DOCSIS 1.0 Baseline-Datenschutz auf Cisco CMTS

Inhalt

Einführung

Das Hauptziel von Data-over-Cable Service Interface Specifications (DOCSIS) Baseline Privacy Interface (BPI) ist die Bereitstellung eines einfachen Datenverschlüsselungsschemas zum Schutz von Daten, die an und von Kabelmodems in einem Data-over-Cable-Netzwerk gesendet werden. Der grundlegende Datenschutz kann auch als Mittel zur Authentifizierung von Kabelmodems und zur Autorisierung der Übertragung von Multicast-Datenverkehr an Kabelmodems verwendet werden.

Cisco Cable Modem Termination System (CMTS)- und Kabelmodemprodukte mit Cisco IOS®

Software-Images mit einem Feature-Set, einschließlich der Zeichen "k1" oder "k8", unterstützen den Baseline-Datenschutz, z. B. ubr7200-k1p-mz.121-6.EC1.bin.

In diesem Dokument wird der grundlegende Datenschutz für Cisco Produkte im DOCSIS1.0-Modus erläutert.

Bevor Sie beginnen

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Voraussetzungen

Für dieses Dokument bestehen keine besonderen Voraussetzungen.

Verwendete Komponenten

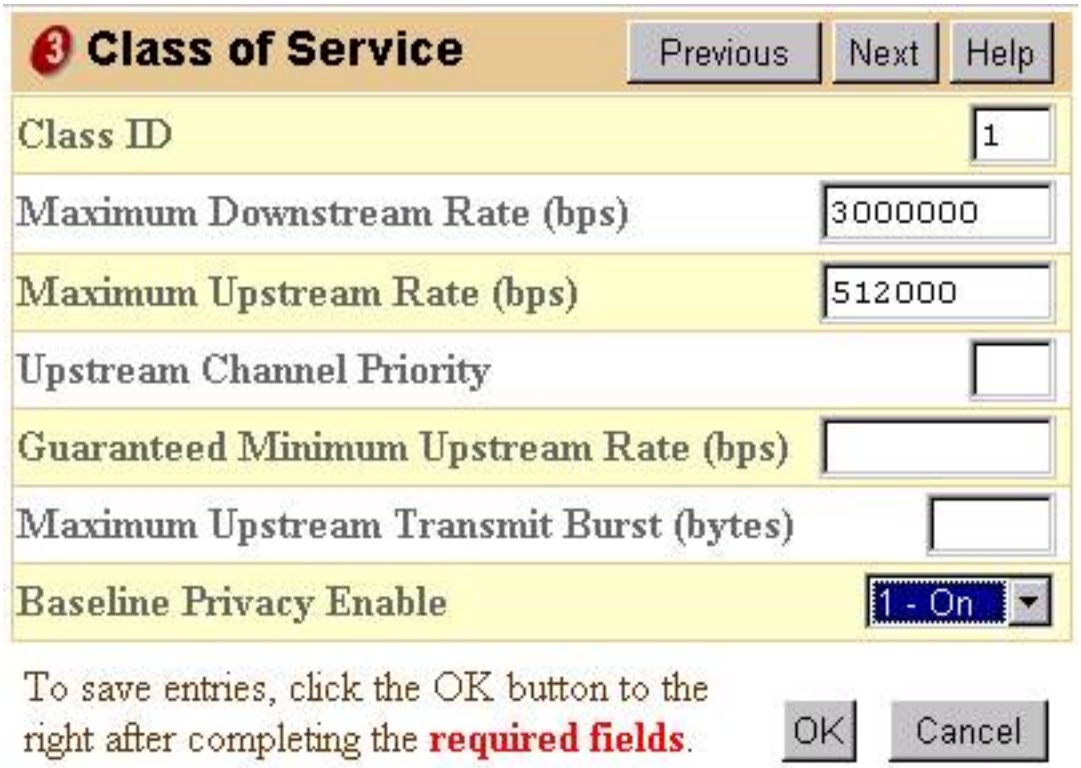
Die Informationen in diesem Dokument basieren auf der Konfiguration eines uBR7246VXR mit Cisco IOS® Softwareversion 12.1(6)EC, aber auch auf allen anderen Cisco CMTS-Produkten und -Softwareversionen.

