Cisco CMTS上的DOCSIS 1.0基線隱私

目錄

簡介

有線電纜資料服務介面規範(DOCSIS)基線保密介面(BPI)的主要目標是提供簡單資料加密方案，以保護有線電纜資料網路中收發有線資料機的資料。基線保密也可用作驗證纜線資料機的一種方式，並授權將多點傳播流量傳輸到纜線資料機。

思科纜線資料機終端系統(CMTS)和纜線資料機產品執行Cisco IOS®軟體映像，其功能集包括字元「k1」或「k8」支援基線隱私設定，例如ubr7200-k1p-mz.121-6.EC1.bin。

本文檔討論在DOCSIS1.0模式下運行的思科產品的基線隱私保護。

開始之前

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

必要條件

本文件沒有特定先決條件。

採用元件

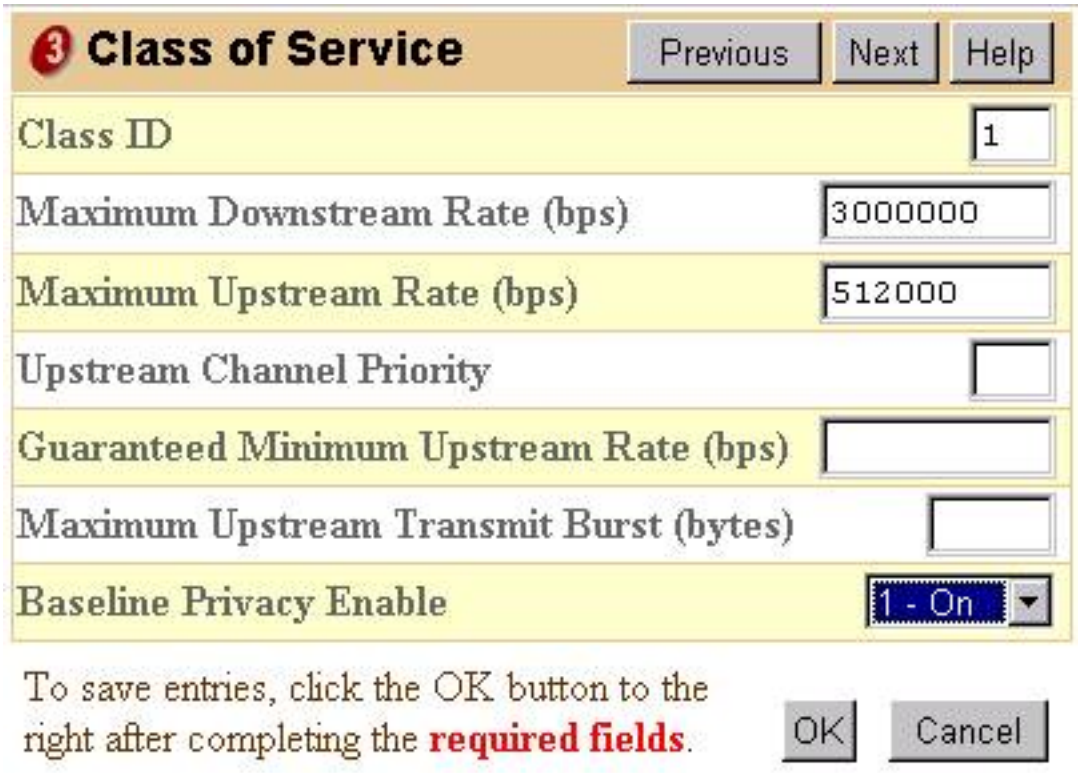
本文中的資訊是根據設定執行Cisco IOS®軟體版本12.1(6)EC的uBR7246VXR，但也適用於所有其他Cisco CMTS產品和軟體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您在即時網路中工作，請確保在使用任何命令之前瞭解其潛在影響。

