解決方法並恢復uBR10K上過期的製造商證書

目錄

簡介

本文檔介紹用於防止、解決和恢復電纜數據機(CM)拒絕(pk)服務對uBR10K電纜數據機終端系統(CMTS)產生的製造商證書（手動證書）到期影響的選項。

問題

在uBR10K上，CM停滯在reject(pk)狀態的原因不同。一個原因是手動證書過期。Manu Cert用於CM和CMTS之間的身份驗證。在本文檔中，Manu Cert是DOCSIS 3.0安全規範CM-SP-SECv3.0所說的CableLabs Mfg CA證書或製造商CA證書。Expire表示uBR10K系統日期/時間超出手動證書有效結束日期/時間。

在Manu Cert過期後嘗試向uBR10K註冊的CM被CMTS標籤為reject(pk)，並且不在服務中。已在uBR10K中註冊並在服務中的CM在Manu Cert過期時可以保持服務狀態，直到CM嘗試註冊下次為止，這可以在單個數據機離線事件、uBR10K電纜線卡重新啟動、uBR10K重新載入或觸發數據機註冊

的其他事件之後發生。此時，CM身份驗證失敗，被uBR10K標籤為拒絕(pk)，並且不在服務中。

適用於Cisco CMTS路由器的DOCSIS 1.1提供有關uBR10K支援和配置DOCSIS基線隱私介面(BPI+)的其他資訊。

Manu證書資訊

可通過uBR10K CLI命令或簡單網路管理協定(SNMP)檢視手動證書資訊。 這些命令和資訊用於本文檔中介紹的解決方案。

手動證書資訊欄位和屬性

- 索引：分配給uBR10K資料庫/MIB中每個Manu證書的唯一整數
- 主題： 使用者名稱與它在X509憑證中編碼的完全相同
  cn:公用名ou:組織單位o:組織l:地區s:StateOrProvinceName思:國家/地區名稱
- 頒發者：證書頒發機構
- 串列：以十六進位制八位位元組字串表示的證書序列號
- 狀態:證書的信任狀態
  可信不可信鏈接根
- 來源：憑證如何到達CMTS
  snmp配置檔案外部資料庫其他authentInfocompiledInfoCode
- 狀態/行狀態：證書狀態
  active（作用中）notInService未就緒createAndGocreateandWait銷毀
- 證書：X509 DER編碼的證書頒發機構證書
- 有效日期：定義相對於CMTS系統日期和時間的manu證書有效期的起始日期和終止日期
  開始日期：Manu證書生效的日期和時間結束日期：Manu證書不再有效的日期和時間
- 證書：X509 DER編碼的證書頒發機構證書
- 指紋：CA憑證的SHA-1雜湊

uBR10K CLI命令

此命令的輸出包括一些手動證書資訊。手動證書索引只能通過SNMP獲取

- 在uBR10K CLI exec模式或線路卡CLI exec模式下：uBR10K#**show cable privacy manufacturer-cert-list**
- 在uBR10K線路卡CLI執行模式下：Slot-6-0#**show crypto pki certificates**

以下纜線介面組態指令用於解決和復原

- uBR10K(config-if)#cable privacy retain-failed-certificates
- uBR10K(config-if)#cable privacy skip-validity-period

DOCSIS-BPI-PLUS-MIB OID

Manu證書資訊在docsBpi2CmtsCACertEntry OID分支1.3.6.1.2.1.10.127.6.1.2.5.2.1中定義，如SNMP對象導航器中所述。

附註：在uBR10k軟體中，RFC 4131 docsBpi2MIB / DOCS-IETF-BPI2-MIB是用錯誤的OID

MIB分支/路徑實現的。uBR10k平台已停止銷售，並且已超過軟體支援結束日期，因此沒有針對此軟體缺陷的修復。取代預期的MIB路徑/分支1.3.6.1.2.10.127.6, **MIB路徑/分支1.3.6.1.2.1.9999必須用於uBR10k上與BPI2 MIB/OID的SNMP互動。**
相關思科錯誤ID CSCum28486

