Cisco CMTS 上的 DOCSIS 1.0 基线私密性

目录

简介
开始使用前
规则
先决条件
使用的组件
如何配置电缆调制解调器的基本保密功能
如何判断电缆调制解调器是否正在使用基本保密功能
对基本保密性的建立与维护有影响的计时器
KEK生命周期
KEK宽限时间
TEK生命周期
TEK 宽限时间
授权等待超时
重新授权等待超时
授权宽限超时
授权拒绝等待超时
运行等待超时
密钥刷新等待超时
Cisco CMTS 基本保密配置命令
电缆保密性
cable privacy mandatory
cable privacy authenticate-modem
用于监测 BPI 状态的命令
BPI 故障排除
特别注释 - 隐藏命令
相关信息

简介

有线数据服务接口规范(DOCSIS)基线隐私接口(BPI)的主要目标是提供简单的数据加密方案，以保护有线数据网络中的电缆调制解调器发送的数据和从电缆调制解调器发送的数据。基线隐私也可用作验证电缆调制解调器以及授权向电缆调制解调器传输组播流量的手段。

运行Cisco IOS®软件映像的思科电缆调制解调器终端系统(CMTS)和电缆调制解调器产品，其功能集包括“k1”或“k8”字符，支持基线隐私，例如ubr7200-k1p-mz.121-6.EC1.bin。

本文档讨论在DOCSIS1.0模式下运行的思科产品的基准隐私。

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

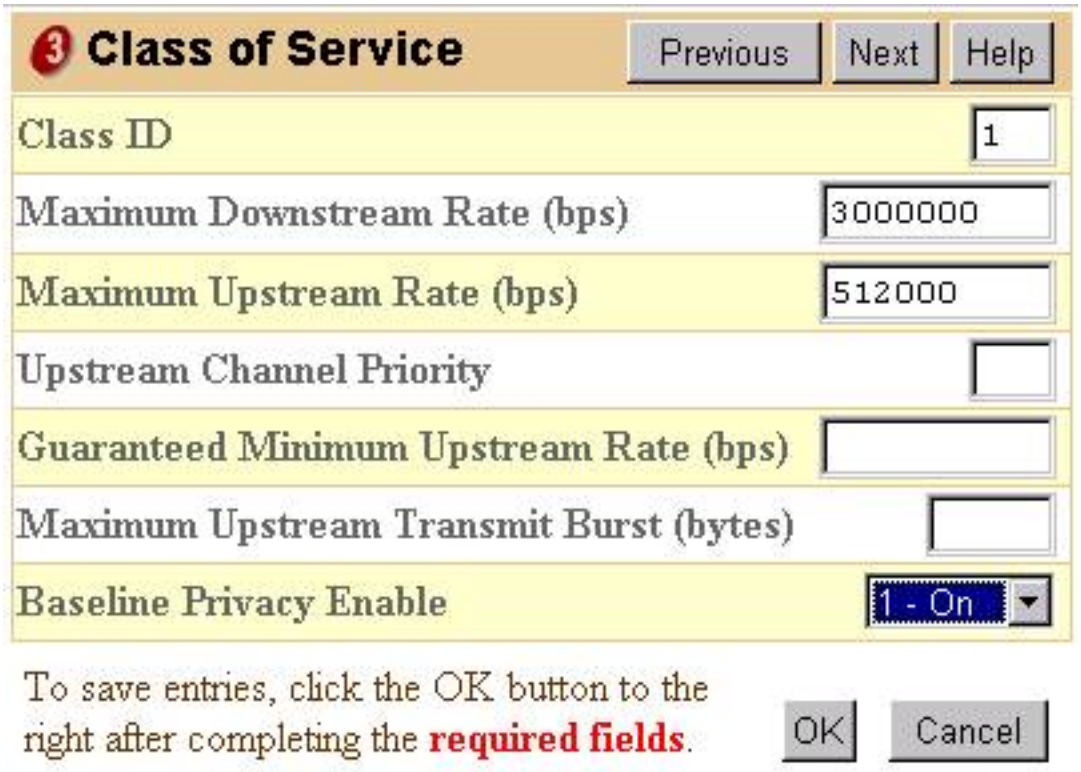
本文档中的信息基于配置运行Cisco IOS®软件版本12.1(6)EC的uBR7246VXR，但也适用于所有其他Cisco CMTS产品和软件版本。