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

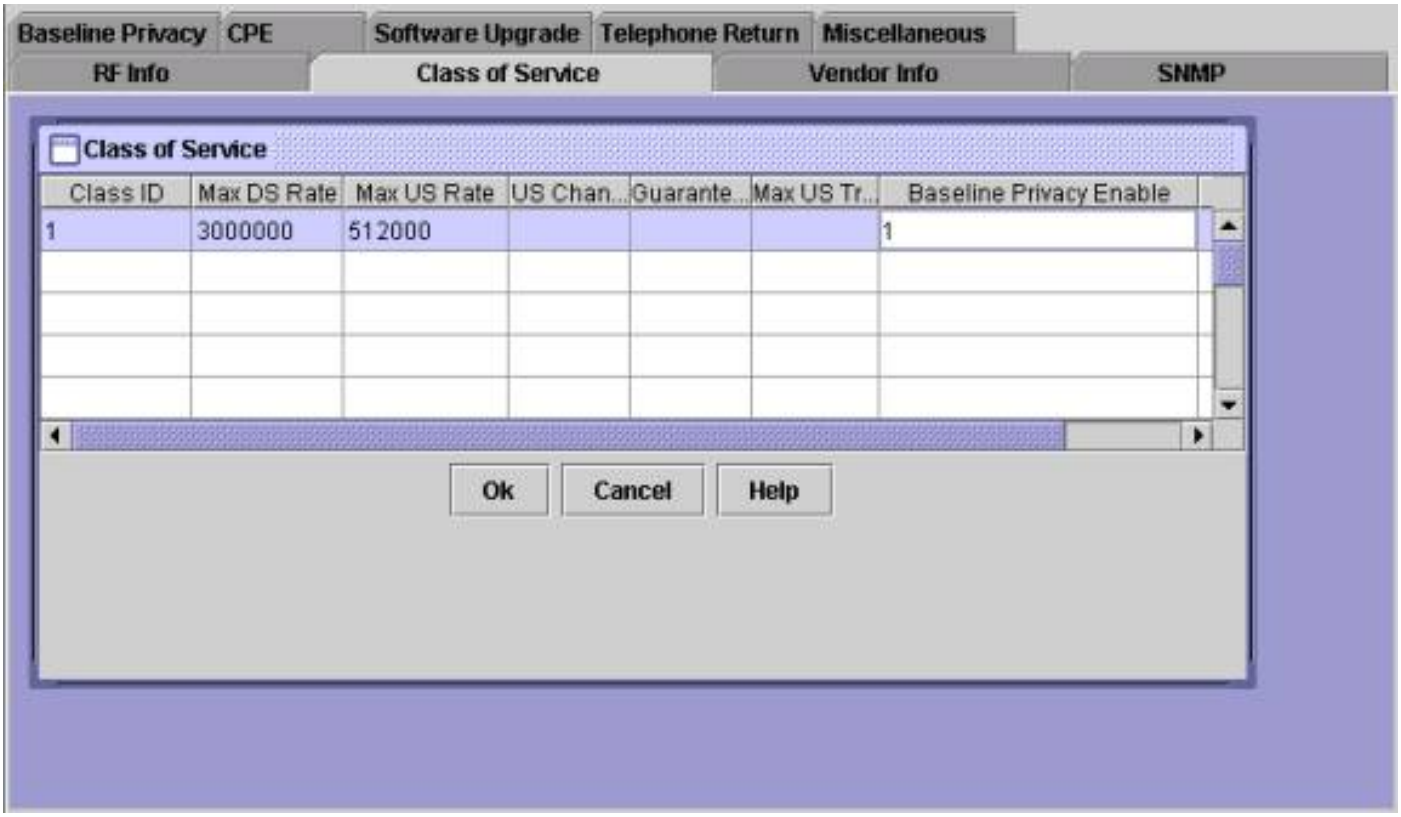
Konfigurieren von Baseline-Datenschutz für Kabelmodems

Ein Kabelmodem versucht nur dann, die Baseline-Privatsphäre zu verwenden, wenn dies über die Class of service-Parameter in einer DOCSIS-Konfigurationsdatei vorgeschrieben ist. Die DOCSIS-Konfigurationsdatei enthält die Betriebsparameter für das Modem und wird über TFTP als Teil des Online-Vorgangs heruntergeladen.

