Cisco CMTS 上的 DOCSIS 1.0 基线私密性

目录

简介

有线电缆数据服务接口规范(DOCSIS)保密性基准接口(BPI)主要目标是提供简单数据加密机制保护到/从在Data over Cable网络的电缆调制解调器发送的数据。基本保密功能可能也使用作为方法验证电缆调制解调器和授权组播传输流量到电缆调制解调器。

Cisco电缆调制解调器终端运行Cisco IOS软件镜像的系统(CMTS)和有线调制解调器产品以一特性组包括字符"k1" or"k8"支持基本保密功能，例如ubr7200-k1p-mz.121-6.EC1.bin。

本文在DOCSIS1.0模式讨论在操作的思科产品的基本保密功能。

开始使用前

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

先决条件

本文档没有任何特定的前提条件。

使用的组件

本文档中的信息根据配置运行Cisco IOS软件版本12.1(6)EC的uBR7246VXR，但是也应用对所有其他Cisco CMTS产品和软件版本。

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

如何配置电缆调制解调器的基本保密功能

如果发出命令通过在DOCSIS配置文件的服务等级参数如此执行有线调制解调器只将尝试使用基本保密功能。DOCSIS配置文件包含调制解调器的操作参数和通过TFTP下载作为联机的进程来一部分。

创建DOCSIS配置文件一个方法将使用在Cisco.com的DOCSIS有线调制解调器配置器。使用DOCSIS有线调制解调器配置器，您能创建发出命令有线调制解调器通过设置Baseline Privacy Enable字段使用基本保密功能在Class of Service选项下到的DOCSIS配置文件。参考下面示例：

或者， DOCSIS文件配置的独立版本从可以的用于启用基本保密功能如下所示：

一旦支持BPI的DOCSIS配置文件创建，电缆调制解调器将需要重置为了下载新配置文件和随后使用基本保密功能。

如何判断电缆调制解调器是否正在使用基本保密功能

在Cisco CMTS，一个能使用show cable modem命令查看单个有线调制解调器状态。有使用基本保密功能的调制解调器能出现的几状态。

联机

在有线调制解调器注册与Cisco CMTS后进入在线状态。在能协商与Cisco CMTS前的基本保密功能参数有线调制解调器需要到此状态。这时数据流发送在有线调制解调器和CMTS之间未加密。如果有线调制解调器留在此状态，并且不进行对任何状态如下所述，则调制解调器不使用基本保密功能。

online(pk)

online(pk)状态意味着有线调制解调器能协商**授权密钥**，也叫作与Cisco CMTS的一**Key Encryption**

Key (KEK)。这意味着有线调制解调器授权使用基本保密功能和是成功的在协商基本保密功能第一阶段。一56位关键用于的KEK保护随后的基本保密功能协商。当调制解调器在online(pk)状态数据流发送在有线调制解调器和Cisco CMTS之间时未加密，因为数据流的加密的密钥未协商。一般，online(pk)由online(pt)跟随。

reject(pk)

此状态表明有线调制解调器的尝试协商KEK失败。多数常见原因调制解调器在此状态是Cisco CMTS有打开的调制解调器验证和调制解调器有失败的认证。

online(pt)

这时调制解调器顺利地协商与Cisco CMTS的数据流加密密钥(TEK)。TEK用于加密有线调制解调器和Cisco CMTS之间的数据流。使用KEK， TEK协商进程加密。一56或40位关键用于的TEK加密有线调制解调器和Cisco CMTS之间的数据流。这时基本保密功能是成功设立和运行，因此用户数据发送在Cisco CMTS和有线调制解调器之间加密。

reject(pt)

此状态表明有线调制解调器无法成功协商与Cisco CMTS的一TEK。

下面请参阅关于输出示例: show cable modem命令显示的电缆调制解调器以与基本保密功能涉及的多种状态。

注意： 关于电缆调制解调器状态的更多信息，参考针对UBR电缆调制解调器不在线问题的故障排除。

对基本保密性的建立与维护有影响的计时器

有可以修改更改基本保密功能行为的某些超时值。其中一些参数在Cisco CMTS和其他可能配置通过DOCSIS配置文件。有一点原因更改这些参数中的任一个除了KEK寿命和TEK寿命。可能修改这些计时器强化在电缆装置的安全或减少CPU和流量在头顶上由于BPI管理。

