CHAPTER 2

Cisco CMTS におけるケーブル重複 MAC アドレス拒否

改訂：February 5, 2007, OL-1467-08-J

Cisco IOS Release 12.3(21)BC は、DOCSIS 1.1 に準拠するとともに、クローン ケーブル モデルによって引き起こされる DOS 攻撃（サービス拒絶攻撃）を排除できる、より強力なセキュリティ拡張機能を備えています。クローンは、同じ Cisco CMTS シャーシ上の、同じ HFC インターフェイス MAC アドレスを持つ 2 つの物理的なケーブル モデムの一方であると見なされます。クローン ケーブル モデムは、DOCSIS 1.0 以上に準拠している場合もあれば、DOCSIS 仕様のある程度の部分しか満たしていないか、非準拠である場合もあります。

Cisco CMTS では、この機能はデフォルトでイネーブルで、関連付けられた CLI（コマンドライン インターフェイス）コンフィギュレーション コマンドはありません。この機能は、新しいログ メッセージを作成します。デフォルトでは、このメッセージは syslog に記録されますが、**cable logging layer2events** コンフィギュレーション コマンドを使用して、cable layer2 イベント ログに移動できます。

ここでは、クローン ケーブル モデム セキュリティ検知機能について説明します。また、**cable privacy bpi-plus-enforce** コマンドとその他の追加コマンド、Cisco.com およびインターネットで入手可能な補足資料について記載します。

このモジュールの機能に関する情報の入手方法

Cisco IOS ソフトウェア リリースは、このモジュールについて記載されたすべての機能をサポートしているわけではありません。このモジュールの特定機能に関する資料へのリンクや、各機能がサポートされているリリースの一覧については、「追加情報」（p.2-8）を参照してください。

プラットフォームおよび Cisco IOS ソフトウェア イメージのサポート情報

プラットフォームおよび Cisco IOS ソフトウェア イメージのサポート情報を調べるには、Cisco Feature Navigator を使用します。Cisco Feature Navigator は、http://www.cisco.com/go/fn からアクセスできます。Feature Navigator にアクセスするには、Cisco.com のアカウントが必要です。アカウントを登録していない場合、またはユーザ名とパスワードを忘れた場合には、ログイン ダイアログ ボックスで **Cancel** をクリックして表示される手順に従います。

内容

ケーブル重複 MAC アドレス拒否の前提条件

この機能を使用するには、DOCSIS 準拠のネットワークで次の動作および前提条件を満たしている必要があります。

- Cisco CMTS では、DOCSIS 1.1 Baseline Privacy Interface Plus（BPI+; ベースライン プライバシー インターフェイス プラス）に準拠した合法的なケーブル モデムを使用する必要があります。つまり、少なくとも 1 つの BPI+ 関連の Type/Length Value（TLV）を含む DOCSIS コンフィギュレーション ファイルを使用してプロビジョニングされたときに、ケーブル モデムが次の 4 つのオンライン状態のいずれかになる必要があります。簡潔のため、ここでは、これらの状態を online(p_) で示します。
- Cisco CMTS は、次の 4 つのうちいずれかの状態の Cisco CMTS に登録するすべてのケーブル モデムにプライオリティを付与します。
  - online(pt)
  - online(pk)
  - online(ptd)
  - online(pkd)

  Cisco CMTS は、既に、これら 4 つの状態のいずれかで動作中のモデムと同じ MAC アドレスを使用することを表明した別のデバイスからの登録要求を廃棄します。

ケーブル重複 MAC アドレス拒否の制限事項

- ケーブル モデムは、DOCSIS BPI+ を使用するようにプロビジョニングされていない場合、上記の online(p_) の初期状態でオンラインになりません。そのため、Cisco CMTS の既存の動作はそのまま変わりません。プロビジョニング システムが BPI+ をイネーブルに指定した DOCSIS コンフィギュレーション ファイルを提供しないと、Cisco CMTS は 2 つのケーブル モデムを区別しようとしません。
- この機能が Cisco CMTS でイネーブルの場合、Cisco CMTS はセキュリティ侵犯通知を発行します。この通知は、ログ メッセージとして、cable logging layer2events ログに記録されるか、または、Cisco CMTS で **cable logging layer2events** コマンドが設定されていない場合は汎用ログに記録されます。

ケーブル重複 MAC アドレス拒否の概要

ここでは、クローン ケーブル モデムに関連する DOCSIS BPI+ セキュリティと、準拠および非準拠のケーブル モデムが混在するネットワークでのこの機能の動作について説明します。