Eine Möglichkeit zum Erstellen einer DOCSIS-Konfigurationsdatei ist die Verwendung des DOCSIS Cable Modem Configurator auf Cisco.com. Mit dem DOCSIS Cable Modem Configurator können Sie eine DOCSIS-Konfigurationsdatei erstellen, die ein Kabelmodem zur Verwendung des Baseline-Datenschutzes befehligt, indem Sie auf der Registerkarte "Class of Service" (Serviceklasse) das Feld "Baseline Privacy Enable" (Baseline-Datenschutz aktivieren) auf **On** festlegen. Nachstehend finden Sie ein Beispiel:



Alternativ kann die eigenständige Version der DOCSIS-Dateikonfiguration von verwendet werden, um Baseline-Datenschutz zu aktivieren (siehe unten):



Nachdem eine DOCSIS-Konfigurationsdatei erstellt wurde, die BPI unterstützt, müssen die Kabelmodems zurückgesetzt werden, um die neue Konfigurationsdatei herunterzuladen und anschließend den Schutz der Baseline-Daten zu gewährleisten.

So ermitteln Sie, ob ein Kabelmodem Baseline-Datenschutz verwendet

Auf einem Cisco CMTS kann der Status einzelner Kabelmodems mit dem Befehl show cable modem **(Kabelmodem anzeigen)** angezeigt werden. Es gibt mehrere Zustände, in denen ein Modem mit Baseline-Datenschutz angezeigt werden kann.

online

Nachdem sich ein Kabelmodem bei einem Cisco CMTS registriert hat, wechselt es in den Online-Status. Ein Kabelmodem muss diesen Status erreichen, bevor es Baseline-Datenschutzparameter mit einem Cisco CMTS aushandeln kann. An diesem Punkt wird der zwischen dem Kabelmodem und CMTS gesendete Datenverkehr unverschlüsselt. Wenn sich ein Kabelmodem in diesem Zustand befindet und mit keinem der unten genannten Zustände fortfährt, wird der Schutz der Baseline-Daten vom Modem nicht verwendet.

online (pk)

Der Online(pk)-Status bedeutet, dass das Kabelmodem einen **Autorisierungsschlüssel** aushandeln konnte, der auch als **Schlüssel-Verschlüsselungsschlüssel (KEK)** bezeichnet wird, mit dem Cisco CMTS. Das bedeutet, dass das Kabelmodem autorisiert ist, die grundlegende Privatsphäre zu verwenden, und dass es die erste Phase des grundlegenden Datenschutzes erfolgreich verhandelt hat. Das KEK ist ein 56-Bit-Schlüssel zum Schutz der nachfolgenden Baseline-Datenschutzverhandlungen. Wenn sich ein Modem im Online(pk)-Status befindet, wird der Datenverkehr zwischen dem Kabelmodem und dem Cisco CMTS noch nicht verschlüsselt, da noch kein Schlüssel für die Verschlüsselung des Datenverkehrs verhandelt wurde. In der Regel wird online(pk) gefolgt von online(pt).

Ablehnen (pk)

Dieser Status weist darauf hin, dass die Versuche des Kabelmodems, eine KEK auszuhandeln, fehlgeschlagen sind. Der häufigste Grund dafür, dass sich ein Modem in diesem Zustand befindet, ist, dass die Modemauthentifizierung in Cisco CMTS aktiviert ist und das Modem die Authentifizierung fehlgeschlagen ist.

online(pt)

An diesem Punkt hat das Modem erfolgreich einen Datenverkehrsverschlüsselungsschlüssel (Traffic Encryption Key, TEK) mit dem Cisco CMTS ausgehandelt. Das TEK wird zur Verschlüsselung des Datenverkehrs zwischen dem Kabelmodem und Cisco CMTS verwendet. Der TEK-Verhandlungsprozess wird mit dem KEK verschlüsselt. Das TEK ist ein 56- oder 40-Bit-Schlüssel zur Verschlüsselung des Datenverkehrs zwischen dem Kabelmodem und Cisco CMTS. Zu diesem Zeitpunkt wurde der grundlegende Datenschutz erfolgreich eingerichtet und ausgeführt, sodass die zwischen dem Cisco CMTS und dem Kabelmodem gesendeten Benutzerdaten verschlüsselt werden.

Ablehnen(pt)

Dieser Status weist darauf hin, dass das Kabelmodem nicht in der Lage war, erfolgreich ein TEK mit dem Cisco CMTS auszuhandeln.

