DOCSIS 1.0在Cisco CMTS的基本保密性

Contents

Introduction

有线电缆数据服务接口规范(DOCSIS)保密性基准接口(BPI)的主要目标是提供一个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被发送的数据。基本保密性可能也使用作为方法验证电缆调制解调器和核准组播传输数据流到电缆调制解调器。

Cisco电缆调制解调器终端系统(CMTS)和运行Cisco IOS软件镜像的有线调制解调器产品以一个功能集包括字符"k1" or"k8"支持基本保密性，例如ubr7200-k1p-mz.121-6.EC1.bin。

本文在DOCSIS1.0模式讨论在运行的思科产品的基本保密性。

开始使用前

Conventions

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

Prerequisites

本文档没有任何特定的前提条件。

Components Used

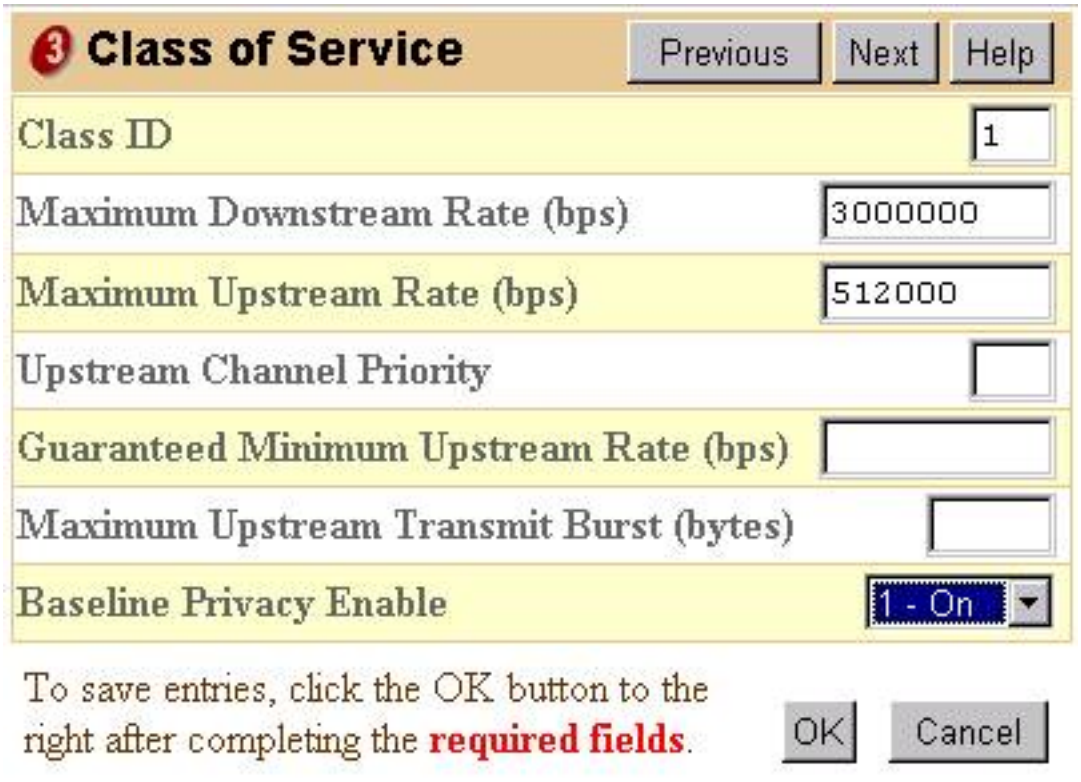
本文的信息根据配置运行Cisco IOS软件版本12.1(6)EC的uBR7246VXR，但是也应用于所有其他Cisco CMTS产品和软件版本。

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。All of the devices used in this document started with a cleared (default) configuration.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。

