

DOCSIS 1.0 Privacy op basis van Cisco CMTS

Inhoud

[Inleiding](#)

[Voordat u begint](#)

[Conventies](#)

[Voorwaarden](#)

[Gebruikte componenten](#)

[Hoe u de basisprivacy voor kabelmodems kunt instellen](#)

[Hoe moet u vertellen of een kabelmodem gebruik maakt van de privacy van de basislijn](#)

[Timers die invloed hebben op de vaststelling en handhaving van de basisprivacy](#)

[KEK Lifetime](#)

[KEK Grace Time](#)

[TEK Lifetime](#)

[TEK Grace Time](#)

[Time-out autoriseren](#)

[Time-out voor wachten opnieuw autoriseren](#)

[Time-out bij autorisatie](#)

[Time-out bij afwijzen autoriseren](#)

[Time-out bij operationele wachten](#)

[Rekey Wacht Time-out](#)

[Opdrachten voor Cisco CMTS-configuratie voor basislijn](#)

[kabelprivacy](#)

[privacy verplicht](#)

[authenticatie van kabelprivacy](#)

[Opdrachten gebruikt om de status van BPI te controleren](#)

[BPI-probleemoplossing](#)

[Speciale opmerking - verborgen opdrachten](#)

[Gerelateerde informatie](#)

[Inleiding](#)

Het belangrijkste doel van Data-over-Cable Service Interface Specifications (DOCSIS) Privacyinterface (BPI) is een eenvoudige gegevenscoderingsregeling te bieden om gegevens te beschermen die naar en van kabelmodems in een Data-over-Cable netwerk worden verzonden. De privacy van de basislijn kan ook als middel worden gebruikt om kabelmodems echt te maken, en de overdracht van multicast verkeer naar kabelmodems toe te staan.

Cisco Cable Modem Termination System (CMTS) en kabelmodemproducten met Cisco IOS[®] Software-afbeeldingen met een functieset inclusief de tekens "k1" of "k8" ondersteuning voor basisprivacy, bijvoorbeeld ubr7200-k1p-mz.121-6.EC1.bin.

Dit document heeft betrekking op de privacy van de basislijn op Cisco-producten die in de DOCSIS1.0-modus werken.

[Voordat u begint](#)

[Conventies](#)

Zie de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

[Voorwaarden](#)

Er zijn geen specifieke voorwaarden van toepassing op dit document.

[Gebruikte componenten](#)

De informatie in dit document is gebaseerd op het configureren van een uBR7246VXR-actieve Cisco IOS[®] softwarerelease 12.1(6)EC, maar het is ook van toepassing op alle andere Cisco CMTS-producten en -softwarereleases.

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de potentiële impact van om het even welke opdracht begrijpt alvorens het te gebruiken.

[Hoe u de basisprivacy voor kabelmodems kunt instellen](#)

Een kabelmodem zal alleen proberen de privacy van de basislijn te gebruiken als dit wordt geadviseerd via de Klasse van de dienstparameters in een DOCSIS configuratiebestand. Het DOCSIS-configuratiebestand bevat operationele parameters voor de modem en wordt via TFTP gedownload als onderdeel van het proces van online verschijnen.

Eén methode om een DOCSIS-configuratiebestand te maken, is door de DOCSIS-configurator voor de kabelmodem op Cisco.com te gebruiken. Met behulp van de DOCSIS-configurator voor kabelmodems kunt u een DOCSIS-configuratiebestand maken waarmee u een kabelmodems kunt besturen om de Privacyfunctie bij basislijn te gebruiken door het veld Privacy Enable onder het tabblad Service-on in te stellen. Raadpleeg het onderstaande voorbeeld:

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

U kunt ook de standalone versie van de DOCSIS-bestandsconfiguratie van ABBYY gebruiken om Privacy zoals hieronder wordt getoond, mogelijk te maken:

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

Zodra een DOCSIS-configuratiebestand voor BPI is gemaakt, moeten kabelmodems worden gereset om het nieuwe configuratiebestand te kunnen downloaden en vervolgens de basisprivacy te kunnen gebruiken.

[Hoe moet u vertellen of een kabelmodem gebruik maakt van de privacy van de basislijn](#)

Op een Cisco CMTS kan men de opdracht [Show kabelmodems](#) gebruiken om de status van afzonderlijke kabelmodems te bekijken. Er zijn verschillende staten dat een modem die de privacy van de Basislijn gebruikt kan verschijnen.

