Problemumgehung und Wiederherstellung abgelaufener Herstellerzertifikate auf uBR10K

Inhalt

Einleitung

In diesem Dokument werden Optionen beschrieben, mit denen verhindert werden kann, eine Umgehung durchzuführen ist und die Wiederherstellung nach einer Ablehnung des Kabelmodems (CM) durch einen Service beeinträchtigt wird, der sich auf das uBR10K Cable Modem Termination System (CMTS) auswirkt, das sich aus dem Ablauf des Manufacturer Certificate (Manu Cert) ergibt.

Problem

Es gibt verschiedene Ursachen dafür, dass ein CM im Ablehnungszustand(pk) auf dem uBR10K 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 uBR10K-Systems überschreitet das Enddatum/die Endzeit der Gültigkeit des Manu-Zertifikats.

Ein CM, der versucht, sich nach Ablauf der Manu-Zertifizierung beim uBR10K anzumelden, wird vom CMTS als "Ablehnen(pk)" markiert und ist nicht in Betrieb. Ein bereits beim uBR10K 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 Offline-Ereignis eines Modems, einem Neustart der uBR10K-Kabel, einem Neustart des uBR10K oder anderen Ereignissen auftreten, die eine Modemregistrierung auslösen. Zu diesem Zeitpunkt schlägt der CM Authentifizierung fehl, wird durch den uBR10K als Ablehnen(pk) markiert und ist nicht in Betrieb.

DOCSIS 1.1 für die Cisco CMTS-Router enthält zusätzliche Informationen zur Unterstützung und Konfiguration der DOCSIS Baseline Privacy Interface (BPI+) durch uBR10K.

Informationen zu Manu-Zertifizierungen

Manu-Zertifikate können über uBR10K CLI-Befehle oder Simple Network Management Protocol (SNMP) angezeigt werden. 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 uBR10K-Datenbank/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 bereitcreateAndGoCreateWaitzerstören
- 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

uBR10K CLI-Befehle

Die Ausgabe dieses Befehls enthält einige Manu Cert-Informationen. Der Manu Cert-Index kann nur über SNMP abgerufen werden.

- Aus dem Modus uBR10K CLI Exec oder dem CLI Exec-Modus von Linecard: uBR10K**#show cable privacy hersteller-cert-list**
- Aus dem UBR10K Linecard-CLI-Exec-Modus: Steckplatz-6-0**#Krypto-Pki-Zertifikate anzeigen**

Diese Befehle zur Konfiguration der Kabelschnittstellen werden für Workarounds und Recovery verwendet.

- uBR10K(config-if)**#Kabelschutz - fehlgeschlagene Zertifikate**
- uBR10K(config-if)**#SKU-Gültigkeitsdauer**

DOCSIS-BPI-PLUS-MIB-OIDs

SNMP-Informationen für das Manu-Zertifikat werden im DOCSIS-BPI-PLUS-MIB-docsBpi2CmtsCACertEntry OID Branch 1.3.6.1.2.1.10.127.6.1.2.5.2.1 definiert, der im SNMP-Objektnavigator beschrieben wird. In der Software uBR10k wurde jedoch die RFC 4131 docsBpi2MIB / DOCS-IETF-BPI2-MIB mit der falschen OID-MIB-Verzweigung/-Pfad implementiert. Die uBR10k-Plattform läuft aus und läuft nach dem Software-Support-Datum aus, daher gibt es keine Lösung für diesen Softwarefehler.

Zugehörige Cisco Bug-ID CSCum28486

Problemumgehung: Anstelle des richtigen MIB-Pfads/der richtigen Verzweigung 1.3.6.1.2.10.127.6 **muss der MIB-Pfad/Zweig 1.3.6.1.2.1.999 für SNMP-Interaktionen mit den BPI2 MIB/OIDs auf der uBR10k verwendet werden.** Die BPI2 MIB OID-Vollpfad-Äquivalente auf dem uBR10k, die für diesen Fehler und die Problemumgehung relevant sind, sind:

```
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
```

In den Befehlsbeispielen SNMP und uBR10k CLI weisen Auslassungszeichen (..) darauf hin, dass einige Informationen für die Lesbarkeit entfallen.

