43 de DHCP y, de estar presente, DEBE ser ignorada por el servidor de aprovisionamiento. |

**Cuadro 9/J.167 – Sintaxis de la opción 43 de DHCP**

| Subopciones de la opción 43 de DHCP para el MTA | Requerido/ no utilizado en la opción 43 | Valor | Descripción |
|---|---|---|---|
| Subopción 4 | Requerido | <device serial number> | La subopción 4 contiene el número de serie del dispositivo representado como una cadena ASCII.<br>El MTA DEBE enviar la subopción 4 de la opción 43 de DHCP. El valor de la subopción 4 de la opción 43 de DHCP DEBE ser idéntico al valor del objeto MIB pktcMtaDevSerialNumber. |
| Subopción 5 | Requerido | <Hardware version> | La subopción 5 contiene el número de versión de hardware representado como una cadena al ASCII.<br>El MTA DEBE enviar la subopción 5 de la opción 43 de DHCP. La subopción 5 de la opción 43 de DHCP DEBE ser idéntica al valor del número de versión de Hardware del campo <Hardware version> del objeto MIB II sysDescr. |
| Subopción 6 | Requerido | <Software version> | La subopción 6 contiene el número de versión de software representado como una cadena ASCII.<br>El MTA DEBE enviar la subopción 6 de la opción 43 de DHCP. El valor de la subopción 6 de la opción 43 de DHCP DEBE ser idéntico al valor del objeto MIB pktcMtaDevSwCurrentVers. |
| Subopción 7 | Requerido | <Boot ROM Version> | La subopción 7 contiene la versión ROM de arranque representada como una cadena ASCII.<br>El MTA DEBE enviar la subopción 7 de la opción 43 de DHCP.<br>El valor de la subopción 7 de la opción 43 de DHCP DEBE ser idéntico al campo <Boot ROM version> del objeto MIB II sysDescr. |
| Subopción 8 | Requerido | <OUI> | La subopción 8 contiene el identificador único de organización (OUI) representado como una cadena de octetos de 3 bytes con codificación hexadecimal. PUEDE corresponder al OUI de la dirección MAC del MTA.<br>El MTA DEBE enviar la subopción 8 de la opción 43 de DHCP.<br>Si se omite, el servidor de aprovisionamiento DEBERÍA utilizar la dirección MAC MTA en tanto que OUI del MTA. |
| Subopción 9 | Requerido | <Model Number> | La subopción 9 contiene el número de modelo del dispositivo MTA representado como una cadena ASCII.<br>El MTA DEBE enviar la subopción 9 de la opción 43 de DHCP.<br>El valor de la subopción 9 de la opción 43 de DHCP DEBE ser idéntico al campo <Model Number> del objeto MIB-II sysDescr. |

**Cuadro 9/J.167 – Sintaxis de la opción 43 de DHCP**

| Subopciones de la opción 43 de DHCP para el MTA | Requerido/ no utilizado en la opción 43 | Valor | Descripción |
|---|---|---|---|
| Subopción 10 | Requerido | <Vendor Name> | La subopción 10 contiene el nombre del vendedor representado como una cadena ASCII.<br>El MTA DEBE enviar la subopción 10 de la opción 43 de DHCP. EL valor de la subopción 10 de la opción 43 de DHCP DEBE ser idéntico al campo <Vendor Name> del objeto MIB-II sysDescr. |
| Subopciones 11-30 | | | Reservado para CableHome. |
| Subopción 31 | Requerido | <MTA MAC Address> | La subopción 31 contiene la dirección MAC de MTA codificada como una cadena de octetos de 6 bytes.<br>El MTA DEBE enviar la subopción 31 de la opción 43 de DHCP. El valor de la subopción 31 de la opción 43 de DHCP DEBE ser idéntico al contenido del objeto MIB pktcMtaDevMacAddress. |
| Subopción 32 | Requerido | <Correlation ID> | La subopción 32 contiene el número del identificador de correlación codificado como un ENTERO de 4 bytes en el orden de red.<br>El MTA DEBE enviar la subopción 32 de la opción 43 de DHCP.<br>El valor de la subopción 32 de la opción 43 de DHCP DEBE ser idéntico al contenido del objeto MIB pktcMtaDevCorrelationId. |
| Subopciones 33-50 | | | Reservado para IPCablecom. |
| Subopciones 51 a 127 | | | Reservado para CableLabs. |
| Subopciones 128 a 254 | | | Reservado para vendedores. |

### 8.6 Opción 1 de DHCP 1

La opción 1 de DHCP está definida en RFC 2132.

### 8.7 Opción 3 de DHCP

La opción 3 de DHCP está definida en RFC 2132.

## 9 Atributos aprovisionables de MTA

Esta cláusula contiene la lista de atributos, y sus correspondientes propiedades, utilizados en el aprovisionamiento de un dispositivo. Todos los atributos aprovisionables especificados en esta cláusula PUEDEN ser actualizados por conducto del fichero de datos de definición de la configuración del MTA, o bien atributo por atributo utilizando el SNMP.

IPCablecom exige que el fichero de datos de configuración de un MTA pueda ser proporcionado a todos los MTA incorporados durante la secuencia de registro. Los servicios vocales del punto extremo no tienen que estar habilitados en el momento de la inicialización. Los datos de configuración a nivel de dispositivo del MTA DEBEN aprovisionarse durante la inicialización. Estos elementos figuran en 9.1.1.

La URL de datos de la configuración del MTA generado por la aplicación de aprovisionamiento DEBE tener una longitud inferior a 255 bytes y no puede ser NULO. Puesto que este nombre de fichero se lo proporciona al MTA la aplicación de aprovisionamiento durante la secuencia registrada, no es necesario especificar un convenio de denominación de ficheros.

## 9.1 Fichero de definición de la configuración de MTA

En esta cláusula se explican el formato y los contenidos del fichero de definición de la configuración MTA. El fichero contiene una serie de parámetros "tipo/longitud/valor" (TLV). Cada parámetro TLV del fichero de la configuración describe un atributo de MTA o punto extremo. El fichero de datos de la configuración incluye los parámetros TLV que tienen acceso de lectura-escritura, de lectura solamente o ningún acceso a la base de información de gestión (MIB). A menos que se indique otra cosa de manera específica, todos los parámetros del fichero de configuración con acceso a la MIB DEBEN ser definidos utilizando el tipo 11 TLV DOCSIS, el tipo 64 IPCablecom o el tipo 38 TLV IPCablecom. El tipo 64 TLV es un TLV definido por IPCablecom con un valor de longitud de 2 bytes, en vez de 1 byte, como es el caso del tipo 11 TLV DOCSIS. DEBE utilizarse el tipo 64 TLV cuando la longitud es superior a 254 bytes. Si se prefiere, puede añadirse información específica del vendedor al fichero de definición de la configuración utilizando el TLV-43, que es específico del vendedor. Este TLV está definido en la especificación DOCSIS (Rec. UIT-T J.112). Los vendedores NO DEBEN aprovisionar la información que les es específica utilizando los tipos 11 ó 64 TLV. TLV 38 es un TLV definido por IPCablecom, análogo al TLV-38 utilizado por DOCSIS e IPCable2Home. El MTA DEBE poder procesar los TLV que figuran en el cuadro 10:

**Cuadro 10/J.167 – Fichero de definición de la configuración de MTA**

| Tipo | Longitud | Valor |
|---|---|---|
| 11 | n, donde n es un 1 byte | Vinculación variable |
| 64 | m, donde m es 2 bytes | Vinculación variable |
| 38 | n, donde n es 1 byte | Compuesto (contiene subTLV) |
| 254 | 1 byte | 0xFE al principio del fichero y and0xFF al final del fichero |
| NOTA – Se recomienda, siempre que sea posible, utilizar el tipo 11 TLV en vez de TLV 64. | | |

En el futuro, los TLV que se introduzcan en IPCablecom deberán tener un "campo longitud" de 2 bytes.

La vinculación variable se codifica aplicando las reglas de codificación básica ASN.1, como si fuera parte de una petición fijar de SNMP.

El fichero de definición de la configuración del MTA DEBE empezar con el rótulo "comienzo de fichero de definición de la configuración de telefonía" y DEBE terminar con el rótulo "final de fichero de definición de la configuración de telefonía". Estos rótulos permiten establecer una distinción entre los parámetros TLV del MTA y los parámetros TLV de DOCSIS. Son unos rótulos que proporcionan además indicaciones determinísticas para el arranque y la parada del fichero de definición de la configuración de MTA.

El fichero de definición de la configuración del MTA DEBE contener los atributos identificados como "requerido" en el cuadro de datos de configuración a nivel de dispositivo que figura en 9.1.1. En caso contrario, el MTA DEBE rechazar el fichero de configuración y realizar los pasos necesarios, como se define en 7.2 (fallo del paso MTA 23 por 'error de fichero de definición de la configuración'). El fichero de definición de la configuración del MTA PUEDE contener cualquier atributo no requerido que aparezca en el cuadro de datos de configuración a nivel de dispositivo. Si el fichero de definición de la configuración no contiene los atributos requeridos, DEBE rechazarse.

El fichero de definición de la configuración del MTA DEBE ser enviado al MTA incorporado cada vez que se active la potencia de este dispositivo.

Los datos de servicio a nivel de dispositivo PUEDEN enviarse al MTA como parte del fichero de definición de la configuración del MTA o PUEDEN enviarse al MTA utilizando SNMP. Si se incluyen en el fichero de definición de la configuración, éste DEBE contener todos los atributos identificados como 'requeridos' en los datos de servicio a nivel de dispositivo, de haberlos. El fichero de definición de la configuración del MTA PUEDE además contener cualquier atributo no requerido que aparezca en el cuadro de datos de servicio a nivel de dispositivo.

Si se requieren servicios vocales en el MTA o en cualquier punto extremo, DEBEN seguirse los siguientes pasos:

1) pktcMtaDevEnabled DEBE estar puesto a VERDADERO.
2) DEBE realizarse una configuración para cada punto extremo utilizando el fichero de definición de la configuración del MTA (durante el aprovisionamiento) o mediante la configuración del punto extremo (utilizando SNMP) en la fase posterior al aprovisionamiento.

Los detalles del punto extremo, cuando estén incluidos, DEBEN contener los atributos identificados como "requerido" en el cuadro de datos de configuración por punto extremo, que puede encontrarse en 9.1.3. El fichero de definición de la configuración del MTA PUEDE contener cualquier atributo que aparezca en el cuadro de datos de configuración por punto extremo de 9.1.3. DEBEN enviarse al MTA los datos de configuración por punto extremo cuando esté activado el servicio de comunicaciones vocales.

Cabe señalar que los datos de servicio a nivel de dispositivo y los datos de configuración por punto extremo PUEDEN igualmente enviarse al MTA mediante un aprovisionamiento incremental utilizando SNMP. El MTA DEBE soportar el aprovisionamiento incremental.

El MTA DEBE poder procesar todos los valores TLV-11 y TLV-64 con vinculaciones variables que contengan todos los objetos MIB definidos en la Rec. UIT-T J.166, a menos que se especifique lo contrario.

El parámetro 'pktcMtaDevEnabled' de los datos de aprovisionamiento a nivel de servicio se utiliza en realidad para habilitar o inhabilitar los servicios vocales en un MTA.

Puede consultarse en 7.6.1 la sincronización de los atributos de aprovisionamiento en los sistemas de fondo de oficina.

En el caso de los flujos de aprovisionamiento seguro e híbrido, el MTA DEBE autenticar el fichero de configuración de acuerdo con la especificación de seguridad IPCablecom J.170. El MTA DEBE rechazar el fichero de definición de la configuración, si no se logra su autenticación, y realizar los pasos necesarios que se definen en 7.2 para el flujo seguro y en 7.4 para el flujo híbrido. Si el fichero de definición de la configuración contiene el objeto MIB "pktcMtaDevProvConfigHash" en el flujo seguro o el flujo híbrido, el MTA DEBE ignorar el valor de este objeto MIB y seguir procesando el fichero de definición de la configuración y emitir un informe de paso con aviso y llenar el cuadro de OID erróneos (pktcMtaDevErrorOidsTable).

En el caso del flujo básico, el servidor de aprovisionamiento y el MTA DEBEN soportar el proceso de verificación de los datos del fichero de definición de la configuración, como se describe a continuación:

1) Cuando el servidor de aprovisionamiento crea un nuevo fichero de definición de la configuración del MTA, o modifica uno existente, que se va a entregar a un MTA previsto para ser configurado con el flujo básico, DEBE calcular el valor generado SHA-1 de los contenidos de todo el fichero de definición de la configuración del MTA, incluidos los marcadores de inicio y final, tomados como una cadena de bytes.

2) El servidor de aprovisionamiento DEBE añadir el valor generado, calculado en el Paso 1, al fichero de definición de la configuración del MTA como una tripleta TLV-11 correspondiente al objeto MIB pktcMtaDevProvConfigHash. El servidor de aprovisionamiento DEBE insertar la tripleta TLV-11 antes del marcador final del fichero de definición del aprovisionamiento. El servidor de aprovisionamiento NO DEBE modificar el orden de los TLV en el fichero de definición de la configuración una vez calculado el valor generado. El fichero de definición de la configuración del MTA se presenta entonces al MTA a través del servidor TFTP/HTTP correspondiente.

3) Una vez que se reciba el fichero de definición de la configuración, el MTA DEBE hacer lo siguiente: Si el objeto MIB 'pktcMtaDevProvConfigHash' está ausente, el MTA DEBE rechazar el fichero de definición de la configuración y DEBE enviar un informe 'fallo por otros motivos'.

Si el objeto MIB 'pktcMtaDevProvConfigHash' está presente, el MTA DEBE:

a) Calcular el SHA-1 del contenido del fichero sin la tripleta TLV-11 que contiene el 'pktcMtaDevProvConfigHash' y DEBE insertar el valor calculado en el objeto MIB pktcMtaDevProvConfigHash. El MTA debe mantener el orden de los TLV para el cálculo del valor generado sea correcto.

b) Si el valor calculado y el valor del objeto MIB 'pktcMtaDevProvConfigHash' son idénticos, queda verificada la integridad del fichero de definición de la configuración del MTA y el MTA DEBE aceptar el fichero de definición de la configuración para un procesamiento posterior. En caso contrario, el MTA DEBE rechazar el fichero de definición de la configuración y DEBE enviar un informe 'fallo por otros motivos'.

El MTA debe asimismo verificar la existencia de errores en el fichero de definición de la configuración. Como se describe anteriormente, los errores en cualquiera de los parámetros obligatorios DEBE tratarse como un error del fichero de definición de la configuración y han de seguirse los pasos correspondientes (fallo del paso MTA23 por 'error del fichero de definición de la configuración').

