Privacidad de la línea base DOCSIS 1.0 en el CMTS de Cisco

Contenido

Introducción

El objetivo principal de la Interfaz de Privacidad de la Línea Base (BPI) de Data-over-Cable Service Interface Specifications (DOCSIS) es proporcionar un esquema de encripción de datos simple para proteger los datos enviados a y desde módems de cable en una red Data over Cable. La privacidad de la línea de base también puede utilizarse como forma de autenticar los cablemódem y autorizar la transmisión de tráfico multidifusión a los cablemódem.

Cisco Cable Modem Termination System (CMTS) y productos de cablemódem que ejecutan

imágenes de Cisco IOS® Software con un conjunto de funciones que incluye los caracteres "k1" o "k8" que admiten privacidad de línea de base, por ejemplo ubr7200-k1p-mz.121-6.EC1.bin.

Este documento explica la privacidad de línea de base en los productos de Cisco que funcionan en el modo DOCSIS1.0.

Antes de comenzar

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Prerequisites

No hay requisitos previos específicos para este documento.

Componentes Utilizados

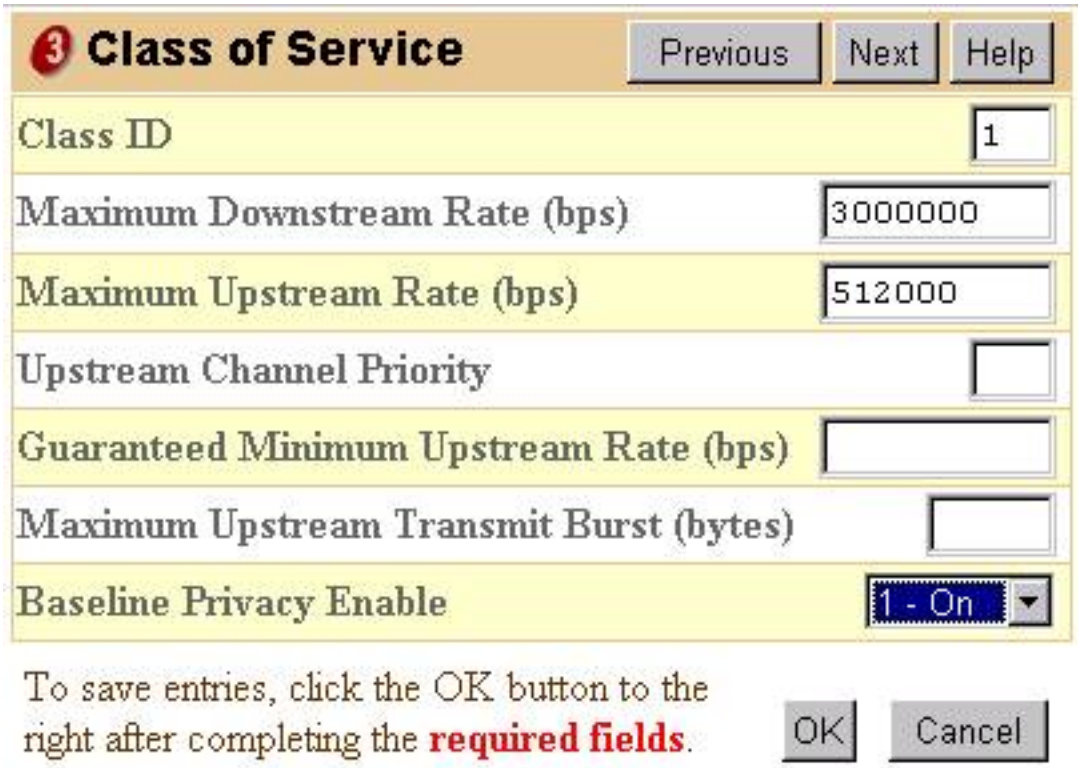
La información en este documento se basa en la configuración de un uBR7246VXR que ejecuta Cisco IOS® Software Release 12.1(6)EC, pero también se aplica a todos los demás productos CMTS y versiones de software de Cisco.

