uBR10Kでの回避策と期限切れメーカー証明書の回復

内容

概要

このドキュメントでは、製造元の証明書(Manu Cert)の期限切れによるuBR10K Cable Modem Termination System(CMTS)への影響を防止、回避、およびケーブルモデムからの回復(CM)reject(pk)サービスの影響を回避するオプションについて説明します。

問題

uBR10KでCMがreject(pk)状態のままになる原因はさまざまです。原因の1つは、Manu証明書の有効期限です。Manu証明書は、CMとCMTS間の認証に使用されます。このドキュメントでは、Manu証明書は、DOCSIS 3.0セキュリティ仕様CM-SP-SECv3.0がCableLabs Mfg CA証明書また

は製造元CA証明書と呼ぶものです。[期限切れ(Expire)]は、uBR10Kシステムの日付/時刻がManu Certの有効終了日時を超えていることを意味します。

Manu証明書が期限切れになった後にuBR10Kへの登録を試みるCMは、CMTSによってreject(pk)とマークされ、サービス中ではありません。uBR10Kに登録済みで、Manu証明書が期限切れになった時点で使用中のCMは、CMが次に登録を試行するまでサービス中のままになります。これは、1つのモデムオフラインイベント、uBR10Kケーブルラインカードの再起動、またはその他トリガーイベント後です。その時点で、CMは認証に失敗し、uBR10Kによってreject(pk)とマークされ、サービス中ではありません。

Cisco CMTSルータ用のDOCSIS 1.1には、uBR10KのサポートとDOCSIS Baseline Privacy Interface(BPI+)の設定に関する追加情報が記載されています。

Manu証明書情報

Manu証明書情報は、uBR10K CLIコマンドまたはSimple Network Management Protocol(SNMP)を使用して表示できます。 これらのコマンドと情報は、このドキュメントで説明するソリューションで使用されます。

[Manu Cert Information]フィールドと属性

- インデックス:uBR10Kデータベース/MIBの各Manu証明書に割り当てられる一意の整数
- Subject: サブジェクト名は、X509証明書でエンコードされた名前と完全に同じです cn:CommonNameou:組織単位o:組織l:地域s：StateOrProvinceNamec:国名
- Issuer:認証局
- シリアル:16進数のオクテット文字列で表される証明書のシリアル番号
- State :証明書の信頼ステータス trusteduntrustedチェーン証明書root
- 送信元：証明書がCMTSに到達した方法 snmpconfigurationFileexternalDatabaseその他authentInfocompiledInfoCode
- Status/RowStatus:Cert Status activenotInService受信不可createAndGocreateandWait破壊する
- CERT:X509 DERでエンコードされた認証局(CA)証明書
- Validity Date:CMTSシステムの日付と時刻に対する手動証明書の有効期間を定義する開始日と終了日 start date:Manu証明書が有効になる日時end date:Manu証明書が無効になった日時
- CERT:X509 DERでエンコードされた認証局(CA)証明書
- 拇印：CA証明書のSHA-1ハッシュ

uBR10K CLIコマンド

このコマンドの出力には、Manu証明書情報が含まれています。Manu Certインデックスは、SNMPによってのみ取得できます

- uBR10K CLI execモードまたはラインカードCLI execモードから：uBR10K#**show cable privacy manufacturer-cert-list**
- uBR10KラインカードのCLI execモードから：Slot-6-0#**show crypto pki certificates**

次のケーブルインターフェイス設定コマンドは、回避策とリカバリに使用されます

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

DOCSIS-BPI-PLUS-MIB OID

Manu証明書情報は、SNMPオブジェクトナビゲーターで説明されているdocsBpi2CmtsCACertEntry OIDブランチ1.3.6.1.2.1.10.127.6.1.2.5.2.1で定義されています。

