Sécurisation de base de DOCSIS 1.0 sur Cisco CMTS

Contenu

Introduction
Avant de commencer
Conventions
Conditions préalables
Composants utilisés
Comment configurer la sécurisation de base pour des Modems câble
Comment dire si un modem câble utilise la sécurisation de base
Temporisateurs affectant l'établissement et la maintenance de la sécurisation de base
Vie KEK
Délai de grâce KEK
Vie TEK
Délai de grâce TEK
Autorisez le délai d'attente
Reauthorize le délai d'attente
Délai d'attente de grâce d'autorisation
Autorisez le délai d'attente d'anomalie
Délai d'attente opérationnel
Délai d'attente de rekey
Commandes de configuration de sécurisation de base de Cisco CMTS
cable privacy
cable privacy obligatoire
authentifier-modem de cable privacy
Commandes utilisées pour surveiller l'état de BPI
Dépannage du BPI
Note spéciale - Commandes masquées
Informations connexes

Introduction

L'objectif principal de l'interface de sécurisation de base de Data-over-Cable Service Interface Specifications (DOCSIS) (BPI) est de fournir un schéma simple de chiffrement de données de protéger des données transmises à et des Modems câble dans des données au-dessus de réseau câblé. La sécurisation de base peut également être utilisée en tant que des moyens d'authentifier des Modems câble, et d'autoriser la transmission du trafic de multidiffusion aux Modems câble.

Produits du système (CMTS) et du modem câble d'arrêt de modem câble Cisco exécutant des images logicielles de Cisco IOS® avec un ensemble de caractéristiques comprenant la

sécurisation de base de support des caractères "k1" or"k8", par exemple ubr7200-k1p-mz.121-6.EC1.bin.

Ce document discute la sécurisation de base sur des Produits Cisco fonctionnant dans le mode DOCSIS1.0.

Avant de commencer

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Conditions préalables

Aucune condition préalable spécifique n'est requise pour ce document.

Composants utilisés

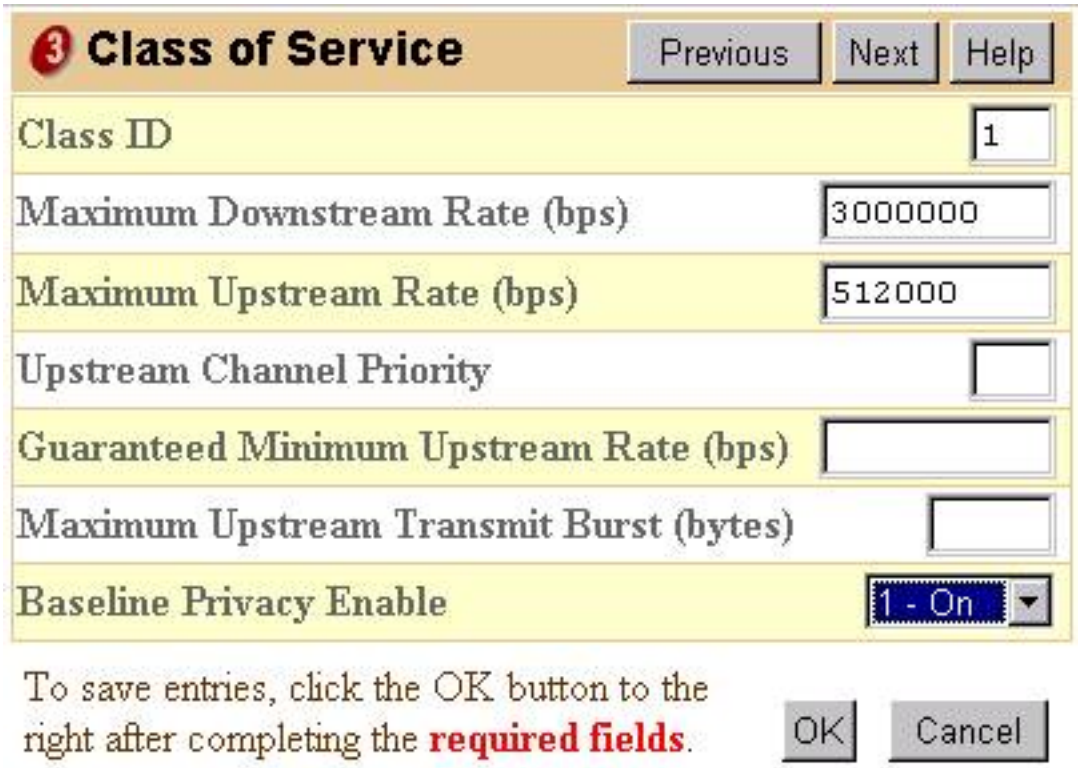
Les informations dans ce document sont basées sur configurer une version de logiciel 12.1(6)EC courante de Cisco IOS® uBR7246VXR, mais elles appliquent également à tous autres Produits et versions logicielles de Cisco CMTS.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

