Solution et récupération des certificats de fabricant expirés sur uBR10K

Contenu

[Introduction](#)
[Problème](#)
[Informations sur le certificat Manu](#)
[Champs et attributs des informations de certification Manu](#)
[Commandes CLI uBR10K](#)
[OID DOCSIS-BPI-PLUS-MIB](#)
[Solution](#)
[Mettre à jour le micrologiciel CM](#)
[Définir un certificat Manu connu sur Trusted](#)
[Afficher les nombreuses informations de certificat de l'interface de ligne de commande uBR10K](#)
[Afficher les informations de certificat Manu avec SNMP à partir d'un périphérique distant](#)
[Définir l'état d'approbation du certificat Manu connu expiré sur Trusted avec SNMP](#)
[Confirmer la modification de la certification Manu avec l'interface de ligne de commande uBR10K ou avec SNMP](#)
[Récupérer le service CM après l'expiration d'un certificat Manu connu](#)
[Identifier le numéro de série du certificat Manu connu expiré](#)
[Identifier l'index du certificat Manu connu expiré et définir l'état de confiance du certificat Manu sur Fisted](#)
[Installer un certificat Manu périmé inconnu sur le uBR10K et Mark Trusted](#)
[Ajouter un certificat Manu inconnu expiré au uBR10K avec SNMP](#)
[Ajouter un certificat Manu expiré lors de l'enregistrement de CM dans l'interface de ligne de commande](#)
[Autoriser l'ajout de certificats CM et de certificats Manu expirés par AuthInfo avec une commande CLI uBR10K](#)
[Additional Information](#)
[Examen de la configuration des interfaces de domaine/câble MAC](#)
[Prise en compte de la taille des paquets SNMP](#)
[Débogage du certificat Manu](#)
[Documentation d'assistance associée](#)

Introduction

Ce document décrit les options permettant d'empêcher, de contourner et de récupérer les impacts du service de rejet de modem câble (CM) sur le système CMTS (Cable Modem Termination System) uBR10K résultant de l'expiration du certificat de fabricant (Manu Cert).

Problème

Il existe différentes causes de blocage d'un CM dans l'état de rejet (pk) sur le uBR10K. L'une des

causes est l'expiration du certificat Manu. Le certificat Manu est utilisé pour l'authentification entre un CM et un CMTS. Dans ce document, un certificat Manu est ce que la spécification de sécurité DOCSIS 3.0 CM-SP-SECv3.0 désigne comme certificat d'autorité de certification Mfg CableLabs ou certificat d'autorité de certification Fabricant. Expire signifie que la date/heure système uBR10K dépasse la date/heure de fin de validité du certificat Manu.

Un CM qui tente de s'enregistrer auprès de l'uBR10K après l'expiration du certificat Manu est marqué comme rejeté(pk) par le CMTS et n'est pas en service. Un CM déjà enregistré avec l'uBR10K et en service lorsque le certificat Manu expire peut rester en service jusqu'à la prochaine tentative d'enregistrement du CM, qui peut se produire après un événement hors connexion de modem unique, redémarrage de la carte de ligne câblée uBR10K, rechargement de l'uBR10K ou d'autres événements déclenchant l'enregistrement du modem. À ce moment-là, le CM échoue à l'authentification, est marqué de rejet (pk) par le uBR10K et n'est pas en service.

DOCSIS 1.1 pour les routeurs CMTS Cisco fournit des informations supplémentaires sur la prise en charge et la configuration de l'interface de confidentialité de ligne de base DOCSIS (BPI+) uBR10K.

Informations sur le certificat Manu

Les informations Manu Cert peuvent être affichées via les commandes de l'interface de ligne de commande uBR10K ou le protocole SNMP (Simple Network Management Protocol). Ces commandes et informations sont utilisées par les solutions décrites dans ce document.

