Fabrikant certificaten maken voor Workround en herstellen op uBR10K

Inhoud

Inleiding

In dit document worden opties beschreven om servicetechnicus (CM) van de kabelmodemuitgangen te voorkomen, te bewerken en te herstellen. Dit heeft gevolgen voor de uBR10K Cable Modem Termination System (CMTS), die afkomstig zijn van de verlopen Fabrikant certificaatrelease (Manu Cert).

Probleem

Er zijn verschillende oorzaken voor een CM om vast te komen in de ' werp' -status (pk) op uBR10K. Eén oorzaak is het verdwijnen van de Manu Cert. De Manu Cert wordt gebruikt voor

authenticatie tussen een CM en CMTS. In dit document is een Manu Cert wat de DOCSIS 3.0 Security Specification CM-SP-SECv3.0 refereert aan het CableLabs Mfg CA-certificaat of het CA-certificaat van de fabrikant. Verlopen betekent dat de uBR10K systeemdatum/-tijd de einddatum/tijd van de Manu Cert-geldigheid overschrijdt.

Een CM die probeert zich te registreren bij uBR10K nadat de Manu Cert is verlopen, is gemarkeerd van afwijzing (pk) door CMTS en is niet in gebruik. Een CM die al bij uBR10K is geregistreerd en in gebruik is wanneer de studie wordt voltooid, kan in gebruik blijven tot de volgende keer dat de CM probeert te registreren. UBR10K-kabellijnkaart, uBR10K-herstart of andere gebeurtenissen die modemregistratie veroorzaken, kunnen voorkomen. Op dat moment is de echtheidscontrole van het CM-systeem niet voltooid, wordt de uBR10K gemarkeerd (pk) en is het niet in gebruik.

DOCSIS 1.1 voor Cisco CMTS-routers biedt extra informatie over uBR10K-ondersteuning en configuratie van DOCSIS Privacy Interface (BPI+).

Informatie over communicatiemiddelen van Manu

Manu Cert-informatie kan worden bekeken via uBR10K CLI-opdrachten of Simple Network Management Protocol (SNMP). Deze opdrachten en informatie worden gebruikt door oplossingen die in dit document worden beschreven.

Manu Cert-informatievelden en -kenmerken

- Index: Een uniek geheel dat aan elke Manu Cert in de uBR10K database/MIB wordt toegewezen

- Onderwerp: De naam van het onderwerp precies zoals het in het X509-certificaat is gecodeerd
  n.: Algemene naamU: Organisatorische eenheido: Organisatiel: Locaties: StateorProvinceNamec: Landnaam
- Afgever: De certificeringsinstantie
- Serieel: Cert Serienummer weergegeven in een hexadecimale octet string
- Staat: De vertrouwensstatus van het certificaat
  vertrouwdonbetrouwbaargeketendwortel
- Bron: Hoe het certificaat de CMTS bereikte
  verklikkenconfiguratiebestandexterne databaseOther (Overig)auteurInfoverzameldeInfoCode
- Status/RowStatus: Status weergeven
  actiefnietIn serviceNietKlaaraanmakenGoaanmaken en wachtenvernietigen
- Cert: Het certificaat van de autoriteit die het certificaat onder code heeft
- Geldigheidsdatum: De begin- en einddatums die de manu Cert-geldigheidsperiode met betrekking tot de CMTS-systeemdatum en -tijd definiëren
  startdatum: De datum en het tijdstip waarop de Manu Cert geldig wordteinddatum : De datum en het tijdstip waarop de Manu Cert niet langer geldig is
- Cert: Het certificaat van de autoriteit die het certificaat onder code heeft
- Thumbprint: De SHA-1 hash van een CA-certificaat

uBR10K CLI-opdrachten

De uitvoer van deze opdracht bevat informatie over de herkenning van Manu. De Manu Cert-index kan alleen worden verkregen door SNMP

- vanuit uBR10K CLI-exc-modus of Linecard CLI-exc-modus: uBR10K#**show kabelprivacy-fabrikant-cert-lijst**
- vanuit uBR10K lijnkaartmodus: Sleuf-6-0#**show cryptografische kaarten**

Deze opdrachten voor het configureren van de kabelinterface worden gebruikt voor het herstel en het herstel van de werkpunten

- uBR10K (configuratie-als)#**kabelprivacy behoudt-faalde-certificaten**
- uBR10K (configuratie-als)#**kabelprivacy-geldigheid**

DOCSIS-BPI-PLUS-MIB OID's

De informatie van Manu Cert wordt gedefinieerd in docsBpi2CMTSCACertEntry OID tak 1.3.6.1.2.1.10.127.6.1.2.5.2.1, beschreven in de SNMP Object Navigator.

