Problemumgehung und Wiederherstellung abgelaufener Herstellerzertifikate auf cBR-8

Inhalt

Einleitung

In diesem Dokument werden Optionen zum Vermeiden, Umkehren und Wiederherstellen von Problemen mit dem Ablehnen (pk) des Kabelmodems (CM) auf cBR-8 Cable Modem Termination System (CMTS) beschrieben, das sich aus dem Ablauf des Manufacturer Certificate (Manu Cert) ergibt.

Problem

Es gibt verschiedene Ursachen dafür, dass ein CM im Ablehnungszustand(pk) des cBR-8 feststeckt. Eine Ursache ist der Ablauf der Manu-Zertifizierung. Das Manu-Zertifikat wird für die Authentifizierung zwischen einem CM und CMTS verwendet. In diesem Dokument wird ein Manu-Zertifikat als das DOCSIS 3.0 Security Specification CM-SP-SECv3.0-Zertifikat bezeichnet, das als CableLabs Mfg CA-Zertifikat oder Manufacturer CA-Zertifikat bezeichnet wird. Ablaufdatum: Das Datum/die Uhrzeit des cBR-8-Systems überschreitet das Enddatum/die Endzeit der Gültigkeit des Manu-Zertifikats.

Ein CM, der versucht, sich nach Ablauf der Manu-Zertifizierung beim cBR-8 zu registrieren, wird vom CMTS als Ablehnen(pk) markiert und ist nicht in Betrieb. Ein bereits bei cBR-8 registrierter und bei Ablauf des Manu Cert in Betrieb befindlicher CM kann so lange in Betrieb bleiben, bis der CM das nächste Mal versucht, sich zu registrieren. Dies kann nach einem einzigen CM Offline-Ereignis, einem Neustart der cBR-8-Kabel-Linecard, einem erneuten Laden des cBR-8 oder anderen Ereignissen auftreten, die die CM-Registrierung auslösen. Zu diesem Zeitpunkt schlägt der CM die Authentifizierung fehl, wird durch den cBR-8 als Ablehnen(pk) markiert und ist nicht in Betrieb.

Die Informationen in diesem Dokument erweitern und formatieren Inhalte, die in den Zertifikaten der Kabelmodems und ablaufenden Hersteller in cBR-8-Produktbulletin veröffentlicht wurden.

> **Anmerkung:** Cisco Bug-ID CSCvv21785; In einigen Versionen von Cisco IOS XE führt dieser Fehler dazu, dass die Validierung eines vertrauenswürdigen Manu Cert nach einem erneuten Laden von cBR-8 fehlschlägt. In einigen Fällen ist die Manu-Zertifizierung vorhanden, aber nicht mehr im vertrauenswürdigen Zustand. In diesem Fall kann der Vertrauensstatus von Manu Cert mit den in diesem Dokument beschriebenen Schritten zu Trusted geändert werden. Wenn das Manu-Zertifikat nicht in der Ausgabe des Befehls show cable privacy-cert-list vorhanden ist, kann das Manu-Zertifikat manuell oder von AuthInfo mit den in diesem Dokument beschriebenen Schritten erneut hinzugefügt werden.

Informationen zu Manu-Zertifizierungen

Die Manu-Zertifikate können über cBR-8-CLI-Befehle oder SNMP-Befehle (Simple Network Management Protocol) von einem Remote-Gerät aus angezeigt werden. Die cBR-8-CLI unterstützt außerdem SNMP-Befehle zum Festlegen, Abrufen und Abrufen von Massenprotokollen. Diese Befehle und Informationen werden von in diesem Dokument beschriebenen Lösungen verwendet.

Manu-Zertifikate-Informationsfelder und -Attribute

- Index: Eine eindeutige Ganzzahl, die jedem Manu-Zertifikat in der Datenbank cBR-8/MIB zugewiesen wird
- Betreff: Der Betreffname ist genau wie im X509-Zertifikat verschlüsselt cn: CommonNameSie: Organisationseinheito: Organisationl: Lokalitäts: StateOrProvinceNamec) Ländername
- Emittent: Zertifizierungsstelle
- Seriell: Die in einer Hexadezimalquettszeichenfolge dargestellte Cert-Seriennummer
- Bundesland: Der Vertrauensstatus des Zertifikats

vertrauenswürdignicht vertrauenswürdigverkettetWurzel
- Quelle: Wie das Zertifikat den CMTS erreicht hat snmpKonfigurationsdateiexterne DatenbankandereauthentInfocompiledInfoCode
- Status/RowStatus: Zertifizierungsstatus aktivNichtInServicenicht bereitcreateAndGoErstellen und Wartenzerstören