Champs et attributs des informations de certification Manu

- Index : Entier unique attribué à chaque certificat Manu dans la base de données/MIB uBR10K
- Objet : Nom du sujet tel qu'il est codé dans le certificat X509
  cn : NomCommunou : Unité d'organisationo : Organisationl : Localités :
  NomProvinceOuÉtatc : NomPays
- Émetteur : L'autorité de certification
- Série : Numéro de série de certificat représenté dans une chaîne d'octet hexadécimale
- Province: Statut d'approbation du certificat
  fiablenon fiableen chaîneracine
- Source : Comment le certificat a atteint le CMTS
  snmp fichierConfigurationexternalDatabaseother (autre)authentInfocompiléInfoCode
- Status/RowStatus : État du certificat
  actifnonEnServicenon prêtcreateAndGocréer et attendredétruire
- Cert : Le certificat d'autorité de certification encodé en DER X509
- Date de validité : Les dates de début et de fin qui définissent la période de validité du certificat Manu par rapport à la date et à l'heure système CMTS
  date de début : Date et heure auxquelles le certificat Manu devient validedate de fin : Date et heure auxquelles le certificat Manu n'est plus valide
- Cert : Le certificat d'autorité de certification encodé en DER X509
- Empreinte numérique : Hachage SHA-1 d'un certificat CA

Commandes CLI uBR10K

Le résultat de cette commande inclut certaines informations de certificat Manu. L'index Manu Cert ne peut être obtenu que par SNMP

- Àpartir du mode d'exécution uBR10K CLI ou du mode d'exécution CLI de la carte de ligne : uBR10K**#show cable privacy maker-cert-list**
- En mode d'exécution CLI de la carte de ligne uBR10K : Slot-6-0**#show crypto pki certificate**

Ces commandes de configuration d'interface de câble sont utilisées pour les contournements et la récupération

- uBR10K(config-if)# cable privacy keep-fail-certificate
- uBR10K(config-if)#intervalle de validité de la confidentialité des câbles

OID DOCSIS-BPI-PLUS-MIB

Les informations de certificat manu sont définies dans la branche OID docsBpi2CmtsCACertEntry 1.3.6.1.2.1.10.127.6.1.2.5.2.1, décrite dans le Navigateur d'objets SNMP.

> **Note**: Dans le logiciel uBR10k, le RFC 4131 docsBpi2MIB / DOCS-IETF-BPI2-MIB a été mis en oeuvre avec la branche/le chemin OID MIB incorrect. La plate-forme uBR10k est en fin de commercialisation et après la date de fin de prise en charge logicielle, il n'y a donc pas de solution pour ce défaut logiciel. Au lieu du chemin MIB/Branch 1.3.6.1.2.10.127.6 attendu, **le chemin MIB/Branch 1.3.6.1.2.1.9999 doit être utilisé pour les interactions SNMP avec les MIB/OID BPI2 sur le uBR10k.**
> ID de bogue Cisco associé CSCum28486