BPI+ セキュリティおよびクローン ケーブル モデム

この機能は、同じケーブル モデム MAC アドレスを使用するケーブル モデム登録要求を受け取ると、BPI+ を使ってオンラインになっているケーブル モデムの方を優先します。そのため、同じ HFC MAC アドレスを持つ非準拠のケーブル モデムが登録を試みた場合でも、HFC MAC アドレスに一致する BPI+ セキュリティ証明書を持つ合法なケーブル モデルでサービスが中断されることはありません。

検出機能を動作させるには、ケーブル モデムが DOCSIS 1.1 以上を使用しており、BPI+ がイネーブルとしてプロビジョニングされている必要があります。つまり、1 つの BPI+ TLV が DOCSIS コンフィギュレーション ファイルに含まれている必要があります。DOCSIS BPI+ がイネーブルとしてプロビジョニングされていない、DOCSIS 1.0 および DOCSIS 1.1 以上のケーブル モデムはすべて、引き続きレガシーな DOCSIS 動作を実行し、Cisco CMTS 上にクローン ケーブル モデムが出現したときに DoS 攻撃を受けることがあります。

また、Cisco IOS Release 12.3(21)BC では、**cable privacy bpi-plus-enforce** コマンドが導入されています。このコマンドは、クローン ケーブル モデム検出機能を使用して完全なセキュリティを確保するために必要です。このコマンドを使用するには、ケーブル モデムが BPI+ を使用してプロビジョニングされており、DOCSIS 1.1 QOS が BPI ではなく BPI+ とともに登録されている必要があります。一般に入手可能な DOCSIS 非準拠のケーブル モデムには、DOCSIS 1.1 QOS と BPI+ が DOCSIS コンフィギュレーション ファイルに指定されている場合でも、BPI+ モードではなく BPI に強制的に登録するオプションがあります。

クローン ケーブル モデムのロギング

クローン ケーブル モデムは、システム ロギングを使用して検出および追跡されます。通常、実稼働ネットワークでは大量の DOCSIS レイヤ 2 メッセージが生成されるため、クローン関連のメッセージを分離するために個別のログを使用できます。グローバル コンフィギュレーション モードで **cable logging layer2events** コマンドを設定した場合、クローン ケーブル モデム メッセージはシステム ログ（syslog）から削除され、代わりに cable layer2logging ログに記録されます。

クローン ケーブル モデムは、短期間に多数の登録試行を試みることがあります。生成されるログ メッセージの数を抑制するために、Cisco CMTS は、クローン検出メッセージの生成を、特定の条件下での約 3 分間に抑制します。

ケーブル モデムが登録を試みたときに、同じ MAC アドレスを持つ別の物理モデムが Cisco CMTS 上のどこかで既に online(P_) 状態であった場合は、ログ メッセージに、登録を試行したモデムのケーブル インターフェイスと MAC アドレスが示されます。

Cisco CMTS における DOCSIS BPI+ への準拠とレイヤ 2 ロギングの強制実行

最強の DOCSIS BPI+ セキュリティを確保し、クローン ケーブル モデム検出機能の最適なパフォーマンスを得るには、**cable privacy bpi-plus-enforce** コマンドを使用して、次のステップを実行します。

ステップの概略

1. **enable**
2. **configure terminal**
3. **cable privacy bpi-plus-enforce**
4. **cable logging layer2events**
5. **exit**
6. **show cable logging**

ステップの詳細

	コマンドまたは処理	目的
ステップ 1	**enable** `Router> enable`	特権 EXEC モードを開始します。 • 必要な場合は、パスワードを入力します。

ステップ 2	**configure *terminal***
	
	`Router# configure terminal`
	`Router(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 3	***cable privacy bpi-plus-enforce*** `Router(config)# cable privacy bpi-plus-enforce`	DOCSIS 1.1 以上でプロビジョニングされたケーブル モデムは、以前の DOCSIS BPI セキュリティを使用せず、強制的に DOCSIS BPI+ セキュリティ証明書を使用して登録します。
ステップ 4	***cable logging layer2events*** `Router# cable logging layer2events`	Cisco CMTS MIB レジストリに指定されている中から選択された DOCSIS イベントをケーブル ロギング バッファ（汎用ロギング バッファの代わりに）に保存します。このコマンドは、Cisco IOS Release 12.3(21)BC 以降のリリースで、クローン ケーブル モデム検出機能をサポートします。

ステップ 5	**exit**
	
	`Router(config)# exit`
	`Router#`
		特権 EXEC モードに戻ります。

ステップ 6	**show cable logging** `Router# show cable logging`	レイヤ 2 ロギング機能がイネーブルかどうかと、ロギング バッファのステータスを表示します。

