解决方法，并在uBR10K上恢复过期制造商证书

目录

简介

本文档介绍防止、解决和从电缆调制解调器(CM)拒绝(pk)服务中恢复对制造商证书(Manu Cert)过期导致的uBR10K电缆调制解调器终端系统(CMTS)的影响的选项。

问题

CM在uBR10K上陷入拒绝(pk)状态有不同的原因。原因之一是Manu证书过期。Manu证书用于CM和CMTS之间的身份验证。在本文档中，Manu Cert是DOCSIS 3.0安全规范CM-SP-SECv3.0所指的CableLabs Mfg CA证书或制造商CA证书。过期表示uBR10K系统日期/时间超过Manu Cert有效期结束日期/时间。

尝试在Manu证书到期后向uBR10K注册的CM被CMTS标记为reject(pk)，且未在服务中。已向uBR10K注册并在Manu Cert到期时服务的CM可在CM下次尝试注册之前保持服务，这可能发生在单个调制解调器脱机事件、uBR10K电缆线卡重新启动、uBR10K重新加载或触发调制解调器注册的其

他事件之后。当时，CM身份验证失败，被uBR10K标记为reject(pk)，并且未在服务中。

适用于Cisco CMTS路由器的DOCSIS 1.1提供了有关uBR10K支持和DOCSIS基线隐私接口(BPI+)配置的其他信息。

Manu认证信息

可以通过uBR10K CLI命令或简单网络管理协议(SNMP)查看Manu Cert信息。 本文档中介绍的解决方案使用了这些命令和信息。

Manu证书信息字段和属性

- 索引：分配给uBR10K数据库/MIB中每个Manu证书的唯一整数
- 主题： 与X509证书中编码的使用者名称完全相同
  cn:公用名ou:组织单位o:组织l:地区s:StateOrProvinceNamec：国家/地区名称
- 颁发机构：证书颁发机构
- 序列：以十六进制二进制八位数字符串表示的证书序列号
- 状态:证书的信任状态
  可信不可信链式根
- 来源：证书如何到达CMTS
  snmpconfigurationFileexternalDatabaseother（其他）authentInfocompiledInfoCode
- 状态/行状态：证书状态
  主用notInService未就绪createAndGocreateandWait销毁
- 证书：X509 DER编码的证书颁发机构证书
- 有效日期：与CMTS系统日期和时间相关，定义Manu Cert有效期的开始和结束日期
  开始日期:Manu证书生效的日期和时间终止日期：Manu证书不再有效的日期和时间
- 证书：X509 DER编码的证书颁发机构证书
- 指纹：CA证书的SHA-1哈希

uBR10K CLI命令

此命令的输出包括一些Manu Cert信息。Manu Cert索引只能通过SNMP获取

- 在uBR10K CLI执行模式或线路卡CLI执行模式：uBR10K#**show cable privacy manufacturer-cert-list**
- 在uBR10K线卡CLI执行模式下：Slot-6-0#**show crypto pki certificates**

这些电缆接口配置命令用于解决方法和恢复

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

DOCSIS-BPI-PLUS-MIB OID

Manu证书信息在docsBpi2CmtsCACertEntry OID分支1.3.6.1.1.127.6.1.2.5.2.1中定义，在SNMP对象导航器中描述。

注意：在uBR10k软件中，RFC 4131 docsBpi2MIB / DOCS-IETF-BPI2-MIB使用错误的OID

MIB分支/路径实施。uBR10k平台已停售，已过软件支持日期，因此没有修复此软件缺陷。而不是预期的MIB路径/branch 1.3.6.1.2.10.127.6, **MIB路径/branch 1.3.6.1.2.1.9999必须用于与uBR10k上的BPI2 MIB/OID的SNMP交互。**
相关思科漏洞ID CSCum28486