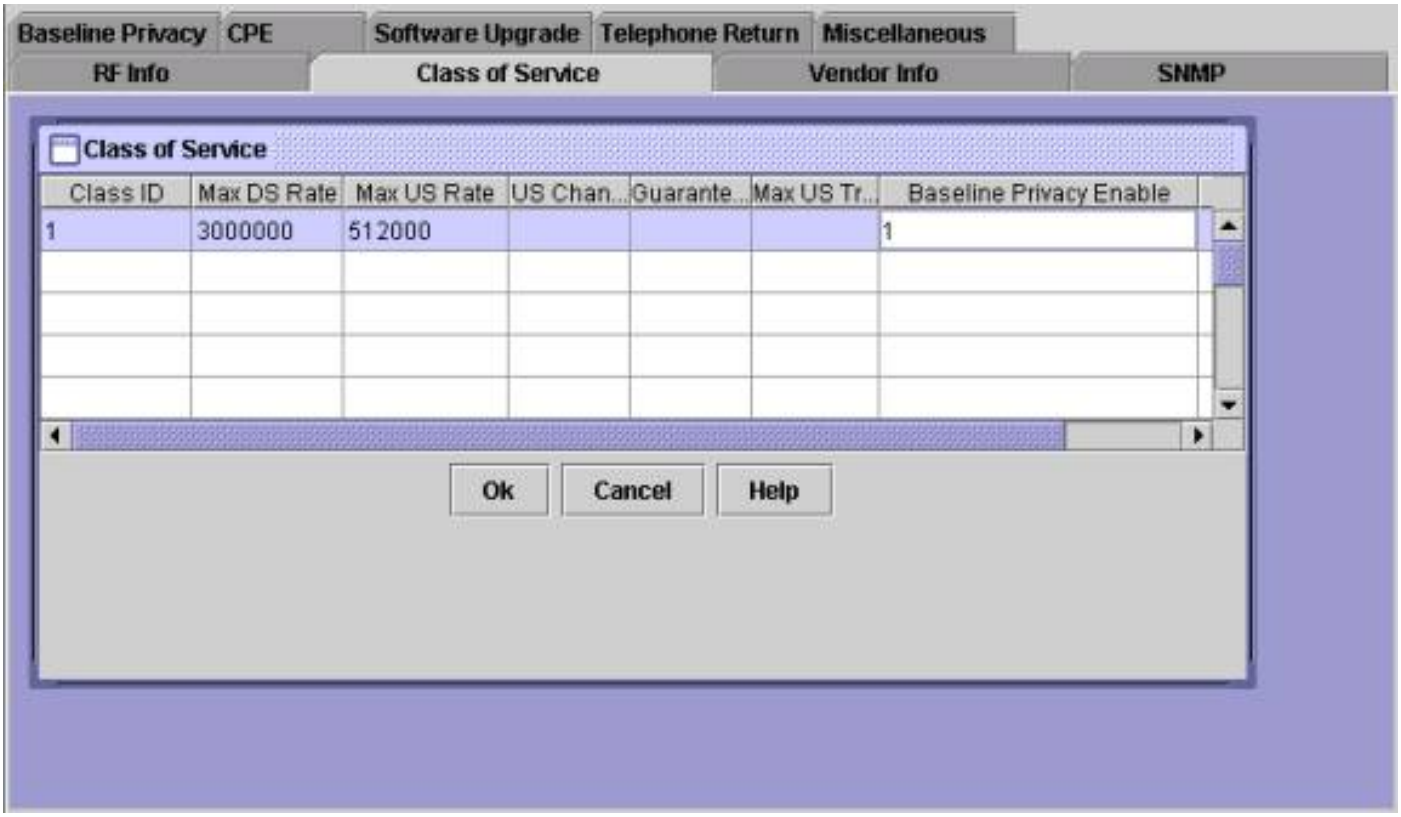
Comment configurer la sécurisation de base pour des Modems câble

