Solución alternativa y recuperación de certificados de fabricante caducados en cBR-8

Contenido

Introducción

Este documento describe las opciones para evitar, solucionar y recuperarse de los impactos del servicio reject(pk) del cablemódem (CM) en el sistema de terminación del cablemódem cBR-8 (CMTS) que resultan del vencimiento del certificado del fabricante (Manu Cert).

Problema

Hay diferentes causas para que un CM se atasque en el estado reject(pk) en el cBR-8. Una de las causas es el vencimiento del certificado Manu. El certificado Manu se utiliza para la autenticación entre un CM y CMTS. En este documento, un certificado de Manu es lo que la especificación de seguridad de DOCSIS 3.0 CM-SP-SECv3.0 se refiere como certificado CA de fabricante de CableLabs o certificado CA de fabricante. Expire significa que la fecha/hora del sistema cBR-8 excede la fecha/hora de finalización de la validez de la certificación Manu.

El CMTS marca reject(pk) un CM que intenta registrarse con el cBR-8 después de que caduque el certificado Manu y no está en servicio. Un CM ya registrado con el cBR-8 y en servicio cuando vence el certificado Manu puede permanecer en servicio hasta la próxima vez que el CM intente registrarse, lo que puede ocurrir después de un único evento CM fuera de línea, cBR-8 Cable Linecard restart, cBR-8 reload u otros eventos que activan el registro de CM. En ese momento, el cBR-8 marca reject(pk) del CM falla la autenticación, y no está en servicio.

La información de este documento se expande y reda el formato del contenido publicado en los Cable Modems y los Certificados de Fabricante Vencidos en el Boletín de Producto cBR-8.

> **Nota:** Id. de bug Cisco CSCvv21785; En algunas versiones de Cisco IOS XE, este bug hace que un certificado Manu confiable falle a la validación después de una recarga cBR-8. En algunos casos, el certificado Manu está presente pero ya no se encuentra en el estado de confianza. En ese caso, se puede cambiar el estado de confianza del certificado de Manu a confiable con los pasos descritos en este documento. Si el certificado Manu no está presente en la salida del comando show cable privacy fabricante-cert-list, el certificado Manu puede ser agregado de nuevo manualmente o por AuthInfo con los pasos descritos en este documento.

Información de certificación de Manu

La información del certificado de manu se puede ver a través de comandos de CLI cBR-8 o comandos SNMP (Simple Network Management Protocol) desde un dispositivo remoto. La CLI cBR-8 también admite comandos SNMP set, get y get-bulk. Estos comandos e información son utilizados por las soluciones descritas en este documento.

Campos y atributos de información de certificados de Manu

- Índice: Un entero único asignado a cada certificado de manu en la base de datos/MIB cBR-8
- Asunto: El nombre del asunto tal como está codificado en el certificado X509 cn: NombreComúnou: Unidad organizativao: Organizaciónl: Localidads: NombreProvinciaDeEstadoc: Nombre del país
- Emisor: La autoridad certificadora
- Serie: Número de serie del certificado representado en una cadena de octetos hexadecimal
- Estado: El estado de confianza del certificado confiableno confiableencadenadoraíz
- Fuente: Cómo llegó el certificado al CMTS snmpconfigurationFileexternalDatabaseotroauthentInfocódigoDeInformaciónCompilado
- Status/RowStatus: Estado del certificado activonotInServicenotReadycreateAndGocrear y esperardestruir

- Certificado: El certificado de autoridad certificadora codificado en DER X509

- Fecha de validez: Las fechas de inicio y de finalización que definen el período de validez de la certificación Manu en relación con la fecha y hora del sistema CMTS
  fecha de inicio: La fecha y hora en la que el certificado de Manu pasa a ser válidofecha de finalización: La fecha y hora en la que el certificado de Manu ya no es válido
- Certificado: El certificado de autoridad certificadora codificado en DER X509
- Huella digital: El hash SHA-1 de un certificado CA

Comandos CLI cBR-8

La información del certificado de Manu se puede ver con estos comandos CLI cBR-8.