例

次に、クローン ケーブル モデムの検出で作成されたロギング メッセージの例を示します。この例では、クローン モデムが合法なモデムの直前にオンラインになり、レガシー動作に従ってオフラインになりました（*同じ* MAC アドレスを持つ別のモデムがオンラインになろうとしたときに、ケーブル モデムは online(p_) 状態ではありませんでした）。

```
SLOT 7/0: Nov 14 12:07:26: %UBR10000-6-CMMOVED: Cable modem 0007.0e03.3e71 has been
moved from interface Cable7/0/1 to interface Cable7/0/0.

Nov 14 12:07:57: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address
0013.7116.e726 access detected at Cable7/0/0 interface
```

この機能とサポートされているシステム ログ メッセージのその他の例については、「ケーブル重複 MAC アドレス拒否をサポートするシステム メッセージ」（p.2-6）を参照してください。

次に行う作業

Cisco CMTS のクローン ケーブル モデム検出機能は、複数の BPI+ 証明書と DOCSIS 1.1 の要素に関連しています。クローン ケーブル モデム検出機能の実装については、このマニュアルの該当カ所を参照してください。

ケーブル重複 MAC アドレス拒否をサポートするシステム メッセージ

次に、クローン ケーブル モデム検出機能と、Cisco IOS Release 12.3(21)BC で見られることのあるアクティビティに関して、ログに記録されたイベントの例を示します。この例では、PRE2 モジュールを装備した Cisco uBR10012 ルータ上の ubr10k2-k9p6u2-mz.12.3(21)BC システム イメージ ファイルを使用しています。

以下のシナリオでは、クローンされた MAC アドレスを持つ 2 つのケーブル モデムがあります。

- MAC アドレス 000f.66f9.48b1 の場合、合法なケーブル モデムが C5/0/0 アップストリーム 0 に、クローン ケーブル モデムが C7/0/0 にあります。
- MAC アドレス 0013.7116.e726 の場合、合法なケーブル モデムが C7/0/0 アップストリーム 0 に、クローン ケーブル モデムも同じインターフェイス上にあります。
- 以下の例では、MAC アドレス 000f.66f9.48b1 のクローン ケーブル モデムが合法なケーブル モデムの前にオンラインになったため、CMMOVED メッセージが発生しました。
- 合法なケーブル モデムは、クローン ケーブル モデムがオンライン化を試みる前に、online(pt) 状態でオンラインになったため、MAC アドレス 0013.7116.e726 をもつインターフェイス C7/0/0 上のケーブル モデムに関する CMMOVED メッセージはありません。

```
Dec 5 13:08:18: %UBR10000-6-CMMOVED: Cable modem 000f.66f9.48b1 has been moved from
interface Cable7/0/0 to interface C able5/0/0.
Dec 5 13:08:44: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address
0013.7116.e726 connection attempt rejected o n Cable7/0/0 U0
Dec 5 13:10:48: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address
000f.66f9.48b1 connection attempt rejected on Cable7/0/0 U1
Dec 5 13:12:37: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address
0013.7116.e726 connection attempt rejected on Cable7/0/0 U0
Dec 5 13:18:28: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address
0013.7116.e726 connection attempt rejected on Cable7/0/0 U0
Dec  5 13:18:28: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address
0013.7116.e726 connection attempt rejected o n Cable7/0/0 U0
```

次に、指定された MAC アドレスに関する上記シナリオでの追加のケーブル モデム情報を表示する **show cable modem** コマンドの例を示します。

```
Router# scm 000f.66f9.48b1
MAC Address    IP Address      I/F       MAC          Prim RxPwr  Timing Num BPI
                                          State        Sid  (dBmv) Offset
CPE Enb
000f.66f9.48b1 4.222.0.253     C5/0/0/U0 online(pt)   24    0.50  1045    1   Y

Router# scm 0013.7116.e726
MAC Address    IP Address      I/F       MAC          Prim RxPwr  Timing Num BPI
                                          State        Sid  (dBmv) Offset
CPE Enb
0013.7116.e726 4.175.0.18      C7/0/0/U0 online(pt)   4     0.00  1789    0   Y
```

