해결 방법 및 uBR10K에서 만료된 제조업체 인증서 복구

목차

소개

이 문서에서는 제조업체 인증서(Manu Cert) 만료로 인한 uBR10K CMTS(Cable Modem Termination System)에 대한 CM(케이블 모뎀 거부) 서비스 영향을 방지, 해결 방법 및 복구하는 옵션에 대해 설명합니다.

문제

uBR10K에서 CM이 reject(pk) 상태로 고정되는 데에는 다른 원인이 있습니다. 한 가지 원인은 Manu Cert의 만료입니다. Manu Cert는 CM과 CMTS 간의 인증에 사용됩니다. 이 문서에서 Manu Cert는 DOCSIS 3.0 Security Specification CM-SP-SECv3.0이 CableLabs Mfg CA 인증서 또는 제조업체

CA 인증서라고 하는 것입니다. 만료는 uBR10K 시스템 날짜/시간이 Manu Cert 유효 종료 날짜/시간을 초과함을 의미합니다.

Manu Cert가 만료된 후 uBR10K에 등록하려고 시도하는 CM은 CMTS에 의해 reject(pk)로 표시되고 서비스가 제공되지 않습니다. uBR10K에 이미 등록되어 있고 Manu Cert가 만료될 때 서비스 중인 CM은 다음 번에 CM이 등록을 시도할 때까지 서비스 상태를 유지할 수 있습니다. 단 하나의 모뎀 오프라인 이벤트, uBR10K Cable Linecard 재시작, uBR10K 다시 로드 또는 모뎀 등록을 트리거하는 기타 이벤트가 발생할 수 있습니다. 그 때 CM이 인증에 실패하는 경우 uBR10K에 의해 reject(pk)로 표시되고 서비스가 제공되지 않습니다.

Cisco CMTS 라우터용 DOCSIS 1.1에서는 uBR10K 지원 및 DOCSIS BPI+(Baseline Privacy Interface) 구성에 대한 추가 정보를 제공합니다.

Manu 인증서 정보

Manu Cert 정보는 uBR10K CLI 명령 또는 SNMP(Simple Network Management Protocol)를 통해 볼 수 있습니다. 이러한 명령과 정보는 이 문서에 설명된 솔루션에 의해 사용됩니다.

Manu 인증서 정보 필드 및 특성

- 인덱스: uBR10K 데이터베이스/MIB의 각 Manu 인증서에 할당된 고유 정수
- 제목: X509 인증서에 인코딩된 것과 정확히 동일한 주체 이름
  cn: 공용 이름ou: 조직 단위o: 조직l: 구/군/시s: 주/도 이름c: 국가 이름
- 발급자: 인증 기관
- 일련 번호: 16진수 8진수 문자열로 표시되는 인증서 일련 번호
- 상태: 인증서의 신뢰 상태
  신뢰신뢰회사슬로루트
- 출처: 인증서가 CMTS에 도달하는 방법
  snmp구성 파일외부 데이터베이스기타인증 정보컴파일된 정보 코드
- 상태/행 상태: 인증서 상태
  활성서비스 안 함준비 안 됨만들기 및 이동생성 및 대기파괴
- 인증서: X509 DER 인코딩 인증 기관 인증서
- 유효 날짜: CMTS 시스템 날짜 및 시간을 기준으로 Manu Cert 유효 기간을 정의하는 시작 및 종료 날짜
  시작 날짜: Manu Cert 가 유효한 날짜 및 시간종료 날짜: Manu 인증서가 더 이상 유효하지 않은 날짜 및 시간
- 인증서: X509 DER 인코딩 인증 기관 인증서
- 지문: CA 인증서의 SHA-1 해시

uBR10K CLI 명령

이 명령의 출력에는 일부 Manu Cert 정보가 포함됩니다. Manu Cert 인덱스는 SNMP에서만 얻을 수 있습니다.

