Privacidade de linha de base DOCSIS 1.0 no Cisco CMTS

Contents

Introduction

O objetivo principal das Especificações de Interface de Serviço de Dados sobre Cabo (DOCSIS - Data-over-Cable Service Interface Specifications) da Interface de Privacidade de Linha de Base (BPI - Baseline Privacy Interface) é fornecer um esquema simples de criptografia de dados para proteger os dados enviados de e para modems a cabo em uma rede de Dados sobre Cabo. A privacidade de linha de base pode também ser usada como meio de autenticar modems a cabo e autorizar a transmissão de tráfego multicast para modems a cabo.

Cisco Cable Modem Termination System (CMTS) e produtos de modem a cabo executando

imagens do Software Cisco IOS® com um conjunto de recursos que inclui os caracteres "k1" ou "k8" suportam a privacidade de linha de base, por exemplo, ubr7200-k1p-mz.121-6.EC1.bin.

Este documento discute a privacidade de linha de base em produtos Cisco que operam no modo DOCSIS1.0.

Antes de Começar

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Prerequisites

Não existem requisitos específicos para este documento.

Componentes Utilizados

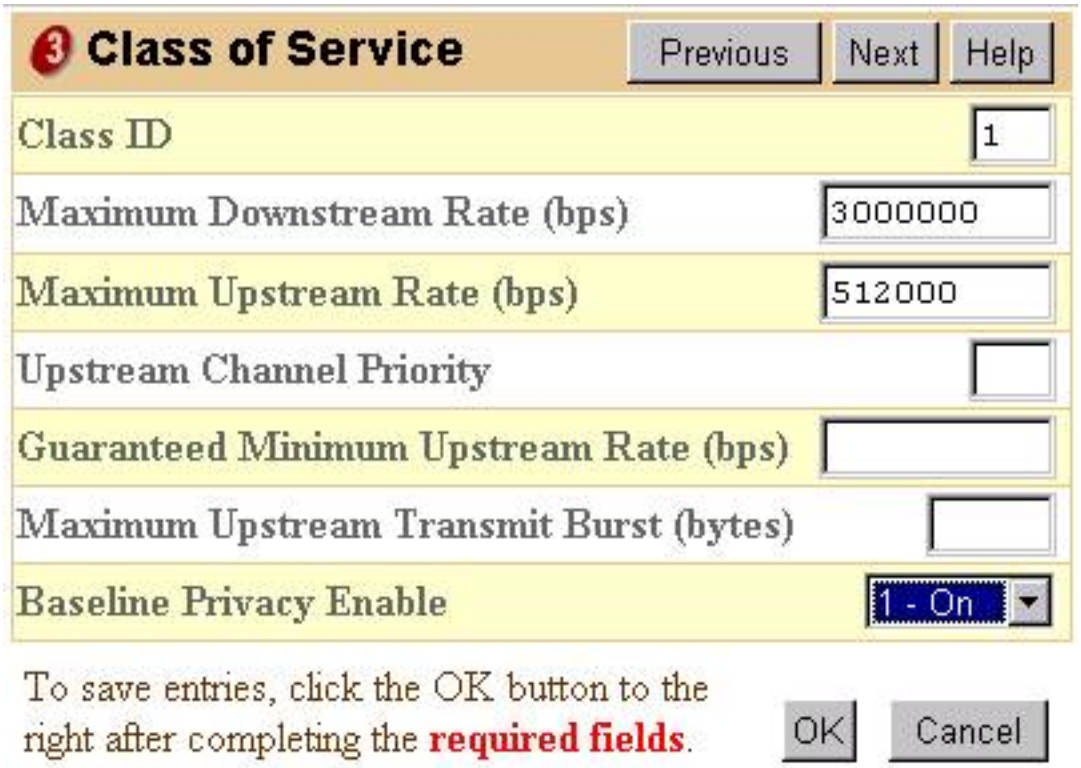
As informações neste documento são baseadas na configuração de um uBR7246VXR executando o Cisco IOS® Software Release 12.1(6)EC, mas também se aplicam a todos os outros produtos Cisco CMTS e versões de software.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se você estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

