Confidentialité de base DOCSIS 1.0 sur Cisco CMTS

Contenu

Introduction

L'objectif principal de l'interface de ligne de base (BPI) DOCSIS (Data-over-Cable Service Interface Specifications) est de fournir un système de cryptage des données simple pour protéger les données envoyées aux modems câble et en provenance de ces derniers dans un réseau Data over Cable. La confidentialité de la ligne de base peut également être utilisée comme moyen d'authentifier les modems câble et d'autoriser la transmission du trafic de multidiffusion vers les modems câble.

Les produits CMTS (Cable Modem Termination System) et les modems câble Cisco exécutant

des images logicielles Cisco IOS® avec un jeu de fonctions comprenant les caractères « k1 » ou « k8 » prennent en charge la confidentialité de base, par exemple ubr7200-k1p-mz.121-6.EC1.bin.

Ce document traite de la confidentialité de base sur les produits Cisco fonctionnant en 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.

Components Used

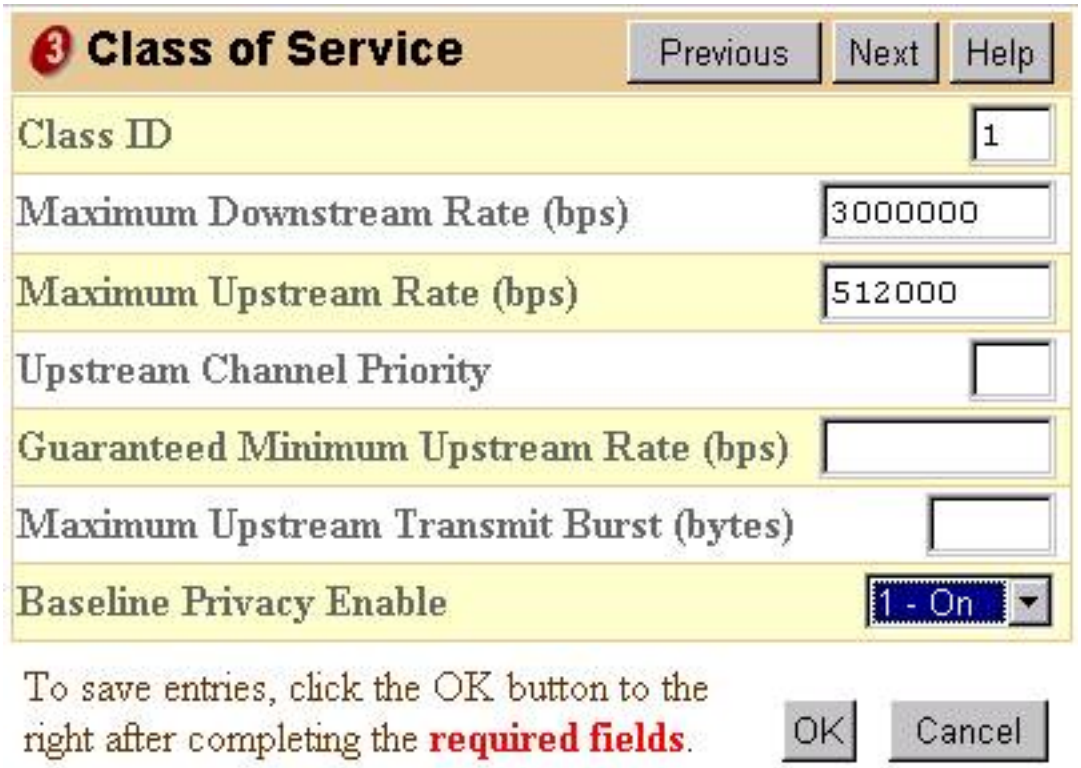
Les informations de ce document sont basées sur la configuration d'un uBR7246VXR exécutant le logiciel Cisco IOS® Version 12.1(6)EC, mais elles s'appliquent également à tous les autres produits et versions de logiciel Cisco CMTS.

