Cisco cBR コンバージド ブロードバンド ルータ DOCSIS ソフトウェア コンフィギュレーション ガイド（Cisco IOS XE Fuji 16.7.x 用）

初版：2017 年 11 月 23 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 I 部

基本設定

第 1 章

Cisco cBR ルータの構成開始

このマニュアルでは、 Cisco cBR シリーズ コンバージド ブロードバンド ルータで完了する必要がある基本的なスタートアップ設定タスクについて説明します。

Cisco CMTS 設定の前提条件

Cisco CMTS の電源をオンにして設定を開始する前に、必要な次の手順を実行します。

- ネットワークで信頼性の高いブロードバンドデータ伝送がサポートされていることを確認します。使用する設備は、National Television Standards Committee（NTSC）または該当する国際ケーブル設備勧告に基づいて、クリーンに保たれ、安定化され、認定を受けている必要があります。使用する設備が、Data-over-Cable Service Interface Specifications（DOCSIS）のダウンストリームとアップストリームの無線周波数（RF）の要件をすべて満たしていることを確認します。

- ハードウェア設置ガイド（Cisco.com から入手可能）の手順に従って、Cisco CMTS が設置されていることを確認します。
- その他の必要なヘッドエンドまたは配線ハブ ルーティングおよびネットワーク インターフェイス装置がすべて設置され、設定され、（サポートされているサービスに基づいて）動作できる状態になっていることを確認します。次の内容が含まれています。
  - すべてのルータ
  - サーバ（Dynamic Host Configuration Protocol（DHCP）サーバ、Trivial File Transfer Protocol（TFTP）サーバ、および Time-of-Day（ToD）サーバ）
  - ネットワーク管理システム
  - その他の設定または課金システム
- DHCP および DOCSIS コンフィギュレーション ファイルが作成され、適切なサーバに転送されて、各 CM の初期化時に次の動作が可能になっていることを確認します。
  - DHCP 要求の送信
  - IP アドレスの受信
  - TFTP および ToD サーバ アドレスの取得
  - DOCSIS コンフィギュレーション ファイル（または、ネットワーク内の Cisco uBR924 ケーブル アクセス ルータまたは Cisco uBR910 ケーブル データ サービス装置（DSU）を使用する場合は更新済みソフトウェア イメージ）をダウンロードします。
- 顧客宅内装置（CPE）（CM またはセットトップ ボックス（STB）、PC、電話機、またはファクシミリ装置）がネットワークおよびサービスの要件を満たしていることを確認します。
- 適切な周波数を割り当てるために、チャネル計画について理解しておく必要があります。使用するヘッドエンドまたは配線ハブに該当する場合、バンドリングのおおまかなセットアップ方針を作成します。必要に応じて、次の情報を入手します。
  - パスワード
  - IP アドレス
  - サブネット マスク
  - デバイス名

これらの前提条件が満たされたら、Cisco CMTS の設定を開始できます。これには、少なくとも次の作業が含まれます。

- Cisco CMTS のホスト名およびパスワードの設定
- ケーブル設備とネットワーク バックボーン上で IP をサポートするための CMTS の設定

（注） サービスクラスベースのプロビジョニングを使用する場合は、CM で接続が試行される前に、CMTS でサービス クラスを設定する必要があります。

（注） システム初期化中に **logging event link-status** コマンドを設定しないでください。長い時間がかかったり、スタンバイ SUP が起動できなくなったりする可能性があります。

Cisco CMTS のブートとロギング

Cisco CMTS は、EXEC と呼ばれるシスコのコマンド インタープリタを使用して管理されます。EXEC コマンドを入力するには、ルータをブートしてログインする必要があります。

手順

ステップ 1 スーパーバイザ PIC とスーパーバイザ カードのコンソール ポートに接続します。

ステップ 2 ターミナル セッションを確立します。次のように、PC 上の端末アプリケーション（ハイパーターミナル）を開くことができます。

a) Direct to Com 1 を使用して接続します。
b) ビット/秒を 9600 に設定します。
c) データ ビットを 8 に設定します。
d) パリティを none に設定します。
e) ストップ ビットを 1 に設定します。
f) フロー制御を none に設定します。
次のメッセージが表示されたら、no と入力します。

```
Would you like to enter the initial dialog?[yes]: no
Router>
```

ROMMON を使用した初めてのブート

Cisco cBR-8 は、9600 ボーのコンソールのデフォルト設定で、ROMMON を使用して起動します。これにより、TFTP またはローカル デバイスからイメージが起動します。サポートされるローカル デバイスは、ブートフラッシュや USB などです。

ブートはたとえば次のように表示されます。

```
Initializing Hardware ...˘

System Bootstrap, Version 15.5(2r)S, RELEASE SOFTWARE
Copyright (c) 1994-2015  by cisco Systems, Inc.
```

```
Current image running: Boot ROM0

Last reset cause: PowerOn

CPUID: 0x000206d7
UCODE: 0x00000710_00000000
Viper version register: 0x14121111
Set Chassis Type to 13RU
Cisco cBR-8  platform with 50331648 Kbytes of main memory

rommon 1 >
```

コンフィギュレーション レジスタ

confreg ROMMON コマンドを使用して設定を表示し、設定を変更できます。

```
rommon > confreg

           Configuration Summary
   (Virtual Configuration Register: 0x0)
enabled are:
 [ 0 ] break/abort has effect
 [ 1 ] console baud: 9600
 boot: ...... the ROM Monitor

do you wish to change the configuration? y/n  [n]:  y
 enable  "diagnostic mode"? y/n  [n]:
 enable  "use net in IP bcast address"? y/n  [n]:
 enable  "load rom after netboot fails"? y/n  [n]:
 enable  "use all zero broadcast"? y/n  [n]:
 disable "break/abort has effect"? y/n  [n]:
 enable  "ignore system config info"? y/n  [n]:
 change console baud rate? y/n  [n]:
change the boot characteristics? y/n  [n]:

           Configuration Summary
   (Virtual Configuration Register: 0x0)
enabled are:
 [ 0 ] break/abort has effect
 [ 1 ] console baud: 9600
 boot: ...... the ROM Monitor
do you wish to change the configuration? y/n  [n]:
Console baud rate options:
change console baud rate? y/n  [n]:  y
0=9600, 1=4800, 2=1200, 3=2400, 4=19200, 5=38400, 6=57600, 7=115200
enter rate  [0]:
Boot characteristics options:
change the boot characteristics? y/n  [n]:  y

 enter to boot:
 0 = ROM Monitor
 1 = the boot helper image
 2-15 = boot system
 [0]:
```

環境変数の設定

Cisco IOS XE イメージをブートするのに環境変数は必要ありません。

デフォルトで変数が設定されています。ROMMON コマンド **set** により、デフォルトの変数が表示されます。

```
rommon  > set
PS1=rommon ! >
?=0
rommon  >
```

変数を設定する場合、フォーマットは VARIABLE="value" です。

set コマンドによって新しい変数が表示され、**sync** コマンドによって変数が NVRAM に保存されます。

（注） 変数の値の途中にスペースがある場合は、引用符に囲まれた値を指定します。

```
rommon  > set
PS1=rommon ! >
?=0
rommon  > IP_ADDRESS=1.2.3.4
rommon  > IP_SUBNET_MASK=255.255.255.128
rommon  > DEFAULT_GATEWAY=1.2.9.10
rommon  > TFTP_SERVER=1.2.3.6
rommon  > sync
```

環境変数の設定解除

unset ROMMON コマンドにより環境変数が削除され、**sync** コマンドにより変数が NVRAM に保存されます。

```
rommon 1 > set
PS1=rommon ! >
?=0
BSI=0
BOOT=bootflash:cbrsup-adventerprisek9.SSA.bin,12;
RANDOM_NUM=1357042312
RET_2_RTS=17:45:06 PDT Sat Dec 31 2011
RET_2_RCALTS=1325378706
rommon 2 > unset BOOT
rommon 3 > sync
rommon 4 > set
PS1=rommon ! >
?=0
BSI=0
RANDOM_NUM=1357042312
RET_2_RTS=17:45:06 PDT Sat Dec 31 2011
RET_2_RCALTS=1325378706
rommon 5 >
```

Cisco cBR の TFTP からのブート

ROMMON はデフォルトの環境変数で起動します。BinOS イメージは、管理ポート上の TFTP から起動されます。このためには、少なくとも次の環境変数が必要です。IP_ADDRESS、IP_SUBNET_MASK、DEFAULT_GATEWAY、および TFTP_SERVER。

手順

ステップ 1 **set** コマンドを入力し、必要な環境変数を定義します。

```
rommon  > set
PS1=rommon ! >
?=0
rommon  > IP_ADDRESS=1.2.3.4
rommon  > IP_SUBNET_MASK=255.255.255.128
rommon  > DEFAULT_GATEWAY=1.2.9.10
rommon  > TFTP_SERVER=1.2.3.6
rommon  > sync
```

ステップ 2 **sync** コマンドを入力し、NVRAM に変数を保存します。

```
rommon 6 > sync
```

ステップ 3 **boot** コマンドを入力し、イメージをロードします。

```
rommon 7 > boot tftp:/tftpboot/username/cbrsup-universalk9.SSA.bin

          IP_ADDRESS: 1.2.3.4
      IP_SUBNET_MASK: 255.255.255.128
     DEFAULT_GATEWAY: 1.2.9.10
         TFTP_SERVER: 1.2.3.6
           TFTP_FILE: /tftpboot/username/cbrsup-universalk9.SSA.bin
        TFTP_MACADDR: c4:14:3c:17:e8:00
        TFTP_VERBOSE: Progress
    TFTP_RETRY_COUNT: 18
        TFTP_TIMEOUT: 7200
       TFTP_CHECKSUM: Yes
          ETHER_PORT: 2

    ETHER_SPEED_MODE: Auto Detect
link up........
Receiving /tftpboot/username/cbrsup-universalk9.SSA.bin from 172.19.211.47
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

サポート デバイスのリスト

dev コマンドは、ルータでサポートされているデバイスの一覧を表示します。

```
rommon 1 > dev
Devices in device table:
        id  name
 harddisk:  Internal hard disk
bootflash:  Internal flash drive
     usb0:  External USB drive 0
     usb1:  External USB drive 1
rommon 2 >
```

Cisco cBR の デバイスからのブート

手順

ステップ 1 **dir bootflash:** コマンドを入力します。

```
rommon  > dir bootflash:
File System: EXT2/EXT3

12         691955580 -rw-r--r--     cbrsup-xe315.SSA.bin
45         83475     -rw-r--r--     reload.log.20120103004502
```

ステップ 2 **boot bootflash:***imagename* コマンドを入力します。

```
rommon  > boot bootflash:cbrsup-xe315.bin
File size is 0x293e67bc
Located cbrsup-xe315.bin
Image size 691955644 inode num 145153, bks cnt 168935 blk size 8*512
################################################################################
```

ROMMON での AUTOBOOT イメージの設定

ブートフラッシュからイメージの AUTOBOOT を設定するには、環境変数 BOOT を追加し、コンフィギュレーション レジスタの起動特性を変更して、システムを起動およびリセットします。

手順

ステップ 1 **boot=bootflash:***imagename* コマンドを入力して、イメージをロードします。

```
rommon  > BOOT=bootflash:cbrsup-xe315-20150131.bin
```

ステップ 2 **sync** コマンドを入力して、変数を NVRAM にコピーします。

```
rommon  > sync
```

ステップ 3 **confreg** コマンドを入力して、設定を指定および変更します。

```
rommon  > confreg

           Configuration Summary
   (Virtual Configuration Register: 0x0)
enabled are:
 [ 0 ] break/abort has effect
 [ 1 ] console baud: 9600
 boot: ...... the ROM Monitor

do you wish to change the configuration? y/n  [n]:  y
 enable  "diagnostic mode"? y/n  [n]:
 enable  "use net in IP bcast address"? y/n  [n]:
```

```
 enable  "load rom after netboot fails"? y/n  [n]:
 enable  "use all zero broadcast"? y/n  [n]:
 disable "break/abort has effect"? y/n  [n]:
 enable  "ignore system config info"? y/n  [n]:
 change console baud rate? y/n  [n]:  n
change the boot characteristics? y/n  [n]:  y

 enter to boot:
 0 = ROM Monitor
 1 = the boot helper image
 2-15 = boot system
 [0]:  2

           Configuration Summary
   (Virtual Configuration Register: 0x2)
enabled are:
 [ 0 ] break/abort has effect
 [ 1 ] console baud: 9600
 boot: ...... image specified by the boot system commands or default to: cisco2-Cisco cBR-8


do you wish to change the configuration? y/n  [n]:

You must reset or power cycle for new config to take effect
```

ステップ 4 **reset** コマンドを入力すると、新しい設定が有効になります。

```
rommon  > reset
```

次の作業

ROMMON バージョンの確認

ROMMON バージョンを表示するには、**showmon** コマンドを使用します。

```
rommon  > showmon
Current image running (0/1): Boot ROM0
System Bootstrap, Version 15.5(2r)S, RELEASE SOFTWARE
Copyright (c) 1994-2015  by cisco Systems, Inc.

Viper version register: 0x14121111
rommon  >
```

Cisco cBR のリセット

reset コマンドを使用すると、スーパーバイザをソフト リセットできます。

```
rommon  > reset

Resetting .......


Initializing Hardware ...˘
```

```
System Bootstrap, Version 15.5(2r)S, RELEASE SOFTWARE
Copyright (c) 1994-2015  by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: LocalSoftware

CPUID: 0x000206d7
UCODE: 0x00000710_00000000
Viper version register: 0x14121111
Set Chassis Type to 13RU
Cisco cBR-8  platform with 50331648 Kbytes of main memory

rommon  >
```

ファイル システム

Cisco cBR-8 ルータは、Cisco IOS-XE イメージ上で実行されます。サポートされているファイル システムは次のとおりです。

1. IOS の IOS File System（IFS）
2. Linux の ext2、vfs、jffs2、tmpfs、autofs、およびそのような共通ファイル システム

ファイル システムの機能：

1. ハードディスクと USB の両方がホット プラグ可能です。
2. ハードディスクは Rommon でアクセスできません。
3. ブートフラッシュおよび USB ディスクは Rommon でアクセスできます。
4. **dir**、**show**、**copy**、**delete**、**mkdir**、**rmdir**、および **fsck** コマンドがブートフラッシュ、ハードディスク、および USB でサポートされます。

スーパーバイザのファイル システム テーブル

名前	デバイス	サイズ	タイプ	表示	使用法	物理的な説明
bootflash	/dev/bootflash1	7800705024	ext2	IOS/Binos	image、IOScrasinfo など	ブートフラッシュ（eUSB フラッシュ）のパーティション 1。
flash	/dev/bootflash1	7800705024	ext2	IOS	image	ブートフラッシュのコピー。
nvram	/dev/bootflash2	32M	該当なし	IOS	configuretion など	ブートフラッシュ（eUSB フラッシュ）のパーティション 2。
harddisk	/dev/harddisk1	98394218496	ext2	IOS/Binos	tracelog、corefile など	100G ハードディスクのパーティション 1。

名前	デバイス	サイズ	タイプ	表示	使用法	物理的な説明
usb0	/dev/usb11	8G	vfat	IOS/Binos	image	2 つの USB を 1 つの SUP に挿入できます。

ハードウェア内容の確認

CLI を使用した Cisco cBR シャーシのモニタリング

- **show platform**：取り付けたカードの状態が **Ok** または **Inserted** であるかを確認します。

```
Router# show platform

Chassis type: CBR-8-CCAP-CHASS

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
1         CBR-CCAP-LC-40G     ok                    03:22:58
1/1       CBR-RF-PIC          ok                    03:19:40
SUP0      CBR-CCAP-SUP-160G   inserted              03:22:58
 R0                           ok, active
 F0                           ok, active
 4                            ok, active
 4/1      CBR-SUP-8X10G-PIC   ok                    03:20:30
P0        PWR-2KW-DC-V2       ok                    03:21:20
P1        PWR-2KW-DC-V2       ok                    03:21:20
P2        PWR-2KW-DC-V2       ok                    03:21:20
P3        PWR-2KW-DC-V2       ok                    03:21:20
P4        PWR-2KW-DC-V2       ok                    03:21:20
P5        PWR-2KW-DC-V2       ok                    03:21:20
P10       CBR-FAN-ASSEMBLY    ok                    03:21:10
P11       CBR-FAN-ASSEMBLY    ok                    03:21:10
P12       CBR-FAN-ASSEMBLY    ok                    03:21:10
P13       CBR-FAN-ASSEMBLY    ok                    03:21:10
P14       CBR-FAN-ASSEMBLY    ok                    03:21:10
```

- **show platform hardware slot** *slot***serdes status**：すべてのリンクが **locked** 状態であるかどうかを確認します。

```
Router# show platform hardware slot F1 serdes status

Slot R1-Link A
  RX link locked
  58-bit scrambler, 20 Gbps
  0 Overruns, 0 Underruns
  0 Reframe, 0 Disparity
  0 Out of band, 0 Illegal control codes

Slot 3-Link A
  RX link locked
  58-bit scrambler, 20 Gbps
  0 Overruns, 0 Underruns
  0 Reframe, 0 Disparity
  0 Out of band, 0 Illegal control codes

Slot 5-Link A
  RX link locked
  58-bit scrambler, 20 Gbps
  0 Overruns, 0 Underruns
  0 Reframe, 0 Disparity
  0 Out of band, 0 Illegal control codes
```

```
Slot 5-Link B
  RX link locked
  58-bit scrambler, 20 Gbps
  0 Overruns, 0 Underruns
  0 Reframe, 0 Disparity
  0 Out of band, 0 Illegal control codes

Slot 5-Link C
  RX link locked
  58-bit scrambler, 20 Gbps
  0 Overruns, 0 Underruns
  0 Reframe, 0 Disparity
  0 Out of band, 0 Illegal control codes

Slot 5-Link D
  RX link locked
  58-bit scrambler, 20 Gbps
  0 Overruns, 0 Underruns
  0 Reframe, 0 Disparity
  0 Out of band, 0 Illegal control codes

Slot 5-Link E
  RX link Init
  58-bit scrambler, 20 Gbps
  0 Overruns, 0 Underruns
  0 Reframe, 0 Disparity
  0 Out of band, 0 Illegal control codes

Slot 5-Link F
  RX link Init
  58-bit scrambler, 20 Gbps
  0 Overruns, 0 Underruns
  0 Reframe, 0 Disparity
  0 Out of band, 0 Illegal control codes

Slot 5-Link G
  RX link Init
  58-bit scrambler, 20 Gbps
  0 Overruns, 0 Underruns
  0 Reframe, 0 Disparity
  0 Out of band, 0 Illegal control codes

Slot 5-Link H
  RX link Init
  58-bit scrambler, 20 Gbps
  0 Overruns, 0 Underruns
  0 Reframe, 0 Disparity
  0 Out of band, 0 Illegal control codes
```

- **show environment all**：取り付け後に各 FRU の環境ステータスを確認します。

  このコマンドにより、システムの温度、電圧、ファン、および電源装置の状態が表示されます。

```
Router# show environment all

Sensor List:  Environmental Monitoring
 Sensor           Location          State             Reading
 AVCC&1P2: Sens   4/1               Normal            81 mV
 AVCC&1P2: Vin    4/1               Normal            12600 mV
 AVCC&1P2: ADin   4/1               Normal            0 mV
 VP1P35: Sens     4/1               Normal            8 mV
 VP1P35: Vin      4/1               Normal            12650 mV
 VP1P35: ADin     4/1               Normal            112 mV
 VP1P0: Sens      4/1               Normal            15 mV
 VP1P0: Vin       4/1               Normal            12625 mV
 VP1P0: ADin      4/1               Normal            0 mV
 MGTAVTT: Sens    4/1               Normal            21 mV
 MGTAVTT: Vin     4/1               Normal            12625 mV
 MGTAVTT: ADin    4/1               Normal            0 mV
```

```
VP1P8: Sens      4/1              Normal           41 mV
VP1P8: Vin       4/1              Normal           12600 mV
VP1P8: ADin      4/1              Normal           0 mV
VP3P3: Sens      4/1              Normal           39 mV
VP3P3: Vin       4/1              Normal           12625 mV
VP3P3: ADin      4/1              Normal           0 mV
Temp: RTMAC      4/1              Normal           34 Celsius
Temp: INLET      4/1              Normal           29 Celsius
Temp: OUTLET     4/1              Normal           27 Celsius
Temp: MAX6697    4/1              Normal           50 Celsius
Temp: TCXO       4/1              Normal           37 Celsius
Temp: SUP_OUT    4/1              Normal           49 Celsius
Temp: 3882_1 P   4/1              Normal           44 Celsius
Temp: 3882_2 P   4/1              Normal           39 Celsius
Temp: 3882_3 P   4/1              Normal           39 Celsius
VP5P0: Sens      4/1              Normal           6 mV
VP5P0: Vin       4/1              Normal           12650 mV
VP5P0: ADin      4/1              Normal           0 mV
VP1P8: Sens      4/1              Normal           33 mV
VP1P8: Vin       4/1              Normal           12625 mV
VP1P8: ADin      4/1              Normal           0 mV
3P3&1P0: Sens    4/1              Normal           24 mV
3P3&1P0: Vin     4/1              Normal           12625 mV
3P3&1P0: ADin    4/1              Normal           0 mV
Temp: INLET PD   4/1              Normal           27 Celsius
Temp: OUTLETPD   4/1              Normal           36 Celsius
Temp: 6697-DC    4/1              Normal           38 Celsius
Temp: PHYOUT     4/1              Normal           49 Celsius
Temp: PHYIN      4/1              Normal           38 Celsius
Temp: SSD        4/1              Normal           40 Celsius
Temp: SFP+       4/1              Normal           36 Celsius
Temp: 3882_1PD   4/1              Normal           42 Celsius
3882_PC1_0: VO   4/1              Normal           1198 mV
3882_PC1_1: VO   4/1              Normal           999 mV
3882_PC2_0: VO   4/1              Normal           998 mV
3882_PC3_0: VO   4/1              Normal           1349 mV
PSOC-PC1_0: VO   4/1              Normal           3300 mV
PSOC-PC1_1: VO   4/1              Normal           12590 mV
PSOC-PC1_2: VO   4/1              Normal           6997 mV
PSOC-PC1_3: VO   4/1              Normal           5000 mV
PSOC-PC1_4: VO   4/1              Normal           3299 mV
PSOC-PC1_5: VO   4/1              Normal           1000 mV
PSOC-PC1_6: VO   4/1              Normal           1010 mV
PSOC-PC1_7: VO   4/1              Normal           1801 mV
PSOC-PC1_8: VO   4/1              Normal           2000 mV
PSOC-PC1_9: VO   4/1              Normal           1198 mV
PSOC-PC1_10: V   4/1              Normal           1798 mV
PSOC-PC1_11: V   4/1              Normal           2500 mV
PSOC-PC1_12: V   4/1              Normal           1353 mV
PSOC-PC1_13: V   4/1              Normal           1223 mV
PSOC-PC1_14: V   4/1              Normal           592 mV
PSOC-PC1_15: V   4/1              Normal           596 mV
3882_PDC_0: VO   4/1              Normal           1000 mV
3882_PDC_1: VO   4/1              Normal           3300 mV
PSOC-DC1_0: VO   4/1              Normal           4998 mV
PSOC-DC1_1: VO   4/1              Normal           3280 mV
PSOC-DC1_2: VO   4/1              Normal           1005 mV
PSOC-DC1_3: VO   4/1              Normal           1801 mV
PSOC-DC1_4: VO   4/1              Normal           2500 mV
12_CUR: Sens     9                Normal           14 mV
12_CUR: Vin      9                Normal           12650 mV
12_CUR: ADin     9                Normal           267 mV
G0_CUR: Sens     9                Normal           69 mV
G0_CUR: Vin      9                Normal           12550 mV
G0_CUR: ADin     9                Normal           0 mV
G1_CUR: Sens     9                Normal           69 mV
G1_CUR: Vin      9                Normal           12575 mV
G1_CUR: ADin     9                Normal           0 mV
LB_CUR: Sens     9                Normal           11 mV
LB_CUR: Vin      9                Normal           12525 mV
LB_CUR: ADin     9                Normal           0 mV
Temp: CAPRICA    9                Normal           40 Celsius
Temp: BASESTAR   9                Normal           47 Celsius
```

```
Temp: RAIDER     9               Normal          45 Celsius
Temp: CPU        9               Normal          31 Celsius
Temp: INLET      9               Normal          25 Celsius
Temp: OUTLET     9               Normal          35 Celsius
Temp: DIGITAL    9               Normal          31 Celsius
Temp: UPX        9               Normal          29 Celsius
Temp: LEOBEN1    9               Normal          31 Celsius
Temp: LEOBEN2    9               Normal          35 Celsius
Temp: 3.3-18     9               Normal          43 Celsius
Temp: BS_1V      9               Normal          45 Celsius
Freq: 5338-49    9               Normal          0 MHz
Freq: 5338-52    9               Normal          0 MHz
Freq: 5338-89    9               Normal          0 MHz
3882_1_0: VOUT   9               Normal          3299 mV
3882_1_1: VOUT   9               Normal          1800 mV
3882_2_0: VOUT   9               Normal          2500 mV
3882_2_1: VOUT   9               Normal          1199 mV
3882_3_0: VOUT   9               Normal          1419 mV
3882_4_0: VOUT   9               Normal          1350 mV
3882_5_0: VOUT   9               Normal          1000 mV
3882_6_0: VOUT   9               Normal          1021 mV
3882_7_0: VOUT   9               Normal          1199 mV
3882_7_1: VOUT   9               Normal          1000 mV
3882_8_0: VOUT   9               Normal          1000 mV
3882_9_0: VOUT   9               Normal          999 mV
V2978: VSENSE0   9               Normal          0 mV
V2978: VSENSE1   9               Normal          0 mV
V2978: VSENSE2   9               Normal          0 mV
V2978: VSENSE3   9               Normal          6000 mV
V2978: VSENSE4   9               Normal          2400 mV
V2978: VSENSE5   9               Normal          0 mV
V2978: VSENSE6   9               Normal          6598 mV
V2978: VSENSE7   9               Normal          4998 mV
V2978: VIN       9               Normal          25218 mV
PSOC_2_0: VOUT   9               Normal          12582 mV
PSOC_2_1: VOUT   9               Normal          4985 mV
PSOC_2_2: VOUT   9               Normal          3256 mV
PSOC_2_3: VOUT   9               Normal          1982 mV
PSOC_2_4: VOUT   9               Normal          1990 mV
PSOC_2_5: VOUT   9               Normal          1782 mV
PSOC_2_6: VOUT   9               Normal          1793 mV
PSOC_2_7: VOUT   9               Normal          1786 mV
PSOC_2_8: VOUT   9               Normal          1483 mV
PSOC_2_9: VOUT   9               Normal          1193 mV
PSOC_2_10: VOU   9               Normal          995 mV
PSOC_2_11: VOU   9               Normal          987 mV
PSOC_2_12: VOU   9               Normal          994 mV
PSOC_2_13: VOU   9               Normal          707 mV
PSOC_2_14: VOU   9               Normal          592 mV
PSOC_2_15: VOU   9               Normal          593 mV
LTC4261: Power   9               Normal          340 Watts
PEM Iout         P0              Normal          5 A
PEM Vout         P0              Normal          55 V DC
PEM Vin          P0              Normal          202 V AC
Temp: INLET      P0              Normal          26 Celsius
Temp: OUTLET     P0              Normal          48 Celsius
PEM Iout         P1              Normal          6 A
PEM Vout         P1              Normal          55 V DC
PEM Vin          P1              Normal          204 V AC
Temp: INLET      P1              Normal          30 Celsius
Temp: OUTLET     P1              Normal          53 Celsius
PEM Iout         P2              Normal          3 A
PEM Vout         P2              Normal          55 V DC
PEM Vin          P2              Normal          204 V AC
Temp: INLET      P2              Normal          25 Celsius
Temp: OUTLET     P2              Normal          51 Celsius
PSOC-MB2_0: VO   R0              Normal          12758 mV
PSOC-MB2_1: VO   R0              Normal          4998 mV
PSOC-MB2_2: VO   R0              Normal          7082 mV
PSOC-MB2_3: VO   R0              Normal          3287 mV
PSOC-MB2_4: VO   R0              Normal          989 mV
PSOC-MB2_5: VO   R0              Normal          1047 mV
PSOC-MB2_6: VO   R0              Normal          1500 mV
```

```
PSOC-MB2_7: VO   R0                Normal             1800 mV
PSOC-MB2_8: VO   R0                Normal             914 mV
PSOC-MB2_9: VO   R0                Normal             885 mV
PSOC-MB2_10: V   R0                Normal             994 mV
PSOC-MB2_11: V   R0                Normal             989 mV
PSOC-MB2_12: V   R0                Normal             1479 mV
PSOC-MB2_13: V   R0                Normal             989 mV
PSOC-MB2_14: V   R0                Normal             984 mV
PSOC-MB2_15: V   R0                Normal             890 mV
PSOC-MB2_16: V   R0                Normal             2485 mV
PSOC-MB2_17: V   R0                Normal             1346 mV
PSOC-MB2_18: V   R0                Normal             1458 mV
PSOC-MB2_19: V   R0                Normal             1208 mV
PSOC-MB2_20: V   R0                Normal             1791 mV
PSOC-MB2_21: V   R0                Normal             3293 mV
PSOC-MB2_22: V   R0                Normal             3250 mV
PSOC-MB2_23: V   R0                Normal             3284 mV
PSOC-MB2_24: V   R0                Normal             4970 mV
PSOC-MB2_25: V   R0                Normal             4451 mV
PSOC-MB3_0: VO   R0                Normal             4983 mV
PSOC-MB3_1: VO   R0                Normal             4979 mV
PSOC-MB3_2: VO   R0                Normal             1500 mV
PSOC-MB3_3: VO   R0                Normal             1192 mV
PSOC-MB3_4: VO   R0                Normal             705 mV
PSOC-MB3_5: VO   R0                Normal             752 mV
PSOC-MB3_6: VO   R0                Normal             579 mV
PSOC-MB3_7: VO   R0                Normal             1500 mV
PSOC-MB3_8: VO   R0                Normal             1501 mV
PSOC-MB3_9: VO   R0                Normal             1250 mV
PSOC-MB3_10: V   R0                Normal             1247 mV
PSOC-MB3_11: V   R0                Normal             1260 mV
PSOC-MB3_12: V   R0                Normal             1038 mV
PSOC-MB3_13: V   R0                Normal             1343 mV
PSOC-MB3_14: V   R0                Normal             670 mV
PSOC-MB3_15: V   R0                Normal             1800 mV
PSOC-MB3_16: V   R0                Normal             908 mV
PSOC-MB3_17: V   R0                Normal             823 mV
PSOC-MB3_18: V   R0                Normal             992 mV
PSOC-MB3_19: V   R0                Normal             984 mV
PSOC-MB3_20: V   R0                Normal             1046 mV
PSOC-MB3_21: V   R0                Normal             1192 mV
PSOC-MB3_22: V   R0                Normal             1169 mV
PSOC-MB3_23: V   R0                Normal             1187 mV
PSOC-MB3_24: V   R0                Normal             1796 mV
PSOC-MB3_25: V   R0                Normal             1792 mV
PSOC-MB3_26: V   R0                Normal             1787 mV
PSOC-MB3_27: V   R0                Normal             1034 mV
3882_MB1_0: VO   R0                Normal             1001 mV
3882_MB1_1: VO   R0                Normal             1022 mV
3882_MB2_0: VO   R0                Normal             1197 mV
3882_MB3_0: VO   R0                Normal             1045 mV
3882_MB3_1: VO   R0                Normal             996 mV
3882_MB4_0: VO   R0                Normal             898 mV
3882_MB5_0: VO   R0                Normal             1348 mV
3882_MB6_0: VO   R0                Normal             1350 mV
3882_MB6_1: VO   R0                Normal             3297 mV
3882_MB7_0: VO   R0                Normal             998 mV
3882_MB8_0: VO   R0                Normal             1501 mV
3882_MB8_1: VO   R0                Normal             1551 mV
3882_MB9_0: VO   R0                Normal             999 mV
3882_MB9_1: VO   R0                Normal             3296 mV
15301_1: VOUT    R0                Normal             2500 mV
15301_2: VOUT    R0                Normal             1200 mV
15301_3: VOUT    R0                Normal             1200 mV
AS_VRM: Sens     R0                Normal             40 mV
AS_VRM: Vin      R0                Normal             12725 mV
AS_VRM: ADin     R0                Normal             0 mV
Y0_VRM: Sens     R0                Normal             23 mV
Y0_VRM: Vin      R0                Normal             12675 mV
Y0_VRM: ADin     R0                Normal             380 mV
CPU_VCC: Sens    R0                Normal             6 mV
CPU_VCC: Vin     R0                Normal             12725 mV
CPU_VCC: ADin    R0                Normal             0 mV
```

```
5P0_BIAS: Sens   R0              Normal           19 mV
5P0_BIAS: Vin    R0              Normal           12700 mV
5P0_BIAS: ADin   R0              Normal           0 mV
7P0_BIAS: Sens   R0              Normal           45 mV
7P0_BIAS: Vin    R0              Normal           12725 mV
7P0_BIAS: ADin   R0              Normal           0 mV
1P0_AA: Sens     R0              Normal           37 mV
1P0_AA: Vin      R0              Normal           12700 mV
1P0_AA: ADin     R0              Normal           0 mV
1P0_RT: Sens     R0              Normal           16 mV
1P0_RT: Vin      R0              Normal           12725 mV
1P0_RT: ADin     R0              Normal           0 mV
1P2: Sens        R0              Normal           37 mV
1P2: Vin         R0              Normal           12675 mV
1P2: ADin        R0              Normal           0 mV
0P9_T0: Sens     R0              Normal           7 mV
0P9_T0: Vin      R0              Normal           12750 mV
0P9_T0: ADin     R0              Normal           0 mV
1P05_CPU: Sens   R0              Normal           11 mV
1P05_CPU: Vin    R0              Normal           12700 mV
1P05_CPU: ADin   R0              Normal           0 mV
1P0_CC: Sens     R0              Normal           16 mV
1P0_CC: Vin      R0              Normal           12700 mV
1P0_CC: ADin     R0              Normal           0 mV
1P35_DDR: Sens   R0              Normal           6 mV
1P35_DDR: Vin    R0              Normal           12725 mV
1P35_DDR: ADin   R0              Normal           0 mV
1P35_RLD: Sens   R0              Normal           0 mV
1P35_RLD: Vin    R0              Normal           12675 mV
1P35_RLD: ADin   R0              Normal           2047 mV
3P3_CCC: Sens    R0              Normal           16 mV
3P3_CCC: Vin     R0              Normal           12700 mV
3P3_CCC: ADin    R0              Normal           1375 mV
1P0_R: Sens      R0              Normal           29 mV
1P0_R: Vin       R0              Normal           12700 mV
1P0_R: ADin      R0              Normal           0 mV
1P5_A0: Sens     R0              Normal           41 mV
1P5_A0: Vin      R0              Normal           12700 mV
1P5_A0: ADin     R0              Normal           0 mV
1P5: Sens        R0              Normal           34 mV
1P5: Vin         R0              Normal           12675 mV
1P5: ADin        R0              Normal           0 mV
2P5: Sens        R0              Normal           5 mV
2P5: Vin         R0              Normal           12700 mV
2P5: ADin        R0              Normal           0 mV
1P8_A: Sens      R0              Normal           10 mV
1P8_A: Vin       R0              Normal           12675 mV
1P8_A: ADin      R0              Normal           947 mV
1P0_BV: Sens     R0              Normal           24 mV
1P0_BV: Vin      R0              Normal           12700 mV
1P0_BV: ADin     R0              Normal           0 mV
3P3: Sens        R0              Normal           16 mV
3P3: Vin         R0              Normal           12725 mV
3P3: ADin        R0              Normal           0 mV
1P2_B: Sens      R0              Normal           41 mV
1P2_B: Vin       R0              Normal           12725 mV
1P2_B: ADin      R0              Normal           0 mV
ADM1075: Power   R0              Normal           329 Watts
Temp: Y0_DIE     R0              Normal           33 Celsius
Temp: BB_DIE     R0              Normal           29 Celsius
Temp: VP_DIE     R0              Normal           26 Celsius
Temp: RT-E_DIE   R0              Normal           31 Celsius
Temp: INLET_1    R0              Normal           23 Celsius
Temp: INLET_2    R0              Normal           22 Celsius
Temp: OUTLET_1   R0              Normal           25 Celsius
Temp: 3882_1     R0              Normal           46 Celsius
Temp: 3882_1A    R0              Normal           43 Celsius
Temp: 3882_1B    R0              Normal           43 Celsius
Temp: 3882_2     R0              Normal           41 Celsius
Temp: 3882_2A    R0              Normal           40 Celsius
Temp: 3882_2B    R0              Normal           41 Celsius
Temp: 3882_3     R0              Normal           37 Celsius
Temp: 3882_3A    R0              Normal           34 Celsius
```

```
Temp: 3882_3B    R0                Normal            33 Celsius
Temp: 3882_4     R0                Normal            46 Celsius
Temp: 3882_4A    R0                Normal            38 Celsius
Temp: 3882_4B    R0                Normal            35 Celsius
Temp: 3882_5     R0                Normal            32 Celsius
Temp: 3882_5A    R0                Normal            23 Celsius
Temp: 3882_5B    R0                Normal            23 Celsius
Temp: 3882_6     R0                Normal            37 Celsius
Temp: 3882_6A    R0                Normal            30 Celsius
Temp: 3882_6B    R0                Normal            32 Celsius
Temp: 3882_7     R0                Normal            38 Celsius
Temp: 3882_7A    R0                Normal            35 Celsius
Temp: 3882_7B    R0                Normal            35 Celsius
Temp: 3882_8     R0                Normal            47 Celsius
Temp: 3882_8A    R0                Normal            45 Celsius
Temp: 3882_8B    R0                Normal            41 Celsius
Temp: 3882_9     R0                Normal            37 Celsius
Temp: 3882_9A    R0                Normal            33 Celsius
Temp: 3882_9B    R0                Normal            32 Celsius
Temp: 8314_1     R0                Normal            40 Celsius
Temp: 8314_2     R0                Normal            36 Celsius
Temp: 3536_1A    R0                Normal            26 Celsius
Temp: 3536_1B    R0                Normal            26 Celsius
Temp: 15301_1A   R0                Normal            31 Celsius
Temp: 15301_1B   R0                Normal            32 Celsius
Temp: 15301_2A   R0                Normal            28 Celsius
Temp: 15301_2B   R0                Normal            34 Celsius
Temp: 15301_3A   R0                Normal            38 Celsius
Temp: 15301_3B   R0                Normal            45 Celsius
Temp: AS_DIE     R0                Normal            70 Celsius
Temp: XPT1_DTL   R0                Normal            42 Celsius
Temp: XPT1_DTR   R0                Normal            42 Celsius
Temp: XPT1_DBL   R0                Normal            42 Celsius
Temp: XPT1_DBR   R0                Normal            42 Celsius
Temp: XPT2_DTL   R0                Normal            42 Celsius
Temp: XPT2_DTR   R0                Normal            42 Celsius
Temp: XPT2_DBL   R0                Normal            42 Celsius
Temp: XPT2_DBR   R0                Normal            42 Celsius
Temp: XPT3_DTL   R0                Normal            42 Celsius
Temp: XPT3_DTR   R0                Normal            42 Celsius
Temp: XPT3_DBL   R0                Normal            42 Celsius
Temp: XPT3_DBR   R0                Normal            42 Celsius
Freq: MAX3674    R0                Normal            500 MHz
Freq: SQ420D     R0                Normal            24 MHz
```

- **show facility-alarm status** ：シャーシのステータスを確認します。

```
Router# show facility-alarm status

System Totals  Critical: 4  Major: 1  Minor: 8

Source                    Time                   Severity      Description [Index]
------                    ------                 --------      -------------------
slot 3/0                  Apr 13 2015 16:25:58   CRITICAL      Active Card Removed
OIR Alarm [0]
Power Supply Bay 3        Apr 13 2015 13:41:56   CRITICAL      Power Supply/FAN
Module Missing [0]
Power Supply Bay 4        Apr 13 2015 13:41:56   CRITICAL      Power Supply/FAN
Module Missing [0]
Power Supply Bay 5        Apr 13 2015 13:41:56   CRITICAL      Power Supply/FAN
Module Missing [0]
Cable3/0/15-US0           Apr 13 2015 17:32:53   MINOR         Physical Port Link
Down [0]
Cable3/0/15-US1           Apr 13 2015 17:32:53   MINOR         Physical Port Link
Down [0]
Cable3/0/15-US2           Apr 13 2015 17:32:53   MINOR         Physical Port Link
Down [0]
Cable3/0/15-US3           Apr 13 2015 17:32:53   MINOR         Physical Port Link
Down [0]
Cable3/0/15-US4           Apr 13 2015 17:32:53   MINOR         Physical Port Link
Down [0]
```

ギガビット イーサネット管理インターフェイスの概要

このインターフェイスの目的は、ユーザがルータ上で管理タスクを実行できるようにすることです。基本的には、インターフェイスが原因で不要にネットワーク トラフィックが転送されたり、また、ほとんどの場合は転送できなかったりしますが、Telnet およびセキュア シェル（SSH）を経由すれば、ルータへのアクセスが可能となり、ルータ上のほとんどの管理タスクを実行することができます。

管理イーサネット インターフェイスでは、次の点に注意してください。

- 管理イーサネットインターフェイスは各SUPにありますが、アクセス可能な管理イーサネットインターフェイスは、アクティブなSUPだけに備わっています（ただし、スタンバイ SUPの場合はコンソール ポートを使用してアクセスできます）。
- インターフェイスでサポートされるルーテッドプロトコルは、IPv4、IPv6、およびARPだけです。
- インターフェイスでは、一部のソフトウェアプロセスがダウンしている場合でもルータにアクセスする方式を提供しています。
- イーサネット管理インターフェイスは、合法的傍受のMDソースインターフェイスとしては使用できません。
- 管理イーサネット インターフェイスは、自身の VPN ルーティングおよび転送（VRF）の一部です。

ギガビット イーサネット ポートの番号

ギガビット イーサネット管理ポートは、常に GigabitEthernet0 です。

デュアル SUP 構成の場合、アクティブ SUP 上の管理イーサネット インターフェイスは、常に Gigabit Ethernet 0 になります。一方、スタンバイ SUP 上の管理イーサネット インターフェイスには同一 Telnet セッションの Cisco IOS-XE CLI を使用してアクセスできません。ただし、スタンバイ SUP にはコンソール ポートを介して Telnet 接続できます。

ポートには、Cisco cBR シリーズルータ上のその他のポートと同様にコンフィギュレーション モードでアクセスできます。

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface gigabitethernet0
Router(config-if)#
```

ROMMON および管理イーサネット ポートの IP アドレス処理

Cisco cBR シリーズ ルータ上で IOS-XE プロセスが開始しない場合、ROMMON に設定された IP アドレスが管理イーサネット インターフェイスの IP アドレスとして動作します。IOS-XE プロセスが稼働中で、管理イーサネット インターフェイスを制御している場合は、IOS-XE CLI のイン

ターフェイス Gigabit Ethernet 0 の設定時に指定した IP アドレスが、管理イーサネット インターフェイスの IP アドレスとなります。ROMMON で定義された IP アドレスは、IOS-XE プロセスが非アクティブな場合にだけインターフェイス アドレスとして使用されます。

このため、ROMMON と IOS-XE CLI で指定された IP アドレスは同一になり、管理イーサネット インターフェイスはシングル SUP 構成で適切に機能します。

ただし、デュアル SUP 構成では、SUP0 または SUP1 のいずれにおいても相互に一致する ROMMON の IP アドレス、または IOS-XE CLI で定義された IP アドレスは設定しないでください。一致する IP アドレスを設定すると、アクティブおよびスタンバイの管理イーサネット インターフェイスで、MAC アドレスが異なった、同じ IP アドレスが割り当てられる可能性があり、トラフィックに予期せぬ処理が実行される場合があります。

ギガビット イーサネット管理インターフェイスの VRF

管理イーサネット インターフェイスを自身の VRF 内に配置すると、管理イーサネット インターフェイスに次のような影響が発生します。

- VRF 内では多数の機能を設定して使用する必要があるため、特定の管理イーサネット機能に関して、CLI が Cisco cBR シリーズ ルータ上と他のルータの管理イーサネット インターフェイス上とで異なる可能性があります。
- VRF は、ルート リークを防ぎ、管理ポートからの不要なトラフィックを回避します。

管理イーサネット インターフェイスの VRF では、IPv4 と IPv6 の両方のアドレス ファミリがサポートされます。

共通のイーサネット管理タスク

ユーザは管理イーサネット インターフェイスを介してルータ上のほとんどのタスクを実行できます。

ここでは、Cisco cBR シリーズ ルータ上で共通のタスクまたは少し注意が必要なタスクについて説明します。ただし、管理イーサネット インターフェイスで実行できるすべてのタスクを包括的に説明するわけではありません。

VRF 設定の表示

管理イーサネット インターフェイスの VRF 設定を表示するには、 **show running-config vrf** コマンドを使用できます。

次に、デフォルトの VRF 設定の例を示します。

```
Router# show running-config vrf
Building configuration...

Current configuration : 351 bytes
vrf definition Mgmt-intf
!
```

```
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
(some output removed for brevity)
```

管理イーサネット インターフェイス VRF でのデフォルト ルートの設定

管理イーサネット インターフェイス VRF 内でデフォルト ルートを設定するには、**ip route vrf Mgmt-intf 0.0.0.0 0.0.0.0** *next-hop-IP-address* コマンドを使用します。

管理イーサネット IP アドレスの設定

管理イーサネット ポートの IP アドレスは、その他のインターフェイス上の IP アドレスと同じように設定します。

次に、管理イーサネット インターフェイス上で IPv4 アドレスおよび IPv6 アドレスを設定する簡単な例を 2 つ示します。

IPv4 の例

```
Router(config)# interface GigabitEthernet 0
Router(config-if)# ip address A.B.C.D A.B.C.D
```

IPv6 の例

```
Router(config)# interface GigabitEthernet 0
Router(config-if)# ipv6 address X:X:X:X::X /prefix-length
```

管理イーサネット インターフェイス上での Telnet 接続

Telnet 接続は、管理イーサネット インターフェイスを使用して VRF 経由で行うことができます。

次の例では、ルータは管理イーサネット インターフェイスの VRF を介して 172.17.1.1 に Telnet 接続します。

```
Router# telnet 172.17.1.1 /vrf Mgmt-intf
```

管理イーサネット インターフェイス上での PING の実行

他のインターフェイスへの PING の実行は、管理イーサネット インターフェイスを使用して VRF 経由で行うことができます。

次の例では、ルータは管理イーサネット インターフェイスを介して、172.17.1.1 の IP アドレスが設定されたインターフェイスに PING を送信します。

```
Router# ping vrf Mgmt-intf 172.17.1.1
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 172.17.1.1, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 1/1/1 ms
```

TFTP または FTP を使用したコピー

管理イーサネット インターフェイスから TFTP を使用してファイルをコピーするには、**ip tftp source-interface GigabitEthernet 0** コマンドを入力した後で **copy tftp** コマンドを入力する必要があります。これは、VRF 名を指定するためのオプションが **copy tftp** コマンドにないためです。

同様に、管理イーサネット インターフェイスで FTP を使用してファイルをコピーする場合も、**copy ftp** コマンドには VRF 名を指定するオプションがないため、**ip ftp source-interface GigabitEthernet 0** コマンドを入力した後で **copy ftp** コマンドを入力する必要があります。

TFTP の例

```
Router(config)# ip tftp source-interface gigabitethernet 0
```

FTP の例

```
Router(config)# ip ftp source-interface gigabitethernet 0
```

NTP サーバ

管理イーサネット インターフェイスを通じて Network Time Protocol（NTP）タイム サーバと同期できるようにソフトウェア クロックを設定するには、**ntp server vrf Mgmt-intf** コマンドを入力し、アップデートを提供するデバイスの IP アドレスを指定します。

次の CLI では、このプロシージャの例を示します。

```
Router(config)# ntp server vrf Mgmt-intf 172.17.1.1
```

SYSLOG サーバ

ログに記録するために送信元 IP または IPv6 アドレスとして管理イーサネット インターフェイスを指定するには、**logging host** *ip-address***vrf Mgmt-intf** コマンドを入力します。

次の CLI では、このプロシージャの例を示します。

```
Router(config)# logging host ip-address vrf Mgmt-intf
```

SNMP 関連サービス

管理イーサネット インターフェイスをすべての SNMP トラップ メッセージのソースとして指定するには、**snmp-server source-interface traps gigabitEthernet 0** コマンドを入力します。

次の CLI では、このプロシージャの例を示します。

```
Router(config)# snmp-server source-interface traps gigabitEthernet 0
```

ドメイン名の割り当て

管理イーサネットインターフェイスへのドメイン名の割り当ては、VRFを介して実行されます。

デフォルトのドメイン名を管理イーサネット VRF インターフェイスとして定義するには、**ip domain-name vrf Mgmt-intf** *domain* コマンドを入力します。

```
Router(config)# ip domain-name vrf Mgmt-intf cisco.com
```

DNS サービス

管理イーサネット インターフェイスの VRF をネーム サーバとして指定するには、**ip name-server vrf Mgmt-intf** *IPv4/IPv6 address* コマンドを入力します。

RADIUS サーバまたは TACACS+ サーバ

管理 VRF を AAA サーバ グループの一部としてグループ化するには、AAA サーバ グループの設定時に **ip vrf forward Mgmt-intf** コマンドを入力します。

TACACS+ サーバ グループを設定する場合も、同様にします。管理 VRF を TACACS+ サーバ グループの一部としてグループ化するには、TACACS+ サーバ グループの設定時に **ip vrf forwarding Mgmt-intf** コマンドを入力します。

RADIUS サーバ グループの設定

```
Router(config)# aaa group server radius hello
Router(config-sg-radius)# ip vrf forwarding Mgmt-intf
```

TACACS+ サーバ グループ コンフィギュレーション

```
Router(config)# aaa group server tacacs+ hello
Router(config-sg-tacacs+)# ip vrf forwarding Mgmt-intf
```

ACL を使用した VTY 回線

VRF を使用する（または使用しない）vty 回線にアクセス コントロール リスト（ACL）を確実に関連付けるには、ACL を vty 回線に関連付ける際に **vrf-also** オプションを使用します。

```
Router(config)# line vty 0 4
Router(config-line)#access-class 90 in vrf-also
```

ネットワーク管理用補助ポートの設定

手順

ステップ 1 補助ポートは IOSd コマンド プロンプトで使用されます。rommon プロンプトで **set** コマンドを入力します。

ステップ 2 BOOT_PARAM が定義されているかどうかを確認します。定義されていてはいけません。

ステップ 3 BOOT_PARAM が定義されている場合は、次の手順に従います。

a) **unset BOOT_PARAM** を入力します。

b) **sync** を入力します。

c) **reset** を入力します。

ステップ 4 最新のイメージで起動します。補助ポートに IOS コマンド プロンプトが表示されます。

Cisco cBR シャーシでのスーパーバイザの事前プロビジョニング

Cisco cBRで事前プロビジョニングを使用すると、スーパーバイザをシャーシに物理的に装着せずに設定することができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**card** *slot*/**1 sup-pic-8x10g** 例： `Router(config)# card 4/1 sup-pic-8x10g`	Cisco cBR シャーシにスーパーバイザを事前にプロビジョニングします。 • *slot*：スーパーバイザ PICのシャーシ スロット番号を特定します。有効な値は 4 と 5 です。

ネットワーク管理用ギガビット イーサネット インターフェイスの設定

GigabitEthernet0 インターフェイスを設定し、NME ポートを使用できるようにします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface GigabitEthernet0** 例： `Router(config)# interface GigabitEthernet0`	ギガビット イーサネット インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**vrf forwarding** *vrf-name* 例： `Router(config-if)# vrf forwarding Mgmt-intf`	Virtual Routing and Forwarding（VRF）インスタンスをインターフェイスに関連付けます。 • *vrf-name*：指定した VRF に関連付けられたインターフェイス名。
ステップ 5	**ip address** *ip-address subnet-mask* 例： `Router(config-if)# ip address 192.71.0.1 255.255.255.0`	ギガビット イーサネット インターフェイスの IP アドレスを設定します。 • *ip-address*：ギガビット イーサネット インターフェイスの IP アドレス。 • *subnet -mask*：ネットワークのサブネット マスク。
ステップ 6	**no shutdown** 例： `Router(config-if)# no shutdown`	ギガビット イーサネット インターフェイスを有効にします。
ステップ 7	**speed 1000** [**negotiate**] 例： `Router(config-if)# speed 1000`	ギガビット イーサネット インターフェイスの速度を設定します。

	コマンドまたはアクション	目的
ステップ 8	**duplex full** 例： `Router(config-if)# duplex full`	ギガビット イーサネット インターフェイスの全二重通信を設定します。
ステップ 9	**negotiation auto** 例： `Router(config-if)# negotiation auto`	自動ネゴシエーション モードを選択します。
ステップ 10	**end** 例： `Router(config-if)# end`	ギガビット イーサネット インターフェイス コンフィギュレーション モードを終了します。特権 EXEC モードに戻ります。

スーパーバイザ PIC の DTI ポートの設定

Cisco cBR ルータはスタンドアロン モードで動作します。内部クロックを使用するため、外部基準クロック ソースは必要ありません。また、Cisco cBR ルータは、外部クロック ソースとして DTI サーバもサポートします。基準クロック ソースとして DTI サーバを使用するには、スーパーバイザ PIC の DTI ポートを有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 clock dti** 例： `Router(config)# cable clock dti`	スーパーバイザ PIC の DTI クロック基準モードを設定します。

ネットワーク管理用 10 ギガビット イーサネット インターフェイスの設定

TenGigabitEthernet インターフェイスを設定し、NME ポートを使用できるようにします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface TenGigabitEthernet** 例： `Router(config)# interface TenGigabitEthernet4/1/0`	TenGigabit イーサネット インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address subnet-mask* 例： `Router(config-if)# ip address 1.2.3.4 255.255.255.0`	TenGigabit イーサネット インターフェイスの IP アドレスを設定します。
ステップ 5	**load-interval** *seconds* 例： `Router(config-if)# load-interval 30`	データが負荷統計情報の計算に使用される時間の長さを変更します。
ステップ 6	**no shutdown** 例： `Router(config-if)# no shutdown`	TenGigabit イーサネット インターフェイスを有効にします。
ステップ 7	**end** 例： `Router(config-if)# end`	TenGigabit イーサネット インターフェイス コンフィギュレーション モードを終了します。特権 EXEC モードに戻ります。

ネットワークへの新しいルータの接続

イーサネット インターフェイスを使用して、ネットワークに新しいルータを接続します。ルータがそのホスト名を正常に解決したら、新しいルータは、name-confg または name.cfg ファイルを要求する TFTP ブロードキャストを送信します。本来のホスト名が小文字でなくても、ルータ名はすべて小文字で表記する必要があります。ファイルが新しいルータにダウンロードされ、コンフィギュレーション コマンドがすぐに適用されます。コンフィギュレーション ファイルが完了すると、新しいルータは完全に動作可能となります。

NVRAM の設定をすべて保存するには、特権 EXEC モードで次のコマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable password**	新しいルータで特権モードを開始します。
ステップ 2	**copy running-config startup-config**	name-config ファイルの情報をスタートアップ コンフィギュレーションに保存します。ほとんどのプラットフォームでは、この手順によって設定が NVRAM に保存されます。 （注） 設定の変更を保存する **copy running-config startup-config** EXEC コマンドを入力する前に、既存のルータおよび新しいルータ（またはアクセス サーバ）が接続されていることを確認します。接続を確認するには、**ping** EXEC コマンドを使用します。誤ったコンフィギュレーション ファイルがダウンロードされると、新しいルータは AutoInstall インストール モードを開始する前に、NVRAM 設定情報をロードします。 コンフィギュレーション ファイルが最小コンフィギュレーション ファイルの場合、新しいルータは稼動しますが、動作するインターフェイスは 1 つのみです。新しいルータに接続して設定するには、次のコマンドを使用します。
ステップ 3	**telnet existing**	既存のルータへの Telnet 接続を確立します。
ステップ 4	**telnet newrouter**	既存のルータから、新しいルータへの Telnet 接続を確立します。
ステップ 5	**enable password**	特権 EXEC モードを開始します。
ステップ 6	**setup**	新しいルータを設定するには、セットアップ モードを開始します。

Cisco CMTS でのパスワード保護の設定

（注） セキュリティ上の目的で、EXEC にはユーザ EXEC モードと特権 EXEC モードの 2 つのコマンド アクセス レベルがあります。ユーザ レベルで使用できるコマンドは、特権レベルで使用できるコマンドのサブセットです。

ヒント 特権レベルEXECコマンドの多くは動作パラメータの設定に使用されるので、不正使用を避けるために、これらのコマンドをパスワード保護します。

（注） イネーブル シークレット パスワードは、1 ～ 25 文字の大文字と小文字の英数字で構成されます。イネーブル パスワードには、任意の数の大文字と小文字の英数字を使用できます。数字は先頭文字として使用できません。パスワードにはスペースを使用できます。たとえば、「two words」は有効なパスワードです。先行スペースは無視されます。後続スペースは認識されます。英数字は大文字と小文字が区別されます。

最大限のセキュリティを確保するために、パスワードはそれぞれ異なるものにする必要があります。セットアップ スクリプトで両方に同じパスワードを入力した場合、システムには受け入れられますが、異なるパスワードの入力を指示する警告メッセージが表示されます。

EXEC プロンプトで、次のいずれかのコマンドを入力してパスワード保護を設定します。

- **enable secret password**：非常にセキュアな暗号化パスワード。
- **enable**：セキュリティ性が低い非暗号化パスワード。

特権レベル コマンドにアクセスするには、必要なパスワードを入力します。

Cisco CMTS での紛失したパスワードの回復

イネーブル パスワード、イネーブル シークレット パスワード、またはコンソール ログイン パスワードを回復または再設定するには、次のステップを実行します。

手順

ステップ 1 Cisco CMTS のコンソール ポートに ASCII 端末を接続します。

ステップ 2 端末を 9600 ボー、8 データ ビット、パリティなし、および 1 ストップ ビットで動作するように設定します。

ステップ 3 ルータに非特権ユーザとしてログインできる場合は、**show version** コマンドを入力して既存のコンフィギュレーション レジスタ値を表示します。後で使用するためにその値をメモします。ルータにログインできない場合は、次のステップに進みます。

ステップ 4 Break キーを押すか、またはコンソール端末から Break を送信します。

- ブレークがイネーブルの場合は、ルータの ROM モニタが起動し、ROM モニタ プロンプト（rommon n>）が表示されます。n はコマンド ラインの番号です。登録の設定に進みます。
- ブレークがディセーブルの場合は、ルータの電源を再投入します（ルータの電源をオフにするか、電源コードを抜いてから、電源を元に戻します）。ルータの電源を再投入してから 60 秒以内に、Break キーを押すか、または Break を送信します。この操作によってルータの ROM モニタが起動し、ROM モニタ プロンプト（rommon 1>）が表示されます。

ステップ 5 Cisco CMTS 上でコンフィギュレーション レジスタを設定するには、ROM モニタ プロンプトで次のように **confreg** コマンドを入力して、コンフィギュレーション レジスタ ユーティリティを使用します。

```
rommon 1> confreg
```

enable ignore system config info? プロンプトに yes と答え、現在のコンフィギュレーション レジスタの設定をメモしておきます。

ステップ 6 次のように **reset** コマンドを入力してルータを初期化します。

```
rommon 2> reset
```

ルータが初期化され、コンフィギュレーション レジスタが 0x142 に設定されます。ルータはフラッシュ メモリからシステム イメージをブートして、次のようにシステム コンフィギュレーション ダイアログ（セットアップ）に入ります。

```
--- System Configuration Dialog --
```

ステップ 7 次のメッセージが表示されるまで、システム コンフィギュレーション ダイアログのプロンプトへの応答として no を入力します。

```
Press RETURN to get started!
```

ステップ 8 Return キーを押します。次のようにユーザ EXEC プロンプトが表示されます。

```
Router>
```

ステップ 9 **enable** コマンドを入力して特権 EXEC モードを開始します。

ステップ 10 次のように **show startup-config** コマンドを入力して、コンフィギュレーション ファイル内のパスワードを表示します。

```
Router# show startup-config
```

ステップ 11 コンフィギュレーションファイルの表示を調べてパスワードを探します。イネーブルパスワードは通常、ファイルの先頭付近にあります。コンソール ログイン パスワードまたはユーザ EXEC パスワードは末尾付近にあります。パスワードは次のように表示されます。

```
enable secret 5 $1$ORPP$s9syZt4uKn3SnpuLDrhuei
enable password 23skiddoo
.
.
line con 0
 password onramp
```

（注） イネーブル シークレット パスワードは暗号化されているため回復できず、再設定する必要があります。イネーブル パスワードとコンソール パスワードは、暗号化テキストにすることも、クリア テキストにすることもできます。

イネーブル シークレット パスワード、コンソール ログイン パスワード、またはイネーブル パスワードを再設定するには、次のステップに進んでください。イネーブル シークレット パスワードがなく、イネーブル パスワードおよびコンソール ログイン パスワードが暗号化されていない場合は、コンフィギュレーション レジスタを元の値に設定します。

注意 イネーブル パスワード、イネーブル シークレット パスワード、またはコンソール ログイン パスワードを変更または置換する必要があるかどうかが不明な場合は、次のステップを実行しないでください。ここで示すステップに従わなかった場合、ルータ コンフィギュレーションが消去される可能性があります。

ステップ 12 （任意） configure memory コマンドを入力して、実行中のメモリにスタートアップ コンフィギュレーション ファイルをロードします。この操作によって、パスワードを変更したり再設定することができます。

```
Router# configure memory
```

ステップ 13 **configure terminal** コマンドを入力してコンフィギュレーション モードを開始します。

```
Router# configure terminal
```

ステップ 14 3 つすべてのパスワードを変更するには、次のコマンドを入力します。

```
Router(config)# enable secret newpassword1

Router(config)# enable password newpassword2
Router(config)# line con 0

Router(config)# password newpassword3
```

設定に必要なパスワードだけを変更してください。上記のコマンドの **no** 形式を使用すると、個別のパスワードを削除できます。たとえば、**no enable secret** コマンドを入力すると、イネーブル シークレット パスワードが削除されます。

ステップ 15 次のように、すべてのインターフェイスに管理上のシャットダウンの解除を設定する必要があります。

```
Router(config)# interface gigabitethernet 0

Router(config)# no shutdown
```

もともと設定されていたすべてのインターフェイスに対して、同等なコマンドを入力します。このステップを省略すると、すべてのインターフェイスが管理上のシャットダウン状態になり、ルータの再起動時に使用できなくなります。

ステップ 16 **config-register** コマンドを使用して、コンフィギュレーション レジスタを上記の元の値に設定します。

ステップ 17 Ctrl-Z を押すか、**end** と入力してコンフィギュレーション モードを終了します。

```
Router(config)# end
```

注意 パスワードを変更または置換していない場合は、次のステップを実行しないでください。イネーブル、イネーブル シークレット、コンソール ログイン パスワードの変更または置き換えを以前回避した場合は、ここでリロードします。この手順に従わなかった場合、ルータ コンフィギュレーション ファイルが消去される可能性があります。

ステップ 18 **copy running-config startup-config** コマンドを入力して、新しい設定を不揮発性メモリに保存します。

```
Router# copy running-config startup-config
```

ステップ 19 **reload** コマンドを入力して、ルータを再起動します。

```
Router# reload
```

ステップ 20 新しいパスワードまたは回復されたパスワードを使用して、ルータにログインします。

構成時の設定の保存

NVRAM にあるスタートアップ コンフィギュレーションに設定や変更を保存するには、次のように *Router#* プロンプトで **copy running-config startup-config** コマンドを入力します。

このコマンドにより、コンフィギュレーション モードである Setup facility または AutoInstall を使用して設定したコンフィギュレーション設定が保存されます。

（注） 設定を保存しなかった場合は、次にルータをリロードしたときにコンフィギュレーションが失われます。

```
Router# copy running-config startup-config
```

設定と構成の確認

- Cisco CMTS の現在の設定を表示するには、EXEC モードまたは特権 EXEC モードでコマンドライン インターフェイス（CLI）のプロンプトから **show running-config** コマンドを実行します。

- 設定の変更内容を確認するには、EXECモードで**show startup-config**コマンドを使用すると、NVRAM に保存されている情報が表示されます。

第 2 章

シスコ スマート ライセンシング

シスコでは、スマート ライセンシングと呼ばれる、単一のテクノロジーに基づく新しいライセンス モデルが設計されています。これは、すべてのシスコ製品に企業レベルの契約と同等の機能を提供することを目的としています。シスコ スマート ライセンシングは、Trust but Verify モデルに基づいています。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

- シスコ スマート ライセンシングに関する機能情報，61 ページ

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *1*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

シスコ スマート ライセンシングの前提条件

- **ip name-server** グローバル コンフィギュレーション コマンドを使用して DNS サーバを設定する必要があります。
- **ip domain-lookup** グローバル コンフィギュレーション コマンドを使用して、IP DNS ベースのホスト名からアドレスへの変換を設定する必要があります。
- シスコ スマート ライセンシングは、Cisco cBR ルータでデフォルトでイネーブルに設定されています。ただし、**show call-home profile CiscoTAC-1** コマンドを使用して、Cisco TAC-1 call-home プロファイルで Smart Software Manager（以下の URL）を指定していることを確認する必要があります。

  https://software.cisco.com/#module/SmartLicensing

  次に、**show call-home profile CiscoTAC-1** コマンドの出力例を示します。

```
Router# show call-home profile CiscoTAC-1

Load for five secs: 10%/1%; one minute: 9%; five minutes: 8%
Time source is NTP, 16:49:35.525 PDT Thu Oct 29 2015

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Profile mode: Anonymous Reporting Only
    Reporting Data: Smart Call Home, Smart Licensing
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: http
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

   Periodic configuration info message is scheduled every 19 day of the month at 11:41


    Periodic inventory info message is scheduled every 19 day of the month at 11:26

    Alert-group               Severity
    ------------------------  ------------
    crash                     debug
    diagnostic                minor
    environment               minor
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major
```

- DNS サーバを ping できることを確認してください。サーバを ping できない場合は、Cisco cBR ルータの NME ポートへの接続を確認します。

（注） Virtual Routing and Forwarding（VRF）インスタンスを使用している場合は、VRF インスタンスを ping できることを確認してください。

シスコ スマート ライセンシングの情報

シスコ スマートライセンシングは、ソフトウェアベースのライセンシングであり、顧客によるシスコ製品の使用や報告を承認するためのツールおよびプロセスで構成されています。この機能では、顧客注文をキャプチャし、製品の登録と承認を完了するために Smart Call Home 伝送メディアを通じて Cisco Cloud License Service と通信できます。シスコ製品が Cisco Cloud License Service との通信を 90 日間停止すると、シスコ製品のケーブルインターフェイスがロックされ、顧客はケーブル インターフェイスを有効または無効にできなくなります。

シスコ スマートライセンシングの目的は、すべてのシスコ製品に対する単一の標準化されたライセンシング ソリューションをユーザに提供することです。

シスコ スマート ライセンシング モデルでは、特別なソフトウェア キーまたはアップグレード ライセンス ファイルを使用せずに、ライセンス付き機能をアクティベートできます（エンタイトルメントとも呼ばれます）。新しい機能をアクティベートするには、適切な製品コマンドおよび設定を使用します。機能がアクティベートされます。Cisco cBR ルータでは、ソフトウェア再起動は必要ありません。

Cisco cBRルータはシスコ スマート ライセンシングを使用したソフトウェア アクティベーションをサポートしています。シスコ スマート ライセンシングは、Cisco cBR ルータでデフォルトでイネーブルに設定されています。

（注） 保護ラインカードで保護された動作中のラインカードごとに LCHA ライセンスが必要です。

ダウンストリーム ライセンス

DOCSIS 3.1 ライセンス スキームは、DOCSIS 3.1 チャネルとその幅を特定する機能をサポートします。DOCSIS 3.1 エンタイトルメントは、DOCSIS 3.1 ダウンストリーム チャネル ライセンスです。

コンプライアンス違反適用

次の 2 つのイベントにより、DOCSIS 設定ロック適用が開始します。

Eval-Expired（評価期間満了）

90 日を経過してもルータがスマート ライセンス マネージャに登録されない場合。

Auth-Expired（認証期間満了）

登録済みルータが 90 日間を超えてスマート ライセンス マネージャと通信できない場合。

上記のいずれかのイベントが発生すると、スマート エージェントがプラットフォームに通知を送信します。プラットフォームはこの通知を受信した時点で、次の CLI コマンドを**ロック**します。

- **[no] cable upstream shutdown** *upstream-port-number*

- **contoller upstream-cable** *slot/subslot/controller-port-number*
- **rf-chan***channel-number*

この状態で上記の CLI を設定しようとすると、その試行が失敗して警告メッセージが表示されます。この状態でも、上記以外のすべての CLI は設定可能です。これらの CLI の一部は、Cisco ライセンス Call Home を設定し、シスコに接続してデバイスを登録することで、上記 2 つのイベントのいずれかを解除して許可状態またはコンプライアンス違反（OOC）状態になるために必要です。

変更されたコンフィギュレーション ファイルをスタートアップ コンフィギュレーション ファイルにコピーしてデバイスをリロードすると、その設定が有効になります。ただし、デバイスが強制状態にある場合は、実行コンフィギュレーションファイルをスタートアップ コンフィギュレーション ファイルにコピーする操作だけが可能です。

（注） 他のファイルをコピーしようとしても失敗し、警告メッセージが表示されます。

シスコ スマート ライセンシングの設定方法

この項の構成は、次のとおりです。

ルータでのシスコ スマート ライセンシングエージェントの使用

手順

ステップ 1 シスコ スマート アカウントをセットアップします。シスコ スマート アカウントのセットアップ, （40 ページ）を参照してください。

ステップ 2 Smart Software Manager にログインします。

ステップ 3 （任意）バーチャル アカウントを作成します。バーチャル アカウントの作成, （47 ページ）を参照してください。

（注） 1 つのバーチャル アカウントをデフォルトで使用できます。

ステップ 4 製品インスタンスの登録トークンを作成します。製品インスタンスの登録トークンの作成, （49 ページ）を参照してください。

ステップ 5 製品インスタンス登録トークンを使用して、シスコ ライセンス クラウドでルータを登録します。登録トークンを使用したシスコ ライセンス クラウドでのルータの登録, （50 ページ）を参照してください。

ステップ 6 ライセンスの管理については、Smart Software Manager にログインします。
詳細については、Smart Software Manager ツールからアクセスできる『*Cisco Smart Software Manager User Guide*』を参照してください。

シスコ スマート アカウントのセットアップ

シスコ スマートアカウントにより、スマート対応製品のライセンス管理機能をすべて使用できます。

はじめる前に

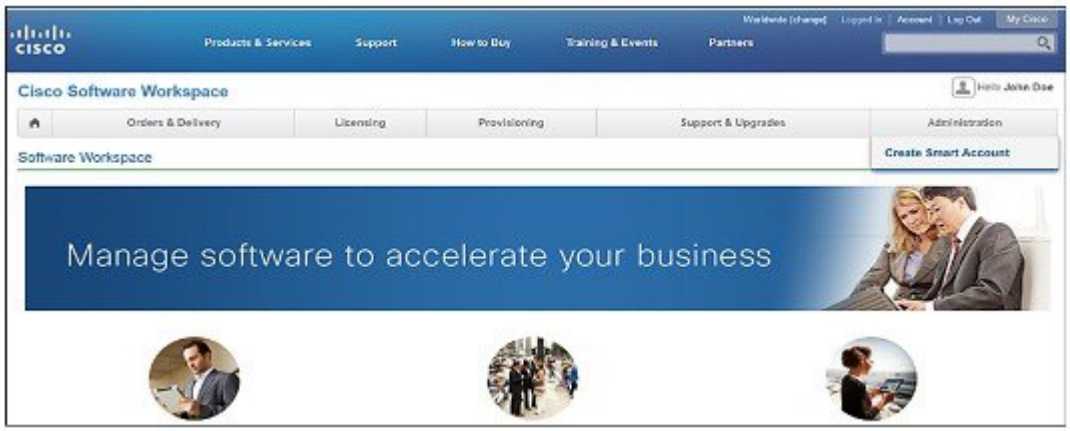
- CCO ID を所有していることを確認します。

手順

ステップ 1 CCO ID を使用して、Cisco Software Central（CSC）にログインします。

ステップ 2 [Administration] タブにカーソルを合わせ、[Request a Smart Account] をクリックします。

図 *1*：スマート アカウントの作成

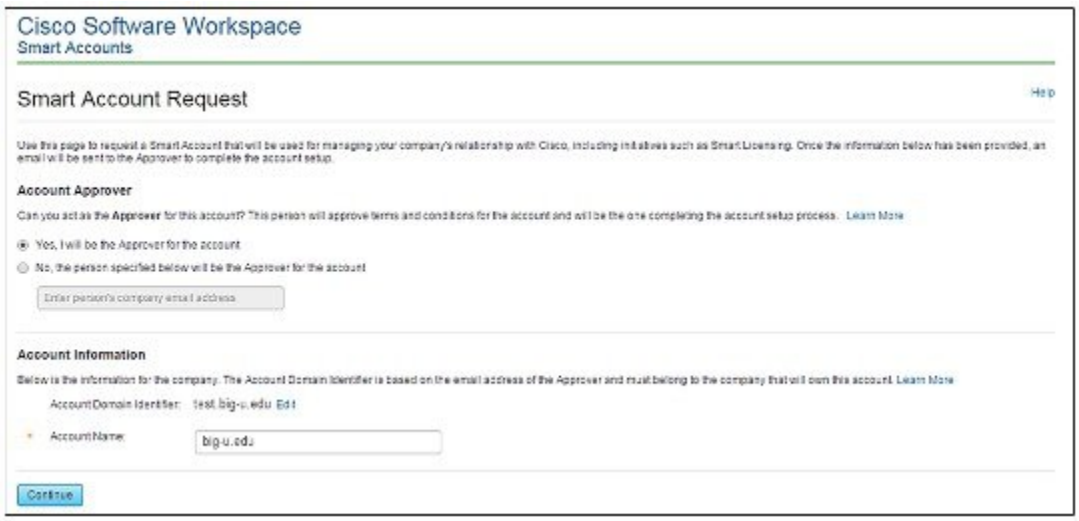


ステップ 3 アカウント承認者を選択するには、次のいずれかを実行します。

- 承認者として自分を選択するには、[Yes, I have authority to represent my company and want to create the Smart Account.] ラジオ ボタンをクリックします。
- 承認者として第三者を選択するには、[No, the person specified below will create the account:] ラジオ ボタンをクリックし、その人物の電子メール ID を指定します。

（注） 指定した承認者には、合意する権限が必要です。承認者は第一所有者の役割を務め、アカウント管理者を任命します。

図 *2*：承認者の選択



ステップ 4 承認者の場合は、次の作業を実行します。

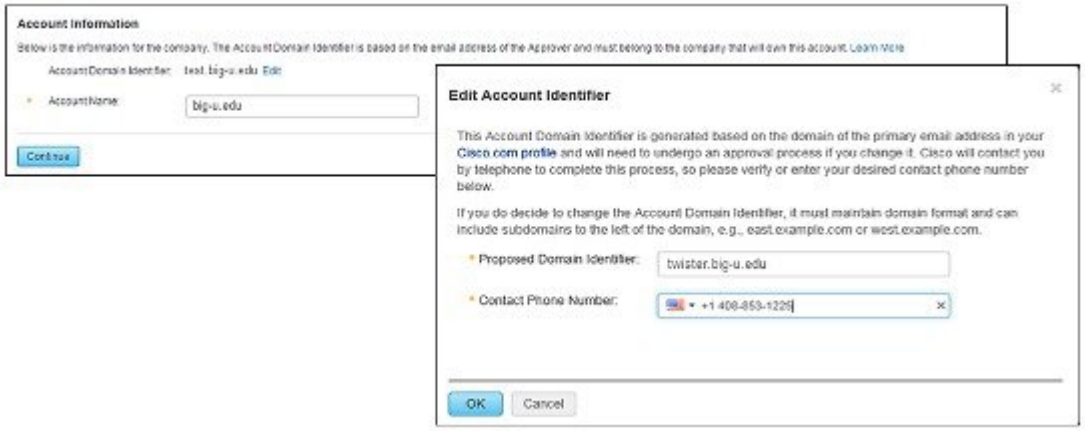
a) デフォルトでは、作成者の CCO ID プロファイルのプライマリ電子メール ID およびドメイン名が、[Account Name] フィールドおよび [Account Domain Identifier] フィールドにそれぞれ表示されます。

b) （任意）通常はデフォルトのドメイン ID を使ってください。どうしても変更が必要な場合は、[Edit] をクリックします。[Edit Account Identifier] ウィンドウで、有効な推奨ドメイン ID と連絡先電話番号を入力して、[OK] をクリックします。

（注） デフォルトのドメイン ID は承認者の電子メール ドメインです。ドメイン ID を編集する場合、その変更は手動承認プロセスに進みます。

c) [Continue] をクリックします。 アカウント情報を確認し、[Create Account] をクリックします。

図 *3*：承認者である場合のアカウント情報のセットアップ



ステップ 5 承認者でない場合は、次の作業を実行します。

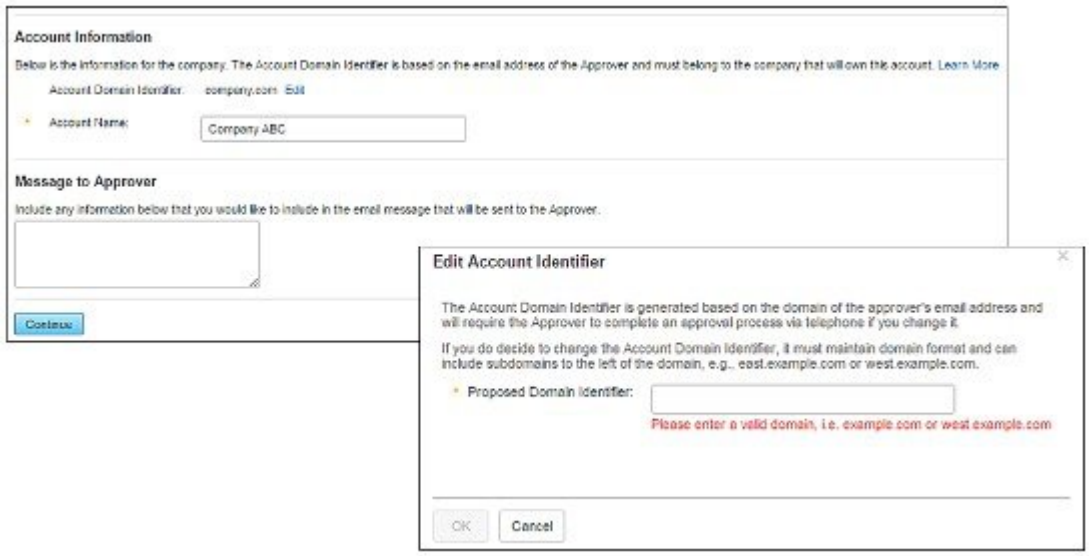
a) 別の作成者の E メールアドレス、アカウント名、作成者へのメッセージを入力します。

b) （任意）[Edit] をクリックします。[Edit Account Identifier] ウィンドウで、有効な推奨ドメイン ID を入力します。[OK] をクリックします。

（注） デフォルトのドメイン ID は承認者の電子メール ドメインです。ドメイン ID を編集する場合、その変更は手動承認プロセスに進みます。

c) [Continue] をクリックします。

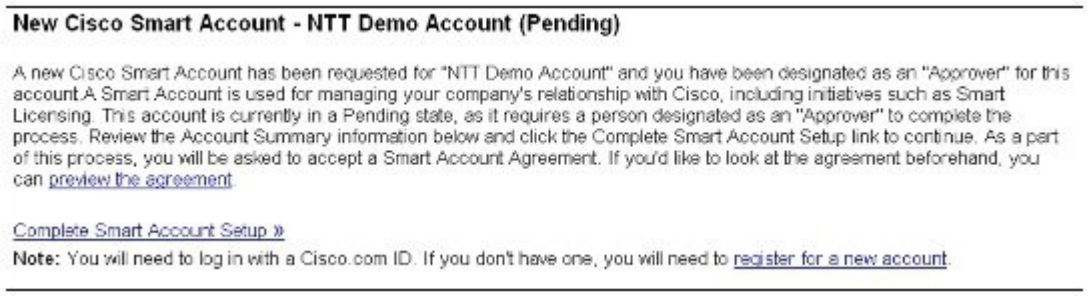
図 *4*：承認者ではない場合のアカウント情報のセットアップ



ステップ 6 承認者ではない場合、承認者は電子メールを受信し、次の作業を実行する必要があります。

a) 受信した電子メールの [Complete Smart Account Setup] をクリックします。

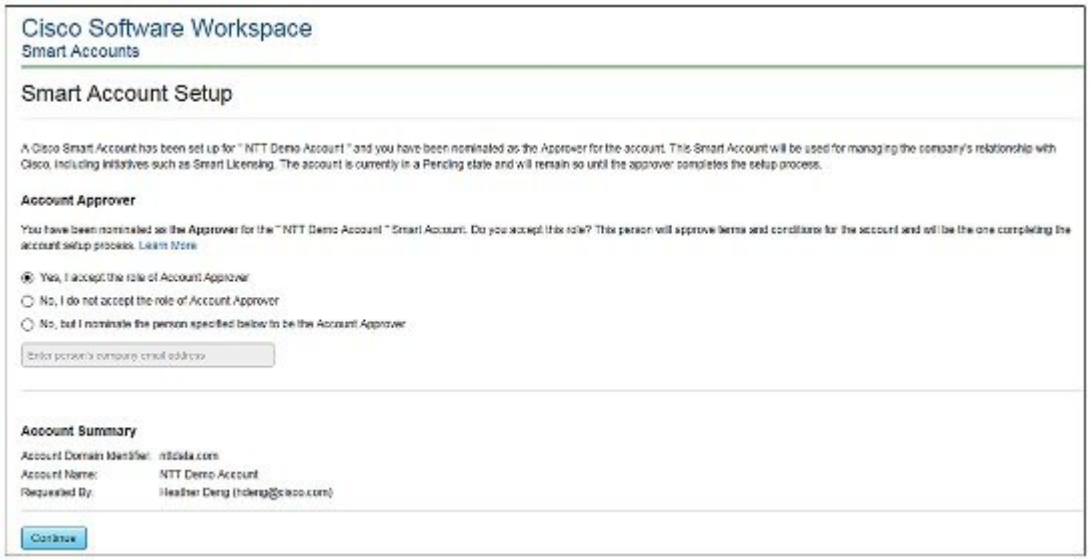
図 *5*：電子メールのスマート アカウント セットアップ リンクの実行



b) 適切なラジオボタンをクリックして、別の承認者の承認、拒否、または任命を行います。別の承認者を任命するには、ユーザの電子メール アドレスを入力します。[Continue] をクリックします。

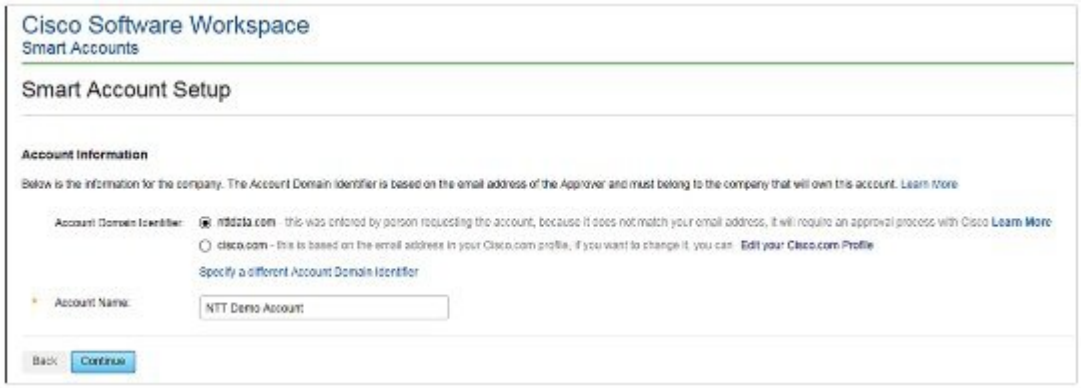
（注） 承認者が拒否した場合は、シスコ スマート アカウントが削除されます。承認者が別の承認者を任命した場合、新しい承認者はそのロールを承認する必要があります。