- uBR10K CLI exec 모드 또는 Linecard CLI exec 모드에서 다음을 수행합니다. uBR10K**#show cable privacy manufacturer-cert-list**
- uBR10K Linecard CLI exec 모드에서: Slot-6-0**#show crypto pki certificates**

이러한 케이블 인터페이스 컨피그레이션 명령은 해결 및 복구에 사용됩니다.

- uBR10K(config-if)#cable privacy retain-failed-certificates
- uBR10K(config-if)#cable privacy skip-validity-period

DOCSIS-BPI-PLUS-MIB OID

Manu Cert 정보는 docsBpi2CmtsCACertEntry OID 분기 1.3.6.1.2.10.127.6.1.2.5.2.1에서 정의되며 SNMP Object Navigator에 설명되어 있습니다.

> **참고:** uBR10k 소프트웨어에서 RFC 4131 docsBpi2MIB / DOCS-IETF-BPI2-MIB는 잘못된 OID MIB 지사/경로로 구현되었습니다. uBR10k 플랫폼은 판매가 종료되고 소프트웨어 지원 종료일이 지난 상태이므로 이 소프트웨어 결함에 대한 수정 사항은 없습니다. 예상 MIB 경로/브랜치 1.3.6.1.2.10.127.6 대신 **uBR10k에서 BPI2 MIB/OID와의 SNMP 상호 작용에 MIB 경로/브랜치 1.3.6.1.2.1.9999을 사용해야 합니다.**
> 관련 Cisco 버그 ID CSCum28486

다음은 Cisco 버그 ID CSCum28486에 설명된 대로 uBR10k의 Manu Cert 정보에 대한 BPI2 MIB OID 전체 경로 등가입니다.

```
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
```

이 문서의 명령 예제에서는 생략 부호(...)를 사용하여 가독성을 위해 일부 정보가 생략되었음을 나타냅니다.

솔루션

CM 펌웨어 업데이트는 가장 장기적인 솔루션입니다. 이 문서에서는 만료된 Manu Certs가 있는 CM이 등록하고 uBR10K에 온라인으로 유지되도록 하는 방법에 대해 설명하지만 이러한 해결 방법은 단기간 사용에만 권장됩니다. CM 펌웨어 업데이트가 옵션이 아닌 경우 CM 교체 전략은 보안 및 운영 측면에서 좋은 장기적 솔루션입니다. 여기에서 설명하는 솔루션은 다양한 조건이나 시나리오를 다루며 개별적으로 또는 서로 조합하여 사용할 수 있습니다.

- CM 펌웨어 업데이트
- 알려진 Manu Cert를 Trusted로 설정
- 알려진 Manu 인증서가 만료된 후 CM 서비스 복구
- uBR10k에 Unknown Expired Manu Cert 설치 및 Mark Trusted
- uBR10K CLI 명령을 사용하여 AuthInfo에서 만료된 CM 인증서 및 Manu 인증서 추가 허용

> **참고:** BPI가 제거되면 암호화 및 인증이 비활성화되어 해결 방법으로 그 실행 가능성을 최소화합니다.

CM 펌웨어 업데이트

대부분의 경우 CM 제조업체는 Manu Cert의 유효 종료 날짜를 연장하는 CM 펌웨어 업데이트를 제공합니다. 이 솔루션은 최상의 선택이며, Manu Cert가 만료되기 전에 수행할 경우 관련 서비스에 영향을 주지 않습니다. CM은 새 펌웨어를 로드하고 새 Manu Certs 및 CM Certs에 다시 등록합니다. 새 인증서는 제대로 인증되고 CM은 uBR10K에 성공적으로 등록할 수 있습니다. 새 Manu Cert 및 CM Cert는 uBR10K에 이미 설치된 알려진 루트 인증서로 새 인증서 체인을 다시 생성할 수 있습니다.

알려진 Manu Cert를 Trusted로 설정

CM 제조업체가 폐업하거나 CM 모델에 대한 추가 지원이 없는 등의 이유로 CM 펌웨어 업데이트를 사용할 수 없는 경우, 곧 유효 종료 날짜가 가까운 uBR10k에 이미 알려진 Manu Certs는 만료 전에 미리 uBR10k에서 신뢰할 수 있는 것으로 표시될 수 있습니다. Manu Cert 일련 번호, 유효 종료 날짜 및 상태는 uBR10K CLI 명령에서 확인할 수 있습니다. SNMP를 통해 Manu Cert 일련 번호, Trust State 및 인덱스를 찾을 수 있습니다.