Un modem câble tentera seulement d'utiliser la sécurisation de base si on lui commande de faire ainsi par l'intermédiaire des paramètres de classe de service dans un fichier de configuration DOCSIS. Le fichier de configuration DOCSIS contient des paramètres opérationnels pour le modem, et est téléchargé par le TFTP en tant qu'élément du processus d'être livré en ligne.

Une méthode de créer un fichier de configuration DOCSIS est d'utiliser le configurateur de modem câblé de câble DOCSIS sur Cisco.com. Utilisant le configurateur de modem câblé de câble DOCSIS, vous pouvez créer un fichier de configuration DOCSIS qui commande un modem câble d'utiliser la sécurisation de base en plaçant le champ d'enable de sécurisation de base sous l'onglet de classe de service à **en fonction**. Référez-vous à l'exemple ci-dessous :



Alternativement, la version autonome de la configuration de fichier DOCSIS du du pouvoir être utilisé pour activer la sécurisation de base comme affiché ci-dessous :



Une fois qu'un fichier de configuration DOCSIS prenant en charge le BPI a été créé, des Modems câble devront être remis à l'état initial afin de télécharger le nouveau fichier de configuration et utiliser ultérieurement la sécurisation de base.

Comment dire si un modem câble utilise la sécurisation de base

Sur Cisco CMTS, on peut utiliser la commande de show cable modem de visualiser l'état des modems câble individuels. Il y a plusieurs déclarer dans lesquels un modem utilisant la sécurisation de base peut apparaître.

en ligne

Après qu'un modem câble s'inscrive à Cisco CMTS il entre dans l'état en ligne. Un modem câble doit obtenir à cet état avant qu'il puisse être en pourparlers des paramètres de sécurisation de base avec Cisco CMTS. En ce moment le trafic de données envoyé entre le modem câble et le CMTS est décrypté. Si un modem câble reste dans cet état et ne poursuit pas aux états l'uns des mentionnés ci-dessous, alors le modem n'utilise pas la sécurisation de base.

online(pk)

L'état d'online(pk) signifie que le modem câble a pu négocier une **clé d'autorisation**, autrement connu comme **clé de chiffrement à clé (KEK)** avec Cisco CMTS. Ceci signifie que le modem câble est autorisé à utiliser la sécurisation de base et a été réussi en négociant la première phase de la sécurisation de base. Le KEK est un 56 principal de bit utilisé pour protéger des négociations ultérieures de sécurisation de base. Quand un modem est dans le trafic de données d'état d'online(pk) envoyé entre le modem câble et Cisco CMTS est encore décrypté car aucune clé pour le cryptage du trafic de données n'a été négociée encore. Typiquement, l'online(pk) est suivi par l'online(pt).

reject(pk)

Cet état indique que les tentatives du modem câble de négocier un KEK ont manqué. La raison la plus commune pour laquelle un modem serait dans cet état serait que Cisco CMTS a l'authentification de modem activée et le modem a l'authentification défaillante.

online(pt)

En ce moment le modem a avec succès été en pourparlers une clé de cryptage du trafic (TEK) avec Cisco CMTS. Le TEK est utilisé pour chiffrer le trafic de données entre le modem câble et Cisco CMTS. Le procédé de négociation TEK est chiffré utilisant le KEK. Le TEK est un 56 ou 40 principal de bit utilisé pour chiffrer le trafic de données entre le modem câble et Cisco CMTS. En ce moment la sécurisation de base est avec succès établie et s'exécutante, donc des données transmises d'utilisateur entre Cisco CMTS et modem câble sont chiffrées.

reject(pt)

Cet état indique que le modem câble ne pouvait pas être en pourparlers avec succès un TEK avec Cisco CMTS.