以下是uBR10k上的Manu Cert信息的BPI2 MIB OID完整路径等价项，如Cisco Bug 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
```

本文档中的命令示例使用省略号(...)来表示为了可读性，已省略某些信息。

解决方案

CM固件更新是最佳的长期解决方案。本文档介绍允许具有过期Manu Cert的CM注册并保持在uBR10K在线的解决方法，但建议这些解决方法仅用于短期使用。如果CM固件更新不是选项，则从安全和运营角度来说，CM更换策略是一个好的长期解决方案。此处介绍的解决方案可解决不同的情况或场景，并可单独使用，也可部分组合使用；

- 更新CM固件
- 将已知Manu证书设置为受信任
- 在已知Manu证书过期后恢复CM服务
- 在uBR10k上安装未知过期的Manu证书并标记受信任
- 使用uBR10K CLI命令允许AuthInfo添加过期的CM证书和Manu证书

注意：如果删除BPI，则会禁用加密和身份验证，这会将这种解决方法的可行性降至最低。

更新CM固件

在许多情况下，CM制造商提供CM固件更新，以延长Manu证书的有效结束日期。此解决方案是最佳选项，在Manu Cert到期前执行时，可防止相关服务影响。CM加载新固件，并向新的Manu Certs和CM Certs重新注册。新证书可以正确进行身份验证，CM可以成功注册到uBR10K。新的Manu Cert和CM Cert可以创建新的证书链，返回到uBR10K中已安装的已知根证书。

将已知Manu证书设置为受信任

当CM固件更新因CM制造商停业、不再支持CM型号等而不可用时，在uBR10k上已知的具有近期有效结束日期的Manu Certs在到期前可在uBR10k中主动标记为受信任。使用uBR10K CLI命令可以找到Manu Cert序列号、有效性结束日期和状态。使用SNMP可以找到Manu Cert序列号、Trust State和索引。

当前服务中和在线调制解调器的已知Manu Certs通常由uBR10K通过DOCSIS基线隐私接口(BPI)协

议从CM获取。从CM发送到uBR10K的AUTH-INFO消息包含Manu证书。每个唯一的Manu Cert都存储在uBR10K内存中，并且其信息可通过uBR10K CLI命令和SNMP查看。

当Manu Cert被标记为受信任时，这将做两件重要事。首先，它允许uBR10K BPI软件忽略过期的有效日期。其次，它将Manu证书存储为受信任的uBR10K NVRAM。这可在uBR10K重新加载期间保留Manu Cert状态，并在uBR10K重新加载时无需重复此过程

CLI和SNMP命令示例演示如何识别Manu Cert索引、序列号、信任状态；然后使用该信息将信任状态更改为受信任状态。这些示例重点介绍具有索引5和序列号45529C2654797E1623C6E723180A9E9C的Manu证书。

从uBR10K CLI查看多证书信息

在本示例中，uBR10K CLI命令**show crypto pki certificates**和**show cable privacy manufacturer-cert-list**用于查看已知的Manu Cert信息。

```
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
```

从远程设备查看SNMP的Manu证书信息

相关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命令用于查看uBR10k Manu证书表中的信息。已知的Manu Cert序列号可以与Manu Cert Index关联，后者可用于设置信任状态。特定SNMP命令和格式取决于用于执行SNMP命令/请求的设备和操作系统。

```
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)
```

将过期的已知Manu证书信任状态设置为SNMP信任

OID的值： docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5（uBR10k上的OID为1.3.6.1.2.1.9999.1.2.2.1.5）

1:可信
2:不可信
3:链式
4:根

示例显示索引= 5且序列号= 45529C2654797E1623C6E723180A9E9C的Manu证书的信任状态从链接更改为受信任。

```
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确认Manu证书已更改

- 信任值从链接更改为“受信任”
- 源值更改为“SNMP”，表示证书上次由SNMP管理，而不是来自BPI协议身份验证信息消息

```
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
```

在已知Manu证书过期后恢复CM服务

以前已知的Manu Cert是已存在于uBR10K数据库中的证书，通常是来自先前CM注册的AuthInfo消息的结果。如果Manu Cert未标记为受信任且证书过期，则使用过期Manu Cert的所有CM随后都可以脱机并尝试注册，但uBR10K将其标记为reject(pk)，并且它们不在服务中。本节介绍如何从此情况中恢复并允许具有过期Manu Certs的CM注册并保持服务。

确定已过期的已知Manu证书序列号

使用uBR10K CLI命令show cable modem <CM MAC Address> privacy可以检**查滞留在reject(pk)中的CM的Manu Cert信息**。

```
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
```

