Workaround and Recover Expired Manufacturer Certificates on cBR-8

Contents

Introduction
Problem
Manu Cert Information
Manu Cert Information Fields and Attributes
cBR-8 CLI Commands
DOCSIS-BPI-PLUS-MIB OIDs
Solution
Update CM Firmware
Set a Known Manu Cert to Trusted
View Manu Cert Information from the cBR-8 CLI
View Manu Cert Information with SNMP from the cBR-8 CLI
View Manu Cert Information with SNMP from a Remote Device
Identify the Manu Cert Validity End Date in the CLI
Set the Manu Cert Trust State to Trusted
Confirm Manu Cert Changes with the cBR-8 CLI or with SNMP
Recover CM Service After a Known Manu Cert Expires
Identify the Expired Manu Cert Serial Number from the cBR-8 Log Message
Identify the Index for the Expired Manu Cert and Set the Manu Cert Trust State to Trusted
Install an Unknown Expired Manu Cert on the cBR-8 and Mark Trusted
Add an Expired Manu Cert to the cBR-8 with SNMP
Permit an Expired Manu Cert to be Added by AuthInfo with a cBR-8 CLI Command
Permit Expired CM Certs and Manu Certs to be Added by AuthInfo with a cBR-8 CLI Command
Additional Information
MAC Domain/Cable Interface Configuration Consideration
SNMP Packet Size Consideration
Manu Cert Debug
Related Support Documentation

Introduction

This document describes options to prevent, workaround, and recover from cable modem (CM) reject(pk) service impacts on the cBR-8 Cable Modem Termination System (CMTS) that result from Manufacturer Certificate (Manu Cert) expiration.

Problem

There are different causes for a CM to become stuck in the reject(pk) state on the cBR-8. One cause is expiration of the Manu Cert. The Manu Cert is used for authentication between a CM and CMTS. In this document, a Manu Cert is what the DOCSIS 3.0 Security Specification CM-SP-

SECv3.0 refers to as CableLabs Mfg CA certificate or Manufacturer CA certificate. Expire means the cBR-8 system date/time exceeds the Manu Cert validity end date/time.

A CM that attempts to register with the cBR-8 after the Manu Cert expires is marked reject(pk) by the CMTS and is not in service. A CM already registered with the cBR-8 and in service when the Manu Cert expires can remain in service until the next time the CM attempts to register, which can occur after a single CM offline event, cBR-8 Cable Linecard restart, cBR-8 reload, or other event triggers CM registration. At that time the CM fails authentication, is marked reject(pk) by the cBR-8, and is not in service.

The information in this document expands upon and reformats content published in the Cable Modems and Expiring Manufacturer Certificates in cBR-8 Product Bulletin.

> **Note**: Cisco bug ID CSCvv21785; In some versions of Cisco IOS XE, this bug causes a trusted Manu Cert to fail validation after a cBR-8 reload. In some cases the Manu Cert is present but no longer in the trusted state. In that case, the Manu Cert trust state can be changed to trusted with steps described in this document. If the Manu Cert is not present in the output of the show cable privacy manufacturer-cert-list command, the Manu Cert can be re-added manually or by AuthInfo with steps described in this document.

Manu Cert Information

Manu Cert information can be viewed via cBR-8 CLI commands or Simple Network Management Protocol (SNMP) commands from a remote device. The cBR-8 CLI also supports SNMP set, get and get-bulk commands. These commands and information are used by solutions described in this document.

Manu Cert Information Fields and Attributes

- Index: A unique integer assigned to each Manu Cert in the cBR-8 database/MIB
- Subject: The subject name exactly as it is encoded in the X509 certificate
  cn: CommonNameou: OrganizationalUnito: Organizationl: Localitys: StateOrProvinceNamec: CountryName
- Issuer: The certificate authority
- Serial: Cert Serial Number represented in a hexadecimal octet string
- State: The Trust status of the certificate
  trusteduntrustedchainedroot
- Source: How the certificate reached the CMTS
  snmpconfigurationFileexternalDatabaseotherauthentInfocompiledInfoCode
- Status/RowStatus: Cert Status
  activenotInServicenotReadycreateAndGocreateand Waitdestroy

- Cert: The X509 DER-encoded certificate authority certificate
- Validity Date: The start and end dates that define the Manu Cert validity period relative to the CMTS system date and time
  start date: The date and time at which the Manu Cert becomes validend date: The date and time at which the Manu Cert is no longer valid
- Cert: The X509 DER-encoded certificate authority certificate
- Thumbprint: The SHA-1 hash of a CA certificate

cBR-8 CLI Commands

Manu Cert information can be viewed with these cBR-8 CLI commands.