[online](#)

Na een kabelmodemregisters met een Cisco CMTS ingaat het de online staat. Een kabelmodemmodule moet deze status bereiken voordat hij kan onderhandelen met de privacy-parameters van de basislijn met een Cisco CMTS. Op dit punt is het gegevensverkeer tussen de kabelmodem en CMTS niet versleuteld. Als een kabelmodem in deze staat blijft en niet naar een van de hieronder genoemde staten gaat, dan gebruikt de modem geen privacy van de Basislijn.

[online \(pk\)](#)

De online (pk) staat betekent dat de kabelmodem met Cisco CMTS heeft kunnen onderhandelen over een **machtigingssleutel**, die ook bekend staat als een **Key Encryption Key (KEK)**. Dit betekent dat de kabelmodems geautoriseerd is om de privacy van de basislijn te gebruiken en succesvol in de onderhandelingen over de eerste fase van de privacy van de basislijn is geweest. De KEK is een 56 bit key die wordt gebruikt om de daaropvolgende onderhandelingen over privacy bij aanvang te beschermen. Wanneer een modem in online (pk) het staatsgegevensverkeer binnen is dat tussen de kabelmodem en Cisco CMTS wordt verzonden is nog niet gecodeerd aangezien geen sleutel voor de encryptie van gegevensverkeer nog is overeengekomen. Online(pk) wordt doorgaans gevolgd door [online\(pt\)](#).

[afwijzen\(pk\)](#)

Deze staat geeft aan dat de pogingen van de kabelmodems om te onderhandelen over een KEK mislukt zijn. De meest algemene reden dat een modem in deze staat zou zijn, zou zijn dat de Cisco CMTS de modem van de Verificatie aan en de modem heeft gefaalde authenticatie geactiveerd.

[online \(pt\)](#)

Op dit punt heeft de modem met succes een Traffic Encryption Key (TEK) met Cisco CMTS besproken. TEK wordt gebruikt om gegevensverkeer tussen de kabelmodem en Cisco CMTS te versleutelen. Het TEK onderhandelingsproces is versleuteld met de KEK. TEK is een 56 of 40 bit key die wordt gebruikt om het gegevensverkeer tussen de kabelmodem en Cisco CMTS te versleutelen. Op dit punt is de privacy van de basislijn met succes vastgesteld en uitgevoerd, daarom worden de gebruikersgegevens die tussen de Cisco CMTS en de kabelmodem worden verzonden versleuteld.

[verwerping\(pt\)](#)

Deze staat geeft aan dat de kabelmodem niet met succes een TEK met Cisco CMTS kon onderhandelen.

Zie hieronder voor een voorbeelduitvoer van een show kabelmodemopdracht die kabelmodems in verschillende staten toont met betrekking tot privacy in basislijn.

CMTS# show cable modem								
Interface	Prim Sid	Online State	Timing Offset	Rec Power	QoS	CPE	IP address	MAC address
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

N.B.: Raadpleeg voor meer informatie over de status van de kabelmodems de [probleemoplossing bij uBR-kabelmodems die niet online komen](#).

Timers die invloed hebben op de vaststelling en handhaving van de basisprivacy

Er zijn bepaalde timeout waarden die kunnen worden aangepast om het gedrag van de privacy van de basislijn te veranderen. Sommige van deze parameters kunnen in Cisco CMTS en andere in het DOCSIS-configuratiebestand worden geconfigureerd. Er is weinig reden om een van deze parameters te veranderen behalve de levensduur van KEK en de levensduur van TEK. Deze timers kunnen worden gewijzigd om de beveiliging van een kabelfabriek te verhogen of om CPU en verkeeroverheadkosten te beperken door BPI-beheer.

KEK Lifetime

De levensduur van KEK is de hoeveelheid tijd die de kabelmodem en Cisco CMTS als de overeengekomen KEK geldig moeten beschouwen. Voordat deze hoeveelheid tijd is verstreken, moet de kabelmodem opnieuw onderhandelen over een nieuwe KEK met de Cisco CMTS.

U kunt deze keer configureren met behulp van de opdracht Cisco CMTS-kabelinterface:

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

De standaardinstelling is 604800 seconden, die gelijk is aan zeven dagen.