以下是uBR10k上手動證書資訊的BPI2 MIB OID完整路徑等價物，如思科錯誤ID CSCum28486中所述：

```
docsBpi2CmtsCACertTable = 1.3.6.1.2.1.9999.1.2.5.2
docsBpi2CmtsCACertEntry = 1.3.6.1.2.1.9999.1.2.5.2.1
docsBpi2CmtsCACertIndex = 1.3.6.1.2.1.9999.1.2.5.2.1.1
docsBpi2CmtsCACertSubject = 1.3.6.1.2.1.9999.1.2.5.2.1.2
docsBpi2CmtsCACertIssuer = 1.3.6.1.2.1.9999.1.2.5.2.1.3
docsBpi2CmtsCACertSerialNumber = 1.3.6.1.2.1.9999.1.2.5.2.1.4
docsBpi2CmtsCACertTrust = 1.3.6.1.2.1.9999.1.2.5.2.1.5
docsBpi2CmtsCACertSource = 1.3.6.1.2.1.9999.1.2.5.2.1.6
docsBpi2CmtsCACertStatus = 1.3.6.1.2.1.9999.1.2.5.2.1.7
docsBpi2CmtsCACert = 1.3.6.1.2.1.9999.1.2.5.2.1.8
```

本文檔中的命令示例使用省略號(...)表示為便於閱讀，某些資訊已被省略。

解決方案

CM韌體更新是最好的長期解決方案。本文檔中介紹了允許具有已過期的Manu證書的CM註冊並使用uBR10K保持線上的解決方法，但僅建議短期使用這些解決方法。如果CM韌體更新不可行，則從安全和運營的角度來看，CM更換策略是一個很好的長期解決方案。此處描述的解決方案可解決不同的條件或情形，並可以單獨使用，有些還可相互結合使用；

- 更新CM韌體
- 將已知手動證書設定為「可信」
- 已知手動證書到期後恢復CM服務
- 在uBR10k上安裝未知的過期手動證書並標籤為受信任
- 允許通過AuthInfo使用uBR10K CLI命令新增過期的CM證書和手動證書

附註：如果刪除BPI，則會禁用加密和身份驗證，從而最大程度地降低了作為解決方案的可行性。

更新CM韌體

在許多情況下，CM製造商會提供CM韌體更新，以延長Manu證書的有效結束日期。此解決方案是最佳選擇，當在Manu Cert過期之前執行時，可防止相關服務影響。CM載入新韌體，並用新的手動證書和CM證書重新註冊。新證書可以正確進行身份驗證，並且CM可以成功向uBR10K註冊。新的Manu Cert和CM Cert可以建立一個新的證書鏈，使其返回已安裝在uBR10K中的已知根證書。

將已知手動證書設定為「可信」

當CM韌體更新因CM製造商停業、不再支援CM型號等而不可用時，可以在到期前在uBR10k中主動標籤已知、有效終止日期不久的手動證書。使用uBR10K CLI命令可以找到手動證書序列號、有效結束日期和狀態。使用SNMP可以找到手動證書序列號、信任狀態和索引。

當前服務中數據機的已知手動證書通常由uBR10K通過DOCSIS基線隱私介面(BPI)協定從CM獲取。

從CM傳送到uBR10K的AUTH-INFO消息包含手動證書。每個唯一的Manu證書儲存在uBR10K記憶體中，其資訊可通過uBR10K CLI命令和SNMP檢視。

當Manu Cert標籤為可信任時，它會執行兩個重要操作。首先，它允許uBR10K BPI軟體忽略過期有效日期。其次，它將Manu Cert儲存為uBR10K NVRAM中受信任的。這保留了uBR10K重新載入的Manu Cert狀態，並消除了在uBR10K重新載入時重複此過程的需要

CLI和SNMP命令示例演示了如何識別手動證書索引、序列號、信任狀態；然後使用該資訊將信任狀態更改為可信。示例重點介紹具有索引5和序列號45529C2654797E1623C6E723180A9E9C的Manu證書。

