Cable Modems and Expiring Manufacturer Certificates on cBR-8

Contents

1. Background

In the near future, Cable providers will be facing the issue where cable modems deployed in their networks will encounter expired Manufacturer Certificates (Manu Cert). For this document, a Manu Cert is what CM-SP-SECv3.0 refers to as CableLabs Mfg CA certificate or Manufacturer CA certificate.

An expired certificate in the certificate chain will fail CM authentication and will be prevented from registering on the CMTS. These CMs will be marked reject(pk) by the CMTS and will not be in service.

Cable providers would like to keep these modems in service. In most cases, modem manufacturers will provide firmware updates to extend the validity of the manufacturer certificates before the existing certificates expire. However, a subset of modem manufacturers may no longer be in a position to provide support. While planning a long term modem replacement strategy, continued use of CMs with expired Manu Certs is the short-term strategy. Removing BPI disables encryption and authentication, minimizing the viability of this option. Configuring the CMTS to ignore validity dates of Manu Certs is desired.

Things to consider:

- Update CM Firmware
- Marking “to be” Expired Manu Certs TRUSTED
- Recovering after Previously Known Manu Cert Expires
- Installing Expired Manu Certs and marking TRUSTED
- Expiring CM Device Certificates

2. Update CM Firmware

Ideally, CM manufacturers will provide updated CM firmware with new Manu Certs with extended Validity Dates. These CMs can be loaded with the new firmware and re-register with new Manu Certs and CM Certs. The new certificates will authenticate properly and the CMs will register w-online(pt). The new Manu Cert and CM Cert will create a new certificate chain back to the existing Root Certificate already installed in the CMTS.

3. Marking "to be" Expired Manu Certs TRUSTED

In the case where updated CM firmware is unavailable, as a result of a CM Manufacturer going out of business, no longer supporting a CM model, etc, the CMTS operator should plan ahead and mark "to be" expiring Manu Certs TRUSTED prior to the expiration dates. Here we will describe a procedure to TRUST a Manu Cert allowing associated CMs to register online(pt) and remain in-service.

Manu Certs for currently in-service and online(pt) modems are in the CMTS database as a result of the DOCSIS BPI protocol. The AUTH-INFO message sent from the CM to the CMTS contains the CM's Manu Cert. Each unique Manu Cert is stored in memory and it's information can be viewed by CLI command or SNMP.

e.g.

The CLI command show cable privacy manufacturer-cert-list shows information on each Manu Cert in the CMTS.

```
cmts-Boston-Ma#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
```

The following certificate info is shown using SNMP:

