解决方法，并恢复cBR-8上的过期制造商证书

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)服务中恢复因制造商证书(Manu Cert)过期而对cBR-8电缆调制解调器终端系统(CMTS)产生影响的选项。

问题

CM在cBR-8上陷入拒绝(pk)状态有不同的原因。其中一个原因是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cBR-8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cBR-8注册的CM被CMTS标记为reject(pk)，且未在服务中。已向cBR-8注册并在Manu Cert到期时服务的CM可以在CM下次尝试注册前保持服务，这可能发生在单个CM脱机事件、cBR-8 Cable Linecard重新启动、cBR-8重新加载或其他事件触发CM注册后。当时，CM身份验证失败，由cBR-8标记为reject(pk)，并且未在服务中。

本文档中的信息将扩展并重新格式化cBR-8产品公告中“电缆调制解调器和即将过期的制造商证书”中发布的内容。

> **注意：**思科漏洞ID CSCv21785;在某些版本的Cisco IOS XE中，此Bug会导致在cBR-8重新加载后，受信任Manu证书失败验证。在某些情况下，Manu Cert存在，但不再处于受信任状态。在这种情况下，Manu Cert信任状态可以按照本文档中所述的步骤更改为受信任。如果show cable privacy manufacturer-cert-list命令的输出中不存在Manu Cert，则可以手动或通过AuthInfo重新添加Manu Cert，步骤如本文档所述。

Manu认证信息

可以从远程设备通过cBR-8 CLI命令或简单网络管理协议(SNMP)命令查看Manu Cert信息。cBR-8 CLI还支持SNMP set、get和get-bulk命令。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cBR-8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createAndGo创建并等待销毁

- 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

cBR-8 CLI命令

使用这些cBR-8 CLI命令可以查看Manu Cert信息。

- 在cBR-8 CLI执行模式或线卡CLI执行模式：CBR8-1#**show cable privacy manufactor-cert-list**
- 在cBR-8线路卡CLI执行模式下：Slot-6-0#**show crypto pki certificates**

从cBR-8 CLI使用这些Cisco IOS® XE SNMP命令来获取和设置SNMP OID。

- snmp get
- snmp get-bulk
- snmp set

这些cBR-8电缆接口配置命令用于本文档“解决方案”部分所述的解决方法和恢复。

- cable privacy retain-failed-certificates
- cable privacy skip-validity-period

DOCSIS-BPI-PLUS-MIB OID

Manu Cert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。

相关SNMP OID

```
docsBpi2CmtsCACertSubject 1.3.6.1.2.1.10.127.6.1.2.5.2.1.2
docsBpi2CmtsCACertIssuer 1.3.6.1.2.1.10.127.6.1.2.5.2.1.3
docsBpi2CmtsCACertSerialNumber 1.3.6.1.2.1.10.127.6.1.2.5.2.1.4
docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5
docsBpi2CmtsCACertSource 1.3.6.1.2.1.10.127.6.1.2.5.2.1.6
docsBpi2CmtsCACertStatus 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7
docsBpi2CmtsCACert 1.3.6.1.2.1.10.127.6.1.2.5.2.1.8
```

在命令示例中，省略号(...)表示为了可读性，已省略一些信息。

解决方案

CM固件更新是最佳的长期解决方案。本文档中介绍的解决方法允许具有过期Manu Cert的CM注册并保持在cBR-8的在线状态，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cBR-8上安装未知过期的Manu证书并标记受信任
- 使用cBR-8 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cBR-8。新的Manu证书和CM证书可以创建新的证书链，返回到cBR-8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制造商停业而不可用时，不再支持CM型号等，在有效结束日期之前，在cBR-

8上已知的具有近期有效结束日期的Manu Certs可以在cBR-8中主动标记为受信任。cBR-8 CLI命令和SNMP用于识别Manu Cert信息（如序列号和信任状态），而SNMP用于将Manu Cert信任状态设置为cBR-8中的受信任状态，这允许关联的CM注册并保持服务。