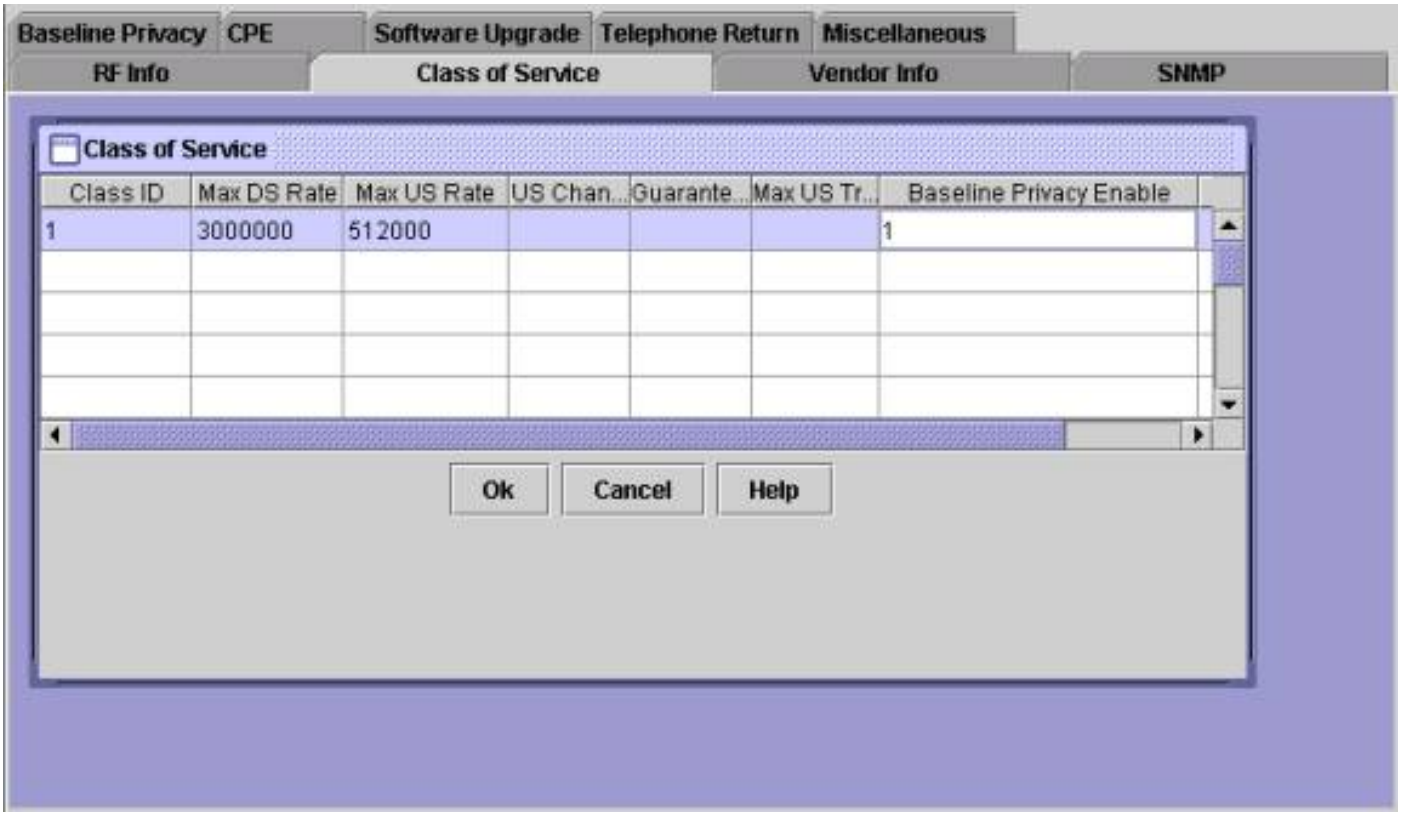
如何配置電纜數據機的基線隱私

如果通過DOCSIS配置檔案中的「服務類別」引數命令纜線資料機使用基線隱私，則只會嘗試使用基線隱私。DOCSIS配置檔案包含數據機的運行引數，在聯機過程中通過TFTP下載。