KEK寿命

KEK寿命是有线调制解调器和Cisco CMTS应该认为经过协商的KEK有效的时间。在此时间通过前，有线调制解调器应该重新协商与Cisco CMTS的一新的KEK。

您能配置这次使用cable interface命令的Cisco CMTS ：

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

等于七天的默认设置是604800秒。

有一个更加小的KEK寿命强化安全，因为每KEK将持续在时期并且，如果删改KEK较少将来TEK协商是易受被劫机。对此的缺点是KEK重新协商增加在电缆调制解调器的CPU利用率并且增加在电缆装置的BPI管理数据流。

KEK充足时间

KEK充足时间是时间，在KEK寿命超时前，有线调制解调器被认为开始协商与一新的KEK的Cisco CMTS的那。在有后此计时器的想法是，以便有线调制解调器有足够的时间更新KEK，在超时前。

您能配置这次使用cable interface命令的Cisco CMTS ：

cable privacy kek grace-time *60-1800 seconds*
您能也配置这次使用DOCSIS配置文件通过填写字段被标记**授权宽限超时**在Baseline Privacy选项下。如果此DOCSIS配置文件领域填写那么优先于在Cisco CMTS配置的所有值。等于10分钟的此计时器的默认值是600秒。

TEK寿命

TEK寿命是有线调制解调器和Cisco CMTS应该认为经过协商的TEK有效的时间。在此时间通过前，有线调制解调器应该重新协商与Cisco CMTS的一新的TEK。

您能配置这次使用cable interface命令的Cisco CMTS ：

cable privacy tek life-time <180-604800 seconds>
等于12个小时的默认设置是43200秒。

有一个更加小的TEK寿命强化安全，因为每TEK将持续在时期并且，如果删改TEK较少数据将显示在未授权的解密。对此的缺点是TEK重新协商增加在电缆调制解调器的CPU利用率并且增加在电缆装置的BPI管理数据流。

TEK 宽限时间

TEK宽限时间是时间，在TEK寿命超时前有线调制解调器被认为开始协商与一新的TEK的Cisco CMTS。在有后此计时器的想法是，以便有线调制解调器有足够的时间更新TEK，在超时前。

您能配置这次使用cable interface命令的Cisco CMTS ：

cable privacy tek grace-time *60-1800 seconds*
您能也配置这次使用DOCSIS配置文件通过填写字段被标记**TEK雍容超时**在Baseline Privacy选项下。如果此DOCSIS配置文件领域填写那么优先于在Cisco CMTS配置的所有值。

等于10分钟的此计时器的默认值是600秒。

授权等待超时

这次管理有线调制解调器将等待从Cisco CMTS的一答复，当第一次时协商KEK的时间。

您能配置在DOCSIS配置文件的这次由正在修改**Authorize Wait Timeout字段**在Baseline Privacy选项下。

此字段的默认值是10秒，并且有效范围是2到30秒。

重新授权等待超时

这次管理有线调制解调器将等待从Cisco CMTS的一答复，当协商一新的KEK时的时间，因为

KEK寿命将超时。

您能配置在DOCSIS配置文件的这次由正在修改**Reauthorize Wait Timeout字段**在Baseline Privacy选项下。

此计时器的默认值是10秒，并且有效范围是2到30秒。

授权宽限超时

指定再认可的宽限期(以秒钟)。默认值是600。有效范围是1到1800秒。

授权拒绝等待超时

如果有线调制解调器设法协商与Cisco CMTS的一KEK，但是拒绝，必须在再尝试前协商一新的KEK等待授权拒绝等待超时。

您能配置在DOCSIS配置文件的此参数通过使用**Authorize Reject Wait Timeout字段**在Baseline Privacy选项下。此计时器的默认值是60秒，并且有效范围是10秒到600秒。

