Cisco CMTS での DOCSIS 1.0 ベースライン プライバシ

内容

概要

データオーバーケーブル サービス インターフェイス仕様（DOCSIS）ベースライン プライバシー インターフェイス（BPI）の主要な目的は、Data over Cable ネットワークでケーブル モデムを介して送受信されるデータを保護する簡単なデータ暗号化スキームを提供することです。ベースライン プライバシは、ケーブル モデムの認証、およびマルチキャスト トラフィックのケーブル モデムへの伝送の承認の手段としても使うことができます。

Cisco Cable Modem Termination System（CMTS）、および、文字「k1」または「k8」を含む機能セットを持つ Cisco IOS® ソフトウェア イメージを実行するケーブル モデム製品はベースライン プライバシを

サポートします。たとえば、ubr7200-k1p-mz.121-6.EC1.bin がこれにあたります。

この文書では、DOCSIS1.0 モードで動作するシスコ製品でのベースライン プライバシを取り上げます。

はじめに

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

前提条件

このドキュメントに関しては個別の前提条件はありません。

使用するコンポーネント

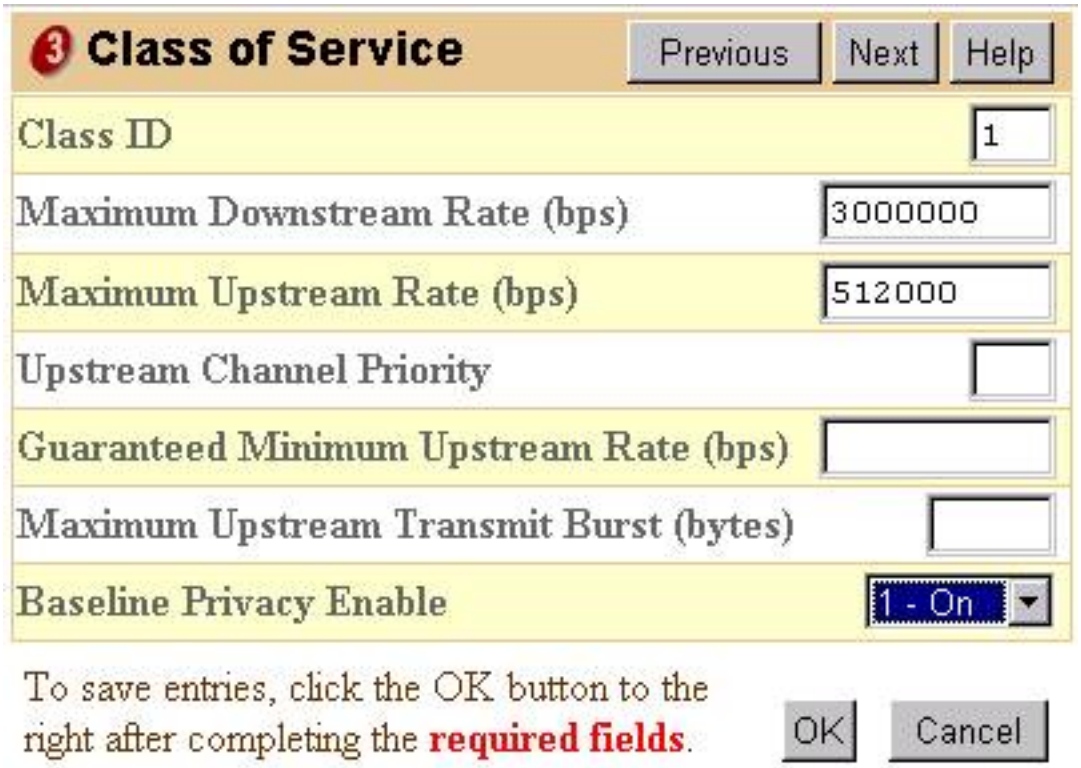
このドキュメントの情報は、Cisco IOS® ソフトウェア リリース 12.1(6)EC が稼働する uBR7246VXR の設定に基づいていますが、その他のすべての Cisco CMTS 製品とソフトウェア リリースにも適用されます。