建立DOCSIS配置檔案的方法之一是使用Cisco.com上的DOCSIS電纜數據機配置器。使用DOCSIS纜線資料機配置器，您可以建立一個DOCSIS配置檔案，通過將「服務類別」頁籤下的「基線隱私啟用」欄位設定為「開**啟**」，命令纜線資料機使用基線隱私。請參閱以下範例：



或者，可使用中的獨立版本的DOCSIS檔案配置來啟用基線隱私，如下所示：



建立支援BPI的DOCSIS配置檔案後，需要重置電纜數據機以下載新的配置檔案，然後使用基線隱私。

如何告知電纜數據機是否使用基線隱私

在Cisco CMTS上，可以使用show cable modem 命令檢視個別纜線資料機的狀態。使用基線保密性的數據機可能會出現幾種狀態。

線上

纜線資料機向Cisco CMTS註冊後，會進入線上狀態。纜線資料機需要達到此狀態，才能與Cisco CMTS交涉基線隱私引數。此時，在電纜數據機和CMTS之間傳送的資料流量未加密。如果電纜數據機保持此狀態，並且未進入下面提及的任何狀態，則數據機未使用基線隱私。

線上(pk)

online(pk)狀態表示纜線資料機能夠與**Cisco CMTS協商授權金鑰**，也稱為**金鑰加密金鑰(KEK)**。這意味著纜線資料機已獲得使用基線隱私的授權，並且已成功協商基線隱私的第一階段。KEK是用於保護後續基線隱私協商的56位金鑰。當數據機處於線上(pk)狀態時，在電纜數據機和Cisco CMTS之間傳送的資料流量仍然未加密，因為尚未協商資料流量加密的金鑰。通常，online(pk)後跟online(pt)。

拒絕(pk)

此狀態表示纜線資料機協商KEK的嘗試已失敗。數據機處於此狀態的最常見原因是Cisco CMTS已開啟數據機身份驗證，並且數據機身份驗證失敗。

online(pt)

此時，數據機已成功與Cisco CMTS協商流量加密金鑰(TEK)。TEK用於加密電纜數據機和Cisco CMTS之間的資料流量。TEK協商過程使用KEK加密。TEK是一個56位或40位金鑰，用於加密電纜數據機與Cisco CMTS之間的資料流量。此時，已成功建立並運行基線隱私，因此在Cisco CMTS和電纜數據機之間傳送的使用者資料正在加密。

reject(pt)

此狀態表示纜線資料機無法成功與Cisco CMTS交涉TEK。

有關show cable modem命令的輸出示例，請參閱以下內容，該命令顯示與基線保密性相關的各種狀態的電纜數據機。

```
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
```

註：有關電纜數據機狀態的詳細資訊，請參閱排除uBR電纜數據機未聯機故障。

影響基線隱私的建立和維護的計時器

可以修改某些超時值以更改「基線」隱私的行為。其中部分引數可在Cisco CMTS上配置，其他引數可通過DOCSIS配置檔案進行配置。除了KEK壽命和TEK壽命外，幾乎沒有理由更改任何這些引數。可以修改這些計時器，以提高電纜裝置的安全性或減少由於BPI管理而產生的CPU和流量開銷。

KEK生存期

KEK生存期是纜線資料機和Cisco CMTS應將交涉的KEK視為有效的時間長度。在此時間過之前，纜線資料機應與Cisco CMTS重新交涉新的KEK。

這一次，您可以使用Cisco CMTS電纜介面指令進行設定：

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

預設設定為604800秒，等於七天。

KEK壽命更短會提高安全性，因為每個KEK將持續更短的時間，因此，如果KEK被駭客侵入，TEK未來的談判將更易被劫持。缺點在於KEK重新協商會增加纜線資料機的CPU使用率，並增加纜線裝置的BPI管理流量。