- Zertifikat: Das Zertifikatszertifikat der X509 DER-codierten Zertifizierungsstelle
- Gültigkeitsdatum: Das Start- und Enddatum, das die Gültigkeitsdauer der Manu-Zertifizierung relativ zum Datum und der Uhrzeit des CMTS-Systems definiert. Startdatum: Datum und Uhrzeit der Gültigkeit der Manu-ZertifizierungEnddatum: Datum und Uhrzeit, zu der das Manu-Zertifikat nicht mehr gültig ist
- Zertifikat: Das Zertifikatszertifikat der X509 DER-codierten Zertifizierungsstelle
- Daumenabdruck: Der SHA-1-Hash eines Zertifizierungsstellenzertifikats

cBR-8 CLI-Befehle

Manu-Zertifizierungen können mit diesen cBR-8-CLI-Befehlen angezeigt werden.

- Aus dem cBR-8 CLI Exec-Modus oder dem Linecard CLI Exec-Modus: CBR8-1**#show cable privacy hersteller-cert-list**
- Aus dem cBR-8 Linecard-CLI-Exec-Modus: Steckplatz-6-0**#Krypto-Pki-Zertifikate anzeigen**

Diese Cisco IOS® XE SNMP-Befehle werden von der CLI cBR-8 verwendet, um SNMP-OIDs abzurufen und festzulegen.

- SNMP bekommen
- SNMP Get-Bulk
- Schnappschuss

Diese Konfigurationsbefehle für die cBR-8-Kabelschnittstellen werden für die Problemumgehung und Wiederherstellung verwendet, die im Abschnitt "Lösung" dieses Dokuments beschrieben werden.

- Aufbewahrung fehlgeschlagener Zertifikate für den Kabelschutz
- Gültigkeitsdauer des Kabels

DOCSIS-BPI-PLUS-MIB-OIDs

Manu-Zertifizierungen werden in der docsBpi2CmtsCACertEntry-OID-Verzweigung 1.3.6.1.2.1.10.127.6.1.2.5.2.1 definiert, die im SNMP Object Navigator beschrieben wird.

Relevante 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 Befehlsbeispielen weisen Auslassungszeichen (..) darauf hin, dass einige Informationen zur Lesbarkeit weggelassen wurden.

Lösung

Das CM-Firmware-Update ist die beste langfristige Lösung. Die in diesem Dokument beschriebenen Problemumgehungen ermöglichen es CMs mit abgelaufenen Manu-Zertifikaten, sich zu registrieren und beim cBR-8 online zu bleiben. Diese Problemumgehungen werden jedoch nur zur kurzfristigen Verwendung empfohlen. Wenn eine Aktualisierung der CM-Firmware nicht möglich ist, ist eine CM-Ersatzstrategie aus Sicherheits- und Betriebsperspektive eine gute langfristige Lösung. Die hier beschriebenen Lösungen sind auf unterschiedliche Bedingungen oder Szenarien ausgelegt und können einzeln oder in Kombination miteinander verwendet werden.

- CM Firmware aktualisieren
- Legen Sie ein bekanntes Manu-Zertifikat auf Trusted fest.
- CM-Dienst nach Ablauf eines bekannten Manu-Zertifikats wiederherstellen
- Installieren Sie ein unbekanntes abgelaufenes Manu-Zertifikat auf cBR-8, und markieren Sie Trusted.
- Zulassen, dass abgelaufene CM-Zertifikate und Manu-Zertifikate von AuthInfo mit einem cBR-8-CLI-Befehl hinzugefügt werden

  Anmerkung: Wenn BPI entfernt wird, werden Verschlüsselung und Authentifizierung deaktiviert, wodurch die Lebensfähigkeit dieser Daten als Problemumgehung minimiert wird.