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

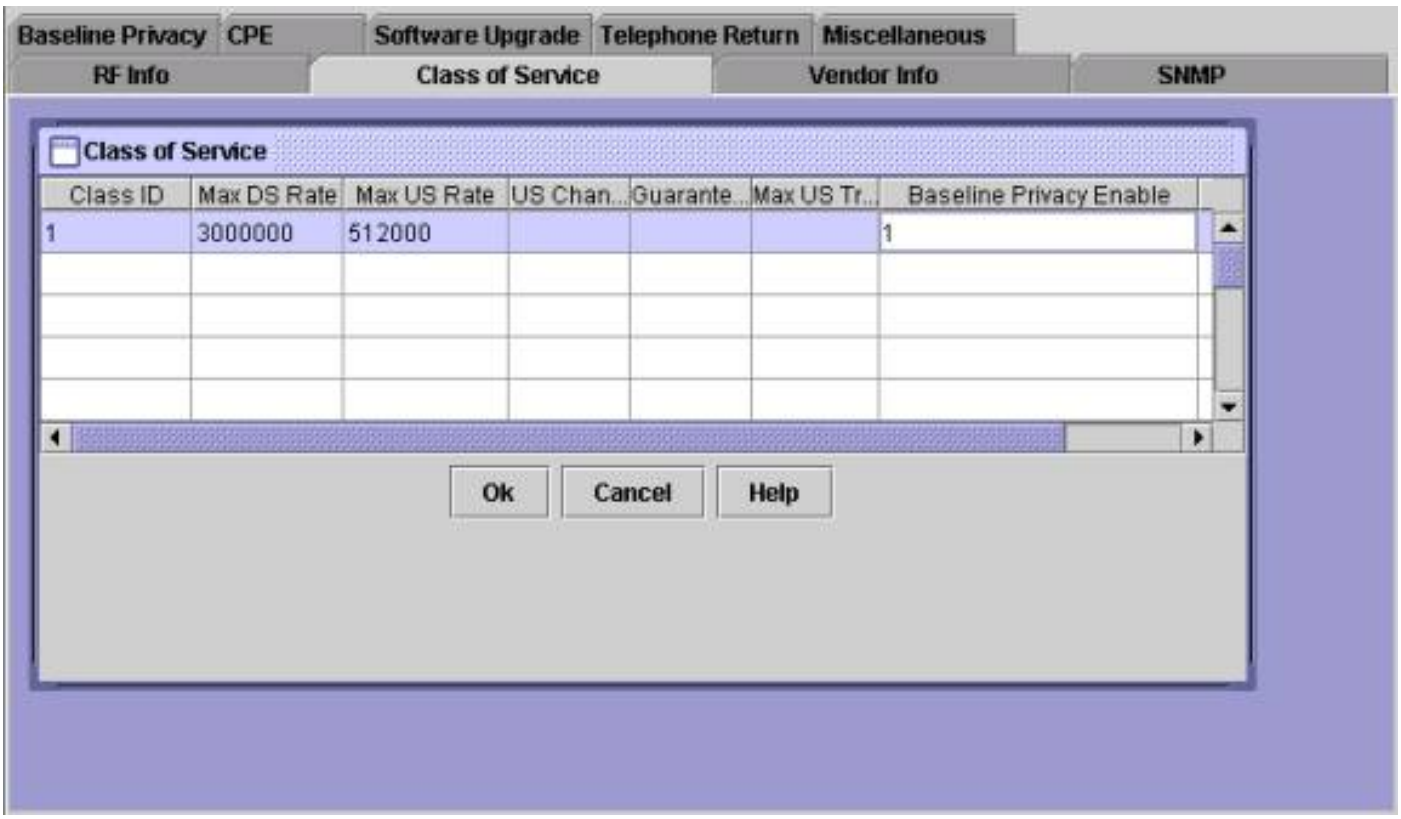
Comment configurer la confidentialité de base pour les modems câble

Un modem câble ne tente d'utiliser la confidentialité de la ligne de base que s'il est ordonné de le faire via les paramètres de classe de service dans un fichier de configuration DOCSIS. Le fichier de configuration DOCSIS contient les paramètres opérationnels du modem et est téléchargé via TFTP dans le cadre du processus de mise en ligne.

