

Baseline Privacy di DOCSIS 1.0 su Cisco CMTS

Sommario

[Introduzione](#)

[Operazioni preliminari](#)

[Convenzioni](#)

[Prerequisiti](#)

[Componenti usati](#)

[Come configurare la privacy della linea di base per i modem via cavo](#)

[Come stabilire se un modem via cavo utilizza la privacy prevista](#)

[Timer che influiscono sull'istituzione e il mantenimento della privacy di base](#)

[Durata KEK](#)

[Ora di tolleranza KEK](#)

[Durata TEK](#)

[Tempo di grazia TEK](#)

[Autorizza timeout di attesa](#)

[Timeout attesa riautorizzazione](#)

[Timeout di prova autorizzazione](#)

[Timeout di attesa rifiuto autorizzazione](#)

[Timeout di attesa operativo](#)

[Timeout attesa reimpostazione chiavi](#)

[Comandi di configurazione della privacy per Cisco CMTS Baseline](#)

[privacy del cavo](#)

[privacy cavo obbligatoria](#)

[cable privacy authentication-modem](#)

[Comandi utilizzati per monitorare lo stato di BPI](#)

[Risoluzione dei problemi BPI](#)

[Nota speciale - Comandi nascosti](#)

[Informazioni correlate](#)

[Introduzione](#)

L'obiettivo principale di DOCSIS (Data-over-Cable Service Interface Specifications) BPI (Baseline Privacy Interface) è fornire un semplice schema di crittografia dei dati per proteggere i dati inviati a e dai modem via cavo in una rete Data over Cable. La privacy di base può essere utilizzata anche per autenticare i modem via cavo e autorizzare la trasmissione del traffico multicast ai modem via cavo.

I prodotti Cisco Cable Modem Termination System (CMTS) e modem via cavo con immagini software Cisco IOS[®] con una serie di funzionalità che includono i caratteri "k1" o "k8" supportano la privacy di base, ad esempio ubr7200-k1p-mz.121-6.EC1.bin.

In questo documento viene descritta la privacy della baseline sui prodotti Cisco in modalità DOCSIS1.0.

Operazioni preliminari

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento [Cisco sulle convenzioni nei suggerimenti tecnici](#).

Prerequisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è la configurazione di un uBR7246VXR con software Cisco IOS® versione 12.1(6)EC, ma si applica anche a tutti gli altri prodotti e versioni software Cisco CMTS.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Come configurare la privacy della linea di base per i modem via cavo

Un modem via cavo tenterà di utilizzare la privacy della linea di base solo se gli viene richiesto di farlo tramite i parametri Class of Service in un file di configurazione DOCSIS. Il file di configurazione DOCSIS contiene i parametri operativi per il modem e viene scaricato tramite TFTP come parte del processo di connessione.

Un metodo per creare un file di configurazione DOCSIS è usare DOCSIS Cable Modem Configurator su Cisco.com. Utilizzando DOCSIS Cable Modem Configurator, è possibile creare un file di configurazione DOCSIS che comandi a un modem via cavo di utilizzare la privacy della linea di base impostando il campo Abilita privacy della linea di base nella scheda Classe di servizio su **Attivo**. Fare riferimento all'esempio seguente:

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

In alternativa, è possibile utilizzare la versione standalone del file di configurazione DOCSIS da per abilitare la privacy di base, come mostrato di seguito:

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

Dopo aver creato un file di configurazione DOCSIS che supporta BPI, è necessario reimpostare i modem via cavo per scaricare il nuovo file di configurazione e quindi utilizzare la privacy della linea di base.

[Come stabilire se un modem via cavo utilizza la privacy prevista](#)

Su un Cisco CMTS, è possibile usare il comando [show cable modem](#) per visualizzare lo stato dei singoli modem via cavo. In è possibile visualizzare diversi stati di un modem che utilizza la privacy della linea di base.

