cBR-8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)の期限切れによって発生するcBR-8ケーブルモデム終端システム(CMTS)でのケーブルモデム(CM)reject(pk)サービスへの影響を防止、回避、および回復するオプションについて説明します。

問題

cBR-8でCMがreject(pk)状態のままになる原因はさまざまです。1つの原因は、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、cBR-8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cBR-8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。Manu証明書が期限切れになった時点でcBR-8に登録済みのCMは、単一のCMオフラインイベント、cBR-8ケーブルラインカードの再起動、cBR-8のリロード、またはその他のイベントによってCM登録がトリガーされるまで、サービス中です。その時点で、CMは認証に失敗し、cBR-8によってreject(pk)とマークされ、サービス中ではありません。

このドキュメントの情報は、Cable Modems and Expiring Manufacturer Certificates in cBR-8 Product Bulletinで公開されたコンテンツを拡張および再フォーマットします。

> **注**：Cisco Bug ID CSCvv21785、Cisco IOS XEの一部のバージョンでは、この不具合により、cBR-8のリロード後に、信頼できるManu証明書の検証が失敗します。場合によっては、Manu証明書が存在しますが、信頼できる状態ではなくなっています。この場合、このドキュメントで説明する手順を使用して、Manu証明書の信頼状態を信頼できる状態に変更できます。Manu証明書がshow cable privacy manufacturer-cert-listコマンドの出力に存在しない場合、このドキュメントで説明する手順を使用して、手動またはAuthInfoによってManu証明書を再度追加できます。

Manu証明書情報

多数の証明書情報は、リモートデバイスからcBR-8 CLIコマンドまたはSimple Network Management Protocol(SNMP)コマンドで表示できます。cBR-8 CLIでは、SNMP set、get、get-bulkコマンドもサポートされています。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:cBR-8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createAndGocreateand Wait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

cBR-8 CLIコマンド

Manu証明書情報は、次のcBR-8 CLIコマンドで表示できます。

- cBR-8 CLI execモードまたはラインカードCLI execモードから：CBR8-1#**show cable privacy manufacturer-cert-list**
- cBR-8ラインカードのCLI execモードから：Slot-6-0#**show crypto pki certificates**

これらのCisco IOS® XE SNMPコマンドは、cBR-8 CLIからSNMP OIDの取得と設定に使用されます。

- snmp get
- snmp get-bulk
- snmp set

これらのcBR-8ケーブルインターフェイス設定コマンドは、このドキュメントの「ソリューション」セクションで説明されている回避策とリカバリに使用されます。

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

DOCSIS-BPI-PLUS-MIB OID

Manu Cert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 branch 1.3.6.1.2.1.10.127.6.1.2.5.2.1で定義されています。

関連するSNMP OID

```
docsBpi2CmtsCACertSubject 1.3.6.1.2.1.10.127.6.1.2.5.2.1.2
docsBpi2CmtsCACertIssuer 1.3.6.1.2.1.10.127.6.1.2.5.2.1.3
docsBpi2CmtsCACertSerialNumber 1.3.6.1.2.1.10.127.6.1.2.5.2.1.4
docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5
docsBpi2CmtsCACertSource 1.3.6.1.2.1.10.127.6.1.2.5.2.1.6
docsBpi2CmtsCACertStatus 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7
docsBpi2CmtsCACert 1.3.6.1.2.1.10.127.6.1.2.5.2.1.8
```

コマンドの例では、省略記号(...)は、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説明する回避策は、期限切れのManu Certsを持つCMがcBR-8に登録してオンライン状態を維持することを許可しますが、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
- cBR-8にUnknown Expired Manu Certをインストールし、[Mark Trusted]をオンにします
- cBR-8 CLIコマンドを使用した、AuthInfoによる期限切れCM証明書およびManu証明書の追加の許可

