Solução alternativa e recuperação de certificados de fabricantes expirados em uBR10K

Contents

[Introduction](#)
[Problema](#)
[Manu Cert Information](#)
[Campos e atributos das informações do certificado Manu](#)
[Comandos CLI uBR10K](#)
[OIDs DOCSIS-BPI-PLUS-MIB](#)
[Solução](#)
[Atualizar firmware CM](#)
[Defina um certificado manu conhecido como confiável](#)
[Veja as muitas informações de certificado da CLI uBR10K](#)
[Visualize as informações do certificado Manu com SNMP a partir de um dispositivo remoto](#)
[Defina o estado de confiança do certificado Manu conhecido expirado como confiável com SNMP](#)
[Confirme se o certificado Manu foi alterado com a CLI uBR10K ou com SNMP](#)
[Recupere o serviço CM depois que um certificado Manu conhecido expirar](#)
[Identificar o número de série do certificado Manu conhecido expirado](#)
[Identifique o índice do certificado Manu conhecido expirado e defina o estado de confiança do certificado Manu como confiável](#)
[Instale um certificado Manu Expired desconhecido no uBR10K e Mark Trusted](#)
[Adicione um certificado Manu desconhecido expirado ao uBR10K com SNMP](#)
[Adicionar um certificado Manu expirado durante o registro CM na CLI](#)
[Permitir certificados CM expirados e certificados Manu a serem adicionados por AuthInfo com um comando CLI uBR10K](#)
[Additional Information](#)
[Consideração de configuração de interface de cabo/domínio MAC](#)
[Consideração do tamanho do pacote SNMP](#)
[Depuração de certificado Manu](#)
[Documentação de suporte relacionada](#)

Introduction

Este documento descreve as opções para impedir, contornar e recuperar os impactos do serviço de rejeição (pk) de modem a cabo (CM) no CMTS (Cable Modem Termination System) uBR10K que resultam da expiração do Certificado do fabricante (Certificado Manu).

Problema

Há diferentes causas para um CM ficar preso no estado reject(pk) no uBR10K. Uma causa é o

vencimento do certificado Manu. O certificado Manu é usado para autenticação entre um CM e CMTS. Neste documento, um certificado Manu é o que a Especificação de Segurança DOCSIS 3.0 CM-SP-SECv3.0 se refere como certificado CA Mfg do CableLabs ou certificado CA do fabricante. Expirar significa que a data/hora do sistema uBR10K excede a data/hora de término da validade do certificado Manu.

Um CM que tenta se registrar no uBR10K após o certificado Manu expirar está marcado como reject(pk) pelo CMTS e não está em serviço. Um CM já registrado no uBR10K e em serviço quando o certificado Manu expira pode permanecer em serviço até a próxima vez que o CM tentar registrar-se, o que pode ocorrer após um único evento de modem offline, reinicialização da placa de linha de cabo uBR10K, recarregamento uBR10K ou outros eventos que acionam o registro de modem. Nesse momento, o CM falhou na autenticação, está marcado como reject(pk) pelo uBR10K e não está em serviço.

O DOCSIS 1.1 para os Cisco CMTS Routers fornece informações adicionais sobre o suporte uBR10K e a configuração da DOCSIS Baseline Privacy Interface (BPI+).

Manu Cert Information

As informações do certificado Manu podem ser visualizadas através de comandos CLI uBR10K ou SNMP (Simple Network Management Protocol). Esses comandos e informações são usados pelas soluções descritas neste documento.

Campos e atributos das informações do certificado Manu

- Índice: Um inteiro exclusivo atribuído a cada certificado Manu no banco de dados/MIB uBR10K

- Assunto: O nome do requerente tal como está codificado no certificado X509
  cn: CommonNameou: Unidade organizacionalo: OrganizaçãoI: Localidades: EstadoOuNomeDaProvínciac : Nome do país
- Emissor: Autoridade de certificação
- Série: Número de série do certificado representado em uma string de octeto hexadecimal
- Estado: O status de Confiança do certificado
  confiávelnão confiávelem cadeiaroot
- Fonte: Como o certificado atingiu o CMTS
  snmp:arquivo de configuraçãoexternalDatabaseoutrosauthentInfocompiladoInfoCode
- Status/Status da linha: Status do certificado
  ativonãoEmServiçonãoProntocriarEgocriar eEsperadestruir
- Cert: O certificado de autoridade de certificação codificado X509 DER
- Data de validade: As datas de início e término que definem o período de validade do certificado Manu relativo à data e hora do sistema CMTS
  data de início: A data e a hora em que o certificado Manu se torna válidodata de término: A data e a hora em que o certificado Manu já não é válido
- Cert: O certificado de autoridade de certificação codificado X509 DER
- Impressão digital: O hash SHA-1 de um certificado CA