Il s'agit des équivalents de chemin complet de la MIB BPI2 pour les informations du Cert Manu sur le uBR10k, comme indiqué dans l'ID de bogue 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
```

Les exemples de commandes de ce document utilisent l'ellipse (...) pour indiquer que certaines informations ont été omises pour la lisibilité.

Solution

La mise à jour du micrologiciel CM est la meilleure solution à long terme. Les solutions de contournement qui permettent aux modems ayant des certificats Manu expirés de s'enregistrer et de rester en ligne avec le uBR10K sont décrites dans ce document, mais ces solutions de contournement ne sont recommandées que pour une utilisation à court terme. Si une mise à jour du micrologiciel CM n'est pas une option, une stratégie de remplacement CM est une bonne solution à long terme du point de vue de la sécurité et des opérations. Les solutions décrites ici traitent de conditions ou de scénarios différents et peuvent être utilisées individuellement ou, dans

certains cas, en association ;

- Mettre à jour le micrologiciel CM
- Définir un certificat Manu connu sur Trusted
- Récupérer le service CM après l'expiration d'un certificat Manu connu
- Installez un certificat Manu périmé inconnu sur le uBR10k et Mark Trusted
- Autoriser l'ajout de certificats CM et de certificats Manu expirés par AuthInfo avec une commande CLI uBR10K

Note: Si le BPI est supprimé, cela désactive le chiffrement et l'authentification, ce qui réduit la viabilité de cette solution de contournement.

Mettre à jour le micrologiciel CM

Dans de nombreux cas, les fabricants de CM fournissent des mises à jour du micrologiciel de CM qui prolongent la date de fin de validité du certificat Manu. Cette solution est la meilleure option et, lorsqu'elle est exécutée avant l'expiration d'un certificat Manu, elle prévient les impacts de services associés. Les CM chargent le nouveau micrologiciel et se réinscrivent avec les nouveaux certificats Manu et CM. Les nouveaux certificats peuvent s'authentifier correctement et les CM peuvent s'enregistrer avec le uBR10K. Le nouveau certificat Manu et le nouveau certificat CM peuvent créer une nouvelle chaîne de certificats vers le certificat racine connu déjà installé dans le uBR10K.

Définir un certificat Manu connu sur Trusted

Lorsqu'une mise à jour du micrologiciel CM n'est pas disponible en raison d'une interruption de l'activité d'un fabricant CM, de l'absence de prise en charge d'un modèle CM, etc., les certificats Manu déjà connus sur l'uBR10k avec des dates de fin de validité dans un avenir proche peuvent être marqués de manière proactive comme approuvés dans l'uBR10k avant expiration. Le numéro de série du certificat Manu, la date de fin de validité et l'état sont disponibles avec les commandes CLI uBR10K. Le numéro de série Manu Cert, l'état de confiance et l'index sont disponibles avec SNMP.

Les certificats Manu connus pour les modems actuellement en service et en ligne sont généralement acquis par le uBR10K à partir d'un CM via le protocole BPI (Baseline Privacy Interface) DOCSIS. Le message AUTH-INFO envoyé par le CM au uBR10K contient le certificat Manu. Chaque certificat Manu unique est stocké dans la mémoire uBR10K et ses informations peuvent être affichées avec les commandes CLI uBR10K et SNMP.

Lorsque le certificat Manu est marqué comme étant fiable, cela fait deux choses importantes. Tout d'abord, il permet au logiciel BPI uBR10K d'ignorer la date de validité expirée. Deuxièmement, il stocke le certificat Manu comme approuvé dans la mémoire NVRAM uBR10K. Cela préserve l'état de Cert Manu sur un rechargement uBR10K et élimine la nécessité de répéter cette procédure en cas de rechargement uBR10K

Les exemples de commandes CLI et SNMP montrent comment identifier un index de certificat Manu, un numéro de série, un état d'approbation ; ensuite, utilisez ces informations pour modifier l'état d'approbation en approuvé. Les exemples portent sur un certificat Manu avec index 5 et numéro de série 45529C2654797E1623C6E723180A9E9C.

Afficher les nombreuses informations de certificat de l'interface de ligne de commande uBR10K

Dans cet exemple, les commandes de l'interface de ligne de commande uBR10K **show crypto pki certificate** et **show cable privacy maker-cert-list** sont utilisées pour afficher les informations Manu Cert connues.

```
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
```

Afficher les informations de certificat Manu avec SNMP à partir d'un périphérique distant

OID SNMP uBR10K pertinents :

```
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
```

Dans cet exemple, la commande snmpwalk est utilisée pour afficher les informations de la table de certificats de manu uBR10k. Le numéro de série Manu Cert connu peut être corrélé à l'index

Manu Cert, qui peut être utilisé pour définir l'état d'approbation. Les commandes et formats SNMP spécifiques dépendent du périphérique et du système d'exploitation utilisés pour exécuter la commande/requête 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)
```

Définir l'état d'approbation du certificat Manu connu expiré sur Trusted avec SNMP

