Privacidade de linha de base DOCSIS 1.0 no Cisco CMTS

Índice

Introdução

O objetivo principal do Baseline Privacy Interface (BPI) do Data-over-Cable Service Interface Specifications (DOCSIS) é fornecer um esquema de criptografia dos dados simples proteger os dados enviados a e do Modems a cabo em uns dados sobre a rede de 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.

Produtos do sistema de terminação de Cable Modem da Cisco (CMTS) e do modem a cabo que executa imagens do Cisco IOS ® Software com um conjunto de recursos que inclui a privacidade

da linha de base do apoio dos caráteres "k1" or"k8", por exemplo ubr7200-k1p-mz.121-6.EC1.bin.

Este documento discute a privacidade da linha de base no Produtos da Cisco que opera-se no modo DOCSIS1.0.

Antes de Começar

Convenções

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

Pré-requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada em configurar um uBR7246VXR que executa a liberação 12.1(6)EC do Cisco IOS ® Software, mas igualmente aplica a todo outros Cisco produtos cmts e software release.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. 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 tentará somente usar a privacidade da linha de base se se comanda para fazer assim através das classes de parâmetro de serviço em um arquivo de configuração DOCSIS. O arquivo de configuração DOCSIS contém parâmetros operacionais para o modem, e é transferido com o TFTP como parte do processo de vinda em linha.

Um método de criar um arquivo de configuração DOCSIS é usar o configurador do Cable Modem DOCSIS no cisco.com. Usando o configurador do Cable Modem DOCSIS, você pode criar um arquivo de configuração DOCSIS que comande um modem a cabo para usar a privacidade da linha de base ajustando o campo do Baseline Privacy Enable sob a aba da classe de serviço a **sobre**. Refira o exemplo abaixo:

Alternativamente, a versão independente da configuração do arquivo DOCSIS do pode ser usada para permitir como mostrado a privacidade da linha de base 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 Cisco CMTS entra no estado on-line. Um modem a cabo precisa de obter a este estado antes que possa negociar parâmetros da privacidade da linha de base com Cisco CMTS. Neste momento o tráfego de dados enviado entre o modem a cabo e o CMTS é unencrypted. 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 do online(pk) significa que o modem a cabo pôde negociar um **Authorization Key**, se não sabido como uma **chave de criptografia chave (KEK)** com 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 um 56 chaves do bit usado para proteger negociações subsequentes da privacidade da linha de base. Quando um modem está no tráfego de dados do estado do online(pk) enviado entre o modem a cabo e Cisco CMTS é ainda unencrypted porque nenhuma chave para a criptografia do tráfego de dados foi negociada ainda. Tipicamente, o online(pk) é seguido pelo online(pt).

rejeitar(pk)

Esse estado indica que as tentativas do modem a cabo de negociar um KEK falharam. A maioria de motivo comum que um modem estaria neste estado seria que Cisco CMTS tem a autenticação de modem girada sobre e o modem tem a autenticação falha.

online(pt)

Neste momento o modem negociou com sucesso uma chave de criptografia de tráfego (TEK) com Cisco CMTS. O TEK é usado para cifrar o tráfego de dados entre o modem a cabo e Cisco CMTS. O processo de negociação TEK foi criptografado, usando o KEK. O TEK é um 56 ou 40 chaves do bit usado para cifrar o tráfego de dados entre o modem a cabo e Cisco CMTS. Neste momento a privacidade da linha de base é estabelecida com sucesso e sendo executado, consequentemente os dados do usuário enviados entre Cisco CMTS e modem a cabo estão sendo cifrados.

reject(pt)

Este estado indica que o modem a cabo era incapaz de negociar com sucesso um TEK com 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.

Nota: Para obter mais informações sobre status de modem a cabo, consulte Troubleshooting uBR Cable Modems Not Coming Online (Solucionando problemas de modems a cabo uBR que não ficam 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 destes parâmetros podem ser configurados em Cisco CMTS e outro através do arquivo de configuração DOCSIS. Há pouca razão mudar qualquens um parâmetros à exceção do tempo de vida de KEK e da duração de 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.

Tempo de vida de KEK

O tempo de vida de KEK é a quantidade de tempo que o modem a cabo e Cisco CMTS devem considerar o KEK negociado para ser válida. Antes que esta quantidade de tempo passe, o modem a cabo deve renegociar um KEK novo com Cisco CMTS.