确定已过期的已知Manu证书的索引并将Manu证书信任状态设置为Trusted

使用与上一节中所述相同的uBR10K CLI和SNMP命令，根据Manu Cert序列号确定Manu Cert的索引。 使用过期的Manu Cert索引号将Manu Cert信任状态设置为受SNMP信任。

```
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上安装未知过期的Manu证书并标记受信任

如果uBR10K不知道过期的Manu证书，因此在过期之前无法对其进行管理（标记为受信任）并且无法恢复，则必须将Manu证书添加到uBR10K并标记为受信任。当之前未知且未在uBR10K上注册的CM尝试向未知且过期的Manu证书注册时，会发生此情况。

Manu Cert可通过SNMP Set或电缆隐私保留失败证书配置添加到uBR10K。

使用SNMP将过期的未知Manu证书添加到uBR10K

要添加制造商的证书，请向docsBpi2CmtsCACertTable表添加条目。为每个条目指定这些属性。

- docsBpi2CmtsCACertStatus 1.3.6.1.2.1.9999.1.2.5.2.1.7（设置为4以创建行条目）
- docsBpi2CmtsCACert = 1.3.6.1.2.1.9999.1.2.5.2.1.8（作为实际X.509证书的X509证书值的十六进制数据）
- docsBpi2CmtsCACertTrust 1.3.6.1.2.1.9999.1.2.5.2.1.5（设置为1，将Manu证书信任状态设置为受信任）

大多数操作系统无法接受输入指定证书的十六进制字符串所需的输入行。因此，建议使用图形SNMP管理器来设置这些属性。对于许多证书，如果更方便，可以使用脚本文件。

SNMP命令并导致本示例将ASCII DER编码ASN.1 X.509证书添加到uBR10K数据库，其参数为：

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

为已添加的Manu证书使用唯一索引号。添加过期的Manu证书时，状态不可信，除非手动将其设置为受信。如果添加了自签名证书，则必须在uBR10K电缆接口配置下配置**cable privacy accept-self-signed-certificate**命令，然后uBR10K才能接受证书。

在本例中，为了可读性，省略了一些证书内容，以elipsis(...)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注册期间添加过期的Manu证书

Manu Cert通常通过从CM发送到uBR10K的BPI协议AuthInfo消息进入uBR10K数据库。在AuthInfo消息中收到的每个唯一有效的Manu证书都会添加到数据库。如果CMTS（不在数据库中）未知Manu Cert且其有效日期已过期，则AuthInfo被拒绝，Manu Cert不会添加到uBR10K数据库。当在uBR10K电缆接口配置下存在**cable privacy retain-failed-certificates解决方法配置时，AuthInfo可以向uBR10K添加无效Manu Cert。**这允许将过期的Manu证书添加到未受限制的uBR10K数据库。要使用过期的Manu证书，必须使用SNMP将其标记为受信任。

```
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
```

当过期的Manu证书被添加到uBR10K并标记为信任时，建议删除**cable privacy retain-failed-certificates配置，以防止在uBR10K上添加其他未知过期的Manu证书。**

使用uBR10K CLI命令允许AuthInfo添加过期的CM证书和Manu证书

在某些情况下，CM证书会过期。在这种情况下，除了电缆隐**私保留失败证书配置**外，uBR10K上还需要另一个配置。在每个相关的uBR10K MAC域（电缆接口）下，添加**电缆隐私跳过有效期配**置并保存配置。这会导致uBR10K忽略在CM BPI AuthInfo消息中发送的所有CM和Manu证书的过期有效期检查。

```
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
```

其他信息

MAC域/电缆接口配置注意事项

cable privacy retain-failed-certificates和cable privacy skip-validity-period配置命令在MAC域/电缆接口级别使用，且不受限制。retain-failed-certificates命令可以将任何失败的证书添加到uBR10K数据库，skip-validity-period命令可跳过所有Manu和CM证书上的有效日期检查。

SNMP数据包大小注意事项

当使用大型证书时，可能需要额外的uBR10K SNMP配置。如果证书的二进制八位数字符串大于SNMP数据包大小，则证书的SNMP获取数据可以为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
```

Manu证书调试

uBR10K上的Manu Cert调试支持**debug cable privacy ca-cert**和**debug cable mac-address <cm mac-address>命**令。 其他调试信息在支持文章“How to Decode DOCSIS Certificate for Modem Stuck State Diagnosis(如何解码调制解调器停滞状态诊断的DOCSIS证书)”中进行了说明。

相关支持文档

- cBR-8产品公告中的电缆调制解调器和即将过期的制造商证书 — 思科
- 思科uBR10000系列通用宽带路由器
- 技术支持和文档 - Cisco Systems