Nachfolgend finden Sie eine Beispielausgabe eines Befehls zum Anzeigen von Kabelmodems, der Kabelmodems in verschiedenen Zuständen im Zusammenhang mit dem Baseline-Datenschutz

zeigt.

```
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
```

Hinweis: Weitere Informationen zum Status des Kabelmodems finden Sie unter Fehlerbehebung bei uBR-Kabelmodems, die nicht online verfügbar sind.

Timer, die die Herstellung und Pflege von Baseline-Datenschutz beeinträchtigen

Es gibt bestimmte Timeout-Werte, die geändert werden können, um das Verhalten der Baseline-Privatsphäre zu ändern. Einige dieser Parameter können im Cisco CMTS und andere über die DOCSIS-Konfigurationsdatei konfiguriert werden. Es gibt keinen Grund, diese Parameter außer der KEK-Lebensdauer und der TEK-Lebensdauer zu ändern. Diese Timer können geändert werden, um die Sicherheit in einer Kabelanlage zu erhöhen oder den CPU- und Datenverkehrsaufwand aufgrund des BPI-Managements zu reduzieren.

KEK-Lebensdauer

Die KEK-Lebensdauer ist die Zeit, die das Kabelmodem und Cisco CMTS den ausgehandelten KEK als gültig ansehen sollten. Bevor dieser Zeitraum verstrichen ist, sollte das Kabelmodem einen neuen KEK mit dem Cisco CMTS aushandeln.

Sie können dieses Mal den folgenden Befehl für die Cisco CMTS-Kabelschnittstelle verwenden:

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

Die Standardeinstellung ist 604800 Sekunden, was sieben Tage entspricht.

Eine kleinere KEK-Lebensdauer erhöht die Sicherheit, da jede KEK eine kürzere Lebensdauer hat und daher bei gehackten KEK-Verhandlungen weniger zukünftige TEK-Verhandlungen anfällig für eine Hijacking wären. Der Nachteil dabei ist, dass die Neuverhandlung der KEK die CPU-Auslastung auf Kabelmodems erhöht und den BPI-Management-Datenverkehr in einer Kabelanlage erhöht.

KEK Grace Time

Die KEK-Kulanzzeit ist die Zeitspanne bis zum Ablauf der Lebensdauer des KEK, für die ein Kabelmodem mit dem Cisco CMTS Verhandlungen über eine neue KEK aufnehmen soll. Die Idee hinter diesem Timer ist, dass das Kabelmodem genügend Zeit hat, die KEK zu verlängern, bevor sie abläuft.

Sie können dieses Mal den folgenden Befehl für die Cisco CMTS-Kabelschnittstelle verwenden:

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

Sie können dieses Mal auch mithilfe einer DOCSIS-Konfigurationsdatei konfigurieren, indem Sie das Feld **Authorization Grace Timeout** unter der Registerkarte Baseline Privacy (**Autorisierungs-Grace-Timeout**) ausfüllen. Wenn dieses Feld der DOCSIS-Konfigurationsdatei ausgefüllt wird, hat es Vorrang vor jedem im Cisco CMTS konfigurierten Wert. Der Standardwert für diesen Timer ist 600 Sekunden, was 10 Minuten entspricht.

TEK-Lebenszeitgarantie

Die TEK-Lebensdauer ist die Zeit, die das Kabelmodem und Cisco CMTS das ausgehandelte TEK als gültig ansehen sollten. Vor Ablauf dieser Zeit sollte das Kabelmodem ein neues TEK mit dem Cisco CMTS aushandeln.

Sie können dieses Mal den folgenden Befehl für die Cisco CMTS-Kabelschnittstelle verwenden:

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

Die Standardeinstellung ist 43200 Sekunden, was 12 Stunden entspricht.

Eine kleinere TEK-Lebensdauer erhöht die Sicherheit, da jedes TEK eine kürzere Lebensdauer hat und daher weniger Daten gehackt werden, die nicht autorisiert entschlüsselt werden können. Der Nachteil dabei ist, dass TEK-Neuverhandlungen die CPU-Auslastung auf Kabelmodems erhöhen und den BPI-Management-Datenverkehr in einer Kabelanlage erhöhen.

Anlaufzeit für TEK

Die TEK-Kulanzzeit ist die Zeit bis zum Ablauf der TEK-Lebensdauer, für die ein Kabelmodem mit dem Cisco CMTS Verhandlungen über ein neues TEK aufnehmen soll. Die Idee hinter diesem Timer ist, dass das Kabelmodem genügend Zeit hat, das TEK zu verlängern, bevor es abläuft.