MIB definitions

```
docsBpi2CmtsCACertTable OBJECT-TYPE
     SYNTAX SEQUENCE OF DocsBpi2CmtsCACertEntry
     MAX-ACCESS  not-accessible
     STATUS   current
     DESCRIPTION
          "The table of known certificate authority certificates
     acquired by this device."
     ::= { docsBpi2CmtsCertObjects 2 }

docsBpi2CmtsCACertEntry OBJECT-TYPE
     SYNTAX DocsBpi2CmtsCACertEntry
     MAX-ACCESS not-accessible
     STATUS   current
     DESCRIPTION
          "A row in the Certificate Authority certificate
     table."
     INDEX { docsBpi2CmtsCACertIndex }
     ::= {docsBpi2CmtsCACertTable 1 }

DocsBpi2CmtsCACertEntry ::= SEQUENCE {
     docsBpi2CmtsCACertIndex Integer32,
     docsBpi2CmtsCACertSubject SnmpAdminString,
     docsBpi2CmtsCACertIssuer SnmpAdminString,
     docsBpi2CmtsCACertSerialNumber OCTET STRING,
     docsBpi2CmtsCACertTrust INTEGER,
     docsBpi2CmtsCACertSource INTEGER,
     docsBpi2CmtsCACertStatus RowStatus,
     docsBpi2CmtsCACert X509Certificate
```

```
jdoe@server1[977]-->./getmany -v2c 8.1.1.1 private docsBpi2CmtsCACertSubject
docsBpi2CmtsCACertSubject.1 = Data Over Cable Service Interface Specifications
docsBpi2CmtsCACertSubject.2 = tComLabs - Euro-DOCSIS
docsBpi2CmtsCACertSubject.3 = CableLabs
docsBpi2CmtsCACertSubject.4 = Motorola Corporation
docsBpi2CmtsCACertSubject.5 = CableLabs
jdoe@server1[978]-->./getmany -v2c 8.1.1.1 private docsBpi2CmtsCACertIssuer
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
jdoe@server1[979]-->./getmany -v2c 8.1.1.1 private docsBpi2CmtsCACertSerialNumber
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
jdoe@server1[980]-->./getmany -v2c 8.1.1.1 private docsBpi2CmtsCACertTrust
docsBpi2CmtsCACertTrust.1 = root(4)

docsBpi2CmtsCACertTrust.2 = root(4)
docsBpi2CmtsCACertTrust.3 = root(4)
docsBpi2CmtsCACertTrust.4 = chained(3)
docsBpi2CmtsCACertTrust.5 = chained(3)
jdoe@server1[981]-->./getmany -v2c 8.1.1.1 private docsBpi2CmtsCACertStatus
docsBpi2CmtsCACertStatus.1 = active(1)
docsBpi2CmtsCACertStatus.2 = active(1)
docsBpi2CmtsCACertStatus.3 = active(1)
docsBpi2CmtsCACertStatus.4 = active(1)
docsBpi2CmtsCACertStatus.5 = active(1)
jdoe@server1[982]-->./getmany -v2c 8.1.1.1 private docsBpi2CmtsCACertSource
docsBpi2CmtsCACertSource.1 = other(4)
docsBpi2CmtsCACertSource.2 = other(4)
docsBpi2CmtsCACertSource.3 = other(4)
docsBpi2CmtsCACertSource.4 = authentInfo(5)
docsBpi2CmtsCACertSource.5 = authentInfo(5)
```

In the example above, indices 4 and 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 since their expiration dates are much longer.

Examining the **CLC** CLI command **`show crypto pki certificates`** we can identify the Manu Certs Validity Date.

```
telnet 10.86.27.101
Trying 10.86.27.101...
Connected to 10.86.27.101.
Escape character is '^]'.

Linux 4.19.88 (cmts-Boston-Ma_RP_1) (0)

2019/07/16 18:43:13 : <anon>

 [cmts-Boston-Ma_RP_1:~]$ telnet cc6-0
Trying 10.0.3.6...
Connected to cc6-0.
Escape character is '^]'.

Linux 4.9.206 (cmts-Boston-Ma_SIP_6) (0)

  [cmts-Boston-Ma_SIP_6:~]$ ioucon 6

Slot-6-0>
Slot-6-0>ena
Slot-6-0#
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
```

SNMP can be used to mark Manu Certs TRUSTED. For our example we will identify Index 4, using certificate serial number, as our “to be” expiring Manu Cert. Let’s use SNMP to mark this Manu Cert TRUSTED. e.g.

```
docsBpi2CmtsCACertTrust OBJECT-TYPE
        SYNTAX    INTEGER {
                  trusted (1),
                  untrusted (2),
                  chained (3),
                  root (4)
                  }


jdoe@server1[983]-->./setany -v2c 8.1.1.1 private docsBpi2CmtsCACertTrust.4 -i 1
docsBpi2CmtsCACertTrust.4 = trusted(1)
jdoe@server1[984]-->
```

Marking the Manu Cert TRUSTED does two important things. First, it allows the CMTS BPI software to ignore the expired validity date. Second, it stores the Manu Cert as TRUSTED in the CMTS nvram. This preserves the Manu Cert state across a CMTS reload. This removes the need to repeat this procedure in the event of a CMTS reload.

