Solución alternativa y recuperación de certificados de fabricante caducados en uBR10K

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 uBR10K (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 uBR10K. 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 uBR10K supera la fecha/hora de finalización de la validez de la certificación Manu.

El CMTS marca reject(pk) un CM que intenta registrarse con el uBR10K después de que caduque el certificado de Manu y no está en servicio. Un CM ya registrado con el uBR10K y en servicio cuando vence el certificado de Manu puede permanecer en servicio hasta la próxima vez que el CM intente registrarse, lo que puede ocurrir después de un único evento de desconexión de módem, reinicio de la tarjeta de línea de cable uBR10K, recarga uBR10K u otros eventos que activan el registro del módem. En ese momento, el uBR10K marca reject(pk) del CM falla la autenticación, y no está en servicio.

DOCSIS 1.1 para los routers Cisco CMTS proporciona información adicional sobre el soporte uBR10K y la configuración de la interfaz de privacidad de línea de base DOCSIS (BPI+).

Información de certificación de Manu

La información del certificado de manu se puede ver a través de comandos uBR10K CLI o protocolo simple de administración de red (SNMP). 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 uBR10K

- 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 activonotInServicenotReadycreateAndGocreateyWaitdestruir
- 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 uBR10K

El resultado de este comando incluye información de la certificación Manu. El índice de certificado

de Manu sólo puede obtenerse mediante SNMP

- Desde el modo exec uBR10K CLI o el modo exec de CLI de la tarjeta de línea: uBR10K**#show cable privacy fabricante-cert-list**
- Desde el modo exec uBR10K Linecard CLI: Slot-6-0**#show crypto pki certificates**

Estos comandos de configuración de la interfaz de cable se utilizan para soluciones temporales y recuperación

- uBR10K(config-if)#cable privacy keep-failed-certificates
- uBR10K(config-if)#cable privacy saltar-validar-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.

> **Nota:** En el software uBR10k, el RFC 4131 docsBpi2MIB / DOCS-IETF-BPI2-MIB fue implementado con la ramificación/trayectoria incorrecta de OID MIB. La plataforma uBR10k ha llegado al final de su ciclo de comercialización y ha superado la fecha de fin del soporte de software, por lo que no hay solución para este defecto de software. En lugar de la ruta/rama MIB esperada 1.3.6.1.2.10.127.6, **la trayectoria/bifurcación MIB 1.3.6.1.2.1.9999 se debe utilizar para las interacciones SNMP con los MIB/OID BPI2 en el uBR10k.**
> Id. de bug Cisco relacionado CSCum28486

Estos son los equivalentes de trayectoria completa OID de MIB BPI2 para la información de certificado de manu en el uBR10k, como se indica en el Id. de bug de Cisco 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
```

Los ejemplos de comandos de este documento utilizan puntos suspensivos (...) para indicar que se ha omitido alguna información para su legibilidad.

Solución

La actualización del firmware de CM es la mejor solución a largo plazo. En este documento se describen las soluciones alternativas que permiten que los CM con certificados Manu caducados se registren y permanezcan en línea con el uBR10K, 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 manu caducado desconocido en uBR10k y marque Trusted
- Permita que los certificados CM caducados y los certificados Manu sean agregados por AuthInfo con un comando uBR10K CLI

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 uBR10K. El nuevo certificado Manu y el certificado CM pueden crear una nueva cadena de certificados de vuelta al certificado raíz conocido ya instalado en el uBR10K.

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 ha dejado de funcionar, no hay soporte adicional para un modelo de CM, etc., los certificados de Manu ya conocidos en el uBR10k con fechas de finalización de validez en un futuro próximo se pueden marcar proactivamente como de confianza en el uBR10k antes de su vencimiento. El número de serie de la certificación Manu, la fecha de finalización de validez y el estado se pueden encontrar con los comandos uBR10K CLI. El número de serie del certificado Manu, el estado de confianza y el índice se pueden encontrar con SNMP.

Los certificados Manu conocidos para módems en servicio y en línea actualmente son aprendidos normalmente por el uBR10K de un CM a través del protocolo de interfaz de privacidad de línea de base (BPI) de DOCSIS. El mensaje AUTH-INFO enviado desde el CM al uBR10K contiene el certificado Manu. Cada certificado Manu único se almacena en la memoria uBR10K y su información se puede ver con los comandos uBR10K CLI y SNMP.

Cuando el certificado Manu se marca como de confianza, esto hace dos cosas importantes. Primero, permite que el software uBR10K BPI ignore la fecha de validez vencida. En segundo lugar, almacena el certificado Manu como de confianza en la NVRAM uBR10K. Esto preserva el estado del certificado de origen en una recarga uBR10K y elimina la necesidad de repetir este procedimiento en caso de una recarga uBR10K

Los ejemplos de comandos CLI y SNMP muestran cómo identificar un índice de certificación de Manu, número de serie, estado de confianza; a continuación, utilice esa información para cambiar el estado de confianza a confiable. Los ejemplos se centran en un certificado Manu con el índice 5 y el número de serie 45529C2654797E1623C6E723180A9E9C.

Vea la información de muchos certificados de la CLI uBR10K

En este ejemplo, los comandos uBR10K CLI **show crypto pki certificates** y **show cable privacy fabricante-cert-list** se utilizan para ver la información conocida del certificado Manu.