從uBR10K CLI檢視許多證書資訊

在本示例中，uBR10K CLI命令**show crypto pki certificates**和**show cable privacy manufacturer-cert-list**用於檢視已知的Manu Cert資訊。

```
UBR10K-01#telnet 127.0.0.81
Trying 127.0.0.81 ... Open

clc_8_1>en
clc_8_1#show crypto pki certificates
CA Certificate
 Status: Available
  Certificate Serial Number: 45529C2654797E1623C6E723180A9E9C
 Certificate Usage: Not Set
 Issuer:
   cn=DOCSIS Cable Modem Root Certificate Authority
   ou=Cable Modems
   o=Data Over Cable Service Interface Specifications
   c=US
 Subject:
   cn=Arris Cable Modem Root Certificate Authority
   ou=Suwanee\
    Georgia
   ou=DOCSIS
   o=Arris Interactive\
    L.L.C.
   c=US
 Validity Date:
   start date: 20:00:00 EDT Sep 11 2001
    end   date: 19:59:59 EDT Sep 11 2021
 Associated Trustpoints: 0edbf2a98b45436b6e4b464797c08a32f2a2cd66
clc_8_1#exit

[Connection to 127.0.0.81 closed by foreign host]

uBR10K-01#show cable privacy manufacturer-cert-list
Cable Manufacturer Certificates:

Issuer: cn=DOCSIS Cable Modem Root Certificate Authority,ou=Cable Modems,o=Data Over Cable
Service Interface Specifications,c=US
Subject: cn=Arris Cable Modem Root Certificate Authority,ou=Suwanee\, Georgia,ou=DOCSIS,o=Arris
Interactive\, L.L.C.,c=US
State: Chained  <-- Cert Trust State is Chained
Source: Auth Info    <-- CertSource is Auth Info
RowStatus: Active
Serial: 45529C2654797E1623C6E723180A9E9C  <-- Serial Number
Thumbprint: DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
```

從遠端裝置檢視SNMP手動證書資訊

相關uBR10K SNMP OID:

```
docsBpi2CmtsCACertTable = 1.3.6.1.2.1.9999.1.2.5.2.1
docsBpi2CmtsCACertSubject = 1.3.6.1.2.1.9999.1.2.5.2.1.2
docsBpi2CmtsCACertIssuer = 1.3.6.1.2.1.9999.1.2.5.2.1.3
docsBpi2CmtsCACertSerialNumber = 1.3.6.1.2.1.9999.1.2.5.2.1.4
docsBpi2CmtsCACertTrust = 1.3.6.1.2.1.9999.1.2.5.2.1.5
docsBpi2CmtsCACertSource = 1.3.6.1.2.1.9999.1.2.5.2.1.6
```

在本示例中，snmpwalk命令用於檢視uBR10k手動證書表中的資訊。已知的Manu Cert序列號可與用於設定信任狀態的Manu Cert Index關聯。特定的SNMP命令和格式取決於用於執行SNMP命令/請求的裝置和作業系統。

```
Workstation-1$snmpwalk -v 2c -c snmpstring1 192.168.1.1 1.3.6.1.2.1.9999.1.2.5.2.1
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.2.1 = STRING: "Data Over Cable Service Interface
Specifications"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.2.2 = STRING: "tComLabs - Euro-DOCSIS"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.2.3 = STRING: "Scientific-Atlanta\\"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.2.4 = STRING: "CableLabs\\"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.2.5 = STRING: "Arris Interactive\\"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.3.1 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.3.2 = STRING: "Euro-DOCSIS Cable Modem Root CA"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.3.3 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.3.4 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.3.5 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.4.1 = Hex-STRING: 58 53 64 87 28 A4 4D C0 33 5F 0C DB 33 84 9C
19
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.4.2 = Hex-STRING: 63 4B 59 63 79 0E 81 0F 3B 54 45 B3 71 4C F1
2C
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.4.3 = Hex-STRING: 57 BF 2D F6 0E 9F FB EC F8 E6 97 09 DE 34 BC
26
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.4.4 = Hex-STRING: 26 B0 F6 BD 1D 85 E8 E8 E8 C1 BD DF 17 51 ED
8C
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.4.5 = Hex-STRING: 45 52 9C 26 54 79 7E 16 23 C6 E7 23 18 0A 9E
9C <-- Serial Number
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.1 = INTEGER: 4
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.2 = INTEGER: 4
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.3 = INTEGER: 3
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.4 = INTEGER: 3
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.5 = INTEGER: 3 <-- Trust State (3 = Chained)
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.6.1 = INTEGER: 4
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.6.2 = INTEGER: 4
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.6.3 = INTEGER: 5
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.6.4 = INTEGER: 5
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.6.5 = INTEGER: 5 <-- Source authentInfo (5)
```