Si existen errores en los OID no requeridos, el MTA DEBE aceptar el fichero de definición de la configuración, pero incluirlos en un informe de estado (MTA25).

Si el fichero de definición de la configuración contiene datos de cms y parámetros de puntos extremos relacionados con los CMS que no están asociados a los puntos extremos, el MTA NO DEBE establecer asociaciones de seguridad hasta que los puntos extremos se asocien con dicho CMS en concreto (utilizando los SNMP o vía redireccionamiento NCS).

El MTA DEBE informar del estado del fichero de definición de la configuración que ha recibido en un 'Informe de configuración completa' (paso MTA25 del proceso de aprovisionamiento), como se indica a continuación:

- Si el fichero de definición de la configuración puede analizarse sintácticamente de manera satisfactoria y el MTA puede reflejarlo en su MIB, devolverá un mensaje 'paso'.
- Si el fichero de definición de la configuración es erróneo debido a que contiene valores incorrectos en los parámetros obligatorios, el MTA DEBE rechazar el fichero de configuración y devolver un mensaje 'fallo por error del fichero de definición de la configuración'.
- DEBE igualmente llenar el objeto 'pktcMtaDevErrorOidsTable' con los parámetros que contienen valores incorrectos y PUEDE también introducir los avisos/OID erróneos, si ha analizado sintácticamente todo el fichero.
- Si el fichero de definición de la configuración tiene valores apropiados para todos los parámetros obligatorios, pero contiene errores en cualquiera de los parámetros facultativos

(lo que incluye cualquier OID específico del vendedor que sea incorrecto o desconocido para el MTA), debe devolver un mensaje 'paso con aviso'.

- DEBE introducir en el objeto 'pktcMtaDevErrorOidsTable' una lista de todos los parámetros rechazados y el motivo de rechazo. El MTA DEBE igualmente utilizar los valores por defecto de tales parámetros, a menos que queden anulados por cualquier otro medio, como el DHCP, en cuyo caso se utilizarán los valores de anulación.
- Si el fichero de definición de la configuración es adecuado, pero el MTA no puede reflejarlo en su MIB (por ejemplo, porque hay demasiadas entradas que agotan la memoria), DEBE aceptar los detalles relacionados con los CMS asociados con los puntos extremos y devolver un mensaje 'paso con análisis incompleto'.
- DEBE asimismo introducir en el objeto 'pktcMtaDevErrorOidsTable' una lista de todos los parámetros que no puedan reflejarse en la MIB.
- Si el fichero de definición de la configuración no puede analizarse sintácticamente por un error interno, debe devolver un mensaje 'fallo por error interno'. DEBERÍA intentar introducir en el objeto 'pktcMtaDevErrorOidsTable' los parámetros que han causado tal fallo.
- Si el MTA no puede aceptar el fichero de definición de la configuración por cualquier motivo distinto de los ya expuestos, debe devolver un mensaje 'fallo por otros motivos'. DEBERÍA intentar introducir en el objeto 'pktcMtaDevErrorOidsTable' los parámetros que han causado el fallo.

El fichero de definición de la configuración del MTA DEBE contener los datos de definición por sector. En el caso del flujo de configuración seguro, los datos de configuración por sector DEBEN contener al menos los datos del sector de aprovisionamiento que se identifican en la subopción 6 de la opción 122 de DHCP.

En el caso de flujo de aprovisionamiento seguro, una vez recibido el fichero de definición de la configuración del MTA, éste DEBE validar lo siguiente:

- El objeto MIB "pktcMtaDevRealmName" del cuadro de sector DEBE ser idéntico al nombre de sector proporcionado al MTA en la subopción 6 de la opción 122 de DHCP.
- El objeto MIB "pktcMtaDevRealmOrgName" del cuadro de sector DEBE ser idéntico al atributo "Nombre de Organización" del Certificado de Proveedor de Servicio.
- La criptación y autenticación del fichero de definición de la configuración del MTA debe ser compatible con la Rec. UIT-T J.170.

Un MTA DEBE tratar los fallos de validación anteriores como un fallo de flujo de aprovisionamiento MTA23 y DEBE descartar el fichero de definición de la configuración.

Si el MTA se encuentra con un TLV-43 específico del vendedor con un ID de vendedor que no reconoce como propio, el MTA debe ignorar el TLV-43 y DEBE continuar con el procesamiento del fichero de definición de la configuración. Si el MTA detecta la presencia de un TLV no reconocido (TLV de un tipo distinto a TLV-11, TLV-43, TLV-64, TLV-38 o TLV-254), DEBE ignorar el TLV asumiendo que el campo de longitud del TLV no reconocido es de 2 bytes y seguir con el procesamiento. El MTA DEBE presentar un informe de estado del aprovisionamiento "paso con aviso" e introducir en el cuadro de OID erróneos (pktcMtaDevErrorOidsTable) si detecta la presencia de un TLV no reconocido. Si el MTA encuentra una vinculación variable no reconocida en un TLV-11 o un TLV-64, DEBE ignorar dicha vinculación, DEBE presentar un informe de estado de aprovisionamiento de "pasos con aviso" e introducirla en el cuadro de errores de OID (pktcMtaDevErrorOidsTable). Se recomienda vivamente a los vendedores que consideren seriamente las cuestiones relativas con la compatibilidad con versiones anteriores al modificar los subTLV existentes de TLV-43 o introducir nuevos.

El MTA DEBE intentar aceptar el fichero de definición de configuración que contiene conjuntos válidos de datos de configuración por sector y por CMS identificados en 9.1.4 y 9.1.5, incluso si los puntos extremos MTA no están asociados con el CMS y los datos de configuración por CMS.

Los objetos MIB IPCablecom en la MIB-MTA (Rec. UIT-T J.166), la MIB de señalización (Rec. UIT-T J.166) y la MIB de eventos (Rec. UIT-T J.166), y el tipo estado de fila NO DEBEN incluirse en el fichero de definición de la configuración del MTA. Si cualquiera de los objetos MIB IPCablecom (MIB MTA, MIB de señalización y MIB de evento) del tipo 'RowStatus' (estado de fila) se incluye en el fichero de definición de la configuración, el MTA DEBE ignorar el valor presentado en cualquier objeto RowStatus, enviar un informe 'pasos con aviso' e introducirlo en el cuadro MIB 'pktcMtaDevErrorOidsTable', convenientemente. Independientemente de las medidas que adopte, el MTA DEBE introducir adecuadamente los OID de estado de línea en el cuadro de OID erróneos. Ningún objeto MIB IPCablecom del tipo estado de fila puede estar presente o ausente en el fichero de definición de la configuración del MTA, y el MTA DEBE procesar estos objetos de acuerdo con las RFC correspondientes a cada uno de los objetos MIB (por ejemplo, cuadro SNMPv2c).

El objeto MIB IPCablecom pktcEnMtaDevMltplGrantsPerInterval, de estar incluido en el fichero de definición de la configuración y puesto a la funcionalidad múltiples concesiones por intervalo (MGPI, *multiple grants per interval*), y si el MTA no soporta esta funcionalidad, DEBE señalar el objeto y enviar un informe 'paso con aviso' e introducirlo en el cuadro de OID erróneos.

### 9.1.1 Datos de configuración a nivel dispositivo

Para una información más detallada a propósito de estos atributos y sus valores por defecto véase (Rec. UIT-T J.166) relativa a la base de información de gestión (MIB) del adaptador de terminal de medios (MTA) (véase el cuadro 11).

- El certificado del fabricante del MTA valida el certificado del dispositivo MTA.

**Cuadro 11/J.167 – Configuración a nivel de dispositivo**

| Atributo | Sintaxis | Acceso a la configuración | Acceso al SNMP | Fichero MIB | Objeto | Comentarios |
|---|---|---|---|---|---|---|
| Comienzo del fichero de definición de la configuración de telefonía | Entero | W, requerido | Ninguno | No aplicable | No aplicable | Tipo Longitud Valor<br>254 1 1<br>El fichero de definición de la configuración del MTA DEBE empezar con este atributo. |
| Final del fichero de definición de la configuración de telefonía | Entero | W, requerido | Ninguno | No aplicable | No aplicable | Tipo Longitud Valor<br>254 1 255<br>Éste DEBE ser el último atributo del fichero de definición de la configuración del MTA. |

## Cuadro 11/J.167 – Configuración a nivel de dispositivo

| Atributo | Sintaxis | Acceso a la configuración | Acceso al SNMP | Fichero MIB | Objeto | Comentarios |
|---|---|---|---|---|---|---|
| Estado administrativo del MTA de telefonía | ENUM | W, requerido | R/W | MIB del dispositivo MTA | pktcMtaDevEnabled | Se utiliza para habilitar/ inhabilitar todos los puertos de telefonía del MTA. Se aplica al lado MTA del MTA incorporado o al MTA autónomo en su totalidad. Permite la gestión genérica de todos los puertos de telefonía (interfaces externas) del dispositivo. El estado del MTA está controlado por este objeto MIB. Puede encontrarse más información sobre este objeto en el MIB MTA (Rec. UIT-T J.166). |
| Nombre de organización del sector | Cadena | W, requerido (flujo de aprovisionamiento seguro)<br>W, opcional (flujos de aprovisionamiento básico e híbrido) | R/W | MIB del dispositivo MTA | pktcMtaDevRealmOrgName | El valor del atributo nombre de organización del nombre X.500 en el sujeto del certificado de proveedor de servicios. |
| Expiración del temporizador de clave solicitada | Entero | W, opcional | R/W | No aplicable | pktcMtaDevProvSolicitedKeyTimeout | Esta expiración del temporizador se aplica únicamente cuando el servidor de aprovisionamiento ha iniciado una gestión de claves (con un mensaje de activación) para SNMPv3. Es el periodo durante el cual el MTA guardará un nonce (dentro del campo número de secuencia) del envío de la petición AP y esperará a la correspondiente respuesta AP del servidor de aprovisionamiento. Es opcional porque existe un valor por defecto. |

**Cuadro 11/J.167 – Configuración a nivel de dispositivo**

| Atributo | Sintaxis | Acceso a la configuración | Acceso al SNMP | Fichero MIB | Objeto | Comentarios |
|---|---|---|---|---|---|---|
| Información del tique reiniciar Kerberos | Entero 32 | W, opcional | R/W | MIB del dispositivo MTA | pktcMtaDevResetKrbTickets | La especificación de seguridad (J.170) permite que los tiques Kerberos asociados con cualquiera de los servidores de aplicación (servidor de aprovisionamiento o CMS) se almacenen en el NVRAM del MTA hasta la expiración del tique. Para controlar la invalidación de los tiques almacenados en el NVRAM, este atributo MIB se utiliza para comunicar al MTA las acciones que es necesario realizar. Una vez recibido este atributo en el fichero definición de la configuración, el MTA DEBE realizar la acción especificada. Puede encontrarse más información en J.166. |

### 9.1.2 Datos de servicio a nivel de dispositivo

Para una información más detallada a propósito de estos atributos y sus valores por defecto, véanse la Recomendación relativa a la base de información de gestión (MIB) del adaptador de terminal de medios (MTA) (Rec. UIT-T J.166), la Recomendación relativa a la MIB de la señalización de llamada de red (NCS), (Rec. UIT-T J.166) relativa a la especificación de la señalización de llamada de red (Rec. UIT-T J.162) y la RFC 2475 (véase el cuadro 12).

**Cuadro 12/J.167 – Servicio a nivel de dispositivo**

| Atributo | Sintaxis | Acceso a la configuración | Acceso al SNMP | Fichero MIB | Objeto | Comentarios pktcDevEvSyslo |
|---|---|---|---|---|---|---|
| TOS de señalización de llamada por defecto NCS | Entero | W, opcional | R/W | MIB de señalización del MTA | pktcSigDefCallSigTos | Valor por defecto utilizado en el encabezamiento IP para la fijación del valor TOS a efectos de señalización de llamada de red (NCS). |
| TOS de tren de medios por defecto NCS | Entero | W, opcional | R/W | MIB de señalización del MTA | pktcSigDefMediaStreamTos | Valor por defecto utilizado en el encabezamiento IP para la fijación del valor TOS de los paquetes de trenes de medios de NCS. |
| Puerto de recepción UDP del MTA utilizado para NCS | Entero (1025..65535) | W, opcional | R/O | MIB de señalización del MTA | pktcSigDefNcsReceiveUdpPort | Este objeto contiene el puerto de recepción del protocolo de datagrama de usuario del MTA que se utiliza para la señalización de llamada NCS. Este objeto sólo puede ser modificado por el fichero definición de la configuración. |

## Cuadro 12/J.167 – Servicio a nivel de dispositivo

| Atributo | Sintaxis | Acceso a la configuración | Acceso al SNMP | Fichero MIB | Objeto | Comentarios pktcDevEvSyslo |
|---|---|---|---|---|---|---|
| Selector de formato TOS de NCS | ENUM | W, opcional | R/W | MIB de señalización del MTA | pktcSigTos Format Selector | Formato de los valores por defecto de TOS de medios y señalización NCS.<br>Los valores permitidos son "octeto TOS de IPv4" o "punto de código de DSCP". Véase RFC 2475. |
| Cadencia R0 | Campo de bits | W, opcional | R/W | MIB de señalización del MTA | pktcSigDev R0Cadence | Campo definido por el usuario en el que cada bit representa una duración de 100 ms (6 s en total).<br>1 = señal acústica activa, 0 = silencio.<br>Se utilizan 64 bits para la representación; 60 bits MSB para la cadencia de tono. El bit 61 se utiliza para representar la repetibilidad (cuando está puesto a CERO) y la no repetibilidad (cuando está puesto a UNO). Los otros tres bits se reservan para uso futuro y en la actualidad se ponen a 000. |
| Cadencia R6 | Campo de bits | W, opcional | R/W | MIB de señalización del MTA | pktcSigDev R6Cadence | Campo de bits definido por el usuario en el que cada bit representa una duración de 100 ms (6 s en total).<br>1 = señal acústica activa, 0 = silencio.<br>Se utilizan 64 bits para la representación; 60 bits MSB para la cadencia de tono. El bit 61 se utiliza para representar la repetibilidad (cuando está puesto a CERO) y la no repetibilidad (cuando está puesto a UNO). Los otros tres bits se reservan para uso futuro y en la actualidad se ponen a 000. |

