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

Contenido

Introducción
Antes de comenzar
Convenciones
prerrequisitos
Componentes Utilizados
Cómo configurar la privacidad de la línea base para cablemódems
Cómo determinar si un cablemódem usa privacidad de línea de base
Temporizadores que afectan el establecimiento y el mantenimiento de la privacidad de la línea base
Vida útil de KEK
Tiempo de tolerancia KEK
Vida útil de TEK
Tiempo de tolerancia TEK
Autorizar el tiempo de espera
Vuelva a autorizar el tiempo de espera
Autorización de tiempo de espera tolerado
Autorizar el tiempo de espera para el rechazo
Tiempo de espera operativo
Regenerar valor de tiempo de espera
Comandos de configuración de Privacidad de la línea base del CMTS de Cisco.
cable privacy
cable privacy mandatory
cable privacy authenticate-modem
Comandos utilizados para supervisar el estado de BPI
Solución de problemas de BPI
Nota especial – comandos ocultos
Información Relacionada

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.

Productos del sistema de terminación del módem de cable de Cisco (CMTS) y del módem de

cable que funcionan con las imágenes del Cisco IOS ® Software con un conjunto de características incluyendo la privacidad de la línea base del soporte de los caracteres el "k1" el or"k8", por ejemplo ubr7200-k1p-mz.121-6.EC1.bin.

Este documento discute la privacidad de la línea base en los Productos Cisco que actúan 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.

prerrequisitos

No hay requisitos previos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en configurar un uBR7246VXR que funciona con la versión 12.1(6)EC del Cisco IOS ® Software, pero también aplica a todo otros Cisco los productos CMTS y las versiones de software.

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). 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 módem de cable intentará solamente utilizar la privacidad de la línea base si ordenan que haga tan vía los parámetros de clase de servicio en un archivo de configuración de DOCSIS. El archivo de configuración de DOCSIS contiene los parámetros del funcionamiento para el módem, y se descarga con el TFTP como parte del proceso de venir en línea.

Un método de crear un archivo de configuración de DOCSIS es utilizar el configurador del cablemódem DOCSIS en el cisco.com. Usando el configurador del cablemódem DOCSIS, usted puede crear un archivo de configuración de DOCSIS que ordene a un módem de cable que utilice la privacidad de la línea base fijando el campo del Baseline Privacy Enable bajo lengueta de la clase del servicio a **encendido**. Refiera al ejemplo abajo:

Alternativamente, la versión autónoma de la configuración del archivo de DOCSIS del se puede utilizar para habilitar la privacidad de la línea base como se muestra abajo:

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 módem de cable se registre con un Cisco CMTS ingresa al estado en línea. Un módem de cable necesita conseguir a este estado antes de que pueda negociar los parámetros de la privacidad de la línea base con Cisco CMTS. En este momento el tráfico de datos enviado entre el módem de cable y el CMTS es unencrypted. 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 del online(pk) significa que el módem de cable ha podido negociar un **Authorization Key**, si no conocido como **clave de encripción de claves (KEK)** con Cisco CMTS. 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. El KEK es 56 dominantes del bit usado para proteger las negociaciones subsiguientes de la privacidad de la línea base. Cuando un módem está en el tráfico de datos del estado del online(pk) enviado entre el módem de cable y Cisco CMTS es todavía unencrypted pues no se ha negociado ninguna clave para el tráfico de la encripción de datos todavía. Típicamente, el online(pk) es seguido por el online(pt).

reject(pk)

Este estado indica que los intentos del cablemódem de negociar una KEK han fallado. La mayoría de las razones comunes que un módem estaría en este estado serían que Cisco CMTS tiene autenticación de módem girada y el módem tienen autenticación fallida.

online(pt)

En este momento el módem ha negociado con éxito una clave de encripción de tráfico (TEK) con Cisco CMTS. El TEK se utiliza para cifrar el tráfico de datos entre el módem de cable y Cisco CMTS. El proceso de negociación TEK se cifró mediante el uso de KEK. El TEK es 56 o 40 dominantes del bit usado para cifrar el tráfico de datos entre el módem de cable y Cisco CMTS. En este momento la privacidad de la línea base es establecida con éxito y que se ejecuta, por lo tanto los datos del usuario enviados entre Cisco CMTS y módem de cable se están cifrando.

reject(pt)

Este estado indica que el módem de cable no podía negociar con éxito un TEK con Cisco CMTS.

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.

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

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 de DOCSIS. Hay poca razón para cambiar ninguno de estos parámetros a excepción de la vida útil de KEK y de la vida útil de 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 vida útil de KEK es la cantidad de tiempo que el módem de cable y Cisco CMTS deben considerar el KEK negociado para ser válida. Antes de que esta cantidad de tiempo haya pasado, el módem de cable debe renegociar un nuevo KEK con Cisco CMTS.