Valeurs pour OID : docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5 (OID sur uBR10k est 1.3.6.1.2.1.999.1.2.5.2.1.5)

1: fiable
2: non fiable
3: en chaîne
4: racine

L'exemple montre que l'état d'approbation est passé de chaîne à confiance pour le certificat Manu avec Index = 5 et Numéro 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
```

Confirmer la modification de la certification Manu avec l'interface de ligne de commande uBR10K ou avec SNMP

- La valeur d'approbation est passée de chaîne à « Fiable »

- La valeur source est passée à « SNMP », ce qui indique que le certificat a été géré pour la dernière fois par SNMP et non à partir du message AuthInfo du protocole 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
```

Récupérer le service CM après l'expiration d'un certificat Manu connu

Un certificat Manu précédemment connu est un certificat déjà présent dans la base de données uBR10K, généralement à la suite de messages AuthInfo provenant d'un enregistrement CM précédent. Si un certificat Manu n'est pas marqué comme approuvé et que le certificat expire, tous les CM qui utilisent le certificat Manu expiré peuvent par la suite se déconnecter et tenter de s'enregistrer, mais le uBR10K les marque de rejet (pk) et ils ne sont pas en service. Cette section décrit comment se rétablir de cette condition et permettre aux CM ayant des certificats Manu expirés de s'enregistrer et de rester en service.

Identifier le numéro de série du certificat Manu connu expiré

Les informations Manu Cert pour un CM coincé dans le rejet(pk) peuvent être vérifiées à l'aide de la commande 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
```

Identifier l'index du certificat Manu connu expiré et définir l'état de confiance du certificat Manu sur Fisted

Utilisez les mêmes commandes uBR10K CLI et SNMP que celles décrites dans la section précédente pour identifier l'index du certificat Manu en fonction du numéro de série du certificat Manu. Utilisez le numéro d'index du certificat manu expiré pour définir l'état d'approbation du certificat manu sur approuvé avec 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)
```

Installer un certificat Manu périmé inconnu sur le uBR10K et Mark Trusted

Dans le cas où un certificat Manu expiré n'est pas connu du uBR10K, il ne peut donc pas être géré (marqué comme approuvé) avant l'expiration et ne peut pas être récupéré, le certificat Manu doit être ajouté au uBR10K et marqué comme approuvé. Cette condition se produit lorsqu'un CM précédemment inconnu et non enregistré sur un uBR10K tente de s'enregistrer auprès d'un certificat Manu inconnu et expiré.

Le certificat Manu peut être ajouté à l'uBR10K par SNMP Set ou par la configuration des certificats de rétention de confidentialité des câbles ayant échoué.

Ajouter un certificat Manu inconnu expiré au uBR10K avec SNMP

Afin d'ajouter un certificat de fabricant, ajoutez une entrée à la table docsBpi2CmtsCACertTable. Spécifiez ces attributs pour chaque entrée.

- docsBpi2CmtsCACertStatus 1.3.6.1.2.1.999.1.2.5.2.1.7 (Défini sur 4 pour créer l'entrée de ligne)
- docsBpi2CmtsCACert = 1.3.6.1.2.1.999.1.2.5.2.1.8 (Les données hexadécimales, en tant que valeur de certificat X509, pour le certificat X.509 réel)
- docsBpi2CmtsCACertTrust 1.3.6.1.2.1.999.1.2.5.2.1.5 (Défini sur 1 pour définir l'état

d'approbation du certificat Manu sur approuvé)

La plupart des systèmes d'exploitation ne peuvent pas accepter les lignes d'entrée aussi longues que nécessaire pour entrer la chaîne hexadécimale qui spécifie un certificat. Pour cette raison, il est recommandé de configurer ces attributs à l'aide d'un gestionnaire SNMP graphique. Pour un certain nombre de certificats, un fichier de script peut être utilisé, si cela est plus pratique.