CM Firmware aktualisieren

In vielen Fällen stellen CM-Hersteller CM-Firmware-Updates zur Verfügung, die das Gültigkeitsenddatum des Manu Cert verlängern. Diese Lösung ist die beste Option und verhindert bei Ausführung vor Ablauf einer Manu-Zertifizierung zugehörige Serviceauswirkungen. CMs laden die neue Firmware und registrieren sich erneut bei neuen Manu Certs und CM Certs. Die neuen Zertifikate können sich ordnungsgemäß authentifizieren, und die CMs können sich erfolgreich bei cBR-8 registrieren. Mit dem neuen Manu Cert und CM Cert kann eine neue Zertifikatskette bis zum bekannten, bereits in cBR-8 installierten Root Certificate erstellt werden.

Legen Sie ein bekanntes Manu-Zertifikat auf Trusted fest.

Wenn ein CM-Firmware-Update nicht verfügbar ist, weil ein CM-Hersteller außer Betrieb ist, keine weitere Unterstützung für ein CM-Modell usw., können Manu-Zertifizierungen, die bereits auf dem cBR-8 mit Ablaufdaten für die Gültigkeit in naher Zukunft bekannt sind, in cBR-8 vor dem Gültigkeitsenddatum proaktiv als vertrauenswürdig gekennzeichnet werden. Die cBR-8-CLI-Befehle und SNMP werden zur Identifizierung von Manu Cert-Informationen wie Seriennummer und Vertrauensstatus verwendet. SNMP wird verwendet, um den Manu Cert-Vertrauensstatus auf "Trusted" in cBR-8 festzulegen, wodurch die angeschlossenen CMs registriert und im Betrieb bleiben können.

Bekannte Manu-Zertifikate für aktuell in Betrieb befindliche und Online-CMs werden in der Regel von cBR-8 von einem CM über das DOCSIS Baseline Privacy Interface (BPI)-Protokoll erfasst. Die vom CM an den cBR-8 gesendete AuthInfo-Nachricht enthält die Manu-Zertifizierung. Jedes eindeutige Manu Cert wird im cBR-8-Speicher gespeichert, und seine Informationen können über

cBR-8-CLI-Befehle und SNMP angezeigt werden.

Wenn die Manu Cert als vertrauenswürdig markiert ist, tut dies zwei wichtige Dinge. Erstens kann die cBR-8 BPI-Software das abgelaufene Gültigkeitsdatum ignorieren. Zweitens speichert es die Manu-Zertifizierung im cBR-8 NVRAM als vertrauenswürdig. Dadurch wird der Manu-Zertifikat-Status während eines cBR-8-Neuladens erhalten, und es ist nicht erforderlich, diesen Vorgang im Falle eines cBR-8-Neuladens zu wiederholen.

Die Befehlsbeispiele für CLI und SNMP veranschaulichen, wie ein Manu Cert-Index, eine Seriennummer und ein Vertrauenszustand identifiziert werden. und anschließend diese Informationen verwenden, um den Vertrauenszustand in vertrauenswürdig zu ändern. Die Beispiele konzentrieren sich auf das Manu-Zertifikat mit Index 4 und der Seriennummer 437498F09A7DCBC1FA7AA101FE976E40.

Manu-Zertifikatinformationen über die cBR-8-CLI anzeigen

In diesem Beispiel wird der Befehl cBR-8 CLI **show cable privacy hersteller-cert-list** verwendet.

```
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
```

Manu-Zertifikatinformationen mit SNMP über die cBR-8-CLI anzeigen

In diesem Beispiel wird der Befehl cBR-8 CLI snmp get-Bulk verwendet. Die Cert-Indizes 4 und 5 sind die im CMTS-Speicher gespeicherten Manu-Zertifikate. Die Indizes 1, 2 und 3 sind Wurzelzertifikate. Die Wurzelzertifikate sind hier nicht das Problem, da ihr Ablaufdatum viel länger ist.

```
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
```

Manu-Zertifikatinformationen mit SNMP von einem Remote-Gerät anzeigen

Die SNMP-Beispiele für Remote-Geräte in diesem Dokument verwenden SNMP-Befehle von einem Remote-Ubuntu Linux-Server. Bestimmte SNMP-Befehle und -Formate hängen vom Gerät

und vom Betriebssystem ab, das zum Ausführen der SNMP-Befehle verwendet wird.

```
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
```

Identifizieren des Enddatums der Gültigkeit von Manu Cert in der CLI

Verwenden Sie den Befehl cBR-8-Linecard-CLI, um **Crypto Pki-Zertifikate anzuzeigen**, um das Ablaufdatum für die Gültigkeit von Manu Cert anzugeben. Diese Befehlsausgabe enthält nicht den Manu Cert Index. Die Certificate Serial Number kann verwendet werden, um die Manu Cert-

Informationen, die von diesem Befehl abgerufen wurden, mit den von SNMP erfassten Manu Cert-Informationen zu korrelieren.

```
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
```

Stellen Sie den Manu Zertifikat-Vertrauensstaat auf Trusted ein.

