Solución y recuperación de certificados de fabricante caducados en uBR10K

Contenido

- Introducción
- Problema
  - Información de certificado de Manu
    - Campos y atributos de información de certificado de Manu
    - Comandos uBR10K CLI
    - OID DOCSIS-BPI-PLUS-MIB
- Solución
  - Actualizar firmware de CM
  - Establecer un certificado de Manu conocido como de confianza
    - Ver la información de muchos certificados de la CLI uBR10K
    - Ver la información del certificado del manual con SNMP desde un dispositivo remoto
    - Establezca el estado de confianza de certificado de Manu conocido caducado en De confianza con SNMP
    - Confirme que el certificado del manual ha cambiado con la CLI uBR10K o con SNMP
  - Recuperar el servicio CM después de que caduque un certificado de Manu conocido
    - Identificar el número de serie del certificado de Manu conocido caducado
    - Identifique el índice para el certificado de Manu conocido caducado y establezca el estado de confianza de certificado de Manu como fiable
  - Instale un certificado de manual caducado desconocido en el uBR10K y marque como de confianza
    - Agregar un certificado de manual desconocido caducado al uBR10K con SNMP
    - Agregar un certificado de manual caducado durante el registro de CM en la CLI
  - Permitir que los certificados CM y los certificados Manu caducados sean agregados por AuthInfo con un comando uBR10K CLI
  - Additional Information
    - Consideración de la Configuración de la Interfaz de Cable/Dominio MAC
    - Consideración del Tamaño del Paquete SNMP
    - Depuración de certificado manual
    - Documentación de asistencia relacionada

Introducción

Este documento describe las opciones para prevenir, solucionar y recuperarse de los impactos del servicio de rechazo (pk) del cablemódem (CM) en el Sistema de terminación de cablemódem (CMTS) uBR10K que resultan del vencimiento del Certificado del fabricante (Certificado de Manu).

Problema

Hay diferentes causas para que un CM se atasque en el estado reject(pk) en el uBR10K. Una de

las causas es la expiración del Certificado de Manu. El certificado Manu se utiliza para la autenticación entre un CM y CMTS. En este documento, un certificado manual es lo que la especificación de seguridad CM-SP-SECv3.0 de DOCSIS 3.0 denomina certificado CA de Fabricante o certificado CA de Fabricante de CableLabs Mfg. Vencimiento significa que la fecha/hora del sistema uBR10K excede la fecha/hora de finalización de validez del certificado de Manu.

Un CM que intenta registrarse con el uBR10K después de que caduque el certificado de Manu es marcado como reject(pk) por el CMTS y no está en servicio. Un CM ya registrado con el uBR10K y en servicio cuando caduca el certificado de Manu puede permanecer en servicio hasta la próxima vez que el CM intente registrarse, lo que puede ocurrir después de un evento sin conexión de módem único, reinicio de la tarjeta de línea de cable uBR10K, recarga de uBR10K u otros eventos que activen el registro del módem. En ese momento, el CM no logra autenticarse, es marcado como reject(pk) por uBR10K y no está en servicio.

DOCSIS 1.1 para los routers CMTS de Cisco proporciona información adicional sobre la compatibilidad con uBR10K y la configuración de la interfaz de privacidad DOCSIS Baseline Privacy Interface (BPI+).

Información de certificado de Manu

La información del certificado de Manu se puede ver a través de los comandos uBR10K CLI o del protocolo simple de administración de red (SNMP). Estos comandos e información se utilizan en las soluciones descritas en este documento.

Campos y atributos de información de certificado de Manu

- Índice: Un entero único asignado a cada certificado de manual en la base de datos/MIB uBR10K

- Asunto: El nombre del sujeto exactamente como está codificado en el certificado X509
    - cn: CommonName
    - ou: Unidad organizativa
    - o: Organización
    - l: Localidad
    - s: NombreProvinciaOEstado
    - c: NombrePaís
- Emisor: La autoridad de certificación
- Serie: Número de serie de certificado representado en una cadena de octetos hexadecimal
- Estado: El estado de confianza del certificado
    - de confianza
    - no confiable
    - encadenado
    - raíz
- Fuente: Cómo llegó el certificado al CMTS
    - snmp
    - archivoDeConfiguración

    - externalDatabase
    - otro
    - authentInfo
    - compiledInfoCode
- Estado/RowStatus: Estado del certificado
    - activo
    - notInService
    - notReady
    - createAndGo
    - createandWait
    - destruir
- Certificado: El certificado de autoridad de certificados X509 con codificación DER
- Fecha de validez: Las fechas de inicio y finalización que definen el período de validez del certificado de 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 válido
    - fecha de finalización: La fecha y hora en la que el certificado de Manu ya no es válido
- Certificado: El certificado de autoridad de certificados X509 con codificación DER
- Huella digital: Hash SHA-1 de un certificado de CA

