Workaround and Recover Expired Manufacturer Certificates on uBR10K

Contents

Introduction

This document describes options to prevent, workaround, and recover from cable modem (CM) reject(pk) service impacts on the uBR10K Cable Modem Termination System (CMTS) that result from Manufacturer Certificate (Manu Cert) expiration.

Problem

There are different causes for a CM to become stuck in the reject(pk) state on the uBR10K. One cause is expiration of the Manu Cert. The Manu Cert is used for authentication between a CM and CMTS. In this document, a Manu Cert is what the DOCSIS 3.0 Security Specification CM-SP-SECv3.0 refers to as CableLabs Mfg CA certificate or Manufacturer CA certificate. Expire means the uBR10K system date/time exceeds the Manu Cert validity end date/time.

A CM that attempts to register with the uBR10K after the Manu Cert expires is marked reject(pk) by the CMTS and is not in service. A CM already registered with the uBR10K and in service when the Manu Cert expires can remain in service until the next time the CM attempts to register, which can occur after a single modem offline event, uBR10K Cable Linecard restart, uBR10K reload, or other events that trigger modem registration. At that time the CM fails authentication, is marked reject(pk) by the uBR10K and is not in service.

DOCSIS 1.1 for the Cisco CMTS Routers provides additional information about uBR10K support and configuration of DOCSIS Baseline Privacy Interface (BPI+).

Manu Cert Information

Manu Cert information can be viewed via uBR10K CLI commands or Simple Network Management Protocol (SNMP). These commands and information are used by solutions described in this document.

Manu Cert Information Fields and Attributes

- Index: A unique integer assigned to each Manu Cert in the uBR10K database/MIB
- Subject: The subject name exactly as it is encoded in the X509 certificate
  cn: CommonNameou: OrganizationalUnito: Organizationl: Localitys: StateOrProvinceNamec: CountryName
- Issuer: The certificate authority
- Serial: Cert Serial Number represented in a hexadecimal octet string
- State: The Trust status of the certificate
  trusteduntrustedchainedroot
- Source: How the certificate reached the CMTS
  snmpconfigurationFileexternalDatabaseotherauthentInfocompiledInfoCode
- Status/RowStatus: Cert Status
  activenotInServicenotReadycreateAndGocreateandWaitdestroy
- Cert: The X509 DER-encoded certificate authority certificate
- Validity Date: The start and end dates that define the Manu Cert validity period relative to the CMTS system date and time
  start date: The date and time at which the Manu Cert becomes validend date: The date and time at which the Manu Cert is no longer valid
- Cert: The X509 DER-encoded certificate authority certificate
- Thumbprint: The SHA-1 hash of a CA certificate

uBR10K CLI Commands

The output of this command includes some Manu Cert information. The Manu Cert index can only be obtained by SNMP

- From uBR10K CLI exec mode or Linecard CLI exec mode: uBR10K#**show cable privacy manufacturer-cert-list**
- From uBR10K Linecard CLI exec mode: Slot-6-0#**show crypto pki certificates**

These cable interface configuration commands are used for workarounds and recovery

- uBR10K(config-if)#**cable privacy retain-failed-certificates**
- uBR10K(config-if)#**cable privacy skip-validity-period**

DOCSIS-BPI-PLUS-MIB OIDs

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

> **Note**: In uBR10k software, the RFC 4131 docsBpi2MIB / DOCS-IETF-BPI2-MIB was implemented with the incorrect OID MIB branch/path. The uBR10k platform is end of sale and past the end of software support date, so there is no fix for this software defect. Instead of the expected MIB path/branch 1.3.6.1.2.10.127.6, **the MIB path/branch 1.3.6.1.2.1.9999 must be used for SNMP interactions with the BPI2 MIB/OIDs on the uBR10k.** Related Cisco bug ID CSCum28486