図 *6*：アカウント承認者ロールの承認



c) 承認者ロールを承認したら、適切なラジオ ボタンをクリックして、アカウント ドメイン ID を選択するか、または別のアカウント ドメイン ID を指定します。

図 *7*：アカウント情報の入力



d) アカウント名を入力し、[Continue] をクリックします。

承認者ロールが承認され、シスコ スマート アカウントはアカウント ドメインの承認を保留にします。

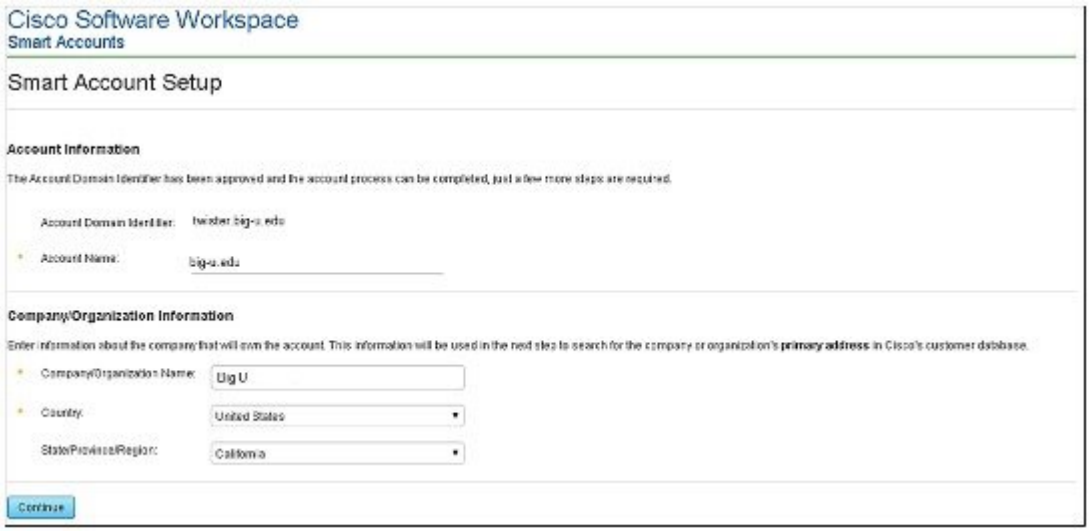
ステップ *7* アカウント ドメインが承認されると、承認者は電子メールを受信し、次の作業を実行する必要があります。

a) 受信した電子メールの [Complete Smart Account Setup] をクリックします。

図 *8*：シスコ スマート アカウント *ID* 承認済み電子メール

b) アカウント名を入力します。必要であればドメイン ID を編集し、[Continue] をクリックします。

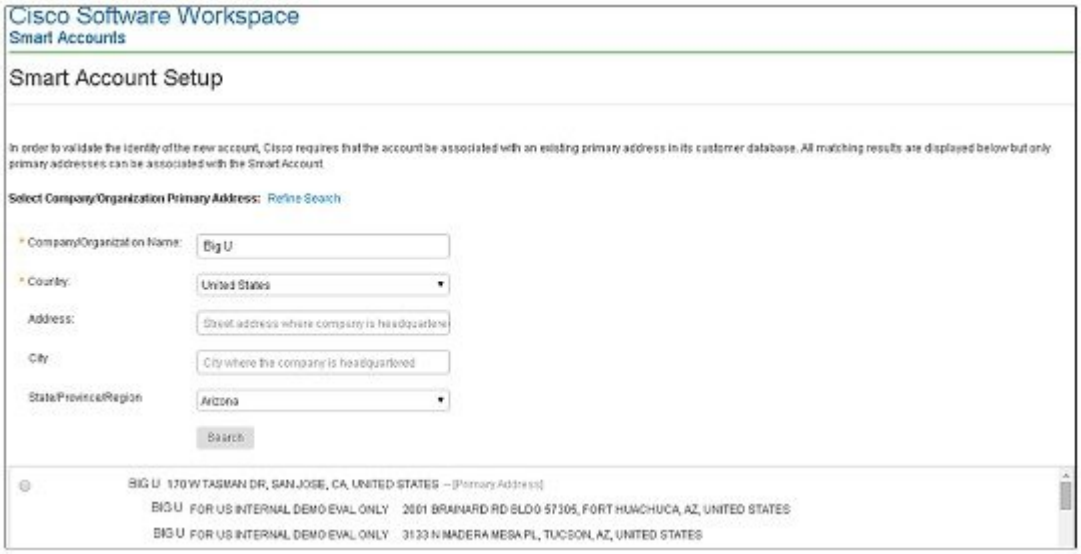
図 *9*：アカウント情報と会社/組織情報の入力



c) スマートアカウントの本社の法的所在地（国）を選択し、会社名を入力すると検索結果が表示されます。正しい住所が検索されない場合は [Show more Results] をクリックします。適切なアドレスを選択し、[Continue] をクリックします。

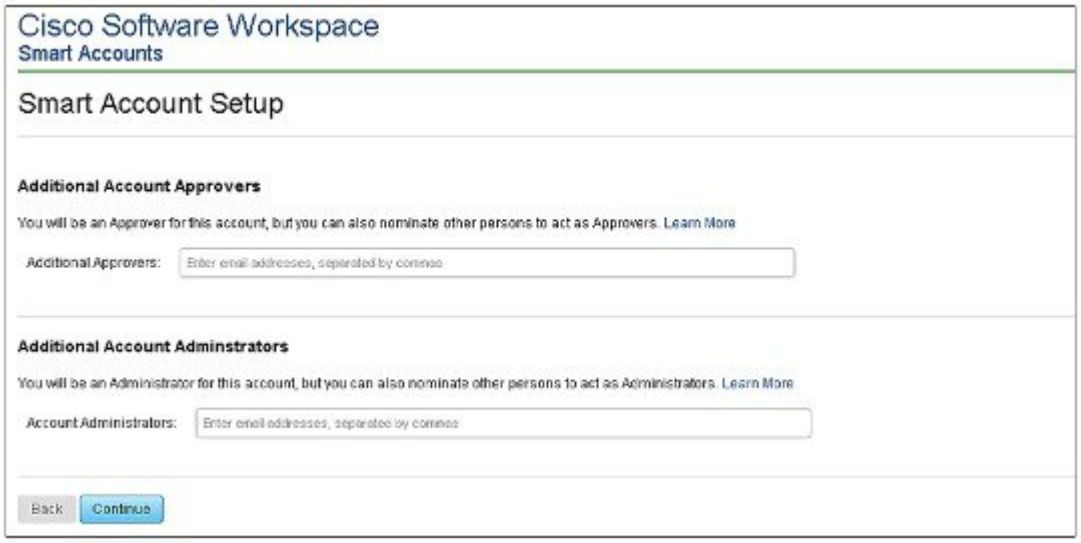
d) 住所が見つからない場合は [Can't find the address?] のボックスをクリックし、会社/組織の本社住所を入力後に [Continue] をクリックし、[Use Modified Address] をクリックします。

図 *10*：会社/組織の第一住所の選択



e) （任意）追加アカウント承認者および追加アカウント管理者の電子メールアドレスを入力します。
最初の承認者が自動的に管理者になります。追加管理者は、承認者作成プロセスとは別に作成または割り当てを行うことができます。

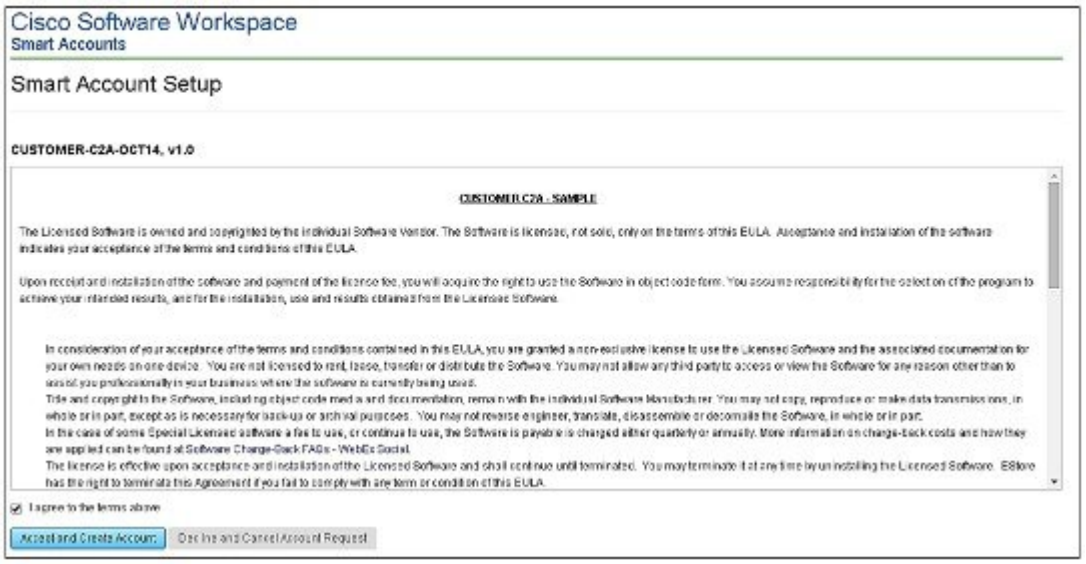
図 *11*：追加アカウント承認者と管理者の任命



f) [Continue] をクリックします。
g) アカウント サマリ情報が正しいかどうか確認し、[Create Account] をクリックします。
h) ライセンスを使用するためには契約に合意する必要があります。契約に合意する権限がある場合は、スマート アカウントを作成した後 SSM にアクセスし、[View/Accept] をクリックしま

す。契約を確認し、契約内容に合意する場合はチェックボックスをクリックし [Accept] をクリックします。

図 *12*：シスコ スマート アカウント作成後の合意の承認



シスコ スマート アカウントの作成を確認する電子メールを受信します。

バーチャル アカウントの作成

この手順は任意です。バーチャル アカウントは、ライセンスと製品インスタンスの集合体です。Cisco Software Central（CSC）でバーチャル アカウントを作成して、自社のライセンスを論理的に整理できます。1 つのバーチャルアカウントをデフォルトで使用できます。

はじめる前に

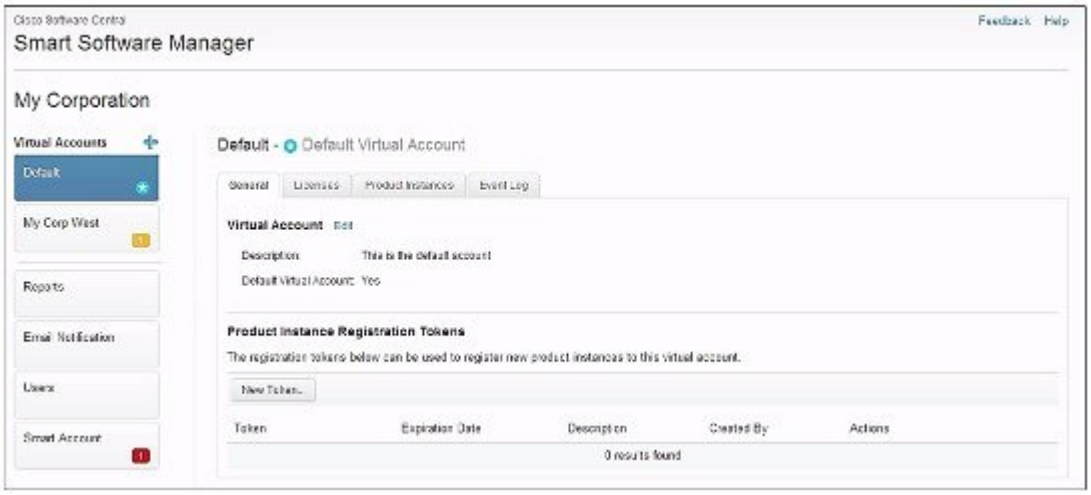
シスコ スマート アカウントをセットアップします。シスコ スマート アカウントのセットアップ, （40 ページ）を参照してください。

手順

ステップ 1 CCO ID を使用して、Cisco Software Central（CSC）にログインします。

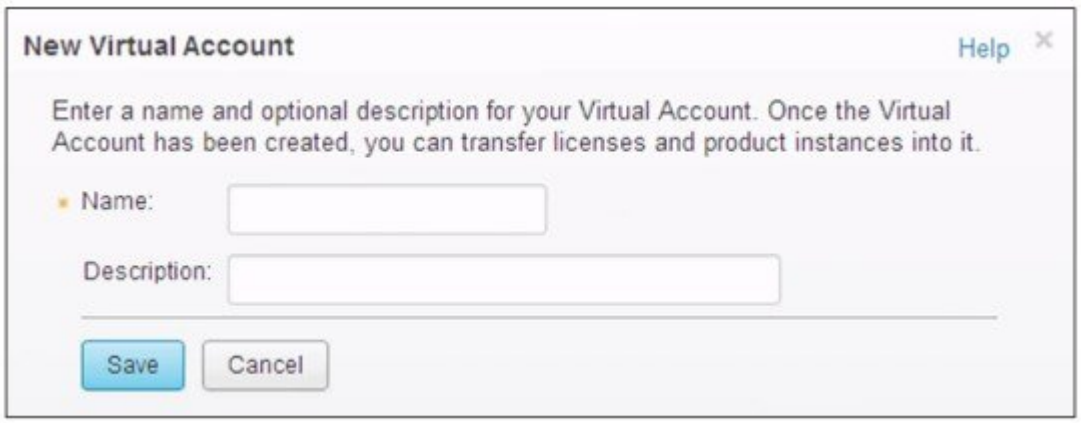
ステップ 2 [+]（プラス）記号をクリックして、バーチャル アカウントを作成します。

図 *13*：バーチャル アカウントの作成



ステップ 3 [New Virtual Account] ダイアログボックスで、[Name] と [Description] を入力します。

図 *14*：新規バーチャル アカウント ダイアログボックス



ステップ 4 **[Save]** をクリックします。

製品インスタンスの登録トークンの作成

製品インスタンスの登録トークンを使用して、製品にシスコ スマート ライセンシングを登録し、消費します。製品を登録し、製品インスタンスを特定のバーチャル アカウントに追加するには、トークンを生成する必要があります。登録トークンの有効日数は、1～365 日間に設定できます。

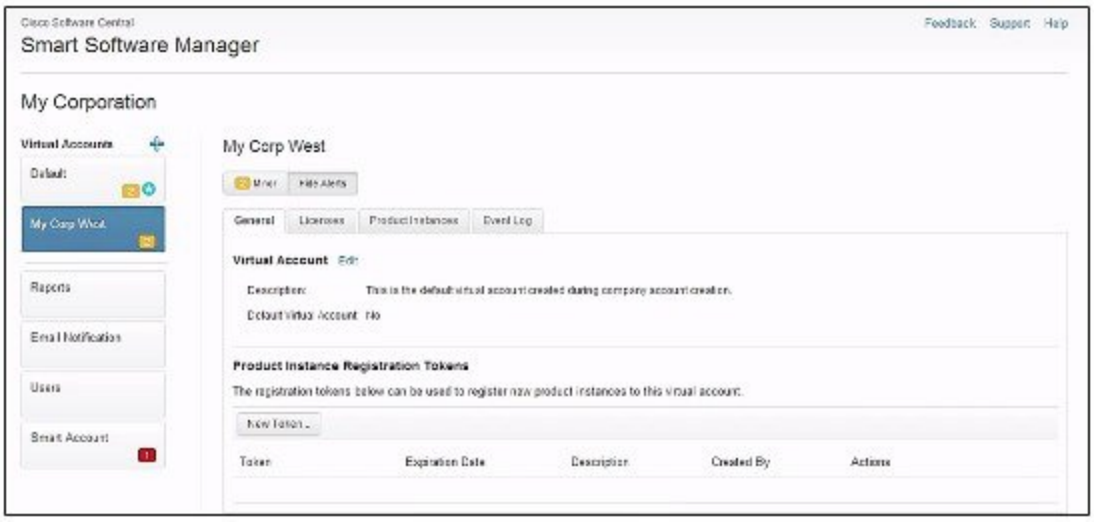
手順

ステップ 1 Smart Software Manager にログインします。

ステップ 2 既存のバーチャル アカウントをクリックします。

ステップ 3 [General] タブで、[New Token] をクリックします。

図 *15*：新規登録トークンの作成



ステップ 4 [Create Registration Token] ダイアログボックスで、[Description] と [Expire After] の情報を入力し、[Create Token] をクリックします。

図 *16*：登録トークン ダイアログ ボックスの作成

次の作業

シスコ ライセンス クラウドを使用してルータを登録します。詳細については、「登録トークンを使用したシスコ ライセンス クラウドでのルータの登録」を参照してください。

登録トークンを使用したシスコ ライセンス クラウドでのルータの登録

ルータの登録は、製品インスタンスごとに一度だけ実行します。

（注） 製品インスタンス登録トークンを所有していることを確認します。

登録トークンを使用してシスコ ライセンス クラウドにルータを登録するには、次のコマンドを使用します。

```
enable
license smart register idtoken id-token
```

次に例を示します。

```
Router#license smart register idtoken
YjBkOWM5YTItMDFiOS00ZjBmLTllY2YtODEzMzg1YTMyZDVhLTEz
ODE0MjE0%0ANzc5NDF8U1BDUTAySWFRTmJqa1NnbmlzRUIyaGlYU
053L0pHZTNvUW9VTFpE%0AekxCOD0%3D%0A
```

システムが Cisco Smart Licensing サーバに接続し、Smart Licensing の認証を取得します。

ライセンス エージェントは製品をシスコに登録し、ID証明書を受け取ります。この証明書は保存され、それ以降のシスコとのすべての通信で自動的に使用されます。ライセンス エージェントは、シスコへの登録情報を 30 日ごとに自動的に更新します。

（注） いずれかのインターフェイスで IPv6 が設定されている場合、インターネットや Cisco Smart Software Agent（ools.cisco.com）への IPv6 接続がルータになければ、スマート ライセンス付与が失敗することがあります。ログ ファイルに次のようなエラー メッセージが記録されることがあります。

（他の条件が該当する場合にも、これらのメッセージが表示されることがあります。）

```
%SMART_LIC-3-AGENT_REG_FAILED: Smart Agent for Licensing Registration with Cisco licensing
 cloud failed: Fail to send out Call Home HTTP message.
%SMART_LIC-3-COMM_FAILED: Communications failure with Cisco licensing cloud: Fail to
send out Call Home HTTP message.
```

この問題により接続に失敗した場合は、「Cisco Smart Call Home サーバとの接続の再確立」を参照してください。

接続が確立された後、シスコ ライセンス クラウドにルータを登録します。

Cisco Smart Call Home サーバとの接続の再確立

ここでは、IPv6 が設定された状態で、ルータが Cisco Smart Call Home サーバと接続できない場合の対処方法について説明します。

次のシナリオが当てはまります。

- **ip http client source-interface interface** CLI を使ってインターフェイスが設定され、IPv6 アドレスが割り当てられている場合、ルータは IPv6 接続でリモート サーバとのセッションを確立します。
- **ip http client source-interface interface** コマンドを使ってインターフェイスが設定され、IPv4 アドレスが割り当てられている場合、ルータは IPv4 接続でリモート サーバとのセッションを確立します。
- **ip http client source-interface interface** コマンドを使ってインターフェイスが設定され、IPv6 アドレスと IPv4 アドレスが割り当てられている場合、ルータは IPv6 接続でリモート サーバとのセッションを確立します。
- **ip http client source-interface interface** を使ってインターフェイスが設定されない場合、ルータは IPv6 アドレスでリモート サーバとのセッションを確立します。

Cisco IOS XE Everest 16.5.1 以降では、インターフェイスで IPv6 アドレスを使用できる場合、デバイスがインターネットや Cisco Smart Software Agent に接続できなければ、次のコンフィギュレーション モード コマンドを実行して、スマート ライセンシングに IPv4 だけを使用するようインターフェイスを設定してください。

```
ip http client source-interface interface
```

トランスポートゲートウェイソリューションを使用したシスコスマート ライセンシングの設定方法

次の手順では、トランスポート ゲートウェイ ソリューションを使用したシスコ スマート ライセンシングの設定方法を説明します。

はじめる前に

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**crypto pki trustpoint** 例： `Router(config)# crypto pki trustpoint cisco`	ルータに使用させるトラストポイントを宣言します。
ステップ 4	**enrollment terminal** 例： `Router(ca-trustpoint)# enrollment terminal`	カットアンドペーストによる手動での証明書登録を指定します。
ステップ 5	**revocation-check** *method* 例： `Router(ca-trustpoint)# revocation-check none`	証明書の失効ステータスを検査します。method が

	コマンドまたはアクション	目的
		none に設定されている場合、証明書の検査が必要ではないことを意味します。
ステップ 6	**crypto pki authenticate** 例： `Router(config)# crypto pki authenticate cisco`	証明機関を認証します。

ステップ 7	**no reporting smart-licensing-data**
	
	例：
	
	`Router(config)# call-home`
	`Router(cfg-call-home)# profile CiscoTAC-1`
	`Router(cfg-call-home-profile)# no reporting smart-licensing-data`
		tools.cisco.com と通信しないようにデフォルト プロファイルを設定します。

ステップ 8	**destination address http** *address*
	
	例：
	
	`Router(config)# call-home`
	`Router(cfg-call-home)# profile Custom-Profile-1`
	`Router(cfg-call-home-profile)# reporting smart-licensing-data`
	`Router(cfg-call-home-profile)# destination transport-method http`
	`Router(cfg-call-home-profile)# no destination transport-method email`
	`Router(cfg-call-home-profile)# destination address http`
	`https://TDS.IP.HERE:8443/Transportgateway/services/DeviceRequestHandler`
		転送サーバと通信するようにカスタム プロファイルを設定します。ここでは、カスタム プロファイルの名前として Custom Profile 1 を使用します。

シスコ スマート ライセンシング設定の確認

Cisco cBR ルータでシスコ スマート ライセンシング設定を確認するには、次のコマンドを使用します。

- **show license all**：すべてのライセンス情報を表示します。

  次に、このコマンドの出力例を示します。

```
Router# show license all

Smart Licensing Status
======================
```

```
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Virtual Account: auto-test-1
  Initial Registration: SUCCEEDED on Mar  5 02:01:03 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Sep  1 02:03:51 2015 UTC
  Registration Expires: Never

License Authorization:
  Status: OUT OF COMPLIANCE on Mar  5 03:34:54 2015 UTC
  Last Communication Attempt: SUCCEEDED on Mar  5 03:35:57 2015 UTC
  Next Communication Attempt: Mar  5 15:35:57 2015 UTC
  Communication Deadline: Jun  3 03:32:51 2015 UTC

License Usage
==============

(US_License):
  Description:
  Count: 64
  Version: 1.0
  Status: AUTHORIZED

(DS_License):
  Description:
  Count: 768
  Version: 1.0
  Status: AUTHORIZED

(WAN_License):
  Description:
  Count: 8
  Version: 1.0
  Status: OUT OF COMPLIANCE

Product Information
===================
UDI: PID:CBR-8-CCAP-CHASS,SN:FXS1739Q0NT

HA UDI List:
    Active:PID:CBR-8-CCAP-CHASS,SN:FXS1739Q0NT
    Standby:PID:CBR-8-CCAP-CHASS,SN:FXS1739Q0NT

Agent Version
=============
Smart Agent for Licensing: 1.2.1_throttle/5
Component Versions: SA:(1_2_1_throttle)1.1.0, SI:(rel20)1.0.1, CH:(rel4)1.0.15,
PK:(rel16)1.0.7
```

- **show license status**：ライセンス ステータス情報を表示します。

  次に、このコマンドの出力例を示します。

```
Router# show license status

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Virtual Account: auto-test-1
  Initial Registration: SUCCEEDED on Mar  5 02:01:03 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Sep  1 02:03:51 2015 UTC
  Registration Expires: Never

License Authorization:
  Status: OUT OF COMPLIANCE on Mar  5 03:34:54 2015 UTC
  Last Communication Attempt: SUCCEEDED on Mar  5 03:35:57 2015 UTC
  Next Communication Attempt: Mar  5 15:35:56 2015 UTC
```

```
  Communication Deadline: Jun  3 03:32:50 2015 UTC
```

- **show license summary**：ライセンスの概要情報を表示します。

  次に、このコマンドの出力例を示します。

```
Router# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Virtual Account: auto-test-1
  Last Renewal Attempt: None
  Next Renewal Attempt: Sep  1 02:03:51 2015 UTC

License Authorization:
  Status: OUT OF COMPLIANCE
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Mar  5 15:35:56 2015 UTC

License Usage:
               License       Entitlement tag    Count Status
  -----------------------------------------------------------------
                               (US_License) 64       AUTHORIZED
                               (DS_License) 768      AUTHORIZED
                              (WAN_License) 8        OUT OF COMPLIANCE
```

- **show license tech support**：ライセンスのテクニカル サポート情報を表示します。

  次に、このコマンドの出力例を示します。

```
Router# show license tech support

Smart Licensing Tech Support info

Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Virtual Account: auto-test-1
  Initial Registration: SUCCEEDED on Mar  5 02:01:03 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Sep  1 02:03:51 2015 UTC
  Registration Expires: Never

License Authorization:
  Status: OUT OF COMPLIANCE on Mar  5 03:34:54 2015 UTC
  Last Communication Attempt: SUCCEEDED on Mar  5 03:35:57 2015 UTC
  Next Communication Attempt: Mar  5 15:35:57 2015 UTC
  Communication Deadline: Jun  3 03:32:51 2015 UTC

Evaluation Period:
  Evaluation Mode: Not In Use
  Evaluation Period Remaining: 89 days, 23 hours, 25 minutes, 40 seconds

License Usage
=============
Handle: 1
    License: 'nullPtr'
    Entitlement Tag:
regid.2014-11.com.cisco.US_License,1.0_a3f32909-2c71-426c-b3e0-eeefc946f9b3
    Description: <empty>
    Count: 64
    Version: 1.0
    Status: AUTHORIZED(3)
    Status time: Mar  5 03:34:54 2015 UTC
```

```
    Request Time: Mar  5 03:34:17 2015 UTC

Handle: 2
    License: 'nullPtr'
    Entitlement Tag:
regid.2014-11.com.cisco.DS_License,1.0_71ad0ae1-5e5e-4f02-b380-d2e1b8dcfa03
    Description: <empty>
    Count: 768
    Version: 1.0
    Status: AUTHORIZED(3)
    Status time: Mar  5 03:34:54 2015 UTC
    Request Time: Mar  5 03:34:17 2015 UTC

Handle: 3
    License: 'nullPtr'
    Entitlement Tag:
regid.2014-11.com.cisco.WAN_License,1.0_3d8bb7ba-1a92-4f01-a4aa-a4479f1d7612
    Description: <empty>
    Count: 8
    Version: 1.0
    Status: OUT OF COMPLIANCE(4)
    Status time: Mar  5 03:34:54 2015 UTC
    Request Time: Mar  5 03:34:17 2015 UTC

Product Information
===================
UDI: PID:CBR-8-CCAP-CHASS,SN:FXS1739Q0NT

HA UDI List:
    Active:PID:CBR-8-CCAP-CHASS,SN:FXS1739Q0NT
    Standby:PID:CBR-8-CCAP-CHASS,SN:FXS1739Q0NT

Agent Version
=============
Smart Agent for Licensing: 1.2.1_throttle/5
Component Versions: SA:(1_2_1_throttle)1.1.0, SI:(rel20)1.0.1, CH:(rel4)1.0.15,
PK:(rel16)1.0.7

Upcoming Scheduled Jobs
=======================
Current time: Mar  5 03:37:46 2015 UTC
IdCert Expiration Warning: Jan  4 02:00:41 2016 UTC (304 days, 22 hours, 22 minutes,
55 seconds remaining)
Daily: Mar  6 03:21:11 2015 UTC (23 hours, 43 minutes, 25 seconds remaining)
Certificate Renewal: Sep  1 02:03:51 2015 UTC (179 days, 22 hours, 26 minutes, 5 seconds
 remaining)
Certificate Expiration Check: Mar  4 02:00:41 2016 UTC (364 days, 22 hours, 22 minutes,
 55 seconds remaining)
Authorization Renewal: Mar  5 15:35:57 2015 UTC (11 hours, 58 minutes, 11 seconds
remaining)
Authorization Expiration Check: Jun  3 03:32:51 2015 UTC (89 days, 23 hours, 55 minutes,
 5 seconds remaining)
Init Flag Check: Not Available

License Certificates
====================
Production Cert: True
PIID: 36bf91ae-0577-4213-9e62-1b6ee0add02f
Licensing Certificated:
    Id certificate Info:
        Start Date: Mar  5 01:57:54 2015 UTC
        Expiry Date: Mar  4 01:57:54 2016 UTC
        Version Number: 3
        Serial Number: 134418
        Common Name: 05FB26B1A58A106DEA6878C346432186D08BC1C5::1,2

    Signing certificate Info:
        Start Date: Jun 14 20:18:52 2013 UTC
        Expiry Date: Apr 24 21:55:42 2033 UTC
        Version Number: 3
        Serial Number: 3
        Common Name: MMI Signer
```

```
    Sub CA Info:
        Start Date: Apr 24 22:19:15 2013 UTC
        Expiry Date: Apr 24 21:55:42 2033 UTC
        Version Number: 3
        Serial Number: 2
        Common Name: Smart Licensing CA - DEV


HA Info
==========
RP Role: Active
Chassis Role: Active
Behavior Role: Active
RMF: True
CF: True
CF State: Stateless

Other Info
==========
Software ID: regid.2014-12.com.cisco.CBR8V1,1.0_95948658-0b8b-4e8f-838d-b17020364ca9
Agent State: OOC
TS enable: True
Transport: Callhome
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True
Privacy Send IP: True
Build type:: Production
sizeof(char)  : 1
sizeof(int)   : 4
sizeof(long)  : 4
sizeof(char *): 8
sizeof(time_t): 4
sizeof(size_t): 8
Endian: Big
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
WaitForHaRole: False
standbyIsHot: True
chkPtType: 2
delayCommInit: False
roleByEvent: True
maxTraceLength: 150
traceAlwaysOn: False
debugFlags: 7
```

- **show license udi**：ライセンスの Unique Device Identifier（UDI）情報を表示します。

  次に、このコマンドの出力例を示します。

```
Router# show license udi

UDI: PID:CBR-8-CCAP-CHASS,SN:FXS1739Q0NT

HA UDI List:
    Active:PID:CBR-8-CCAP-CHASS,SN:FXS1739Q0NT
    Standby:PID:CBR-8-CCAP-CHASS,SN:FXS1739Q0NT
```

- **show license usage**：ライセンスの使用状況を表示します。

  次に、このコマンドの出力例を示します。

```
Router# show license usage

License Authorization:
  Status: OUT OF COMPLIANCE on Mar  5 03:34:54 2015 UTC

(US_License):
  Description:
  Count: 64
```

```
  Version: 1.0
  Status: AUTHORIZED

(DS_License):
  Description:
  Count: 768
  Version: 1.0
  Status: AUTHORIZED

(WAN_License):
  Description:
  Count: 8
  Version: 1.0
  Status: OUT OF COMPLIANCE
```

- **show call-home profile all**：すべての設定済みプロファイルの Call Home プロファイル情報を表示します。

  次に、このコマンドの出力例を示します。

```
Router# show call-home profile all

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Profile mode: Full Reporting
    Reporting Data: Smart Call Home, Smart Licensing
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: http
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

   Periodic configuration info message is scheduled every 25 day of the month at 10:03


    Periodic inventory info message is scheduled every 25 day of the month at 09:48

    Alert-group               Severity
    ------------------------  ------------
    crash                     debug
    diagnostic                minor
    environment               minor
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major
```

- **show call-home smart-licensing statistics**：Call Home のスマート ライセンシング統計情報を表示します。

  次に、このコマンドの出力例を示します。

```
Router# show call-home smart-licensing statistics

Success: Successfully sent and response received.
Failed : Failed to send or response indicated error occurred.
Inqueue: In queue waiting to be sent.
Dropped: Dropped due to incorrect call-home configuration.

Msg Subtype      Success Failed  Inqueue Dropped Last-sent (GMT-06:00)
-------------------------------------------------------------------------
REGISTRATION     1       0       0       0       2015-03-13 13:12:13
ACKNOWLEDGEMENT  1       0       0       0       2015-03-13 13:12:20
ENTITLEMENT      5       0       0       0       2015-03-13 13:22:18
```

Cisco cBR ルータでの DOCSIS 3.1 ダウンストリーム ライセンスを確認するには、次のコマンドを使用します。

- **show cable license all | begin D3.1**：すべての DOCSIS 3.1 ダウンストリーム ライセンス情報を表示します。

  次に、このコマンドの出力例を示します。

```
Router# show cable license all | begin D3.1

Load for five secs: 21%/1%; one minute: 52%; five minutes: 52%
Time source is NTP, 10:41:11.175 PST Mon May 9 2016
-----------------------------------------
Entitlement:  DOCSIS 3.1 Downstream Channel License
Consumed count: 31
Consumed count reported to SmartAgent: 0
Enforced state: No Enforcement
```

Cisco cBR ルータでの DOCSIS 3.1 アップストリーム専用ライセンスを確認するには、次のコマンドを使用します。

- **• show cable licenses us_d31_exclusive**：DOCSIS 3.1 アップストリーム専用ライセンス情報を表示します。

  次に、このコマンドの出力例を示します。

```
Router# show cable licenses us_d31_exclusive
Load for five secs: 99%/2%; one minute: 21%; five minutes: 6%
Time source is NTP, *10:14:30.935 CST Tue Jun 6 2017

-----------------------------------------
Entitlement:  DOCSIS 3.1 Upstream Channel Exclusive License
Total Licensed Spectrum: 188000000Hz
Consumed count: 188
Consumed count reported to SmartAgent: 188
Enforced state: No Enforcement
```

シスコ スマート ライセンシングのトラブルシューティング

シスコ スマート ライセンシングのトラブルシューティングのために次のステップを実行する前に、顧客はまず設定が正しいことを確認し、スマート ライセンス用に設定した HTTP アドレスを ping できるかどうかを確認する必要があります。**show call-home smart-licensing statistics** コマンド出力に REGISTERED および ACKNOWLEDGE 情報が含まれるはずです。また、**show logging | include SMART | CALL** の出力も確認してください。

シスコ スマート ライセンシング登録の手動確認

ライセンス エージェントは、シスコへの登録情報を 30 日ごとに自動的に更新します。ライセンスがコンプライアンスに違反し、すぐに登録する必要がある場合は、登録を手動で更新する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**license smart renew** 例： `Router# license smart renew`	シスコへのデバイス インスタンスのライセンス登録を手動で更新します。

シスコ スマート ライセンシングからのルータの登録解除

シスコ スマート ライセンシングからルータの登録を解除することができます。ルータの返品許可（RMA）を行う際にルータの登録解除の必要がある場合があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**license smart deregister** 例： `Router# license smart deregister`	デバイス インスタンスのシスコ スマート ライセンシング登録を削除します。シスコ スマート ライセンシングのすべての証明書と権限が削除されます。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
シスコ スマート ライセンシング	『Cisco Smart Software Licensing』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

シスコ スマート ライセンシングに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *2*：シスコ スマート ライセンシングに関する機能情報

機能名	リリース	機能情報
シスコ スマート ライセンシング	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

機能名	リリース	機能情報
DOCSIS 3.1 US チャネル ライセンス	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 3 章

上限付きライセンス適用機能

このドキュメントでは、上限付きライセンス機能と、この機能を Cisco cBR シリーズ ルータで設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *3* : ***Cisco cBR*** シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

上限付きライセンス サポートについて

上限付きライセンス適用機能を使用すると、Cisco cBR-8 のそれぞれのライセンス付き機能の数に上限を設定できます。したがって、この機能を使用することにより、ライセンス付き機能が無制限に使用されたり、より多くのリソースが誤って使用されたりしないように管理状態が維持されます。また、ユーザはデバイスごとの使用状況を追跡し、リソースの使用を前もって管理することもできます。

適用する上限のいずれかが現在の使用数を下回っている場合、条件付きライセンス オプションを適用することはできません。

上限の適用が既に有効になっている場合、ユーザはその上限を超えるリソースにはアクセスできません。使用されている機能ライセンスの数は、上限と等しいか、それより少なくなる必要があります。

スマート ライセンス機能はレポート モデルであるため、ライセンスの適用が推奨されていません。したがって、上限付きライセンス適用機能がデフォルトで無効にされていて、すべての顧客に公表されるわけではありません。

SNMP MIB ベースの上限適用

機能に関する上限を設定して上限適用機能を有効にするには、SNMP set コマンドを使用します。SNMP set コマンドは、すべての機能に関する上限適用カウントが現在の使用数以上である場合にのみ、正常に処理されます。いずれかの機能の使用数が上限を超えている場合は、SET コマンドを発行する前に、それらのリソースをシャットダウンしてリソース使用数が上限以下になるようにしてください。

プラットフォームでこれらの値をスタンバイ RP と同期した後、上限適用機能が有効になります。これにより、ユーザが CAP 値を超えて使用数を増やそうとすると、リソースがブロックされて警告メッセージが表示されます。

SUP の返品許可（RMA）期間中、および SUP がシャーシ間で移動されるときには、保存済みの上限数と、上限適用機能を有効にする際に設定された値がクリアされます。ただし、スタンバイ RP を使用するシステムでは、スタンバイ RP が引き継いだ場合、RMA 中に新しい RP が接続されたときに値が同期されます。非冗長システムでは、RMA 後、または SUP がシャーシ間で移動されたときに、SNMP SET コマンドを再発行してください。

既に設定ロック状態になっている Cisco cBR-8 では、上限適用機能を有効にすることはできません。ただし、上限適用機能が有効になっているかどうかにかかわらず、Cisco cBR8 がライセンス サーバ と 90 日を超えて通信できない場合は、設定ロック状態になります。

機能に対して CAP 値を設定しない場合、値はデフォルトで 0xfff_ffff（268435455）に設定されます。

使用例のシナリオ

次の表は、SNMP MIB に基づく上限適用の使用例を示しています。

権限付与使用数が CAP（上限）カウント以下である場合	制限を設定し、追加のリソースをオンにできます。機能の使用数が CAP カウントに達すると、プラットフォームは追加使用を禁止します。
権限付与使用数が CAP カウントを超える場合	SNMP コマンドの実行を停止します。この状況とカウントの差異について通知するメッセージが表示されます。

次の表は、CAP の有効化と CAP カウント オプションを設定する必要が生じる条件を示しています。

シナリオ	非冗長 Cisco cBR	冗長 Cisco cBR
初回起動	はい	はい

シナリオ	非冗長 Cisco cBR	冗長 Cisco cBR
システム リロード	いいえ	いいえ
SSO	該当なし	非対応
SUP RMA	はい	いいえ
シャーシ間で SUP を移動	はい	いいえ

上限付きライセンス適用機能の設定方法

（注） この項で参照されているコマンドの詳細については、「Cisco IOS Master Command List」を参照してください。

この項の内容は、次のとおりです。

上限付きライセンス適用機能の設定

上限付きライセンス適用機能を設定するには、次の例に示すように SNMP コマンドを使用します。MIB 値を変更するには、Linux サーバから次のコマンドを実行します。

```
snmpget -v <snmp_version_information> -c <snmp_readonly_community>
   <cBR8_Server_IP>   <MIB_OID>
snmpset -v <snmp_version_information> -c <snmp_read_write_community>
   <cBR8_Server_IP>   <MIB_OID>  <object_type>  <value>
```

ライセンス使用数の表示

現在のコンフィギュレーションでのライセンス使用数を表示するには、次の例に示すように show cable license all コマンドを使用します。

```
Router-config# show cable license all
```

設定例

次の例は、SNMP バージョン 2c を使用するサーバ 172.25.15.210 上でコミュニティ プライベートを使用して **EnforcementEnabled** グローバル値を取得する方法を示しています。

```
$ snmpget -v 2c -c public 172.25.15.210 1.3.6.1.4.1.9.9.839.1.1.3.0
```

次の例は、SNMP バージョン 2c を使用するサーバ 172.25.15.210 上でコミュニティ プライベートを使用して **EnforcementEnabled** グローバル値を設定する方法を示しています。

```
$ snmpset -v 2c -c private 172.25.15.210 1.3.6.1.4.1.9.9.839.1.1.3.0 i 1
```

次の例は、DS ライセンス上限値を 999999 に設定する方法を示しています。

```
$ snmpset -v 2c -u private 123 172.25.15.210 1.3.6.1.4.1.9.9.839.1.1.4.1 u 999999
```

上限付きライセンス適用に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *4*：上限付きライセンス適用に関する機能情報

機能名	リリース	機能情報
上限付きライセンス適用機能	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に導入されました。

第 4 章

統合パッケージとサブパッケージの管理

このマニュアルでは、Cisco cBR シリーズ コンバージド ブロードバンド ルータでの統合パッケージとソフトウェア サブパッケージ（個別およびオプション）の動作および管理の方法について説明します。ここで説明する内容は、次のとおりです。

機能情報の確認

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

個別およびオプションのサブパッケージを使用した Cisco cBR シリーズ ルータの実行：概要

Cisco cBR シリーズ コンバージド ブロードバンド ルータは、個別のサブパッケージおよびオプションのサブパッケージを使用して稼働するように設定できます。

ルータが個別およびオプションのサブパッケージを使用して稼働するように設定されている場合:

- 統合パッケージ内の各個別サブパッケージが、固有ファイルとしてルータに抽出されます。
- また、オプションのサブパッケージはすべて個別にダウンロードし、抽出されたプロビジョニング ファイルや他の個別サブパッケージと同じディレクトリに保存する必要があります。
- 次に、ルータは、動作の処理に必要な場合に各ファイルにアクセスすることで実行されます。個別のサブパッケージを使用してルータが適切に動作するように、すべての個別のおよびオプションのサブパッケージ ファイルはルータの同じディレクトリに保存する必要があります。

個別のサブパッケージおよびオプションのサブパッケージを使用してルータを稼働する場合は、統合パッケージ内に個別のサブパッケージ ファイルとともに含まれているプロビジョニング ファイルを使用してルータをブートするように設定する必要があります。プロビジョニング ファイルも個別のサブ パッケージ ファイルおよびオプションのサブパッケージと同じディレクトリ内に格納する必要があります。ルータのブート速度は、統合パッケージで稼働するように設定されている場合よりも、個別のサブパッケージおよびオプションのサブパッケージで稼働するように設定されている方が高速です。

Cisco cBR シリーズ ルータは、Trivial File Transfer Protocol（TFTP）サーバまたはその他のネットワーク サーバに保存されている個別のサブパッケージおよびオプションのサブパッケージを実行するようには設定できません。ルータを稼働するこの方法を使用するには、個別のおよびオプションのサブパッケージをプロビジョニング ファイルとともに bootflash: ファイル システムにコピーします。

統合パッケージを使用した Cisco cBR シリーズ ルータの実行：概要

Cisco cBR シリーズ コンバージド ブロードバンド ルータは、統合パッケージを使用して稼働するように設定できます。

（注） 統合パッケージからルータをブートする場合、オプションのサブパッケージはサポートされません。

ルータで統合パッケージでの実行が設定されている場合は、統合パッケージ ファイル全体がルータにコピーされるか、または TFTP またはその他のネットワーク転送方式でルータからアクセスされます。ルータは、統合パッケージ ファイルを使用して稼働します。

統合パッケージを使用して稼働するように設定されたルータは、統合パッケージ ファイルをブートすることで、起動します。このファイルは容量が大きいため、統合パッケージを使用して稼働するルータのブートプロセスは、個別のサブパッケージで稼働するルータのブートプロセスより低速になります。

統合パッケージで稼働するように設定されたルータには、個別のサブパッケージで稼働するよう設定されたルータと比べて、いくつかの利点もあります。その利点の 1 つとして、統合パッケージが TFTP またはその他のネットワーク転送方式を使用してブートおよび利用できる点が挙げられます。また、1 つの統合パッケージ ファイルを使用するようにルータを設定する方が、複数の個別のサブパッケージ ファイルを管理するよりも簡単です。特定のネットワーキング環境でルータを実行する場合は、統合パッケージを使用した方が望ましい方法です。

この方式を使用してルータを実行する場合は、統合パッケージを bootflash:、usb[0-1]:、またはリモート ファイル システムに保存する必要があります。

Cisco cBR シリーズ ルータの実行：概要

個別のサブパッケージを使用してルータを実行する場合は、次の利点があります。

- ルータは、個別のサブパッケージのブート アプローチを使用して起動すると、最も早く起動します。
- 完全な統合イメージではなく、個別のサブパッケージをアップグレードすることができます。

統合パッケージを使用してルータを実行する場合は、次の利点があります。

- インストールを簡素化：複数の個別のイメージではなく、1 つのソフトウェア ファイルだけが管理されます。
- ストレージ：統合パッケージは個別のサブパッケージとは異なり、bootflash:、USB フラッシュ ディスク、ネットワーク サーバのいずれかに保存した状態でルータを実行できます。統合パッケージは TFTP またはその他のネットワーク転送方式でブートして使用することができますが、個別のサブパッケージ方式では、個々のサブパッケージをルータの bootflash: ファイル ディレクトリにコピーする必要があります。

実現方法	利点	欠点
個別のおよびオプションのサブパッケージ （注） システムでオプションのサブパッケージをインストールする必要がある場合は、この方法を使用する必要があります。	ブート時間が短縮されます。	• 複数のソフトウェア サブパッケージは管理が困難です。 • TFTP サーバまたはその他のネットワーク サーバからはブートできません。個別のサブパッケージのブート方式を使用する場合、各個別サブパッケージ ファイルは、bootflash: ディレクトリにあることが必要です。 • 個別のおよびオプションのサブパッケージ ファイルとプロビジョニング ファイルは、bootflash: に保存する必要があります。
統合パッケージ	• 管理が簡素化されます。多数のファイルではなく、1つのファイルだけが管理されます。 • 統合パッケージ ファイルを bootflash:、任意の TFTP サーバやその他のネットワーク サーバのいずれかに保存できます。	大きなイメージを常時処理する必要があるため、ブートに時間がかかり、最大システム スケーラビリティが低下します。

コマンド セットを使用したソフトウェア ファイルの管理

Cisco cBR シリーズ コンバージド ブロードバンド ルータで、次の個別のコマンド セットを使用してソフトウェア ファイルを管理できます。

request platform コマンド セット

request platform software package コマンドは、 Cisco cBR シリーズ コンバージド ブロードバンド ルータに導入されている request platform コマンド セットの一部です。

request platform software package コマンドは、個別のサブパッケージおよび統合パッケージ全体をアップグレードする場合に使用でき、 Cisco cBR シリーズ コンバージド ブロードバンド ルータ上のソフトウェアのアップグレードに使用されます。**request platform software package** コマンドは、特に個別のサブパッケージをアップグレードする場合に推奨されます。また、ルータが個別のサブパッケージを実行している場合、ルータ上の個別のサブパッケージをダウンタイムなしでアップグレードできる唯一の方法でもあります。

request platform software package コマンドを使用する場合は、コマンド ラインで宛先デバイスまたはプロセスを指定する必要があるので、このコマンドを使用すると、アクティブまたはスタンバイ プロセッサの両方でソフトウェアをアップグレードできます。

コマンド構文

request platform software package install rp *rp-slot-number***file** *file-URL*

値は次のとおりです。

- *rp-slot-number* は RP スロットの数、
- *file-URL* はルータのアップグレードに使用するファイルのパスです。

copy コマンド

copy コマンドを使用すると、ルータに統合パッケージおよび個別のサブパッケージを移動できます。ただし、このコマンドにより特定のストレージから別のストレージに個別のサブパッケージ ファイルを移動するのは、ほとんどの場合、非効率的です（このような場合は、統合パッケージを移動してからサブパッケージを抽出するか、統合パッケージを移動せずにサブパッケージを抽出する方法を推奨します）。

Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の統合パッケージをアップグレードするには、他のほとんどの Cisco ルータの場合と同じように、**copy** コマンドを使用して統合パッケージをファイル システム（通常は bootflash）にコピーします。このコピーを行ってから、統合パッケージ ファイルを使用してブートするようにルータを設定します。

個別のサブパッケージを使用してルータをアップグレードし、リブートするには、**copy** コマンドを使用して統合パッケージをルータにコピーし、 **request platform software package expand** コマンドを入力して個別のサブパッケージを抽出してから、サブパッケージを使ってブートするようにルータを設定します。同一の統合パッケージ内のそれぞれ個別のサブパッケージをディレクトリからコピーしたり、request platform software package コマンドを使用してルータのディレクトリにサブパッケージを抽出したりするなど、他の方式も使用できますが、個別のサブパッケージをコピーすることは、ほとんどの場合、非効率的です。

統合パッケージおよび個別のサブパッケージを使用したルータの管理および設定

このセクションでは、ルータ上のパッケージ、サブパッケージ、パッチを管理および設定するために使用する方法を説明します。

ケーブル ラインカードのプロセス リスタート

パッケージやサブパッケージをアップグレードして管理する方法では多くの場合、最後の手順として、ソフトウェアの設定またはアップグレード先のルータまたはコンポーネントをリロードします。ルータまたはコンポーネントのリロードには、次のデメリットがあります。

- サービスが停止する（制限される）
- モデムのコンフィギュレーション データが失われる
- ラインカードや他のコンポーネントのリブートに時間がかかる

N+1 ライン カード高可用性（LCHA）システムでは、ラインカードでパッケージをアップグレードすると常に、アクティブおよびスタンバイ ラインカードが再起動します。これは、ラインカードの現場交換可能ユニット（FRU）用サブパッケージのアップグレードの場合も同じです。パッケージまたはサブパッケージをアップグレードしたときは常に、ラインカードを再起動する必要があります。N 個のアクティブ ラインカードでパッケージ アップグレードを行った場合、合計で 2xN の再起動を行うことになります。これには多くの時間がかかり、ラインカードの再起動時にサービスが影響を受ける可能性があります。

ルータおよびラインカードのリロードのデメリットを避けるため、RF ラインカードでパッケージをアップグレードする場合は、ケーブル ラインカードのプロセス リスタート機能を使用してください。

（注） プロセス リスタート機能は、RF ライン カードへパッケージをアップグレードまたはインストールして使用してください。

ケーブル ラインカードのプロセスをリスタートする機能として、主に次の 2 つの機能があります。

- ケーブル ライン カードのコントロール プレーン プロセス リスタート
- ケーブル ライン カードのアップストリーム スケジューラ プロセス リスタート

ケーブル ライン カードのコントロール プレーン プロセス リスタート

ケーブル ライン カードのコントロール プレーン プロセス リスタート機能には次のメリットがあります。

- パッケージのアップグレードが簡略化され、アクティブおよびスタンバイ ラインカードの LCHA ベースの再起動が不要です。
- サービスを中断せずに特定のプロセスを再起動します。
- IOSdプロセスの再起動後、モデムのコンフィギュレーションデータはすべて回復されます。
- IOSd プロセスの再起動中のモデムのコンフィギュレーション データの変更は、IOSd プロセスが再起動した後に調整されます。

- セカンダリ ライン カードのシャットダウンおよび非シャットダウン プロセスは、自動的に実行されます。

制約事項

- ケーブル ライン カードのコントロール プレーン プロセス再起動機能を使用してラインカード IOS をアップグレードするには、サブパッケージに cbrsup-clcios および cbrsup-clciosdb に関するパッチが必要です。
- IOSd および US スケジューラの再起動がサポートされています。IOSd のみを再起動する（IOSd/IOSdb パッケージが必要）ことも、US スケジューラのみを再起動する（clc-docsis パッケージが必要）こともできます。また、単一のコマンドで両方を再起動することもでき、その場合、US スケジューラが最初に再起動し、その後、IOSd が再起動します。この場合、IOSd/IOSdb および clc-docsis パッケージが必要となります。

その他の制約事項は、次のとおりです。

- IOSd プロセスは、プライマリ アクティブ RF ラインカードでのみ再起動できます。
- IOSd プロセスを再起動する前にセカンダリ RF ライン カードをシャットダウンする必要があります。
- 二重障害（つまり IOSd と 1 つ以上のプロセスの同時停止）が発生した場合、IOSd プロセスの再起動は機能しません。二重障害の結果、ラインカードのリロードが発生します。
- 現行の IOSd プロセスが完全に回復するまで、次の IOSd（次の RF ラインカード上の IOSd）は実行されません。

ケーブル ライン カードのコントロール プレーン プロセス リスタート機能は、次の再起動オプションを提供します。

- 特定のスロットを再起動するには、**slot** *slot number* オプションを指定した **request platform software process restart** コマンドを使用します。
- 特定のスロットを指定せずにすべてのライン カードを再起動するには、**slot** *slot number* オプションを指定せずに **request platform software process restart** コマンドを使用します。
- すべてのライン カードを間隔ベースで再起動するには、**interval** *secs* オプションを指定した **request platform software process restart** コマンドを使用します。

覚えておく必要のある重要なポイント

- ケーブル ライン カードのコントロール プレーン プロセス再起動機能を使用する前に、**hw-module slot shutdown** コマンドを使用してセカンダリ ライン カードをシャットダウンしてください。
- ケーブル ラインカードのコントロール プレーン プロセス再起動機能が開始すると、セカンダリ ライン カードが自動的にシャットダウンします。
- ケーブル ライン カードのコントロール プレーン プロセス再起動機能を使用する前に、**hw-module slot shutdown** コマンドを使用してセカンダリ ライン カードをシャットダウンしてください。

- ケーブル ライン カードのコントロール プレーン プロセス再起動機能が開始すると、セカンダリ ライン カードが自動的にシャットダウンします。
- サブパッケージのアップグレード後にライン カードがリロードされないようにするには、**noreload linecard** オプションを指定した **request platform software package install node file** コマンドを使用します。
- 再起動プロセスを確認するには、**show platform software ios slot** *slot number***restart info** コマンドを使用します。

クラッシュ時の再起動

クラッシュの発生後は、ケーブル ライン カード コントロール プレーン プロセスおよびアップストリーム スケジューラ プロセスが自動的に再起動されます。プロセスが再起動されると、セカンダリ ライン カードがリセットされます。

制約事項

- クラッシュ時の再起動は、アクティブなプライマリ ライン カードでのみサポートされます。

次の表に、さまざまなルールごとのクラッシュ発生時のケーブル ライン カードの動作を記載します。

表 *5*: ケーブル ライン カード プロセス再起動ポリシー マトリックス

	セカンダリ ケーブル ライン カードの有無	クラッシュ時	セカンダリ ケーブル ライン カードの状態
LCHA または LCPR	あり	ケーブル ライン カードをリセット	スイッチオーバー後、アクティブ
プロセス再起動が有効	なし	再起動	該当なし
LCHA または LCPR	あり	ケーブル ライン カードをリセット	スイッチオーバー後、アクティブ
プロセス再起動が無効	なし	ケーブル ライン カードをリセット	該当なし
優先 LCHA なし、LCPR なし	あり	プロセス再起動	プライマリ ケーブル ライン カードでプロセスが再起動した後、セカンダリ ケーブル ライン カードをリセット
プロセス再起動が有効	なし	プロセス再起動	該当なし
優先 LCHA なし、LCPR なし	あり	ケーブル ライン カードをリセット	スイッチオーバー後、アクティブ

	セカンダリ ケーブル ライン カードの有無	クラッシュ時	セカンダリ ケーブル ライン カードの状態
プロセス再起動が無効	なし	ケーブル ライン カードをリセット	該当なし

（注）

- 手動プロセス再起動は、設定されているポリシーに依存せず、セカンダリ ケーブル ライン カード（存在する場合）を停止/停止解除します。
- 「LCHA 優先」と「プロセス再起動が有効」がデフォルトです。disable-auto-restart および lcha-preferred コマンドを使用して、この 2 つのパラメータを設定できます。詳細については、http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html を参照してください。
- コントロール プレーン プロセス再起動とアップストリーム スケジューラ プロセス再起動の動作は同じです。
- スタンバイ モードのセカンダリ ケーブル ライン カードは、存在すると見なされます。

ケーブル ライン カード プロセス再起動機能に追加された再起動再試行制限機能は、クラッシュ時の再起動にのみ適用されます。この機能を使用すると、再起動再試行回数の制限を設定できます。この制限内でプロセスの再起動が成功しなければ、ライン カードはリロードされます。この機能により、再起動が失敗したときにライン カードがいつまでも再起動されるのを回避できます。

ケーブル ライン カードのコントロール プレーン プロセス リスタート機能の使用

ケーブル ライン カードのコントロール プレーン プロセス リスタート機能を使用するには、コマンドを使用して RF ライン カード サブパッケージ アップグレードをインストールします。

手順

ステップ 1 **request platform software package install node file noreload linecard** コマンドを使用して RF ライン カード サブパッケージ アップグレードをインストールします。

```
Router#request platform software package install node file bootflash:sp/cbr_patch.9.0.tar
noreload linecard
```

ステップ 2 すべてのケーブル ライン カードの RF ライン カード IOSd プロセスを順番に再起動するには、**request platform software process restart** コマンドを使用します。

```
Router# request platform software process restart
```

ステップ 3 特定のケーブル ライン カードの RF ライン カード IOSd プロセスを再起動するには、**request platform software process restart slot** *slot#* コマンドを使用します。

```
Router# request platform software process restart slot 7
```

ケーブル ライン カードのコントロール プレーン プロセス リスタート再試行制限の設定

ケーブル ライン カードのコントロール プレーン プロセス リスタートの再試行制限を設定するには、次の手順に従います。

enable
configure terminal
process-restart
lc-control-plane-timeout *time*
restart-retry *retry-times*
exit

ケーブル ライン カードのコントロール プレーン プロセス リスタート機能の例

ここでは、ケーブル ライン カードのコントロール プレーン プロセスで使用されるコマンドの出力例を示します。

この例には、サブパッケージ アップグレードをインストールする **noreload linecard** オプションを指定した **request platform software package install node file** コマンドの出力が示されています。

```
Router# request platform software package install node file bootflash:sp/cbr_patch.9.0.tar
noreload linecard
Image file expanded and copied
Expanding image file: stby-bootflash:sp/cbr_patch.9.0.tar
Image file expanded and copied
Finished image file expansion
Found clc package
STAGE 1: Installing software on standby RP
==========================================
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0
--- Starting installation state synchronization ---
Finished installation state synchronization
--- Starting local lock acquisition on R1 ---
Finished local lock acquisition on R1
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
Found cbrsup-clcios.2015-03-23_17.53_haolin2.SSA.pkg
Found cbrsup-clciosdb.2015-03-23_17.53_haolin2.SSA.pkg
Verifying image file locations
Inspecting image file types
Processing image file constraints
Creating candidate provisioning file
Finished image file verification
--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction
```

```
--- Starting ISSU compatibility verification ---
Verifying image type compatibility
Checking IPC compatibility with running software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking package specific compatibility
Finished ISSU compatibility verification
--- Starting list of software package changes ---
Old files list:
Removed cbrsup-clcios.2015-03-23_17.28_haolin2.SSA.pkg
Removed cbrsup-clciosdb.2015-03-23_17.28_haolin2.SSA.pkg
New files list:
Added cbrsup-clcios.2015-03-23_17.53_haolin2.SSA.pkg
Added cbrsup-clciosdb.2015-03-23_17.53_haolin2.SSA.pkg
Finished list of software package changes
--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
--- Starting analysis of software changes ---
Finished analysis of software changes
--- Starting update running software ---
Blocking peer synchronization of operating information
Creating the command set placeholder directory
Finding latest command set
Finding latest command shortlist lookup file
Finding latest command shortlist file
Assembling CLI output libraries
Assembling CLI input libraries
Assembling Dynamic configuration files
Applying interim IPC and database definitions
Replacing running software
Replacing CLI software
Restarting software
Restarting software: target frus filtered out ... skipped
Applying final IPC and database definitions
Generating software version information
Notifying running software of updates
Unblocking peer synchronization of operating information
Unmounting old packages
Cleaning temporary installation files
Finished update running software
SUCCESS: Finished installing software.
STAGE 2: Installing software on active RP
========================================
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0
--- Starting installation state synchronization ---
Finished installation state synchronization
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
Found cbrsup-clcios.2015-03-23_17.53_haolin2.SSA.pkg
Found cbrsup-clciosdb.2015-03-23_17.53_haolin2.SSA.pkg
Verifying image file locations
Inspecting image file types
Processing image file constraints
Creating candidate provisioning file
Finished image file verification
--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction
--- Starting ISSU compatibility verification ---
Verifying image type compatibility
```

```
Checking IPC compatibility with running software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking package specific compatibility
Finished ISSU compatibility verification
--- Starting impact testing ---
Checking operational impact of change
Finished impact testing
--- Starting list of software package changes ---
Old files list:
Removed cbrsup-clcios.2015-03-23_17.28_haolin2.SSA.pkg
Removed cbrsup-clciosdb.2015-03-23_17.28_haolin2.SSA.pkg
New files list:
Added cbrsup-clcios.2015-03-23_17.53_haolin2.SSA.pkg
Added cbrsup-clciosdb.2015-03-23_17.53_haolin2.SSA.pkg
Finished list of software package changes
--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
--- Starting analysis of software changes ---
Finished analysis of software changes
--- Starting update running software ---
Blocking peer synchronization of operating information
Creating the command set placeholder directory
Finding latest command set
Finding latest command shortlist lookup file
Finding latest command shortlist file
Assembling CLI output libraries
Assembling CLI input libraries
Assembling Dynamic configuration files
Applying interim IPC and database definitions
Replacing running software
Replacing CLI software
Restarting software
Restarting software: target frus filtered out ... skipped
Applying final IPC and database definitions
Generating software version information
Notifying running software of updates
Unblocking peer synchronization of operating information
Unmounting old packages
Cleaning temporary installation files
Finished update running software
SUCCESS: Finished installing software.
Found clc package
SUCCESS: node ISSU finished successfully.
Invoking cleanup routine
```

次に、**show platform software ios restart info** コマンドの出力例を示します。

```
Router#show platform software ios 6 restart info
IOSD process restart info:
Process restartable: Yes
IOSD restart state : ACTIVE
Total Modem Count : 31
Active Modem Count : 31
```

次に、 **request platform software process restart** コマンドの出力例を示します。

```
Router# request platform software process restart
--- Upgrading/Restarting LineCard-2 Packages/Processes ---
NOTICE: No upgrades available.
Provide process name in cli if you wish to restart a process
--- Upgrading/Restarting LineCard-3 Packages/Processes ---
Available upgrades
cbrsup-clcios.2015-03-23_17.53_haolin2.SSA.pkg
cbrsup-clciosdb.2015-03-23_17.53_haolin2.SSA.pkg
```

```
--- Checking for ready state before IOSD upgrade on LineCard-3
Updating Package cbrsup-clcios.2015-03-23_17.28_haolin2.SSA.pkg
---> cbrsup-clcios.2015-03-23_17.53_haolin2.SSA.pkg
Restarting ubrclc_k9lc_ms
--- Checking for ready state before IOSDB upgrade on LineCard-3
Updating Package cbrsup-clciosdb.2015-03-23_17.28_haolin2.SSA.pkg
---> cbrsup-clciosdb.2015-03-23_17.53_haolin2.SSA.pkg
Restarting iosdb
SUCCESS: Finished


Router#show platform software patch 2 info
cbrsup-clciosdb: 3.17.0 (3.0)
cbrsup-clc-firmware: 3.17.0 (0.0)
cbrsup-clcvideo: 3.17.0 (0.0)
cbrsup-clcios: 3.17.0 (3.0)
cbrsup-clccontrol: 3.17.0 (0.0)
cbrsup-clcdocsis: 3.17.0 (0.0)
```

ケーブル ライン カードのアップストリーム スケジューラ プロセス リスタート

RF ラインカードのアップストリーム スケジューラ プロセスを再起動するには、ケーブル ライン カードのアップストリーム スケジューラ プロセス リスタート機能を使用します。

ケーブルラインカードのアップストリームスケジューラプロセスリスタート機能には次のメリットがあります。

- アップストリーム トラフィックへの影響を最小限にし、ダウンストリーム トラフィックには影響を与えずに、ラインカードの US スケジューラ（CDMAN）プロセスを再起動することができます。
- すべてのモデム設定データが、再起動前の状態に回復しました。
- 再起動中のモデムのコンフィギュレーション データの変更が調整されます。
- 再起動中、オンラインになった新しいモデムはブロックされます。
- ライン カードをリロードせずに新しい DOCSIS サブパッケージ パッチをアップグレードするには、**request platform software package restart** コマンドを使用します。
- Cisco IOS-XE リリース 3.18.0S 以降、クラッシュ後にライン カードが自動的に再起動します。詳細については、クラッシュ時の再起動, （76 ページ）の項を参照してください。

制約事項

この機能には、次の制約事項が適用されます。

- アップストリーム スケジューラ プロセスは、プライマリ アクティブ RF ラインカードでのみ再起動できます。
- 二重障害（つまりアップストリーム スケジューラと 1 つ以上のプロセスの同時停止）が発生した場合、アップストリーム スケジューラ プロセスの再起動は機能しません。二重障害の結果、ラインカードのリロードが発生します。
- 現行のアップストリーム スケジューラ プロセスが完全に回復するまで、次のアップストリーム スケジューラ（次の RF ラインカード上のアップストリーム スケジューラ）は実行されません。

覚えておく必要のある重要なポイント

- Cisco IOS-XE リリース 3.17.0S では、ケーブル ラインカードのアップストリーム スケジューラ プロセス リスタート機能が開始すると、セカンダリ ラインカードは自動的にシャットダウンします。
- サブパッケージのアップグレード後にライン カードがリロードされないようにするには、**noreload linecard** オプションを指定した **request platform software package install node file** コマンドを使用します。
- 再起動プロセスを確認するには、**show platform software us-schedulerrestart info** コマンドを使用します。

```
Router# show platform software us-scheduler 3 restart info
us-scheduler process restart info:
Process restartable : Yes
us-scheduler state : RESTART_OPERATIONAL
Features bit map : 0x001e
us-scheduler restart count : 4
```

ケーブル ライン カードのアップストリーム スケジューラ プロセス リスタート機能の使用

ケーブル ライン カードのアップストリーム スケジューラ プロセス リスタート機能を使用するには、コマンドを使用して RF ライン カード サブパッケージ アップグレードをインストールします。

手順

ステップ 1 **request platform software package install node file noreload linecard** コマンドを使用して RF ライン カード サブパッケージ アップグレードをインストールします。

```
Router#request platform software package install node file bootflash:sp/cbr_patch.9.0.tar
noreload linecard
```

ステップ 2 すべてのケーブル ライン カードのアップストリーム スケジューラ プロセスを順番に再起動するには、**request platform software process restart** コマンドを使用します。

```
Router# request platform software process restart
```

ステップ 3 特定のケーブル ライン カードでアップストリーム スケジューラ プロセスを再起動するには、**request platform software process restart slot** *slot#* コマンドを使用します。

```
Router# request platform software process restart slot 7
```

ケーブル ライン カードのコントロール プレーン プロセス リスタート再試行制限の設定

ケーブル ライン カードのコントロール プレーン プロセス リスタートの再試行制限を設定するには、次の手順に従います。

enable
configure terminal
process-restart
lc-us-scheduler-timeout *time*
restart-retry *retry-times*
exit

ケーブル ライン カードのアップストリーム スケジューラ プロセス リスタート機能の例

ここでは、ケーブル ライン カードのアップストリーム スケジューラ プロセス リスタート機能で使用されるコマンドの出力例を示します。

この例には、**show platform software us-scheduler restart info** コマンドの出力が示されています。

```
Router#show platform software us-scheduler 6 restart info
us-scheduler process restart info:
Process restartable : Yes
us-scheduler state : RESTART_OPERATIONAL
Features bit map : 0x001e
us-scheduler restart count : 1
```

ここでは、アップストリームスケジューラプロセスをリスタートした場合の出力例を示します。

```
Router# request platform software package install node file
bootflash:subpkg/cbr_patch-3.17.0-patch2.tar noreload linecard
NOTE: Currently node has booted from a provisioning file
NOTE: Going to start a dual rp sub-packages node ISSU install
--- Starting initial file path checking --- Copying
bootflash:subpkg/cbr_patch-3.17.0-patch2.tar to
stby-bootflash:subpkg/cbr_patch-3.17.0-patch2.tar
Finished initial file path checking
--- Starting config-register verification --- Finished config-register verification
--- Starting Checking noreload options --- Finished Checking noreload options
--- Starting image file expansion ---
Expanding image file: bootflash:subpkg/cbr_patch-3.17.0-patch2.tar
Image file expanded and copied
Expanding image file: stby-bootflash:subpkg/cbr_patch-3.17.0-patch2.tar
Image file expanded and copied
Finished image file expansion
Found clc package
STAGE 1: Installing software on standby RP ========================================
--- Starting local lock acquisition on R0 --- Finished local lock acquisition on R0
--- Starting installation state synchronization --- Finished installation state
synchronization
--- Starting local lock acquisition on R1 --- Finished local lock acquisition on R1
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification --- Checking image file names Locating image files and
validating name syntax
Found cbrsup-clcdocsis.2015-10-08_18.10_haolin2.SSA.pkg
Verifying image file locations
Inspecting image file types
Processing image file constraints
Creating candidate provisioning file
Finished image file verification
--- Starting candidate package set construction --- Verifying existing software set Processing
candidate provisioning file Constructing working set for
candidate package set Constructing working set for running package set Checking command
output Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete Finished candidate package
```

```
set construction
--- Starting ISSU compatibility verification ---
WARNING:
WARNING: ISSU between engineering builds with release strings in non-standard fo rmat.
Skipping ISSU Software Compatibility checks.
WARNING:
WARNING:
WARNING: ISSU between engineering builds with release strings in non-standard fo rmat.
Skipping ISSU Software Compatibility checks.
WARNING:
WARNING:
WARNING: ISSU between engineering builds with release strings in non-standard fo rmat.
Skipping ISSU Software Compatibility checks.
WARNING:
WARNING:
WARNING: ISSU between engineering builds with release strings in non-standard fo rmat.
Skipping ISSU Software Compatibility checks.
WARNING:
Verifying image type compatibility
Checking IPC compatibility with running software Checking candidate package set infrastructure
compatibility Checking infrastructure compatibility with running
software Checking package specific compatibility Finished ISSU compatibility verification
--- Starting list of software package changes --- Old files list:
Removed cbrsup-clcdocsis.BLD_MCP_DEV_LATEST_20151006_133623.SSA.pkg
New files list:
Added cbrsup-clcdocsis.2015-10-08_18.10_haolin2.SSA.pkg
Finished list of software package changes
--- Starting commit of software changes --- Updating provisioning rollback files Creating
pending provisioning file Committing provisioning file Finished
commit of software changes
--- Starting analysis of software changes --- Finished analysis of software changes
--- Starting update running software --- Blocking peer synchronization of operating
information Creating the command set placeholder directory
Finding latest command set
Finding latest command shortlist lookup file
Finding latest command shortlist file
Assembling CLI output libraries
Assembling CLI input libraries
Assembling Dynamic configuration files
Applying interim IPC and database definitions
Replacing running software
Replacing CLI software
Restarting software
Restarting software: target frus filtered out ... skipped
Applying final IPC and database definitions
Generating software version information
Notifying running software of updates
Unblocking peer synchronization of operating information Unmounting old packages Cleaning
temporary installation files
Finished update running software
SUCCESS: Finished installing software.
STAGE 2: Installing software on active RP ========================================
--- Starting local lock acquisition on R0 --- Finished local lock acquisition on R0
--- Starting installation state synchronization --- Finished installation state
synchronization
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification --- Checking image file names Locating image files and
validating name syntax
Found cbrsup-clcdocsis.2015-10-08_18.10_haolin2.SSA.pkg
Verifying image file locations
Inspecting image file types
Processing image file constraints
Creating candidate provisioning file
Finished image file verification
--- Starting candidate package set construction --- Verifying existing software set Processing
candidate provisioning file Constructing working set for candidate
package set Constructing working set for running package set Checking command output
Constructing merge of running and candidate packages Checking if resulting
candidate package set would be complete Finished candidate package set construction
--- Starting ISSU compatibility verification ---
WARNING:
WARNING: ISSU between engineering builds with release strings in non-standard fo rmat.
```

```
Skipping ISSU Software Compatibility checks.
WARNING:
WARNING:
WARNING: ISSU between engineering builds with release strings in non-standard fo rmat.
Skipping ISSU Software Compatibility checks.
WARNING:
WARNING:
WARNING: ISSU between engineering builds with release strings in non-standard fo rmat.
Skipping ISSU Software Compatibility checks.
WARNING:
WARNING:
WARNING: ISSU between engineering builds with release strings in non-standard fo rmat.
Skipping ISSU Software Compatibility checks.
WARNING:
Verifying image type compatibility
Checking IPC compatibility with running software Checking candidate package set infrastructure
compatibility Checking infrastructure compatibility with running
software Checking package specific compatibility Finished ISSU compatibility verification
--- Starting impact testing ---
Checking operational impact of change
Finished impact testing
--- Starting list of software package changes --- Old files list:
Removed cbrsup-clcdocsis.BLD_MCP_DEV_LATEST_20151006_133623.SSA.pkg
New files list:
Added cbrsup-clcdocsis.2015-10-08_18.10_haolin2.SSA.pkg
Finished list of software package changes
--- Starting commit of software changes --- Updating provisioning rollback files Creating
pending provisioning file Committing provisioning file Finished
commit of software changes
--- Starting analysis of software changes --- Finished analysis of software changes
--- Starting update running software --- Blocking peer synchronization of operating
information Creating the command set placeholder directory
Finding latest command set
Finding latest command shortlist lookup file
Finding latest command shortlist file
Assembling CLI output libraries
Assembling CLI input libraries
Assembling Dynamic configuration files
Applying interim IPC and database definitions
Replacing running software
Replacing CLI software
Restarting software
Restarting software: target frus filtered out ... skipped
Applying final IPC and database definitions
Generating software version information
Notifying running software of updates
Unblocking peer synchronization of operating information Unmounting old packages Cleaning
temporary installation files
Finished update running software
SUCCESS: Finished installing software.
Found clc package
SUCCESS: node ISSU finished successfully.
Invoking cleanup routine
Router#

Router#show platform software us-scheduler 2 restart info
us-scheduler process restart info:
Process restartable : Yes
us-scheduler state : RESTART_OPERATIONAL
Features bit map : 0x001e
us-scheduler restart count : 1

Router#request platform software process restart slot 2
--- Upgrading/Restarting LineCard-2 Packages/Processes ---
Available upgrades
cbrsup-clcdocsis.BLD_MCP_DEV_LATEST_20151006_13362
Updating Package cbrsup-clcdocsis.BLD_MCP_DEV_LATEST_20151006_13362
---> cbrsup-clcdocsis.2015-10-08_18.10_haolin2.SSA.pkg
Restarting us-scheduler
SUCCESS: Finished upgrading the LineCard-2

Router#show platform software patch 2 info
cbrsup-clciosdb: 3.17.0 (0.0)
```

```
cbrsup-clc-firmware: 3.17.0 (0.0)
cbrsup-clcvideo: 3.17.0 (0.0)
cbrsup-clcios: 3.17.0 (0.0)
cbrsup-clccontrol: 3.17.0 (0.0)
cbrsup-clcdocsis: 3.17.0 (2.0)
```

（注） アップグレード パッケージに IOSD-CLC と US スケジューラ サブパッケージの両方が含まれる場合、**request platform software process restart** コマンドにより、まずケーブル ライン カードのアップストリーム スケジューラ プロセスがリスタート（再起動）し、次にケーブル ライン カードのコントロール プレーン プロセスがリスタートします。

ここでは、コントロール プレーンおよびアップストリーム スケジューラ プロセスがリスタートする場合の **request platform software process restart** コマンドの出力例を示します。

（注） キーワード**slot**を使用しない場合は、すべてのライン カード上のアップストリーム スケジューラ プロセスが順番にリスタートします。

```
Router#request platform software process restart


--- Upgrading/Restarting LineCard-1 Packages/Processes ---

    Available upgrades
        cbrsup-clcdocsis.2015-09-24_03.09_johuynh.SSA.pkg
        cbrsup-clcios.2015-09-24_03.09_johuynh.SSA.pkg
        cbrsup-clciosdb.2015-09-24_03.09_johuynh.SSA.pkg

    Updating Package  cbrsup-clcdocsis.2015-09-24_03.09_johuynh.SSA.pkg
                ---> cbrsup-clcdocsis.2015-09-24_19.04_haolin2.SSA.pkg
    Restarting us-scheduler
--- Checking for ready state before IOSD upgrade on LineCard-1
    Updating Package  cbrsup-clcios.2015-09-24_03.09_johuynh.SSA.pkg
                ---> cbrsup-clcios.2015-09-24_19.04_haolin2.SSA.pkg
    Restarting ubrclc_k9lc_ms
--- Checking for ready state before IOSDB upgrade on LineCard-1
    Updating Package  cbrsup-clciosdb.2015-09-24_03.09_johuynh.SSA.pkg
                ---> cbrsup-clciosdb.2015-09-24_19.04_haolin2.SSA.pkg
    Restarting iosdb

    SUCCESS: Finished upgrading the LineCard-1


--- Upgrading/Restarting LineCard-2 Packages/Processes ---

    Available upgrades
        cbrsup-clcdocsis.2015-09-24_03.09_johuynh.SSA.pkg
        cbrsup-clcios.2015-09-24_03.09_johuynh.SSA.pkg
        cbrsup-clciosdb.2015-09-24_03.09_johuynh.SSA.pkg

    Updating Package  cbrsup-clcdocsis.2015-09-24_03.09_johuynh.SSA.pkg
                ---> cbrsup-clcdocsis.2015-09-24_19.04_haolin2.SSA.pkg
    Restarting us-scheduler
--- Checking for ready state before IOSD upgrade on LineCard-2
    Updating Package  cbrsup-clcios.2015-09-24_03.09_johuynh.SSA.pkg
                ---> cbrsup-clcios.2015-09-24_19.04_haolin2.SSA.pkg
    Restarting ubrclc_k9lc_ms
--- Checking for ready state before IOSDB upgrade on LineCard-2
    Updating Package  cbrsup-clciosdb.2015-09-24_03.09_johuynh.SSA.pkg
                ---> cbrsup-clciosdb.2015-09-24_19.04_haolin2.SSA.pkg
    Restarting iosdb

    SUCCESS: Finished upgrading the LineCard-2
```

```
Router#
```

キーワード **interval** を使用すると、シーケンス内の 2 つのライン カード プロセスのリスタート間隔を秒単位で指定できます。デフォルトの間隔は 5 秒です。

この例では、間隔を 6 秒に設定しています。

```
Router#request platform software process restart interval 6
```

クイック スタート ソフトウェア アップグレード

次の手順では、 Cisco cBR シリーズ コンバージド ブロードバンド ルータ を実行するソフトウェアを簡単にアップグレードするための方法について説明します。この手順は、ユーザが統合パッケージにアクセスできること、統合パッケージ ファイルを bootflash: ファイル システムに保存すること、bootflash: ファイル システムに既存のサブパッケージまたは統合パッケージがないこと、および bootflash: ファイル システムにファイルを格納するための領域が十分にあることを前提とします。

手順

ステップ 1 **copy** *URL-to-image***bootflash:** コマンドを使用して、統合パッケージをブートフラッシュにコピーします。

ステップ 2 個別のサブパッケージを使用してルータを実行するには、**request platform software package expand file bootflash:**/*sub_dir*/*base_image* コマンドを使用します。統合パッケージを使用してルータを実行する場合は、この手順を省略します。

ステップ 3 **dir bootflash:** コマンドを入力して、統合パッケージまたは抽出したサブパッケージが bootflash: ディレクトリ内にあることを確認します。

ステップ 4 個別のサブパッケージを実行する場合は、**delete bootflash:***base_image* を使用して統合パッケージを削除します。統合パッケージを使用してルータを実行する場合は、この手順を省略します。

ステップ 5 ブート用のブート パラメータを設定します。**config-register 0x2102** グローバル コンフィギュレーション コマンドを入力してコンフィギュレーション レジスタを 0x2 に設定し、**boot system flash bootflash:***base_image*（統合パッケージを使って実行する場合）または **boot system flash bootflash:***provisionging-file-name*（個別のサブパッケージを使って実行する場合）グローバル コンフィギュレーション コマンドを入力します。

ステップ 6 **copy running-config startup-config** を入力して設定を保存します。

ステップ 7 **reload** コマンドを入力して、ルータをリロードし、ブートを終了します。リロード完了時には、アップグレードされたソフトウェアが実行されています。

copy コマンドを使用した統合パッケージの管理および設定

copy コマンドを使用して Cisco cBR シリーズ ルータ上の統合パッケージをアップグレードするには、他のほとんどのシスコ ルータの場合と同じように、**copy** コマンドを使用して統合パッケージをルータ上のファイル システム（通常は bootflash: ディレクトリ）にコピーします。このコピーを行ってから、統合パッケージ ファイルを使用してブートするようにルータを設定します。

次の例では、統合パッケージ ファイルを TFTP から bootflash: ファイル システムにコピーしています。さらに、**boot system** コマンドを使用してブートするようにコンフィギュレーション レジスタを設定し、**boot system** コマンドにより、bootflash: ファイル システムに保存されている統合パッケージを使用してブートするようルータに指示します。その後、新しい設定は **copy running-config startup-config** コマンドにより保存され、システムがリロードされてプロセスが終了します。

```
Router# dir bootflash:
Directory of bootflash:/

11 drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
86401 drwx 4096 Dec 4 2007 06:06:24 -08:00 .ssh
14401 drwx 4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
28801 drwx 4096 Mar 18 2008 17:31:17 -07:00 .prst_sync
43201 drwx 4096 Dec 4 2007 04:34:45 -08:00 .installer
13 -rw- 45977 Apr 9 2008 16:48:46 -07:00 target_support_output.tgz.tgz

928862208 bytes total (712273920 bytes free)

Router# copy tftp bootflash:
Address or name of remote host []? 172.17.16.81
Source filename []?
/auto/tftp-users/user/cbrsup-universal*.bin Destination filename [cbrsup-universal*.bin]?
Accessing
tftp://172.17.16.81//auto/tftp-users/user/ cbrsup-universal*.bin...

Loading /auto/tftp-users/user/cbrsup-universal*.bin from
172.17.16.81 (via GigabitEthernet0):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!
[OK - 208904396 bytes]

208904396 bytes copied in 330.453 secs (632176 bytes/sec)

Router# dir bootflash:
Directory of bootflash:/

11 drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
86401 drwx 4096 Dec 4 2007 06:06:24 -08:00 .ssh
14401 drwx 4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
28801 drwx 4096 Mar 18 2008 17:31:17 -07:00 .prst_sync
43201 drwx 4096 Dec 4 2007 04:34:45 -08:00 .installer
12 -rw- 208904396 May 28 2008 16:17:34 -07:00
cbrsup-universal*.bin
13 -rw- 45977 Apr 9 2008 16:48:46 -07:00 target_support_output.tgz.tgz

928862208 bytes total (503156736 bytes free)

Router# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#boot system flash
```

```
bootflash:cbrsup-universal*.bin
Router(config)#config-reg 0x2102
Router(config)#exit
Router#show run | include boot
boot-start-marker
boot system flash bootflash:cbrsup-universal*.bin boot-end-marker
Router# copy run start
Destination filename [startup-config]? Building configuration...
[OK]
Router# reload
```

統合パッケージから個別のサブパッケージを使用してルータを実行するための管理と設定

統合パッケージに含まれる個別のサブパッケージを使用してルータを実行するには、次のいずれかの手順を実行します。

統合パッケージの抽出とプロビジョニング ファイルを使用したブート

統合パッケージを抽出し、プロビジョニング ファイルを使用してブートするには、次の手順を実行します。

手順

ステップ 1 次のいずれかの作業を実行します。

a) **copy** コマンドを使用して、統合パッケージ ファイル（または、すべての個別サブパッケージとサブパッケージ用のプロビジョニング ファイルが使用可能な場合は、個別のサブパッケージとプロビジョニング ファイル）を bootflash: ファイル システムにコピーします。プロビジョニング ファイルと個別のイメージ サブパッケージを保存する bootflash: ファイル システムおよびディレクトリに、統合パッケージをコピーするようにしてください。他のオプションを指定せずに **request platform software package expand file bootflash:***url-to-Cisco-IOS-XE-imagename* コマンドを入力し、統合パッケージから bootflash: 内の現在のディレクトリにプロビジョニング ファイルおよび個別のサブパッケージを抽出します。サブパッケージは空のディレクトリに抽出し、これらのファイルを簡単に管理することを推奨します。

b) 統合パッケージ ファイルをルータ上のいずれかのファイル システムにコピーした後、**request platform software package expand file file-system:***url-to-Cisco-IOS-XE-imagename***to bootflash:** コマンドを入力して、bootflash: ファイル システムにプロビジョニング ファイルと個別のイメージ サブパッケージを抽出します。