```
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
```

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

OID de SNMP uBR10K relevantes:

```
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
```

En este ejemplo, el comando snmpwalk se utiliza para ver información en la tabla uBR10k Manu Cert. El número de serie del certificado Manu conocido se puede correlacionar con el Índice de Cert Manu, que se puede utilizar para establecer el estado de confianza. Los comandos y

formatos específicos de SNMP dependen del dispositivo y del sistema operativo utilizado para ejecutar el comando/solicitud SNMP.

```
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)
```

Establezca el estado de confianza del certificado de administrador conocido caducado en Trusted con SNMP

Valores para OID: docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5 (OID en uBR10k es 1.3.6.1.2.1.9999.1.2.5.2.1.5)

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

El ejemplo muestra el estado de confianza cambiado de encadenado a confiable para el certificado Manu con el índice = 5 y el número de serie = 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
```

Confirme el certificado Manu cambiado con la CLI uBR10K o con SNMP

- El valor de confianza ha cambiado de encadenado a "fiable"

- El valor de origen cambió a "SNMP", que indica que el certificado fue administrado por última vez por SNMP y no por el mensaje AuthInfo del Protocolo BPI

```
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
```

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 uBR10K, normalmente como resultado de mensajes AuthInfo del registro CM anterior. Si un certificado de Manu no se marca como de confianza y el certificado caduca, todos los CM que utilizan el certificado de Manu caducado pueden desconectarse e intentar registrarse, pero el uBR10K los marca reject(pk) y no están en servicio. Esta sección describe cómo recuperarse de esta condición y permitir que los CM con certificados Manu caducados se registren y permanezcan en servicio.

Identificar el número de serie del certificado Manu caducado

La información del certificado Manu para un CM atascado en reject(pk) se puede verificar con el comando uBR10K CLI **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
```

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

Utilice los mismos comandos uBR10K CLI y SNMP descritos en la sección anterior para identificar el índice para el certificado de Manu basado en el número de serie del certificado de Manu. Utilice el número de índice de certificado de administrador caducado para establecer el estado de confianza de certificado de administrador en confiable con 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)
```

Instale un certificado de manu caducado desconocido en uBR10K y marque Trusted

En el caso de que el uBR10K desconozca un certificado de Manu caducado, por lo que no se puede administrar (marcado como de confianza) antes de su vencimiento y no se puede recuperar, el certificado de Manu debe agregarse al uBR10K y marcarse como de confianza. Esta condición se produce cuando un CM que antes era desconocido y no estaba registrado en un uBR10K intenta registrarse con un certificado Manu desconocido y caducado.

El certificado Manu se puede agregar al uBR10K mediante SNMP Set o mediante la configuración del cable privacy keep-failed-certificates.