- Desde el modo de ejecución cBR-8 CLI o el modo de ejecución de CLI de Linecard: CBR8-1**#show cable privacy fabricante-cert-list**
- Desde el modo exec de cBR-8 Linecard CLI: Slot-6-0**#show crypto pki certificates**

Estos comandos SNMP de Cisco IOS® XE se utilizan desde la CLI cBR-8 para obtener y establecer OID SNMP.

- get de snmp
- snmp get-bulk
- set de snmp

Estos comandos de configuración de la interfaz de cable cBR-8 se utilizan para soluciones temporales y recuperación descritas en la sección Solución de este documento.

- cable privacy keep-failed-certificates
- cable privacy Ski-invalid-period

OID de DOCSIS-BPI-PLUS-MIB

La información del certificado de manu se define en la rama docsBpi2CmtsCACertEntry OID 1.3.6.1.2.1.10.127.6.1.2.5.2.1, descrita en el Navegador de objetos SNMP.

OID SNMP relevantes

```
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
```

En ejemplos de comandos, los puntos suspensivos (...) indican que se ha omitido alguna información para su legibilidad.

Solución

La actualización del firmware de CM es la mejor solución a largo plazo. Las soluciones descritas en este documento permiten que los CM con certificados Manu caducados se registren y permanezcan en línea con el cBR-8, pero estas soluciones alternativas sólo se recomiendan para

uso a corto plazo. Si una actualización del firmware de CM no es una opción, una estrategia de reemplazo de CM es una buena solución a largo plazo desde una perspectiva de seguridad y operaciones. Las soluciones aquí descritas abordan diferentes condiciones o escenarios y pueden ser utilizadas individualmente o, algunas, en combinación con otras;

- Actualizar el firmware de CM
- Establecer un certificado manual conocido como de confianza
- Recuperación del servicio CM después de que caduque un certificado Manu conocido
- Instale un certificado de administrador caducado desconocido en el cBR-8 y marque Trusted
- Permitir que los certificados CM caducados y los certificados Manu sean agregados por AuthInfo con un comando CLI cBR-8

Nota: Si se elimina BPI, esto inhabilita el cifrado y la autenticación, lo que minimiza la viabilidad de esto como solución alternativa.

Actualizar el firmware de CM

En muchos casos, los fabricantes de CM proporcionan actualizaciones de firmware de CM que amplían la fecha de finalización de validez del certificado Manu. Esta solución es la mejor opción y, cuando se realiza antes de que caduque un certificado de Manu, evita los impactos relacionados con el servicio. Los CM cargan el nuevo firmware y se vuelven a registrar con los nuevos certificados Manu y los certificados CM. Los nuevos certificados pueden autenticarse correctamente y los CM pueden registrarse correctamente con el cBR-8. El certificado Manu y el certificado CM nuevos pueden crear una nueva cadena de certificados de vuelta al certificado raíz conocido que ya está instalado en el cBR-8.

Establecer un certificado manual conocido como de confianza

Cuando una actualización del firmware de CM no está disponible debido a que un fabricante de CM se ha ido de la empresa, no hay soporte adicional para un modelo de CM, y así sucesivamente, los certificados de Manu ya conocidos en el cBR-8 con fechas de finalización de validez en un futuro próximo pueden marcarse proactivamente como de confianza en el cBR-8 antes de la fecha de finalización de validez. Los comandos de CLI cBR-8 y SNMP se utilizan para identificar la información de certificado de administración, como el número de serie y el estado de confianza, y SNMP se utiliza para establecer el estado de confianza de certificado de dominio en el cBR-8, que permite que los CM asociados se registren y permanezcan en servicio.