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

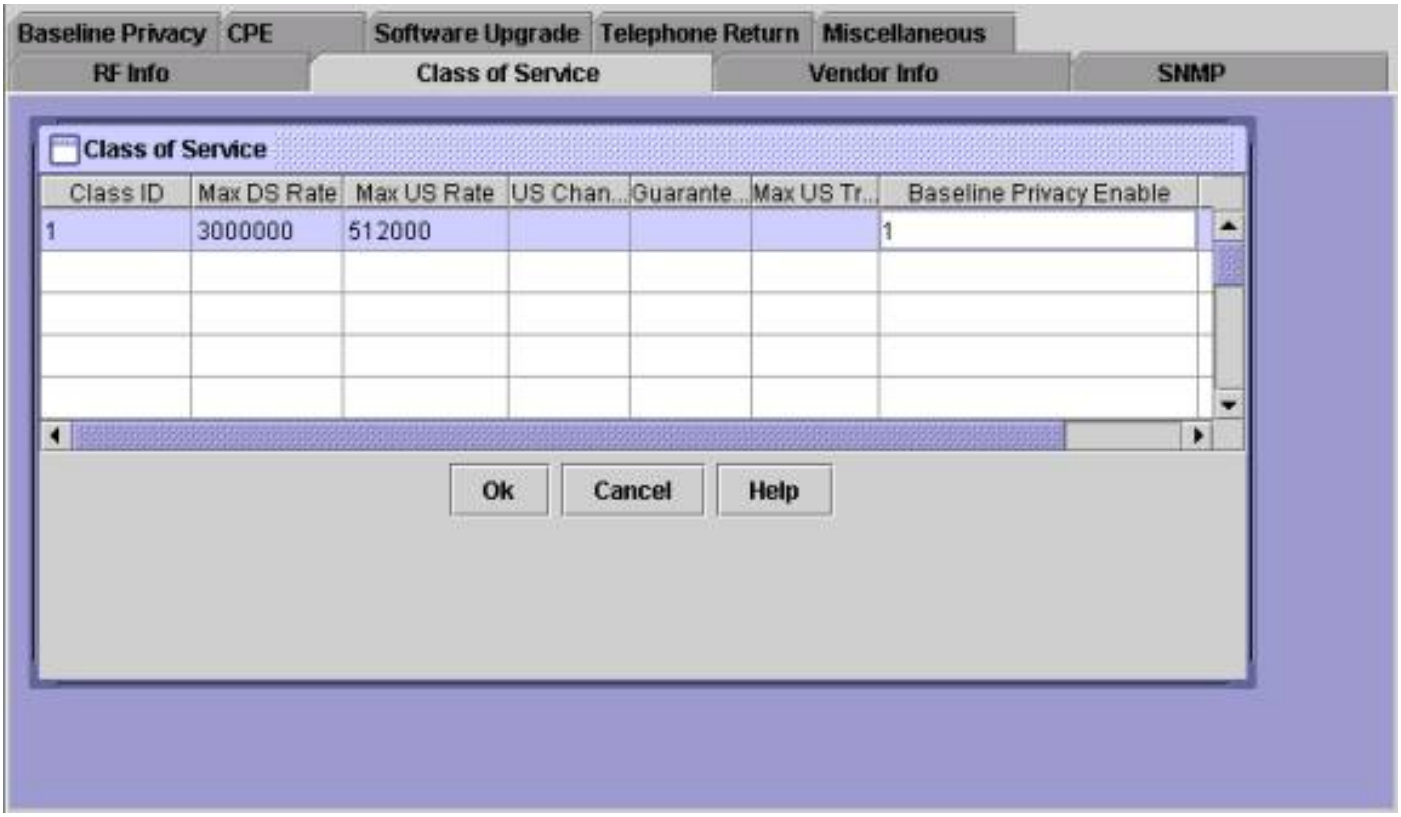
Cómo configurar la privacidad de la línea base para cablemódems

Un cablemódem sólo intentará utilizar la privacidad de línea de base si se le pide que lo haga a través de los parámetros de clase de servicio en un archivo de configuración DOCSIS. El archivo de configuración DOCSIS contiene parámetros operativos para el módem y se descarga a través de TFTP como parte del proceso de conexión.

