

# Cisco CMTS의 DOCSIS 1.0 기본 프라이버시

## 목차

[소개](#)

[시작하기 전에](#)

[표기 규칙](#)

[사전 요구 사항](#)

[사용되는 구성 요소](#)

[케이블 모뎀의 기본 프라이버시 구성 방법](#)

[케이블 모뎀에서 기본 프라이버시를 사용하고 있는지 확인하는 방법](#)

[기본 프라이버시 설정 및 유지에 영향을 주는 타이머](#)

[KEK 수명](#)

[KEK 유예 시간](#)

[TEK 수명](#)

[TEK 유예 시간](#)

[권한 부여 대기 시간 초과](#)

[다시 권한 부여 대기 시간 초과](#)

[권한 부여 유예 시간 초과](#)

[승인 거부 대기 시간 초과](#)

[작동 대기 시간 초과](#)

[키 재설정 대기 시간 초과](#)

[Cisco CMTS 기본 프라이버시 구성 명령](#)

[케이블 프라이버시](#)

[케이블 프라이버시 필수](#)

[케이블 프라이버시 인증 모뎀](#)

[BPI 상태를 모니터링하는 데 사용되는 명령](#)

[BPI 문제 해결](#)

[특수 메모 - 숨겨진 명령](#)

[관련 정보](#)

## 소개

DOCSIS(Data-over-Cable Service Interface Specifications) BPI(Baseline Privacy Interface)의 주요 목표는 케이블 네트워크를 통해 데이터 모뎀으로 주고받는 데이터를 보호하는 간단한 데이터 암호화 체계를 제공하는 것입니다. 또한 기본 프라이버시는 케이블 모뎀을 인증하고 케이블 모뎀에 멀티캐스트 트래픽 전송을 승인하는 수단으로 사용될 수 있습니다.

Cisco CMTS(Cable Modem Termination System) 및 케이블 모뎀 제품으로 "k1" 또는 "k8" 문자를 포함한 기능 세트가 포함된 Cisco IOS® 소프트웨어 이미지를 실행 중입니다. 예를 들어 ubr7200-k1p-mz.121-6.EC1.bin과 같이 기본 프라이버시를 지원합니다.

이 문서에서는 DOCSIS1.0 모드에서 작동하는 Cisco 제품의 기본 프라이버시에 대해 설명합니다.

# 시작하기 전에

## 표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙](#)을 참조하십시오.

## 사전 요구 사항

이 문서에 대한 특정 요건이 없습니다.

## 사용되는 구성 요소

이 문서의 정보는 Cisco IOS® Software Release 12.1(6)EC를 실행하는 uBR7246VXR를 구성하는 것에 기반하지만 다른 모든 Cisco CMTS 제품 및 소프트웨어 릴리스에 적용됩니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 라이브 네트워크에서 작업하는 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

## 케이블 모뎀의 기본 프라이버시 구성 방법

케이블 모뎀은 DOCSIS 컨피그레이션 파일의 서비스 클래스 매개변수를 통해 기본 프라이버시를 사용하도록 명령받은 경우에만 기본 프라이버시를 사용합니다. DOCSIS 컨피그레이션 파일에는 모뎀에 대한 운영 매개변수가 포함되어 있으며, 온라인 프로세스를 진행하는 과정에서 TFTP를 통해 다운로드됩니다.

DOCSIS 구성 파일을 만드는 방법 중 하나는 Cisco.com에서 DOCSIS Cable Modem Configurator를 사용하는 것입니다. DOCSIS Cable Modem Configurator를 사용하여 Class of Service(서비스 클래스) 탭 아래의 Baseline Privacy Enable(기본 프라이버시 활성화) 필드를 On(켜기)으로 설정하여 케이블 모뎀에서 Baseline Privacy(기본 프라이버시)를 사용하도록 명령하는 DOCSIS 구성 파일을 만들 수 있습니다. 아래 예를 참조하십시오.

**3 Class of Service** Previous Next Help

Class ID

Maximum Downstream Rate (bps)

Maximum Upstream Rate (bps)

Upstream Channel Priority

Guaranteed Minimum Upstream Rate (bps)

Maximum Upstream Transmit Burst (bytes)

Baseline Privacy Enable

To save entries, click the OK button to the right after completing the **required fields**.

OK Cancel

또는 다음에서 DOCSIS 파일 구성의 독립형 버전을 사용하여 기본 프라이버시를 활성화할 수 있습니다.