[online](#)

Quando un modem via cavo si registra in Cisco CMTS, entra in modalità online. Un modem via cavo deve raggiungere questo stato prima di poter negoziare i parametri di privacy della linea di base con un Cisco CMTS. A questo punto il traffico di dati inviato tra il modem via cavo e il CMTS non è crittografato. Se un modem via cavo rimane in questo stato e non passa a uno degli stati indicati di seguito, non utilizza la privacy della linea di base.

[online \(pk\)](#)

Lo stato online(pk) indica che il modem via cavo è stato in grado di negoziare una **chiave di autorizzazione**, nota anche come **chiave di crittografia (KEK)** con il Cisco CMTS. Ciò significa che il modem via cavo è autorizzato a utilizzare la privacy della linea di base ed è riuscito a negoziare la prima fase della privacy della linea di base. KEK è una chiave a 56 bit utilizzata per proteggere le successive negoziazioni della privacy di base. Quando un modem è in linea (pk), il traffico di dati inviato tra il modem via cavo e Cisco CMTS non è ancora crittografato, in quanto non è stata ancora negoziata alcuna chiave per la crittografia del traffico di dati. In genere, online(pk) è seguito da [online\(pt\)](#).

[rifiuto \(pk\)](#)

Questo stato indica che i tentativi del modem via cavo di negoziare una chiave non sono riusciti. Il motivo più comune per cui un modem si troverebbe in questo stato è che nel Cisco CMTS l'autenticazione modem è attivata e non è riuscita.

[online \(pt\)](#)

A questo punto, il modem ha negoziato correttamente una chiave di crittografia del traffico (TEK) con Cisco CMTS. Il TEK viene utilizzato per crittografare il traffico di dati tra il modem via cavo e Cisco CMTS. Il processo di negoziazione TEK viene crittografato utilizzando la chiave KEK. Il TEK è una chiave a 56 o 40 bit utilizzata per crittografare il traffico di dati tra il modem via cavo e Cisco CMTS. A questo punto la privacy della linea di base è stata stabilita e attivata correttamente, pertanto i dati utente inviati tra Cisco CMTS e il modem via cavo vengono crittografati.

[rigetto\(pt\)](#)

Questo stato indica che il modem via cavo non è riuscito a negoziare correttamente un TEK con Cisco CMTS.

Di seguito è riportato un output di esempio di un comando show cable modem che mostra i modem via cavo in vari stati relativi alla privacy della linea di base.

```

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

```

Nota: per ulteriori informazioni sullo stato del modem via cavo, consultare il documento sulla [risoluzione dei problemi relativi ai modem cablati uBR che non sono in linea.](#)

Timer che influiscono sull'istituzione e il mantenimento della privacy di base

Alcuni valori di timeout possono essere modificati per modificare il comportamento della privacy della baseline. Alcuni di questi parametri possono essere configurati su Cisco CMTS e altri tramite il file di configurazione DOCSIS. Non c'è motivo di modificare nessuno di questi parametri, ad eccezione della durata KEK e della durata TEK. Questi timer possono essere modificati per aumentare la sicurezza su un impianto cablato o per ridurre il sovraccarico della CPU e del traffico a causa della gestione BPI.

Durata KEK

La durata della chiave è l'intervallo di tempo per cui il modem via cavo e Cisco CMTS devono considerare valida la chiave negoziata. Prima di questo periodo di tempo, il modem via cavo dovrebbe rinegoziare una nuova chiave con il Cisco CMTS.

È possibile configurare questa ora utilizzando il comando Cisco CMTS cable interface:

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

L'impostazione predefinita è 604800 secondi, ovvero sette giorni.

Una durata di KEK inferiore aumenta la sicurezza, in quanto ogni KEK durerà per un periodo di tempo più breve e quindi, se la KEK viene violata meno future negoziazioni TEK, potrebbe essere dirottata. Lo svantaggio è che la rinegoziazione KEK aumenta l'utilizzo della CPU sui modem via cavo e il traffico di gestione BPI su un impianto cablato.