The CLI and SNMP Get output after the SNMP Set to TRUSTED:

```
cmts-Boston-Ma#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

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

jdoe@server1[984]-->./getmany -v2c 8.1.1.1 private docsBpi2CmtsCACertSubject
docsBpi2CmtsCACertSubject.1 = Data Over Cable Service Interface Specifications
docsBpi2CmtsCACertSubject.2 = tComLabs - Euro-DOCSIS
docsBpi2CmtsCACertSubject.3 = CableLabs
docsBpi2CmtsCACertSubject.4 = Motorola Corporation
docsBpi2CmtsCACertSubject.5 = CableLabs
jdoe@server1[985]-->./getmany -v2c 8.1.1.1 private docsBpi2CmtsCACertIssuer
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
jdoe@server1[986]-->./getmany -v2c 8.1.1.1 private docsBpi2CmtsCACertSerialNumber
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
jdoe@server1[987]-->./getmany -v2c 8.1.1.1 private docsBpi2CmtsCACertTrust
docsBpi2CmtsCACertTrust.1 = root(4)
docsBpi2CmtsCACertTrust.2 = root(4)
docsBpi2CmtsCACertTrust.3 = root(4)
docsBpi2CmtsCACertTrust.4 = trusted(1)
docsBpi2CmtsCACertTrust.5 = chained(3)
jdoe@server1[988]-->./getmany -v2c 8.1.1.1 private docsBpi2CmtsCACertStatus
docsBpi2CmtsCACertStatus.1 = active(1)
docsBpi2CmtsCACertStatus.2 = active(1)
docsBpi2CmtsCACertStatus.3 = active(1)
docsBpi2CmtsCACertStatus.4 = active(1)
docsBpi2CmtsCACertStatus.5 = active(1)
jdoe@server1[989]-->./getmany -v2c 8.1.1.1 private docsBpi2CmtsCACertSource
docsBpi2CmtsCACertSource.1 = other(4)
docsBpi2CmtsCACertSource.2 = other(4)
docsBpi2CmtsCACertSource.3 = other(4)
```

```
docsBpi2CmtsCACertSource.4 = snmp(1)
docsBpi2CmtsCACertSource.5 = authentInfo(5)
jdoe@server1[990]-->
```

Notice for Index 4 the Trust State has changed to TRUSTED from CHAINED. Also, the source has changed to snmp(1) from authentInfo(5). This indicates the certificate was last managed by SNMP and not from the BPI Protocol AuthInfo Message.

4. Recovering after Previously Known Manu Cert Expires

A previously known Manu Cert is a certificate already present in the CMTS database. Typically, this manu cert is already present as a result of AuthInfo messages from modems having previously registered.

If a Manu Cert is not marked TRUSTED (as described above) and the certificate expires, all modems using that Manu Cert that subsequently go offline and re-register will be marked reject(pk) and not be in service. This section will describe how to recover and allow CMs to be online(pt).

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

e.g.

Message in syslog

```
CLC 6/0: Jul 11 17:36:07.094: %CBR-3-MANUFACTURE_CA_CM_CERTIFICATE_FORMAT_ERROR:
<133>CMTS[DOCSIS]: CM MAC Addr <001a.de86.9928> on Interface Cable6/0/0 U1 : Manu Cert S/N
437498F09A7DCBC1FA7AA101FE976E40 has Expired
```

4.1 Recovering Using SNMP

As described in 2) above, Manu Certs can be marked TRUSTED using SNMP. Using a combination of SNMP gets and searching for the Manu Cert S/N from the syslog message, the operator can identify the index to use for the SNMP set.

```
jdoe@server1[275]-->snmpwalk -v 2c -c private 8.1.1.1 docsBpi2CmtsCACertSerialNumber
docsBpi2CmtsCACertSerialNumber.1 = Hex-STRING: 58 53 64 87 28 A4 4D C0 33 5F 0C DB 33 84 9C 19
docsBpi2CmtsCACertSerialNumber.2 = Hex-STRING: 63 4B 59 63 79 0E 81 0F 3B 54 45 B3 71 4C F1 2C
docsBpi2CmtsCACertSerialNumber.3 = Hex-STRING: 62 97 48 CA C0 A6 0D CB D0 FF A8 91 40 D8 D7 61
docsBpi2CmtsCACertSerialNumber.4 = Hex-STRING: 43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E 40
docsBpi2CmtsCACertSerialNumber.5 = Hex-STRING: 70 1F 76 05 59 28 35 86 AC 9B 0E 26 66 56 2F 0E

jdoe@server1[983]-->./setany -v2c 8.1.1.1 private docsBpi2CmtsCACertTrust.4 -i 1
docsBpi2CmtsCACertTrust.4 = trusted(1)
jdoe@server1[984]-->
```