Un método para crear un archivo de configuración DOCSIS es utilizar DOCSIS Cable Modem Configurator en Cisco.com. Con el Configurador del cablemódem DOCSIS, puede crear un archivo de configuración DOCSIS que ordene a un cablemódem que utilice la Privacidad de línea de base estableciendo el campo Baseline Privacy Enable en la pestaña Class of Service en **On**. Consulte el ejemplo a continuación:



Alternativamente, la versión independiente de la configuración del archivo DOCSIS de puede utilizarse para habilitar la privacidad de línea base, como se muestra a continuación:



Una vez creado el archivo de configuración de DOCSIS que admite BPI, se deberán reiniciar los cable módems para descargar el nuevo archivo de configuración y luego aplicar la privacidad de línea de base.

Cómo determinar si un cablemódem usa privacidad de línea de base

En un CMTS de Cisco, podemos usar el comando show cable modem para ver el estado de los cablemódems individuales. Existen varios estados en los que puede estar un módem que utiliza privacidad de línea de base.

en línea

Después de que un cable módem se registra con un CMTS de Cisco, ingresa en el estado en línea. Un cablemódem necesita llegar a este estado antes de poder negociar parámetros de privacidad de línea de base con un CMTS de Cisco. En este punto, el tráfico de datos enviado entre el cable módem y el CMTS no está cifrado. Si un cable módem permanece en este estado y no pasa a ninguno de los estados mencionados a continuación, esto significa que el módem no está utilizando la privacidad de línea de base.

en línea (pk)

El estado online(pk) significa que el cablemódem ha podido negociar una **clave de autorización**, también conocida como **clave de cifrado de clave (KEK)** con el CMTS de Cisco. Esto significa que el cable módem está autorizado para utilizar la privacidad de línea de base y ha negociado la primera fase de la privacidad de línea de base con éxito. La clave KEK es una clave de 56 bits utilizada para proteger las posteriores negociaciones de privacidad de línea de base. Cuando un módem se encuentra en el estado en línea (pk), el tráfico de datos enviado entre el cablemodem y Cisco CMTS sigue sin cifrarse, ya que todavía no se ha negociado ninguna clave para el cifrado del tráfico de datos. Normalmente, online(pk) es seguido por online(pt).

reject(pk)

Este estado indica que los intentos del cablemódem de negociar una KEK han fallado. La razón más común por la que un módem estaría en este estado sería que Cisco CMTS tiene la autenticación del módem activada y el módem ha fallado en la autenticación.

online (pt)

En este momento, el módem ha negociado correctamente una clave de cifrado de tráfico (TEK) con Cisco CMTS. El TEK se utiliza para cifrar el tráfico de datos entre el cablemódem y Cisco CMTS. El proceso de negociación TEK se cifró mediante el uso de KEK. TEK es una clave de 56 o 40 bits utilizada para cifrar el tráfico de datos entre el cable módem y Cisco CMTS. En este punto, la privacidad de línea de base se establece y se ejecuta correctamente, por lo que los datos de usuario enviados entre Cisco CMTS y el cablemódem se cifran.

reject(pt)

Este estado indica que el cablemódem no pudo negociar un TEK con el CMTS de Cisco.