Une méthode de création d'un fichier de configuration DOCSIS consiste à utiliser le configurateur de modem câble DOCSIS sur Cisco.com. À l'aide du configurateur de modem câble DOCSIS, vous pouvez créer un fichier de configuration DOCSIS qui commande à un modem câble d'utiliser la Confidentialité de base en définissant le champ Baseline Privacy Enable sous l'onglet Classe de service sur **On**. Reportez-vous à l’exemple ci-dessous :



Vous pouvez également utiliser la version autonome de la configuration de fichier DOCSIS à partir de pour activer la Confidentialité de base, comme indiqué ci-dessous :



Une fois qu'un fichier de configuration DOCSIS prenant en charge BPI a été créé, les modems câble doivent être réinitialisés pour télécharger le nouveau fichier de configuration et utiliser ensuite la confidentialité de la ligne de base.

Comment savoir si un modem câble utilise la confidentialité de base

Sur un système CMTS Cisco, vous pouvez utiliser la commande show cable modem pour afficher l'état de chaque modem câble. Il existe plusieurs états dans lesquels un modem utilisant la confidentialité de la ligne de base peut apparaître.

en ligne

Une fois qu'un modem câble s'enregistre auprès d'un système Cisco CMTS, il passe à l'état en ligne. Un modem câble doit accéder à cet état avant de pouvoir négocier les paramètres de confidentialité de la ligne de base avec un CMTS Cisco. À ce stade, le trafic de données envoyé entre le modem câble et le CMTS n'est pas chiffré. Si un modem câble reste dans cet état et ne passe à aucun des états mentionnés ci-dessous, le modem n'utilise pas la confidentialité de la ligne de base.

en ligne(pk)

L'état en ligne (pk) signifie que le modem câble a pu négocier une **clé d'autorisation**, également appelée **clé de chiffrement de clé (KEK)** avec le système CMTS Cisco. Cela signifie que le modem câble est autorisé à utiliser la confidentialité de base et a réussi à négocier la première phase de confidentialité de base. La clé KEK est une clé de 56 bits utilisée pour protéger les négociations de confidentialité de base ultérieures. Lorsqu'un modem est en ligne (pk), le trafic de données envoyé entre le modem câble et Cisco CMTS n'est toujours pas chiffré car aucune clé de chiffrement du trafic de données n'a encore été négociée. En général, online(pk) est suivi de online(pt).

rejeter(pk)

Cet état indique que les tentatives du modem câble pour négocier une clé KEK ont échoué. La raison la plus courante pour laquelle un modem serait dans cet état est que l'authentification par modem est activée sur le CMTS Cisco et que l'authentification par modem a échoué.

en ligne(pt)

Àce stade, le modem a négocié avec succès une clé de cryptage du trafic (TEK) avec le système CMTS Cisco. Le TEK est utilisé pour chiffrer le trafic de données entre le modem câble et Cisco CMTS. Le processus de négociation TEK est chiffré à l'aide de la clé KEK. Le TEK est une clé de 56 ou 40 bits utilisée pour chiffrer le trafic de données entre le modem câble et le système de terminaison de circuit intégré Cisco. À ce stade, la confidentialité de la ligne de base est correctement établie et en cours d'exécution. Par conséquent, les données utilisateur envoyées entre Cisco CMTS et le modem câble sont chiffrées.

rejeter(pt)

Cet état indique que le modem câble n'a pas pu négocier un TEK avec le CMTS Cisco.

Reportez-vous à la section ci-dessous pour obtenir un exemple de résultat d'une commande show cable modem montrant les modems câble dans différents états liés à la confidentialité de la ligne 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 du modem câble, référez-vous à Dépannage des modems câble uBR non disponibles en ligne.