Comandos uBR10K CLI

El resultado de este comando incluye información de certificado de Manu. El índice de certificado de Manu sólo se puede obtener mediante SNMP

- Desde el modo uBR10K CLI exec o el modo Linecard CLI exec: uBR10K#show cable privacy maker-cert-list
- Desde el modo de ejecución uBR10K Linecard CLI: Slot-6-0#show crypto pki certificates

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

- uBR10K(config-if)#cable privacy keep-failed-certificates
- uBR10K(config-if)#cable privacy skip-valid-period

OID DOCSIS-BPI-PLUS-MIB

La información de certificado del manual se define en la rama DOCEbpi2CmtsCACertEntry OID 1.3.6.1.2.1.10.127.6.1.2.5.2.1, descrita en SNMP Object Navigator.

Nota: En el software uBR10k, el RFC 4131 docsBpi2MIB / DOCS-IETF-BPI2-MIB se implementó con la rama/trayectoria OID MIB incorrecta. La plataforma uBR10k ha llegado al final de su ciclo de comercialización y ha superado la fecha de soporte del 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 rama/trayectoria 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 de Cisco relacionado CSCum28486

Estos son los equivalentes de ruta completa de OID MIB BPI2 para la información de certificado de Manu en uBR10k, como se indica en el Id. de bug 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 información para facilitar su lectura.

Solución

La actualización del firmware de CM es la mejor solución a largo plazo. En este documento se describen soluciones alternativas que permiten a los CM con certificados Manu caducados registrarse y permanecer en línea con uBR10K, pero estas soluciones alternativas sólo se recomiendan para el uso a corto plazo. Si no se puede actualizar el firmware de CM, una estrategia de sustitución de CM es una buena solución a largo plazo desde el punto de vista de la seguridad y las operaciones. Las soluciones descritas aquí abordan diferentes condiciones o escenarios y pueden utilizarse de forma individual o, en algunos casos, en combinación entre sí;

- Actualizar firmware de CM
- Establecer un certificado de Manu conocido como de confianza
- Recuperar el servicio CM después de que caduque un certificado de Manu conocido
- Instale un certificado de manual caducado desconocido en el uBR10k y marque como de confianza
- Permitir que los certificados CM y los certificados Manu caducados sean agregados por AuthInfo con un comando uBR10K CLI

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

Actualizar 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 de Manu. Esta solución es la mejor opción y, cuando se realiza antes de que caduque un certificado de Manu, evita los impactos de servicio relacionados. Los CM cargan el nuevo firmware y se vuelven a registrar con los nuevos certificados de Manu y CM. Los nuevos certificados pueden autenticarse correctamente y los CM

pueden registrarse con éxito con el uBR10K. El nuevo certificado de 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 de Manu conocido como de confianza

Cuando una actualización de firmware CM no está disponible debido a que un fabricante de CM ha dejado de trabajar, no hay más soporte para un modelo 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 la expiración. El número de serie del certificado de Manu, la fecha de finalización de validez y el estado se pueden encontrar con los comandos uBR10K CLI. El número de serie del certificado de Manu, el estado de confianza y el índice se pueden encontrar con SNMP.

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

Cuando el certificado de Manu se marca como confiable, eso hace dos cosas importantes. En primer lugar, permite que el software uBR10K BPI ignore la fecha de validez caducada. En segundo lugar, almacena el certificado de Manu como confiable en la NVRAM uBR10K. Esto preserva el estado del certificado de Manu a través de una recarga uBR10K y elimina la necesidad de repetir este procedimiento en el caso de una recarga uBR10K

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

Ver la información de muchos certificados de la CLI uBR10K

En este ejemplo, los comandos uBR10K CLI show crypto pki certificates y show cable privacy maker-cert-list se utilizan para ver la información de certificados de Manu conocidos.

<#root>

```
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 Inte
Subject: cn=Arris Cable Modem Root Certificate Authority,ou=Suwanee\, Georgia,ou=DOCSIS,o=Arris Interac
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 del certificado del manual 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 de Certificados

del Manual uBR10k. El número de serie de certificado de Manu conocido se puede correlacionar con el índice de certificado de Manu, que se puede utilizar para establecer el estado de confianza. Los formatos y comandos SNMP específicos dependen del dispositivo y del sistema operativo utilizados para ejecutar la solicitud o el comando SNMP.

<#root>

```
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 <-- S


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 de certificado de Manu conocido caducado en De confianza con SNMP

Valores para OID: docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5 (el OID en uBR10k es 1.3.6.1.2.1.999.1.2.5.2.1.5)

1: de confianza
2: no confiable
3: encadenado

4: raíz

El ejemplo muestra el estado de confianza cambiado de encadenado a confiable para el certificado de manual con índice = 5 y número de serie = 45529C2654797E1623C6E723180A9E9C.