These are the BPI2 MIB OID full path equivalents for Manu Cert information on the uBR10k as noted 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
```

Command examples in this document use ellipsis (...) to indicate some information has been omitted for readability.

Solution

CM firmware update is the best long-term solution. Workarounds that permit CMs with expired Manu Certs to register and remain online with the uBR10K are described in this document, but these workarounds are only recommended for short-term use. If a CM firmware update is not an option, a CM replacement strategy is a good long-term solution from a security and operations perspective. The solutions described here address different conditions or scenarios and can be used individually or, some, in combination with each other;

- Update CM Firmware
- Set a Known Manu Cert to Trusted
- Recover CM Service After a Known Manu Cert Expires
- Install an Unknown Expired Manu Cert on the uBR10k and Mark Trusted
- Permit Expired CM Certs and Manu Certs to be Added by AuthInfo with a uBR10K CLI Command

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

Update CM Firmware

In many instances, CM manufacturers provide CM firmware updates that extend the validity end date of the Manu Cert. This solution is the best option and, when performed before a Manu Cert expires, prevents related service impacts. CMs load the new firmware and re-register with new Manu Certs and CM Certs. The new certificates can authenticate properly and the CMs can successfully register with the uBR10K. The new Manu Cert and CM Cert can create a new certificate chain back to the known Root Certificate already installed in the uBR10K.

Set a Known Manu Cert to Trusted

When a CM firmware update is unavailable due to a CM Manufacturer gone out of business, no further support for a CM model, etc, Manu Certs already known on the uBR10k with validity end dates in the near future can be proactively marked trusted in the uBR10k prior to expiration. The Manu Cert serial number, validity end date and state can be found with uBR10K CLI commands. The Manu Cert serial number, Trust State and index can be found with SNMP.

Known Manu Certs for currently in-service and online modems are typically learned by the uBR10K from a CM through the DOCSIS Baseline Privacy Interface (BPI) protocol. The AUTH-INFO message sent from the CM to the uBR10K contains the Manu Cert. Each unique Manu Cert is stored in uBR10K memory and its information can be viewed with uBR10K CLI commands and SNMP.

When the Manu Cert is marked as trusted, that does two important things. First, it allows the uBR10K BPI software to ignore the expired validity date. Second, it stores the Manu Cert as trusted in the uBR10K NVRAM. This preserves the Manu Cert state across a uBR10K reload and eliminates the need to repeat this procedure in the event of a uBR10K reload

The CLI and SNMP command examples demonstrate how to identify a Manu Cert index, serial number, trust state; then use that information to change the trust state to trusted. The examples focus on a Manu Cert with Index 5 and Serial Number 45529C2654797E1623C6E723180A9E9C.

View the Many Cert Information from the uBR10K CLI

In this example the uBR10K CLI commands **show crypto pki certificates** and **show cable privacy manufacturer-cert-list** are used to view the known Manu Cert information.

```
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
```

View the Manu Cert Information with SNMP from a Remote Device

Relevant 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
```

In this example, the snmpwalk command is used to view information in the uBR10k Manu Cert Table. The known Manu Cert serial number can be correlated to the Manu Cert Index, which can be used to set the trust state. Specific SNMP commands and formats depend on the device and operating system used to execute the SNMP command/request.

```
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)
```

Set the Expired Known Manu Cert Trust State to Trusted with SNMP

Values for OID: docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5 (OID on uBR10k is 1.3.6.1.2.1.9999.1.2.5.2.1.5)

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

The example shows the trust state changed from chained to trusted for the Manu Cert with Index = 5 and Serial Number = 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
```

Confirm the Manu Cert Changed with the uBR10K CLI or with SNMP

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

```
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
```

Recover CM Service After a Known Manu Cert Expires

A previously known Manu Cert is a certificate already present in the uBR10K database, typically as a result of AuthInfo messages from previous CM registration. If a Manu Cert is not marked trusted and the certificate expires, all CMs that use the expired Manu Cert can subsequently go offline and attempt to register but the uBR10K marks them reject(pk) and they are not in service. This section describes how to recover from this condition and allow CMs with expired Manu Certs to register and remain in service.

Identify the Expired Known Manu Cert Serial Number

The Manu Cert information for a CM stuck in reject(pk) can be checked with the uBR10K CLI command **show cable modem <CM MAC Address> 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
```