Los certificados Manu conocidos para CM en servicio y en línea son aprendidos normalmente por el cBR-8 de un CM a través del protocolo de la interfaz de privacidad de línea de base DOCSIS (BPI). El mensaje AuthInfo enviado desde el CM al cBR-8 contiene el certificado Manu. Cada certificado Manu único se almacena en la memoria cBR-8 y su información se puede ver mediante comandos CLI cBR-8 y SNMP.

Cuando el certificado Manu se marca como de confianza, esto hace dos cosas importantes. En primer lugar, permite que el software BPI cBR-8 ignore la fecha de validez vencida. En segundo lugar, almacena el certificado Manu como de confianza en la NVRAM cBR-8. Esto preserva el estado de certificación Manu en una recarga cBR-8 y elimina la necesidad de repetir este procedimiento en caso de una recarga cBR-8.

Los ejemplos de comandos CLI y SNMP muestran cómo identificar un índice de certificación de manual, número de serie y estado de confianza; a continuación, utilice esa información para

cambiar el estado de confianza a confiable. Los ejemplos se centran en el certificado Manu con el índice 4 y el número de serie 437498F09A7DCBC1FA7AA101FE976E40.

Ver información de certificación de Manu desde la CLI cBR-8

En este ejemplo se utiliza el comando cBR-8 CLI **show cable privacy fabricante-cert-list**.

```
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
```

Ver información de certificado de administrador con SNMP desde la CLI cBR-8

En este ejemplo se utiliza el comando cBR-8 CLI snmp get-bulk. Los índices de certificación 4 y 5 son los certificados Manu almacenados en la memoria CMTS. Los índices 1, 2 y 3 son certificados raíz. Los certificados raíz no son la preocupación aquí, ya que sus fechas de vencimiento son mucho más largas.

```
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
```

Ver la información de certificación de Manu con SNMP desde un dispositivo remoto

Los ejemplos SNMP del dispositivo remoto en este documento utilizan comandos SNMP desde un servidor Ubuntu Linux remoto. Los comandos y formatos específicos de SNMP dependen del dispositivo y del sistema operativo utilizados para ejecutar los comandos SNMP.

```
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
```

Identificación de la Fecha de finalización de la Validez de Certificados de Manu en la CLI

Utilice el comando cBR-8 linecard CLI **show crypto pki certificates** para identificar la fecha de finalización de la validez del certificado de Manu. Este resultado del comando no incluye el Índice de certificación Manu. El Número de serie del certificado se puede utilizar para correlacionar la información del certificado Manu aprendida de este comando con la información del certificado Manu aprendida de SNMP.

```
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
```

Establezca el estado de confianza del certificado de Manu en Trusted

Los ejemplos muestran el estado de confianza cambiado de encadenado a confiable para el certificado Manu con el índice = 4 y el número de serie = 437498f09a7dcbc1fa7aa101fe976e40

OID: docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5 valores:

1: confiable
2: no confiable
3: encadenado
4: raíz

Este ejemplo muestra el comando cBR-8 CLI snmp-set utilizado para cambiar el estado de confianza

```
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)
```

Este ejemplo muestra un dispositivo remoto que utiliza SNMP para cambiar el estado de confianza

```
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)
```

Confirme los cambios en el certificado Manu con la CLI cBR-8 o con SNMP

- El valor de confianza ha cambiado de encadenado a fiable
- El valor de origen cambiado a SNMP, que indica que el certificado fue administrado por última vez por SNMP y no por el mensaje BPI Protocol AuthInfo

Este ejemplo muestra el comando cBR-8 CLI utilizado para confirmar los cambios

```
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
...
```

Este ejemplo muestra que un dispositivo remoto utiliza SNMP para confirmar los cambios

```
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)
```

Recuperación del servicio CM después de que caduque un certificado Manu conocido

Un certificado Manu previamente conocido es un certificado ya presente en la base de datos cBR-8, normalmente como resultado de mensajes AuthInfo del registro CM anterior. Si un certificado de Manu no se marca como de confianza y caduca, cualquier CM que utilice el certificado de Manu caducado y se desconecte no podrá volver a registrarse y se marcará como reject(pk). Esta sección describe cómo recuperarse de esta condición y permitir que los CM con certificados Manu caducados se registren y permanezcan en servicio.