將過期已知手動證書信任狀態設定為Trusted with SNMP

OID的值： docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5（uBR10k上的OID為1.3.6.1.2.1.999.1.2.5.2.1.5）

1:可信
2:不可信
3:鏈接
4:根

此示例顯示對於索引為= 5且序列號為45529C2654797E1623C6E723180A9E9C的Manu證書，信任狀態從鏈結更改為可信。

```
Workstation-1$ snmpset -v 2c -c snmpstring1 192.168.1.1 1.3.6.1.2.1.9999.1.2.5.2.1.5.5 i 1
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.5 = INTEGER: 1
```

使用uBR10K CLI或SNMP確認手動證書已更改

- 信任值已從連結更改為「信任」
- 來源值變更為「SNMP」，表示憑證上次由SNMP管理，而不是從BPI通訊協定AuthInfo訊息管理

```
Workstation-1$ snmpwalk -v 2c -c snmpstring1 192.168.1.1 1.3.6.1.2.1.9999.1.2.5.2.1
...
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.2.5 = STRING: "Arris Interactive\\"
...
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.3.5 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
...
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.4.5 = Hex-STRING: 45 52 9C 26 54 79 7E 16 23 C6 E7 23 18 0A 9E
9C <-- Serial Number
...
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.5 = INTEGER: 1 <-- Trust State (3 = trusted)
...
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.6.5 = INTEGER: 1 <-- Source (1 = SNMP)
```

```
uBR10K-01#show cable privacy manufacturer-cert-list
Cable Manufacturer Certificates:

Issuer: cn=DOCSIS Cable Modem Root Certificate Authority,ou=Cable Modems,o=Data Over Cable
Service Interface Specifications,c=US
Subject: cn=Arris Cable Modem Root Certificate Authority,ou=Suwanee\, Georgia,ou=DOCSIS,o=Arris
Interactive\, L.L.C.,c=US
State: Trusted
Source: SNMP
RowStatus: Active
Serial: 45529C2654797E1623C6E723180A9E9C
Thumbprint: DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
```

已知手動證書到期後恢復CM服務

以前已知的Manu證書是uBR10K資料庫中已經存在的證書，通常是由來自以前CM註冊的AuthInfo消息導致的。如果Manu Cert未標籤為受信任且證書過期，則使用過期的Manu Cert的所有CM隨後可以離線並嘗試註冊，但uBR10K會將其標籤為reject(pk)，並且它們不在服務中。本節介紹如何從該條件中恢復，以及如何允許具有過期的Manu證書的CM註冊和保持服務。

識別過期的已知手動證書序列號

使用uBR10K CLI命令**show cable modem <CM MAC Address> privacy**可以檢查停滯在reject(pk)中的CM的Manu Cert資訊。

```
show cable modem 1234.5678.9abc privacy verbose

MAC Address : 1234.5678.9abc
Primary SID : 4640
```

```
BPI Mode : BPI+++
BPI State : reject(kek)
Security Capabilities :
BPI Version : BPI+++
Encryption : DES-56
EAE : Unsupported
Latest Key Sequence : 1
...
Expired Certificate : 1
Certificate Not Activated: 0
Certificate in Hotlist : 0
Public Key Mismatch : 0
Invalid MAC : 0
Invalid CM Certificate : 0
CA Certificate Details :
Certificate Serial : 45529C2654797E1623C6E723180A9E9C
Certificate Self-Signed : False
Certificate State : Chained
CM Certificate Details :
CM Certificate Serial : 008D23BE727997B9D9F9D69FA54CF8A25A
CM Certificate State : Chained,CA Cert Expired
KEK Reject Code : Permanent Authorization Failure
KEK Reject Reason : CM Certificate Expired
KEK Invalid Code : None
KEK Invalid Reason : No Information
```