Voir ci-dessous pour un résultat témoin d'une commande de show cable modem affichant des Modems câble dans divers états liés à la sécurisation de 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
```

Remarque: Pour plus d'informations sur l'état de modem câble, référez-vous aux Modems câble d'ubr de dépannage n'étant pas livré en ligne.

Temporisateurs affectant l'établissement et la maintenance de la sécurisation de base

Il y a certaines valeurs du dépassement de durée qui peuvent être modifiées pour changer le comportement de la sécurisation de base. Certains de ces paramètres peuvent être configurés sur Cisco CMTS et d'autres par le fichier de configuration DOCSIS. Il y a peu de raison de changer l'un de ces paramètres excepté la vie KEK et la vie TEK. Ces temporisateurs peuvent être modifiés pour augmenter la Sécurité sur une usine de câble ou pour réduire la CPU et pour trafiquer en raison supplémentaire de la Gestion BPI.

Vie KEK

La vie KEK est la durée que le modem câble et Cisco CMTS devraient considérer comme étant le KEK négocié valides. Avant que cette durée ait passé, le modem câble devrait renégocier un nouveau KEK avec Cisco CMTS.

Vous pouvez configurer cette fois utilisant la commande d'interface de câble de Cisco CMTS :

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

La valeur par défaut est de 604800 secondes qui est égale à sept jours.

Avoir une plus petite vie KEK augmente la Sécurité parce que chaque volonté KEK durent pendant une période plus courte et par conséquent si le KEK est entaillé moins de négociations du futur TEK seraient susceptibles d'être détourné. L'inconvénient à ceci est que la renégociation KEK augmente l'utilisation du processeur sur des Modems câble et augmente le trafic d'administration BPI sur une usine de câble.

Délai de grâce KEK

Le délai de grâce KEK est la durée avant que la vie KEK expire, cela qu'un modem câble est censé pour commencer être en pourparlers avec Cisco CMTS pour un nouveau KEK. L'idée derrière avoir ce temporisateur est de sorte que le modem câble ait assez de temps de renouveler le KEK avant qu'il expire.

Vous pouvez configurer cette fois utilisant la commande d'interface de câble de Cisco CMTS :

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

Vous pouvez également configurer cette fois utilisant un fichier de configuration DOCSIS en complétant le champ étiqueté **délai d'attente de grâce d'autorisation** sous l'onglet de sécurisation de base. Si ce gisement de fichier de configuration DOCSIS est complété puis il a la priorité au-dessus de n'importe quelle valeur configurée sur Cisco CMTS. La valeur par défaut pour ce temporisateur est de 600 secondes qui est égal à 10 minutes.

Vie TEK

La vie TEK est la durée que le modem câble et Cisco CMTS devraient considérer comme étant le TEK négocié valides. Avant que cette durée ait passé, le modem câble devrait renégocier un nouveau TEK avec Cisco CMTS.

Vous pouvez configurer cette fois utilisant la commande d'interface de câble de Cisco CMTS :

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

La valeur par défaut est de 43200 secondes qui est égale à 12 heures.

Avoir une plus petite vie TEK augmente la Sécurité parce que chaque volonté TEK durent pendant une période plus courte et par conséquent si le TEK est entaillé moins de données seront exposées au déchiffrement non autorisé. L'inconvénient à ceci est que la renégociation TEK augmente l'utilisation du processeur sur des Modems câble et augmente le trafic d'administration BPI sur une usine de câble.

Délai de grâce TEK

Le délai de grâce TEK est la durée avant que la vie TEK expire qu'un modem câble est censé pour commencer être en pourparlers avec Cisco CMTS pour un nouveau TEK. L'idée derrière avoir ce temporisateur est de sorte que le modem câble ait assez de temps de renouveler le TEK avant qu'il expire.

Vous pouvez configurer cette fois utilisant la commande d'interface de câble de Cisco CMTS :

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

Vous pouvez également configurer cette fois utilisant un fichier de configuration DOCSIS en complétant le champ étiqueté **délai d'attente de grâce TEK** sous l'onglet de sécurisation de base. Si ce gisement de fichier de configuration DOCSIS est complété puis il a la priorité au-dessus de n'importe quelle valeur configurée sur Cisco CMTS.

La valeur par défaut pour ce temporisateur est de 600 secondes qui est égal à 10 minutes.

Autorisez le délai d'attente

Cette fois régit la durée qu'un modem câble attendra une réponse de Cisco CMTS quand négociant un KEK pour la première fois.

Vous pouvez configurer cette fois dans un fichier de configuration DOCSIS en modifiant le champ de **délai d'attente d'autorisation** sous l'onglet de sécurisation de base.

La valeur par défaut pour ce champ est de 10 secondes et la plage valide est de 2 à 30 secondes.

Reauthorize le délai d'attente

Cette fois régit la durée qu'un modem câble attendra une réponse de Cisco CMTS quand négociant un nouveau KEK parce que la vie KEK est sur le point d'expirer.

Vous pouvez configurer cette fois dans un fichier de configuration DOCSIS en modifiant le champ de **délai d'attente de Reauthorize** sous l'onglet de sécurisation de base.

La valeur par défaut pour ce temporisateur est de 10 secondes et la plage valide est de 2 à 30 secondes.

Délai d'attente de grâce d'autorisation

Spécifie le délai de grâce pour la réautorisation (en quelques secondes). La valeur par défaut est 600. La plage valide est de 1 à 1800 secondes.

Autorisez le délai d'attente d'anomalie