Usted puede configurar este vez usando el comando cmts cable interface 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 voluntad KEK dura por un período de tiempo más corto y por lo tanto si se corta el KEK menos negociaciones del futuro TEK serían susceptibles al secuestro. La desventaja a esto es que la renegociación KEK aumenta la utilización de la CPU en el Cable módems y aumenta el tráfico de la administración de BPI en una planta de cable.

Tiempo de tolerancia KEK

El tiempo de tolerancia KEK es la cantidad de tiempo antes de que expire la vida útil de KEK, eso que un módem de cable se significa para comenzar a negociar con Cisco CMTS para un nuevo KEK. La idea de colocar este temporizador consiste en que el cablemódem tenga tiempo suficiente para renovar el KEK antes de que caduque.

Usted puede configurar este vez usando el comando cmts cable interface 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 completa este campo del archivo de configuración de DOCSIS entonces toma la precedencia 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 vida útil de TEK es la cantidad de tiempo que el módem de cable y Cisco CMTS deben considerar el TEK negociado para ser válida. Antes de que esta cantidad de tiempo haya pasado, el módem de cable debe renegociar un nuevo TEK con Cisco CMTS.

Usted puede configurar este vez usando el comando cmts cable interface de Cisco:

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

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

Teniendo un más pequeño vida útil de TEK aumenta la seguridad porque cada voluntad TEK dura por un período de tiempo más corto y por lo tanto si se corta el TEK menos datos serán expuestos al desciframiento desautorizado. La desventaja a esto es que la renegociación TEK aumenta la utilización de la CPU en el Cable módems y aumenta el tráfico de la administración de BPI en una planta de cable.

Tiempo de tolerancia TEK

El tiempo de tolerancia TEK es la cantidad de tiempo antes de que expire la vida útil de TEK que un módem de cable está significado para comenzar a negociar con Cisco CMTS para un nuevo TEK. La idea detrás del tener este temporizador es de modo que el módem de cable tenga bastante tiempo de renovar el TEK antes de que expire.

Usted puede configurar este vez usando el comando cmts cable interface 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 completa este campo del archivo de configuración de DOCSIS entonces toma la precedencia 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 gobierna la cantidad de tiempo que un módem de cable esperará una respuesta de Cisco CMTS al negociar un KEK por primera vez.

Usted puede configurar este vez en un archivo de configuración de DOCSIS modificando el campo del **tiempo de espera del autorizar** bajo lengueta de la privacidad de la línea 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 gobierna la cantidad de tiempo que un módem de cable esperará una respuesta de Cisco CMTS al negociar un nuevo KEK porque la vida útil de KEK es alrededor expirar.

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 10 segundos y el intervalo válido es 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 1 a 1800 segundos.

Autorizar el tiempo de espera para el rechazo

Si un módem de cable intenta negociar un KEK con Cisco CMTS, pero se rechaza, debe esperar el tiempo de espera del rechazo del autorizar antes de re-intentar negociar un nuevo KEK.

Usted puede configurar este parámetro en un archivo de configuración de DOCSIS usando el campo del **tiempo de espera del rechazo del autorizar** bajo lengueta de la privacidad de la línea 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 gobierna la cantidad de tiempo que un módem de cable esperará una respuesta de Cisco CMTS 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 gobierna la cantidad de tiempo que un módem de cable esperará una respuesta de Cisco CMTS al negociar un nuevo TEK porque la vida útil de TEK es alrededor expirar.

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 configuran al **comando no cable privacy** en una interfaz del cable, después no se permitirá ningún Cable módems negociar la privacidad de la línea base al venir en línea en esa interfaz. Tenga cuidado al inhabilitar la privacidad de la línea base porque si se ordena a un módem de cable que utilice la privacidad de la línea base por su archivo de configuración de DOCSIS, y Cisco CMTS rechaza dejarlo negociar la privacidad de la línea base, después el módem puede no poder permanecer en línea.

cable privacy mandatory

Si configuran al **comando cable privacy mandatory** y un módem de cable tiene privacidad de la línea base habilitada en su archivo de configuración de DOCSIS, después el módem de cable debe negociar con éxito y privacidad de la línea base del uso no será permitido de otra manera permanecer en línea.

Si el archivo de configuración de DOCSIS de un módem de cable no da instrucciones el módem para utilizar la privacidad de la línea base entonces de sigue habiendo el **comando cable privacy mandatory** no parará el módem en línea.

No habilitan al **comando cable privacy mandatory** por abandono.

cable privacy authenticate-modem

Se puede realizar una forma de autenticación para los módems que aplican la privacidad de la línea base. Cuando el Cable módems negocia un KEK con Cisco CMTS, los módems transmiten los detalles de su dirección MAC de 6 bytes y de su número de serie a Cisco CMTS. Estos parámetros se pueden utilizar como Combinación de nombre de usuario/contraseña con el fin del Cable módems de autenticidad. 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.