Baseline Privacy CPE Software Upgrade Telephone Return Miscellaneous

RF Info Class of Service Vendor Info SNMP

Class of Service

Class ID	Max DS Rate	Max US Rate	US Chan...	Guarante...	Max US Tr...	Baseline Privacy Enable
1	3000000	512000				1

Ok Cancel Help

BPI를 지원하는 DOCSIS 구성 파일이 생성되면 새 구성 파일을 다운로드하고 이후에 기본 프라이버시를 사용하기 위해 케이블 모뎀을 재설정해야 합니다.

## [케이블 모뎀에서 기본 프라이버시를 사용하고 있는지 확인하는 방법](#)

Cisco CMTS에서는 [show cable modem](#) 명령을 사용하여 개별 케이블 모뎀의 상태를 볼 수 있습니다. 베이스라인 프라이버시를 사용하는 모뎀이 나타날 수 있는 몇 가지 상태가 있습니다.

## 온라인

케이블 모뎀이 Cisco CMTS에 등록되면 온라인 상태가 됩니다. 케이블 모뎀이 Cisco CMTS와 기본 프라이버시 매개변수를 협상하려면 먼저 이 상태로 전환해야 합니다. 이 시점에서 케이블 모뎀과 CMTS 간에 전송되는 데이터 트래픽은 암호화되지 않습니다. 케이블 모뎀이 이 상태로 남아 있고 아래에 언급된 상태로 진행되지 않으면 모뎀에서 베이스라인 프라이버시를 사용하지 않습니다.

## 온라인(pk)

온라인(pk) 상태는 케이블 모뎀이 Cisco CMTS와 인증 키(KEK(Key Encryption Key))를 협상할 수 있었다는 의미입니다. 즉, 케이블 모뎀은 기본 프라이버시를 사용할 수 있는 권한이 있으며 기본 프라이버시의 첫 번째 단계를 협상하는 데 성공했습니다. KEK는 후속 기본 개인 정보 보호 협상을 보호하는 데 사용되는 56비트 키입니다. 모뎀이 케이블 모뎀과 Cisco CMTS 간에 전송되는 온라인(pk) 상태 데이터 트래픽에 있는 경우 데이터 트래픽의 암호화를 위한 키가 아직 협상되지 않았으므로 여전히 암호화되지 않습니다. 일반적으로 온라인(pk) 뒤에 [온라인\(pt\)](#)이 옵니다.

## reject(pk)

이 상태는 케이블 모뎀이 KEK를 협상하려는 시도가 실패했음을 나타냅니다. 모뎀이 이 이 상태에 있는 가장 일반적인 이유는 Cisco CMTS가 모뎀 인증을 켜고 모뎀이 인증에 실패했기 때문입니다.

## 온라인(pt)

이 시점에서 모뎀은 Cisco CMTS와 TEK(Traffic Encryption Key)을 성공적으로 협상했습니다. TEK은 케이블 모뎀과 Cisco CMTS 간의 데이터 트래픽을 암호화하는 데 사용됩니다. TEK 협상 프로세스는 KEK를 사용하여 암호화됩니다. TEK은 케이블 모뎀과 Cisco CMTS 간의 데이터 트래픽을 암호화하는 데 사용되는 56비트 또는 40비트 키입니다. 이 시점에서는 기본 프라이버시가 성공적으로 설정되고 실행되므로 Cisco CMTS와 케이블 모뎀 간에 전송되는 사용자 데이터가 암호화됩니다.

## 거부(pt)

이 상태는 케이블 모뎀이 Cisco CMTS와 TEK을 협상할 수 없음을 나타냅니다.

베이스라인 프라이버시와 관련된 다양한 상태의 케이블 모뎀을 보여주는 show cable modem 명령의 샘플 출력은 아래를 참조하십시오.

```
CMTS# show cable modem
Interface      Prim Online      Timing Rec      QoS CPE IP address      MAC address
  Sid  State      Offset Power
Cable3/0/U1 1      online(pt) 2208    0.75    7    0    10.1.1.40      0020.4001.5370
Cable3/0/U1 2      online(pk) 2213    0.50    5    0    10.1.1.33      0050.7366.1fb9
Cable3/0/U0 3      online(pt) 2738    0.00    5    0    10.1.1.24      0002.fdfa.0a35
Cable3/0/U1 4      reject(pk) 2738    1.00    5    0    10.1.1.30      0001.9659.4447
```

참고: 케이블 모뎀 상태에 대한 자세한 내용은 [Troubleshooting uBR Cable Modem Not Coming Online](#)을 참조하십시오.