（注） この手順を実行したあとは、ファイルを移動しないでください。起動プロセスは、すべてのサブパッケージおよびプロビジョニング ファイルが同じディレクトリ内にないと、正常に機能しません。また、サブパッケージ ファイルの名前を変更しないでください。名前を変更できるのはプロビジョニング ファイルだけです。また、プロビジョニング ファイルの名前の変更が必要な場合は、ルータをリブートする前にこの手順で行ってください。

ステップ 2 プロビジョニング ファイルを使用してブートするようにルータを設定します。

以下のシーケンスでは、他のサブパッケージとともに bootflash: ファイル システムに保存された「packages.conf」という名前のプロビジョニング ファイルを使用して、ルータをブートする例を示します。

```
Router(config)# no boot system
Router(config)# config-register 0x2102
Router(config)# boot system flash bootflash:packages.conf
Router(config)# exit
*May 11 01:31:04.815: %SYS-5-CONFIG_I: Configured from console by con
Router# copy running-config startup-config
Building configuration... [OK]
Router# reload
```

サブ パッケージおよびプロビジョニング ファイルの抽出：例 1

次に、個別のサブパッケージおよびプロビジョニング ファイルを保存するディレクトリに配置済みの統合パッケージから、個別のサブパッケージおよびプロビジョニング ファイルを抽出する例を示します。サブパッケージは空のディレクトリに抽出し、これらのファイルを簡単に管理することを推奨します。

抽出前後のディレクトリの出力は、ファイルが抽出されたことを確認するために提供されます。

```
Router# dir bootflash:
Directory of bootflash:/

11 drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
86401 drwx 4096 Dec 4 2007 06:06:24 -08:00 .ssh
14401 drwx 4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
28801 drwx 4096 Mar 18 2008 17:31:17 -07:00 .prst_sync
43201 drwx 4096 Dec 4 2007 04:34:45 -08:00 .installer
12 -rw- 208904396 May 9 2008 14:36:31 -07:00
cbrsup-universal*.bin
13 -rw- 45977 Apr 9 2008 16:48:46 -07:00 target_support_output.tgz.tgz

928862208 bytes total (503156736 bytes free)

Router# request platform software package expand file bootflash:cbrsup-universal*.bin
Verifying parameters
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.

Router# dir bootflash:
Directory of bootflash:/

11 drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
86401 drwx 4096 Dec 4 2007 06:06:24 -08:00 .ssh
14401 drwx 4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
28801 drwx 4096 Mar 18 2008 17:31:17 -07:00 .prst_sync
43201 drwx 4096 Dec 4 2007 04:34:45 -08:00 .installer
12 -rw- 208904396 May 9 2008 14:36:31 -07:00
cbrsup-universal*.bin
```

```
57611 -rw- 47071436 May 22 2008 11:26:23 -07:00 cbr000rp1-espbase.02.01.00.122-33.XNA.pkg
57602 -rw- 5740 May 22 2008 11:26:22 -07:00
cbr000rp1-packages-adventerprisek9.02.01.00.122-33.XNA.conf
57612 -rw- 20334796 May 22 2008 11:26:24 -07:00
cbr000rp1-rpaccess.02.01.00.122-33.XNA.pkg
57613 -rw- 22294732 May 22 2008 11:26:24 -07:00 cbr000rp1-rpbase.02.01.00.122-33.XNA.pkg
57614 -rw- 21946572 May 22 2008 11:26:25 -07:00 cbr000rp1-rpcontrol.02.01.00.122-33.XNA.pkg
57615 -rw- 48099532 May 22 2008 11:26:26 -07:00
cbr000rp1-rpios-adventerprisek9.02.01.00.122-33.XNA.pkg
57616 -rw- 34324684 May 22 2008 11:26:27 -07:00 cbr000rp1-sipbase.02.01.00.122-33.XNA.pkg
57617 -rw- 22124748 May 22 2008 11:26:28 -07:00 cbr000rp1-sipspa.02.01.00.122-33.XNA.pkg
57603 -rw- 6256 May 22 2008 11:26:28 -07:00 packages.conf
13 -rw- 45977 Apr 9 2008 16:48:46 -07:00 target_support_output.tgz.tgz

928862208 bytes total (286662656 bytes free)
```

サブパッケージの抽出、プロビジョニング ファイルを使用してルータをブートするための設定、ルータのリロード：例 2

次の例では、統合パッケージからプロビジョニング ファイルと個別のサブパッケージが抽出されます。パッケージの抽出後、ルータはプロビジョニング ファイルを使用してブートするように設定されます。また、ルータを適切にリロードするために必要となるコンフィギュレーション レジスタの設定方法と実行コンフィギュレーションの保存方法も示します。ルータはリロードされ、プロセスが終了します。

```
Router# dir bootflash:
Directory of bootflash:/

11 drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
86401 drwx 4096 Dec 4 2007 06:06:24 -08:00 .ssh
14401 drwx 4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
28801 drwx 4096 Mar 18 2008 17:31:17 -07:00 .prst_sync
43201 drwx 4096 Dec 4 2007 04:34:45 -08:00 .installer
12 -rw- 208904396 May 9 2008 14:36:31 -07:00
cbrsup-universal*.bin
13 -rw- 45977 Apr 9 2008 16:48:46 -07:00 target_support_output.tgz.tgz

928862208 bytes total (503156736 bytes free)

Router# request platform software package expand file bootflash:cbrsup-universal*.bin
Verifying parameters
Validating package type
Copying package files
SUCCESS: Finished expanding all-in-one software package.

Router# dir bootflash:
Directory of bootflash:/

11 drwx 16384 Dec 4 2007 04:32:46 -08:00 lost+found
86401 drwx 4096 Dec 4 2007 06:06:24 -08:00 .ssh
14401 drwx 4096 Dec 4 2007 06:06:36 -08:00 .rollback_timer
28801 drwx 4096 Mar 18 2008 17:31:17 -07:00 .prst_sync
```

```
43201 drwx 4096 Dec 4 2007 04:34:45 -08:00 .installer
12 -rw- 208904396 May 9 2008 14:36:31 -07:00
cbrsup-universal*.bin
57611 -rw- 47071436 May 22 2008 11:26:23 -07:00 cbr000rp1-espbase.02.01.00.122-33.XNA.pkg
57602 -rw- 5740 May 22 2008 11:26:22 -07:00
cbr000rp1-packages-adventerprisek9.02.01.00.122-33.XNA.conf
57612 -rw- 20334796 May 22 2008 11:26:24 -07:00 cbr000rp1-rpaccess.02.01.00.122-33.XNA.pkg
57613 -rw- 22294732 May 22 2008 11:26:24 -07:00 cbr000rp1-rpbase.02.01.00.122-33.XNA.pkg
57614 -rw- 21946572 May 22 2008 11:26:25 -07:00
cbr000rp1-rpcontrol.02.01.00.122-33.XNA.pkg
57615 -rw- 48099532 May 22 2008 11:26:26 -07:00
cbr000rp1-rpios-adventerprisek9.02.01.00.122-33.XNA.pkg
57616 -rw- 34324684 May 22 2008 11:26:27 -07:00 cbr000rp1-sipbase.02.01.00.122-33.XNA.pkg
57617 -rw- 22124748 May 22 2008 11:26:28 -07:00
cbr000rp1-sipspa.02.01.00.122-33.XNA.pkg
57603 -rw- 6256 May 22 2008 11:26:28 -07:00 packages.conf
13 -rw- 45977 Apr 9 2008 16:48:46 -07:00 target_support_output.tgz.tgz

928862208 bytes total (286662656 bytes free)

Router(config)# no boot system
Router(config)# config-register 0x2102
Router(config)# boot system flash bootflash:packages.conf
Router(config)# exit
Router# copy run start
Router# reload
```

個別のサブパッケージ ファイル セットのコピーとプロビジョニング ファイルを使用したブート

個別のサブパッケージファイルのセットをコピーし、プロビジョニングファイルを使用してブートするには、次の手順を実行します。

（注） この方法でもアップグレードは可能ですが、ルータのソフトウェアをアップグレードする他の方法ほど効率的ではありません。

手順

ステップ 1 **copy** コマンドを使用して、個々のサブパッケージとプロビジョニング ファイルを bootflash: ディレクトリにコピーします。この方法でルータを実行できるのは、リリースのすべての個別サブパッケージとプロビジョニング ファイルがルータにダウンロードされ、bootflash: ディレクトリに保存されている場合だけです。個別のサブパッケージを使用してルータをブートする場合、他のファイル ディレクトリが使用されることはありません。
これらのファイルは、USB フラッシュ ドライブを使用してルータに物理的に移動できます。

ステップ 2 プロビジョニング ファイルを使用してブートするようにルータを設定します。

以下のシーケンスでは、他のサブパッケージとともに bootflash: ファイル システムに保存された「packages.conf」という名前のプロビジョニング ファイルを使用して、ルータをブートする例を示します。リロードが完了すると、ルータが個別のサブパッケージを使用して起動します。

```
Router(config)# no boot system
Router(config)# config-register 0x2102
Router(config)# boot system flash bootflash:packages.conf
Router(config)# exit
*May 11 01:31:04.815: %SYS-5-CONFIG_I: Configured from console by con
Router# write memory Building configuration... [OK]
Router# reload
```

オプションのサブパッケージのインストール

オプションのサブパッケージを使用してルータを実行するには、シャーシに搭載されたスーパーバイザごとに次の手順を実行します。

手順

ステップ 1 スーパーバイザが個別サブパッケージモードで実行されていて、プロビジョニング ファイルからブートされたことを確認します。

ステップ 2 インストールするオプション サブパッケージのバージョンが、アクティブ スーパーバイザで実行されているソフトウェアと同じバージョンであることを確認します。

ステップ 3 インストールするオプションのサブパッケージをダウンロードします。オプション サブパッケージは、Cisco cBR シリーズ ルータの統合パッケージとは別にダウンロードする必要があります。

ステップ 4 各スーパーバイザで、他の個別サブパッケージファイルおよびプロビジョニング ファイルが存在するディレクトリにオプション サブパッケージをコピーします。

ステップ 5 次の例に示すように **request platform software package install rp file** コマンドを実行します。初回インストールでは、オプションの slot キーワードまたは bay キーワードは使用しないでください。

```
Router# request platform software package install rp 0 file
bootflash: cbrsup-universal*.bin
--- Starting local lock acquisition on R0 --- Finished local lock acquisition on R0

--- Starting file path checking --- Finished file path checking

--- Starting image file verification --- Checking image file names Verifying image file
locations Locating image files and validating name syntax
Found cbrsup-universal*.bin
Inspecting image file types Processing image file constraints Creating candidate provisioning
 file

WARNING: No package of type sipspawmak9 is installed.
```

```
WARNING: Package will be installed for all SIP slots and bays. Finished image file
verification
--- Starting candidate package set construction --- Verifying existing software set Processing
 candidate provisioning file Constructing working set for candidate package set Constructing
 working set for running package set Checking command output Constructing merge of running
 and candidate packages Checking if resulting candidate package set would be complete
Finished candidate package set construction

--- Starting compatibility testing ---
Determining whether candidate package set is compatible

WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:

Determining whether installation is valid

WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:

Software sets are identified as compatible Checking IPC compatibility with running software
 Checking candidate package set infrastructure compatibility Checking infrastructure
compatibility with running software Checking package specific compatibility Finished
compatibility testing

--- Starting impact testing --- Checking operational impact of change Finished impact testing

--- Starting list of software package changes --- No old package files removed New files
list:
Added cbrsup-universal*.bin Finished list of software package changes

--- Starting commit of software changes --- Updating provisioning rollback files Creating
pending provisioning file Committing provisioning file Finished commit of software changes

--- Starting analysis of software changes --- Finished analysis of software changes

--- Starting update running software --- Blocking peer synchronization of operating
information Creating the command set placeholder directory
Finding latest command set
Finding latest command shortlist lookup file Finding latest command shortlist file Assembling
 CLI output libraries
Assembling CLI input libraries
Applying interim IPC and database definitions
Replacing running software Replacing CLI software Restarting software
Restarting software: target frus filtered out ... skipped
Applying final IPC and database definitions Generating software version information Notifying
 running software of updates
Unblocking peer synchronization of operating information Unmounting old packages
Cleaning temporary installation files
Finished update running software

SUCCESS: Finished installing software.
```

個別のサブパッケージのアップグレード

パッチのインストール

個別のサブパッケージをサブパッケージモードでアップグレードすることができます。パッチリリースは1つまたは複数のサブパッケージから構成されます。パッチをインストールした後、アップデートを有効にするために、シャーシ全体、またはラインカードのみをリブートする必要があることを示すメッセージが表示されます。

ライン カードとスーパーバイザ カードの両方に影響するパッチのインストール

手順

ステップ 1 Cisco cBR ルータはサブパッケージ モードになっている必要があります。

ステップ 2 アクティブとスタンバイのスーパーバイザカード上のアクティブパッケージと同じ場所にパッチファイルをコピーします。

ステップ 3 **request platform software package install rp** *slot***file** *patch file* コマンドを使用して、スタンバイ カードにパッチをインストールします。

ステップ 4 **request platform software package install rp** *slot***file** *patch file* コマンドを使用して、アクティブ カードにパッチをインストールします。

ステップ 5 シャーシをリロードします。

ライン カードのみに影響するパッチのインストール

手順

ステップ 1 Cisco cBR ルータはサブパッケージ モードになっている必要があります。

ステップ 2 アクティブとスタンバイのスーパーバイザカード上のアクティブパッケージと同じ場所にパッチファイルをコピーします。

ステップ 3 **request platform software package install rp** *slot***file** *patch file* コマンドを使用して、スタンバイ カードにパッチをインストールします。

ステップ 4 **request platform software package install rp** *slot***file** *patch file* コマンドを使用して、アクティブ カードにパッチをインストールします。

ステップ 5 ライン カードをリロードします。

スーパーバイザ カードのみに影響するパッチのインストール

手順

ステップ 1 Cisco cBR ルータはサブパッケージ モードになっている必要があります。

ステップ 2 アクティブとスタンバイのスーパーバイザカード上のアクティブパッケージと同じ場所にパッチファイルをコピーします。

ステップ 3 **request platform software package install rp** *slot***file** *patch file* コマンドを使用して、スタンバイ カードにパッチをインストールします。

ステップ 4 スタンバイ カードに切り替えます。これにより、カードはアクティブになります。

ステップ 5 **request platform software package install rp** *slot***file** *patch file* コマンドを使用して、スタンバイ カードにパッチをインストールします。

ラインカードのサブパッケージのアップグレード

ライン カードのサブパッケージをアップグレードするには **request platform software package install node file** *filename* コマンドを使用します。

```
Router# request platform software package install node file
bootflash:/subpkg/cbr_patch.5.0.tar

NOTE: Currently node has booted from a provisioning file
NOTE: Going to start a dual rp sub-packages node ISSU install

--- Starting initial file path checking ---
Copying bootflash:/subpkg/cbr_patch.5.0.tar to stby-bootflash:/subpkg/cbr_patch.5.0.tar
Finished initial file path checking

--- Starting config-register verfication ---
Finished config-register verfication

--- Starting image file expansion ---
Expanding image file: bootflash:/subpkg/cbr_patch.5.0.tar
Image file expanded and copied
Expanding image file: stby-bootflash:/subpkg/cbr_patch.5.0.tar
Image file expanded and copied
Finished image file expansion


STAGE 1: Installing software on standby RP
==========================================
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

--- Starting installation state synchronization ---
Finished installation state synchronization

--- Starting local lock acquisition on R1 ---
Finished local lock acquisition on R1

--- Starting file path checking ---
Finished file path checking

--- Starting image file verification ---
Checking image file names
```

```
Locating image files and validating name syntax
  Found cbrsup-clcdocsis.2015-02-20_01.02.SSA.pkg
Verifying image file locations
Inspecting image file types
Processing image file constraints
Creating candidate provisioning file
Finished image file verification

--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction

--- Starting ISSU compatiblity verficiation ---
Verifying image type compatibility
Checking IPC compatibility with running software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking package specific compatibility
Finished ISSU compatiblity verficiation

--- Starting list of software package changes ---
Old files list:
  Removed cbrsup-clcdocsis.BLD_V155_2_S_XE315_THROTTLE_LATEST_20150217_110041-st
d.SSA.pkg
New files list:
  Added cbrsup-clcdocsis.2015-02-20_01.02.SSA.pkg
Finished list of software package changes

--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes

--- Starting analysis of software changes ---
Finished analysis of software changes

--- Starting update running software ---
Blocking peer synchronization of operating information
Creating the command set placeholder directory
  Finding latest command set
  Finding latest command shortlist lookup file
  Finding latest command shortlist file
  Assembling CLI output libraries
  Assembling CLI input libraries
  Assembling Dynamic configuration files
  Applying interim IPC and database definitions
  Replacing running software
  Replacing CLI software
  Restarting software
  Restarting software: target frus filtered out ... skipped
  Applying final IPC and database definitions
  Generating software version information
  Notifying running software of updates
  Unblocking peer synchronization of operating information
Unmounting old packages
Cleaning temporary installation files
  Finished update running software

SUCCESS: Finished installing software.

STAGE 2: Installing software on active RP
=========================================
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

--- Starting installation state synchronization ---
```

```
Finished installation state synchronization

--- Starting file path checking ---
Finished file path checking

--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
  Found cbrsup-clcdocsis.2015-02-20_01.02.SSA.pkg
Verifying image file locations
Inspecting image file types
Processing image file constraints
Creating candidate provisioning file
Finished image file verification

--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction

--- Starting ISSU compatiblity verficiation ---
Verifying image type compatibility
Checking IPC compatibility with running software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking package specific compatibility
Finished ISSU compatiblity verficiation

--- Starting impact testing ---
Checking operational impact of change
Finished impact testing

--- Starting list of software package changes ---
Old files list:
  Removed cbrsup-clcdocsis.BLD_V155_2_S_XE315_THROTTLE_LATEST_20150217_110041-st
d.SSA.pkg
New files list:
  Added cbrsup-clcdocsis.2015-02-20_01.02.SSA.pkg
Finished list of software package changes

--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes

--- Starting analysis of software changes ---
Finished analysis of software changes

--- Starting update running software ---
Blocking peer synchronization of operating information
Creating the command set placeholder directory
  Finding latest command set
  Finding latest command shortlist lookup file
  Finding latest command shortlist file
  Assembling CLI output libraries
  Assembling CLI input libraries
  Assembling Dynamic configuration files
  Applying interim IPC and database definitions
  Replacing running software
  Replacing CLI software
  Restarting software
  Restarting software: target frus filtered out ... skipped
  Applying final IPC and database definitions
  Generating software version information
  Notifying running software of updates
  Unblocking peer synchronization of operating information
Unmounting old packages
```

```
Cleaning temporary installation files
  Finished update running software

SUCCESS: Finished installing software.
Found clc package
Found clc package
Found clcdocsis package
SUCCESS: Reload Cable Linecard at slot 1
SUCCESS: Reload Cable Linecard at slot 2
SUCCESS: node ISSU finished successfully.
Invoking cleanup routine
```

ライン カードのサブパッケージをアップグレードするには **request platform software package install node file** *filename* **noreload linecard** コマンドを使用します。

```
Router#request platform software package install node file bootflash:/subpkg/cbr_patch.5.0.tar
 noreload linecard
NOTE: Currently node has booted from a provisioning file
NOTE: Going to start a dual rp sub-packages node ISSU install

--- Starting initial file path checking ---
Copying bootflash:/subpkg/cbr_patch.5.0.tar to stby-bootflash:/subpkg/cbr_patch.
5.0.tar
Finished initial file path checking

--- Starting config-register verfication ---
Finished config-register verfication

--- Starting Checking noreload options ---
Finished Checking noreload options

--- Starting image file expansion ---
Expanding image file: bootflash:/subpkg/cbr_patch.5.0.tar
Image file expanded and copied
Expanding image file: stby-bootflash:/subpkg/cbr_patch.5.0.tar
Image file expanded and copied
Finished image file expansion

Found clc package

STAGE 1: Installing software on standby RP
==========================================
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

--- Starting installation state synchronization ---
Finished installation state synchronization

--- Starting local lock acquisition on R1 ---
Finished local lock acquisition on R1

--- Starting file path checking ---
Finished file path checking

--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
  Found cbrsup-clcdocsis.2015-03-01_01.40.SSA.pkg
Verifying image file locations
Inspecting image file types
Processing image file constraints
Creating candidate provisioning file
Finished image file verification

--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
```

```
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction

--- Starting ISSU compatiblity verficiation ---
Verifying image type compatibility
Checking IPC compatibility with running software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking package specific compatibility
Finished ISSU compatiblity verficiation

--- Starting list of software package changes ---
Old files list:
  Removed cbrsup-clcdocsis.2015-03-01_03.43.SSA.pkg
New files list:
  Added cbrsup-clcdocsis.2015-03-01_01.40.SSA.pkg
Finished list of software package changes

--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes

--- Starting analysis of software changes ---
Finished analysis of software changes

--- Starting update running software ---
Blocking peer synchronization of operating information
Creating the command set placeholder directory
  Finding latest command set
  Finding latest command shortlist lookup file
  Finding latest command shortlist file
  Assembling CLI output libraries
  Assembling CLI input libraries
  Assembling Dynamic configuration files
  Applying interim IPC and database definitions
  Replacing running software
  Replacing CLI software
  Restarting software
  Restarting software: target frus filtered out ... skipped
  Applying final IPC and database definitions
  Generating software version information
  Notifying running software of updates
  Unblocking peer synchronization of operating information
Unmounting old packages
Cleaning temporary installation files
  Finished update running software

SUCCESS: Finished installing software.

STAGE 2: Installing software on active RP
=========================================
--- Starting local lock acquisition on R0 ---
Finished local lock acquisition on R0

--- Starting installation state synchronization ---
Finished installation state synchronization

--- Starting file path checking ---
Finished file path checking

--- Starting image file verification ---
Checking image file names
Locating image files and validating name syntax
  Found cbrsup-clcdocsis.2015-03-01_01.40.SSA.pkg
Verifying image file locations
Inspecting image file types
Processing image file constraints
Creating candidate provisioning file
Finished image file verification
```

```
--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Checking if resulting candidate package set would be complete
Finished candidate package set construction

--- Starting ISSU compatiblity verficiation ---
Verifying image type compatibility
Checking IPC compatibility with running software
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking package specific compatibility
Finished ISSU compatiblity verficiation

--- Starting impact testing ---
Checking operational impact of change
Finished impact testing

--- Starting list of software package changes ---
Old files list:
  Removed cbrsup-clcdocsis.2015-03-01_03.43.SSA.pkg
New files list:
  Added cbrsup-clcdocsis.2015-03-01_01.40.SSA.pkg
Finished list of software package changes

--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes

--- Starting analysis of software changes ---
Finished analysis of software changes

--- Starting update running software ---
Blocking peer synchronization of operating information
Creating the command set placeholder directory
  Finding latest command set
  Finding latest command shortlist lookup file
  Finding latest command shortlist file
  Assembling CLI output libraries
  Assembling CLI input libraries
  Assembling Dynamic configuration files
  Applying interim IPC and database definitions


  Replacing running software
  Replacing CLI software
  Restarting software
  Restarting software: target frus filtered out ... skipped
  Applying final IPC and database definitions
  Generating software version information
  Notifying running software of updates
  Unblocking peer synchronization of operating information
Unmounting old packages
Cleaning temporary installation files
  Finished update running software

SUCCESS: Finished installing software.
Found clc package
SUCCESS: node ISSU finished successfully.
Invoking cleanup routine
```

このアップグレードの完了を確認するには **show platform software patch *n*info** コマンドを使用します。

```
Router#show platform software patch 1 info
cbrsup-clciosdb: 3.15 (0.0)
cbrsup-clc-firmware: 3.15 (0.0)
cbrsup-clcvideo: 3.15 (0.0)
cbrsup-clcios: 3.15 (0.0)
cbrsup-clccontrol: 3.15 (0.0)
cbrsup-clcdocsis: 3.15 (1.0)
cbrsup-clcmipsbase: 3.15 (0.0)


Router#show platform software patch 2 info
cbrsup-clciosdb: 3.15 (0.0)
cbrsup-clc-firmware: 3.15 (0.0)
cbrsup-clcvideo: 3.15 (0.0)
cbrsup-clcios: 3.15 (0.0)
cbrsup-clccontrol: 3.15 (0.0)
cbrsup-clcdocsis: 3.15 (1.0)
cbrsup-clcmipsbase: 3.15 (0.0)
```

このアップグレードの完了を確認するには **show platform software ios** *slot-number* **restart info** コマンドを使用します。この例では、RF ラインカード スロット番号 2 に対するこの **show** コマンドの出力を示します。

```
Router#show platform software ios 2 restart info
IOSD process restart info:
  Process restartable: Yes
  IOSD restart state : NOT_RESTARTED_YET
  Total Modem Count  : 251
  Active Modem Count : 251


Router#
```

その他の参考資料

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

統合パッケージとサブパッケージの管理に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *6*：統合パッケージとサブパッケージの管理に関する機能情報

機能名	リリース	機能情報
統合パッケージとサブパッケージの管理	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 II 部

ハイ アベイラビリティ設定

第 5 章

CiscoIOS-XEインサービスソフトウェアアップグレード プロセス

Cisco cBR-8 ルータは、冗長プラットフォームのインサービス ソフトウェア アップグレード（ISSU）をサポートします。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *7*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

インサービス ソフトウェア アップグレードについて

Cisco cBR-8 ルータは、冗長プラットフォームのインサービス ソフトウェア アップグレード（ISSU）をサポートします。ISSU プロセスを使用すると、ソフトウェアを更新または変更している間も

LCHA を利用してパケット転送を続けることができます。ISSU は 2 種類のソフトウェア アップグレード モードをサポートします。

- 統合パッケージ モード
- サブパッケージ モード

Cisco cBR シリーズ ルータの場合、ISSU の互換性はアップグレードされるソフトウェア サブパッケージ、およびハードウェア構成によって異なります。統合パッケージは、デュアル SUP 構成の場合にだけ ISSU 対応となり、その他にもこのマニュアルで後述する制限があります。

このマニュアルに記載された特定の手順は、サポートされているテスト済みのインストール シーケンスを表します。特別な目的のために、シスコカスタマーサポート担当者の指示を受けながら他のインストール シーケンスを使用して Cisco IOS-XE システム ソフトウェアをアップグレードすることもできますが、それ以外の場合はこのマニュアルに記載されたステップに従ってください。Cisco cBR シリーズ ルータは、SUP 上のすべての統合パッケージおよびサブパッケージについて 1 つのバージョンの Cisco IOS-XE を実行するように設計されており、異なるバージョンの Cisco IOS-XE に含まれるサブパッケージを実行すると、予測できないルータの動作を引き起こす可能性があります。そのため、このマニュアルに記載されたステップに完全に従う必要があります。

インサービス ソフトウェア アップグレードの設定方法

ここでは、ISSU 機能の設定について説明します。

統合パッケージ アップグレードの設定

統合パッケージ アップグレード

ISSU を使用した統合パッケージのアップグレードは、SUP 構成の場合にだけ実行できます。シングル SUP 構成での統合パッケージのアップグレードでは、ISSU はサポートされません。

インサービスのワンショット ソフトウェア アップグレード手順を使用すると、1 つのコマンドを使用してソフトウェアをアップグレードまたはダウングレードできます。ワンショット ISSU で必要なユーザ介入やモニタリングは最小限です。

ワンショット アップグレードの手順は複数の段階に分割されます。障害が発生した場合は、コマンドの実行は停止され、ユーザはロールバック タスクを手動で実行する必要があります。アップグレードの 1 段階では、必要なスイッチ オーバーが自動的に処理されます。スイッチオーバー時に、コンソールおよび出力は失われます。追加コマンドが、コンソールに再び接続するために使用されます。

（注） ワンショット アップグレードは複数の同時アップグレードをサポートしません。

はじめる前に

統合パッケージ アップグレード プロセスを実行する前に、次の前提条件を完了してください。

- ルータに 2 つの SUP をセットアップします。
- スタンバイ SUP はホット スタンバイ モードになっている必要があります。
- 自動起動をイネーブルにします。
- SUP は両方とも統合パッケージ モードで、同じパスから同じイメージを実行しています。
- 両方の SUP の ブートフラッシュの空き容量は 700 MB 以上です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**requestplatformsoftwarepackageinstallnodebootflash:** 例： `Router# request platform software package install node bootflash:subpkg_3_16/cbrsup-universalk9.03.16.00.S.155-3.S-std.SPA.bin`	ワンショット ISSU 手順を使用して cBR-8 ルータをアップグレードします。

統合パッケージ アップグレードの中止

ISSU 手順を中止するには、**requestplatformsoftwarepackageinstallnodeabort** コマンドを使用します。

ユーザが ISSU を中断する場合、SUP にあるラインカードのバージョンは異なります。

新しいバージョンが安定せず、アップグレードを停止したいと顧客が考えている場合は、このコマンドを使用して現在のアップグレード プロセスを中断することができます。顧客は、このコマ

ンドを入力したら、SUP と LC の両方の状態を確認し、次の手順で何（ロールバックなど）を実行するかを決定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権EXECモードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**requestplatformsoftwarepackageinstallnodeabort** 例： `Router# request platform software package install node abort`	ISSU 手順を中断します。

統合パッケージ アップグレードのロールバック

アップグレード後に顧客が新しいパッケージに満足しない場合、ロールバック操作を使用して以前の動作状態にシステムを戻すことができます。冗長グループ外のラインカードはリロードされます。

（注） ロールバック操作では、履歴における一段階前にしか戻れません。顧客がもっと以前のイメージに戻ることを望む場合は、ダウングレード操作を使用する必要があります。

統合パッケージ アップグレードのロールバックを実行するは、次の手順を使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**requestplatformsoftwarepackageinstallnoderollback** 例： `Router# request platform software package install node rollback`	前の作業状態に戻ります。

サブパッケージ アップグレードの設定

サブパッケージ アップグレード

サブパッケージのアップグレードにより、実行中のソフトウェアのサブセットをアップグレードできます。その目的は、完全なイメージアップグレードではなく、細かい、ターゲットを絞った修正をパッチすることです。サブパッケージのアップグレードは、シングルおよびデュアル SUP セットアップをサポートします。

単一の *SUP* サブパッケージのアップグレード

はじめる前に

ISSU プロセスを実行する前に、次の前提条件を完了してください。

- コンフィギュレーション レジスタのオートブートがイネーブルになっている。
- packages.conf ファイル システムの同じディレクトリ内にあるアクティブな SUP にコピーされるターゲット パッチが一緒に起動している。
- 必要に応じて、パッチ情報ファイルを SUP にコピーする。
- SUP に十分なブートフラッシュのディスク領域がある。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**requestplatformsoftwarepackageinstallrp** *rp-slot***filebootflash:** 例： `Router# request platform software package install rp 1 file bootflash:cbrsup-universalk9.03.17.00.S.156-1.S-std.SPA.bin`	サブパッケージ ISSU 手順に従って、1 つの SUP を搭載した cBR-8 ルータをアップグレードします。

デュアル *SUP* サブパッケージのアップグレード

はじめる前に

ISSU プロセスを実行する前に、次の前提条件を完了してください。

- スタンバイ SUP がホット スタンバイになっている。
- コンフィギュレーション レジスタのオートブートがイネーブルになっている。
- サブパッケージ モードの両方の SUP が同じ基本イメージとパッチを同じパスから実行している。
- packages.conf ファイル システムの同じディレクトリ内にあるアクティブな SUP にコピーされるターゲット パッチが一緒に起動している。
- 必要に応じて、パッチ情報ファイルを両方の SUP にコピーする。
- 両方の SUP に十分なブートフラッシュのディスク領域がある。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**requestplatformsoftwarepackageinstallnodefilebootflash:** 例： `Router# request platform software package install node file bootflash:cbrsup-universalk9.03.17.00.S.156-1.S-std.SPA.bin`	サブパッケージ ISSU 手順に従って、デュアル SUP を搭載した cBR-8 ルータをアップグレードします。

サブパッケージ アップグレードのロールバック

アップグレード後に顧客が新しいパッケージに満足しない場合、ロールバック操作を使用して以前の動作状態にシステムを戻すことができます。冗長グループ外のラインカードはリロードされます。

（注） ロールバック操作では、履歴における一段階前にしか戻れません。顧客がもっと以前のイメージに戻ることを望む場合は、ダウングレード操作を使用する必要があります。

サブパッケージ アップグレードのロールバックを実行するは、次の手順を使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権EXECモードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**requestplatformsoftwarepackageinstallrp 0rollback** 例： `Router# request platform software package install rp 0 rollback`	前の作業状態に戻ります。

ラインカードのみのインサービス ソフトウェア アップグレード

ライン カードのアップグレード段階でアップグレードが失敗したり手動で強制終了したりした場合は、ライン カードのみのアップグレードを開始できます。

現在のアクティブ SUP と同じバージョンにライン カードだけをアップグレードするには、**requestplatformsoftwarepackageinstallnodelinecard-only** コマンドを使用します。この場合、特定のラインカードをアップグレードするか、シャーシ内のすべてのライン カードをアップグレードするかを選択できます。

このコマンドを **requestplatformsoftwarepackageinstallnodefile** *file-path* **noreloadlinecard** コマンドと併せて使用すると、最初にSUPをアップグレードしてから、ライン カードをアップグレードすることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**requestplatformsoftwarepackageinstallnodelinecard-only** 例： `Router# request platform software package install node linecard-only all`	すべてのラインカードを現在のアクティブ SUP のラインカードと同じバージョンにアップグレードします。

メジャー リリース間での ISSU アップグレード

Cisco IOS XE Fuji 16.7.1 リリース以降、ISSU ではメジャー リリース間で cbr-8 をアップグレードできます。

手順

ステップ 1 基本イメージをアクティブ SUP とスタンバイ SUP にコピーします。ISSU ターゲット イメージをアクティブ SUP にコピーします。

copy <location>/<base_image> <location_active_sup>
copy <location>/<base_image> <location_standby_sup>
copy <location>/<target_image> <location_active_sup>

ステップ 2 基本イメージを、同じフォルダにある両方の SUP に展開します。

request platform software package expand file <location_active_sup>/<base_image>
request platform software package expand file <location_standby_sup>/<base_image>

ステップ 3 自動ブート（例）config-reg 0x2102 のレジスタを設定します。

config-register 0x2102
boot system <location_active_sup>/packages.conf

ステップ 4 ルータを保存し、サブパッケージ モードでリロードします。

reload

ステップ 5 起動後、**show version running** を使用して、ロードされた基本イメージの詳細を確認します。

ステップ 6 前と同じ場所にあるアクティブ SUP にターゲット イメージをコピーします。

copy <location>/<target_image> <location_active_sup>

ステップ 7 要求コマンドを使用して ISSU を行います。

```
request platform software package install node file <location_active_sup>/<target_image>
```

その他の参考資料

ここでは、ISSU 機能に関する参考資料について説明します。

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

インサービス ソフトウェア アップグレードに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *8* : *ISSU* に関する機能情報

機能名	リリース	機能情報
ISSU	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 6 章

スーパーバイザ冗長性

スーパーバイザ冗長性機能により、予定外のダウンタイムを減らすことができます。この機能を使用すると、アクティブ スーパーバイザに重大なエラーが発生した場合、アクティブおよびスタンバイ スーパーバイザの間で迅速にスイッチオーバーできます。スーパーバイザ冗長性が設定されている場合、スタンバイ スーパーバイザがアクティブ スーパーバイザと同期されます。アクティブ スーパーバイザで重大なエラーが発生した場合、システムは直ちにスタンバイ スーパーバイザに切り替えます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *9* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

スーパーバイザ冗長性の前提条件

- 2 つのスーパーバイザ（つまり、2 つのスーパーバイザ カードおよび 2 つの スーパーバイザ PIC）を Cisco cBR シャーシにインストールする必要があります。

- 両方のスーパーバイザで同じソフトウェア リリースを実行する必要があります。

スーパーバイザ冗長性の情報

スーパーバイザ 冗長性機能では、Cisco cBR ルータが 2 つの スーパーバイザ を冗長構成で使用できます。そのため、アクティブ スーパーバイザが失敗したり非アクティブになったりすると、システムは自動的にスイッチオーバーを実行します。その結果、スタンバイ スーパーバイザがテイクオーバーして、システムの動作にすべての責任を負います。

スーパーバイザ 冗長性機能は、スイッチオーバーを実行するためにシステムの完全リブートが必要ありません。システムがブートすると、スタンバイ スーパーバイザは完全初期化を実行します（自己の初期化、アクティブ スーパーバイザ からの実行コンフィギュレーションの同期、アクティブ スーパーバイザ からの SSO 機能データ同期など）。その後、ホット スタンバイ状態になり、アクティブ スーパーバイザ をモニタします。スタンバイ スーパーバイザ がアクティブ スーパーバイザ の障害を検出すると、すぐにシステム動作をアクティブに担当できます。

各 スーパーバイザ には、ブートフラッシュ メモリ、ハード ディスク、イーサネット ポート、コンソール ポートなど、ルータの動作に必要なすべてのリソースが含まれています。デフォルトの動作では、スタンバイ スーパーバイザ は、実行コンフィギュレーション ファイルなどの主要なシステム ファイルも同期して、スイッチオーバー時にスタンバイ スーパーバイザ がアクティブ スーパーバイザ のコンフィギュレーションを複製できるようにします。

Cisco IOS CLI コマンドを使用して、ブートフラッシュやハード ディスクなどのスタンバイ スーパーバイザ リソースにアクセスできます。たとえば、**dir** コマンドを使用してデバイスの内容を一覧表示したり、**copy** コマンドを使用してアクティブおよびスタンバイ スーパーバイザの間でファイルを転送したりできます。

スイッチオーバー手順

アクティブ スーパーバイザからスタンバイ スーパーバイザに責任が引き継がれると、スイッチオーバーが発生します。アクティブ スーパーバイザに障害が発生したことをスタンバイ スーパーバイザが判定して自動的にスイッチオーバーが行われる場合と、オペレータが必要に応じて手動スイッチオーバーを開始する場合があります。

スイッチオーバーは次のイベントをトリガーします。

1. 手動スイッチオーバーの場合、アクティブ スーパーバイザは、スタンバイ スーパーバイザが存在すること、SSO になっていることを確認します。これが確認されると、スタンバイ スーパーバイザはスイッチオーバー手順を開始します。アクティブ スーパーバイザは、そのコンフィギュレーション レジスタの設定に応じて、そこで設定された Cisco IOS ソフトウェア イメージのリロードを試みるか、または ROM モニタ モードに入ります。
2. スタンバイ スーパーバイザはアクティブ スーパーバイザとしての責任を引き受け、Cisco cBR シャーシをアクティブ状態にして、アクティブ スーパーバイザとしてサービスを続行します。
3. 新しいアクティブ スーパーバイザは、トラフィックの受け渡しを含む通常のシステム動作を開始します。

（注） スーパーバイザは、適切な Cisco IOS ソフトウェアでブートするまで、スタンバイ スーパーバイザとしての機能を開始しません。

スーパーバイザ スイッチオーバーが失敗する場合

一般に、アクティブ スーパーバイザに次のような問題があると、スーパーバイザ スイッチオーバーが影響を受ける場合があります。

- スーパーバイザのハング
- スーパーバイザ コンソールへのログインまたはシャーシへの Telnet の失敗
- クラッシュが原因で、インターフェイス カードがアクティブ スーパーバイザに接続できない
- ケーブル モデムのドロップによるオフライン化
- シャーシのリロードが必要
- サービスの復旧のためにアクティブ スーパーバイザのリセットが必要

（注） スーパーバイザにハードウェアの問題がある場合は、障害のあるスーパーバイザをシャーシに再挿入しないでください。障害のあるスーパーバイザを挿入すると（スタンバイ スーパーバイザであっても）、インターフェイス カードが障害のあるスーパーバイザにスイッチし、これによりインターフェイス カードのクラッシュやケーブル モデムのオフライン化が起きる場合があります。

冗長性ファイル システムの使用

アクティブおよびスタンバイ スーパーバイザの両方に、ファイルを保存および転送するためにアクセス可能なアクティブなファイル システムがあります。次の表に、使用可能なファイル システム、ファイル システムにアクセスするのに CLI コマンドで使用できるファイル名、およびそれぞれの簡単な説明を示します。

ファイル システム	CLI コマンド用のファイル名	説明
• ブートフラッシュ • フラッシュ • ハードディスク • USB • スタンバイ ブートフラッシュ • スタンバイ ハードディスク • スタンバイ USB	• bootflash: • flash: • harddisk: • usb0: • usb1: • stby-bootflash: • stby-harddisk: • stby-usb0: • stby-usb1:	イメージ、クラッシュ ファイル、コア ファイル、保存されたコンフィギュレーションファイル、およびさまざまなユーザ ファイルを保存します。
• システム • 一時的なシステム • ヌル • tar • Syslog • CNS • RCSF	• system: • tmpsys: • null: • tar: • syslog: • cns: • revrcsf:	実行コンフィギュレーションおよび他のシステム ファイルを保存します。
• NVRAM • スタンバイ NVRAM • スタンバイ RCSF	• nvram: • stby-nvram: • stby-rcsf:	通常、システムのデフォルトのコンフィギュレーション ファイルおよびスタートアップ コンフィギュレーション ファイルを保存します。
• TFTP • RCP • PRAM • FTP • HTTP • SCP • HTTPS	• tftp: • rcp: • pram: • ftp: • http: • scp: • https:	リモートデバイスとの間でファイルを転送するために使用されるプロトコル。

特権 EXEC コマンド **dir**、**del**、および **copy** を使用して、ファイル システムの内容を管理できます。また、**mkdir** および **rmdir** コマンドを使用して、ブートフラッシュまたはハードディスクのディレクトリを作成および削除できます。

次に、Cisco cBR ルータに対する **show file systems** コマンドの出力例を示します。

```
Router# show file systems

File Systems:

Size(b)       Free(b)      Type  Flags  Prefixes
             -             -    opaque     rw   system:
             -             -    opaque     rw   tmpsys:
*   7800705024    1574408192      disk     rw   bootflash:
    7800705024    1574408192      disk     rw   flash:
   98394218496   79534682112      disk     rw   harddisk:
    8009056256    8009023488      disk     rw   usb1:
      33554432      33507452     nvram     rw   stby-nvram:
             -             -    opaque     rw   null:
             -             -    opaque     ro   tar:
             -             -   network     rw   tftp:
             -             -    opaque     wo   syslog:
      33554432      33508476     nvram     rw   nvram:
             -             -   network     rw   rcp:
             -             -   network     rw   pram:
             -             -   network     rw   ftp:
             -             -   network     rw   http:
             -             -   network     rw   scp:
             -             -   network     rw   https:
             -             -    opaque     ro   cns:
             -             -     nvram     rw   stby-rcsf:
    7800705024    1635270656      disk     rw   stby-bootflash:
   98394218496   89040576512      disk     rw   stby-harddisk:
             -             -      disk     rw   stby-usb0:
    1000787968     301559808      disk     rw   stby-usb1:
             -             -    opaque     rw   revrcsf:
```

スーパーバイザ スイッチオーバー後のコンソール ポートの使用

アクティブ スーパーバイザ が失敗し、スタンバイ スーパーバイザ がアクティブ スーパーバイザになったら、CLI コマンドを入力したりルータの統計情報を表示したりするために新しいアクティブ スーパーバイザ のコンソール ポートを使用する必要があります。スタンバイ スーパーバイザ コンソールはデフォルトでは無効であり、CLI コマンドを実行するために使用することができません。次に、スタンバイ スーパーバイザ コンソールの出力例を示します。

```
Router-stby>
Standby console disabled
Router-stby>
```

コンソールにアクセスするには、PC または端末のシリアル ケーブルを他方の スーパーバイザ（アクティブ スーパーバイザ として動作するようになった方）のコンソール ポートに移動します。

利点

- スーパーバイザは、ハードウェア障害のシングルポイントではありません。アクティブ スーパーバイザ で永続的なハードウェア障害が発生すると、スタンバイ スーパーバイザ がシステムを回復し、ネットワーク サービスや信頼性のレベルを上げます。

- スタンバイ スーパーバイザ は、システム オペレータによる手動の介入なしでアクティブ スーパーバイザになることができます。このため、リカバリ時間が短縮され、ネットワーク管理者が即時対応する必要性が低下します。
- アクティブ スーパーバイザ は、システムが SSO に到達した後で、変更された構成と機能のデータをスタンバイ スーパーバイザ と動的に同期します。したがって、スタンバイ スーパーバイザ は、常にホット スタンバイとして動作し、引き継ぐ準備ができています。

スーパーバイザ冗長性の設定方法

Cisco cBR シャーシに 2 つのスーパーバイザが インストールされると、スーパーバイザ冗長性機能が自動的にイネーブルになります。アクティブ スーパーバイザは、スタンバイ スーパーバイザの起動時に、実行コンフィギュレーションファイルとスタンバイ スーパーバイザを自動的に同期します。

（注） Cisco cBR ルータでは SSO モードのスーパーバイザ 冗長性のみがサポートされます。デフォルトの冗長モードは SSO で、このモードに新しい設定は必要ありません。

この項の構成は、次のとおりです。

強制スイッチオーバー

スイッチオーバーを手動で強制するには、スタンバイ スーパーバイザがアクティブになるように、アクティブ スーパーバイザで特権 EXEC モードで **redundancy force-switchover** コマンドを使用します。手動による強制スイッチオーバーは、次の状況で役立ちます。

- 現在のアクティブ スーパーバイザを削除、交換、またはアップグレードする必要がある。
- 以前のスイッチオーバーでスタンバイ スーパーバイザがアクティブになっているため、以前のアクティブ スーパーバイザを復元したいと考えている。

ヒント アクティブ スーパーバイザを削除するだけでもスイッチオーバーはトリガーされますが、**redundancy force-switchover** コマンドを使用すると、ハードウェア アラームが生成されません。

はじめる前に

show redundancy コマンドを使用して、スタンバイ スーパーバイザが SSO 状態であることを確認します。詳細については、スーパーバイザ冗長性の確認, （132 ページ）を参照してください。

手順

ステップ 1 コンフィギュレーション レジスタを 0x02 に設定し、両方のスーパーバイザに適したイメージをロードします。

例：

```
Router# configure terminal
Router(config)# config-register 0x02
Router(config)# boot system bootflash:cbrsup-universalk9.2015-03-08_01.38_xxxxx.SSA.bin
```

（注） 以前のアクティブ スーパーバイザを設定して、ROM モニタ モードを維持したり、スイッチオーバー後に手動で起動したりする場合は、この手順を実行しないでください。

ステップ 2 スイッチオーバーを強制するには、**redundancy force-switchover** コマンドを使用します。

例：

```
Router# redundancy force-switchover

Proceed with switchover to standby RP? [confirm]
Manual Swact = enabled

Jan 1 19:23:22.483 R0/0: %PMAN-5-EXITACTION: Process manager is exiting: process exit with
 reload fru code

Initializing Hardware ...

System Bootstrap, Version 12.2(20141120:061458) [153], DEVELOPMENT SOFTWARE
Copyright (c) 1994-2014 by cisco Systems, Inc.
Compiled Thu 11/20/2014 18:04:24.91 by xxxxx
```

スタンバイ スーパーバイザ がアクティブ スーパーバイザ になります。

ステップ 3 （任意）ステップ 1, （126 ページ）を実行していない場合、スイッチオーバー後に以前のアクティブ スーパーバイザは ROM モニタ モードになります。以前のアクティブ スーパーバイザを新しいスタンバイ スーパーバイザにするには、新しいスタンバイ スーパーバイザを手動で起動し、SSO モードに移行します。

システム ブート動作の変更

ここでは、システムの起動時または再起動時のシステムの動作を変更するために Cisco IOS ソフトウェア コンフィギュレーション レジスタを変更する方法について説明します。ソフトウェア コンフィギュレーション レジスタは、起動に関する次の機能を制御する NVRAM 内の 16 ビット レジスタです。

- ロードする Cisco IOS ソフトウェア イメージのソースを指定します
- NVRAM メモリに保存されたコンフィギュレーション ファイルの内容を Cisco IOS ソフトウェアが無視する必要があるかどうかを指定します
- Break 機能の使用を有効または無効にします

ソフトウェア コンフィギュレーション レジスタの設定を変更するには、次の手順に従ってください。

手順

ステップ 1 グローバル コンフィギュレーション モードに移行し、**config-register** コマンドを使用して、ソフトウェア コンフィギュレーション レジスタの内容を新しい値に設定します。
次の表に示す値を使用して、新しい値を 16 ビット 16 進数ビットマスクとして指定します。

表 *10*：ソフトウェア コンフィギュレーション レジスタのビットの定義

ビット番号	16 進数	意味/機能
00 ～ 03	0x0000 ～ 0x000F	ルータの実行に必要なデフォルトの Cisco IOS ソフトウェア イメージのソースを定義します。 • 00：起動時に、システムは ROM モニタ プロンプト（rommon）のままで、ユーザが rommon **boot** コマンドを使用してシステムを手動で起動するのを待機します。 • 01：起動時に、システムは スーパーバイザ 上のフラッシュ メモリ Single In-line Memory Module（SIMM）にある最初のシステム イメージを自動的に起動します。 • 02 ～ 0F：起動時に、システムはネットワーク内の TFTP サーバに保存されたデフォルトの Cisco IOS ソフトウェア イメージから自動的に起動します。この設定の場合、スーパーバイザ 上でネットワーク管理イーサネット ポートを設定して有効にしてください。ポートが動作可能である必要があります。また、この設定により、boot system コマンドが有効になります。これは、デフォルト ファイル名をオーバーライドできます。
06	0x0040	システム ソフトウェアに NVRAM コンフィギュレーション ファイルの内容を無視させます。

ビット番号	16 進数	意味/機能
07	0x0080	Original Equipment Manufacturer（OEM）ビットを有効にします。
08	0x0100	30 秒後に Break 機能を無効にします。
09	0x0200	未使用。
10	0x0400	ブロードキャスト パケットの IP アドレスが 0.0.0.0 になるように指定します。
11 および 12	0x0800 ～ 0x1000	コンソール ボー レートを定義します（デフォルト値は 9600 ボーです）。
13	0x2000	ブート フラッシュ メモリからイメージを起動します。
14	0x4000	ブロードキャスト パケットがサブネット ブロードキャスト アドレスを使用する必要があることを指定します。
15	0x8000	診断メッセージを有効にして、NVRAM コンフィギュレーション ファイルの内容を無視します。

たとえば、ROM モニタ プロンプトを起動するようにルータを設定するには、次のコマンドを使用してコンフィギュレーション レジスタを **0x2100** に設定します。

例：

```
Router# config t
Router(config)# config-register 0x2100
Router(config)#
```

ヒント　通常使用での標準的なビットマスクは 0x2102 です。これは、ルータがフラッシュ メモリから Cisco IOS ソフトウェアを読み込んで Cisco IOS CLI プロンプトを起動する必要があることを指定します。Break キーが 30 秒間だけ有効になります。したがって、必要に応じて ROM モニタ プロンプトに切り替えることができます。

ステップ 2　グローバル コンフィギュレーション モードを終了します。

例：

```
Router(config)# exit
Router#
```

ステップ 3 **show version** コマンドを使用して、新しいソフトウェア コンフィギュレーション レジスタの設定を表示します。
最後の行には、コンフィギュレーション レジスタの設定が表示されます。

例：

```
Router# show version
Cisco IOS XE Software, Version 2015-03-04_00.38_xxxxx
Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Experimental  \
Version 15.5(20150302:044048) [v155_2_s_xe315_throttle-xxxxx-XE315_0301 121]
This software is an Engineering Special
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 04-Mar-15 00:21 by xxxxx


Cisco IOS-XE software, Copyright (c) 2005-2015 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

Router uptime is 14 minutes
Uptime for this control processor is 17 minutes
System returned to ROM by SSO Switchover
System image file is "bootflash:cbrsup-universalk9.2015-03-04_00.38_xxxxx.SSA.bin"
Last reload reason: Reload Command



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

cisco cBR1013 (CBR) processor (revision CBR) with 3647635K/6147K bytes of memory.
Processor board ID CSJ13152101
16 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
50331648K bytes of physical memory.
7739391K bytes of eUSB flash at bootflash:.
97620247K bytes of SATA hard disk at harddisk:.
979258K bytes of USB flash at usb1:.

Configuration register is 0x2
```

コンフィギュレーション レジスタを変更する場合、**show version** コマンドを使用すると、レジスタの現在の値および次回の再起動/リロード時に使用される値が表示されます。

ステップ 4 新しいソフトウェア コンフィギュレーション レジスタ設定をコンフィギュレーション ファイルに保存するには、次のいずれかを実行します。

- **copy running-config startup-config** コマンドを使用します。
- **write** コマンドを使用します。

例：

```
Router# copy running-config startup-config

Router# write
Building configuration...
[OK]
```

ステップ 5 ソフトウェアコンフィギュレーションレジスタの変更は、ルータを次回リブートまたは再起動した場合に適用されます。ルータを手動でリブート（再起動）するには、**reload** コマンドを使用します。

例：

```
Router# reload
System configuration has been modified. Save? [yes/no]: yes
Proceed with reload? [confirm]
```

ブートフラッシュまたはハードディスクへのコンフィギュレーションファイルの保存

ここでは、コンフィギュレーションファイルをブートフラッシュまたはハードディスクにコピーし、Cisco cBR ルータを設定する方法について説明します。

手順

ステップ 1 両方のスーパーバイザのブートフラッシュまたはハードディスクにコンフィギュレーションファイルをコピーします。

例：

```
Router# copy running-config bootflash:cbr8-config
Router# copy running-config stby-bootflash:cbr8-config
Router# copy running-config harddisk:cbr8-config
Router# copy running-config stby-harddisk:cbr8-config
```

ステップ 2 （任意） コンフィギュレーション ファイルが TFTP サーバに格納されている場合は、TFTP サーバのファイルを各スーパーバイザのブートフラッシュまたはハード ディスクにコピーします。

例：
```
Router# copy tftp://192.168.100.10/router-config bootflash:cbr8-config
Router# copy tftp://192.168.100.10/router-config stby-bootflash:cbr8-config
Router# copy tftp://192.168.100.10/router-config harddisk:cbr8-config
Router# copy tftp://192.168.100.10/router-config stby-harddisk:cbr8-config
```

スーパーバイザ冗長性の設定の確認

ここでは、次の内容について説明します。

スーパーバイザ冗長性の確認

手順

ステップ 1 スタートアップ コンフィギュレーションを表示して、冗長性を構成するための回線の有無を確認します。

例：
```
Router# show startup-config

...
redundancy
mode sso
...
```

ステップ 2 **show redundancy** コマンドを実行して、スーパーバイザの現在の冗長性の状態を確認します。通常、アクティブなスーパーバイザはスロット 4（SUP0）に表示されます。
```
Router# show redundancy

Redundant System Information :
------------------------------
Available system uptime = 28 minutes
Switchovers system experienced = 0
Standby failures = 0
Last switchover reason = none

Hardware Mode = Duplex
Configured Redundancy Mode = sso
Operating Redundancy Mode = sso
Maintenance Mode = Disabled
Communications = Up

Current Processor Information :
-------------------------------
Active Location = slot 4
Current Software state = ACTIVE
Uptime in current state = 28 minutes
```

```
Image Version = Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Experimental Version 15.5(20150302:044048) [v155_2_s_xe315_throttle-xxxxx-XE315_0301 121]
This software is an Engineering Special
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 04-Mar-15 00:21 by xxxxx
BOOT = bootflash:cbrsup-universalk9.2015-03-04_00.38_xxxxx.SSA.bin,12;
CONFIG_FILE = bootflash:startup_config1419513118
Configuration register = 0x2

Peer Processor Information :
----------------------------
Standby Location = slot 5
Current Software state = STANDBY HOT
Uptime in current state = 24 minutes
Image Version = Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Experimental Version 15.5(20150302:044048) [v155_2_s_xe315_throttle-xxxxx-XE315_0301 121]
This software is an Engineering Special
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 04-Mar-15 00:21 by xxxxx
BOOT = bootflash:cbrsup-universalk9.2015-03-04_00.38_xxxxx.SSA.bin,12;
CONFIG_FILE = bootflash:startup_config1419513118
Configuration register = 0x2
```

スイッチオーバーが発生した場合、**show redundancy** コマンドにより、アクティブなスーパーバイザのスロットがスロット 4（SUP0）からスロット 5（SUP1）に変更されたことが示されます。出力は次の例のようになります。

```
Router# show redundancy

Redundant System Information :
------------------------------
Available system uptime = 39 minutes
Switchovers system experienced = 1
Standby failures = 0
Last switchover reason = user forced

Hardware Mode = Duplex
Configured Redundancy Mode = sso
Operating Redundancy Mode = sso
Maintenance Mode = Disabled
Communications = Up

Current Processor Information :
-------------------------------
Active Location = slot 5
Current Software state = ACTIVE
Uptime in current state = 10 minutes
Image Version = Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Experimental Version 15.5(20150302:044048) [v155_2_s_xe315_throttle-xxxxx-XE315_0301 121]
This software is an Engineering Special
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 04-Mar-15 00:21 by xxxxx
BOOT = bootflash:cbrsup-universalk9.2015-03-04_00.38_xxxxx.SSA.bin,12;
CONFIG_FILE = bootflash:startup_config1419513118
Configuration register = 0x2
```

```
Peer Processor Information :
----------------------------
Standby Location = slot 4
Current Software state = STANDBY HOT
Uptime in current state = 4 minutes
Image Version = Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Experimental Version 15.5(20150302:044048) [v155_2_s_xe315_throttle-xxxxx-XE315_0301 121]
This software is an Engineering Special
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 04-Mar-15 00:21 by xxxxx
BOOT = bootflash:cbrsup-universalk9.2015-03-04_00.38_xxxxx.SSA.bin,12;
CONFIG_FILE = bootflash:startup_config1419513118
Configuration register = 0x2
```

スタンバイのスーパーバイザが未設置または非稼動の場合、**show redundancy** コマンドの出力は次の例のようになります。

```
Router# show redundancy

Redundant System Information :
------------------------------
Available system uptime = 31 minutes
Switchovers system experienced = 1
Standby failures = 0
Last switchover reason = user forced

Hardware Mode = Simplex
Configured Redundancy Mode = sso
Operating Redundancy Mode = Non-redundant
Maintenance Mode = Disabled
Communications = Down Reason: Failure

Current Processor Information :
-------------------------------
Active Location = slot 5
Current Software state = ACTIVE
Uptime in current state = 2 minutes
Image Version = Cisco IOS Software, IOS-XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Experimental Version 15.5(20150302:044048) [v155_2_s_xe315_throttle-xxxxx-XE315_0301 121]
This software is an Engineering Special
Copyright (c) 1986-2015 by Cisco Systems, Inc.
Compiled Wed 04-Mar-15 00:21 by xxxxx
BOOT = bootflash:cbrsup-universalk9.2015-03-04_00.38_xxxxx.SSA.bin,12;
CONFIG_FILE = bootflash:startup_config1419513118
Configuration register = 0x2

Peer (slot: 4) information is not available because it is in 'DISABLED' state
```

show redundancy コマンドでは、冗長性の状態、ソフトウェアの状態、システム稼働時間、イメージ バージョン、起動、コンフィギュレーション ファイル、およびコンフィギュレーション レジスタに関する詳細情報が表示されます。

スーパーバイザ スイッチオーバーの確認

手順

ステップ 1 スーパーバイザ カードの LED を確認します。
スーパーバイザがアクティブになると、スーパーバイザ カードの RP ACT および FP ACT LED が緑に点灯し、初期化が完了してアクティブ スーパーバイザとして機能していることを示します。スタンバイ スーパーバイザ カードの RP ACT および FP ACT はオフです。詳細は、「Monitoring the Supervisor in the Cisco cBR Chassis」を参照してください。

ステップ 2 スーパーバイザ スイッチオーバーを確認するために、**show redundancy switchover history** コマンドを実行します。
元のスーパーバイザがスロット 4（SUP0）にあり、スタンバイ スーパーバイザがスロット 5（SUP1）にある場合、出力は次の例のようになります。

例：

```
Router# show redundancy switchover history

Index Previous Current Switchover Switchover
      active   active  reason     time
----- -------- ------- ---------- ----------
1     48       49      user forced 19:23:11 CST Sun Jan 1 2012
```

値 48 は SUP0 を、49 は SUP1 を示しています。

スーパーバイザ冗長性の後に、メッセージが表示されます。次はその例です。

```
CLC 3/0: May 20 07:26:01.992: %CBR-4-RECONCL_CM_FINISH_CLC: Reconciliation (cdm->ios) for
slot 3 finished: total 7, success 5, failed 2, ios-only 2, cdm-only 0, mismatch 0, offline
 0, in-transaction-reconl 0, in-transaction-recover 0.
```

表 *11*：メッセージの説明

名前	説明
total	フェールオーバー前の各ライン カード上のケーブル モデムの合計数。
success	フェールオーバー時にオンライン状態を維持したケーブル モデムの数を示します。
failed	調整チェックに失敗してデータベースから削除されたケーブル モデムの数を示します。
ios-only	ライン カード IOSd のみにデータ エントリがある、データベースから削除されたケーブル モデムの数を示します。

名前	説明
cdm-only	ライン カード CDMAN（US スケジューラ）のみにデータ エントリがある、データベースから削除されたケーブル モデムの数を示します。
mismatch	フェールオーバー後にモデム インスタンス内またはサービス フロー内でデータ不一致があるケーブル モデムの数を示します。これらのモデムはすでにデータベースから削除されています。
offline	フェールオーバー時にオフラインになったケーブル モデムの数を示します。
in-transaction-reconl	フェールオーバー時に in dsx 操作により削除されたケーブル モデムの数を示します。
in-transaction-recove	フェールオーバー時に in dsx 操作中であったケーブル モデムの数を示します。

スーパーバイザ冗長性の設定例

次の例では、Cisco IOS コンフィギュレーション ファイルの中で、スーパーバイザ冗長性機能のデフォルト設定に関する部分を記載します。ほとんどのアプリケーションには、この設定を使用できます。

```
Router# show running-config | sec redundancy

redundancy
 mode sso

Router#
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
CMTS コマンド	『Cisco IOS CMTS Cable Command Reference』
ステートフル スイッチオーバー	『Stateful Switchover』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

スーパーバイザ冗長性に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *12*：スーパーバイザ冗長性に関する機能情報

機能名	リリース	機能情報
スーパーバイザ の冗長性	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 7 章

ライン カード冗長性

ライン カードは冗長方式の高可用性をサポートします。ライン カード冗長性により、局所的なシステム障害が発生した場合に堅牢な自動スイッチオーバーおよびリカバリを可能にすることで、顧客宅内機器（CPE）のダウンタイムを制限することができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *13* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

ライン カード冗長性の前提条件

- 少なくとも 1 つの RF Through PIC とその対応するインターフェイス ライン カードが、プライマリ カードとして設定されるシャーシにインストールされている必要があります。

- RF Protect PIC とその対応するインターフェイス ライン カードが、セカンダリ カードとして設定されるシャーシにインストールされている必要があります。

ライン カード冗長性の制限事項

- Cisco cBR-8 ルータのスロット 3 およびスロット 6 にインストールされたラインカードをセカンダリ カードとして設定することはできません。
- RF Protect PIC は、（より大きいスロット番号を持つ）下部スロットにのみ RF 信号を送信できます。したがって、セカンダリ カードのスロット番号は、冗長グループの中で最小の番号である必要があります。

（注） シャーシの最上部スロット（スロット 0）に RF Protect PIC をインストールし、これをセカンダリ カードとして設定することをお勧めします。

- RF Through PIC は、上部スロットから下部スロットにのみ RF 信号を送信できます。したがって、セカンダリ カードとプライマリ カードの間にはいかなる RF Blank PIC もインストールしないでください。
- セカンダリ カードがアクティブなときにプライマリまたはセカンダリ カードの設定を変更することはできません。
- 冗長グループ内にセカンダリ カードがある場合は、最後のプライマリ カードを削除することはできません。セカンダリ カードを削除してから、プライマリ カードを削除する必要があります。
- プライマリ カードのロールが standby の場合は、プライマリ カードに戻してから、冗長グループから削除する必要があります。

ライン カード冗長性の情報

ラインカードの冗長性は予定外のダウンタイムを短縮します。ライン カード冗長性を設定すると、ルータ上に保護ゾーン（冗長グループ）が作成され、プライマリ カードとセカンダリ カードの設定が同期されます。

次のイベントにより、アクティブ カードからスタンバイ カードへのスイッチオーバーをトリガーできます。

- **redundancy linecard-group switchover from slot** *slot* コマンドを使用した手動スイッチオーバー。
- **hw-module slot reload** コマンドを使用したライン カードのリロード。
- ライン カードのクラッシュ。
- ラインカードの活性挿抜（OIR）。

セカンダリ カードは、スイッチオーバー後、リロードを実行します。ライン カードの OIR またはクラッシュによってトリガーされた予定外のスイッチオーバー後、プライマリ カードがホットスタンバイになった場合、自動的にプライマリ カードに戻るようルータを設定することができます。

次に、ラインカードの冗長性の状態を示します。

- **Unavail**：ラインカードは使用できない状態です。
- **Init**：ラインカードは起動していません。
- **Active Cold**：アクティブ カードが設定をダウンロード中です。
- **Active**：アクティブ カードは設定が完了し動作中です。
- **Stdby Cold**：スタンバイ カードの設定はアクティブ カードと同期されています。
- **Stdby Warm**：（セカンダリ カードのみ）スタンバイカードは完全に同期され、スイッチオーバーの準備ができています。これはセカンダリ スタンバイ カードが安定している状態です。
- **Stdby Hot**：プライマリ スタンバイ カードは完全に同期されています。これはプライマリ スタンバイ カードが安定している状態です。プライマリ カードとスイッチオーバーするセカンダリ スタンバイ カードは選択されており、すぐにアクティブになります。これはセカンダリ カードがアクティブになる移行状態です。

N+1 ライン カード冗長性

Cisco cBR-8 ルータはラインカードの N+1 冗長方式をサポートします。単一の RF Protect PIC を複数の RF Through PIC（プライマリ カード）に対するセカンダリ カードとし設定できます。この冗長方式では、セカンダリ カードがプライマリ カードに対してアクティブなカードになると、冗長方式が 1+1 冗長性に変更されます。

Cisco cBR-8 ルータは単一の保護ゾーンまたは冗長グループ（グループ 0）をサポートします。

ラインカード冗長性の設定方法

この項の構成は、次のとおりです。

ライン カードの手動スイッチオーバーの設定

はじめる前に

ライン カードは、アクティブ ロールのウォーム スタンバイ状態またはホット スタンバイ状態である必要があります。カードのロールと状態を確認するには、**show redundancy linecard all** コマンドを使用します。

制限事項

- スタンバイ スーパーバイザは起動しているけれども、SSO はまだ開始されていない場合、手動スイッチオーバーは実行できません。

- 手動で開始したスイッチオーバーは自動復帰できません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**redundancy linecard-group switchover from slot** *slot* 例： `Router# redundancy linecard-group switchover from slot 9`	アクティブなラインカードから手動スイッチオーバーを行います。

N+1 ラインカード冗長性の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**redundancy** 例： `Router(config)# redundancy`	冗長性をイネーブルにし、冗長性コンフィギュレーション モードを開始します。
ステップ 4	**linecard-group** *group-id***internal-switch** 例： `Router(config-red)# linecard-group 0 internal-switch`	冗長グループを設定し、ライン カードの冗長性コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**description** *group-description* 例： `Router(config-red-lc)# description RedundancyGroup0`	（任意）冗長グループの説明を設定します。
ステップ 6	**class 1:N** 例： `Router(config-red-lc)# class 1:N`	冗長グループの N+1 冗長性クラスを設定します。
ステップ 7	**revertive** *seconds* 例： `Router(config-red-lc)# revertive 60`	（任意）プライマリ カードの自動復帰時間を秒単位で設定します。
ステップ 8	**member slot** *slot***primary** 例： `Router(config-red-lc)# member slot 1 primary`	冗長グループにライン カードをプライマリ カードとして追加します。 （注） 冗長グループに追加するプライマリ カードごとに、この手順を繰り返してください。
ステップ 9	**member slot** *slot***secondary** 例： `Router(config-red-lc)# member slot 0 secondary`	冗長グループにライン カードをプライマリ カードとして追加します。
ステップ 10	**end** 例： `Router(config-red-lc)# end`	特権 EXEC モードに戻ります。

ライン カード冗長性の設定の確認

- **show redundancy linecard group all**：冗長グループ情報を表示します。

  次に、このコマンドの出力例を示します。

```
Router# show redundancy linecard group all

Group Identifier: 0
Revertive, Revert Timer: OFF (60000 sec)
Reserved Cardtype: 0xFFFFFFFF  4294967295
Group Redundancy Type: INTERNAL SWITCH
Group Redundancy Class: 1:N
Group Redundancy Configuration Type: LINECARD GROUP
Primary: Slot 6
Primary: Slot 7
```

```
Secondary: Slot 0
```

- **show redundancy linecard all**：すべてのライン カードのロールと状態の情報を表示します。

  次に、このコマンドの出力例を示します。

```
Router# show redundancy linecard all

               LC     My         Peer       Peer     Peer
Slot Subslot   Group  State      State      Slot     Subslot  Role     Mode
------------------------------------------------------------------------------
 9   -         0      Active     Stdby Cold 0        -        Active   Primary
 8   -         0      Active     Stdby Warm 0        -        Active   Primary
 7   -         0      Active     Stdby Warm 0        -        Active   Primary
 6   -         0      Active     Stdby Cold 0        -        Active   Primary
 3   -         0      Active     Stdby Cold 0        -        Active   Primary
 2   -         0      Active     Stdby Cold 0        -        Active   Primary
 1   -         0      Active     Stdby Cold 0        -        Active   Primary
 0   -         0      -          -          Multiple None     Standby  Secondary
```

（注） セカンダリ カードのロールが *Standby* である場合、複数 のプライマリ カードのピアとなっているため、セカンダリ カードの有効な *My State* はありません。セカンダリ カードには複数 のピア状態あります。たとえば、いくつかのプライマリ カードはコールド スタンバイで、他のプライマリ カードはウォーム スタンバイです。

次に、セカンダリ カードがプライマリ カードに対してアクティブになり、N+1 冗長性が 1+1 冗長性に変化した場合のコマンドの出力例を示します。

```
Router# show redundancy linecard all

               LC     My         Peer       Peer     Peer
Slot Subslot   Group  State      State      Slot     Subslot  Role     Mode
------------------------------------------------------------------------------
 9   -         0      Stdby Hot  Active     0        -        Standby  Primary
 8   -         0      Active     Unavail    0        -        Active   Primary
 7   -         0      Active     Unavail    0        -        Active   Primary
 6   -         0      Active     Unavail    0        -        Active   Primary
 3   -         0      Active     Unavail    0        -        Active   Primary
 2   -         0      Active     Unavail    0        -        Active   Primary
 1   -         0      Active     Unavail    0        -        Active   Primary
 0   -         0      Active     Stdby Hot  9        -        Active   Secondary
```

- **show redundancy linecard slot**：ラインカードの冗長性に関する情報を表示します。

  次に、コマンドの出力例を示します。

```
Router# show redundancy linecard slot 9

 LC Redundancy Is Configured:
 LC Group Number: 0
 LC Slot: 9 (idx=9)
 LC Peer Slot: 0
 LC Card Type: 0x4076 , 16502
 LC Name: 9
 LC Mode: Primary
 LC Role: Active
 LC My State: Active
 LC Peer State: Stdby Warm
```

- **show redundancy linecard history**：すべてのライン カードの状態変更履歴を表示します。

次に、コマンドの出力例を示します。

```
Router# show redundancy linecard history

Jan 05 2012 12:24:27 20559 - st_mem(9): MY State Change, (Active Wait) -> (Active)
Jan 05 2012 12:24:27 20559 - st_mem(9): MY FSM execution, Active Wait:Init:State Ntfy
Jan 05 2012 12:24:27 20559 - st_mem(9): MY State Change, (Active LC Cfg Dnld) -> (Active
 Wait)
Jan 05 2012 12:24:27 20559 - st_mem(9): MY FSM execution, Active LC Cfg Dnld:Init:Cfg
 Dnld Done
Jan 05 2012 12:24:27 20559 - st_mem(9): MY State Change, (Active Cold) -> (Active LC
Cfg Dnld)
Jan 05 2012 12:23:09 12763 - st_mem(9): MY FSM execution, Active Cold:Init:Cfg Dnld
Jan 05 2012 12:23:09 12760 - st_mem(9): MY State Change, (Init) -> (Active Cold)
Jan 05 2012 12:23:09 12760 - st_mem(9): MY FSM execution, Init:Init:Up
Jan 05 2012 12:21:39 3746 - st_mem(9): PEER FSM Execution , Init:Init:Reset
```

- **show lcha rfsw**：内部 RF スイッチ PIC の状態情報を表示します。

  次に、コマンドの出力例を示します。

```
Router# show lcha rfsw

Slot 0 ===================================
Type : Secondary PIC State: normal
Slot 1 ===================================
Type : Primary PIC State: normal
```

- **show lcha logging level**：ケーブル モデム ライン カードのログを表示します。

  次に、コマンドの出力例を示します。

```
Router# show lcha logging level noise

11:02:03.313 CST Tue Nov 18 2014 [error] [slot=3] [txn=229] Peer-Up Message [tag=1011]
 to slot 3 complete [36144 ms]; status=nak response
11:02:03.313 CST Tue Nov 18 2014 [error] [slot=0] [txn=229] Slot 0 downloaded
configuration for slot 3; result=peer-up notification failed
11:02:03.316 CST Tue Nov 18 2014 [noise] [slot=0] [txn=none]
lcha_plfm_get_max_port_count_for_slot: slot 0 maximum port count is 1794
11:02:03.316 CST Tue Nov 18 2014 [noise] [slot=0] [txn=none]
lcha_plfm_get_starting_port_index: slot 0 starting port count is 0
11:02:03.331 CST Tue Nov 18 2014 [note]  [slot=0] [txn=none] Slot 0 is being reset
11:02:04.352 CST Tue Nov 18 2014 [note]  [slot=0] [txn=none] slot 0 removed
```

- セカンダリ カードがアクティブである場合、**show** コマンドでプライマリ カードまたはセカンダリ カードのスロット番号を使用できます。

  次に、スロット 8 のプライマリ カードがスロット 0 のセカンダリ カードに切り替わった後の、**show interfaces** コマンドの出力例を示します。

```
Router# show interfaces c0/0/0

Cable0/0/0 is up, line protocol is up
  Hardware is CMTS MD interface, address is 0000.0000.031e (bia 0000.0000.031e)
  MTU 1500 bytes, BW 26000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation MCNS, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 19500 kilobits/sec
```

```
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 13000 bits/sec, 17 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     140520 packets output, 14052672 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out

Router# show interfaces c8/0/0

Cable0/0/0 is up, line protocol is up
  Hardware is CMTS MD interface, address is 0000.0000.031e (bia 0000.0000.031e)
  MTU 1500 bytes, BW 26000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation MCNS, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
     Available Bandwidth 19500 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 14000 bits/sec, 18 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     140616 packets output, 14062272 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

- セカンダリ カードがアクティブである場合、**show running-config** コマンドにより、セカンダリ カードの出力が表示されます。

（注） セカンダリ カードがアクティブの場合、**show running-config** コマンドの出力は、プライマリ カードに関しては空になります。

次に、スロット 8 のプライマリ カードがスロット 0 のセカンダリ カードに切り替わった後の、**show running-config** コマンドの出力例を示します。

```
Router# show running-config | begin controller Upstream-Cable 0

controller Upstream-Cable 0/0/0
 us-channel 0 channel-width 1600000 1600000
 us-channel 0 docsis-mode atdma
 us-channel 0 minislot-size 4
 us-channel 0 modulation-profile 221
 no us-channel 0 shutdown
 us-channel 1 channel-width 1600000 1600000
 us-channel 1 docsis-mode atdma

Router# show running-config | begin controller Upstream-Cable 8
Router#
Router#
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
CMTS コマンド	『Cisco CMTS Cable Command Reference』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

ライン カード冗長性に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *14*：ライン カード冗長性に関する機能情報

機能名	リリース	機能情報
ライン カード冗長性	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 III 部

レイヤ 2 および DOCSIS 3.0 構成

第 8 章

ダウンストリーム インターフェイス設定

このマニュアルでは、 Cisco cBR シリーズ コンバージド ブロードバンド ルータ上のダウンストリーム インターフェイスを設定する方法について説明します。

機能情報の確認

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *15* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

ダウンストリーム インターフェイス設定に関する情報

概要

- 各ダウンストリーム ポートは、ポート レベルの設定とチャネル レベルの設定が必要です。ポート レベルの設定は、ポートで使用できる周波数の範囲を定義する周波数プロファイルで最適化されています。チャネル レベルの設定は、QAM プロファイルおよびチャネル範囲の設定ブロックで最適化されます。この設定ブロックは、周波数を自動的に増加し、Annex、変調、インターリーバを複製します。
- 各チャネルには、周波数、Annex、変調、インターリーバ、およびDOCSIS チャネル ID という一連のパラメータが必要です。
- 設定は、4 つの主要な設定ブロックで行われます。
  - QAM プロファイル：例：「cable downstream qam-profile 1」
  - 周波数プロファイル：例：「cable downstream freq-profile 2」
  - ポート/コントローラ：例：「controller Integrated-Cable 3/0/0」
  - RF チャネル ブロック：例：「rf-chan 0 31」

ダウンストリーム RF ポートとチャネル管理

ダウンストリーム RF ポートとチャネル機能は、ダウンストリーム RF ポートとチャネルの設定と監視を行います。各ダウンストリーム RF チャネルは、DOCSIS または従来の MPEG ビデオ QAM チャネルとしてプロビジョニングできます。

QAM プロファイル

QAM プロファイルは物理層パラメータとも呼ばれる共通ダウンストリーム チャネル モジュレータ設定を記述します。これには、QAM コンステレーション、シンボル レート、インターリーバ深度、スペクトル反転、およびAnnex が含まれます。QAM プロファイルは *CCAP DownPhyParams* オブジェクトによって記述されます。デフォルトの QAM プロファイルが DOCSIS または MPEG ビデオ用にサポートされ、カスタマイズされます。それぞれ *DocsisPhyDefault* オブジェクトおよび *VideoPhyDefault* オブジェクトとして記述されます。

最大 32 個の QAM プロファイルを定義できます。4 つのシステム定義 QAM プロファイル（0 ～ 3）があり、これらは削除または変更できません。プロファイル 4 ～ 31 を定義できます。

システム定義プロファイルは次のとおりです。

- プロファイル 0：default-annex-b-64-qam
  - インターリーバ深度：I32-J4
  - シンボル レート：5057 キロ シンボル/秒
  - スペクトル反転：オフ

- プロファイル 1：default-annex-b-256-qam
  - インターリーバ深度：I32-J4
  - シンボル レート：5361 キロ シンボル/秒
  - スペクトル反転：オフ
- プロファイル 2：default-annex-a-64-qam
  - インターリーバ深度：I12-J17
  - シンボル レート：6952 キロ シンボル/秒
  - スペクトル反転：オフ
- プロファイル 3：default-annex-a-256-qam
  - インターリーバ深度：I12-J17
  - シンボル レート：6952 キロ シンボル/秒
  - スペクトル反転：オフ

周波数プロファイル

周波数プロファイルは、ポートで使用できる周波数の範囲を定義します。最大16個の周波数プロファイルを定義できます。4 つのシステム定義周波数プロファイル（0 ～ 3）があり、これらは削除または変更できません。プロファイル 4 ～ 15 を定義できます。

システム定義プロファイルは次のとおりです。

- プロファイル 0：annex-b-low、周波数範囲（Hz）：90000000 ～ 863999999
- プロファイル 1：annex-b-high、周波数範囲（Hz）：234000000 ～ 1002999999
- プロファイル 2：annex-a-low、周波数範囲（Hz）：94000000 ～ 867999999
- プロファイル 3：annex-a-high、周波数範囲（Hz）：267000000 ～ 1002999999

周波数範囲はレーンおよびブロックを使用して定義されます。

- ポートあたり 4 つのレーンがあり、各レーンは 216 MHz 範囲をサポートできます。
- レーンあたり 4 つのブロックがあり、各ブロックは 54 MHz 範囲をサポートできます。
- レーンとブロックは、周波数範囲が重複することがあります。

ダウンストリーム インターフェイスの設定方法

この項の構成は、次のとおりです。

設定モードを使用した Cisco CMTS の手動設定

コンソール端末を I/O コントローラのコンソール ポートに接続します。初期ダイアログを開始するかどうかの質問に対して、no と応答し、ルータのユーザ動作モードを開始します。数秒後にユーザ EXEC プロンプト（**Router>**）が表示されます。

ダウンストリーム チャネルの QAM プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 downstream qam-profile** *Qam_Profile_ID* 例： `Router(config)# cable downstream qam-profile 3`	QAM プロファイルを定義または変更します。
ステップ 4	**annex** {**A** | **B** | **C**} 例： `Router(config-qam-prof)# annex A`	プロファイル MPEG フレーミング形式を定義します。デフォルトは Annex B です。
ステップ 5	**description** *LINE* 例： `Router(config-qam-prof)# description qam1`	このプロファイルの名前または説明。
ステップ 6	**interleaver-depth** {**I12-J17** | **I128-J1** | **I128-J2** | **I128-J3** | **I128-J4** | **I128-J5** | **I128-J6** | **I128-J7** | **I128-J8** | **I16-J8** | **I32-J4** | **I64-J2** | **I8-J16**} 例： `Router(config-qam-prof)# interleaver-depth I64-J2`	インターリーブ深度を定義します。DOCSIS のデフォルトは I32 J4 です。

	コマンドまたはアクション	目的
ステップ 7	**modulation** {**256** | **64**} 例： `Router(config-qam-prof)# modulation 64`	変調を定義します。デフォルトは256QAM です。
ステップ 8	**spectrum-inversion** {**off** | **on**} 例： `Router(config-qam-prof)# spectrum-inversion on`	スペクトル反転を有効または無効にします。デフォルトはオフです。
ステップ 9	**symbol-rate** *value* 例： `Router(config-qam-prof)# symbol-rate 5057`	シンボル レートを定義します。値はキロ シンボル/秒で表されます。
ステップ 10	**exit** 例： `Router(config-qam-prof)# exit`	QAM プロファイル コンフィギュレーション モードを終了します。

ダウンストリーム チャネルの周波数プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 downstream freq-profile** *DS_frequency_profile_ID* 例： `Router(config)# cable downstream freq-profile 4`	周波数プロファイルを定義または変更します。

	コマンドまたはアクション	目的
ステップ 4	**lane** *lane_id***start-freq** *start_freq_value* 例： `Router(config-freq-prof)# lane 1 start-freq 90000000`	周波数レーンを定義します。

ステップ 5	**block** *block_id***start-freq** *bl_start_freq_value*
	
	例：
	
	`Router(config-freq-prof-lane)#block 1 start-freq 90000000`
	`Router(config-freq-prof-lane)#`
		レーンの周波数ブロックを設定します。

ステップ 6	**exit** 例： `Router(config-freq-prof-lane)# exit`	周波数レーン コンフィギュレーション モードを終了します。

ダウンストリーム チャネルのコントローラの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**controller integrated-cable** *slot*/*subslot*/*port* 例： `Router(config)#controller Integrated-Cable 3/0/0`	コントローラ サブモードを開始します。
ステップ 4	**base-channel-power** *value* 例： `Router(config-controller)#base-channel-power 26`	基本チャネルの電力レベルを設定します。指定しない場合、デフォルト値はキャリアの数に基づいて計算されます。最大値は 34 dBmV DRFI です。DRFI で指定された最大値よりも

	コマンドまたはアクション	目的
		大きい値を設定すると、次のメッセージが表示されます。 Caution: RF Power above DRFI specification.May result in minor fidelity degradation.
ステップ 5	**freq-profile** *number* 例： `Router(config-controller)#freq-profile 0`	ポートの周波数プロファイルを指定します。
ステップ 6	**max-carrier** *value* 例： `Router(config-controller)#max-carrier 1`	キャリアの最大数を指定します。
ステップ 7	**mute** 例： `Router(config-controller)#mute`	ポートをミュート設定します。ポートのミュートを解除するには、**no** プレフィックスを使用します。デフォルトは「no mute」です。
ステップ 8	**rf-chan** *starting_Qam_ID ending_Qam_ID* 例： `Router(config-controller)#rf-chan 0 1`	RF チャネル コンフィギュレーション サブモードを開始し、個別のチャネルまたはチャネルのブロックを設定します。
ステップ 9	**shutdown** 例： `Router(config-controller)#shutdown`	ポートの管理状態を down に変更します。ポートの管理状態を up に変更するには、**no** プレフィックスを使用します。

コントローラの RF チャネルの設定

RF チャネル サブモードを開始するには、前の項で説明したようにチャネル コントローラ コンフィギュレーション サブモードで **rf-chan** コマンドを使用します。個々のチャネルを **rf-chan** コマンドで指定した場合は、そのチャネルの設定だけが変更されます。チャネルのブロックを **rf-chan** コマンドで指定した場合、そのブロック内のすべてのチャネルに設定変更が適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**docsis-channel-id** *dcid* 例： `Router(config-rf-chan)#docsis-channel-id 1`	チャネルの DOCSIS チャネル ID を変更します。ブロック モードでは、値が最初のチャネルに割り当てられ、連続するチャネルごとに増えていきます。
ステップ 2	**frequency** *value* 例： `Router(config-rf-chan)#frequency 93000000`	チャネルの中心周波数を Hz で設定します。ポートの周波数プロファイルを設定している場合は、利用可能な周波数範囲がこのプロファイルにより決まります。設定していない場合、利用可能な範囲はすべてのポートのスペクトルになります。ブロック モードでは、周波数が最初のチャネルに割り当てられます。連続するチャネルには、QAMプロファイルで指定した Annex の次の中心周波数が設定されます（Annex B の場合は +6 Hz、Annex A の場合は +8 Hz）。
ステップ 3	**mute** 例： `Router(config-rf-chan)#mute`	RF チャネルをミュートにします。チャネルのミュートを解除するには、**no** プレフィックスを入力します。デフォルトは「no mute」です。
ステップ 4	**power-adjust** *pwr_adj_range* 例： `Router(config-rf-chan)#power-adjust 8.0 - 0.0 dBmV`	RF チャネルの出力を調整します。
ステップ 5	**qam-profile** *qam_profile_number* 例： `Router(config-rf-chan)#qam-profile 0`	このチャネルの QAM プロファイルを指定します。
ステップ 6	**rf-output** *value* 例： `Router(config-rf-chan)#rf-output normal`	チャネルをテストするには、RF 出力モードを変更します。
ステップ 7	**shutdown** 例： `Router(config-rf-chan)#shutdown`	チャネルの管理状態を down に変更します。チャネルの管理状態を up に変更するには、**no** プレフィックスを使用します。デフォルトは「no shut」です。

	コマンドまたはアクション	目的
ステップ 8	**type** *value* 例： `Router(config-rf-chan)#type video`	チャネルの QAM タイプを設定します。デフォルトは DOCSIS です。

設定例

ダウンストリーム インターフェイスの設定例

次に、以下の設定例を示します。

- QAM プロファイル：Annex B と 256 QAM のシステム定義 QAM プロファイル。
- 周波数プロファイル：システム定義周波数プロファイル annex-b-low。
- コントローラと RF チャネル：周波数プロファイル 0 でスロット 3/0 のポート 0、QAM プロファイル 1 で 96 チャネル、93 MHz で始まる中心周波数。