현재 사용 중인 모뎀 및 온라인 모뎀에 대해 알려진 Manu Certs는 일반적으로 uBR10K에서 DOCSIS BPI(Baseline Privacy Interface) 프로토콜을 통해 CM에서 학습합니다. CM에서 uBR10K로 전송된 AUTH-INFO 메시지에는 Manu Cert가 포함되어 있습니다. 각 고유한 Manu Cert는 uBR10K 메모리에 저장되며 해당 정보는 uBR10K CLI 명령 및 SNMP를 통해 볼 수 있습니다.

Manu Cert가 신뢰할 수 있는 것으로 표시되면 두 가지 중요한 작업을 수행합니다. 먼저 uBR10K BPI 소프트웨어가 만료된 유효 날짜를 무시할 수 있습니다. 둘째, Manu Cert를 uBR10K NVRAM에 신뢰할 수 있는 인증서로 저장합니다. 이렇게 하면 uBR10K 다시 로드에서 Manu Cert 상태가 유지되며 uBR10K 다시 로드될 경우 이 절차를 반복할 필요가 없습니다

CLI 및 SNMP 명령 예는 Manu Cert 인덱스, 일련 번호, 신뢰 상태를 식별하는 방법을 보여줍니다. 그런 다음 해당 정보를 사용하여 신뢰 상태를 신뢰할 수 있는 상태로 변경합니다. 이 예제는 인덱스 5 및 일련 번호 45529C2654797E1623C6E723180A9E9C가 있는 Manu Cert에 중점을 둡니다.

uBR10K CLI에서 여러 인증서 정보 보기

이 예에서 uBR10K CLI 명령은 crypto pki **certificates** 및 **show cable privacy manu manu cert-list**를 사용하여 알려진 Manu Cert 정보를 확인합니다.

```
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
```

원격 디바이스에서 SNMP를 사용하여 Manu Cert 정보 보기

관련 uBR10K SNMP OID:

```
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
```

이 예에서 snmpwalk 명령은 uBR10k Manu Cert Table의 정보를 보는 데 사용됩니다. 알려진 Manu Cert 일련 번호는 신뢰 상태를 설정하는 데 사용할 수 있는 Manu Cert Index와 상호 연결될 수 있습니다. 특정 SNMP 명령 및 형식은 SNMP 명령/요청을 실행하는 데 사용되는 디바이스 및 운영 체제에 따라 달라집니다.

```
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)
```

Expired Known Manu Cert Trust State(만료된 알려진 Manu 인증서 신뢰 상태)를 Trusted with SNMP로 설정

OID 값: docsBpi2CmtsCACertTrust 1.3.6.1.2.1.10.127.6.1.2.5.2.1.5(uBR10k의 OID는 1.3.6.1.2.1.9999.1.2.5.2.1.5)

1: 신뢰
2: 신뢰
3: 쇠사슬로
4: 루트

이 예에서는 Index = 5 및 Serial Number = 45529C2654797E1623C6E723180A9E9C와 함께 신뢰 상태를 신뢰 상태로 체인으로 변경한 것을 보여줍니다.

```
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
```

uBR10K CLI 또는 SNMP를 사용하여 변경된 Manu Cert 확인

- 신뢰 값이 chained에서 "Trusted"로 변경되었습니다.
- 소스 값이 "SNMP"로 변경되었습니다. 이는 인증서가 BPI 프로토콜 인증 정보 메시지에서가 아니라 SNMP에서 마지막으로 관리되었음을 나타냅니다.

```
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
```

알려진 Manu 인증서가 만료된 후 CM 서비스 복구

이전에 알려진 Manu Cert는 uBR10K 데이터베이스에 이미 있는 인증서로서, 일반적으로 이전 CM 등록에서 AuthInfo 메시지를 수신한 것입니다. Manu Cert가 신뢰할 수 있는 것으로 표시되지 않고 인증서가 만료되면 만료된 Manu Cert를 사용하는 모든 CM은 나중에 오프라인으로 전환하여 등록을 시도할 수 있지만 uBR10K는 거부(pk)로 표시하고 서비스가 제공되지 않습니다. 이 섹션에서는 이 상태에서 복구하는 방법과 만료된 Manu Certs가 있는 CM이 등록되고 서비스 상태로 유지되는 방법에 대해 설명합니다.