Consulte a continuación para obtener una salida de muestra de un comando show cable modem que muestra los módems de cable en varios estados relacionados con la privacidad de la línea base.

```
CMTS# show cable modem
Interface    Prim Online      Timing Rec    QoS CPE IP address      MAC address
             Sid  State       Offset Power
Cable3/0/U1 1    online(pt) 2208    0.75  7   0   10.1.1.40       0020.4001.5370
Cable3/0/U1 2    online(pk) 2213    0.50  5   0   10.1.1.33       0050.7366.1fb9
Cable3/0/U0 3    online(pt) 2738    0.00  5   0   10.1.1.24       0002.fdfa.0a35
Cable3/0/U1 4    reject(pk) 2738    1.00  5   0   10.1.1.30       0001.9659.4447
```

Nota: Para obtener más información sobre el estado del cablemódem, consulte Resolución de problemas de cablemódems uBR que no se conectan.

Temporizadores que afectan el establecimiento y el mantenimiento de la privacidad de la línea base

Hay ciertos valores de agotamiento del tiempo de espera que pueden modificarse para cambiar el comportamiento de la privacidad de la línea base. Algunos de estos parámetros se pueden configurar en Cisco CMTS y otros a través del archivo de configuración DOCSIS. Hay pocas razones para cambiar cualquiera de estos parámetros excepto por la vida útil del KEK y la vida útil del TEK. Estos temporizadores podrán ser modificados para aumentar la seguridad en una planta de cable o para reducir el exceso de operaciones de tráfico y de la CPU debido a la administración de BPI.

Vida útil de KEK

La duración de KEK es la cantidad de tiempo que el cablemódem y Cisco CMTS deben considerar válida la KEK negociada. Antes de que transcurra este tiempo, el cable módem debe renegociar un nuevo KEK con el CMTS de Cisco.

Puede configurar esta hora mediante el comando de interfaz de cable CMTS de Cisco:

cable privacy kek life-time *300-6048000 seconds*

La configuración predeterminada es 604800 segundos, lo que equivale a 7 días.

Tener una vida útil de KEK más pequeña aumenta la seguridad porque cada KEK durará un período más corto y, por lo tanto, si se hackea la KEK, menos negociaciones TEK futuras podrían ser secuestradas. La desventaja de esto es que la re-negociación de KEK aumenta el uso de la CPU en los cablemódems y aumenta el tráfico de administración de BPI en una planta de cable.

Tiempo de gracia de KEK

El tiempo de gracia de KEK es la cantidad de tiempo antes de que expire la vida útil de KEK, que un cable módem está destinado a comenzar la negociación con Cisco CMTS para una nueva KEK. La idea de colocar este temporizador consiste en que el cablemódem tenga tiempo suficiente para renovar el KEK antes de que caduque.

Puede configurar esta hora mediante el comando de interfaz de cable CMTS de Cisco:

```
cable privacy kek grace-time 60-1800 seconds
```

Se puede configurar este horario mediante un archivo de configuración DOCSIS completando el campo denominado Agotamiento del tiempo de espera para la tolerancia de autorización en la ficha de privacidad de línea de base. Si se rellena este campo de archivo de configuración DOCSIS, tendrá prioridad sobre cualquier valor configurado en Cisco CMTS. El valor predeterminado para este temporizador es 600 segundos, lo que equivale a 10 minutos.

Vida útil de TEK

La duración de TEK es la cantidad de tiempo que el cablemódem y Cisco CMTS deben considerar válido el TEK negociado. Antes de que transcurra este tiempo, el cable módem debe renegociar un nuevo TEK con Cisco CMTS.

Puede configurar esta hora mediante el comando de interfaz de cable CMTS de Cisco:

```
cable privacy tek life-time <180-604800 seconds>
```

La configuración predeterminada es 43200 segundos, lo que equivale a 12 horas.

Disponer de una duración TEK más pequeña aumenta la seguridad porque cada TEK durará menos tiempo y, por lo tanto, si se hackea el TEK, menos datos quedarán expuestos al descifrado no autorizado. La desventaja de esto es que la renegociación TEK aumenta el uso de la CPU en los cablemódems y aumenta el tráfico de administración BPI en una planta de cable.

Tiempo de tolerancia TEK

El tiempo de gracia TEK es la cantidad de tiempo antes de que venza la vida útil de TEK que un cablemódem debe comenzar a negociar con Cisco CMTS para un nuevo TEK. La idea detrás de este temporizador es que el cablemódem tenga tiempo suficiente para renovar el TEK antes de que caduque.