Een kleinere levensduur van KEK verhoogt de veiligheid omdat elke KEK een kortere periode zal aanhouden en dus als de KEK minder toekomstige TEK-onderhandelingen zou worden gehackt, zou het vatbaar zijn om gekaapt te worden. Het nadeel hiervan is dat KEK opnieuw onderhandelt het gebruik van CPU's op kabelmodems verhoogt en het BPI-beheerverkeer op een kabelfabriek verhoogt.

KEK Grace Time

De respondertijd van KEK is de hoeveelheid tijd voordat het leven van KEK verstrijkt, die een kabelmodem is bedoeld om met de Cisco CMTS te beginnen voor een nieuwe KEK. Het idee achter het hebben van deze timer is zodat de kabelmodem genoeg tijd heeft om de KEK te vernieuwen voor het verstrijken ervan.

U kunt deze keer configureren met behulp van de opdracht Cisco CMTS-kabelinterface:

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

U kunt deze keer ook configureren met behulp van een DOCSIS-configuratiebestand door het veld met het label **Time-out** voor **autorisatie bij uitlijning** onder het tabblad Privacy van de basislijn in te vullen. Als dit veld van het DOCSIS is ingevuld, heeft dit voorrang op elke waarde die in Cisco CMTS is ingesteld. De standaardwaarde voor deze timer is 600 seconden, wat gelijk is aan 10 minuten.

[TEK Lifetime](#)

De levensduur van de TEK is de hoeveelheid tijd die de kabelmodem en Cisco CMTS als geldig moeten beschouwen voor de onderhandelde TEK. Voordat deze hoeveelheid tijd is verstreken, moet de kabelmodem opnieuw onderhandelen over een nieuwe TEK met de Cisco CMTS.

U kunt deze keer configureren met behulp van de opdracht Cisco CMTS-kabelinterface:

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

De standaardinstelling is 43200 seconden, wat gelijk is aan 12 uur.

Een kleinere TEK-levensduur verhoogt de veiligheid omdat elke TEK een kortere periode zal aanhouden en dus als de TEK minder gegevens heeft gehackt, zal hij worden blootgesteld aan ongeoorloofde decryptie. Het nadeel hiervan is dat TEK-heronderhandeling het gebruik van CPU's op kabelmodems verhoogt en het BPI-beheerverkeer op een kabelfabriek verhoogt.

[TEK Grace Time](#)

De TEK responduur is de hoeveelheid tijd vóór het verstrijken van de TEK-levensduur dat een kabelmodem met Cisco CMTS voor een nieuwe TEK moet starten. Het idee achter het hebben van deze timer is zodat de kabelmodem genoeg tijd heeft om de TEK te vernieuwen voor het verlopen is.

U kunt deze keer configureren met behulp van de opdracht Cisco CMTS-kabelinterface:

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

U kunt deze keer ook configureren met behulp van een DOCSIS-configuratiebestand door het veld met het label **TEK Grace Time-out** in te vullen onder het tabblad Privacy van de basislijn. Als dit veld van het DOCSIS is ingevuld, heeft dit voorrang op elke waarde die in Cisco CMTS is ingesteld.

De standaardwaarde voor deze timer is 600 seconden, wat gelijk is aan 10 minuten.

[Time-out autoriseren](#)

Deze keer bepaalt de hoeveelheid tijd die een kabelmodem voor het eerst op een reactie van een

Cisco CMTS zal wachten wanneer u op een KEK onderhandelt.

U kunt deze keer in een DOCSIS-configuratiebestand configureren door het veld **Time-out** autoriseren te wijzigen onder het tabblad Privacy van de basislijn.

De standaardwaarde voor dit veld is 10 seconden en het geldige bereik is 2 tot 30 seconden.

[Time-out voor wachten opnieuw autoriseren](#)

Deze keer bepaalt de hoeveelheid tijd die een kabelmodem op een antwoord van een Cisco CMTS zal wachten wanneer het aan het onderhandelen is over een nieuwe KEK omdat het leven van KEK op het punt staat te verlopen.

U kunt deze keer in een DOCSIS-configuratiebestand configureren door het veld **Time-out** opnieuw **machtigen** te wijzigen onder het tabblad Privacy-basislijn.

De standaardwaarde voor deze timer is 10 seconden en het geldige bereik is 2 tot 30 seconden.

[Time-out bij autorisatie](#)

Geeft de aflossingsvrije periode voor hertoelating (in seconden) aan. De standaardwaarde is 600. Het geldige bereik is 1 tot 1800 seconden.