Temporisateurs affectant l'établissement et le maintien de la vie privée de base

Certaines valeurs de délai d'attente peuvent être modifiées pour modifier le comportement de la confidentialité de la ligne de base. Certains de ces paramètres peuvent être configurés sur Cisco CMTS et d'autres via le fichier de configuration DOCSIS. Il y a peu de raisons de modifier ces paramètres à l'exception de la durée de vie de KEK et de la durée de vie de TEK. Ces temporisateurs peuvent être modifiés pour renforcer la sécurité sur une installation de câblage ou pour réduire la charge de CPU et de trafic due à la gestion BPI.

Durée de vie de KEK

La durée de vie de la clé est la durée pendant laquelle le modem câble et le système CMTS Cisco doivent considérer la clé négociée comme valide. Avant que ce délai ne soit écoulé, le modem câble doit renégocier une nouvelle clé avec le système Cisco CMTS.

Vous pouvez configurer cette fois à l'aide de la commande d'interface de câble Cisco CMTS :

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

Le paramètre par défaut est 604800 secondes, soit sept jours.

La réduction de la durée de vie de la clé augmente la sécurité, car chaque clé durera plus longtemps et, par conséquent, si la clé est piratée, moins de futures négociations de la clé seront susceptibles d'être piratées. L'inconvénient est que la renégociation KEK augmente l'utilisation du CPU sur les modems câble et augmente le trafic de gestion BPI sur une installation de câblage.

Durée de grâce KEK

Le délai de grâce KEK est le délai avant l'expiration de la durée de vie KEK, pendant lequel un modem câble est censé commencer à négocier avec le CMTS Cisco pour une nouvelle clé KEK. L'idée derrière cette temporisation est que le modem câble dispose de suffisamment de temps pour renouveler la clé avant son expiration.

Vous pouvez configurer cette fois à l'aide de la commande d'interface de câble Cisco CMTS :

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

Vous pouvez également configurer cette fois-ci à l'aide d'un fichier de configuration DOCSIS en remplissant le champ **Authorization Grace Timeout** sous l'onglet Baseline Privacy. Si ce champ de fichier de configuration DOCSIS est renseigné, il est prioritaire sur toute valeur configurée sur le système CMTS Cisco. La valeur par défaut de ce compteur est 600 secondes, soit 10 minutes.

Durée de vie du TEK

La durée de vie du TEK est la durée pendant laquelle le modem câble et le CMTS Cisco doivent considérer le TEK négocié comme valide. Avant que ce délai ne soit écoulé, le modem câble doit renégocier un nouveau TEK avec le CMTS Cisco.

Vous pouvez configurer cette fois à l'aide de la commande d'interface de câble Cisco CMTS :

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

Le paramètre par défaut est 43 200 secondes, soit 12 heures.

La réduction de la durée de vie du TEK augmente la sécurité car chaque TEK durera plus longtemps et, par conséquent, si le TEK est piraté, moins de données seront exposées au déchiffrement non autorisé. L'inconvénient est que la renégociation du TEK augmente l'utilisation du CPU sur les modems câble et augmente le trafic de gestion BPI sur une installation de câblage.

TEK Grace Time

Le délai de grâce TEK est le délai avant l'expiration de la durée de vie TEK pendant lequel un modem câble est censé commencer à négocier avec le CMTS Cisco pour un nouveau TEK. L'idée de disposer de ce compteur est de sorte que le modem câble dispose de suffisamment de temps pour renouveler le TEK avant son expiration.

Vous pouvez configurer cette fois à l'aide de la commande d'interface de câble Cisco CMTS :

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

Vous pouvez également configurer cette fois-ci à l'aide d'un fichier de configuration DOCSIS en remplissant le champ **TEK Grace Timeout** sous l'onglet Baseline Privacy. Si ce champ de fichier de configuration DOCSIS est renseigné, il est prioritaire sur toute valeur configurée sur le système CMTS Cisco.

La valeur par défaut de ce compteur est 600 secondes, soit 10 minutes.

Autoriser le délai d'attente

Cette fois-ci régit la durée pendant laquelle un modem câble attend une réponse d'un système CMTS Cisco lors de la négociation d'une clé pour la première fois.