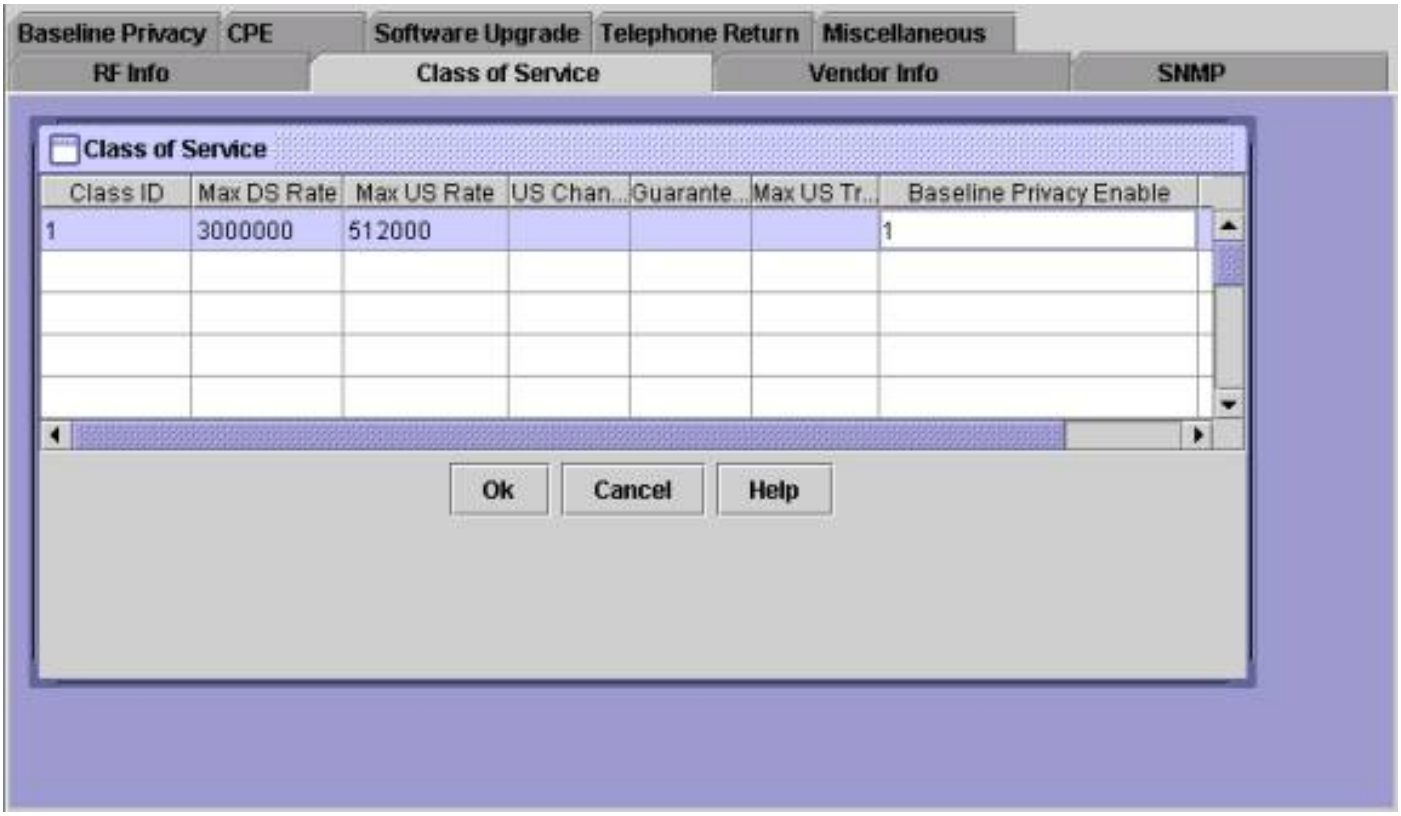
如何配置电缆调制解调器的基本保密性

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性。DOCSIS配置文件包含调制解调器的操作参数和通过TFTP下载作为来一部分的进程联机。

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字段使用基本保密性在Class of Service选项下至**开的**DOCSIS配置文件。请参见下面示例：



或者， DOCSIS文件配置的独立版本从可以的使用到enable (event)基本保密性如下所示：



一旦支持BPI的DOCSIS配置文件被创建了，将需要重置电缆调制解调器为了下载新配置文件和随后使用基本保密性。

如何告诉有线调制解调器是否使用基本保密性

在Cisco CMTS，一个能使用show cable modem命令查看单个电缆调制解调器的状态。有使用基本保密性的调制解调器能出现于的几个状态。

联机

在有线调制解调器注册与Cisco CMTS后进入在线状态。在能与Cisco CMTS前，协商基本保密性参数有线调制解调器需要达到此状态。这时数据流量被发送在有线调制解调器和CMTS之间末加密。如果有线调制解调器在此状态保持，并且不进行对如下所述的任何状态，则调制解调器不使用基本保密性。