[Time-out bij afwijzen autoriseren](#)

Als een kabelmodem probeert om een KEK met een CMTS van Cisco te onderhandelen, maar wordt verworpen, moet het op de Time-out van het Afwijzen van vergunning wachten alvorens opnieuw te proberen om een nieuwe KEK te onderhandelen wachten.

U kunt deze parameter in een DOCSIS-configuratiebestand configureren door het veld **Time-out** bij **autoriseren** afwijzen te gebruiken onder het tabblad Privacy van de basislijn. De standaardwaarde voor deze timer is 60 seconden en het geldige bereik is 10 seconden tot 600 seconden.

[Time-out bij operationele wachten](#)

Deze keer bepaalt de hoeveelheid tijd die een kabelmodem voor het eerst op een antwoord van een Cisco CMTS zal wachten wanneer u op een TEK onderhandelt.

U kunt deze keer in een DOCSIS-configuratiebestand configureren door het veld **Time-out** bij **gebruik** te wijzigen onder het tabblad Privacy van de basislijn.

De standaardwaarde voor dit veld is 1 seconde en het geldige bereik is 1 tot 10 seconden.

[Rekey Wacht Time-out](#)

Deze keer bepaalt de hoeveelheid tijd die een kabelmodem op een antwoord van een Cisco CMTS zal wachten wanneer het over een nieuwe TEK onderhandelen omdat het leven van de TEK op het punt staat te verlopen.

U kunt deze keer in een DOCSIS-configuratiebestand configureren door het veld **Time-out** bij **Rekenen** te wijzigen onder het tabblad Privacy van de basislijn.

De standaardwaarde voor deze timer is 1 seconde en het geldige bereik is 1 tot 10 seconden.

Opdrachten voor Cisco CMTS-configuratie voor basislijn

De volgende kabelinterfaceopdrachten kunnen worden gebruikt om de privacy van de basislijn en de privacy-gerelateerde functies op een Cisco CMTS te configureren.

kabelprivacy

De opdracht **privacy** van de kabel stelt de onderhandeling van de privacy van de basislijn op een bepaalde interface mogelijk. Als de opdracht **geen privacy**-opdracht op een kabelinterface is geconfigureerd dan mogen kabelmodems niet onderhandelen over privacy op basislijn wanneer ze op die interface online komen. Gebruik voorzichtigheid wanneer u de privacy van de basislijn uitschakelt omdat als een kabelmodem de privacy van de basislijn door zijn DOCSIS-configuratiebestand moet gebruiken en de Cisco CMTS weigert om de privacy van de basislijn te laten onderhandelen, dan kan de modem niet online blijven.

privacy verplicht

Als de **verplichte** opdracht voor de **kabelprivacy** is ingesteld en een kabelmodem een privacy bij de basislijn heeft ingeschakeld in zijn DOCSIS-configuratiebestand, moet de kabelmodem met succes onderhandelen en de privacy bij de basislijn gebruiken anders mag het niet online blijven.

Als het DOCSIS-configuratiebestand van een kabelmodems de modem niet heeft geïnstrueerd om de basisprivacy te gebruiken, dan zal de **verplichte** opdracht van de **kabelprivacy** de modem niet verhinderen om online te blijven.

De **verplichte** opdracht voor **kabelprivacy** is standaard niet ingeschakeld.

authenticatie van kabelprivacy

Het is mogelijk een vorm van authenticatie uit te voeren voor modems die zich bezighouden met privacy in de basislijn. Wanneer kabelmodems een KEK met Cisco CMTS onderhandelen, verzenden modems details van hun 6 bytes MAC-adres en hun serienummer naar Cisco CMTS. Deze parameters kunnen worden gebruikt als een gebruikersnaam/wachtwoordcombinatie om kabelmodems te authentifieren. Cisco CMTS gebruikt de Cisco IOS Verificatie, autorisatie en accounting (AAA) service om dit te doen. Kabelmodems die niet gewaarmerkt zijn, mogen niet online gaan. Bovendien worden kabelmodems die de privacy van de basislijn niet gebruiken niet door deze opdracht beïnvloed.

Waarschuwing: aangezien deze optie gebruik maakt van de AAA-service, moet u ervoor zorgen dat u voorzichtig bent bij het wijzigen van de AAA-configuratie, anders kunt u per ongeluk het vermogen verliezen om in te loggen en uw Cisco CMTS te beheren.