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。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。

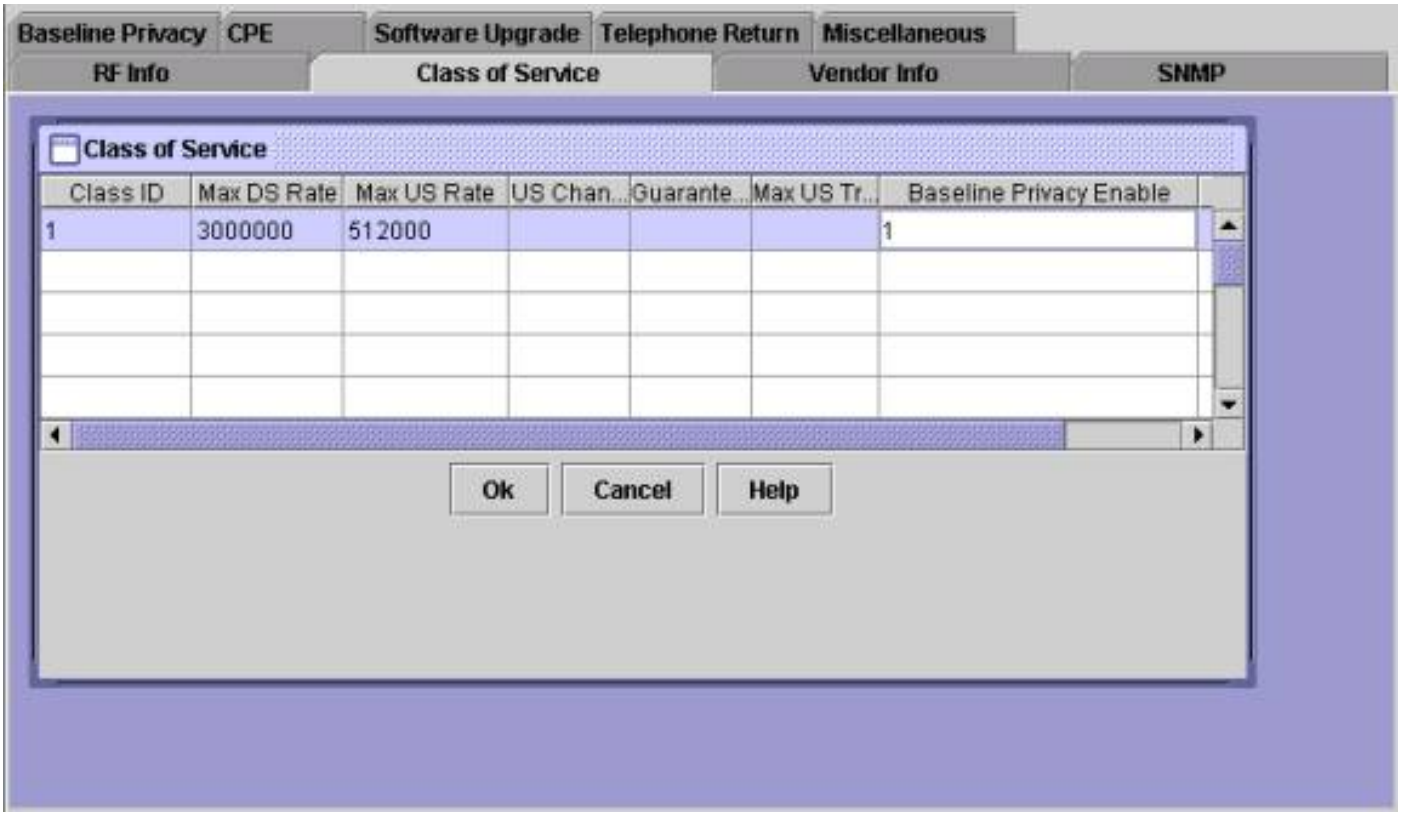
如何配置电缆调制解调器的基本保密功能

只有通过DOCSIS配置文件中的服务类别参数命令电缆调制解调器使用基线隐私时，它才会尝试使用。DOCSIS配置文件包含调制解调器的操作参数，在上线过程中通过TFTP下载。

创建DOCSIS配置文件的一种方法是使用Cisco.com上的DOCSIS电缆调制解调器配置器。使用DOCSIS电缆调制解调器配置器，您可以创建DOCSIS配置文件，该文件命令电缆调制解调器使用基线隐私，方法是将“服务类别”选项卡下的“基线隐私启用”字段设置为“开”。请参考以下示例：



或者，可以使用中的DOCSIS文件配置的独立版本启用基线隐私，如下所示：



创建支持BPI的DOCSIS配置文件后，需要重置电缆调制解调器以下载新的配置文件，然后使用基线隐私。

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上，可以使用show cable modem命令查看各个电缆调制解调器的状态。使用基线隐私的调制解调器可能出现在以下几种状态中。

在线

电缆调制解调器向Cisco CMTS注册后，它进入在线状态。电缆调制解调器需要到达此状态，才能与Cisco CMTS协商基线隐私参数。此时，电缆调制解调器和CMTS之间发送的数据流量未加密。如果电缆调制解调器保持此状态，并且未进入下述任何状态，则调制解调器不使用基线隐私。

在线(pk)