Vous pouvez configurer cette heure dans un fichier de configuration DOCSIS en modifiant le champ **Autoriser le délai d'attente** sous l'onglet Confidentialité de la ligne de base.

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

Réautoriser le délai d'attente

Cette fois-ci régit la durée pendant laquelle un modem câble attend une réponse d'un CMTS Cisco lors de la négociation d'une nouvelle clé KEK, car la durée de vie de la clé KEK est sur le point d'expirer.

Vous pouvez configurer cette heure dans un fichier de configuration DOCSIS en modifiant le champ **ReAuthorization Wait Timeout** sous l'onglet Baseline Privacy.

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

Délai de grâce de l'autorisation

Spécifie le délai de grâce pour la réautorisation (en secondes). La valeur par défaut est 600. La plage valide est comprise entre 1 et 1 800 secondes.

Autoriser le délai d'attente de rejet

Si un modem câble tente de négocier une clé avec un système Cisco CMTS, mais qu'il est rejeté, il doit attendre le délai d'attente d'autorisation de rejet avant de tenter à nouveau de négocier une nouvelle clé.

Vous pouvez configurer ce paramètre dans un fichier de configuration DOCSIS à l'aide du champ **Autoriser le délai d'attente de rejet** sous l'onglet Confidentialité de la ligne de base. La valeur par défaut de ce compteur est 60 secondes et la plage valide est comprise entre 10 et 600 secondes.

Délai d'attente opérationnel

Cette fois-ci régit la durée pendant laquelle un modem câble attend une réponse d'un CMTS Cisco lors de la négociation d'un TEK pour la première fois.

Vous pouvez configurer cette heure dans un fichier de configuration DOCSIS en modifiant le champ **Operational Wait Timeout** sous l'onglet Baseline Privacy.

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

Délai d'attente de la nouvelle clé

Cette fois-ci régit la durée pendant laquelle un modem câble attend une réponse d'un CMTS Cisco lors de la négociation d'un nouveau TEK, car la durée de vie du TEK est sur le point d'expirer.

Vous pouvez configurer cette heure dans un fichier de configuration DOCSIS en modifiant le champ **Rekey Wait Timeout** sous l'onglet Baseline Privacy.

La valeur par défaut de ce compteur est 1 seconde et la plage valide est comprise entre 1 et 10 secondes.

Commandes de configuration de la confidentialité de la ligne de base de Cisco CMTS

Les commandes d'interface de câble suivantes peuvent être utilisées pour configurer les fonctions de confidentialité de ligne de base et de confidentialité de ligne de base sur un système CMTS Cisco.

confidentialité des câbles

La commande cable privacy permet de négocier la confidentialité de la ligne de base sur une interface particulière. Si la commande **no cable privacy** est configurée sur une interface de câble, aucun modems câble ne sera autorisé à négocier la confidentialité de la ligne de base lors de sa mise en ligne sur cette interface. Soyez prudent lorsque vous désactivez la confidentialité de la ligne de base, car si un modem câble est invité à utiliser la confidentialité de la ligne de base par son fichier de configuration DOCSIS et que le système CMTS de Cisco refuse de lui permettre de négocier la confidentialité de la ligne de base, le modem risque de ne pas pouvoir rester en ligne.

confidentialité des câbles obligatoire

Si la commande de **confidentialité obligatoire** du **câble** est configurée et qu'un modem câble a activé la confidentialité de la ligne de base dans son fichier de configuration DOCSIS, le modem câble doit négocier et utiliser correctement la confidentialité de la ligne de base, sinon il ne sera pas autorisé à rester en ligne.

Si le fichier de configuration DOCSIS d'un modem câble n'indique pas au modem d'utiliser la confidentialité de base, la commande **cable privacy Required** n'empêche pas le modem de rester en ligne.