Puede configurar esta hora mediante el comando de interfaz de cable CMTS de Cisco:

```
cable privacy tek grace-time 60-1800 seconds
```

También puede configurar este lapso de tiempo mediante un archivo de configuración DOCSIS completando el campo Tiempo de espera de tolerancia TEK en la ficha Privacidad de línea de base. Si se rellena este campo de archivo de configuración DOCSIS, tendrá prioridad sobre cualquier valor configurado en Cisco CMTS.

El valor predeterminado para este temporizador es 600 segundos, lo que equivale a 10 minutos.

Autorizar el tiempo de espera

Esta vez se determina el tiempo que un cablemódem esperará una respuesta de un CMTS de

Cisco cuando negocie por primera vez un KEK.

Puede configurar este tiempo en un archivo de configuración DOCSIS modificando el campo **Autorizar** tiempo de **espera** en la pestaña Privacidad de línea de base.

El valor predeterminado para este campo es de 10 segundos y el intervalo válido es de 2 a 30 segundos.

Vuelva a autorizar el tiempo de espera

Esta vez se determina el tiempo que un cablemódem esperará una respuesta de un CMTS de Cisco al negociar un nuevo KEK porque la vida útil del KEK está a punto de caducar.

Puede configurar este tiempo en un archivo de configuración DOCSIS mediante la modificación del campo Reauthorize Wait Timeout (Volver a autorizar el tiempo de espera) agotado en la ficha Baseline Privacy tab (Privacidad de línea de base).

El valor predeterminado para este temporizador es de 10 segundos y el intervalo válido es de 2 a 30 segundos.

Autorización de tiempo de espera tolerado

Especifica el período de gracia para la nueva autorización (en segundos). El valor predeterminado es 600. El intervalo válido es de 1 a 1800 segundos.

Autorizar el tiempo de espera para el rechazo

Si un cablemódem intenta negociar un KEK con un CMTS de Cisco, pero se rechaza, debe esperar al tiempo de espera de rechazo de autorización antes de volver a intentar negociar un nuevo KEK.

Puede configurar este parámetro en un archivo de configuración de DOCSIS utilizando el campo **Autorizar** tiempo de espera de **rechazo** en la ficha Privacidad de línea de base. El valor predeterminado para este temporizador es de 60 segundos y el intervalo válido es de 10 a 600 segundos.

Tiempo de espera operativo

Esta vez se determina el tiempo que un cablemódem esperará una respuesta de un CMTS de Cisco al negociar un TEK por primera vez.

Puede configurar este tiempo en un archivo de configuración de DOCSIS al modificar el campo Operational Wait Timeout (Tiempo de espera operativo) en la ficha Baseline Privacy (Privacidad de la línea de base).

El valor predeterminado para este campo es de 1 segundo y el rango válido es de 1 a 10 segundos.

Regenerar valor de tiempo de espera

Esta vez, se determina el tiempo que un cablemódem esperará una respuesta de un CMTS de Cisco al negociar un nuevo TEK porque la duración del TEK está a punto de caducar.

Puede configurar este tiempo en un archivo de configuración DOCSIS mediante la modificación del campo Rekey Wait Timeout (Regenerar valor de tiempo de espera) debajo de la ficha Baseline Privacy (Privacidad de línea de base).

El valor predeterminado para este temporizador es de 1 segundo y el intervalo válido es de 1 a 10 segundos.

Comandos de configuración de Privacidad de la línea base del CMTS de Cisco.