Cuando los CM no se conectan y se marcan reject(pk) como resultado de los certificados Manu caducados, se genera un mensaje syslog que contiene la dirección MAC de CM y el número de serie de certificado Manu caducado.

Identificación del Número de Serie del Certificado Manu Expired del Mensaje de Registro cBR-8

```
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
```

Identifique el índice del certificado de manu caducado y establezca el estado de confianza de certificado de manu en Trusted

Este ejemplo muestra los comandos cBR-8 CLI SNMP utilizados para identificar el índice para el número de serie del certificado de Manu del mensaje de registro, que luego se utiliza para establecer el estado de confianza del certificado de Manu en confiable.

```
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)
```

Estos ejemplos muestran que un dispositivo remoto utiliza comandos SNMP para identificar el índice del número de serie del certificado Manu del mensaje de registro, que luego se utiliza para establecer el estado de confianza del certificado Manu en confiable.

```
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)
```

Instale un certificado de administrador caducado desconocido en el cBR-8 y marque Trusted

Cuando el cBR-8 desconoce un certificado Manu caducado, no se puede administrar (marcado como de confianza) antes de su vencimiento y no se puede recuperar. Esto sucede cuando un CM que previamente es desconocido y no está registrado en un cBR-8 intenta registrarse con un certificado Manu desconocido y caducado. SNMP debe agregar el certificado Manu al cBR-8 desde un dispositivo remoto o utilizar la configuración de la interfaz del cable **cable privacy keep-failed-certificates** cBR-8 para permitir que AuthInfo agregue un certificado Manu caducado. Los comandos cBR-8 CLI SNMP no se pueden utilizar para agregar un certificado porque el número de caracteres en los datos del certificado supera los caracteres máximos aceptados por la CLI. Si se agrega un certificado autofirmado, el comando **cable privacy accept-self-signed-certificate** se debe configurar en la interfaz de cable cBR-8 antes de que cBR-8 pueda aceptar el certificado.

Agregar un certificado de administrador vencido al cBR-8 con SNMP

Utilice estos valores OID de docsBpi2CmtsCACertTable para agregar el certificado Manu como una nueva entrada de tabla. El valor hexadecimal del certificado Manu definido por el OID docsBpi2CmtsCACert se puede aprender con los pasos del volcado de certificado CA descritos en el artículo de soporte Cómo Decodificar el certificado DOCSIS para el diagnóstico de estado de anclaje del módem.

```
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)
```

Utilice un número de índice único para el certificado de Manu agregado. Los índices de los certificados Manu ya presentes en el cBR-8 se pueden verificar con el comando **show cable privacy fabricante-cert-list**.

```
CBR8-2#show cable privacy manufacturer-cert-list | i Index
Index: 4
Index: 5
Index: 6
Index: 7
```

Los ejemplos de esta sección utilizan un valor de índice de 11 para el certificado Manu agregado a la base de datos cBR-8.

> **Consejo:** Establezca siempre los atributos CertStatus antes de los datos reales del certificado. De lo contrario, el CMTS asume que el certificado está encadenado e inmediatamente intenta verificarlo con los fabricantes y los certificados raíz.

Algunos sistemas operativos no pueden aceptar las líneas de entrada que son el tiempo necesario para introducir la cadena de datos hexadecimal que especifica un certificado. Por esta razón, se puede utilizar un administrador SNMP gráfico para establecer estos atributos. Para varios certificados, se puede utilizar un archivo de script, si es más conveniente.