5. Installing Expired Manu Certs and marking TRUSTED

In the case when the Expired Manu Certs are not known to the CMTS and cannot be managed (marked TRUSTED) prior to expiration as described in 2) or not recovered as described in 3) above, the Manu Cert must be added to the CMTS and marked TRUSTED.

A modem or group of modems that were previously unknown and not registered on a CMTS could try to register with Expired Manu Certs. In this case, the Manu Cert are NOT present in the CMTS database and cannot be managed. The Manu Cert must be added to the CMTS database.

There are two ways to add a Manu Cert to the CMTS:

5.1 Option 1: SNMP Set

Using the SNMP set command createAndGo with a ASCII DER Encoded ASN.1 X.509 Certificate.

e.g.

```
/auto/tftpboot-pit/peastone/tools/snmpr/15.4.1.9/bin:755 ->./setany -v2c 8.23.1.1 private
docsBpi2CmtsCACertStatus.11 -i 4 docsBpi2CmtsCACert.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 31 39 30 37 06 03 55 04 0a 13 30 44 61 74
61 20 4f 76 65 72 20 43 61 62 6c 65 20 53 65 72 76 69 63 65 20 49 6e 74 65 72 66 61 63 65 20 53
70 65 63 69 66 69 63 61 74 69 6f 6e 73 31 15 30 13 06 03 55 04 0b 13 0c 43 61 62 6c 65 20 4d 6f
64 65 6d 73 31 36 30 34 06 03 55 04 03 13 2d 44 4f 43 53 49 53 20 43 61 62 6c 65 20 4d 6f 64 65
6d 20 52 6f 6f 74 20 43 65 72 74 69 66 69 63 61 74 65 20 41 75 74 68 6f 72 69 74 79 30 1e 17 0d
30 31 30 37 31 31 30 30 30 30 30 30 5a 17 0d 32 31 30 37 31 30 32 33 35 39 35 39 5a 30 81 ba 31
0b 30 09 06 03 55 04 06 13 02 55 53 31 1d 30 1b 06 03 55 04 0a 13 14 4d 6f 74 6f 72 6f 6c 61 20
43 6f 72 70 6f 72 61 74 69 6f 6e 31 13 30 11 06 03 55 04 08 13 0a 43 61 6c 69 66 6f 72 6e 69 61
31 12 30 10 06 03 55 04 07 13 09 53 61 6e 20 44 69 65 67 6f 31 0f 30 0d 06 03 55 04 0b 13 06 44
4f 43 53 49 53 31 0c 30 0a 06 03 55 04 0b 13 03 41 53 47 31 44 30 42 06 03 55 04 03 13 3b 4d 6f
74 6f 72 6f 6c 61 20 43 6f 72 70 6f 72 61 74 69 6f 6e 20 43 61 62 6c 65 20 4d 6f 64 65 6d 20 52
6f 6f 74 20 43 65 72 74 69 66 69 63 61 74 65 20 41 75 74 68 6f 72 69 74 79 30 82 01 22 30 0d 06
09 2a 86 48 86 f7 0d 01 01 01 05 00 03 82 01 0f 00 30 82 01 0a 02 82 01 01 00 b5 12 ba c5 5d 88
25 1f c8 ec 46 d7 7f 63 b1 a6 c9 98 d4 79 bc 65 e5 f8 a3 94 e9 7c 38 dd 60 fe f9 9e 09 d9 33 43
45 2a 42 44 de 89 a2 ad 9b bb 1a 72 42 a5 53 da 3d 87 9c 78 42 9c c3 3d e1 7a 77 1d 5e 33 4f c2
fb 16 67 37 cf 9a 86 5a 4f 3a 9b 6a cf 31 09 3c b6 e1 a4 46 96 e4 ea ca 64 e0 1c 0c 40 f4 b7 83