識別已過期已知Manu證書的索引，並將Manu證書信任狀態設定為「可信」

使用上一節所述的相同uBR10K CLI和SNMP命令，根據手動證書序列號識別Manu Cert的索引。使用過期的Manu Cert索引號將Manu Cert信任狀態設定為SNMP可信任狀態。

```
jdoe@server1[983]-->./snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.9999.1.2.5.2.1.4
...
1.3.6.1.2.1.9999.1.2.5.2.1.4.5 = Hex-STRING: 45 52 9C 26 54 79 7E 16 23 C6 E7 23 18 0A 9E 9C
...

jdoe@server1[983]-->./setany -v2c 192.168.1.1 private 1.3.6.1.2.1.9999.1.2.5.2.1.5.5 -i 1
docsBpi2CmtsCACertTrust.5 = trusted(1)
```

在uBR10K上安裝未知的過期手動證書並標籤為受信任

如果uBR10K不知道已到期的Manu證書，因此無法在到期之前對其進行管理（標籤為可信）且無法恢復，則必須將該Manu證書新增到uBR10K並標籤為可信。如果以前未知且未在uBR10K上註冊的CM嘗試向未知且過期的Manu證書註冊，則會發生此情況。

Manu Cert可以通過SNMP Set或cable privacy retain-failed-certificates配置新增到uBR10K。

使用SNMP向uBR10K新增到期的未知手動證書

要新增製造商的證書，請向docsBpi2CmtsCACertTable表新增一個條目。為每個條目指定這些屬性。

- docsBpi2CmtsCACertStatus 1.3.6.1.2.1.999.1.2.5.2.1.7（設定為4以建立行條目）
- docsBpi2CmtsCACert = 1.3.6.1.2.1.999.1.2.5.2.1.8（對於實際X.509證書，十六進位制資料作為X509證書值）
- docsBpi2CmtsCACertTrust 1.3.6.1.2.1.999.1.2.5.2.1.5（設定為1將手動證書信任狀態設定為可信）

大多數作業系統無法接受輸入行，這些行與輸入指定證書的十六進位制字串所需的長度一樣長。因此，建議使用圖形SNMP管理器來設定這些屬性。對於許多證書，如果更方便，可以使用指令碼檔案。

SNMP命令和示例中的結果將ASCII DER編碼的ASN.1 X.509證書新增到uBR10K資料庫中，其引數如下：

```
Index = 11
Status = createAndGo (4)
Trust state =  trusted (1)
```

為新增的Manu證書使用唯一的索引號。新增過期的手動證書時，除非手動將其設定為可信，否則該狀態將不可信。如果新增了自簽名證書，則必須在uBR10K接受證書之前，在uBR10K電纜介面配置下配置**cable privacy accept-self-signed-certificate** 命令。

在本示例中，由於可讀性而省略了某些證書內容，這些內容用說明(...)表示。

```
jdoe@server1[983]-->./setany -v2c 192.168.1.1 private 1.3.6.1.2.1.9999.1.2.5.2.1.7.11 -i 4
1.3.6.1.2.1.9999.1.2.5.2.1.8.11 - o "30 82 04 00 30 82 02 e8 a0 03 02 01
02 02 10 43 74 98 f0 9a 7d cb c1 fa 7a a1 01 fe 97 6e 40 30 0d 06 09 2a 86 48 86 f7 0d 01 01 05
05 00 30 81 97 31 0b 30 09 06 03 55 04 06 13 02 55 53
...
d8 26 21 f1 41 eb c4 87 90 65 2d 23 38 08 31 9c 74 16 30 05 18 d2 89 5e 9b 21 13 e3 e9 6a f9 3b
59 5e e2 05 0e 89 e5 9d 2a 40 c2 9b 4f 21 1f 1b b7 2c
13 19 3d 56 ab 4b 09 a9 1e 62 5c ee c0 d2 ba 2d" 1.3.6.1.2.1.9999.1.2.5.2.1.5.11 -i 1
docsBpi2CmtsCACertStatus.11 = createAndGo(4)
docsBpi2CmtsCACert.11 =
30 82  04 00   30 82  02 e8    a0 03  02 01   02 02  10 43
74 98  f0 9a   7d cb  c1 fa    7a a1  01 fe   97 6e  40 30
...
f9 3b  59 5e   e2 05  0e 89    e5 9d  2a 40   c2 9b  4f 21
1f 1b  b7 2c   13 19  3d 56    ab 4b  09 a9   1e 62  5c ee
c0 d2  ba 2d
docsBpi2CmtsCACertTrust.11 = trusted(1)
```