Ora di tolleranza KEK

Il periodo di prova di KEK è il periodo di tempo prima della scadenza della durata di KEK durante il quale un modem via cavo inizia a negoziare con Cisco CMTS per un nuovo KEK. L'idea alla base di questo timer è che il modem via cavo abbia abbastanza tempo per rinnovare il KEK prima che scada.

È possibile configurare questa ora utilizzando il comando Cisco CMTS cable interface:

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

È inoltre possibile configurare questa ora utilizzando un file di configurazione DOCSIS compilando il campo **Timeout di prova autorizzazione** nella scheda Privacy baseline. Se questo campo del file di configurazione DOCSIS è compilato, ha la precedenza su qualsiasi valore configurato sul Cisco CMTS. Il valore predefinito per questo timer è 600 secondi, pari a 10 minuti.

Durata TEK

La durata TEK è il periodo di tempo durante il quale il modem via cavo e Cisco CMTS devono considerare valido il TEK negoziato. Prima di tale periodo di tempo, il modem via cavo dovrebbe rinegoziare un nuovo TEK con il Cisco CMTS.

È possibile configurare questa ora utilizzando il comando Cisco CMTS cable interface:

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

L'impostazione predefinita è 43200 secondi, ovvero 12 ore.

Una durata TEK inferiore aumenta la sicurezza perché ogni TEK durerà per un periodo di tempo più breve e quindi, se il TEK viene violato, una quantità inferiore di dati sarà esposta alla decrittografia non autorizzata. Lo svantaggio è che la rinegoziazione TEK aumenta l'utilizzo della CPU sui modem via cavo e aumenta il traffico di gestione BPI su un impianto cablato.

Tempo di grazia TEK

Il tempo di tolleranza TEK è il periodo di tempo prima della scadenza della durata TEK durante il quale un modem via cavo deve iniziare a negoziare con Cisco CMTS per un nuovo TEK. L'idea alla base di questo timer è che il modem via cavo abbia abbastanza tempo per rinnovare il TEK prima che scada.

È possibile configurare questa ora utilizzando il comando Cisco CMTS cable interface:

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

È inoltre possibile configurare questa ora utilizzando un file di configurazione DOCSIS compilando il campo **TEK Grace Timeout** (Timeout di prova TEK) nella scheda Privacy di baseline. Se questo campo del file di configurazione DOCSIS è compilato, ha la precedenza su qualsiasi valore configurato sul Cisco CMTS.

Il valore predefinito per questo timer è 600 secondi, pari a 10 minuti.

Autorizza timeout di attesa

Questa volta stabilisce per quanto tempo un modem via cavo attende una risposta da un Cisco CMTS quando negozia un KEK per la prima volta.

È possibile configurare questa ora in un file di configurazione DOCSIS modificando il campo **Autorizza timeout di attesa** nella scheda Privacy della baseline.

Il valore predefinito per questo campo è 10 secondi e l'intervallo valido è compreso tra 2 e 30 secondi.

[Timeout attesa riautorizzazione](#)

Questo periodo determina il tempo di attesa di una risposta da un Cisco CMTS da parte di un modem via cavo durante la negoziazione di un nuovo KEK perché la durata del KEK sta per scadere.

È possibile configurare questa ora in un file di configurazione DOCSIS modificando il campo **Reauthorization Wait Timeout** (Riautorizza timeout di attesa) nella scheda Baseline Privacy.

Il valore predefinito del timer è 10 secondi, mentre l'intervallo valido è da 2 a 30 secondi.

[Timeout di prova autorizzazione](#)

Specifica il periodo di prova per la riautorizzazione (in secondi). Il valore predefinito è 600. L'intervallo valido è compreso tra 1 e 1800 secondi.

