在uBR10K上解决和恢复过期的制造商证书

目录

简介

问题

- Manu证书信息
  - Manu证书信息字段和属性
  - uBR10K CLI命令
  - DOCSIS-BPI-PLUS-MIB OID

解决方案

- 更新CM固件
- 将已知Manu证书设置为Trusted
  - 从uBR10K CLI查看许多证书信息
  - 从远程设备使用SNMP查看手动证书信息
  - 使用SNMP将过期的Known Manu Cert Trust状态设置为Trusted
  - 确认使用uBR10K CLI或使用SNMP更改了手动证书
- 已知Manu证书到期后恢复CM服务
  - 识别过期的已知手动证书序列号
  - 识别已过期已知Manu证书的索引，并将Manu证书信任状态设置为“可信”
- 在uBR10K上安装未知过期的Manu证书并标记为受信任
  - 使用SNMP向uBR10K添加到期的未知手动证书
  - 在CLI的CM注册期间添加过期的Manu证书
- 允许通过uBR10K CLI命令通过AuthInfo添加过期的CM证书和手动证书
- Additional Information
  - MAC域/电缆接口配置注意事项
  - SNMP数据包大小注意事项
  - Manu证书调试
  - 相关支持文档

简介

本文档介绍防止、解决和恢复有线调制解调器(CM)拒绝(pk)服务对uBR10K有线调制解调器终端系统(CMTS)产生的制造商证书(Manu Cert)到期影响的选项。

问题

在uBR10K上，CM停滞在reject(pk)状态的原因有很多。原因之一是马努证书到期。Manu证书用于CM和CMTS之间的身份验证。在本文档中，Manu证书是DOCSIS 3.0安全规范CM-SP-SECv3.0所说的CableLabs Mfg CA证书或制造商CA证书。到期表示uBR10K系统日期/时间超过手动证书有效结束日期/时间。

在Manu证书到期后尝试向uBR10K注册的CM被CMTS标记为reject(pk)，并且不在服务中。在uBR10K中注册并在服务中的CM在Manu证书到期时可以保持服务状态，直到CM下次尝试注册为止，这可以在单个调制解调器脱机事件、uBR10K电缆线路卡重新启动、uBR10K重新加载或其他触发

调制解调器注册的事件之后发生。此时，CM身份验证失败，被uBR10K标记为reject(pk)，并且不在服务中。

[适用于Cisco CMTS路由器的DOCSIS 1.1提供有关uBR10K支持和配置DOCSIS基线隐私接](#)口(BPI+)的其他信息。

Manu证书信息

可通过uBR10K CLI命令或简单网络管理协议(SNMP)查看手动证书信息。 本文档中介绍的解决方案使用这些命令和信息。

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： 主题名称与X509证书中编码的内容完全相同
  - cn:公用名
  - ou:组织单位
  - o:组织
  - l:位置
  - s:StateOrProvinceName
  - c：国家/地区名称
- 颁发机构：证书颁发机构
- 串行：以十六进制八位组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
  - snmp
  - 配置文件
  - externalDatabase
  - other（其他）
  - authentInfo
  - compiledInfoCode
- 状态/行状态：证书状态
  - 主用
  - notInService
  - 未就绪
  - 创建并执行
  - createandwait
  - 销毁
- 证书：X509 DER编码的证书颁发机构证书
- 有效日期：定义相对于CMTS系统日期和时间的手动证书有效期的起始日期和终止日期
  - 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散列

uBR10K CLI命令

此命令的输出包括一些Manu证书信息。Manu证书索引只能通过SNMP获取

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

这些电缆接口配置命令用于解决和恢复问题

- 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1.3.6.1.2.1.10.127.6.1.2.5.2.1中定义，如SNMP对象导航器中所述。

注意：在uBR10k软件中，RFC 4131 docsBpi2MIB / DOCS-IETF-BPI2-MIB是使用错误的OID MIB分支/路径实现的。uBR10k平台已停止销售，且已超过软件支持终止日期，因此没有针对此软件缺陷的修复方法。不是预期的MIB路径/分支1.3.6.1.2.10.127.6, mib path/branch 1.3.6.1.2.1.9999必须用于uBR10k上与BPI2 MIB/OID的SNMP交互。
相关Cisco Bug ID CSCum28486