联机(pk)状态表示电缆调制解调器能够与Cisco CMTS**协商授**权密钥(**也称为密钥**加密密钥(KEK))。这意味着电缆调制解调器已获得使用基线隐私的授权，并且已成功协商了基线隐私的第一阶段。KEK是用于保护后续基线隐私协商的56位密钥。当调制解调器处于在线(pk)状态时，电缆调制解调器和Cisco CMTS之间发送的数据流量仍未加密，因为尚未协商用于数据流量加密的密钥。通常，在线(pk)后跟在在线(pt)。

reject(pk)

此状态表示电缆调制解调器尝试协商KEK失败。调制解调器处于此状态的最常见原因是Cisco CMTS启用了调制解调器身份验证，而调制解调器身份验证失败。

在线(pt)

此时，调制解调器已成功与Cisco CMTS协商流量加密密钥(TEK)。TEK用于加密电缆调制解调器和Cisco CMTS之间的数据流量。TEK协商过程使用KEK进行加密。TEK是56或40位密钥，用于加密电缆调制解调器与Cisco CMTS之间的数据流量。此时，基线隐私已成功建立并运行，因此Cisco CMTS和电缆调制解调器之间发送的用户数据正在加密。

拒绝(pt)

此状态表示电缆调制解调器无法与Cisco CMTS成功协商TEK。

有关show cable modem命令的输出示例，请参阅下文，该命令显示电缆调制解调器处于与基线隐私相关的各种状态。

```
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
```

注：有关电缆调制解调器状态的详细信息，请参阅排除uBR电缆调制解调器未联机故障。

对基本保密性的建立与维护有影响的计时器

可以修改某些超时值以更改基线隐私的行为。这些参数中的一些可以通过DOCSIS配置文件在Cisco CMTS上配置，而其他参数可以通过DOCSIS配置文件配置。除了KEK寿命和TEK寿命外，没有理由更改任何这些参数。可以修改这些计时器，以增加电缆设备的安全性，或减少因BPI管理而导致的CPU和流量开销。