> **Opmerking:** In uBR10k-software is de RFC 4131 docsBpi2MIB / DOCS-IETF-BPI2-MIB geïmplementeerd met de incorrecte OID MIB tak/pad. Het uBR10k-platform is te koop en voorbij de end-of-support datum van de software, zodat er geen oplossing is voor dit softwaredefect. In plaats van het verwachte MIB pad/bijkantoor 1.3.6.1.2.10.127.6, **het MIB pad/tak 1.3.6.1.2.1.999 moet worden gebruikt voor SNMP-interacties met de BPI2 MIB/OIDs op uBR10k.**
> Verwante Cisco bug-id CSCum28486

Dit zijn de BPI2 MIB OID volledige pad-equivalenten voor Manu Cert-informatie over uBR10k zoals opgemerkt in Cisco bug-ID CSCum28486:

```
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
```

Opdrachtvoorbeelden in dit document gebruiken ellips (...) om aan te geven dat bepaalde informatie is weggelaten voor leesbaarheid.

Oplossing

CM firmware update is de beste langetermijnoplossing. De bedenkingen die CM's met verlopen Manu Certs toestaat om zich te registreren en online te blijven bij uBR10K worden in dit document beschreven, maar deze werkronden worden slechts aanbevolen voor kortetermijngebruik. Als een CM firmware-update geen optie is, is een CM-vervangingsstrategie een goede oplossing op lange termijn vanuit het oogpunt van beveiliging en werking. De hier beschreven oplossingen hebben betrekking op verschillende omstandigheden of scenario's en kunnen afzonderlijk of, sommige, in combinatie met elkaar worden gebruikt;

- CM-firmware bijwerken
- Een gekend Manu Cert op Trusted instellen
- CM-service herstellen nadat een bekende Manu-schijf is verlopen
- Installeer een onbekende Verlopen Manu Cert op de uBR10k en Mark Trusted
- Verlopen CM-certificering en Manu-certificering die door AuthInfo met een uBR10K CLI-opdracht wordt toegevoegd

Opmerking: Als BPI wordt verwijderd, is encryptie en authenticatie hierdoor onmogelijk, waardoor de levensvatbaarheid van dat systeem als een werkweg wordt geminimaliseerd.

CM-firmware bijwerken

In veel gevallen bieden CM-fabrikanten CM-firmware-updates die de geldigheidsduur van de Manu Cert verlengen. Deze oplossing is de beste optie en voorkomt, als deze wordt uitgevoerd voordat een Manu Cert afloopt, gerelateerde effecten op de service. CM's laden de nieuwe firmware en registreren met nieuwe Manu Certs en CM Certs. De nieuwe certificaten kunnen worden geauthentiseerd en de CM's kunnen zich met succes registreren bij uBR10K. Met de nieuwe munt van Manu en CM Cert kan een nieuwe certificeringsketen worden gemaakt naar het bekende Root Certificate dat al is geïnstalleerd in uBR10K.

Een gekend Manu Cert op Trusted instellen

Wanneer een CM firmware-update niet beschikbaar is vanwege een CM-fabrikant die niet actief is, kan er geen verdere ondersteuning voor een CM-model, enz., reeds bekende Manu Certs op uBR10k met geldigheideinddatums in de nabije toekomst proactief worden gemarkeerd met een uBR10k voorafgaand aan het verlopen. Het Manu Cert serienummer, de geldigheids einddatum en de staat kunnen met uBR10K CLI opdrachten worden gevonden. Het Manu Cert serienummer, de Staat van het Vertrouwen en de index kunnen met SNMP worden gevonden.

Bekende Manu-certificaten voor momenteel in gebruik zijnde en online modems worden doorgaans door uBR10K geleerd van een CM via het DOCSIS Privacy Interface (BPI)-protocol. Het AUTH-INFO-bericht van de CM naar uBR10K bevat de Manu Cert. Elke unieke Manu Cert wordt opgeslagen in uBR10K geheugen en de informatie ervan kan met uBR10K CLI opdrachten en SNMP worden bekeken.

Wanneer de Manu Cert is gemarkeerd als vertrouwd, dan doet dat twee belangrijke dingen. Ten eerste, laat het de software uBR10K BPI toe om de verlopen geldigheidsdatum te negeren. Ten tweede slaat het de Manu Cert op zoals vertrouwd in uBR10K NVRAM. Dit bewaart de status Manu Cert in een uBR10K herlading en maakt het overbodig om deze procedure te herhalen in het geval van een uBR10K herlading

De CLI- en SNMP-opdrachtvoorbeelden tonen hoe een Manu Cert-index, serienummer, vertrouwensstaat te identificeren; gebruik die informatie dan om de vertrouwensstaat in vertrouwen te veranderen. De voorbeelden zijn gericht op een Manu Cert met Index 5 en serienummer 45529C2654797E1623C6E723180A9E9C.