Sie können dieses Mal den folgenden Befehl für die Cisco CMTS-Kabelschnittstelle verwenden:

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

Sie können dieses Mal auch mithilfe einer DOCSIS-Konfigurationsdatei konfigurieren, indem Sie das Feld **TEK Grace Timeout** unter der Registerkarte Baseline Privacy ausfüllen. Wenn dieses Feld der DOCSIS-Konfigurationsdatei ausgefüllt wird, hat es Vorrang vor jedem im Cisco CMTS konfigurierten Wert.

Der Standardwert für diesen Timer ist 600 Sekunden, was 10 Minuten entspricht.

Wartezeitüberschreitung autorisieren

Dieses Mal legt fest, wie lange ein Kabelmodem auf eine Antwort eines Cisco CMTS warten muss, wenn ein KEK zum ersten Mal verhandelt wird.

Sie können dieses Mal in einer DOCSIS-Konfigurationsdatei konfigurieren, indem Sie das Feld **"Authorize Wait Timeout" (Wartezeit** für **Autorisierung**) auf der Registerkarte "Baseline Privacy" (Baseline-Datenschutz) ändern.

Der Standardwert für dieses Feld ist 10 Sekunden, und der gültige Bereich liegt zwischen 2 und 30 Sekunden.

Wartezeitüberschreitung erneut autorisieren

Dieses Mal legt fest, wie lange ein Kabelmodem auf eine Antwort eines Cisco CMTS warten muss, wenn ein neues KEK verhandelt wird, da die Lebensdauer des KEK bald abläuft.

Sie können dieses Mal in einer DOCSIS-Konfigurationsdatei konfigurieren, indem Sie das Feld **Reauthorized Wait Timeout (Wartezeit** erneut **autorisieren)** auf der Registerkarte Baseline Privacy (Baseline-Datenschutz) ändern.

Der Standardwert für diesen Timer ist 10 Sekunden, und der gültige Bereich liegt zwischen 2 und 30 Sekunden.

Timeout für Autorisierungsgrad

Gibt die Kulanzfrist für die erneute Autorisierung (in Sekunden) an. Der Standardwert ist 600. Der gültige Bereich liegt zwischen 1 und 1800 Sekunden.

Autorisieren Zurückwartezeitüberschreitung ablehnen

Wenn ein Kabelmodem versucht, einen KEK mit einem Cisco CMTS auszuhandeln, aber abgelehnt wird, muss es auf das Timeout "Authorize Reject Timeout" (Autorisierte Ablehnung) warten, bevor erneut versucht wird, einen neuen KEK auszuhandeln.

Sie können diesen Parameter in einer DOCSIS-Konfigurationsdatei konfigurieren, indem Sie auf der Registerkarte Baseline-Datenschutz das Feld **Authorize Reject Wait Timeout** (**Wartezeit für Autorisieren** zulassen) verwenden. Der Standardwert für diesen Timer ist 60 Sekunden und der gültige Bereich ist 10 Sekunden bis 600 Sekunden.

Timeout für Betriebswartung

Dieses Mal legt fest, wie lange ein Kabelmodem auf eine Antwort eines Cisco CMTS warten muss, wenn ein TEK zum ersten Mal verhandelt wird.

Sie können dieses Mal in einer DOCSIS-Konfigurationsdatei konfigurieren, indem Sie das Feld **Operational Wait Timeout** (**Operatives Wartezeit**) auf der Registerkarte Baseline Privacy (Baseline-Datenschutz) ändern.

Der Standardwert für dieses Feld ist 1 Sekunde, und der gültige Bereich liegt zwischen 1 und 10 Sekunden.

Neustart-Wartezeit

Dieses Mal legt fest, wie lange ein Kabelmodem auf eine Antwort eines Cisco CMTS warten muss, wenn ein neues TEK verhandelt wird, da die Lebensdauer des TEK bald abläuft.

Sie können dieses Mal in einer DOCSIS-Konfigurationsdatei konfigurieren, indem Sie das Feld **Rekey Wait Timeout** (**Neustart-Timeout**) auf der Registerkarte Baseline Privacy (Baseline-Datenschutz) ändern.