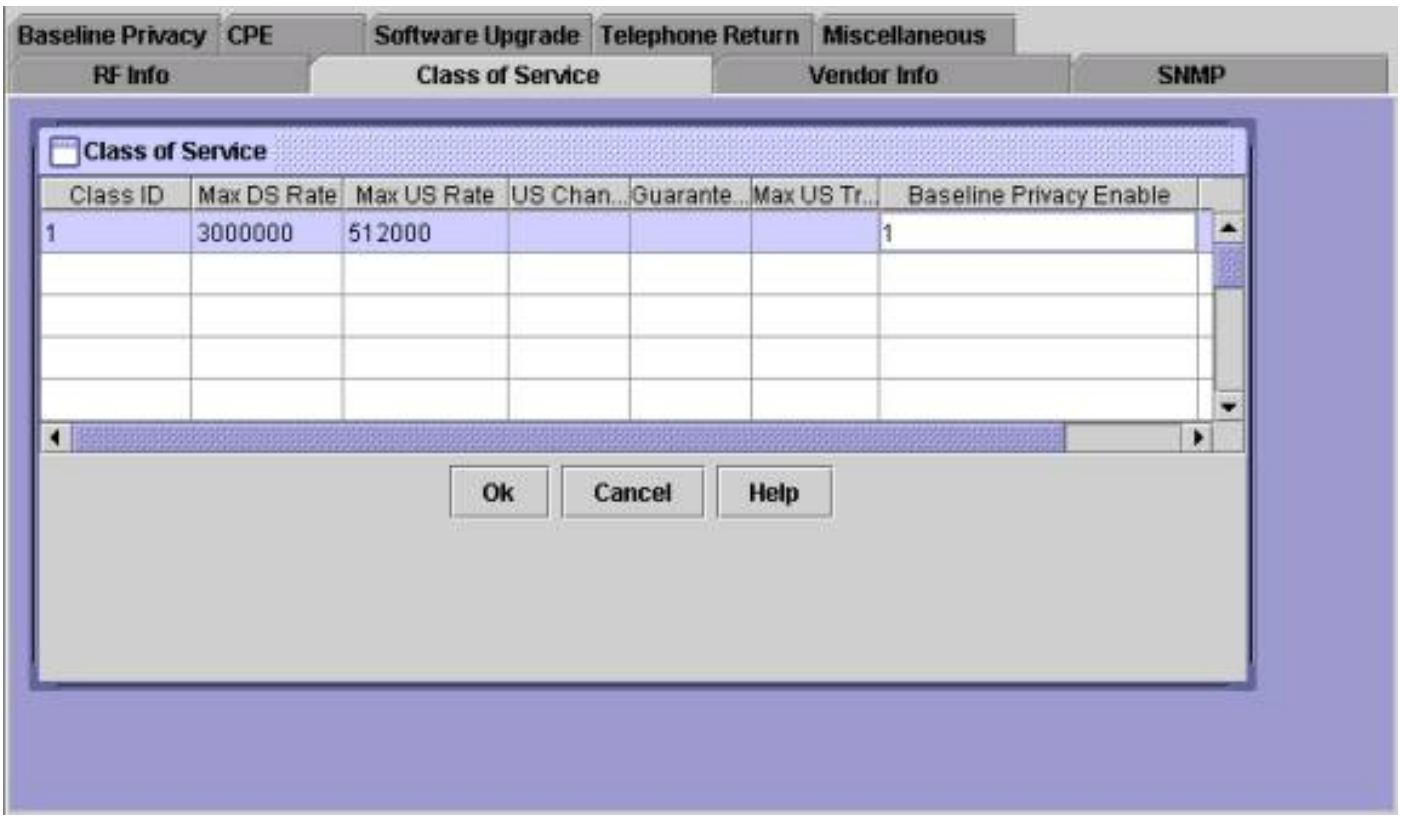
Como configurar privacidade de linha de base para modems a cabo

Um modem a cabo só tentará usar a privacidade de linha de base se for solicitado a fazê-lo através dos parâmetros de classe de serviço em um arquivo de configuração DOCSIS. O arquivo de configuração DOCSIS contém parâmetros operacionais para o modem e é baixado através do TFTP como parte do processo de entrada on-line.