> **注**：uBR10kソフトウェアでは、RFC 4131 docsBpi2MIB / DOCS-IETF-BPI2-MIBが正しくないOID MIBブランチ/パスで実装されました。uBR10kプラットフォームは販売終了で、ソフトウェアサポート終了日を過ぎているため、このソフトウェア不具合の修正はありません。予想されるMIBパス/ブランチ1.3.6.1.2.10.127.6の代わりに、 **uBR10kのBPI2 MIB/OIDとのSNMPインタラクションには、MIBパス/ブランチ1.3.6.1.2.1.9999を使用する必要があります。**
> 関連Cisco Bug ID CSCum28486

Cisco Bug ID CSCum28486に記載されているように、uBR10kのManu Cert情報に対応するBPI2 MIB OIDのフルパスは次のとおりです。

```
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
```

このドキュメントのコマンド例では、省略記号(..)を使用して、一部の情報が読みやすくするために省略されていることを示します。

解決方法

CMファームウェアのアップデートが最適な長期的ソリューションです。このドキュメントでは、期限切れのManu証明書を持つCMを登録し、uBR10Kとオンライン状態に維持するための回避策について説明していますが、これらの回避策は短期間での使用にのみ推奨されます。CMファームウェアのアップデートがオプションではない場合、CMの交換戦略は、セキュリティと運用の観点から見た長期的なソリューションとして適しています。ここで説明するソリューションは、さまざまな条件やシナリオに対応しており、個別に使用することも、組み合わせて使用することもできます。

- CMファームウェアの更新
- 既知のManu証明書を[Trusted]に設定する
- 既知のManu証明書が期限切れになった後のCMサービスの回復
- uBR10kにUnknown Expired Manu Certをインストールし、[Mark Trusted]をオンにします
- uBR10K CLIコマンドを使用して、期限切れのCM証明書とManu証明書をAuthInfoによって追加することを許可する

> **注**：BPIが削除されると、暗号化と認証が無効になり、回避策としてのその実行可能性が最

小限に抑えられます。

CMファームウェアの更新

多くの場合、CMメーカーは、Manu証明書の有効終了日を延長するCMファームウェアアップデートを提供します。このソリューションは最適なオプションであり、Manu証明書が期限切れになる前に実行すると、関連するサービスへの影響を防止できます。CMは新しいファームウェアをロードし、新しいManu CertsとCM Certsを再登録します。新しい証明書は正しく認証され、CMはuBR10Kに正常に登録できます。新しいManu証明書とCM証明書は、uBR10Kにすでにインストールされている既知のルート証明書に新しい証明書チェーンを作成できます。

既知のManu証明書を[Trusted]に設定する

CMメーカーの事業停止によりCMファームウェアアップデートが利用できない場合、CMモデルなどのサポートが終了します。有効終了日が近いuBR10kですでに知られているManu Certsは、有効期限前にuBR10kで信頼できます。Manu証明書のシリアル番号、有効終了日、および状態は、uBR10K CLIコマンドで確認できます。Manu証明書のシリアル番号、信頼状態、およびインデックスは、SNMPで検索できます。

現在サービス中およびオンラインモデムに関する既知のManu証明書は、通常、DOCSIS Baseline Privacy Interface(BPI)プロトコルを通じて、uBR10KによってCMから学習されます。CMからuBR10Kに送信されるAUTH-INFOメッセージには、Manu証明書が含まれています。各固有のManu証明書はuBR10Kメモリに保存され、その情報はuBR10K CLIコマンドとSNMPで表示できます。

Manu証明書が信頼できるとマークされている場合、2つの重要な処理が行われます。最初に、uBR10K BPIソフトウェアが期限切れの有効期限日を無視できるようにします。次に、uBR10K NVRAMに信頼できるManu証明書を保存します。これにより、uBR10Kのリロード全体でManu Cert状態が維持され、uBR10Kのリロード時にこの手順を繰り返す必要がなくなります

CLIおよびSNMPコマンドの例では、Manu Certインデックス、シリアル番号、信頼状態を識別する方法を示します。その情報を使用して、信頼状態を信頼できる状態に変更します。この例では、インデックス5とシリアル番号45529C2654797E1623C6E723180A9E9CのManu証明書を中心に説明しています。

uBR10K CLIからの多数の証明書情報の表示

この例では、uBR10K CLIコマンド**show crypto pki certificates**と**show cable privacy manufacturer-cert-list**を使用して、既知のManu証明書情報を表示します。

```
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
```