Caution: Puesto que esta característica hace uso del servicio AAA usted necesita aseegurarse que usted tenga cuidado al modificar la configuración AAA, si no usted puede perder inadvertidamente la capacidad de registrar en y de manejar su Cisco CMTS.

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. Observe que un módem se ha configurado con un número de serie obviamente incorrecto.

Lo que sigue ejemplo parcial de configuración CMTS de Cisco utiliza una base de datos de autenticación local para autenticar vario Cable módems.

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

Otro método de autenticar los módems sería emplear a un servidor RADIUS externo. Aquí está un ejemplo parcial de la Configuración CMTS de Cisco que utiliza a un servidor RADIUS externo para autenticar los módems

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

Abajo está un archivo de base de datos de los usuarios de RADIUS de la muestra con la información equivalente al ejemplo anterior que utilizó la autenticación local. El archivo de usuarios es utilizado por varios servidores de RADIUS comerciales y del freeware como base de datos donde se salva la información de autenticación de usuario.

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

Se muestra abajo la salida de un comando show cable modem ejecutado en Cisco CMTS cuál utiliza cualquiera de los ejemplos de configuración antedichos. 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.

El módem con SID 17 no tiene una entrada en la base de datos de autenticación sino puede venir en línea porque su archivo de configuración de DOCSIS no le ha ordenado a que utilice la privacidad de la línea 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 venir en línea porque, aunque haya una entrada en la base de datos de autenticación con la dirección MAC de este módem, el número de serie correspondiente es incorrecto. Este módem está en el estado del reject(pk) pero actualmente transición al estado fuera de línea después de un período breve.

Cuando la autenticación del fall de los módems un mensaje a lo largo de las siguientes líneas se agrega 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.

Note: Cisco no recomienda que los clientes utilicen el comando cable privacy autenticate-modem para evitar que se conecten cablemódems no autorizados. Una manera más eficiente de asegurarse de que los clientes no autorizados no consigan el acceso a una red de proveedor de servicio es configurar el sistema de abastecimiento tales que el Cable módems desautorizado está dado instrucciones para descargar un archivo de configuración de DOCSIS con el campo definido del acceso a la red a apagado. De esta manera, el módem no desperdiciará ancho de banda ascendente de valor al volver a determinar las distancias continuamente. En lugar, el módem conseguirá al **en línea (d) el** estado que indica que no concederán los usuarios detrás del módem el acceso al módem de proveedor de servicio a la red y utilizará solamente 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] — se utiliza este comando de visualizar los temporizadores asociados al KEK o al TEK como fija en una interfaz CMTS.

Abajo está una salida de ejemplo 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 statistic — Este comando oculto puede ser utilizado para ver las estadísticas sobre el número de SID usando la privacidad de la línea base en una interfaz del cable particular.

Abajo está una salida de ejemplo 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 el debugging de la privacidad de la línea base. Cuando se activa este comando, siempre que ocurra un cambio en el estado de la privacidad de la línea base o un evento de la privacidad de la línea base, los detalles serán visualizados en la consola. Este comando trabaja solamente cuando está precedido con el **comando debug cable interface cable X/0 o debug cable mac-address mac-address**.

bpiatp del cable del debug — Este comando activa el debugging de la privacidad de la línea base. Cuando se activa este comando, siempre que un mensaje de la privacidad de la línea base sea enviado o recibido por Cisco CMTS, el volcado hexadecimal del mensaje será visualizado. Este comando trabaja solamente cuando está precedido con el **comando debug cable interface cable X/0 o debug cable mac-address mac-address**.

keyman del cable del debug — Este debugging activado comando de la administración de claves de la privacidad de la línea base. Cuando se activa este comando visualizan a los detalles de la administración de claves de la privacidad de la línea 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. Entre en contacto a su proveedor de módem para una más versión reciente del firmware que soporta el 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.

Note: Para información general sobre la conectividad de cable módem del troubleshooting, refiera al Online que no viene del Cable módems del uBR del troubleshooting.

Nota especial – comandos ocultos

Las referencias a los comandos ocultos en este documento aparecen únicamente con fines informativos. El Centro de Asistencia Técnica de Cisco (TAC) no soportan a los comandos ocultos. Además comandos ocultos:

- No es seguro que siempre genere información correcta o confiable.
- Si se lo ejecuta, puede causar efectos colaterales inesperados
- No puede comportarse la misma manera en diversas versiones del Cisco IOS Software
- Puede ser quitado de las futuras versiones del Cisco IOS Software en cualquier momento sin previó aviso

Información Relacionada

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