Um método para criar um arquivo de configuração DOCSIS é usar o Configurador de Modem a Cabo DOCSIS em Cisco.com. Usando o Configurador de Modem a Cabo DOCSIS, você pode criar um arquivo de configuração DOCSIS que comanda um Modem a Cabo para usar a privacidade da linha de base, definindo o campo Baseline Privacy Enable (Ativação da privacidade da linha de base) na guia Class of Service (Classe de serviço) como **On (Ativado)**. Consulte o exemplo abaixo:



Como alternativa, a versão independente da configuração do arquivo DOCSIS de pode ser usada para ativar a privacidade da linha de base, como mostrado abaixo:



Após a criação de um arquivo de configuração de DOCSIS que suporte BPI, os modems a cabo precisam ser reinicializados para fazer o download do novo arquivo de configuração e, em seguida, empregar a privacidade da linha de base.

Como saber se um modem a cabo está utilizando privacidade de linha de base

Em um Cisco CMTS, é possível usar o comando show cable modem para visualizar o status dos cable modems individuais. Existem vários estados nos quais um modem que utiliza a privacidade de Linha de Base pode aparecer.

on-line

Depois que um modem a cabo se registra com um Cisco CMTS, ele entra no estado on-line. Um modem a cabo precisa chegar a esse estado antes de poder negociar parâmetros de privacidade de linha de base com um Cisco CMTS. Nesse ponto, o tráfego de dados enviado entre o modem a cabo e o CMTS é descriptografado. Se um modem a cabo permanecer nesse estado e não prosseguir para nenhum dos estados mencionados abaixo, é sinal de que o modem não esta utilizando a privacidade da linha de base.

online(pk)

O estado online(pk) significa que o modem a cabo foi capaz de negociar uma **chave de autorização**, também conhecida como **chave de criptografia chave (KEK)** com o Cisco CMTS. Isso significa que o modem a cabo está autorizado a usar a privacidade da linha de base e foi bem-sucedido na negociação da primeira fase da privacidade da linha de base. O KEK é uma chave de 56 bits usada para proteger as negociações de privacidade de linha de base subsequentes. Quando um modem está no estado on-line (pk), o tráfego de dados enviado entre o modem a cabo e o Cisco CMTS ainda é não criptografado, pois nenhuma chave para a criptografia do tráfego de dados foi negociada ainda. Normalmente, online(pk) é seguido por online(pt).

rejeitar(pk)

Esse estado indica que as tentativas do modem a cabo de negociar um KEK falharam. O motivo mais comum para um modem estar nesse estado é que o Cisco CMTS tem a autenticação de modem ativada e o modem não tem autenticação.

online(pt)

Nesse ponto, o modem negociou com êxito uma chave de criptografia de tráfego (TEK) com o Cisco CMTS. O TEK é usado para criptografar o tráfego de dados entre o modem a cabo e o Cisco CMTS. O processo de negociação TEK foi criptografado, usando o KEK. O TEK é uma chave de 56 ou 40 bits usada para criptografar o tráfego de dados entre o modem a cabo e o Cisco CMTS. Neste ponto, a privacidade da linha de base é estabelecida e executada com êxito, portanto, os dados do usuário enviados entre o Cisco CMTS e o modem a cabo estão sendo criptografados.

reject(pt)

Esse estado indica que o modem a cabo não conseguiu negociar um TEK com o Cisco CMTS.

Consulte os itens abaixo para obter uma saída de exemplo de um comando show cable modem exibindo cable modems em vários estados relacionados à privacidade da linha de 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 obter mais informações sobre o status do modem a cabo, consulte Troubleshooting uBR Cable Modems Not Coming Online (Solucionando problemas de modems a cabo uBR não entrando on-line).