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cBR-8に正常に登録できます。新しいManu CertとCM Certは、cBR-8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やCMモデルのサポートが終了したためにCMファームウェアのアップデートが利用できない場合など、cBR-8で既に存在する有効終了日の近いManu Certsは、有効終了日より前にcBR 8での信頼マークできます。cBR-8 CLIコマンドとSNMPは、シリアル番号や信頼状態などのManu Cert情報を識別するために使用され、SNMPは、関連付けられたCMの登録とサービス継続を可能にするcBR-8でManu Cert trust状態を設定するために使用されます。

現在サービス中およびオンラインCM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、CMからcBR-8によって学習されます。CMからcBR-8に送信されるAuthInfo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cBR-8メモリに保存され、その情報はcBR-8 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、cBR-8 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、Manu証明書をcBR-8 NVRAMに信頼できるものとして保存します。これにより、cBR-8のリロード全体でManu Cert(MCERT)状態が維持され、cBR-8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、および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、Manu Cert with Index 4とシリアル番号437498F09A7DCBC1FA7AA101FE976E40に焦点を当てています。

cBR-8 CLIからのManu証明書情報の表示

この例では、cBR-8 CLIコマンド**show cable privacy manufacturer-cert-listを使用**します。

```
CBR8-1#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
```

cBR-8 CLIからのSNMPを使用したManu証明書情報の表示

この例では、cBR-8 CLIコマンドsnmp get-bulkを使用します。Cert Indices 4 & 5は、CMTSメモリに保存されているManu Certsです。インデックス1、2、および3はルート証明書です。ルート証明書は有効期限が長いため、ここでは問題になりません。

```
docsBpi2CmtsCACertSubject
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.2
SNMP Response: reqid 1752673, errstat 0, erridx 0
docsBpi2CmtsCACertSubject.1 = Data Over Cable Service Interface Specifications
docsBpi2CmtsCACertSubject.2 = tComLabs - Euro-DOCSIS
docsBpi2CmtsCACertSubject.3 = CableLabs
docsBpi2CmtsCACertSubject.4 = Motorola
docsBpi2CmtsCACertSubject.5 = CableLabs

docsBpi2CmtsCACertIssuer
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.3
SNMP Response: reqid 1752746, errstat 0, erridx 0
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

CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.4
SNMP Response: reqid 2300780, errstat 0, erridx 0
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

docsBpi2CmtsCACertTrust
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.5
SNMP Response: reqid 1752778, errstat 0, erridx 0
docsBpi2CmtsCACertTrust.1 = 4
docsBpi2CmtsCACertTrust.2 = 4
docsBpi2CmtsCACertTrust.3 = 4
docsBpi2CmtsCACertTrust.4 = 3    (3 = chained)
docsBpi2CmtsCACertTrust.5 = 3

docsBpi2CmtsCACertSource
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.6
SNMP Response: reqid 1752791, errstat 0, erridx 0
docsBpi2CmtsCACertSource.1 = 4
docsBpi2CmtsCACertSource.2 = 4
docsBpi2CmtsCACertSource.3 = 4
docsBpi2CmtsCACertSource.4 = 5   (5 = authentInfo)
docsBpi2CmtsCACertSource.5 = 5

docsBpi2CmtsCACertStatus
CBR8-1#snmp get-bulk v2c 10.122.151.12 vrf Mgmt-intf Cisco123 non-repeaters 0 max-repetitions 5
oid 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7
SNMP Response: reqid 1752804, errstat 0, erridx 0
docsBpi2CmtsCACertStatus.1 = 1
docsBpi2CmtsCACertStatus.2 = 1
docsBpi2CmtsCACertStatus.3 = 1
docsBpi2CmtsCACertStatus.4 = 1   (1 = active)
docsBpi2CmtsCACertStatus.5 = 1
```