Bekijk de veel populaire informatie van uBR10K CLI

In dit voorbeeld **tonen** de uBR10K CLI-opdrachten **cryptografische kaarten** en **tonen** de **kabelprivacy-producent-cert-list** worden gebruikt om de bekende Manu Cert-informatie te bekijken.

```
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
```

Bekijk de informatie over het menu met SNMP vanaf een afstandsapparaat

Relevante uBR10K SNMP-id's:

```
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
```

In dit voorbeeld, wordt de korte opdracht gebruikt om informatie in de uBR10k Manu Cert Tabel te bekijken. Het bekende Manu Cert serienummer kan worden gecorreleerd aan de Manu Cert Index, die kan worden gebruikt om de vertrouwenstatus in te stellen. De specifieke SNMP-opdrachten en -formaten zijn afhankelijk van het apparaat en het besturingssysteem dat wordt gebruikt om de SNMP-opdracht/aanvraag uit te voeren.

```
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)
```

Stel de Verlopen bekende Manu Cert Trust State in op Trusted met SNMP

Waarden voor OID: docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5 (OID op uBR10k is 1.3.6.1.2.1.999.1.2.5.2.1.5)

1: vertrouwd
2: onbetrouwbaar
3: geketend
4: wortel

Het voorbeeld toont de truststaat die is veranderd van geketend in vertrouwd voor de Manu Cert met Index = 5 en serienummer = 45529C2654797E1623C6E723180A9E9C.

```
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
```

Bevestig de Manu Cert die met de uBR10K CLI of met SNMP is gewijzigd

- De waarde van de trust is veranderd van verbonden in "Trusted"
- De bronwaarde is gewijzigd in "SNMP", wat aangeeft dat het certificaat voor het laatst werd beheerd door SNMP en niet vanuit het BPI Protocol Auth Info Message

```
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-service herstellen nadat een bekende Manu-schijf is verlopen

Een eerder bekende Manu Cert is een certificaat dat reeds in de uBR10K-database aanwezig is, doorgaans als resultaat van AuthInfo-berichten van vorige CM-registratie. Als een Manu Cert niet is gemarkeerd en het certificaat afloopt, kunnen alle CM's die de verlopen Manu Cert gebruiken daarna offline gaan en proberen te registreren, maar de uBR10K markeert ze (pk) en ze zijn niet in gebruik. In dit hoofdstuk wordt beschreven hoe deze conditie kan worden hersteld en hoe CM's met verlopen Manu Certs kunnen worden geregistreerd en in bedrijf kunnen blijven.

Identificeer het verloopde gekende Manu Cert Serienummer

De Manu Cert-informatie voor een CM die geplakt is in diskette (pk) kan worden gecontroleerd met de uBR10K CLI-opdracht voor een kabelmodem van <CM MAC-adres> privacy.

```
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
```

Identificeer de index voor de verlopen gekende Manu kert en stel de Manu Cert Trust State in op Trusted

Gebruik dezelfde uBR10K CLI- en SNMP-opdrachten als in de vorige sectie zijn beschreven om de index voor de studie te identificeren op basis van het Manu Cert-serienummer. Gebruik het verlopen Manu Cert indexnummer om de Manu Cert trust status in te stellen op vertrouwd met SNMP.

```
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)
```

Installeer een onbekende Verlopen Manu Cert op uBR10K en Mark Trusted

In het geval dat een verlopen Manu Cert niet bekend is bij uBR10K, zodat het niet kan worden beheerd (gemarkeerd vertrouwd) voor het verstrijken en niet kan worden hersteld, moet de Manu Cert aan uBR10K worden toegevoegd en moet de markering op het vertrouwde worden aangebracht. Deze voorwaarde gebeurt wanneer een CM die voorheen onbekend is en niet op een uBR10K is geregistreerd, probeert te registreren met een onbekende en verlopen Manu Cert.

De Manu Cert kan aan uBR10K worden toegevoegd door SNMP Set of door de configuratie van de kabelprivacy-faalde certificaten.

Voeg een Verlopen Onbekend Rapport toe aan uBR10K met SNMP

Om het certificaat van een fabrikant toe te voegen, voegt u een ingang aan de tabel DOSBpi2CMSertTable toe. Specificeer deze eigenschappen voor elke ingang.

- docsBPi2CMSCACertStatus 1.3.6.1.2.1.999.1.2.5.2.1.7 (ingesteld op 4 om de rij te maken)
- docsBpi2CmtsCACert = 1.3.6.1.2.1.999.1.2.5.2.1.8 (De hexadecimale gegevens, als X509 certificaatwaarde, voor het eigenlijke X.509-certificaat)
- docsBpi2CmtsCACertTrust 1.3.6.1.2.1.999.1.2.5.2.1.5 (ingesteld op 1 om de vertrouwelijkheidsstaat van de Manu Cert in te stellen op betrouwbaar)

De meeste besturingssystemen kunnen invoerlijnen niet aanvaarden die zo lang nodig zijn om de hexadecimale string in te voeren die een certificaat specificeert. Om deze reden wordt een grafische SNMP manager aanbevolen om deze eigenschappen in te stellen. Voor een aantal certificaten kan een script, indien makkelijker, worden gebruikt.

De opdracht SNMP en de resultaten in het voorbeeld voegen een ASCII DER Encoded ASN.1

X.509 certificaat aan de uBR10K database toe met parameters:

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

Gebruik een uniek indexnummer voor de toegevoegde Manu Cert. Wanneer een verlopen Manu Cert wordt toegevoegd, is de Staat onbetrouwbaar tenzij deze handmatig is ingesteld op vertrouwd. Als een zichzelf ondertekend certificaat wordt toegevoegd, moet de **privacy-privacy-accepteren-certificaat** opdracht worden geconfigureerd onder de uBR10K-kabelinterfaceconconfiguratie voordat uBR10K het certificaat kan accepteren.

In dit voorbeeld wordt een deel van de inhoud van het certificaat weggelaten voor leesbaarheid, aangegeven door elipsis (...).