[Timeout di attesa rifiuto autorizzazione](#)

Se un modem via cavo tenta di negoziare un KEK con un Cisco CMTS, ma viene rifiutato, deve attendere il timeout di attesa per il rifiuto dell'autorizzazione prima di tentare nuovamente di negoziare un nuovo KEK.

È possibile configurare questo parametro in un file di configurazione DOCSIS utilizzando il campo **Autorizza timeout di rifiuto** nella scheda Privacy della baseline. Il valore predefinito del timer è 60 secondi, mentre l'intervallo valido è compreso tra 10 e 600 secondi.

[Timeout di attesa operativo](#)

Questa volta stabilisce per quanto tempo un modem via cavo attende una risposta da un Cisco CMTS quando negozia un TEK per la prima volta.

È possibile configurare questo tempo in un file di configurazione DOCSIS modificando il campo **Timeout di attesa operativo** nella scheda Privacy della baseline.

Il valore predefinito per questo campo è 1 secondo e l'intervallo valido è compreso tra 1 e 10 secondi.

[Timeout attesa reimpostazione chiavi](#)

Questa volta stabilisce per quanto tempo un modem via cavo deve attendere una risposta da un Cisco CMTS durante la negoziazione di un nuovo TEK perché la durata del TEK sta per scadere.

È possibile configurare questa ora in un file di configurazione DOCSIS modificando il campo **Rekey Wait Timeout** (Timeout di attesa per la reimpostazione della chiave) nella scheda Privacy della

baseline.

Il valore predefinito del timer è 1 secondo, l'intervallo valido è compreso tra 1 e 10 secondi.

Comandi di configurazione della privacy per Cisco CMTS

Baseline

I comandi dell'interfaccia dei cavi riportati di seguito possono essere utilizzati per configurare le funzioni relative alla privacy della linea di base e della linea di base su un Cisco CMTS.

privacy del cavo

Il comando [cable privacy](#) consente di negoziare la privacy della baseline su un'interfaccia specifica. Se il comando **no cable privacy** è configurato su un'interfaccia di cavo, nessun modem via cavo sarà autorizzato a negoziare la privacy della linea di base quando accede a Internet su tale interfaccia. Prestare attenzione quando si disabilita la privacy della linea di base perché se a un modem via cavo viene richiesto di utilizzare la privacy della linea di base tramite il relativo file di configurazione DOCSIS e Cisco CMTS rifiuta di consentire la negoziazione della privacy della linea di base, il modem potrebbe non essere in grado di rimanere online.

privacy cavo obbligatoria

Se il comando **cable privacy required** è configurato e per un modem via cavo è abilitata la privacy della linea di base nel file di configurazione DOCSIS, il modem via cavo deve eseguire correttamente la negoziazione e utilizzare la privacy della linea di base, altrimenti non potrà rimanere online.

Se il file di configurazione DOCSIS di un modem via cavo non indica al modem di utilizzare la privacy della linea di base, il comando **cable privacy required** non interrompe la modalità in linea del modem.

il comando **cable privacy required** non è abilitato per impostazione predefinita.

cable privacy authentication-modem

È possibile eseguire una forma di autenticazione per i modem che utilizzano la privacy prevista. Quando i modem via cavo negoziano una chiave con il Cisco CMTS, trasmettono i dettagli dell'indirizzo MAC da 6 byte e del numero di serie al Cisco CMTS. Questi parametri possono essere utilizzati come combinazione di nome utente e password per autenticare i modem via cavo. Per eseguire questa operazione, il Cisco CMTS utilizza il servizio di autenticazione, autorizzazione e accounting (AAA) di Cisco IOS. I modem via cavo che non superano l'autenticazione non possono connettersi. Inoltre, i modem via cavo che non utilizzano la privacy della linea di base non vengono influenzati da questo comando.

Attenzione: poiché questa funzione utilizza il servizio AAA, è necessario prestare attenzione quando si modifica la configurazione AAA, altrimenti si potrebbe perdere inavvertitamente la possibilità di accedere e gestire il Cisco CMTS.