Die Beispiele zeigen, dass der Vertrauensstatus für die Manu-Zertifizierung mit Index = 4 und Seriennummer = 437498f09a7dcbc1fa7aa101fe976e40 geändert wurde.

OID: docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5-Werte:

1: vertrauenswürdig
2: nicht vertrauenswürdig
3: verkettet
4: Wurzel

Dieses Beispiel zeigt den Befehl cBR-8 CLI snmp-set, der zum Ändern des Vertrauensstatus

verwendet wird.

```
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)
```

Dieses Beispiel zeigt ein Remote-Gerät, das SNMP zum Ändern des Vertrauensstatus verwendet.

```
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)
```

Manu-Zertifikataänderungen mit der cBR-8-CLI oder mit SNMP bestätigen

- Der Vertrauenswert wechselte von verketteten zu vertrauenswürdigen Werten.
- Der Quellwert wurde in SNMP geändert. Dies bedeutet, dass das Zertifikat zuletzt von SNMP und nicht von der AuthInfo-Nachricht des BPI-Protokolls verwaltet wurde.

Dieses Beispiel zeigt den CLI-Befehl cBR-8, mit dem die Änderungen bestätigt werden.

```
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
...
```

Dieses Beispiel zeigt ein Remote-Gerät, das SNMP verwendet, um die Änderungen zu bestätigen.

```
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)
```

CM-Dienst nach Ablauf eines bekannten Manu-Zertifikats wiederherstellen

Ein zuvor bekanntes Manu Cert ist ein Zertifikat, das bereits in der Datenbank cBR-8 vorhanden ist. Dies ist in der Regel das Ergebnis von AuthInfo-Meldungen aus der vorherigen CM-Registrierung. Wenn ein Manu-Zertifikat nicht als vertrauenswürdig eingestuft ist und abläuft, kann sich jeder CM, der das abgelaufene Manu-Zertifikat verwendet und offline geht, nicht erneut registrieren und wird als reject(pk) markiert. In diesem Abschnitt wird beschrieben, wie CMs mit abgelaufenen Manu-Zertifikaten nach dieser Bedingung wieder registriert und in Betrieb bleiben können.

Wenn CMs nicht online gestellt werden und als Ergebnis abgelaufener Manu-Zertifikate als

reject(pk) (ablehnen) markiert sind, wird eine Syslog-Meldung generiert, die die CM-MAC-Adresse und die abgelaufene Manu-Zertifizierungs-Seriennummer enthält.

Identifizieren Sie die abgelaufene Manu-Zertifikat-Seriennummer aus der cBR-8-Protokollmeldung.

```
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
```

Identifizieren Sie den Index für die abgelaufene Manu-Zertifizierung, und legen Sie den Manu Cert Trust State auf Trusted fest.

Dieses Beispiel zeigt die cBR-8 CLI-SNMP-Befehle, die verwendet werden, um den Index für die Seriennummer von Manu Cert aus der Protokollmeldung zu identifizieren. Diese Befehle werden verwendet, um den Vertrauensstatus von Manu Cert auf vertrauenswürdig festzulegen.

```
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)
```

Dieses Beispiel zeigt, dass ein Remote-Gerät SNMP-Befehle verwendet, um den Index für die Seriennummer von Manu Cert aus der Protokollmeldung zu identifizieren, die dann verwendet wird, um den Vertrauensstatus von Manu Cert auf vertrauenswürdig festzulegen.

```
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)
```

Installieren Sie ein unbekanntes abgelaufenes Manu-Zertifikat auf cBR-8, und markieren Sie Trusted.