Comandos CLI uBR10K

A saída desse comando inclui algumas informações do certificado Manu. O índice Manu Cert só pode ser obtido por SNMP

- A partir do modo exec CLI uBR10K ou do modo exec CLI do Linecard: uBR10K**#show cable privacy manufaturer-cert-list**
- A partir do modo exec CLI da placa de linha uBR10K: Slot-6-0**#show crypto pki certificate**

Esses comandos de configuração de interface de cabo são usados para soluções alternativas e recuperação

- uBR10K(config-if)#cable privacy retents-failed-certificate
- uBR10K(config-if)#cable privacy skip-valid-period

OIDs DOCSIS-BPI-PLUS-MIB

As informações do certificado Manu são definidas na seção docsBpi2CmtsCACertEntry OID 1.3.6.1.2.1.10.127.6.1.2.5.2.1, descrita no SNMP Object Navigator.

> **Note**: No software uBR10k, o RFC 4131 docsBpi2MIB / DOCS-IETF-BPI2-MIB foi implementado com a ramificação/caminho de MIB de OID incorreto. A plataforma uBR10k está no fim da venda e ultrapassou a data de suporte do software, portanto não há correção para esse defeito de software. Em vez do caminho/filial MIB esperado 1.3.6.1.2.10.127.6, **o caminho/filial MIB 1.3.6.1.2.1.9999 deve ser usado para interações SNMP com MIB/OIDs BPI2 no uBR10k.**
> ID de bug da Cisco relacionada CSCum28486

Estes são os equivalentes de caminho completo OID MIB BPI2 para informações de certificado Manu sobre o uBR10k conforme observado na ID de bug da 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
```

Exemplos de comandos neste documento usam elipse (...) para indicar que algumas informações foram omitidas para leitura.

Solução

A atualização do firmware CM é a melhor solução a longo prazo. As soluções alternativas que permitem que CMs com certificados Manu expirados se registrem e permaneçam on-line com o uBR10K estão descritas neste documento, mas essas soluções alternativas são recomendadas somente para uso a curto prazo. Se uma atualização de firmware de CM não for uma opção, uma estratégia de substituição de CM é uma boa solução de longo prazo do ponto de vista da segurança e das operações. As soluções aqui descritas abordam diferentes condições ou cenários e podem ser utilizadas individualmente ou em combinação entre si;

- Atualizar firmware CM
- Defina um certificado manu conhecido como confiável
- Recupere o serviço CM depois que um certificado Manu conhecido expirar
- Instalar um certificado Manu Expired desconhecido no uBR10k e Marcar como confiável
- Permitir certificados CM expirados e certificados Manu a serem adicionados por AuthInfo com um comando CLI uBR10K

Note: Se o BPI for removido, isso desabilitará a criptografia e a autenticação, o que minimizará a viabilidade disso como uma solução alternativa.

Atualizar firmware CM

Em muitos casos, os fabricantes de CM fornecem atualizações de firmware CM que estendem a data final de validade do certificado Manu. Essa solução é a melhor opção e, quando executada antes da expiração do certificado Manu, evita os impactos relacionados ao serviço. Os CMs carregam o novo firmware e registram-se novamente com os novos certificados Manu e CM. Os novos certificados podem ser autenticados corretamente e os CMs podem se registrar com êxito no uBR10K. O novo certificado Manu e o certificado CM podem criar uma nova cadeia de certificados de volta ao certificado raiz conhecido já instalado no uBR10K.

Defina um certificado manu conhecido como confiável

Quando uma atualização de firmware CM não está disponível devido ao fato de um fabricante de CM ter deixado de funcionar, não há suporte adicional para um modelo CM, etc., os certificados Manu já conhecidos no uBR10k com datas finais de validade no futuro próximo podem ser marcados proativamente como fidedignos no uBR10k antes da expiração. O número de série do certificado Manu, a data de término da validade e o estado podem ser encontrados com comandos CLI uBR10K. O número de série do certificado Manu, o estado de confiança e o índice podem ser encontrados com SNMP.

Os certificados Manu conhecidos para modems on-line e em serviço atualmente são normalmente aprendidos pelo uBR10K a partir de um CM através do protocolo DOCSIS Baseline Privacy Interface (BPI). A mensagem AUTH-INFO enviada do CM para o uBR10K contém o certificado Manu. Cada certificado Manu exclusivo é armazenado na memória uBR10K e suas informações podem ser visualizadas com comandos CLI uBR10K e SNMP.

Quando o certificado Manu é marcado como confiável, isso faz duas coisas importantes. Primeiro, ele permite que o software uBR10K BPI ignore a data de validade expirada. Segundo, armazena o certificado Manu como confiável na NVRAM uBR10K. Isso preserva o estado do certificado Manu em um recarregamento uBR10K e elimina a necessidade de repetir esse procedimento no caso de um recarregamento uBR10K

Os exemplos de comandos CLI e SNMP demonstram como identificar um índice Manu Cert, número de série, estado de confiança; em seguida, use essas informações para alterar o estado confiável para confiável. Os exemplos se concentram em um certificado Manu com índice 5 e número de série 45529C2654797E1623C6E723180A9E9C.

Veja as muitas informações de certificado da CLI uBR10K

Neste exemplo, os comandos uBR10K CLI **show crypto pki certificate** e **show cable privacy**

manufaturer-cert-list são usados para exibir as informações de certificado Manu conhecidas.