La commande **de confidentialité des câbles obligatoire** n'est pas activée par défaut.

cable privacy authenticate-modem

Il est possible d'exécuter une forme d'authentification pour les modems qui s'engagent dans la vie privée de la ligne de base. Lorsque les modems câble négocient une clé avec le système Cisco CMTS, les modems transmettent les détails de leur adresse MAC de 6 octets et de leur numéro de série au système Cisco CMTS. Ces paramètres peuvent être utilisés comme combinaison nom d'utilisateur/mot de passe pour l'authentification des modems câble. Pour ce faire, Cisco CMTS utilise le service AAA (Authentication, Authorization and Accounting) de Cisco IOS. Les modems câble qui échouent à l'authentification ne sont pas autorisés à se connecter. En outre, les modems câble qui n'utilisent pas la confidentialité de la ligne de base ne sont pas affectés par cette commande.

Attention : Puisque cette fonctionnalité utilise le service AAA, vous devez vous assurer d'être prudent lors de la modification de la configuration AAA, sinon vous risquez de perdre la possibilité de vous connecter et de gérer votre système Cisco CMTS.

Voici quelques exemples de configuration pour les méthodes d'authentification par modem. Dans

ces exemples de configuration, un certain nombre de modems ont été entrés dans une base de données d'authentification. L'adresse MAC à 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 manifestement incorrect.

L'exemple partiel suivant de configuration Cisco CMTS utilise une base de données d'authentification locale pour authentifier un certain nombre de modems câble.

```
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
```

Une autre méthode d'authentification des modems consiste à utiliser un serveur RADIUS externe. Voici un exemple partiel de configuration de Cisco CMTS qui utilise un serveur RADIUS externe pour authentifier les modems

```
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
```

Vous trouverez ci-dessous un exemple de fichier de base de données d'utilisateurs RADIUS avec les informations équivalentes à l'exemple ci-dessus qui a utilisé l'authentification locale. Le fichier d'utilisateurs est utilisé par un certain nombre de serveurs RADIUS commerciaux et gratuits comme base de données où les informations d'authentification des utilisateurs sont stockées.

```
# 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
```

La sortie ci-dessous est celle d'une commande **show cable modem** exécutée sur un système CMTS Cisco qui utilise l'un des exemples de configuration ci-dessus. Vous verrez que tous les modems activés pour la confidentialité de la ligne de base qui ne figurent pas dans la base de données d'authentification locale ou dont le numéro de série est incorrect entreront l'état **de rejet(pk)** et ne resteront 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 d'entrée dans la base de données d'authentification, mais peut se connecter car son fichier de configuration DOCSIS ne lui a pas ordonné d'utiliser la confidentialité de la ligne de base.

Les modems dotés des SID 18, 21 et 22 peuvent être mis en ligne car ils ont des entrées correctes dans la base de données d'authentification

Le modem avec SID 19 ne peut pas se connecter car il a été commandé d'utiliser la confidentialité de la ligne de base, mais il n'y a aucune entrée dans la base de données d'authentification pour ce modem. Ce modem aurait été récemment dans l'état de rejet(pk) pour indiquer qu'il a échoué à l'authentification.

Le modem avec SID 20 ne peut pas se connecter car, 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. À l'heure actuelle, ce modem est en état de rejet (pk), mais il passera à l'état hors connexion après une courte période.

Lorsque l'authentification des modems échoue, un message suivant les lignes suivantes est ajouté au journal Cisco CMTS.

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

Le modem câble est ensuite retiré de la liste de maintenance de la station et sera marqué comme étant hors connexion dans les 30 secondes. Le modem câble tentera alors très probablement de se reconnecter et sera rejeté à nouveau.

Remarque : Cisco ne recommande pas aux clients d'utiliser la commande **cable privacy authenticate-modem** pour empêcher les modems câble non autorisés de se connecter. Une manière plus efficace de s'assurer que les clients non autorisés n'ont pas accès au réseau d'un fournisseur de services consiste à configurer le système de mise en service de sorte que les modems câble non autorisés soient invités à télécharger un fichier de configuration DOCSIS avec le champ d'accès réseau désactivé. De cette manière, le modem ne gaspillera pas une bande passante ascendante précieuse en redimensionnant continuellement. Au lieu de cela, le modem accède à l'état **online(d)** qui indique que les utilisateurs derrière le modem n'auront pas accès au réseau du fournisseur de services et que le modem n'utilisera que la bande passante en amont pour la maintenance de la station.