コマンド リファレンス

ここでは、Cisco IOS Release 12.3(21) BC で、クローン ケーブル モデム検出機能をサポートするために導入または拡張されたコマンドについて説明します。

cable privacy bpi-plus-enforce

DOCSIS 1.1 以上でプロビジョニングされたケーブル モデムが、以前の DOCSIS BPI を使用せずに、DOCSIS Baseline Privacy Interface Plus（BPI+; ベースライン プライバシー インターフェイス プラス）を使用して登録するように命令するには、グローバル コンフィギュレーション モードで、**cable privacy bpi-plus-enforce** コマンドを使用します。このコンフィギュレーションを削除にするには、このコマンドの **no** 形式を使用します。

cable privacy bpi-plus-enforce

no cable privacy bpi-plus-enforce

（注） 一般に入手可能な DOCSIS 非準拠のケーブル モデムには、DOCSIS 1.1 でプロビジョニングされたネットワークであっても、DOCSIS BPI+ モードではなく DOCSIS BPU に強制的に登録するためのオプションがあります。

シンタックスの説明

追加のキーワードまたは引数はありません。

デフォルト

cable privacy bpi-plus-enforce コマンドはデフォルトではイネーブルではありませんが、最適な DOCSIS BPI+ セキュリティを確保するために設定する必要があります。DOCSIS 1.1 QOS でプロビジョニングされたケーブル モデムを、敢えて DOCSIS 1.0 BPI を使用して登録する正当な理由はありません。このような動作は、DOCSIS 1.1 仕様に反しています。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更
12.3(21)BC	このコマンドは、Cisco uBR10012 および Cisco uBR7246VXR ルータ上で DOCSIS BPI+ 対応のクローン ケーブル モデム検出をサポートするために、導入されました。

使用上のガイドライン

ケーブル モデムは、DOCSIS BPI または BPI+ セキュリティ証明書を使用するようにプロビジョニングされていない場合、上記の初期状態ではオンラインになりません。そのため、Cisco CMTS の既存の動作はそのまま変わりません。Cisco CMTS は、2 つのケーブル モデムがどちらも BPI+ セキュリティ用としてプロビジョニングされていない場合、両者を区別しようとしません。

この機能は、Cisco CMTS でデフォルトでイネーブルであるため、Cisco CMTS はセキュリティ侵犯通知を生成し、ログ っセージとしてログに記録します。Cisco CMTS に **cable logging layer2events** が設定されていない場合、このメッセージは、汎用システム ログ（syslog）に記録されます。

cable privacy bpi-plus enforce コマンドおよびクローン ケーブル モデム検出機能のその他のガイドラインについては、このマニュアルの該当カ所を参照してください。

例

次に、上記手順で設定した場合に、クローン ケーブル モデムの検出により作成されるロギング メッセージの例を示します。

```
SLOT 7/0: Nov 14 12:07:26: %UBR10000-6-CMMOVED: Cable modem 0007.0e03.3e71 has been
moved from interface Cable7/0/1 to interface Cable7/0/0.

Nov 14 12:07:57: %UBR10000-5-CLONED_CM_DETECTED: Cloned CM with MAC address
0013.7116.e726 access detected at Cable7/0/0 interface
```

この機能とサポートされているシステム ログ メッセージのその他の例については、「ケーブル重複 MAC アドレス拒否をサポートするシステム メッセージ」（p.2-6）を参照してください。

関連コマンド

コマンド	説明
cable logging layer2events	Cisco CMTS MIB レジストリに指定されている中から選択された（低プライオリティ）DOCSIS イベントをケーブル ロギング バッファ（汎用ロギング バッファの代わりに）に保存します。
show cable logging	不正な IP 送信元アドレス、またはケーブル インターフェイスでの DOCSIS レイヤ イベントに関するメッセージのログを表示します。
show cable modem	Cisco CMTS に登録済みおよび未登録のケーブル モデムに関する情報を表示します。

追加情報

BPI+ セキュリティ、システム メッセージ、および DOCSIS 1.1 サポートに関する詳細については、次の資料を参照してください。

- *Theft of Service — Inevitable?*Cable360.Net の記事。シスコシステムズ、Mark Millet 執筆。http://www.cable360.net/ct/data/15302.html
- 『*DOCSIS 1.1 for the Cisco CMTS*』。次の URL でアクセスできます。http://www.cisco.com/en/US/products/hw/cable/ps2217/products_feature_guide_chapter09186a008019b576.html
- 『*Cisco Broadband Cable Command Reference Guide*』http://www.cisco.com/en/US/products/hw/cable/ps2217/products_command_reference_chapter09186a0080189802.html#wp1019568
- 『*Cisco CMTS System Messages*』http://www.cisco.com/en/US/products/hw/cable/ps2217/products_system_message_guide09186a0080134033.html
- 『*Cisco CMTS MIB Specifications Guide*』http://www.cisco.com/en/US/products/hw/cable/ps2217/products_technical_reference_book09186a00801e8b9c.html