运行等待超时

这次管理有线调制解调器将等待从Cisco CMTS的一答复，当第一次时协商TEK的时间。

您能配置在DOCSIS配置文件的这次由正在修改**Operational Wait Timeout字段**在Baseline Privacy选项下。

此字段的默认值是1秒，并且有效范围是1到10秒。

密钥刷新等待超时

这次管理有线调制解调器将等待从Cisco CMTS的一答复，当协商一新的TEK时的时间，因为TEK寿命将超时。

您能配置在DOCSIS配置文件的这次由正在修改**Rekey Wait Timeout字段**在Baseline Privacy选项下。

此计时器的默认值是1秒，并且有效范围是1到10秒。

Cisco CMTS 基本保密配置命令

以下电缆接口命令可能用于配置在Cisco CMTS的基本保密功能和基准与秘密有关的功能。

电缆保密性

cable privacy命令启用基本保密功能的协商在特定接口的。如果**no cable privacy命令**在电缆接口配置，则电缆调制解调器不会允许协商基本保密功能，当来联机在该接口时。请当心，当禁用的基本保密功能，因为时，如果有线调制解调器由其DOCSIS配置文件发出命令使用基本保密功能，并且Cisco CMTS拒绝让它协商基本保密功能，然后调制解调器可能不能保持联机。

cable privacy mandatory

如果**cable privacy mandatory命令**配置，并且有线调制解调器有启用的基本保密功能在其DOCSIS配置文件，则有线调制解调器必须成功协商，并且使用基本保密功能不会否则允许保持联机。

如果有线调制解调器的DOCSIS配置文件不指示调制解调器使用基本保密功能**cable privacy mandatory命令**从保持然后不会终止调制解调器联机。

默认情况下**cable privacy mandatory命令没有**启用。

cable privacy authenticate-modem

执行参与基本保密功能的调制解调器的一个认证形式是可能的。当电缆调制解调器协商与Cisco CMTS时的一KEK，调制解调器传送他们的6个字节MAC地址和他们的序列号详细信息对Cisco CMTS。这些参数可以使用作为用户名/密码组合为正在验证电缆调制解调器的目的。Cisco CMTS使用Cisco IOS验证、授权和核算(AAA)服务执行此。发生故障验证的电缆调制解调器没有允许联机。另外，不使用基本保密功能的电缆调制解调器没有影响的是受此命令的。

警告： 因为此功能利用AAA服务您需要确保，您小心，当正在修改的AAA配置时，否则您可以疏忽地丢失能力登录和管理您的Cisco CMTS。

这是方式的一些配置示例能执行调制解调器验证。在这些配置示例中，一定数量的调制解调器被输入了到身份验证数据库。调制解调器的6个八位位组MAC地址担当用户名，并且可变长的序列号担当密码。注意一个调制解调器用一明显错误的序列号配置。

以下部分示例Cisco CMTS配置使用一个本地认证数据库验证一定数量的电缆调制解调器。

```
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
```

正在验证调制解调器另一个方法将雇用外部RADIUS服务器。这是使用一个外部RADIUS服务器验证

调制解调器的部分Cisco CMTS配置示例

```
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
```

下面有等同的信息的示例RADIUS用户数据库文件对使用本地认证的以上示例。一定数量的商业和免费软件RADIUS服务器利用用户文件作为用户认证信息存储的数据库。

```
# 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
```

如下所示在Cisco CMTS执行的输出**show cable modem命令**哪些使用上述配置示例之一。您看到所有基本保密功能启用在本地认证数据库没列出的调制解调器，否则用不正确序列号将进入**reject(pk)**状态并且不保持联机。

因为其DOCSIS配置文件未发出命令它使用基本保密功能，有SID的17调制解调器没有在身份验证数据库的一个条目，然而能来联机。

因为他们有正确条目在身份验证数据库，有Sids的18， 21和22调制解调器能来联机

有SID的19调制解调器无法来联机，因为发出命令使用基本保密功能，但是没有在身份验证数据库的条目此调制解调器的。此调制解调器最近在表明的reject(pk)状态它失败的认证。