当前服务中和在线CM的已知Manu证书通常由cBR-8通过DOCSIS基线隐私接口(BPI)协议从CM获取。从CM发送到cBR-8的AuthInfo消息包含Manu证书。每个唯一的Manu Cert都存储在cBR-8内存中，其信息可通过cBR-8 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cBR-8 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cBR-8 NVRAM。这可在cBR-8重新加载期间保留Manu Cert状态，并在cBR-8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、序列号和信任状态；然后使用该信息将信任状态更改为受信任状态。这些示例重点介绍带索引4和序列号437498F09A7DCBC1FA7AA101FE976E40的Manu证书。

从cBR-8 CLI查看Manu证书信息

在本示例中，使用cBR-8 CLI命令**show cable privacy manufacturer-cert-list**。

```
CBR8-1#show cable privacy manufacturer-cert-list

Cable Manufacturer Certificates:

Index: 4
Issuer: cn=DOCSIS Cable Modem Root Certificate Authority,ou=Cable Modems,o=Data Over Cable
Service Interface Specifications,c=US
Subject: cn=Motorola Corporation Cable Modem Root Certificate Authority,ou=ASG,ou=DOCSIS,l=San
Diego,st=California,o=Motorola Corporation,c=US
State: Chained
Source: Auth Info
RowStatus: Active
Serial:      437498F09A7DCBC1FA7AA101FE976E40
Thumbprint:  FA07609998FDCAFA8F80D87F1ACFC70E6C52C80F
Fingerprint: 0EABDBD19D8898CA9C720545913AB93B

Index: 5
Issuer: cn=CableLabs Root Certification Authority,ou=Root CA01,o=CableLabs,c=US
Subject: cn=CableLabs Device Certification Authority,ou=Device CA01,o=CableLabs,c=US
State: Chained
Source: Auth Info
RowStatus: Active
Serial:      701F760559283586AC9B0E2666562F0E
Thumbprint:  E85319D1E66A8B5B2BF7E5A7C1EF654E58C78D23
Fingerprint: 15C18A9D6584D40E88D50D2FF4936982
```

从cBR-8 CLI使用SNMP查看Manu证书信息

在本示例中，使用cBR-8 CLI命令snmp get-bulk。证书索引4和5是存储在CMTS内存中的Manu证书。索引1、2和3是根证书。根证书不是此处的问题，因为其到期日期要长得多。

```
docsBpi2CmtsCACertSubject
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.2
SNMP Response: reqid 1752673, errstat 0, erridx 0
docsBpi2CmtsCACertSubject.1 = Data Over Cable Service Interface Specifications
```

```
docsBpi2CmtsCACertSubject.2 = tComLabs - Euro-DOCSIS
docsBpi2CmtsCACertSubject.3 = CableLabs
docsBpi2CmtsCACertSubject.4 = Motorola
docsBpi2CmtsCACertSubject.5 = CableLabs

docsBpi2CmtsCACertIssuer
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.3
SNMP Response: reqid 1752746, errstat 0, erridx 0
docsBpi2CmtsCACertIssuer.1 = DOCSIS Cable Modem Root Certificate Authority
docsBpi2CmtsCACertIssuer.2 = Euro-DOCSIS Cable Modem Root CA
docsBpi2CmtsCACertIssuer.3 = CableLabs Root Certification Authority
docsBpi2CmtsCACertIssuer.4 = DOCSIS Cable Modem Root Certificate Authority
docsBpi2CmtsCACertIssuer.5 = CableLabs Root Certification Authority

CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.4
SNMP Response: reqid 2300780, errstat 0, erridx 0
docsBpi2CmtsCACertSerialNumber.1 =
58 53 64 87 28 A4 4D C0 33 5F 0C DB 33 84 9C 19
docsBpi2CmtsCACertSerialNumber.2 =
63 4B 59 63 79 0E 81 0F 3B 54 45 B3 71 4C F1 2C
docsBpi2CmtsCACertSerialNumber.3 =
62 97 48 CA C0 A6 0D CB D0 FF A8 91 40 D8 D7 61
docsBpi2CmtsCACertSerialNumber.4 =
43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E 40
docsBpi2CmtsCACertSerialNumber.5 =
70 1F 76 05 59 28 35 86 AC 9B 0E 26 66 56 2F 0E

docsBpi2CmtsCACertTrust
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.5
SNMP Response: reqid 1752778, errstat 0, erridx 0
docsBpi2CmtsCACertTrust.1 = 4
docsBpi2CmtsCACertTrust.2 = 4
docsBpi2CmtsCACertTrust.3 = 4
docsBpi2CmtsCACertTrust.4 = 3    (3 = chained)
docsBpi2CmtsCACertTrust.5 = 3

docsBpi2CmtsCACertSource
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.6
SNMP Response: reqid 1752791, errstat 0, erridx 0
docsBpi2CmtsCACertSource.1 = 4
docsBpi2CmtsCACertSource.2 = 4
docsBpi2CmtsCACertSource.3 = 4
docsBpi2CmtsCACertSource.4 = 5   (5 = authentInfo)
docsBpi2CmtsCACertSource.5 = 5

docsBpi2CmtsCACertStatus
CBR8-1#snmp get-bulk v2c 10.122.151.12 vrf Mgmt-intf Cisco123 non-repeaters 0 max-repetitions 5
oid 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7
SNMP Response: reqid 1752804, errstat 0, erridx 0
docsBpi2CmtsCACertStatus.1 = 1
docsBpi2CmtsCACertStatus.2 = 1
docsBpi2CmtsCACertStatus.3 = 1
docsBpi2CmtsCACertStatus.4 = 1   (1 = active)
docsBpi2CmtsCACertStatus.5 = 1
```