1e 85 36 e6 77 56 e7 f9 2a 16 c9 c1 8b 09 f0 31 d0 2d 9d f3 e2 a7 a1 76 db 7f 2b 72 68 74 7c 81
35 af f1 df b5 7d aa de c0 4c 0f c7 7e 70 d4 87 fe 85 cd 2d ee d6 27 8f 5f 43 cc dc c7 f1 e4 56
6f 40 72 81 59 62 b3 fd ff a2 dc 1a 33 3e 53 da 71 2c 37 cd b8 22 c0 72 d9 7e 4a 62 ad 66 7c d6
71 c9 0d c0 e8 0d f7 9e 04 2f 9e e8 ee a4 1c 95 60 81 b1 00 5e 80 30 30 1a cd fe bb ca 2a 6e ff
52 72 81 b8 fb ba e9 79 cd f5 ee c3 c1 6a 37 10 bb 96 49 23 f6 d8 c5 76 4f eb 02 03 01 00 01 a3
23 30 21 30 12 06 03 55 1d 13 01 01 ff 04 08 30 06 01 01 ff 02 01 00 30 0b 06 03 55 1d 0f 04 04
03 02 01 06 30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00 03 82 01 01 00 21 06 81 90 00 17 ef 15
83 d4 ca fe 32 cc 89 00 75 26 77 4c 05 0c e4 42 78 2f 1b be 4f be d6 8c c6 e7 d3 0b 86 87 99 ba
30 e8 98 a2 ba ba 22 41 27 76 be d9 9f b2 89 5c 07 5e 5e 3d fe 7d 11 06 a8 7c 5a 26 b6 5c dd 07
3b 5a c3 2e ed b5 64 be 41 d1 5c ea f4 de e4 6e b5 ad 3b 07 3f 7d 60 f6 bd 9f 9f 47 94 d4 a5 ab
```

```
81 f6 10 01 46 fe dc 0a a1 1a 5b 38 60 3b 97 0b be 12 44 1b 10 e3 b5 d6 3c 05 5c 84 90 2c 78 a6
df 5d 2f a0 f5 ac 6f 4f c4 d6 c5 c5 56 15 44 8d 55 57 3f e8 6e 55 21 46 64 50 3b 0f 2d 31 78 ac
24 0c 3f 9c 2e 1e 33 62 ea 17 e6 db 47 a9 59 05 ba d9 1b 11 8b a9 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"

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
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   31 39
30 37   06 03   55 04   0a 13   30 44   61 74   61 20   4f 76
65 72   20 43   61 62   6c 65   20 53   65 72   76 69   63 65
20 49   6e 74   65 72   66 61   63 65   20 53   70 65   63 69
66 69   63 61   74 69   6f 6e   73 31   15 30   13 06   03 55
04 0b   13 0c   43 61   62 6c   65 20   4d 6f   64 65   6d 73
31 36   30 34   06 03   55 04   03 13   2d 44   4f 43   53 49
53 20   43 61   62 6c   65 20   4d 6f   64 65   6d 20   52 6f
6f 74   20 43   65 72   74 69   66 69   63 61   74 65   20 41
75 74   68 6f   72 69   74 79   30 1e   17 0d   30 31   30 37
31 31   30 30   30 30   30 30   5a 17   0d 32   31 30   37 31
30 32   33 35   39 35   39 5a   30 81   ba 31   0b 30   09 06
03 55   04 06   13 02   55 53   31 1d   30 1b   06 03   55 04
0a 13   14 4d   6f 74   6f 72   6f 6c   61 20   43 6f   72 70
6f 72   61 74   69 6f   6e 31   13 30   11 06   03 55   04 08
13 0a   43 61   6c 69   66 6f   72 6e   69 61   31 12   30 10
06 03   55 04   07 13   09 53   61 6e   20 44   69 65   67 6f
31 0f   30 0d   06 03   55 04   0b 13   06 44   4f 43   53 49
53 31   0c 30   0a 06   03 55   04 0b   13 03   41 53   47 31