Wenn dem cBR-8 kein abgelaufenes Manu-Zertifikat bekannt ist, kann es vor dem Ablauf nicht verwaltet (als vertrauenswürdig eingestuft) werden und kann nicht wiederhergestellt werden. Dies

geschieht, wenn ein CM, der bisher unbekannt ist und nicht auf einem cBR-8 registriert ist, versucht, sich bei einem unbekannten und abgelaufenen Manu Cert zu registrieren. Das Manu-Zertifikat muss von einem Remote-Gerät zum cBR-8 über SNMP hinzugefügt werden oder die **cBR-8**-Kabelschnittstellenkonfiguration zum **Beibehalten von** ausgefallenen Manu-Zertifikaten verwenden, um das Hinzufügen eines abgelaufenen Manu-Zertifikats durch AuthInfo zu ermöglichen. Mit den cBR-8 CLI-SNMP-Befehlen kann kein Zertifikat hinzugefügt werden, da die Anzahl der Zeichen in den Zertifikatsdaten die von der CLI akzeptierten Höchstzeichen überschreitet. Wenn ein selbstsigniertes Zertifikat hinzugefügt wird, muss der Befehl **privacy accept-self-signed-certificate** unter der Schnittstelle cBR-8 konfiguriert werden, bevor der cBR-8 das Zertifikat akzeptieren kann.

Fügen Sie dem cBR-8 ein abgelaufenes Manu-Zertifikat mit SNMP hinzu.

Verwenden Sie diese docsBpi2CmtsCACertTable-OID-Werte, um die Manu-Zertifizierung als neuen Tabelleneintrag hinzuzufügen. Der Hexadezimalwert der Manu-Zertifizierung, die durch die docsBpi2CmtsCACert-OID definiert wird, kann mit den Zertifizierungsstellen-Zertifikatsdumpunkten erlernt werden, die im Support-Artikel How to Decode DOCSIS Certificate for Modem Stuck State Diagnosis beschrieben werden.

```
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)
```

Verwenden Sie eine eindeutige Indexnummer für das hinzugefügte Manu-Zertifikat. Die Indizes von Manu Certs, die bereits im cBR-8 vorhanden sind, können mit dem Befehl **show cable privacy-cert-list** überprüft werden.

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

In den Beispielen in diesem Abschnitt wird für die der Datenbank cBR-8 hinzugefügte Manu Cert ein Indexwert von 11 verwendet.

> **Tipp:** Legen Sie immer das CertStatus-Attribut vor den eigentlichen Zertifikatsdaten fest. Andernfalls geht der CMTS davon aus, dass das Zertifikat verkettet ist, und versucht sofort, es mit den Herstellern und Stammzertifikaten zu überprüfen.

Einige Betriebssysteme können keine Eingabelinien akzeptieren, die so lange benötigt werden, um die Hexadezimaldatenzeichenfolge einzugeben, die ein Zertifikat angibt. Aus diesem Grund kann ein grafischer SNMP-Manager verwendet werden, um diese Attribute festzulegen. Für eine Reihe von Zertifikaten kann eine Skriptdatei verwendet werden, wenn dies praktischer ist.

Dieses Beispiel zeigt ein Remote-Gerät, das SNMP verwendet, um dem cBR-8 ein Manu-Zertifikat hinzuzufügen. Die meisten Zertifikatsdaten werden für die Lesbarkeit angegeben, die durch Buchstaben (...) angegeben ist.

```
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
```

Zulassen, dass ein abgelaufenes Manu-Zertifikat von AuthInfo mit einem cBR-8-CLI-Befehl hinzugefügt wird