```
cable downstream qam-profile 1
  annex B
  modulation 256
  interleaver-depth I32-J4
  symbol-rate 5361
  spectrum-inversion off
  description default-annex-b-256-qam
cable downstream freq-profile 0
  lane 1 start-freq 90000000
    block 1 start-freq 90000000
    block 2 start-freq 138000000
    block 3 start-freq 186000000
    block 4 start-freq 234000000
  lane 2 start-freq 282000000
    block 1 start-freq 282000000
    block 2 start-freq 330000000
    block 3 start-freq 378000000
    block 4 start-freq 426000000
  lane 3 start-freq 474000000
    block 1 start-freq 474000000
    block 2 start-freq 522000000
    block 3 start-freq 570000000
    block 4 start-freq 618000000
  lane 4 start-freq 666000000
    block 1 start-freq 666000000
    block 2 start-freq 714000000
    block 3 start-freq 762000000
    block 4 start-freq 810000000
controller Integrated-Cable 3/0/0
 max-carrier 128
 base-channel-power 34
 freq-profile 0
 rf-chan 0 95
  type DOCSIS
  frequency 93000000
  rf-output NORMAL
  power-adjust 0
  docsis-channel-id 1
```

```
  qam-profile 1
```

状態を表示する show コマンドの例

QAM プロファイル、周波数プロファイル、ダウンストリーム コントローラ、またはチャネルの状態を表示するには、次のコマンドを使用します。

QAM プロファイル設定の例

```
Router#show cable qam-profile 0
QAM Profile ID 0: default-annex-b-64-qam
        annex: B
        modulation: 64
        interleaver-depth: I32-J4
        symbol rate: 5057 kilo-symbol/second
        spectrum-inversion: off
Router#
```

周波数プロファイル設定の例

```
Router#show cable freq-profile 0
Frequency Profile ID 0 annex-b-low:
        Lane 1 start-freq 90000000hz
                Block 1 start-freq 90000000hz
                Block 2 start-freq 138000000hz
                Block 3 start-freq 186000000hz
                Block 4 start-freq 234000000hz
        Lane 2 start-freq 282000000hz
                Block 1 start-freq 282000000hz
                Block 2 start-freq 330000000hz
                Block 3 start-freq 378000000hz
                Block 4 start-freq 426000000hz
        Lane 3 start-freq 474000000hz
                Block 1 start-freq 474000000hz
                Block 2 start-freq 522000000hz
                Block 3 start-freq 570000000hz
                Block 4 start-freq 618000000hz
        Lane 4 start-freq 666000000hz
                Block 1 start-freq 666000000hz
                Block 2 start-freq 714000000hz
                Block 3 start-freq 762000000hz
                Block 4 start-freq 810000000hz
Router#
```

コントローラ設定の例

```
Router#show controller Integrated-Cable 3/0/0 rf-port
  Admin:  UP  MaxCarrier: 128  BasePower: 34 dBmV  Mode: normal
  Rf Module 0: UP
  Frequency profile: 0
  Free freq block list has 1 blocks:
    666000000 - 863999999
  Rf Port Status: UP
Router#
```

RF チャネル設定の例

```
Router#show controller integrated-Cable 3/0/0 rf-channel 0-3 95
Chan State Admin Frequency  Type   Annex Mod  srate Interleaver  dcid  power  output
 0     UP   UP   93000000   DOCSIS  B    256   5361  I32-J4       1    34     NORMAL
 1     UP   UP   99000000   DOCSIS  B    256   5361  I32-J4       2    34     NORMAL
 2     UP   UP   105000000  DOCSIS  B    256   5361  I32-J4       3    34     NORMAL
 3     UP   UP   111000000  DOCSIS  B    256   5361  I32-J4       4    34     NORMAL
 95    UP   UP   663000000  DOCSIS  B    256   5361  I32-J4       96   34     NORMAL
```

```
Router# show controller integrated-Cable 3/0/0 rf-channel 0 verbose
Chan State Admin Frequency  Type   Annex Mod  srate Interleaver  dcid  power  output
 0     UP   UP   93000000   DOCSIS  B    256   5361  I32-J4       1    34     NORMAL
 Qam profile: 1
 Spectrum Inversion: Off
 Frequency Lane: 1  Block: 1  index: 1
 Resource status:   OK
 License: granted <02:00:04 EDT Jan 2 2012>
 JIB channel number: 0
Chan EnqQ  Pipe  RAF SyncTmr Vid Mac            Video Primary DqQ  TM Mpts Sniff
   0     0     0   4       0   0 0000.0000.0000     0       0    0  0    0 NO
Grp  Prio P  Prate Phy0-ctl Phy1-ctl Enable Tun-Id  L2TPv3_Ses_id
   0    0  0     1        1        0   TRUE       0      0
Chan  Qos-Hi Qos-Lo  Med-Hi Med-Lo  Low-Hi Low-Lo
   0  32774  16384   32768  16384   65536  32768
Chan  Med Low TB-neg Qos_Exc  Med_Xof  Low_Xof       Qdrops  Pos Qlen(Hi-Med-lo) Fl
    0   0   0      0        0        0        0            0  Y     0     0     0  0
DSPHY Info:
  DSPHY Register Local Copy: QPRHI = c0000163, QPRLO = e30d0
  DSPHY Register Local Copy Vaddr = 80000290, qam2max_mapping = 80000000
  DSPHY Register Local Copy: SPR ID = 0, SPR Mapping= c200000a
  Last read from HW: Mon Jan  2 02:02:04 2012
   QPRHI = c0000163, QPRLO = e30d0, SPR = c200000a SPRMAPING c0000000 Q2Max 80000000
  Last time read spr rate info from HW: Mon Jan  2 13:21:41 2012
    SPR ID 0, rate value in kbps 0, overflow count 0, underflow count 0


Router#show controllers Integrated-Cable 3/0/0 counter rf-channel

Controller  RF    MPEG       MPEG       MPEG       Sync       MAP/UCD
            Chan  Packets    bps        Mbps       Packets    Packets
                  Tx                               Tx         Tx
3/0/0       0     6          0          0.000000   0          6
3/0/0       1     6          0          0.000000   0          6
3/0/0       2     6          0          0.000000   0          6
3/0/0       3     6          0          0.000000   0          6
3/0/0       4     6          0          0.000000   0          6
3/0/0       5     6          0          0.000000   0          6
3/0/0       6     6          0          0.000000   0          6
3/0/0       7     6          0          0.000000   0          6
3/0/0       8     5124124    1381035    1.332459   329444     6531411


Router# show cable licenses ds
-----------------------------------------------
Entitlement:  Downstream License
Consumed count: 672
Consumed count reported to SmartAgent: 672
Forced-Shut count: 0
Enforced state: No Enforcement

Router#
```

その他の参考資料

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

Cisco cBR ルータのダウンストリーム インターフェイス設定に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *16*：ダウンストリーム インターフェイスの設定に関する機能情報

機能名	リリース	機能情報
ダウンストリームインターフェイス設定	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 9 章

アップストリーム インターフェイス設定

このマニュアルでは、 Cisco cBR シリーズ コンバージド ブロードバンド ルータ上のアップストリーム インターフェイスを設定する方法について説明します。

機能情報の確認

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *17* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

アップストリーム インターフェイス設定の情報

アップストリーム チャネル管理

アップストリーム チャネル管理（UCM）は、 Cisco cBR シリーズ コンバージド ブロードバンド ルータ のアップストリームチャネルの物理（PHY）層の設定およびリソース管理を実行します。

アップストリーム コントローラ

アップストリーム ポートは、ケーブル ライン カードにある、1 つ以上のファイバ ノードに接続された物理アップストリーム RF コネクタを表します。アップストリーム RF ポートは、アップストリーム RF チャネルのコンテナであり、物理ポートに含まれる RF チャネル グループのトポロジとスペクトルの両方に制限を課します。アップストリーム RF ポートは、ケーブル ライン カード上の RF フロントエンド ハードウェア コンポーネント（コネクタ、可変ゲイン調整（VGA）、A/D コンバータなど）を表します。これは、アップストリーム物理チャネルの受信側に直接接続されます。ポートあたりのアップストリーム物理チャネルの数は、ポートにアクセス可能な受信側の数に制限されます。

アップストリーム チャネル

アップストリーム RF チャネルは、特定のチャネル幅の単一アップストリーム中心周波数における DOCSIS 物理層操作を表します。これは、CMTS ライン カード ハードウェア上の単一物理ポートに含まれています。

アップストリーム リソース管理

アップストリーム リソース管理（URM）機能は、ライン カード上の物理アップストリーム コネクタとそのコネクタ上で受信したアップストリーム RF チャネルとの間の関係を維持するという主な役割があります。

アップストリーム インターフェイスの設定方法

この項の構成は、次のとおりです。

設定モードを使用した Cisco CMTS の手動設定

コンソール端末を I/O コントローラのコンソール ポートに接続します。初期ダイアログを開始するかどうかの質問に対して、no と応答し、ルータのユーザ動作モードを開始します。数秒後にユーザ EXEC プロンプト（**Router>**）が表示されます。

変調プロファイルの設定とアップストリーム チャネルの割り当て

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 modulation-profile** *profile mode_of_oper qam_profile* 例： `Router(config)# cable modulation-profile 23 tdma qam-16`	バースト パラメータが各バースト タイプのそれぞれのデフォルト値に設定されている、定義済み変調プロファイルを作成します。
ステップ 4	**Controller Upstream-Cable** *slot/subslot/port* 例： `Router(config)# Controller Upstream-Cable 7/0/0`	コントローラ インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**us-channel** *n***modulation-profile** *primary-profile-number* [*secondary-profile-number*] [*tertiary-profile-number*] 例： `Router(config-if)#cable upstreamus-channel 0 modulation-profile 23`	アップストリーム ポートに最大 3 つの変調プロファイルを割り当てます。
ステップ 6	**end** 例： `Router(config-controller)# end`	コントローラ コンフィギュレーション サブモードを終了し、特権EXECモードに戻ります。

PHY レイヤでのアップストリーム チャネルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**controller upstream-cable** *slot*/*subslot*/*port* 例： `Router(config)# controller upstream-cable 1/0/0`	コントローラ インターフェイス ライン カードを指定し、アップストリーム コントローラ コンフィギュレーション サブモードを開始します。
ステップ 4	**us-channel** *rf-channel* **frequency** *freq-val* 例： `Router(config-controller)# us-channel 1 frequency 20000000`	コントローラ インターフェイスの RF チャネルに周波数を割り当てます。
ステップ 5	**us-channel** *rf-channel* **docsis-mode** *mode* 例： `Router(config-controller)# us-channel 1 docsis-mode tdma`	コントローラ インターフェイスの RF チャネルに DOCSIS モードを割り当てます。
ステップ 6	**us-channel** *rf-channel* **channel-width** *value* 例： `Router(config-controller)# us-channel 1 channel-width 3200000`	コントローラ インターフェイスの RF チャネルにチャネル幅を Hz で割り当てます。
ステップ 7	**us-channel** *rf-channel* **modulation-profile** *profile* 例： `Router(config-controller)# us-channel 1 modulation-profile 21`	コントローラ インターフェイスの RF チャネルに変調プロファイルを割り当てます。
ステップ 8	**no us-channel** *rf-channel* **shutdown** 例： `Router(config-controller)# no us-channel 1 shutdown`	アップストリーム チャネルをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Router(config-controller)# end`	アップストリーム コントローラ コンフィギュレーション サブモードを終了して、特権 EXEC モードに戻ります。

MAC ドメインでのアップストリーム チャネルの関連付けとアップストリーム ボンディングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface cable** *slot*/*subslot*/*cable-interface-index* 例： `Router(config)# interface cable 7/0/0`	Cisco CMTS ルータでケーブル インターフェイス ライン カードを指定します。
ステップ 4	**downstream integrated-cable** *slot*/*subslot*/*port***rf-channel** *rf-chan* [**upstream** *grouplist*] 例： `Router(config-if)# downstream integrated-cable 7/0/0 rf-channel 3 upstream 3`	一連のアップストリーム チャネルと内蔵ダウンストリーム チャネルを関連付けます。
ステップ 5	**upstream** *md-us-chan-id***upstream-cable** *slot*/*subslot*/*port***us-channel** *rf-channel* 例： `Router(config-if)# upstream 0 upstream-cable 7/0/0 us-channel 0`	一連の物理チャネル アップストリームと MAC ドメインを関連付けます。

	コマンドまたはアクション	目的
ステップ 6	**cable upstream bonding-group** *id* 例： `Router(config-if)# cable upstream bonding-group 200`	指定したケーブルインターフェイスでアップストリームボンディング グループを作成し、アップストリーム ボンディング コンフィギュレーション サブモードを開始します。
ステップ 7	**upstream** *number* 例： `Router(config-upstream-bonding)# upstream 1`	アップストリームボンディング グループにアップストリーム チャネルを追加します。 MAC ドメインごとに最大 16 個のアップストリーム チャネルを設定できます。これらは次の 2 つのグループに分けられます。 • グループ 1：アップストリーム チャネル 0 ～ 7 • グループ 2：アップストリーム チャネル 8 ～ 15 **アップストリーム ボンディング グループ**には、グループ 1 のすべてのアップストリーム チャネルのみ、またはグループ 2 のすべてのアップストリームチャネルのみが含まれている必要があります。
ステップ 8	**attributes** *value* 例： `Router(config-upstream-bonding)# attributes eeeeeeee`	指定したアップストリームボンディング グループの属性値を変更します。
ステップ 9	**end** 例： `Router(config-upstream-bonding)# end`	アップストリーム ボンディング コンフィギュレーション サブモードを停止して、特権 EXEC モードに戻ります。

設定例

PHY レイヤを持つアップストリーム チャネルの設定例

```
...
us-channel 0 frequency 20000000
us-channel 0 channel-width 3200000 3200000
us-channel 0 power-level 0
us-channel 0 docsis-mode tdma
us-channel 0 minislot-size 2
us-channel 0 modulation-profile 21
```

```
no us-channel 0 shutdown
...
```

MAC ドメインを持つアップストリーム チャネルの設定例

```
...
interface Cable8/0/0
downstream Modular-Cable 8/0/0 rf-channel 0
upstream 0 Upstream-Cable 8/0/0 us-channel 0
upstream 1 Upstream-Cable 8/0/0 us-channel 1
cable mtc-mode
cable upstream bonding-group 1
  upstream 0
  upstream 1
  attributes 80000000

...
```

その他の参考資料

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

Cisco cBR ルータのアップストリーム インターフェイス設定に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *18*：アップストリーム インターフェイスの設定に関する機能情報

機能名	リリース	機能情報
アップストリームインターフェイス設定	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 10 章

DOCSISインターフェイスとファイバノードの設定

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *19*：***Cisco cBR*** シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

DOCSIS のインターフェイスおよびファイバ ノード設定の概要

Cisco cBR シャーシで使用されるインターフェイス ラインカードは、2 つのダウンストリーム モジュールと 1 つのアップストリーム モジュールを搭載した統合型ラインカードです。このラインカードは、ダウンストリーム ボンディング グループおよびアップストリーム ボンディング グループを含む DOCSIS 3.0 機能をサポートします。

ダウンストリームの機能

物理的には、DS（ダウンストリーム）モジュールは 8 つの物理コネクタ（ポート）をサポートします。DS モジュールは、以下の機能をサポートします。

- DS モジュールはこれら 8 つのポート用に 8 つのダウンストリーム内蔵ケーブル コントローラをサポートします。各ダウンストリーム内蔵ケーブル コントローラは RF ポートに関連付けられます。
- 各ダウンストリーム コントローラは最大 128 のダウンストリーム チャネル（0 ～ 127）をサポートします。
- 各ダウンストリームコントローラは128の内蔵ケーブルインターフェイスで設定できます。したがって、各ライン カードには 1024 の内蔵ケーブル インターフェイスがあります。
- 各内蔵ケーブル インターフェイスには、内蔵ケーブル コントローラ RF チャネルに静的にマッピングされます。たとえば、内蔵ケーブル インターフェイス 3/0/0:0 は内蔵ケーブル コントローラ 3/0/0 の RF チャネル 0 にマッピングされます。
- 768 のダウンストリーム DOCSIS チャネルを各ライン カードで設定できます。
- 合計で 512 のワイドバンド ケーブル インターフェイス（ダウンストリーム ボンディング グループ）を各ラインカードで設定できます。
  - 各ワイドバンド ケーブルインターフェイスは最大 64 のダウンストリーム チャネルをサポートします。
  - 512 のワイドバンド ケーブルインターフェイス（ダウンストリーム ボンディング グループ）のうち 128 で 33 以上のチャネルを含めることができます。

アップストリーム機能

インターフェイス ラインカードには、16 の物理コネクタまたはポートをサポートする 1 つのアップストリーム モジュールがあります。アップストリーム機能は次のとおりです。

- ラインカードは、それぞれが 1 つのアップストリーム コネクタにマッピングしている 16 のアップストリーム ケーブル コントローラをサポートします。
- 1 つのアップストリーム コントローラには 12 のアップストリーム チャネルを設定できます。
- 1 対のアップストリーム コントローラでは、12 のアップストリーム チャネルをイネーブルにできます。

アップストリーム機能の詳細については、『*Downstream Upstream Guide*』を参照してください。

MAC ドメイン（ケーブル インターフェイス）

1. 1 つのライン カードあたり 16 の MAC ドメイン（ケーブル インターフェイス）を設定できます。
2. 各 MAC ドメインには、最大 16 個のアップストリーム チャネルを設定できます。
3. 最大 255 個のダウンストリーム チャネルを MAC ドメインに追加できます。

4 1 つの MAC ドメインにプライマリ可能なダウンストリーム チャネルの最大数は 32 です。ファイバ ノードの設定時に、非プライマリ ダウンストリーム チャネルが MAC ドメインに自動的に追加されます。

ファイバ ノード

Cisco cBR-8 シャーシごとに 512 のファイバ ノードを設定できます。

DOCSIS インターフェイスとファイバ ノードの設定

アップストリーム チャネルの設定

コントローラ設定の確認

コントローラのアップストリーム チャネルの設定を確認するには、**show controllers upstream-cable** コマンドを使用します。修飾子 **| include upstream** を使用すると、コントローラの管理状態と運用状態を確認できます。

```
Router#show controllers upstream-Cable 1/0/0 | include upstream
Controller 1/0/0 upstream 0  AdminState:UP OpState: UP
Controller 1/0/0 upstream 1  AdminState:UP OpState: UP
Controller 1/0/0 upstream 2  AdminState:UP OpState: UP
Controller 1/0/0 upstream 3  AdminState:UP OpState: UP
Controller 1/0/0 upstream 4  AdminState:DOWN Opstate: DOWN (Reason: Default)
Controller 1/0/0 upstream 5  AdminState:DOWN Opstate: DOWN (Reason: Default)
Controller 1/0/0 upstream 6  AdminState:DOWN Opstate: DOWN (Reason: Default)
Controller 1/0/0 upstream 7  AdminState:DOWN Opstate: DOWN (Reason: Default)
Router#
```

MAC ドメインへのアップストリーム チャネルのバインド

デフォルトでは、MAC ドメインにはいかなるアップストリーム チャネルも含まれません。ここでは、1 つの MAC ドメインに 1 つ以上のアップストリーム チャネルをバインドする必要のある設定について説明します。各アップストリーム チャネルがバインドされる MAC ドメインは 1 つのみです。MAC ドメインおよびアップストリーム チャネルは、同じライン カード（同じスロット）に常駐する必要があります。必要に応じて、同じアップストリーム コントローラ内のアップストリーム チャネルを異なる MAC ドメインにバインドすることができます。

はじめる前に

制限事項

- 最大 8 つのアップストリーム チャネルを 1 つの MAC ドメインに追加できます。

（注） MAC ドメインごとに最大16個のアップストリームチャネルを設定できます。

- MAC ドメインおよびチャネルは同じスロットを共有する必要があります。つまり、MAC ドメインには、同じスロットのコントローラのチャネルが含まれる場合があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface cable** 例： `Router#interface cable 1/0/0`	MAC ドメイン設定モードを開始します。スロットの値は 0 ～ 3 と 6 ～ 9 で、サブスロットは常に 0 となり、MD インデックスは 0 ～ 15 です。
ステップ 4	**upstream upstream-Cable us-channel** 例： `Router(config-if)#upstream 4 upstream-Cable 1/0/0 us-channel 7`	指定したアップストリーム チャネルを MAC ドメインにバインドします。
ステップ 5	**end** 例： `Router# end`	特権 EXEC モードに戻ります。

次の作業

アップストリームの MAC ドメインの設定を確認するには、**cgd-associations** キーワードを指定した **show cable mac-domain** コマンドを使用します。

MD US バインド テーブルには、アップストリーム チャネル バインドが表示されます。

```
Router#show cable mac-domain c1/0/0 cgd-associations
Load for five secs: 1%/0%; one minute: 2%; five minutes: 2%
Time source is NTP, *13:36:26.209 PST Fri Jan 20 2012
CGD Host  Resource  DS Channels           Upstreams    (ALLUS)   Active DS
Ca1/0/0   1/0/0     8                     0-1          Yes        8

                    16                    0-1          Yes        16

                    24                    0-1          Yes        24

                    32-33                 0-1          Yes        32-33
```

```
                    40                    0-1          Yes        40

MD US binding:
Host    MD Controller US channel State
Ca1/0/0 U0 1/0/0      0          UP
Ca1/0/0 U1 1/0/0      1          UP
Ca1/0/0 U2 1/0/0      2          UP
Ca1/0/0 U3 1/0/0      3          UP
Ca1/0/0 U4 1/0/1      0          UP
Ca1/0/0 U5 1/0/1      1          UP
Ca1/0/0 U6 1/0/1      2          UP
Ca1/0/0 U7 1/0/1      3          UP

Router#
```

プライマリ対応ダウンストリーム チャネルの設定

コントローラのダウンストリーム設定の確認

内蔵ケーブル コントローラで設定されているダウンストリーム チャネルのステータスを確認するには、 **show controller Integrated-Cable** コマンドを使用します。

```
Router# show controller Integrated-Cable 1/0/0 rf-channel 0-127
Chan State Admin Frequency Type   Annex Mod srate Interleaver dcid power output
0 UP UP    381000000       DOCSIS B     256 5361  I32-J4      1    32    NORMAL
1 UP UP    387000000       DOCSIS B     256 5361  I32-J4      2    34    NORMAL
2 UP UP    393000000       DOCSIS B     256 5361  I32-J4      3    34    NORMAL
3 UP UP    399000000       DOCSIS B     256 5361  I32-J4      4    34    NORMAL
```

内蔵ケーブル インターフェイスの設定

プライマリ対応ダウンストリーム チャネルとして MAC ドメイン内に追加するダウンストリーム チャネルを準備できるように内蔵ケーブル インターフェイスを設定します。インターフェイスの設定には次のようなメリットがあります。

- 帯域幅をダウンストリーム チャネルに割り当てられるようになります。
- チャネル インターフェイスの管理状態（shut/no shut）を制御できるようになります。

同じコントローラの shut 管理状態と no shut 管理状態の間で必要な時間間隔は、約 30 秒です。スクリプトやコピー アンド ペーストで、遅延を設けることなく直ちに shut および no shut 状態を変更してはなりません。これにより、予期しないエラーが発生する可能性があります。

各内蔵ケーブル インターフェイスは、内蔵ケーブル コントローラ RF チャネルに静的にマッピングされます。たとえば、IC インターフェイス 1/0/0:0 は、IC コントローラ 1/0/0 RF チャネル 0 にマッピングされます。同様に、IC インターフェイス 1/0/0:1 は、IC コントローラ 1/0/0 RF チャネル 1 にマッピングされます。

IC コントローラには 0 ～ 7 の番号が付けられ、各コントローラの RF チャネルには 0 ～ 127 の番号が付けられます。

はじめる前に

チャネルに割り当てる帯域幅の割合を決定します。設定した帯域幅の割合は、インターフェイスの認定情報レート（CIR）値に変換されます。この値を使用すると、このチャネルで未ボンディングのサービス フローを許可できます。詳細については、「*Dynamic Bandwidth Sharing on the Cisco CMTS Router*」を参照してください。

手順

ステップ 1 **enable**

例：
```
Router> enable
```
特権 EXEC モードをイネーブルにします。

パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：
```
Router# configure terminal
```
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 **interface integrated-cable**

例：
```
Router(config)# interface integrated-cable 1/0/0:0
```
指定した内蔵ケーブル インターフェイスの内蔵ケーブル インターフェイス コンフィギュレーション モードを開始します。

ステップ 4 **cable rf-bandwidth-percent** *percentage-number*

例：
```
Router(config-if)# cable rf-bandwidth-percent 30
```
指定した内蔵ケーブル インターフェイスに割り当てる帯域幅を設定します。

ステップ 5 **end**

例：
```
Router# end
```
特権 EXEC モードに戻ります。

次の作業

次の条件を使用すると、IC（内蔵ケーブル）インターフェイスが現在のソフトウェアで稼働状態であるかを判断できます。

- IC インターフェイスが MD（MAC ドメイン）インターフェイスに関連付けられている。

- IC インターフェイスが関連付けられている MD インターフェイスが稼働状態にある。
- IC インターフェイスがシャットダウンに設定されていない。
- IC インターフェイスの帯域幅が設定されている。
- IC コントローラ内で関連付けられたダウンストリーム チャネルが動作状態である。

show interface Integrated-Cable controller コマンドを使用すると、指定した内蔵ケーブル インターフェイスのステータスを確認できます。State info テーブルには、インターフェイスの動作状態に影響を与える問題の診断に関する情報が表示されます。

```
Router# show interface Integrated-Cable 1/0/0:0 controller
Integrated-Cable1/0/0:0 is up, line protocol is up
…
----------------------------------------------
State info (DSNB if and its underlying states)
----------------------------------------------
DSNB IF state : UP
RF Chan state : UP
RF Chan frequency : 381000000
Bandwidth configured on DSNB IF : YES
Inject Header/HW flow creation status : DSNB_IF_SM_UP
MD state (9/0/0) : UP
*DSNB i/f Line State : UP
----------------------------------------------
```

MAC ドメインへのプライマリ対応ダウンストリーム チャネルのバインド

ダウンストリームチャネルで内蔵ケーブルインターフェイスを適切に設定すると、プライマリ対応チャネルとして MAC ドメインにバインドできます。チャネル グループ ドメイン（CGD）設定では、指定したダウンストリーム チャネルをプライマリ対応チャネルとして MAC ドメインにバインドできます。必要に応じて、ダウンストリーム チャネルを MAC ドメイン内のアップストリーム チャネルのサブセットと関連付けることもできます。

はじめる前に

制限事項

- ダウンストリーム チャネルおよび MAC ドメインは、同じライン カード（同じスロット）に常駐する必要があります。
- 最大 32 のプライマリ ダウンストリーム チャネルを 1 つの MAC ドメインに追加できます。

手順

ステップ 1 **enable**

例：

```
Router> enable
```

特権 EXEC モードをイネーブルにします。

パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：
```
Router# configure terminal
```
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 **interface cable**

例：

```
Router#interface cable 1/0/0
```
MAC ドメイン設定モードを開始します。

- *slot*：インターフェイス ライン カードのシャーシ スロット番号を指定します。有効な値は、0 ～ 3 および 6 ～ 9 です。
- *subslot*：インターフェイス ライン カードのセカンダリ スロット番号を指定します。有効なサブスロットは 0 です。
- *MD index*：MAC ドメイン インデックス番号を指定します。有効な値は 0 ～ 15 です。

ステップ 4 **downstream Integrated-Cable** *slot/subslot/port***rf-channels** *grouplist*

例：

```
Router#downstream Integrated-Cable 1/0/0 rf-channels 1-6
```
ダウンストリーム プライマリ対応チャネルを設定します。

- *grouplist*：ダウンストリーム RF チャネルの範囲を指定します。

ステップ 5 **end**

例：
```
Router# end
```
特権 EXEC モードに戻ります。

次の作業

ダウンストリーム プライマリ ケーブル チャネルを確認するには、**cgd-associations** キーワードを指定した **show cable mac-domain** コマンドを使用します。

```
Router#show cable mac-domain c1/0/0 cgd-associations
Load for five secs: 1%/0%; one minute: 2%; five minutes: 2%
Time source is NTP, *13:36:26.209 PST Fri Jan 20 2012
CGD Host  Resource  DS Channels           Upstreams    (ALLUS)   Active DS
Ca1/0/0   1/0/0     8                     0-1          Yes        8

                    16                    0-1          Yes        16

                    24                    0-1          Yes        24

                    32-33                 0-1          Yes        32-33

                    40                    0-1          Yes        40
```

```
MD US binding:
Host    MD Controller US channel State
Ca1/0/0 U0 1/0/0      0          UP
Ca1/0/0 U1 1/0/0      1          UP
Ca1/0/0 U2 1/0/0      2          UP
Ca1/0/0 U3 1/0/0      3          UP
Ca1/0/0 U4 1/0/1      0          UP
Ca1/0/0 U5 1/0/1      1          UP
Ca1/0/0 U6 1/0/1      2          UP
Ca1/0/0 U7 1/0/1      3          UP

Router#
```

MAC ドメイン サービス グループの設定

ファイバ ノードの設定

1 つの CMTS に対して最大 512 のファイバ ノードを設定できます。CMTS で設定したファイバ ノードには、HFC 設備で一致する物理ファイバ ノードが 1 つ以上表示されます。CMTS は、設備内の物理ファイバ ノードの DOCSIS ダウンストリーム サービス グループ（DS-SG）および DOCSIS アップストリーム サービス グループ（US-SG）を特定するのに、ファイバノード構成を使用します。MAC ドメイン内の MAC ドメイン ダウンストリームおよびアップストリームのサービス グループ（それぞれ MD-DS-SG と MD-US-SG）の計算が自動的に行われるように、サービス グループ情報は MAC ドメイン チャネル設定と比較されます。

有効なファイバ ノード設定を作成するには、次の作業が必要です。

- 各ファイバ ノード設定に、少なくとも 1 つのダウンストリーム コントローラおよび 1 つのアップストリーム コントローラを追加する必要があります。
- ファイバ ノード内のチャネルが含まれる各 MAC ドメインおよびワイドバンド インターフェイスは、同じバンドル インターフェイスを使用する必要があります。
- ファイバ ノードに含まれるすべてのダウンストリーム チャネルには、独自の周波数を割り当てる必要があります。
- 特定の MAC ドメインに関連付けられたすべてのダウンストリーム チャネルに、独自の DOCSIS チャネル ID を割り当てる必要があります。

手動 DOCSIS チャネル ID 設定よりも自動 DOCSIS チャネル ID の割り当ての方が適切な場合は、**cable downstream-channel-id automatic** コマンドを使用して、CMTS の自動 DOCSIS チャネル ID 割り当てを有効にできます。

詳細については、『*Cisco CMTS Cable Command Reference*』を参照してください。

手順

ステップ 1 **enable**

例：
```
Router> enable
```
特権 EXEC モードをイネーブルにします。

パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：
```
Router# configure terminal
```
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 fiber-node** *id*

例：

```
Router(config)#cable fiber-node 1
Router(config-fiber-node)#
```
ファイバ ノードを設定するには、ケーブル ファイバ ノード コンフィギュレーション モードを開始します。

- *id*：ケーブル ファイバ ノード ID。有効な範囲は 1 ～ 512 です。

ステップ 4 **downstream Integrated-Cable** *slot/subslot/port*

例：

```
Router(config-fiber-node)#downstream Integrated-Cable 1/0/0
```
ファイバ ノードにコントローラ内の DOCSIS ダウンストリーム チャネルを追加します。

ステップ 5 **upstream upstream-Cable** *slot/subslot/port*

例：

```
Router(config-fiber-node)#upstream upstream-Cable 1/0/0
```
ファイバ ノードにコントローラ内のアップストリーム チャネルを追加します。

ステップ 6 **end**

例：
```
Router# end
```
特権 EXEC モードに戻ります。

次の作業

ファイバ ノード設定を確認するには、**show cable fiber-node** コマンドを使用します。

```
Router# show cable fiber-node 1
------------------------------------------------------------------------------
--
Fiber-Node 1
```

```
Description: Feed Mac Domain: Cable1/0/0
Channel(s) : downstream Integrated-Cable 1/0/0: 0-3, 32-35, 64-67,
96-99
Channel ID(s): 1 2 3 4 33 34 35 36 65 66 67 68 97 98
99 100
Upstream-Cable 1/0/0
FN Config Status: Configured (status flags = 0x01)
MDD Status: Valid
Router#
```

出力には、ファイバ ノードに設定されているダウンストリーム チャネル ID が表示されます。また、ファイバノードに設定されているアップストリームケーブルのステータスも表示します。さらに、MAC ドメイン記述子（MDD）メッセージングのステータスも表示します。

MD-DS-SG チャネル メンバーシップの確認

ファイバ ノードが有効の場合は、関連する MAC ドメイン内の MD-DS-SG がダウンストリーム チャネルに自動的に統合されます。MD-DS-SG には、MAC ドメイン内のアクティブなプライマリ ダウンストリーム チャネルと、ファイバ ノード設定を介して MAC ドメインと自動的に関連付けられた非プライマリ ダウンストリームチャネルがあります。非プライマリ チャネルは、MD-DS-SG に含まれるようにコントローラ（オプションを指定して）内で正しく設定する必要があります。

MD-DS-SG チャネル メンバーシップを表示するには、**downstream-service-group** オプションを指定した **show cable mac-domain** コマンドを使用します。

```
outer#show cable mac-domain c1/0/0 downstream-service-group
Cable MD-DS-SG RF
IF Id Resource Chan  Primary Chan
C1/0/0 5 1/0/0 0-3   0-3
               32-35 32-35
               64-67
               96-99
```

プライマリ ダウンストリーム チャネルが MAC 管理メッセージ（MMM）を送信していることを確認するには、**show controller Integrated-Cable counter rf-channel** コマンドを使用します。

```
Router#show controller Integrated-Cable 1/0/0 counter rf-channel
Controller  RF    MPEG       MPEG       MPEG       Sync       MAP/UCD
            Chan  Packets    bps        Mbps       Packets    Packets
                  Tx                               Tx         Tx
1/0/0       0     51256      1504       0.001504   0          51256
1/0/0       1     51256      1504       0.001504   0          51256
1/0/0       2     51256      1504       0.001504   0          51256
1/0/0       3     51256      1504       0.001504   0          51256
1/0/0       4     51256      1504       0.001504   0          51256
1/0/0       5     51256      1504       0.001504   0          51256
1/0/0       6     51256      1504       0.001504   0          51256
1/0/0       7     51256      1504       0.001504   0          51256
1/0/0       8     47625214   1416567    1.367991   5124345    50884388
1/0/0       9     51256      1504       0.001504   0          51256
1/0/0       10    51256      1504       0.001504   0          51256
1/0/0       11    51256      1504       0.001504   0          51256
1/0/0       12    51256      1504       0.001504   0          51256
1/0/0       13    51256      1504       0.001504   0          51256
1/0/0       14    51256      1504       0.001504   0          51256
1/0/0       15    51256      1504       0.001504   0          51256
1/0/0       16    47627672   1414913    1.366337   5124342    50884344
1/0/0       17    51256      1504       0.001504   0          51256
1/0/0       18    51256      1504       0.001504   0          51256
1/0/0       19    51256      1504       0.001504   0          51256
1/0/0       20    51256      1504       0.001504   0          51256
```

```
1/0/0       21    51256      1504       0.001504   0          51256
1/0/0       22    51256      1504       0.001504   0          51256
1/0/0       23    51256      1504       0.001504   0          51256
1/0/0       24    47629532   1414862    1.366286   5124341    50884325
1/0/0       25    51256      1504       0.001504   0          51256
1/0/0       26    51256      1504       0.001504   0          51256
1/0/0       27    51256      1504       0.001504   0          51256
1/0/0       28    51253      1504       0.001504   0          51253
1/0/0       29    51253      1504       0.001504   0          51253
1/0/0       30    51253      1504       0.001504   0          51253
1/0/0       31    51253      1504       0.001504   0          51253
1/0/0       32    47642351   1412005    1.363429   5124337    50891994
1/0/0       33    47646042   1412757    1.364181   5124336    50892055
1/0/0       34    51251      1504       0.001504   0          51251
1/0/0       35    51251      1504       0.001504   0          51251
1/0/0       36    51251      1504       0.001504   0          51251
1/0/0       37    51251      1504       0.001504   0          51251
1/0/0       38    51251      1504       0.001504   0          51251
1/0/0       39    51251      1504       0.001504   0          51251
1/0/0       40    47634991   1409649    1.361073   5124329    50884177
1/0/0       41    51251      1504       0.001504   0          51251
```

MD-US-SG チャネル メンバーシップの確認

MD-US-SG チャネル メンバーシップを表示するには、**upstream-service-group** オプションを指定した **show cable mac-domain** コマンドを使用します。

```
Router#show cable mac-domain c1/0/0 upstream-service-group
Cable MD 1/0/0
US-SG-ID : 5 US-Chan : U0,1,2,3
Primary-DS: 1/0/0:0 US-SG-ID: 5
MDD US-List : U0,1,2,3
MDD Ambiguity : U0,1,2,3
Primary-DS: 1/0/0:1 US-SG-ID: 5
MDD US-List : U0,1,2,3
MDD Ambiguity : U0,1,2,3
Primary-DS: 1/0/0:2 US-SG-ID: 5
MDD US-List : U0,1,2,3
MDD Ambiguity : U0,1,2,3
Primary-DS: 1/0/0:3 US-SG-ID: 5
MDD US-List : U0,1,2,3
MDD Ambiguity : U0,1,2,3
```

ダウンストリーム ボンディング グループの設定

ワイドバンド ケーブル インターフェイス（ダウンストリーム ボンディング グループ）の設定

ワイドバンド ケーブル インターフェイスは、ダウンストリーム方向にボンディングされたトラフィックを転送します。一連のダウンストリーム RF チャネルは、ワイドバンド インターフェイスで設定します。各ライン カードは、最大 512 のワイドバンドインターフェイスをサポートします。

これらのワイドバンド インターフェイスと 8 つのコントローラ（ポート）の間に実際の関係性はありませんが、コントローラごとのグループにワイドバンド インターフェイスを分割するルールがあります。

512 のワイドバンド インターフェイスは、8 つのコントローラに分割され、各コントローラに 64 のインターフェイスが割り当てられます。

ダウンストリーム ボンディング グループを定義するワイドバンド ケーブル インターフェイスを作成できます。ダウンストリーム ボンディング グループは、一連のダウンストリーム RF チャネルを 1 つにまとめます。これには同じライン カードの RF チャネルのみが含まれます。

ボンディング グループと MAC ドメイン間の関連付けは自動的に作成されます。関連付けは、ボンディング グループ チャネル セットが MAC ドメイン内の MAC ドメイン ダウンストリーム サービス グループ（MD-DS-SG）のサブセットにある場合に行われます。自動関連付けにより、MAC ドメイン内にボンディング グループのチャネル セットを含む RCC の作成が開始されます。

はじめる前に

制約事項

1. 含まれるダウンストリームチャネルは、同じライン カードスロット内にある必要があります。
2. すべてのダウンストリーム チャネルは、内蔵ケーブル コントローラ 0 ～ 3 または 4 ～ 7 に含まれる必要があります。

手順

ステップ 1 **enable**

例：

```
Router> enable
```

特権 EXEC モードをイネーブルにします。

パスワードを入力します（要求された場合）。

ステップ 2 **configure terminal**

例：

```
Router# configure terminal
```

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 **interface wideband-Cable**

例：

```
Router(config)#interface wideband-Cable 1/0/0:1
Router(config-if)#
```

指定したワイドバンド ケーブル インターフェイスのワイドバンド ケーブル インターフェイス コンフィギュレーション モードを開始します。

ステップ 4 **cable bundle** *id*

例：

```
Router(config-if)#cable bundle 1
```

このワイドバンド ケーブルインターフェイスのケーブル バンドル ID を設定します。設定されたケーブル バンドル ID は、関連する MAC ドメインで設定されたケーブル バンドル ID と一致する必要があります。

- *Bundle number*：ケーブル バンドル番号。有効な範囲は 1 ～ 255 です。

ステップ 5 **cable rf-channels channel-list** *grouplist***bandwidth-percent** *percentage-bandwidth*

例：

```
Router(config-if)#cable rf-channel channel-list 1-3 bandwidth-percent 10
```

指定したチャネル リストに帯域幅の割り当てを設定し、ダウンストリーム ボンディング グループにチャネルを追加します。チャネル番号の範囲は 0 ～ 127（<first channel num-last channel num>）です。

- *grouplist*：ダウンストリーム RF チャネルの範囲を指定します。

ステップ 6 **cable rf-channels controller** *controller number***channel-list** *grouplist***bandwidth-percent** *percentage-bandwidth*

例：

```
Router(config-if)#cable rf-channel controller 1 channel-list 1-3 bandwidth-percent 10
```

ダウンストリームコントローラ上で指定したチャネルリストに帯域幅の割り当てを設定し、ダウンストリーム ボンディング グループにチャネルを追加します。チャネル番号の範囲は 0 ～ 127 です。

- *controller number*：ダウンストリーム コントローラ番号。有効な番号は 0 ～ 7 です。
- *grouplist*：ダウンストリーム RF チャネルの範囲を指定します。

ステップ 7 **end**

例：

```
Router# end
```

特権 EXEC モードに戻ります。

次の作業

ボンディング グループ インターフェイスを確認します。

ボンディング グループ インターフェイスの確認

ボンディング グループ インターフェイスを表示するには、**wideband-channel** オプションを指定した **show controllers integrated-Cable** コマンドを使用します。

```
Router# show controllers integrated-cable 1/0/0 wideband-channel
```

```
Load for five secs: 2%/0%; one minute: 2%; five minutes: 2%
Time source is NTP, *17:45:51.964 PST Thu Jan 12 2012
WB                      BG    Primary
channel                 ID    BG
Wideband-Cable1/0/0:0   12289 Yes
Wideband-Cable1/0/0:1   12290 Yes
Wideband-Cable1/0/0:2   12291 Yes
Wideband-Cable1/0/0:3   12292 Yes
Wideband-Cable1/0/0:4   12293 Yes
Wideband-Cable1/0/0:5   12294 Yes
Wideband-Cable1/0/0:6   12295 Yes
Wideband-Cable1/0/0:7   12296 Yes
Wideband-Cable1/0/0:8   12297 Yes
Wideband-Cable1/0/0:9   12298 Yes
Wideband-Cable1/0/0:10  12299 Yes
Wideband-Cable1/0/0:11  12300 Yes
Wideband-Cable1/0/0:12  12301 Yes
Wideband-Cable1/0/0:13  12302 Yes
Wideband-Cable1/0/0:14  12303 Yes
Wideband-Cable1/0/0:15  12304 Yes
Wideband-Cable1/0/0:16  12305 Yes
Wideband-Cable1/0/0:17  12306 Yes
Wideband-Cable1/0/0:18  12307 Yes
Wideband-Cable1/0/0:19  12308 Yes
Wideband-Cable1/0/0:20  12309 Yes
Wideband-Cable1/0/0:21  12310 Yes
Wideband-Cable1/0/0:22  12311 Yes
Wideband-Cable1/0/0:23  12312 Yes
Wideband-Cable1/0/0:24  12313 Yes
Wideband-Cable1/0/0:25  12314 Yes
```

- ワイドバンド チャネルにマッピングする RF チャネルを表示するには、 **mapping wb-channel** オプションを使用します。

```
Router# show controllers Integrated-Cable 1/0/0 mapping wb-channel 0
Ctrlr    WB       RF         WB %   WB Rem
1/0/0    0        1/0/0:0    40     1
                  1/0/0:1    40     1
```

- ダウンストリームの MAC ドメイン サービス グループを表示するには、**dsbg-associations** オプションを指定した **show cable mac-domain** コマンドを使用します。

```
Router# show cable mac-domain c1/0/0 dsbg-associations
Wi1/0/0:0       Wi1/0/0:1
```

ボンディング グループの設定を確認するには、 **show interface Wideband-Cable controller** コマンドを使用します。State info テーブルには、ダウンストリームのボンディング グループの状態情報が表示されます。

```
Router#show interface Wideband-Cable 1/0/0:0 controller
Wideband-Cable1/0/0:0 is up, line protocol is up
  Hardware is CMTS WB interface, address is c414.3c17.1dcb (bia c414.3c17.1dcb)
  MTU 1500 bytes, BW 150000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation MCNS, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/256 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
```

```
     Available Bandwidth 112500 kilobits/sec
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out


BG controller details
Wi1/0/0:0 BGID: 12289
Member RFIDs:
  Config RFIDs: 12288-12291 Count: 4
  Active RFIDs: 12288-12291 Count: 4
Attribute mask: 0x80000000
---------------------------------------------
State info (DSBG if and its underlying states)
---------------------------------------------
DSBG IF state               : UP
DSBG Member RF chan states  : UP (4 out of 4 chans are UP)
DSBG HWID(FCID)             : 0x3800
*DSBG i/f Line State        : UP
---------------------------------------------
-----------------------------
DMP Resources
DMP handle     : 0x10000800
-----------------------------
DMP BG pool entry details
HW-id   BGid  BGSize  Enabled
-----------------------------
0     : 12289 4        1
-----------------------------
Bgid  BGecnt BGaddr Channels (1023 means invalid/Unused)
    0      0      0:   0    1    2    3 1023 1023 1023 1023
BG         Rate   Neg   Pos    LastTS  CurrCr  Pos
   0      25000 65535 65535         0       0   N

-----------------------------
RFID - JIB chan mapping for active RFIDs: [rfid:jib-chan-no]
[12288:0] [12289:1] [12290:2] [12291:3]

Router#
```

アップストリーム ボンディング グループの設定

アップストリーム ボンディング グループの制限事項

- アップストリーム ボンディング グループは MAC ドメイン インターフェイス内で設定されます。
- アップストリーム ボンディング グループは、ボンディングされた一連のアップストリーム チャネルから構成されます。
- MAC ドメインごとに最大 16 個のアップストリーム チャネルを設定できます。これらは次の 2 つのグループに分けられます。
  - グループ 1：アップストリーム チャネル 0 ～ 7
  - グループ 2：アップストリーム チャネル 8 ～ 15

アップストリーム ボンディング グループには、グループ 1 のすべてのアップストリーム チャネルのみ、またはグループ 2 のすべてのアップストリーム チャネルのみが含まれている必要があります。

アップストリーム ボンディング グループの設定

はじめる前に

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface cable** *slot*/*subslot*/*MD index* 例： `Router(config)# interface cable 1/0/0`	MAC ドメイン設定モードを開始します。 • *slot*：インターフェイス ライン カードのシャーシ スロット番号を指定します。有効な値は、0 ～ 3 および 6 ～ 9 です。 • *subslot*：インターフェイス ライン カードのセカンダリ スロット番号を指定します。有効なサブスロットは 0 です。 • *MD index*：MAC ドメイン インデックス番号を指定します。有効な値は 0 ～ 15 です。

ステップ 4	**cable upstream bonding-group**
	
	例：
	`Router(config-if)#cable upstream bonding-group 7`
	`Router(config-upstream-bonding)#`
		MAC ドメインで静的アップストリーム ボンディング グループを作成します。

	コマンドまたはアクション	目的
ステップ 5	**upstream** 例： `Router(config-upstream-bonding)#upstream 7`	アップストリーム ボンディング グループにアップストリーム チャネルを追加します。 MAC ドメインごとに最大 16 個のアップストリーム チャネルを設定できます。これらは次の 2 つのグループに分けられます。 • グループ 1：アップストリーム チャネル 0 ～ 7 • グループ 2：アップストリーム チャネル 8 ～ 15 **アップストリーム ボンディング グループ**には、グループ 1 のすべてのアップストリーム チャネルのみ、またはグループ 2 のすべてのアップストリーム チャネルのみが含まれている必要があります。
ステップ 6	**end** 例： `Router# end`	特権 EXEC モードに戻ります。

次の作業

アップストリーム ボンディング グループの情報を表示するには、**show interface cable upstream bonding-group** コマンドを使用します。

```
Router#show interface cable 1/0/0 upstream bonding-group
Load for five secs: 1%/0%; one minute: 2%; five minutes: 2%
Time source is NTP, *10:47:17.142 PST Thu Jan 12 2012

Cable1/0/0: Upstream Bonding Group 1
     0 packets input, 0 octets input
     Segments: 0 valid, 0 discarded, 0 lost
     Reserved Bandwidth Max : 0 bits/sec
     Reserved Bandwidth     : 0 bits/sec
     Available Bandwidth    : 46080000 bits/sec
     Total Service Flows On This Bonding Group: 0
Cable1/0/0: Upstream Bonding Group 2
     0 packets input, 0 octets input
     Segments: 0 valid, 0 discarded, 0 lost
     Reserved Bandwidth Max : 0 bits/sec
     Reserved Bandwidth     : 0 bits/sec
     Available Bandwidth    : 46080000 bits/sec
     Total Service Flows On This Bonding Group: 0
Cable1/0/0: Upstream Bonding Group 65536
     0 packets input, 0 octets input
     Segments: 0 valid, 0 discarded, 0 lost
     Reserved Bandwidth Max : 0 bits/sec
     Reserved Bandwidth     : 0 bits/sec
     Available Bandwidth    : 15360000 bits/sec
```

```
     Total Service Flows On This Bonding Group: 0
Cable1/0/0: Upstream Bonding Group 65537
     0 packets input, 0 octets input
     Segments: 0 valid, 0 discarded, 0 lost
     Reserved Bandwidth Max : 0 bits/sec
     Reserved Bandwidth     : 0 bits/sec
     Available Bandwidth    : 15360000 bits/sec
     Total Service Flows On This Bonding Group: 0

Router#
```

アップストリーム ボンディング グループの確認

show cable upstream bonding-group コマンドを使用します。

```
Router#show interface cable 1/0/0 upstream bonding-group
Load for five secs: 1%/0%; one minute: 2%; five minutes: 2%
Time source is NTP, *10:47:17.142 PST Thu Jan 12 2012

Cable1/0/0: Upstream Bonding Group 1
     0 packets input, 0 octets input
     Segments: 0 valid, 0 discarded, 0 lost
     Reserved Bandwidth Max : 0 bits/sec
     Reserved Bandwidth     : 0 bits/sec
     Available Bandwidth    : 46080000 bits/sec
     Total Service Flows On This Bonding Group: 0
Cable1/0/0: Upstream Bonding Group 2
     0 packets input, 0 octets input
     Segments: 0 valid, 0 discarded, 0 lost
     Reserved Bandwidth Max : 0 bits/sec
     Reserved Bandwidth     : 0 bits/sec
     Available Bandwidth    : 46080000 bits/sec
     Total Service Flows On This Bonding Group: 0
Cable1/0/0: Upstream Bonding Group 65536
     0 packets input, 0 octets input
     Segments: 0 valid, 0 discarded, 0 lost
     Reserved Bandwidth Max : 0 bits/sec
     Reserved Bandwidth     : 0 bits/sec
     Available Bandwidth    : 15360000 bits/sec
     Total Service Flows On This Bonding Group: 0
Cable1/0/0: Upstream Bonding Group 65537
     0 packets input, 0 octets input
     Segments: 0 valid, 0 discarded, 0 lost
     Reserved Bandwidth Max : 0 bits/sec
     Reserved Bandwidth     : 0 bits/sec
     Available Bandwidth    : 15360000 bits/sec
     Total Service Flows On This Bonding Group: 0

Router#
```

その他の参考資料

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

DOCSIS インターフェイスとファイバ ノード設定に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *20* : *DOCSIS* インターフェイスとファイバ ノード設定に関する機能情報

機能名	リリース	機能情報
DOCSIS インターフェイスとファイバ ノードの設定	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 11 章

サービス グループ ベースの Cisco cBR ルータの設定

サービス グループ プロファイルに基づく設定

『DOCSIS Interface and Fiber Node Configuration』ガイドでは、Cisco cBR ルータを運用可能にするために必要なインターフェイスとファイバ ノードの設定について説明しています。この設定に含まれるタスクを完了するための手順は、複雑な説明となっています。

Cisco cBR ルータの素早い導入に必要な物理/論理インターフェイスを設定するプロセスを簡素化および迅速化する目的で、サービス グループ（SG）プロファイル ベースの手法が採用されています。このドキュメントでは、簡素化された SG プロファイル手法について説明します。

この手法には次の利点があります。

- Cisco cBR ルータの導入プロセスを改善および簡素化します。
- 重複する設定を排除することで、Cisco cBR ルータの設定を改善および簡素化します。
- Cisco cBR ルータのトラブルシューティングを改善および簡素化します。
- ノード間およびリージョン間で共通の迅速なレプリケーションを使用することで、より素早い Converged Cable Access Platform（CCAP）プロビジョニングをサポートします。

インタ フェースを設定して Cisco cBR ルータを短時間で運用可能にするために、一連の共通プロファイルが作成されて、グローバル サービス グループ プロファイル内で設定されます。これらのグローバル サービス グループ プロファイルを、サービス グループ インターフェイスと物理インターフェイスの間のマッピングとともに、ファイバ ノードインターフェイスに適用できます。

共通プロファイルとは、MAC ドメイン、ワイドバンド ケーブル、プライマリ ダウンストリームなどの共通のサービス グループ（SG）インターフェイス設定を格納するプロファイルのことです。

共通プロファイルとグローバル SG プロファイルを、それらが適用されるネットワークのトポロジから切り離すことができます。SG インターフェイスと物理インタ フェースの間のマッピングは、SG プロファイルの適用先のトポロジにおけるプロファイルの動作を定義します。

制限事項：

- ファイバ ノードに関連付けられている共通プロファイルを削除することはできません。これを変更するには、**cable profile** コマンドを使ってプロファイル コンフィギュレーション モードに入ることができます。
- ファイバ ノードに関連付けられているサービス グループ プロファイルを削除したり変更したりすることはできません。
- 新しいグローバル SG プロファイルをファイバ ノードに関連付けるには、ファイバ ノードと現在のグローバル SG プロファイルとの関連付けを解除します。
- 固有のトポロジに応じて設定するには、『DOCSIS Interface and Fiber Node Configuration』ガイドで説明されている完全な設定アプローチを使用します。
- セカンダリ ライン カードがアクティブ モードになっている場合は、次の制限事項が適用されます。
  - ファイバ ノードに関連付けられている MAC ドメイン、ワイドバンド ケーブル インターフェイス、ダウンストリーム チャネル、および SG プロファイルを変更することはできません。
  - SG プロファイルとファイバ ノードとの関連付けを解除することはできません。
  - MAC ドメイン、ワイドバンド ケーブル インターフェイス、ダウンストリーム チャネル、および SG プロファイルを作成できますが、これらをファイバ ノードに関連付けることはできません。
  - SG 運用簡素化機能を有効にするには、**cable wideband auto-reset** コマンドを使用して自動リセット機能を有効にする必要があります。
- MAC ドメイン分割設定が設定に含まれている場合、16.7.x から以前のイメージにダウングレードする cBR-8 イメージをサポートすることはできません。

共通プロファイルと SG プロファイルを定義して導入する大まかな手順は次のとおりです。

1. 共通プロファイルを定義して設定します。SG インターフェイス プロファイルまたは共通プロファイルは、類似するインターフェイスからなるグループに共通する設定パラメータを格納します。たとえば、複数のワイドバンド ケーブル インターフェイスで共有され、複数のライン カードで関連付けられる特定の設定パラメータをプロファイルに格納できます。共通プロファイルはグローバルまたはシャーシ レベルで設定されます。プロファイルに関連付けられているすべてのインタ フェースは、そのプロファイル内の設定を継承します。任意の共通プロファイルを任意のグローバル SG プロファイルに関連付けることができます。次の共通プロファイルを定義するには、**cable profile** *profile-type profile-name* コマンドを使用します。

- MAC ドメイン（MD）プロファイル
- プライマリ ダウンストリーム チャネル（DS）プロファイル
- ワイドバンド ケーブル インターフェイス（WB）プロファイル
- グローバル サービス グループ（SG）プロファイル

2 **cable fiber-node** コマンドを使用して、ファイバ ノード インターフェイスに対する次の設定を完了します。

- ダウンストリームおよびアップストリーム ポートを定義します。**downstream interface-cable** コマンドを使用して、適切なインターフェイス ケーブルをマッピングします。**upstream upstream-cable** コマンドを使用して、適切なアップストリーム ケーブル インターフェイスをマッピングします。
- **downstream sg-channel** コマンドを使用して論理ダウンストリーム SG チャネルを物理 RF チャネルにマッピングし、**upstream sg-channel** コマンドを使用して論理アップストリーム SG チャネルを物理アップストリーム チャネルにマッピングします。
- **service-group profile** を使用して、グローバル サービス グループ プロファイルをファイバ ノードに関連付けます。

設定および例については、ユース ケース シナリオを参照してください。

1 つの MAC ドメインを使用した 16x8 のサービス プロファイル設定

ここでは、1 つの MAC ドメインを使用した 16x8 サービス グループに関するサービス グループ ベースの設定について説明します。

手順

ステップ 1 **cable profile** *profile-type profile-name*
MAC ドメイン プロファイルには、*profile-type* として **mac-domain** を指定します。

```
Router(config)#cable profile mac-domain MD1
Router(config-profile-md)#cable dynamic-secret mark
Router(config-profile-md)#cable shared-secret 0 cisco
Router(config-profile-md)#cable ip-init ipv4
Router(config-profile-md)#cable mtc-mode
Router(config-profile-md)#cable mrc-mode
Router(config-profile-md)#cable privacy mandatory
Router(config-profile-md)#cable privacy bpi-plus-policy
```

プライマリ ダウンストリーム プロファイルには、*profile-type* として **downstream** を指定します。

```
Router(config)#cable profile downstream DS1
Router(config-profile-ds)#cable rf-bandwidth-percent 20
```

```
Router(config-profile-ds)#cable attribute-mask 0x80000000
```

ワイドバンド ケーブル インターフェイス プロファイルには、*profile-type* として **wideband-interface** を指定します。

```
Router(config)#cable profile wideband-interface BG1
Router(config-profile-wb)#cable downstream attribute-mask 0x80000000
```

グローバル サービス グループ プロファイルには、*profile-type* として service-group を指定します。サービス グループ プロファイル内で、ケーブル バンドル関連の MAC ドメイン プロファイルとワイドバンド インターフェイス プロファイルを設定します。

```
Router(config)#cable profile service-group SG-16x8-1_1
Router(config-profile-sg)#cable bundle 71
Router(config-profile-sg)#mac-domain 0 profile md1
Router(config-profile-sg-md)#downstream sg-channel 0-7  profile ds1 upstream 0-3
Router(config-profile-sg-md)#upstream 0 sg-channel 0
Router(config-profile-sg-md)#upstream 1 sg-channel 1
Router(config-profile-sg-md)#upstream 2 sg-channel 2
Router(config-profile-sg-md)#upstream 3 sg-channel 3
Router(config-profile-sg-md)#upstream 4 sg-channel 4
Router(config-profile-sg-md)#upstream 5 sg-channel 5
Router(config-profile-sg-md)#upstream 6 sg-channel 6
Router(config-profile-sg-md)#upstream 7 sg-channel 7
Router(config-profile-sg-md)#us-bonding-group 1
Router(config-profile-sg-md-usbg)#upstream 0
Router(config-profile-sg-md-usbg)#upstream 1
Router(config-profile-sg-md-usbg)#upstream 2
Router(config-profile-sg-md-usbg)#upstream 3
Router(config-profile-sg-md-usbg)#upstream 4
Router(config-profile-sg-md-usbg)#upstream 5
Router(config-profile-sg-md-usbg)#upstream 6
Router(config-profile-sg-md-usbg)#upstream 7
Router(config-profile-sg-md-usbg)#attributes 8000000
Router(config-profile-sg-md-usbg)#exit
Router(config-profile-sg-md)#exit
Router(config-profile-sg)#

Router(config-profile-sg)#wideband-interface 1 profile BG1
Router(config-profile-sg-bg)#downstream sg-channel 0 15 rf-bandwidth-percent 10
Router(config-profile-sg-bg)#end
Router#
```

ステップ 2 **cable fiber-node**

ファイバ ノード コンフィギュレーション モードを開始します。ファイバ ノード コンフィギュレーション モードで次の項目を設定します。

- ダウンストリーム ポート
- アップストリーム ポート
- ダウンストリーム SG チャネルと RF チャネルのマッピング

- アップストリーム SG チャネルと US チャネルのマッピング
- グローバル サービス グループ マッピング
- 管理対象 MAC ドメイン

```
Router(config)#cable fiber-node 1
Router(config-fiber-node)#downstream integrated-cable 3/0/0
Router(config-fiber-node)#upstream upstream-cable 3/0/0
Router(config-fiber-node)#downstream sg-channel 0 15 integrated-cable 3/0/0 rf-channel 0
15
Router(config-fiber-node)#upstream sg-channel 0 7 upstream-cable 3/0/0 us-channel 0 7
Router(config-fiber-node)#service-group profile SG-16X8-1_1
```

次の作業

show cable fiber-node [*id*] **mapping** および **show cable fiber-node** [*id*] **derived** コマンドを使用して、インターフェイスの設定を確認します。

```
Router#show cable fiber-node 1 mapping
Fiber-node 1:
Upstream:
Sg chan       Us-chan        Op state
0             3/0/0 0        Up
1             3/0/0 1        Up
2             3/0/0 2        Up
3             3/0/0 3        Up
4             3/0/0 4        Up
5             3/0/0 5        Up
6             3/0/0 6        Up
7             3/0/0 7        Up
Downstream:
Sg chan       Ds-rf-chan     Op state
0             3/0/0:0        Up
1             3/0/0:1        Up
2             3/0/0:2        Up
3             3/0/0:3        Up
4             3/0/0:4        Up
5             3/0/0:5        Up
6             3/0/0:6        Up
7             3/0/0:7        Up
8             3/0/0:8        Up
9             3/0/0:9        Up
10            3/0/0:10        Up
11            3/0/0:11        Up
12            3/0/0:12        Up
13            3/0/0:13        Up
14            3/0/0:14        Up
15            3/0/0:15        Up
```

```
Router#show cable fiber-node 1 derived
Fiber-node 1:
              interface                   Assoc successed
mac-domain 0  Cable3/0/0                  Y
Wideband 1    Wideband-Cable3/0/0:0       Y
Router#
```

インターフェイスの関連付けを確認するには、**show cable mac-domain fiber-node** コマンドを使用します。

```
Router#show cable mac-domain fiber-node 1 md 0 downstream-service-group
Cable    MD-DS-SG              RF
IF       Id        Resource    Chan     Primary Chan
C3/0/0
Router#
```

```
Router#show cable mac-domain fiber-node 1 md 0 upstream-service-group
Cable MD 3/0/0
Router#
```

2 つの MAC ドメインを使用した16x8 のサービス プロファイル設定

ここでは、2 つの MAC ドメイン、分割ダウンストリーム、およびオーバーレイ アップストリーム チャネルを使用した 16x8 サービス グループに関するサービス グループ ベースの設定について説明します。

手順

ステップ 1 **cable profile** *profile-type profile-name*
MAC ドメイン プロファイルには、*profile-type* として **mac-domain** を指定します。

```
Router(config)#cable profile mac-domain MD1
Router(config-profile-md)#cable dynamic-secret mark
Router(config-profile-md)#cable shared-secret 0 cisco
Router(config-profile-md)#cable ip-init ipv4
Router(config-profile-md)#cable mtc-mode
Router(config-profile-md)#cable mrc-mode
Router(config-profile-md)#cable privacy mandatory
Router(config-profile-md)#cable privacy bpi-plus-policy
```

プライマリ ダウンストリーム プロファイルには、*profile-type* として **downstream** を指定します。

```
Router(config)#cable profile downstream DS1
Router(config-profile-ds)#cable rf-bandwidth-percent 20
Router(config-profile-ds)#cable attribute-mask 0x80000000
```

ワイドバンド ケーブル インターフェイス プロファイルには、*profile-type* として **wideband-interface** を指定します。

```
Router(config)#cable profile wideband-interface BG1
Router(config-profile-wb)#cable downstream attribute-mask  0x80000000
```

グローバル サービス グループ プロファイルには、*profile-type* として service-group を指定します。サービス グループ プロファイル内で、ケーブル バンドル関連の MAC ドメイン プロファイルとワイドバンド インターフェイス プロファイルを設定します。

```
Router(config)#cable profile service-group SG-16x4-1_2
Router(config-profile-sg)#cable bundle 71
Router(config-profile-sg)#mac-domain 0 profile md1
Router(config-profile-sg-md)#downstream sg-channel 0-15  profile ds1 upstream 0-3
Router(config-profile-sg-md)#upstream 0 sg-channel 0
Router(config-profile-sg-md)#upstream 1 sg-channel 1
Router(config-profile-sg-md)#upstream 2 sg-channel 2
Router(config-profile-sg-md)#upstream 3 sg-channel 3
Router(config-profile-sg-md)#us-bonding-group 1
Router(config-profile-sg-md-usbg)#upstream 0
Router(config-profile-sg-md-usbg)#upstream 1
Router(config-profile-sg-md-usbg)#upstream 2
Router(config-profile-sg-md-usbg)#upstream 3
Router(config-profile-sg-md-usbg)#exit
Router(config-profile-sg-md)#exit
Router(config-profile-sg)#

Router(config-profile-sg)#wideband-interface 1 profile BG1
Router(config-profile-sg-bg)#downstream sg-channel 0 7 rf-bandwidth-percent 10
Router(config-profile-sg-bg)#exit
Router(config-profile-sg)#wideband-interface 2 profile BG1
Router(config-profile-sg-bg)#downstream sg-channel 8 15 rf-bandwidth-percent 10
Router#
```

ステップ 2 **cable fiber-node**

ファイバ ノード コンフィギュレーション モードを開始します。ファイバ ノード コンフィギュレーション モードで次の項目を設定します。

- ダウンストリーム ポート
- アップストリーム ポート
- ダウンストリーム SG チャネルと RF チャネルのマッピング
- アップストリーム SG チャネルと US チャネルのマッピング
- グローバル サービス グループ マッピング
- 管理対象 MAC ドメイン

```
Router(config)#cable fiber-node 1
Router(config-fiber-node)#downstream integrated-cable 3/0/0
Router(config-fiber-node)#upstream upstream-cable 3/0/0
Router(config-fiber-node)#downstream sg-channel 0 7 integrated-cable 3/0/0 rf-channel 0 15
Router(config-fiber-node)#upstream sg-channel 0 3 upstream-cable 3/0/1 us-channel 0 3
Router(config-fiber-node)#service-group profile SG-16X4-1_2
Router(config-fiber-node)#exit
Router(config)#
```

```
Router(config)#cable fiber-node 2
Router(config-fiber-node)#downstream integrated-cable 3/0/0
Router(config-fiber-node)#upstream upstream-cable 3/0/1
Router(config-fiber-node)#downstream sg-channel 0 7 integrated-cable 3/0/0 rf-channel 8 15
Router(config-fiber-node)#downstream sg-channel 8 15 integrated-cable 3/0/0 rf-channel 0 7
Router(config-fiber-node)#upstream sg-channel 0 3 upstream-cable 3/0/1 us-channel 0 3
Router(config-fiber-node)#service-group profile SG-16X4-1_2
Router(config-fiber-node)#exit
Router(config)#
```

次の作業

show cable fiber-node [*id*] **mapping** および **show cable fiber-node** [*id*] **derived** コマンドを使用して、インターフェイスの設定を確認します。

MAC ドメイン分割設定

ここでは、MAC ドメイン分割設定について説明します。

（注）

- MAC ドメイン分割のシナリオでは、アップストリームの peer-node-us と管理対象 MAC ドメインを設定する必要があります。
- ファイバ ノード管理対象 MAC ドメインを設定した後、**cable managed fiber-node** コマンドによってケーブル インターフェイスを予約します。
- ファイバ ノードにピアがある場合、管理対象 MAC ドメインを追加することはできません。
- ファイバ ノードにピアがある場合、チャネル マッピングとアップストリーム peer-node-us の設定を変更することはできません。
- ファイバ ノードに管理対象 MAC ドメインがある場合、アップストリーム peer-node-us を削除することはできません。
- 2 つのファイバ ノードの両方だけがサービス グループ プロファイルに関連付けられ、MAC ドメインとワイドバンド インターフェイスが生成されます。
- 1 つのファイバ ノードとサービス グループ プロファイルの関連付けが解除されると、ただちに MAC ドメインおよびワイドバンド インターフェイスが削除されます。

手順

ステップ 1 cable profile mac-domain

MAC ドメイン、ボンディング グループ、プライマリ ダウンストリームに関するグローバル共通プロファイルを定義します。

```
Router(config)#cable profile mac-domain MD
Router(config-profile-md)#load-interval 30
Router(config-profile-md)#cable dynamic-secret mark
Router(config-profile-md)#cable shared-secret 0 cisco
Router(config-profile-md)#cable ip-init ipv4
Router(config-profile-md)#cable mtc-mode
Router(config-profile-md)#cable mrc-mode
Router(config-profile-md)#cable privacy mandatory
Router(config-profile-md)#cable privacy bpi-plus-policy
Router(config-profile-md)#cable privacy accept-self-signed-certificate
Router(config-profile-md)#cable privacy dsx-support
Router(config-profile-md)#cable privacy eae-policy capability-enforcement
Router(config-profile-md)#cable privacy kek life-time 300
Router(config-profile-md)#cable privacy retain-failed-certificates
Router(config-profile-md)#cable privacy skip-validity-period
Router(config-profile-md)#cable privacy tek life-time 180
Router(config-profile-md)#cable cm-status enable 3
Router(config-profile-md)#cable map-advance dynamic
Router(config-profile-md)#cable upstream 0 attribute-mask FFFFFFFF
Router(config-profile-md)#cable upstream 0 power-adjust continue 5
Router(config-profile-md)#cable upstream balance-scheduling
Router(config)#cable profile downstream DS
Router(config-profile-ds)#cable rf-bandwidth-percent 20
Router(config-profile-ds)#cable attribute-mask 0x80000000
Router(config)#cable profile wideband-interface BG
Router(config-profile-wb)#cable downstream attribute-mask 0x80000000
Router(config-profile-wb)#description BG
Router(config-profile-wb)#load-interval 30
```

ステップ 2 cable profile service-group

サービス グループ プロファイル内で、ケーブル バンドル関連の MAC ドメイン プロファイルとワイドバンド インターフェイス プロファイルを設定します。

```
Router(config)#cable profile service-group MD_SPLIT
Router(config-profile-sg)#cable bundle 1
Router(config-profile-sg)#mac-domain 0 profile MD
Router(config-profile-sg-md)#downstream sg-channel 0-15 profile DS
Router(config-profile-sg-md)#upstream 0 sg-channel 0
Router(config-profile-sg-md)#upstream 1 sg-channel 1
Router(config-profile-sg-md)#upstream 2 sg-channel 2
Router(config-profile-sg-md)#upstream 3 sg-channel 3
Router(config-profile-sg-md)#upstream 4 sg-channel 4
Router(config-profile-sg-md)#upstream 5 sg-channel 5
Router(config-profile-sg-md)#upstream 6 sg-channel 6
Router(config-profile-sg-md)#upstream 7 sg-channel 7
```

```
Router(config-profile-sg-md)#us-bonding-group 1
Router(config-profile-sg-md-usbg)#upstream 0
Router(config-profile-sg-md-usbg)#upstream 1
Router(config-profile-sg-md-usbg)#upstream 2
Router(config-profile-sg-md-usbg)#upstream 3
Router(config-profile-sg-md-usbg)#attributes 8000000
Router(config-profile-sg-md-usbg)#exit
Router(config-profile-sg-md)#us-bonding-group 2
Router(config-profile-sg-md-usbg)#upstream 4
Router(config-profile-sg-md-usbg)#upstream 5
Router(config-profile-sg-md-usbg)#upstream 6
Router(config-profile-sg-md-usbg)#upstream 7
Router(config-profile-sg-md-usbg)#attributes 8000000
Router(config-profile-sg-md-usbg)#exit
Router(config-profile-sg-md)#exit
Router(config-profile-sg)#wideband-interface 0 profile WB
Router(config-profile-sg-bg)#downstream sg-channel 0 7 rf-bandwidth-percent 1
Router(config-profile-sg-bg)#exit
Router(config-profile-sg)#wideband-interface 1 profile WB
Router(config-profile-sg-bg)#downstream sg-channel 8 15 rf-bandwidth-percent 1
```

ステップ 3 **cable fiber-node**

ファイバ ノード コンフィギュレーション モードを開始します。ファイバ ノード コンフィギュレーション モードで次の項目を設定します。

- ダウンストリーム ポート
- アップストリーム ポート
- ダウンストリーム SG チャネルと RF チャネルのマッピング
- アップストリーム SG チャネルと US チャネルのマッピング
- 抽象アップストリーム チャネル
- 管理対象 MAC ドメイン
- グローバル サービス グループ マッピング

```
Router(config)#cable fiber-node 67
Router(config-fiber-node)#downstream integrated-cable 6/0/6
Router(config-fiber-node)#upstream upstream-cable 6/0/6
Router(config-fiber-node)#downstream sg-channel 0 15 integrated-cable 6/0/6 rf-channel 0
15
Router(config-fiber-node)#upstream sg-channel 0 3 upstream-cable 6/0/6 us-channel 0 3
Router(config-fiber-node)#upstream sg-channel 4 7 peer-node-us
Router(config-fiber-node)#service-group managed md 0 cable6/0/6
Router(config-fiber-node)#service-group profile MD_SPLIT

Router(config)#cable fiber-node 69
Router(config-fiber-node)#downstream integrated-cable 6/0/6
Router(config-fiber-node)#upstream upstream-cable 6/0/1
Router(config-fiber-node)#downstream sg-channel 0 15 integrated-cable 6/0/6 rf-channel 0
15
```