## Cuadro 12/J.167 – Servicio a nivel de dispositivo

| Atributo | Sintaxis | Acceso a la configuración | Acceso al SNMP | Fichero MIB | Objeto | Comentarios pktcDevEvSyslo |
|---|---|---|---|---|---|---|
| Cadencia R7 | Campo de bits | W, opcional | R/W | MIB de señalización del MTA | pktcSigDevR7Cadence | Campo de bits definido por el usuario en el que cada bit representa una duración de 100 ms (6 s en total).<br>1 = señal acústica activa, 0 = silencio.<br>Se utilizan 64 bits para la representación; 60 bits MSB para la cadencia de tono. El bit 61 se utiliza para representar la repetibilidad (cuando está puesto a CERO) y la no repetibilidad (cuando está puesto a UNO). Los otros tres bits se reservan para uso futuro y en la actualidad se ponen a 000. |
| Cadencia R1 | Campo de bits | W, opcional | R/W | MIB de señalización del MTA | pktcSigDevR1Cadence | Campo definido por el usuario en el que cada bit (bit menos significativo) representa una duración de 100 ms (6 s en total).<br>1 = señal acústica activa, 0 = silencio.<br>Se utilizan 64 bits para la representación; 60 bits MSB para la cadencia de tono. El bit 61 se utiliza para representar la repetibilidad (cuando está puesto a CERO) y la no repetibilidad (cuando está puesto a UNO). Los otros tres bits se reservan para uso futuro y en la actualidad se ponen a 000. |
| Cadencia R2 | Campo de bits | W, opcional | R/W | MIB de señalización del MTA | pktcSigDevR2Cadence | Campo de bits definido por el usuario en el que cada bit (bit menos significativo) representa una duración de 100 ms (6 s en total).<br>1 = señal acústica activa, 0 = silencio.<br>Se utilizan 64 bits para la representación; 60 bits MSB para la cadencia de tono. El bit 61 se utiliza para representar la repetibilidad (cuando está puesto a CERO) y la no repetibilidad (cuando está puesto a UNO). Los otros tres bits se reservan para uso futuro y en la actualidad se ponen a 000. |

## Cuadro 12/J.167 – Servicio a nivel de dispositivo

| Atributo | Sintaxis | Acceso a la configuración | Acceso al SNMP | Fichero MIB | Objeto | Comentarios pktcDevEvSyslo |
|---|---|---|---|---|---|---|
| Cadencia R3 | Campo de bits | W, opcional | R/W | MIB de señalización del MTA | pktcSigDevR3Cadence | Campo definido por el usuario en el que cada bit (bit menos significativo) representa una duración de 100 ms (6 s en total).<br>1 = señal acústica activa, 0 = silencio.<br>Se utilizan 64 bits para la representación; 60 bits MSB para la cadencia de tono. El bit 61 se utiliza para representar la repetibilidad (cuando está puesto a CERO) y la no repetibilidad (cuando está puesto a UNO). Los otros tres bits se reservan para uso futuro y en la actualidad se ponen a 000. |
| Cadencia R4 | Campo de bits | W, opcional | R/W | MIB de señalización del MTA | pktcSigDevR4Cadence | Campo definido por el usuario en el que cada bit (bit menos significativo) representa una duración de 100 ms (6 s en total).<br>1 = señal acústica activa, 0 = silencio.<br>Se utilizan 64 bits para la representación; 60 bits MSB para la cadencia de tono. El bit 61 se utiliza para representar la repetibilidad (cuando está puesto a CERO) y la no repetibilidad (cuando está puesto a UNO). Los otros tres bits se reservan para uso futuro y en la actualidad se ponen a 000. |
| Cadencia R5 | Campo de bits | W, opcional | R/W | MIB de señalización del MTA | pktcSigDevR5Cadence | Campo definido por el usuario en el que cada bit (bit menos significativo) representa una duración de 100 ms (6 s en total).<br>1 = señal acústica activa, 0 = silencio.<br>Se utilizan 64 bits para la representación; 60 bits MSB para la cadencia de tono. El bit 61 se utiliza para representar la repetibilidad (cuando está puesto a CERO) y la no repetibilidad (cuando está puesto a UNO). Los otros tres bits se reservan para uso futuro y en la actualidad se ponen a 000. |

## Cuadro 12/J.167 – Servicio a nivel de dispositivo

| Atributo | Sintaxis | Acceso a la configuración | Acceso al SNMP | Fichero MIB | Objeto | Comentarios pktcDevEvSyslo |
|---|---|---|---|---|---|---|
| Cadencia Rg | Campo de bits | W, opcional | R/W | MIB de señalización del MTA | pktcSigDevRgCadence | Campo definido por el usuario en el que cada bit (bit menos significativo) representa una duración de 100 ms (6 s en total).<br>1 = señal acústica activa, 0 = silencio.<br>Se utilizan 64 bits para la representación; 60 bits MSB para la cadencia de tono. El bit 61 se utiliza para representar la repetibilidad (cuando está puesto a CERO) y la no repetibilidad (cuando está puesto a UNO). Los otros tres bits se reservan para uso futuro y en la actualidad se ponen a 000. |
| Cadencia Rt | Campo de bits | W, opcional | R/W | MIB de señalización del MTA | pktcSigDevRtCadence | Campo definido por el usuario en el que cada bit (bit menos significativo) representa una duración de 100 ms (6 s en total).<br>1 = señal acústica activa, 0 = silencio.<br>Se utilizan 64 bits para la representación; 60 bits MSB para la cadencia de tono. El bit 61 se utiliza para representar la repetibilidad (cuando está puesto a CERO) y la no repetibilidad (cuando está puesto a UNO). Los otros tres bits se reservan para uso futuro y en la actualidad se ponen a 000. |
| Cadencia Rs | Campo de bits | W, opcional | R/W | MIB de señalización del MTA | pktcSigDevRsCadence | Campo definido por el usuario en el que cada bit (bit menos significativo) representa una duración de 100 ms (6 s en total).<br>1 = señal acústica activa, 0 = silencio.<br>Se utilizan 64 bits para la representación; 60 bits MSB para la cadencia de tono. El bit 61 se utiliza para representar la repetibilidad (cuando está puesto a CERO) y la no repetibilidad (cuando está puesto a UNO). Los otros tres bits se reservan para uso futuro y en la actualidad se ponen a 000. |

### 9.1.3 Datos de configuración por punto extremo

Para una información más detallada a propósito de estos atributos y de sus valores por defecto, véanse la Recomendación relativa a la MIB de la NCS (Rec. UIT-T J.166), la relativa a la especificación de la NCS (Rec. UIT-T J.162), la relativa a la especificación de la seguridad (Rec. UIT-T J.170) y la relativa a la MIB del MTA (Rec. UIT-T J.166) (véase el cuadro 13).

- El MTA envía al KDC el certificado MTA/CMS, el FQDN del MTA y el ID del CMS. El KDC devuelve al MTA un "tique Kerberos" que dice "este MTA está asignado a este CMS".
- El certificado del proveedor del servicio de telefonía valida el certificado de telefonía del MTA.
- Si dos puntos extremos diferentes comparten el mismo dominio Kerberos y el mismo FQDN de CMS, DEBEN ser idénticos los cuatro atributos siguientes: periodo de gracia de PKINIT, lista de nombres del KDC, certificado de telefonía del MTA y certificado del proveedor del servicio de telefonía.

**Cuadro 13/J.167 – Configuración por punto extremo**

| Atributo | Sintaxis | Acceso a la configuración | Acceso al SNMP | Fichero MIB | Objeto | Comentarios |
|---|---|---|---|---|---|---|
| Estado administrativo del puerto | ENUM | W, opcional | R/W | IF-MIB (RFC 2863) | ifAdmin Status | Estado administrativo del puerto al que el operador puede acceder para habilitar o inhabilitar el servicio al mismo. El estado administrativo se puede utilizar para inhabilitar el acceso al puerto del usuario sin desaprovisionar al abonado. Valores permitidos para este atributo son:<br>up(1) o down(2).<br>Para el acceso al SNMP ifAdminStatus figuran en el ifTable de MIB-II. |
| Nombre de servidor de gestión de llamadas | Cadena | W, requerido | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig CallAgentId | Este atributo es una cadena que indica el nombre del CMS asignado al punto extremo. El nombre del agente de llamada después del carácter '@' DEBE ser un nombre de dominio plenamente calificado y DEBE tener una fila conceptual correspondiente en el cuadro pktcMtaDevCms. Se supone el soporte del DNS para soportar múltiples CMS como se describe en la especificación relativa a la NCS. |
| Puerto UDP de servidor de gestión de llamada | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig CallAgent UdpPort | Puerto UDP para el CMS. |

## Cuadro 13/J.167 – Configuración por punto extremo

| Atributo | Sintaxis | Acceso a la configuración | Acceso al SNMP | Fichero MIB | Objeto | Comentarios |
|---|---|---|---|---|---|---|
| Temporización de marcación parcial | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig PartialDialTO | Valor en segundos de la temporización de la marcación parcial. |
| Temporización de marcación crítica | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig CriticalDialTO | Valor en segundos de la temporización de la marcación crítica. |
| Temporización del tono de ocupado | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig BusyToneTO | Valor en segundos de la temporización del tono de ocupado. |
| Temporización del tono de marcación | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig DialToneTO | Valor en segundos de la temporización del tono de marcación. |
| Temporización de mensaje en espera | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig Message WaitingTO | Valor en segundos de la temporización de mensaje en espera. |
| Temporización del aviso de descolgado | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfigOff HookWarn ToneTO | Valor en segundos de la temporización del aviso de descolgado. |
| Temporización del tono de llamada | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig RingingTO | Valor en segundos de la temporización del tono de llamada. |
| Temporización del tono de llamada de retorno | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig RingBackTO | Valor en segundos de la temporización del tono de llamada de retorno. |
| Temporización del tono de volver a llamar | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig Reorder ToneTO | Valor en segundos de la temporización de tono de volver a llamar. |
| Temporización de marcación con tartamudeo | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig StutterDial ToneTO | Valor en segundos de la temporización de tono de marcación con tartamudeo. |
| TS Máximo | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfigTS Max | Contiene el tiempo máximo en segundos a partir del envío del datagrama inicial. |
| Max1 | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig Max1 | Umbral de error sospechoso para cada retransmisión de punto extremo. |
| Max2 | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig Max2 | Umbral de error de desconexión por cada retransmisión de punto extremo. |
| Habilitación de cola Max1 | Enum | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig Max1Q Enable | Habilita/inhabilita la operación de indagación de DNS Max1 cuando Max1 expira. |
| Habilitación de cola Max2 | Enum | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig Max2Q Enable | Habilita/inhabilita la operación de indagación de DNS Max2 cuando Max2 expira. |

**Cuadro 13/J.167 – Configuración por punto extremo**

| Atributo | Sintaxis | Acceso a la configuración | Acceso al SNMP | Fichero MIB | Objeto | Comentarios |
|---|---|---|---|---|---|---|
| MWD | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig MWD | Número de segundos de espera para empezar de nuevo tras recibir una orden de recomenzar. |
| Tdinit | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig Tdinit | Número de segundos de espera tras una desconexión. |
| TDMin | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig Tdmin | Número mínimo de segundos de espera tras una desconexión. |
| TDMax | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig Tdmax | Número máximo de segundos de espera tras una desconexión. |
| RTO Max | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig RtoMax | Número máximo de segundos del temporizador de retransmisión. |
| RTO Init | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig RtoInit | Valor inicial del temporizador de retransmisión. |
| Larga duración Mantener vivo | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig LongDuration KeepAlive | Temporización en minutos para el envío de mensajes de notificación de llamada de larga duración. |
| Thist | Entero | W | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfig Thist | Periodo de temporización en segundos antes de declarar ausencia de respuesta. |
| Reposo máximo de espera de llamada | Entero | W, opcional | R/W | MIB de señalización del MTA | pktcNcsEnd PntConfigCall Waiting MaxRep | Este objeto contiene el número máximo de repeticiones de llamada en espera que efectuará el MTA a partir de una única petición CMS. Se utilizará un valor cero (0), cuando el CMS invoque una repetición de reproducción. |
| Retardo de llamada en espera | Entero | W, opcional | R/W | MIB-IF (RFC 2863) | pktcNcsEnd PntConfigCall WaitingDelay | Este objeto contiene el retardo entre repeticiones de la llamada en espera que el MTA efectuará a partir de una única petición CMS. |

### 9.1.4 Datos de configuración por sector

Puede encontrarse en la MIB del MTA (J.166) información más detallada relativa a estos atributos y a sus valores por defecto. Puede encontrarse en la Recomendación relativa a la seguridad (J.170) más información sobre la utilización de los sectores Kerberos. DEBE haber al menos una fila conceptual en el cuadro pktcMtaDevRealm para establecer el servicio una vez completada la configuración. Estos parámetros de configuración son opcionales dentro del fichero de definición de la configuración, pero de estar incluidos en él, este fichero DEBE contener al menos un nombre de sector para que pueda instanciarse adecuadamente el cuadro. Puede haber más de un conjunto de entradas si se soportan múltiples sectores.

**Cuadro 14/J.167 – Datos de configuración por sector**

| Atributo | Sintaxis | Acceso | Acceso SNMP | Fichero MIB | Objeto | Comentarios |
|---|---|---|---|---|---|---|
| Periodo de gracia Pkinit | Entero | W, opcional | R/W | MIB del dispositivo MTA | pktcMtaDevRealm PkinitGracePeriod | Para realizar la gestión de claves IPSec con un CMS, el MTA DEBE obtener un nuevo tique Kerberos (con intercambio PKINIT), varios minutos antes de la expiración del antiguo tique. El valor mínimo permisible es de 15 minutos. El valor por defecto es de 30 minutos. Este parámetro también PUEDE utilizarse con otras aplicaciones kerberizadas. |
| Periodo de gracia TGS | Entero | W, opcional | R/W | MIB del dispositivo MTA | pktcMtaDevRealm TgsGracePeriod | Cuando la implementación del MTA utiliza los mensajes Kerberos petición TGS/respuesta TGS para realizar la gestión de claves de IPSec con el CMS, el MTA DEBE obtener un nuevo tique de servicio para el CMS (con una petición TGS) varios minutos antes de que expire el antiguo tique. El valor mínimo permisible es de 1 minuto. El valor por defecto es de 10 minutos. Este parámetro también PUEDE utilizarse con otras aplicaciones kerberizadas. |
| Nombre de organización de sector | Entero | W, requerido | R/W | MIB del dispositivo MTA | pktcMtaDevRealm OrgName | El valor del atributo nombre de organización X.500 en el sujeto de certificado de proveedor de servicio. |
| Expiración máxima del temporizador de creación de claves no solicitada | Entero | W, opcional | R/W | MIB del dispositivo MTA | pktcMtaDevRealm UnsolicitedKeyMax Timeout | Esta expiración del temporizador se aplica únicamente cuando el MTA ha iniciado la gestión de claves. La expiración máxima temporizador es el valor que no puede superarse en el algoritmo de retroceso exponencial. |
| Expiración nominal del temporizador de creación de claves no solicitada | Entero | W, opcional | R/W | MIB del dispositivo MTA | pktcMtaDevRealm UnsolicitedKeyNom Timeout | Esta expiración del temporizador se aplica únicamente cuando el MTA ha iniciado la gestión de claves. Normalmente se trata del tiempo medio que un mensaje tarda en ir y volver entre el MTA y el KDC. |
| Número máximo de reintentos de creación de claves no solicitada | Entero | W, opcional | R/W | MIB del dispositivo MTA | pktcMtaDevRealm UnsolicitedKeyMax Retries | Es el número máximo de reintentos antes de que el MTA deje de intentar el establecimiento de una asociación de seguridad |

### 9.1.5 Datos de configuración por CMS

Pueden encontrarse en la MIB del MTA (J.166) información más detallada sobre estos atributos y sus valores por defecto. DEBE haber al menos una fila conceptual en el cuadro pktcDevCms para establecer un servicio, una vez completada la configuración. Estos parámetros de configuración son facultativos en el fichero de definición de la configuración, pero de estar incluidos en él, este fichero DEBE identificar al menos un CMS y su correspondiente nombre de sector Kerberos. Puede haber más de un conjunto de entradas si se soportan múltiples CMS.