KEK寬限時間

KEK寬限期是KEK有效期到期之前的時間量，即電纜數據機開始與思科CMTS協商新的KEK。設定此計時器的想法是讓纜線資料機有足夠的時間在KEK到期前進行續訂。

這一次，您可以使用Cisco CMTS電纜介面指令進行設定：

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

您也可以使用DOCSIS配置檔案配置這一次，方法是填寫「基線隱私」頁籤下標籤為**Authorization Grace Timeout**的欄位。如果填寫此DOCSIS配置檔案欄位，則其優先於在Cisco CMTS上配置的任何值。此計時器的預設值為600秒，等於10分鐘。

TEK壽命

TEK生存期是電纜數據機和Cisco CMTS應將協商的TEK視為有效的時間。在此時間過去之前，纜線資料機應與Cisco CMTS重新交涉新的TEK。

這一次，您可以使用Cisco CMTS電纜介面指令進行設定：

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

預設設定為43200秒，等於12小時。

具有較小的TEK壽命會提高安全性，因為每個TEK都會持續較短的時間，因此，如果TEK被駭客侵入，那麼較少的資料會受到未經授權的解密。缺點是TEK重新協商會增加電纜數據機的CPU利用率，並增加電纜工廠的BPI管理流量。

TEK寬限時間

TEK寬限期是指在TEK有效期到期之前，纜線數據機開始與Cisco CMTS協商新TEK所需的時間。設定此計時器的想法是，使電纜數據機有足夠的時間在TEK過期之前進行更新。

這一次，您可以使用Cisco CMTS電纜介面指令進行設定：

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

您也可以使用DOCSIS配置檔案配置這一次，方法是填寫「基線隱私」頁籤下標籤為**TEK Grace Timeout**的欄位。如果填寫此DOCSIS配置檔案欄位，則其優先於在Cisco CMTS上配置的任何值。

此計時器的預設值為600秒，等於10分鐘。

授權等待超時

此時間控制纜線資料機在首次協商KEK時等待思科CMTS回應的時間量。

您可以通過修改「基線隱私」頁籤下的**授權等待超時**欄位，在DOCSIS配置檔案中配置此時間。

此欄位的預設值為10秒，有效範圍為2到30秒。

重新授權等待超時

此時間控制由於KEK有效期即將到期而協商新KEK時，纜線資料機等待來自Cisco CMTS的響應的時間。

可以通過修改「基線隱私」頁籤下的**重新授權等待超時**欄位，在DOCSIS配置檔案中配置此時間。

此計時器的預設值為10秒，有效範圍為2到30秒。

授權寬限超時

指定重新授權的寬限期（以秒為單位）。 預設值為600。有效範圍為1到1800秒。

授權拒絕等待超時

如果纜線資料機嘗試與Cisco CMTS交涉KEK，但遭到拒絕，它必須等待授權拒絕等待逾時，才能重新嘗試交涉新的KEK。

可以使用Baseline Privacy頁籤下的**Authorize Reject Wait Timeout**欄位在DOCSIS配置檔案中配置此引數。此計時器的預設值為60秒，有效範圍為10秒至600秒。