Este ejemplo muestra que un dispositivo remoto utiliza SNMP para agregar un certificado de certificado de Manu al cBR-8. La mayor parte de los datos del certificado se compromete a la legibilidad, indicada por elipses (...).

```
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
```

Permitir que AuthInfo agregue un certificado de dominio caducado con un comando CLI cBR-8

Un certificado Manu ingresa típicamente a la base de datos cBR-8 por el mensaje AuthInfo del protocolo BPI enviado al cBR-8 desde el CM. Cada certificado Manu único y válido recibido en un mensaje AuthInfo se agrega a la base de datos. Si el CMTS desconoce el certificado Manu (no en la base de datos) y tiene fechas de validez vencidas, se rechaza AuthInfo y el certificado Manu no se agrega a la base de datos cBR-8. El intercambio AuthInfo puede agregar un certificado Manu caducado al CMTS cuando la configuración de solución alternativa **cable privacy keep-failed-certificates** está presente en la configuración de la interfaz de cable cBR-8. Esto permite agregar el certificado Manu caducado a la base de datos cBR-8 como no confiable. Para utilizar el certificado de Manu caducado, se debe utilizar SNMP para marcarlo como confiable. Cuando se agrega el certificado Manu caducado al cBR-8 y se marca como de confianza, se recomienda

quitar la configuración del cable privacy keep-failed-certificates para que los certificados Manu adicionales, potencialmente no deseados, no entren en el sistema.

```
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
```

Permitir que los certificados CM caducados y los certificados Manu sean agregados por AuthInfo con un comando CLI cBR-8

El intercambio AuthInfo puede agregar un certificado CM caducado al CMTS cuando los comandos **cable privacy keep-failed-certificates** y **cable privacy Ski-valid-period** se configuran en cada interfaz de cable pertinente. Esto hace que el cBR-8 ignore las verificaciones de fecha de validez vencidas para TODOS los certificados CM y Manu enviados en el mensaje CM BPI AuthInfo. Cuando los certificados CM y Manu caducados se agregan al cBR-8 y se marcan como de confianza, se recomienda quitar la configuración descrita para que los certificados adicionales y potencialmente no deseados no entren en el sistema.

```
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
```

Additional Information

Consideración de la Configuración de la Interfaz de Cable/Dominio MAC

Los comandos de configuración **cable privacy keep-failed-certificates** y **cable privacy salt-invalid-period** se utilizan en el nivel de la interfaz de cable / dominio MAC y no son restrictivos. El comando keep-failed-certificates puede agregar cualquier certificado que haya fallado a la base de datos cBR-8 y el comando omitir-validez-period puede saltar las verificaciones de fecha de validez en todos los certificados de Manu y CM.

Consideración del Tamaño del Paquete SNMP

Un SNMP get para datos de certificado puede devolver un valor NULL si Cert OctetString es mayor que el tamaño del paquete SNMP. Se puede utilizar una configuración cBR-8 SNMP cuando se utilizan certificados de gran tamaño;

```
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
```

Depuración de certificados de Manu

La depuración de certificado de manu en el cBR-8 se soporta con los comandos **debug cable**

privacy ca-cert y **debug cable mac-address <CM mac-address>**. La información de depuración adicional se explica en el artículo de soporte Cómo Decodificar el Certificado DOCSIS para el Diagnóstico de Estado Atascado del Módem. Esto incluye los pasos de descarga de certificado CA utilizados para aprender el valor hexadecimal de un certificado Manu.

Documentación de soporte relacionada

- DOCSIS 1.1 para los routers Cisco CMTS proporciona información adicional sobre la compatibilidad con cBR-8 y la configuración de la interfaz de privacidad de línea de base DOCSIS (BPI+).
- Cisco CMTS Cable Command Reference proporciona información sobre los comandos CLI cBR-8 a los que se hace referencia en este documento.
- Trabajar alrededor y recuperar certificados de fabricante caducados en uBR10K proporciona información similar a la de este documento para uBR10K CMTS.
- Soporte Técnico y Documentación - Cisco Systems