リモートデバイスからのSNMPによるManu証明書情報の表示

このドキュメントのリモートデバイスのSNMPの例では、リモートUbuntu Linuxサーバからの SNMPコマンドを使用します。特定のSNMPコマンドと形式は、SNMPコマンド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。

```
docsBpi2CmtsCACertSubject
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.2
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.1 = STRING: "Data Over Cable Service Interface
Specifications"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.2 = STRING: "tComLabs - Euro-DOCSIS"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.3 = STRING: "CableLabs"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.4 = STRING: "Motorola Corporation"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.2.5 = STRING: "CableLabs"

docsBpi2CmtsCACertIssuer
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.3
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.1 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.2 = STRING: "Euro-DOCSIS Cable Modem Root CA"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.3 = STRING: "CableLabs Root Certification Authority"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.4 = STRING: "DOCSIS Cable Modem Root Certificate Authority"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.3.5 = STRING: "CableLabs Root Certification Authority"

docsBpi2CmtsCACertSerialNumber
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.1 = Hex-STRING: 58 53 64 87 28 A4 4D C0 33 5F 0C DB 33 84 9C
19
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.2 = Hex-STRING: 63 4B 59 63 79 0E 81 0F 3B 54 45 B3 71 4C F1
2C
```

```
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.3 = Hex-STRING: 62 97 48 CA C0 A6 0D CB D0 FF A8 91 40 D8 D7
61
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.4 = Hex-STRING: 43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E
40
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.5 = Hex-STRING: 70 1F 76 05 59 28 35 86 AC 9B 0E 26 66 56 2F
0E

docsBpi2CmtsCACertTrust
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.1 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.2 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.3 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 = INTEGER: 3   (3 = chained)
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.5 = INTEGER: 3

docsBpi2CmtsCACertSource
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.6
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.1 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.2 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.3 = INTEGER: 4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.4 = INTEGER: 5   (5 = authentInfo)
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.5 = INTEGER: 5

docsBpi2CmtsCACertStatus
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.1 = INTEGER: 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.2 = INTEGER: 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.3 = INTEGER: 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.4 = INTEGER: 1   (1 = active)
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.7.5 = INTEGER: 1
```

CLIでのManu Cert Validity End Dateの確認

cBR-8ラインカードのCLIコマンドshow crypto pki certificatesを使用して、Manu証明書の有効終了日を確認します。このコマンド出力には、Manu Cert Indexは含まれていません。証明書のシリアル番号を使用すると、このコマンドから学習したManu証明書情報と、SNMPから学習したManu証明書情報を関連付けることができます。

```
CBR8-1#request platform software console attach

request platform software console attach 6/0
#
# Connecting to the CLC console on 6/0.
# Enter Control-C to exit the console connection.
#
Slot-6-0>enable
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
```

[Manu Cert Trust State]を[Trusted]に設定します

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4のManu証明書とシリアル番号が437498f09a7dcbc1fa7aa101fe976e40になっています

OID:docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5の値：

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

次の例は、信頼状態を変更するために使用するcBR-8 CLI snmp-setコマンドを示しています

```
CBR8-1#snmp set v2c 192.168.1.1 vrf Mgmt-intf private oid 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4
integer 1
SNMP Response: reqid 2305483, errstat 0, erridx 0
docsBpi2CmtsCACertTrust.4 = 1 (1 = trusted)
```

次の例は、リモートデバイスがSNMPを使用して信頼状態を変更することを示しています

```
jdoe@server1:~$ snmpset -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 i 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 = INTEGER: 1 (1 = trusted)
```

cBR-8 CLIまたはSNMPを使用したManu証明書の変更の確認

- 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

次の例は、変更を確認するために使用するcBR-8 CLIコマンドを示しています

```
CBR8-1#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
...
```

この例では、リモートデバイスがSNMPを使用して変更を確認しています

```
jdoe@server1:~$ snmpget -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 = INTEGER: 1 (1 = trusted)

jdoe@server1:~$ snmpget -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.6.4
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.6.4 = INTEGER: 1 (1 = snmp)
```

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、cBR-8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証明書が信頼されていないと期限切れになると、期限切れのManu証明書を使用してオフラインになるCMは再登録できず、reject(pk)としてマークされます。 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。