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

Use the same uBR10K CLI and SNMP commands as described in the previous section to identify the index for the Manu Cert based on the Manu Cert serial number. Use the expired Manu Cert index number to set the Manu Cert trust state to trusted with 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)
```

Install an Unknown Expired Manu Cert on the uBR10K and Mark Trusted

In the case when an expired Manu Cert is not known to the uBR10K, so it cannot be managed (marked trusted) prior to expiration and cannot be recovered, the Manu Cert must be added to the uBR10K and marked trusted. This condition happens when a CM that is previously unknown and not registered on a uBR10K attempts to register with an unknown and expired Manu Cert.

The Manu Cert can be added to the uBR10K by SNMP Set or by the cable privacy retain-failed-certificates configuration.

Add an Expired Unknown Manu Cert to the uBR10K with SNMP

In order to add a manufacturer's certificate, add an entry to the docsBpi2CmtsCACertTable table. Specify these attributes for each entry.

- docsBpi2CmtsCACertStatus 1.3.6.1.2.1.9999.1.2.5.2.1.7 (Set to 4 to create the row entry)
- docsBpi2CmtsCACert = 1.3.6.1.2.1.9999.1.2.5.2.1.8 (The hexadecimal data, as an X509 Certificate value, for the actual X.509 certificate)
- docsBpi2CmtsCACertTrust 1.3.6.1.2.1.9999.1.2.5.2.1.5 (Set to 1 to set the Manu Cert Trust state to trusted)

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

The SNMP command and results in the example adds an ASCII DER Encoded ASN.1 X.509 certificate to the uBR10K database with parameters:

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

Use a unique index number for the added Manu Cert. When an expired Manu Cert is added, the State is untrusted unless it is manually set to trusted. If a self-signed certificate is added, the **cable privacy accept-self-signed-certificate** command must be configured under the uBR10K Cable Interface configuration before the uBR10K can accept the certificate.

In this example, some of the certificate content is omitted for readability, indicated by 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)
```

Add an Expired Manu Cert During CM Registration in the CLI

A Manu Cert typically enters the uBR10K database by the BPI Protocol AuthInfo message sent to the uBR10K from the CM. Each unique and valid Manu Cert received in an AuthInfo message is added to the database. If the Manu Cert is unknown to the CMTS (not in the database) and has expired validity dates, AuthInfo is rejected and the Manu Cert is not added to the uBR10K database. An Invalid Manu Cert can be added to the uBR10K by AuthInfo when the **cable privacy retain-failed-certificates** workaround configuration is present under the uBR10K cable interface configuration. This allows the addition of the expired Manu Cert to the uBR10K database as unstrusted. In order to use the expired Manu Cert, SNMP must be used to mark it trusted.

```
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
```

When the expired Manu Cert is added to the uBR10K and marked tusted, removal of the **cable privacy retain-failed-certificates** configuration is recommended to prevent addition of other unknown expired Manu Certs on the uBR10K.

Permit Expired CM Certs and Manu Certs to be Added by AuthInfo with a uBR10K CLI Command

In some cases, the CM certificate expires. For this situation, in addition to the **cable privacy retain-failed-certificates** configuration, another configuration is needed on the uBR10K. Under each relevant uBR10K MAC Domain (Cable Interface), add the **cable privacy skip-validity-period** configuration and save the configuration. This causes the uBR10K to ignore expired validity period checks for ALL CM and Manu Certs sent in the CM BPI AuthInfo message.

```
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
```

Additional Information

MAC Domain/Cable Interface Configuration Consideration

The cable privacy retain-failed-certificates and cable privacy skip-validity-period configuration commands are used at the MAC Domain / Cable Interface level and are not restrictive. The retain-failed-certificates command can add any failed certificate to the uBR10K database and skip-

validity-period command can skip Validity Date checks on all Manu and CM certs.

SNMP Packet Size Consideration

An additional uBR10K SNMP configuration can be needed when large-sized certificates are used. SNMP Get of Cert data can be NULL if the cert OctetString is larger than the SNMP packet size. For example;

```
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 on the uBR10K us supported with the **debug cable privacy ca-cert** and **debug cable mac-address <cm mac-address>** commands. Additional debug information is explained in the support article How to Decode DOCSIS Certificate for Modem Stuck State Diagnosis.

Related Support Documentation

- Cable Modems and Expiring Manufacturer Certificates on cBR-8 Product bulletin - Cisco
- Cisco uBR10000 Series Universal Broadband Routers
- Technical Support & Documentation - Cisco Systems