KEK生命周期

KEK生存期是电缆调制解调器和Cisco CMTS应考虑协商的KEK有效的时间量。在这段时间过去之前，电缆调制解调器应与Cisco CMTS重新协商新的KEK。

您可以使用Cisco CMTS cable interface命令配置此次：

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

默认设置为604800秒，等于7天。

科索沃公司寿命更短会提高安全性，因为每家科索沃公司的寿命将更短，因此，如果科索沃公司被黑客侵入，未来的联发科技谈判就容易被劫持。其缺点是KEK重新协商提高了电缆调制解调器的CPU利用率，并增加了电缆设备的BPI管理流量。

KEK宽限时间

KEK宽限时间是KEK生命期到期前的时间，即电缆调制解调器用于开始与Cisco CMTS协商新的KEK。使用此计时器的想法是使电缆调制解调器有足够的时间在KEK过期之前续约。

您可以使用Cisco CMTS cable interface命令配置此次：

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

您还可以使用DOCSIS配置文件配置此次，方法是填写Baseline Privacy选项卡下标记Authorization Grace Timeout的字段。如果填入此DOCSIS配置文件字段，则其优先于Cisco CMTS上配置的任何值。此计时器的默认值为600秒，等于10分钟。

TEK生命周期

TEK生存期是电缆调制解调器和Cisco CMTS认为协商的TEK有效的时间量。在经过此时间段之前，电缆调制解调器应与Cisco CMTS重新协商新的TEK。

您可以使用Cisco CMTS cable interface命令配置此次：

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

默认设置为43200秒，等于12小时。

拥有更小的TEK寿命可提高安全性，因为每个TEK将持续更短的时间，因此，如果TEK被黑客攻击，则较少的数据将暴露在未经授权的解密中。其缺点是TEK重新协商提高了电缆调制解调器的CPU利用率，并增加了电缆设备的BPI管理流量。

TEK 宽限时间

TEK宽限时间是TEK生命期到期之前，电缆调制解调器开始与Cisco CMTS协商新TEK的时间。使用此计时器的想法是，电缆调制解调器有足够的时间在TEK过期之前进行更新。

您可以使用Cisco CMTS cable interface命令配置此次：

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

您还可以使用DOCSIS配置文件配置此次，方法是填写“基线隐私”(Baseline Privacy)选项卡下标记为“TEK Grace Timeout”(TEK Grace Timeout)的字段。如果填入此DOCSIS配置文件字段，则其优先于Cisco CMTS上配置的任何值。

此计时器的默认值为600秒，等于10分钟。

授权等待超时

此时间控制电缆调制解调器在首次协商KEK时等待Cisco CMTS响应的时间。

您可以通过修改Baseline Privacy选项卡下的Authorize Wait Timeout字段，在DOCSIS配置文件中配置此时间。

此字段的默认值为10秒，有效范围为2至30秒。

重新授权等待超时

此时间控制电缆调制解调器在协商新KEK时等待Cisco CMTS响应的时间，因为KEK生命期即将到期。

您可以通过修改Baseline Privacy选项卡下的Reauthorize Wait Timeout字段，在DOCSIS配置**文件中配**置此时间。

此计时器的默认值为10秒，有效范围为2至30秒。

授权宽限超时

指定重新授权的宽限期（以秒为单位）。 默认值为600。有效范围为1到1800秒。

授权拒绝等待超时

如果电缆调制解调器尝试与Cisco CMTS协商KEK，但被拒绝，则必须等待授权拒绝等待超时，然后再尝试协商新的KEK。

您可以使用Baseline Privacy选项卡下的Authorize Reject Wait Timeout字段在DOCSIS配**置文件中配**置此参数。此计时器的默认值为60秒，有效范围为10秒到600秒。