```
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
```

Visualize as informações do certificado Manu com SNMP a partir de um dispositivo remoto

OIDs 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
```

Neste exemplo, o comando snmpwalk é usado para exibir informações na Tabela de Certificados ManuBR10k. O número de série do certificado Manu pode ser correlacionado ao índice do certificado Manu, que pode ser usado para definir o estado de confiança. Os comandos e formatos específicos do SNMP dependem do dispositivo e do sistema operacional usados para

executar o comando/solicitação 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)
```

Defina o estado de confiança do certificado Manu conhecido expirado como confiável com SNMP

Valores para OID: docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5 (OID em uBR10k é 1.3.6.1.2.1.999.1.2.5.2.1.5)

1: confiável
2: não confiável
3: em cadeia
4: root

O exemplo mostra o estado de confiança alterado de encadeado para confiável para o certificado Manu com índice = 5 e número de série = 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 se o certificado Manu foi alterado com a CLI uBR10K ou com SNMP

- O valor de confiança mudou de encadeado para "Confiável"
- O valor de origem foi alterado para "SNMP", indicando que o certificado foi gerenciado pela última vez pelo SNMP e não pela Mensagem AuthInfo do 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
```

Recupere o serviço CM depois que um certificado Manu conhecido expirar

Um certificado Manu conhecido anteriormente já está presente no banco de dados uBR10K, normalmente como resultado de mensagens AuthInfo de registro CM anterior. Se um certificado Manu não estiver marcado como confiável e o certificado expirar, todos os CMs que usam o certificado Manu expirado poderão posteriormente ficar offline e tentar se registrar, mas o uBR10K marca-os reject(pk) e não estão em serviço. Esta seção descreve como se recuperar dessa condição e permite que CMs com certificados Manu expirados se registrem e permaneçam em serviço.

Identificar o número de série do certificado Manu conhecido expirado

As informações do certificado Manu para um CM travado em reject(pk) podem ser verificadas com o 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 o índice do certificado Manu conhecido expirado e defina o estado de confiança do certificado Manu como confiável

Use os mesmos comandos uBR10K CLI e SNMP conforme descrito na seção anterior para identificar o índice para o certificado Manu com base no número de série do certificado Manu. Use o número de índice do certificado Manu expirado para definir o estado confiável do certificado Manu como confiável com 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 um certificado Manu Expired desconhecido no uBR10K e Mark Trusted

Se um certificado Manu expirado não for conhecido pelo uBR10K, portanto ele não pode ser gerenciado (marcado como confiável) antes da expiração e não pode ser recuperado, o certificado Manu deve ser adicionado ao uBR10K e marcado como confiável. Essa condição acontece quando um CM que é anteriormente desconhecido e não está registrado em um uBR10K tenta se registrar com um certificado Manu desconhecido e expirado.

O certificado Manu pode ser adicionado ao uBR10K pelo SNMP Set ou pela configuração dos certificados retardados de privacidade do cabo.

Adicione um certificado Manu desconhecido expirado ao uBR10K com SNMP

Para adicionar um certificado do fabricante, adicione uma entrada à tabela docsBpi2CmtsCACertTable. Especifique esses atributos para cada entrada.