```
Router(config-fiber-node)#upstream sg-channel 4 7 upstream-cable 6/0/1 us-channel 0 3
Router(config-fiber-node)#upstream sg-channel 0 3 peer-node-us
Router(config-fiber-node)#service-group managed md 0 cable6/0/6
Router(config-fiber-node)#service-group profile MD_SPLIT
```

第 12 章

DOCSIS ロード バランシング グループ

初版：2015 年 4 月 11 日

制限付きロード バランシング グループ（RLBG）/汎用ロード バランシング グループ（GLBG）のサポートは、DOCSIS 3.0 仕様に基づきます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *21*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

DOCSIS ロード バランシング グループの前提条件

ダウンストリームの動的ロードバランシング機能による制限付き/汎用ロードバランシング グループを含む DOCSIS ロード バランシング グループには、次の前提条件があります。

- RLBG 1 つと DOCSIS 2.0 GLBG 1 つにつきロード バランシング グループ（LBG）ID が 1 つ必要です。
- LBG 1 つにつきデフォルト ポリシー ID が 1 つ必要です。
- 登録時に、LBG に割り当てられたケーブル モデム（CM）に、シンプル ネットワーク管理プロトコル（SNMP）、ケーブル モデムのコンフィギュレーション ファイル、または Cisco ケーブル モデム終端システム（CMTS）設定により、ポリシー ID と優先順位も割り当てる必要があります。
- フィールドで一般的なタギングが使用されている場合、ケーブル モデムを登録するには、サービス タイプ識別子（STID）、サービス クラス名、DOCSIS のバージョンおよび機能のタイプ/長さ/値（TLV）の設定を Cisco CMTS に送信する必要があります。

DOCSIS ロード バランシング グループの制限事項

RLBG/GLBG サポートと DLB サポート機能を含む DOCSIS ロード バランシング グループ（LBG）には次の制限事項があります。

- 最大 256 の DOCSIS ポリシー、1 シャーシあたり 256 のルールがサポートされます。
- 最大 4 つのアップストリーム チャネルと最大 8 つのダウンストリーム チャネルがサポートされます。
- ラインカード（LC）間のケーブル モデムの設定、移動はサポートされません。
- チャネル制限機能が導入され、ターゲット アップストリーム チャネルの属性マスクがケーブル モデムの属性マスクと対立する場合、より高い負荷のアップストリームにあるケーブル モデムはロード バランシングの対象になりません。現在のロード バランシングにより、ケーブル モデムはターゲット アップストリームにのみ移動されるためです。ただし、属性マスクが設定されていないケーブル モデムは、そのままロード バランシングの対象である場合があります。ロード バランシング グループを導入する場合は、次のことを考慮してください。ターゲット アップストリームは常に、最も低い負荷を持つアップストリームです。同じ負荷を持つアップストリームが他にある場合、最も低いインデックスを持つアップストリームがターゲット アップストリームとして選択されます。
- チャネルを共有するすべての LBG で同じ LB 方法を使用することを推奨します。

RLBG/GLBG サポートと DLB サポート機能を含む DOCSIS LBG には、機能を横断する次の制限事項があります。

- Multiple Transmit Channel（MTC）モードで動作するケーブル モデムは、そのコンフィギュレーション ファイルに STID や LBG ID などの関連 TLV が含まれる場合も、RLBG 割り当てに登録することはありません。ただし、Multiple Receive Channel（MRC）モードで動作するケーブル モデムは、RLBG 割り当てに登録することができます。
- Cisco CMTS では、ケーブル モデムのコンフィギュレーション ファイルにエンコードされている特定の TLV を解析して、そのケーブル モデムに対する DCC 操作を禁止することができます。

- 複数のラインカード タイプからのチャネルの組み合わせが同じファイバ ノードに配置されている場合、MDD メッセージで DOCSIS MAC ドメイン ダウンストリーム サービス グループ（MD-DS-SG）チャネルは無視されます。

複数のラインカードからのチャネル、または複数のファイバ ノード内の 1 つの MAC ドメインのダウンストリーム チャネルを含む複雑なファイバ ノード設定の場合、モデムが w-online（ワイドバンド オンライン）にならない場合があります。MAC ドメインに複数の MD-DS-SG があると MDD には複数の MD-DS-SG が含まれることになるため、モデムはダウンストリームのあいまいさの解決を実行します。モデムは、他のラインカードからのダウンストリーム チャネルを解析する際に、MDD パケットを見逃し、チャネルと MD-DS-SG を不適格にします。次いでモデムは、要求されている MD-DS-SG はゼロであること（つまり MD-DS-SG はボンディング グループに参加しないこと）を CMTS に送信します。

同じ MD-DS-SG 内のチャネルを表示するには、**showcablemac-domaindownstream-service-group** コマンドを使用します。

RLBG/GLBG サポートと DLB サポート機能を含む DOCSIS LBG には、数量に関して次の制限事項があります。

- RLBG と DOCSIS 2.0 GLBG の合計数が 256 を超えることはできません。
- Cisco CMTS でタグの合計数が 256 を超えることはできません。
- DOCSIS 3.0 GLBG の合計数は、空きメモリによって制限されます。
- CM が 1 つのケーブル インターフェイスから別のインターフェイスに移動すると、ケーブル モデムのリセットが発生します。これは、LB による移動中に DCC の初期化 0 テクニックによってケーブル モデムがリセットされるためです。2 つのケーブル インターフェイスがそれぞれに異なる **cableip-init** コマンドで設定されている場合にもケーブル モデムはリセットされます。

DOCSIS ロード バランシング グループに関する情報

DOCSIS 2.0 の「自律的ロード バランシング」仕様は CM 集中型であり、1 チャネル（US または DS）を複数の RLBG の一部にします。したがって、DOCSIS 2.0 仕様を使用して、CM をどのチャネルにロード バランシングできるかを決定できます。

ダウンストリームの動的ロード バランシング機能により制限付き/汎用ロード バランシング、ナローバンド動的帯域幅共有を設定するには、次の概念を理解する必要があります。

サービス ベースのロード バランシング

DOCSIS 3.0 のモデム ベースのロード バランシング仕様を使用して、次のモデムごとの LB アクティビティを管理できます。

1. STID によるモデムと RLBG 間の関連付け
2. LBG ID によるモデムと RLBG 間の関連付け
3. モデムごとの LB ポリシーの割り当て

4 モデムごとの LB プライオリティの割り当て
5 モデムごとのチャネル制限

DOCSIS 3.0 モデム ベースの LB 仕様を実装することにより、Cisco CMTS は拡張されたサービス ベースの LB を提供することができます。サービス ベースの LB を使用すると、モデム ベースのプロビジョニングの負担が軽減され、オペレータはモデムのサービス タイプに基づいて LB アクティビティを選択的に制御できるようになります。たとえば、次に基づいてモデムを LB 用に分類できます。

- デバイス タイプ
- DOCSIS バージョン
- サービス クラス

その後、分類結果を使用してモデムを次の設定にマッピングすることにより、モデムの LB アクティビティを選択的に制御できます。

- LBG
- ポリシー（Policy）

サービス ベースの LB がイネーブルの場合、既存のサービス ベースのケーブル モデムの分離機能とチャネル制限は特殊なケースになり、同じ LB フレームワーク内で処理できます。

機能

一般的なタギングおよびサービス ベースの LB で、Cisco CMTS は次のように機能します。

- Cisco CMTS は、STID、サービス クラス名、DOCSIS バージョン、機能の TLV と MAC 組織固有識別子（OUI）を使用して、一部のモデムをユーザ定義のモデム分類子により分類できます。
- 各モデム分類子には固有のタグがあります。Cisco CMTS は各モデムに 1 つのタグを付けます。複数のタグが 1 つのケーブル モデムを照合する場合、最小のインデックスを持つタグがそのケーブル モデムに適用されます。
- Cisco CMTS は CM を分類してタグを割り当てます。そのタグを持つ RLBG が設定されている場合、CM はその RLBG に割り当てられます。
- Cisco CMTS は RLBG および DOCSIS ポリシーに対し、複数のタグを照合できます。
- Cisco CMTS では、競合が発生した場合、ユーザは CM コンフィギュレーション ファイルと SNMP 内の TLV を使用して、一般的なタギングが RLBG または DOCSIS ポリシー割り当てをオーバーライドするかどうかを設定できます。
- 自律的 LB を実行する場合、Cisco CMTS は、アドミッション制御、SF 属性マスク、CM 属性マスクについて、特定の CM でターゲット チャネルを使用できることを保証します。
- ユーザは、CM で DCC が何回失敗するとその CM が Cisco CMTS での動的 LB から除外されるかを設定できます。

- Cisco CMTS でユーザは DCC 初期化テクニックを設定するか、またはアップストリーム チャネル変更（UCC）を LBG に対して使用するか、特定の送信元と宛先のペアに対して使用するかを設定できます。ただし、DCC は DOCSIS 1.0 モードでプロビジョニングされたケーブル モデムには発行されません。デフォルトでは、LBG に対する UCC は設定されていないため、DCC によりすべてのチャネルの変更が実行されます。
- Cisco CMTS は複数の論理 US チャネルを持つ物理 US チャネル上の少なくとも 1 つの論理チャネルでの LB をサポートします。
- DOCSIS 3.0 仕様により、ロード バランシング プライオリティが低いほど、ロード バランシング動作により CM が移動する可能性が高くなることが示されています。
- CM に低帯域幅を設定するポリシーを作成できます。LBG は、スループットがしきい値を超えているケーブル モデムのみを移動できます。

互換性

ダウンストリームおよびアップストリームの自律的ロード バランシングはともに単一チャネルのケーブル モデムでサポートされます。

RLBG/GLBG 割り当て

ユーザは各 RLBG に 1 つ以上のサービス タイプ ID を設定できます。ユーザはさらに、CLI または SNMP を使用して、特定のケーブル モデムを特定の STID および RLBG ID に限定するよう Cisco CMTS を設定できます。ただしこのような設定が行われると、Cisco CMTS ではコンフィギュレーション ファイルの STID および RLBG ID が無視されます。

STID が CLI または SNMP で設定されているか、または STID がケーブル モデムのコンフィギュレーション ファイルに存在する場合、Cisco CMTS は、信号送信済みサービス タイプのある、RLBG からのアップストリームおよびダウンストリーム チャネル（そのようなチャネルが存在する場合）を選択します。ただし、信号送信済みサービス タイプのあるアップストリームおよびダウンストリーム チャネルが存在しない場合、Cisco CMTS は信号送信済みサービス タイプのないアップストリームおよびダウンストリーム チャネルを割り当てます。

LBG ID が CLI または SNMP で設定されているか、または LBG ID がケーブル モデムのコンフィギュレーション ファイルに存在する場合、Cisco CMTS は、選択可能なアップストリームおよびダウンストリーム チャネルを確認し、そこに信号送信済み LBG に関連付けられたチャネル ペアが含まれる場合にはその信号送信済み LBG にケーブル モデムを割り当てます。これらの条件が満たされない場合、Cisco CMTS は LBG ID を無視します。

STID（存在する場合）および LBG ID（存在する場合）の要件を満たす選択可能なアップストリームおよびダウンストリーム チャネルが複数存在する場合、Cisco CMTS は、コンフィギュレーション ファイルで要求されているケーブル モデムの必須および禁止属性マスクを満たすアップストリームおよび/またはダウンストリーム チャネルを選択します。アップストリームおよびダウンストリーム チャネルがこれらの基準を満たさない場合、Cisco CMTS はケーブル モデムの属性マスクを無視して代替のアップストリームおよび/またはダウンストリーム チャネルを選択できます。

登録時にケーブル モデムのターゲット チャネル ペアを決定する際、Cisco CMTS は、現在のチャネル ペア、ケーブル モデム（CM-US-SG-ID）の MD-DS-SG-ID（メディア アクセス制御ドメイン

のダウンストリーム サービス グループ ID）およびケーブル モデム（CM-DS-SG-ID）の MD-US-SG-ID（メディア アクセス制御ドメインのアップストリーム サービス グループ ID）、さらに存在する場合はファイバ ノード（FN）の設定をチェックすることにより、ケーブル モデムに実際に到達可能なターゲット チャネル ペアを検出しようと試みます。このターゲット チャネル ペアがケーブル モデムで使用可能であり、現在のチャネル ペアとは異なる場合、Cisco CMTS は DCC テクニック 0 またはダウンストリーム周波数オーバーライド（DFO）を使用して CM を移動する必要があります。

Cisco CMTS が CM 用に複数の候補 RLBG を特定しても、ケーブル モデムを実際に関連付けるファイバ ノード設定を決定できない、または関連付けられた RLBG が使用不可であるか（ロード バランス グループのインターフェイスがディセーブルになっているか管理上のダウン状態になっている）を判断できない場合、Cisco CMTS は最も低いグループ インデックスを持つ RLBG にケーブル モデムを割り当てます。この割り当てにより、Cisco CMTS はケーブル モデムをそれが物理的に接続されていないインターフェイスに移動しようと試みることになり、その結果、その CM へのサービスが停止します。

Cisco CMTS は RLBG 割り当て時にファイバ ノードのチェックを実施します。

Cisco CMTS は次の RLBG 割り当てルールに従います。

- ファイバ ノード設定がない場合、RLBG の候補リストは変更されません。ただし、ファイバ ノードが設定される場合、ファイバ ノードは実際のファイバ ノード接続を反映するよう適切に設定される必要があります。
- ケーブル モデムがファイバ ノード内にある場合、ファイバ ノード内にある RLBG のみが選択されます。
- ケーブル モデムがファイバ ノード内にない場合、つまりファイバ ノード設定が全チャネルには適用しない場合、ファイバ ノード内に存在しない RLBG のみが選択されます。
- RLBG が複数のファイバ ノードをまたいでいる場合、RLBG はファイバ ノード内にはないと見なされます。
- 候補の RLBG が検出されない場合、ケーブル モデムは GLBG（存在する場合）に割り当てられます。

チャネルの割り当て

MRC モードで動作するケーブル モデムの場合、登録要求メッセージでは、Cisco CMTS が割り当てるアップストリームおよびダウンストリーム チャネルの選択に影響する複数の TLV を使用できます。複数の TLV の競合を避けるため、Cisco CMTS は以下に定義されている優先順位に従います。

1. TLV 56：チャネルの割り当て
2. TLV 43.11：サービス タイプ識別子
3. TLV 43.3：ロード バランシング グループ ID
4. TLV 24/25.31-33：サービス フロー属性マスク
5. TLV 43.9：CM 属性マスク

MRC モードで動作しないケーブル モデムの場合、Cisco CMTS はこの TLV 優先順位に従う必要があります。

1. TLV 43.11：サービス タイプ識別子
2. TLV 43.3：ロード バランシング グループ ID
3. TLV 43.9：CM 属性マスク
4. TLV 24/25.31-33：サービス フロー属性マスク

（注） 新しい受信チャネル構成（RCC）および送信チャネル構成（TCC）のターゲットが選択されたときは、ケーブル モデムのサービス レベルが低下しないことを確認してください。ケーブル モデムがサービス レベルを変更しないままにできるように、ターゲットの合計 RCC および TCC はソースの合計 RCC および TCC 未満にならないようにしてください。そうしないと、以降のリリースで、大容量のケーブル モデムがオンラインになったときに不均衡な結果が生じる可能性があります。

また Cisco CMTS は、登録要求メッセージで定義された DOCSIS 3.0 ケーブル モデムの機能を考慮して、CM が要求するチャネルの最大数を割り当てます。

次の表は、RLBG と GLBG 割り当てのロード バランシング マトリクスを定義するものです。

表 *22*：*DOCSIS* ケーブル モデムの *RLBG* 割り当て

動作モード	MAC バージョン				
	DOCSIS 3.0 CM	**DOCSIS 2.x CM**	**DOCSIS 2.0 CM**	**DOCSIS 1.1 CM**	**DOCSIS 1.0 CM**
非 MRC モード（オンライン）	割り当て	割り当て	割り当て	割り当て	割り当て
MRC モードのみ（w-online）	割り当て	割り当て	割り当て	該当なし	該当なし
MRC/MTC モード（UB-online）	割り当て	該当なし	該当なし	該当なし	該当なし
	DOCSIS 3.0 ケーブル モデムは DOCSIS 3.0 RLBG に割り当て	該当なし	該当なし	該当なし	該当なし

表 *23*：*DOCSIS* ケーブル モデムの *GLBG* 割り当て

動作モード	MAC バージョン				
	DOCSIS 3.0 CM	**DOCSIS 2.x CM**	**DOCSIS 2.0 CM**	**DOCSIS 1.1 CM**	**DOCSIS 1.0 CM**

動作モード	MAC バージョン				
非 MRC モード（オンライン）	MD-DS-SG-ID/MD-US-SG-ID なしで DOCSIS 2.0 GLBG に割り当て				
	MD-DS-SG-ID/MD-US-SG-ID ありで DOCSIS 3.0 GLBG に割り当て		該当なし	該当なし	該当なし
MRC モードのみ（w-online）	MD-DS-SG-ID/MD-US-SG-ID なしで DOCSIS 2.0 GLBG に割り当て				
	MD-DS-SG-ID/MD-US-SG-ID ありで DOCSIS 3.0 GLBG に割り当て		該当なし	該当なし	該当なし
MRC/MTC モード（UB-online）	割り当て	該当なし	該当なし	該当なし	該当なし
	DOCSIS 3.0 ケーブル モデムは DOCSIS 3.0 GLBG に割り当て	該当なし	該当なし	該当なし	該当なし

次の表に、ボンディングされた CM および未ボンディングの CM の「移動」に使用されるロード バランシング メソッドおよび動作の一覧を示します。

表 *24*：ボンディングされた（および未ボンディングの）ケーブル モデムを移動するためのロード バランシング メソッド

モデムのモード	動的サービスの要求（初期化テクニック）	
	MAC ドメイン内	**MAC ドメイン間**
DOCSIS 3.0 ケーブルモデム（MTC モード）	該当なし	DCC 初期化テクニック 0
DOCSIS 3.0/DOCSIS 2.x ケーブルモデム（MRC 単独モード）	DCC 初期化テクニック 0 （注） RLBG 外のプライマリ DS を含む CM は、DOCSIS 2.0 LB により RLBG 内に移されます。	DCC 初期化テクニック 0
DOCSIS 3.0 ケーブルモデム（MRC 単独モード）	DCC （注） RLBG 外の CM は、DOCSIS 2.0 LB により RLBG 内に移されます。	DCC 初期化テクニック 0
DOCSIS 2.x ケーブルモデム（MRC 単独モード）	DCC/UCC （注） RLBG 外の CM は、DOCSIS 2.0 LB により RLBG 内に移されます。	DCC 初期化テクニック 0

モデムのモード	動的サービスの要求（初期化テクニック）	
DOCSIS 2.0/DOCSIS 1.1 ケーブルモデム（NB モード）	DCC （注） RLBG 外の CM は、DOCSIS 2.0 LB により RLBG 内に移されます。	DCC 初期化テクニック 0
	UCC （注） RLBG 外の CM は、DOCSIS 2.0 LB により RLBG 内に移されます。	UCC
DOCSIS 1.0（NB モード）	CM の再初期化を強制 （注） RLBG 外の CM は、DOCSIS 2.0 LB により RLBG 内に移されます。	CM の再初期化を強制
	UCC （注） RLBG 外の CM は、DOCSIS 2.0 LB により RLBG 内に移されます。	UCC

表 *25* : ***DCC/DBC*** を使用した、ボンディングされた（および未ボンディングの）ケーブル モデムのロード バランシング

チャネル	**MRC、非 MTC モードの CM**	**単一の US/DS を含む DOCSIS 1.1/DOCSIS 2.0 ケーブルモデム**	**単一の US/DS を含む DOCSIS 1.0 ケーブルモデム**
アップストリーム（US）	DCC	DCC	UCC
ダウンストリーム（DS）	NA（同じ MAC ドメイン内）	DCC（同じ MAC ドメイン内）。	CM の再初期化を強制
	MAC ドメイン間でケーブルモデムを移動させる場合は、DCC と初期化テクニック 0。	MAC ドメイン間でケーブルモデムを移動させる場合は、DCC と初期化テクニック 0。	CM の再初期化を強制

チャネル割り当てのエラー処理

この制限が変更されます。チャネルのインターフェイス状態が「administratively down」ではない限り、すべてのチャネルが LBG 割り当てに使用できます。その他のロード バランシング動作（DCC、UCC、またはDBCを使用してモデムを移動するなど）では、チャネルのインターフェイス状態は「initial」、「up」、「suspicious」、または「testing」ステータスである必要があります。

LBG が無効なときは次の条件が適用されます。

- すべてのロード バランシング条件に一致するケーブル モデムは LBG に割り当てできます。
- ロード バランシングのためのケーブル モデム移動は無効ですが、LBG 外部から LBG 内部へのケーブル モデムの移動は許可されます。

DOCSIS 3.0 ケーブル モデムの単一アップストリーム モードでのアップストリーム ロード バランシング

アップストリーム ロード バランシング機能により、Cisco CMTS ルータは、単一アップストリーム モードのワイドバンドおよびナローバンド ケーブル モデムのアップストリーム トラフィックを、効果的に処理することができます。単一アップストリーム モード（Mx1）とは、モデムが複数のアップストリームチャネル上のアップストリームトラフィックを送信できないことを意味します。ワイドバンドまたはナローバンド ケーブル モデムの 1 つのアップストリーム チャネルにトラフィックの過負荷が発生すると、Cisco CMTS ルータは、同じロード バランシング グループ内の別のアップストリーム チャネルにケーブル モデムを自動的に移動します。

（注） 単一アップストリーム モードで動作しているケーブル モデムは、モデムのプライマリ チャネルに基づいて 1 つのロード バランシング グループに割り当てられます。単一アップストリーム モードのケーブル モデムは、Multiple Receive Channel（MRC）モードまたはナローバンド モードをサポートすることができます。ただし、単一アップストリーム モードのケーブル モデムは、Multiple Transmit Channel（MTC）モードをサポートできません。

DOCSIS 2.0 GLBG の自動生成

Cisco CMTS は、DOCSIS 2.0 GLBG を自動的に実装しません。DOCSIS 2.0 GLBG は、ファイバノードと MAC ドメイン（FN-MD）の新しいペアが追加された後に、手動で構成します。

新しい FN-MD ペアの追加、および MAC ドメイン、ケーブル モデム、サービス グループ（MD-CM-SG）の新しい組み合わせの解決の後に、DOCSIS 2.0 GLBG を自動的に生成するような強化です。この機能強化は、新しいコマンド **cableload-balanced20GLBGauto-generate** によって実装されます。このコマンドには、ファイバノード設定用に DOCSIS 2.0 GLBG を更新するオプションがあります。

独立したアップストリーム/ダウンストリーム スループットのルール

現在のアップストリームまたはダウンストリームのロードバランシングでは、ロードバランシング動作でモデムを移動するために、Cisco CMTS はアップストリームまたはダウンストリームのロード バランシング動作に対して、アップストリームとダウンストリームの両方のスループットに関する DOCSIS ポリシー スループット ルールを適用します。つまり、ダウンストリームのロードバランシングでは、アップストリームとダウンストリームの両方のルールセットが適用され、アップストリームのロードバランシングでも同様に、両方のルールセットが適用されます。これにより、低アップストリームまたは高ダウンストリーム スループット、かつ高アップストリームまたは低ダウンストリーム スループットでのモデムの移動が防止されます。

アップストリームまたはダウンストリーム スループット ルールは、対応するアップストリームまたはダウンストリーム ロードバランシング動作に対して個別に確認されます。アップストリーム ロードバランシングではアップストリーム スループット ルールのみが確認され、ダウンストリーム ロード バランシングではダウンストリーム スループット ルールのみが確認されます。

独立したアップストリーム/ダウンストリーム ルールにおいては、次の重要なポイントが実装されます。

- ロード バランシング動作にケーブル モデムのダウンストリーム チャネルの変更のみが含まれ、アップストリームチャネルの変更が含まれない場合、ダウンストリームの下位境界ルールだけが確認されます。
- ロード バランシング動作にケーブル モデムのアップストリーム チャネルの変更のみが含まれ、ダウンストリームチャネルの変更が含まれない場合、アップストリームの下位境界ルールだけが確認されます。
- ロード バランシング動作にケーブル モデムのアップストリーム チャネルとダウンストリーム チャネルの両方の変更が含まれる場合、モデム ルール チェックではその（アップストリームまたはダウンストリーム）ロードバランシングのすべてのルールに合格する必要があります。
- 設定されたロードバランシング ポリシーが **pure-ds-load** である場合、ダウンストリーム ルールのみが検査されます。
- 設定されたロードバランシング ポリシーが **us-across-ds** であるか、**us-across-ds** と **pure-ds-load** の両方である場合は、2 種類のターゲット インターフェイスが次のように発生します。
  - ローカル インターフェイス：ケーブル モデムは、アップストリームを送信元と共有します。ダウンストリーム ロード バランシング動作だけが発生します。
  - リモート インターフェイス：ケーブル モデムは、アップストリームを送信元と共有しません。アップストリーム/ダウンストリーム ロード バランシングは、アップストリームの負荷によってトリガーされます。

設定されたロード バランシング ポリシーが us-across-ds でも pure-ds-load でもない場合、ロード バランシングは Mac ドメインの負荷に基づいて行われます。

DOCSIS ロード バランシング グループの設定方法

ダウンストリームの動的ロード バランシング機能による制限付き/汎用ロード バランシングおよびナローバンド動的帯域幅共有は、次のように設定できます。

- DOCSIS 仕様により、ユーザは Cisco CMTS で DOCSIS 2.0 汎用ロード バランシング グループ（GLBG）を設定できます。Cisco CMTS は、メディア アクセス制御ドメイン、ケーブル モデム、サービス グループ（MD-CM-SG）のそれぞれに DOCSIS 3.0 GLBG を自動的に作成し、GLBG がアップストリームとダウンストリームの両チャネルを含むかどうかをチェックします。

- どの RLBG にもプロビジョニングされておらず、MD-CM-SG を解決できないケーブル モデムは、DOCSIS 2.0 GLBG に割り当てられます。ただし、ケーブル モデムは、MD-CM-SG を解決すると DOCSIS 3.0 GLBG に割り当てられます。
- ユーザは、RLBG と任意のアップストリームまたはダウンストリーム チャネルを Cisco CMTS 上の複数の RLBG に設定できます。RLBG がアップストリーム チャネルとダウンストリーム チャネルの両方を含むかどうかが、Cisco CMTS によりチェックされます。RLBG は複数の MD をまたぐことができます。
- 既存の Cisco LB 方式による下位互換性は維持されます。ユーザは、新旧の DOCSIS 3.0 準拠 LB 方式を切り替えることができます。

（注） Cisco IOS システムがアップグレードされたときに、DOCSIS ロード バランシング グループの docsis-policy 設定が **show running-config** コマンド出力からなくなった場合は、**docsis-policy** *policy-id* コマンドを再度使用して docsis-policy を DOCSIS ロード バランシング グループに適用してください。

次の項では、DOCSIS ロードバランシング グループを作成および設定して Cisco CMTS で DOCSIS ロード バランシングを有効にする方法について説明します。

DOCSIS 3.0、2.0 RLBG、DOCSIS 2.0 GLBG の設定

ここでは、DOCSIS ロード バランシング グループの作成方法と設定方法について説明します。従来のワークロード バランシング グループとは異なる DOCSIS ロード バランシング グループには個別のコンフィギュレーション モードがあります。

（注） UGS/PCMM ポリシーとしきい値は DOCSIS 3.0 LB には適用されません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**cableload-balancedocsis-enable** 例： `Router(config)# cable load-balance docsis-enable`	Cisco CMTS での DOCSIS ロード バランシングをイネーブルにします。
ステップ 4	**cableload-balancedocsis-group** *docsis-group-id* 例： `Router(config)# cable load-balance docsis-group 1`	次のパラメータを使用して、Cisco CMTS で DOCSIS ロード バランシング グループを作成します。 ルータは、DOCSIS ロード バランシング グループのコンフィギュレーション モードを開始します。
ステップ 5	**init-tech-list** *tech-list* [**ucc**] 例： `Router(config-lb-group)# init-tech-list 1 ucc`	Cisco CMTS でケーブル モデムをロード バランシングする DCC 初期化テクニックを設置します。
ステップ 6	**downstream** {**Cable**{*slot/subslot/port*|*slot/port*}|**Integrated-Cable**{*slot/subslot/bay*|*slot/port*} {**rf-channel** *group list*}|{| *slot/port*} {**rf-channel** *group list*}} 例： `Router(config-lb-group)# downstream integrated-Cable 5/0/0 rf-channel 2`	ダウンストリーム RF チャネルを設定します。
ステップ 7	**upstreamCable** {*slot/subslot/port*| *slot/port*} *upstream-list* 例： `Router(config-lb-group)# upstream Cable 1/0 2`	次のパラメータを使用してアップストリーム チャネルを設定します。
ステップ 8	**docsis-policy** *policy-id* 例： `Router(config-lb-group)# docsis-policy 0`	CM で別のポリシーを選択していない場合、CM に割り当てられたデフォルト ポリシーになるパラメータを使用してグループにポリシーを割り当てます。

	コマンドまたはアクション	目的
ステップ 9	**restricted** 例： `Router(config-lb-group)# restricted`	制限されたグループ タイプを選択します。デフォルトでは、一般グループ タイプが選択されています。
ステップ 10	**init-tech-ovrCable** {*slot/subslot/port*| *slot/port*} *upstream* **Cable** {*slot/subslot/port*} | *slot/port upstream* **init-tech-list** *0-4*[**ucc**] 例： `Router(config-lb-group)# init-tech-ovr Cable 8/1/0 0 Cable 8/1/1 1 init-tech-list 1 ucc`	物理アップストリーム チャネル ペアを上書きする DCC 初期化テクニックを設定します。また、**init-tech-ovr** コマンドを使用すると、動的アップストリーム ロード バランシング中にモデムに対して UCC を使用できるかどうかを判断できます。 次のパラメータは、物理アップストリーム チャネル ペアを上書きします。 （注） **init-tech-list** キーワードは、ロードバランシング グループに追加されないアップストリームを受け入れます。アップストリーム チャネル ペアは、アップストリームが追加されるまで無効です。ロードバランシング グループが削除されると、すべてのアップストリームチャネルペアも削除されます。
ステップ 11	**service-type-id** *string* 例： `Router(config-lb-group)# service-type-id commercial`	適切に制限されたロード バランシング グループ（RLBG）を決定するには、次のパラメータを使用して、ケーブル モデムがプロビジョニングされたサービス タイプ ID と比較するサービス タイプ ID を追加します。
ステップ 12	**tag** *tag name* 例： `Router(config-lb-group)# tag t1`	RLBG にタグを追加します。
ステップ 13	**interval** <*1-1000*> 例： `Router(config-lb-group)# interval 60`	インターフェイスの負荷を確認するまで Cisco CMTS が待機する時間の間隔を設定します。

	コマンドまたはアクション	目的
ステップ 14	**method** {**modems** | **service-flows** | **utilization**} {**us-method** {**modems** | **service-flows** | **utilization**}} 例： `Router(config-lb-group)# method modems us-method modems`	負荷の決定にCisco CMTSが使用する方法を選択します。

ステップ 15	**policy**{**pcmm** | **ugs** | **us-across-ds** | **pure-ds-load**}
	
	例：
	
	`Router(config-lb-group)# policy us-across-ds`
	`Router(config-lb-group)# policy ugs`
	`Router(config-lb-group)# policy pure-ds-load`
		バランシングするサービス フロー タイプに基づいてモデムを選択します。

ステップ 16	**threshold** {**load** {**minimum** *<1-100>* | *<1-100>*}| **pcmm** *<1-100>* | **stability** *<0-100>* | **ugs** *<1-100>*}
	
	例：
	
	`Router(config-lb-group)# threshold load minimum 10`
	`Router(config-lb-group)# threshold pcmm 70`
	`Router(config-lb-group)# threshold load 10`
	`Router(config-lb-group)# threshold stability 50`
	`Router(config-lb-group)# threshold ugs 70`
		ロード バランシングが発生する下限の使用率を選択します。

ステップ 17	**exit** 例： `Router# exit`	DOCSIS LBG コンフィギュレーションを終了します。

DOCSIS 3.0 GLBG の設定

ここでは、DOCSIS 3.0 GLBG を設定する方法と DOCSIS 3.0 の一般グループに DOCSIS 3.0 認定のデフォルト値を設定する方法について説明します。

（注） このライン カードのケーブル インターフェイスが「シャットダウンなし」状態の場合、関連する DOCSIS 3.0 GLBG は実行中の設定で復元されます。

DOCSIS 3.0 汎用ロード バランシング グループの設定

ここでは、DOCSIS 3.0 汎用ロード バランシング グループの設定方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cableload-balancedocsis-enable** 例： `Router(config)# cable load-balance docsis-enable`	Cisco CMTS での DOCSIS ロード バランシングをイネーブルにします。
ステップ 4	**cableload-balancedocsis-groupFN** *fn-id***MD** *cable*{*slot/subslot/port*| *slot/port*} 例： `Router(config)# cable load-balance docsis-group FN 1 MD c5/0/0`	DOCSIS ロード バランシング グループのコンフィギュレーション モードを開始します。
ステップ 5	**init-tech-list***tech-list*[**ucc**] 例： `Router(config-lb-group)# init-tech-list 1 ucc`	次のパラメータを使用して、DCC 初期化テクニック リストを設定します。
ステップ 6	**disable** 例： `Router(config-lb-group)# disable`	ロード バランシング グループを無効にします。
ステップ 7	**docsis-policy** *policy-id* 例： `Router(config-lb-group)# docsis-policy 0`	ロード バランシング グループのポリシーを設定します。

	コマンドまたはアクション	目的
ステップ 8	**interval** *1 ～ 1000* 例： `Router(config-lb-group)# interval 10`	インターフェイス ポーリングの間隔を設定します。
ステップ 9	**method** {**modems** | **service-flows** | **utilization**} {**us-method** {**modems** | **service-flows** | **utilization**}} 例： `Router(config-lb-group)# method modems us-method modems`	ロード バランシングのタイプまたは方法を設定します。
ステップ 10	**policy** {**pcmm** | **ugs** | **us-across-ds** | **pure-ds-load**} 例： `Router(config-lb-group)# policy us-across-ds`	ロード バランシングのポリシーを設定します。
ステップ 11	**threshold** {**load** {**minimum** *1-100* | *1-100*} | **pcmm** *1-100* | **stability** *0-100* | **ugs** *1-100*} 例： `Router(config-lb-group)# threshold pcmm 70`	ロード バランシングのしきい値をパーセントで設定します。
ステップ 12	**exit** 例： `Router# exit`	DOCSIS ロード バランシング グループのコンフィギュレーション モードを終了します。

DOCSIS 3.0 ロード バランシング グループのデフォルト値の設定

ここでは、Cisco CMTS で DOCSIS 3.0 汎用グループ用の DOCSIS 3.0 認定のデフォルト値を設定する方法について説明します。DOCSIS 3.0 汎用グループは、ファイバ ノード（FN）設定から取得した各 MD-CM-SG に対して自動的に作成されます。グループ パラメータはデフォルト値として設定されます。

（注） DOCSIS 3.0 認証に設定されたデフォルト値は、新しく自動的に作成された DOCSIS 3.0 GLBG に適用可能であり、既存の DOCSIS 3.0 GLBG には影響しません。DOCSIS 3.0 GLBG を削除して再作成しても、そのグループ パラメータは変わりません。

（注） インターフェイス ポーリング間隔、ロード バランシング メソッド、モデム選択のポリシー、およびしきい値の使用率（%）のデフォルト設定は、DOCSIS 3.0 汎用グループで設定できます。詳細については、『Cisco CMTS Cable Command Reference』を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cableload-balanced30-ggrp-defaultdisable** 例： `Router(config)# cable load-balance d30-ggrp-default disable`	DOCSIS 3.0 の汎用ロード バランシング グループ（GLBG）のデフォルト値を無効にします。
ステップ 4	**cableload-balanced30-ggrp-defaultinit-tech-list** *tech-list* 例： `Router(config)# cable load-balance d30-ggrp-default init-tech-list 1`	デフォルトの DOCSIS 3.0 GLBG DCC と動的ボンディング変更（DBC）の初期化テクニックを設定します。
ステップ 5	**cableload-balanced30-ggrp-defaultdocsis-policy** *0-0xffffffff* 例： `Router(config)# cable load-balance d30-ggrp-default docsis-policy 2`	デフォルトの DOCSIS 3.0 GLBG ポリシー ID を設定します。
ステップ 6	**exit** 例： `Router# exit`	グローバル コンフィギュレーション モードを終了します。

RLBG またはサービス タイプ ID へのケーブル モデムの設定

ここでは、Cisco CMTS で静的にプロビジョニングされたケーブル モデムのリストを RLBG またはサービス タイプ ID に設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cableload-balancerestrictmodem** *index mac-addr*[*mac-mask*] {**docsis-group** *docsis-group-id* |**service-type-id** *string*} 例： `Router(config)# cable load-balance restrict modem 1 001a.c30c.7eee FFFF.FFFF.0000 docsis-group 100`	共通 MAC マスクを使用してモデムまたはモデム グループをロード バランシング グループまたはサービス タイプ ID に割り当てます。
ステップ 4	**exit** 例： `Router# exit`	グローバル コンフィギュレーション モードを終了します。

ルールとポリシーの設定

ここでは、ロード バランシング時のモデムの移動を制限するために、ルールと DOCSIS ポリシーを作成および設定する方法について説明します。ルールでは、モデムの移動とその時間帯を決定します。時間帯は秒単位で測定され、開始時間は午前 0 時から始まり、秒単位で測定されます。ルールは個別に作成され、ポリシーと組み合わせることができます。ユーザは 1 つ以上のルールで構成される DOCSIS ポリシーを作成できます。複数のルールが DOCSIS ポリシーに含まれる場合は、すべてのルールが適用されます。各グループにはデフォルトの DOCSIS ポリシーがあります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cableload-balancerule** *rule-id* 例： `Router(config)# cable load-balance rule 1`	モデムの移動を防止するルールを作成します。
ステップ 4	**cableload-balancerule** rule-id {**enabled** | **disabled** | {**disable-perioddis-start** *0-86400* **dis-period** <*0-86400*>}| **disable-throughput-lowerboundds**| **us** *thrupt in kbps* | **vdoc-enabled}** 例： `Router(config)# cable load-balance rule 1 disable-period dis-start 40 dis-period 50`	ルールを作成します。 （注） 静的マルチキャスト グループは、適切なバンドル インターフェイスと転送インターフェイスで、このルールを有効にするように設定する必要があります。この機能は、ファイバ ノード設定およびマルチキャスト暗号化から派生するロード バランシング グループではサポートされません。
ステップ 5	**cableload-balancedocsis-policy** *policy-id* **rule** *rule-id* 例： `Router(config)# cable load-balance docsis-policy 2 rule 1`	次のパラメータを設定したDOCSISポリシーと特定のルールを関連付けます。
ステップ 6	**exit** 例： `Router# exit`	グローバル コンフィギュレーション モードを終了します。

トラブルシューティングのヒント

問題 **cable load-balance rule** *rule-id***disable-period dis-start** *start-time***dis-period** *disable-period* コマンドを使用することで、ロード バランシングを無効にして翌日有効にすると、設定済みの *disable-period* ではなく、午前 12 時にロード バランシングが有効になります。

考えられる原因 ロード バランシング ルールは、1 つのロード バランシング ルールを使用して翌日（つまり、24 時間後）に無効および有効にすることはできません。

解決法 ロード バランシングを無効にして、翌日に有効にするには、別のロード バランシング ルールを設定します。ロードバランシングを無効にするルールを設定するには、**cable load-balance rule** *rule-id***disable-period dis-start** *start-time***dis-period 0** コマンドを使用します。ロード バランシングを有効にするルールを設定するには、**cable load-balance rule** *rule-id***disable-period dis-start 0 dis-period** *disable-period* コマンドを使用します。これにより、翌日に有効になります。

ケーブル モデム移動の失敗に応じたロード バランシング パラメータの設定

ここでは、CM が動的ロード バランシング グループから削除されるまでに、失敗可能な回数を設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cableload-balancemodemmax-failures** *0 ～ 100* 例： `Router(config)# cable load-balance modem max-failures 10`	CM が動的ロードバランシング グループから削除されるまでに、失敗可能な回数を設定します。
ステップ 4	**exit** 例： `Router# exit`	グローバル コンフィギュレーション モードを終了します。

TLV タイプ タグの作成と設定

TLV タイプ一致ルールのタグは、このセクションで作成および設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権EXECモードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cabletag** *1 ～ 1000* 例： `Router(config)# cable tag 1`	タグを作成します。 cmts-tag コンフィギュレーション モードを開始します。
ステップ 4	**name** *tag name* 例： `Router(cmts-tag)# name CSCO`	タグの名前を指定します。
ステップ 5	[**exclude**]**service-type-id** *service-type-id* 例： `Router(cmts-tag)# service-type-id HSD`	指定されたサービス タイプ ID をタグに設定します。
ステップ 6	[**exclude**]**service-class***service-class-name* 例： `Router(cmts-tag)# service-class work`	指定されたサービス クラス名をタグに設定します。
ステップ 7	[**exclude**]**docsis-version** *docsis version* 例： `Router(cmts-tag)# docsis-version docsis20`	指定した DOCSIS バージョンのケーブル モデムをタグに設定します。
ステップ 8	**[exclude]oui** *oui of CM* 例： `Router(cmts-tag)# oui 00.1a.c3`	指定した OUI のケーブル モデムをタグに設定します。
ステップ 9	[**exclude**] **tlv** *type value* 例： `Router(cmts-tag)# tlv mrcs 4`	指定した TLV タイプをタグに設定します。

	コマンドまたはアクション	目的
ステップ 10	**override** 例： `Router(cmts-tag)# override`	RLBG のロード バランシング中に TLV または SNMP を上書きします。
ステップ 11	**exit** 例： `Router(cmts-tag)# exit`	cmts-tag コンフィギュレーション モードを終了します。
ステップ 12	**cableload-balancedocsis-group** *docsis-group-id* 例： `Router(config)# cable load-balance docsis-group 1`	Cisco CMTS で DOCSIS ロード バランシング グループを作成します。 DOCSIS ロード バランシング グループがすでに存在する場合は、ルータは指定した DOCSIS ロード バランシング グループのコンフィギュレーション モードを開始します。
ステップ 13	**tag** *tag name* 例： `Router(config-lb-group)# tag CSCO`	ロード バランシング グループにタグを追加します。
ステップ 14	**exit** 例： `Router(config-lb-group)# exit`	DOCSIS ロード バランシング グループのコンフィギュレーション モードを終了します。
ステップ 15	**cableload-balancedocsis-policy** *policy-id* **tag** *tag name*[**override**] 例： `Router(config)# cable load-balance docsis-policy 2 tag CSCO`	DOCSIS ポリシーを作成し、新しいルールまたは既存のルールをこのポリシーと関連付けます。
ステップ 16	**exit** 例： `Router# exit`	グローバル コンフィギュレーション モードを終了します。

DOCSIS ロード バランシング グループの設定例

ここでは、制限付き/汎用ロード バランシングおよびダウンストリームの動的ロード バランシングを含む DOCSIS ロード バランシング グループを構成するための設定例を示します。

例：タグの設定

次に、DOCSIS バージョン、MAC アドレス、サービス クラス名、またはサービス タイプ ID を除外するタグの設定方法について示します。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# cable tag 1
Router(cmts-tag)# exclude ?
  docsis-version   set the match rule for docsis version
  oui              set the match rule for oui
  service-class    set the match rule for service class name
  service-type-id  set the match rule for service type id
Router(cmts-tag)# exclude docsis-version ?
  docsis10  Match docsis 1.0 modems
  docsis11  Match docsis 1.1 modems
  docsis20  Match docsis 2.0 modems
  docsis30  Match docsis 3.0 modems
Router(cmts-tag)# exclude docsis-version docsis10
Router(cmts-tag)# exclude oui ?
  WORD  OUI of the vendor in the format xx.xx.xx or xx:xx:xx
Router(cmts-tag)# exclude oui 00.1a.c3
Router(cmts-tag)# exclude service-class ?
  WORD  Service class name
Router(cmts-tag)# exclude service-class work
Router(cmts-tag)# exclude service-type-id ?
  WORD  Service Type ID
Router(cmts-tag)# exclude service-type-id commercial
```

例：ロード バランシングの無効化

次のコマンドを使用して DOCSIS 3.0 GLBG を無効にします。

```
Router(config)# cable load-balance docsis-group FN 1 MD cable 6/0/0
Router(config-lb-group)# disable
Router(config-lb-group)#
```

次のコマンドを使用して DOCSIS 3.0 RLBG を無効にします。

```
Router(config)# cable load-balance docsis-group 1
Router(config-lb-group)# disable
Router(config-lb-group)#
```

DOCSIS ロード バランシング グループの確認

ここでは、ダウンストリームの動的ロード バランシング機能を使用した制限付き/汎用ロード バランシングとナローバンド動的帯域幅共有の設定を確認するために、特定の show コマンドを使用する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権EXECモードをイネーブルにします。 • パスワードを入力します（要求された場合）。

ステップ 2	**showcableload-balancedocsis-group** {*docsis-group-id*| **FN** *fn-id* **MD cable** {*slot/subslot/port*| *slot/port*}} [**all** | **load**| **pending** | **statistics**| **target** | **modem-list**|**primary-load**]
	
	例：
	`Router# show cable load-balance docsis-group 1`
	`Router# show cable load-balance docsis-group fn 1 MD c8/1/4`
		ルータで動作するロード バランシングの設定情報、統計情報、および動作情報をリアルタイムに表示します。

ステップ 3	**showcablefiber-node** *fiber-node-id* [**spectrum**] 例： `Router# show cable fiber-node 3`	ファイバ ノードの情報を表示します。
ステップ 4	**showcableload-balance**[**group***n*]| [**all** | **load**|**pending**| **statistics** |**target**|**fiber-node-validation**] 例： `Router# show cable load-balance group 1`	ロードバランシング動作の統計情報および動作情報をリアルタイムに表示します。オプションを指定しない場合、このコマンドでは、ロードバランシング グループと各ケーブル インターフェイスの現在の負荷とロード バランシングのステータスに関する情報が表示されます。
ステップ 5	**show cable modem** [*ip-address* | *mac-address* |**cable** *slot/port* [**upstream** *port*]	**name** *fqdn*] [*verbose*] 例： `Router# show cable modem 40.3.160.15 verbose`	登録および未登録の CM の情報を表示します。

例

showcableload-balancedocsis-group コマンドを使用して、DOCSIS グループ ステータスおよびグループに含まれるモデムのリストを表示します。**showcablefiber-node** コマンドを使用してファイバ ノードに関する情報を表示し、**showcableload-balance** コマンドを使用してLBGおよびDOCSIS

チャネルに関する情報を表示します。また、**showcablemodem** コマンドを使用してすべての CM に関する情報を表示します。

次に、**showcableload-balancedocsis-group** コマンドの出力例を示します。

```
Router# show cable load-balance docsis-group 2
DOCSIS LB Enabled: Yes
DOCSIS     Group Status Interval DCC mask  Policy     Method Threshold
Group      Index                /UCC                  DS/US  M/E/U/P/S
2          82    RE 10       0xF8(0)/N 0          s/s    1/1/70/70/50
Router# show cable load-balance docsis-group 1 modem-list
US                    Group Index Mac Address      Priority
Mo1/0/0:0/U0          81          (1)
                                  0000.ca45.9898   0
Mo1/0/0:0/U1          81          (0)
Mo1/0/0:0/U2          81          (2)
                                  0013.711c.0820   0
                                  0016.924f.8300   0
```

DOCSIS グループに含まれるモデムの詳細なステータス情報を表示するために、**showcableload-balancedocsis-group** コマンドの出力が変更されて MUPFXLR フィールドが追加されています。詳細については、『Cisco IOS CMTS Cable Command Reference』を参照してください。

次に、変更された **showcableload-balancedocsis-group** コマンドの出力例を示します。

```
Router#show cable load docsis-group fn 1 md c6/0/0 modem-list
Load for five secs: 1%/0%; one minute: 2%; five minutes: 1%
Time source is NTP, 13:39:31.300 PDT Thu Mar 28 2013
Codes: M - Multicast, U - UGS, P - PCMM, F - Max-Failures, X - eXcluded
       L - L2vpn, R - RSVP
Primary DS     Grp Idx MAC Address    RCC-ID Bad Rfid Priority MUPFXLR
In6/0/0:0/UB   40448   (6)
                       e448.c70c.98af 1               2        -------
                       e448.c70c.9b76 1               2        -------
                       e448.c70c.9c15 1               2        -------
                       e448.c70c.9a92 1               2        -------
                       e448.c70c.99e4 1               2        -------
                       e448.c70c.9a35 1               2        -------
In6/0/0:0/U0   40448   (0)
In6/0/0:0/U1   40448   (1)
                       e448.c70c.9915                 2        -------
In6/0/0:0/U2   40448   (0)
In6/0/0:0/U3   40448   (0)
In6/0/0:1/UB   40448   (5)
                       e448.c70c.9abc 1               2        -------
                       e448.c70c.993f 1               2        -------
                       e448.c70c.9927 1               2        -------
                       e448.c70c.9b82 1               2        -------
                       4458.2945.2cb8 1               2        -------
In6/0/0:1/U0   40448   (0)
In6/0/0:1/U1   40448   (0)
In6/0/0:1/U2   40448   (0)
In6/0/0:1/U3   40448   (0)
In6/0/0:2/UB   40448   (5)
                       e448.c70c.9759 1               2        -------
                       e448.c70c.9a0e 1               2        -------
                       e448.c70c.992d 1               2        -------
                       e448.c70c.9a38 1               2        -------
                       0025.2ed9.9984 1               2        -----L-
In6/0/0:2/U0   40448   (0)
In6/0/0:2/U1   40448   (0)
In6/0/0:2/U2   40448   (0)
In6/0/0:2/U3   40448   (0)
In6/0/0:3/UB   40448   (5)
```

```
                      e448.c70c.9c00 1               2        -------
                      e448.c70c.99a5 1               2        -------
                      e448.c70c.9a5f 1               2        -------
                      e448.c70c.9a3b 1               2        -------
                      e448.c70c.96b1 1               2        -------
In6/0/0:3/U0   40448   (0)
In6/0/0:3/U1   40448   (0)
In6/0/0:3/U2   40448   (0)
In6/0/0:3/U3   40448   (0)
```

次に、**showcablefiber-node** コマンドの出力例を示します。

```
Router# show cable fiber-node
Fiber-Node         Config Status
Fiber-Node 1
       Modular-Cable 1/0/0:  0-1
    FN Config Status: Configured (status flags = 0x01)
    MDD Status: Valid
```

次に、**showcableload-balance** コマンドの出力例を示します。

```
Router#show cable load-balance
Group  Interval  Method        DCC Init   Threshold
                               Technique  Minimum  Static  Enforce  Ugs   PCMM
1      10        service-flows 1          1        2%      2%       ---   ---
2      10        modems        0          5        10%     ---      ---   ---

DOCSIS LB Enabled: No
Router# show cable load-balance load
Interface            State      Group  Utilization  Reserved Modems Flows Weight
                                Index
Cable5/0/3 (459 MHz) up         1      0%(0%/0%)       0%    7      7     37
Cable5/0/3/U0        up         1      0%              0%    2      2     1.2
Cable5/0/3/U1        up         1      0%              0%    2      2     1.2
Cable5/0/3/U2        up         1      0%              0%    2      2     1.2
Cable5/0/3/U3        up         1      0%              0%    1      1     1.2
Cable5/0/4 (465 MHz) up         1      0%(0%/0%)       0%    7      7     37
Cable5/0/4/U0        up         1      0%              0%    1      1     1.2
Cable5/0/4/U1        up         1      0%              0%    2      2     1.2
Cable5/0/4/U2        up         1      0%              0%    2      2     1.2
Cable5/0/4/U3        up         1      0%              0%    2      2     1.2
Mo1/0/0:0 (555 MHz)  down       1      0%(0%/0%)       0%    0      0     0
Router# show cable load-balance fiber-node-validation
DOCSIS LBG ID    Match    Channel    Fiber-node list
1                match    Ca5/0/0/U0 {1}
                          Ca5/0/0/U1 {1}
                          Ca5/0/0/U2 {1}
                          Ca5/0/0/U3 {1}
                          Mo1/0/0:0  {1}
                          Mo1/0/0:1  {1}
2                mismatch Ca5/0/0/U0 {1}
                          Ca5/0/0/U1 {1}
                          Ca5/0/0/U2 {1}
                          Ca5/0/0/U3 {1}
                          Ca5/0/0    {}
```

次に、**showcablemodem** コマンドの出力例を示します。

```
Router# show cable modem 40.3.160.19 verbose
LB group ID assigned(index)         : 1(81)
LB group ID in config file(index)   : N/A(N/A)
LB policy ID  : 0
LB policy ID in config file         : 0
LB priority                         : 0
Tag                                 :
```

有効なファイバ ノードが設定されると、DOCSIS 3.0 GLBG はファイバ ノード設定によって動的に生成されます。

たとえば、ファイバ ノードの設定が次のような場合です。

```
cable fiber-node 2
 downstream Modular-Cable 1/0/0 rf-channel 0-3
 downstream Cable7/0/0
 upstream Cable 7/0 connector 0-3
!
```

このファイバ ノードによって生成される GLBG は次のようになります。

```
Router# show cable load-balance docsis-group fn 2 md cable 7/0/0
DOCSIS 3.0 General LB
MD       FN  Group S Intv DCC mask  Policy     Mtd MD-CM-SG Threshold
             Index        /UCC                 D/U          M/E/U/P/S
Ca7/0/0  2   48129 E 30   0xF8(0)/N 0          m/m 0x3C0101 5/10/70/70/50



Router# show cable load-balance docsis-group fn 2 md cable 7/0/0 all
DOCSIS 3.0 General LB
MD       FN  Group S Intv DCC mask  Policy     Mtd MD-CM-SG Threshold
             Index        /UCC                 D/U          M/E/U/P/S
Ca7/0/0  2   48129 E 30   0xF8(0)/N 0          m/m 0x3C0101 5/10/70/70/50
Current load:
DOCSIS load-balancing load
Interface            State   Group  Utilization Rsvd NBCM  WB/UB Flows Weight
                             Index                    Total Total
Cable7/0/0 (333 MHz) up      48129  0%(0%/0%)   0%   2     8     7     37
Cable7/0/0/U0        up      48129  0%          0%   22    7     29    7.6
Cable7/0/0/U1        up      48129  0%          0%   21    8     28    7.6
Cable7/0/0/U2        up      48129  0%          0%   21    8     28    7.6
Cable7/0/0/U3        up      48129  0%          0%   20    10    30    7.6
Mo1/0/0:0 (501 MHz)  up      48129  0%(0%/0%)   0%   2     63    2     36
Mo1/0/0:0/U0         up      48129  0%          0%   22    7     29    7.6
Mo1/0/0:0/U1         up      48129  0%          0%   21    8     28    7.6
Mo1/0/0:0/U2         up      48129  0%          0%   21    8     28    7.6
Mo1/0/0:0/U3         up      48129  0%          0%   20    10    30    7.6
Mo1/0/0:1 (507 MHz)  up      48129  0%(0%/0%)   0%   1     58    1     36
Mo1/0/0:1/U0         up      48129  0%          0%   22    7     29    7.6
Mo1/0/0:1/U1         up      48129  0%          0%   21    8     28    7.6
Mo1/0/0:1/U2         up      48129  0%          0%   21    8     28    7.6
Mo1/0/0:1/U3         up      48129  0%          0%   20    10    30    7.6
Mo1/0/0:2 (513 MHz)  up      48129  0%(0%/0%)   0%   2     59    2     36
Mo1/0/0:2/U0         up      48129  0%          0%   22    7     29    7.6
Mo1/0/0:2/U1         up      48129  0%          0%   21    8     28    7.6
Mo1/0/0:2/U2         up      48129  0%          0%   21    8     28    7.6
Mo1/0/0:2/U3         up      48129  0%          0%   20    10    30    7.6
Mo1/0/0:3 (519 MHz)  up      48129  0%(0%/0%)   0%   1     61    1     36
Mo1/0/0:3/U0         up      48129  0%          0%   22    7     29    7.6
Mo1/0/0:3/U1         up      48129  0%          0%   21    8     28    7.6
Mo1/0/0:3/U2         up      48129  0%          0%   21    8     28    7.6
Mo1/0/0:3/U3         up      48129  0%          0%   20    10    30    7.6
Target assignments:
Interface            State      Group   Target
                                Index
Cable7/0/0 (333 MHz) up         48129
Cable7/0/0/U0        up         48129
Cable7/0/0/U1        up         48129
Cable7/0/0/U2        up         48129
Cable7/0/0/U3        up         48129
Mo1/0/0:0 (501 MHz)  up         48129   Mo1/0/0:1 (507 MHz)
Mo1/0/0:0/U0         up         48129
Mo1/0/0:0/U1         up         48129
Mo1/0/0:0/U2         up         48129
```

```
Mo1/0/0:0/U3          up          48129
Mo1/0/0:1 (507 MHz)   up          48129
Mo1/0/0:1/U0          up          48129
Mo1/0/0:1/U1          up          48129
Mo1/0/0:1/U2          up          48129
Mo1/0/0:1/U3          up          48129
Mo1/0/0:2 (513 MHz)   up          48129
Mo1/0/0:2/U0          up          48129
Mo1/0/0:2/U1          up          48129
Mo1/0/0:2/U2          up          48129
Mo1/0/0:2/U3          up          48129
Mo1/0/0:3 (519 MHz)   up          48129
Mo1/0/0:3/U0          up          48129
Mo1/0/0:3/U1          up          48129
Mo1/0/0:3/U2          up          48129
Mo1/0/0:3/U3          up          48129
Statistics:
Target interface       State      Transfers
                                  Complete  Pending   Retries   Failures
Cable7/0/0 (333 MHz)   up         8         0         0         0
Cable7/0/0/U0          up         30        0         0         0
Cable7/0/0/U1          up         83        0         0         0
Cable7/0/0/U2          up         48        0         0         0
Cable7/0/0/U3          up         34        0         0         0
Mo1/0/0:0 (501 MHz)    up         19        0         0         0
Mo1/0/0:0/U0           up         33        0         0         0
Mo1/0/0:0/U1           up         46        0         0         0
Mo1/0/0:0/U2           up         22        0         0         0
Mo1/0/0:0/U3           up         22        0         0         0
Mo1/0/0:1 (507 MHz)    up         22        0         0         0
Mo1/0/0:1/U0           up         9         0         0         0
Mo1/0/0:1/U1           up         19        0         0         0
Mo1/0/0:1/U2           up         15        0         0         0
Mo1/0/0:1/U3           up         21        0         0         0
Mo1/0/0:2 (513 MHz)    up         21        0         0         0
Mo1/0/0:2/U0           up         4         0         0         0
Mo1/0/0:2/U1           up         3         0         0         0
Mo1/0/0:2/U2           up         6         0         0         0
Mo1/0/0:2/U3           up         7         0         0         0
Mo1/0/0:3 (519 MHz)    up         9         0         0         0
Mo1/0/0:3/U0           up         1         0         0         0
Mo1/0/0:3/U1           up         2         0         0         0
Mo1/0/0:3/U2           up         4         0         0         0
Mo1/0/0:3/U3           up         4         0         0         0
Pending:
Modem          Grp Idx Primary RF/RCC              MD/TCS        Action Active Retries
                       Src           Target       Src    Target         Time
```

その他の参考資料

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

DOCSIS ロード バランシング グループに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *26* : *DOCSIS* ロード バランシング グループに関する機能情報

機能名	リリース	機能情報
DOCSIS ロード バランシング グループ	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 13 章

DOCSIS ロード バランシング移動

Cisco CMTS は、MTC/MRC モデムの静的ロード バランシングおよび非 MTC および/または非 MRC モデムの動的ロード バランシングをサポートします。ラインカード間のサポートも含まれます。複数のインターフェイス、複数のロード バランシング ポリシー、および複数のロード バランシング パラメータを設定するためのオプションを伴うロードバランシング グループ（LBG）の設定のサポートも含まれます。

Cisco CMTS でロード バランシング ポリシーを ID によるインデックス付きで設定して、ケーブル モデムの移動をロード バランシング グループ（LBG）内に制限することができます。ケーブル モデムは登録要求（REG-REQ）メッセージで TLV43.1 を転送し、その後これは解析されて Cisco CMTS に保存されます。ポリシーにより、ケーブル モデムがそのロード バランシング グループ内で移動可能か、およびいつ移動可能かが定義されます。

動的ロード バランシングの間、ケーブル モデムを移動できるかどうかを決定するために、そのケーブル モデムに指定されたポリシーがチェックされます。

ロード バランシングは動的チャネル変更（DCC）をサポートします。DOCSIS 1.1 の DCC は、ケーブル モデムを強制的にオフラインにしたり、変更後に再登録したりせずに、ケーブル モデムのアップストリームまたはダウンストリームのチャネルを動的に変更します。

ロード バランシングは、アップストリーム チャネル ロードによりダウンストリーム ロード バランシングを同じアップストリーム ロード バランシング グループ内に分散します。これは、ロード バランシングがダウンストリーム チャネル ロード全体に基づいて実施されていた以前のロード バランシング制限より優れています。

ロード バランシングは、ルールとポリシーを使用して、ケーブル モデムの LB グループ内での移動を決定します。これらのポリシーは Cisco CMTS で作成され、REG-REQ の type-length-value（TLV）部分（43.1、ポリシー ID）を使用して CM 単位で選択されます。これらのポリシーは、モデムが移動または制限されることを禁止します。

ポリシーは、一連のルールが含まれています。ポリシーが複数のルールによって定義されている場合、すべてのルールは組み合わせで適用されます。ルールは、[enabled]、[disabled]、または [disabled during time period] に定義できます。それぞれのルールを 1 つまたは複数のポリシーで使用することができます。

DOCSIS 3.0 のモデム数ベース静的ロード バランシングでは、動的ボンディング変更（DBC）を使用して、複数のプライマリ チャネルを変更せずに、Multiple Transmit Channel（MTC）モード

または Multiple Receive Channel（MRC）モードで DOCSIS 3.0 ケーブル モデムの次のパラメータを変更します。

- 送信チャネル セット（TCS）
- 受信チャネル セット（RCS）
- ダウンストリーム ID（DSID）または DSID 関連の属性
- ダウンストリーム トラフィックを暗号化するためのセキュリティ アソシエーション

Cisco CMTS では、これらのパラメータと追加のロードバランシング方式が サポートされており、このマニュアルで説明されています。このマニュアルでは、インストールされた Cisco IOS リリース、および任意のパラメータに応じた、Cisco CMTS でのロード バランスのあらゆる実装について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

- Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス，245 ページ
- 前提条件，246 ページ
- 制限事項，246 ページ
- Cisco CMTS でのロード バランシングに関する情報，252 ページ
- ロード バランシングの設定方法，271 ページ
- ロード バランシングの動的チャネル変更の設定方法，275 ページ
- ロード バランシングの設定例，281 ページ
- その他の参考資料，285 ページ
- DOCSIS ロード バランシング移動に関する機能情報，285 ページ

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *27* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

前提条件

ロード バランシングの前提条件

ロード バランシング機能の前提条件は、次のとおりです。

- ロード バランシングは、同じグループのケーブル モデムと物理接続を共有するアップストリームおよびダウンストリームでのみ実行できます。

ロード バランシングのための動的チャネル変更の前提条件

- DCC の対象となるのは、送信元、ターゲット両方のアップストリームまたはダウンストリーム チャネル、あるいはその両チャネルに物理的に接続されたケーブル モデムのみです。
- 同じ物理接続を共有するダウンストリームおよびアップストリーム チャネルの中心周波数は、チャネル幅で区切られた異なる中心周波数である必要があります。
- 送信元とターゲット DCC チャネルの物理層パラメータの差は、目的の DCC 初期化テクニックに必要なしきい値の範囲内である必要があります。
- モデムが DCC 操作を適切に実行するためには、DOCSIS 1.1 をイネーブルにする必要があります。完全にカバーするために CableLabs DCC ATP テストの拡張が必要なため、すべての DOCSIS 1.1 認定モデムが DCC 対応ではないことに注意してください。

DOCSIS 3.0 のモデム数ベース静的ロード バランシングのための動的ボンディング変更の前提条件

- 初期化テクニック 1 ～ 4 を使用するには、Cisco CMTS で DBC-REQ メッセージにアップストリーム チャネル記述子（UCD）TLV（TLV46.5）を含める必要があります。
- DBC をサポートするには、ターゲット ボンディング グループに十分な帯域幅があることが必要です。これはアドミッション制御 API によって決まります。
- DOCSIS 3.0 のモデム数ベース静的ロード バランシングを設定する前に、ファイバ ノードを設定する必要があります。

制限事項

ここでは、ロード バランシング、動的チャネル変更、および動的ボンディング変更機能に適用される制限について説明します。

ロード バランシングの制限事項

ロード バランシング機能には次の制限事項があります。

- ロードバランシングはラインカード単位でのみ実行できます。つまり、1 つのロード バランシング グループ内のすべてのインターフェイスは同じラインカードから提供される必要があります。
- 1 つのロード バランシング グループ内のダウンストリームおよびアップストリームはすべて、同じケーブル モデム グループへの物理接続を共有する必要があります。同じ RF 物理接続を持つ全ダウンストリーム、または全アップストリームは同じロードバランシング グループのメンバーである必要があります。
- 各ラインカードに最大 256 のロード バランシング グループを作成できます。
- （**noshutdown** コマンドを使用して）アップストリーム ポートが動作可能な状態で、使用/接続されていない場合、このポートに登録されているケーブル モデムがなくてもロード バランシングはこのポートを使用しようと試みます。アップストリーム ポートがアップすると、INIT ステートとなり、ロード バランシングにより潜在的ターゲットに含められます。ただし、ロード バランシングでこのアップストリームへの移動を複数回失敗すると DISABLE ステートに設定され、ロード バランシングのその後の過程ではこのポートは除外されます。
- ロード バランシング アルゴリズムでは、モデム間の使用率は比較的均等に配分されます。1 つのケーブル モデムが 1 つのインターフェイス上に大部分の負荷を生成する状況では、1 つのモデムによって生成される負荷より大きい値にロードバランシングしきい値を設定する必要があります。
- ロード バランシングで自動的に移動する特定のケーブル モデムを選択することはできませんが、MAC アドレスまたは組織固有識別子（OUI）に基づいて、いくつかのケーブル モデムをまとめてロードバランシング動作から除外することはできます。（手動で特定のケーブル モデムをアップストリーム間で移動するには、**testcableload-balance** コマンドを使用します。ただし、この操作は通常、ロード バランシング グループの設定をテストする場合に実行します）。
- アップストリーム共有スペクトル グループが設定されている状態でダウンストリーム ロード バランシングを行う場合、各 MAC ドメイン内のダウンストリームが重複するアップストリーム グループを使用することはできません。たとえば、ある MAC ドメイン内のダウンストリームは 10 ～ 30 MHz のアップストリーム スペクトル帯域を使用し、第 2 の MAC ドメイン内のダウンストリームは 30 ～ 42 MHz のアップストリーム スペクトル帯域を使用することが可能です。ロード バランシング グループに両方の MAC ドメイン用のダウンストリームが含まれるよう、それぞれの MAC ドメインにはそれぞれ固有のアップストリーム共有スペクトル グループが含められます。
- 同じスプリッタから伸びるすべてのアップストリーム ポートは、チャネル幅で区切られた異なる中心周波数を使用する必要があります。たとえば、アップストリームが 3.2 MHz のチャネル幅を使用している場合、すべてのアップストリームの中心周波数は少なくとも 3.2 MHz に区切られる必要があります。
- 動的チャネル変更（DCC）では 4 つの初期化テクニックを使用できます。

- ロード バランシングを設定している場合、プロビジョニング システムにより DOCSIS コンフィギュレーション ファイルで個々のケーブル モデムに特定のアップストリーム チャネルまたはダウンストリーム周波数を割り当てることはできません。特定のアップストリーム チャネルまたはダウンストリーム周波数を必要とするすべてのケーブル モデムを、ロード バランシング動作から除外する必要があります（**cableload-balanceexclude** コマンドを使用）。
- ケーブル モデムの数が少ないケーブル インターフェイスや、インターフェイス負荷の大部分を単一のモデムが担当している場合には、ロードバランシングの使用率による方法を使用しないでください。このような状況では、Cisco CMTS はあるインターフェイスから別のインターフェイスへケーブル モデムを移動し続け、インターフェイスをロード バランシングする試みが終わらなくなる可能性があります。これを避けるには、使用率のしきい値を、単一ケーブル モデムによって発生する可能性のある値よりも大きい値に設定します。
- チャネル制限機能が導入され、ターゲット アップストリーム チャネルの属性マスクがケーブル モデムの属性マスクと対立する場合、より高い負荷のアップストリームにあるケーブル モデムはロードバランシングの対象になりません。現在のロードバランシングにより、ケーブル モデムはターゲット アップストリームにのみ移動されるためです。ただし、属性マスクが設定されていないケーブル モデムは、そのままロード バランシングの対象である場合があります。ロード バランシング グループを導入する場合は、次のことを考慮してください。ターゲットアップストリームは常に、最も低い負荷を持つアップストリームです。同じ負荷を持つアップストリームが他にある場合、最も低いインデックスを持つアップストリームがターゲット アップストリームとして選択されます。
- ケーブル モデム コンフィギュレーション ファイル中の TLV はモデムごとの動的ロード バランシングを制限します。
- DOCSIS ポリシーの最後のルールを削除すると、ポリシー自体が削除されます。
- Cisco CMTS のロード バランシング機能は、ケーブル モデムが拡張周波数範囲（5 MHz ～ 85 MHz）をサポートするかどうかをチェックせずに、ロード バランシング グループ内のチャネルの負荷に基づいてケーブル モデムを移動します。このため、標準周波数範囲（5 MHz ～ 65 MHz）をサポートするケーブル モデムが拡張周波数範囲が設定されたチャネルに移動される可能性があります。このようなシナリオを克服するため、グループ内のすべてのモデムが拡張周波数をサポートするのでないかぎり、オペレータは、同じロード バランシング グループ内に標準周波数および拡張周波数を持つアップストリームを混在させて設定しないようにする必要があります。

ロード バランシングのための動的チャネル変更の制限事項

- DCC 初期化 0 が、ロード バランシング DCC のデフォルトのテクニックです。
- 複数のカード間での（カード間）ロード バランシングでは、LB グループにどのテクニックが設定されているか、またはどのカード タイプが使用されているかに関係なく、どんな場合にも DCC 初期化テクニック 0 が使用されます。
- 送信元とターゲットのアップストリームおよびダウンストリームは、DCC トランザクションに望ましいモデムと物理接続を共有する必要があります。

- 個別のダウンストリーム変更はサポートされません。対応するダウンストリーム変更によって MAC ドメインをまたぐアップストリーム変更が起きる必要があります。
- ロード バランシングに DCC を使用する場合、送信元とターゲットのダウンストリーム インターフェイスは、同じ仮想バンドルおよび同じロード バランシング グループに属している必要があります。
- DCC 初期化テクニック 1 ～ 4 では、動的チャネル変更要求（DCC-REQ）メッセージのエンコーディングによって明示的に変更された設定変数を除き、ケーブル モデムのすべての設定変数が一定に保持される必要があります。
- 新旧チャネル間の伝搬遅延の差が DOCSIS で定義されている範囲精度要件（たとえば、±0.25 usec（マイクロ秒）プラス ± シンボル時間）を超える場合、DCC 初期化テクニック 2 ～ 4 を使用する必要があります。

  たとえば、1.28 Msps のシンボル レートの場合、送信元とターゲットのアップストリーム チャネル間のタイミング オフセット差は、± floor[(0.250 us + 0.5*0.781us)/(1/10.24)] = ± 6 となります。
- 新旧のアップストリーム チャネル間の減衰または周波数応答の差により、Cisco CMTS での受信電力が 6 dB 以上変化します。
- DCC 初期化テクニック 3 は、テクニック 2 を使用するための条件が満たされていない場合には使用しないでください。
- DCC 初期化テクニック 4 は、テクニック 2 を使用するための条件が満たされていない場合には使用しないでください。
- 新しいアップストリーム チャネル上の微小反射により、初期設定に設定された事前均等化係数で許容されない BER（1e-8 以上）が発生します。
- DCC は DOCSIS 1.1 以降の CM の動的ダウンストリーム ロード バランシングのためだけに使用されます。DOCSIS 1.x CM での動的アップストリーム ロード バランシングでは常に、アップストリーム チャネル変更（UCC）が使用されます。DOCSIS 2.x CM では、*ucc* オプションが設定されている場合、UCC が使用されます。DOCSIS 3.x CM では、*ucc* オプションが設定されているかに関係なく、DCC が使用されます。
- DCC により移動されたケーブル モデムがターゲット インターフェイス上の動的マルチキャスト グループにとって最初のケーブル モデムであった場合、マルチキャスト トラフィックの中断が長引くことが予想されます。Internet Group Management Protocol（IGMP）のクエリ間隔が 1 分に設定されている場合、Cisco CMTS IGMP クエリの結果として Cisco CMTS が IGMP Join メッセージを顧客宅内機器（CPE）から受信するまで、ダウンストリーム マルチキャスト サービス フローを再確立することはできません。これは、IGMPv2 の制限です。
- CPE に静的に割り当てられた複数の IP アドレスを ping することができます。ただし、これを実行できるのは、ケーブル モデムの IP アドレスおよびアップストリーム上の CPE デバイスの検証などのセキュリティ機能、および他のセキュリティ メカニズムがディセーブルになっているときだけです。

- DOCSIS 3.0 ケーブル モデムに割り当てられる TCS および RCS は、Cisco CMTS で設定されているアップストリームおよびダウンストリーム ボンディング グループにより制限されます。
- ロード バランシングおよび DCC はレイヤ 2 VPN（L2VPN）サポートがイネーブルになっている CM ではサポートされません。
- DCC が起きると、ケーブル モデムの US および DS カウンタはリセットされます。US カウンタと DS カウンタには、**showcablemodem(mac-address) verbose** コマンド出力に示されるデータとスループット、**showcablemodem(mac-address)counters** コマンド出力に示されるパケットとバイトなどのカウンタが含まれます。

N+1 冗長性とカード間ロード バランシングに関する DCC の制限

- カード間のロード バランシングは、N+1 冗長構成を使用するケーブル インターフェイス ライン カードではサポートされていません。詳細については、一般的な DCC の制限を参照してください。
- 動的ロード バランシングは、N+1 冗長性とともに使用できません。未処理の DCC トランザクションがあるケーブル モデムは、スイッチオーバー イベント後にオフラインになります。

（注） ケーブル モデムがスイッチオーバー イベント中にオフラインになると、ロード バランシング機能がアクティブになります。ケーブル モデムは、スイッチオーバー イベントに関連して移動します。ケーブル モデムがオンラインに戻ると、ロード バランシングを再び開始する必要があることがあります。

スイッチオーバー中にリセットされるケーブル モデムの割合がシステムで構成されている場合、スイッチオーバー時にロード バランシングを実現するために、動的なロード バランスのしきい値を増やすことができます。代替方法は、N+1 冗長性が有効な静的ロード バランシングを使用することです。詳細については、「Types of Load Balancing Operations」を参照してください。

DOCSIS 3.0 モデム数ベース静的ロード バランシングの制約事項

- モデム数ベース静的ロード バランシングは、MTC ケーブル モデムおよび MRC 単独ケーブル モデムでサポートされます。シングル チャネル、ナローバンド ケーブル モデムは、動的ロード バランシングとともに継続してサポートされます。MRC 単独モデムは、アップストリーム チャネルの動的ロード バランシングによりサポートされます。

（注） DOCSIS 3.0 静的モデム カウントベース ロード バランシングは、次の環境でサポートされません。

- 複数のラインカード。
- 複数のライン カード間で共有されるロードバランシング グループとダウンストリーム チャネル。

- DOCSIS 3.0 モデム数ベース静的ロード バランシングは、ロード バランシングのサービス フローによる方法をサポートしません。

DOCSIS 3.0 モデム数ベース静的ロード バランシングのための動的ボンディング変更の制約事項

- Cisco CMTS では、MAC ドメイン内でのモデムの移動に DBC メッセージングのみを使用できます。適用対象はプライマリ ダウンストリームに変更がなく、MTC モードまたは MRC 単独モードで動作しているケーブル モデムのみです。
- Cisco CMTS は DCC と初期化テクニック 0 を使用するプライマリ チャネル変更によって、MRC 単独のケーブル モデムを移動します。
- Cisco CMTS は DCC と初期化テクニック 0 のみを使用して、MAC ドメイン間でケーブル モデムを移動します。
- Cisco CMTS では、ケーブル設備の状態に適した初期化テクニックを考慮する際に、既存の QoS サービスの中断を最小限にすることを確認する必要があります。

（注） DOCSIS 3.0 静的ロード バランシングは、初期化テクニック 1 を使用して DBC の移動のためにケーブル モデムを移動します。

  - 初期化テクニック 1：（ブロードキャスト初期レンジング）長い中断をもたらす可能性がありますが、これは新しいチャネルに QoS リソースを予約することによって軽減されます。Cisco CMTS で新しいチャネルに初期レンジングのより頻繁な機会を提供することに加え、DBC 要求に UCD TLV を追加することにより、サービスの中断をさらに軽減することができます。
  - 初期化テクニック 2：（ユニキャスト レンジング）サービスの中断をわずかに抑える可能性を提供します。このテクニックを使用するには、アップストリーム チャネルが変更された場合に Cisco CMTS で DBC メッセージ に UCD TLV を含める必要があります。
  - 初期化テクニック 3：（ブロードキャストまたはユニキャスト レンジング）サービスの中断をわずかに抑える可能性を提供します。CM が DBC コマンドをいつ実行するかが不明であり、そのためにステーション メンテナンス スロットが見逃される可能性がある場合、このテクニックを使用します。ただし、テクニック 1 および 2 を 使用するため

の条件が完全に満たされていない場合、Cisco CMTS はこのテクニックを使用できません。

- 初期化テクニック 4：（新しいチャネルを即使用）サービスの中断が最小になります。

- DOCSIS 3.0 静的ロード バランシング グループ内にある DOCSIS 3.0 ケーブル モデムでは、マルチキャストの結合は REG-HOLD 時間が経過する前にドロップされます。

MRC 単独ケーブル モデムの制限事項

- MRC 単独ケーブル モデムでは、単一チャネルの未ボンディングのアップストリーム（ナローバンド（NB）モデムと同様）、およびダウンストリーム上の複数チャネル ボンディング グループを使用します。

（注） 次の制限事項は MRC 単独モードの DOCSIS 2.0 および DOCSIS 3.0 ケーブル モデムにのみ適用されます。

- ケーブル モデムの移動は、DCC を使用してアップストリーム チャネル間で行われます。
- プライマリ ダウンストリーム チャネルには変更がなく、アップストリーム チャネルとダウンストリーム チャネル ボンディング グループに変更がある場合、ケーブル モデムは DBC により異なるダウンストリーム チャネルに移動されます。アップストリーム チャネル変更は無視されます。

  ただし、プライマリ ダウンストリーム チャネルにも変更がある場合は、DCC と初期化テクニック 0 が使用されて、ケーブル モデムのバランシングが行われます。
- MRC 単独モデムは MTC モードで動作しているケーブル モデムと同様に処理され、ダウンストリーム チャネル間でモデムが移動されす。アップストリーム チャネルに変更がある場合、MRC 単独ケーブル モデムは単一チャネル NB ケーブル モデムと同様に処理されます。

Cisco CMTS でのロード バランシングに関する情報

ここでは、Cisco CMTS でのロード バランシング機能の動作、概念、および利点について説明します。

機能の概要

Cisco CMTS のロード バランシング機能では、サービス プロバイダーがダウンストリームおよびアップストリームの両方の帯域を最適に使用できます。音声やビデオ サービスなどの新しい高速サービスを導入できます。この機能を使用すると、ケーブル モデムの分配がケーブル ネットワーク全体で不均一であること、および個々の顧客による使用パターンがさまざまであることが原因であるネットワークの輻輳を軽減できます。

デフォルトで Cisco CMTS プラットフォームが使用するロード バランシング形式では、ケーブル モデムの登録時に異なるアップストリームにケーブル モデムを均一に分散させようとします。

この機能は強化され、DOCSIS ポリシーおよびルールを利用してロード バランシング グループ内での移動を制限するようになりました。ポリシーにより、ケーブルモデムがそのロードバランシング グループ内で移動可能か、およびいつ移動可能かが定義されます。

ポリシーは、一連のルールで構成されます。各ルールは、「有効」、「無効」、または「期間中に無効」として定義できます。複数のポリシーで1つのルールを共有できます。ただし、ポリシーの最後のルールを削除すると、ポリシーも削除されます。

各ルールは、任意の数のポリシーで使用できます。複数のルールによって定義される場合、すべてのルールは組み合わせて適用されます。各ルールは、特定のケーブル モデムを使用するロードバランシングを禁止したり、1 日のうち特定の時間帯で特定のケーブル モデムを使用するロードバランシングを禁止したりできます。

ルールとポリシーの一般的なガイドラインを以下に示します。

- ポリシーまたはルールは 32 ビットの ID で認識されます。
- 各ケーブル モデムには 1 つのポリシーのみを設定できます。
- 各ルールは、1 つ以上のポリシーに関連付けることができます。
- 各ポリシーは、少なくとも 1 つのルールで記述されます。そうでない場合は作成できません。
- ポリシー ID 0 は Cisco CMTS によって予約されていて、「LB 禁止に対して何もしない」ことを示します。
- ケーブル モデムのコンフィギュレーション ファイルで指定されたポリシー ID が Cisco CMTS 上で設定されていない場合、LB 禁止がその CM に適用されません。ただし、ID が一致するポリシーが設定されると、LB 禁止はすぐに反映されます。

インターフェイスのバランシング時期の判定方法

インターフェイスをどのようにバランシングするか（静的、受動的、または動的タイプのロードバランシングの使用）の選択に加え、インターフェイスをいつバランシングしたらよいかを判定するのに Cisco CMTS が使用する方法を以下から選択することができます。

- モデムによる方法：インターフェイス上のアクティブなケーブル モデムの数を使用します。
- 使用率による方法：インターフェイスの使用率の現在の割合を使用します。

それぞれの方法の詳細については、以下の項を参照してください。

モデムによる方法

モデムを利用するロードバランシング メソッドでは、インターフェイス上のアクティブなケーブル モデム数を使用して現在の負荷を判定します。これは分散ベース形式のロードバランシングで

あり、インターフェイスがロード バランシングされているかどうかを判断するのに、モデムの絶対数が使用されます。

この方式では、ケーブル モデムを通過するトラフィックの量は考慮されませんが、システムでは使用されているチャネルの相対帯域幅が考慮されるため、高帯域幅のチャネルには多数のケーブル モデムが割り当てられます。つまり、インターフェイスがそれぞれ異なるチャネル幅または変調プロファイルを使用している場合、システムはロード バランスを実現するためにインターフェイスに異なる数のケーブル モデムを割り当てることができます。次に例を示します。

- チャネル幅：2 つのアップストリームをロード バランシングする場合に、一方のアップストリームが 1.6 MHz のチャネル幅に設定され、他方のアップストリームは 3.2 MHz のチャネル幅に設定されている場合、後者のケーブル モデムは前者の 2 倍のアップストリーム チャネル幅であるため、Cisco CMTS は後者のアップストリームに 2 倍の数のケーブル モデムを割り当てます。
- 変調プロファイル：一方のダウンストリームが 64-QAM に設定され、他方のダウンストリームが 256-QAM に設定されている場合、バランシングされた負荷を達成するために、Cisco CMTS は後者のダウンストリームに比例してより多くの数のケーブル モデムを割り当てます。

2 つのインターフェイスでチャネル幅と変調プロファイルの両方が 異なるように設定されている場合、システムは、インターフェイスの相対的な帯域幅を決定するための目安として、「重み」値を計算します。

ヒント ロードバランシングされたシステムでは、設定されたチャネル幅と変調パラメータがインターフェイス間で同一の場合のみ、それらのインターフェイスには同じ数のケーブル モデムが含まれます。

使用率による方法

（注） 使用率による方法は、ナローバンド ケーブル モデム、複数のダウンストリーム ケーブル モデム、および MRC 単独ケーブル モデムのアップストリームのみで使用されます。

使用率による方法では、インターフェイスの現在の使用率を使用して現在の負荷が判断されます。この方法は、インターフェイス上で送信されるトラフィックの量を、使用中の帯域幅合計におけるパーセンテージの形式で使用します。システムでは、各インターフェイスの負荷を評価する際、これらのインターフェイスの（変調プロファイルとチャネル幅によって決定される）相対的なスループットと帯域幅が考慮されます。

たとえば、使用率による方法を使用して 2 つのアップストリームがロード バランシングされ、最初のアップストリームが 2 番目のアップストリームの 2 倍の帯域幅を持つ場合、2 つのアップストリームは、使用率が同じパーセンテージに到達したときにバランシングされていると見なされます。最初のアップストリームはトラフィック用の容量がより大きいため、2 番目のアップストリームよりも多くのトラフィックを転送しますが、使用率のパーセンテージは同じになります。

ワイドバンド インターフェイスの平均使用率とスループット

同じサイズのワイドバンド インターフェイス間の平均使用率と平均スループットは以下によって計算できます。

平均使用率（WB）$= \sum^{n}_{i-1}$rfch - util(rf_i)/n

- n は、ワイドバンド インターフェイスのサイズを表します。
- $\sum^{n}_{i-1}$rfch - util(rf_i) は、ワイドバンド インターフェイス内の QAM チャネルの rfch - util の合計を表します。

平均スループット（WB）= 直近の 30s/$\sum^{n}_{i=1}$BW(rf_i) の平均スループット（WB）

- 平均スループット（WB）は、直近の 30 秒に記録された KB を表します。
- $\sum^{n}_{i=1}$BW(rf_i) は、ワイドバンド インターフェイスの帯域幅合計を表します。

（注） ワイドバンド インターフェイス間での平均使用率と平均スループットを表示するには、**show cable load-balance load wideband** コマンドを使用します。

ロード バランシング パラメータ

ロードバランシング動作にどのケーブルインターフェイスを関与させるかを指定できます。ケーブル インターフェイス上の現在のロードを、次のうちどの方法で判定するかを選択でき、したがって、ケーブル モデムを移動する必要があるかどうかを決定できます。

- アクティブなケーブル モデムの数
- チャネル帯域幅の利用率

また、アップストリーム、ダウンストリームの両タイプのロード バランシングのために、Cisco CMTS が新しいケーブル モデムをそれぞれに割り当てる方法を判定するのに使用するしきい値を指定できます。さらに、アクティブな Voice-over-IP（VoIP）コールを伴うケーブル モデムを移動する必要があるかどうかを設定でき、その場合に使用するしきい値を設定できます。また、1 つの形式またはあらゆる形式のロードバランシングから、特定のケーブルモデムを除外することができます。

使用率による方法で構成可能な最小しきい値

使用率による方法では、少なくとも 1 つのインターフェイスの仕様率が最小しきい値に達するまで、ロードバランシングのためにケーブルモデムを移動しません。これは、インターフェイスの使用率が一時的に急増することが原因で、ケーブル モデムの不必要な移動を避けるためです。

最小使用率しきい値は、使用率による方法で構成できます。最小使用率しきい値は 10 ～ 90 パーセントの範囲で構成できます。その結果、インターフェイスで構成された最小使用率しきい値に達したときにケーブル モデムが移動します。

使用率による方法で最小しきい値を設定するには、グローバル コンフィギュレーション モードで **cableload-balancemethod-utilizationmin-threshold** コマンドを使用します。詳細については、**cableload-balancemethod-utilizationmin-threshold** コマンド リファレンスを参照してください。

単一チャネルのロード バランシング

チャネル割り当てのエラー処理

チャネルのインターフェイス状態が「administratively down」ではない限り、すべてのチャネルが LBG 割り当てに使用できます。その他のロード バランシング動作（DCC や UCC を使用してモデムを移動するなど）では、チャネルのインターフェイス状態は「initial」、「up」、「suspicious」、または「testing」ステータスである必要があります。

アップストリーム ロード バランシングを使用したダウンストリーム ロード バランシングの分散

ダウンストリーム ロード バランシングは、アップストリーム グループ メンバー間で均等なロード バランシングを提供します。この強化は、「保留中」統計をロード バランシング グループ内のさまざまなケーブル インターフェイス ライン カード間で同期します。その結果、ダウンストリームの合計負荷ではなくアップストリームごとの負荷を利用する、ダウンストリーム ロード バランシングの代替スキームとなります。

この強化では、ダウンストリーム チャネル負荷全体に基づくのではなく、同じアップストリーム ロードバランシング グループにおけるアップストリーム チャネル負荷を考慮してダウンストリーム ロード バランシングを実行します。以前の Cisco IOS リリースでは、個々のアップストリーム チャネル間で均等に、またはダウンストリームとアップストリームを同時に考慮した方法で、分散したケーブル モデムを使用できませんでした。

ロードバランシング強化は、別々のアップストリーム ロードバランシング セグメントを持つヘッドエンド システムでダウンストリーム ロードバランシングが発生するときに適用されます。アップストリーム セグメントは複数のダウンストリーム セグメントに展開されます。

ダウンストリーム ロードバランシングを決定するための設定と動作は、次のように有効になります。

- ターゲット ダウンストリーム セグメントは、ソース ダウンストリーム セグメントと同じダウンストリーム ロード バランシング グループ内にあります。
- アップストリーム ロード バランシング グループは、ケーブル モデムがバランスしている該当チャネルに対して設定できます。
- Cisco CMTS は、ロード バランシング グループのアップストリーム セグメントを自動的に検出し、負荷が最も小さいソース インターフェイスでアップストリーム グループ ステータスを処理します。
- ターゲット ダウンストリーム セグメントには、アップストリーム ロード バランシング グループで設定したアップストリーム チャネルが必要です。

- 最上位のターゲット アップストリーム セグメントでは、他のインターフェイス上の最上位アップストリームセグメントなど、他の潜在的なターゲットよりも負荷を少なくする必要があります。

たとえば、複数のアップストリームセグメントを次のように複数のダウンストリームセグメント全体で設定できます。

```
       U0      U1      U2      U3     Downstream
3/0    LB10    LB11    LB12    LB13      LB1
4/0    LB10    LB11    LB12    LB13      LB1
5/0    LB10    LB11    LB12    LB13      LB1
6/0    LB10    LB11    LB12    LB13      LB1
```

この例では、インターフェイス ケーブル 5/0 アップストリーム 2 でオンラインになったケーブル モデムは、次のインターフェイスでオンラインになる可能性があります。

- ケーブル 3/0 アップストリーム 2
- ケーブル 4/0 アップストリーム 2
- ケーブル 6/0 アップストリーム 2

この強化では、次の利点と動作が実現されます。

- この強化により、「保留中」統計をさまざまなケーブル インターフェイス ライン カードとネットワーク プロセッシング エンジン（NPE）との間で同期するためのサポートが追加され、ケーブルモデムの移動先に関して判断を向上させることができます。この機能は、必要に応じて通常のダウンストリーム ロード バランシングの実装として使用できます。
- この強化により、アップストリーム リソースを使用してダウンストリーム ロード バランシング グループを設定するための **us-groups-across-ds** キーワードが **cable load-balance group** コマンドに追加されました。

（注） DOCSIS 2.0 の動的ダウンストリームおよびアップストリームのロード バランシングを無効にするには、**no cable load-balance docsis20-enable** コマンドを使用します。