Der Standardwert für diesen Timer ist 1 Sekunde, und der gültige Bereich liegt zwischen 1 und 10 Sekunden.

Befehle zur Basiskonfiguration der Cisco CMTS-Privatsphäre

Die folgenden Befehle für die Kabelschnittstelle können verwendet werden, um Funktionen zum Basisdatenschutz und zum Datenschutz auf Basis von Baseline auf einem Cisco CMTS zu konfigurieren.

Kabelschutz

Der **Befehl** zum **Datenschutz** von **Kabeln** ermöglicht die Aushandlung der Baseline-Privatsphäre auf einer bestimmten Schnittstelle. Wenn der Befehl **Kein Kabelschutz** auf einer Kabelschnittstelle konfiguriert ist, dürfen keine Kabelmodems beim Online-Zugriff auf diese Schnittstelle die Baseline-Privatsphäre aushandeln. Seien Sie vorsichtig, wenn Sie den Schutz der Baseline-Daten deaktivieren, denn wenn ein Kabelmodem durch seine DOCSIS-Konfigurationsdatei zum Schutz der Baseline-Daten aufgefordert wird und das Cisco CMTS sich weigert, die Aushandlung der Baseline-Datenschutzbestimmungen zuzulassen, kann das Modem möglicherweise nicht online bleiben.

Kabelschutz erforderlich

Wenn der **obligatorische** Befehl zum **Schutz der Kabeldaten** konfiguriert ist und in der DOCSIS-Konfigurationsdatei für ein Kabelmodem der grundlegende Datenschutz aktiviert ist, muss das Kabelmodem erfolgreich verhandeln und den Baseline-Datenschutz verwenden. Andernfalls darf es nicht online bleiben.

Wenn die DOCSIS-Konfigurationsdatei eines Kabelmodems das Modem nicht anweist, den Basisdatenschutz zu verwenden, wird der Befehl zum **Schutz der Privatsphäre** des **Kabels** nicht verhindern, dass das Modem online bleibt.

Der **obligatorische** Befehl zum **Kabelschutz** ist standardmäßig nicht aktiviert.

Kabelmodem authentifizieren

Es ist möglich, eine Form der Authentifizierung für Modems durchzuführen, die den Schutz der Baseline-Daten gewährleisten. Wenn Kabelmodems einen KEK mit dem Cisco CMTS aushandeln, übermitteln Modems dem Cisco CMTS Details zu ihrer 6-Byte-MAC-Adresse und ihrer Seriennummer. Diese Parameter können zur Authentifizierung von Kabelmodems als Benutzername/Kennwort-Kombination verwendet werden. Cisco CMTS verwendet dazu den Cisco IOS Authentication, Authorization and Accounting (AAA)-Service. Kabelmodems, die nicht authentifiziert werden können, dürfen nicht online gehen. Darüber hinaus wird dieser Befehl keine Auswirkungen auf Kabelmodems haben, die die Baseline-Datenschutzbestimmungen nicht

verwenden.

Vorsicht: Da diese Funktion den AAA-Service nutzt, müssen Sie beim Ändern der AAA-Konfiguration vorsichtig sein. Andernfalls können Sie sich unbeabsichtigt bei Ihrem Cisco CMTS anmelden und dieses verwalten.

Nachfolgend finden Sie einige Beispielkonfigurationen für Möglichkeiten zur Durchführung der Modemauthentifizierung. In diesen Konfigurationsbeispielen wurden mehrere Modems in eine Authentifizierungsdatenbank eingegeben. Die 6-Oktett-MAC-Adresse des Modems dient als Benutzername, und die Seriennummer variabler Länge dient als Kennwort. Beachten Sie, dass ein Modem mit einer offensichtlich falschen Seriennummer konfiguriert wurde.

In der folgenden Teilkonfiguration von Cisco CMTS wird eine lokale Authentifizierungsdatenbank verwendet, um eine Reihe von Kabelmodems zu authentifizieren.

```
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
```

Eine andere Methode zur Modemanzeige wäre die Verwendung eines externen RADIUS-Servers. Im folgenden Beispiel wird eine teilweise Cisco CMTS-Konfiguration mit einem externen RADIUS-Server zur Authentifizierung von Modems beschrieben.

```
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
```