# 기본 프라이버시 설정 및 유지에 영향을 주는 타이머

특정 시간 초과 값을 수정하여 기존 요소 프라이버시의 동작을 변경할 수 있습니다. 이러한 매개변수 중 일부는 Cisco CMTS에서, 나머지는 DOCSIS 구성 파일을 통해 구성할 수 있습니다. KEK 수명 및 TEK 수명을 제외하고 이러한 매개변수를 변경할 이유는 거의 없습니다. 이러한 타이머는 케이블 플랜트의 보안을 강화하거나 BPI 관리로 인한 CPU 및 트래픽 오버헤드를 줄이기 위해 수정할 수 있습니다.

## KEK 수명

KEK 수명은 케이블 모뎀과 Cisco CMTS가 협상된 KEK가 유효하다고 간주해야 하는 시간입니다. 이 시간이 지나기 전에 케이블 모뎀은 Cisco CMTS와 새 KEK를 재협상해야 합니다.

Cisco CMTS 케이블 인터페이스 명령을 사용하여 이 시간을 구성할 수 있습니다.

```
cable privacy kek life-time 300-6048000 seconds
```

기본 설정은 7일과 같은 604800초입니다.

KEK 수명이 더 작으면 각 KEK가 더 짧은 기간 동안 지속되므로 KEK가 더 적게 해킹될 경우 KEK 협상이 납치될 가능성이 적기 때문에 보안을 강화됩니다. 이에 대한 단점은 KEK 재협상이 케이블 모뎀의 CPU 사용률을 높이고 케이블 플랜트의 BPI 관리 트래픽을 증가시킨다는 것입니다.

## KEK 유예 시간

KEK 유예 시간은 케이블 모뎀이 새 KEK를 위해 Cisco CMTS와 협상을 시작하기 위해 KEK 수명이 만료되기 전 시간입니다. 이 타이머의 배후에는 케이블 모뎀이 만료되기 전에 KEK를 갱신하는 데 충분한 시간이 있을 수 있습니다.

Cisco CMTS 케이블 인터페이스 명령을 사용하여 이 시간을 구성할 수 있습니다.

```
cable privacy kek grace-time 60-1800 seconds
```

또한 Baseline Privacy(기본 요소 프라이버시) 탭 아래의 Authorization Grace Timeout(권한 부여 유예 시간 초과)이라는 필드를 입력하여 DOCSIS 구성 파일을 사용하여 이 시간을 구성할 수 있습니다. 이 DOCSIS 컨피그레이션 파일 필드가 채워지면 Cisco CMTS에 구성된 모든 값보다 우선합니다. 이 타이머의 기본값은 600초이며, 이는 10분입니다.

## TEK 수명

TEK 수명은 케이블 모뎀과 Cisco CMTS가 협상된 TEK이 유효하다고 간주해야 하는 시간입니다. 이 시간이 지나기 전에 케이블 모뎀은 Cisco CMTS와 새 TEK을 재협상해야 합니다.

Cisco CMTS 케이블 인터페이스 명령을 사용하여 이 시간을 구성할 수 있습니다.

`cable privacy tek life-time <180-604800 seconds>`

기본 설정은 43200초이며 이는 12시간과 같습니다.

TEK의 수명이 더 짧으면 각 TEK의 지속 시간이 단축되므로 TEK에서 해킹된 데이터가 더 적으면 무단 암호 해독에 노출될 수 있기 때문에 보안이 강화됩니다. 이에 대한 단점은 TEK 재협상이 케이블 모뎀에서 CPU 사용률을 높이고 케이블 플랜트에서 BPI 관리 트래픽을 증가시킨다는 것입니다.

## TEK 유예 시간

TEK 유예 시간은 TEK 수명이 만료되기 전에 케이블 모뎀이 Cisco CMTS와 새 TEK에 대한 협상을 시작하려는 시간입니다. 이 타이머의 배후에 있는 생각은 케이블 모뎀이 만료되기 전에 TEK을 갱신할 수 있는 충분한 시간을 갖는다는 것입니다.

Cisco CMTS 케이블 인터페이스 명령을 사용하여 이 시간을 구성할 수 있습니다.