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。実稼動中のネットワークで作業をしている場合、実際にコマンドを使用する前に、その潜在的な影響について理解しておく必要があります。

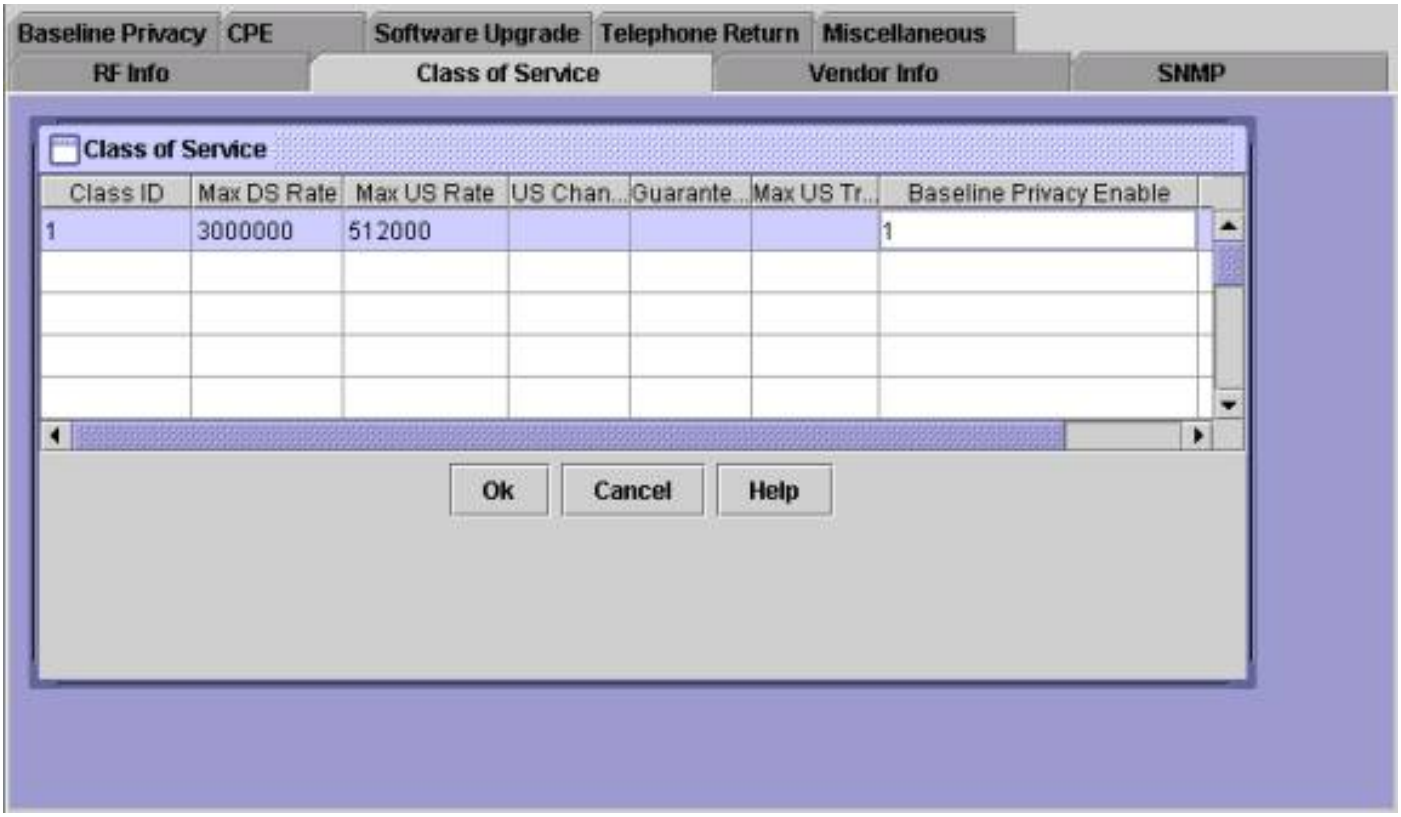
ケーブル モデムのためのベースライン プライバシの設定方法

ケーブル モデムは、DOCSIS 設定ファイルでサービス パラメータの Class 経由でベースライン プライバシを使うように命令された場合にのみ、これを試みます。DOCSIS コンフィギュレーション ファイルはモデムの動作パラメータを含んでおり、オンラインになる手順の一部として TFTP 経由でダウンロードされます。