以下是uBR10k上Manu Cert信息的BPI2 MIB OID完整路径等效项，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(...)表示为便于阅读，已省略某些信息。

解决方案

CM固件更新是最好的长期解决方案。本文档中介绍了允许具有已过期Manu证书的CM注册并保持uBR10K在线状态的解决方法，但仅建议短期使用这些解决方法。如果CM固件更新不可行，那么CM更换策略从安全和运营角度而言是一个很好的长期解决方案。这里描述的解决方案可解决不同的条件或方案，可以单独使用，也可以相互结合使用；

- 更新CM固件
- 将已知Manu证书设置为Trusted
- 已知Manu证书到期后恢复CM服务
- 在uBR10k上安装未知过期的Manu证书并标记为受信任
- 允许通过uBR10K CLI命令通过AuthInfo添加过期的CM证书和手动证书

注意：如果删除BPI，则会禁用加密和身份验证，从而最大限度地降低其作为解决方案的可行性。

更新CM固件

在许多情况下，CM制造商会提供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择，当在Manu证书到期之前执行时，可防止相关服务影响。CM加载新固件并使用新的Manu证书和CM证书重新注册。新证书可以正确进行身份验证，并且CM可以成功注册到uBR10K。新的Manu Cert和CM Cert可以创建一个新的证书链，使其返回已安装在uBR10K中的已知根证书。

将已知Manu证书设置为Trusted

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，可以在到期前在uBR10k中主动标记已知、有效结束日期不久的手动证书。使用uBR10K CLI命令可以找到手动证书序列号、有效结束日期和状态。使用SNMP可以找到Manu证书序列号、信任状态和索引。

当前在役和在线调制解调器的已知手动证书通常由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证书存储在uBR10K内存中，其信息可通过uBR10K CLI命令和SNMP查看。

当Manu Cert标记为可信任时，会执行两项重要操作。首先，它允许uBR10K BPI软件忽略过期的有效日期。其次，在uBR10K NVRAM中将Manu证书存储为受信任证书。这保留了uBR10K重新加载的Manu Cert状态，并消除了在uBR10K重新加载时重复此过程的需要

CLI和SNMP命令示例演示了如何识别手动证书索引、序列号、信任状态；然后使用该信息将信任状态更改为可信。示例重点介绍具有索引5和序列号45529C2654797E1623C6E723180A9E9C的Manu证书。

从uBR10K CLI查看许多证书信息

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。

<#root>

```
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 Inte
Subject: cn=Arris Cable Modem Root Certificate Authority,ou=Suwanee\, Georgia,ou=DOCSIS,o=Arris Interac
State: Chained  <-- Cert Trust State is Chained


Source: Auth Info    <-- CertSource is Auth Info


RowStatus: Active
Serial: 45529C2654797E1623C6E723180A9E9C  <-- Serial Number


Thumbprint: DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
```

从远程设备使用SNMP查看手动证书信息

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证书序列号可以与用于设置信任状态的Manu证书索引关联。具体的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。

<#root>

```
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 <-- S


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)
```

使用SNMP将过期的Known Manu Cert Trust状态设置为Trusted

OID的值： docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5（uBR10k上的OID为

1.3.6.1.2.1.999.1.2.5.2.1.5)

1:可信
2:不可信
3:链式
4:根

此示例显示，对于索引为5且序列号为45529C2654797E1623C6E723180A9E9C的Manu证书，信任状态已从链变为可信。

<#root>

```
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
```

确认使用uBR10K CLI或使用SNMP更改了手动证书

- 信任值从链接更改为“信任”
- 源值更改为“SNMP”，表示证书上次由SNMP管理，而不是从BPI协议AuthInfo消息管理

<#root>

```
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 <-- S


...
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 Inte
Subject: cn=Arris Cable Modem Root Certificate Authority,ou=Suwanee\, Georgia,ou=DOCSIS,o=Arris Interac
State: Trusted
```