De conformidad con la Rec. UIT-T J.170, la seguridad de la señalización IPSEC debe estar controlada por el operador dependiendo de la instalación y de las condiciones de funcionamiento. Puesto que la asociación de seguridad IPSec se establece entre un MTA y un CMS, el control de habilitación/inhabilitación de IPSec también debe hacerse para cada CMS. La habilitación/inhabilitación de la seguridad de señalización IPSec DEBE estar definida únicamente por la información contenida en el fichero de definición de la configuración del MTA, cuando éste se descarga; y la habilitación/inhabilitación de alternación DEBE efectuarse únicamente como resultado de la puesta a cero del MTA.

Pueden encontrarse más detalles sobre el objeto MIB que controla la habilitación/inhabilitación de IPSec en la MIB MTA (J.166).

**Cuadro 15/J.167 – Datos de configuración por CMS**

| Atributo | Sintaxis | Acceso | Acceso SNMP | Fichero MIB | Object | Comentarios |
|---|---|---|---|---|---|---|
| Nombre de sector Kerberos | Cadena | W, requerido (Nota) | R/W | MIB del dispositivo MTA | pktcMtaDevCms KerbRealmName | El nombre del sector Kerberos asociado es el nombre del sector Kerberos correspondiente en los datos de configuración por sector. |
| Desvío de reloj máximo de CMS | Entero | W, opcional | R/W | MIB del dispositivo MTA | pktcMtaDevCms MaxClockSkew | Es el desvío de reloj máximo permisible entre el MTA y el CMS. |
| Expiración del temporizador de clave solicitada CMS | Entero | W, opcional | R/W | MIB del dispositivo MTA | pktcMtaDevCms SolicitedKey Timeout | Esta expiración del temporizador se aplica únicamente cuando el CMS ha iniciado la gestión de claves (mediante un mensaje activación o reclave). Es el periodo durante el cual el MTA salvará un nonce (dentro del campo número de secuencia) del mensaje petición AP enviado y esperará a la correspondencia de la respuesta AP que envíe el CMS. |
| Expiración máxima del temporizador de clave no solicitada | Entero | W, opcional | R/W | MIB del dispositivo MTA | pktcMtaDevCms UnsolicitedKey MaxTimeout | Esta expiración del temporizador se aplica únicamente cuando el MTA ha iniciado la gestión de claves. La expiración máxima del temporizador es el valor que no puede excederse en el algoritmo de retroceso exponencial. |
| Expiración nominal del temporizador de clave no solicitada | Entero | W, opcional | R/W | MIB del dispositivo MTA | pktcMtaDevCms UnsolicitedKey NomTimeout | Esta expiración del temporizador se aplica únicamente cuando el MTA ha iniciado la gestión de claves. Normalmente se trata del tiempo medio que tarda el mensaje en ir y volver del MTA CMS. |
| Número máximo de reintentos de clave no solicitada | Entero | W, opcional | R/W | MIB del dispositivo MTA | pktcMtaDevCms UnsolicitedKey MaxRetries | Es el número máximo de reintentos antes de que el MTA deje de intentar establecer una asociación de seguridad. |
| Control IPSec | Entero | W, opcional | R/O | MIB del dispositivo MTA | pktcMtaDevCms IpsecCtrl | Control IPSec de cada CMS: controla el establecimiento IPSec y la gestión de claves relacionada con IPSec. |
| NOTA – Si cualquiera de los datos del cuadro de datos por CMS está incluido en el fichero definición de la configuración, DEBE incluirse esta entrada. | | | | | | |

### 9.1.6 Exclusión de objetos MIB del fichero definición de la configuración

Los siguientes objetos MIB NO DEBEN enviarse en el fichero definición de la configuración, pues los valores de estos objetos pueden ser definidos únicamente por el MTA o por las opciones de DHCP durante la configuración. Si el MTA recibe los siguientes objetos MIB en su fichero definición de la configuración, DEBE ignorar el objeto y enviar un informe "paso con aviso" e introducirlo en el cuadro de OID erróneos.

- PktcMtaDevSnmpEntity
- PktcMtaDevProvKerbRealmName
- PktcMtaDevFqdn
- PktcMtaDevSerialNumber
- PktcMtaDevMacAddress
- PktcMtaDevEndPntCount
- PktcMtaDevTypeIdentifier
- PktcEnNcsEndPntQuarantineState
- PktcEnNcsEndPntHookState
- pktcEnEndPntInfoTable
- pktcDevEventDescrEnterprise
- pktcDevEventDescrFacility
- pktcDevEventDescrText
- pktcDevEvLogIndex
- pktcDevEvLogTime
- pktcDevEvLogLevel
- pktcDevEvLogId
- pktcDevEvLogText
- pktcDevEvLogEndpointName
- pktcDevEvLogType
- pktcDevEvLogTargetInfo
- pktcDevEvLogCorrelationId
- pktcMtaDevProvConfigKey

NOTA – Para las entradas Syslog, específicamente los objetos MIB "pktcDevEvSyslogAddressType" y "pktcDevEvSyslogAddress", el MTA DEBE validar el 'tipo' proporcionado (o almacenado) con la 'dirección Syslog' proporcionada (o almacenada). Si son incompatibles, DEBE ignorar estas entradas del fichero de definición de la configuración y crear un informe 'paso con aviso' e introducir el error en el cuadro de OID erróneos.

## 10 Capacidades de dispositivo MTA

La cadena de capacidades del MTA se proporciona al servidor de aprovisionamiento en el código de opción 60 (Identificador de clase de vendedor) para que el fondo de oficina pueda diferenciar entre los distintos MTA durante el proceso de aprovisionamiento. La aplicación de aprovisionamiento tiene la posibilidad de utilizar o no la información de capacidades.

La cadena de capacidades está codificada como una cadena ASCII que contiene la Información de capacidades en formato Tipo/Longitud/Valor (TLV).

Por ejemplo, la codificación ASCII de los dos primeros TLV (IPCablecom con Versión 1.0 y número de puntos extremos de telefonía = 2) de un MTA sería 05nn0101020102. Cabe señalar que se necesitan muchos más TLV para un MTA IPCablecom y que el campo "nn" contendrá la longitud de todos los TLV. Este ejemplo muestra sólo dos TLV para mayor sencillez.

El campo "valor" describe las capacidades de un módem específico, es decir, la limitación de características concretas o número de características que el módem puede soportar dependiendo de la implementación. Este campo está compuesto por un número de campos TLV encapsulados. Los subtipos encapsulados definen las capacidades específicas del MTA. Nótese que los campos subtipo definidos sólo son válidos dentro de la cadena de fijación de la configuración de capacidades encapsuladas.

| Tipo | Longitud | Valor |
|---|---|---|
| 5 | n | |

El conjunto de campos encapsulados posibles se describe a continuación.

El MTA DEBE enviar la cadena de capacidades en la opción 60 de la petición DESCUBRIMIENTO de DHCP.

### 10.1 Versión IPCablecom

Este TLV DEBE proporcionarse en la cadena de capacidades.

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.1 | 1 | 0 | PacketCable 1.0 | NINGUNO |
| | | 1 | PacketCable 1.5 | |

### 10.2 Número de puntos extremos de telefonía

Este TLV de subtipo 5.2 (número de puntos extremos de telefonía) DEBE proporcionarse en la cadena de capacidades.

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.2 | 1 | n | Número de puntos extremos | NINGUNO |

### 10.3 Soporte de TGT

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.3 | 1 | 0 | 0: No | 0 |
| | | 1 | 1: Sí | |

### 10.4 Soporte del método de acceso al fichero de descarga HTTP

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.4 | 1 | 0 | 0: No | 0 |
| | | 1 | 1: Sí | |

### 10.5 Soporte de la notificación SYSLOG de evento MTA24

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.5 | 1 | 0 | 0: No | 1 |
| | | 1 | 1: Sí | |

### 10.6 Soporte del flujo de servicio NCS

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.6 | 1 | No definido | Reservado | No definido |

El subtipo 5.6, que anteriormente se utilizaba para indicar el soporte de la funcionalidad de flujo de servicio NCS, está en la actualidad sin definir y se reserva para uso futuro.

### 10.7 Soporte de línea primaria

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.7 | 1 | 0 | 0: No | 0 |
| | | 1 | 1: Sí | |

### 10.8 Tipo(s) de TLV específico(s) del vendedor

Este TLV puede proporcionarse en la cadena de capacidades, si el MTA requiere un procesamiento específico de los tipos TLV específicos del vendedor.

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.8 | n | {secuencia de bytes}: | Un tipo por byte | 43 |

El subtipo 5.8, que anteriormente se utilizaba para indicar el soporte de los TLV específicos del vendedor por parte de los MTA, ha quedado obsoleto y el subtipo (5.8) se reserva para uso futuro. Los MTA no DEBEN utilizarlo.

### 10.9 Soporte de almacenamiento de información de tique/tique NVRAM

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.9 | 1 | 0 | 0: No | 1 |
| | | 1 | 1: Sí | |

### 10.10 Soporte de informe de evento de aprovisionamiento

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.10 | 1 | 0 | 0: No | 1 |
| | | 1 | 1: Sí | |

### 10.11 CÓDEC(s) soportado(s)

Este TLV DEBE proporcionarse en la cadena de capacidades.

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.11 | n | {secuencia de bytes} | un ID por byte | NINGUNO |

El ID de CÓDEC es el valor representado por el tipo enumerado del CONVENIO TEXTUAL "PktcCodecType" de la MIB de MTA:

1: otro,

2: desconocido,

3: G.729,

4: reservado,

5: G.729E,

6: PCMU,

7: G.726-32,

8: G.728,

9: PCMA,

10: G.726-16,

11: G.726-24,

12: G.726-40,

13: iLBC,

14: BV16,

15: evento de teléfono.

Evento de teléfono representa los eventos DTMF de RFC 2833. Puede encontrarse más información al respecto en UIT-T J.161.

### 10.12 Soporte de supresión de silencios

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.12 | 1 | 0 | 0: No | 0 |
| | | 1 | 1: Sí | |

### 10.13 Soporte de compensación de eco

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.13 | 1 | 0 | 0: No | 0 |
| | | 1 | 1: Sí | |

### 10.14 Soporte de RSVP

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.14 | 1 | No definido | Reservado para uso futuro | No definido |

El subtipo 5.14, que se utilizaba anteriormente para indicar el soporte de RSVP, queda en la actualidad sin definir y se reserva para uso futuro.

### 10.15 Soporte de UGS-AD

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.15 | 1 | 0 | 0: No | 0 |
| | | 1 | 1: Sí | |

### 10.16 Número de inicio "ifIndex" del MTA en "ifTable"

Este TLV contiene el valor del "ifIndex" para la primera interfaz de telefonía MTA del cuadro MIB "ifTable". El TLV DEBE proporcionarse en la cadena de capacidades.

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.16 | 1 | n | primera interfaz MTA | 9 |

### 10.17 Soporte de registro cronológico del flujo de aprovisionamiento

Esta capacidad se fija a un valor dependiente del soporte de la capacidad de registro cronológico del flujo de aprovisionamiento (de conformidad con 5.4.3).

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.17 | 1 | 0 | 0: No | 0 |
| | | 1 | 1: Sí | |

### 10.18 Flujos de aprovisionamiento soportados

Un MTA DEBE incluir este TLV de subtipo 5.18 (flujos de aprovisionamiento soportados) en la cadena de capacidades. Este TLV indica los flujos de aprovisionamiento que soporta el MTA (básico, híbrido y seguro). Contiene una máscara de bits que indica todos los flujos de configuración que soporta el MTA.

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.18 | 2 | {máscara de bits} | Véase *infra* | NINGUNO |

El campo Valor es un entero de 16 bits sin signo codificado en el orden de bytes de red. Cada bit representa un flujo de aprovisionamiento específico. Si un bit se pone a 1, el MTA soporta dicho flujo. Si un bit está puesto a 0 (cero), el MTA no lo soporta.

Asignación de bits:

Bit 0 – Flujo seguro (flujo de configuración plenamente seguro)

Bit 1 – Flujo híbrido

Bit 2 – Flujo básico

El MTA DEBE poner todos los bits no utilizados de la máscara de bits a 0. El MTA DEBE poner el bit 0 del TLV a 1 para indicar que se soporta el flujo seguro. El MTA DEBE fijar los bits a 1 y 2 del TLV para indicar si se soportan los flujos básico e híbrido. Por ejemplo, si un MTA soporta los flujos de aprovisionamiento seguro y básico, el valor entero de la máscara es 0x0005, y la capacidad se codificará en la opción 60 como la siguiente secuencia de octetos (en notación hexadecimal): 12 02 00 05.

Para garantizar la compatibilidad con versiones anteriores antes de la introducción de los flujos básico e híbrido, la ausencia de este TLV indica que el MTA sólo soporta el flujo seguro.

### 10.19 Soporte de la versión T38

Un MTA DEBE incluir este TLV de subtipo 5.19 (soporte de versión T38) en la cadena de capacidades. Este TLV indica la versión de T.38 que soporta el MTA. Pueden encontrarse más detalles al respecto en la Rec. UIT-T J.161.

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.19 | 1 | 0 | 0: No soportado | 1 |
| | | 1 | 1: Versión cero | |
| | | 2 | 2: Versión uno | |
| | | 3 | 3: Versión dos | |
| | | 4 | 4: Versión tres | |

### 10.20 Soporte de corrección de errores T38

Un MTA DEBE incluir este TLV de subtipo 5.20 (soporte de corrección de errores T38) en la cadena de capacidades. Este TLV indica el tipo de corrección de errores que soporta el MTA para T.38. Pueden encontrarse más detalles al respecto en la Rec. UIT-T J.161.