Los siguientes comandos de interfaz de cable se pueden utilizar para configurar la privacidad de línea base y las funciones relacionadas con la privacidad de línea base en un CMTS de Cisco.

cable privacy

El comando cable privacy habilita la negociación de la privacidad Baseline en una interfaz particular. Si el comando **no cable privacy** se configura en una interfaz de cable, no se permitirá a ningún cable módem negociar la privacidad de línea de base cuando se conecte en esa interfaz. Tenga cuidado al inhabilitar la privacidad de línea de base porque si a un cablemódem se le pide que utilice la privacidad de línea de base por medio de su archivo de configuración DOCSIS y Cisco CMTS se niega a permitirle negociar la privacidad de línea de base, es posible que el módem no pueda permanecer en línea.

cable privacy mandatory

Si el comando **cable privacy required** se configura y un cablemódem tiene la privacidad de línea de base habilitada en su archivo de configuración DOCSIS, entonces el cablemódem debe negociar exitosamente y utilizar la privacidad de línea de base; de lo contrario, no se le permitirá permanecer en línea.

Si el archivo de configuración DOCSIS de un cablemódem no indica al módem que utilice la privacidad de línea de base, el comando **cable privacy required** no detendrá el módem de permanecer en línea.

El comando **cable privacy required** no está habilitado de forma predeterminada.

cable privacy authenticate-modem

Se puede realizar una forma de autenticación para los módems que aplican la privacidad de la línea base. Cuando los cablemódems negocian un KEK con el CMTS de Cisco, los módems transmiten los detalles de su dirección MAC de 6 bytes y su número de serie al CMTS de Cisco. Estos parámetros se pueden utilizar como una combinación de nombre de usuario y contraseña para autenticar cablemódems. El CMTS de Cisco utiliza el servicio de Autenticación, Autorización y Contabilidad de Cisco IOS (AAA) para realizar esta tarea. A los cable módems con errores de autenticación no se les permite ponerse en línea. Además, los módem de cable que no utilizan la privacidad de la línea base no están afectados por este comando.

Precaución: Puesto que esta función hace uso del servicio AAA, debe asegurarse de que tiene cuidado al modificar la configuración AAA, de lo contrario, puede perder involuntariamente la capacidad de iniciar sesión y administrar su CMTS de Cisco.

A continuación se presentan algunas configuraciones de muestra correspondientes a las maneras de realizar la autenticación del módem. En estos ejemplos de configuración, se ha ingresado una cantidad de módems en una base de datos de autenticación. La dirección MAC de 6 octetos del módem funciona como nombre de usuario y el número de serie de longitud variable funciona como contraseña. Tenga en cuenta que se ha configurado un módem con un número de serie obviamente incorrecto.

El siguiente ejemplo parcial de configuración de Cisco CMTS utiliza una base de datos de autenticación local para autenticar un número de cablemódems.

```
aaa new-model

aaa authentication login cmts local

aaa authentication login default line

!

username 009096073831 password 0 009096073831

username 0050734eb419 password 0 FAA0317Q06Q

username 000196594447 password 0 **BAD NUMBER**

username 002040015370 password 0 03410390200001835252

!

interface Cable 3/0

 cable privacy authenticate-modem

!

line vty 0 4

 password cisco
```

Otro método de autenticación de módems sería emplear un servidor RADIUS externo. Este es un ejemplo de configuración parcial de Cisco CMTS que utiliza un servidor RADIUS externo para autenticar módems

```
aaa new-model

aaa authentication login default line

aaa authentication login cmts group radius

!

interface Cable 3/0

 cable privacy authenticate-modem

!
```

```
radius-server host 172.17.110.132 key cisco

!

line vty 0 4

 password cisco
```

A continuación se muestra un archivo de base de datos de usuarios RADIUS de ejemplo con la información equivalente al ejemplo anterior que utilizó autenticación local. El archivo de usuarios es utilizado por varios servidores RADIUS comerciales y freeware como una base de datos donde se almacena la información de autenticación de usuarios.

```
# Sample RADIUS server users file.



# Joe Blogg's Cable Modem

009096073831 Password = "009096073831"

             Service-Type = Framed



# Jane Smith's Cable Modem



0050734EB419 Password = "FAA0317Q06Q"



             Service-Type = Framed



# John Brown's Cable Modem

000196594477 Password = "**BAD NUMBER**"

             Service-Type = Framed



# Jim Black's Cable Modem

002040015370 Password = "03410390200001835252"



             Service-Type = Framed
```