从远程设备使用SNMP查看Manu证书信息

本文档中的远程设备SNMP示例使用来自远程Ubuntu Linux服务器的SNMP命令。特定SNMP命令和格式取决于用于执行SNMP命令的设备和操作系统。

```
docsBpi2CmtsCACertSubject
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.2
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.1 = STRING: "Data Over Cable Service Interface
Specifications"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.2 = STRING: "tComLabs - Euro-DOCSIS"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.3 = STRING: "CableLabs"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.4 = STRING: "Motorola Corporation"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.5 = STRING: "CableLabs"

docsBpi2CmtsCACertIssuer
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.3
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.1 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.2 = STRING: "Euro-DOCSIS Cable Modem Root CA"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.3 = STRING: "CableLabs Root Certification Authority"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.4 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.5 = STRING: "CableLabs Root Certification Authority"

docsBpi2CmtsCACertSerialNumber
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.1 = Hex-STRING: 58 53 64 87 28 A4 4D C0 33 5F 0C DB 33 84 9C
19
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.2 = Hex-STRING: 63 4B 59 63 79 0E 81 0F 3B 54 45 B3 71 4C F1
2C
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.3 = Hex-STRING: 62 97 48 CA C0 A6 0D CB D0 FF A8 91 40 D8 D7
61
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.4 = Hex-STRING: 43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E
40
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.5 = Hex-STRING: 70 1F 76 05 59 28 35 86 AC 9B 0E 26 66 56 2F
0E

docsBpi2CmtsCACertTrust
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.1 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.2 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.3 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 = INTEGER: 3   (3 = chained)
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.5 = INTEGER: 3

docsBpi2CmtsCACertSource
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.6
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.1 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.2 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.3 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.4 = INTEGER: 5   (5 = authentInfo)
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.5 = INTEGER: 5

docsBpi2CmtsCACertStatus
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.1 = INTEGER: 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.2 = INTEGER: 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.3 = INTEGER: 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.4 = INTEGER: 1   (1 = active)
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.5 = INTEGER: 1
```