Lösung

Das CM-Firmware-Update ist die beste langfristige Lösung. Workarounds, die es CMs mit abgelaufenen Manu-Zertifikaten erlauben, sich zu registrieren und beim uBR10K online zu bleiben, werden in diesem Dokument beschrieben. Diese Workarounds werden jedoch nur für die kurzfristige 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 dem uBR10k, und markieren Sie Trusted
- Konfigurieren Sie uBR10K so, dass das Enddatum für die Gültigkeit der Manu-Zertifizierung ignoriert und das abgelaufene Manu-Zertifikat beibehalten wird.

  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 uBR10K registrieren. Mit dem neuen Manu Cert und CM Cert kann eine neue Zertifikatskette bis zum bekannten, bereits im uBR10K 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, kein weiterer Support für ein CM-Modell usw., können Manu-Zertifikate, die bereits auf dem uBR10k mit Ablaufdaten für die Gültigkeit in naher Zukunft bekannt sind, im uBR10k proaktiv als TRUSTED markiert werden, bevor es abläuft. Die Manu Cert-Seriennummer, das Gültigkeitsenddatum und der Status sind mit den Befehlen uBR10K CLI zu finden. Die Seriennummer, der Trust State und der Index von Manu Cert sind im SNMP zu finden.

Bekannte Manu-Zertifikate für aktuell in Betrieb befindliche und Online-Modems werden in der Regel vom uBR10K von einem CM über das DOCSIS Baseline Privacy Interface (BPI)-Protokoll erfasst. Die AUTH-INFO-Nachricht, die vom CM an den uBR10K gesendet wird, enthält das Manu-Zertifikat. Jedes einzelne Manu Cert wird im uBR10K-Speicher gespeichert und die zugehörigen Informationen können mit uBR10K CLI-Befehlen und SNMP angezeigt werden.

Wenn das Manu-Zertifikat als TRUSTED markiert ist, tut dies zwei wichtige Dinge. Erstens kann die Software uBR10K BPI das abgelaufene Gültigkeitsdatum ignorieren. Zweitens speichert es die Manu-Zertifizierung als TRUSTED im uBR10K NVRAM. Dadurch wird der Manu-Zertifikat-Status während eines uBR10K-Neuladens erhalten, und es ist nicht erforderlich, diesen Vorgang zu wiederholen, wenn uBR10K neu geladen wird.

Die Befehlsbeispiele CLI und SNMP veranschaulichen die Identifizierung eines Manu Cert-Index, einer Seriennummer und eines Vertrauensstatus. diese Informationen dann verwenden, um den Vertrauenszustand in Trusted (Vertrauenswürdig) zu ändern. Die Beispiele konzentrieren sich auf ein Manu-Zertifikat mit Index 5 und der Seriennummer 45529C2654797E1623C6E723180A9E9C.

Anzeigen der Many Cert-Informationen in der CLI

Verwenden Sie die Befehle uBR10K CLI, um **Crypto Pki-Zertifikate anzuzeigen** und die **Hersteller-cert-Liste** zum Anzeigen der bekannten Manu Cert-Informationen zum **Schutz** des **Kabelvertrauens** anzuzeigen.

```
UBR10K-01#telnet 127.0.0.81
Trying 127.0.0.81 ... Open

clc_8_1>en
clc_8_1#show crypto pki certificates
CA Certificate
 Status: Available
  Certificate Serial Number: 45529C2654797E1623C6E723180A9E9C
 Certificate Usage: Not Set
 Issuer:
   cn=DOCSIS Cable Modem Root Certificate Authority
   ou=Cable Modems
   o=Data Over Cable Service Interface Specifications
   c=US
 Subject:
   cn=Arris Cable Modem Root Certificate Authority
   ou=Suwanee\
    Georgia
   ou=DOCSIS
   o=Arris Interactive\
    L.L.C.
   c=US
 Validity Date:
   start date: 20:00:00 EDT Sep 11 2001
    end   date: 19:59:59 EDT Sep 11 2021
 Associated Trustpoints: 0edbf2a98b45436b6e4b464797c08a32f2a2cd66
clc_8_1#exit

[Connection to 127.0.0.81 closed by foreign host]

uBR10K-01#show cable privacy manufacturer-cert-list
Cable Manufacturer Certificates:

Issuer: cn=DOCSIS Cable Modem Root Certificate Authority,ou=Cable Modems,o=Data Over Cable
Service Interface Specifications,c=US
Subject: cn=Arris Cable Modem Root Certificate Authority,ou=Suwanee\, Georgia,ou=DOCSIS,o=Arris
Interactive\, L.L.C.,c=US
State: Chained  <-- Cert Trust State is Chained
Source: Auth Info    <-- CertSource is Auth Info
RowStatus: Active
Serial: 45529C2654797E1623C6E723180A9E9C  <-- Serial Number
Thumbprint: DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
```