有SID的20调制解调器无法来联机，因为，虽然有在身份验证数据库的一个条目与此调制解调器的MAC地址，对应的序列号不正确。当前此调制解调器在reject(pk)状态，但是过渡到脱机状态在短期之后。

当调制解调器失败验证一个消息沿着以下线路被添加到Cisco CMTS日志。

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

有线调制解调器从站点维护列表然后删除，并且被标记作为脱机在30秒以内。有线调制解调器在再只将拒绝的线路很可能然后将设法再次来。

注意： Cisco不建议客户使用**cable privacy authenticate-modem命令**从来终止未授权的电缆调制解调器联机。更有效的方式保证未授权的客户没获得对服务提供商的网络的访问将配置设置系统这样未授权的电缆调制解调器被指示下载一个DOCSIS配置文件网络访问字段设置对。这样，调制解调器不会由连续重新划定范围浪费重要的上行带宽。反而，调制解调器将达到**联机(d)**表明的状态用户在调制解调器背后不会是授权访问到服务提供商的网络和调制解调器只将使用上行带宽站点维护。

用于监测 BPI 状态的命令

show interface cable X/0 privacy [kek|tek] —此命令用于显示计时器关联与KEK或TEK作为在CMTS接口的集。

下面此命令示例输出。

```
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 —使用在特定电缆接口的基本保密功能此隐藏命令可能用于查看在Sids编号的统计信息。

下面此命令示例输出。

```
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 —此命令激活基本保密功能调试。当此命令被启动，每当在基本保密功能状态或基本保密功能事件上的一个变化发生，详细信息在控制台将显示。此命令只运作，当先于与**debug cable interface cable X/0**或**debug cable mac-address mac-address命令**。

debug cable bpiatp —此命令激活基本保密功能调试。当此命令被启动，每当基本保密功能信息由

Cisco CMTS传送或接收，消息的十六进制转储将显示。此命令只运作，当先于与**debug cable interface cable X/0**或**debug cable mac-address mac-address命令**。

debug cable keyman —基本保密功能密钥管理此命令激活的调试。当此命令被启动时基本保密功能密钥管理详细信息显示。

BPI 故障排除

电缆调制解调器出现作为联机而不是online(pt)。

如果调制解调器在线状态出现而不是online(pt)那么通常含义三件事之一。

第一个可能的原因是有线调制解调器未给指定的DOCSIS配置文件有线调制解调器使用基本保密功能。检查DOCSIS配置文件有启用的BPI在服务等级(COS)配置文件发送对调制解调器。

看到一个调制解调器的第二个原因在线状态可能是调制解调器等待，在开始协商BPI前。是否等待一两分钟发现调制解调器更改状态到online(pt)。

最终原因可能是调制解调器不包含固件该支持基本保密功能。联系您的支持BPI固件的更多最新版本的调制解调器供应商。

电缆调制解调器在reject(pk)状态出现然后脱机。

输入reject(pk)状态的调制解调器的最可能原因是有线调制解调器验证用**cable privacy authenticate-modem命令**启用，但是AAA被不正确配置。检查受影响的调制解调器的序列号和MAC地址正确地被输入了到身份验证数据库，并且所有外部RADIUS服务器是可及的和作用。您能使用路由器调试命令**debug aaa authentication**和**debug radius**有RADIUS服务器的状态的想法或调制解调器为什么是失败验证。

注意： 关于故障排除有线调制解调器连通性的一般信息，参考针对UBR电缆调制解调器不在线问题的故障排除。

特别注释 - 隐藏命令

对隐藏命令的所有参考在本文只是作为提供情报的目的。Cisco技术支持中心(TAC)不支持隐藏命令。另外隐藏命令：

- 不总是生成可靠或正确信息
- 5月原因意外的副作用是否执行
- 不同样正常运行用Cisco IOS软件不同的版本
- 从Cisco IOS软件将来版本在任何时间不预先通知删除

相关信息

- CableLabs
- DOCSIS CPE Configurator
- 验证、授权和记帐 (AAA)
- 技术支持 - Cisco Systems