Cronômetros que afetam o estabelecimento e a manutenção de privacidade da linha de base

Há alguns valores de timeout que podem ser modificados para alterar o comportamento da privacidade de linha de base. Alguns desses parâmetros podem ser configurados no Cisco CMTS e outros através do arquivo de configuração DOCSIS. Há poucos motivos para alterar qualquer um desses parâmetros, exceto pelo tempo de vida do KEK e pelo tempo de vida do TEK. Esses cronômetros podem ser modificados de forma a aumentar a segurança em uma planta de cabos ou reduzir a overhead de CPU e tráfego devido ao gerenciamento da BPI.

KEK Lifetime

O tempo de vida do KEK é o tempo que o Cable Modem e o Cisco CMTS devem considerar válido o KEK negociado. Antes que esse período tenha passado, o modem a cabo deve renegociar um novo KEK com o Cisco CMTS.

Você pode configurar desta vez usando o comando de interface de cabo Cisco CMTS:

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

A configuração padrão é 604.800 segundos, que corresponde a sete dias.

Ter uma vida KEK menor aumenta a segurança porque cada KEK irá durar um período mais curto e, portanto, se o KEK for hackeado menos as futuras negociações TEK seriam susceptíveis de serem sequestradas. A desvantagem disso é que a renegociação KEK aumenta a utilização da CPU em modems a cabo e aumenta o tráfego de gerenciamento de BPI em uma planta a cabo.

KEK Grace Time

O tempo de carência KEK é o período de tempo antes da expiração do KEK, que um modem a cabo deve começar a negociar com o Cisco CMTS para um novo KEK. O propósito desse temporizador é fazer com que o modem a cabo tenha tempo suficiente para renovar o KEK antes que ele expire.

Você pode configurar desta vez usando o comando de interface de cabo Cisco CMTS:

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

Você também pode configurar esse horário usando o arquivo de configuração DOCSIS preenchendo o campo rotulado Authorization Grace Timeout (Tempo Limite Gratuito de Autorização) na guia Baseline Privacy (Privacidade de Linha de Base). Se esse campo de arquivo de configuração DOCSIS for preenchido, ele terá precedência sobre qualquer valor configurado no Cisco CMTS. O valor padrão para esse cronômetro é de 600 segundos, o que equivale a 10 minutos.

Vida útil do TEK

O tempo de vida útil do TEK é o tempo que o Cable Modem e o Cisco CMTS devem considerar válido o TEK negociado. Antes que esse período tenha passado, o modem a cabo deve renegociar um novo TEK com o Cisco CMTS.

Você pode configurar desta vez usando o comando de interface de cabo Cisco CMTS:

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

A configuração padrão são 43200 segundos, o que equivale a 12 horas.

Ter uma vida útil de TEK menor aumenta a segurança porque cada TEK durará por um período de tempo mais curto e, portanto, se o TEK for hackeado, menos dados serão expostos à descriptografia não autorizada. A desvantagem disso é que a renegociação TEK aumenta a utilização da CPU em modems a cabo e aumenta o tráfego de gerenciamento de BPI em uma planta a cabo.

Tempo adicional do TEK

O tempo de carência do TEK é o tempo antes da expiração do TEK que um modem a cabo deve começar a negociar com o Cisco CMTS para um novo TEK. A ideia por trás desse temporizador é que o modem a cabo tenha tempo suficiente para renovar o TEK antes que ele expire.

Você pode configurar desta vez usando o comando de interface de cabo Cisco CMTS:

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

Você também pode configurar esse horário usando o arquivo de configuração DOCSIS preenchendo o campo rotulado TEK Grace Timeout (Tempo Limite Gratuito TEK) na guia Baseline Privacy (Privacidade de Linha de Base). Se esse campo de arquivo de configuração DOCSIS for preenchido, ele terá precedência sobre qualquer valor configurado no Cisco CMTS.

O valor padrão para esse cronômetro é de 600 segundos, o que equivale a 10 minutos.

Autorize o intervalo de parada de espera

Esse tempo controla a quantidade de tempo que um modem a cabo esperará por uma resposta de um Cisco CMTS ao negociar um KEK pela primeira vez.