- From cBR-8 CLI exec mode or Linecard CLI exec mode: CBR8-1#**show cable privacy manufacturer-cert-list**
- From cBR-8 Linecard CLI exec mode: Slot-6-0#**show crypto pki certificates**

These Cisco IOS® XE SNMP commands are used from the cBR-8 CLI to get and set SNMP OIDs.

- snmp get
- snmp get-bulk
- snmp set

These cBR-8 cable interface configuration commands are used for workarounds and recovery described in the Solution section of this document.

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

DOCSIS-BPI-PLUS-MIB OIDs

Manu Cert information is defined in the docsBpi2CmtsCACertEntry OID branch 1.3.6.1.2.1.10.127.6.1.2.5.2.1, described in the SNMP Object Navigator.

Relevant SNMP OIDs

```
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
```

In command examples, ellipsis (...) indicate some information has been omitted for readability.

Solution

CM firmware update is the best long-term solution. Workarounds described in this document permit CMs with expired Manu Certs to register and remain online with the cBR-8, but these workarounds are only recommended for short-term use. If a CM firmware update is not an option, a CM replacement strategy is a good long-term solution from a security and operations perspective. The solutions described here address different conditions or scenarios and can be used individually or, some, in combination with each other;

- Update CM Firmware
- Set a Known Manu Cert to Trusted
- Recover CM Service After a Known Manu Cert Expires
- Install an Unknown Expired Manu Cert on the cBR-8 and Mark Trusted
- Permit Expired CM Certs and Manu Certs to be Added by AuthInfo with a cBR-8 CLI

Command

Note: If BPI is removed, this disables encryption and authentication, which minimizes the viability of that as a workaround.

Update CM Firmware

In many instances, CM manufacturers provide CM firmware updates that extend the validity end date of the Manu Cert. This solution is the best option and, when performed before a Manu Cert expires, prevents related service impacts. CMs load the new firmware and re-register with new Manu Certs and CM Certs. The new certificates can authenticate properly and the CMs can successfully register with the cBR-8. The new Manu Cert and CM Cert can create a new certificate chain back to the known Root Certificate already installed in the cBR-8.

Set a Known Manu Cert to Trusted

When a CM firmware update is unavailable due to a CM Manufacturer gone out of business, no further support for a CM model, and so on, Manu Certs already known on the cBR-8 with validity end dates in the near future can be proactively marked trusted in the cBR-8 prior to the validity end date. The cBR-8 CLI commands and SNMP are used to identify Manu Cert information such as serial number and trust state, and SNMP is used to set the Manu Cert trust state to trusted in the cBR-8, which allows associated CMs to register and remain in service.

Known Manu Certs for currently in-service and online CMs are typically learned by the cBR-8 from a CM through the DOCSIS Baseline Privacy Interface (BPI) protocol. The AuthInfo message sent from the CM to the cBR-8 contains the Manu Cert. Each unique Manu Cert is stored in cBR-8 memory and its information can be viewed by cBR-8 CLI commands and SNMP.

When the Manu Cert is marked as trusted, that does two important things. First, it allows the cBR-8 BPI software to ignore the expired validity date. Second, it stores the Manu Cert as trusted in the cBR-8 NVRAM. This preserves the Manu Cert state across a cBR-8 reload and eliminates the need to repeat this procedure in the event of a cBR-8 reload.

The CLI and SNMP command examples demonstrate how to identify a Manu Cert index, serial number, and trust state; then use that information to change the trust state to trusted. The examples focus on the Manu Cert with Index 4 and Serial Number 437498F09A7DCBC1FA7AA101FE976E40.