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.20 | 1 | 0 | 0: Ninguno | 1 |
| | | 1 | 1: Redundancia | |
| | | 2 | 2: FEC | |

Si se soporta FEC, quiere decir que también se soporta la redundancia. Pueden encontrarse más detalles al respecto en la Rec. UIT-T J.161.

### 10.21 Soporte DTMF de RFC 2833

Un MTA DEBE incluir este TLV de subtipo 5.21 (soporte de DTMF de RFC 2833) en la cadena de capacidades. Este TLV indica que se soporta la retransmisión DTMF de RFC 2833. Pueden encontrarse más detalles al respecto en la Rec. UIT-T J.161.

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.21 | 1 | 0 | 0: No | 1 |
| | | 1 | 1: Sí | |

### 10.22 Soporte de métrica vocal

Un MTA DEBE incluir este TLV de subtipo 5.22 (soporte de métrica vocal) en la cadena de capacidades. Este TLV indica que se soporta la métrica vocal como se define en RFC 3611.

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.22 | 1 | 0 | 0: No | 1 |
| | | 1 | 1: Sí | |

### 10.23 Soporte de la MIB del dispositivo

El MTA DEBE incluir este TLV de subtipo 5.23 (soporte de la MIB del dispositivo) en la cadena de capacidades. Este TLV indica las distintas MIB que soporta el MTA.

| Tipo | Longitud | Valores | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.23 | n | {secuencia de bytes} | Soporte de MIB codificado como pares 'longitud-valor' | NINGUNO |

Los pares 'longitud-valor' se definen de la siguiente manera:

[L1] [OCTETO-1] [OCTETO-2][OCTETO-3] …[OCTETO-L1],

[L2] [OCTETO-1] [OCTETO-2][OCTETO-3] …[OCTETO-L2]

(y otros pares longitud-valor que se consideren adecuados.)

donde:

'L1' y 'L2' indican las longitudes.

El primer OCTETO (OCTETO-1) siempre representa la organización responsable de la MIB (por ejemplo, CableLabs, IETF etc.).

Los demás OCTETOS se sitúan siempre en el orden de bytes de red para formar una cadena de bits en la que cada uno de ellos representa una MIB concreta. Poner un bit (a un valor de 1) indica que se soporta dicha MIB, y ponerlo (a un valor de 0) indica que no se soporta tal MIB.

Los MTA NO DEBEN utilizar 'asignaciones reservadas' a menos que estén definidas por IPCablecom o asignadas como 'específicas del vendedor'.

### 10.23.1 Asignaciones de organización responsable

El OCTETO-1 del par 'longitud-valor' indica la organización responsable de la MIB, y las asignaciones son las siguientes:

| Asignación | Indicador de organización |
|---|---|
| 0 | CableLabs |
| 1 | IETF |
| 2-9 | *reservado* |
| 10-63 | *específico del vendedor* |

NOTA – Los dos bits de orden superior de OCTETO-1 se reservan, lo que deja abiertas 64 posibilidades.

### 10.23.2 MIB de CableLabs

Para las MIB de CableLabs (OCTETO-1 = 0) la máscara de bits se define de la siguiente manera:

| | |
|---|---|
| Bit 0 | MIB del MTA PacketCable 1.5. |
| Bit 1 | MIB de señalización PacketCable 1.5. |
| Bit 2 | MIB de evento de gestión PacketCable 1.5. |
| Bit 3 | MIB de extensión de MTA PacketCable 1.5. |
| Bit 4 | MIB de extensión de señalización PacketCable 1.5. |
| Bit 5 | MIB de extensión MEM PacketCable 1.5. |
| Bit 6 | *reservado* |
| Bit 7 | *reservado* |

Situándose los bits de la siguiente manera:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |

Dado que sólo se utiliza en la actualidad un octeto para la máscara de bits, la longitud de este par longitud-valor DEBE ser dos (uno para el indicador de organización y para la máscara de bits, respectivamente).

### 10.23.3 MIB de IETF

Para las MIB de las RFC de IETF (OCTETO-1 = 1) la máscara de se define de la siguiente manera:

| | |
|---|---|
| Bit 0 | MIB de MTA |
| Bit 1 | MIB de señalización |
| Bit 2 | MIB de evento de gestión |
| Bit 3 | *reservado* |
| Bit 4 | *reservado* |
| Bit 5 | *reservado* |
| Bit 6 | *reservado* |
| Bit 7 | *reservado* |

Dado que en la actualidad sólo se utiliza un octeto para la máscara de bits, la longitud de este par longitud-valor DEBE ser dos (uno para el indicador de organización y otro para la máscara de bits, respectivamente).

**Ejemplo**

Para un MTA que soporta todos las MIB definidas por IETF (MTA, señalización y MEM) y todas las MIB de extensión definidas por IPCablecom 1.5 (extensión de MTA, extensión de señalización y extensión MEM), esta subopción se codificará (en notación hexadecimal) de la siguiente manera (como instantánea de la opción 60):

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| … | … | 17 | 06 | 02 | 00 | 38 | 02 | 00 | 07 | … | … |

NOTA – De conformidad con el presente documento, ninguno de los proyectos propuestos por IETF tiene la condición de RFC y esta referencia se ha utilizado únicamente como ejemplo.

### 10.24 Soporte de múltiples concesiones por intervalo

Un MTA DEBE incluir este TLV de subtipo 5.24 (soporte de múltiples concesiones por intervalo) en la cadena de capacidades. Este TLV indica el soporte de múltiples concesiones por intervalo. Pueden encontrarse más detalles al respecto en la Rec. UIT-T J.163.

| Tipo | Longitud | Valor | Observaciones | Valor por defecto |
|---|---|---|---|---|
| 5.24 | 1 | 0 | 0: No | 0 |
| | | 1 | 1: Sí | |

## 11 Especificación del receptor de notificaciones SNMP TLV-38

Este TLV-38 de IPCablecom especifica una o más estaciones de gestión de red que deben recibir notificaciones del MTA (MTA25 o H-MTA-25 o B-MTA-25 y posconfiguración, de ser necesario). Si TLV-38 y sus subTLV definidos en esta cláusula contienen un valor incorrecto en el valor 'longitud', el MTA DEBE rechazar el fichero de definición de la configuración e informar de un error 'fallo en el fichero de configuración'. Si TLV-38 contiene subtipos con valores erróneos, el MTA DEBE ajustarse a los requisitos que se especifican a continuación para cada subTLV.

Además, si el MTA se encuentra con subTLV desconocidos dentro de TLV-38, DEBE:

- asumir un tamaño del campo longitud de 1 byte para tal TLV,
- ignorar el subTLV y continuar con el procesamiento, y
- enviar un informe de estado de aprovisionamiento de "paso con aviso" e introducirlo en el cuadro de OID erróneos.

| Tipo | Longitud | Valor |
|---|---|---|
| 38 | N | Compuesto (contiene subTLV) |

A menos que se especifique o se configure de otra manera, el MTA DEBE enviar notificaciones al sistema de configuración por defecto (definido en la subopción 3 de la opción 122 de DHCP).

### 11.1 SubTLV de TLV-38

#### 11.1.1 Dirección IP de receptor de notificación SNMP

Este subTLV especifica la dirección IP del receptor de la notificación.

| Tipo | Longitud | Valor |
|---|---|---|
| 38.1 | 4 | 4 bytes de una dirección IPv4 en orden de bytes de red |

Si TLV-38 está presente en el fichero de definición de la configuración y no se encuentra el subTLV 38.1, el MTA DEBE ignorar el TLV-38 y proseguir con el procesamiento del fichero de definición de la configuración, y DEBE enviar un informe de estado de configuración de paso con aviso e introducir el error en el cuadro de OID erróneos (pktcMtaDevErrorOidsTable).

### 11.1.2 Número de puerto UDP del receptor de notificación SNMP

Este subTLV especifica el número de puerto del receptor de notificación que ha de recibir las notificaciones.

| Tipo | Longitud | Valor |
|---|---|---|
| 38.2 | 2 | Número de puerto UDP |

Si TLV-38 está presente y está ausente el subTLV 38.2, se DEBE utilizar un valor por defecto de 162.

### 11.1.3 Tipo de receptor de notificaciones SNMP

Este subTLV especifica el tipo de receptor de notificaciones SNMP, que es el tipo de notificaciones SNMP que el MTA DEBE enviar al receptor de notificaciones SNMP asociado.

| Tipo | Longitud | Valor |
|---|---|---|
| 38.3 | 2 | 1: Trampa SNMPv1 en un paquete SNMPv1 |
| | | 2: Trampa SNMPv2c en un paquete SNMPv2c |
| | | 3: INFORME SNMP en un paquete SNMPv2c |
| | | 4: Trampa SNMP en un paquete SNMPv3 |
| | | 5: INFORME SNMP en un paquete SNMPv3 |

Si en el fichero de definición de la configuración está presente TLV-38, pero está ausente el subTLV 38.3, el MTA DEBE ignorar todo el TLV-38 y proseguir con el procesamiento de definición de la configuración y DEBE crear un informe paso con aviso e introducir el error en el cuadro de OID erróneos (pktcMtaDevErrorOidsTable). El MTA y el servidor de aprovisionamiento DEBEN soportar los valores 2 y 3 de tipo de notificación y PUEDEN soportar los valores 1, 4 ó 5 de los tipos de notificación del cuadro anterior. Si se recibe un valor de tipo de notificación que no se soporta o es no válido, el MTA DEBE ignorar todo el TLV-38 que contiene esta entrada y DEBE emitir un informe paso con aviso e introducirlo en el cuadro de OID erróneos (pktcMtaDevErrorOidsTable). Si se utilizan en los flujos de aprovisionamiento básico o híbrido los tipos de notificación 4 ó 5, se supone que la comunicación SNMPv3 se aplica de acuerdo con las recomendaciones SNMPv3 y queda fuera del alcance de esta Recomendación.

### 11.1.4 Expiración del temporizador del receptor de notificaciones SNMP

Este subTLV especifica el tiempo de espera antes de realizar un intento cuando el emisor de un INFORME SNMP no recibe un acuse de recibo. Cabe señalar que el número de intentos está definido en el subTLV 38.5.

| Tipo | Longitud | Valor |
|---|---|---|
| 38.4 | 2 | Tiempo en milisengundos |

Si en el fichero de configuración está presente el TLV-38, pero no lo está el subTLV 38.4, el MTA DEBE asumir un valor por defecto de 15 000 milisegundos, lo que corresponde a un valor por defecto de 1500 centésimas de segundo que se define para el objeto de MIB snmpTargetAddrTimeout (véase RFC 3413).

### 11.1.5 Reintentos del receptor de notificaciones SNMP

Este subTLV especifica el número máximo de veces que el MTA DEBE reintentar el envío de un mensaje INFORME SNMP, en caso de no recibir un acuse de recibo. Cabe señalar que el tiempo de espera entre cada reintento está definido por el subTLV 38.4.

| Tipo | Longitud | Valor |
|---|---|---|
| 38.5 | 2 | Número de reintentos |

De no estar presente, el MTA DEBE utilizar un valor por defecto de 3. El número máximo de reintentos que puede especificarse es 255.

### 11.1.6 Parámetros de filtrado del receptor de notificaciones SNMP

Este subTLV especifica el plan de filtrado para las notificaciones y contiene el OID raíz del subárbol de la MIB que define las notificaciones que han de enviarse al receptor de notificaciones. El MTA DEBE filtrar las notificaciones que se envían al gestor SNMP que se especifica en el subTLV 38.1 utilizando la información proporcionada. De no estar presente este subTLV, el MTA DEBE utilizar el valor OID por defecto para la raíz "iso".

| Tipo | Longitud | Valor |
|---|---|---|
| 38.6 | n | Filtro OID (Identificador de objeto en formato ASN.1) |

La codificación de este campo de valor TLV empieza con el tipo universal 6 ASN.1 (identificador de objeto) seguido del campo longitud ASN.1 y termina con el componente de identificador objeto codificado ASN.1.

### 11.1.7 Nombre de seguridad del receptor de notificaciones SNMPv3

Este subTLV especifica el nombre de seguridad SNMPv3 que hay que utilizar cuando se envían notificaciones SNMPv3. Este subTLV tan sólo se utiliza si el MTA soporta los tipos 4 y 5 de subTLV 38.3 (tipo de receptor de notificación). El MTA DEBE ignorar este subTLV 38.7 si en el fichero de definición de la configuración se incluye un tipo de receptor de notificación (subTLV 38.3) distinto de 4 ó 5.

Los siguientes requisitos se aplican a los MTA que soportan los valores 4 ó 5 de tipo de receptor de notificación en el subTLV 38.3:

- Si se omite este subTLV 38.7, la notificación SNMPv3 DEBE enviarse en el nivel de seguridad noAuthNoPriv utilizando el nombre de seguridad "@mtaconfig".
- Si se incluye este subTLV, el MTA verificará que el valor del nombre de seguridad existe en el motor SNMP con autoridad local sobre el MTA y creará una entrada para asociarlo posteriormente al motor con autoridad sobre el receptor de notificación (utilizando los niveles de seguridad y claves del nombre de seguridad existente). Si el nombre de seguridad de este subTLV no existe para el motor local, DEBE ignorarse el TLV-38 y el MTA DEBE generar un informe paso con aviso e introducir el error en el cuadro de OID erróneos (pktcMtaDevErrorOidsTable) para todo el TLV-38 y los subTLV asociados, que se ignoran.

| Tipo | Longitud | Valor |
|---|---|---|
| 38.7 | 2-26 | Nombre de seguridad |

## 11.2 Correspondencia de los campos TLV en los cuadros SNMP

En las siguientes cláusulas se detalla la correspondencia entre el TLV-38 "receptor de notificación SNMP de PacketCable" del fichero de definición de la configuración del MTA y los cuadros funcionales de SNMP.

Cada vez que se reciba un valor TLV-38, el MTA DEBE insertar entradas en los siguientes cuadros para crear la transmisión de TRAMPA o INFORME SNMP que se desea: snmpNotifyTable, snmpTargetAddrTable, snmpTargetAddrExtTable, snmpTargetParamsTable, snmpNotifyFilterProfileTable, snmpNotifyFilterTable, snmpCommunityTable, usmUserTable, vacmSecurityToGroupTable, vacmAccessTable y vacmViewTreeFamilyTable. Un MTA DEBE soportar un mínimo de diez elementos TLV-38 en un fichero de definición de la configuración.

### 11.2.1 Correspondencia de los campos TLV en las filas del cuadro SNMP creado

Los cuadros de esta cláusula muestran cómo los campos del elemento TLV del fichero de definición de la configuración (los rótulos entre <>) se sitúan en los cuadros SNMP.