DOCSIS コンフィギュレーション ファイルを作成するメソッドの 1 つは、Cisco.com 上の DOCSIS Cable Modem Configurator を使用することです。DOCSIS Cable Modem Configurator を使って、DOCSIS 設定ファイルを作成できます。このファイルでは Class of Service タブにある Baseline Privacy Enable フィールドを On にすることにより、ベースライン プライバシを使うようにケーブル モデムに命令します。次の例を参照してください。



あるいは、DOCSIS ファイル設定のスタンドアロン バージョンを使って、次のようにベースライン プライバシを有効にできます。



BPI をサポートする DOCSIS 設定ファイルが作成されると、新しい設定ファイルをダウンロードしてベースライン プライバシを適用するために、ケーブル モデムをリセットする必要があります。

ケーブル モデムがベースライン プライバシを使っているかどうかを識別する方法

Cisco CMTS では、show cable modem コマンドを使って個々のケーブル モデムの状態を表示できます。ベースライン プライバシを使っているモデムが示す状態には次のものがあります。

online

Cisco CMTS に登録すると、ケーブル モデムは online 状態になります。ケーブル モデムは、この状態になっていないと Cisco CMTS とベースライン プライバシ パラメータをネゴシエートできません。この時点では、ケーブル モデムと CMTS 間を伝送されるトラフィックは暗号化されていません。ケーブル モデムがこの状態のままで、次に述べるどの状態にも遷移していなければ、そのモデムはベースライン プライバシを利用していません。

online(pk)

online（pk）状態とは、ケーブル モデムが **Authorization Key** をネゴシエートできていることを表します。Cisco CMTS ではこれは **Key Encryption Key（KEK）として知られています。**このことは、ケーブル モデムがベースライン プライバシの使用を承認されており、ベースライン プライバシの第 1 フェーズのネゴシエーションに成功したことを意味します。KEK は 56 ビット キーで、あとに続くベースライン プライバシのネゴシエーションに使われます。モデムが online（pk）状態にあると、まだデータ トラフィックのための暗号化キーがネゴシエートされていないので、そのケーブル モデムと Cisco CMTS 間で伝送されるデータ トラフィックはまだ暗号化されていません。通常は、online（pk）のあとには、online（pt）が続きます。

reject(pk)

この状態は、ケーブル モデムが KEK へのネゴシエートを試みて失敗したことを示しています。モデムがこの状態になる最も一般的な理由は、Cisco CMTS がモデム認証をオンにしており、モデムが認証に失敗した場合です。

online(pt)

この時点で、モデムは Cisco CMTS との Traffic Encryption Key（TEK）のネゴシエーションに成功しています。TEK はケーブル モデムと Cisco CMTS 間のデータ トラフィックの暗号化に使われます。TEK ネゴシエーションの手順は KEK を使って暗号化されます。TEK は 56 あるいは 40 ビットのキーで、ケーブル モデムと Cisco CMTS 間のデータ トラフィックの暗号化に使用されます。この時点で、ベースライン プライバシは正しく確立されて実行中なので、Cisco CMTS とケーブル モデム間を伝送されるユーザ データは暗号化されています。

reject(pt)

この状態は、ケーブル モデムが Cisco CMTS と TEK をネゴシエートできなかったことを示しています。

ベースライン プライバシ関連の、さまざまな状態にあるケーブル モデムを表示する show cable modem コマンドの出力例は、次をご覧ください。

```
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
```