44 30   42 06   03 55   04 03   13 3b   4d 6f   74 6f   72 6f
6c 61   20 43   6f 72   70 6f   72 61   74 69   6f 6e   20 43
61 62   6c 65   20 4d   6f 64   65 6d   20 52   6f 6f   74 20
43 65   72 74   69 66   69 63   61 74   65 20   41 75   74 68
6f 72   69 74   79 30   82 01   22 30   0d 06   09 2a   86 48
86 f7   0d 01   01 01   05 00   03 82   01 0f   00 30   82 01
0a 02   82 01   01 00   b5 12   ba c5   5d 88   25 1f   c8 ec
46 d7   7f 63   b1 a6   c9 98   d4 79   bc 65   e5 f8   a3 94
e9 7c   38 dd   60 fe   f9 9e   09 d9   33 43   45 2a   42 44
de 89   a2 ad   9b bb   1a 72   42 a5   53 da   3d 87   9c 78
42 9c   c3 3d   e1 7a   77 1d   5e 33   4f c2   fb 16   67 37
cf 9a   86 5a   4f 3a   9b 6a   cf 31   09 3c   b6 e1   a4 46
```

```
96 e4   ea ca   64 e0   1c 0c   40 f4   b7 83   1e 85   36 e6
77 56   e7 f9   2a 16   c9 c1   8b 09   f0 31   d0 2d   9d f3
e2 a7   a1 76   db 7f   2b 72   68 74   7c 81   35 af   f1 df
b5 7d   aa de   c0 4c   0f c7   7e 70   d4 87   fe 85   cd 2d
ee d6   27 8f   5f 43   cc dc   c7 f1   e4 56   6f 40   72 81
59 62   b3 fd   ff a2   dc 1a   33 3e   53 da   71 2c   37 cd
b8 22   c0 72   d9 7e   4a 62   ad 66   7c d6   71 c9   0d c0
e8 0d   f7 9e   04 2f   9e e8   ee a4   1c 95   60 81   b1 00
5e 80   30 30   1a cd   fe bb   ca 2a   6e ff   52 72   81 b8
fb ba   e9 79   cd f5   ee c3   c1 6a   37 10   bb 96   49 23
f6 d8   c5 76   4f eb   02 03   01 00   01 a3   23 30   21 30
12 06   03 55   1d 13   01 01   ff 04   08 30   06 01   01 ff
02 01   00 30   0b 06   03 55   1d 0f   04 04   03 02   01 06
30 0d   06 09   2a 86   48 86   f7 0d   01 01   05 05   00 03
82 01   01 00   21 06   81 90   00 17   ef 15   83 d4   ca fe
32 cc   89 00   75 26   77 4c   05 0c   e4 42   78 2f   1b be
4f be   d6 8c   c6 e7   d3 0b   86 87   99 ba   30 e8   98 a2
ba ba   22 41   27 76   be d9   9f b2   89 5c   07 5e   5e 3d
fe 7d   11 06   a8 7c   5a 26   b6 5c   dd 07   3b 5a   c3 2e
ed b5   64 be   41 d1   5c ea   f4 de   e4 6e   b5 ad   3b 07
3f 7d   60 f6   bd 9f   9f 47   94 d4   a5 ab   81 f6   10 01
46 fe   dc 0a   a1 1a   5b 38   60 3b   97 0b   be 12   44 1b
10 e3   b5 d6   3c 05   5c 84   90 2c   78 a6   df 5d   2f a0
f5 ac   6f 4f   c4 d6   c5 c5   56 15   44 8d   55 57   3f e8
6e 55   21 46   64 50   3b 0f   2d 31   78 ac   24 0c   3f 9c
2e 1e   33 62   ea 17   e6 db   47 a9   59 05   ba d9   1b 11
8b a9   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
```