Agregar un certificado de manu desconocido caducado al uBR10K con SNMP

Para agregar un certificado de fabricante, agregue una entrada a la tabla docsBpi2CmtsCACertTable. Especifique estos atributos para cada entrada.

- docsBpi2CmtsCACertStatus 1.3.6.1.2.1.9999.1.2.5.2.1.7 (Se establece en 4 para crear la entrada de fila)
- docsBpi2CmtsCACert = 1.3.6.1.2.1.999.1.2.5.2.1.8 (Los datos hexadecimales, como valor de certificado X509, para el certificado X.509 real)

- docsBpi2CmtsCACertTrust 1.3.6.1.2.1.9999.1.2.5.2.1.5 (Establecido en 1 para establecer el estado de confianza de certificados de manu en confiable)

La mayoría de los sistemas operativos no pueden aceptar líneas de entrada que sean lo más largas que sea necesario para introducir la cadena hexadecimal que especifica un certificado. Por esta razón, se recomienda un administrador SNMP gráfico para establecer estos atributos. Para varios certificados, se puede utilizar un archivo de script, si es más conveniente.

El comando SNMP y el resultado en el ejemplo agrega un certificado ASCII DER codificado ASN.1 X.509 a la base de datos uBR10K con parámetros:

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

Utilice un número de índice único para el certificado de Manu agregado. Cuando se agrega un certificado Manu caducado, el estado no es de confianza a menos que se establezca manualmente en confiable. Si se agrega un certificado autofirmado, el comando **cable privacy accept-self-signed-certificate** se debe configurar en la configuración de la interfaz de cable uBR10K antes de que el uBR10K pueda aceptar el certificado.

En este ejemplo, parte del contenido del certificado se omite para legibilidad, indicado por 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)
```

Agregar un certificado de administrador vencido durante el registro de CM en la CLI

Un certificado Manu ingresa típicamente a la base de datos uBR10K por el mensaje AuthInfo del protocolo BPI enviado al uBR10K 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 uBR10K. AuthInfo puede agregar un certificado Manu no válido al uBR10K cuando la configuración de solución alternativa **cable privacy keep-failed-certificates** está presente en la configuración de la interfaz de cable uBR10K. Esto permite agregar el certificado de Manu caducado a la base de datos uBR10K como no confiado. Para utilizar el certificado de Manu caducado, se debe utilizar SNMP para marcarlo como confiable.

```
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
```

Cuando se agrega el certificado de Manu caducado al uBR10K y se marca como de confianza, se recomienda **eliminar la** configuración de conservarcertificados **conservados fallidos del cable** para evitar la adición de otros certificados de Manu caducados desconocidos en el uBR10K.

Permita que los certificados CM caducados y los certificados Manu sean agregados por AuthInfo con un comando uBR10K CLI

En algunos casos, el certificado CM caduca. Para esta situación, además de la configuración **cable privacy keep-failed-certificates**, se necesita otra configuración en el uBR10K. En cada dominio MAC uBR10K (interfaz de cable) pertinente, agregue la configuración **cable privacy saltear-validar-period** y guarde la configuración. Esto hace que el uBR10K ignore las verificaciones del período de validez vencido para TODOS los certificados CM y Manu enviados en el mensaje CM BPI AuthInfo.

```
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

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

Los comandos de configuración de la privacidad del cable keep-failed-certificates y cable privacy salt-valid-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 uBR10K y el comando omitir-validez-periodo puede saltar las verificaciones de Fecha de validez en todos los certificados Manu y CM.

Consideración del Tamaño del Paquete SNMP

Se puede necesitar una configuración uBR10K SNMP adicional cuando se utilizan certificados de gran tamaño. SNMP Get of Cert data puede ser NULL si el cert OctetString es mayor que el tamaño del paquete SNMP. Por ejemplo;

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

Depuración de certificados de Manu

Manu Cert debug en el us uBR10K soportado 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.

Documentación de soporte relacionada

- Cable Modems y certificados de fabricante caducados en el boletín de producto cBR-8 - Cisco
- Routers de banda ancha universales de la serie Cisco uBR1000
- Soporte Técnico y Documentación - Cisco Systems