リモートデバイスからのSNMPによるManu証明書情報の表示

関連するuBR10K SNMP OID:

```
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
```

この例では、snmpwalkコマンドを使用して、uBR10k Manu Cert Tableの情報を表示します。既知のManu証明書のシリアル番号は、Manu Cert Indexに関連付けることができます。Manu Cert Indexを使用して信頼状態を設定できます。特定のSNMPコマンドと形式は、SNMPコマンド/要求の実行に使用されるデバイスとオペレーティングシステムによって異なります。

```
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)
```

[Expired Known Manu Cert Trust State]を[Trusted with SNMP]に設定します

OIDの値： docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5(uBR10kのOIDは1.3.6.1.2.1.9999.1.2.5.2.1.5)

1：trusted
2：untrusted
3：チェーン証明書
4：root

この例では、信頼状態がチェーンから信頼に変更され、インデックスが5でManu証明書が使用され、シリアル番号が45529C2654797E1623C6E723180A9E9Cになっています。

```
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
```

uBR10K CLIまたはSNMPで変更されたManu証明書を確認します。

- 信頼値が「チェーン」から「信頼」に変更されました
- 送信元の値が「SNMP」に変更されました。これは、証明書がBPIプロトコルのAuthInfoメッセージではなく、SNMPによって最後に管理されたことを示します

```
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
```

既知のManu証明書が期限切れになった後のCMサービスの回復

以前に既知のManu証明書は、uBR10Kデータベースにすでに存在する証明書です。通常、以前のCM登録からのAuthInfoメッセージの結果として使用されます。Manu証明書が信頼できないとマークされ、証明書が期限切れになると、期限切れのManu証明書を使用するすべてのCMはオフラインになり、登録を試行できますが、uBR10Kはreject(pk)とマークし、サービス中ではありません。このセクションでは、この状態から回復し、期限切れのManu証明書を持つCMを登録してサービスを継続する方法について説明します。

期限切れの既知のManu証明書のシリアル番号の特定

reject(pk)でスタックしたCMのManu Cert情報は、uBR10K CLIコマンド**show cable modem <CM MAC Address> privacyで確認できます。**

```
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
```

期限切れの既知のManu証明書のインデックスを特定し、[Manu Cert Trust State]を[Trusted]に設定します

前のセクションで説明した同じuBR10K CLIおよびSNMPコマンドを使用して、Manu証明書のシ

リアル番号に基づいてManu証明書のインデックスを特定します。 期限切れのManu Certインデックス番号を使用して、Manu Cert信頼状態をSNMPで信頼できる状態に設定します。

```
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)
```

uBR10KにUnknown Expired Manu Certをインストールし、Mark Trustedをチェックする

期限切れのManu証明書がuBR10Kに認識されず、期限切れの前に管理（信頼とマーク）できず、回復できない場合、Manu証明書をuBR10Kに追加し、信頼とマークする必要があります。この状態は、以前は不明で、uBR10Kに登録されていないCMが、不明で期限切れのManu証明書を登録しようとしたときに発生します。

Manu証明書は、SNMPセットまたはcable privacy retain-failed-certificates設定によってuBR10Kに追加できます。

SNMPを使用してuBR10Kに期限切れの不明なManu証明書を追加する

製造元の証明書を追加するには、docsBpi2CmtsCACertTableテーブルにエントリを追加します。各エントリにこれらの属性を指定します。

- docsBpi2CmtsCACertStatus 1.3.6.1.2.1.9999.1.2.5.2.1.7（行エントリを作成するには4に設定）
- docsBpi2CmtsCACert = 1.3.6.1.2.1.9999.1.2.5.2.1.8（実際のX.509証明書の16進数のデータをX509証明書値として）
- docsBpi2CmtsCACertTrust 1.3.6.1.2.1.9999.1.2.5.2.1.5（Manu Cert Trust状態をtrustedに設定するには1に設定）