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被核准使用基本保密性和是成功的在协商第一阶段基本保密性。一56位关键用于的KEK保护随后的基本保密性协商。当调制解调器在online(pk)状态数据流量被发送在有线调制解调器和Cisco CMTS之间时末加密，因为数据流量的加密的键未协商。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失败了。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认证和调制解调器有失败的认证。

online(pt)

这时调制解调器与Cisco CMTS成功协商数据流加密密钥(TEK)。TEK用于加密有线调制解调器和Cisco CMTS之间的数据流量。使用KEK， TEK协商进程被加密。一56或40位关键用于的TEK加密有线调制解调器和Cisco CMTS之间的数据流量。这时基本保密性是成功设立和运行，因此用户数据被发送在Cisco CMTS和有线调制解调器之间被加密。

reject(pt)

此状态表明有线调制解调器无法与Cisco CMTS成功协商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多种状态与基本保密性有关。

```
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
```

Note: 关于有线调制解调器状态的更多信息，请参见针对UBR电缆调制解调器不在线问题的故障排除。

影响基本保密性的建立与维护的计时器

有可以修改更改基本保密性工作情况的某些超时值。其中一些参数在Cisco CMTS和其他可能被配置通过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和数据流在头顶上由于BPI管理。

KEK寿命

KEK寿命是有线调制解调器和Cisco CMTS应该认为协商的KEK有效的时间。在此时间通过了前，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。

有一个更小的KEK寿命强化安全，因为每KEK将持续在短时间内并且，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BPI在电缆装置的管理数据流。

KEK充足时间

KEK充足时间是时间，在KEK寿命到期前，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，在到期前。

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file字段此的DOCSIS配置填写那么优先于在Cisco CMTS配置的所有值。DEFAULT值等于10分钟的此计时器的是600秒。

TEK寿命

TEK寿命是有线调制解调器和Cisco CMTS应该认为协商的TEK有效的时间。在此时间通过了前，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小时的默认设置是43200秒。

有一个更小的TEK寿命强化安全，因为每TEK将持续在短时间内并且，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BPI在电缆装置的管理数据流。

TEK宽限时间

TEK宽限时间是时间，在TEK寿命到期前有线调制解调器被认为启动协商与一新的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，在到期前。

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file字段此的DOCSIS配置填写那么优先于在Cisco CMTS配置的所有值。

DEFAULT值等于10分钟的此计时器的是600秒。

授权等待超时

这次管理有线调制解调器将等待自Cisco CMTS的一种回应，当第一次时协商KEK的时间。

您能通过修改**Authorize Wait Timeout字段**配置在DOCSIS配置文件的这次在Baseline Privacy选项下。

DEFAULT值此字段的是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自Cisco CMTS的一种回应，当协商一新的KEK时的时间，因为KEK寿命将到期。

您能通过修改**Reauthorize Wait Timeout字段**配置在DOCSIS配置文件的这次在Baseline Privacy选项下。

DEFAULT值此计时器的是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)。DEFAULT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与Cisco CMTS协商KEK，但是被拒绝，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。DEFAULT值此计时器的是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自Cisco CMTS的一种回应，当第一次时协商TEK的时间。

您能通过修改**Operational Wait Timeout字段**配置在DOCSIS配置文件的这次在Baseline Privacy选项下。

DEFAULT值此字段的是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自Cisco CMTS的一种回应，当协商一新的TEK时的时间，因为TEK寿命将到期。

您能通过修改**Rekey Wait Timeout字段**配置在DOCSIS配置文件的这次在Baseline Privacy选项下。

DEFAULT值此计时器的是1秒，并且有效范围是1到10秒。

Cisco CMTS Cisco CMTS基本保密配置命令

以下电缆接口命令可能用于配置基本保密性和基准与秘密有关的功能在Cisco CMTS。

电缆保密性

cable privacy命令enable (event)基本保密性的协商在一个特殊接口的。如果**no cable privacy命令**在

电缆接口被配置，则电缆调制解调器不会允许协商基本保密性，当来联机在该接口时。请当心，当禁用基本保密性，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性，并且Cisco CMTS拒绝让它协商基本保密性，然后调制解调器可能不能保持在线。

cable privacy mandatory

如果配置**cable privacy mandatory命令，**并且有线调制解调器有被启用的基本保密性在其DOCSIS配置文件，则有线调制解调器必须成功协商，并且使用基本保密性不会否则允许保持在线。