Você pode configurar esse tempo em um arquivo de configuração DOCSIS modificando o campo **Autorizar tempo limite de espera** na guia Privacidade da linha de base.

O valor padrão para este campo é 10 segundos, e o intervalo válido é de 2 a 30 segundos.

Autorize novamente o intervalo de parada de espera

Esse tempo regula o tempo que um modem a cabo esperará por uma resposta de um Cisco CMTS ao negociar um novo KEK porque o tempo de vida do KEK está prestes a expirar.

Você pode configurar desta vez em um arquivo de configuração DOCSIS pela modificação do campo Reauthorize Wait Timeout (Reautorizar intervalo de espera) na guia Baseline Privacy (Privacidade da linha de base).

O valor padrão para esse temporizador é de 10 segundos e o intervalo válido é de 2 a 30 segundos.

Intervalo gratuito de autorização

Especifica o período de cortesia para reautorização (em segundos). O valor padrão é 600. O intervalo válido é de 1 a 1800 segundos.

Autorize o intervalo de parada de rejeição

Se um modem a cabo tentar negociar um KEK com um Cisco CMTS, mas for rejeitado, ele deve aguardar o tempo limite de espera de rejeição de autorização antes de tentar negociar novamente um novo KEK.

Você pode configurar esse parâmetro em um arquivo de configuração DOCSIS usando o campo **Autorizar Rejeitar Tempo Limite de Espera** na guia Privacidade da Linha de Base. O valor padrão desse temporizador é de 60 segundos e o intervalo válido é de 10 segundos a 600 segundos.

Intervalo de parada de espera operacional

Esse tempo controla a quantidade de tempo que um modem a cabo esperará por uma resposta de um Cisco CMTS ao negociar um TEK pela primeira vez.

Você pode configurar esse tempo em um arquivo de configuração DOCSIS por meio da modificação do campo Operational Wait Timeout na guia Baseline Privacy.

O valor padrão deste campo é 1 segundo e o intervalo válido é de 1 a 10 segundos.

Intervalo de parada da espera de Rekey

Esse tempo regula o tempo que um modem a cabo esperará por uma resposta de um Cisco CMTS ao negociar um novo TEK porque a vida útil do TEK está prestes a expirar.

Você pode configurar esse período de tempo em um arquivo de configuração do DOCSIS, modificando o campo Rekey Wait Timeout (Intervalo de Espera) na guia Baseline Privacy (Privacidade de Linha de Base).

O valor padrão para este temporizador é 1 segundo e a faixa válida é de 1 a 10 segundos.

Comandos de configuração do Cisco CMTS Baseline Privacy

Os comandos da interface de cabo a seguir podem ser utilizados para configurar a função de privacidade da linha de base e as funções relacionadas a ela em um CMTS da Cisco.

cable privacy

O comando cable privacy habilita a negociação de privacidade de linha de base em uma interface específica. Se o comando **no cable privacy** estiver configurado em uma interface de cabo, nenhum modems a cabo terá permissão para negociar a privacidade da linha de base ao entrar on-line nessa interface. Tenha cuidado ao desabilitar a privacidade da linha de base, pois se um modem a cabo for solicitado a usar a privacidade da linha de base por seu arquivo de configuração DOCSIS, e o Cisco CMTS se recusar a permitir que ele negocie a privacidade da linha de base, o modem talvez não possa permanecer on-line.

cable privacy mandatory

Se o comando **cable privacy required** estiver configurado e um modem a cabo tiver a privacidade de linha de base habilitada em seu arquivo de configuração DOCSIS, então o modem a cabo deve negociar e usar com êxito a privacidade de linha de base, caso contrário, ele não poderá permanecer on-line.

Se o arquivo de configuração DOCSIS de um modem a cabo não instruir o modem a usar a privacidade da linha de base, o comando **cable privacy required** não impedirá que o modem permaneça on-line.