View Manu Cert Information from the cBR-8 CLI

In this example the cBR-8 CLI command **show cable privacy manufacturer-cert-list** is used.

```
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
```

View Manu Cert Information with SNMP from the cBR-8 CLI

In this example the cBR-8 CLI command snmp get-bulk is used. Cert Indices 4 & 5 are the Manu Certs stored in the CMTS memory. Indices 1, 2, and 3 are Root Certificates. Root Certificates are not the concern here as their expiration dates are much longer.

```
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
```

View Manu Cert Information with SNMP from a Remote Device

The remote device SNMP examples in this document use SNMP commands from a remote Ubuntu Linux server. Specific SNMP commands and formats depend on the device and operating system used to execute the SNMP commands.

```
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
```

Identify the Manu Cert Validity End Date in the CLI

Use the cBR-8 linecard CLI command **show crypto pki certificates** to identify the Manu Cert validity end date. This command output does not include the Manu Cert Index. The Certificate Serial Number can be used to correlate Manu Cert information learned from this command with the Manu Cert information learned from SNMP.

```
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
```

Set the Manu Cert Trust State to Trusted

The examples show the trust state changed from chained to trusted for the Manu Cert with Index = 4 and Serial Number = 437498f09a7dcbc1fa7aa101fe976e40

OID: docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5 values:

1 : trusted
2 : untrusted
3 : chained
4 : root

This example shows the cBR-8 CLI snmp-set command used to change the trust state

```
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)
```

This example shows a remote device use SNMP to change the trust state

```
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)
```

Confirm Manu Cert Changes with the cBR-8 CLI or with SNMP

- The trust value changed from chained to trusted
- The source value changed to SNMP, which indicates the certificate was last managed by SNMP and not from the BPI Protocol AuthInfo Message

This example shows the cBR-8 CLI command used to confirm the changes

```
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
...
```

This example shows a remote device use SNMP to confirm the changes

```
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)
```

Recover CM Service After a Known Manu Cert Expires

A previously known Manu Cert is a certificate already present in the cBR-8 database, typically as a result of AuthInfo messages from previous CM registration. If a Manu Cert is not marked trusted and expires, any CM that uses the expired Manu Cert and goes offline cannot re-register and is marked as reject(pk). This section describes how to recover from this condition and allow CMs with expired Manu Certs to register and remain in service.

When CMs fail to come online and are marked reject(pk) as a result of expired Manu Certs, a syslog message is generated and contains the CM MAC Address and the expired Manu Cert Serial Number.

Identify the Expired Manu Cert Serial Number from the cBR-8 Log Message

```
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
```

Identify the Index for the Expired Manu Cert and Set the Manu Cert Trust State to Trusted

This example shows the cBR-8 CLI SNMP commands used to identify the index for the Manu Cert serial number from the log message, which is then used to set the Manu Cert trust state to trusted.

```
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)
```

This examples shows a remote device use SNMP commands to identify the index for the Manu Cert serial number from the log message, which is then used to set the Manu Cert trust state to trusted.

```
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)
```

Install an Unknown Expired Manu Cert on the cBR-8 and Mark Trusted

When an expired Manu Cert is not known to the cBR-8 it cannot be managed (marked trusted) prior to expiration and cannot be recovered. This happens when a CM that is previously unknown and not registered on a cBR-8 attempts to register with an unknown and expired Manu Cert. The Manu Cert must be added to the cBR-8 by SNMP from a remote device or use the **cable privacy retain-failed-certificates** cBR-8 cable interface configuration to permit an expired Manu Cert to be added by AuthInfo. The cBR-8 CLI SNMP commands cannot be used to add a certificate because the numer of characters in the certificate data exceeds the maximum characters accepted by the CLI. If a self-signed certificate is added, the **cable privacy accept-self-signed-certificate** command must be configured under the cBR-8 cable interface before the cBR-8 can accept the certificate.