运行等待超时

此时间控制电缆调制解调器在首次协商TEK时等待Cisco CMTS响应的时间。

您可以通过修改Baseline Privacy选项卡下的Operational Wait Timeout字段，在DOCSIS配**置文件中**配置此时间。

此字段的默认值为1秒，有效范围为1至10秒。

密钥刷新等待超时

此时间控制电缆调制解调器在协商新TEK时等待Cisco CMTS响应的时间，因为TEK生命期即将到期。

您可以通过修改Baseline Privacy选项卡下的Rekey Wait Timeout字段，在DOCSIS配**置文件中**配置此时间。

此计时器的默认值为1秒，有效范围为1至10秒。

Cisco CMTS 基本保密配置命令

以下电缆接口命令可用于在Cisco CMTS上配置与基线隐私和基线隐私相关的功能。

电缆保密性

cable privacy命令可在特定接口上启用基线隐私协商。如果在有**线接口上配**置了no cable privacy命令，则在该接口上联机时，不允许有线调制解调器协商基线隐私。禁用基线隐私时请小心，因为如

果电缆调制解调器的DOCSIS配置文件命令其使用基线隐私，而Cisco CMTS拒绝让其协商基线隐私，则调制解调器可能无法保持在线。

cable privacy mandatory

如果配置了**cable privacy mandatory** 命令，并且电缆调制解调器在其DOCSIS配置文件中启用了基线隐私，则电缆调制解调器必须成功协商并使用基线隐私，否则它将不允许保持在线。

如果电缆调制解调器的DOCSIS配置文件未指示调制解调器使用基线隐私，则**cable privacy mandatory**命令不会阻止调制解调器保持联机。

默认**情况下，**未启用cable privacy mandatory命令。

cable privacy authenticate-modem

可以对参与基线隐私的调制解调器执行某种形式的身份验证。当电缆调制解调器与Cisco CMTS协商KEK时，调制解调器将其6字节MAC地址及其序列号的详细信息传输到Cisco CMTS。这些参数可用作用户名/密码组合，用于验证电缆调制解调器。Cisco CMTS使用Cisco IOS身份验证、授权和记帐(AAA)服务来执行此操作。身份验证失败的电缆调制解调器不允许联机。此外，不使用基线隐私的电缆调制解调器不受此命令的影响。

注意：由于此功能使用AAA服务，因此您需要确保在修改AAA配置时非常小心，否则，您可能会在无意中失去登录和管理Cisco CMTS的能力。

以下是一些用于执行调制解调器身份验证的配置示例。在这些配置示例中，许多调制解调器已输入到身份验证数据库中。调制解调器的6个二进制八位数MAC地址用作用户名，可变长度序列号用作密码。请注意，一个调制解调器配置了明显不正确的序列号。

以下部分示例Cisco CMTS配置使用本地身份验证数据库对许多电缆调制解调器进行身份验证。

```
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
```

另一种验证调制解调器的方法是使用外部RADIUS服务器。以下是使用外部RADIUS服务器对调制解调器进行身份验证的部分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
```

以下是示例RADIUS用户数据库文件，其信息与上面使用本地身份验证的示例相同。用户文件被许多商业和免费软件RADIUS服务器用作存储用户验证信息的数据库。

```
# 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
```

下面显示的是在使用上述任**一配置示**例的Cisco CMTS上执行的show cable modem命令的输出。您将看到，任何未在本地身份验证数据库中列出的启用基线隐私的调制解调器，或者序列号不正确的调制解调器将进入**reject(pk)**状态，并且不会保持联机。