O comando **cable privacy required** não está ativado por padrão.

cable privacy authenticate-modem

Épossível realizar uma forma de autenticação para modems que participam da privacidade de linha de base. Quando os modems a cabo negociam um KEK com o Cisco CMTS, os modems transmitem detalhes de seu endereço MAC de 6 bytes e seu número de série para o Cisco CMTS. Esses parâmetros podem ser usados como uma combinação de nome de usuário/senha para fins de autenticação de modems a cabo. O CMTS da Cisco utiliza o serviço AAA (Autenticação, autorização e contabilização) do Cisco IOS para fazer isso. Os modems a cabo que não passam na autenticação não podem ficar on-line. Além disso, os modems a cabo que não utilizam privacidade de linha de base não são afetados por este comando.

Cuidado: como esse recurso usa o serviço AAA, você precisa ter cuidado ao modificar a configuração AAA, caso contrário, você pode perder inadvertidamente a capacidade de fazer login e gerenciar seu Cisco CMTS.

Aqui estão alguns exemplos de configuração para as maneiras de executar a autenticação de

modem. Nesses exemplos de configuração, diversos modems foram digitados em um banco de dados de autenticação. O endereço MAC de 6 octetos do modem serve como um nome de usuário, e o número de série de comprimento variável serve como uma senha. Observe que um modem foi configurado com um número de série obviamente incorreto.

A seguinte configuração parcial do Cisco CMTS usa um banco de dados de autenticação local para autenticar vários modems a cabo.

```
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
```

Outro método de autenticação de modems seria empregar um servidor RADIUS externo. Aqui está um exemplo de configuração parcial do Cisco CMTS que usa um servidor RADIUS externo para autenticar modems

```
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
```

Abaixo está um exemplo de arquivo de banco de dados de usuários RADIUS com informações equivalentes ao exemplo acima que usou a autenticação local. O arquivo de usuários é utilizado por vários servidores RADIUS comerciais e freeware como um banco de dados onde as informações de autenticação do usuário são armazenadas.

```
# 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
```

Abaixo é mostrada a saída de um comando **show cable modem** executado em um Cisco CMTS que usa um dos exemplos de configuração acima. Você verá que quaisquer modems ativados por privacidade de linha de base não listados no banco de dados de autenticação local, ou com o número de série incorreto entrarão no estado rejeitar(pk) e não permanecerão on-line.

```
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
```

O modem com SID 17 não tem uma entrada no banco de dados de autenticação, mas pode ficar on-line porque seu arquivo de configuração DOCSIS não o ordenou a usar a privacidade da linha de base.

Os modems com SIDs 18, 21 e 22 podem ficar on-line porque têm entradas corretas no banco de dados de autenticação

O modem com SID 19 não está habilitado a ficar on-line porque recebeu um comando para usar a privacidade de linha de base, mas não há nenhuma entrada no banco de dados de autenticação para esse modem. Para que o modem indique uma falha na autenticação, ele deve ter passado recentemente pelo estado de rejeição (de pacote).

O modem com SID 20 não pode ficar online porque, embora haja uma entrada no banco de dados de autenticação com o endereço MAC desse modem, o número de série correspondente está incorreto. No momento, esse modem está no estado reject(pk), mas passará para o estado offline após um curto período.

Quando os modems falham na autenticação, uma mensagem nas seguintes linhas é adicionada ao registro do Cisco CMTS.

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

O cable modem é removido da lista de manutenção de estações e será marcado como off-line dentro de 30 segundos. O modem a cabo provavelmente tentará ficar on-line novamente somente para ser mais uma vez rejeitado.

Observação: a Cisco não recomenda que os clientes usem o comando **cable privacy authenticate-modem** para impedir que modems a cabo não autorizados fiquem on-line. Uma maneira mais eficiente de garantir que clientes não autorizados não obtenham acesso à rede de um provedor de serviços é configurar o sistema de provisionamento de modo que modems a cabo não autorizados sejam instruídos a baixar um arquivo de configuração DOCSIS com o campo de acesso à rede definido como desativado. Dessa maneira, o modem não desperdiçará largura de banda upstream valiosa através de uma reorganização contínua. Em vez disso, o modem chegará ao estado **online(d)**, que indica que os usuários por trás do modem não terão acesso à rede do provedor de serviços e que o modem usará apenas a largura de banda upstream para manutenção da estação.