Anzeigen der Manu-Zertifikatinformationen mit SNMP

In diesem Beispiel wird der Befehl snmpwalk verwendet, um Informationen in der Manu-Zertifizierungstabelle uBR10k anzuzeigen. Die bekannte Seriennummer von Manu Cert kann mit dem Manu Cert Index korreliert werden, der zum Festlegen des Vertrauensstatus verwendet werden kann. Bestimmte SNMP-Befehle und -Formate hängen vom Gerät und vom Betriebssystem ab, das zum Ausführen des SNMP-Befehls bzw. der SNMP-Anforderung verwendet wird.

Relevante uBR10K SNMP-OIDs:

```
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

Workstation-1$snmpwalk -v 2c -c snmpstring1 192.168.1.1 1.3.6.1.2.1.9999.1.2.5.2.1
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.2.1 = STRING: "Data Over Cable Service Interface
Specifications"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.2.2 = STRING: "tComLabs - Euro-DOCSIS"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.2.3 = STRING: "Scientific-Atlanta\\"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.2.4 = STRING: "CableLabs\\"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.2.5 = STRING: "Arris Interactive\\"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.3.1 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.3.2 = STRING: "Euro-DOCSIS Cable Modem Root CA"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.3.3 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.3.4 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.3.5 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.4.1 = Hex-STRING: 58 53 64 87 28 A4 4D C0 33 5F 0C DB 33 84 9C
19
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.4.2 = Hex-STRING: 63 4B 59 63 79 0E 81 0F 3B 54 45 B3 71 4C F1
2C
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.4.3 = Hex-STRING: 57 BF 2D F6 0E 9F FB EC F8 E6 97 09 DE 34 BC
26
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.4.4 = Hex-STRING: 26 B0 F6 BD 1D 85 E8 E8 E8 C1 BD DF 17 51 ED
8C
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.4.5 = Hex-STRING: 45 52 9C 26 54 79 7E 16 23 C6 E7 23 18 0A 9E
9C <-- Serial Number
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.1 = INTEGER: 4
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.2 = INTEGER: 4
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.3 = INTEGER: 3
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.4 = INTEGER: 3
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.5 = INTEGER: 3 <-- Trust State (3 = Chained)
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.6.1 = INTEGER: 4
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.6.2 = INTEGER: 4
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.6.3 = INTEGER: 5
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.6.4 = INTEGER: 5
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.6.5 = INTEGER: 5 <-- Source authentInfo (5)
```

Legen Sie den Status des abgelaufenen als Manu Cert Trust bekannten Manu Cert auf Trusted mit SNMP fest.

Das Beispiel zeigt, dass der Vertrauensstatus für das Manu-Zertifikat mit Index = 5 und der Seriennummer = 45529C2654797E1623C6E723180A9E9C von verkettet in vertrauenswürdig geändert wurde.

Werte für OID: docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5 (Die OID für uBR10k lautet 1.3.6.1.2.1.999.1.2.5.2.1.5)

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

```
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
```

Bestätigen Sie das Manu-Zertifikat, das mit der uBR10K-CLI oder mit SNMP geändert wurde.