`cable privacy tek grace-time 60-1800 seconds`

Baseline Privacy(기본 정보) 탭 아래의 TEK Grace Timeout(TEK 유예 시간 초과)이라는 필드를 입력하여 DOCSIS 구성 파일을 사용하여 이 시간을 구성할 수도 있습니다. 이 DOCSIS 컨피그레이션 파일 필드가 채워지면 Cisco CMTS에 구성된 모든 값보다 우선합니다.

이 타이머의 기본값은 600초이며, 이는 10분입니다.

## 권한 부여 대기 시간 초과

이 시간은 케이블 모뎀이 처음으로 KEK를 협상할 때 Cisco CMTS의 응답을 기다리는 시간을 제어합니다.

Baseline Privacy 탭 아래의 Authorize Wait Timeout 필드를 수정하여 DOCSIS 구성 파일에서 이 시간을 구성할 수 있습니다.

이 필드의 기본값은 10초이며 유효한 범위는 2~30초입니다.

## 다시 권한 부여 대기 시간 초과

이 시간은 KEK 수명이 곧 만료되기 때문에 케이블 모뎀이 새 KEK를 협상할 때 Cisco CMTS의 응답을 기다리는 시간을 제어합니다.

Baseline Privacy 탭 아래의 Reauthorize Wait Timeout(대기 시간 제한 재승인) 필드를 수정하여 DOCSIS 구성 파일에서 이 시간을 구성할 수 있습니다.

이 타이머의 기본값은 10초이며 유효한 범위는 2~30초입니다.

## 권한 부여 유예 시간 초과

재인증을 위한 유예 기간(초)을 지정합니다. 기본값은 600입니다. 유효한 범위는 1~1800초입니다.

## 승인 거부 대기 시간 초과

케이블 모뎀이 Cisco CMTS와 KEK를 협상하려고 하지만 거부되면 Authorize Reject Wait Timeout(거부 대기 시간 제한 승인)을 기다렸다가 새 KEK를 협상해야 합니다.

Baseline Privacy 탭 아래의 Authorize Reject Wait Timeout(거부 대기 시간 초과 권한 부여) 필드를 사용하여 DOCSIS 구성 파일에서 이 매개변수를 구성할 수 있습니다. 이 타이머의 기본값은 60초이며 유효한 범위는 10초~600초입니다.

## 작동 대기 시간 초과

이 시간은 케이블 모뎀이 처음으로 TEK을 협상할 때 Cisco CMTS의 응답을 기다리는 시간을 제어합니다.

Baseline Privacy 탭 아래의 Operational Wait Timeout 필드를 수정하여 DOCSIS 구성 파일에서 이 시간을 구성할 수 있습니다.

이 필드의 기본값은 1초이며 유효한 범위는 1~10초입니다.

## 키 재설정 대기 시간 초과

이 시간은 TEK 수명이 곧 만료되기 때문에 케이블 모뎀이 새 TEK을 협상할 때 Cisco CMTS의 응답을 기다리는 시간을 제어합니다.

Baseline Privacy 탭 아래의 Rekey Wait Timeout 필드를 수정하여 DOCSIS 구성 파일에서 이 시간을 구성할 수 있습니다.

이 타이머의 기본값은 1초이며 유효한 범위는 1~10초입니다.

## Cisco CMTS 기본 프라이버시 구성 명령

다음 케이블 인터페이스 명령을 사용하여 Cisco CMTS에서 Baseline privacy 및 Baseline privacy 관련 기능을 구성할 수 있습니다.

### 케이블 프라이버시

cable privacy 명령은 특정 인터페이스에서 베이스라인 프라이버시 협상을 활성화합니다. 케이블 인터페이스에 no cable privacy 명령이 구성된 경우 해당 인터페이스에서 온라인으로 전환될 때 케이블 모뎀에서 베이스라인 프라이버시를 협상할 수 없습니다. 케이블 모뎀이 DOCSIS 컨피그레이션 파일에서 기본 프라이버시를 사용하도록 명령되고 Cisco CMTS가 기본 프라이버시 협상을 거부하면 모뎀이 온라인 상태를 유지할 수 없기 때문에 베이스라인 프라이버시를 비활성화할 때는 주의해야 합니다.

### 케이블 프라이버시 필수

케이블 프라이버시 필수 명령이 구성되어 있고 케이블 모뎀이 DOCSIS 컨피그레이션 파일에서 기본 프라이버시를 사용하도록 설정한 경우 케이블 모뎀이 성공적으로 협상하고 베이스라인 프라이버시를 사용해야 합니다. 그렇지 않으면 베이스라인 프라이버시를 온라인 상태로 유지할 수 없습니다.