CMがオンラインにならず、Manu Certsの期限切れの結果としてreject(pk)とマークされると、syslogメッセージが生成され、CM MACアドレスと期限切れのManu証明書シリアル番号が含まれます。

cBR-8ログメッセージから期限切れのManu証明書のシリアル番号を確認する

```
CLC 6/0: Jan 11 17:36:07.094: %CBR-3-MANUFACTURE_CA_CM_CERTIFICATE_FORMAT_ERROR:
<133>CMTS[DOCSIS]: CM MAC Addr <1234.5678.9ABC> on Interface Cable6/0/0 U1 : Manu Cert S/N
437498F09A7DCBC1FA7AA101FE976E40 has Expired
```

期限切れの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

次の例は、ログメッセージからManu Certシリアル番号のインデックスを識別するために使用されるcBR-8 CLI SNMPコマンドを示しています。このコマンドは、Manu Certの信頼状態を信頼できる状態に設定するために使用されます。

```
CBR8-1#snmp get-bulk v2c 192.168.1.1 vrf Mgmt-intf private non-repeaters 0 max-repetitions 5 oid
1.3.6.1.2.1.10.127.6.1.2.5.2.1.4
SNMP Response: reqid 2351849, errstat 0, erridx 0
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

CBR8-1#snmp set v2c 192.168.1.1 vrf Mgmt-intf private oid 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4
integer 1
SNMP Response: reqid 2353143, errstat 0, erridx 0
docsBpi2CmtsCACertTrust.4 = 1 (1 = trusted)
```

この例では、リモートデバイスがSNMPコマンドを使用してログメッセージからManu Certシリアル番号のインデックスを識別し、その後Manu Certの信頼状態を信頼できる状態に設定するために使用されます。

```
jdoe@server1:~$ snmpwalk -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.4 | grep
"43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E 40"
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.4.4 = Hex-STRING: 43 74 98 F0 9A 7D CB C1 FA 7A A1 01 FE 97 6E
40

jdoe@server1:~$ snmpset -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 i 1
iso.3.6.1.2.1.10.127.6.1.2.5.2.1.5.4 = INTEGER: 1 (1 = trusted)
```

cBR-8にUnknown Expired Manu Certをインストールし、[Mark Trusted]をオンにします

期限切れのManu証明書がcBR-8に認識されない場合、期限切れ前に管理（信頼できるマーク）することはできず、回復できません。これは、cBR-8で以前に不明で登録されていない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、リモートデバイスからのSNMPによってcBR-8に追加する必要があります。または、**cable privacy retain-failed-certificates** cBR-8ケーブルインターフェイス設定を使用して、期限切れのManu証明書をAuthInfoで追加できるようにする必要があります。cBR-8 CLI SNMPコマンドを使用して証明書を追加することはできません。証明書データの文字数が、CLIで受け付けられる最大文字数を超えているためです。 自己署名証明書が追加されている場合は、cBR-8が証明書を受け入れる前に、cBR-8ケーブルインターフェイスで**cable privacy accept-self-signed-certificate**コマンドを設定する必要があります。

SNMPを使用してcBR-8に期限切れのManu証明書を追加する

これらのdocsBpi2CmtsCACertTable OID値を使用して、Manu Certを新しいテーブルエントリとして追加します。docsBpi2CmtsCACert OIDで定義されたManu証明書の16進数値は、サポート記事「How to Decode DOCSIS Certificate for Modem Stuck State Diagnosis」で説明されているCA証明書ダンプ手順で学習できます。

```
docsBpi2CmtsCACertStatus 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7 (Set to 4 to create the row entry)
docsBpi2CmtsCACert 1.3.6.1.2.1.10.127.6.1.2.5.2.1.8 (The hexadecimal data, as an X509Certificate
value, for the actual X.509 certificate)
docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5 (Set to 1 to set the Manu Cert Trust
state to trusted)
```

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。cBR-8にすでに存在するManu Certsのインデックスは、**show cable privacy manufacturer-cert-list**コマンドで確認できます。

```
CBR8-2#show cable privacy manufacturer-cert-list | i Index
Index: 4
```

```
Index: 5
Index: 6
Index: 7
```