Im Folgenden sehen Sie eine Beispieldatenbankdatei für RADIUS-Benutzer mit den entsprechenden Informationen zum Beispiel oben, in dem die lokale Authentifizierung verwendet wurde. Die Benutzerdatei wird von einer Reihe kommerzieller und kostenloser RADIUS-Server als Datenbank verwendet, in der die Benutzerauthentifizierungsinformationen gespeichert werden.

```
# 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
```

Im Folgenden sehen Sie die Ausgabe eines Befehls **zum Anzeigen** von **Kabelmodems**, der auf einem Cisco CMTS ausgeführt wird und eines der oben genannten Konfigurationsbeispiele verwendet. Sie sehen, dass alle Modems mit aktiviertem Basisdatenschutz, die nicht in der lokalen Authentifizierungsdatenbank aufgeführt sind, oder mit der falschen Seriennummer in den **Ablehnungsstatus(pk)** eingegeben werden und nicht online bleiben.

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

Das Modem mit SID 17 verfügt über keinen Eintrag in der Authentifizierungsdatenbank, ist jedoch online verfügbar, da es in seiner DOCSIS-Konfigurationsdatei nicht zum Einsatz der Baseline-Datenschutz aufgefordert wurde.

Die Modems mit den SIDs 18, 21 und 22 können online gehen, da sie die richtigen Einträge in der Authentifizierungsdatenbank haben

Das Modem mit SID 19 kann nicht online gehen, da es angewiesen wurde, den Baseline-Datenschutz zu verwenden. Es gibt jedoch keinen Eintrag in der Authentifizierungsdatenbank für dieses Modem. Dieses Modem wäre vor kurzem im Ablehnungszustand (pk) gewesen, um anzuzeigen, dass die Authentifizierung fehlgeschlagen ist.

Das Modem mit SID 20 kann nicht online gehen, da die entsprechende Seriennummer falsch ist, obwohl ein Eintrag in der Authentifizierungsdatenbank mit der MAC-Adresse dieses Modems vorhanden ist. Dieses Modem befindet sich derzeit im Ablehnungszustand (pk), wechselt jedoch nach kurzer Zeit in den Offline-Status.

Wenn Modems nicht authentifiziert werden können, wird dem Cisco CMTS-Protokoll eine Nachricht in der folgenden Zeile hinzugefügt.

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

Das Kabelmodem wird dann aus der Wartungsliste der Station entfernt und innerhalb von 30 Sekunden als offline markiert. Das Kabelmodem wird dann höchstwahrscheinlich noch einmal versuchen, online zu gehen, nur um wieder abgelehnt zu werden.

Hinweis: Cisco empfiehlt nicht, dass Kunden den Befehl **zum Authentifizieren** von **Kabelmodems** verwenden, um nicht autorisierte Kabelmodems vom Internet abzuhalten. Eine effizientere Möglichkeit, um zu gewährleisten, dass nicht autorisierte Kunden keinen Zugriff auf das Netzwerk eines Service Providers erhalten, besteht darin, das Bereitstellungssystem so zu konfigurieren, dass nicht autorisierte Kabelmodems angewiesen werden, eine DOCSIS-Konfigurationsdatei herunterzuladen, wobei das Feld für den Netzwerkzugriff deaktiviert ist. Auf diese Weise verschwendet das Modem keine wertvolle Upstream-Bandbreite, indem es kontinuierlich neu sortiert wird. Stattdessen wechselt das Modem in den **Online(d)**-Status, der anzeigt, dass Benutzer hinter dem Modem keinen Zugriff auf das Netzwerk des Service Providers erhalten und dass das Modem nur Upstream-Bandbreite für die Wartung von Stationen verwendet.

Befehle zur Überwachung des BPI-Zustands

show interface cable X/0 privacy [kek | tek] - Mit diesem Befehl werden die Timer angezeigt, die entweder der KEK oder dem TEK zugeordnet sind, wie sie auf einer CMTS-Schnittstelle festgelegt sind.

Im Folgenden finden Sie ein Beispiel für die Ausgabe dieses Befehls.

```
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 - Dieser versteckte Befehl kann verwendet werden, um Statistiken über die Anzahl der SIDs anzuzeigen, die den Basisdatenschutz auf einer bestimmten Kabelschnittstelle verwenden.

Im Folgenden finden Sie ein Beispiel für die Ausgabe dieses Befehls.