케이블 모뎀의 DOCSIS 컨피그레이션 파일에서 기본 프라이버시를 사용하도록 모뎀에 지시하지 않으면 케이블 프라이버시 필수 명령이 모뎀이 온라인 상태로 남아 있는 것을 막지 않습니다.



케이블 프라이버시 필수 명령은 기본적으로 활성화되지 않습니다.

## 케이블 프라이버시 인증 모델

기본 프라이버시와 관련된 모뎀에 대해 인증 형식을 수행할 수 있습니다. 케이블 모뎀이 Cisco CMTS와 KEK를 협상할 때 모뎀은 6바이트 MAC 주소와 일련 번호의 세부 정보를 Cisco CMTS로 전송합니다. 이러한 매개변수는 케이블 모뎀 인증을 위해 사용자 이름/비밀번호 조합으로 사용할 수 있습니다. Cisco CMTS는 Cisco IOS AAA(Authentication, Authorization and Accounting) 서비스를 사용하여 이를 수행합니다. 인증에 실패한 케이블 모뎀은 온라인 상태가 될 수 없습니다. 또한 베이스라인 프라이버시를 사용하지 않는 케이블 모뎀은 이 명령의 영향을 받지 않습니다.

**주의:** 이 기능을 사용하면 AAA 서비스를 사용할 수 있으므로 AAA 컨피그레이션을 수정할 때 주의해야 합니다. 그렇지 않으면 실수로 Cisco CMTS에 로그인하고 관리할 수 있는 기능이 손실될 수 있습니다.

다음은 모뎀 인증을 수행하는 방법에 대한 몇 가지 샘플 컨피그레이션입니다. 이러한 컨피그레이션 예에서는 여러 모뎀이 인증 데이터베이스에 입력되었습니다. 모뎀의 68진수 MAC 주소는 사용자 이름 역할을 하며 가변 길이 일련 번호는 비밀번호 역할을 합니다. 하나의 모뎀이 잘못된 일련 번호로 구성되었습니다.

다음 부분 샘플 Cisco CMTS 컨피그레이션에서는 로컬 인증 데이터베이스를 사용하여 여러 케이블 모뎀을 인증합니다.

```
aaa new-model

aaa authentication login cmts local

aaa authentication login default line

!

username 009096073831 password 0 009096073831

username 0050734eb419 password 0 FAA0317Q06Q

username 000196594447 password 0 **BAD NUMBER**

username 002040015370 password 0 03410390200001835252

!

interface Cable 3/0

    cable privacy authenticate-modem

!

line vty 0 4

    password cisco
```

모뎀을 인증하는 또 다른 방법은 외부 RADIUS 서버를 사용하는 것입니다. 다음은 모뎀을 인증하기 위해 외부 RADIUS 서버를 사용하는 부분 Cisco CMTS 구성 예입니다

```
aaa new-model
```



```
aaa authentication login default line
aaa authentication login cmts group radius
!
interface Cable 3/0
    cable privacy authenticate-modem
!
radius-server host 172.17.110.132 key cisco
!
line vty 0 4
    password cisco
```

다음은 로컬 인증을 사용한 위의 예와 동일한 정보를 가진 샘플 RADIUS 사용자 데이터베이스 파일입니다. 사용자 파일은 여러 상용 및 프리웨어 RADIUS 서버에서 사용자 인증 정보가 저장되는 데이터베이스로 사용됩니다.

```
# Sample RADIUS server users file.

# Joe Blogg's Cable Modem
009096073831 Password = "009096073831"
    Service-Type = Framed

# Jane Smith's Cable Modem
0050734EB419 Password = "FAA0317Q06Q"
    Service-Type = Framed

# John Brown's Cable Modem
000196594477 Password = "***BAD NUMBER**"
    Service-Type = Framed

# Jim Black's Cable Modem
002040015370 Password = "03410390200001835252"
    Service-Type = Framed
```

아래 그림에는 위 구성 샘플 중 하나를 사용하는 Cisco CMTS에서 실행된 **show cable modem** 명령의 출력이 나와 있습니다. 로컬 인증 데이터베이스에 나열되지 않거나 일련 번호가 잘못된 기본 프라이버시 지원 모뎀은 **reject(pk)** 상태로 **입력되며** 온라인 상태로 유지되지 않습니다.