このセクションの例では、cBR-8データベースに追加されたManu証明書のインデックス値11を使用します。

> **ヒント**：実際の証明書データの前に、必ずCertStatus属性を設定してください。それ以外の場合、CMTSは証明書がチェーンされていると仮定し、ただちに製造元とルート証明書との検証を試みます。

一部のオペレーティングシステムでは、証明書を指定する16進数のデータ文字列を入力する必要がある限り、入力行を受け入れることはできません。このため、グラフィカルなSNMPマネージャを使用してこれらの属性を設定できます。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。

この例では、リモートデバイスがSNMPを使用してManu Cert証明書をcBR-8に追加する方法を示しています。証明書データの大部分は、読みやすいように省略されています。これはelipses (..)で示されます。

```
jdoe@server1:~$ snmpset -v 2c -c private 192.168.1.1 1.3.6.1.2.1.10.127.6.1.2.5.2.1.7.11 i 4
1.3.6.1.2.1.10.127.6.1.2.5.2.1.8.11 x "0x3082...38BD" 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5.11 i 1
```

cBR-8 CLIコマンドを使用した、AuthInfoによる期限切れManu証明書の追加の許可

Manu証明書は通常、CMからcBR-8に送信されるBPIプロトコルAuthInfoメッセージによってcBR-8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cBR-8データベースに追加されません。cBR-8ケーブルインターフェイス設定で**cable privacy retain-failed-certificates回避策の設定が存在する場合、AuthInfo交換によって期限切れのManu証明書をCMTSに追加できます**。これにより、期限切れのManu証明書を信頼できないとしてcBR-8データベースに追加できます。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。期限切れのManu証明書がcBR-8に追加され、信頼できるとマークされている場合は、**cable privacy retain-failed-certificates設定を削除することをお勧めします**。追加の不要な可能性があるため、Manu Certsはシステムに入されません。

```
CBR8-1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
CBR8-1(config)#int Cable6/0/0
CBR8-1(config-if)#cable privacy retain-failed-certificates
CBR8-1(config-if)#end
```

cBR-8 CLIコマンドを使用した、AuthInfoによる期限切れCM証明書およびManu証明書の追加の許可

AuthInfo交換では、**cable privacy retain-failed-certificatesコマンドとcable privacy skip-validity-periodコマンドの両方が関連するケーブルインターフェイスで設定されている場合、期限切れのCM証明書をCMTSに追加できます**。これにより、cBR-8は、CM BPI AuthInfoメッセージで送信されたすべてのCMおよびManu証明書の有効期限日チェックを無視します。期限切れのCMおよびManu証明書がcBR-8に追加され、信頼できる場合は、追加の不要です。

```
CBR8-1#config t
Enter configuration commands, one per line.  End with CNTL/Z.
CBR8-1(config)#interface Cable6/0/0
CBR8-1(config-if)#cable privacy retain-failed-certificates
CBR8-1(config-if)#cable privacy skip-validity-period
CBR8-1(config-if)#end
CBR8-1#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cBR-8データベースに追加できます。また、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

Cert OctetStringがSNMPパケットサイズより大きい場合、CertデータのSNMP getはNULL値を返します。cBR-8 SNMP設定は、大規模な証明書を使用する場合に使用できます。

```
CBR8-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
CBR8-1(config)#snmp-server packetsize 3000
CBR8-1(config)#end
CBR8-1#copy run start
```

Manu証明書のデバッグ

cBR-8のManu Certデバッグは、**debug cable privacy ca-cert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。これには、Manu証明書の16進値を学習するために使用されるCA証明書ダンプ手順が含まれます。

関連サポートドキュメント

- Cisco CMTSルータ用のDOCSIS 1.1には、cBR-8のサポートとDOCSISベースラインプライバシーインターフェイス(BPI+)の設定に関する追加情報が提供されます。
- Cisco CMTSケーブルコマンドリファレンスには、このドキュメントで参照されているcBR-8 CLIコマンドに関する情報が記載されています。
- uBR10K CMTSに関するこのドキュメントと同様の情報を提供する「uBR10Kでの期限切れメーカー証明書の回避策と回復」。
- テクニカル サポートとドキュメント – Cisco Systems