ほとんどのオペレーティングシステムでは、証明書を指定する16進数文字列を入力する必要がある限り、入力行を受け付けることはできません。このため、これらの属性を設定するには、グラフィカルなSNMPマネージャを使用することをお勧めします。多くの証明書では、便利であればスクリプトファイルを使用できます。

SNMPコマンドを発行すると、次の例の結果で、ASCII DER Encoded ASN.1 X.509証明書がuBR10Kデータベースにパラメータを使用して追加されます。

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

追加したManu証明書に一意のインデックス番号を使用します。期限切れのManu証明書が追加されると、手動で信頼に設定されていない限り、状態は信頼できません。自己署名証明書を追加する場合は、uBR10Kが証明書を受け入れる前に、uBR10Kケーブルインターフェイス設定で**cable privacy accept-self-signed-certificate**コマンドを設定する必要があります。

この例では、証明書の内容の一部が読みやすいように省略されています。これはエリプナズナ(...)で示されています。

```
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)
```

CLIでのCM登録時の期限切れManu証明書の追加

Manu証明書は通常、CMからuBR10Kに送信されるBPIプロトコルAuthInfoメッセージによってuBR10Kデータベースに入ります。AuthInfoメッセージで受信した一意で有効なManu証明書がデータベースに追加されます。Manu証明書が（データベースにない）CMTSで不明であり、有効期限が切れた場合、AuthInfoは拒否され、Manu証明書はuBR10Kデータベースに追加されません。uBR10Kケーブルインターフェイス設定の下に**cable privacy retain-failed-certificates回避策の設定がある場合、無効なManu証明書をAuthInfoによってuBR10Kに追加できます**。これにより、uBR10Kデータベースに期限切れのManu証明書を無制限として追加できます。期限切れのManu証明書を使用するには、SNMPを使用して信頼できるとマークする必要があります。

```
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
```

期限切れのManu証明書がuBR10Kに追加され、適合とマークされている場合は、uBR10Kで他の不明な期限切れManu証明書が追加されないように、**cable privacy retain-failed-certificates設定を削除することをお勧**勧めします。

uBR10K CLIコマンドを使用して、期限切れのCM証明書とManu証明書をAuthInfoによって追加することを許可する

場合によっては、CM証明書の有効期限が切れます。この状況では、**cable privacy retain-failed-certificates**設定に加えて、uBR10Kで別の設定が必要になります。関連する各uBR10K MACドメイン（ケーブルインターフェイス）の下に、**cable privacy skip-validity-period設定を追加**し、設定を保存します。これにより、uBR10Kは、CM BPI AuthInfoメッセージで送信されたすべてのCMおよびManu証明書の有効期限チェックを無視します。

```
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
```

追加情報

MACドメイン/ケーブルインターフェイス設定の考慮事項

cable privacy retain-failed-certificatesおよびcable privacy skip-validity-period設定コマンドは、MACドメイン/ケーブルインターフェイスレベルで使用され、制限はありません。retain-failed-certificatesコマンドは、失敗した証明書をuBR10Kデータベースに追加できます。skip-validity-periodコマンドは、すべてのManuおよびCM証明書の有効日付チェックをスキップできます。

SNMPパケットサイズの考慮事項

大規模な証明書を使用する場合は、追加のuBR10K SNMP設定が必要になる場合があります。証明書のOctetStringがSNMPパケットサイズより大きい場合、証明書データのSNMP GetはNULLになる可能性があります。 たとえば、

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

Manu証明書のデバッグ

uBR10K usでのManu Certデバッグは、**debug cable privacy ca-certコマンドおよびdebug cable mac-address <cm mac-address>コマンドでサポートされます。** その他のデバッグ情報については、サポート記事『How to Decode DOCSIS Certificate for Modem Stuck State Diagnosis』で説明しています。

関連サポートドキュメント

- cBR-8のケーブルモデムと期限切れメーカー証明書に関する製品速報：シスコ
- Cisco uBR10000 シリーズ ユニバーサル ブロードバンド ルータ
- テクニカル サポートとドキュメント – Cisco Systems