DOCSIS 3.0 ケーブル モデムの単一アップストリーム モードでのアップストリーム ロード バランシング

アップストリーム ロード バランシング機能により、Cisco CMTS ルータは、単一アップストリーム モードのワイドバンドおよびナローバンド ケーブル モデムのアップストリーム トラフィックを、効果的に処理することができます。単一アップストリーム モード（Mx1）とは、モデムが複数のアップストリームチャネル上のアップストリームトラフィックを送信できないことを意味します。ワイドバンドまたはナローバンド ケーブル モデムの 1 つのアップストリーム チャネルにトラフィックの過負荷が発生すると、Cisco CMTS ルータは、同じロード バランシング グループ内の別のアップストリーム チャネルにケーブル モデムを自動的に移動します。

（注） 単一アップストリーム モードで動作しているケーブル モデムは、モデムのプライマリ チャネルに基づいて 1 つのロード バランシング グループに割り当てられます。単一アップストリーム モードのケーブル モデムは、Multiple Receive Channel（MRC）モードまたはナローバンド モードをサポートすることができます。ただし、単一アップストリーム モードのケーブル モデムは、Multiple Transmit Channel（MTC）モードをサポートできません。

スペクトル管理とのインタラクション

Cisco ケーブル インターフェイス ラインカードは、チャネル帯域幅を最大化し、ケーブル モデム トラフィックのイングレス ノイズの影響を最小化する多くの機能をサポートします。これらの機能は、ロード バランシング動作に次の影響を及ぼします。

- 周波数ホッピング：周波数ホッピングは、チャネル帯域幅、インターフェイス上のケーブル モデムの数のいずれも変更しないため、ロード バランシング アルゴリズムに影響を及ぼしません。
- ダイナミック変調の変更：ダイナミック変調機能は、インターフェイス上のノイズ状態に応じて、高帯域幅変調プロファイルから低帯域幅変調プロファイルにインターフェイスを切り替えるため、ロード バランシング アルゴリズムに影響を及ぼします。

  たとえば、アップストリームが 16-QAM に設定されている場合、十分なノイズ レベルにより、アップストリームが QPSK 変調プロファイルに切り替わる場合があります。ロード バランシングの設定によっては、この結果、ケーブル モデムが他のチャネルに移動する可能性があります。同様に、ノイズ状態が改善されて変調が元の高帯域幅プロファイルに戻ると、ケーブル モデムはアップストリーム チャネルを再調整するために再び移動する場合があります。
- チャネル幅の変更：Cisco ケーブル インターフェイス ラインカードはノイズ状態に応じたチャネル幅への自動変更をサポートします。チャネル幅を変更するとチャネルのスループットに影響するため、これもロード バランシング アルゴリズムに影響を及ぼします。

  たとえば、ノイズによって現在のチャネル幅を使用不可になると、Cisco ケーブル インターフェイス ラインカードは使用可能なチャネル幅が見つかるまでチャネル幅を減らします。これによりチャネル上の使用可能な帯域幅が減少するので、ロード バランシング アルゴリズムは、アップストリームを再調整するためにケーブル モデムを移動します。

  また、ノイズ状態が改善された場合、Cisco ケーブル インターフェイス ラインカードは自動的に元のチャネル幅を回復しません。その代わりに、新たなノイズ状態に応じてさらなる周波数ホッピングが起きた場合、またはオペレータが手動で周波数ホッピングを実行した場合に限り、カードはチャネル幅を変更します。ホッピングが発生するとカードは可能な最大のチャネル幅を検索しますが、これによりチャネルを再調整するためのケーブル モデムの別の移動が発生する可能性があります。

動的チャネル変更の使用

DOCSIS 1.1 の DCC は、ケーブル モデムを強制的にオフラインにしたり、変更後に再登録したりせずに、ケーブル モデムのアップストリームまたはダウンストリームのチャネルを動的に変更します。DCC は 5 つの異なる初期化メソッド（0 ～ 4）をサポートします。

- ロード バランシング手法により、設定可能な初期化テクニックを使用して DCC 搭載のケーブル モデムを移動できます。
- DCC を 0 ～ 4 の範囲の DCC 初期化テクニックとともに使用すると、同じケーブル インターフェイス ライン カード内の個々のダウンストリーム チャネル間でライン カード チャネルを変更できるようになります。
- DCC は、ケーブル モデム状態の情報を発信ダウンストリーム チャネルから対象のダウンストリーム チャネルに転送し、ケーブル インターフェイス ライン カードとネットワーク プロセッシング エンジン（NPE）またはルート プロセッサ（RP）間のケーブル モデム情報の同期化を維持します。
- PacketCable（PC）や PacketCable Multimedia（PCMM）などの遅延に敏感なアプリケーションは、DCC 初期化テクニック 4 を使用し、ケーブル モデムが DCC を実行している間のサービスを維持します。
- チャネルが混合モードまたは ATDMA のみモードの場合、プライマリ サービス ID（SID）を ATDMA のみモードに切り替える必要があります。

（注） DOCSIS 2.0 の動的ダウンストリームおよびアップストリームのロード バランシングを無効にするには、**no cable load-balance docsis20-enable** コマンドを使用します。

複数チャネルのロード バランシング

束ねられたチャネル ケーブル モデムのロード バランシングのアルゴリズム

ケーブル モデムの登録時に、モデム数ベースの方法では各チャネルの現在の負荷を決定するために、許可された RCS 上でアクティブなケーブル モデム数を使用します。モデムに RCS が割り当てられると、トラフィックの状態が変化しても Cisco CMTS はケーブル モデムを移動しません。

ケーブル モデムが登録要求を送信すると、モデム数ベースのロード バランシング メソッドでは、モデム数に基づいて許可された受信チャネル セット（RCS）をランク付けし、CM 数が最小のセットを範囲内にあるケーブル モデムに割り当てます。

DOCSIS 3.0 モデム数ベース静的ロード バランシング

モデム数ベース静的ロード バランシングは、次をサポートします。

- DOCSIS 汎用/制限付きロード バランシング グループの割り当てにより、MTC モードおよび MRC 単独モードの DOCSIS 3.0 ケーブル モデムを含めます。

（注） DOCSIS 3.0 モデム数ベース静的ロード バランシングは、次の環境でサポートされません。

- 複数のライン カード間。
- 複数のライン カード間で共有されるロード バランシング グループとダウンストリーム チャネルの場合。ただし、自律的ロード バランシング ベースの CM のステアリングおよびロード バランシング グループの割り当ては、複数のラインカード間でサポートされています。

- ロード バランシングにおける DCC および DBC の使用。
- ダウンストリーム移動中の MRC 単独モデムでの DBC の使用。
- プライマリ ダウンストリーム チャネルが MRC 単独 CM で変更された場合は、初期化テクニック 0 と DCC の使用。
- すべてのアップストリームおよびダウンストリーム モデム移動における MTC モードのケーブル モデムでの DBC の使用。
- NB およびワイドバンド（WB）/アップストリーム ボンディング（UB）CM に別々のカウンタ。詳細については、『Cisco IOS CMTS Cable Command Reference』で **showcableload-balancedocsis-group** コマンドを参照してください。
- ロードバランシングのために論理チャネルを物理チャネルへ集約。物理チャネルの負荷は、すべての論理チャネル間の平均ウェイトを使用して計算されます。
- SPA QAM の使用率が考慮された非プライマリ ダウンストリーム チャネルの負荷。

（注）

（注） 異なる WB インターフェイス全体の CM 数が事前定義されたしきい値レベル内にあるとき、負荷はバランスが取れているものとして常に考慮され、LB システムによるこれ以上の CM 移動は開始されません。この LB プロセス中、サービス フロー数は、プライマリもセカンダリも考慮されません。

（注） サービス フロー（SF）の転送インターフェイスのために考慮される属性は、属性マスクおよび使用可能な帯域幅であり、チャネルごとのサービス フロー数ではありません。チャネルが新しいRCS内にある場合、ナローバンドSFのタイプ（プライマリかセカンダリか、または静的か動的か）に関係なく、SF は現在のチャネルを使用し続けます。

（注） US PHY モード カウンタ（scdma、atdma、および tdma）は、UB インターフェイスでは 0 のままです。

DOCSIS 3.0 モデム数ベース静的ロード バランシングは、レガシーのロード バランシングに基づいており、任意のタイプのチャネルの組み合わせ（アップストリームとダウンストリーム）MxN もサポートします。1x1 の組み合わせはそのサブセットです。

DOCSIS 3.0 モデム数ベース静的ロード バランシングは、登録済み CM で使用されるダウンストリームおよびアップストリーム チャネルへの動的な変更を制御します。次がサポートされています。

- 複数チャネルのロード バランシング動作。
- ポリシーと優先順位に基づくロード バランシング動作。
- マルチキャストを使用するロード バランシング。DOCSIS 3.0 モデム数ベース静的ロード バランシングは、アクティブなビデオ セッションのある CM を移動しません。

DOCSIS 3.0 モデム数ベース静的ロード バランシングは、DOCSIS 1.x、2.0、および 3.0 ケーブル モデムのハイブリッド導入におけるモデム数ベースのロード バランシングをサポートします。

モデム数ベース静的ロード バランシングは、DOCSIS 3.0 CM の場合のみサポートされます。シングル チャネルのナローバンド ケーブル モデムは、動的ロード バランシングで引き続きサポートされます。MRC 単独ケーブル モデムは、アップストリーム チャネルの動的ロード バランシングによりサポートされます。

DOCSIS 3.0 モデム数ベース静的ロード バランシングを使用すると、LBG 内のロード バランシング関連の設定が次のように変更されると、ケーブル モデムが強制的に再登録されます。

- LBG ドメイン下にあるインターフェイスの部分的シャットダウンまたはシャットダウンなし
- ケーブル モデムの MRC または MTC モードがオンまたはオフになった
- GLBG に関するファイバ ノードでの変更
- ダウンストリーム グループに関するワイドバンド設定の変更
- アップストリーム ボンディング グループでの変更

ケーブル モデムを強制的に再登録するには、次のコマンドを使用します。

- **clearcablemodemdelete**
- **clearcableloadstate**

- **clearcableloadcounters**

ターゲット *RCS* のプライマリ チャネル ロード表示

この機能を使用すると、ボンディングされたモデムが登録時に移動され、ターゲットの DS チャネルでロードバランシングが行われる以外に、プライマリ チャネルがプライマリ可能なチャネル間で均等に分散されるようにすることができます。モデムによる方法では、RCS はプライマリ ロードに基づいてランク付けされ、最もプライオリティが低いロード セットが範囲内のケーブル モデムに割り当てられます。

RCS のプライマリ ロードを表示するためのオプション キーワード **primary-load** が **showcableload-balancedocsis-group** コマンドに追加されています。詳細については、『Cisco CMTS Command Reference』を参照してください。

モデム カウントベースの方法では、登録時にケーブル モデムは均等に分散されますが、次のような状況が原因でシステムに不均衡が生じる場合があります。

- 計画された（管理上のシャットダウン）または計画外のイベントにより、チャネルまたはチャネル グループに障害が発生する。
- 部分的モードで動作を続けるケーブル モデムもあるが、一部のケーブル モデムは障害が原因で再登録をし、アクティブなチャネルに割り当てられる。
- 障害が発生したチャネルが再び動作を開始しても、ケーブル モデムは再登録せず、システムに不均衡が発生する。

この場合、モデム カウントベースの方法では、オペレータへのアラートとして SNMP トラップが送信されます。オペレータは、MAC ドメインをリセットしてすべてのケーブル モデムを強制的に再登録することにより、ケーブル モデムのバランスを再調整するよう手動で介入することを選択できます。

（注） MRC および MTC モードのケーブル モデムの場合、モデム カウントベースのロード バランシング メソッドには、ケーブル モデムの RCS および TCS におけるプライマリ チャネル上のアクティブなモデムとサービス フローの数が考慮されます。

（注） この機能を無効にするには **no cable load-balance docsis30-enable static** コマンドを使用します。

DOCSIS 3.0 ケーブル モデムの動的ロード バランシング

既存のロード バランシング（LB）機能が強化され、マルチサービス オペレータ（MSO）によるダウンストリームおよびアップストリーム チャネルの数の増加に対応したほか、16チャネル、24チャネル、および複数ダウンストリーム チャネルのケーブル モデム（CM）の広範な導入に対応しました。この強化により、顧客は使用可能な帯域幅を効率よく使用することができます。既存の LB 機能に対する強化は以下の通りです。

- DOCSIS 3.0 の使用率ベースの動的ダウンストリーム LB

- DOCSIS 3.0 LB 統計のサポート
- DOCSIS 3.0 LB 機能の有効化または無効化
- DOCSIS 3.0 LB の動的移動を行う際に、ターゲット インターフェイスのすべてのプライマリ チャネルで CM を分散します。この機能は、DOCSIS 3.0 LB の動的移動でのみ使用されます。この機能はデフォルトではディセーブルになっています。この機能を有効にするには、DOCSIS ロード バランシング グループ モードで **method utilization primary-distributed** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用するか、**method utilization us-method** コマンドを使用します。

（注） この機能を有効にするには **cable load-balance docsis-enable** コマンドを使用します。さらに、DOCSIS 3.0 ケーブル モデムの動的な使用率ベースの動的ダウンストリーム LB を有効にするには、**cable load-balance docsis30-enable** および **cable load-balance docsis30-enable dynamic downstream** コマンドを使用します。

マルチチャネル ロード バランシング動作

CM のロード バランシングは、MRC モードと MTC モードで行われます。これらのモードで動作中の CM をロード バランシングする際、次のルールが適用されます。

- MRC および MTC モードで動作している CM では、DBC を使用して、同じ MAC ドメイン内にある CM の RCS を変更することによりダウンストリーム間で CM を移動させます。

  MRC 単独モードで動作している CM は、DCC 要求のみでアップストリーム間を移動させることができます。ただし、MRC モードで動作している CM のダウンストリーム チャネルを変更している場合、DCC と初期化テクニック 0（MAC ドメインを再初期化）が使用されます。

- CM の登録中、Cisco CMTS から CM に TCC TLV のエンコーディングを含むようマルチパート登録応答（REG-RSP-MP）メッセージが送信される場合があります。この CM は TCC-capable としてマーキングされます。

  MRC、非 MTC、非 TCC-capable モードで動作している CM のロード バランシングでは以下が使用されます。

  - DBC（CM の RCS を変更するため）
  - DCC（CM のアップストリーム チャネルを変更するため）

- ナローバンド モードで動作している CM では、DCC を使用して CM を MAC ドメイン内、MAC ドメイン間で移動させます。

次の表に、ボンディングされた CM および未ボンディングの CM の移動に使用されるロード バランシング メソッドおよび動作の一覧を示します。

表 *28*：ボンディングされた *CM* および未ボンディングの *CM* を移動するためのロード バランシング メソッド

モデムのモード	ロード バランシング メソッド	ロード バランシング カウンタ	チャネル	動的サービスの要求（初期化テクニック）	
				MAC ドメイン内	**MAC** ドメイン間
DOCSIS 3.0 CM（MTC モード）	DOCSIS 3.0 静的モデム カウントベース ロード バランシング（MCBLB） DOCSIS 3.0 動的ロード バランシング	WB/UB	DS	DBC （注） DOCSIS 3.0 LB がイネーブル化され、MTC CM が RLBG 外の場合、CM は RLBG 内に移されます。	DCC init tech 0
	DOCSIS 3.0 静的モデム カウントベース ロード バランシング（MCBLB）	WB/UB	US	DBC （注） DOCSIS 3.0 LB がイネーブル化され、MTC CM が RLBG 外の場合、CM は RLBG 内に移されます。	DCC init tech 0

モデムのモード	ロード バランシング メソッド	ロード バランシング カウンタ	チャネル	動的サービスの要求（初期化テクニック）	
DOCSIS 3.0/D2.x CM（MRC 単独モード）	DOCSIS 3.0 静的 MCBLB DOCSIS 3.0 動的ロード バランシング	WB/UB	プライマリ DS チャネルの変更なし	DBC （注） DOCSIS 3.0 LB がイネーブル化され、すべての DS を含む CM が RLBG 外の場合、CM は RLBG 内に移されます。	DCC init tech 0
			プライマリ DS チャネルに変更	DCC init tech 0 （注） RLBG 外のプライマリ DS を含む CM は、DOCSIS 2.0 LB により RLBG 内に移されます。	DCC init tech 0
DOCSIS 3.0 CM（MRC 単独モード）	DOCSIS 2.0 の静的および動的MCBLB、動的使用	NB	US	DCC （注） RLBG 外の CM は、DOCSIS 2.0 LB により RLBG 内に移されます。	DCC init tech 0

モデムのモード	ロード バランシング メソッド	ロード バランシング カウンタ	チャネル	動的サービスの要求（初期化テクニック）	
D2.x CM（MRC 単独モード）	DOCSIS 2.0 の静的および動的MCBLB、動的使用	NB	US	DCC/UCC （注） RLBG 外の CM は、DOCSIS 2.0 LB により RLBG 内に移されます。	DCC init tech 0
DOCSIS 2.0 /DOCSIS 1.1 CM（NB モード）	DOCSIS 2.0 の動的MCBLB、動的使用	NB	DS	DCC （注） RLBG 外の CM は、DOCSIS 2.0 LB により RLBG 内に移されます。	DCC init tech 0
			US	UCC （注） RLBG 外の CM は、DOCSIS 2.0 LB により RLBG 内に移されます。	UCC

モデムのモード	ロード バランシング メソッド	ロード バランシング カウンタ	チャネル	動的サービスの要求（初期化テクニック）	
DOCSIS 1.0（NB モード）	DOCSIS 2.0 の動的 MCBLB、動的使用	NB	DS	CM の再初期化を強制 （注） RLBG 外の CM は、DOCSIS 2.0 LB により RLBG 内に移されます。	CM の再初期化を強制
			US	UCC （注） RLBG 外の CM は、DOCSIS 2.0 LB により RLBG 内に移されます。	UCC

表 *29* : ***DCC/DBC*** を使用した、ボンディングされた（および未ボンディングの）ケーブル モデムのロード バランシング

チャネル	**MRC、MTC** モードの **CM**	**MRC**、非 **MTC** モードの **CM**	単一の **US/DS** を含む **DOCSIS 1.1/2.0 CM**	単一の **US/DS** を含む **DOCSIS 1.0 CM**
アップストリーム（US）	DBC	DCC	DCC	UCC
ダウンストリーム（DS）	DBC（同じ MAC ドメイン内）	DBC（同じ MAC ドメイン内）	DCC（同じ MAC ドメイン内）	CM の再初期化を強制
	MAC ドメイン間で CM を移動させる場合は、DCC と初期化テクニック 0	MAC ドメイン間で CM を移動させる場合は、DCC と初期化テクニック 0	MAC ドメイン間で CM を移動させる場合は、DCC と初期化テクニック 0	CM の再初期化を強制

DBC を使用した DOCSIS 3.0 ロード バランシング移動

DOCSIS 3.0 仕様の一部として、登録後はいつでも Cisco CMTS は DBC コマンドを使用して次の任意の DOCSIS 3.0 CM のパラメータを変更できます。

- 受信チャネル セット
- 送信チャネル セット
- DSID 属性または DSID 関連の属性
- ダウンストリーム トラフィックを暗号化するためのセキュリティ アソシエーション
- サービス フロー クラスタ割り当て

（注） DOCSIS 3.0 静的ロード バランシングには、RCS と TCS のみが使用されます。

ロード バランシング処理の現在のリアルタイム統計情報を表示するには、**showcableload-balancedocsis-group** コマンドを使用します。詳細については、『Cisco IOS CMTS Cable Command Reference』を参照してください。

DBC を使用した受信チャネル セットの変更

Cisco CMTS は、DBC-REQ に RCC を含めることにより、ケーブル モデムの RCS 内のチャネルを追加、削除または変更することができます。

RCS の変更がケーブル モデムのプライマリ ダウンストリーム チャネルに影響を与える場合、ケーブル モデムをアップストリーム チャネルで再登録する必要があります。

RCS からチャネルが削除された場合、Cisco CMTS は削除される必要があるダウンストリーム チャネル上のトラフィックの送信を停止し、これにより、トラフィックの損失が起きる場合があります。Cisco CMTS は、ケーブル モデムから DBC-RSP を受け取るまでは新旧 RCS 上でトラフィックを重複させることにより、パケット損失を最小限にします。

（注） MRC 単独モードのケーブル モデムでは、ダウンストリーム チャネルの移動は DBC メッセージによって開始されます。ただし、プライマリ ダウンストリーム チャネルに変更がある場合は、DCC 初期化テクニック 0 が使用されます。

DBC を使用した送信チャネル設定の変更

Cisco CMTS は、単一の DBC メッセージ内の TCS で 1 つまたは複数のチャネルを追加、削除、または置換できます。ケーブル モデムの TCS が変化するたびに、CMTS は影響を受けるサービス フローに関連付けられているサービス ID（SID）を変更します。

TCS の変更では、有効な初期化テクニックも実行します。

DBC を使用したダウンストリーム *ID* の変更

DBC を使用して、Cisco CMTS はダウンストリーム ID（DSID）の次の属性を変更できます。

- 再シーケンシングのエンコーディング：
  - ダウンストリーム再シーケンシング チャネル リスト：CMTS は、DS 再シーケンシング チャネル リスト内のチャネルを追加、削除、置換できます。
  - DSID 再シーケンシング待機時間：CMTS は、DSID 再シーケンシング待機時間により、ネットワークまたは設定の変更による偏りの変更を示すことができます。
- 再シーケンシング警告しきい値
- 範囲外イベントに対する CM-STATUS Hold-Off タイマー
- マルチキャスト エンコーディング：CMTS は、既存のマルチキャスト DSID の属性を追加、削除、または変更する DBC トランザクションを開始できます。
  - クライアント MAC アドレス
  - マルチキャスト ケーブル モデム インターフェイス マスク
  - グループ MAC アドレス

DBC を使用したダウンストリーム トラフィック暗号化のセキュリティ アソシエーションの変更

- CMTS は、ダウンストリーム トラフィックの暗号化に使用されるセキュリティ アソシエーション（SA）を追加または削除する DBC トランザクションを開始できます。
- CMTS は、[Authorized] 状態でないケーブル モデムに DBC 要求を送信できません。
- CMTS は、ケーブル モデムでサポートされていない暗号スイートを使用する SA により DBC 要求を送信できます。ただし、ケーブル モデムが使用できない SA を含む DBC 要求を受信すると、ケーブル モデムは DBC 要求を拒否します。

DBC を使用したサービス フロー *SID* クラスタ割り当ての変更

Cisco CMTS では、サービス フロー SID クラスタ割り当ての TLV を DBC 要求で使用して、新しいチャネルをサービス フローに割り当てたり、チャネルをサービス フローから削除したり、サービス フロー用のチャネルを置換することができます。

（注） 1 つの DBC メッセージで複数のアクションが発生する可能性があります。

ロード バランシングの利点

Cisco CMTS のロード バランシング機能では、ケーブル サービス プロバイダーとそのパートナーおよびカスタマーに次の利点があります。

- 特にファイバ ノードあたり複数のアップストリーム チャネルを使用するときに、サービス プロバイダーが効率的な帯域幅利用のために使用できる方法を提供します。

- サービス プロバイダーは効率的な方法でネットワークを拡張でき、追加の光ファイバ設備を設置したり物理設備のセグメント化を促進するためのコストが回避されます。
- ダウンストリーム チャネルでのロード バランシングにより、Video over IP や、高帯域幅のリアルタイム ストリームを必要とするその他のサービス フローを有効にするためにファイバ ノードあたり複数のダウンストリーム チャネルを使用するときに、効率的な帯域幅使用を可能にします。
- アップストリームおよびダウンストリーム チャネルのロードバランシングでは、プロビジョニング サーバや DOCSIS コンフィギュレーション ファイルを変更する必要はありません。
- アップストリームおよびダウンストリーム チャネルのロード バランシングでは、管理者やユーザの介入（手動でケーブル インターフェイスをリセットしたり、手動でケーブル モデムをリブートしたりなど）は必要ありません。
- サービス プロバイダーは、すべてのケーブル モデムが同じダウンストリームで登録されないようにするために、ケーブル モデムの登録時にダウンストリームを均等にバランス調整できます。その結果、多数のケーブル モデムが登録に失敗して新しいダウンストリームを探す必要が生じます。
- ケーブル モデムには、IP アドレスなどのネットワーク パラメータを手作業で変更することなく、ダウンストリーム チャネルおよびアップストリーム チャネル間で移動できます。
- サービス プロバイダーは、現在の負荷使用状況に動的に対応することで、カスタマーの帯域幅需要を先回りできます。
- サービス プロバイダー、Voice over IP（VoIP）などの重要なサービスのロード バランシング パラメータを最適化できます。

ロード バランシング グループからのケーブル モデムの除外

ロード バランシング プロセス

ロード バランシング プロセスには 2 つのフェーズがあります。

- 割り当てフェーズ。

  モデムが割り当てフェーズでオンラインになると、ロード バランシング グループ（LBG）ID をモデムに割り当てることで、モデムがロード バランシング グループに移動します。割り当てフェーズは、モデムがオンラインになるときにのみ発生します。

- バランシング フェーズ。

  バランシング フェーズでは、負荷の分散のために、モデムはLBGに再び割り当てられます。

ロード バランシングからのケーブル モデムの除外

LBG からケーブル モデムを除外するのに使用するオプションは 4 つあります。

- **assignment** オプション：

  割り当てフェーズでモデムを除外するには、**assignment** オプションを使用します。モデムは LBG に割り当てられず、LBG ID は **show cable modem verbose** コマンドの出力に表示されま

せん。モデムがすでにオンラインである場合は、**assignment** オプションを使用することはできません。

- **static** オプション：

  バランシング フェーズでモデムを除外するには、**static** オプションを使用します。モデムは、LBG ID を使用して LBG に割り当てられます。静的ロード バランシングでモデムを除外するには、**static** オプションを使用します。

- **enforce** オプション：

  enforce オプションは **static** オプションと同様ですが、**enforce** オプションは動的ロード バランシングの際にモデムを除外するという点が異なります。

assignment オプションを使用してケーブル モデムをロード バランシングから除外した場合、そのケーブル モデムは **static** または **enforce** オプションを使用したロード バランシングに使用できなくなります。

- **strict** オプション：

  strict オプションは、ロード バランシングの両方のフェーズでモデムを除外します。モデムが既にオンラインになっている場合、 **strict** オプションによって **static** および **enforce** オプションが適用されます。ケーブル モデムが再びオンラインになった場合にのみ、**assignment** オプションが適用されます。

ロード バランシングの設定方法

ロード バランシング グループを設定してロード バランシングをイネーブルにする方法については、『*DOCSIS Load Balancing Groups*』を参照してください。必要に応じて、各作業には、必須または任意のマークが付けられています。

単一チャネルのロード バランシングの有効化

単一チャネルのロード バランシングを設定するには、『*DOCSIS Load Balancing Groups guide*』を参照してください。

DOCSIS 3.0 静的ロード バランシングの動的ボンディング変更の設定

DOCSIS 3.0 静的ロードバランシングを有効にするには、グローバル コンフィギュレーション モードで **cable load-balance docsis30-enabled** コマンドを使用します。

（注） DOCSIS 3.0 静的ロード バランシングでは、ロードバランシングにモデム カウント方式を常に使用します。

はじめる前に

ロード バランシング グループを設定します。詳細については、『*DOCSIS Load Balancing Groups guide*』を参照してください。

ロード バランシング グループからのケーブル モデムの除外

この設定は任意です。ここでは、静的または動的ロード バランシング動作への登録や、受動的ロードバランシングのためのモデムの任意のマーキングから、特定のケーブルモデムまたは特定のベンダーのすべてのケーブル モデムを除外する方法について説明します。デフォルトでは、インターフェイス上のケーブルモデムは、ロードバランシング動作が設定されたモデムに登録されているため、このタスクは任意です。

（注） この手順は、DOCSISに準拠していないケーブル モデムで必要となる可能性があります。そのようなケーブル モデムは、DOCSIS MAC メッセージを使用してロード バランシングが実行されると、長期間オフラインになります。この場合、そのようなケーブル モデムが DOCSIS 準拠ソフトウェアにアップグレードされるまで、 **cable load-balance exclude** コマンドを使用し、ロード バランシング動作からケーブル モデムを除外します。

ヒント 特定のアップストリーム チャネルまたはダウンストリーム周波数を必要とするケーブル モデムを除外する必要があります。DOCSIS コンフィギュレーション ファイルでケーブル モデムに特定のチャネルまたは周波数が割り当てられている場合は、ロード バランシングを実行できません。

古いデバイスの除外のサポート

セット トップ ボックス（STB）など、ロード バランシングをサポートしない古いケーブル デバイスのロード バランシングは失敗します。**showcableload-balancegroup** コマンドの出力では、これらのデバイスは「suspicious」と表示され、次に「disabled」と表示されます。これにより、ロード バランシング グループの他のモデムの正常な動作が妨害されます。これらの STB を除外するには、各 STB を除外するように **cableload-balanceexclude** コマンドを設定します。

（注） 一致対象のMACアドレスを使ってコマンドを複数回設定する代わりに、**cableload-balanceexclude** コマンドを一度設定すれば、ロード バランシングをサポートしないすべての STB を除外できます。また、割り当てフェーズでロード バランシング グループに移動したケーブル モデムも移動できます。

cableload-balanceexclude モデム コマンドが変更され、オプション引数として *mask* 引数が含まれるようになりました。MACアドレスマスクによって指定される範囲に属するケーブルモデムのMACアドレスは、マスクの1ビットが一致すると除外されます。*mask* 引数を使用して新しい範囲ルールを設定すると、同じ範囲の既存のルールは上書きされます。

cableload-balanceexclude モデム コマンドが修正されて、**assignment** オプションが含まれるようになりました。このオプションにより、割り当てフェーズでロード バランシング グループに移動されたケーブル モデムを除外できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cableload-balanceexclude** {**modem** *mac-address* [*mac-mask*] | **oui** *oui-value*} [**assignment** | **enforce** | **static** | **strict**] 例： `Router(config)# cable load-balance exclude oui 00:00:0c`	1つ以上のケーブルモデムをロードバランシング動作から除外する必要があることを指定します。 デフォルトでは、ケーブルモデムは動的および静的ロードバランシングから除外されますが、受動的ロード バランシングには引き続き登録されます。他ロードバランシングの組み合わせからケーブルモデムを除外するには、次のオプションを使用します。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

アップストリーム ロード バランシングを使用したダウンストリーム ロード バランシングの分散

Cisco CMTS で分散型ロード バランシングの構成とステータスを設定または表示するには、2 つのコマンドを使用します。

- **cableload-balancegroup** *ds-lb-group-id* **policy**{**pcmm** | **ugs** | **us-groups-across-ds**}
- **showcableloadall**

ダウンストリーム ロードバランシングの決定を行うオプション設定は、次のようにイネーブルにします。

- ターゲット ダウンストリーム セグメントは、ソース ダウンストリーム セグメントと同じダウンストリーム ロードバランシング グループ内にあります。この機能は、送信元と同じアップストリーム グループ内のアップストリームの負荷に基づいてターゲット周波数とインターフェイスを探します。
- アップストリーム ロード バランシング グループは、ケーブル モデムのバランシングが行われるダウンストリーム チャネルで対応するチャネルに対して設定できます。
- Cisco CMTS は、ロード バランシング グループのアップストリーム セグメントを自動的に探し、最も負荷の少ない送信元インターフェイスのアップストリーム グループ ステータスを処理します。
- ターゲット ダウンストリーム セグメントには、アップストリーム ロード バランシング グループで設定したアップストリーム チャネルが必要です。
- 最上位のターゲット アップストリーム セグメントでは、他のインターフェイス上の最上位アップストリームセグメントなど、他の潜在的なターゲットよりも負荷を少なくする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cableload-balancegroup** *ds-lb-group-id* **policy**{**pcmm** | **ugs** | **us-groups-across-ds**}	ロード バランシングで使用するサービス フロー ポリシーのタイプを設定します。このコマンドは、ロード バランシング グループ内のさまざまなケー

	コマンドまたはアクション	目的
	例： `Router(config)# cable load-balance group 1 policy us-groups-across-ds`	ブル インターフェイス ライン カード間にある保留中の統計情報を同期します。その結果、ロードバランシングの決定時のダウンストリームの総負荷よりも、アップストリーム単位の負荷を使用する別のダウンストリーム ロード バランシング方式になります。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 5	**showcableloadall** 例： `Router# show cable load all`	Cisco CMTS のロード バランシングの統計情報およびロードバランシング設定のステータスを表示し、設定時のアップストリームとダウンストリームの分散型ロード バランシングを含めます。

ロード バランシングの動的チャネル変更の設定方法

DOCSIS 1.1 の DCC は、ケーブル モデムを強制的にオフラインにしたり、変更後に再登録したりせずに、ケーブル モデムのアップストリームまたはダウンストリームのチャネルを動的に変更します。DCC は、以前の DOCSIS サポートのように 1 つではなく、異なる 5 つの初期化テクニック（0 - 4）をサポートします。

Cisco CMTS での動的チャネル変更（DCC）およびロード バランシングのための DCC は、次の項目をサポートします。

- ロード バランシング手法により、設定可能な初期化テクニックを使用して DCC 搭載のケーブル モデムを移動できます。
- DCC を 0 ～ 4 の範囲の DCC 初期化テクニックとともに使用すると、同じケーブル インターフェイス ライン カード内の個々のダウンストリーム チャネル間でライン カード チャネルを変更できるようになります。
- DCC は、ケーブル モデム状態の情報を発信ダウンストリーム チャネルから対象のダウンストリーム チャネルに転送し、ケーブル インターフェイス ライン カードとネットワーク プロセッシング エンジン（NPE）またはルート プロセッサ（RP）間のケーブル モデム情報の同期化を維持します。
- PacketCable（PC）や PacketCable Multimedia（PCMM）などの遅延に敏感なアプリケーションは、DCC 初期化テクニック 4 を使用し、ケーブル モデムが DCC を実行している間のサービスを維持します。
- チャネルが混合モードまたは ATDMA のみモードの場合、プライマリ サービス ID（SID）を ATDMA のみモードに切り替える必要があります。

ロード バランシングの動的チャネル変更の設定

ロード バランシングの DCC 機能を設定するには、次の手順を実行します。表示されている値はサンプルであり、使用する値とは異なる場合があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cableload-balancedocsis-enable** 例： `Router(config)# cable load-balance docsis-enable`	Cisco CMTS での DOCSIS ロード バランシングをイネーブルにします。
ステップ 4	**cableload-balancedocsis-group** *docsis-group-id* 例： `Router(config)# cable load-balance docsis-group 1`	次のパラメータを使用して、Cisco CMTS で DOCSIS ロード バランシング グループを作成します。 ルータは、DOCSIS ロードバランシング グループのコンフィギュレーション モードを開始します。
ステップ 5	**init-tech-list** *tech-list* [**ucc**] 例： `Router(config-lb-group)# init-tech-list 1 ucc`	Cisco CMTS でケーブル モデムをロード バランシングする DCC 初期化テクニックを設置します。

ステップ 6	**policy**{**pcmm** | **ugs** | **us-across-ds** | **pure-ds-load**}
	
	例：
	`Router(config-lb-group)# policy us-across-ds`
	`Router(config-lb-group)# policy ugs`
	`Router(config-lb-group)# policy pure-ds-load`
		バランシングするサービス フロー タイプに基づいてモデムを選択します。

	コマンドまたはアクション	目的

ステップ 7	**threshold** {**load** {**minimum** *<1-100>* | *<1-100>*}| **pcmm** *<1-100>* | **stability** *<0-100>* | **ugs** *<1-100>*}
	
	例：
	`Router(config-lb-group)# threshold load minimum 10`
	`Router(config-lb-group)# threshold pcmm 70`
	`Router(config-lb-group)# threshold load 10`
	`Router(config-lb-group)# threshold stability 50`
	`Router(config-lb-group)# threshold ugs 70`
		ロードバランシングが発生する下限の使用率を選択します。

ステップ 8	**end** 例： `Router# end`	特権 EXEC モードに戻ります。

次の作業

ロード バランシングの DCC をテストおよび確認するには、次の 2 つのコマンドを使用します。

- **testcabledcc**
- **showcontrollerscable**

これらのコマンドの説明は、『*Cisco CMTS Cable Command Reference*』に記載されています。

ロード バランシング動作の確認

ここでは、Cisco CMTS でロード バランシング機能または動的チャネル変更機能の設定と動作を確認するために、特定のテストおよび show コマンドを使用する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**showcableload-balance** [**group** *n*] [**all** | **load**| **pending** | **statistics**| **target**]	ロード バランシング 動作の統計情報および動作情報をリアルタイムに表示します。オプションを指定しない場合、このコマンドでは、ロード バランシング グ

	コマンドまたはアクション	目的
	例： `Router# show cable load-balance group 1`	ループと各ケーブルインターフェイスの現在の負荷とロードバランシングのステータスに関する情報が表示されます。次のオプションを指定することもできます。
ステップ3	**testcabledcc** [*mac-addr* | *ip-addr* | *cable-if-src sid*] *cable-if-target uschan* {*ranging-tech* } 例： `Router# test cable dcc 0000.394e.4e59`	MAC アドレス、IP アドレス、またはプライマリ サービスID（SID）値で指定したとおりにターゲット ケーブルモデムを移動し、動的チャネル変更（DCC）をテストします。指定した初期化テクニックを使用して、送信元インターフェイスのケーブルモデムをターゲット ダウンストリーム インターフェイスのアップストリーム チャネルに適用します。

例

次に、ロード バランシング操作の結果例を示します。

```
Router#show cable load all
DOCSIS 2.0 LB Enabled: Yes DOCSIS 3.0 LB Enabled: No
DOCSIS     Status Interval DCC mask  Policy     Method Threshold
Group                      /UCC                DS/US  M/E/U/P/S
1          RE     30       0xF8(0)/N 0         m/m    5/10/70/70/50
12345      GE     30       0xF8(0)/N 0         m/m    5/10/70/70/50
12346      RE     30       0xF8(0)/N 0         m/m    5/10/70/70/50
12347      RE     30       0xF8(0)/N 0         m/m    5/10/70/70/50
12348      RE     30       0xF8(0)/N 0         m/m    5/10/70/70/50
12349      RE     30       0xF8(0)/N 0         m/m    5/10/70/70/50

DOCSIS 3.0 General LB
MD       FN  Group ID   S Intv DCC mask  Policy     Mtd MD-CM-SG  Threshold
                                /UCC                D/U           M/E/U/P/S
Ca8/0/0  1   2147631104 E 30   0x30(2)/N 0         m/m 0x1200301 5/10/70/70/50
Ca8/0/1  3   2147631618 E 30   0x30(2)/N 0         m/m 0x1210301 5/10/70/70/50
Ca8/0/2  5   2147632132 E 30   0x30(2)/N 0         m/m 0x1220401 5/10/70/70/50
Ca8/0/2  6   2147632133 E 30   0x30(2)/N 0         m/m 0x1220402 5/10/70/70/50
Ca8/0/3  7   2147632646 E 30   0x30(2)/N 0         m/m 0x1230501 5/10/70/70/50
Ca8/0/3  8   2147632647 E 30   0x30(2)/N 0         m/m 0x1230502 5/10/70/70/50
Ca8/0/8  2   2147635201 E 30   0x30(2)/N 0         m/m 0x1280201 5/10/70/70/50
Ca8/0/9  4   2147635715 E 30   0x30(2)/N 0         m/m 0x1290201 5/10/70/70/50

Current load:

DOCSIS load-balancing load
Interface           State   Group      Utilization     Rsvd NBCM  WB/UB Weight
                                                           Total Total
In8/0/0:0(411 MHz)  initial 1          0%(0%/0%)       0%   0     11    37
In8/0/0:0(411 MHz)  initial 2147631104 0%(0%/0%)       0%   0     11    37
Us8/0/0:0           initial 1          0%              0%   0     31    30.7
Us8/0/0:0           initial 2147631104 0%              0%   0     31    30.7
Us8/0/0:1           initial 1          0%              0%   0     31    30.7
Us8/0/0:1           initial 2147631104 0%              0%   0     31    30.7
Us8/0/0:2           initial 2147631104 0%              0%   0     31    30.7
Us8/0/0:2           initial 1          0%              0%   0     31    30.7
Us8/0/0:3           initial 2147631104 0%              0%   0     31    30.7
Us8/0/0:3           initial 1          0%              0%   0     31    30.7
In8/0/0:4(435 MHz)  up      2147635201 0%(0%/0%)       0%   48    11    37
```

```
Us8/0/1:0           up      2147635201 0%              0%   15    0     30.7
Us8/0/1:1           up      2147635201 0%              0%   11    0     30.7
Us8/0/1:2           up      2147635201 0%              0%   11    0     30.7
Us8/0/1:3           up      2147635201 0%              0%   11    0     30.7
In8/0/0:8(459 MHz)  initial 1          0%(0%/0%)       0%   0     9     37
In8/0/0:8(459 MHz)  initial 2147631104 0%(0%/0%)       0%   0     9     37
Us8/0/0:0           initial 1          0%              0%   0     31    30.7
Us8/0/0:0           initial 2147631104 0%              0%   0     31    30.7
Us8/0/0:1           initial 1          0%              0%   0     31    30.7
Us8/0/0:1           initial 2147631104 0%              0%   0     31    30.7
Us8/0/0:2           initial 2147631104 0%              0%   0     31    30.7
Us8/0/0:2           initial 1          0%              0%   0     31    30.7
Us8/0/0:3           initial 2147631104 0%              0%   0     31    30.7
Us8/0/0:3           initial 1          0%              0%   0     31    30.7
In8/0/0:12(483 MHz) down    2147635201 0%(0%/0%)       0%   0           0
In8/0/0:16(507 MHz) initial 2147631104 0%(0%/0%)       0%   0     11    37
In8/0/0:16(507 MHz) initial 1          0%(0%/0%)       0%   0     11    37
Us8/0/0:0           initial 2147631104 0%              0%   0     31    30.7
Us8/0/0:0           initial 1          0%              0%   0     31    30.7
Us8/0/0:1           initial 2147631104 0%              0%   0     31    30.7
Us8/0/0:1           initial 1          0%              0%   0     31    30.7
Us8/0/0:2           initial 2147631104 0%              0%   0     31    30.7
Us8/0/0:2           initial 1          0%              0%   0     31    30.7
Us8/0/0:3           initial 2147631104 0%              0%   0     31    30.7
Us8/0/0:3           initial 1          0%              0%   0     31    30.7
In8/0/0:20(531 MHz) down    2147635201 0%(0%/0%)       0%   0           0
In8/0/1:0(555 MHz)  initial 2147631618 0%(0%/0%)       0%   0     12    37
Us8/0/2:0           initial 2147631618 0%              0%   0     19    30.7
Us8/0/2:1           initial 2147631618 0%              0%   0     19    30.7
Us8/0/2:2           initial 2147631618 0%              0%   0     19    30.7
```

トラブルシューティングのヒント

問題 あるチャネルから別のチャネルにケーブル モデムを移動すると、パケットがドロップされる。

考えられる原因 **testcabledcc** コマンドを使用し、DCC 初期化テクニック 3 を使って 1 つのチャネルから別のチャネルに移動すると、以下が実行されます。

- 事前均等化係数を有効にすると、ケーブル モデムは移動し、パケットのドロップが 5 秒間実行されます。
- 事前均等化係数を無効にすると、ケーブル モデムは移動し、パケットのドロップが 1 秒未満実行されます。

考えられる原因 **testcabledcc** コマンドを使用し、DCC 初期化テクニック 4 を使って 1 つのチャネルから別のチャネルに移動すると、以下が実行されます。

- 事前均等化係数を有効にすると、ケーブル モデムは移動し、パケットのドロップが 1 秒未満実行されます。
- 事前均等化係数を無効にすると、パケットがドロップされることなく、ケーブル モデムは移動します。

解決法 特に対処の必要はありません。

例

ロード バランシングに使用されているインターフェイスを表示するには、**showcableload-balancetarget** コマンドを使用します。ケーブル モデムをインターフェイス間で移動できるかどうかをテストするには**testcableload-balance** コマンドを使用し、テストの結果を表示するには **showcableload-balancestatistics** コマンドを使用します。

次の例では、特定のケーブルモデムがUCC要求とアップストリーム チャネルの上書きに応答し、対応するロードバランシング グループ内にあるアップストリームから別のアップストリームに移動できるかをテストする方法について説明します。

```
Router# show cable load-balance target

Target assignments:
Interface            State      Group  Target
Cable1/0/0 (669 MHz) up         1
Cable1/0/0/U0        up         1      Cable1/0/0/U1 [enforce]
Cable1/0/0/U1        up         1

Router# show cable load-balance statistics

Statistics:

Target interface     State      Transfers
                                Complete  Pending   Retries   Failures
Cable1/0/0 (669 MHz) up         15        0         1         0
Cable1/0/0/U0        up         33        0         1         0
Cable1/0/0/U1        up         22        0         2         0

Router# test cable load-balance 0000.394e.4e59

Sending UCC request: Cable1/0/0/U0 --> U1
Waiting for test completion ........
Test results:
    UCC Response: 0.0s
    Initial Ranging: 8.5s
    Ranging Complete: failed.
    Modem replied to DOCSIS ping.
Test summary:
    UCC Response: success rate 100% min 0.0s max 0.0s avg 0.0s
    Initial Ranging: success rate 100% min 8.5s max 8.5s avg 8.5s
Testing US Channel Override: Cable1/0/0/U1 --> U0
Waiting for test completion ...........
Test results:
    Initial Ranging: 8.5s
    Ranging Complete: failed.
    Modem replied to DOCSIS ping.
Test summary:
    UCC Response: success rate 100% min 0.0s max 0.0s avg 0.0s
    Initial Ranging: success rate 100% min 8.5s max 8.5s avg 8.5s

Router# show cable load-balance statistics

Statistics:

Target interface     State      Transfers
                                Complete  Pending   Retries   Failures
Cable1/0/0 (669 MHz) up         15        0         1         0
Cable1/0/0/U0        up         34        0         1         0
Cable1/0/0/U1        up         23        0         2         0
```

次の例では、特定のケーブル モデムが UCC 要求に応答し、対応するロード バランシング グループ内にあるアップストリームから別のアップストリームに移動できるかをテストする方法について説明します。

```
Router# show cable load-balance statistics

Statistics:
```

```
Target interface     State      Transfers
                                Complete  Pending   Retries   Failures
Cable1/0/0 (669 MHz) up         15        0         1         0
Cable1/0/0/U0        up         34        0         1         0
Cable1/0/0/U1        up         23        0         2         0

Router# test cable load-balance 0007.0e01.4129 ucc 1

Sending UCC request: Cable1/0/0/U0 --> U1
Waiting for test completion ........
Test results:
    UCC Response: 0.0s
    Initial Ranging: 10.3s
    Ranging Complete: 11.2s
    Modem replied to DOCSIS ping.
Test summary:
    UCC Response: success rate 100% min 0.0s max 0.0s avg 0.0s
    Initial Ranging: success rate 100% min 10.3s max 10.3s avg 10.3s
    Ranging Complete: success rate 100% min 11.2s max 11.2s avg 11.2s

Router# show cable load-balance statistics

Statistics:

Target interface     State      Transfers
                                Complete  Pending   Retries   Failures
Cable1/0/0 (669 MHz) up         15        0         1         0
Cable1/0/0/U0        up         35        0         1         0
Cable1/0/0/U1        up         24        0         2         0
```

次の例では、DCC 初期化テクニック 1 を使用して、ケーブル モデムを別のアップストリーム チャネルに移動する場合の情報が表示されます。この例では、DCC 初期化テクニック 1 を使用して、インターフェイス c7/1/0 アップストリーム 1 からインターフェイス c7/1/1 アップストリーム 0 にケーブル モデム 0012.17ea.f563 を移動します。

```
Router# show cable modem

MAC Address    IP Address      I/F       MAC         Prim RxPwr  Timing  Num BPI
                                         State       Sid  (dB)   Offset  CPE Enb
 State       Sid  (dB)   Offset  CPE Enb
0012.17ea.f563 12.0.0.2        C7/1/0/U1 online      4    0.00  2449     0   N

Router# test cable dcc 0012.17ea.f563 c7/1/1 0 1

Router# show cable modem

MAC Address    IP Address      I/F       MAC         Prim RxPwr  Timing  Num BPI
                                         State       Sid  (dB)   Offset  CPE Enb
0012.17ea.f563 12.0.0.2        C7/1/1/U0 online      3    0.00  2451     0   N
```

ロード バランシングの設定例

ここでは、次の設定例について説明します。

例：ロード バランシングの動的チャネル変更の設定

次に、DOCSIS 3.0 ケーブル モデムでの動的ロード バランシングの動作プロセスの仕組みについて説明します。

設定の確認：

```
Router#  show cable load-balance docsis-group 1
DOCSIS LB Enabled: Yes
```

```
DOCSIS 2.0 LB Enabled: No
DOCSIS 3.0 LB Enabled: Yes
DOCSIS 3.0 Static LB Enabled: No
DOCSIS 3.0 Dynamic Downstream LB Enabled: Yes
DOCSIS Status Interval DCC mask Policy Method Threshold
Group /UCC DS/US M/E/U/P/S
1 RE 60 0x38(2)/N 0 u/u 1/10/70/70/50
```

チャネル流負荷の確認：

```
Router#  show cable load-balance docsis-group 1 load wideband
DOCSIS load-balancing wide band load
Interface Size Group Throughput(Kbps)/bw(Mbps) Avg-Util
Wi9/0/0:1 8 1 93324/300 36%
Wi9/0/0:2 8 1 37329/300 39%
Wi9/0/0:3 8 1 74659/300 31%
Wi9/0/0:4 8 1 0/300 13%
Wi9/0/0:5 8 1 9332/300 2%
```

チャネル オーバーロードとターゲットの確認：

```
Router#  show cable load-balance docsis-group 1 target wideband
Interface Bg-Id State Group Target
Wi9/0/0:1 28674 up 1 Wi9/0/0:5 ...
Wi9/0/0:2 28675 up 1 Wi9/0/0:5 ...
Wi9/0/0:3 28676 up 1 Wi9/0/0:5 ...
Wi9/0/0:4 28677 up 1 Wi9/0/0:5
Wi9/0/0:5 28678 up 1
```

チャネル モデム リストの確認：

```
Router#  show cable load-balance docsis-group 1 modem-list wideband
Codes: M - Multicast, U - UGS, P - PCMM, F - Max-Failures, X - eXcluded
L - L2vpn, R - RSVP
Primary WB MAC Address Primary DS RCC-ID Priority MUPFXLR State
Wi9/0/0:1 (10)
c8fb.26a6.c02c In9/0/0:4 1 0 ------- LB_CM_READY
c8fb.26a6.c62c In9/0/0:4 1 0 ------- LB_CM_READY
c8fb.26a6.c706 In9/0/0:4 1 0 ------- LB_CM_READY
c8fb.26a6.c0dc In9/0/0:4 1 0 ------- LB_CM_READY
c8fb.26a6.c53a In9/0/0:4 1 0 ------- LB_CM_READY
```

QAM チャネル使用率の確認：

```
Router#  show cable load-balance docsis-group 1 rfch-util
Interface Pstate Pending-In Pending-Out Throughput(Kbps) Util
In9/0/0:4 up No No 6517 17
In9/0/0:5 NA No No 6574 17
In9/0/0:6 NA No No 6520 17
In9/0/0:7 NA No No 6738 17
In9/0/0:8 up No No 8624 22
In9/0/0:9 NA No No 8482 22
In9/0/0:10 NA No No 8353 22
```

チャネル統計動向の確認：

```
Router#  show cable load-balance docsis-group 1 statistics wideband
Target interface State Transfers
Complete Pending Total Failures Disabled
Wi9/0/0:1 up 0 0 0 0 0
Wi9/0/0:2 up 0 0 0 0 0
Wi9/0/0:3 up 3 0 3 0 0
Wi9/0/0:4 up 0 0 0 0 0
Wi9/0/0:5 up 9 0 9 0 0
```

次の実行コンフィギュレーションの例では、ロード バランシングの DCC について説明します。

```
Router# show cable load all

*Nov 11 15:42:18.955: %SYS-5-CONFIG_I: Configured from console by conscable load all
Group  Interval  Method      DCC Init     Threshold
                           Technique    Minimum  Static  Enforce  Ugs   PCMM
1      10        modems      0             5        10%     ---     ---   ---

Current load:

Interface            State      Group Utilization  Reserved Modems Flows Weight
```

```
Cable3/0 (0 MHz)     initial    1     0%(0%/0%)    0%       0      0     26

Target assignments:

Interface            State      Group  Target
Cable3/0 (0 MHz)     initial    1

Statistics:

Target interface       State      Transfers
                                  Complete  Pending   Retries   Failures
Cable3/0 (0 MHz)       initial    0         0         0         0
Pending:
Modem          Group  Source interface  Target interface     Retries
```

次の実行コンフィギュレーションの例では、ロード バランシングの DCC について説明します。

```
Router# show running configuration

Building configuration...
Current configuration : 11889 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname Router
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$tEvV$8xICVVbFm10hx0hAB7DO90
enable password lab
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable load-balance group 1 threshold load 75 enforce
cable load-balance group 1 threshold stability 75
cable load-balance group 1 policy ugs
cable load-balance group 1 threshold ugs 75
cable load-balance group 1 policy pcmm
cable load-balance group 1 threshold pcmm 75
no aaa new-model
ip subnet-zero
!
!
ip cef
no ip domain lookup
!
!
interface GigabitEthernet0/1
 ip address 10.14.1.130 255.255.0.0
 duplex auto
 speed auto
 media-type rj45
 no negotiation auto
!
interface GigabitEthernet0/2
```

次の show cable load all コマンドの例では、ロード バランシングの DCC について説明します。

```
Router# show cable load all

*Nov 11 15:43:39.979: %SYS-5-CONFIG_I: Configured fromconf t
Group  Interval  Method      DCC Init     Threshold
                           Technique    Minimum  Static  Enforce  Ugs   PCMM
1      10        modems      0             5        75%     75%     75%   75%

Current load:
```

```
Interface            State      Group Utilization  Reserved Modems Flows Weight
Cable3/0 (0 MHz)     initial    1     0%(0%/0%)    0%       0      0     26

Target assignments:

Interface            State      Group  Target
Cable3/0 (0 MHz)     initial    1

Statistics:

Target interface       State      Transfers
                                  Complete  Pending   Retries   Failures
Cable3/0 (0 MHz)       initial    0         0         0         0

Pending:

Modem          Group  Source interface  Target interface     Retries
```

次に、デフォルトの DCC 初期化テクニックを使用した DCC ロード バランシング グループの例を示します。次のコマンドは、ロード バランシング グループ 1 を設定します。

```
Router(config)# cable load-balance group 1 threshold load 10 enforce
```

この設定により、次のデフォルト設定で動的ロード バランシング グループが作成されます。

```
cable load-balance group 1 method modem
cable load-balance group 1 threshold load 10 enforce
cable load-balance group 1 interval 10
cable load-balance group 1 dcc-init-technique 0
```

次に、この DCC ロード バランシング設定を初期化テクニック 4 に変更する例を示します。

```
Router# cable load-balance group 1 dcc-init-technique 4
```

（注） デフォルトでは、UGS および PCMM ポリシーが有効ではないため、アクティブな音声コールを持つ CM または PCMM コールがロード バランシングに参加します。

その他の参考資料

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

DOCSIS ロード バランシング移動に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *30* : *DOCSIS* ロード バランシング グループに関する機能情報

機能名	リリース	機能情報
DOCSIS ロードバランシング移動	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 14 章

DOCSIS 3.0 ダウンストリーム ボンディング

DOCSIS 3.0 ダウンストリーム ボンディング機能により、ケーブル オペレータは、標準ブロードバンド DOCSIS システムに 1 つまたは複数のダウンストリーム直交振幅変調（QAM）チャネルを追加することで、新規でより帯域消費型のサービスを提供できるようになります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *31*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

DOCSIS 3.0 ダウンストリーム ボンディングの情報

DOCSIS 3.0 ダウンストリーム ボンディングを使用すると、高速ブロードバンド アクセスが有効になり、ケーブル オペレータは1つ以上の直交振幅変調（QAM）チャネルを標準のブロードバンド DOCSIS システムに追加することで帯域幅をさらに大量に消費するサービスを提供できます。

このような新しいダウンストリーム チャネルのセットは、「束ねられたチャネル」と呼ばれる大きな 1 つのチャネルにグループ化されます。

チャネル ボンディングは、複数の RF チャネルを 1 つの仮想チャネルに結合します。この仮想チャネルのデータ レートは、数百メガビット/秒からときには数ギガビット/秒にまで及び、ネットワークでより多くの使用可能な帯域幅が作成されます。

受信チャネル プロファイル

RCP は、ケーブル モデムの受信チャネルおよび受信モジュールを表すエンコーディングです。ケーブル モデムは、DOCSIS 3.0 で定義された完全なサブタイプ エンコーディングを含む冗長な記述、または RCP ID のみを含む簡易な記述のいずれかを使用して、CMTS の登録要求において 1 つ以上の RCP エンコーディングを CMTS に通知します。

ケーブル モデムのレポート方法は MAC ドメイン内で設定することができ、MDD 経由でケーブル モデムに通知されます。

RCP-ID を定義し、その RCP-ID に対するケーブル モデムの機能を記述し、システムで定義されていないケーブル モデムに関する情報を入力する必要があります。RCP-ID はカード専用または MAC ドメイン専用に意図されていないため、設定後はシステム全体に対して使用できます。パス選択モジュールにより、RCC プロファイルの一部として RCP ID が正しく送信されていることが確認されます。

CableLabs MULPI 仕様は、CMTS によって自動的に作成される標準 RCP を定義します。

受信チャネル設定

ケーブル モデムは、REG-REQ または REG-REQ-MP メッセージ中の 1 つ以上の RCP エンコーディングを使用して、複数チャネルを受信できる能力について報告します。各受信チャネル プロファイルには、ケーブル モデムのダウンストリーム物理層の論理表現が、受信チャネル（RC）および受信モジュール（RM）の観点から記述されます。CMTS は最初に、登録応答で RCC エンコーディングを使用して、ケーブル モデムの受信チャネルおよび受信モジュールを設定します。

この機能は、Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の任意の RCP ID 設定および受信チャネル設定をサポートします。

RCC テンプレート

RCP では、1 つ以上の RCC テンプレートを設定できます。RCC テンプレートにより、RCP により記述される物理層コンポーネント、たとえば特定のダウンストリーム周波数に対する受信モジュール、受信チャネルなどが設定されます。また、このテンプレートでは、受信モジュール間、または受信モジュールと受信チャネル間の相互接続を指定します。RCC テンプレートはケーブル インターフェイス（MAC ドメイン）にのみ関連付けることができます。

RCC テンプレートが設定されると、ケーブル モデムの RCP ID は RCC と一致します。RCC テンプレートが設定されると、ケーブル モデムの RCP ID は RCC テンプレートによって作成された RCC と一致する場合があります。パス選択モジュールにより、RCC プロファイルの一部として送信された RCP ID が正しいことが確認されます。

登録時、CableLabs MULPI 仕様に示された一連のチェックの実行後に CM に割り当てることが可能な有効 RCC が複数ある場合、最も多くのチャネルを含む RCC が選択されるチャネルとなります。同じサイズの有効 RCC が複数ある場合、ケーブル モデムの量が最も少ない RCC が選択されます。

Channel Assignment

CMTS は、ケーブル モデムの登録中に、Multiple Receive Channel（MRC）モードで動作する DOCSIS 3.0 認定ケーブル モデムに対して受信チャネル構成エンコーディングを割り当てます。

この機能の実装により、DOCSIS 3.0 認定ケーブル モデムは、登録要求メッセージで受信チャネル プロファイルのタイプ、長さ、値（TLV）リストを使用してその受信能力および特性をレポートします。このレポートに基づいて、CMTS はレポートされた RCP と互換性のある RCC エンコーディングを割り当てます。

MRC モードで動作するケーブル モデムは、RCP に関連付けられた RCC エンコーディングが割り当てられます。RCC エンコーディングは RCC テンプレートまたはワイドバンド ケーブル インターフェイス構成から取得できます。

RCC エンコーディングは、ワイドバンド インターフェイス構成からも取得できます。

ダウンストリーム トラフィックの転送

DOCSIS 3.0 では、ダウンストリーム（DS）チャネルまたはボンディング グループに MRC モードで動作するケーブル モデムのダウンストリーム サービス フローを割り当てるという概念が導入されました。サービス フロー（SF）に割り当てられる転送インターフェイスは、DS チャネル インターフェイス（内蔵ケーブル インターフェイス）またはダウンストリーム ボンディング グループ（ワイドバンド インターフェイス）です。

（注） SF 割り当てに使用できる有効なインターフェイスは、ケーブル モデムに割り当てられた RCC エンコーディングのサブセットである必要があります。

ダウンストリーム拡張ヘッダーのサービス フロー プライオリティ

この機能の目的は、DOCSIS の拡張ヘッダーにダウンストリーム パケットのトラフィック プライオリティを反映できるようにすることです。プライオリティは、パケットがマッピングされたサービス フローから取得されます。プライオリティとは、CM コンフィギュレーション ファイル、または Cisco CMTS サービス クラス構成で指定されているサービス フロー プライオリティを意味します。

サービス フロー プライオリティはケーブル モデムのコンフィギュレーション ファイル、または動的設定を使用して設定できます。

Cisco cBR-8 ルータでは、この機能はデフォルトで無効になっています。ユーザは **cable service flow priority** コマンドを使用してこの機能を有効にすることができます。

RCP および RCC エンコーディングの設定方法

以下に示す作業により、受信チャネル プロファイルおよび受信チャネル構成エンコーディングの設定方法について説明します。

RCP ID の設定

CMTS で定義されていないケーブル モデムの機能で RCP ID を設定する必要があります。これは、CMTS ですでに作成した標準規格 MULPI RCP ID を補足するために行われます。

はじめる前に

制限事項

RCC テンプレートおよび RCP インタラクションに適用される設定は次のとおりです。

- RCC テンプレートは、システムですでに定義された RCP に対してのみ作成できます。デフォルトでは、システムには MULPI 仕様で規定された RCP が含まれます。
- 特定の RCP の RCC テンプレートを定義すると、RCC テンプレートで設定された情報が対応する RCP 情報に違反していないことを確認するために、エラー チェックが実行されます。たとえば、RCP 情報で受信モジュールは 2 つと規定されている場合は、RCC テンプレート設定で 3 つ以上のモジュールを設定することはできなくなります。
- RCP が RCC テンプレートに含まれると、RCP を修正できなくなります。修正できるのは、RCC テンプレートで使用されていない RCP のみです。
- rcc-template に適用できる有効な RCP には、次の項目を設定する必要があります。
  - center-frequency-spacing
  - 最小および最大の中心周波数の範囲を定義する 1 つ以上のモジュール。
  - 継承のルール。
  - center-frequency-spacing など、関連するユーザ定義 RCP からの rcc-template 継承の定義。
  - rcc-template チャネル周波数は、対応する RCP モジュールごとに最小および最大の中心周波数の範囲内に収まる必要があります。
  - common-module 定義は、同じインデックスで参照される rcc-template モジュールに適用されます。
  - rcc-template モジュール チャネル周波数は、対応する common-module の同じチャネルを上書きします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 rcp-id** *rcp-id*
	
	例：
	`Router(config)#cable rcp-id 00 10 00 01 08`
	`Router(config-rcp)#`
		RCC テンプレートを定義します。
		• *rcp-id*：RCP ID を 16 進数で指定します。
		このコマンドは、入力モードを RCC コンフィギュレーション モードに変更します。

ステップ 4	**name** *word* 例： `Router(config-rcp)# name rcp-id_1`	**name**：RCP ID に名前を割り当てます。 • *word*：RCP ID の名前に文字列を使用します。 （注） 名前に含まれる単語の間にスペースを含めないでください
ステップ 5	**center-frequency-spacing** *frequency* 例： `Router(config-rcp)#center-frequency-spacing 6`	RCP ID に中心周波数の空間を割り当てます。有効な値は 6 と 8 です。
ステップ 6	**module** *module index* **minimum-center-frequency** *Hz* **maximum-center-frequency** *Hz* 例： `Router(config-rcp)# module 1 minimum-center-frequency 120000000 maximum-center-frequency 800000000`	選択した RCP の受信モジュール設定を設定します。 • *module index*：受信モジュールのモジュール番号を指定します。有効な範囲は 1 ～ 12 です。 • **minimum-center-frequency** ：受信モジュール チャネルの最小中心周波数を指定します。

	コマンドまたはアクション	目的
		• *Hz*：中心周波数を Hz で指定します。有効な範囲は 111000000 ～ 999000000 です。 • **maximum-center-frequency** ：受信モジュールチャネルの最大中心周波数を指定します。
ステップ 7	**module** *module index***number-of-adjacent-channels** *Integrer* 例： `Router(config-rcp)#module 2 number-of-adjacent-channels 10 Router(config-rcp)#`	受信モジュールの周波数帯域を指定します。有効な値は 1 ～ 255 です。
ステップ 8	**module** *module index***connected-module** *module index* 例： `Router(config-rcp)# module 1 connected-module 0`	選択した RCP の受信チャネル設定を指定します。 • **connected-receive-module**：（任意）RCC テンプレートでネストした受信モジュールを指定します。通常、1 つの RCC テンプレートに設定できる受信モジュールは 1 つのみです。 • *module index*：受信モジュールのモジュール番号を指定します。有効な範囲は 1 ～ 12 です。
ステップ 9	**number-of-channels** チャネルの番号 例： `Router (config-rcp)#number-of-channels 8`	RCP ID で受信チャネルの番号を指定します。
ステップ 10	**primary-capable-channels** チャネルの番号 例： `Router(config-rcp)# primary-capable-channels 1`	プライマリ対応チャネルで定義される受信モジュールの数を指定します。

次の作業

show cable rcps コマンドを使用して、RCP ID の設定を確認します。

```
Router# show cable rcps
RCP ID  : 00 10 00 01 08
  Name  : rcp-id 1
  Center Frequency Spacing      : 6
  Max number of Channels        : 8
  Primary Capable Channel       : 1
  Number of Modules             : 2
   Module[1]:
     Number of Adjacent Channels: 10
     Minimum Center Frequency-Hz: 111000000
     Maximum Center Frequency-Hz: 999000000
   Module[2]:
     Number of Adjacent Channels: 10
     Minimum Center Frequency-Hz: 120000000
     Maximum Center Frequency-Hz: 800000000

RCP ID  : 00 10 00 00 02
  Name  : rcp-id 2
  Center Frequency Spacing      : 6
  Max number of Channels        : 2
  Primary Capable Channel       : 1
  Number of Modules             : 1
   Module[1]:
     Number of Adjacent Channels: 10
Minimum Center Frequency-Hz: 111000000
     Maximum Center Frequency-Hz: 867000000
     Connected Module           : 64
```

RCC テンプレートの設定

特定の CMTS に固有の RCP ID を使用して RCC テンプレートを設定する必要があります。有効な RCC テンプレートは、設定済みの RCP ID、RM、RC で構成されます。RCP 設定に含まれる情報は RCC テンプレートにも含まれるため、RCC テンプレートと RCP の間には依存関係があります。

各 RCC エンコーディングには、RCC テンプレートで指定された周波数一致 RC 属性など、チャネル パラメータで動作可能な DS チャネルが含まれています。RCC テンプレートでは、利用可能な DS スペクトル内の任意の受信チャネルの割り当てを指定します。

（注） 設定を介して MAC ドメインから RCC テンプレートを削除した場合、CMTS は RCC テンプレートから派生した RCC エンコーディングをすべて削除します。それらの RCC エンコーディングに割り当てられたすべてのケーブル モデムには、オフラインのマークが付けられます。

はじめる前に

プライマリ受信チャネル（RC）として少なくとも 1 つの RC を設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 rcc-templates frequency-based** *id*
	
	例：
	`Router(config)#cable rcc-templates frequency-based 1`
	`Router(config-rcc-freq-based)#`
		id：RCCテンプレートを指定します。有効な範囲は 1 ～ 64 です。

ステップ 4	**rcp-id** *id* 例： `Router(config-rcc-freq-based)#rcp-id 00 10 00 01 08`	*id*：RCC テンプレートの RCP ID を指定します。有効な範囲は 00 00 00 00 00 ～ FF FF FF FF です。デフォルトで、RCP ID は 00 00 00 00 00 に設定されます。

ステップ 5	**common-module** *module-index* **channel** *grouplist* **start-frequency** *Hz*
	
	例：
	`Router(config-rcc-freq-based)#`
	`common-module 1 channels 0-6 start-frequency 555000000`
		選択した RCP ID に割り当てられたチャネルの選択セットに共通するモジュール設定を指定します。
		• *Module-index*：受信モジュールのインデックス値を指定します。有効な範囲は 1 ～ 12 です。
		• **channels**：共通設定を適用するチャネルのリストを指定します。
		• *grouplist*：特定の設定リストを適用するチャネルのリストを指定します。値の範囲は 1 ～ 64 です。
		• **start-frequency**：開始周波数値（Hz）を指定します。
		• *Hz*：共通モジュールの開始周波数に周波数値を指定します。有効な範囲は 111000000 ～ 999000000 です。

	コマンドまたはアクション	目的
ステップ 6	**rcc-template** *Id* 例： `Router(config-rcc-freq-based)# rcc-template 1`	選択した RCC テンプレートを設定するための RCC テンプレート ID を指定します。 • *Id*：RCC テンプレートの ID を指定します。有効な範囲は 1 ～ 8 です。
ステップ 7	**cm-attribute-mask** *value* 例： `Router (config-rcc-freq-based-tmplt)# cm-attribute-mask 1`	（任意）CM のコンフィギュレーション ファイルで定義された CM 属性マスクとの照合に使用できるように、これを設定します。 • *value*：有効な範囲は 00 00 00 00 00 ～ FF FF FF FF です。
ステップ 8	**module***module-index***channel** *grouplist***start-frequency** *Hz*. 例： `Router(config-rcc-freq-based)# common-module 1 channels 0-6 start-frequency 555000000`	選択した RCP ID に割り当てられたチャネルの選択セットに共通するモジュール設定を指定します。 • *Module-index*：受信モジュールのインデックス値を指定します。有効な範囲は 1 ～ 12 です。 • **channels**：共通設定を適用するチャネルのリストを指定します。 • *grouplist*：特定の設定リストを適用するチャネルのリストを指定します。値の範囲は 1 ～ 64 です。 • **start-frequency**：開始周波数値（Hz）を指定します。 • *Hz*：共通モジュールの開始周波数に周波数値を指定します。有効な範囲は 111000000 ～ 999000000 です。 他の周波数ベースの RCC テンプレートを設定するには、ステップ 3 およびステップ 7 を繰り返します。

次の作業

次に、cable rcc-template の設定例を示します。

```
cable rcc-templates frequency-based 2
  rcp-id 00 10 00 01 08
  common-module 1 channels 1-4 start-frequency 381000000
  rcc-template 1
```

```
  module 1 channels 5-8 start-frequency 501000000
  rcc-template 2
  module 1 channels 5-8 start-frequency 669000000
  rcc-template 3

cable rcc-templates frequency-based 1
  rcp-id 00 10 00 01 08
  rcc-template 1
  cm-attribute-mask 2
  module 1 channels 1-4 start-frequency 381000000
  module 2 channels 5-8 start-frequency 501000000
  rcc-template 2
  module 1 channels 1-4 start-frequency 381000000
  module 2 channels 5-8 start-frequency 669000000
  rcc-template 3
  module 1 channels 1-4 start-frequency 381000000
```

RCCテンプレートの定義後、ケーブルインターフェイスにテンプレートを割り当てる必要があります。

MAC ドメイン（ケーブル インターフェイス）への RCC テンプレートの割り当て

CMTS は、各 MAC ドメイン ダウンストリーム サービス グループ（MD-DS-SG）の RCC テンプレートから RCC を 1 つまたは複数取得します。

次の情報は、RCC をケーブル モデムに割り当てる際に必要です。

- MAC ドメインに割り当てられた RCC テンプレート。
- 周波数と connected-receive-module インデックスを含む DS チャネルの物理パラメータ。
- DS チャネルのプライマリ対応インジケータ。
- MD-DS-SG に対する DS チャネル メンバーシップ。
- MD-DS-SG に対するケーブル モデム メンバーシップ。

ここでは、RCC テンプレートを MAC ドメインに割り当てる方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface cable** *slot*/*subslot*/*port* 例： `Router(config)# interface cable 1/0/0`	MAC ドメイン設定モードを開始します。 • *slot*：インターフェイス ライン カードのシャーシ スロット番号を指定します。

	コマンドまたはアクション	目的
		• *subslot*：インターフェイス ライン カードのセカンダリ スロット番号を指定します。有効なサブスロットは 0 です。 • *MD index*：MAC ドメイン インデックス番号を指定します。有効な値は 0 ～ 15 です。
ステップ 4	**cable rcc-template frequency-based** *Id* 例： `Router(config-if)# cable rcc-template frequency-based 1`	指定したケーブル インターフェイスに RCC テンプレートを割り当てます。 • *Id*：ケーブルインターフェイスに割り当てるテンプレートを指定します。有効な範囲は 1 ～ 64 です。

次の作業

MD にバインドする RCC テンプレートを確認します。

次に、RCC テンプレートのバインド例を示します。 **show cable mac-domain rcc**

```
Router#show cable mac-domain c1/0/0 rcc

RCC-ID   RCP                RCs MD-DS-SG CMs   WB/RCC-TMPL
1        00 00 00 00 00     4   0        2     WB (Wi1/0/0:0)
2        00 00 00 00 00     4   0        2     WB (Wi1/0/0:1)
3        00 00 00 00 00     4   0        0     WB (Wi1/0/1:2)
4        00 00 00 00 00     4   0        0     WB (Wi1/0/2:3)
8        00 10 00 01 08     8   5        0     RCC-TMPL (1:1)
9        00 10 00 01 08     8   5        0     RCC-TMPL (1:2)
10       00 10 00 01 08     4   5        0     RCC-TMPL (1:3)
14       00 10 00 01 08     8   5        0     RCC-TMPL (2:1)
15       00 10 00 01 08     8   5        0     RCC-TMPL (2:2)
16       00 10 00 01 08     4   5        0     RCC-TMPL (2:3)
```

次に、**show cable mac-domain rcc** *id* コマンドを使用した RCC テンプレート バインドの例を示します。

```
Router#show cable mac-domain c1/0/0 rcc 8

RCC ID                  : 8
RCP                     : 00 10 00 01 08
Created Via             : rcc-template - 1:1
CM attribute mask       : 0x2
Receive Channels        : 8
  Receive Channel       : 1
    Center Frequency    : 381000000
    Primary Capability  : YES
    Receive Module Conn : 1
  Receive Channel       : 2
    Center Frequency    : 387000000
    Primary Capability  : NO
    Receive Module Conn : 1
  Receive Channel       : 3
    Center Frequency    : 393000000
```

```
    Primary Capability  : NO
    Receive Module Conn : 1
  Receive Channel       : 4
    Center Frequency    : 399000000
    Primary Capability  : NO
    Receive Module Conn : 1
  Receive Channel       : 5
    Center Frequency    : 501000000
    Primary Capability  : NO
    Receive Module Conn : 2
  Receive Channel       : 6
    Center Frequency    : 507000000
    Primary Capability  : NO
    Receive Module Conn : 2
  Receive Channel       : 7
    Center Frequency    : 513000000
    Primary Capability  : NO
    Receive Module Conn : 2
  Receive Channel       : 8
    Center Frequency    : 519000000
    Primary Capability  : NO
    Receive Module Conn : 2
Receive Modules         : 2
  Receive Module        : 1
    First Frequency     : 381000000
  Receive Module        : 2
    First Frequency     : 501000000
```

```
Router#show cable mac-domain c9/0/2 rcc 9

RCC ID                  : 9
RCP                     : 00 10 00 01 08
Created Via             : rcc-template - 1:2
CM attribute mask       : 0x0
Receive Channels        : 8
  Receive Channel       : 1
    Center Frequency    : 381000000
    Primary Capability  : YES
    Receive Module Conn : 1
  Receive Channel       : 2
    Center Frequency    : 387000000
    Primary Capability  : NO
    Receive Module Conn : 1
  Receive Channel       : 3
    Center Frequency    : 393000000
    Primary Capability  : NO
    Receive Module Conn : 1
  Receive Channel       : 4
    Center Frequency    : 399000000
    Primary Capability  : NO
    Receive Module Conn : 1
  Receive Channel       : 5
    Center Frequency    : 669000000
    Primary Capability  : NO
    Receive Module Conn : 2
  Receive Channel       : 6
    Center Frequency    : 675000000
    Primary Capability  : NO
    Receive Module Conn : 2
  Receive Channel       : 7
    Center Frequency    : 681000000
    Primary Capability  : NO
    Receive Module Conn : 2
  Receive Channel       : 8
    Center Frequency    : 687000000
    Primary Capability  : NO
    Receive Module Conn : 2
Receive Modules         : 2
  Receive Module        : 1
    First Frequency     : 381000000
  Receive Module        : 2
    First Frequency     : 669000000
```

```
Router#show cable mac-domain c1/0/0 rcc 10

RCC ID                  : 10
RCP                     : 00 10 00 01 08
Created Via             : rcc-template - 1:3
CM attribute mask       : 0x0
Receive Channels        : 4
  Receive Channel       : 1
    Center Frequency    : 381000000
    Primary Capability  : YES
    Receive Module Conn : 2
  Receive Channel       : 2
    Center Frequency    : 387000000
    Primary Capability  : NO
    Receive Module Conn : 2
  Receive Channel       : 3
    Center Frequency    : 393000000
    Primary Capability  : NO
    Receive Module Conn : 2
  Receive Channel       : 4
    Center Frequency    : 399000000
    Primary Capability  : NO
    Receive Module Conn : 2
Receive Modules         : 1
  Receive Module        : 2
    First Frequency     : 381000000
```

RCC 設定の確認

ケーブル インターフェイス上のランタイム RCC を確認するには、**showcablemac-domainrcc** コマンドを使用します。

```
Router#show cable mac-domain c1/0/0 rcc

RCC-ID   RCP               RCs MD-DS-SG CMs   WB/RCC-TMPL
1        00 00 00 00 00     4   0        2     WB (Wi1/0/0:0)
2        00 00 00 00 00     4   0        2     WB (Wi1/0/0:1)
3        00 00 00 00 00     4   0        0     WB (Wi1/0/1:2)
4        00 00 00 00 00     4   0        0     WB (Wi1/0/2:3)
8        00 10 00 01 08     8   5        0     RCC-TMPL (1:1)
9        00 10 00 01 08     8   5        0     RCC-TMPL (1:2)
10       00 10 00 01 08     4   5        0     RCC-TMPL (1:3)
14       00 10 00 01 08     8   5        0     RCC-TMPL (2:1)
15       00 10 00 01 08     8   5        0     RCC-TMPL (2:2)
16       00 10 00 01 08     4   5        0     RCC-TMPL (2:3)
```

（注） RCP または MD-DS-SG フィールドのゼロ（0）の値は、RCC エンコーディングが、RCC テンプレートではなく、ワイドバンド インターフェイス設定を介して直接設定されていることを示します。

属性マスクの設定方法

DOCSIS 3.0 は、サービス フローをチャネルに割り当てたり、バイナリ属性に基づいてグループを結び付けたりする際のコンセプトを導入しています。ケーブル、モジュラ、統合型またはワイド

バンドインターフェイスで設定された属性マスクは、プロビジョニングされた属性マスクと呼ばれます。

属性には次の 2 つのタイプがあります。

- 仕様定義された属性：チャネルまたはボンディング グループの特性に基づいたデフォルト値が含まれます。
- オペレータ定義された属性：デフォルトはゼロです。

オペレータは、各チャネルにプロビジョニングされた属性マスクとプロビジョニングされたボンディング グループを設定し、オペレータ定義されたバイナリ属性に値を割り当てることができます。また、仕様定義された属性のデフォルト値を上書きする新しい値を割り当てることもできます。

オペレータは、ケーブル モデムのコンフィギュレーション ファイル内のサービス フローの必須属性マスクと禁止属性マスクを設定できます。この必須属性マスクと禁止属性マスクは、DOCSIS 3.0 サービス フローにオプションで提供されており、インターフェイスでプロビジョニングされた属性マスクと一致します。

各サービス フローは、次の TLV パラメータを使用してオプション設定されます。

- サービス フローの必須属性マスク：これを設定するには、サービス フローの必須属性マスクの 1 ビットに対応するプロビジョニングされた属性マスクのすべての位置に 1 ビットを指定したチャネルにサービス フローを割り当てます。
- サービス フローの禁止属性マスク：これを設定するには、サービス フローの禁止属性マスクの 0 ビットに対応するプロビジョニングされた属性マスクのすべての位置に 1 ビットを指定したチャネルにサービス フローを割り当てます。

また、ケーブル モデムで開始されるダイナミック サービス要求で、ケーブル モデムには、サービス フローの必須属性マスクおよび禁止属性マスクを含めることができます。ケーブル モデム コンフィギュレーション ファイルに必須属性がすべて設定され、禁止属性が何も設定されないように、CMTS はサービス フローをチャネルまたはボンディング グループに割り当てます。

以下の表に、チャネルおよびボンディング グループでサポートされるバイナリ属性を示します。

表 *32*：バイナリ属性

ビット位置	定義
ビット 0	結合：このビットは、すべてのチャネル インターフェイスで 0 に、すべてのボンディング グループで 1 に設定します。
ビット 1	低遅延：このビットは、インターフェイスが比較的低遅延サービスを提供する場合に設定されます。このビットは、すべてのチャネルで 0 に設定されていますが、オペレータが定義できるようになっています。

ビット位置	定義
ビット 2	高可用性：このビットは、すべてのチャネルで 0 に設定されていますが、オペレータが定義できるようになっています。
ビット 3 ～ 15	予約済み：0 に設定されています。
ビット 16 ～ 31	オペレータによる定義：デフォルトでは 0 に設定されています。

ケーブル、内蔵ケーブル、ワイドバンドケーブル、およびモジュラ ケーブルのインターフェイスにプロビジョニングされる属性マスクを設定できます。

前提条件

- ワイドバンド ケーブル モデムのサービス フローにインターフェイスを割り当てるために、このインターフェイスはケーブル モデムの RCC に含める必要があります。
- 内蔵ケーブル（IC）チャネルにサービス フローを割り当てるために、対応する内蔵ケーブル インターフェイスを設定し、動作可能にしておく必要があります。

制限事項

- ナローバンド ケーブル モデムのサービス フローは、ケーブル モデムのプライマリ インターフェイスに常に割り当てられます。この場合、属性確認は実行されません。

ここでは、次の内容について説明します。

内蔵ケーブル インターフェイスにプロビジョニングされる属性の設定

内蔵ケーブル インターフェイスにデフォルトでプロビジョニングされる属性はゼロです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**interface integrated-cable** {*slot/port* | *slot/subslot/port*}:*rf-channel* 例： `Router(config)# interface integrated-cable 1/0/0:0`	Cisco CMTS ルータでケーブル インターフェイス ライン カードを指定します。 • *slot*：ケーブルインターフェイスライン カードのシャーシ スロット番号。 • *subslot*：ケーブル インターフェイス ライン カードのサブスロット番号。有効なサブスロットは常に 0 です。 • *port*：ダウンストリーム ポート番号。 • *rf-channel*：範囲 0 ～ 3 の RF チャネル番号。
ステップ 4	**cableattribute-mask** *mask* 例： `Router(config-if)# cable attribute-mask 800000ff`	インターフェイスのマスクを指定します。

ワイドバンド ケーブル インターフェイスにプロビジョニングされる属性の設定

ワイドバンドケーブルインターフェイスにデフォルトでプロビジョニングされる属性は0x80000000で、そのインターフェイスの属性が変更されるたびに、ゼロ ビットがワイドバンド ケーブル インターフェイスに自動的に追加されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権EXECモードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacewideband-cable** {*slot/port* | *slot/subslot/port*}:*wideband-channel* 例： `Router(config)# interface wideband-cable 1/0/1:4`	ワイドバンド ケーブル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**cabledownstreamattribute-mask** *mask* 例： `Router(config-if)# cable downstream attribute-mask 800000ff`	インターフェイスのマスクを指定します。