- docsBpi2CmtsCACertStatus 1.3.6.1.2.1.9999.1.2.5.2.1.7 (Defina como 4 para criar a entrada da linha)
- docsBpi2CmtsCACert = 1.3.6.1.2.1.9999.1.2.5.2.1.8 (Os dados hexadecimais, como um valor de certificado X509, para o certificado X.509 real)
- docsBpi2CmtsCACertTrust 1.3.6.1.2.1.9999.1.2.5.2.1.5 (Defina como 1 para definir o estado de confiança do certificado Manu como confiável)

A maioria dos sistemas operacionais não pode aceitar linhas de entrada que sejam o tempo necessário para inserir a string hexadecimal que especifica um certificado. Por esse motivo, recomenda-se um gerenciador de SNMP gráfico para definir esses atributos. Para vários

certificados, um arquivo de script pode ser usado, se mais conveniente.

O comando SNMP e os resultados no exemplo adicionam um certificado ASCII DER Codificado ASN.1 X.509 ao banco de dados uBR10K com parâmetros:

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

Use um número de índice exclusivo para o certificado Manu adicionado. Quando um certificado Manu expirado é adicionado, o Estado não é confiável, a menos que seja definido manualmente como confiável. Se um certificado autoassinado for adicionado, o comando **cable privacy accept-self-signed-certificate** deverá ser configurado na configuração da Interface de Cabo uBR10K antes que o uBR10K possa aceitar o certificado.

Neste exemplo, parte do conteúdo do certificado é omitido para leitura, indicado por elipse (...).

```
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)
```

Adicionar um certificado Manu expirado durante o registro CM na CLI

Um certificado Manu normalmente insere o banco de dados uBR10K pela mensagem BPI Protocol AuthInfo enviada ao uBR10K do CM. Cada certificado Manu exclusivo e válido recebido em uma mensagem AuthInfo é adicionado ao banco de dados. Se o certificado Manu for desconhecido do CMTS (não no banco de dados) e tiver expirado as datas de validade, AuthInfo será rejeitado e o certificado Manu não será adicionado ao banco de dados uBR10K. Um certificado Manu inválido pode ser adicionado ao uBR10K por AuthInfo quando a configuração alternativa **de certificados retardados de retenções de cabos** está presente na configuração da interface de cabo uBR10K. Isso permite a adição do certificado Manu expirado ao banco de dados uBR10K como inconfiável. Para usar o certificado Manu expirado, o SNMP deve ser usado para marcá-lo como confiável.

```
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
```

Quando o certificado Manu expirado é adicionado ao uBR10K e marcado como testado, a remoção da configuração **de certificados retidos com falha na privacidade do cabo** é

recomendada para evitar a adição de outros certificados Manu expirados desconhecidos no uBR10K.

Permitir certificados CM expirados e certificados Manu a serem adicionados por AuthInfo com um comando CLI uBR10K

Em alguns casos, o certificado CM expira. Para essa situação, além da configuração **de certificados de retenção de privacidade de cabo com falha**, outra configuração é necessária no uBR10K. Em cada domínio uBR10K MAC (Cable Interface) relevante, adicione a **privacidade do cabo ignore a** configuração do **período de validade** e salve a configuração. Isso faz com que o uBR10K ignore as verificações do período de validade expirado para TODOS os certificados CM e Manu enviados na mensagem 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

Consideração de configuração de interface de cabo/domínio MAC

Os certificados de retenção de privacidade do cabo com falha e os comandos de configuração do período de validade do ignorado da privacidade do cabo são usados no nível de Domínio MAC / Interface do cabo e não são restritivos. O comando reter certificados com falha pode adicionar qualquer certificado com falha ao banco de dados uBR10K e o comando skip-valid-period pode ignorar as verificações de Data de validade em todos os certificados Manu e CM.

Consideração do tamanho do pacote SNMP

Uma configuração SNMP uBR10K adicional pode ser necessária quando certificados de grande porte são usados. SNMP Get of Cert data pode ser NULL se cert OctetString for maior que o tamanho do pacote SNMP. Por exemplo;

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

Depuração de certificado Manu

Manu Cert debug no uBR10K us suportado com os comandos **debug cable privacy ca-cert** e **debug cable mac-address <cm mac-address>**. Informações adicionais de depuração são explicadas no artigo de suporte Como decodificar o certificado DOCSIS para o diagnóstico de estado de pilha de modem.

Documentação de suporte relacionada

- Modems a cabo e certificados de fabricantes prestes a expirar no boletim do produto cBR-8 -

Cisco

- Roteadores de banda larga universais Cisco uBR1000 Series
- Suporte Técnico e Documentação - Cisco Systems