Add an Expired Manu Cert to the cBR-8 with SNMP

Use these docsBpi2CmtsCACertTable OID values to add the Manu Cert as a new table entry. The hexadecimal value of the Manu Cert defined by the docsBpi2CmtsCACert OID can be learned with CA Certificate Dump steps described in the support article How to Decode DOCSIS Certificate for Modem Stuck State Diagnosis.

```
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)
```

Use a unique index number for the added Manu Cert. The indices of Manu Certs already present on the cBR-8 can be checked with the **show cable privacy manufacturer-cert-list** command.

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

The examples in this section use an index value of 11 for the Manu Cert added to the cBR-8 database.

> **Tip**: Always set the CertStatus attributes before the actual certificate data. Otherwise, the CMTS assumes the certificate is chained and immediately attempts to verify it with the manufacturers and root certificates.

Some operating systems cannot accept input lines that are as long as needed to input the hexadecimal data string that specifies a certificate. For this reason, a graphical SNMP manager can be used to set these attributes. For a number of certificates, a script file can be used, if more convenient.

This example shows a remote device use SNMP to add a Manu Cert certificate to the cBR-8. Most of the certificate data is ommitted for readability, indicated by elipses (...).

```
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
```

Permit an Expired Manu Cert to be Added by AuthInfo with a cBR-8 CLI Command

A Manu Cert typically enters the cBR-8 database by the BPI Protocol AuthInfo message sent to the cBR-8 from the CM. Each unique and valid Manu Cert received in an AuthInfo message is added to the database. If the Manu Cert is unknown to the CMTS (not in the database) and has expired validity dates, AuthInfo is rejected and the Manu Cert is not added to the cBR-8 database. An expired Manu Cert can be added to the CMTS by the AuthInfo exchange when the **cable privacy retain-failed-certificates** workaround configuration is present under the cBR-8 cable interface configuration. This allows the addition of the expired Manu Cert to the cBR-8 database as untrusted. In order to use the expired Manu Cert, SNMP must be used to mark it trusted. When the expired Manu Cert is added to the cBR-8 and marked trusted, removal of the **cable privacy retain-failed-certificates** configuration is recommended so additional, potentially unwanted, Manu Certs do not enter the system.

```
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
```

Permit Expired CM Certs and Manu Certs to be Added by AuthInfo with a cBR-8 CLI Command

An expired CM certificate can be added to the CMTS by the AuthInfo exchange when both the **cable privacy retain-failed-certificates** and **cable privacy skip-validity-period** commands are configured under each relevant cable interface. This causes the cBR-8 to ignore expired validity date checks for ALL CM and Manu Certs sent in the CM BPI AuthInfo message. When the expired CM and Manu Certs are added to the cBR-8 and marked trusted, removal of the described configuration is recommended so additional, potentially unwanted, Certs do not enter the system.

```
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
```

Additional Information

MAC Domain/Cable Interface Configuration Consideration

The **cable privacy retain-failed-certificates** and **cable privacy skip-validity-period** configuration commands are used at the MAC Domain / cable interface level and are not restrictive. The retain-failed-certificates command can add any failed certificate to the cBR-8 database and skip-validity-period command can skip validity date checks on all Manu and CM certs.

SNMP Packet Size Consideration

An SNMP get for Cert data can return a NULL value if the Cert OctetString is larger than the SNMP packet size. A cBR-8 SNMP configuration can be used when large-sized certificates are used;

```
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 Cert Debug

Manu Cert debug on the cBR-8 is supported with the **debug cable privacy ca-cert** and **debug cable mac-address <CM mac-address>** commands. Additional debug information is explained in the support article How to Decode DOCSIS Certificate for Modem Stuck State Diagnosis. This includes CA Certificate Dump steps used to learn the hexadecimal value of a Manu Cert.

Related Support Documentation

- DOCSIS 1.1 for the Cisco CMTS Routers provides additional information about cBR-8 support and configuration of DOCSIS Baseline Privacy Interface (BPI+).
- Cisco CMTS Cable Command Reference provides information about cBR-8 CLI commands referenced in this document.
- Work Around and Recover Expired Manufacturer Certificates on uBR10K provides similar information as this document for the uBR10K CMTS.
- Technical Support & Documentation - Cisco Systems