- Der Vertrauenswert änderte sich von verkettet zu "vertrauenswürdig"
- 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.

```
Workstation-1$ snmpwalk -v 2c -c snmpstring1 192.168.1.1 1.3.6.1.2.1.9999.1.2.5.2.1
...
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.2.5 = STRING: "Arris Interactive\\"
...
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.3.5 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
...
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.4.5 = Hex-STRING: 45 52 9C 26 54 79 7E 16 23 C6 E7 23 18 0A 9E
9C <-- Serial Number
...
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.5.5 = INTEGER: 1 <-- Trust State (3 = trusted)
...
SNMPv2-SMI::mib-2.9999.1.2.5.2.1.6.5 = INTEGER: 1 <-- Source (1 = SNMP)
```

```
uBR10K-01#show cable privacy manufacturer-cert-list
Cable Manufacturer Certificates:

Issuer: cn=DOCSIS Cable Modem Root Certificate Authority,ou=Cable Modems,o=Data Over Cable
Service Interface Specifications,c=US
Subject: cn=Arris Cable Modem Root Certificate Authority,ou=Suwanee\, Georgia,ou=DOCSIS,o=Arris
Interactive\, L.L.C.,c=US
State: Trusted
Source: SNMP
RowStatus: Active
Serial: 45529C2654797E1623C6E723180A9E9C
Thumbprint: DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
```

CM-Dienst nach Ablauf eines bekannten Manu-Zertifikats wiederherstellen

Ein zuvor bekanntes Manu Cert ist ein Zertifikat, das bereits in der uBR10K-Datenbank vorhanden ist, in der Regel als Ergebnis von AuthInfo-Meldungen aus der vorherigen CM-Registrierung. Wenn ein Manu-Zertifikat nicht als TRUSTED markiert ist und das Zertifikat abläuft, können alle CMs, die das abgelaufene Manu-Zertifikat verwenden, anschließend offline gehen und versuchen, sich zu registrieren, aber der uBR10K markiert sie ablehnen(pk) und sind nicht in Betrieb. In diesem Abschnitt wird beschrieben, wie CMs mit abgelaufenen Manu-Zertifikaten nach dieser Bedingung wieder registriert und in Betrieb bleiben können.

Identifizieren Sie die abgelaufene bekannte Manu-Zertifikat-Seriennummer.

Die Manu Cert-Informationen für einen CM, der in reject (pk) fixiert ist, können mit dem Befehl uBR10K CLI **show cable modem <CM MAC Address> privacy** überprüft werden.

```
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
```

Identifizieren Sie den Index für das abgelaufene bekannte Manu-Zertifikat, und legen Sie den Manu Cert Trust State auf Trusted fest.

Verwenden Sie die gleichen Befehle für die Befehlszeilenschnittstelle uBR10K und das SNMP, wie im vorherigen Abschnitt beschrieben, um den Index für das Manu-Zertifikat anhand der Seriennummer von Manu Cert zu identifizieren. Verwenden Sie die abgelaufene Manu Cert-Indexnummer, um den Manu Cert-Vertrauenszustand auf "vertrauenswürdig" mit SNMP einzustellen.

```
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)
```

Installieren Sie ein unbekanntes abgelaufenes Manu-Zertifikat und markieren Sie Trusted.

Wenn ein abgelaufenes Manu-Zertifikat für den uBR10K nicht bekannt ist, daher kann es vor dem Ablauf nicht verwaltet (als TRUSTED gekennzeichnet) werden und kann nicht wiederhergestellt werden, muss das Manu-Zertifikat zum uBR10K hinzugefügt und als TRUSTED gekennzeichnet werden. Diese Bedingung tritt ein, wenn ein CM, der bisher unbekannt ist und nicht auf einem uBR10K registriert ist, versucht, sich bei einem unbekannten und abgelaufenen Manu Cert zu registrieren.

Das Manu-Zertifikat kann dem uBR10K über SNMP Set oder durch die Konfiguration zum Beibehalten von fehlgeschlagenen Zertifikaten zum Kabelschutz hinzugefügt werden.