Di seguito sono riportate alcune configurazioni di esempio per le modalità di autenticazione del modem. In questi esempi di configurazione sono stati immessi diversi modem in un database di

autenticazione. L'indirizzo MAC di 6 ottetti del modem funge da nome utente e il numero di serie di lunghezza variabile da password. Notare che un modem è stato configurato con un numero di serie ovviamente errato.

Nella configurazione Cisco CMTS di esempio parziale seguente viene utilizzato un database di autenticazione locale per autenticare diversi modem via cavo.

```
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
```

Un altro metodo di autenticazione dei modem consiste nell'utilizzare un server RADIUS esterno. Di seguito è riportato un esempio di configurazione Cisco CMTS parziale che utilizza un server RADIUS esterno per autenticare i modem

```
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
```

Di seguito è riportato un esempio di file del database degli utenti RADIUS con le informazioni equivalenti a quelle dell'esempio precedente che utilizza l'autenticazione locale. Il file degli utenti viene utilizzato da diversi server RADIUS commerciali e freeware come database in cui vengono memorizzate le informazioni di autenticazione degli utenti.

```
# 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
```

Di seguito viene riportato l'output di un comando **show cable modem** eseguito su un Cisco CMTS che utilizza uno degli esempi di configurazione riportati sopra. Tutti i modem Baseline che supportano la privacy non elencati nel database di autenticazione locale o con il numero di serie errato entreranno nello stato **Rifiutato (pk)** e non resteranno in linea.

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	

Il modem con SID 17 non dispone di una voce nel database di autenticazione, ma è in grado di

connettersi in quanto il file di configurazione DOCSIS non ha impostato l'utilizzo della privacy di base.

I modem con SID 18, 21 e 22 possono connettersi perché hanno voci corrette nel database di autenticazione

Impossibile connettere il modem con SID 19. È stato richiesto di utilizzare la privacy della linea di base, ma non è presente alcuna voce nel database di autenticazione per il modem. Il modem sarebbe stato recentemente in stato Rifiutato (pk) per indicare che non ha superato l'autenticazione.

Impossibile connettere il modem con SID 20. Sebbene nel database di autenticazione sia presente una voce con l'indirizzo MAC del modem, il numero di serie corrispondente non è corretto. Al momento il modem è in stato rifiutato (pk) ma passerà allo stato offline dopo un breve periodo.

Quando l'autenticazione dei modem non riesce, al registro Cisco CMTS viene aggiunto un messaggio con le seguenti righe.

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

Il modem via cavo viene quindi rimosso dall'elenco di manutenzione della stazione e verrà contrassegnato come non in linea entro 30 secondi. Il modem via cavo proverà quindi molto probabilmente a collegarsi nuovamente per poi essere rifiutato di nuovo.

Nota: Cisco sconsiglia agli utenti di utilizzare il comando **cable privacy authentication-modem** per impedire che modem via cavo non autorizzati siano in linea. Un modo più efficiente per garantire che i clienti non autorizzati non abbiano accesso alla rete di un provider di servizi è configurare il sistema di provisioning in modo che i modem via cavo non autorizzati vengano autorizzati a scaricare un file di configurazione DOCSIS con il campo di accesso alla rete impostato su off. In questo modo, il modem non sprecherà preziosa larghezza di banda a monte tramite una continua modifica della gamma. Al contrario, il modem raggiungerà lo stato **online(d)** che indica che agli utenti dietro il modem non verrà concesso l'accesso alla rete del provider di servizi e il modem utilizzerà solo la larghezza di banda a monte per la manutenzione della stazione.

[Comandi utilizzati per monitorare lo stato di BPI](#)

show interface cable X/0 privacy [key | tek] - Questo comando viene utilizzato per visualizzare i timer associati al KEK o al TEK impostato su un'interfaccia CMTS.