Você pode configurar esta vez usando o comando cmts cable interface de Cisco:

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

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

Ter um tempo de vida de KEK menor aumenta a Segurança porque cada vontade KEK dura por um período de tempo mais curto e daqui se o KEK é cortado menos negociações do futuro TEK seriam susceptíveis à sequestração. O inconveniente a este é que a negociação nova KEK aumenta a utilização CPU no Modems a cabo e aumenta o tráfego do gerenciamento BPI em uma planta de cabos.

Tempo adicional KEK

O tempo adicional KEK é a quantidade de tempo antes que o tempo de vida de KEK expire, isso que um modem a cabo é significado começar negociar com Cisco CMTS para um KEK novo. 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 esta vez usando o comando cmts cable interface de Cisco:

```
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 este campo do arquivo de configuração DOCSIS é preenchido então toma a precedência sobre todo o valor configurado em Cisco CMTS. O valor padrão para esse cronômetro é de 600 segundos, o que equivale a 10 minutos.

Duração de TEK

A duração de TEK é a quantidade de tempo que o modem a cabo e Cisco CMTS devem considerar o TEK negociado para ser válida. Antes que esta quantidade de tempo passe, o modem a cabo deve renegociar um TEK novo com Cisco CMTS.

Você pode configurar esta vez usando o comando cmts cable interface de Cisco:

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

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

Ter uma Vida útil do TEK aumenta a segurança menor porque cada vontade TEK dura por um período de tempo mais curto e daqui se o TEK é cortado menos dados será exposto a descriptografia desautorizada. O inconveniente a este é que a negociação nova TEK aumenta a utilização CPU no Modems a cabo e aumenta o tráfego do gerenciamento BPI em uma planta de cabos.

Tempo adicional do TEK

O tempo do grace do tek é a quantidade de tempo antes que a duração de TEK expire que um modem a cabo está significado começar negociar com Cisco CMTS para um TEK novo. A ideia atrás de ter este temporizador é de modo que o modem a cabo tenha bastante tempo para renovar o TEK antes que expire.

Você pode configurar esta vez usando o comando cmts cable interface de Cisco:

```
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 este campo do arquivo de configuração DOCSIS é preenchido então toma a precedência sobre todo o valor configurado em 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

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

Você pode configurar esta vez em um arquivo de configuração DOCSIS alterando o campo do **timeout de espera da autorização** sob a aba da 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

Esta vez governa a quantidade de tempo que um modem a cabo esperará uma resposta de Cisco CMTS ao negociar um KEK novo porque o tempo de vida de KEK está a ponto de 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 este temporizador é os segundos 10 e o intervalo válido é 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 1 a 1800 segundos.

Autorize o intervalo de parada de rejeição

Se um modem a cabo tenta negociar um KEK com Cisco CMTS, mas é rejeitado, deve esperar o timeout de espera da rejeição da autorização antes de re-tentar negociar um KEK novo.

Você pode configurar este parâmetro em um arquivo de configuração DOCSIS usando o campo do **timeout de espera da rejeição da autorização** sob a aba da 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

Esta vez governa a quantidade de tempo que um modem a cabo esperará uma resposta de 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

Esta vez governa a quantidade de tempo que um modem a cabo esperará uma resposta de Cisco CMTS ao negociar um TEK novo porque a duração de TEK está a ponto de 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** é configurado em uma interface de cabo, a seguir nenhum Modems a cabo estará permitido negociar a privacidade da linha de base ao vir em linha nessa relação. Use o cuidado ao desabilitar a privacidade da linha de base porque se um modem a cabo está comandado para usar a privacidade da linha de base por seu arquivo de configuração DOCSIS, e Cisco CMTS recusa o deixar negociar a privacidade da linha de base, a seguir o modem não pode poder permanecer em linha.

cable privacy mandatory

Se o **comando cable privacy mandatory** é configurado e um modem a cabo tem a privacidade da linha de base permitida em seu arquivo de configuração DOCSIS, a seguir o modem a cabo deve com sucesso negociar e privacidade da linha de base do uso não será permitido de outra maneira permanecer em linha.

Se o arquivo de configuração DOCSIS de um modem a cabo não instrui o modem para usar a privacidade da linha de base então o **comando cable privacy mandatory** não parará o modem de permanecer em linha.

O comando cable privacy mandatory não é permitido à revelia.

cable privacy authenticate-modem

Épossível realizar uma forma de autenticação para modems que participam da privacidade de linha de base. Quando o Modems a cabo negocia um KEK com Cisco CMTS, o Modems transmite detalhes de seu MAC address do byte 6 e de seu número de série a Cisco CMTS. Estes parâmetros podem ser usados como uma combinação de nome de usuário/senha com a finalidade do Modems a cabo de autenticação. 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: Desde que esta característica utiliza o serviço AAA você precisa de certificar-se de que você é cuidadoso ao alterar a configuração de AAA, se não você pode inadvertidamente perder a capacidade para registrar em e controlar 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. Note que um modem esteve configurado com um número de série obviamente incorreto.