操作等待超時

此時間控制首次協商TEK時，纜線資料機等待來自Cisco CMTS響應的時間。

可以通過修改Baseline Privacy頁籤下的**Operational Wait Timeout**欄位在DOCSIS配置檔案中配置此時間。

此欄位的預設值為1秒，有效範圍為1到10秒。

重新生成金鑰等待超時

此時間控制電纜數據機在協商新的TEK時等待來自Cisco CMTS的響應的時間，因為TEK生存期即將到期。

可以通過修改「基線隱私」頁籤下的**金鑰等待超時**欄位在DOCSIS配置檔案中配置此時間。

此計時器的預設值為1秒，有效範圍為1到10秒。

Cisco CMTS基線隱私配置命令

以下電纜介面命令可用於在Cisco CMTS上配置基線隱私和基線隱私相關功能。

電纜隱私

cable privacy 命令可在特定介面上啟用基線隱私協商。如果在電纜介面上配置了**no cable privacy**命令，則在該介面上聯機時，不允許電纜數據機協商基線隱私。禁用基線隱私時應小心，因為如果電纜數據機的DOCSIS配置檔案命令其使用基線隱私，而Cisco CMTS拒絕讓其協商基線隱私，那麼數據機可能無法保持聯機。

必須提供電纜隱私

如果配置了**cable privacy mandatory**命令，並且纜線資料機在其DOCSIS配置檔案中啟用了基線隱私，則纜線資料機必須成功協商並使用基線隱私，否則不允許其保持聯機。

如果電纜數據機的DOCSIS配置檔案沒有指示數據機使用基線隱私，則**cable privacy mandatory**命令不會使數據機保持聯機。

預設情況下，未啟用**cable privacy mandatory**命令。

cable privacy authenticate-modem

可以對參與基線保密性的數據機執行一種形式的認證。當纜線資料機與Cisco CMTS交涉KEK時，資料機會將其6位元組MAC位址和序列編號的詳細資訊傳輸到Cisco CMTS。這些引數可以用作驗證纜線資料機的使用者名稱/密碼組合。Cisco CMTS使用Cisco IOS驗證、授權和記帳(AAA)服務來完成此操作。身份驗證失敗的電纜數據機不允許聯機。此外，不使用基線保密性的纜線資料機不受此命令的影響。

注意：由於此功能使用AAA服務，因此您需要確保在修改AAA配置時小心謹慎，否則可能會無意中失去登入和管理Cisco CMTS的能力。

以下是執行數據機身份驗證的方法的一些配置示例。在這些組態範例中，許多資料機已輸入驗證資料庫。數據機的6個二進位制八位數MAC地址用作使用者名稱，可變長度序列號用作密碼。請注意，一個數據機的序列號明顯不正確。

以下部分示例Cisco CMTS配置使用本地身份驗證資料庫對多個電纜數據機進行身份驗證。

```
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
```

另一種驗證資料機的方法是使用外部RADIUS伺服器。以下是使用外部RADIUS伺服器驗證資料機的部分Cisco CMTS組態範例

```
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
```

下面是一個示例RADIUS使用者資料庫檔案，其中包含與以上使用本地身份驗證的示例相同的資訊。使用者檔案被許多商業和免費的RADIUS伺服器用作儲存使用者身份驗證資訊的資料庫。

```
# 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
```

以下是在使用上述任一組態範例的Cisco CMTS上執行的**show cable modem**命令的輸出。您會看到，任何未列在本機身份驗證資料庫中、或序列號不正確的啟用基線隱私的數據機都將進入**reject(pk)狀**態，並且不會保持聯機。

```
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
```

SID為17的數據機在身份驗證資料庫中沒有條目，但能夠聯機，因為其DOCSIS配置檔案未命令它使用基線隱私。

具有SID 18、21和22的數據機能夠聯機，因為它們具有身份驗證資料庫中的正確條目

SID為19的數據機無法聯機，因為已命令它使用基線隱私，但該數據機的身份驗證資料庫中沒有條目。此數據機最近會處於reject(pk)狀態，表明其身份驗證失敗。

SID為20的數據機無法聯機，因為儘管身份驗證資料庫中有一個條目使用此數據機的MAC地址，但相應的序列號不正確。目前，此數據機處於reject(pk)狀態，但將在很短時間後轉換到離線狀態。