A continuación se muestra la correspondencia entre los rótulos y los subTLV mismos:

<IP Address> TLV 38.1

<Port> – TLV 38.2

<Trap type> TLV 38.3

<Timeout> TLV 38.4

<Retries> TLV 38.5

<Filter OID> TLV 38.6

<Security Name> TLV 38.7

La creación de estas filas con valores o índices de columna que contienen el sufijo "n" en los siguientes cuadros indica que estas entradas se han creado con el (n – 1)ésimo TLV-38 encontrado en el fichero de definición de la configuración del MTA.

#### 11.2.1.1 snmpNotifyTable

Si hay presentes elementos TLV-38, independientemente de su número, el MTA DEBE crear dos filas con valores fijos como se muestra en el cuadro 16.

**Cuadro 16/J.167 – snmpNotifyTable**

| **snmpNotifyTable (RFC 3413, MIB DE NOTIFICACIÓN de SNMP)** | **Primera fila** | **Segunda fila** |
|---|---|---|
| Nombre de columna (* = Parte del índice) | Valor de la columna | Valor de la columna |
| * snmpNotifyName | "@mtaconfig_inform" | "@mtaconfig_trap" |
| snmpNotifyTag | "@mtaconfig_inform" | "@mtaconfig_trap" |
| snmpNotifyType | inform (2) | trap (1) |
| snmpNotifyStorageType | Transitorio | Transitorio |
| snmpNotifyRowStatus | active (1) | active (1) |

#### 11.2.1.2 snmpTargetAddrTable

Para cada elemento TLV-38 del fichero definición de la configuración, el MTA DEBE crear una fila según el cuadro 17.

**Cuadro 17/J.167 – snmpTargetAddrTable**

| **snmpTargetAddrTable (RFC 3413, MIB DE OBJETIVO SNMP)** | **Nueva fila** |
|---|---|
| Nombre de columna (* = Parte del índice) | Valor de la columna |
| * snmpTargetAddrName | "@mtaconfig_n" donde n va de 0 a m – 1, siendo m el número de receptores de notificación de elementos TLV del fichero definición de la configuración |
| snmpTargetAddrTDomain | snmpUDPDomain = snmpDomains.1 |
| snmpTargetAddrTAddress (dirección IP y puerto UDP del receptor de notificación) | OCTET STRING (6)<br>Octets 1-4: <IP Address><br>Octets 5-6: <Port> |
| snmpTargetAddrTimeout | <Timeout> from the TLV |
| snmpTargetAddrRetryCount | <Retries> from the TLV |
| snmpTargetAddrTagList | Si <Trap type> = 2<br>"@mtaconfig_trap"<br>Si <Trap type> = 3<br>"@mtaconfig_inform" |
| snmpTargetAddrParams | "@mtaconfig_n" ((Lo mismo que el valor snmpTargetAddrName value) |
| snmpTargetAddrStorageType | Transitorio |
| snmpTargetAddrRowStatus | active (1) |

#### 11.2.1.3 snmpTargetAddrExtTable

Para cada elemento TLV-38 del fichero definición de la configuración, el MTA DEBE crear una fila de acuerdo con el cuadro 18.

**Cuadro 18/J.167 – snmpTargetAddrExtTable**

| **snmpTargetAddrExtTable (RFC 3584, MIB DE COMUNIDAD SNMP)** | **Nueva fila** |
|---|---|
| Nombre de columna (* = Parte del índice) | Valor de la columna |
| * snmpTargetAddrName | "@mtaconfig_n", donde n va de 0 a m – 1, siendo m el número de elementos TLV del receptor de notificación del fichero definición de la configuración |
| snmpTargetAddrTMask | <Zero length octet string> |
| snmpTargetAddrMMS | 0 |

#### 11.2.1.4 snmpTargetParamsTable

Para elemento TLV-38 del fichero definición de la configuración, el MTA DEBE crear una fila de conformidad con el cuadro 19.

**Cuadro 19/J.167 – snmpTargetParamsTable**

| **snmpTargetParamsTable (RFC 3413, MIB DE OBJETIVO SNMP)** | **Nueva fila** |
|---|---|
| Nombre de columna (* = Parte del índice) | Valor de la columna |
| * snmpTargetParamsName | "@mtaconfig_n", donde n va de 0 a m – 1, siendo m el número de elementos TLV del receptor de notificación del fichero definición de la configuración |
| snmpTargetParamsMPModel<br>SYNTAX:<br>snmpMessageProcessingModel | SNMPv2c (1) |
| snmpTargetParamsSecurityModel<br>SYNTAX: snmpSecurityModel | SNMPv2c (2)<br>NOTA – La correspondencia entre los tipos de protocolo SNMP y los valores que aquí se muestran difiere de snmpTargetParamsMPModel |
| snmpTargetParamsSecurityName | "@mtaconfig" |
| snmpTargetParamsSecurityLevel | NoAuthNoPriv |
| snmpTargetParamsStorageType | Transitorio |
| snmpTargetParamsRowStatus | active (1) |

#### 11.2.1.5 snmpNotifyFilterProfileTable

Para cada elemento TLV-38 del fichero definición de la configuración con un subtipo 6 de TLV-38 con un valor distinto de cero, el MTA DEBE crear una fila de acuerdo con el cuadro 20.

**Cuadro 20/J.167 – snmpNotifyFilterProfileTable**

| **snmpNotifyFilterProfileTable (RFC 3413, MIB DE NOTIFICACIÓN de SNMP)** | **Nueva fila** |
|---|---|
| Nombre de columna<br>(* = Parte del índice) | Valor de la columna |
| * snmpTargetParamsName | "@mtaconfig_n", donde n va de 0 a m – 1, siendo m el número de elementos TLV del receptor de notificación del fichero definición de la configuración |
| snmpNotifyFilterProfileName | "@mtaconfig_n", donde n va de 0 a m – 1, siendo m el número de elementos TLV del receptor de notificación del fichero definición de la configuración |
| snmpNotifyFilterProfileStorageType | Transitorio |
| snmpNotifyFilterProfileRowStatus | active (1) |

#### 11.2.1.6 snmpNotifyFilterTable

Para cada elemento TLV-38 del fichero de definición de la configuración con un subtipo 6 de TLV-38 con valor distinto de cero, el MTA DEBE crear una fila de acuerdo con el cuadro 21.

**Cuadro 21/J.167 – snmpNotifyFilterTable**

| **snmpNotifyFilterTable (RFC 3413, MIB DE NOTIFICACIÓN SNMP)** | **Nueva fila** |
|---|---|
| Nombre de columna (* = Parte del índice) | Valor de la columna |
| * snmpNotifyFilterProfileName | "@mtaconfig_n", donde n va de 0 a m – 1, siendo m el número de elementos TLV del receptor de notificación del fichero definición de la configuración |
| * snmpNotifyFilterSubtree | <Filter OID> del TLV |
| snmpNotifyFilterMask | <Zero Length Octet String> |
| snmpNotifyFilterType | included (1) |
| snmpNotifyFilterStorageType | Transitorio |
| snmpNotifyFilterRowStatus | active (1) |

#### 11.2.1.7 snmpCommunityTable

De haber elementos TLV-38 presentes, independientemente de su número, el MTA DEBE crear una fila con valores fijos como se describe en el cuadro 22.

**Cuadro 22/J.167 – snmpCommunityTable**

| **snmpCommunityTable (RFC 3584, MIB DE COMUNIDAD de SNMP)** | **Primera fila** |
|---|---|
| Nombre de columna (* = Parte del índice) | Valor de la columna |
| * snmpCommunityIndex | "@mtaconfig" |
| snmpCommunityName | "public" |
| snmpCommunitySecurityName | "@mtaconfig" |
| snmpCommunityContextEngineID | <The engineID of the MTA> |
| snmpCommunityContextName | <Zero length octet string> |
| snmpCommunityTransportTag | <Zero length octet string> |
| snmpCommunityStorageType | Transitorio |
| snmpCommunityStatus | active (1) |

#### 11.2.1.8 usmUserTable

El cuadro usmUserTable está definido en RFC 3414. Las entradas del cuadro especifican el nombre de usuario en el receptor de notificación distante al que se debe enviar la notificación. Las filas en usmUserTable se crean de dos maneras distintas cuando el MTA soporta los valores 4 y 5 de <Notification Receiver Type> (TLV-38.3) y se incluyen en TLV-38.

- Si no está incluido <Security Name> (TLV-38.7), independientemente del número de elementos TLV-38 que haya en el fichero de definición de la configuración, el MTA DEBE crear una entrada con valores fijos, como se describe en la primera columna (fila "estática") del cuadro 23.

- Si se incluye <Security Name> (TLV-38.7), el MTA DEBE crear entradas adicionales, como se indica en la segunda columna ("otras filas") del cuadro 23. En este caso, la creación de filas adicionales en usmUserTable ocurre cada vez que el ID de motor de un receptor de notificación ha de ser descubierto (véanse más detalles al respecto en RFC 3414).

**Cuadro 23/J.167 – usmUserTable**

| **usmUserTable (RFC 3414, MIB de SM POR USUARIO SNMP)** | **Fila estática Caso 1** | **Otras filas Caso 2** |
|---|---|---|
| Nombre de columna (* = Parte del índice) | Valor de la columna | Valor de la columna |
| * usmUserEngineID | 0x00, crea una nueva fila cada vez que se descubre el ID de motor del receptor de notificación autorizado. | 0x00, crea una nueva fila cada vez que se descubre el ID de motor del receptor de notificación autorizado. |
| usmUserName | "@mtaconfig". | Cuando se crean otras filas, esto se sustituye por el campo <Security Name> del elemento TLV. |
| usmUserSecurityName | "@mtaconfig" | Cuando se crean otras filas, esto se sustituye por el campo <Security Name> del elemento TLV. |
| usmUserCloneFrom | <ignore> (cero.cero) Esta fila no se crea por mecanismo de clonaje | <ignore> (cero.cero) Esta fila no se crea por mecanismo de clonaje |
| usmUserAuthProtocol | Ninguno (usmNoAuthProtocol) | Cuando se crean otras filas, esto se sustituye por ninguno (usmNoAuthProtocol), o MD5 (usmHMACMD5AuthProtocol), o SHA (usmHMACSHAAuthProtocol),dependiendo del nivel de seguridad del usuario SNMPv3. |
| usmUserAuthKeyChange | Vacío | Vacío |
| usmUserOwnAuthKeyChange | Vacío | Vacío |
| usmUserPrivProtocol | Caso 1: ninguno (usmNoPrivProtocol) | Cuando se crean otras filas, esto se sustituye por ninguno (usmNoPrivProtocol) o DES (usmDESPrivProtocol), dependiendo del nivel de seguridad del usuario SNMPv3. |
| usmUserPrivKeyChange | Vacío | Vacío |
| usmUserOwnPrivKeyChange | Vacío | Vacío |
| usmUserPublic | Vacío | Vacío |
| usmUserStorageType | Volatile (2) | Volatile (2) |
| usmUserStatus | Active (1) | Active (1) |

#### 11.2.1.9 vacmSecurityToGroupTable

De haber elementos TLV-38 presentes, independientemente de su número, el MTA DEBE crear una columna "segunda fila" y PUEDE crear columnas "primera fila" o "tercera fila" con valores fijos como se describe en el cuadro 24 el MTA DEBE llenar las columnas "segunda fila" y "tercera fila" únicamente en el caso del flujo de aprovisionamiento seguro.

**Cuadro 24/J.167 – vacmSecurityToGroupTable**

| vacmSecurityToGroupTable (RFC 3415, MIB ACM POR VISTAS SNMP) | Primera fila | Segunda fila | Tercera fila |
|---|---|---|---|
| Nombre de columna (* = Parte del índice) | Valor de la columna | Valor de la columna | Valor de la columna |
| * vacmSecurityModel | SNMPV1 (1) | SNMPV2c (2) | SNMPUSM (3) |
| * vacmSecurityName | "@mtaconfig" | "@mtaconfig" | "@mtaconfig" |
| vacmGroupName | "@mtaconfigV1" | "@mtaconfigV2" | "@mtaconfigUSM" |
| vacmSecurityToGroupStorageType | volatile (2) | volatile (2) | volatile (2) |
| vacmSecurityToGroupStatus | Active (1) | active (1) | active (1) |

#### 11.2.1.10 VacmAccessTable

De haber elementos TLV-38 presentes, independientemente de su número, el MTA DEBE crear una columna "segunda fila" y PUEDE crear columnas "primera fila" o "tercera fila" con valores fijos, como se indica en el cuadro 25. El MTA DEBE llenar las columnas "segunda fila" y "tercera fila" únicamente en el caso del flujo de aprovisionamiento seguro.

**Cuadro 25/J.167 – vacmAccessTable**

| vacmSecurityToGroupTable (RFC 3415, MIB ACM POR VISTAS SNMP) | Primera fila | Segunda fila | Tercera fila |
|---|---|---|---|
| Nombre de columna (* = Parte del índice) | Valor de la columna | Valor de la columna | Valor de la columna |
| * vacmGroupName | "@mtaconfigV1" | "@mtaconfigV2" | "@mtaconfigUSM" |
| * vacmAccessContextPrefix | Vacío | Vacío | Vacío |
| * vacmAccessSecurityModel | SNMPv1 (1) | SNMPv2c (2) | USM (3) |
| * vacmAccessSecurityLevel | noAuthNoPriv (1) | noAuthNoPriv (1) | noAuthNoPriv (1) |
| vacmAccessContextMatch | exact (1) | exact (1) | exact (1) |
| vacmAccessReadViewName | Vacío | Vacío | Vacío |
| vacmAccessWriteViewName | Vacío | Vacío | Vacío |
| vacmAccessNotifyViewName | "@mtaconfig" | "@mtaconfig" | "@mtaconfig" |
| vacmAccessStorageType | volatile (2) | volatile (2) | volatile (2) |
| vacmAccessStatus | active (1) | active (1) | active (1) |

#### 11.2.1.11 vacmViewTreeFamilyTable

Si hay elementos TLV-38 presentes, independientemente de su número, DEBE crearse la entrada siguiente, como se define en el cuadro 26. Cabe señalar que esta entrada ya se crea en la inicialización del MTA.

**Cuadro 26/J.167 – vacmViewTreeFamilyTable**

| vacmViewTreeFamilyTable (RFC 3415, MIB de ACM POR VISTA SNMP) | Primera fila |
|---|---|
| Nombre de columna (* = Parte del índice) | Valor de la columna |
| * vacmViewTreeFamilyViewName | "@mtaconfig" |
| * vacmViewTreeFamilySubtree | 1.3 |
| vacmViewTreeFamilyMask | <Default from MIB> |
| vacmViewTreeFamilyType | included (1) |
| vacmViewTreeFamilyStorageType | Transitorio |
| vacmViewTreeFamilyStatus | active (1) |

### 11.3 Ejemplo de configuración TLV-38 y TLV-11

En esta cláusula se presentan ejemplos de configuración para la generación de TLV-38 y TLV-11 con el objetivo de una configuración marco SNMP basada en el modelo general y en el procesamiento de mensajes que se describe en RFC 3410, RFC 3411 y RFC 3412.