Source: SNMP

RowStatus: Active

Serial: 45529C2654797E1623C6E723180A9E9C

Thumbprint: DA39A3EE5E6B4B0D3255BFEF95601890AFD80709

已知Manu证书到期后恢复CM服务

以前已知的Manu证书是uBR10K数据库中已经存在的证书，通常是由以前的CM注册的AuthInfo消息导致的。如果Manu证书未标记为受信任且证书过期，则使用已过期的Manu证书的所有CM随后可以脱机并尝试注册，但uBR10K会将其标记为reject(pk)，并且它们不在服务中。本节介绍如何从此条件中恢复，以及如何允许具有过期的Manu证书的CM注册和保持服务。

识别过期的已知手动证书序列号

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。

<#root>

```
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
```

识别已过期已知Manu证书的索引，并将Manu证书信任状态设置为“可信”

使用上一节中介绍的相同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索引编号将Manu Cert trust状态设置为SNMP可信。

<#root>

```
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证书并标记为受信任

如果uBR10K不知道已到期的Manu证书，因此无法在到期之前对其进行管理（标记为受信任）且无法恢复，则必须将Manu证书添加到uBR10K并标记为受信任。当以前未知且未在uBR10K上注册的CM尝试向未知和过期的Manu证书注册时，会发生此情况。

Manu证书可以通过SNMP Set或通过电缆隐私retain-failed-certificates配置添加到uBR10K。

使用SNMP向uBR10K添加到期的未知手动证书

要添加制造商的证书，请向docsBpi2CmtsCACertTable表添加一个条目。为每个条目指定这些属性。

- docsBpi2CmtsCACertStatus 1.3.6.1.2.1.999.1.2.5.2.1.7（设置为4可创建行条目）
- docsBpi2CmtsCACert = 1.3.6.1.2.1.999.1.2.5.2.1.8（实际X.509证书的十六进制数据，作为X509证书值）

- docsBpi2CmtsCACertTrust 1.3.6.1.2.1.999.1.2.5.2.1.5（设置为1可将Manu Cert Trust状态设置为trusted）

大多数操作系统不接受指定证书的十六进制字符串输入所需的输入行。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命令和结果在示例中将一个ASCII DER编码的ASN.1 X.509证书添加到uBR10K数据库，其参数如下：

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

为添加的Manu证书使用唯一的索引编号。添加到期的Manu证书时，除非手动将其设置为trusted，否则状态为不可信。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，省略了部分证书内容以方便阅读，以省略(...)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.
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 3
...
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 e
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的CM注册期间添加过期的Manu证书

Manu证书通常通过从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且有效的手动证书都将添加到数据库。如果Manu证书对CMTS（不在数据库中）未知且有效期已过期，则AuthInfo会被拒绝，并且Manu证书不会添加到uBR10K数据库。当uBR10K电缆接口配置下存在cable privacy retain-failed-certificates配置时，AuthInfo可以向uBR10K添加无效的Manu证书。这允许将过期的手动证书作为untrusted添加到uBR10K数据库。要使用到期的Manu证书，必须使用SNMP将其标记为受信任。

<#root>

```
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
```

当过期的手动证书添加到uBR10K并标记为已信任时，建议删除cable privacy retain-failed-certificates配置，以防止在uBR10K上添加其他未知的过期的手动证书。

允许通过uBR10K CLI命令通过AuthInfo添加过期的CM证书和手动证书

在某些情况下，CM证书会过期。对于这种情况，除了cable privacy retain-failed-certificates配置之外，还需要在uBR10K上进行其他配置。在每个相关的uBR10K MAC域（电缆接口）下，添加cable privacy skip-validity-period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。

<#root>

```
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
```

Additional Information

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，并且不受限制。retain-failed-certificates命令可以将任何失败的证书添加到uBR10K数据库中，而skip-validity-period命令可以跳过所有Manu和CM证书的有效日期检查。

SNMP数据包大小注意事项

使用大型证书时，可能需要额外的uBR10K SNMP配置。如果证书OctetString大于SNMP数据包大小，则证书数据的SNMP获取可以为空。 例如;

<#root>

```
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

在uBR10K用户上使用debug cable privacy ca-cert和debug cable mac-address <cm mac-address>命令支持的Manu Cert debug。 有关其他调试信息，请参阅支持文章如何解码调制解调器停滞状态诊断的DOCSIS证书。

相关支持文档

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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。