當數據機身份驗證失敗時，會向Cisco CMTS日誌新增一條沿以下行的消息。

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

然後將電纜數據機從站台維護清單中刪除，並在30秒內標籤為離線。然後，電纜數據機很可能會再次嘗試聯機，但被再次拒絕。

注意：思科不建議客戶使用**cable privacy authenticate-modem命令**來阻止未授權的電纜數據機聯機。確保未授權客戶無法訪問服務提供商網路的更高效的方法是配置調配系統，以便在網路訪問欄位設定為off的情況下指示未授權電纜數據機下載DOCSIS配置檔案。這樣，數據機不會因不斷重新調整範圍而浪費寶貴的上行頻寬。相反，數據機將進入**online(d)狀**態，這表示數據機後面的使用者不會被授予訪問服務提供商網路的許可權，並且數據機將僅使用上行頻寬進行站台維護。

用於監視BPI狀態的命令

show interface cable X/0 privacy [kek | tek] — 此命令用於顯示與KEK或TEK關聯的計時器，如CMTS介面上設定的計時器。

以下是此命令的示例輸出。

```
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 — 此隱藏命令可用於檢視在特定電纜介面上使用基線隱私的SID數量的統計資訊。

以下是此命令的示例輸出。

```
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 — 此命令啟用基線隱私的調試。啟用此命令後，每當發生基線隱私狀態更改或基線隱私事件時，詳細資訊將顯示在控制檯上。此命令僅在使用**debug cable interface cable X/0**或**debug cable mac-address** *mac-address* 命令之前起作用。

debug cable bpiatp — 此命令啟用基線隱私的調試。啟用此命令後，每當Cisco CMTS傳送或接收基線隱私消息時，都會顯示消息的十六進位制轉儲。此命令僅在使用**debug cable interface cable X/0**或**debug cable mac-address** *mac-address* 命令之前起作用。

debug cable keyman — 此命令啟用基線隱私金鑰管理的調試。啟用此命令時，會顯示基線隱私金鑰管理的詳細資訊。

排除BPI故障

纜線資料機顯示為聯機，而非聯機(pt)。

如果數據機處於聯機狀態而不是聯機(pt)，則通常意味著以下三種情況之一。

第一個可能的原因是，尚未為電纜數據機提供DOCSIS配置檔案，指定電纜數據機使用基線隱私。檢查DOCSIS配置檔案在傳送到數據機的服務類別配置檔案中是否啟用了BPI。

數據機處於聯機狀態的第二個原因可能是數據機正在等待開始協商BPI。等待一兩分鐘，檢視數據機是否將狀態更改為online(pt)。

最終原因可能是數據機不包含支援基線隱私的韌體。請聯絡您的數據機供應商，獲取支援BPI的韌體的最新版本。

纜線資料機顯示為拒絕(pk)狀態，然後離線。

數據機進入reject(pk)狀態的最可能原因是電纜數據機身份驗證已經使用**cable privacy authenticate-modem**命令啟用，但AAA配置錯誤。檢查受影響的數據機的序列號和mac地址是否已正確輸入身份驗證資料庫，以及任何外部RADIUS伺服器是否可訪問且運行正常。您可以使用路由器調試命令

debug aaa authentication和**debug radius**來瞭解RADIUS伺服器的狀態或數據機身份驗證失敗的原因。

註：有關對電纜數據機連線進行故障排除的一般資訊，請參閱對uBR電纜數據機不能聯機進行故障排除。

特殊註釋 — 隱藏命令

本文檔對隱藏命令的任何引用均僅供參考。思科技術協助中心(TAC)不支援隱藏命令。 此外還有隱藏命令：

- 不一定生成可靠或正確的資訊
- 如果執行，可能會導致意外的副作用
- 在不同版本的Cisco IOS軟體中行為可能不同
- 可以隨時從未來版本的Cisco IOS軟體中刪除，恕不另行通知

相關資訊

- CableLabs
- **驗證、授權及記帳(AAA)**
- 技術支援 - Cisco Systems