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性**cable privacy mandatory命令**从保持然后不会终止调制解调器在线。

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

cable privacy authenticate-modem

执行认证形式参与基本保密性的调制解调器的是可能的。当电缆调制解调器与Cisco CMTS时协商KEK，调制解调器传输他们的6个字节MAC地址和他们的序列号详细资料对Cisco CMTS。这些参数可以使用作为用户名/密码组合为验证的电缆调制解调器的目的。Cisco CMTS使用Cisco IOS认证、授权和记帐(AAA)服务执行此。发生故障认证的电缆调制解调器没有允许联机。另外，不使用基本保密性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服务您需要确信，您小心，当修改AAA配置时，否则您可以疏忽地丢失能力记录到和管理您的Cisco CMTS。

这是方式的一些配置示例能进行调制解调器认证。在这些配置示例中，一定数量的调制解调器被输入了认证数据库。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配置有一明显错误的序列号。

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。

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

验证调制解调器另一个方法将雇用一个外部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

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

下面与等同的信息的示例RADIUS用户数据库文件对使用本地认证的上面的例子。一定数量的商业和免费软件RADIUS服务器利用用户文件作为存储用户认证信息的数据库。

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

如下所示在Cisco CMTS执行的输出的**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性启用了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)状态并且不保持在线。

```
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
```

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

因为他们有正确的条目在认证数据库，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性，但是没有在认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，虽然有在认证数据库的一个条目与此调制解调器的MAC地址，对应的序列号是不正确的。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。

当调制解调器失败认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被去除，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被拒绝的线路很可能然后将设法再次来。

Note: Cisco不建议用户使用**cable privacy authenticate-modem命令**从来终止未授权的电缆调制解调器联机。一个效率更高方式保证未授权的用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。

用于的命令监控BPI状态

show interface cable X/0 privacy [kek|tek] —此命令用于显示与KEK或TEK产生关联的计时器和设置在CMTS接口。

下面此命令的输出示例。

```
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 —使用在一个特定的电缆接口的基本保密性此隐藏的命令可能用于查看对Sids的编号的统计数据。

下面此命令的输出示例。

```
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性调试。当启动此命令，每当在基本保密性状态或基本保密性事件上的一个变化发生，详细资料在控制台将显示。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性调试。当启动此命令，每当Cisco CMTS传送基本保密性信息或收到，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 —此命令激活了基本保密性密钥管理调试。当启动时此命令基本保密性密钥管理详细资料显示。

排除BPI故障

电缆调制解调器出现作为联机而不是online(pt)。

如果调制解调器出现于一个在线状态而不是online(pt)那么通常意味着三件事之一。

第一个可能的原因是未产生有线调制解调器指定的一个DOCSIS配置文件有线调制解调器使用基本保密性。检查DOCSIS配置文件有被启用的BPI在业务类别配置文件被发送到调制解调器。

看到在线状态的一个调制解调器的第二个原因可能是调制解调器等待，在开始协商的BPI前。等待一两分钟发现调制解调器是否更改状态到online(pt)。

最终原因可能是调制解调器不包含支持基本保密性的固件。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。

电缆调制解调器出现于reject(pk)状态然后脱机。

调制解调器进入的reject(pk)状态的最可能原因是有线调制解调器认证启用了**cable privacy authenticate-modem命令**，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认证数据库，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debug aaa authentication命令和**debug radius**有RADIUS服务器的状态的想法或调制解调器为什么

是失败认证。

Note: 关于排除有线调制解调器连通性故障的一般信息，请参见针对UBR电缆调制解调器不在线问题的故障排除。

特殊注释-隐藏的命令

在隐藏的in命令的所有参考本文只是作为提供情报的目的。Cisco技术支持中心(TAC)不支持隐藏的命令。另外隐藏的命令：

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

Related Information

- CableLabs
- DOCSIS CPE Configurator
- 验证、授权和统计(AAA)
- Technical Support - Cisco Systems