サービス フローの属性ベースの割り当ての確認

ケーブルインターフェイスでのサービスフローの属性ベースの割り当てを確認するには、次の例のように **showinterfacecableservice-flow** または **showinterfacewideband-cableservice-flow** コマンドを使用します。

```
Router# show interface cable 3/0 service-flow

Sfid  Sid   Mac Address     QoS  Param Index Type  Dir  Curr  Active  DS-ForwIf/
                            Prov Adm   Act              State Time    US-BG/CH
17    4     001c.ea37.9aac  3    3     3     P     US   act   13h21m  CH 3
18    N/A   001c.ea37.9aac  4    4     4     P     DS   act   13h21m  Wi3/0:0
21    6     001c.ea37.9b5a  3    3     3     P     US   act   13h21m  CH 4
22    N/A   001c.ea37.9b5a  4    4     4     P     DS   act   13h21m  Wi3/0:0
23    7     0016.925e.654c  3    3     3     P     US   act   13h21m  CH 3
24    N/A   0016.925e.654c  4    4     4     P     DS   act   13h21m  In3/0:0

Router# show interface wideband-cable 5/1:0 service-flow
Sfid  Sid   Mac Address     QoS Param Index Type  Dir Curr   Active  DS-ForwIf/
                            Prov  Adm  Act            State  Time    US-BG/CH
3     8193  ffff.ffff.ffff   3     3    3   S(s)  DS  act    2h06m   Wi5/1:0
```

以下の表には、このコマンドで表示されるフィールドの説明を示します。

表 *33*：*show interface cable service-flow* フィールドの説明

フィールド	説明
Sfid	サービス フロー ID 番号を示します。 （注） プライマリ サービス フロー ID はモデムの再登録に必要になるため、オフライン ケーブル モデムでも表示されます。
Sid	サービス ID 番号（アップストリーム サービス フローのみ）を示します。
Mac Address	ケーブル モデムの MAC アドレスを示します。
QoS Parameter Index Prov	このフローのプロビジョニングされた状態の QoS パラメータ インデックスを示します。

フィールド	説明
QoS Parameter Index Adm	このフローの許可された状態のQoSパラメータインデックスを示します。
QoS Parameter Index Act	このフローのアクティブな状態のQoSパラメータ インデックスを示します。
Type	サービス フローがプライマリ フローまたはセカンダリ サービス フローのどちらであるかを示します。セカンダリ サービス フローは、「S」（DOCSIS コンフィギュレーション ファイルを使用して、登録時に静的に作成）または「D」（ケーブル モデムと CMTS 間のダイナミック サービス メッセージの交換で動的に作成）で示されます。
Dir	このサービス フローが DS または US のどちらかであることを示します。
Curr State	サービスフローの現在のランタイムの状態を示します。
Active Time	このサービスフローがアクティブな時間を示します。
DS-ForwIf/US-BG/CH BG/DS	ダウンストリーム サービス フローに割り当てられた転送インターフェイスのボンディング グループIDまたはダウンストリームRFIDを示します。

ダウンストリーム拡張ヘッダーのサービス フロー プライオリティを有効にする方法

次に示すタスクにより、ダウンストリーム拡張ヘッダーのサービスフロープライオリティを有効にする方法について説明します。

ダウンストリーム拡張ヘッダーのサービス フロー プライオリティの有効化

ここでは、Cisco cBR-8ルータでダウンストリーム拡張ヘッダーのサービスフロープライオリティをイネーブルにする方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cableserviceflowpriority** 例： `Router(config)# cable service flow priority`	ダウンストリーム拡張ヘッダーのサービスフロープライオリティをイネーブルにします。

ダウンストリーム拡張ヘッダーにおけるサービスフロープライオリティの有効化の確認

ダウンストリーム拡張ヘッダー内でサービスフロープライオリティが有効にされていることを確認するには、次の例に示すように **showrunning-config|inserviceflow** または **showcablemodem** [*ip-address* | *mac-address*] **verbose** コマンドを使用します。

```
Router# show running-config | in service flow
cable service flow priority

Router# show cable modem 100.1.2.110 verbose

MAC Address                          : 0025.2e2d.74f8
IP Address                           : 100.1.2.110
IPv6 Address                         : 2001:420:3800:909:7964:98F3:7760:ED2
Dual IP                              : Y
Prim Sid                             : 1
Host Interface                       : C3/0/0/U0
MD-DS-SG / MD-US-SG                  : N/A / N/A
MD-CM-SG                             : 0x900000
Primary Downstream                   : In3/0/0:32 (RfId : 12320, SC-QAM)
Wideband Capable                     : Y
DS Tuner Capability                  : 8
RCP Index                            : 6
RCP ID                               : 00 00 00 00 00
Downstream Channel DCID RF Channel   : 191   3/0/0:32 (SC-QAM)
UDC Enabled                          : N
US Frequency Range Capability        : Standard (5-42 MHz)
Extended Upstream Transmit Power     : 0dB
Multi-Transmit Channel Mode          : N
Upstream Channel                     : US0
Ranging Status                       : sta
Upstream SNR (dB)                    : 39.8
Upstream Data SNR (dB)               : 36.12
Received Power (dBmV)                : -1.00
Timing Offset              (97.6 ns): 1799
```

```
Initial Timing Offset              : 1799
Rng Timing Adj Moving Avg(0.381 ns): 0
Rng Timing Adj Lt Moving Avg       : 0
Rng Timing Adj Minimum             : 0
Rng Timing Adj Maximum             : 0
Pre-EQ Good                        : 0
Pre-EQ Scaled                      : 0
Pre-EQ Impulse                     : 0
Pre-EQ Direct Loads                : 0
Good Codewords rx                  : 8468
Corrected Codewords rx             : 0
Uncorrectable Codewords rx         : 0
Phy Operating Mode                 : atdma
sysDescr                           :
Downstream Power                   : 0.00 dBmV (SNR = ----- dB)
MAC Version                        : DOC3.0
QoS Provisioned Mode               : DOC1.1
Enable DOCSIS2.0 Mode              : Y
Service Flow Priority              : N
Modem Status                       : {Modem= online, Security=disabled}
Capabilities                       : {Frag=Y, Concat=Y, PHS=Y}
Security Capabilities              : {Priv=, EAE=N, Key_len=}
L2VPN Capabilities                 : {L2VPN=N, eSAFE=N}
L2VPN type                         : {CLI=N, DOCSIS=N}
Sid/Said Limit                     : {Max US Sids=16, Max DS Saids=15}
Optional Filtering Support         : {802.1P=N, 802.1Q=N, DUT=N}
Transmit Equalizer Support         : {Taps/Symbol= 1, Num of Taps= 24}
CM Capability Reject               : {15,22,23,24,25,26,27,28,29,35,36,38}
Flaps                              : 3(Oct 8  16:22:23)
Errors                             : 0 CRCs, 0 HCSes
Stn Mtn Failures                   : 0 aborts, 2 exhausted
Total US Flows                     : 1(1 active)
Total DS Flows                     : 1(1 active)
Total US Data                      : 294 packets, 25903 bytes
Total US Throughput                : 143 bits/sec, 0 packets/sec
Total DS Data                      : 91 packets, 10374 bytes
Total DS Throughput                : 0 bits/sec, 0 packets/sec
LB group ID assigned               : 1
LB group ID in config file         : N/A
LB policy ID                       : 0
LB policy ID in config file        : 0
LB priority                        : 0
Tag                                : d30
Required DS Attribute Mask         : 0x0
Forbidden DS Attribute Mask        : 0x0
Required US Attribute Mask         : 0x0
Forbidden US Attribute Mask        : 0x0
Service Type ID                    :
Service Type ID in config file     :
Active Classifiers                 : 0 (Max = NO LIMIT)
CM Upstream Filter Group           : 0
CM Downstream Filter Group         : 0
CPE Upstream Filter Group          : 0
CPE Downstream Filter Group        : 0
DSA/DSX messages                   : permit all
Voice Enabled                      : NO
DS Change Times                    : 0
Boolean Services                   : 0
CM Energy Management Capable       : N
CM Enable Energy Management        : N
CM Enter Energy Management         : NO
Battery Mode                       : N
Battery Mode Status                :
Number of Multicast DSIDs Support  : 16
MDF Capability Mode                : 2
IGMP/MLD Version                   : MLDv2
FCType10 Forwarding Support        : Y
Features Bitmask                   : 0x0
Total Time Online                  : 6h00m   (6h00m    since last counter reset)
CM Initialization Reason           : POWER_ON
```

受信チャネル プロファイルの冗長レポートの有効化

受信チャネルプロファイルは、ケーブルモデムの受信チャネルおよび受信モジュールを表すエンコーディングです。ケーブルモデムは、DOCSIS 3.0 で定義された完全なサブタイプエンコーディングを含む冗長な記述、またはRCP IDのみを含む簡易な記述のいずれかを使用して、CMTSの登録要求において 1 つ以上の RCP エンコーディングを CMTS に通知します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacecable** {*slot/port* | *slot*/*subslot*/*port*} 例： `Router(config)# interface cable7/0/0`	Cisco CMTS ルータでケーブル インターフェイス ライン カードを指定します。 • *slot*：ケーブルインターフェイス ライン カードのシャーシ スロット番号。 • *subslot*：ケーブル インターフェイス ライン カードのサブスロット番号。有効なサブスロットは 0 です。 • *port*：ダウンストリーム ポート番号。
ステップ 4	**cablercp-controlverbose** 例： `Router(config-if)# cable rcp-control verbose`	冗長な記述を含む RCP レポートをイネーブルにします。

RCC テンプレートの設定例

次に、RCP ID の設定例を示します。

```
...
!
cable rcp-id 00 10 00 01 08
  center-frequency-spacing 6
```

```
  module 1 minimum-center-frequency 120000000 maximum-center-frequency 800000000 module 1
number-of-adjacent-channels 10
  module 2 minimum-center-frequency 120000000 maximum-center-frequency 800000000 module 2
 number-of-adjacent-channels 10
  number-of-channels 8
  primary-capable-channels 1
!
```

次に、RCC テンプレートの設定例を示します。

```
...
!
cable rcc-templates frequency-based 1
  rcp-id 00 10 00 01 08
  rcc-template 1
  cm-attribute-mask 2
  module 1 channels 1-4 start-frequency 381000000
  module 2 channels 5-8 start-frequency 501000000
  rcc-template 2
  module 1 channels 1-4 start-frequency 381000000
  module 2 channels 5-8 start-frequency 669000000
  rcc-template 3
  module 1 channels 1-4 start-frequency 381000000
!
```

次に、**common-module** オプションを使用した RCC テンプレートの設定例を示します。

```
...
!
cable rcc-templates frequency-based 2
   rcp-id 00 10 00 01 08
   common-module 1 channels 1-4 start-frequency 381000000
   rcc-template 1
   module 1 channels 5-8 start-frequency 501000000
   rcc-template 2
   module 1 channels 5-8 start-frequency 669000000
   rcc-template 3
!
```

次に、MAC ドメインへの RCC テンプレートの割り当て例を示します。

```
...
!
configure terminal
interface c1/0/0
 cable rcc-templates frequency-based 1
 end

...
```

その他の参考資料

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

DOCSIS 3.0 ダウンストリーム ボンディングに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *34*：ダウンストリーム インターフェイスの設定に関する機能情報

機能名	リリース	機能情報
DOCSIS 3.0 ダウンストリーム ボンディング	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ に統合されました。

機能名	リリース	機能情報
ダウンストリーム拡張ヘッダーのサービス フロー プライオリティ	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ に統合されました。

第 15 章

DOCSIS 2.0 A-TDMA 変調プロファイル

このマニュアルでは、DOCSIS 2.1 Advanced Time Division Multiple Access（A-TDMA）アップストリーム変調プロファイルへのサポートをルータに提供する DOCSIS 2.0 A-TDMA サービスの機能について説明します。この機能は、DOCSIS 1.0 および DOCSIS 1.1 Time Division Multiple Access（TDMA）への既存のサポートを補足します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *35* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

DOCSIS 2.0 A-TDMA 変調プロファイルの前提条件

- ケーブル物理プラントが高帯域 DOCSIS 2.0 A-TDMA 変調プロファイルをサポートできる必要があります。

- ケーブルモデムはDOCSIS準拠であることが必要です。ケーブルモデムがオフラインになった場合、またはオンラインに思われても TDMA/A-TDMA 混在モードでトラフィックを転送しない場合は、モデム ソフトウェアをDOCSISに準拠したバージョンにアップグレードします。
- DOCSIS 2.0 A-TDMA 機能をサポートするための要件は次のとおりです。
  - ケーブル モデムが DOCSIS 2.0 対応である必要があります。
  - DOCSIS 2.0 ケーブル モデムの DOCSIS コンフィギュレーション ファイルの DOCSIS 2.0 Enable フィールド（TLV 39）が除外されているか、TLV 39 が 1（イネーブル）に設定されている必要があります。TLV 39 を 0（ディセーブル）に設定した場合、DOCSIS 2.0 CM は TDMA モードを使用します。
  - アップストリームを A-TDMA-only モードまたは TDMA/A-TDMA 混在モードに設定する必要があります。6.4 MHz チャネル帯域を使用するには、アップストリームを A-TDMA-only モードに設定する必要があります。
- 少なくとも次の作業を行い、ルータの基本設定を完了します。
  - ルータのホスト名とパスワードを設定する。
  - ルータがインターネット プロトコル（IP）動作をサポートするように設定する。
  - 少なくとも 1 つの WAN アダプタを取り付け、バックボーン接続を提供するよう設定する。
- ルータおよびそのすべてのケーブル インターフェイスのチャネル計画を決定します。
- 使用するヘッドエンドサイトにDOCSISおよびインターネット接続のサポートに必要なすべてのサーバ（DHCP、ToD、TFTP サーバを含む）が搭載されていることを確認します。
- ルータのシステム クロックを現在の日付および時刻に設定してシステム ログに正しいタイムスタンプを表示し、BPI+ サブシステムがケーブル モデムのデジタル証明書の確認に正しいタイムスタンプを使用できるようにします。

DOCSIS 2.0 A-TDMA サービスの制約事項

- DOCSIS 2.0 仕様に記載されているとおり、仮想チャネルはサポートしません。
- Synchronous Code Division Multiple Access（S-CDMA）チャネルをサポートしません。
- アップストリームの DOCSIS モードを変更するとそのアップストリームのすべてのケーブル モデムがオフラインになり、ケーブル モデムが再登録され、その結果、新しいチャネルのケーブル モデムの機能が CMTS によって決定されます。

DOCSIS 2.0 A-TDMA サービスに関する情報

DOCSIS 2.0 A-TDMA サービスは、新しい DOCSIS 2.0 仕様によって指定されている多数の拡張 PHY 機能を提供することで、既存の DOCSIS 1.0 および DOCSIS 1.1 ケーブル ネットワークの最大アップストリーム帯域幅を拡大します。

DOCSIS 2.0 A-TDMA サービスは、DOCSIS 2.0 ネットワークに次の利点と改良点を導入します。

- 既存の DOCSIS 1.0 および DOCSIS 1.1 ケーブル モデムとの完全な互換性を提供しているため、既存の DOCSIS ケーブル ネットワークで構築されます（各ケーブル モデムの機能を特定するために、登録応答（REG-RSP）メッセージには DOCSIS のバージョン番号が含まれています）。
- 次のように、3 つの異なるモードに対してアップストリームを設定することで、さまざまなケーブル モデムの混在にも対応することができます。
  - TDMA モードのアップストリームは、DOCSIS 1.0 および DOCSIS 1.1 ケーブル モデムのみをサポートするよう設定できます。
  - A-TDMA モードのアップストリームは、DOCSIS 2.0 ケーブル モデムのみをサポートするよう設定できます。
  - TDMA/A-TDMA 混在モードのアップストリームは、DOCSIS 1.0/DOCSIS 1.1 および DOCSIS 2.0 ケーブル モデムの両方を同じアップストリーム上でサポートするよう設定できます。

（注） A-TDMA または混在型アップストリームが同じ MAC ドメインにある場合、CMTS がケーブル モデムをアップストリーム チャネル変更（UCC）メッセージを使って明示的に他のアップストリームに切り替えない限り、TDMA アップストリームに DOCSIS 2.0 A-TDMA ケーブル モデムは登録されません。DOCSIS 1.0 および DOCSIS 1.1 ケーブル モデムを A-TDMA 専用アップストリームに登録することはできません。

- A-TDMA モードは、A-TDMA の短期データ認可、長期データ認可、非送信請求許可サービス（UGS）認可の Interval Usage Code（IUC）を新しく定義し（IUC 9、10、11）、既存の DOCSIS 1.1 IUC タイプを補完します。
- A-TDMA アップストリームの最大チャネル容量を、6 MHz チャネルあたり 30 Mbps に増やします。
- A-TDMA および混在型の動作モードは、新しい 32-QAM および 64-QAM 変調プロファイルを使用してアップストリームの帯域幅を上げますが、既存の 16-QAM および QPSK 変調プロファイルは引き続きサポートされます。さらに、特定のアプリケーションでは、8-QAM 変調プロファイルがサポートされます。
- A-TDMA 動作で、ミニスロット サイズの 1 ティックをサポートします。

- A-TDMA 動作のチャネル帯域を 6.4 MHz（5.12 Msymbol レート）に上げます。
- A-TDMA および混在型動作モードは、次のようなさまざまな新しい機能により、イングレスノイズや他の信号劣化の保護が強化され、動作環境の安定度が高くなりました。
  - シンボル（T）間隔による適応イコライザ構造を使用し、DOCSIS 1.x モードでは 8 タップだったイコライザ タップ サイズが 24 タップになりました。この結果、より厳しいマルチパスとマイクロリフレクションが存在する場合の動作も可能になり、グループ遅延が問題となり得る帯域端付近での動作に対応できるようになりました。
  - 新しい QPSK0 および QPSK1 プリアンブルをサポートすることで、搬送波とタイミングのロック、電力推定、イコライザ トレーニング、コンステレーション位相ロックを同時に取得してバースト取得を向上させます。これにより、プリアンブルが短くなり、実装ロスが減少します。
  - プログラマブル インターリーブ機能を使って、リード ソロモン ブロックあたりの前方誤り訂正（FEC）T バイト サイズを 16 バイト（T = 16）に増やします。

動作モード

コンフィギュレーションに応じて、DOCSIS 2.0 A-TDMA サービス機能は、DOCSIS または Euro-DOCSIS のいずれかの動作をサポートします。

- DOCSIS ケーブル ネットワークは、ITU J.83 Annex B 物理層規格および Data-over-Cable Service Interface Specifications（DOCSIS、Annex B）規格に基づき、6 MHz の National Television Systems Committee（NTSC）チャネル プランを使用します。このモードでは、ダウンストリームは 85 ～ 860 MHz の周波数範囲で 6 MHz のチャネル幅を使用し、アップストリームは 5 ～ 42 MHz の周波数範囲で複数のチャネル幅をサポートします。
- EuroDOCSIS ケーブル ネットワークは、ITU J.112 Annex A 物理層規格および European DOCSIS（EuroDOCSIS、Annex A）規格に基づき、8 MHz の位相反転線（PAL）および Systeme Electronique Couleur Avec Memoire（SECAM）チャネル プランを使用します。このモードでは、ダウンストリームは 85 ～ 860 MHz の周波数範囲で 8 MHz のチャネル幅を使用し、アップストリームは 5 ～ 65 MHz の周波数範囲で複数のチャネル幅をサポートします。

（注） DOCSIS と EuroDOCSIS の違いは物理層にあります。DOCSIS または EuroDOCSIS ネットワークをサポートするには、DOCSIS 2.0 A-TDMA サービス カードの正しい設定、アップコンバータ、ダイプレックス フィルタ、およびこのネットワーク タイプをサポートする他の機器が必要です。

次の表に、サポートされている DOCSIS 1.1 の最大データ レートを示します。

表 *36*：*DOCSIS 1.1* の最大データ レート

アップストリームチャネル幅	変調方式	ボー レート、Sym/秒	最大 Raw ビット レート、Mb/秒
3.2 MHz	16-QAM QPSK	2.56 M	10.24 5.12
1.6 MHz	16-QAM QPSK	1.28 M	5.12 2.56

次の表に、サポートされている DOCSIS 2.0（A-TDMA モード）の最大データ レートを示します。

表 *37*：*DOCSIS 2.0*（*A-TDMA* モード）の最大データ レート

アップストリームチャネル幅	変調方式	ボー レート、Sym/秒	最大 Raw ビット レート、Mb/秒
6.4 MHz	64-QAM 32-QAM 16-QAM 8-QAM QPSK	5.12 M	30.72 25.60 20.48 15.36 10.24
3.2 MHz	64-QAM 32-QAM 16-QAM 8-QAM QPSK	2.56 M	15.36 12.80 10.24 7.68 5.12
1.6 MHz	64-QAM 32-QAM 16-QAM 8-QAM QPSK	1.28 M	7.68 6.40 5.12 3.84 2.56

変調プロファイル

A-TDMA と TDMA/A-TDMA 混在型変調プロファイルの管理を簡略化するために、DOCSIS 2.0 A-TDMA サービス機能には異なる変調方式に最適化された設定済み変調方式が多数用意されています。これらの設定済みプロファイルの使用を推奨します。

それぞれの動作モードではデフォルトの変調プロファイルも定義されており、アップストリームにプロファイルが割り当てられていないときは自動的に使用されます。デフォルト変調プロファ

イルは削除できません。次の表に、ケーブル インターフェイスおよび変調方式別の有効範囲を示します。

表 *38*：変調プロファイルの許容範囲

ケーブルインターフェイス	DOCSIS 1.X（TDMA）	DOCSIS 1.X/2.0 混合	DOCSIS 2.0（A-TDMA）
Cisco cBR-8 CCAP ライン カード	1～400（デフォルトは 21）	1～400（デフォルトは 121）	1～400（デフォルトは 221）

利点

DOCSIS 2.0 A-TDMA サービス機能では、ケーブル サービス プロバイダーとそのパートナーおよびカスタマーに次の利点があります。

- DOCSIS 1.0 と DOCSIS 1.1 ケーブル モデム（CM）、およびケーブル モデム終端システム（CMTS）と完全な互換性があります。
- アップストリーム パスのスループット容量のデジタル ビットを追加することで、チャネル容量を追加します。
- ケーブル システムで発生する電気劣化に対する保護を向上させることで、より堅牢な動作環境を実現します。

DOCSIS 2.0 A-TDMA サービスの設定方法

この項の構成は、次のとおりです。

変調プロファイルの作成

ここでは、事前設定された変調プロファイル オプションを使用して、DOCSIS のさまざまな動作モードで変調プロファイルを作成する方法について説明します。

TDMA 変調プロファイルの作成

ここでは、設定済み変調プロファイルのいずれかを使用して、DOCSIS 1.0/DOCSIS 1.1 TDMA 動作モードの変調プロファイルを作成する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cablemodulation-profile** *profile* **tdma** {**mix**| **qam-16** | **qpsk** | **robust-mix**}
	
	例：
	`Router(config)# cable modulation-profile 3 tdma mix`
	`Router(config)# cable modulation-profile 4 tdma qpsk`
		バーストパラメータが各バーストタイプのそれぞれのデフォルト値に設定されている、定義済み変調プロファイルを作成します。
		（注） また、個別のバーストパラメータの値を設定することにより、**cablemodulation-profile** コマンドでカスタム変調プロファイルを作成することもできます。ただし、各パラメータの変更が DOCSIS MAC レイヤにどのような影響を与えるかを熟知していない場合は、このパラメータを変更しないでください。ケーブル設備の大部分には、デフォルトの定義済み変調プロファイルを使用することを推奨します。

ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

混合モード変調プロファイルの作成

ここでは、設定済み変調プロファイルのいずれかを使用して、混合 TDMA/A-TDMA 動作モードの変調プロファイルを作成する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cablemodulation-profile** *profile* **mixed** {**mix-high** | **mix-low** | **mix-mid** | **mix-qam** | **qam-16** | **qpsk** | **robust-mix-high**| **robust-mix-mid** | **robust-mix-qam**}
	
	例：
	`Router(config)# cable modulation-profile 143 mixed mix-medium`
	`Router(config)# cable modulation-profile 144 mixed mix-high`
		バーストパラメータが各バーストタイプのそれぞれのデフォルト値に設定されている、定義済み変調プロファイルを作成します。
		（注） **robust-mix** プロファイルは **mix** プロファイルと似ていますが、それよりも堅牢で、アップストリームのノイズをより適切に処理できます。
		（注） また、個別のバーストパラメータの値を設定することにより、**cablemodulation-profile** コマンドでカスタム変調プロファイルを作成することもできます。ただし、各パラメータの変更が DOCSIS MAC レイヤにどのような影響を与えるかを熟知していない場合は、このパラメータを変更しないでください。ケーブル設備の大部分には、デフォルトの定義済み変調プロファイルを使用することを推奨します。

ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

A-TDMA 変調プロファイルの作成

ここでは、設定済み変調プロファイルのいずれかを使用して、DOCSIS 2.0 A-TDMA 動作モードの変調プロファイルを作成する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cablemodulation-profile** *profile* **atdma** {**mix-high** | **mix-low** | **mix-mid** | **mix-qam** | **qam-8** | **qam-16** | **qam-32** | **qam-64** | **qpsk** | **robust-mix-high** | **robust-mix-low** | **robust-mix-mid**}
	
	例：
	`Router(config)# cable modulation-profile 242 atdma qam-32`
	`Router(config)# cable modulation-profile 243 atdma qam-64`
		バースト パラメータが各バースト タイプのそれぞれのデフォルト値に設定されている、定義済み変調プロファイルを作成します。
		（注） **robust-mix** プロファイルは **mix** プロファイルと似ていますが、それよりも堅牢で、アップストリームのノイズをより適切に処理できます。
		（注） また、個別のバーストパラメータの値を設定することにより、**cablemodulation-profile** コマンドでカスタム変調プロファイルを作成することもできます。ただし、各パラメータの変更が DOCSIS MAC レイヤにどのような影響を与えるかを熟知していない場合は、このパラメータを変更しないでください。ケーブル設備の大部分には、デフォルトの定義済み変調プロファイルを使用することを推奨します。

ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

アップストリームの DOCSIS モードとプロファイルの設定

ここでは、DOCSIS 動作モードのアップストリームを設定する方法と、そのアップストリームに特定の変調プロファイルを割り当てる方法について説明します。

（注） デフォルトでは、すべてのアップストリームは、デフォルトの変調プロファイルを使用して ATDMA 専用モードに設定されています。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**controller upstream-Cable** *slot/subslot/port* 例： `Router(config)# controller upstream-Cable 2/0/1`	インターフェイスのコントローラ コンフィギュレーション モードを開始します。
ステップ 4	**us-channel** *n***docsis-mode** {**atdma**| **tdma**| **tdma-atdma**} 例： `Router(config-controller)# us-channel 0 docsis-mode atdma`	任意の DOCSIS 動作モードのアップストリームを設定します。
ステップ 5	**us-channel** *n***modulation-profile** *primary-profile-number* [*secondary-profile-number*] [*tertiary-profile-number*] 例： `Router(config-controller)# us-channel 0 modulation-profile 241`	アップストリーム ポートに最大 3 つの変調プロファイルを割り当てます。 （注） 変調プロファイルのタイプは、**us-channeldocsis-mode** コマンドを使ってアップストリーム用に設定させた DOCSIS モードと一致する必要があります。
ステップ 6	**us-channel** *n***equalization-coefficient** 例： `Router(config-controller)# us-channel 0 equalization-coefficient`	（任意）アップストリーム ポートで DOCSIS 事前均等化係数を使用できるようにします。
ステップ 7	**us-channel** *n***ingress-noise-cancellation** *interval* 例： `Router(config-controller)# us-channel 0 ingress-noise-cancellation 400`	（任意）アップストリームのイングレス ノイズを修正するために、インターフェイス カードがアップストリームの信号をサンプリングする場合の間隔をミリ秒単位で設定します。

	コマンドまたはアクション	目的
ステップ 8	**us-channel** *n* **maintain-psd** 例： `Router(config-controller)# us-channel 0 maintain-psd`	（任意）変調レート変更後、一定のスペクトル密度（PSD）を維持するためにATDMA専用のアップストリーム上で動作するDOCSIS 2.0ケーブル モデムが必要です。 （注） 設定する各アップストリームで、ステップ 3, （323 ページ）～ステップ 8, （324 ページ）を繰り返します。
ステップ 9	**end** 例： `Router(config-controller)# end`	コントローラ コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DOCSIS 2.0 A-TDMA サービスのモニタリング

この項の構成は、次のとおりです。

変調プロファイルの表示

CMTS で現在定義されている変調プロファイルを表示するには、オプションを指定せずに **showcablemodulation-profile** コマンドを使用します。

```
Router# show cable modulation-profile

Mod Docsis  IUC     Type   Pre Diff FEC  FEC  Scrmb  Max Guard Last Scrmb Pre   Pre   RS
    -Mode                  len enco T    k    seed   B   time  CW         offst Type
                                   BYTE BYTE         siz size  short
1   atdma   request 16qam 32  no   0x0  0x10 0x152  0   22    no   yes   0     qpsk1 no
1   atdma   initial 16qam 64  no   0x5  0x22 0x152  0   48    no   yes   0     qpsk1 no
1   atdma   station 16qam 64  no   0x5  0x22 0x152  0   48    no   yes   0     qpsk1 no
1   atdma   a-short 16qam 64  no   0x4  0x4C 0x152  7   22    yes  yes   0     qpsk1 no
1   atdma   a-long  16qam 64  no   0x9  0xE8 0x152  0   22    yes  yes   0     qpsk1 no
1   atdma   a-ugs   16qam 64  no   0x9  0xE8 0x152  0   22    yes  yes   0     qpsk1 no
2   atdma   request 16qam 32  no   0x0  0x10 0x152  0   22    no   yes   0     qpsk1 no
2   atdma   initial 16qam 64  no   0x5  0x22 0x152  0   48    no   yes   0     qpsk1 no
2   atdma   station 16qam 64  no   0x5  0x22 0x152  0   48    no   yes   0     qpsk1 no
2   atdma   a-short 16qam 64  no   0x4  0x4C 0x152  7   22    yes  yes   0     qpsk1 no
2   atdma   a-long  16qam 64  no   0x9  0xE8 0x152  0   22    yes  yes   0     qpsk1 no
2   atdma   a-ugs   16qam 64  no   0x9  0xE8 0x152  0   22    yes  yes   0     qpsk1 no
21  tdma    request qpsk  36  no   0x0  0x10 0x152  0   22    no   yes   0     qpsk  na
21  tdma    initial qpsk  98  no   0x5  0x22 0x152  0   48    no   yes   0     qpsk  na
21  tdma    station qpsk  98  no   0x5  0x22 0x152  0   48    no   yes   0     qpsk  na
21  tdma    short   qpsk  64  no   0x3  0x4C 0x152  12  22    yes  yes   0     qpsk  na
21  tdma    long    qpsk  64  no   0x9  0xE8 0x152  0   22    yes  yes   0     qpsk  na
121 mixed   request qpsk  36  no   0x0  0x10 0x152  0   22    no   yes   0     qpsk  na
121 mixed   initial qpsk  98  no   0x5  0x22 0x152  0   48    no   yes   0     qpsk  na
121 mixed   station qpsk  98  no   0x5  0x22 0x152  0   48    no   yes   0     qpsk  na
121 mixed   short   qpsk  64  no   0x3  0x4C 0x152  12  22    yes  yes   0     qpsk  na
121 mixed   long    qpsk  64  no   0x9  0xE8 0x152  0   22    yes  yes   0     qpsk  na
121 mixed   a-short 64qam 64  no   0x6  0x4C 0x152  6   22    yes  yes   0     qpsk1 no
121 mixed   a-long  64qam 64  no   0x9  0xE8 0x152  0   22    yes  yes   0     qpsk1 no
```

```
121 mixed   a-ugs   64qam 64  no   0x9  0xE8 0x152  0   22    yes  yes   0     qpsk1 no
221 atdma   request qpsk  36  no   0x0  0x10 0x152  0   22    no   yes   0     qpsk0 no
221 atdma   initial qpsk  98  no   0x5  0x22 0x152  0   48    no   yes   0     qpsk0 no
221 atdma   station qpsk  98  no   0x5  0x22 0x152  0   48    no   yes   0     qpsk0 no
221 atdma   a-short 64qam 64  no   0x6  0x4C 0x152  6   22    yes  yes   0     qpsk1 no
221 atdma   a-long  64qam 64  no   0x9  0xE8 0x152  0   22    yes  yes   0     qpsk1 no
```

特定の変調プロファイルの詳細を表示するには、プロファイル番号を指定した **showcablemodulation-profile** コマンドを使用します。

```
Router# show cable modulation-profile 221
```

```
Mod Docsis  IUC     Type  Pre Diff FEC  FEC  Scrmb  Max Guard Last Scrmb Pre   Pre   RS
    -Mode                 len enco T    k    seed   B   time  CW         offst Type
                                  BYTE BYTE        siz size  short
221 atdma   request qpsk  36  no   0x0  0x10 0x152  0   22    no   yes   0     qpsk0 no
221 atdma   initial qpsk  98  no   0x5  0x22 0x152  0   48    no   yes   0     qpsk0 no
221 atdma   station qpsk  98  no   0x5  0x22 0x152  0   48    no   yes   0     qpsk0 no
221 atdma   a-short 64qam 64  no   0x6  0x4C 0x152  6   22    yes  yes   0     qpsk1 no
221 atdma   a-long  64qam 64  no   0x9  0xE8 0x152  0   22    yes  yes   0     qpsk1 no
221 atdma   a-ugs   64qam 64  no   0x9  0xE8 0x152  0   22    yes  yes   0     qpsk1 no
```

ケーブル モデムの機能とプロビジョニングの表示

オンライン ケーブル モデムの機能と、モデムがどのようにプロビジョニングされたかを表示するには、**showcablemodemmac** コマンドを使用します。

```
Router# show cable modem mac
```

```
MAC Address     MAC          Prim  Ver    QoS    Frag Concat PHS Priv DS    US
                State        Sid          Prov                        Saids Sids
1859.334d.7b4c  init(i)      145   DOC1.0 DOC1.0 no   no     no       0     0
1859.334d.fa8c  offline      146   DOC1.0 DOC1.0 no   no     no       0     0
1859.334d.fa02  offline      147   DOC1.0 DOC1.0 no   no     no       0     0
1859.334d.65b0  online(pt)   148   DOC3.0 DOC1.1 yes  yes    yes BPI+ 15    16
1859.334d.6622  offline      149   DOC1.0 DOC1.0 no   no     no       0     0
1859.334d.7a50  init(i)      150   DOC1.0 DOC1.0 no   no     no       0     0
1859.334d.7a2e  offline      151   DOC1.0 DOC1.0 no   no     no       0     0
1859.334d.7d14  online(pt)   152   DOC2.0 DOC1.1 yes  yes    yes BPI+ 15    16
1859.334d.6636  online(pt)   153   DOC2.0 DOC1.1 yes  yes    yes BPI+ 15    16
1859.334d.7cf0  online(pt)   154   DOC2.0 DOC1.1 yes  yes    yes BPI+ 15    16
1859.334d.6742  online(pt)   155   DOC2.0 DOC1.1 yes  yes    yes BPI+ 15    16
1859.334d.7b2a  online(pt)   156   DOC2.0 DOC1.1 yes  yes    yes BPI+ 15    16
1859.334d.7e64  online(pt)   157   DOC2.0 DOC1.1 yes  yes    yes BPI+ 15    16
1859.334d.ede0  online(pt)   158   DOC2.0 DOC1.1 yes  yes    yes BPI+ 15    16
1859.334d.7b8a  online(pt)   159   DOC2.0 DOC1.1 yes  yes    yes BPI+ 15    16
1859.334d.6604  online(pt)   160   DOC2.0 DOC1.1 yes  yes    yes BPI+ 15    16
1859.334d.f93a  online(pt)   161   DOC2.0 DOC1.1 yes  yes    yes BPI+ 15    16
1859.334d.7bf0  online(pt)   162   DOC2.0 DOC1.1 yes  yes    yes BPI+ 15    16
1859.334d.596a  online(pt)   163   DOC2.0 DOC1.1 yes  yes    yes BPI+ 15    16
1859.334d.7d38  online(pt)   164   DOC2.0 DOC1.1 yes  yes    yes BPI+ 15    16
1859.334d.fc64  online(pt)   165   DOC2.0 DOC1.1 yes  yes    yes BPI+ 15    16
1859.334d.6434  online(pt)   166   DOC2.0 DOC1.1 yes  yes    yes BPI+ 15    16
1859.334d.f62a  online(pt)   167   DOC2.0 DOC1.1 yes  yes    yes BPI+ 15    16
!
```

DOCSIS タイプごとに各アップストリームでオンラインになっているケーブル モデムの数を表示するには、**showcablemodemmacsummary** コマンドを使用します。

```
Router# show cable modem mac summary
```

```
                           Cable Modem Summary
                           -------------------
                        Mac Version                        QoS Provision Mode
Interface        Total  DOC3.0  DOC2.0  DOC1.1  DOC1.0  Reg/Online  DOC1.1  DOC1.0
Cable3/0/1/U0    20     0       5       0       15      5           5       0
Cable3/0/1/U1    23     0       9       0       14      9           9       0
Cable3/0/1/U2    21     0       8       0       13      8           8       0
```

```
Cable3/0/1/U4    42      0       9       0       33      9       9       0
Cable3/0/1/U5    20      0       15      0       5       15      15      0
Cable3/0/1/U6    18      1       14      0       3       15      15      0
Cable3/0/2/U0    26      0       26      0       0       26      26      0
Cable3/0/2/U1    28      0       28      0       0       28      28      0
Cable3/0/2/U2    24      0       24      0       0       24      24      0
Cable3/0/2/U4    72      0       72      0       0       72      72      0
Cable3/0/3/U0    67      0       63      0       4       63      63      0
Cable3/0/3/U1    85      1       84      0       0       85      85      0
Cable3/0/3/U2    1       0       1       0       0       1       1       0
Cable3/0/4/U0    12      0       1       0       11      1       1       0
Cable3/0/4/U1    39      0       0       0       39      0       0       0
Cable3/0/4/U2    12      0       1       0       11      1       1       0
Cable3/0/4/U4    65      0       11      0       54      11      11      0
Cable3/0/4/U5    10      0       10      0       0       10      10      0
Cable3/0/4/U6    5       0       5       0       0       5       5       0
Cable3/0/5/U0    27      0       27      0       0       27      27      0
Cable3/0/5/U1    27      0       27      0       0       27      27      0
Cable3/0/5/U2    26      0       26      0       0       26      26      0
Cable3/0/5/U4    77      0       77      0       0       77      77      0
Cable3/0/6/U4    14      14      0       0       0       14      14      0
Cable3/0/6/U5    12      12      0       0       0       12      12      0
Cable3/0/6/U6    5       5       0       0       0       5       5       0
```

DOCSIS 2.0 A-TDMA サービスの設定例

この項の構成は、次のとおりです。

変調プロファイルの作成例

この項の構成は、次のとおりです。

例：DOCSIS 1.0/DOCSIS 1.1 TDMA 変調プロファイル

次に、DOCSIS 1.0/DOCSIS 1.1 TDMA 動作モードの一般的な変調プロファイルの設定例を示します。

- プロファイル 21 は、TDMA 動作のデフォルト プロファイルです。
- プロファイル 24 および 25 は、事前に設定された 16-QAM および QPSK 変調プロファイルを使用します。
- プロファイル 26 は、カスタマイズしたいくつかのバースト パラメータを使用した一般的な QPSK 変調プロファイルです。

```
cable modulation-profile 24 tdma qam-16
cable modulation-profile 25 tdma qpsk
cable modulation-profile 26 tdma request 0 16 0 8 qpsk scrambler 152 no-diff 68 fixed
cable modulation-profile 26 tdma initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed
cable modulation-profile 26 tdma station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed
cable modulation-profile 26 tdma short 4 76 12 8 qpsk scrambler 152 no-diff 80 shortened
cable modulation-profile 26 tdma long 8 236 0 8 qpsk scrambler 152 no-diff 80 shortened
```

例：TDMA/A-TDMA 混合変調プロファイル

次に、DOCSIS 1.X/DOCSIS 2.0 混合 TDMA/A-TDMA 動作モードの一般的な変調プロファイルの設定例を示します。

- プロファイル 121 は、混合モード動作のデフォルト プロファイルです。
- プロファイル 122 から 126 は、事前に設定された混合モード変調プロファイルを使用します。
- プロファイル 127 は、カスタマイズしたいくつかのバースト パラメータを使用した一般的な混合モード変調プロファイルです。

```
cable modulation-profile 121 mixed request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 121 mixed initial 5 34 0 48 qpsk scrambler 152 no-diff 32 fixed
cable modulation-profile 121 mixed station 5 34 0 48 qpsk scrambler 152 no-diff 32 fixed
cable modulation-profile 121 mixed short 5 75 6 8 qpsk scrambler 152 no-diff 72 shortened
cable modulation-profile 121 mixed long 8 220 0 8 qpsk scrambler 152 no-diff 80 shortened
cable modulation-profile 121 mixed a-short 0 16 15 99 64qam scrambler 152 no-diff 128
shortened qpsk0 0 18
cable modulation-profile 121 mixed a-long 0 16 15 200 64qam scrambler 152 no-diff 128
shortened qpsk0 0 18

cable modulation-profile 122 mixed mix-high
cable modulation-profile 123 mixed mix-low
cable modulation-profile 124 mixed mix-medium
cable modulation-profile 125 mixed qam-16
cable modulation-profile 126 mixed qpsk

cable modulation-profile 127 mixed request 0 16 0 8 qpsk scrambler 152 no-diff 68 fixed
cable modulation-profile 127 mixed initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed
cable modulation-profile 127 mixed station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed
cable modulation-profile 127 mixed short 6 76 7 8 16qam scrambler 152 no-diff 160 shortened

cable modulation-profile 127 mixed long 8 231 0 8 16qam scrambler 152 no-diff 160 shortened

cable modulation-profile 127 mixed a-short 9 76 6 8 32qam scrambler 152 no-diff 160 shortened
 qpsk1 1 2048
cable modulation-profile 127 mixed a-long 12 231 0 8 64qam scrambler 152 no-diff 132 shortened
 qpsk1 1 2048
```

例：DOCSIS 2.0 A-TDMA 変調プロファイル

次に、DOCSIS 2.0 A-TDMA 動作モードの一般的な変調プロファイルの設定例を示します。

- プロファイル 221 は、A-TDMA 動作モードのデフォルト プロファイルです。
- プロファイル 222 から 226 は、事前に設定された A-TDMA モード変調プロファイルを使用します。
- プロファイル 227 は、カスタマイズしたいくつかのバースト パラメータを使用した一般的な A-TDMA モード変調プロファイルです。

```
cable modulation-profile 221 atdma request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed
qpsk0 0 18
cable modulation-profile 221 atdma initial 5 34 0 48 qpsk scrambler 152 no-diff 32 fixed
qpsk0 0 18
cable modulation-profile 221 atdma station 5 34 0 48 qpsk scrambler 152 no-diff 32 fixed
qpsk0 0 18
cable modulation-profile 221 atdma short 5 75 6 8 qpsk scrambler 152 no-diff 72 shortened
qpsk0 0 18
```

```
cable modulation-profile 221 atdma long 8 220 0 8 qpsk scrambler 152 no-diff 80 shortened
qpsk0 0 18
cable modulation-profile 221 atdma a-short 5 99 10 8 64qam scrambler 152 no-diff 128 shortened
 qpsk0 0 18
cable modulation-profile 221 atdma a-long 15 200 0 8 64qam scrambler 152 no-diff 128 shortened
 qpsk0 0 18

cable modulation-profile 222 atdma qam-8
cable modulation-profile 223 atdma qam-16
cable modulation-profile 224 atdma qam-32
cable modulation-profile 225 atdma qam-64
cable modulation-profile 226 atdma qpsk

cable modulation-profile 227 atdma request 0 16 0 8 qpsk scrambler 152 no-diff 68 fixed
qpsk0 1 2048
cable modulation-profile 227 atdma initial 0 16 0 0 qpsk no-scrambler no-diff 2 fixed qpsk1
 0 18
cable modulation-profile 227 atdma station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed
qpsk0 1 2048
cable modulation-profile 227 atdma a-short 9 76 6 8 32qam scrambler 152 no-diff 160 shortened
 qpsk1 1 2048
cable modulation-profile 227 atdma a-long 12 231 0 8 64qam scrambler 152 no-diff 132 shortened
 qpsk1 1 2048
cable modulation-profile 227 atdma a-ugs 3 231 0 8 16qam scrambler 152 no-diff 80 shortened
 qpsk1 1 2048
```

アップストリームへの変調プロファイル割り当ての例

この項の構成は、次のとおりです。

例：DOCSIS 1.0/DOCSIS 1.1 TDMA 変調プロファイルの割り当て

次の設定例では、アップストリームに割り当てられたDOCSIS 1.0/DOCSIS 1.1 TDMA変調プロファイルを示します。TDMA変調プロファイル（プロファイル21）は、アップストリームコントローラ 2/0/0 に割り当てられます。

```
controller Upstream-Cable 2/0/0
 us-channel 0 channel-width 1600000 1600000
 us-channel 0 docsis-mode tdma
 us-channel 0 minislot-size 4
 us-channel 0 modulation-profile 21
 no us-channel 0 shutdown
 us-channel 1 channel-width 1600000 1600000
 us-channel 1 docsis-mode tdma
 us-channel 1 minislot-size 4
 us-channel 1 modulation-profile 21
 no us-channel 1 shutdown
 us-channel 2 channel-width 1600000 1600000
 us-channel 2 docsis-mode tdma
 us-channel 2 minislot-size 4
 us-channel 2 modulation-profile 21
 no us-channel 2 shutdown
 us-channel 3 channel-width 1600000 1600000
 us-channel 3 docsis-mode tdma
 us-channel 3 minislot-size 4
 us-channel 3 modulation-profile 21
 no us-channel 3 shutdown
 !
```

例：TDMA/A-TDMA 混合変調プロファイルの割り当て

次の設定例では、アップストリームに割り当てられた混合モード TDMA/A-TDMA 変調プロファイルを示します。混合変調プロファイル（プロファイル 121）は、アップストリーム コントローラ 2/0/15 に割り当てられます。

```
controller Upstream-Cable 2/0/15
 us-channel 0 channel-width 1600000 1600000
 us-channel 0 docsis-mode tdma-atdma
 us-channel 0 minislot-size 4
 us-channel 0 modulation-profile 121
 no us-channel 0 shutdown
 us-channel 1 channel-width 1600000 1600000
 us-channel 1 docsis-mode tdma-atdma
 us-channel 1 minislot-size 4
 us-channel 1 modulation-profile 121
 no us-channel 1 shutdown
 us-channel 2 channel-width 1600000 1600000
 us-channel 2 docsis-mode tdma-atdma
 us-channel 2 minislot-size 4
 us-channel 2 modulation-profile 121
 no us-channel 2 shutdown
 us-channel 3 channel-width 1600000 1600000
 us-channel 3 docsis-mode tdma-atdma
 us-channel 3 minislot-size 4
 us-channel 3 modulation-profile 121
 no us-channel 3 shutdown
!
```

例：DOCSIS 2.0 A-TDMA 変調プロファイルの割り当て

次の設定例では、アップストリームに割り当てられた DOCSIS 2.0 A-TDMA 変調プロファイルを示します。A-TDMA 変調プロファイル（プロファイル 221）は、アップストリーム コントローラ 2/0/10 に割り当てられます。

```
controller Upstream-Cable 2/0/10
 us-channel 0 channel-width 1600000 1600000
 us-channel 0 docsis-mode atdma
 us-channel 0 minislot-size 4
 us-channel 0 modulation-profile 221
 no us-channel 0 shutdown
 us-channel 1 channel-width 1600000 1600000
 us-channel 1 docsis-mode atdma
 us-channel 1 minislot-size 4
 us-channel 1 modulation-profile 221
 no us-channel 1 shutdown
 us-channel 2 channel-width 1600000 1600000
 us-channel 2 docsis-mode atdma
 us-channel 2 minislot-size 4
 us-channel 2 modulation-profile 221
 no us-channel 2 shutdown
 us-channel 3 channel-width 1600000 1600000
 us-channel 3 docsis-mode atdma
 us-channel 3 minislot-size 4
 us-channel 3 modulation-profile 221
 no us-channel 3 shutdown
 us-channel 4 channel-width 1600000 1600000
 us-channel 4 docsis-mode atdma
 us-channel 4 minislot-size 4
 us-channel 4 modulation-profile 221
 us-channel 4 shutdown
 us-channel 5 channel-width 1600000 1600000
 us-channel 5 docsis-mode atdma
 us-channel 5 minislot-size 4
 us-channel 5 modulation-profile 221
 us-channel 5 shutdown
!
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco CMTS コマンド	『*Cisco IOS CMTS Cable Command Reference*』 http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

標準

標準	タイトル
SP-RFIv1.1-I09-020830	『Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1』
SP-RFIv2.0-I03-021218	『Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 2.0』
SP-OSSIv2.0-I03-021218	『Data-over-Cable Service Interface Specifications Operations Support System Interface Specification, version 2.0』
SP-BPI+-I09-020830	『Data-over-Cable Service Interface Specifications Baseline Privacy Plus Interface Specification, version 2.0』
RFC 2233	『DOCSIS OSSI Objects Support』
RFC 2665	『DOCSIS Ethernet MIB Objects Support』
RFC 2669	『Cable Device MIB』

MIB

MIB	MIB のリンク
• DOCS-BPI-PLUS-MIB • DOCS-CABLE-DEVICE-MIB (RFC 2669) • DOCS-CABLE-DEVICE-TRAP-MIB • DOCS-IF-EXT-MIB • DOCS-IF-MIB (RFC 2670) • DOCS-QOS-MIB • DOCS-SUBMGT-MIB • IGMP-STD-MIB (RFC 2933)	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

DOCSIS 2.0 A-TDMA 変調プロファイルに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *39* : ***DOCSIS 2.0 A-TDMA*** 変調プロファイルに関する機能情報

機能名	リリース	機能情報
DOCSIS 2.0 A-TDMA 変調プロファイル	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 16 章

ダウンストリーム復元力ボンディング グループ

ケーブル設備に導入されるワイドバンド（WB）モデムの数が多くなると、WB モデムの復元力が重要な機能になってきます。比較的少数のケーブル モデム（CM）で RF チャネルの障害が検出された場合も、その RF チャネルを使用しているすべてのケーブル モデムが、影響を受けたかどうかに関係なくシャットダウンします。これを避けるため、影響を受けたケーブル モデムと良好な RF チャネルを使用して通信し、他のケーブル モデムには影響を及ぼさないようにする解決法が必要です。

ダウンストリーム復元力ボンディング グループ機能では、障害のある複数の RF チャネルを含むケーブルモデムを、動的に作成されたワイドバンドインターフェイスに割り当てることができ、これにより、ワイドバンド ケーブル モデムのパフォーマンスが大幅に影響を受けることがなくなります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *40* : ***Cisco cBR*** シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE** リリース **16.5.1** 以降のリリース Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE** リリース **16.5.1** 以降のリリース Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

ダウンストリーム復元力ボンディング グループの前提条件

- 予約済み WB インターフェイスのリストから新しい WB インターフェイスが動的に作成されるよう、WB インターフェイスを確保します。
- これらの RF チャネルが復元力ボンディング グループ（RBG）に追加されるよう、RF の帯域幅を解放します。
- WB インターフェイスから既存の RBG 設定をすべて削除します。

ダウンストリーム復元力ボンディング グループの制約事項

- 既存のワイドバンド インターフェイスが復元力ボンディング グループ（RBG）として予約され、その後（**nocableds-resiliency** コマンドにより）RBG が削除されると、この RBG を使用するモデムはオフラインになり、RBG 設定そのものは削除されます。したがって、既存の BG は RBG として設定しないことを強く推奨します。
- この機能は、RF チャネルの障害を確認するケーブル モデムの数が復元力のしきい値よりも少ない場合にのみ有効になります。障害のある RF チャネル上のケーブル モデムの数が復元力のしきい値より多い場合、障害のある RF チャネルはボンディング グループから一時的に削除されます。
- ケーブル モデムは先着順に RBG に割り当てられます。この機能を適切に処理するために、追加の WB インターフェイスと RF チャネルの帯域幅を確保することを推奨します。
- RGB を使用するモデムが存在しない場合、Cisco CMTS は使用されていない RBG の解放を制御します。使用されない RGB の解放にはある程度の時間がかかります。完全に解放されていない RGB をモデムで使用することはできません。設定されている RBG の数に関係なく、すべての古い RBG が完全に解放されていないときに Cisco CMTS が新しいケーブル モデムを RBG に移動しようとすると、ケーブル モデムは RBG ではなくプライマリ DS チャネルに移動されます。
- プライマリ SF に関連付けられた WB インターフェイス上の SF だけが RBG に移動されます。他のインターフェイス上の SF は移動されません。
- 静的 SF は、ベスト エフォートのサービス品質（QoS）で RBG に割り当てられます。
- **resiliency rf-change-trigger** 設定に **secondary** キーワードが設定されていない場合、プライマリ SF のみが RBG または NB インターフェイスに移動します。
- ダウンストリーム復元力ボンディング グループ機能がイネーブルでなく、したがって RBG を使用できない場合、プライマリ WB インターフェイス上の障害のあるケーブル モデムだけが NB インターフェイスに移動されます。
- SF を伝送するマルチキャスト トラフィックは移動されません。

指定されたどの時点にも、障害が起きたすべてのモデムをサポートする十分な予約済みボンディング グループがあるとは限りません。したがって、次の制約事項を考慮する必要があります。

- 各 RBG に少なくとも 2 つの RF チャネルがある。
- RBG の RF 割り当ては常に、親 WB インターフェイスの RF チャネル割り当てのサブセットである。
- ケーブル モデムで RBG を使用できない場合、CM の SF は NB インターフェイスに移動される。
- ケーブル モデムの大部分で RF 障害が発生し、使用可能なボンディング グループ ID が残っていない場合、障害のある RF 自体をボンディング グループから削除することができる。障害のある RF を親ボンディング グループから削除すると、RBG にも反映されます。1 つの

RBG が単一の RF にドロップされると、すべての SF が NB インターフェイスに移動されます。

ダウンストリーム復元力ボンディング グループ機能には、機能を横断する次の制限事項があります。

- RFチャネルに障害が発生すると、認定情報レート（CIR）を必要とするかに関わりなく、すべての動的サービス フロー（典型的には音声フロー）が NB インターフェイスに作成されます。RBG に割り当てられる SF はすべてベスト エフォートであるため、音声コールは音声品質の問題を報告する場合があります。
- 復元力モードに参加するケーブル モデムはロード バランシングに参加しません。
- ダウンストリーム復元力ボンディング グループ機能は、動的帯域幅共有（DBS）モードでのみサポートされます。

ダウンストリーム復元力ボンディング グループの情報

未使用のボンディング グループを RBG として確保できます。各 RF チャネルが使用可能な帯域幅のうち少なくとも 1 %以上に割り当てられていることを確認します。
cablerf-channelbandwidth-percent コマンドを使用して、RF チャネルの帯域幅を設定します。

（注） bandwidth-percent を 100 に設定すると、Cisco CMTS は RF を RBG に追加しません。つまり、この機能は有効になりません。

Cisco CMTS は、未使用の RBG の割り当てと解放を制御します。RF チャネルが WB インターフェイスから削除されると、関連するすべての RBG からも削除されます。

（注） ワイドバンド インターフェイスがスタンバイ モードである場合、Cisco CMTS は未使用のダウンストリーム ボンディング グループを割り当てまたは解放しません。

指定された数のケーブル モデムがチャネル接続の復元を（CM-STATUS 経由で）報告すると、中断状態の RF チャネルがすべての影響を受けるワイドバンド インターフェイスで復元されます。ワイドバンド モデム復元力機能は、「指定された数のケーブル モデム」を rf-change-trigger に設定したカウントまたは割合（またはそれら両方）の半分として定義します。たとえば、カウントが 20 で割合が 10 の場合、中断状態の RF チャネルを復元するには、リカバリを報告するケーブル モデムの数はカウントの場合は 10、割合の場合は 5 に減らします。

ケーブル モデムに最適な RBG の検出

ボンディング グループとは、ボンディングされたチャネルを特定する方法を提供するチャネルのリストです。Cisco CMTS は、サービス フロー（SF）の属性とボンディング グループの個々のチャネルの属性に基づいて、RBG に SF を割り当てます。

ダウンストリーム復元力ボンディング グループ機能では、ラインカードがケーブル モデムから RF チャネル障害があることを知らせる CM-STATUS メッセージを受信すると、ラインカードは正常な RF チャネルの数を確認し、さらに以下を実行します。

- 利用可能な RF チャネルが 1 つしかない場合は、ケーブル モデムをナローバンド モードに移行します。
- すべての RF チャネルが正常な状態であることをケーブル モデムが報告する場合は、ケーブル モデムをワイドバンド モードに移行します。
- 正常な RF チャネルが 2 つ以上あり、障害のある RF チャネルが少なくとも 1 つある場合、ダウンストリーム復元力ボンディング グループ機能が有効になっていれば、ケーブル モデムを RBG に移行します。

ケーブル モデムを RBG に移行するというメッセージを Cisco CMTS がライン カードから受信すると、Cisco CMTS は既存の RBG を検索するか、障害を満たす RBG を作成します。

（注） 2 つ以上の RBG が同じワイドバンド コントローラ用に予約されている場合、Cisco CMTS はケーブル モデムごとに 1 つの RBG を作成します。

（注） ユーザが複数の WB インターフェイスを RBG として確保していて、RF 帯域幅が 100% を超過しない場合、Cisco CMTS は親 WB インターフェイスから複数の RBG を作成します。

一致する RBG が見つからないか作成できない場合、Cisco CMTS は必要な RF チャネルのサブセットで RBG を検索し、可能な場合はケーブル モデムがそのような RBG に割り当てられます。

ただし、このような RBG が存在しない場合、Cisco CMTS はケーブル モデムを NB モードに移行するようにライン カードに指示します。

ダウンストリーム復元力ボンディング グループの設定方法

この項の構成は、次のとおりです。

ダウンストリーム復元力ボンディング グループの有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cablerf-change-trigger**{**percent** *value*|**count** *number*} [**secondary**] 例： `Router(config)# cable rf-change-trigger percent 50 count 1 secondary`	CM報告用のアクションをトリガーまでイベントが持続する時間を指定します。
ステップ 4	**cableresiliencyds-bonding** 例： `Router(config)# cable resiliency ds-bonding`	ダウンストリーム復元力ボンディング グループをイネーブルにします。
ステップ 5	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードに戻ります。

次の作業

（注） **cablerf-change-trigger** コマンドを **cableresiliencyds-bonding** コマンドと併せて使用すると、**cablerf-change-trigger** コマンドだけを使用した場合とは異なる結果になります。詳細については、ダウンストリームの復元力ナローバンド モードと復元力ボンディング グループ，（341 ページ）を参照してください。

ライン カードに対する復元力ボンディング グループの予約

ここでは、コントローラごとのラインカードに対するボンディング グループまたはワイドバンド インターフェイスの予約について説明します。

制約事項

cable ds-resiliency コマンドを使用して復元力ボンディング グループを予約すると、ワイドバンドインターフェイスの既存のバンドルとRFチャネル設定が自動的に削除されます。アドミッション制御などのその他の設定は、手動で削除する必要があります。

ダウンストリームの復元力ボンディング グループを設定したら、他の手動設定は行わないでください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacewideband-cable** *slot/subslot/port:wideband-channel* 例： `Router(config)# interface wideband-cable 1/0/0:7`	ワイドバンド ケーブル インターフェイスを設定します。
ステップ 4	**cableds-resiliency** 例： `Router(config-if)# cable ds-resiliency`	ライン カードまたはコントローラごとの使用に合わせて、個別のボンディング グループまたは WB インターフェイスを予約します。
ステップ 5	**exit** 例： `Router(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。

ダウンストリームの復元力ボンディング グループ設定の確認

この項の構成は、次のとおりです。

ダウンストリームの復元力ボンディング グループの確認

ダウンストリームの復元力ボンディング グループ機能が有効かどうかを確認するには、次の例に示すように **showcablemodemresiliency** コマンドを使用します。

```
Router# show cable modem resiliency
                                Orig BG                 Curr BG
I/F     MAC Address    ID   I/F            RFs ID   I/F            RFs
------- -------------- ---- ---------------- --- ---- ---------------
C7/0/0  0025.2eaf.843e 897  Wi7/0/0:0      4   898  Wi7/0/0:1      3
C7/0/0  0025.2eaf.8356 897  Wi7/0/0:0      4   899  Wi7/0/0:2      3
C7/0/0  0015.d176.5199 897  Wi7/0/0:0      4   720  In7/0/0:0
```

CurrentBGI/F フィールドには、ダウンストリームの復元力ボンディング グループ機能が有効かどうか、およびケーブル モデムが WB インターフェイスに割り当てられているかどうかが示されます。

予約済み復元力ボンディング グループの確認

ライン カードの BG が予約されているかどうか確認するには、次の例に示すように **showcableresiliency** コマンドを使用します。

```
Router# show cable resiliency
                BG   Resil BG                                    RF
Resil BG I/F    ID   State          Count Time              Ctrl  Num
--------------- ---- -------------- ----- ----------------- ----------
Wi1/0/0:10      10   Free
Wi1/0/0:20      20   Free
Wi7/0/0:1       1    Assigned       3     Nov 3  09:55:49 0     0
                                                               1
                                                               2
Wi7/0/0:2       2    Assigned       3     Nov 3  09:57:09 0     0
                                                               1
                                                               3
```

ダウンストリームの復元力ナローバンド モードと復元力ボンディング グループ

ここでは、**cablerf-change-trigger** コマンドを **cableresiliencyds-bonding** コマンドと併せて使用した場合の出力例と、**cablerf-change-trigger** コマンドだけを使用した場合の出力例を記載します。

表 *41*：ダウンストリームの復元力ナローバンド モードと復元力ボンディング グループ - シナリオ *1*

効果	**cable rf-change-trigger** コマンドのみの使用（ダウンストリームの復元力 **NB** モード）		**cable resiliency ds-bonding** での **cable rf-change-trigger** コマンドの使用（ダウンストリームの復元力ボンディング グループ）	
	しきい値未満	しきい値超え	しきい値未満	しきい値超え
プライマリ サービス フロー	プライマリ チャネルに移動します。	元のボンディング グループで維持されます。不良のダウンストリームチャネルは使用されず、DOWN として報告されます。	動的ボンディング グループに移動します。	元のボンディング グループで維持されます。不良のダウンストリームチャネルは使用されず、DOWN として報告されます。
セカンダリ サービス フロー	元の WB インターフェイスで維持されます。	元のボンディング グループで維持されます。不良のダウンストリームチャネルは使用されず、DOWN として報告されます。	元のボンディング グループで維持されます。	元のボンディング グループで維持されます。不良のダウンストリームチャネルは使用されず、DOWN として報告されます。

次の出力例は、ケーブル モデムに対して **cablerf-change-trigger** コマンドと **cableresiliencyds-bonding** コマンドを併せて使用し、RF チャネル障害の観測されているケーブル モデム数が復元力しきい値を下回っている場合です。

```
Router# show cable modem

                                                                                  D
MAC Address    IP Address     I/F            MAC             Prim RxPwr  Timing Num I
                                             State           Sid  (dBmv) Offset CPE P
0023.be83.1c9e 10.1.11.46     C5/0/0/UB      w-online        922  -0.50  1055   0   N
0023.be83.1caa 10.1.11.28     C5/0/0/UB      w-online        923  0.00   1043   0   N
0025.2ecf.f19c 10.1.11.53     C5/0/0/UB      w-online        925  0.00   1057   0   N
0022.3a30.9fc0 10.1.11.47     C5/0/0/UB      w-online        926  0.00   1055   0   N
001a.c3ff.e3d4 10.1.11.39     C5/0/0/UB      p-online        927  0.00   1307   0   N
0023.be83.1c9a 10.1.11.61     C5/0/0/UB      w-online        928  0.00   1057   0   N
0022.3a30.9fbc 10.1.11.60     C5/0/0/UB      p-online        929  -0.50  1055   0   N
0023.be83.1c8c 10.1.11.38     C5/0/0/UB      w-online        930  0.00   1061   0   N
001e.6bfb.1964 10.1.11.63     C5/0/0/UB      p-online        931  0.50   1305   0   N
0025.2ecf.f196 10.1.11.29     C5/0/0/UB      w-online        932  0.00   1057   0   N
0025.2ecf.f04e 10.1.11.54     C5/0/0/UB      w-online        933  0.00   1054   0   N
0022.3a30.9fc8 10.1.11.43     C5/0/0/UB      w-online        934  0.00   1056   0   N
0025.2ecf.f190 10.1.11.55     C5/0/0/UB      w-online        935  0.00   1059   0   N
0022.3a30.9fd0 10.1.11.52     C5/0/0/UB      p-online        936  0.00   1057   0   N
0022.ce97.8268 10.1.11.31     C5/0/0/UB      w-online        937  -0.50  1056   0   N
0022.ce97.8281 10.1.11.25     C5/0/0/UB      w-online        938  0.00   1058   0   N
001a.c3ff.e4ce 10.1.11.44     C5/0/0/UB      w-online        940  -0.50  1304   0   N
0022.ce9c.839e 10.1.11.32     C5/0/0/UB      w-online        941  -0.50  1305   0   N
0022.cea3.e768 10.1.11.41     C5/0/0/UB      w-online        942  -1.00  1305   0   N
0022.ce9c.8398 10.1.11.33     C5/0/0/UB      w-online        943  0.00   1306   0   N
001a.c3ff.e50a 10.1.11.59     C5/0/0/UB      w-online        944  0.00   1304   0   N
001a.c3ff.e3f8 10.1.11.57     C5/0/0/UB      w-online        945  -1.00  1306   0   N
001e.6bfb.1a14 10.1.11.37     C5/0/0/UB      w-online        946  0.00   1305   0   N
```

（注） p-online は、ケーブル モデムに NP RF の障害があり、ダウンストリームの部分サービス モードであることを示しています。

```
Router# show cable resiliency

              BG   Resil BG                                  RF
Resil BG I/F  ID   State          Count Time              Ctrl  Num
------------- ---- -------------- ----- ---------------- ----------
Wi5/0/0:2     2    Assigned       1     Mar 30 14:46:43 0     0
                                                               1
                                                               2
Wi5/0/0:3     3    Assigned       1     Mar 30 14:46:43 0     0
                                                               1
                                                               2
                                                         1     0
                                                               1
                                                               2
                                                               3
Wi5/0/0:4     4    Free           0
Wi5/0/0:5     5    Free           0

Router# show cable modem resiliency
                                  Orig BG                Curr BG
I/F     MAC Address    ID   I/F            RFs ID   I/F            RFs
------- -------------- ---  ---------------------- ----------------------
C5/0/0  001a.c3ff.e3d4 258  Wi5/0/0:1     4   259  Wi5/0/0:2     3 <- Dynamic Bonding Group
C5/0/0  0022.3a30.9fbc 257  Wi5/0/0:0     8   260  Wi5/0/0:3     7 <- Dynamic Bonding Group
C5/0/0  001e.6bfb.1964 258  Wi5/0/0:1     4   259  Wi5/0/0:2     3 <- Dynamic Bonding Group
C5/0/0  0022.3a30.9fd0 257  Wi5/0/0:0     8   260  Wi5/0/0:3     7 <- Dynamic Bonding Group
```

次に、以下の条件下のケーブル モデムの出力例を示します。

- **cablerf-change-trigger** コマンドを **cableresiliencyds-bonding** コマンドと併せて使用
- RF チャネル の障害を確認するケーブル モデムの数が復元力のしきい値より少ない場合
- 復元力のボンディング グループで使用可能な WB インターフェイスがない場合

```
Router# show cable modem
 0025.2ecf.f196 service-flow version

SUMMARY:
MAC Address    IP Address      Host          MAC           Prim  Num Primary    DS
                               Interface     State         Sid   CPE Downstream RfId
0025.2ecf.f196 10.1.11.29      C5/0/0/UB     p-online
      932   0   In5/0/0:0  240
Sfid  Dir Curr  Sid   Sched  Prio MaxSusRate  MaxBrst     MinRsvRate  Throughput
          State       Type
1867  US  act   932   BE     0    0           10000       0           294
1868  DS  act   N/A   N/A    0    0           3044        0           154

Router# show cable resiliency
                BG   Resil BG                                  RF
Resil BG I/F    ID   State          Count Time                 Ctrl  Num
--------------- ---- -------------- ----- -------------------- ----------
Wi5/0/0:2       2    Assigned       6     Mar 30 15:57:09 0      0
                                                                  1
                                                                  2
                                                                  3
                                                             1    0
                                                                  2
                                                                  3
Wi5/0/0:3       3    Assigned       8     Mar 30 15:53:58 0      0
                                                                  1
                                                                  2
                                                             1    1
                                                                  2
                                                                  3
Wi5/0/0:4       4    Assigned       2     Mar 30 15:53:58 0      0
                                                                  1
                                                                  2
                                                                  3
                                                             1    1
                                                                  2
                                                                  3
Wi5/0/0:5       5    Assigned       2     Mar 30 15:58:35 0      0
                                                                  1
                                                                  2
                                                                  3
                                                             1    0
                                                                  1
                                                                  3

Router# show cable modem resiliency

                                Orig BG                Curr BG
I/F     MAC Address    ID   I/F            RFs ID   I/F            RFs
------- -------------- ---- ---------------------- ----------------------
C5/0/0  0025.2ecf.f19c 257  Wi5/0/0:0      8   259  Wi5/0/0:2      7
C5/0/0  0025.2ecf.f196 257  Wi5/0/0:0      8   240  In5/0/0:0      <-- move NB for no available
 WB interface
C5/0/0  0025.2ecf.f04e 257  Wi5/0/0:0      8   262  Wi5/0/0:5      7
C5/0/0  0022.3a30.9fbc 257  Wi5/0/0:0      8   260  Wi5/0/0:3      6
C5/0/0  0022.3a30.9fd0 257  Wi5/0/0:0      8   261  Wi5/0/0:4      7
```

表 *42*：ダウンストリームの復元力ナローバンド モードと復元力ボンディング グループ - シナリオ *2*

効果	**cable rf-change-trigger** セカンダリ コマンドのみの使用 （ダウンストリームの復元力 **NB** モード）		**cable resiliency ds-bonding** での **cable rf-change-trigger** セカンダリ コマンドの使用 （ダウンストリームの復元力ボンディング グループ）	
	しきい値未満	しきい値超え	しきい値未満	しきい値超え
プライマリ サービス フロー	プライマリ チャネルにすべてのサービス フローを移動します。	元のボンディング グループで維持されます。不良のダウンストリームチャネルは使用されず、DOWN として報告されます。	動的ボンディング グループにすべてのサービスフローを移動します。	元のボンディング グループで維持されます。不良のダウンストリームチャネルは使用されず、DOWN として報告されます。
セカンダリ サービス フロー				

次の出力例は、ケーブル モデムに対して **cablerf-change-triggersecondary** コマンドと **cableresiliencyds-bonding** コマンドを併せて使用し、RF チャネル障害の観測されているケーブル モデム数が復元力しきい値を下回っている場合です。

```
Router# show cable modem 0025.2ecf.f196 service-flow

SUMMARY:
MAC Address    IP Address      Host          MAC           Prim  Num Primary    DS
                               Interface     State         Sid   CPE Downstream RfId
0025.2ecf.f196 10.1.11.29      C5/0/0/UB     p-online      955   0   In5/0/0:0  240
Sfid  Dir Curr  Sid   Sched  Prio MaxSusRate  MaxBrst     MinRsvRate  Throughput
          State       Type
1913  US  act   955   BE     0    10000000    10000       0           425
1915  US  act   956   RTPS   7    0           3044        100000      0
1916  US  act   957   BE     0    0           3044        50000       0
1917  US  act   958   BE     4    0           3044        0           0
1914  DS  act   N/A   N/A    0    100000000   20000       0           0       <-- Primary
Service-Flow
1918  DS  act   N/A   N/A    0    0           3044        0           0       <-- Secondary
 Service-Flow
1919  DS  act   N/A   N/A    0    0           3044        0           0       <-- Secondary
 Service-Flow
1920  DS  act   N/A   N/A    4    4500000     3044        0           0       <-- Secondary
 Service-Flow
UPSTREAM SERVICE FLOW DETAIL:
SFID  SID   Requests   Polls      Grants     Delayed    Dropped    Packets
                                             Grants     Grants
1913  955   83         0          83         0          0          92
1915  956   0          0          0          0          0          0
1916  957   0          0          0          0          0          0
1917  958   0          0          0          0          0          0
DOWNSTREAM SERVICE FLOW DETAIL:
SFID  RP_SFID QID    Flg Policer               Scheduler             FrwdIF
                         Xmits      Drops      Xmits      Drops
1914  33210   131555     90         0          6          0          Wi5/0/0:3 <-- Dynamic
 Bonding Group
1918  33211   131556     0          0          0          0          Wi5/0/0:3
1919  33212   131557     0          0          0          0          Wi5/0/0:3
1920  33213   131558     0          0          0          0          Wi5/0/0:3
```

ダウンストリームの復元力ボンディンググループ設定のトラブルシューティング

次のコマンドを使用すると、WBインターフェイスの情報、障害状態のCMの数、復元力ボンディング グループ、それに関連するボンディング グループ、利用可能なRF チャネル、そのチャネルに割り当てられたCMS とサービス フローの数を取得できます。

- **debugcablewbcmtsresiliency**
- **debugcablewbcmtsresiliencyreport**
- **showcableresiliency**
- **showcablemodemresiliency**
- **showcablemodemwidebandrcs-status**
- **showcablemodemservice-flowverbose**
- **show cable resil-rf-status**
- **showcablemodemsummarywb-rfs**

ダウンストリーム復元力ボンディング グループの設定例

次に、ダウンストリーム復元力ボンディング グループ機能の設定例を示します。

```
cable rf-change-trigger count 10 secondary
cable resiliency ds-bonding
!
controller Upstream-Cable 9/0/1
us-channel 0 frequency 13200000
us-channel 0 channel-width 6400000 6400000
us-channel 0 power-level -1
us-channel 0 docsis-mode atdma
us-channel 0 minislot-size 8
us-channel 0 modulation-profile 221
no us-channel 0 shutdown
us-channel 1 frequency 19600000
us-channel 1 channel-width 6400000 6400000
us-channel 1 power-level -1
us-channel 1 docsis-mode atdma
us-channel 1 minislot-size 8
us-channel 1 modulation-profile 221
no us-channel 1 shutdown
us-channel 2 frequency 26000000
us-channel 2 channel-width 6400000 6400000
us-channel 2 power-level -1
us-channel 2 docsis-mode atdma
us-channel 2 minislot-size 8
us-channel 2 modulation-profile 221
no us-channel 2 shutdown
us-channel 3 frequency 32400000
us-channel 3 channel-width 6400000 6400000
us-channel 3 power-level -1
us-channel 3 docsis-mode atdma
us-channel 3 minislot-size 8
us-channel 3 modulation-profile 221
no us-channel 3 shutdown
!
controller Integrated-Cable 9/0/1
```

```
max-carrier 128
base-channel-power 34
rf-chan 0
  type DOCSIS
  frequency 381000000
  rf-output NORMAL
  power-adjust -2
  docsis-channel-id 1
  qam-profile 1
rf-chan 1 3
  type DOCSIS
  frequency 387000000
  rf-output NORMAL
  power-adjust 0
  docsis-channel-id 2
  qam-profile 1
rf-chan 32 35
  type DOCSIS
  frequency 477000000
  rf-output NORMAL
  power-adjust 0
  docsis-channel-id 33
  qam-profile 1
rf-chan 64 67
  type DOCSIS
  frequency 501000000
  rf-output NORMAL
  power-adjust 0
  docsis-channel-id 65
  qam-profile 1
rf-chan 96 99
  type DOCSIS
  frequency 669000000
  rf-output NORMAL
  power-adjust 0
  docsis-channel-id 97
  qam-profile 1
!
interface Cable9/0/1
downstream Integrated-Cable 9/0/1 rf-channel 0-3
downstream Integrated-Cable 9/0/1 rf-channel 32-35
upstream 0 Upstream-Cable 9/0/1 us-channel 0
upstream 1 Upstream-Cable 9/0/1 us-channel 1
upstream 2 Upstream-Cable 9/0/1 us-channel 2
upstream 3 Upstream-Cable 9/0/1 us-channel 3
cable upstream bonding-group 1
  upstream 0
  upstream 1
  upstream 2
  attributes 80000000
cable upstream bonding-group 2
  upstream 0
  upstream 1
  attributes 80000000
cable upstream bonding-group 3
  upstream 1
  upstream 2
  attributes 80000000
cable upstream bonding-group 4
  upstream 0
  upstream 2
  attributes 80000000
cable upstream bonding-group 5
  attributes 80000000
cable bundle 1
no cable mtc-mode
cable privacy accept-self-signed-certificate
end
!
interface Integrated-Cable9/0/1:0
cable bundle 1
cable rf-bandwidth-percent 65
!
```

```
interface Wideband-Cable9/0/1:0
cable bundle 1
cable privacy accept-self-signed-certificate
cable rf-channels channel-list 0-3 bandwidth-percent 20
!
interface Integrated-Cable9/0/1:1
cable bundle 1
cable rf-bandwidth-percent 65
!
interface Wideband-Cable9/0/1:1
cable bundle 1
cable privacy accept-self-signed-certificate
cable rf-channels channel-list 32-35 bandwidth-percent 20
!
!
interface Wideband-Cable9/0/1:60
cable ds-resiliency
!
interface Wideband-Cable9/0/1:61
cable ds-resiliency
!
interface Wideband-Cable9/0/1:62
cable ds-resiliency
!
```

次に、復元力しきい値を下回る障害のあるケーブル モデムを表示するための **show cable modem** コマンドの出力例を示します。

```
Router# show cable modem

MAC Address    IP Address      I/F           MAC           Prim  RxPwr  Timing Num I
                                             State         Sid   (dBmv) Offset CPE  P
e448.c70c.96d5 80.17.150.6     C9/0/1/U2     p-online      1     0.00   1784   0    N
e448.c70c.96f3 80.17.150.14    C9/0/1/U1     w-online      2     -1.00  1797   0    N
68ee.9633.0699 80.17.150.31    C9/0/1/U0     w-online      3     -1.00  2088   1    N
e448.c70c.96e7 80.17.150.29    C9/0/1/U3     p-online      4     -0.50  1785   0    N
e448.c70c.982b 80.17.150.18    C9/0/1/U2     w-online      5     0.00   1780   0    N
e448.c70c.9804 80.17.150.13    C9/0/1/U3     w-online      6     -0.50  1788   0    N
e448.c70c.9819 80.17.150.30    C9/0/1/U0     w-online      7     -1.00  1782   0    N
e448.c70c.980d 80.17.150.17    C9/0/1/U0     w-online      8     -1.00  1787   0    N
```

（注） p-online は、ケーブル モデムに NP RF の障害があり、ダウンストリームの部分サービス モードであることを示しています。

次に、RBG 作成時の出力例を示します。

```
Router# show cable resiliency

              BG    Resil BG                                  RF
Resil BG I/F  ID    State          Count Time              Ctrl  Num
------------- ----- -------------- ----- ----------------- ----------
Wi9/0/1:60    28989 Assigned       1     Jan 9  07:35:08 1     0
                                                               1
                                                               2
Wi9/0/1:61    28990 Assigned       1     Jan 9  07:36:54 1     0
                                                               1
                                                               3
Wi9/0/1:62    28991 Free           0
```

次に、ケーブル モデムのサービス フローが RBG に割り当てられたときの出力例を示します。

```
Router# show cable modem resiliency

                              Orig BG                 Curr BG
I/F     MAC Address    ID    I/F           RFs ID    I/F           RFs
------- -------------- ----------------------- ----------------------
C9/0/1  e448.c70c.96d5 28929 Wi9/0/1:0     4   28989 Wi9/0/1:60    3
```

```
C9/0/1  e448.c70c.96e7 28929 Wi9/0/1:0     4   28990 Wi9/0/1:61    3
```

次に、障害のあるケーブル モデムが復元された場合の **show cable modem** コマンドの出力例を示します。

```
Router# show cable modem

MAC Address    IP Address      I/F           MAC           Prim  RxPwr  Timing Num I
                                             State         Sid   (dBmv) Offset CPE P
e448.c70c.96d5 80.17.150.6     C9/0/1/U2     w-online      1     0.00   1784   0   N
e448.c70c.96f3 80.17.150.14    C9/0/1/U1     w-online      2     -1.00  1797   0   N
68ee.9633.0699 80.17.150.31    C9/0/1/U0     w-online      3     -1.00  2088   1   N
e448.c70c.96e7 80.17.150.29    C9/0/1/U3     w-online      4     -0.50  1785   0   N
e448.c70c.982b 80.17.150.18    C9/0/1/U2     w-online      5     0.00   1780   0   N
e448.c70c.9804 80.17.150.13    C9/0/1/U3     w-online      6     -0.50  1788   0   N
e448.c70c.9819 80.17.150.30    C9/0/1/U0     w-online      7     -1.00  1782   0   N
e448.c70c.980d 80.17.150.17    C9/0/1/U0     w-online      8     -1.00  1787   0   N
```

次に、障害のあるケーブル モデムが復元された場合の **show cable resiliency** コマンドの出力例を示します。

```
Router# show cable resiliency

              BG    Resil BG                                  RF
Resil BG I/F  ID    State           Count Time              Ctrl  Num
------------- ----- --------------- ----- ----------------- ----------
Wi9/0/1:60    28989 Free            1     Jan 9  07:35:08
Wi9/0/1:61    28990 Free            1     Jan 9  07:36:54
Wi9/0/1:62    28991 Free            0
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco CMTS コマンド リファレンス	http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ダウンストリーム復元力ボンディング グループに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *43*：ダウンストリーム復元力ボンディング グループに関する機能情報

機能名	リリース	機能情報
ダウンストリーム復元力ボンディング グループ	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 17 章

ダウンストリーム チャネル ID 割り当て

初版：2015年4月17日

DOCSIS ダウンストリーム チャネル ID（DCID）は、MAC ドメイン内のダウンストリーム チャネルを認識するために、8 ビットの識別子で定義されます。すべての CMTS ダウンストリーム チャネルには、その後に設定により変更可能な DCID がデフォルトで割り当てられています。これは、ほとんどの DOCSIS ダウンストリーム パケット ヘッダーで使用され、有効な範囲は 1 ～ 255 です（0 はネットワーク管理用に予約されています）。

（注） MAC ドメイン内のすべてのダウンストリーム チャネルは、MAC ドメイン内で一意の DCID を持つ必要があります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

• ダウンストリーム チャネル ID 割り当てに関する機能情報，359 ページ

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *44*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

Cisco CMTS ルータでのダウンストリーム チャネル ID 割り当てに関する情報

これらは、ダウンストリーム チャネル ID 割り当て機能です。

- デフォルトでは、単一コントローラ内のすべてのチャネルに対して、一意の DCID が提供されます。

（注） 同じ MAC ドメイン内にあるダウンストリーム チャネルの DCID 値は一意である必要があります。MAC ドメインに含まれるチャネルが 1 つのコントローラからのみである場合は、デフォルトの DCID 値で十分です。MAC ドメインに複数のコントローラからのチャネルが含まれる場合は、MAC ドメイン内で DCID の競合が発生することがあります。DCID の競合を解決するには、コントローラ コンフィギュレーション内の競合しているチャネルの DCID 値を変更するか、または自動チャネル ID 割り当て機能を有効にします。

- コントローラ内の各ダウンストリーム チャネルのデフォルト DCID 値は、RF チャネル番号に 1 を足した値と同じです。たとえば、RF チャネル 0 のデフォルト値は 1、RF チャネル 1 の場合は 2 です。

ダウンストリーム チャネル ID の手動割り当て

手動 DCID プロビジョニング機能を使用している場合、システム内のすべてのダウンストリーム チャネルは、（コントローラの QAM id + 1）であるデフォルトの DCID 値を割り当てます。次の表に、ダウンストリーム コントローラごとのデフォルト DCID 範囲を示します。

表 *45*：スロット/サブスロット/コントローラごとのデフォルト ダウンストリーム チャネル *ID*

	0/0	1/0	2/0	3/0	6/0	7/0	8/0	9/0
DS コントローラ 0	1-128	1-128	1-128	1-128	1-128	1-128	1-128	1-128
DS コントローラ 1	1-128	1-128	1-128	1-128	1-128	1-128	1-128	1-128
DS コントローラ 2	1-128	1-128	1-128	1-128	1-128	1-128	1-128	1-128