SNMP Set verwenden, um ein abgelaufenes unbekanntes Manu-Zertifikat zum uBR10K hinzuzufügen

Um ein Herstellerzertifikat hinzuzufügen, fügen Sie der docsBpi2CmtsCACertTable-Tabelle einen Eintrag hinzu. Geben Sie diese Attribute für jeden Eintrag an:

- docsBpi2CmtsCACertStatus 1.3.6.1.2.1.999.1.2.5.2.1.7 (Festlegen auf 4, um den

Zeileneintrag zu erstellen)
- docsBpi2CmtsCACert = 1.3.6.1.2.1.999.1.2.5.2.1.8 (Die hexadezimalen Daten als X509-Zertifikatswert für das tatsächliche X.509-Zertifikat)
- docsBpi2CmtsCACertTrust 1.3.6.1.2.1.999.1.2.5.2.1.5 (Legen Sie "1" fest, um den Manu Cert Trust-Status als vertrauenswürdig festzulegen)

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

Der SNMP-Befehl und die Ergebnisse im Beispiel fügen der uBR10K-Datenbank ein ASCII DER Encoded ASN.1 X.509-Zertifikat mit folgenden Parametern hinzu:

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

Verwenden Sie eine eindeutige Indexnummer für das hinzugefügte Manu-Zertifikat. Wenn ein abgelaufenes Manu-Zertifikat hinzugefügt wird, ist der Zustand UNTRUSTED, es sei denn, er wird manuell auf TRUSTED festgelegt. Wenn ein selbstsigniertes Zertifikat hinzugefügt wird, muss der **Befehl zum Datenschutz des selbstsignierten Zertifikats unter der** Konfiguration der uBR10K-Kabelschnittstelle konfiguriert werden, bevor das Zertifikat vom uBR10K akzeptiert werden kann.

Im Beispiel wird aus Gründen der Lesbarkeit ein Teil des Zertifikatinhalts weggelassen, der durch elipsis (...) angegeben wird.

```
jdoe@server1[983]-->./setany -v2c 192.168.1.1 private 1.3.6.1.2.1.9999.1.2.5.2.1.7.11 -i 4
1.3.6.1.2.1.9999.1.2.5.2.1.8.11 - o "30 82 04 00 30 82 02 e8 a0 03 02 01
02 02 10 43 74 98 f0 9a 7d cb c1 fa 7a a1 01 fe 97 6e 40 30 0d 06 09 2a 86 48 86 f7 0d 01 01 05
05 00 30 81 97 31 0b 30 09 06 03 55 04 06 13 02 55 53
...
d8 26 21 f1 41 eb c4 87 90 65 2d 23 38 08 31 9c 74 16 30 05 18 d2 89 5e 9b 21 13 e3 e9 6a f9 3b
59 5e e2 05 0e 89 e5 9d 2a 40 c2 9b 4f 21 1f 1b b7 2c
13 19 3d 56 ab 4b 09 a9 1e 62 5c ee c0 d2 ba 2d" 1.3.6.1.2.1.9999.1.2.5.2.1.5.11 -i 1
docsBpi2CmtsCACertStatus.11 = createAndGo(4)
docsBpi2CmtsCACert.11 =
30 82  04 00   30 82  02 e8    a0 03  02 01   02 02  10 43
74 98  f0 9a   7d cb  c1 fa    7a a1  01 fe   97 6e  40 30
...
f9 3b  59 5e   e2 05  0e 89    e5 9d  2a 40   c2 9b  4f 21
1f 1b  b7 2c   13 19  3d 56    ab 4b  09 a9   1e 62  5c ee
c0 d2  ba 2d
docsBpi2CmtsCACertTrust.11 = trusted(1)
```

Fügen Sie während der CM-Registrierung eine abgelaufene Manuskripte in der CLI hinzu.