CMTS# show cable modem								
Interface	Prim Sid	Online State	Timing Rec Offset	Power	QoS	CPE	IP address	MAC address
Cable3/0/U0	17	online	2810	0.00	6	0	10.1.1.11	0001.9659.43fd
Cable3/0/U1	18	online (pt)	2739	0.00	5	0	10.1.1.29	0050.734e.b419
Cable3/0/U0	19	offline	2815	0.00	2	0	10.1.1.52	0001.9659.4461
Cable3/0/U0	20	reject (pk)	2810	-0.75	5	0	10.1.1.30	0001.9659.4447
Cable3/0/U1	21	online (pt)	2212	0.75	7	0	10.1.1.40	0020.4001.5370
Cable3/0/U0	22	online (pt)	2806	0.00	5	0	10.1.1.44	0090.9607.3831

SID 17을 사용하는 모뎀은 인증 데이터베이스에 항목이 없지만 DOCSIS 구성 파일에서 기본 프라이버시 사용을 명령하지 않았으므로 온라인 상태로 올 수 있습니다.

SID가 18, 21, 22인 모뎀은 인증 데이터베이스에 올바른 항목이 있으므로 온라인 상태가 될 수 있습니다.

SID 19를 사용하는 모뎀은 기본 프라이버시를 사용하도록 명령되었지만 이 모뎀에 대한 인증 데이터베이스에 항목이 없기 때문에 온라인 상태가 될 수 없습니다. 이 모뎀은 인증에 실패했음을 나타내기 위해 최근에 reject(pk) 상태에 있었습니다.

이 모뎀의 MAC 주소를 사용하는 인증 데이터베이스에 항목이 있지만 해당 일련 번호가 잘못되어 SID 20을 사용하는 모뎀이 온라인 상태가 될 수 없습니다. 현재 이 모뎀은 거부(pk) 상태이지만 잠시 후에 오프라인 상태로 전환됩니다.

모뎀이 인증에 실패할 경우 다음 행에 있는 메시지가 Cisco CMTS 로그에 추가됩니다.

```
%UBR7200-5-UNAUTHSIDTIMEOUT: CMTS deleted      BPI unauthorized Cable Modem 0001.9659.4461
```

그러면 케이블 모뎀이 스테이션 유지 보수 목록에서 제거되고 30초 이내에 오프라인으로 표시됩니다. 그러면 케이블 모뎀이 다시 한번 온라인 상태로 전환하려고 시도할 수 있지만 다시 거부됩니다.

**참고:** Cisco는 고객이 케이블 모뎀이 온라인으로 들어오는 것을 막기 위해 **cable privacy authenticate-modem** 명령을 사용하지 않는 것을 권장합니다. 권한이 없는 고객이 서비스 공급자의 네트워크에 액세스하지 못하도록 하는 보다 효율적인 방법은 네트워크 액세스 필드가 꺼져 있는 상태로 DOCSIS 구성 파일을 다운로드하도록 무단 케이블 모뎀에 지시하는 프로비저닝 시스템을 구성하는 것입니다. 이렇게 하면 모뎀이 지속적으로 범위를 조정함으로써 귀중한 업스트림 대역폭을 낭비하지 않습니다. 대신 모뎀은 **온라인(d)** 상태로 이동되며, 이는 모뎀의 사용자가 서비스 공급자의 네트워크에 액세스할 수 없음을 나타내며 모뎀은 스테이션 유지 관리에 업스트림 대역폭만 사용합니다.

## BPI 상태를 모니터링하는 데 사용되는 명령

**show interface cable x/0 privacy [kek | tek]**—이 명령은 CMTS 인터페이스에 설정된 대로 KEK 또는 TEK과 연결된 타이머를 표시하는 데 사용됩니다.

다음은 이 명령의 출력 예입니다.

```
CMTS# show interface cable 4/0 privacy kek
```

```
Configured KEK lifetime value = 604800
```

```
Configured KEK grace time value = 600
```

```
CMTS# show interface cable 4/0 privacy tek
```

```
Configured TEK lifetime value = 60480
```

```
Configured TEK grace time value = 600
```

**show interface cable X/0 privacy statistics** - 이 숨겨진 명령은 특정 케이블 인터페이스에서 기본 프라이버시를 사용하여 SID 수에 대한 통계를 보는 데 사용할 수 있습니다.

다음은 이 명령의 출력 예입니다.

```
CMTS# show interface cable 4/0 privacy statistic
```

```
CM key Chain Count : 12
```

```
CM Unicast key Chain Count : 12
```

```
CM Mucast key Chain Count : 3
```