A continuación se muestra el resultado de un comando **show cable modem** ejecutado en un CMTS de Cisco que utiliza cualquiera de los ejemplos de configuración anteriores. Podrá ver que cualquiera de los módems con privacidad de la línea base habilitados que no esté listado en la base de datos de autenticación local o que tenga el número de serie incorrecto, ingresará al estado reject(pk) y no permanecerá en línea.

```
CMTS# show cable modem
Interface   Prim Online      Timing Rec    QoS CPE IP address      MAC address
            Sid  State       Offset Power
Cable3/0/U0 17   online      2810    0.00  6   0   10.1.1.11       0001.9659.43fd
Cable3/0/U1 18   online(pt)  2739    0.00  5   0   10.1.1.29       0050.734e.b419
Cable3/0/U0 19   offline     2815    0.00  2   0   10.1.1.52       0001.9659.4461
Cable3/0/U0 20   reject(pk)  2810   -0.75  5   0   10.1.1.30       0001.9659.4447
Cable3/0/U1 21   online(pt)  2212    0.75  7   0   10.1.1.40       0020.4001.5370
Cable3/0/U0 22   online(pt)  2806    0.00  5   0   10.1.1.44       0090.9607.3831
```

El módem con SID 17 no tiene una entrada en la base de datos de autenticación, pero puede conectarse porque su archivo de configuración DOCSIS no le ha ordenado utilizar la privacidad de línea de base.

Los módems con SID 18, 21 y 22 son capaces de conectarse porque tienen entradas correctas en la base de datos de autenticación.

El módem con el SID 18 no puede conectarse porque se le ha indicado que utilice la privacidad de línea base pero no hay ninguna entrada en la base de datos de autenticación para este módem. Este módem habría estado recientemente en el estado reject(pk) para indicar que falló la autenticación.

El módem con SID 20 no puede conectarse porque, aunque hay una entrada en la base de datos de autenticación con la dirección MAC de este módem, el número de serie correspondiente es incorrecto. Actualmente, este módem se encuentra en el estado reject(pk), pero pasará al estado sin conexión después de un breve período.

Cuando los módems fallan en la autenticación, se agrega un mensaje en las siguientes líneas al registro de Cisco CMTS.

```
%UBR7200-5-UNAUTHSIDTIMEOUT: CMTS deleted    BPI unauthorized Cable Modem 0001.9659.4461
```

Luego, el cablemódem se elimina de la lista de mantenimiento de estación y se lo indicará como desconectado dentro de un lapso de 30 segundos. Por lo tanto, el cable módem muy probablemente intentará conectarse una vez más sólo para ser rechazado nuevamente.

Nota: Cisco no recomienda que los clientes utilicen el comando **cable privacy authenticate-modem** para evitar que los cablemódems no autorizados se conecten. Una forma más eficaz de garantizar que los clientes no autorizados no tengan acceso a la red de un proveedor de servicios es configurar el sistema de aprovisionamiento de modo que se indique a los cablemódems no autorizados que descarguen un archivo de configuración DOCSIS con el campo de acceso a la red desactivado. De esta manera, el módem no desperdiciará ancho de banda ascendente de valor al volver a determinar las distancias continuamente. En su lugar, el módem llegará al estado **online(d)** que indica que a los usuarios detrás del módem no se les concederá acceso a la red del proveedor de servicios y el módem sólo utilizará el ancho de banda ascendente para el mantenimiento de la estación.

Comandos utilizados para supervisar el estado de BPI

show interface cable X/0 privacy [kek | tek]: este comando se utiliza para mostrar los temporizadores asociados con el KEK o el TEK como se configuró en una interfaz CMTS.