#### 11.3.1 Ejemplo TLV-38

Esta cláusula se incluye únicamente con fines informativos. El ejemplo que se presenta a continuación muestra cómo se utiliza TLV-38. Uno de los objetivos de esta cláusula es mostrar la utilización de @mtaConfig_n. Se asumen las siguientes premisas:

- El MTA ignora las entradas con <trap type> 1 y soporta los <trap type> 2, 3, 4 y 5.
- El MTA ya dispone, mediante un proceso de configuración, de una entrada con usmUserName y usmUserSecurityName que es 'mtaUser' y otra entrada para 'superUser'. Para mayor sencillez, no se incluyen las entradas VACM asociadas con este perfil.

El cuadro 27 contiene los elementos del fichero descripción de la configuración. Las celdas vacías indican que se utilizan, cuando los haya, valores por defecto.

**Cuadro 27/J.167 – Ejemplo de elementos del fichero definición de la configuración**

| Sub-TLV | | | | | |
|---|---|---|---|---|---|
| **Orden TLV-38 en el fichero de definición de la configuración** | **TLV-38 Número 1** | **TLV-38 Número 2** | **TLV-38 Número 3** | **TLV-38 Número 4** | **TLV-38 Número 5** |
| Dirección IP del receptor de notificación SNMP | 10.0.5.9 | 10.0.5.9 | 10.0.4.9 | 10.0.4.9 | 10.0.8.9 |
| Número de puerto UDP del receptor de notificación SNMPv2c | | 162 | | 57000 | |
| Tipo de trampa del receptor de notificación en SNMPv2c | 2 | 3 | 1 | 4 | 5 |

**Cuadro 27/J.167 – Ejemplo de elementos del fichero definición de la configuración**

| **Sub-TLV** | | | | | |
|---|---|---|---|---|---|
| **Orden TLV-38 en el fichero de definición de la configuración** | **TLV-38 Número 1** | **TLV-38 Número 2** | **TLV-38 Número 3** | **TLV-38 Número 4** | **TLV-38 Número 5** |
| Expiración del temporizador del receptor de notificación SNMPv2c | 1500 | | 2000 | | |
| Reintentos del receptor de notificación SNMPv2c | 3 | 1 | 2 | | |
| Parámetros de filtrado del receptor de notificación | org | pktcMtaDev ProvisioningStatus | mib-2 | pktcMtaMib | pktcMtaDev Provisioning Status |
| Nombre de seguridad del receptor de notificación | | notused | | SuperUser | mtaUser |
| | | | | | |
| @mta@config_n | 0 | 1 | 2 | 3 | 4 |

### 11.3.2 Contenido de los cuadros marco SNMP tras el procesamiento del anterior ejemplo de TLV-38

De acuerdo con las premisas enunciadas y los contenidos de TLV-38 especificados en cláusulas anteriores, esta cláusula muestra los cuadros que el MTA debe crear. El MTA ignora el número 1 de TLV-38 (tipo de notificación = 1), por lo que no existen entradas @mtaconfig_2. Se ignora el nombre de seguridad en TLV n = 2.

**Cuadro 28/J.167 – snmpCommunityTable**

| **Índice** | **[@mtaconfig]** |
|---|---|
| Nombre | "public" |
| Nombre de seguridad | @mtaconfig |
| ID de motor de contexto | <MTA ENGINEID> |
| Nombre de contexto | "" |
| Rótulo de transporte | "" |
| Tipo de almacenamiento | transitorio |
| Estado | activo |

**Cuadro 29/J.167 – snmpTargetAddrExtTable**

| **Índice** | **[@mtaconfig_0]** | **[@mtaconfig_1]** | **[@mtaconfig_2]** | **[@mtaconfig_3]** | **[@mtaconfig_4]** | **[@mtaconfig_5]** |
|---|---|---|---|---|---|---|
| Máscara T | "" | "" | "" | "" | "" | "" |
| MMS | 0 | 0 | 0 | 0 | 0 | 0 |

## Cuadro 30/J.167 usmUserTable

| Índice | [0x00][@ mtaconfig] | [<local-EngineID>] [mtaUser] | [<local-EngineID>] [superUser] | [0x00/<Notif-recv-EngineID>] [mtaUser] | [0x00/<Notif-recv-EngineID>] [superUser] |
|---|---|---|---|---|---|
| Nombre de seguridad | @mtaconfig | MtaUser | superUser | mtaUser | superUser |
| De Clon | ZeroDotZero | ZeroDotZero | zeroDotZero | zeroDotZero | zeroDotZero |
| Protocolo de autenticación | usmNoAuthProtocol | usmNoAuthProtocol | usmHMACMD5Auth Protocol | usmNoAuthProtocol | usmHMACMD5Auth Protocol |
| Cambio de clave autenticada | "" | "" | "" | "" | "" |
| Cambio de clave autoautenticada | "" | "" | "" | "" | "" |
| Protocolo de privacidad | usmNoPrivProtocol | usmNoPrivProtocol | usmDESPrivProtocol | usmNoPrivProtocol | usmDESPrivProtocol |
| Cambio de clave privada | "" | "" | "" | "" | "" |
| Cambio de clave privada propia | "" | "" | "" | "" | "" |
| Público | "" | "" | "" | "" | "" |
| Tipo de almacenamiento | Transitorio | Transitorio | Transitorio | Transitorio | Transitorio |
| Estado | activo | activo | activo | activo | activo |

## Cuadro 31/J.167 – vacmContextTable

| Índice |
|---|
| VacmContextName |

## Cuadro 32/J.167 – vacmSecurityToGroupTable

| Índice | [1][@mtaconfig] | [2][@mtaconfig] | [3][@mtaconfig] |
|---|---|---|---|
| Nombre de grupo | @mtaconfigV1 | @mtaconfigV2 | @mtaconfigUSM |
| Tipo de almacenamiento de seguridad al grupo | Transitorio | Transitorio | Transitorio |
| Estado de seguridad al grupo | activo | activo | activo |

## Cuadro 33/J.167 – vacmAccessTable

| Índice | [@mtaconfigV1][] [1][noAuthNoPriv] | [@mtaconfigV2][] [2][noAuthNoPriv] | [@mtaconfigUSM][] [3][noAuthNoPriv] |
|---|---|---|---|
| Correspondencia de contexto | exacto | exacto | exacto |
| Nombre de vista de lectura | "" | "" | "" |
| Nombre de vista de escritura | "" | "" | "" |
| Nombre de vista de notificación | @mtaconfig | @mtaconfig | @mtaconfig |
| Tipo de almacenamiento | Transitorio | Transitorio | Transitorio |
| Estado | activo | activo | activo |

**Cuadro 34/J.167 – vacmViewTreeFamilyTable**

| Índice | [@mtaconfig][org] |
|---|---|
| Máscara | "" |
| Tipo | Incluido |
| Tipo de almacenamiento | Transitorio |
| Estado | Activo |

**Cuadro 35/J.167 – snmpNotifyTable**

| Índice | [@mtaconfig_inform] | [@mtaconfig_trap] |
|---|---|---|
| Rótulo | @mtaconfig_inform | @mtaconfig_trap |
| Tipo | Informe | Trampa |
| Tipo de almacenamiento | Transitorio | Transitorio |
| Estado de fila | Activo | Activo |

**Cuadro 36/J.167 – snmpTargetAddrTable**

| Índice | [@mtaconfig_0] | [@mtaconfig_1] | [@mtaconfig_3] | [@mtaconfig_4] |
|---|---|---|---|---|
| Dominio T | snmpUDPDomain | snmpUDPDomain | snmpUDPDomain | snmpUDPDomain |
| Dirección T | "0A 00 05 09 00 82" | "0A 00 05 09 00 82" | "0A 00 04 09 DE A8" | "0A 00 08 09 00 82" |
| Expiración del temporizador | 1500 | 1500 | 1500 | 1500 |
| Cómputo de reintentos | 3 | 1 | 3 | 3 |
| Lista de rótulos | @mtaconfig_trap | @mtaconfig_inform | @mtaconfig_trap | @mtaconfig_inform |
| Parámetros | @mtaconfig_0 | @mtaconfig_1 | @mtaconfig_3 | @mtaconfig_4 |
| Tipo de almacenamiento | Transitorio | Transitorio | Transitorio | Transitorio |
| Estado de fila | activo | activo | activo | activo |

**Cuadro 37/J.167 – snmpTargetParamsTable**

| Índice | [@mtaconfig_0] | [@mtaconfig_1] | [@mtaconfig_3] | [@mtaconfig_4] |
|---|---|---|---|---|
| Modelo MP | 1 | 1 | 3 | 3 |
| Modelo de seguridad | 2 | 2 | 3 | 3 |
| Nombre de seguridad | @mtaconfig | @mtaconfig | @mtaconfig | @mtaconfig |
| Nivel de seguridad | noAuthNoPriv | noAuthNoPriv | noAuthNoPriv | NoAuthNoPriv |
| Tipo de almacenamiento | Transitorio | Transitorio | Transitorio | Transitorio |
| Estado de fila | activo | activo | activo | activo |

**Cuadro 38/J.167 – snmpNotifyFilterProfileTable**

| Índice | [@mtaconfig_0] | [@mtaconfig_1] | [@mtaconfig_3] | [@mtaconfig_4] |
|---|---|---|---|---|
| Nombre | [@mtaconfig_0] | [@mtaconfig_1] | [@mtaconfig_3] | [@mtaconfig_4] |
| Tipo de almacenamiento | Transitorio | Transitorio | Transitorio | Transitorio |
| Estado de fila | activo | activo | activo | activo |

**Cuadro 39/J.167 – snmpNotifyFilterTable**

| Índice | [@mtaconfig_0] [org] | [@mtaconfig_1] [pktcMtaProvision-ingStatus] | [@mtaconfig_3] [PktcMtaMib] | [@mtaconfig_4] [pktcMtaProvision-ingStatus] |
|---|---|---|---|---|
| Máscara | "" | "" | "" | "" |
| Tipo | Incluido | Incluido | Incluido | Incluido |
| Tipo de almacenamiento | Transitorio | Transitorio | Transitorio | Transitorio |
| Estado de fila | Activo | Activo | Activo | Activo |

## 12 Requisitos de gestiones SNMPv2c

La gestión de un dispositivo MTA utilizando SNMPv2c puede estar configurada, de ser necesario, por un operador que fije los cuadros de coexistencia correspondientes (y utilizando TLV-11) en el fichero de definición de la configuración MTA o mediante gestión postconfiguración.

- En el caso de que se utilicen los flujos básico e híbrido, el MTA DEBE configurar los cuadros descritos en 12.1 y 12.2 después de MTA4 para dar a SNMPv2c acceso de lectura/escritura al sistema de gestión por defecto (entidad de configuración proporcionada en la subopción 3 de la opción 122 de DHCP).
- Cuando se utiliza el flujo seguro, el MTA DEBE configurar los cuadros de 12.2, si el fichero de definición de la configuración contiene vinculaciones variables TLV-11 con los datos de snmpCommunityTable. Además, para restringir el acceso SNMP al MTA en dirección entrante, el fichero de definición de la configuración también puede contener vinculaciones variables TLV-11 para snmpTargetAddrTable y/o snmpTargetAddrExtTab.

En el apéndice I puede encontrarse un ejemplo modelo de habilitación de las gestiones SNMPv2c para operadores.

### 12.1 Contenido de los cuadros de modo coexistencia SNMPV2c creados por el MTA después de MTA4 con los flujos básico e híbrido

Véanse los cuadros 40 a 42.

**Cuadro 40/J.167 – Contenido de snmpCommunityTable**

| snmpCommunityTable (RFC 3584, MIB DE COMUNIDADES SNMP) | Acceso de lectura/escritura |
|---|---|
| Nombre de columna (* = Parte del índice) | Valor de la columna |
| * snmpCommunityIndex | "@mtaprov" |
| snmpCommunityName | "private" |
| snmpCommunitySecurityName | "@mtaprov" |
| snmpCommunityContextEngineID | <The engineID of the MTA> |
| snmpCommunityContextName | Vacío |
| snmpCommunityTransportTag | "@mtaprovTag" |
| snmpCommunityStorageType | Volatile (2) |
| snmpCommunityStatus | active(1) |

**Cuadro 41/J.167 – Contenido de snmpTargetAddrTable**

| snmpTargetAddrTable (RFC 3413, MIB DE OBJETIVO SNMP) | Primera fila |
|---|---|
| Nombre de la columna (* = Parte del índice) | Valor de la columna |
| * snmpTargetAddrName | "@mtaprov" |
| snmpTargetAddrTDomain | snmpUDPDomain = snmpDomains.1 |
| snmpTargetAddrTAddress<br>(IP Address non-Authoritative SNMP entity) | CADENA DE OCTETOS (6)<br>Octetos 1-4:<br><IP address of SNMP Entity derived from 122.3><br>Octetos 5-6:<br>cualquier valor de puerto de 2 bytes |
| snmpTargetAddrTimeout | Ignorar, <use default> |
| snmpTargetAddrRetryCount | ignorar, <use default> |
| snmpTargetAddrTagList | "@mtaprovTag" |
| snmpTargetAddrParams | "@mtaprov" |
| snmpTargetAddrStorageType | volatile (2) |
| snmpTargetAddrRowStatus | active(1) |

**Cuadro 42/J.167 – Contenido de snmpTargetAddrExtTable**

| snmpTargetAddrExtTable (RFC 3584, MIB DE COMUNIDAD SNMP) | Primera fila |
|---|---|
| Nombre de la columna (* = Parte del índice ) | Valor de la columna |
| * snmpTargetAddrName | "@mtaprov" |
| snmpTargetAddrTMask | FFFFFFFF:0000 |
| snmpTargetAddrMMS | 0 |

## 12.2 Entradas por defecto SNMP para el acceso a SNMPv2

El MTA DEBE crear los cuadros 43 a 49 durante la inicialización del agente SNMP para configurar el acceso a SNMPv2.