**debug cable privacy** - 이 명령은 베이스라인 프라이버시 디버깅을 활성화합니다. 이 명령이 활성화되면 베이스라인 프라이버시 상태 또는 베이스라인 프라이버시 이벤트가 변경될 때마다 세부 정보가 콘솔에 표시됩니다. 이 명령은 **debug 케이블 인터페이스 케이블 X/0** 또는 **debug cable mac-address mac-address** 명령과 함께 앞에 오는 경우에만 작동합니다.

**debug cable bpiatp** - 이 명령은 베이스라인 프라이버시 디버깅을 활성화합니다. 이 명령이 활성화되면 Cisco CMTS에서 Baseline privacy 메시지를 보내거나 받을 때마다 16진수 메시지 덤프가 표시됩니다. 이 명령은 **debug 케이블 인터페이스 케이블 X/0** 또는 **debug cable mac-address mac-address** 명령과 함께 앞에 오는 경우에만 작동합니다.

**debug cable keyman** - 이 명령은 베이스라인 개인 정보 보호 키 관리의 디버깅을 활성화했습니다. 이 명령이 활성화되면 기본 프라이버시 키 관리의 세부 정보가 표시됩니다.

## BPI 문제 해결

케이블 모뎀은 온라인(pt)이 아닌 온라인 상태로 나타납니다.

모뎀이 온라인(pt)이 아닌 온라인 상태로 나타나면 일반적으로 세 가지 중 하나를 의미합니다.

첫 번째 가능한 이유는 케이블 모뎀에 Baseline 프라이버시를 사용하도록 지정하는 DOCSIS 구성 파일이 제공되지 않았기 때문입니다. DOCSIS 구성 파일이 모뎀으로 전송된 서비스 클래스 프로필에서 BPI가 활성화되어 있는지 확인합니다.

모뎀이 온라인 상태에서 나타나는 두 번째 원인은 모뎀이 BPI 협상을 시작하기 전에 대기 중이기 때문일 수 있습니다. 1~2분 정도 기다렸다가 모뎀 상태가 온라인(pt)으로 변경되는지 확인합니다.

마지막 원인은 모뎀에 기본 프라이버시를 지원하는 펌웨어가 포함되어 있지 않기 때문일 수 있습니다. BPI를 지원하는 최신 버전의 펌웨어는 모뎀 공급업체에 문의하십시오.

케이블 모뎀이 reject(pk) 상태로 나타난 다음 오프라인으로 전환합니다.

모뎀이 reject(pk) 상태로 전환되는 경우 **케이블 프라이버시 authenticate-modem** 명령을 사용하여 케이블 모뎀 인증을 활성화했지만 AAA가 잘못 구성되었기 때문입니다. 영향을 받는 모뎀의 일련 번호와 mac 주소가 인증 데이터베이스에 올바르게 입력되었는지, 그리고 외부 RADIUS 서버가 연결 가능하고 작동하는지 확인합니다. 라우터 디버깅 명령을 사용하여 **debug aaa authentication** 및 **debug radius**를 사용하여 RADIUS 서버의 상태 또는 모뎀이 인증에 실패한 이유를 알 수 있습니다.

**참고:** 케이블 모뎀 연결 문제 해결에 대한 일반적인 정보는 [Troubleshooting uBR Cable Modem Not Coming Online](#)을 참조하십시오.

## 특수 메모 - 숨겨진 명령

이 문서에서 숨겨진 명령에 대한 참조는 정보 제공용으로만 제공됩니다. 숨겨진 명령은 [Cisco TAC\(Technical Assistance Center\)](#)에서 지원되지 않습니다. 숨겨진 명령 외에도

- 항상 신뢰할 수 있거나 정확한 정보를 생성하지 못할 수 있음
- 실행할 경우 예기치 않은 부작용이 발생할 수 있습니다.
- 다른 버전의 Cisco IOS Software에서 동일한 방식으로 작동하지 않을 수 있습니다.
- Cisco IOS Software의 향후 릴리스에서 예고 없이 언제든지 제거할 수 있음

## 관련 정보

- [케이블 랩](#)
- [AAA\(Authentication, Authorization, and Accounting\)](#)
- [Technical Support - Cisco Systems](#)