注：ケーブルモデムのステータスの詳細は、『uBRケーブルモデムがオンラインにならない場合のトラブルシューティング』を参照してください。

ベースライン プライバシの確立と維持に影響するタイマー

特定のタイムアウト値があり、これらを変更してベースライン プライバシの動作を変えることができます。パラメータによっては Cisco CMTS 上で設定でき、他のパラメータは DOCSIS コンフィギュレーション ファイルで設定できます。KEK lifetime と TEK lifetime 以外では、これらのパラメータを変更する意味はほとんどありません。これらのタイマーを変更すると、ケーブル プラントのセキュリティを向上させたり、BPI 管理による CPU とトラフィックのオーバーヘッドを削減することができます。

KEK Lifetime

KEK lifetime は、ケーブル モデムと Cisco CMTS が、ネゴシエートされた KEK を有効であると認識するのに要する時間です。この時間が経過する前に、ケーブル モデムは Cisco CMTS と新しい KEK を再ネゴシエートする必要があります。

この時間は Cisco CMTS cable interface コマンドを使って設定できます。

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

デフォルトの設定は 604800 秒で 7 日間に相当します。

KEK lifetime を少なくすることによりセキュリティが向上します。つまり、それぞれの KEK の存続時間がより短くなることによって、もし KEK がハッキングされても、TEK ネゴシエーションが乗っ取られる可能性が少なくなるからです。これの問題点は、KEK の再ネゴシエーションがケーブル モデムの CPU 使用率を増加させ、ケーブル プラントの BPI 管理トラフィックを増加させることです。

KEK 猶予期間

KEK grace time は KEK lifetime が満了するまでの合計時間で、ここでケーブル モデムが新しい KEK について Cisco CMTS とネゴシエーションを開始することになります。このタイマーの目的は、ケーブル モデムに、KEK が満了する前にそれを更新させる充分な時間を与えることです。

この時間は Cisco CMTS cable interface コマンドを使って設定できます。

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

この時間は、DOCSIS 設定ファイルの Baseline Privacy タブにある Authorization Grace Timeout と表示されたフィールドに記入することによっても設定できます。この DOCSIS コンフィギュレーション ファイルのフィールドに記入された値は、Cisco CMTS 上で設定されたどの値よりも優先されます。このタイマーのデフォルト値は 600 秒で、10 分に相当します。

TEK Lifetime

TEK lifetime は、ケーブル モデムと Cisco CMTS が、ネゴシエートされた TEK を有効であると認識するのに要する時間です。この時間が経過する前に、ケーブル モデムは Cisco CMTS と新しい TEK を再ネゴシエートする必要があります。

この時間は Cisco CMTS cable interface コマンドを使って設定できます。

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

デフォルトの設定は 43200 秒で 12 時間に相当します。

TEK lifetime を少なくすることによりセキュリティが向上します。つまり、それぞれの TEK の存続時間がより短くなることによって、もし TEK がハッキングされても、未認証の解読にさらされるデータが少なくなるからです。これの問題点は、TEK の再ネゴシエーションがケーブル モデムの CPU 使用率を増加させ、ケーブル プラントの BPI 管理トラフィックを増加させることです。

TEK 猶予期間

TEK grace time は TEK lifetime が満了するまでの合計時間で、ここでケーブル モデムが新しい TEK について Cisco CMTS とネゴシエーションを開始することになります。このタイマーの目的は、ケーブル モデムに、TEK が満了する前にそれを更新する充分な時間を与えることです。

この時間は Cisco CMTS cable interface コマンドを使って設定できます。

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

この時間は、DOCSIS 設定ファイルの Baseline Privacy タブにある TEK Grace Timeout と表示されたフィールドに記入することによっても設定できます。この DOCSIS コンフィギュレーション ファイルのフィールドに記入された値は、Cisco CMTS 上で設定されたどの値よりも優先されます。