在CLI中确定Manu证书有效性结束日期

使用cBR-8线卡CLI命令show crypto pki certificates来标识Manu Cert有效性结束日期。此命令输出不包括Manu证书索引。证书序列号可用于将从此命令获取的Manu Cert信息与从SNMP获取的Manu Cert信息关联起来。

```
CBR8-1#request platform software console attach

request platform software console attach 6/0
#
# Connecting to the CLC console on 6/0.
# Enter Control-C to exit the console connection.
#
Slot-6-0>enable
Slot-6-0#show crypto pki certificates

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 701F760559283586AC9B0E2666562F0E   Certificate Usage:
Signature
 Issuer:
    cn=CableLabs Root Certification Authority
    ou=Root CA01
    o=CableLabs
    c=US
  Subject:
    cn=CableLabs Device Certification Authority
    ou=Device CA01
    o=CableLabs
    c=US
 Validity Date:
    start date: 00:00:00 GMT Oct 28 2014
    end   date: 23:59:59 GMT Oct 27 2049
 Associated Trustpoints: e85319d1e66a8b5b2bf7e5a7c1ef654e58c78d23

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 437498F09A7DCBC1FA7AA101FE976E40
 Certificate Usage: Signature
 Issuer:
   cn=DOCSIS Cable Modem Root Certificate Authority
   ou=Cable Modems
   o=Data Over Cable Service Interface Specifications
    c=US
  Subject:
   cn=Motorola Corporation Cable Modem Root Certificate Authority
   ou=ASG
   ou=DOCSIS
   l=San Diego
   st=California
   o=Motorola Corporation
   c=US
  Validity Date:
     start date: 00:00:00 GMT Jul 11 2001
     end   date: 23:59:59 GMT Jul 10 2021
 Associated Trustpoints: fa07609998fdcafa8f80d87f1acfc70e6c52c80f

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 629748CAC0A60DCBD0FFA89140D8D761
 Certificate Usage: Signature
 Issuer:
   cn=CableLabs Root Certification Authority
   ou=Root CA01
   o=CableLabs
   c=US
  Subject:
   cn=CableLabs Root Certification Authority
   ou=Root CA01
   o=CableLabs
```

```
   c=US
  Validity Date:
    start date: 00:00:00 GMT Oct 28 2014
    end   date: 23:59:59 GMT Oct 27 2064
  Associated Trustpoints: DOCSIS-D31-TRUSTPOINT

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 634B5963790E810F3B5445B3714CF12C
 Certificate Usage: Signature
 Issuer:
    cn=Euro-DOCSIS Cable Modem Root CA
    ou=Cable Modems
    o=tComLabs - Euro-DOCSIS
    c=BE   Subject:
    cn=Euro-DOCSIS Cable Modem Root CA
    ou=Cable Modems
    o=tComLabs - Euro-DOCSIS
    c=BE
  Validity Date:
   start date: 00:00:00 GMT Sep 21 2001
   end   date: 23:59:59 GMT Sep 20 2031
  Associated Trustpoints: DOCSIS-EU-TRUSTPOINT

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 5853648728A44DC0335F0CDB33849C19
  Certificate Usage: Signature
 Issuer:
    cn=DOCSIS Cable Modem Root Certificate Authority
    ou=Cable Modems
    o=Data Over Cable Service Interface Specifications
    c=US
  Subject:
     cn=DOCSIS Cable Modem Root Certificate Authority
     ou=Cable Modems
     o=Data Over Cable Service Interface Specifications
     c=US
   Validity Date:
     start date: 00:00:00 GMT Feb 1 2001
     end   date: 23:59:59 GMT Jan 31 2031
  Associated Trustpoints: DOCSIS-US-TRUSTPOINT
```

将Manu Cert Trust State设置为Trusted

示例显示，索引= 4且序列号= 437498f09a7dcbc1fa7aa101fe976e40的Manu证书的信任状态从链接更改为受信任

OID:docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5值：

1:可信
2:不可信
3:链式
4:根

本示例显示用于更改信任状态的cBR-8 CLI snmp-set命令

```
CBR8-1#snmp set v2c 192.168.1.1 vrf Mgmt-intf private oid 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4
integer 1
SNMP Response: reqid 2305483, errstat 0, erridx 0
```

```
docsBpi2CmtsCACertTrust.4 = 1 (1 = trusted)
```

此示例显示远程设备使用SNMP更改信任状态

```
jdoe@server1:~$ snmpset -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 i 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 = INTEGER: 1 (1 = trusted)
```

使用cBR-8 CLI或SNMP确认Manu证书更改

- 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

此示例显示用于确认更改的cBR-8 CLI命令

```
CBR8-1#show cable privacy manufacturer-cert-list
Cable Manufacturer Certificates:
...
Index: 4
Issuer: cn=DOCSIS Cable Modem Root Certificate Authority,ou=Cable Modems,o=Data Over Cable
Service Interface Specifications,c=US
Subject: cn=Motorola Corporation Cable Modem Root Certificate Authority,ou=ASG,ou=DOCSIS,l=San
Diego,st=California,o=Motorola Corporation,c=US
State: Trusted
Source: SNMP
RowStatus: Active
Serial:      437498F09A7DCBC1FA7AA101FE976E40
Thumbprint:  DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
Fingerprint: D41D8CD98F00B204E9800998ECF8427E
...
```