Hier zijn een paar voorbeelden van formaties voor het uitvoeren van modemverificatie. In deze configuratievoorbeelden is een aantal modems ingevoerd in een authenticatiedatabase. Het 6 octet MAC-adres van de modem dient als een gebruikersnaam en het variabele lengte

serienummer dient als wachtwoord. Merk op dat één modem is ingesteld met een duidelijk onjuist serienummer.

De volgende gedeeltelijke steekproef van Cisco CMTS configuratie gebruikt een lokale authenticatiedatabank om een aantal kabelmodems voor authentiek te verklaren.

```
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
```

Een andere methode om modems te authenticeren zou zijn om een externe RADIUS-server te gebruiken. Hier is een gedeeltelijk Cisco CMTS-configuratievoorbeeld dat een externe RADIUS-server gebruikt om modems te authenticeren

```
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
```

Hieronder staat een RADIUS-gebruikersdatabank met dezelfde informatie als het voorbeeld

hierboven, waarin lokale authenticatie wordt gebruikt. Het gebruikersbestand wordt door een aantal commerciële en vrije RADIUS-servers gebruikt als een database waar de informatie over gebruikersverificatie wordt opgeslagen.

```
# 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
```

Hieronder weergegeven is de uitvoer van een opdracht voor een **show-kabelmodems** uitgevoerd op een Cisco CMTS-platform dat gebruikmaakt van één van de bovengenoemde configuratiemonsters. U zult zien dat elke privacy-enabled modems die niet in de lokale authenticatie database zijn vermeld, of met het onjuiste serienummer de **diskettatie(pk)** staat zullen invoeren en niet online zullen blijven.

CMTS# show cable modem									
Interface	Prim Sid	Online State	Timing Offset	Rec 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	

De modem met SID 17 heeft geen ingang in de authenticatiedatabank maar kan online komen

omdat zijn DOCSIS configuratiebestand het niet heeft verplicht om privacy van de basislijn te gebruiken.

De modems met SID's 18, 21 en 22 kunnen online komen omdat ze correcte ingangen in de authenticatiedatabank hebben

De modem met SID 19 kan niet online komen omdat het wordt verplicht om de privacy van de Basislijn te gebruiken maar er is geen ingang in de authenticatiedatabank voor deze modem. Deze modem zou onlangs in de diskant(pk) staat geweest zijn om aan te geven dat het faalde authenticatie.

De modem met SID 20 kan niet online komen omdat, alhoewel er een ingang in de authenticatiedatabank met het MAC-adres van deze modem is, het corresponderende serienummer niet correct is. Op dit moment is deze modem in de afwijzende (pk) staat maar zal hij na een korte periode naar de offline status overstappen.

Wanneer modems geen verificatie uitvoeren wordt een bericht langs de volgende lijnen toegevoegd aan het Cisco CMTS-logbestand.

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

De kabelmodem wordt dan verwijderd uit de lijst van het stationonderhoud en zal als offline binnen 30 seconden worden gemarkeerd. De kabelmodem zal dan waarschijnlijk opnieuw proberen om opnieuw online te komen om slechts opnieuw te worden verworpen.

Opmerking: Cisco adviseert niet dat klanten de **kabelprivacy-authenticate-modemopdracht** gebruiken om niet-geautoriseerde kabelmodems te stoppen om online te komen. Een efficiëntere manier om ervoor te zorgen dat niet-geautoriseerde klanten geen toegang krijgen tot het netwerk van een dienstverlener is om het voorzieningssysteem te configureren zodat niet-geautoriseerde kabelmodems geïnstrueerd worden om een DOCSIS-configuratiebestand te downloaden, waarbij het veld voor netwerktoegang is uitgeschakeld. Op deze manier verspilt de modem geen waardevolle upstream bandbreedte door voortdurend opnieuw te verdelen. In plaats daarvan krijgt de modem de **online(d)** status die aangeeft dat gebruikers achter de modem geen toegang tot het netwerk van de serviceprovider krijgen en dat de modem alleen upstream bandbreedte voor stationonderhoud gebruikt.

[Opdrachten gebruikt om de status van BPI te controleren](#)

toon interfacekabel X/0 privacy [kek] | tek—Deze opdracht wordt gebruikt om de timers weer te geven die gekoppeld zijn aan de KEK of de TEK zoals deze op een CMTS-interface is ingesteld.