**Cuadro 43/J.167 – Entradas por defecto de vacmSecurityToGroupTable**

| vacmSecurityToGroupTable (RFC 3415, MIB de ACM POR VISTA SNMP) | Primera fila | Segunda fila | Tercera fila |
|---|---|---|---|
| Nombre de columna (* = Parte del Índice) | Valor de columna | Valor de columna | Valor de columna |
| * vacmSecurityModel | SNMPv2c (2) | SNMPv2c (2) | SNMPv2c (2) |
| * vacmSecurityName | "@mtaprov" | "admin" | "operator" |
| vacmGroupName | "@mtaprov" | "admin" | "operator" |
| vacmSecurityToGroupStorageType | permanent (4) | permanent (4) | permanent (4) |
| vacmSecurityToGroupStatus | active (1) | active (1) | active (1) |

**Cuadro 44/J.167 – Entradas por defecto de vacmAccessTable**

| vacmAccessTable (RFC 3415, MIB de ACM POR VISTA SNMP) | Primera fila | Segunda fila | Tercera fila |
|---|---|---|---|
| Nombre de columna (* = Parte del Índice) | Valor de columna | Valor de columna | Valor de columna |
| * vacmGroupName | "@mtaprov" | "admin" | "operator" |
| * vacmAccessContextPrefix | Vacío | Vacío | Vacío |
| * vacmAccessSecurityModel | SNMPv2 (2) | SNMPv2 (2) | SNMPv2 (2) |
| * vacmAccessSecurityLevel | noAuthNoPriv (1) | noAuthNoPriv (1) | noAuthNoPriv (1) |
| vacmAccessContextMatch | exact (1) | exact (1) | exact (1) |
| vacmAccessReadViewName | "@mtaconfig" | "@mtaconfig" | "@mtaconfig" |
| vacmAccessWriteViewName | "@mtaconfig" | "@mtaconfig" | Vacío |
| vacmAccessNotifyViewName | "@mtaconfig" | Vacío | Vacío |
| vacmAccessStorageType | permanent (4) | permanent (4) | permanent (4) |
| vacmAccessStatus | active (1) | active (1) | active (1) |

**Cuadro 45/J.167 – Entradas por defecto de vacmViewTreeFamilyTable**

| vacmViewTreeFamilyTable (RFC 3415, MIB de ACM POR VISTA SNMP) | Primera fila |
|---|---|
| Nombre de columna (* = Parte del Índice) | Valor de columna |
| * vacmViewTreeFamilyViewName | @mtaconfig |
| vacmViewTreeFamilySubtree | 1.3 |
| vacmViewTreeFamilyMask | Vacío <default from MIB> |
| vacmViewTreeFamilyType | included (1) |
| vacmViewTreeFamilyStorageType | volatile (2) |
| vacmViewTreeFamilyStatus | active (1) |

Cabe señalar que esta entrada también se crea por defecto para el procesamiento de TLV-38, lo que significa que sólo se necesita una entrada por defecto en el MTA para definir las gestiones SNMPv2 y la configuración TLV-38.

**Cuadro 46/J.167 – Entradas por defecto de snmpTargetParamsTable**

| snmpTargetParamsTable (RFC 3413, MIB DE OBJETIVO SNMP) | Primera fila |
|---|---|
| Nombre de columna (* = Parte del índice) | Valor de columna |
| * snmpTargetParamsName | "@mtaprov" |
| snmpTargetParamsMPModel | 1 |
| snmpTargetParamsSecurityModel | 2 |
| snmpTargetParamsSecurityName | "@mtaprov" |
| snmpTargetParamsSecurityLevel | noAuthNoPriv |
| snmpTargetParamsStorageType | permanent (4) |
| snmpTargetParamsRowStatus | active (1) |

**Cuadro 47/J.167 – Entradas por defecto de snmpNotifyTable**

| snmpNotifyTable (RFC 3413, MIB DE NOTIFICACIÓN de SNMP) | Primera fila |
|---|---|
| Nombre de columna (* = Parte del índice) | Valor de columna |
| * snmpNotifyName | "@mtaprov" |
| snmpNotifyTag | "@mtaprovTag" |
| snmpNotifyType | inform (2) |
| snmpNotifyStorageType | permanent (4) |
| snmpNotifyRowStatus | active (1) |

**Cuadro 48/J.167 – Entradas por defecto de snmpNotifyFilterProfileTable**

| snmpNotifyFilterProfileTable (RFC 3413, MIB DE NOTIFICACIÓN de SNMP) | Primera fila |
|---|---|
| Nombre de columna (* = Parte del índice) | Valor de columna |
| * snmpTargetParamsName | "@mtaprov" |
| snmpNotifyFilterProfileName | "@mtaprov" |
| snmpNotifyFilterProfileStorageType | permanent (4) |
| snmpNotifyFilterProfileRowStatus | active (1) |

**Cuadro 49/J.167 – Entradas por defecto de snmpNotifyFilterTable**

| snmpNotifyFilterTable (RFC 3413, MIB DE NOTIFICACIÓN SNMP) | Primera fila | Segunda fila |
|---|---|---|
| Nombre de columna (* = Parte del Índice) | Valor de columna | Valor de columna |
| *snmpNotifyFilterProfileName | "@mtaprov" | "@mtaprov" |
| *snmpNotifyFilterSubtree | pktcMtaNotification | snmpTraps |
| snmpNotifyFilterMask | Vacío | Vacío |
| snmpNotifyFilterType | included (1) | included (1) |
| snmpNotifyFilterStorageType | permanent (4) | permanent (4) |
| snmpNotifyFilterRowStatus | active (1) | active (1) |

# 13 Informe de repercusión de interrupción del servicio y soporte de otras características superiores

## 13.1 Soporte de los requisitos eDOCSIS

El MTA de IPCablecom se considera un dispositivo eSAFE de acuerdo con eDOCSIS y DEBE ajustarse a las cláusulas pertinentes de la especificación eDOCSIS que se recoge en la Rec. UIT-T J.126. Además de los requisitos comunes, la especificación incluye otros que atañen a la definición de la correspondiente especificación eSAFE. Esta cláusula trata de dichos requisitos adicionales, que se suponen necesarios en el marco de la especificación IPCablecom para su implementación.

Estos requisitos pueden agruparse en dos categorías:

- Requisitos de análisis de impactos e informe.
- Directivas de rearranque eSAFE.

### 13.1.1 Requisitos de análisis de repercusiones e informe

Como se especifica en la Rec. UIT-T J.126, el eCM tiene la capacidad de emitir un uniforme 'repercusión de la interrupción del servicio' para cada dispositivo eSAFE si, de hecho, se interrumpió el servicio de datos en el momento de la consulta. Esta cláusula trata de los niveles de repercusión y del mecanismo de emisión de informes. Cabe señalar que el eMTA de IPCablecom suele estar asociado con múltiples servicios (voz, fax) y múltiples ejemplares de cada servicio (en cada punto extremo configurado), por lo que el eMTA DEBE rendir informe del mayor número posible de repercusiones en todos los servicios/extremos.

#### 13.1.1.1 Análisis de repercusiones

Se considera que hay repercusión en un servicio en un punto extremo cuando el punto extremo está 'activo' y el servicio de datos interrumpido. La condición 'activo' se define como los estados offHook(3) y onHookPlusNCSActivity (2), como se define en pktcNcsEndPntHookState (puede encontrarse más información al respecto en la Rec. UIT-T J.126).

#### 13.1.1.2 Niveles de repercusión soportados e informe

En IPCablecom, cualquier interrupción de un servicio 'activo' (incluso potencialmente) DEBE considerarse como una 'repercusión importante' y todo lo demás se considerará como una 'repercusión menor'.

Así, el MTA DEBE rendir informe de las repercusiones de la siguiente manera:

- Repercusión importante – Si cualquiera de los puntos extremos asociados con el MTA está 'activo', la repercusión DEBE incluirse en el informe como 'repercusión importante'.
- Repercusión menor – Si todos los puntos extremos asociados con un MTA que son capaces de proporcionar un servicio no están 'activos' DEBE consignarse en el informe que la repercusión es una 'repercusión menor'.

## 13.2 MIB de extensión IPCablecom

Se ha definido la MIB de extensión de IPCablecom para todas las nuevas MIB que forman parte de IPCablecom 1.5. Puede encontrarse más información al respecto en la Rec. UIT-T J.166. Las extensiones atañen a la MIB de MTA y a la MIB de señalización.

### 13.2.1 Extensión de la MIB de MTA

La extensión de la MIB de MTA de IPCablecom está definida en la Rec. UIT-T J.166 y proporciona una funcionalidad adicional para controlar las nuevas funcionalidades, como las múltiples concesiones por intervalo (MGPI, *multiple grants per interval*) en el punto extremo.

### 13.2.2 Extensión de la MIB de señalización

La extensión de la MIB de señalización de IPCablecom está definida en la Rec. UIT-T J.166 y proporciona un control adicional así como la funcionalidad de emisión de informes para los puntos extremos en cuanto a retardo DTMF, tratamiento de la cuarentena, estado de colgado, etc.

## 13.3 MIB de batería de reserva

El E-MTA es un dispositivo incorporado dentro del módem de cable. Puesto que la telefonía es un servicio de gran disponibilidad, es fundamental contar con una batería de reserva. Para mantener y hacer funcionar los modelos de batería se ha creado un conjunto de MIB, definido en el proyecto de Recomendación UIT-T J.bb. Los dispositivos E-MTA con la funcionalidad de batería de reserva DEBEN soportar las MIB definidas en el proyecto de Recomendación UIT-T J.bb.

## 13.4 MIB de Syslog

Para mantener la granularidad del servicio Syslog, se ha definido en la Rec. UIT-T J.166 un conjunto de MIB. Estas MIB ayudan al operador a eliminar los problemas del servicio Syslog y a obtener un mayor nivel de control sobre los mensajes Syslog.

## 13.5 Detección de potencial extraño

La detección de potencial extraño es muy importante a la hora de proporcionar un servicio de telefonía. En la Rec. UIT-T J.166 se ha definido una MIB "pktcEnEndPntInfoTable" para reunir informes de tal detección. Los E-MTA DEBERÍAN aplicar esta funcionalidad.

# Apéndice I

# Ejemplo de configuración de coexistencia SNMPv2c – Modelo para proveedores de servicio

Los operadores pueden utilizar el modelo que se define en esta cláusula para habilitar la gestión SNMPv2c (se reutilizan en este ejemplo las entradas por defecto de 12.2). Cabe señalar que los proveedores de servicio no han de restringirse a utilizar este modelo. Véanse los cuadros I.1 a I.3.

**Cuadro I.1/J.167 – Fichero definición de la configuración para los flujos básico e híbrido del modelo snmpCommunityTable**

| **snmpCommunityTable (RFC 3584, MIB DE COMUNIDAD)** | **Acceso de lectura/escritura** | **Acceso de sólo lectura** |
|---|---|---|
| Nombre de columna (* = Parte del índice) | Valor de la columna | Valor de la columna |
| * snmpCommunityIndex | "admin" | "operator" or <any> |
| snmpCommunityName | <SNMP Community Name> | <SNMP Community Name> |
| snmpCommunitySecurityName | "admin" | "operator" |
| snmpCommunityContextEngineID | <The engineID of the MTA> | <The engineID of the MTA> |
| snmpCommunityContextName | Vacío | Vacío |
| snmpCommunityTransportTag | "adminTag" | "operatorTag" |
| snmpCommunityStorageType | volatile (2) | volatile (2) |
| snmpCommunityStatus | createAndGo (4) | createAndGo (4) |

**Cuadro I.2/J.167 – Modelo de snmpTargetAddrTable para el fichero definición de la configuración de los flujos básico e híbrido**

| **snmpTargetAddrTable (RFC-3413 – MIB DE OBJETIVO SNMP** | **Primera fila** | **Segunda fila** |
|---|---|---|
| Nombre de columna<br>(* = Parte del índice) | Valor de la columna | Valor de la columna |
| * snmpTargetAddrName | "admin" | "operator" |
| snmpTargetAddrTDomain | snmpUDPDomain = snmpDomains.1 | snmpUDPDomain = snmpDomains.1 |
| snmpTargetAddrTAddress<br>(entidades SNMP sin autoridad sobre la dirección IP) | CADENA DE OCTETOS (6)<br>Octetos 1-4:<br><SNMP Mgmt Station IPv4 Address><br>Octets 5-6:<br><0x0000> | CADENA DE OCTETOS (6)<br>Octetos 1-4:<br><SNMP Mgmt Station IPv4 Address><br>Octets 5-6:<br><0x0000> |
| snmpTargetAddrTimeout | Ignorar<use default> | Ignorar, <use default> |
| snmpTargetAddrRetryCount | Ignorar, <use default> | Ignorar, <use default> |
| snmpTargetAddrTagList | "adminTag" | "operatorTag" |
| snmpTargetAddrParams | Vacío | Vacío |
| snmpTargetAddrStorageType | volatile (2) | volatile (2) |
| snmpTargetAddrRowStatus | createAndGo (4) | createAndGo (4) |

**Cuadro I.3/J.167 – Modelo de snmpTargetAddrExtTable para el fichero definición de la configuración de los flujos básico e híbrido**

| **snmpTargetAddrExtTable (RFC 3584, MIB DE COMUNIDAD SNMP)** | **Primera fila** | **Segunda fila** |
|---|---|---|
| Nombre de columna<br>(* = Parte del índice) | Valor de la columna | Valor de la columna |
| * snmpTargetAddrName | "admin" | "operator" |
| snmpTargetAddrTMask | CADENA DE OCTETOS (6)<br>Octetos 1-4:<br><SNMP Mgmt Station Sub Net Mask><br>Octetos 5-6:<br><0x0000> | CADENA DE OCTETOS (6)<br>Octetos 1-4:<br><SNMP Mgmt Station Sub Net Mask><br>Octetos 5-6:<br><0x0000> |
| snmpTargetAddrMMS | 0 | 0 |

## SERIES DE RECOMENDACIONES DEL UIT-T

| | |
|---|---|
| Serie A | Organización del trabajo del UIT-T |
| Serie D | Principios generales de tarificación |
| Serie E | Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos |
| Serie F | Servicios de telecomunicación no telefónicos |
| Serie G | Sistemas y medios de transmisión, sistemas y redes digitales |
| Serie H | Sistemas audiovisuales y multimedios |
| Serie I | Red digital de servicios integrados |
| **Serie J** | **Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedios** |
| Serie K | Protección contra las interferencias |
| Serie L | Construcción, instalación y protección de los cables y otros elementos de planta exterior |
| Serie M | Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes |
| Serie N | Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión |
| Serie O | Especificaciones de los aparatos de medida |
| Serie P | Calidad de transmisión telefónica, instalaciones telefónicas y redes locales |
| Serie Q | Conmutación y señalización |
| Serie R | Transmisión telegráfica |
| Serie S | Equipos terminales para servicios de telegrafía |
| Serie T | Terminales para servicios de telemática |
| Serie U | Conmutación telegráfica |
| Serie V | Comunicación de datos por la red telefónica |
| Serie X | Redes de datos, comunicaciones de sistemas abiertos y seguridad |
| Serie Y | Infraestructura mundial de la información, aspectos del protocolo Internet y Redes de la próxima generación |
| Serie Z | Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación |

Impreso en Suiza
Ginebra, 2006