Si des essais d'un modem câble pour être en pourparlers un KEK avec Cisco CMTS, mais est rejetés, il doit attendre le délai d'attente d'anomalie d'autorisation avant de re-tenter pour négocier un nouveau KEK.

Vous pouvez configurer ce paramètre dans un fichier de configuration DOCSIS à l'aide du champ de **délai d'attente d'anomalie d'autorisation** sous l'onglet de sécurisation de base. La valeur par défaut pour ce temporisateur est de 60 secondes et la plage valide est de 10 secondes à de 600 secondes.

Délai d'attente opérationnel

Cette fois régit la durée qu'un modem câble attendra une réponse de Cisco CMTS quand négociant un TEK pour la première fois.

Vous pouvez configurer cette fois dans un fichier de configuration DOCSIS en modifiant le champ **opérationnel de délai d'attente** sous l'onglet de sécurisation de base.

La valeur par défaut pour ce champ est 1 seconde et la plage valide est de 1 à 10 secondes.

Délai d'attente de rekey

Cette fois régit la durée qu'un modem câble attendra une réponse de Cisco CMTS quand négociant un nouveau TEK parce que la vie TEK est sur le point d'expirer.

Vous pouvez configurer cette fois dans un fichier de configuration DOCSIS en modifiant le champ de **délai d'attente de rekey** sous l'onglet de sécurisation de base.

La valeur par défaut pour ce temporisateur est 1 seconde et la plage valide est de 1 à 10 secondes.

Commandes de configuration de sécurisation de base de Cisco CMTS

Les commandes suivantes d'interface de câble peuvent être utilisées pour configurer des fonctions relatives à la vie privée de sécurisation de base et de spécification de base sur Cisco CMTS.

cable privacy

Les commandes enables de cable privacy la négociation de la sécurisation de base sur une interface spécifique. Si l'**aucune** commande de **cable privacy** n'est configurée sur une interface de câble, alors on ne permettra à aucun Modems câble pour négocier la sécurisation de base quand étant livré en ligne sur cette interface. La précaution d'usage en désactivant la sécurisation de base parce que si un modem câble est commandé d'utiliser la sécurisation de base par son fichier de configuration DOCSIS, et Cisco CMTS refuse de le permettre de négocier la sécurisation de base, alors le modem peut ne pas pouvoir rester en ligne.

cable privacy obligatoire

Si la commande **obligatoire de cable privacy** est configurée et un modem câble a la sécurisation de base activée dans son fichier de configuration DOCSIS, alors le modem câble doit avec succès négocier et sécurisation de base d'utilisation autrement il ne sera pas permis de rester en ligne.

Si le fichier de configuration DOCSIS d'un modem câble ne demande pas au modem d'utiliser la sécurisation de base puis la commande **obligatoire de cable privacy** n'arrêtera pas le modem de rester en ligne.

La commande **obligatoire de cable privacy** n'est pas activée par défaut.

authentifier-modem de cable privacy

Il est possible d'exécuter une forme d'authentification pour les Modems qui s'engagent dans la sécurisation de base. Quand les Modems câble sont en pourparlers un KEK avec Cisco CMTS, les Modems transmettent des détails de leur adresse MAC de 6 octets et de leur numéro de série à Cisco CMTS. Ces paramètres peuvent être utilisés comme combinaison de nom d'utilisateur/mot de passe afin d'authentifier des Modems câble. Cisco CMTS utilise le service d'authentification, d'autorisation et de comptabilité de Cisco IOS (AAA) de faire ceci. On ne permet pas aux des Modems câble qui échouent authentification pour aller en ligne. En outre, des Modems câble qui n'utilisent pas la sécurisation de base ne sont pas affectés par cette commande.

Attention : Puisque cette caractéristique se sert du service d'AAA vous devez s'assurer que vous faites attention en modifiant la configuration d'AAA, autrement vous pouvez par distraction perdre la capacité de se connecter dans et de gérer votre Cisco CMTS.

Voici quelques configurations d'échantillon pour que les manières exécutent l'authentification de modem. Dans ces exemples de configuration, un certain nombre de Modems ont été entrés dans une base de données d'authentification. L'adresse MAC de 6 octets du modem sert de nom d'utilisateur et le numéro de série de longueur variable sert de mot de passe. Notez qu'un modem a été configuré avec un numéro de série évidemment incorrect.

La configuration partielle suivante de Cisco CMTS témoin emploie une base de données d'authentification locale pour authentifier un certain nombre de Modems câble.

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

Une autre méthode d'authentifier des Modems serait d'employer un serveur RADIUS externe. Voici un exemple partiel de configuration de Cisco CMTS qui utilise un serveur RADIUS externe pour authentifier des Modems

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

Est ci-dessous un fichier de base de données d'utilisateurs RADIUS témoin avec les informations équivalentes à l'exemple au-dessus duquel a utilisé l'authentification locale. Le fichier d'utilisateurs ser par un certain nombre de serveurs commerciaux et de logiciel gratuit de RADIUS d'une base de données où les informations d'authentification de l'utilisateur sont stockées.

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

Affichée ci-dessous est la sortie d'une commande de **show cable modem** exécutée sur Cisco CMTS ce qui utilise l'un ou l'autre des exemples de configuration ci-dessus. Vous verrez que n'importe quelle sécurisation de base a activé des Modems non répertoriés dans la base de données d'authentification locale, ou avec le numéro de série incorrect entrera dans l'état de **reject(pk)** et ne restera pas en ligne.