Di seguito è riportato un esempio di output di questo comando.

```
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 statistic - Questo comando nascosto può essere utilizzato per visualizzare le statistiche sul numero di SID che utilizzano la privacy della linea di base su una particolare interfaccia di cavo.

Di seguito è riportato un esempio di output di questo comando.

```
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: questo comando attiva il debug della privacy della linea di base. Quando questo comando è attivato, ogni volta che si verifica una modifica nello stato di privacy della baseline o un evento di privacy della baseline, i dettagli vengono visualizzati sulla console. Questo comando funziona solo se preceduto dal comando **debug cable interface cable X/0** o **debug cable mac-address mac-address**.

debug cable bpiatp: questo comando attiva il debug della privacy della linea di base. Quando questo comando è attivato, ogni volta che un messaggio di privacy della baseline viene inviato o ricevuto dal Cisco CMTS, viene visualizzato il dump esadecimale del messaggio. Questo comando funziona solo se preceduto dal comando **debug cable interface cable X/0** o **debug cable mac-address mac-address**.

debug cable keyman: questo comando ha attivato il debug di Baseline privacy key management. Quando questo comando è attivato, vengono visualizzati i dettagli relativi alla gestione delle chiavi di privacy della linea di base.

[Risoluzione dei problemi BPI](#)

I modem via cavo vengono visualizzati come in linea anziché in linea (pt).

Se il modem è in linea anziché in linea (pt), in genere è possibile che si verifichi una delle tre situazioni seguenti.

Il primo motivo probabile è che al modem via cavo non sia stato assegnato un file di configurazione DOCSIS che specifica che il modem via cavo utilizza la privacy prevista. Verificare che nel file di configurazione DOCSIS sia abilitato BPI nel profilo Class of Service inviato al modem.

La seconda causa della presenza di un modem in linea potrebbe essere l'attesa del modem prima che inizi la negoziazione BPI. Attendere qualche minuto per verificare se lo stato del modem passa a online(pt).

La causa finale potrebbe essere che il modem non contiene firmware che supporta la privacy della

linea di base. Contattare il fornitore del modem per ottenere una versione più recente del firmware che supporti BPI.

I modem via cavo vengono visualizzati nello stato rifiutato (pk) e quindi passano alla modalità offline.

La causa più probabile dell'attivazione dello stato Rifiutato (pk) per un modem è che l'autenticazione del modem via cavo è stata abilitata con il comando **cable privacy authentication-modem**, ma il server AAA non è stato configurato correttamente. Verificare che i numeri di serie e gli indirizzi MAC dei modem interessati siano stati immessi correttamente nel database di autenticazione e che qualsiasi server RADIUS esterno sia raggiungibile e funzionante. È possibile utilizzare i comandi di debug del router **debug aaa authentication** e **debug radius** per avere un'idea dello stato del server RADIUS o del motivo per cui l'autenticazione del modem non riesce.

Nota: per informazioni generali sulla risoluzione dei problemi relativi alla connettività del modem via cavo, consultare il documento sulla [risoluzione dei problemi relativi ai modem via cavo uBR che non sono in linea](#).

[Nota speciale - Comandi nascosti](#)

Ogni riferimento ai comandi nascosti in questo documento ha uno scopo puramente informativo. I comandi nascosti non sono supportati dal [Cisco Technical Assistance Center \(TAC\)](#). Oltre ai comandi nascosti:

- Potrebbe non sempre generare informazioni affidabili o corrette
- Può causare effetti collaterali imprevisti se eseguito
- Il comportamento potrebbe non essere lo stesso in versioni diverse del software Cisco IOS
- Può essere rimosso dalle future versioni del software Cisco IOS in qualsiasi momento senza preavviso

[Informazioni correlate](#)

- [CableLabs](#)
- [Autenticazione, autorizzazione e accounting \(AAA\)](#)
- [Supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).