Commandes utilisées pour surveiller l'état des BPI

show interface cable X/0 privacy [kek | tek] : cette commande permet d'afficher les temporisateurs associés à la clé ou au TEK comme définis sur une interface CMTS.

Voici un exemple de résultat 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
```

show interface cable X/0 privacy statistics - Cette commande masquée peut être utilisée pour afficher des statistiques sur le nombre de SID utilisant la confidentialité de base sur une interface de câble particulière.

Voici un exemple de résultat 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 active le débogage de la confidentialité de la ligne de base. Lorsque cette commande est activée, chaque fois qu'une modification de l'état de confidentialité de la ligne de base ou un événement de confidentialité de la ligne de base se produit, les détails s'affichent sur la console. Cette commande ne fonctionne que lorsqu'elle est précédée de la commande **debug cable interface cable X/0** ou **debug cable mac-address** ***mac-address***.

debug cable bpiatp : cette commande active le débogage de la confidentialité de la ligne de base. Lorsque cette commande est activée, chaque fois qu'un message de confidentialité de la ligne de base est envoyé ou reçu par le système Cisco CMTS, le vidage hexadécimal du message s'affiche. Cette commande ne fonctionne que lorsqu'elle est précédée de la commande **debug cable interface cable X/0** ou **debug cable mac-address** ***mac-address***.

debug cable keyman : cette commande a activé le débogage de la gestion des clés de confidentialité de la ligne de base. Lorsque cette commande est activée, les détails de la gestion des clés de confidentialité de la ligne de base s'affichent.

Dépannage BPI

Les modems câble apparaissent en ligne plutôt qu'en ligne(pt).

Si un modem apparaît dans un état en ligne plutôt qu'en ligne(pt), cela signifie généralement l'une des trois choses suivantes.

La première raison probable est que le modem câble n'a pas reçu de fichier de configuration DOCSIS spécifiant que le modem câble utilise la confidentialité de base. Vérifiez que le BPI du fichier de configuration DOCSIS est activé dans le profil de classe de service envoyé au modem.

La deuxième raison de voir un modem en ligne pourrait être que le modem attend avant de commencer à négocier des BPI. Attendez une minute ou deux pour voir si le modem passe à l'état

en ligne(pt).

La dernière cause pourrait être que le modem ne contient pas de microprogramme prenant en charge la confidentialité de base. Contactez le fabricant de votre modem pour obtenir une version plus récente du micrologiciel prenant en charge BPI.

Les modems câble apparaissent en état de rejet (pk), puis passent hors connexion.

La cause la plus probable d'un modem entrant dans l'état de rejet (pk) est que l'authentification par modem câble a été activée avec la commande **cable privacy authenticate-modem** mais qu'AAA a été mal configuré. Vérifiez que les numéros de série et les adresses MAC des modems concernés ont été correctement entrés dans la base de données d'authentification et que tout serveur RADIUS externe est accessible et fonctionne. Vous pouvez utiliser les commandes de débogage du routeur **debug aaa authentication** et **debug radius** pour obtenir une idée de l'état du serveur RADIUS ou de la raison pour laquelle un modem échoue à l'authentification.

Remarque : Pour obtenir des informations générales sur le dépannage de la connectivité par modem câble, référez-vous à Dépannage des modems câble uBR non disponibles en ligne.

Remarque spéciale - Commandes masquées

Toute référence aux commandes masquées dans ce document est uniquement à titre d'information. Les commandes masquées ne sont pas prises en charge par le centre d'assistance technique Cisco (TAC). En outre, les commandes cachées :

- Peut ne pas toujours générer des informations fiables ou correctes
- Peut provoquer des effets secondaires inattendus si exécuté
- Peut ne pas se comporter de la même manière dans différentes versions du logiciel Cisco IOS
- Peut être supprimé des versions futures du logiciel Cisco IOS à tout moment et sans préavis

Informations connexes

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