```
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)
```

Voeg een verlopen Manu Cert toe tijdens CM Registratie in CLI

Een Manu Cert voert doorgaans de uBR10K-database in door het bericht AuthInfo van het BPI-protocol dat uBR10K vanaf de CM naar de uBR10K wordt gestuurd. Elke unieke en geldige Manu Cert die in een AuthInfo bericht wordt ontvangen wordt toegevoegd aan de database. Als de Manu Cert niet bekend is met de CMTS (niet in de database) en de geldigheiddata is verlopen, wordt AuthInfo verworpen en wordt de Manu Cert niet toegevoegd aan de uBR10K database. Er kan een Ongeldige Manu Cert aan uBR10K worden toegevoegd door AuthInfo wanneer de configuratie van de **kabelprivacy-faalde-certificaten** van de werkrondeconfiguratie aanwezig is onder de uBR10K kabelinterfaceconfiguratie. Hiermee kan de verlopen Manu Cert aan de uBR10K database worden toegevoegd als ongeremd. Om het verlopen Manu Cert te gebruiken, moet SNMP worden gebruikt om het vertrouwde op te merken.

```
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
```

Wanneer de verlopen Manu Cert aan uBR10K wordt toegevoegd en de markering wordt aangebracht, wordt het verwijderen van de **kabelprivacy behouden-faalde** configuratie aanbevolen om de toevoeging van andere onbekende verlopen Manu Certs op uBR10K te voorkomen.

Verlopen CM-certificering en Manu-certificering die door AuthInfo met een uBR10K CLI-opdracht wordt toegevoegd

In sommige gevallen vervalt het CM-certificaat. In deze situatie **is**, naast de configuratie van de **kabelprivacy en de** configuratie **van** de **niet-geannuleerde certificaten**, nog een configuratie nodig op de uBR10K. Onder elk relevant uBR10K MAC-domein (Kabelinterface), voegt u de configuratie van de **kabelprivacy toe aan** de **geldig-**geldigheidsperiode en slaat u de configuratie op. Hierdoor negeert uBR10K verlopen geldigheidstermijnen voor ALLE CM- en Manu-certificaten die in het CM BPI Auth Info-bericht worden verzonden.

```
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
```

Aanvullende informatie

Configuratie-overweging voor MAC-domein/Cable Interface

De configuratieopdrachten voor de kabelprivacy behouden-faalde-certificaten en de kabelprivacy blijven geldig in de periode en worden gebruikt op het MAC Domain/Cable Interface-niveau en zijn niet restrictief. De opdracht vasthouden-default certificaten kan elk mislukt certificaat aan de uBR10K-database toevoegen en de opdracht skip-validiteitsperiode kan de Datumcontroles op alle Manu- en CM-certs overslaan.

SNMP-pakketgrootte

Een extra uBR10K SNMP-configuratie kan nodig zijn wanneer grote certificaten worden gebruikt. SNMP het krijgen van geheime gegevens kan NULL zijn als de cert OctetString groter is dan de SNMP pakketgrootte. Bijvoorbeeld;

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

Manu Cert Debug

Manu Cert debug op uBR10K wij die wordt ondersteund met de opdrachten **debug van kabelprivacy** en **debug van kabeladres <cm mac-adres>**. Aanvullende debug-informatie wordt uitgelegd in het ondersteuningsartikel How to Decode DOCSIS Certificate for Modem Stuck Diagnosis.

Verwante ondersteuningsdocumentatie

- Kabelmodems en verlopende fabriekscertificaten op cBR-8-productbulletin - Cisco
- Cisco uBR10000 Series universele breedbandrouters
- Technische ondersteuning en documentatie – Cisco Systems