<#root>

```
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 que el certificado del manual ha cambiado con la CLI uBR10K o con SNMP

- El valor de confianza cambió de encadenado a "De confianza"
- El valor de origen cambió a "SNMP", lo que indica que el certificado fue administrado por última vez por SNMP y no desde el mensaje de información de autenticación del protocolo BPI

<#root>

```
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 <-- S


...
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 Inte
Subject: cn=Arris Cable Modem Root Certificate Authority,ou=Suwanee\, Georgia,ou=DOCSIS,o=Arris Interac
State: Trusted
```

```
Source: SNMP

RowStatus: Active
Serial: 45529C2654797E1623C6E723180A9E9C

Thumbprint: DA39A3EE5E6B4B0D3255BFEF95601890AFD80709
```

Recuperar el servicio CM después de que caduque un certificado de Manu conocido

Un certificado Manu conocido anteriormente es un certificado que ya está presente en la base de datos uBR10K, generalmente como resultado de mensajes de AuthInfo del registro CM anterior. Si un certificado de Manu no se marca como confiable y el certificado expira, todos los CM que utilizan el certificado de Manu caducado pueden desconectarse posteriormente e intentar registrarse, pero el uBR10K los marca como 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 de Manu conocido caducado

La información de certificado de Manu para un CM atascado en reject(pk) se puede verificar con el comando uBR10K CLI show cable modem <CM MAC Address> privacy.

```
<#root>

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 para el certificado de Manu conocido caducado y establezca el estado de confianza de certificado de Manu como fiable

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

```
<#root>
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 manual caducado desconocido en el uBR10K y marque como de confianza

En caso de que el uBR10K no conozca un certificado de Manu caducado, por lo que no se pueda administrar (marcar como de confianza) antes de la expiración y no se pueda recuperar, el certificado de Manu se debe agregar al uBR10K y marcar como de confianza. Esta condición ocurre cuando un CM que es anteriormente desconocido y no está registrado en un uBR10K intenta registrarse con un certificado Manu desconocido y expirado.

El certificado de Manu se puede agregar al uBR10K mediante SNMP Set o mediante la

configuración de cable privacy keep-failed-certificates.

Agregar un certificado de manual 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 1.3.6.1.2.1.999.1.2.5.2.1.7 (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 1.3.6.1.2.1.999.1.2.5.2.1.5 (se establece en 1 para establecer el estado de confianza de certificados de manual en confiable)

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

El comando SNMP y los resultados del ejemplo agregan un certificado ASCII DER ASN.1 X.509 codificado 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 de Manu caducado, el estado no es de confianza a menos que se establezca manualmente como de confianza. Si se agrega un certificado autofirmado, se debe configurar el comando cable privacy accept-self-signed-certificate bajo la configuración de la interfaz de cable uBR10K para que 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.
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 3
...
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 e
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 manual caducado durante el registro de CM en la CLI

Normalmente, un certificado de manual ingresa a la base de datos uBR10K por el mensaje BPI Protocol AuthInfo enviado al uBR10K desde el CM. Cada certificado de Manu único y válido recibido en un mensaje AuthInfo se agrega a la base de datos. Si el CMTS desconoce el certificado de Manu (no está en la base de datos) y tiene fechas de validez vencidas, se rechaza AuthInfo y el certificado de Manu no se agrega a la base de datos uBR10K. AuthInfo puede agregar un certificado de manual no válido al uBR10K cuando la configuración de la solución alternativa cable privacy keep-failed-certificates está presente en la configuración de la interfaz de cable uBR10K. Esto permite agregar el certificado de manual caducado a la base de datos uBR10K como no fiable. Para utilizar el certificado de Manu caducado, se debe utilizar SNMP para marcarlo como confiable.

<#root>

```
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 el certificado de Manu caducado se agrega al uBR10K y se marca como confiable, se recomienda quitar la configuración de cable privacy keep-failed-certificates para evitar que se agreguen otros certificados de Manu caducados desconocidos en el uBR10K.

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

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

<#root>

```
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 cable privacy keep-failed-certificates y cable privacy skip-validation-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 fallido a la base de datos uBR10K y el comando skip-validez-period puede omitir las comprobaciones de la fecha de validez en todos los certificados Manu y CM.

Consideración del Tamaño del Paquete SNMP

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

<#root>

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

uBR10K(config)#end
```

Depuración de certificado manual

El debug de certificado de Manu en el uso uBR10K es compatible 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 descodificar el certificado DOCSIS para el diagnóstico de estado de bloqueo del módem.

Documentación de asistencia relacionada

- Módems por cable y certificados de fabricante caducados en el boletín de producto de cBR-8 - Cisco
- Cisco uBR10000 Series Universal Broadband Routers

- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).