在CLI中的CM註冊期間新增過期的Manu證書

手動證書通常通過從CM傳送到uBR10K的BPI協定AuthInfo消息進入uBR10K資料庫。在AuthInfo消息中收到的每個唯一且有效的手動證書都會新增到資料庫中。如果CMTS（不在資料庫中）未知的Manu Cert且有效期已過期，則AuthInfo會被拒絕，並且Manu Cert不會新增到uBR10K資料庫中。當uBR10K電纜介面配置下存在**cable privacy retain-failed-certificates**配置時，AuthInfo可以將Invalid Manu Cert新增到uBR10K。這樣允許將過期的手動證書作為不可信的證書新增到uBR10K資料庫。要使用過期的Manu證書，必須使用SNMP將其標籤為可信。

```
uBR10K#config t
Enter configuration commands, one per line.  End with CNTL/Z.
uBR10K(config)#int Cable6/0/0
uBR10K(config-if)#cable privacy retain-failed-certificates
uBR10K(config-if)#end
```

將過期的手動證書新增到uBR10K並標籤為託管時，建議刪除**cable privacy retain-failed-certificates**配置，以防止在uBR10K上新增其他未知的過期的手動證書。

允許通過AuthInfo使用uBR10K CLI命令新增過期的CM證書和手動證書

在某些情況下，CM證書會過期。在這種情況下，除了**cable privacy retain-failed-certificates**配置之

外，還需要在uBR10K上進行其他配置。在每個相關uBR10K MAC域（電纜介面）下，新增**cable privacy skip-validity-period**配置並儲存配置。這會導致uBR10K忽略在CM BPI AuthInfo消息中傳送的所有CM和Manu證書的過期有效期檢查。

```
uBR10K#config t
Enter configuration commands, one per line.  End with CNTL/Z.
uBR10K(config)#interface Cable6/0/0
uBR10K(config-if)#cable privacy skip-validity-period
uBR10K(config-if)#end
uBR10K#copy run start
```

其他資訊

MAC域/電纜介面配置注意事項

cable privacy retain-failed-certificates和cable privacy skip-validity-period配置命令在MAC域/電纜介面級別使用，不受限制。retain-failed-certificates命令可以將任何失敗的證書新增到uBR10K資料庫中，而skip-validity-period命令可以跳過所有Manu和CM證書上的生效日期檢查。

SNMP封包大小注意事項

使用大型證書時，可能需要額外的uBR10K SNMP配置。如果證書OctetString大於SNMP資料包大小，則證書資料的SNMP獲取可以為NULL。 例如；

```
uBR10K#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
uBR10K(config)#snmp-server packetsize 3000
uBR10K(config)#end
```

手動證書調試

使用**debug cable privacy ca-cert**和**debug cable mac-address <cm mac-address>**命令支援uBR10K使用者上的Manu Cert debug。 有關其他調試資訊，請參閱支援文章[如何解碼數據機停滯狀態診斷的DOCSIS證書。]

相關支援檔案

- [cBR-8產品公告上的纜線資料機和即將到期的製造商證書 — 思科]
- [Cisco uBR10000系列通用寬頻路由器]
- [技術支援與文件 - Cisco Systems]