このタイマーのデフォルト値は 600 秒で、10 分に相当します。

Authorize Wait Timeout

この時間は、ケーブル モデムが最初に KEK をネゴシエートするときに、Cisco CMTS からの応答を待つ合計時間を管理します。

この時間は、DOCSIS 設定ファイルの Baseline Privacy タブにある Authorize Wait Timeout フィールドを修正することにより設定できます。

このフィールドのデフォルト値は 10 秒で、有効な範囲は 2 秒から 30 秒です。

Reauthorize Wait Timeout

この時間は、KEK lifetime が間もなく満了するため、ケーブル モデムが新しい KEK をネゴシエートするときに Cisco CMTS からの応答を待つ合計時間を管理します。

この時間は、DOCSIS 設定ファイルの Baseline Privacy タブにある Reauthorize Wait Timeout フィールドを修正することにより設定できます。

このタイマーのデフォルト値は 10 秒で、有効な範囲は 2 秒から 30 秒です。

許可猶予タイムアウト

再認証に使える猶予期間を秒単位で指定します。 デフォルト値は600です。有効な範囲は1 ~ 1800秒です。

Authorize Reject Wait Timeout

もし、ケーブル モデムが Cisco CMTS に KEK のネゴシエーションを試みて拒否されると、新しい KEK のネゴシエーションが再試行されるまで、Authorize Reject Wait Timeout の時間にわたって待機する必要があります。

このパラメータは、DOCSIS コンフィギュレーション ファイルの Baseline Privacy タブにある **Authorize Reject Wait Timeout フィールドを使って設定できます。**このタイマーのデフォルト値は 60 秒で、有効な範囲は 10 秒から 600 秒です。

Operational Wait Timeout

この時間は、ケーブル モデムが最初に TEK をネゴシエートするときに、Cisco CMTS からの応答を待つ合計時間を管理します。

この時間は、DOCSIS 設定ファイルの Baseline Privacy タブにある Operational Wait Timeout フィールドを修正することにより設定できます。

このフィールドのデフォルト値は 1 秒で、有効な範囲は 1 秒から 10 秒です。

Rekey Wait Timeout

この時間は、TEK lifetime が間もなく満了するため、ケーブル モデムが新しい TEK をネゴシエートするときに Cisco CMTS からの応答を待つ合計時間を管理します。

この時間は、DOCSIS 設定ファイルの Baseline Privacy タブにある Rekey Wait Timeout フィールドを修正することにより設定できます。

このタイマーのデフォルト値は 1 秒で、有効な範囲は 1 秒から 10 秒です。

Cisco CMTS ベースライン プライバシ設定コマンド

次のケーブル インターフェイス コマンドを使って、Cisco CMTS 上でベースライン プライバシとそれに関連する機能を設定できます。

cable privacy

cable privacy コマンドは特定のインターフェイスでベースライン プライバシのネゴシエーションを可能にします。ケーブル インターフェイスで **no cable privacy コマンドが設定されると、どのケーブル モデムにも、そのインターフェイスでオンラインになったときにベースライン プライバシのネゴシエーションが許可されません。**もしケーブル モデムが DOCSIS コンフィギュレーション ファイルによりベースライン プライバシを使うように指示され、Cisco CMTS がベースライン プライバシのネゴシエーションを拒否すると、そのモデムはオンライン状態に留まれないので、ベースライン プライバシを無効にする際には注意してください。

cable privacy mandatory

cable privacy mandatory コマンドが設定され、DOCSIS コンフィギュレーション ファイルでケーブル モデムのベースライン プライバシが有効にされていると、そのケーブル モデムはネゴシエートに成功し、ベースライン プライバシを使用するはずです。それ以外の場合は、オンライン状態に留まることができません。

ケーブル モデムの DOCSIS コンフィギュレーション ファイルで、そのモデムがベースライン プライバシを使うように指示されていない場合は、**cable privacy mandatory コマンドはモデムをオンライン状態から停止させることはありません。**