```
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
```

Le modem avec SID 17 n'a pas une entrée dans la base de données d'authentification mais peut être livré en ligne parce que son fichier de configuration DOCSIS ne l'a pas commandée d'utiliser la sécurisation de base.

Les Modems avec SID 18, 21 et 22 peuvent être livré en ligne parce qu'ils ont les entrées correctes dans la base de données d'authentification

Le modem avec SID 19 ne peut pas être livré en ligne parce qu'on lui a commandé d'utiliser la sécurisation de base mais il n'y a aucune entrée dans la base de données d'authentification pour

ce modem. Ce modem aurait récemment été dans l'état de reject(pk) pour indiquer qu'il authentification défaillante.

Le modem avec SID 20 ne peut pas être livré en ligne parce que, bien qu'il y ait une entrée dans la base de données d'authentification avec l'adresse MAC de ce modem, le numéro de série correspondant est incorrect. Actuellement ce modem est dans l'état de reject(pk) mais transition vers l'état hors ligne après une brève période.

Quand l'authentification d'échouer de Modems un message le long des lignes suivantes est ajoutée au log de Cisco CMTS.

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

Le modem câble est alors retiré de la liste de maintenance de station et sera marqué en tant qu'off-line dans 30 secondes. Le modem câble essayera alors très probablement d'être livré sur la ligne de nouveau à rejeter seulement de nouveau.

Remarque: Cisco ne recommande pas que les clients utilisent la commande d'authentifier-**modem de cable privacy** d'arrêter les Modems câble non autorisés d'être livré en ligne. Plus de façon efficace de s'assurer que les clients non autorisés n'obtiennent pas l'accès à un fournisseur de services est de configurer le système de ravitaillement tels que des Modems câble non autorisés sont chargés pour télécharger un fichier de configuration DOCSIS avec le champ d'accès au réseau réglé à hors fonction. De cette façon, le modem ne gaspillera pas l'importante bande passante amont re-en s'étendant continuellement. Au lieu de cela, le modem obtiendra à l'**en ligne (d) l'**état qui indique que des utilisateurs derrière le modem ne seront pas accordés le réseau et le modem de fournisseur d'accès aux services utilisera seulement la bande passante amont pour la maintenance de station.

Commandes utilisées pour surveiller l'état de BPI

intimité du show interface cable X/0 [kek | tek] — cette commande est utilisée d'afficher les temporisateurs associés avec le KEK ou le TEK comme place sur une interface CMTS.

Est ci-dessous un exemple de sortie de cette commande.