La commande SNMP et les résultats dans l'exemple ajoutent un certificat ASN.1 X.509 codé DER ASCII à la base de données uBR10K avec les paramètres suivants :

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

Utilisez un numéro d'index unique pour le certificat Manu ajouté. Lorsqu'un certificat Manu expiré est ajouté, l'état n'est pas approuvé, sauf s'il est défini manuellement sur approuvé. Si un certificat auto-signé est ajouté, la commande **cable privacy accept-self-signed-certificate** doit être configurée dans la configuration de l'interface de câble uBR10K avant que le uBR10K puisse accepter le certificat.

Dans cet exemple, une partie du contenu du certificat est omise pour la lisibilité, indiquée par 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)
```

Ajouter un certificat Manu expiré lors de l'enregistrement de CM dans l'interface de ligne de commande

Un certificat Manu entre généralement dans la base de données uBR10K par le message AuthInfo du protocole BPI envoyé au uBR10K à partir du CM. Chaque certificat Manu unique et valide reçu dans un message AuthInfo est ajouté à la base de données. Si le certificat Manu est inconnu du CMTS (non dans la base de données) et a expiré, AuthInfo est rejeté et le certificat Manu n'est pas ajouté à la base de données uBR10K. Un certificat manu non valide peut être ajouté à uBR10K par AuthInfo lorsque la configuration de contournement de **la confidentialité des câbles avec des certificats d'échec de rétention** est présente dans la configuration de l'interface de câble uBR10K. Cela permet d'ajouter le certificat Manu expiré à la base de données uBR10K comme étant sans problème. Pour utiliser le certificat Manu expiré, SNMP doit être utilisé pour le marquer comme fiable.

```
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
```

Lorsque le certificat Manu expiré est ajouté à l'uBR10K et marqué comme étant optimisé, la suppression de la configuration **de** certificats **de rétention/échec de la confidentialité des câbles** est recommandée pour empêcher l'ajout d'autres certificats Manu expirés inconnus sur l'uBR10K.

Autoriser l'ajout de certificats CM et de certificats Manu expirés par AuthInfo avec une commande CLI uBR10K

Dans certains cas, le certificat CM expire. Dans ce cas, en plus de la configuration **cable privacy keep-fail-certificate**, une autre configuration est nécessaire sur le uBR10K. Sous chaque domaine MAC uBR10K approprié (interface de câble), ajoutez la configuration **de la période de validité de l'absence de confidentialité des câbles** et enregistrez la configuration. Cela fait que le uBR10K ignore les vérifications de période de validité expirées pour TOUS les certificats CM et Manu envoyés dans le message BPI AuthInfo de CM.

```
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

Examen de la configuration des interfaces de domaine/câble MAC

Les commandes de configuration de la période de validité/rétention de la confidentialité des câbles et de la période de non-validité de la confidentialité des câbles sont utilisées au niveau du domaine MAC/de l'interface du câble et ne sont pas restrictives. La commande keep-fail-certificate peut ajouter n'importe quel certificat ayant échoué à la base de données uBR10K et la commande skip-validité-période peut ignorer les vérifications de date de validité sur tous les certificats Manu et CM.

Prise en compte de la taille des paquets SNMP

Une configuration SNMP uBR10K supplémentaire peut être nécessaire lorsque des certificats de grande taille sont utilisés. SNMP Get of Cert peut être NULL si le cert OctetString est supérieur à la taille de paquet SNMP. Exemple ;

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

Débogage du certificat Manu

Manu Cert debug sur uBR10K us pris en charge avec les commandes **debug cable privacy ca-cert** et **debug cable mac-address <cm mac-address>**. Des informations de débogage supplémentaires

sont expliquées dans l'article de support How to Decode DOCSIS Certificate for Modem Stuck State Diagnosis.

Documentation d'assistance associée

- Modems câble et certificats de fabricant arrivant à expiration sur le bulletin de produit cBR-8 - Cisco
- Routeurs haut débit universels de la gamme Cisco uBR10000
- Support et documentation techniques - Cisco Systems