Hieronder staat een voorbeelduitvoer van deze opdracht.

```
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
```

toon de van interfacekabel X/0 privacy statistiek—Deze verborgen opdracht kan worden gebruikt om statistieken over het aantal SIDs te bekijken die de beginprivacy op een bepaalde kabelinterface gebruiken.

Hieronder staat een voorbeelduitvoer van deze opdracht.

```
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 van kabelprivacy—Deze opdracht activeert het zuiveren van de privacy van de basislijn. Wanneer deze opdracht wordt geactiveerd, wanneer een verandering in de toestand van de privacy bij de basislijn of een gebeurtenis van de privacy bij de basislijn optreedt, zullen de details op de console worden weergegeven. Deze opdracht werkt alleen wanneer deze is voorafgegaan door de **opdracht debug kabel interface kabel X/0** of **debug kabel mac-adres**.

debug kabel bpiatp—Deze opdracht activeert het zuiveren van de privacy van de Baseline. Wanneer deze opdracht is geactiveerd, wanneer een bericht van de privacy van de basislijn door Cisco CMTS wordt verzonden of ontvangen, zal het hexadecimale dumpen van het bericht worden weergegeven. Deze opdracht werkt alleen wanneer deze is voorafgegaan door de **opdracht debug kabel interface kabel X/0** of **debug kabel mac-adres**.

debug kabel keyman—Deze opdracht activeerde het zuiveren van de privacy van de basislijn. Wanneer deze opdracht is geactiveerd, worden er gegevens weergegeven over het beheer van de privacy van de basislijn.

BPI-probleemoplossing

Kabelmodems worden eerder online dan online weergegeven (pt).

Als een modem in een online staat in plaats van online (pt) verschijnt dan betekent het meestal één van drie dingen.

De eerste waarschijnlijke reden is dat de kabelmodem geen DOCSIS configuratiebestand heeft gekregen dat de kabelmodem de privacy van de basislijn gebruikt. Controleer of het DOCSIS-configuratiebestand BPI heeft ingeschakeld in het serviceklasse die naar de modem wordt verzonden.

De tweede oorzaak van het zien van een modem in de online staat zou kunnen zijn dat de modem wacht alvorens zij op BPI begint te onderhandelen. Wacht even of twee om te zien of de modem de status online (pt) verandert.

De uiteindelijke oorzaak zou kunnen zijn dat de modem geen firmware bevat die de basisprivacy ondersteunt. Neem contact op met uw modemverkoper voor een recentere versie van firmware die BPI ondersteunt.

Kabelmodems verschijnen in afwijzende (pk) status en gaan vervolgens offline.

De meest waarschijnlijke oorzaak van een modeminvoerend diskette (pk) staat is dat kabelmodemverificatie is ingeschakeld met de opdracht **voor de authenticatie van de kabelprivacy en modem**, maar AAA is niet geconfigureerd. Controleer of de serienummers en mac-adressen van de getroffen modems correct in de authenticatiedatabase zijn ingevoerd en dat een externe RADIUS-server bereikbaar en functioneert. U kunt de opdrachten voor het fouterstellen van de router gebruiken **debug a authenticatie** en **debug straal** om een idee te krijgen van de status van de RADIUS-server of waarom een modem geen verificatie heeft.

N.B.: Raadpleeg voor algemene informatie over het oplossen van problemen bij kabelmodemconnectiviteit het [probleem oplossen uBR kabelmodems die niet online komen](#).

[Speciale opmerking - verborgen opdrachten](#)

Elke verwijzing naar verborgen opdrachten in dit document is uitsluitend bedoeld voor informatieve doeleinden. Verborgen opdrachten worden niet ondersteund door het [Cisco Technical Assistance Center \(TAC\)](#). Daarnaast zijn er verborgen opdrachten:

- Kan niet altijd betrouwbare of correcte informatie opleveren
- Kan onverwachte bijwerkingen veroorzaken indien uitgevoerd
- Kan zich niet op dezelfde manier gedragen in verschillende versies van Cisco IOS-software
- Kan te allen tijde en zonder voorafgaande kennisgeving worden verwijderd van toekomstige releases van Cisco IOS-software

[Gerelateerde informatie](#)

- [CableLabs](#)
- [Verificatie, autorisatie en accounting \(AAA\)](#)
- [Technische ondersteuning - Cisco-systemen](#)