```
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 (**Kabelschutz debuggen**) - Dieser Befehl aktiviert das Debuggen von Baseline-Datenschutz. Wenn dieser Befehl aktiviert ist, werden bei jeder Änderung des Baseline-Datenschutzstatus oder eines Baseline-Datenschutzereignisses Details in der Konsole angezeigt. Dieser Befehl kann nur ausgeführt werden, wenn dem Befehl **debug cable interface cable X/0** oder **debug cable mac-address** ***mac-address (MAC-Adresse)*** vorangestellt wurde.

debug cable bpiatp - Dieser Befehl aktiviert das Debuggen der Baseline-Privatsphäre. Wenn dieser Befehl aktiviert ist und das Cisco CMTS eine grundlegende Datenschutzmeldung sendet oder empfängt, wird das hexadezimale Dump der Nachricht angezeigt. Dieser Befehl kann nur ausgeführt werden, wenn dem Befehl **debug cable interface cable X/0** oder **debug cable mac-address** ***mac-address (MAC-Adresse)*** vorangestellt wurde.

debug cable keyman: Dieser Befehl aktiviert das Debugging der Baseline-Verwaltung von Datenschutzschlüsseln. Wenn dieser Befehl aktiviert ist, werden Details zur Verwaltung der Baseline-Datenschutzschlüssel angezeigt.

Fehlerbehebung BPI

Kabelmodems werden nicht online, sondern online angezeigt (pt).

Wenn ein Modem in einem Online-Status und nicht im Online-Modus (pt) angezeigt wird, bedeutet es in der Regel eine von drei Dingen.

Der erste mögliche Grund ist, dass dem Kabelmodem keine DOCSIS-Konfigurationsdatei gegeben wurde, in der angegeben ist, dass das Kabelmodem den Baseline-Datenschutz verwendet. Überprüfen Sie, ob in der DOCSIS-Konfigurationsdatei BPI im Class of Service-Profil aktiviert ist, das an das Modem gesendet wurde.

Die zweite Ursache für die Online-Anzeige eines Modems könnte darin bestehen, dass das Modem wartet, bevor es mit der Aushandlung von BPI beginnt. Warten Sie ein oder zwei Minuten, um festzustellen, ob das Modem den Status Online(pt) ändert.

Die letzte Ursache könnte sein, dass das Modem keine Firmware enthält, die den Basisschutz unterstützt. Wenden Sie sich an den Hersteller Ihres Modems, um eine neuere Firmware-Version zu erhalten, die BPI unterstützt.

Die Kabelmodems werden im Ablehnungszustand (PK) angezeigt und gehen dann offline.

Die wahrscheinlichste Ursache für die Eingabe des Ablehnungsstatus (pk) eines Modems ist, dass die Authentifizierung des Kabelmodems mit dem Befehl **zum Authentifizieren des Kabelmodems** aktiviert wurde, AAA jedoch falsch konfiguriert wurde. Überprüfen Sie, ob die Seriennummern und MAC-Adressen der betroffenen Modems korrekt in die Authentifizierungsdatenbank eingegeben wurden und ob ein externer RADIUS-Server erreichbar und funktionsfähig ist. Sie können die Router-Debugbefehle verwenden, um **eine Authentifizierung** und einen **Debugradius** zu **debuggen**, um einen Einblick in den Status des RADIUS-Servers zu erhalten oder zu erfahren, warum ein Modem die Authentifizierung nicht erfolgreich durchführt.

Hinweis: Allgemeine Informationen zur Fehlerbehebung bei Kabelmodemverbindungen finden Sie unter Fehlerbehebung bei uBR-Kabelmodems, die nicht online verfügbar sind.

Besondere Anmerkung - Versteckte Befehle

Jede Bezugnahme auf versteckte Befehle in diesem Dokument dient nur zu Informationszwecken. Versteckte Befehle werden vom Cisco Technical Assistance Center (TAC) nicht unterstützt. Hinzu kommen versteckte Befehle:

- Kann nicht immer zuverlässige oder richtige Informationen generieren
- Kann unerwartete Nebenwirkungen hervorrufen, wenn sie ausgeführt werden
- Verhalten in verschiedenen Versionen der Cisco IOS Software möglicherweise nicht gleich
- Kann jederzeit und ohne Vorankündigung aus zukünftigen Versionen der Cisco IOS Software entfernt werden.

Zugehörige Informationen

- Kabellabore
- Authentifizierung, Autorisierung und Abrechnung (AAA)
- Technischer Support - Cisco Systems