此示例显示远程设备使用SNMP确认更改

```
jdoe@server1:~$ snmpget -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 = INTEGER: 1 (1 = trusted)

jdoe@server1:~$ snmpget -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.6.4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.4 = INTEGER: 1 (1 = snmp)
```

在已知Manu证书过期后恢复CM服务

以前已知的Manu Cert是cBR-8数据库中已存在的证书，通常是来自先前CM注册的AuthInfo消息的结果。如果Manu Cert未标记为受信任和过期，则任何使用过期Manu Cert并离线的CM都无法重新注册并标记为reject(pk)。 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。

当CM无法联机并因过期的Manu Certs而被标记为reject(pk)时，系统将生成系统日志消息，其中包含CM MAC地址和过期的Manu Cert序列号。

从cBR-8日志消息中确定过期的Manu证书序列号

```
CLC 6/0: Jan 11 17:36:07.094: %CBR-3-MANUFACTURE_CA_CM_CERTIFICATE_FORMAT_ERROR:
<133>CMTS[DOCSIS]: CM MAC Addr <1234.5678.9ABC> on Interface Cable6/0/0 U1 : Manu Cert S/N
437498F09A7DCBC1FA7AA101FE976E40 has Expired
```

确定过期Manu证书的索引并将Manu证书信任状态设置为Trusted

本示例显示cBR-8 CLI SNMP命令，用于从日志消息中标识Manu Cert序列号的索引，然后该命令用于将Manu Cert信任状态设置为受信任。

```
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.4
SNMP Response: reqid 2351849, errstat 0, erridx 0
docsBpi2CmtsCACertSerialNumber.1 =
58 53 64 87 28 A4 4D C0 33 5F 0C DB 33 84 9C 19
docsBpi2CmtsCACertSerialNumber.2 =
63 4B 59 63 79 0E 81 0F 3B 54 45 B3 71 4C F1 2C
docsBpi2CmtsCACertSerialNumber.3 =
62 97 48 CA C0 A6 0D CB D0 FF A8 91 40 D8 D7 61
docsBpi2CmtsCACertSerialNumber.4 =
43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E 40
docsBpi2CmtsCACertSerialNumber.5 =
70 1F 76 05 59 28 35 86 AC 9B 0E 26 66 56 2F 0E

CBR8-1#snmp set v2c 192.168.1.1 vrf Mgmt-intf private oid 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4
integer 1
SNMP Response: reqid 2353143, errstat 0, erridx 0
docsBpi2CmtsCACertTrust.4 = 1 (1 = trusted)
```

此示例显示远程设备使用SNMP命令从日志消息中标识Manu Cert序列号的索引，然后该消息将Manu Cert信任状态设置为受信任。

```
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.4 | grep
"43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E 40"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.4 = Hex-STRING: 43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E
40

jdoe@server1:~$ snmpset -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 i 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 = INTEGER: 1 (1 = trusted)
```

在cBR-8上安装未知过期的Manu证书并标记受信任

当cBR-8不知道过期的Manu证书时，它在到期前无法管理（标记为受信任），并且无法恢复。当之前未知且未在cBR-8上注册的CM尝试向未知且过期的Manu证书注册时，会发生这种情况。必须通过SNMP从远程设备将Manu证书添加到cBR-8，或使用**cable privacy retain-failed-certificates cBR-8 cable interface配置以允许AuthInfo添加过期的Manu证书。**cBR-8 CLI SNMP命令不能用于添加证书，因为证书数据中的字符数超过了CLI接受的最大字符数。 如果添加了自签名证书，则必须在cBR-8电缆接口下配置**cable privacy accept-self-signed-certificate**命令，然后cBR-8才能接受证书。