Ein Manu Cert wird in der Regel durch die vom CM an den uBR10K gesendete BPI Protocol AuthInfo-Nachricht in die uBR10K-Datenbank eingegeben. Jedes eindeutige und gültige Manu Cert, das in einer AuthInfo-Nachricht empfangen wird, wird der Datenbank hinzugefügt. Wenn das Manu-Zertifikat für den CMTS unbekannt ist (nicht in der Datenbank) und über abgelaufene Validierungsdaten verfügt, wird AuthInfo abgelehnt, und das Manu-Zertifikat wird der uBR10K-Datenbank nicht hinzugefügt. Ein ungültiges Manu-Zertifikat kann dem uBR10K von AuthInfo hinzugefügt werden, wenn die Umgehungskonfiguration für **den Schutz** der **Kabeldaten fehlgeschlagene Zertifikate beibehalten** unter der Konfiguration der uBR10K-Kabelschnittstelle vorhanden ist. Dies ermöglicht das Hinzufügen des abgelaufenen Manu Cert zur uBR10K-

Datenbank als UNTRUSTED. Um das abgelaufene Manu-Zertifikat zu verwenden, muss SNMP verwendet werden, um es TRUSTED zu kennzeichnen.

```
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
```

Wenn der abgelaufene Manu Cert zum uBR10K hinzugefügt und als TRUSTED markiert wird, wird empfohlen, die Konfiguration für den **Schutz** des **Kabelvertrauens zu** entfernen, **wenn Zertifikate nicht mehr** vorhanden sind, um das Hinzufügen weiterer unbekannter abgelaufener Manu Certs zum uBR10K zu verhindern.

Hinzufügen abgelaufener CM-Zertifikate und Manuskripte während der CM-Registrierung in der CLI

In einigen Fällen läuft das CM-Zertifikat ab. In diesem Fall ist neben der Konfiguration für den **Kabelschutz** eine weitere Konfiguration für den uBR10K erforderlich. Fügen Sie unter jeder relevanten uBR10K MAC Domain (Cable Interface) die Konfiguration für die **Gültigkeitsdauer des Kabels hinzu** und speichern Sie die Konfiguration. Dadurch ignoriert der uBR10K abgelaufene Validitätszeitprüfungen für ALLE CM- und Manu-Zertifikate, die in der CM-BPI-AuthInfo-Nachricht gesendet werden.

```
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
```

Zusätzliche Informationen

Überlegungen zur Konfiguration der MAC-Domäne/-Kabelschnittstelle

Die Konfigurationsbefehle für den Kabelschutz behalten fehlgeschlagene Zertifikate und den Kabelschutz-Gültigkeitszeitraum, für den der Gültigkeitszeitraum abgelaufen ist, werden auf der Ebene der MAC-Domäne/Kabelschnittstelle verwendet und sind nicht einschränkend. Mit dem Befehl "Keep-failed-Certificates" können Sie der uBR10K-Datenbank ein ausgefallenes Zertifikat hinzufügen, und der Befehl "SKP-Validation-Period" kann die Überprüfung des Gültigkeitsdatums für alle Manu- und CM-Zertifikate überspringen.

Überlegungen zur SNMP-Paketgröße

Wenn umfangreiche Zertifikate verwendet werden, kann eine zusätzliche uBR10K-SNMP-Konfiguration erforderlich sein. SNMP Get of Cert-Daten können NULL sein, wenn der cert OctetString größer als die SNMP-Paketgröße ist. Beispiele;

```
uBR10K#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
uBR10K(config)#snmp-server packetsize 3000
uBR10K(config)#end
```

Debug mit Manu Cert

Manu Cert Debug auf dem uBR10K uns unterstützt mit den **Debug-Kabel Privatsphäre ca-cert** und **debug Kabel MAC-Adresse <cm MAC-Adresse>** Befehlen. Weitere Debuginformationen finden Sie im Support-Artikel How to Decode DOCSIS Certificate for Modem Stuck State Diagnosis.

Dokumentation des zugehörigen Supports

- Kabelmodems und ablaufende Herstellerzertifizierungen für cBR-8-Produktbulletin - Cisco
- Cisco Universal Broadband Router der Serie uBR10000
- Technischer Support und Dokumentation für Cisco Systeme