デフォルトでは **cable privacy mandatory コマンドは有効にされていません。**

cable privacy authenticate-modem

ベースライン プライバシに関係するモデムのために、ある一定の形式の認証を実行できます。ケーブル モデムは、Cisco CMTS と KEK をネゴシエートする際に、CMTS に 6 バイトの MAC アドレスとシリアル番号の詳細を伝送します。これらのパラメータは username/password の組合せでケーブル モデムの認証のために使用できます。Cisco CMTS では、これを行うために、Cisco IOS Authentication と Authorization and Accounting（AAA）サービスを使います。認証に失敗したケーブル モデムはオンライン状態になれません。さらに、ベースライン プライバシを使わないケーブル モデムでは、このコマンドによる影響はありません。

注意：この機能はAAAサービスを使用するため、AAA設定を変更する際には注意が必要です。そうしないと、Cisco CMTSにログインして管理する機能が誤って失われる可能性があります。

次にモデム認証を行う設定例を示します。これらの設定例では、いくつかのモデムが 1 つの認証データベースに入っています。モデムの 6 オクテット MAC アドレスが、username となり、可変長のシリアル番号が password となります。1 つのモデムは明らかに誤ったシリアル番号で設定されている点に注意してください。

次の部分的な Cisco CMTS 設定例では、いくつかのモデムを認証するのにローカル認証データベースを使います。

```
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
```

モデム認証の別の例は、外部 RADIUS サーバを使うものです。これは、モデムの認証に外部 RADIUS サーバを使う、部分的な Cisco CMTS 設定例です。

```
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
```

次に示すのは、ローカル認証を使った上記の例と同等の情報を持つ RADIUS ユーザ データベース ファイル例です。ユーザ ファイルは商用およびフリーウェアの多くの RADIUS サーバでデータベースとして利用され、ユーザ認証情報が保存されています

```
# 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
```

次は、上記の設定例のいずれかを使う CMTS 上で実行された **show cable modem コマンドの出力です。**ベースライン プライバシを有効にしたモデムのうち、ローカル認証データベースに登録されていないモデム、あるいは誤ったシリアル番号が付いているモデムは **reject (pk) 状態になり、online ではなくなることがわかります。**

```
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
```

SID 17 のモデムは認証データベースにエントリがありませんが、その DOCSIS コンフィギュレーション ファイルではベースライン プライバシを使うようにはモデムに指示していないので、オンラインになることができます。

SID 18、21、22 のモデムは、認証データベースに正しいエントリがあるのでオンラインになることができます。

SID 19 のモデムは、ベースライン プライバシを使うように指示されていますが、このモデムに対するエントリが認証データベースにないので、オンラインになることはできません。このモデムは、最近、認証に失敗したことを示す reject (pk) 状態になっているはずです。

SID 20 のモデムは、認証データベースにこのモデムの MAC アドレスをともなうエントリがありますが、対応するシリアル番号が誤っているので、オンラインになることはできません。現在の時点では、このモデムは reject (pk) 状態にありますが、すぐにオフライン状態に遷移します。

モデムが認証に失敗すると、それに続く行でのメッセージが Cisco CMTS ログに追加されます。

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

このケーブル モデムはステーション メンテナンス リストから削除され、30 秒以内にオフラインとマーク付けされます。このモデムは、おそらく、もう一度オンラインになろうと試みますが、再度、拒否されることになります。

注：シスコでは、お客様がcable privacy authenticate-modemコマンドを使用して不正なケーブル モデムがオンラインになるのを止めることはお勧めしません。非承認顧客がサービス プロバイダーのネットワークにアクセスしないようにするのを保証するより効果的な方法は、非承認ケーブル モデムが、ネットワーク アクセス フィールドをオフにセットした DOCSIS コンフィギュレーション ファイルをダウンロードするように指示されるようなプロビジョニング システムを構成することです。この方法では、モデムは、連続的に re-ranging することで貴重なアップストリームの帯域幅を浪費してしまうことがありません。その代わり、モデムは **online (d) 状態になります。この状態では、このモデムの背後にいるユーザはサービス プロバイダーのネットワークへのアクセスが許可されず、モデムはアップストリームの帯域幅をステーション メンテナンスに使用するだけです。**