Ein Manu Cert wird in der Regel durch die vom CM an den cBR-8 gesendete BPI Protocol AuthInfo-Nachricht in die Datenbank cBR-8 eingegeben. Jedes eindeutige und gültige Manu Cert, das in einer AuthInfo-Nachricht empfangen wird, wird der Datenbank hinzugefügt. Wenn das Manu-Zertifikat dem CMTS nicht bekannt ist (nicht in der Datenbank) und abgelaufene Gültigkeitsdaten hat, wird AuthInfo abgelehnt, und die Manu-Zertifizierung wird der Datenbank cBR-8 nicht hinzugefügt. Ein abgelaufenes Manu-Zertifikat kann dem CMTS durch den AuthInfo-Austausch hinzugefügt werden, wenn die Workaround-Konfiguration für die **Kabeldatenschutzkonfiguration** unter der cBR-8-Kabelschnittstellenkonfiguration **fehlgeschlagene Zertifikate beibehalten** wird. Dies ermöglicht das Hinzufügen des abgelaufenen Manu Cert zur cBR-8-Datenbank als nicht vertrauenswürdig. Um das abgelaufene Manu-Zertifikat zu verwenden, muss SNMP verwendet werden, um es als vertrauenswürdig zu kennzeichnen. Wenn der abgelaufene Manu Cert dem cBR-8 hinzugefügt und als vertrauenswürdig markiert wird, wird empfohlen, die Konfiguration für den **Schutz** des **Kabelvertrauens zu** entfernen**, wenn Zertifikate nicht gespeichert wurden. Aus diesem Grund** wird empfohlen, zusätzliche, möglicherweise unerwünschte Manu Certs nicht in das System aufzunehmen.

```
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
```

Zulassen, dass abgelaufene CM-Zertifikate und Manu-Zertifikate von AuthInfo mit einem cBR-8-CLI-Befehl hinzugefügt werden

Ein abgelaufenes CM-Zertifikat kann dem CMTS durch den AuthInfo-Austausch hinzugefügt werden, wenn sowohl die Befehle **zum** Zurückbehalten **von ausgefallenen Zertifikaten** als auch zum Überspringen der Gültigkeitsdauer von **Kabeln** unter jeder relevanten Kabelschnittstelle konfiguriert sind. Dadurch ignoriert der cBR-8 die Überprüfung des abgelaufenen Gültigkeitsdatums für ALLE CM- und Manu-Zertifikate, die in der CM BPI-AuthInfo-Nachricht gesendet werden. Wenn die abgelaufenen CM- und Manu-Zertifikate dem cBR-8 hinzugefügt und als vertrauenswürdig markiert werden, wird empfohlen, die beschriebene Konfiguration zu entfernen. Aus diesem Grund werden zusätzliche, möglicherweise unerwünschte Certs nicht in das System eingegeben.

```
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
```

Zusätzliche Informationen

Überlegungen zur Konfiguration der MAC-Domäne/-Kabelschnittstelle

Der **Kabelschutz behält fehlgeschlagene Zertifikate** und **die** Konfigurationsbefehle für die **Gültigkeitsdauer** des **Kabels** zum **Überspringen der Kabellängigkeit** werden auf der Ebene der

MAC-Domäne/Kabelschnittstelle verwendet und sind nicht einschränkend. Mit dem Befehl besiegelte Zertifikate können der Datenbank cBR-8 ausgefallene Zertifikate hinzugefügt werden. Der Befehl zum Überspringen der Gültigkeitsdauer kann die Validitätsdatumsüberprüfungen für alle Manu- und CM-Zertifikate überspringen.

Überlegungen zur SNMP-Paketgröße

Ein SNMP Get für Zertifikatsdaten kann einen NULL-Wert zurückgeben, wenn der Cert OctetString größer als die SNMP-Paketgröße ist. Eine cBR-8-SNMP-Konfiguration kann verwendet werden, wenn Zertifikate mit großer Größe verwendet werden.

```
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
```

Debug mit Manu Cert

Manu Cert Debug auf dem cBR-8 wird mit den **Befehlen debug cable privacy ca-cert** und **debug cable mac-address <CM mac-address>** unterstützt. Weitere Debuginformationen finden Sie im Support-Artikel How to Decode DOCSIS Certificate for Modem Stuck State Diagnosis. Dazu gehören die CA Certificate Dump-Schritte zum Erlernen des Hexadezimalwerts eines Manu Cert.

Dokumentation des zugehörigen Supports

- DOCSIS 1.1 für die Cisco CMTS-Router enthält zusätzliche Informationen zur cBR-8-Unterstützung und -Konfiguration der DOCSIS Baseline Privacy Interface (BPI+).
- Die Cisco CMTS Cable Command Reference enthält Informationen zu den in diesem Dokument erwähnten Befehlen der cBR-8-CLI.
- Die "Work Around"- und "Recover Expired Manufacturer"-Zertifikate auf dem uBR10K enthalten ähnliche Informationen wie dieses Dokument für das uBR10K CMTS.
- Technischer Support und Dokumentation für Cisco Systeme