```
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
```

statistique d'intimité du show interface cable X/0 — Cette commande masquée peut être utilisée pour visualiser des statistiques sur le nombre de SID utilisant la sécurisation de base sur une interface de câble particulière.

Est ci-dessous un exemple de sortie de cette commande.

```
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 — Cette commande lance l'élimination des imperfections de la sécurisation de base. Quand cette commande est lancée, toutes les fois qu'un changement d'état de sécurisation de base ou d'un événement de sécurisation de base se produit, des détails seront affichés sur la console. Cette commande fonctionne seulement une fois précédée avec le **câble d'interface de debug cable X/0** ou la commande de *mac-address de* ***mac-address de debug cable***.

debug cable bpiatp — Cette commande lance l'élimination des imperfections de la sécurisation de base. Quand cette commande est lancée, toutes les fois qu'un message de sécurisation de base est envoyé ou reçu par Cisco CMTS, le vidage mémoire hexadécimal du message sera affiché. Cette commande fonctionne seulement une fois précédée avec le **câble d'interface de debug cable X/0** ou la commande de *mac-address de* ***mac-address de debug cable***.

debug cable keyman — Cette élimination des imperfections lancée par commande de gestion des clés de sécurisation de base. Quand cette commande est lancée des coordonnées de la gestion des clés de sécurisation de base sont affichées.

Dépannage du BPI

Les Modems câble apparaissent en tant qu'en ligne plutôt que l'online(pt).

Si un modem apparaît dans un état en ligne plutôt qu'online(pt) alors il signifie généralement une de trois choses.

La première raison probable est que le modem câble n'a pas été donné un fichier de configuration DOCSIS spécifiant que le modem câble utilisent la sécurisation de base. Vérifiez que le fichier de configuration DOCSIS a le BPI activé dans le profil de classe de service envoyé au modem.

La deuxième cause de voir un modem in l'état en ligne pourrait être que le modem attend avant qu'il débute le BPI de négociation. Attendez une minute ou deux pour voir si le modem change l'état à l'online(pt).

La cause finale pourrait être que le modem ne contient pas le micrologiciel qui prend en charge la sécurisation de base. Contactez votre constructeur de modem pour une version du microprogramme plus récente qui prend en charge le BPI.

Les Modems câble apparaissent dans l'état de reject(pk) puis vont off-line.

La cause le plus susceptible d'un modem écrivant l'état de reject(pk) est que l'authentification de modem câble a été activée avec la commande d'authentifier-**modem de cable privacy** mais l'AAA misconfigured. Vérifiez que les numéros de série et les adresses de MAC des Modems affectés

ont été correctement introduits dans la base de données d'authentification et que n'importe quel serveur RADIUS externe est accessible et fonctionnement. Vous pouvez employer le **debug aaa authentication** et le **debug radius de** commandes de débogage de routeur pour avoir une idée de l'état du serveur de RADIUS ou pourquoi un modem est authentification manquante.

Remarque: Pour des informations générales sur la Connectivité de modem câble de dépannage, référez-vous aux Modems câble d'ubr de dépannage n'étant pas livré en ligne.

Note spéciale - Commandes masquées

N'importe quelle référence aux commandes masquées dans ce document est à des fins d'information seulement. Des commandes masquées ne sont pas prises en charge par le centre d'assistance technique Cisco (TAC). En outre commandes masquées :

- Ne peut pas toujours générer fiable ou les informations correctes
- Effets secondaires inattendus de cause de mai si exécuté
- Ne peut pas se comporter la même manière dans les différentes versions du logiciel de Cisco IOS
- Peut être retiré des versions futures de logiciel de Cisco IOS à tout moment sans préavis

Informations connexes

- CableLabs
- Configurateur CPE DOCSIS
- Authentification, autorisation et comptabilité (AAA)
- Support technique - Cisco Systems