A continuación se muestra un ejemplo de salida de este comando.

```
CMTS# show interface cable 4/0 privacy kek

Configured KEK lifetime value = 604800

Configured KEK grace time value = 600


CMTS# show interface cable 4/0 privacy tek

Configured TEK lifetime value = 60480

Configured TEK grace time value = 600
```

show interface cable X/0 privacy statistics: este comando oculto se puede utilizar para ver estadísticas sobre el número de SID que utilizan privacidad de línea de base en una interfaz de cable determinada.

A continuación se muestra un ejemplo de salida de este comando.

```
CMTS# show interface cable 4/0 privacy statistic


CM key Chain Count : 12

CM Unicast key Chain Count : 12

CM Mucast key Chain Count : 3
```

debug cable privacy: este comando activa la depuración de privacidad de línea de base. Cuando se activa este comando, cuando se produce un cambio en el estado de privacidad de la línea de base o un evento de privacidad de línea de base, se mostrarán detalles en la consola. Este comando sólo funciona cuando está precedido por el comando **debug cable interface cable X/0** o el comando **debug cable mac-address** *mac-address*.

debug cable bpiatp: este comando activa la depuración de la privacidad de línea de base. Cuando se activa este comando, cada vez que se envía o recibe un mensaje de privacidad de línea de base por el CMTS de Cisco, se mostrará el volcado hexadecimal del mensaje. Este comando sólo funciona cuando está precedido por el comando **debug cable interface cable X/0** o el comando **debug cable mac-address** *mac-address*.

debug cable keyman: este comando activó la depuración de la administración de claves de privacidad de línea base. Cuando se activa este comando, se muestran los detalles de la administración de claves de privacidad de línea de base.

Solución de problemas de BPI

Los cablemódems aparecen como conectados, en lugar de conectados(pt).

Si aparece un módem en estado conectado, en lugar de conectado(pt), significa, por lo general, una de las tres siguientes opciones.

La primera razón posible es que al cablemódem no se le ha asignado un archivo de configuración DOCSIS que especifique que el cablemódem utiliza privacidad de línea de base. Controle que el archivo de configuración DOCSIS posea activada la BPI en el perfil de clase de servicio enviado al módem.

La segunda causa de ver un módem en el estado en línea pudo ser que el módem está a la espera antes de que comience a negociar la BPI. Espere un minuto o dos para ver si el módem cambia al estado online(pt) (en línea [pt]).

La causa final podría ser que el módem no contiene firmware que admita privacidad en la línea de base. Póngase en contacto con su proveedor de módems para obtener una versión más reciente del firmware compatible con BPI.

Los cablemódems aparecen en estado reject(pk) y luego se desconectan.

El motivo más común por el cual el módem ingresa en el estado reject(pk) es que la autenticación del cablemódem fue habilitada con el comando cable privacy authenticate-modem pero AAA se configuró incorrectamente. Verifique que los números de serie y las direcciones MAC de los módems afectados se hayan ingresado adecuadamente en la base de datos de autenticación y que todo servidor RADIUS externo funcione y se pueda alcanzar. Puede usar los comandos de depuración del router, debug aaa authentication y debug radius, para conocer el estado del servidor RADIUS o la razón por la que un módem no logra la autenticación.

Nota: Para obtener información general sobre la resolución de problemas de conectividad del cablemódem, consulte Resolución de problemas de cablemódems uBR que no se conectan.

Nota especial – comandos ocultos

Las referencias a los comandos ocultos en este documento aparecen únicamente con fines informativos. Los comandos ocultos no son compatibles con el Centro de asistencia técnica de Cisco (TAC). Además, comandos ocultos:

- No es seguro que siempre genere información correcta o confiable.
- Si se lo ejecuta, puede causar efectos colaterales inesperados
- Puede que no se comporte de la misma manera en diferentes versiones de Cisco IOS Software
- Puede eliminarse de futuras versiones del software Cisco IOS en cualquier momento sin previo aviso

Información Relacionada

- CableLabs
- Autenticación, autorización y administración (AAA)
- Soporte Técnico - Cisco Systems