BPI の状態を監視するために使用されるコマンド

show interface cable X/0 privacy [kek | tek]：このコマンドは、CMTSインターフェイスで設定されたKEKまたはTEKのいずれかに関連付けられたタイマーを表示するために使用します。

次に、このコマンドの出力例を示します。

```
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：この隠しコマンドは、特定のケーブルインターフェイスのベースラインプライバシを使用してSIDの数の統計情報を表示するために使用できます。

次に、このコマンドの出力例を示します。

```
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：このコマンドはベースライン プライバシのデバッギングをアクティベートします。このコマンドをアクティベートすると、ベースライン プライバシの状態の変化やベースライン プライバシのイベントが発生する度に、コンソールに詳細が表示されます。このコマンドは、**debug cable interface cable X/0**コマンドまたは**debug cable mac-address *mac-address*コマンドの前にある場合にのみ機能**します。

debug cable bpiatp：このコマンドはベースライン プライバシのデバッギングをアクティベートします。このコマンドがアクティベートされると、ベースライン プライバシ メッセージが送られるか、Cisco CMTS に受け取られる度に、メッセージの 16 進数表示のダンプが表示されます。このコマンドは、**debug cable interface cable X/0**コマンドまたは**debug cable mac-address *mac-address*コマンドの前にある場合にのみ機能**します。

debug cable keyman：このコマンドはベースライン プライバシ キー管理のデバッギングをアクティベートします。このコマンドがアクティベートされると、ベースライン プライバシ キー管理の詳細が表示されます。

BPI のトラブルシューティング

ケーブル モデムが online (pt) ではなく、online のように見える。

モデムが online (pt) ではなく online 状態のように見える場合は、一般的には次の 3 つの状態のいずれかが考えられます。

可能性のある最初の原因は、そのケーブル モデムがベースライン プライバシを使うように指定した DOCSIS コンフィギュレーション ファイルを受け取っていないという点です。DOCSIS 設定ファイルに、モデムに送られた Class of Service プロファイル中で有効にされた BPI があることをチェックします。

モデムが online 状態に見える次の理由として、そのモデムが BPI のネゴシエーションを始める前に待機状態にあることが考えられます。1、2 分待って、そのモデムが online (pt) 状態に遷移するのを確認します。

最後に考えられる理由は、そのモデムにベースライン プライバシをサポートするファームウェアが入っていない点です。そのモデムのベンダーに、BPI をサポートする新しいバージョンのファームウェアについてお問い合わせください。

ケーブル モデムが reject (pk) 状態に見え、その後、offline になる。

モデムが reject (pk) 状態に入る原因として最初に考えられるのは、そのケーブル モデムの認証が cable privacy authenticate-modem で有効にされているが、AAA の設定が誤っている点です。関連するモデムのシリアル番号と MAC アドレスが、認証データベースに正しく入力されており、すべての外部 RADIUS サーバが到達可能であり、作動中であることをチェックします。ルータ デバッグ コマンドの debug aaa authentication と debug radius を使って、RADIUS サーバの状態や、モデムが認証に失敗している理由を調べられます。

注：ケーブルモデム接続のトラブルシューティングに関する一般的な情報は、『uBRケーブルモデムがオンラインにならない場合のトラブルシューティング』を参照してください。

特記事項 - 隠しコマンド

この文書中の隠しコマンドに関する参照情報は、情報を目的とする場合にのみ提供されています。Cisco Technical Assistance Center (TAC) では隠しコマンドのサポートは行っていません。さらに、隠しコマンドには次の制約があります。

- 常に信頼に足る正確な情報を提供するとはかぎりません。
- 実行により、予測できない副作用が発生する可能性があります。
- Cisco IOS ソフトウェアのバージョンにより動作が異なる可能性があります。
- 将来の Cisco IOS ソフトウェアのリリースでは、予告なく削除される可能性があります。

関連情報

- CableLabs
- 認証、許可、アカウンティング (AAA)
- テクニカルサポート - Cisco Systems