The above SNMP command added the certificate to the CMTS database. Be sure to use a unique index number when adding the Manu Cert. Index 11 was used in this example. Notice the Manu Cert was added and its current state is UNTRUSTED. This is because the Manu Cert has expired Validity Dates. This Manu Cert must be marked TRUSTED.

```
cmts-Boston-Ma#show cable priv manu
Cable Manufacturer Certificates:

Index: 4
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

Index: 11
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: Untrusted
Source: SNMP
RowStatus: Active
Serial:      437498F09A7DCBC1FA7AA101FE976E40
Thumbprint:  FA07609998FDCAFA8F80D87F1ACFC70E6C52C80F
Fingerprint: 0EABDBD19D8898CA9C720545913AB93B
```

Use SNMP Set to Mark this Manu Cert as TRUSTED.

```
/auto/tftpboot-pit/peastone/tools/snmpr/15.4.1.9/bin:756 ->./setany -v2c 8.23.1.1 private
docsBpi2CmtsCACertTrust.11 -i 1

docsBpi2CmtsCACertTrust.11 = trusted(1)

cmts-Boston-Ma#show cable priv manu

Cable Manufacturer Certificates:

Index: 4
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

Index: 11
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:  FA07609998FDCAFA8F80D87F1ACFC70E6C52C80F
Fingerprint: 0EABDBD19D8898CA9C720545913AB93B
```

5.2 Option 2: CLI

The typical manner in which a Manu Cert enters the CMTS database is thru the BPI Protocol AuthInfo message sent to the CMTS from the CM. Each unique and valid Manu Cert received in an AuthInfo message is added to the database. If the Manu Cert is “new” to the CMTS (not in the database) and has Expired Validity Dates, AuthInfo is rejected and the Manu Cert is not added to the CMTS database. An Invalid Manu Cert can be added to the CMTS thru AuthInfo using a MAC Domain configuration item. This allows the Invalid Manu Cert to enter the CMTS database as UNTRUSTED. To use this “new” Manu Cert the operator must mark the cert TRUSTED using the techniques described above.

```
conf t
int ca x/y/z
cable privacy retain-failed-certificates

e.g.

cmts-Boston-Ma#conf t
Enter configuration commands, one per line. End with CNTL/Z.
cmts-Boston-Ma(config)#int ca6/0/0
cmts-Boston-Ma(config-if)#cable privacy retain-failed-certificates
cmts-Boston-Ma(config-if)#end
```

After the Manu Cert has entered the CMTS Database and has been marked TRUSTED, the operator should remove this config to prevent additional, potentially unwanted, manu certs to enter the system.

6. Expiring CM Device Certificates

In some cases, the CM Certificate may expire. This requires additional configuration on the CMTS. For each Mac Domain on a CMTS, add the following configuration item and save the config. This configuration will ignore expired Validity dates for **ALL** CM and Manu Certs used in the MAC Domain.

e.g.

```
cmts-Boston-Ma#conf t
Enter configuration commands, one per line. End with CNTL/Z.
cmts-Boston-Ma(config)#int ca6/0/0
cmts-Boston-Ma(config-if)#cable privacy skip-validity-period
cmts-Boston-Ma(config-if)#end
cmts-Boston-Ma#wr
Jul 12 16:20:15.675: %SYS-5-CONFIG_I: Configured from console by console
Building configuration...
 [OK]
cmts-Boston-Ma#
```

7. Additional Information

7.1 MAC Domain Configuration

The operator should be aware the config commands

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

are used at the MAC Domain level and are not restrictive. The retain command will add any failed certificate to the CMTS database and skip-validity will skip Validity Date checks on all Manu and CM certs.

7.2 SNMP Packet Size

The following SNMP configuration may be needed if working with large sized certificates. SNMP Get of Cert data may be NULL if the cert OctetString is larger than the SNMP packet size.

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

7.3 Debug

For debugging the following commands can be used:

```
debug cable privacy ca-cert
debug cable mac-address <cm mac-addr>
```

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C25-2676809-00 10/21