A seguinte amostra parcial de configuração do Cisco CMTS usa um base de dados de autenticação local para autenticar um número de 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
```

Um outro método de autenticar o Modems seria empregar um servidor de raio externo. Está aqui um exemplo parcial da configuração de CMTS de Cisco que use um servidor de raio externo para autenticar o 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
```

Está abaixo um arquivo da base de dados dos usuários RADIUS da amostra com a informação equivalente ao exemplo acima que usou a autenticação local. O arquivo de usuários é utilizado por um número de servidores Radius comerciais e do freeware como um base de dados onde a informação de autenticação de usuário seja armazenada.

```
# 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 = "034103902000018352 52"


             Service-Type = Framed
```

Émostrada abaixo a saída de um **comando show cable modem** executado em Cisco CMTS qual usa qualquer 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.

O modem com SID 17 não tem uma entrada na base de dados de autenticação mas pode vir em linha porque seu arquivo de configuração DOCSIS não a comandou para 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 é incapaz de vir em linha porque, embora haja uma entrada na base de dados de autenticação com MAC address deste modem, o número de série correspondente está incorreto. Presentemente este modem está no estado do reject(pk) mas transição ao estado off-line após um período curto.

Quando a autenticação da falha do Modems uma mensagem ao longo das seguintes linhas for adicionada ao log de 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.

Nota: A Cisco não recomenda que os clientes usem o comando cable privacy authenticate-modem para impedir que cable modems não autorizados sejam colocados on-line. Uma maneira

de mais eficiente de assegurar-se de que os clientes não autorizados não obtenham o acesso a uma rede de provedor de serviços é configurar o sistema de abastecimento tais que o Modems a cabo desautorizado está instruído para transferir um arquivo de configuração DOCSIS com o conjunto de campo do acesso de rede a fora. Dessa maneira, o modem não desperdiçará largura de banda upstream valiosa através de uma reorganização contínua. Em lugar de, o modem obterá ao **em linha (d) o** estado que indica que os usuários atrás do modem não estarão concedidos o acesso à rede e ao modem de provedor de serviços usará somente a largura de banda fluxo acima para a manutenção de estação.

Comandos utilizados para monitorar o estado do BPI

show interface cable X/0 privacy [kek | tek] — este comando é usado indicar os temporizadores associados com o KEK ou o TEK como ajusta-se em uma relação CMTS.

Estão abaixo umas saídas de exemplo deste 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 pode ser usado para ver estatísticas no número de SID usando a privacidade da linha de base em uma relação do cabo específico.

Estão abaixo umas saídas de exemplo deste 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 eliminação de erros da privacidade da linha de base. Quando este comando é ativado, sempre que uma mudança no estado da privacidade da linha de base ou em um evento da privacidade da linha de base ocorre, os detalhes serão indicados no console. Este comando trabalha somente quando precedido com o **comando debug cable interface cable X/0 ou debug cable mac-address mac-address**.

debugar o bpiatp do cabo — Este comando ativa a eliminação de erros da privacidade da linha de base. Quando este comando é ativado, sempre que uma mensagem da privacidade da linha de base está enviada ou recebida por Cisco CMTS, a descarga hexadecimal da mensagem será indicada. Este comando trabalha somente quando precedido com o **comando debug cable interface cable X/0 ou debug cable mac-address mac-address**.

debugar o keyman do cabo — Esta eliminação de erros ativada comando do gerenciamento chave da privacidade da linha de base. Quando este comando é ativado os detalhes de gerenciamento chave da privacidade da linha de base estão indicados.

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. Contacte seu fornecedor de modem para mais versão recente do firmware que apoia o 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 da conectividade de cable modem do Troubleshooting, refira pesquisando defeitos o Online de vinda do Modems a cabo do uBR.

Observação especial – comandos ocultos

Qualquer referência a comandos ocultos neste documento serve apenas para questões informativas. Os comandos ocultos não são apoiados pelo centro de assistência técnica da Cisco (TAC). Além comandos ocultos:

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

Informações Relacionadas

- CableLabs
- DOCSIS CPE Configurator
- Autenticação, Autorização e Contabilidade (AAC).
- Suporte Técnico - Cisco Systems