```
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
```

带SID 17的调制解调器在身份验证数据库中没有条目，但能够联机，因为其DOCSIS配置文件没有命令它使用基线隐私。

SID为18、21和22的调制解调器能够联机，因为它们在身份验证数据库中有正确的条目

SID为19的调制解调器无法联机，因为已命令它使用基线隐私，但此调制解调器的身份验证数据库中没有条目。此调制解调器最近将处于拒绝(pk)状态，表示其身份验证失败。

SID为20的调制解调器无法联机，因为尽管身份验证数据库中有一个条目使用此调制解调器的MAC地址，但相应的序列号不正确。目前，此调制解调器处于拒绝(pk)状态，但在短时间后将转换到脱机状态。

当调制解调器身份验证失败时，会将沿以下行的消息添加到Cisco CMTS日志。

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

然后，电缆调制解调器从站维护列表中删除，并在30秒内标记为离线。然后，电缆调制解调器很可能会再次尝试联机，但会再次被拒绝。

注意：思科不建议客户使用cable privacy authenticate-modem**命令来阻止未授**权的电缆调制解调器上线。确保未授权客户不能访问服务提供商的网络的更有效的方法是配置调配系统，以便指示未授权的电缆调制解调器下载DOCSIS配置文件，且网络访问字段设置为off。这样，调制解调器就不会因持续重新测距而浪费宝贵的上行带宽。相反，调制解调器将进入**在线(d)**状态，表明调制解调器后面的用户将无权访问服务提供商的网络，并且调制解调器将仅使用上游带宽进行站维护。

用于监测 BPI 状态的命令

show interface cable X/0 privacy [kek |tek] — 此命令用于显示与KEK或TEK关联的计时器，如在CMTS接口上所设置。

以下是此命令的输出示例。

```
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 — 此隐藏命令可用于查看有关特定电缆接口上使用基线隐私的SID数量的统计信息。

以下是此命令的输出示例。

```
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 — 此命令激活基线隐私的调试。激活此命令后，每当发生“基线隐私”状态或“基线隐私”事件更改时，详细信息将显示在控制台上。此命令仅在出现debug cable interface cable X/0**或debug cable mac-address mac-address命**令之**前使用时*才起作用***。

debug cable bpiatp — 此命令激活基线隐私的调试。激活此命令后，每当Cisco CMTS发送或接收基线隐私消息时，将显示该消息的十六进制转储。此命令仅在出现debug cable interface cable X/0**或debug cable mac-address mac-address命**令之**前使用时*才起作用***。

debug cable keyman — 此命令激活了基线隐私密钥管理的调试。激活此命令后，将显示基线隐私密钥管理的详细信息。

BPI 故障排除

电缆调制解调器显示为在线，而不是在线(pt)。

如果调制解调器显示为联机状态而不是联机(pt)，则通常意味着三件事之一。

第一个可能原因是电缆调制解调器没有获得DOCSIS配置文件，该配置文件指定电缆调制解调器使用基线隐私。检查DOCSIS配置文件是否在发送到调制解调器的服务类别配置文件中启用了BPI。

看到调制解调器处于在线状态的第二个原因是调制解调器在开始协商BPI之前正在等待。等待一两分钟，查看调制解调器是否将状态更改为联机(pt)。

最终原因可能是调制解调器不包含支持基本隐私的固件。有关支持BPI的更新版本固件，请联系您的调制解调器供应商。

电缆调制解调器显示为拒绝(pk)状态，然后脱机。

调制解调器进入拒绝(pk)状态的最可能原因是电缆调制解调器身份验证已使用cable privacy authenticate-modem命**令启用**，但AAA配置错误。检查受影响调制解调器的序列号和MAC地址是否已正确输入到身份验证数据库中，以及任何外部RADIUS服务器是否可访问且工作正常。您可以使用路由器调试命令**debug aaa authentication**和**debug radius**来了解RADIUS服务器的状态或调制解调器身份验证失败的原因。

注：有关排除电缆调制解调器连接故障的一般信息，请参阅排除uBR电缆调制解调器未联机故障。

特别注释 - 隐藏命令

本文档中对隐藏命令的任何引用仅供参考。思科技术支持中心(TAC)不支持隐藏命令。 此外，隐藏命令：

- 可能并不总是生成可靠或正确的信息
- 如果执行，可能会造成意外的副作用
- 在Cisco IOS软件的不同版本中，行为可能不同
- 可以随时从未来版本的Cisco IOS软件中删除，恕不另行通知

相关信息

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