만료된 알려진 Manu 인증서 일련 번호 식별

reject(pk)에 걸린 CM의 Manu Cert 정보는 uBR10K CLI 명령 **show cable modem <CM MAC Address> privacy**를 사용하여 확인할 수 있습니다.

```
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
```

만료된 알려진 Manu 인증서에 대한 인덱스를 식별하고 Manu Cert Trust State를 Trusted(신뢰할 수 있음)로 설정합니다.

이전 섹션에서 설명한 것과 동일한 uBR10K CLI 및 SNMP 명령을 사용하여 Manu Cert 일련 번호를 기반으로 Manu Cert의 인덱스를 식별합니다. 만료된 Manu Cert 인덱스 번호를 사용하여 Manu Cert 신뢰 상태를 SNMP로 신뢰하도록 설정합니다.

```
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)
```

uBR10K에 Unknown Expired Manu Cert 설치 및 Mark Trusted

만료된 Manu Cert를 uBR10K에서 알 수 없으므로 만료 전에 관리(신뢰할 수 있는 것으로 표시)할 수 없으며 복구할 수 없는 경우 Manu Cert를 uBR10K에 추가하고 trusted로 표시해야 합니다. 이 상태는 이전에는 알 수 없고 uBR10K에 등록되지 않은 CM이 알 수 없고 만료된 Manu Cert로 등록을 시도할 때 발생합니다.

SNMP 세트 또는 케이블 프라이버시 유지-실패 인증서 컨피그레이션을 통해 uBR10K에 Manu 인증서를 추가할 수 있습니다.

SNMP를 사용하여 uBR10K에 만료된 알 수 없는 Manu 인증서 추가

제조업체의 인증서를 추가하려면 docsBpi2CmtsCACertTable 테이블에 항목을 추가합니다. 각 항목에 대해 이러한 특성을 지정합니다.

- docsBpi2CmtsCACertStatus 1.3.6.1.2.1.9999.1.2.5.2.1.7(행 항목을 만들려면 4로 설정)
- docsBpi2CmtsCACert = 1.3.6.1.2.1.9999.1.2.5.2.1.8(실제 X.509 인증서의 X509 인증서 값으로 16진수 데이터)
- docsBpi2CmtsCACertTrust 1.3.6.1.2.1.9999.1.2.5.2.1.5(Manu Cert Trust 상태를 트러스트됨으로 설정하려면 1로 설정)

대부분의 운영 체제에서는 인증서를 지정하는 16진수 문자열을 입력하는 데 필요한 만큼 긴 입력 라인을 사용할 수 없습니다. 따라서 이러한 특성을 설정하는 데 그래픽 SNMP 관리자를 사용하는 것이 좋습니다. 여러 인증서의 경우 더 편리한 경우 스크립트 파일을 사용할 수 있습니다.

SNMP 명령 및 예제의 결과는 다음과 같은 매개변수를 사용하여 uBR10K 데이터베이스에 ASCII DER Encoded ASN.1 X.509 인증서를 추가합니다.

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

추가된 Manu Cert에 고유한 인덱스 번호를 사용합니다. 만료된 Manu Cert가 추가되면 수동으로 Trusted로 설정하지 않는 한 상태가 신뢰할 수 없습니다. 자체 서명 인증서가 추가된 경우 uBR10K가 인증서를 수락하려면 먼저 uBR10K Cable Interface 컨피그레이션에 **cable privacy accept-self-signed-certificate** 명령을 구성해야 합니다.