Comandos utilizados para monitorar o estado do BPI

show interface cable X/0 privacy [kek | tek] — Este comando é usado para exibir os temporizadores associados ao KEK ou ao TEK conforme definido em uma interface CMTS.

Abaixo está um exemplo de saída desse 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 pode ser usado para visualizar estatísticas sobre o número de SIDs usando a privacidade de linha de base em uma interface de cabo específica.

Abaixo está um exemplo de saída desse 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 ativa a depuração da privacidade da linha de base. Quando esse comando é ativado, sempre que ocorre uma alteração no estado de privacidade da linha de base ou um evento de privacidade da linha de base, os detalhes serão exibidos no console. Este comando só funciona quando precedido do comando **debug cable interface cable X/0** ou **debug cable mac-address** *mac-address*.

debug cable piatp — Este comando ativa a depuração da privacidade da linha de base. Quando esse comando é ativado, sempre que uma mensagem de privacidade de linha de base é enviada ou recebida pelo Cisco CMTS, o despejo hexadecimal da mensagem será exibido. Este comando só funciona quando precedido do comando **debug cable interface cable X/0** ou **debug cable mac-address** *mac-address*.

debug cable keyman —Este comando ativou a depuração do gerenciamento da chave de privacidade da linha de base. Quando esse comando é ativado, os detalhes do gerenciamento da chave de privacidade da linha de base são exibidos.

Troubleshooting de BPI

Os modems a cabo aparecem como online, em vez de online(pt).

Se um modem aparece no estado online, em vez de no online(pt), isso geralmente significa uma de três coisas.

O primeiro motivo provável é que o cable modem não recebeu um arquivo de configuração DOCSIS especificando que esse cable modem utiliza a privacidade de Linha de Base. Verifique se o arquivo de configuração DOCSIS tem o BPI habilitado no perfil de classe de serviço enviado ao modem.

A segunda causa para o modem estar no estado on-line pode ser o fato de ele estar esperando para começar a negociar a BPI. Aguarde um ou dois minutos para ver se o estado do modem

muda para on-line(pt).

A causa final pode ser que o modem não contenha um firmware capaz de suportar privacidade de linha de base. Entre em contato com o fornecedor do modem para obter uma versão mais recente do firmware que ofereça suporte a BPI.

Os modems a cabo aparecem no estado reject(pk) e, em seguida, ficam offline.

A causa mais provável para um modem entrar no estado reject(pk) é que a autenticação do modem de cabo foi ativada com o comando cable privacy authenticate-modem, mas AAA foi desconfigurado. Verifique se os números de série e endereços MAC dos modems afetados foram digitados corretamente no banco de dados de autenticação e se todos os servidores RADIUS externos estão acessíveis e funcionando. Você pode utilizar os comandos de depuração do roteador, debug aaa authentication e debug radius, para ter uma idéia do status do servidor RADIUS ou saber o motivo da falha de autenticação.

Nota: Para obter informações gerais sobre como solucionar problemas de conectividade de modem a cabo, consulte Troubleshooting de Modems a Cabo uBR Not Coming Online (SBR não está entrando online).

Observação especial – comandos ocultos

Qualquer referência a comandos ocultos neste documento serve apenas para questões informativas. Comandos ocultos não são suportados pelo Cisco Technical Assistance Center (TAC). Além de comandos ocultos:

- Nem sempre pode gerar informações confiáveis ou corretas
- Se executado, poderá causar efeitos colaterais inesperados
- Pode não se comportar da mesma maneira em diferentes versões do Cisco IOS Software
- Pode ser removido de versões futuras do Cisco IOS Software a qualquer momento sem aviso prévio

Informações Relacionadas

- Laboratórios de cabo
- Autenticação, Autorização e Auditoria (AAA)
- Suporte Técnico - Cisco Systems