使用SNMP将过期的Manu证书添加到cBR-8

使用这些docsBpi2CmtsCACertTable OID值将Manu Cert添加为新表条目。通过支持文章“如何解码调制解调器停滞状态诊断的DOCSIS证书”中介绍的“CA证书转储”步骤，可以获取由docsBpi2CmtsCACert OID定义的Manu证书的十六进制值。

```
docsBpi2CmtsCACertStatus 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7 (Set to 4 to create the row entry)
docsBpi2CmtsCACert 1.3.6.1.2.1.10.127.6.1.2.5.2.1.8 (The hexadecimal data, as an X509Certificate
value, for the actual X.509 certificate)
docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5 (Set to 1 to set the Manu Cert Trust
state to trusted)
```

为已添加的Manu证书使用唯一索引号。可以使用show cable privacy manufacturer-cert-list命令检查cBR-8上已存在的Manu Certs的索引。

```
CBR8-2#show cable privacy manufacturer-cert-list | i Index
Index: 4
Index: 5
Index: 6
Index: 7
```

本节中的示例为添加到cBR-8数据库的Manu Cert使用索引值11。

> **提示：**始终在实际证书数据之前设置CertStatus属性。否则，CMTS会假设证书已链接，并立即尝试与制造商和根证书进行验证。

某些操作系统无法接受输入指定证书的十六进制数据字符串所需的输入行。因此，可使用图形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。

此示例显示远程设备使用SNMP将Manu证书添加到cBR-8。大多数证书数据都为可读性而提交，以条目(...)表示。

```
jdoe@server1:~$ snmpset -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7.11 i 4
1.3.6.1.2.1.10.127.6.1.2.5.2.1.8.11 x "0x3082...38BD" 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.11 i 1
```

使用cBR-8 CLI命令允许AuthInfo添加过期的Manu证书

Manu证书通常通过从CM发送到cBR-8的BPI协议AuthInfo消息输入cBR-8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证书，且其有效日期已过期，则AuthInfo被拒绝，Manu证书不会添加到cBR-8数据库。当在cBR-8电缆接口配置下存在**电缆隐私保留失败证书解决方**法配置时，可通过AuthInfo交换将过期的Manu Cert添加到CMTS。这允许将过期的Manu证书作为不受信任的添加到cBR-8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。当过期的Manu证书添加到cBR-8并标记为受信任时，建议删除**cable privacy retain-failed-certificates配置**，以便Manu Certs不进入系统。

```
CBR8-1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
CBR8-1(config)#int Cable6/0/0
CBR8-1(config-if)#cable privacy retain-failed-certificates
CBR8-1(config-if)#end
```

使用cBR-8 CLI命令允许AuthInfo添加过期的CM证书和Manu证书

当在每个相关电缆接口下都配置了**cable privacy retain-failed-certificates**和**cable privacy skip-validity-period**命令时，AuthInfo交换可将过期的CM证书添加到CMTS。这会导致cBR-8忽略在CM BPI AuthInfo消息中发送的所有CM和Manu Certs的过期有效日期检查。当过期的CM和Manu Certs添加到cBR-8并标记为受信任时，建议删除所述配置，以便添加可能不需要的Certs不进入系统。

```
CBR8-1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
CBR8-1(config)#interface Cable6/0/0
CBR8-1(config-if)#cable privacy retain-failed-certificates
CBR8-1(config-if)#cable privacy skip-validity-period
CBR8-1(config-if)#end
```

```
CBR8-1#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 Domain / cable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cBR-8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

如果证书二进制八位数字串大于SNMP数据包大小，则证书数据的SNMP获取可以返回空值。当使用大型证书时，可以使用cBR-8 SNMP配置；

```
CBR8-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CBR8-1(config)#snmp-server packetsize 3000
CBR8-1(config)#end
CBR8-1#copy run start
```

Manu证书调试

cBR-8上的Manu Cert调试通过**debug cable privacy ca-cert**和**debug cable mac-address <CM mac-address>命令受**支持。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。这包括CA证书转储步骤，用于学习Manu证书的十六进制值。

相关支持文档

- 适用于Cisco CMTS路由器的DOCSIS 1.1提供了有关cBR-8支持和配置DOCSIS基线隐私接口(BPI+)的其他信息。
- Cisco CMTS电缆命令参考提供有关本文档中引用的cBR-8 CLI命令的信息。
- 在uBR10K上解决并恢复过期制造商证书提供与本文档类似的信息，用于uBR10K CMTS。
- 技术支持和文档 - Cisco Systems