이 예에서 인증서 내용 중 일부는 읽기 용이성을 위해 생략되며, elipsis(...)로 표시됩니다.

```
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)
```

CLI에서 CM 등록 중에 만료된 Manu 인증서 추가

Manu Cert는 일반적으로 CM에서 uBR10K로 전송된 BPI 프로토콜 AuthInfo 메시지를 통해 uBR10K 데이터베이스에 들어갑니다. AuthInfo 메시지에서 받은 고유하고 유효한 Manu Cert가 데이터베이스에 추가됩니다. 데이터베이스에 없는 CMTS에서 Manu Cert를 알 수 없고 유효 날짜가 만료된 경우 AuthInfo가 거부되고 Manu Cert가 uBR10K 데이터베이스에 추가되지 않습니다. uBR10K 케이블 인터페이스 컨피그레이션 아래에 **케이블 프라이버시** retain-**failed-certificates** 해결 방법 컨피그레이션이 있는 경우 AuthInfo를 통해 Invalid Manu Cert를 uBR10K에 추가할 수 있습니다. 이렇게 하면 만료된 Manu 인증서를 uBR10K 데이터베이스에 신뢰할 수 없는 상태로 추가할 수 있습니다. 만료된 Manu Cert를 사용하려면 SNMP를 사용하여 신뢰할 수 있는 것으로 표시해야 합니다.

```
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
```

만료된 Manu Cert가 uBR10K에 추가되고 트러스트된 것으로 표시된 경우 uBR10K에서 알려지지 않은 다른 만료된 Manu Certs를 추가하지 못하도록 **케이블 프라이버시 보존-실패 인증서** 컨피그레이션을 제거하는 것이 좋습니다.

uBR10K CLI 명령을 사용하여 AuthInfo에서 만료된 CM 인증서 및 Manu 인증서 추가 허용

경우에 따라 CM 인증서가 만료됩니다. 이러한 경우 **케이블 프라이버시** retain-**failed-certificates 컨피그레이션** 외에도 uBR10K에 다른 컨피그레이션이 필요합니다. 각 관련 uBR10K MAC 도메인(케이블 인터페이스)에서 **케이블 프라이버시 생략 유효 기간** 컨피그레이션을 추가하고 컨피그레이션을 저장합니다. 이로 인해 uBR10K는 CM BPI AuthInfo 메시지에 전송된 모든 CM 및 Manu Certs에 대한 만료된 유효성 검사를 무시합니다.

```
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
```

추가 정보

MAC 도메인/케이블 인터페이스 컨피그레이션 고려 사항

케이블 privacy retain-failed-certificates 및 cable privacy skip-validity-period 컨피그레이션 명령은 MAC Domain/Cable Interface 레벨에서 사용되며 제한적이지 않습니다. retain-failed-certificates 명령은 실패한 모든 인증서를 uBR10K 데이터베이스에 추가할 수 있으며 skip-validity-period 명령은 모든 Manu 및 CM 인증서에 대한 유효성 검사를 건너뛸 수 있습니다.

SNMP 패킷 크기 고려 사항

대용량 인증서를 사용할 경우 추가 uBR10K SNMP 컨피그레이션이 필요할 수 있습니다. 인증서 OctetString이 SNMP 패킷 크기보다 큰 경우 SNMP Get of Cert 데이터는 NULL일 수 있습니다. 예를 들어

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

Manu 인증서 디버그

uBR10K의 Manu Cert debug 는 **debug cable privacy ca-cert** 및 **debug cable mac-address <cm mac-address>** 명령**으로** 지원됩니다. 추가 디버그 정보는 지원 문서 모뎀 장애 상태 진단을 위한 DOCSIS 인증서를 디코딩하는 방법에 설명되어 있습니다.

관련 지원 문서

- cBR-8 제품 게시판의 케이블 모뎀 및 만료 예정 제조업체 인증서 - Cisco
- Cisco uBR1000 Series Universal Broadband Router
- 기술 지원 및 문서 – Cisco Systems