	0/0	1/0	2/0	3/0	6/0	7/0	8/0	9/0
DS コントローラ 3	1-128	1-128	1-128	1-128	1-128	1-128	1-128	1-128
DS コントローラ 4	1-128	1-128	1-128	1-128	1-128	1-128	1-128	1-128
DS コントローラ 5	1-128	1-128	1-128	1-128	1-128	1-128	1-128	1-128
DS コントローラ 6	1-128	1-128	1-128	1-128	1-128	1-128	1-128	1-128
DS コントローラ 7	1-128	1-128	1-128	1-128	1-128	1-128	1-128	1-128

デフォルト DCID 値はユーザ設定可能な値に置き換えることができます。チャネルごとのダウンストリームコントローラで設定できます。ダウンストリームコントローラ内のチャネルの現在の DCID 値は、**show controller Integrated-Cable rf-chan** コマンド出力の dcid 列で確認できます。デフォルトDCID値を持つチャネルの例を示します。DCID値の設定が変更されると、新しい値が次の出力に表示されます。

```
Router#show controllers integrated-Cable 3/0/0 rf-channel 1-127
Chan State Admin Frequency  Type   Annex Mod  srate Interleaver  dcid  power  output
 1   NPRE   UP   99000000   DOCSIS  B    256   5361  I32-J4       2    37     NORMAL
 2   NPRE   UP   105000000  DOCSIS  B    256   5361  I32-J4       3    37     NORMAL
 3   NPRE   UP   111000000  DOCSIS  B    256   5361  I32-J4       4    37     NORMAL
 4   NPRE   UP   117000000  DOCSIS  B    256   5361  I32-J4       5    37     NORMAL
 5   NPRE   UP   123000000  DOCSIS  B    256   5361  I32-J4       6    37     NORMAL
 6   NPRE   UP   129000000  DOCSIS  B    256   5361  I32-J4       7    37     NORMAL
 7   NPRE   UP   135000000  DOCSIS  B    256   5361  I32-J4       8    37     NORMAL
 8   NPRE   UP   141000000  DOCSIS  B    256   5361  I32-J4       9    37     NORMAL
 9   NPRE   UP   147000000  DOCSIS  B    256   5361  I32-J4       10   37     NORMAL
 10  NPRE   UP   153000000  DOCSIS  B    256   5361  I32-J4       11   37     NORMAL
 11  NPRE   UP   159000000  DOCSIS  B    256   5361  I32-J4       12   37     NORMAL
 12  NPRE   UP   165000000  DOCSIS  B    256   5361  I32-J4       13   37     NORMAL
 13  NPRE   UP   171000000  DOCSIS  B    256   5361  I32-J4       14   37     NORMAL
 14  NPRE   UP   177000000  DOCSIS  B    256   5361  I32-J4       15   37     NORMAL
 15  NPRE   UP   183000000  DOCSIS  B    256   5361  I32-J4       16   37     NORMAL

Router#
```

Cisco CMTS ルータでのダウンストリーム チャネル ID の自動割り当て

自動 DCID 割り当て機能を有効にすることで、すべての DOCSIS 要件を満たすために、ダウンストリーム チャネル ID の固有セットを自動的に割り当てることができます。有効にすると、チャ

ネルがファイバ ノードに追加されて MAC ドメインに関連付けられるときに、ダウンストリーム チャネル DCID が自動的に割り当てられます。したがって、ファイバ ノード設定の使用がこの機能の条件になります。

サービスへの影響

DOCSIS ダウンストリーム チャネル ID を変更すると、ケーブル モデムが再登録されます。ケーブル モデムは、ヘッダで DCID が変更された MAC ドメイン記述子（MDD）およびアップストリーム チャネル記述子（UCD）メッセージを受信します。

- 自動 DCID 割り当てを有効にすると、次のメッセージが表示されます。

```
WARNING: Enabling automatic DCID assignment will cause modems to flap and will apply
to all fiber nodes on this CMTS.
```

- 自動 DCID 割り当てを無効にすると、次のメッセージが表示されます。

```
WARNING: Disabling automatic DCID assignment will no longer enforce channel-id uniqueness
 at fiber nodes. Channel ID changes may require manual verification to prevent conflicts.
```

- MAC ドメイン内の別のチャネルと DCID の競合が発生すると、次のエラー メッセージが表示されます。

```
ERROR: <slot>/<subslot>/<controller> rf-channel <channel>: The downstream channel id
conflicts with interface In<slot>/<subslot>/<controller>:channel. Downstream channel
id must be unique in a CGD.
```

- 自動 DCID 割り当てが構成された後、ファイバ ノードに属するダウンストリーム チャネルが MAC ドメインに追加されたときに DCID の競合が発生すると、自動 DCID 機能では別の自動 DCID を割り当てることで競合の解決を試み、次のメッセージが表示されます。

```
WARNING: The downstream channel id conflict for <slot>/<subslot>/<controller> rf-channel
 <channel> was resolved by Automatic DCID Assignment.
Please run "interface <md-slot>/<md-subslot>/<md-index>" followed by
"<slot>/<subslot>/<controller> rf-channel <channel>" again in order to add the channel.
```

  チャネルを追加するには、次のチャネル グループ ドメイン（CGD）コマンドを再度使用します。

  cable downstream *x/y/z* **rf-channel** *channel*

- 自動 DCID が構成されていてもチャネルがファイバ ノードに属していない場合、または自動 DCID が競合を解決できない場合は、次のメッセージが表示されます。

```
WARNING: The downstream channel id conflict for <slot>/<subslot>/<controller> rf-channel
 <channel> could not be resolved by Automatic DCID Assignment.
```

  この問題を解決するには、ファイバ ノードにチャネルを追加します。

Cisco CMTS ルータでのダウンストリーム チャネル ID 割り当ての設定方法

ここでは、ダウンストリーム チャネル ID 割り当ての設定方法について説明します。

ダウンストリーム チャネル ID の手動割り当ての設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface controller integrated-Cable** *slot*/*subslot*/*port* 例： `Router(config)# interface controller integrated-Cable 1/0/1`	チャネル グルーピング ドメインのホスト ライン カードでコントローラ コンフィギュレーション モードを開始します。
ステップ 4	**rf-chan** *downstream QAM ID* • または、ダウンストリーム チャネル ID の範囲を設定するには、**rf-chan** *starting downstream QAM ID ending downstream QAM ID* コマンドを使用します。 例： `Router(config-controller)# rf-chan 0`	RF チャネル コンフィギュレーション モードを開始します。
ステップ 5	**docsis-channel-id** *DCID* 例： `Router(config-rf-chan)#docsis-channel-id 1`	RF チャネルに指定された値にダウンストリーム チャネルの DCID を設定します。 **rf-chan** *starting downstream QAM ID ending downstream QAM ID* コマンドを使って設定された RF チャネル範囲に関して、**docsis-channel-id** *DCID* コマンドはその範囲内の RF チャネルの DCID を設定します。

ダウンストリーム チャネル ID の自動割り当ての設定

自動 DCID 割り当ては完全に設定する必要があります。ただし、この機能を削除する必要がある場合は、**no** または **default** コマンドを使用します。

（注） **no** または **default** 形式のコマンドは startup-config ファイルに書き込まれません。

この場合、DCID はすべてのチャネルで計算済みとして維持されますが、チャネルのデフォルト値には設定されません。**writememory** コマンドを使用して、新しく割り当てた DCID を含む設定を startup-config ファイルに保存します。

自動 DCID 割り当てを有効にすると、MAC ドメインにチャネルを追加する際に発生する DCID の競合が自動的に解決されます。

制約事項

- 設定で **cabledownstream-channel-idautomatic** コマンドを実行した後で、ファイバ ノードに RF チャネルを追加するためにエディタでコンフィギュレーション ファイルを手動で編集すると、DCID の競合が発生することがあります。この機能は、ファイバ ノード内のすべてのチャネルにグローバル コンフィギュレーション モードで固有の自動 DCID が設定されていると仮定しています。設定を手動で編集し、機能で固有の DCID を確認できない場合は、新しく追加されたチャネルの DCID が既存のチャネルの DCID と競合している可能性があります。DCID の競合を解決するには、自動 DCID のグローバル コンフィギュレーションを取り消して、再び適用します。

  （注） 自動 DCID のグローバル コンフィギュレーションの再適用は、破壊的な操作です。

  DCID の競合を回避するには、コンフィギュレーション ファイルを編集してファイバ ノードを設定した後、**cabledownstream-channel-idautomatic** コマンドを実行します。これにより、すべてのチャネルに固有の自動 DCID が設定されます。

  自動 DCID を設定して、Cisco uBR10012 ルータのコマンド ライン インターフェイスのファイバ ノードに追加します。

- startup-config ファイルで **cabledownstream-channel-idautomatic** コマンドを手動で編集しないでください。これは、ファイバ ノード内のチャネルに固有の DCID が保証されないためです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権EXECモードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 downstream-channel-id automatic** 例： `Router(config)# cable downstream-channel-id automatic`	Cisco CMTS で DCID の自動割り当てを指定します。

例

この例では、手動で設定を編集する際の制限を示します。

```
Router# show run | include automatic
cable downstream-channel-id automatic

router# show cable fiber-node 3
------------------------------------------------------------------------------
Fiber-Node 3
Channel(s) : downstream Integrated-Cable 1/0/2: 0-3, 32-35, 64-67, 96-99
Channel ID(s): 1 2 3 4 33 34 35 36 65 66 67 68 97 98 99 100
Upstream-Cable 1/0/2
FN Config Status: Configured (status flags = 0x01)
MDD Status: Valid
Router#
```

1/0/3 などのダウンストリーム コントローラを追加するために、エディタで startup-config ファイルを手動で編集する場合は、競合が発生します。

```
Router> configure terminal
Router# cable fiber-node 3
Router# downstream integrated-Cable 1/0/3
```

このダウンストリーム コントローラが追加されると、自動 DCID 割り当て機能が自動的にこの競合を解決します。ただし、ダウンストリーム コントローラを追加するために、startup-config ファイルが手動で編集されているため、自動 DCID 割り当て機能はこの競合を解決できません。これにより、編集した startup-config ファイルがロードされ、ファイバ ノードを無効にすると、DCID の競合が発生します。

```
down Modular-Cable 5/0/0 rf-channel 0
DS frequency is not unique.
```

```
DS channel id is not unique.
Warning: D3.0 CMs cannot get w-online with an invalid fiber-node.
router#
```

次の作業

ファイバノード内のすべてのチャネルに割り当てられたDCIDを表示するには、**showcablefibernode** コマンドを実行します。

```
Router# show cable fiber-node 3
Fiber-Node 3
Channel(s) : downstream Integrated-Cable 1/0/2: 0-3, 32-35, 64-67,
96-99
Channel ID(s): 1 2 3 4 33 34 35 36 65 66 67 68 97 98
99 100
Upstream-Cable 1/0/2
FN Config Status: Configured (status flags = 0x01)
MDD Status: Valid
```

その他の参考資料

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ダウンストリーム チャネル ID 割り当てに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *46*：ダウンストリーム チャネル *ID* 割り当てに関する機能情報

機能名	リリース	機能情報
ダウンストリーム チャネル ID 割り当て	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 18 章

アップストリーム チャネル ボンディング

アップストリーム チャネル ボンディング（USCB）機能により、ケーブル オペレータは、複数の無線周波数（RF）チャネルを組み合わせて MAC レイヤにより大きいボンディング グループを形成することにより、ケーブル モデム（CM）ユーザ 1 人あたりのアップストリーム（US）帯域幅を上げることができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *47* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

アップストリーム チャネル ボンディングの前提条件

- Cisco ケーブル モデム終端システム（CMTS）ルータのアップストリーム チャネル ボンディング機能を設定する前に、ダウンストリーム チャネル ボンディングをイネーブルにします。

- Cisco CMTS ルータのアップストリーム チャネル ボンディングを設定する前に、CM が Multiple Receive Channel（MRC）モードで登録されていることを確認します。
- CM が DOCSIS 3.0 認定であることを確認します。

アップストリーム チャネル ボンディングの制限事項

アップストリーム チャネル ボンディング機能には、次の制限事項があります。

- 静的ボンディング グループのみサポートされます。
- 同じ MAC ドメインに属するアップストリーム チャネルのみを、アップストリーム ボンディング グループに追加できます。

（注） MAC ドメインごとに最大 16 個のアップストリーム チャネルを設定できます。これらは次の 2 つのグループに分けられます。

- グループ 1：アップストリーム チャネル 0 ～ 7
- グループ 2：アップストリーム チャネル 8 ～ 15

アップストリーム ボンディング グループには、グループ 1 のすべてのアップストリーム チャネルのみ、またはグループ 2 のすべてのアップストリーム チャネルのみが含まれている必要があります。

- 認定情報レート（CIR）オーバーサブスクリプションは USCB グループでサポートされません。

  Cisco CMTS は、個々のアップストリーム チャネルで使用可能な帯域幅のオーバーサブスクリプションを許可します。ただし、帯域幅のオーバーサブスクリプションは USCB グループではサポートされません。

  個々のアップストリームは、音声トラフィック用に生成された静的 CIR サービス フローが原因でオーバーサブスクリプションになる可能性があります。これにより、USCB を含む DOCSIS 3.0 CM が、単一チャネルの US ボンディング グループ（デフォルト ボンディング グループとも呼ばれる）でオンラインになる可能性があります。

  この問題は主に、静的サービス フローを使用した音声展開で発生します。したがって、音声コールを試行する（またはドロップする）場合は、CIR が割り当てられる（または解放される）よう、次の音声展開を選択することを推奨します。

  1. Dynamic Quality of Service（DQoS）Lite
  2. パケット ケーブル（PC）DQoS
  3. パケット ケーブル マルチメディア（PCMM）

  これらの展開は、個々のアップストリームのオーバーサブスクリプションを防ぎ、CM は予測どおりのボンディング グループでオンラインになります。

アップストリーム チャネル ボンディングの情報

DOCSIS 3.0 ベースのアップストリーム チャネル ボンディングは、Cisco CMTS ルータと複数の CM を含むケーブル通信システムでアップストリーム帯域幅を CM ユーザ 1 人あたりの raw スループット 120 Mbps まで拡張するための方法です。アップストリーム チャネル ボンディング方法を使用すると、CM は同時に複数のアップストリーム チャネル上で Cisco CMTS ルータにデータを送信できます。

チャネル ボンディングは、小さな帯域幅アップストリーム チャネルを束ねることで MAC ドメイン内に大きなボンディング グループを作成するための方法です。MAC ドメインは、Cisco CMTS ルータの論理サブコンポーネントであり、一連のダウンストリームおよびアップストリーム チャネルですべての DOCSIS 機能を実装します。

アップストリーム チャネル ボンディング機能は、データおよびビデオ サービスの Multiple Transmit Channel（MTC）モードによるアップストリーム トラフィックをサポートします。これらのサービスは音声ベースのサービスよりも多くの帯域幅が必要になります。音声ベースのサービスは、従来型の単一のアップストリーム チャネル、または単一のアップストリーム チャネル ボンディング グループ設定を使用します。DOCSIS 内の 1 つの RF チャネルの物理容量は 30 Mbps を超えることができないため、30 Mbps を超えるトラフィック コントラクトにはアップストリーム チャネル ボンディングが必要です。

アップストリーム チャネル ボンディング機能は、Cisco cBR-8 ルータでサポートされています。加入者からのアップストリーム データは、ケーブル インターフェイス ライン カード上で自動的に設定されたアップストリーム ポート（US0-US19）を介して送信されます。ケーブル インターフェイス ライン カードは、データを処理して、バックプレーンから WAN カードを通してインターネットに送信します。

ケーブル インターフェイス ライン カードでサポートされるダウンストリームおよびアップストリーム周波数を次の表に示します。

表 *48*：ダウンストリームおよびアップストリーム周波数

ライン カード	ダウンストリーム周波数	アップストリーム周波数
Cisco cBR-8 CCAP	55 ～ 999 MHz[1]	Cisco cBR-8 CCAP ライン カードのアップストリーム周波数範囲は、地域や Annexure 設定に関係なく 5 ～ 85 MHz です。

1 この周波数範囲は、接続された EQAM デバイスの周波数規制の対象になります。

Multiple Transmit Channel モード

Multiple Transmit Channel モードは、CM が複数アップストリーム チャネルにアップストリーム トラフィックを送信することを可能にする CM 機能です。MTC モードは、ケーブル インターフェイス ラインカードでイネーブル化できます。

- MAC ドメイン内のすべての CM の MTC モード：アップストリームのボンディング可能なケーブル インターフェイス ラインカードでは、デフォルトで、MAC ドメイン内のすべての CM で MTC モードがイネーブル化されています。

Multiple Receive Channel モード

MRC モードは、CM が複数ダウンストリーム チャネルのダウンストリーム トラフィックを受信することを可能にする CM 機能です。アップストリーム ボンディングが可能なケーブル インターフェイス ラインカードでは、MRC モードはデフォルトでイネーブル化されています。CM の登録時または登録後に **cable mrc-mode** コマンドを使用して、MAC ドメイン内の MRC モードを有効または無効にすることができます。

アップストリーム チャネル ボンディングの動的範囲ウィンドウと送信電力レベル

動的範囲ウィンドウ機能は、CableLabs DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification および DOCSIS 3.0 Specification に基づいています。DOCSIS 3.0 CM では、アップストリーム送信チャネル電力レベルが送信チャネル セット（TCS）内のすべてのチャネルにおいて 12 dB の範囲内である必要があります。

1 つのアップストリーム チャネルを使用する非 MTC モードで動作する DOCSIS 1.x または 2.0 CM は、2 つ以上のアップストリーム チャネルを使用する MTC モードで動作する DOCSIS 3.0 CM よりも最大送信チャネル電力レベルは高くなります。つまり、MTC モードでは、チャネルごとの最大送信電力レベルが削減されます。

アップストリーム減衰が最大送信電力レベルを超える場合、MTC モードで登録を試行する DOCSIS 3.0 CM はオンラインにならなかったり部分的モードで登録されたりする可能性があります。TCS 内のすべてのアップストリーム チャネルの送信電力レベルが最大送信電力レベルを超えると、CM は登録に失敗します。アップストリーム チャネルのある CM が最大送信電力レベル内にある場合、CM は部分的モードでオンラインになる可能性があります。ただし、最大送信電力レベルを超えるアップストリーム チャネルは、ダウンしているとしてマークされ、アップストリーム トラフィックに使用できません。

CM での送信電力レベルを確認するには、verbose キーワードを指定して show cable modem コマンドを使用します。このコマンドは、割り当てられたアップストリーム チャネルごとに次の送信電力値を表示します。

- 報告送信電力：アップストリーム チャネルごとに CM から報告された送信電力レベルです。
- 最小送信電力：MTC モードの CM がアップストリーム チャネルで送信できる最小送信電力レベルです。
- ピーク送信電力：MTC モードの CM がアップストリーム チャネルで送信できる最大送信電力レベルです。

アップストリーム チャネル ボンディングをサポートするには、最小送信電力が報告送信電力以下であり、報告送信電力がピーク送信電力以下である必要があります。ピーク送信電力レベルと最小送信電力レベルは、CM TCS の割り当ておよび各アップストリーム チャネル設定から取得されます。

最小送信電力が報告送信電力より高い場合、または報告送信電力がピーク送信電力より高い場合、CM はオンラインにならなかったり部分的モードで登録されたりする可能性があります。

この送信電力の問題は、次の 2 つの方法でトラブルシューティングできます。

- 追加の増幅器を挿入してアップストリーム減衰を減らし、アップストリーム送信電力が許容送信電力範囲（12 dB）内に収まるようにします。
- MTC モードを無効にします。CM を MTC モードから非 MTC モードに切り替えるには、CM コンフィギュレーション ファイルを使用してタイプ、長さ、値（TLV）43.9.3 のボンディング ビット（ビット 0）を無効にします。

送信電力の拡張

DOCSIS 3.0 CM の初期導入時に、アップストリーム パスの減衰を補正するために、CM から電力を追加する必要があります。CM は、DOCSIS で定義されているよりも多くの拡張電力レベルを送信する必要があります。USCB が Cisco CMTS でイネーブルで、DOCSIS 3.0 CM が MTC モードで動作しているとき、この状態が一般的に発生します。

アップストリームに電力を追加すると、オペレータに電力の余裕が生まれ、アップストリームの信号損失が減少し、ケーブル設備の運用コストが削減され、DOCSIS 3.0 CM を迅速に導入できるようになります。

Cisco CMTS は、CM が拡張電力でデータを送信する場合に使用する次の機能をサポートします。

- シスコ拡張送信電力機能
- DOCSIS 拡張送信電力機能

シスコ拡張送信電力機能

シスコ拡張送信電力機能は、*DOCSIS 3.0* 仕様で指定された電力レベルよりも高い電力レベルで送信するように、MTC モードで動作する DOCSIS 3.0 CM をサポートします。この機能は、Cisco DPC3000 CM でしかサポートされません。

シスコ拡張送信電力機能により、ケーブル オペレータは、4 チャネルまたは 2 チャネルモード、あるいは MTC 以外のモードで登録され、DOCSIS で定義された最大電力レベルよりも高い電力レベルで送信するケーブル モデムを細かく制御できます。ケーブル オペレータは、グローバル コンフィギュレーション モードで **cabletx-power-headroom** コマンドを使用して拡張送信電力を設定できます。

DOCSIS 拡張送信電力機能

DOCSIS 拡張送信電力機能は、DOCSIS3.0 仕様で定義されているように拡張アップストリーム送信電力機能をサポートします。この機能により、CM は高い拡張電力レベルで送信して、US チャネルの減衰に対応することができます。

次のテーブルに、DOCSIS 拡張送信電力機能でサポートされる新しい TLV を示します。

表 *49* : ***DOCSIS*** 拡張送信電力機能に対応する ***TLV***

TLV 名	タイプ	長さ	値
拡張アップストリーム送信電力サポート	16	1	0：拡張アップストリーム送信電力オフ 1：拡張アップストリーム送信電力オン 2 ～ 255：予約済み
拡張アップストリーム送信電力 CM 機能	5.40	1	0、205 ～ 244（4 分の 1 dB 単位）

Cisco CMTS は TLV16 を送信して、DOCSIS 拡張電力機能が有効かどうかを CM に通知します。その代わりに CM は、Cisco CMTS に TLV5.40 を送信して、その拡張電力機能を通知します。ネゴシエーションの完了後、CM は拡張電力を送信できます。

DOCSIS 拡張送信電力機能はデフォルトで有効です。この機能の有効化と無効化を切り替えるには、cable upstream ext-power コマンドを使用します。DOCSIS 拡張電力機能の有効化と無効化の切り替え方法については、DOCSIS 拡張送信電力機能の設定, （392 ページ）を参照してください。

（注） シスコ拡張送信電力機能と DOCSIS 拡張送信電力機能が設定されている場合は、DOCSIS 拡張送信電力機能が優先されます。

送信チャネル セットの削減

送信チャネル セットの削減機能を使用すると、Cisco CMTS ルータでは、CM の総電力バジェットに基づいて、アップストリーム チャネル セットの割り当てを削減することができます。たとえば、アップストリーム チャネルを 4 から 2 に削減すると、3 dB のヘッドルームが得られます。さらに 2 つのチャネルを単一チャネルに削減すると、3 dB のヘッドルームがさらに得られ、CM は非 MTC モードで動作するようになります。

削減アップストリーム チャネル セットを使用するには、対応する静的ボンディング グループが設定されている必要があります。たとえば、MAC ドメインは 4 つのチャネルを持つボンディング グループで設定されています。チャネルセットが 2 つに削減された CM は、4 チャネルのボンディング グループに対応せず、2 以下のチャネルを含むボンディング グループにのみ対応します。

送信チャネル セットの削減機能は、DOCSIS 3.0 CM で送信電力合計を 3 dB 上げる必要がある場合に便利です。たとえば、DOCSIS 1.0 または 2.0 CM は 4 位相偏移変調（QPSK）で最大 58 dBmV の送信電力をサポートしますが、DOCSIS 3.0 CM は最大 61 dBmV の送信電力をサポートします。この場合、4 チャネル MTC モードで動作する DOCSIS 3.0 CM では、1 アップストリーム チャネルごとの最大送信電力が減ることになります。この機能を使用すると、Cisco CMTS ルータは 6 dB 削減された入力レベルをサポートしてアップストリーム パスの減衰を防ぐことができます。

T4 乗数

T4 乗数は、MTC モードのケーブル モデムについて定義されているデフォルトの T4 タイムアウト値の T4 タイムアウト乗数値です。デフォルト値は、モデムの送信チャネル セットのチャネルの数から取得されます。デフォルトの T4 乗数値は、ケーブル インターフェイス コンフィギュレーション モードで cable upstream ranging-poll コマンドを使用して変更できます。

T4 タイムアウト乗数値の範囲は 1 ～ 10 です。T4 乗数値が 1 の場合、ケーブル モデムは 30 秒で T4 タイムアウトします（1 x 30 = 30）。T4 乗数値を 4 に変更すると、新しい T4 タイムアウト値は 120 秒となります（4 x 30 = 120）。

（注） T4 タイムアウト乗数値の設定が範囲内（1 ～ 10）でない場合、CMTS は T4 タイムアウト値としてモデムの T4 タイムアウト値を使用します。たとえば、モデムの T4 タイムアウトが 90 秒であれば、CMTS は T4 乗数として 3 を適用します。

MTC モードでは、T4 タイムアウト値を増やすことで、レンジング要求（RNG-REQ）スロットおよびレンジング応答メッセージの処理に関連するルータ オーバーヘッドを減らすことができます。RNG-RSP メッセージに T4 タイムアウト乗数値が含まれない場合、CM はデフォルトの T4 タイムアウト値を使用します。

アップストリーム チャネル ボンディングのファイバ ノード設定

Cisco CMTS ルータのファイバ ノード設定は、DOCSIS 3.0 で定義された MAC ドメイン ダウンストリーム サービス グループ（MD-DS-SG）および MAC ドメイン アップストリーム サービス グループ（MD-US-SG）を定義するために使用されます。DOCSIS 3.0 認定モデムのみがこの情報を使用します。

光同軸ハイブリッド（HFC）ネットワークでは、ファイバ ノードの同一同軸セグメントに接続されているすべての CM は、ヘッドエンドにある 1 つまたは複数の Cisco CMTS ルータ上のダウンストリームおよびアップストリーム チャネルの同じセットに到達します。

CM が物理的に接続されているファイバ ノードは 1 つのみです。ファイバ ノードに接続された CM が動作するために、ファイバ ノードにはプライマリ対応コントローラが少なくとも 1 つ含まれる必要があります。

アップストリーム チャネル ボンディング用の新規 TLV

次の表に、アップストリーム チャネル ボンディング機能用に CableLabs で新しく定義されたタイプ、長さ、値（TLV）を示します。

表 *50*：アップストリーム チャネル ボンディング用の新規 *TLV*

TLV 名	タイプ	長さ	値
CM のベンダー ID	43.8	3	ベンダー定義あたり

TLV 名	タイプ	長さ	値
ケーブル モデムの属性マスク	43.9	n	ケーブル モデムの属性マスク サブタイプの符号化

Cisco CMTS では、複数のアップストリーム チャネル ボンディング グループ（USBG）を設定できます。これらのボンディング グループには、それぞれ異なるアップストリーム周波数のアップストリームチャネルを含めることができます。ボンディング グループの中には、拡張周波数範囲内の周波数を持つチャネルを含められるものがあります（表 48：ダウンストリームおよびアップストリーム周波数，（364 ページ）を参照）。HFC ネットワークは、それぞれが標準または拡張アップストリーム周波数をサポートする複数のタイプの CM から構成されます。

CM を登録する際、Cisco CMTS によるボンディング グループの割り当ては、その CM でサポートされるアップストリーム周波数範囲に基づきません。ボンディング グループの割り当ては、各ボンディング グループの CM の数を均衡化するように実行されます。これにより、拡張周波数範囲内のボンディング グループが、拡張周波数をサポートしない CM に割り当てられる可能性があります。この場合、CMは登録できません。このようなシナリオは、85MHz という高周波数をサポートする Cisco cBR-8 CCAP ラインカードの実装（CM の混在あり）の際によく見受けられます（表 48：ダウンストリームおよびアップストリーム周波数，（364 ページ）を参照）。

Cisco CMTS により、拡張周波数範囲内のチャネルを含む USBG を（標準周波数範囲に制限された）CM に割り当てた場合、CM をそのアップストリーム ボンディング グループに登録できない可能性があります。回避策として、TLV 43.9.3（CM US 必須属性マスク）または TLV 43.9.4（CM US 禁止属性マスク）を使用します。これらの TLV により、Cisco CMTS によって CM が割り当てられる USBG がその CM にサポートされるアップストリーム周波数範囲内であるようにすることができます。

CM 属性マスク（TLV 43.9）のデフォルト属性（16 進数）は「80 00 00 00」です。つまり、マスクはデフォルトで、ボンディング ビットがイネーブルな状態ですべてゼロであることを意味します。始めの 4 バイトは事前定義されており、後の 4 バイトはユーザ定義です。Cisco CMTS が CM でサポートされる周波数範囲に基づいてボンディング グループを割り当てられるようにするには、次の手順を実行します。

1. TLV 43.9.3 または TLV 43.9.4 を使用し、後の 4 バイトを変更して、マスクを設定します。マスクは、各ボンディング グループに一意の属性が割り当てられるように設定する必要があります。
2. CM コンフィギュレーション ファイルにこのマスクを適用します。拡張周波数をサポートする CM は、設定された USBG の周波数範囲に関係なく、どの USBG にも登録できます。標準周波数をサポートする CM は、標準周波数範囲に設定された USBG にのみ登録できます。

標準または拡張周波数範囲をサポートする CM に、上記のように設定したマスクを適用します。いずれにせよ、属性マスクを使用する必要があるのは、標準周波数範囲の CM のみです。それらは、拡張アップストリーム周波数範囲に設定されたUSBGに登録できません。拡張周波数をサポートする CM に属性マスクがないのは、それらのモデムはどの USBG にも割り当てられることを意味します。

Cisco CMTS は、登録時に CM コンフィギュレーション ファイルで受信されるこのマスクを使用して、どの USBG を CM に割り当てるかを決定します。

アップストリームの重み付け均等化キューイング

アップストリームの重み付け均等化キューイング（WFQ）は、Cisco CMTS ルータが WFQ パラメータ設定に基づいてアップストリームサービスフローに最適な帯域幅を割り当てることができるようにする Quality of Service（QoS）機能です。アップストリーム WFQ をイネーブルにするには、ケーブル インターフェイス上でクラスベースまたはアクティビティベースの WFQ を設定する必要があります。

次の WFQ パラメータ設定がサポートされます。

Class-Based Weighted Fair Queuing：クラスベース WFQ

クラスベース均等化キューイング構成では、使用可能な帯域幅の割り当ては、サービス クラスでアクティブなサービス フローに基づいています。サービス クラスは、Cisco CMTS ルータで構成されるキューイング属性のグループです。クラスには少なくとも 1 つのアクティブなサービス フローが必要です。クラスは、クラスのウェイトに基づいて使用可能帯域幅の一部を受け取ります。デフォルトでは、各クラス（0 ～ 7）に「クラス + 1」ウェイトが設定されます。たとえば、クラス 0 にはウェイト 1、クラス 1 にはウェイト 2 が設定されます。

アクティビティベースの重み付け均等化キューイング

アクティビティベースの重み付け均等化キューイング構成では、使用可能な帯域幅の割り当ては、サービス クラス マップでアクティブなサービス フローのサービス クラスと総数に基づいています。サービスフローの数が多くなると、サービスクラスが受け取る帯域幅の割合が大きくなります。

サービス フロー プライオリティに対する独自の重み付け

重み付け均等化キューイング機能を使用すると、Cisco CMTS ルータは、アップストリーム サービス フローからの未処理要求に指定されたサービス フロー プライオリティのウェイトに基づいて、使用可能な帯域幅を共有できます。プライオリティとは、CM コンフィギュレーション ファイル、または Cisco CMTS サービス クラス構成で指定されているサービス フロー プライオリティを意味します。デフォルトでは、プライオリティのウェイトは「プライオリティ + 1」となります。たとえば、プライオリティ 0 にはウェイト 1、プライオリティ 1 はウェイト 2 が設定されます。プライオリティが高くなると、未処理要求のウェイトが大きくなります。カスタムのウェイトは、サービス クラスで合計 8 つのプライオリティ（0 ～ 7）を指定できます。

プライオリティ パラメータは、0（最低）～ 7（最高）の範囲でサービス フローのトラフィックのプライオリティを指します。アップストリーム トラフィックでは、プライオリティが高く保留中のすべてのサービスフローが、プライオリティが低いサービスフローより前に送信されるようにスケジュールされます。プライオリティごとに適切なウェイトに基づいて、プライオリティのウェイトを構成できます。

次の表に各サービス フロー プライオリティのデフォルト ウェイトを示します。

表 *51*：サービス フロー プライオリティのデフォルト ウェイト

サービス フロー プライオリティ	デフォルト ウェイト
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

アップストリーム スケジューラとサービス フロー

DOCSIS 準拠の Cisco CMTS ルータは、アップストリーム サービス フローを使用するさまざまなパケット ストリームやアプリケーション用のさまざまなアップストリーム スケジューリング モジュールを提供できます。サービス フローとは、データのアップストリームまたはダウンストリーム フローのいずれかを表します。各サービス フローは固有のサービス フロー ID（SFID）により識別されます。各サービス フローには独自の Quality of Service（QoS）パラメータ（最大スループット、最小保証スループット、プライオリティなど）を指定できます。アップストリーム サービス フローの場合は、スケジューリング モードも指定できます。

スケジューリングは、Cisco CMTS ルータが帯域幅要求を受信してアップストリーム トラフィック用に CM にタイムスロットを付与できるようにするプロセスです。Cisco CMTS ルータは定期的にそれぞれの有効なアップストリーム チャネル用に許可マップを作成します。このマップにより個々のタイムスロットが付与されて、CM はアップストリーム チャネルにパケットを配置できるようになります。

DOCSIS 3.0 には、CM がアップストリーム サービス フローを作成する方法が記述されています。次のスケジューリング タイプは、Cisco CMTS ルータがアップストリーム サービス フロー用に帯域幅を割り当てることを可能にします。

- 非送信請求許可サービス（UGS）
- 送信請求許可サービス

非送信請求許可サービスは主に音声で使用されます。UGS では CM は Cisco CMTS ルータからの付与を明示的に要求する必要はありませんが、送信請求許可サービスでは CM は Cisco CMTS ルータからの付与を明示的に要求する必要があります。送信請求許可サービスは主にベスト エフォート（BE）サービスのために使用されます。

DOCSIS 2.0 とは異なり、DOCSIS 3.0 ではサービスごとに複数の未処理要求が可能です。アップストリーム スケジューラの詳細については、次の URL にある『*Upstream Scheduler Mode for the Cisco CMTS Routers*』を参照してください。

http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_upstm_sch_md_ps2209_TSD_Products_Configuration_Guide_Chapter.html

アップストリーム サービス フローの均等化

同じクラス内のサービス フローが受け取る帯域幅は、ほぼ同量です。均等化により、次を含むさまざまなサービス フロー間の帯域幅分配の格差が解決されます。

- 未ボンディング サービス フローとボンディング サービス フロー
- 異なるベンダー（Intel/TI と Broadcom）のモデム上のサービス フロー
- さまざまなサイズの（1、2、4 チャネルの）ボンディング グループに関連付けられているサービス フロー

アップストリーム スケジューラはフロー ベースのキューイングをサポートします。アップストリーム サービス フローの均等化が設定されている場合、サービス フローが BW を受け取る順序とその量は、同じクラス内の他のフローに比較したそのフローの現在の使用量に基づいてアップストリーム スケジューラにより決定されます。

アップストリーム サービス フローの均等化機能を設定するには、 **cable upstream qos fairness** コマンドを使用します。このコマンドは、インターフェイス コンフィギュレーション モード（または MAC ドメイン コンフィギュレーション モード）で使用します。

USBG のチャネル全体へのトラフィックの分配

アップストリーム チャネル ボンディング（USCB）を有効にすると、1 つのアップストリーム ボンディング グループ上のアップストリーム チャネル間で帯域幅利用のバランスをとるために、USBG のチャネル全体へのトラフィックの分配機能を使用できます。

この機能は、MAC ドメインごとにアップストリーム チャネル ボンディング グループが 1 つ構成されている場合のみ、使用率のバランスをとります。

制約事項

- この機能は、MAC ドメインの 1 つのアップストリーム ボンディング グループでのみサポートされます。MAC ドメインで複数のアップストリーム ボンディング グループが設定されているときは、使用率のバランスがとられません。
- すべてのチャネルは同じ MAC ドメインの下の 1 つのアップストリーム ボンディング グループで設定される必要があります。
- この機能は、UB-online ケーブル モデムにのみ使用されます。

インターフェイス（config-if）コンフィギュレーション モードで **cable upstream balance-scheduler** コマンドを使用して、USCB Balancing Scheduler を有効または無効にできます。

ケーブル モデム機能よりも小型な USBG を使用した DOCSIS 3.0 のロード バランシング

USBGに含まれるアップストリームチャネルがDOCSIS 3.0ロードバランシングの有効な合計アップストリーム チャネル セットより少ないサービス グループでUSCBを使用するときに、CMTSは構成済みUSBGの範囲外であるような用途のために、送信チャネル セット（TCS）をDOCSIS 3.0ケーブル モデムに割り当てることができます。CMTSは、ケーブル モデム サービスを増加させるために、小さいUBGおよびデフォルトの単一チャネル ボンディング グループを大きいチャネル セットにバインドしようとします。たとえば、大規模なTCSを受信するDOCSIS 3.0ケーブルモデムは、動的サービスフローを追加するために、このような追加チャネルを使用できます。DOCSIS 3.0 ロード バランシング機能では、大規模なTCSの結果としてUSBGを使用して明示的に設定されていないアップストリーム チャネルにケーブル モデムを移動することもできます。

アップストリーム ボンディングを使用しているときにDOCSIS 3.0 ロード バランシングを有効化する場合は、次の手順を実行して、アップストリームボンディング グループ設定が組み込みおよび調整されていることを確認してください。

- USBGを設定します。これは、サービス グループ内のケーブル モデム機能に一致します（4チャネルUSBG、2チャネルUSBG、3チャネルUSBGなど適宜）。
- サービス グループ内のモデム機能に基づいて、設定されたUSBGがアップストリーム チャネル セットに最適であることを確認します。たとえば、4つのアップストリーム チャネルが使用可能な場合、動的TCSによってサブ最適化ボンディングのシナリオが生じないようにするため、チャネル0+1および2+3がそれぞれUSBGである必要があります。
- また、USBGで設定されていないアップストリーム チャネルのうちボンディングに使用しないものがあれば、それをシャット ダウンできます。

Cisco cBR-8 CCAP のライン カードのレート制限

レート制限機能は、Cisco cBR-8 CCAP ライン カード上のボンディングされたDOCSIS 3.0サービス フローのアップストリーム トラフィックの集約率およびCPU消費を制御できます。レート制限機能は、Cisco cBR-8 CCAP ライン カードでデフォルトで構成されています。ただし、 **cable upstream rate-limit-ccf** コマンドを使用してデフォルト設定を変更できます。

レート制限機能は、次の2つのレート制限方法を使用します。

- 集約レート制限：これは、Peripheral Component Interconnect（PCI）バスで集約されたスループットに基づきます。すべてのボンディングされたサービス フローについてライン カードごとのスループットです。デフォルトのスループットおよびバースト レート構成を変更できます。最大許容スループットは115 Mbpsです。
- CPUベースのレート制限：この方法では、Continuous Concatenation and Fragmentation（CCF）によって消費されるCPUを制御し、トラフィックがボンディングされたサービス フローで過負荷になるときにライン カードが正しく機能することを保証します。デフォルト設定では、CCFにCPUの50パーセントを割り当てます。必要に応じて、デフォルトのCPUしきい値およびバースト レートを変更できます。

SID トラッキング

サービス ID（SID）トラッキング機能により、アップストリーム帯域幅要求と許可処理に関連するイベントを追跡できます。SID トラッカー モジュールは、1 つの MAC ドメインあたり最大 2 つのサービス フローのイベントを追跡できます。SID トラッカー モジュールは、ケーブル インターフェイス ラインカード上の 1 つのサービス フローあたり最大 40,000 イベントを追跡します。

次のタイプのイベントに対して SID トラッキングをイネーブルにできます。

- DOCSIS 2.0 の帯域幅要求
- DOCSIS 3.0 の帯域幅要求
- 許可
- 保留中の許可（トラフィック輻輳による）
- 保留中の許可（シェーピングによる）

SID トラッキングを有効にするには、**track keyword** とともに **debugcableinterfacesid** コマンドを使用します。SID トラッキングを確認するには、特権 EXEC モードで **show interface cable upstream debug** コマンドを使用します。

サービス ID クラスタ

サービス フローの作成時、Cisco CMTS ルータは、1 つ以上のサービス ID クラスタをアップストリーム ボンディング サービス フロー（アップストリーム ボンディング グループに割り当てられたアップストリーム サービス フロー）に割り当てることができます。SID クラスタは、ボンディング グループ内の 1 アップストリームあたり 1 つの SID を含みます。CM は、帯域幅要求を送信する際に、アップストリーム インターフェイスについて SID クラスタで定義されている SID の 1 つを使用します。CM は、SID クラスタの切り替え条件に基づいて SID または SID クラスタを選択します。

たとえば、ある CM が 1 ～ 4 のアップストリーム チャネル上に配置されているとします。Cisco CMTS ルータは、ボンディング サービス フローを作成し、各アップストリーム チャネルに単一の SID クラスタを割り当てます。つまり、UP1 に対し SID1、UP2 に対し SID2、UP3 に対し SID3、UP4 に対し SID4 を割り当てます。これにより、CM は 4 つのアップストリーム チャネルのいずれかを使用して帯域幅要求を送信できるようになります。つまり、CM は特定のアップストリームに対して定義された SID を使用して、SID クラスタ内の任意のアップストリーム インターフェイス上で帯域幅を要求できます。Cisco CMTS ルータは、アップストリーム チャネルの任意の組み合わせを使用して CM に帯域幅を付与します。

アップストリーム チャネル ボンディングの設定方法

（注） アップストリーム チャネル ボンディング機能を設定する前に、ファイバ ノードが設定されていることを確認します。ファイバ ノードは、実際の設備のトポロジに合わせて設定する必要があります。

次のタスクでは、Cisco cBR-8 ルータでアップストリーム チャネル ボンディングを設定する方法を示します。

Cisco CMTS ルータでの MTC モードの有効化

ここでは、Cisco CMTS ルータで MTC モードをイネーブルにする方法について説明します。

Cisco CMTS ルータでのデフォルト MTC モードの設定

デフォルトで、MTC モードは、ケーブル インターフェイス ライン カード上で構成されます。このデフォルト構成では、Cisco CMTS ルータは各 CM のコンフィギュレーション ファイルに基づき、MAC ドメイン単位で MTC モードを有効にします。CM コンフィギュレーション ファイルで TLV 43.9.3（ケーブル モデムのアップストリームの必須属性マスク）のボンディング ビット（ビット 0）が有効な場合、Cisco CMTS ルータは CM が MTC モードでオンラインになれるようにします。CM コンフィギュレーション ファイルでボンディング ビットがオンになっていない場合、CM は非 MTC モードでオンラインになります。

CM コンフィギュレーション ファイルで必須属性を追加する方法の詳細については、例：CM コンフィギュレーション ファイルを使用した単一 CM の MTC モードの有効化, （395 ページ）を参照してください。

すべての CM に対する MTC モードの有効化

（注） この MTC モード設定は、必須属性が設定されたデフォルトの MTC モード設定（CM 単位）よりも優先されます。MAC ドメイン内のすべての CM の MTC モードを無効にするには、 **cable mtc-mode** コマンドの **no** 形式を使用します。MTC モードをイネーブルにして、TLV 43.9.4 のアップストリーム ボンディングの禁止マスクをディセーブルにしている場合、CM はアップストリーム チャネル ボンディング機能をサポートしません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface cable** {*slot/subslot/port*| *slot/subslot/cable-interface-index*| *slot/port*| *slot/cable-interface-index*} 例： `Router(config)# interface cable 7/0/0`	Cisco CMTS ルータでケーブル インターフェイス ライン カードを指定します。
ステップ 4	**cable mtc-mode** 例： `Router(config-if)# cable mtc-mode`	すべての CM の MAC インターフェイスで MTC モードをイネーブルにします。
ステップ 5	**end** 例： `Router(config-if)# end`	ケーブル インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

UCSB 必須属性の設定

CM コンフィギュレーション ファイルで TLV 43.9.3（CM アップストリーム必須属性マスク）を設定し、ボンディング ビットが 1 に設定されている場合は、モデムは MAC ドメインごとに UB-online になります。CM コンフィギュレーション ファイルで TLV 43.9.3 を設定せず、ボンディング ビットが 1 に設定されていない場合は、モデムは MAC ドメインごとに 1 つのアップストリーム チャネルでオンラインになります。

（注） このように設定しないと、TLV 43.9.3 がモデム コンフィギュレーション ファイルで設定されているかどうかに関係なく、モデムが MAC ドメインで UB-online になります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface cable** { *slot/subslot/port*| *slot/subslot/cable-interface-index*| *slot/port*| *slot/cable-interface-index*} 例： `Router(config)# interface cable 7/0/0`	Cisco CMTS ルータでケーブル インターフェイス ライン カードを指定します。
ステップ 4	**cable mtc-mode required-attribute** 例： `Router(config-if)# cable mtc-mode required-attribute`	UCSB で CM 必須属性が適用されるようにします。
ステップ 5	**end** 例： `Router(config-if)# end`	ケーブル インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ボンディング グループの作成

アップストリーム ボンディング グループは、ケーブル インターフェイス ライン カードで複数のアップストリーム チャネルを同時に組み合わせて作成されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface cable** {*slot/subslot/port*| *slot/subslot/cable-interface-index*| *slot/port*| *slot/cable-interface-index*} 例： `Router(config)# interface cable 7/0/0`	Cisco CMTS ルータでケーブル インターフェイス ライン カードを指定します。
ステップ 4	**cableupstreambonding-group** *id* 例： `Router(config-if)# cable upstream bonding-group 200`	指定したケーブル インターフェイスでボンディング グループを作成します。
ステップ 5	**end** 例： `Router(config-if)# end`	ケーブル インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次の作業

アップストリーム ボンディング グループを作成したら、ボンディング グループにアップストリーム チャネルを追加する必要があります。

ボンディング グループへのアップストリーム チャネルの追加

制約事項 DOCSIS 3.0 認定 CM がサポートするアップストリーム ボンディング グループは 4 つのみです。この CM は、ボンディング グループに追加される別のアップストリーム チャネルを受け入れません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface cable** {*slot/subslot/port*| *slot/subslot/cable-interface-index*| *slot/port*| *slot/cable-interface-index*} 例： `Router(config)# interface cable 7/0/0`	Cisco CMTS ルータでケーブル インターフェイス ライン カードを指定します。
ステップ 4	**cableupstreambonding-group** *id* 例： `Router(config-if)# cable upstream bonding-group 200`	指定したインターフェイスでボンディング グループを作成します。
ステップ 5	**upstream** *number* 例： `Router(config-upstream-bonding)# upstream 1`	アップストリーム ボンディング コンフィギュレーション サブモードを開始し、アップストリーム ボンディング グループにアップストリーム チャネルを追加します。 （注） アップストリームチャネルは、ボンディング グループに追加するよりも先に、MAC ドメインにボンディングする必要があります。アップストリーム チャネル ボンディングの詳細な設定手順については、「アップストリーム チャネル ボンディングの設定例」を参照してください。 MAC ドメインごとに最大 16 個のアップストリーム チャネルを設定できます。これらは次の 2 つのグループに分けられます。 • グループ 1：アップストリーム チャネル 0 ～ 7 • グループ 2：アップストリーム チャネル 8 ～ 15 **アップストリーム ボンディング グループ**には、グループ 1 のすべてのアップストリーム チャネルのみ、またはグループ 2 のすべてのアップストリーム チャネルのみが含まれている必要があります。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Router(config-upstream-bonding)# end`	アップストリームボンディング コンフィギュレーション サブモードを停止して、特権 EXEC モードに戻ります。

ファイバ ノードへのアップストリーム チャネル ポートの追加

ケーブル インターフェイス ライン カード上で基本的なアップストリーム チャネル ボンディングの設定を完了するには、ファイバ ノードにアップストリーム チャネル コントローラを追加する必要があります。ファイバ ノードには、CMからアクセスするアップストリームとダウンストリームのコントローラをすべて含める必要があります。

制約事項

- ファイバ ノードの設定は、ファイバ ノード内のすべてのアップストリーム チャネルに異なるアップストリーム周波数が指定されている場合のみ有効です。
- 1 つのスペクトル グループが 1 つのアップストリーム チャネルに割り当てられており、1 つの周波数が別のアップストリーム チャネルに割り当てられている場合、同じファイバ ノード内のアップストリーム ケーブル コネクタにマップされた 2 つのアップストリーム チャネルについて、最初のアップストリーム チャネルのスペクトル グループと別のアップストリーム チャネルの周波数に関連付けられたバンドが重複すると、ファイバ ノードの設定が無効になります。固定周波数は、別のアップストリーム チャネルで利用可能なスペクトル グループ バンドと重複できません。

（注） ファイバ ノードの設定は、実際の設備のトポロジに合わせて行う必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**cablefiber-node***fiber-node-id* 例： `Router(config)# cable fiber-node 2`	ファイバ ノード設定モードを開始します。
ステップ 4	**upstreamUpstream-Cable** *slot/subslot/port* 例： `Router(config-fiber-node)# upstream Upstream-Cable 7/0/1`	ファイバ ノードのアップストリーム チャネル ポートを指定します。
ステップ 5	**end** 例： `Router(config-fiber-node)# end`	ファイバ ノード設定モードを終了し、特権 EXEC モードに戻ります。

クラスベース均等化キューイングの設定

クラスベースの設定では、使用可能な帯域幅の割り当ては、サービス クラスでアクティブなサービス フローによって異なります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権EXECモードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface cable** {*slot/subslot/port*| *slot/subslot/cable-interface-index*| *slot/port*| *slot/cable-interface-index*} 例： `Router(config)# interface cable 7/0/0`	Cisco CMTS ルータでケーブル インターフェイス ライン カードを指定します。

	コマンドまたはアクション	目的
ステップ 4	**cableupstreamqoswfqclass** 例： `Router(config-if)# cable upstream qos wfq class`	クラスベース均等化キューイングをイネーブルにします。
ステップ 5	**end** 例： `Router(config-if)# end`	ケーブル インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

アクティビティベースの重み付け均等化キューイングの設定

アクティビティベースの設定では、使用可能な帯域幅の割り当ては、サービス クラスマップでアクティブなサービス フローのサービス クラスと総数に基づいています。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface cable** {*slot/subslot/port*| *slot/subslot/cable-interface-index*| *slot/port*| *slot/cable-interface-index*} 例： `Router(config)# interface cable 7/0/0`	Cisco CMTS ルータでケーブル インターフェイス ライン カードを指定します。
ステップ 4	**cableupstreamqoswfqactivity** 例： `Router(config-if)# cable upstream qos wfq activity`	アクティビティベースの重み付け均等化キューイングをイネーブルにします。
ステップ 5	**end** 例： `Router(config-if)# end`	ケーブル インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

サービス フロー プライオリティに対する独自の重み付けの設定

WFQ 機能により、アップストリーム サービス フローからの未処理の要求に対して指定したサービス フロー プライオリティの重み付けに基づいて、Cisco CMTS ルータは利用可能な帯域幅を共有できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface cable** {*slot/subslot/port*| *slot/subslot/cable-interface-index*| *slot/port*| *slot/cable-interface-index*} 例： `Router(config)# interface cable 7/0/0`	Cisco CMTS ルータでケーブル インターフェイス ライン カードを指定します。
ステップ 4	**cableupstreamqoswfqweights***priority0-priority7* 例： `Router(config-if)# cable upstream qos wfq weights 10 20 30 40 50 60 70 80.`	サービス クラス内のすべてのサービス フロー プライオリティで独自の重み付けを有効にします。 （注） プライオリティのデフォルトの重み付けを変更する場合は、8 つすべてのサービス フロー プライオリティ（0 ～ 7）に独自の重み値を指定する必要があります。有効な範囲は 1 ～ 255 です。
ステップ 5	**end** 例： `Router(config-if)# end`	ケーブル インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SID クラスタの設定

ここでは、SID クラスタの設定と、アップストリーム ボンディング サービス フローへの割り当て方法について説明します。

（注） 適切なアップストリーム ボンディング スピードを達成するには、**cablesid-cluster-groupnum-of-cluster2** コマンドを設定します。または、ケーブル モデム ファイルでアップストリームの Max Traffic のバースト値を使用します（30 kB など）。DOCSIS 3.0 では継続的な連結とフラグメンテーション（CCF）が使用され、Max Concat フィールドでデフォルト値 3044 が使用されるため、ケーブル モデム ファイル内の Max Concat のバースト値を変更する必要はありません。

（注） **cablesid-cluster-group** コマンドを使用しない場合、ルータはデフォルトの SID クラスタ設定を受け入れます。デフォルトでは、1 つの SID クラスタだけが設定されます。同様に、**cable sid-cluster-switching** コマンドを使用しない場合、ルータはデフォルトの SID クラスタ スイッチオーバー基準を受け入れます。つまり、SID クラスタを使用して作成できる要求は 1 つのみです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface cable** {*slot/subslot/port*| *slot/subslot/cable-interface-index*| *slot/port*| *slot/cable-interface-index*} 例： `Router(config)# interface cable 7/0/0`	Cisco CMTS ルータでケーブル インターフェイス ライン カードを指定します。
ステップ 4	**cablesid-cluster-group[dynamic|req-multiplier** *value*|**num-of-cluster** *number*] 例： `Router(config-if)# cable sid-cluster-group dynamic`	SID クラスタ グループを作成します。

	コマンドまたはアクション	目的
	Router(config-if)# **cable sid-cluster-group req-multiplier 12** Router(config-if)# **cable sid-cluster-group num-of-cluster 2**	
ステップ 5	**cablesid-cluster-switching[max-outstanding-byte** *value*|**max-request** *value*|**max-time** *seconds*|**max-total-byte** *value*|**]** 例： Router(config-if)# **cable sid-cluster-switching max-outstanding-byte 4444** Router(config-if)# **cable sid-cluster-switching max-request 222** Router(config-if)# **cable sid-cluster-switching max-time 444** Router(config-if)# **cable sid-cluster-switching max-total-byte 67890**	SID クラスタ スイッチオーバー基準を指定します。
ステップ 6	**end** 例： Router(config-if)# **end**	ケーブル インターフェイス コンフィギュレーション モードを終了し、特権EXECモードに戻ります。

次の作業

SID クラスタ設定を確認するには、 **show running-config all** コマンドを使用します。次に、コマンドの出力例を示します。

```
Router# show running-config all
.
.
.
cable sid-cluster-group num-of-cluster 1
cable sid-cluster-group dynamic
cable sid-cluster-group req-multiplier 4
```

ケーブル モデムのチャネル タイムアウトの設定

チャネル タイムアウト設定により、CM が登録応答（REG-RSP）と REG-RSP-MP メッセージ内で記述しているアップストリーム チャネルで初期レンジングを実行するために使用できる最大時間を指定することができます。デフォルトのチャネルタイムアウト値（60秒）が自動的に設定されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface cable** {*slot/subslot/port*| *slot/subslot/cable-interface-index*| *slot/port*| *slot/cable-interface-index*} 例： `Router(config)# interface cable 7/0/0`	Cisco CMTS ルータでケーブル インターフェイス ライン カードを指定します。
ステップ 4	**cableinit-channel-timeout** *value* 例： `Router(config-if)# cable init-channel-timeout 160`	CM がアップストリーム チャネルで初期レンジングを実行するために使用できる最大時間を指定します。
ステップ 5	**end** 例： `Router(config-if)# end`	ケーブル インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ケーブル アップストリームの復元力の設定

ケーブル アップストリームの復元力モジュールは、CM の 1 つ以上の非プライマリ アップストリーム サービス フローが一時的または永続的なエラー状態になっても、CM が引き続き動作するようにします。このモジュールにより、Cisco CMTS ルータがさまざまなイベントを処理し、各 CM の送信チャネル設定を維持することができます。

プライマリ アップストリーム サービス フローの障害時には、アップストリームの復元力モジュールが CM を強制的にオフラインにします。

Multiple Transmit Channel（MTC）モデムでは、障害のあるアップストリーム チャネル上の NRTPS、リアルタイム ポーリング サービス（RTPS）、UGS、および UGS-AD アップストリーム サービス フローが、ケーブル モデムのリセットなしでケーブル モデム内の別の正常なアップストリーム チャネルに移行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 upstream resiliency data-burst polling-interval** *number* 例： `Router(config)# cable upstream resiliency data-burst polling-interval 60`	データバースト復元力のポーリング間隔を秒単位で設定します。範囲は 5 ～ 3600 です。デフォルトでは、ポーリング間隔が 60 に設定されます。
ステップ 4	**interface cable** {*slot/subslot/port*| *slot/subslot/cable-interface-index*| *slot/port*| *slot/cable-interface-index*} 例： `Router(config)# interface cable 7/0/0`	Cisco CMTS ルータでケーブル インターフェイス ライン カードを指定します。

ステップ 5	**cable upstream resiliency**{**channel-down-detect** *number* | **data-burst snr** *number***ufec** *number***cfec** *number***hysteresis** *number* | **modem-offline-detect** *number* | **on-failure** {**disable-channel** | **extended-ranging** | **reset-modem**} | **sf-move** {**NRTPS** | **RTPS** | **UGS** | **UGS-AD**} }
	
	例：
	`Router(config-if)# cable upstream resiliency channel-down-detect 68`
	
	`Router(config-if)# cable upstream resiliency modem-offline-detect 16`
	
	`Router(config-if)# cable upstream resiliency on-failure disable-channel`
	
	`Router(config-if)# cable upstream resiliency sf-move NRTPS`
	
	`Router(config-if)# cable upstream resiliency sf-move RTPS`
	
	`Router(config-if)# cable upstream resiliency sf-move UGS`
	
	`Router(config-if)# cable upstream resiliency sf-move UGS-AD`
		ボンディングされたアップストリーム サービス フローのアップストリームの復元力を設定します。

	コマンドまたはアクション	目的
	`Router(config-if)# cable upstream resiliency data-burst snr 24 ufec 1 cfec 0 hysteresis 3`	
ステップ 6	**end** 例： `Router(config-if)# end`	ケーブルインターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

Cisco cBR-8 CCAP ライン カードでのレート制限の設定

レート制限機能は、Cisco cBR-8 CCAP ライン カードでデフォルトで構成されています。ただし、デフォルト設定は、cable upstream rate-limit-ccf コマンドを使用して変更することができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cableupstreamrate-limit-ccf** [**aggregated-burst** *value* | **aggregated-throughput** *value* | **cpu-burst** *value* | **cpu-threshold** *value*]
	
	例：
	`Router(config)# cable upstream rate-limit-ccf aggregated-burst 25000`
	
	`Router(config)# cable upstream rate-limit-ccf aggregated-throughput 540000`
	
	`Router(config)# cable upstream rate-limit-ccf cpu-burst 30`
	
	`Router(config)# cable upstream rate-limit-ccf cpu-threshold 60`
		ケーブル インターフェイス ライン カード上でアップストリーム ボンディング サービス フローのレート制限パラメータを設定します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

CM ステータス レポートのアップストリーム関連イベントの有効化

ケーブル インターフェイス ライン カードでのみアップストリーム関連 CM ステータス イベントを有効にできます。cable cm-status enable コマンドを使用すると、インターフェイスごとに次のアップストリーム関連 CM ステータス イベントを有効にできます。

- T4 タイムアウト
- T3 リトライ超過回数
- T3 リトライ超過回数後のレンジング成功

アップストリームとダウンストリームに関連する CM ステータス イベントを有効にする方法については、次の URL にあるワイドバンド モデム復元力機能のガイドを参照してください。

http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/ubr_wm_resiliency.html

ボンディング グループ属性の変更

ボンディング グループ属性は、各アップストリーム ボンディング グループに対して自動的に設定されます。アップストリーム ボンディング コンフィギュレーション モードで **attributes** コマンドを使用すると、この属性を変更することができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface cable** {*slot/subslot/port*| *slot/subslot/cable-interface-index*| *slot/port*| *slot/cable-interface-index*}	Cisco CMTS ルータでケーブル インターフェイス ライン カードを指定します。

	コマンドまたはアクション	目的
	例： `Router(config)# interface cable 7/0/0`	
ステップ 4	**cableupstreambonding-group** *id* 例： `Router(config-if)# cable upstream bonding-group 200`	指定したケーブル インターフェイスでボンディング グループを作成し、アップストリーム ボンディング コンフィギュレーション モードを開始します。
ステップ 5	**attributes** *value* 例： `Router(config-upstream-bonding)# attributes eeeeeeee`	指定したボンディング グループの属性値を変更します。
ステップ 6	**end** 例： `Router(config-upstream-bonding)# end`	アップストリームボンディング コンフィギュレーション モードを停止して、特権 EXEC モードに戻ります。

アップストリーム チャネルのレンジング ポーリング間隔の変更

ケーブル インターフェイス コンフィギュレーション モードで cable upstream ranging-poll コマンドを使用すると、アップストリーム チャネルのデフォルトのレンジング ポーリング間隔（20 秒）を変更できます。また、このコマンドを使用すると、T4 タイムアウトの乗数値を指定することもできます。

T4 乗数の詳細については、T4 乗数, （368 ページ）を参照してください。

（注） 必要な場合を除き、デフォルトのレンジング ポーリング間隔を変更しないことを推奨します。デフォルト設定では、非 MTC モードの DOCSIS 2.0 CM は、1 つのアップストリーム チャネルで 20 秒おきにレンジングを実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface cable** {*slot/subslot/port*| *slot/subslot/cable-interface-index*| *slot/port*| *slot/cable-interface-index*} 例： `Router(config)# interface cable 7/0/0`	Cisco CMTS ルータでケーブル インターフェイス ライン カードを指定します。
ステップ 4	**cable upstream ranging-poll** [**interval** *value* | **t4-multiplier** *timeout_value*] 例： `Router(config-if)# cable upstream ranging-poll interval 24000 t4-multiplier 4`	アップストリーム チャネルのレンジング ポーリング間隔を指定します。 （注） **t4-multiplier** *timeout_value* が設定されていない場合、CMTS はモデムの T4 タイムアウトを使用します。たとえば、モデムの T4 タイムアウトが 90 秒の場合、CMTS はモデムの T4 乗数として 3 を適用します。
ステップ 5	**end** 例： `Router(config-if)# end`	ケーブル インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

チャネル セット割り当ての削減設定

Cisco CMTS ルータが CM の総電力バジェットに基づいてアップストリーム チャネル セットの割り当てを削減するように、送信電力のオフセット バジェットを設定する必要があります。

（注） 電力バジェット オフセット（max-channel-power-offset）で指定するしきい値は、Cisco CMTS ルータが CM に送信するレンジング応答（RNG-RSP）メッセージで Ranging Status フィールドの値を決定する電力しきい値（power-adjust continue）よりも小さい必要があります。電力しきい値は、**cableupstreampower-adjust** コマンドを使用して指定できます。

はじめる前に

- グローバル コンフィギュレーション モードで **cabletx-power-headroom** コマンドを使用して拡張送信電力を設定します。
- 対応する静的ボンディング グループが設定されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface cable** {*slot/subslot/port*| *slot/subslot/cable-interface-index*| *slot/port*| *slot/cable-interface-index*} 例： `Router(config)# interface cable 7/0/0`	Cisco CMTS ルータでケーブル インターフェイス ライン カードを指定します。
ステップ 4	**cable upstream max-channel-power-offset** *dB-value* 例： `Router(config-if)# cable upstream max-channel-power-offset 2`	アップストリームチャネルの電力オフセット値を指定します。
ステップ 5	**end** 例： `Router(config-if)# end`	ケーブル インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DOCSIS 拡張送信電力機能の設定

Cisco CMTS の DOCSIS 拡張送信電力機能はデフォルトで有効です。ただし、デフォルト設定は、cable upstream ext-power コマンドを使用して変更することができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface cable** {*slot/subslot/port*| *slot/subslot/cable-interface-index*| *slot/port*| *slot/cable-interface-index*} 例： `Router(config)# interface cable 7/0/0`	Cisco CMTS ルータでケーブル インターフェイス ライン カードを指定します。
ステップ 4	**cableupstreamext-power** 例： `Router(config-if)# cable upstream ext-power`	Cisco CMTS で DOCSIS 拡張送信電力機能を有効にします。 このコマンドの **no** 形式を使用すると、DOCSIS拡張送信電力機能が無効になります。
ステップ 5	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権EXECモードに戻ります。

トラブルシューティングのヒント

次のデバッグ コマンドを使用すると、不適切なアップストリーム チャネル ボンディングの設定とその関連機能のトラブルシューティングを行うことができます。

- **debugcablecm-status**：Cisco CMTS ルータ上の CM ステータス メッセージに関するデバッグ情報を表示します。
- **debugcablemdd**：MAC ドメイン記述子（MDD）のデバッグ情報を表示します。
- **debugcablemd-sg**：サービス グループのデバッグ メッセージに関する情報を表示します。
- **debugcableubg**：アップストリーム ボンディング グループのデバッグ情報を表示します。

アップストリーム チャネル ボンディングの設定例

次に、Cisco cBR-8 ルータの Cisco cBR-8 CCAP ライン カード インターフェイス 7/0/0 の基本アップストリーム チャネル ボンディングを設定する方法について説明します。

```
controller Upstream-Cable 7/0/0
us-channel 0 frequency 10000000
us-channel 0 channel-width 3200000 3200000
us-channel 0 ingress-noise-cancellation 50
```

```
us-channel 0 docsis-mode atdma
us-channel 0 minislot-size 2
us-channel 0 modulation-profile 221
us-channel 0 equalization-coefficient
no us-channel 0 shutdown
us-channel 1 frequency 16400000
us-channel 1 channel-width 6400000 6400000
us-channel 1 ingress-noise-cancellation 50
us-channel 1 docsis-mode atdma
us-channel 1 minislot-size 1
us-channel 1 modulation-profile 221
us-channel 1 equalization-coefficient
no us-channel 1 shutdown
us-channel 2 frequency 22800000
us-channel 2 channel-width 6400000 6400000
us-channel 2 docsis-mode atdma
us-channel 2 minislot-size 1
us-channel 2 modulation-profile 221
us-channel 2 equalization-coefficient
no us-channel 2 shutdown
us-channel 3 frequency 29200000
us-channel 3 channel-width 6400000 6400000
us-channel 3 docsis-mode atdma
us-channel 3 minislot-size 1
us-channel 3 modulation-profile 221
us-channel 3 equalization-coefficient
no us-channel 3 shutdown
us-channel 4 channel-width 1600000 1600000
us-channel 4 docsis-mode tdma
us-channel 4 minislot-size 4
us-channel 4 modulation-profile 21
us-channel 4 shutdown
us-channel 5 channel-width 1600000 1600000
us-channel 5 docsis-mode atdma
us-channel 5 minislot-size 4
us-channel 5 modulation-profile 221
us-channel 5 shutdown
!

interface Cable7/0/0
load-interval 30
downstream Integrated-Cable 7/0/0 rf-channel 0
downstream Integrated-Cable 7/0/0 rf-channel 8
downstream Integrated-Cable 7/0/0 rf-channel 16
upstream 0 Upstream-Cable 7/0/0 us-channel 0
upstream 1 Upstream-Cable 7/0/0 us-channel 1
upstream 2 Upstream-Cable 7/0/0 us-channel 2
upstream 3 Upstream-Cable 7/0/0 us-channel 3
no cable upstream 0 equalization-error-recovery
no cable upstream 1 equalization-error-recovery
no cable upstream 2 equalization-error-recovery
no cable upstream 3 equalization-error-recovery
cable upstream 7 attribute-mask 1FF
cable upstream bonding-group 1
upstream 0
upstream 1
upstream 2
attributes 80000000
cable bundle 1
cable map-advance static 2000
cable sync-interval 121
cable reduction-mode mta-battery enable
cable privacy accept-self-signed-certificate
end

cable fiber-node 1
description Feed Mac Domain: Cable7/0/0
downstream Integrated-Cable 7/0/0
upstream Upstream-Cable 7/0/0
```

（注） 通常、ボンディングには同一コネクタのチャネルを使用しますが、MAC ドメイン内の異なるコネクタのチャネルをボンディングすることもできます。1 つの MAC ドメインで複数のチャネル ボンディング グループをサポートできます。

（注） 1 つのアップストリーム ケーブル コントローラには、最大 8 つの周波数をスタックできます。アップストリーム ケーブル コントローラに 8 つの周波数がスタックされているため、隣接するアップストリーム ケーブル コントローラにスタックできる周波数は残されていません。

例：CM コンフィギュレーション ファイルを使用した単一 CM の MTC モードの有効化

次の例では、CM コンフィギュレーション ファイルを使用して MTC の必須属性を有効にする方法を説明します。

```
03 (Net Access Control) = 1
Unknown Type 005 = 01 01 01
18 (Maximum Number of CPE) = 4
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 1
   S06 (QoS Parameter Set Type) = 7
   S10 (Min Reserved Traffic Rate)= 500000
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 2
   S06 (QoS Parameter Set Type) = 7
   S10 (Min Reserved Traffic Rate) = 1000000
29 (Privacy Enable) = 0
43 (Vendor Specific Options)
   S08 (Vendor ID) = ff ff ff
   S009 (Unknown sub-type) = 03 04 80 00 00 00
```

アップストリーム チャネル ボンディング設定の確認

アップストリームチャネルボンディング設定を確認するには、次の **show** コマンドを使用します。

- **showcablemac-domainupstream-service-group**
- **showcablefiber-node**
- show interface cable upstream
- **showinterfacecableservice-flow**
- **showcablemodem**

ケーブル インターフェイス ライン カードのアップストリーム サービス グループのランタイム統計情報を確認するには、**showcablemac-domainupstream-service-group** コマンドを使用します。

ファイバ ノードの設定を確認するには、**showcablefiber-node** コマンドを使用します。

ケーブル インターフェイス ライン カードで設定されているボンディング グループを確認するには、 **show interface cable upstream** コマンドを使用します。

ケーブルインターフェイス ライン カードのアップストリーム ボンディング情報を確認するには、**showinterfacecableservice-flow** コマンドを使用します。

CM の送信電力レベルを確認するには、**showcablemodem** コマンドを使用します。

アップストリーム サービス フローの重み付け均等化キューイングの確認

ケーブル インターフェイス ライン カードのアップストリーム サービス フローに設定されている WFQ パラメータを確認するには、**show interface cable mac-scheduler** コマンドを使用します。

アップストリーム ボンディング サービス フローのレート制限の確認

アップストリーム ボンディング サービス フローに関して Cisco cBR8 CCAP ライン カードで設定されたレート制限基準を確認するには、**show cable rate-limit-ccf** コマンドを使用します。

（注） **show cable rate-limit-ccf** コマンドは、Cisco cBR8 CCAP ケーブル インターフェイス ライン カードにのみ適用されます。

拡張電力送信の確認

CM が高電力レベルで送信していることを確認するには、**show cable modem** コマンドを使用します。

高電力レベルで送信しているすべての CM を表示するには、**show cable modem extended-power** コマンドを使用します。

その他の参考資料

ここでは、アップストリームチャネルボンディング機能に関する参考資料について説明します。

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

アップストリーム チャネル ボンディングに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *52*：アップストリーム チャネル ボンディングに関する機能情報

機能名	リリース	機能情報
アップストリーム チャネル ボンディング	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 19 章

動的ボンディング グループ

このドキュメントでは、動的ボンディング グループの設定方法を説明します。これにより、ボンディング グループが自動的に作成され、すべてのダウンストリーム ボンディング グループのリソース管理に役立ちます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *53*：***Cisco cBR*** シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

動的ボンディング グループについて

動的ボンディング グループ（DBG）は、ダウンストリーム ボンディング グループの自動作成および回収を含め、すべてのダウンストリームボンディング グループのリソースを管理するのに役立ちます。

動的ボンディング グループの概要

RCC の設定と管理に必要な作業を減らすために、DBG 機能はダウンストリーム ボンディング グループの自動作成および回収を実装しています。DBGはチャネルの負荷状態に応じて自動的にボンディング グループを作成します。静的 RCC 設定がなくても、DBG により、モデムがダウンストリーム ボンディング グループに割り当てられます。ロード バランシング機能は、DBG を利用

してすべてのチャネル間でトラフィックを平衡化します。また、DBG はプライマリ チャネルと CM のキャパシティ配分も自動的に行います。

また、DBG はプライマリ チャネルと CM のキャパシティ配分も自動的に行います。

動的ボンディング グループは次のものをサポートします。

- CYLONS カードの CLC ごとに 896 個のボンディング グループをサポートします。
- DBG の作成および回収をサポートします。
- DOCSIS 3.0 および DOCSIS 3.1 チャネル タイプをサポートします。
- DOCSIS 3.0 および DOCSIS 3.1 ロード バランシングをサポートします。
- DBG 相互運用をサポートします（モデム登録およびロード バランシング）。
- 動的ロード バランシングを強化します（固定プライマリ チャネル移動）。
- 侵入型 FPGA SQF を強化します（チャネル使用率の均等化）。

動的ボンディング グループの設定方法

（注） このモジュールで参照されているコマンドの詳細については、「Cisco IOS Master Command List」を参照してください。

動的ボンディング グループの有効化

DBG を有効にするには、次のコマンドを実行します。

```
ROUTER# config t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER(config)# cable dynamic-bonding-group
ROUTER(config)# end
ROUTER#
ROUTER#
ROUTER# show run
ROUTER# show running-config | in dynamic-bonding
cable dynamic-bonding-group
```

DS 復元力の有効化および復元力ボンディング グループの設定

複数の RF チャネルで障害が発生しても最大限のダウンストリーム機能を伴ってモデムの w-online 状態を維持するには、次のコマンドを実行して DS 復元力機能を有効にします。

```
Router# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# cable resiliency ds-bonding
Router(config)# end
Router#
Router# show running-config | in resiliency
cable resiliency ds-bonding
```

```
Router#
Router# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# interface wideband-Cable 3/0/1:30
Router(config-if)# cable ds-resiliency
Wideband-Cable3/0/1:30 is set to WB resiliency bonding group.
Remove any existing bundle and rf-channel configuration.
Router(config-if)#end
Router#
Router#show running-config interface wideband-Cable 3/0/1:30
Building configuration...
Current configuration : 61 bytes
!
interface Wideband-Cable3/0/1:30
cable ds-resiliency
end
```

ACFE の有効化

QoS障害によってモデムの登録がブロックされないようにするには、ACFE機能を有効にします。

```
Router# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# cable acfe enable
Router(config)# end
Router# show running-config | in acfe
cable acfe enable
```

インターフェイス Mac ドメインとファイバ ノードの設定

（注） サービス グループで推奨されるサイズは 32 または 48 です。推奨されるプライマリ チャネル配分は、隣接する 4 つのチャネルに対して 1 つのプライマリ チャネルです（たとえば 0、4、8、12、16、20、24、28 など）。

インターフェイスMACドメインとファイバノードを設定するには、次のコマンドを実行します。

```
Router# show running-config interface c3/0/1
Building configuration...
Current configuration : 963 bytes
!
interface Cable3/0/1
downstream Integrated-Cable 3/0/1 rf-channel 0
downstream Integrated-Cable 3/0/1 rf-channel 4
downstream Integrated-Cable 3/0/1 rf-channel 8
downstream Integrated-Cable 3/0/1 rf-channel 12
downstream Integrated-Cable 3/0/1 rf-channel 16
downstream Integrated-Cable 3/0/1 rf-channel 20
downstream Integrated-Cable 3/0/1 rf-channel 24
downstream Integrated-Cable 3/0/1 rf-channel 28
upstream 0 Upstream-Cable 3/0/1 us-channel 0
upstream 1 Upstream-Cable 3/0/1 us-channel 1
upstream 2 Upstream-Cable 3/0/1 us-channel 2
upstream 3 Upstream-Cable 3/0/1 us-channel 3
upstream 4 Upstream-Cable 3/0/1 us-channel 4
upstream 5 Upstream-Cable 3/0/1 us-channel 5
upstream 6 Upstream-Cable 3/0/1 us-channel 6
upstream 7 Upstream-Cable 3/0/1 us-channel 7
cable upstream bonding-group 1
upstream 0
upstream 1
attributes 80000002
```

```
cable upstream bonding-group 2
upstream 2
upstream 3
attributes 80000000
cable bundle 255
end

Router# show cab
Router# show cable fib
Router# show cable fiber-node 1
Fiber-Node 1
     Channel(s) : downstream Integrated-Cable 3/0/1: 0-31
     Channel ID(s): 1  2  3  4  5  6  7  8  9  10 11 12 13 14
                    15 16 17 18 19 20 21 22 23 24 25 26 27 28
                    29 30 31 32
     Upstream-Cable 3/0/1
         FN Config Status: Configured (status flags = 0x01)
         MDD Status: Valid
Router# show running-config | sec fiber-node 1
  cable fiber-node 1
   downstream Integrated-Cable 3/0/1
   upstream Upstream-Cable 3/0/1
```

次の例では、OFDMをファイバノードで設定して動的ボンディング グループの一部として追加します。

```
Router# show cable dynamic-bonding-group summary
Dynamic bonding group: Enable
BG ID BG Name      BG Size  CMs  ServFlows Create Time           Create Client        BG
State            RFid list
9219  Wi1/0/4:2    33       36   36        Nov 7  01:56:27.406   MODEM_ONLINE
OPERATIONAL          9216-9247, 9375
9220  Wi1/0/4:3    33       10   10        Nov 7  02:04:31.142   MODEM_ONLINE
OPERATIONAL          9248-9279, 9375
9221  Wi1/0/4:4    8        1    1         Nov 7  02:06:09.949   MODEM_ONLINE
OPERATIONAL          9248-9255

Router# show controller integrated-Cable 1/0/0 rf-channel 158
Load for five secs: 8%/1%; one minute: 8%; five minutes: 8%
Time source is NTP, *14:07:30.643 EST Fri Nov 17 2017
Chan State Admin Mod-Type  Start       Width     PLC        Profile-ID    dcid  power
output
                          Frequency
158 UP     UP   OFDM      258000000   48000000  279000000       100      159   34.0   NORMAL

Router# show cable fiber-node 10
Load for five secs: 9%/0%; one minute: 9%; five minutes: 8%
Time source is NTP, *13:59:39.571 EST Fri Nov 17 2017

--------------------------------------------------------------------------------

Fiber-Node 10
  Channel(s)   :  downstream Integrated-Cable 1/0/0:  0-63, 158
  Channel ID(s):   1   2   3   4   5   6   7   8   9  10  11  12  13  14
                  15  16  17  18  19  20  21  22  23  24  25  26  27  28
                  29  30  31  32  33  34  35  36  37  38  39  40  41  42
                  43  44  45  46  47  48  49  50  51  52  53  54  55  56
                  57  58  59  60  61  62  63  64 159
  Upstream-Cable 1/0/0
    FN Config Status: Configured (status flags = 0x01)
    MDD Status: Valid
```

DOCSIS 3.0 および DOCSIS 3.1 のロード バランシングの有効化

DOCSIS ロード バランシングを有効にするには、cable load-balance docsis-enable コマンドを実行します。DOCSIS ロード バランシングが有効になっている場合、DOCSIS 3.0 および DOCSIS 3.1 に

関するロード バランシングを有効にするには cable load-balance docsis30-enable コマンドを実行します。

（注） **cable load-balance docsis30-enable** コマンドは、DOCSIS 3.0 および DOCSIS 3.1 のロード バランシングを有効にします。

DOCSIS 3.0 および DOCSIS 3.1 の静的ロード バランシングの有効化

プライマリ チャネルの負荷を平衡化するには、次のコマンドを実行して静的ロードバランシングを有効にします。

```
ROUTER# config t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER(config)# cable load-balance docsis30-enable static
ROUTER(config)# end
ROUTER# show cable load-balance
DOCSIS LB Enabled: Yes
DOCSIS 2.0 LB Enabled: Yes
DOCSIS 3.0 LB Enabled: Yes
DOCSIS 3.0 Static LB Enabled: Yes
DOCSIS 3.0 Dynamic Downstream LB Enabled: No
```

DOCSIS 3.0 および DOCSIS 3.1 の汎用ロード バランシング グループの有効化

汎用のロード バランス グループを有効にするには、次のコマンドを実行します。

```
Router# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# cable load-balance docsis-group fn 1 md c3/0/1
Router(config-lb-group)# no disable
Router(config-lb-group)# end
Router# show cable load-balance
DOCSIS LB Enabled: Yes
DOCSIS 2.0 LB Enabled: No
159
DOCSIS 3.0 LB Enabled: Yes
DOCSIS 3.0 Static LB Enabled: Yes
DOCSIS 3.0 Dynamic Downstream LB Enabled: Yes
DOCSIS 3.0 Dynamic Upstream LB Enabled: Yes
DOCSIS     Status Interval  DCC mask  Policy     Method Threshold

DOCSIS 3.0 General LB
MD       FN   Group ID         S Intv  DCC mask  Policy  Mtd     MD-CM-SG  Threshold
                                                          /UCC                        D/U
M/E/U/P/S
Ca3/0/1  1    2147557888 E 90   0xF8(0)/N 0           u/u        0x91010B   5/10/70/70/50
```

動的ロード バランシングおよび固定プライマリ チャネル移動の有効化

（注） 動的ロード バランシングが有効な状態でサービス停止を減らすには、固定プライマリ チャネル移動を有効にします。

ダウンストリームのすべてのチャネルで使用率に基づいて負荷を平衡化するには、次のコマンドを実行して動的ロード バランシングを有効にします。

```
Router# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# cable load-balance docsis30-enable dynamic downstream
Router(config)# end
Router#
Router# show cable load-balance
DOCSIS LB Enabled: Yes
DOCSIS 2.0 LB Enabled: No
DOCSIS 3.0 LB Enabled: Yes
DOCSIS 3.0 Static LB Enabled: Yes
DOCSIS 3.0 Dynamic Downstream LB Enabled: Yes
DOCSIS 3.0 Dynamic Upstream LB Enabled: Yes
DOCSIS     Status Interval  DCC mask  Policy     Method Threshold
Group                       /UCC                DS/US  M/E/U/P/S
1          GE     30        0xF8(0)/N 0          m/m    5/10/70/70/50

DOCSIS 3.0 General LB
MD       FN   Group ID   S Intv DCC mask  Policy    Mtd MD-CM-SG   Threshold
                                /UCC                D/U            M/E/U/P/S
Ca3/0/1  1    2147557888 E 90   0xF8(0)/N 0         u/u 0x91050A   5/10/70/70/50
Router#
Router# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# cable load-balance fixed-primary-channel
Router(config)# end
Router#
Router# show run
Router# show running-config | in fixed
cable load-balance fixed-primary-channel
```

動的ボンディング グループ設定の確認

DBG が作成されていることを確認するには、次のようにします。

show cable modem wideband channel コマンドを使用して、モデムのプライマリ ワイドバンド インターフェイスを確認します。

```
Router# show cable modem 4800.33ee.ebee wideband channel
MAC Address         IP Address         I/F          MAC        DSxUS     Primary
                                                    State                WB
4800.33ee.ebee      30.132.15.246      C3/0/1/UB    w-online   32x2      Wi3/0/1:3
Router# scm 4800.33ee.ebee ver
```

show cable modem verbose | in DS Tuner コマンドを使用して、モデムのダウンストリーム チューナ機能を確認します。

```
Router# show cable modem 4800.33ee.ebee verbose | in DS Tuner
DS Tuner Capability : 32
```

show cable mac-domain rcc コマンドを使用して、関連する RCC を確認します。

```
Router# show cable mac-domain c3/0/1 rcc
RCC-ID   RCP             RCs  MD-DS-SG  CMs  WB/RCC-TMPL       D3.0    D3.1
32 00 00 00 00 00  8    0         11   WB (Wi3/0/1:1)    Y       Y
33 00 00 00 00 00  32   0         6    WB (Wi3/0/1:3)    Y       Y
34 00 00 00 00 00  8    0         7    WB (Wi3/0/1:2)    Y Y
35 00 00 00 00 00  8    0         7    WB (Wi3/0/1:4)    Y Y
36 00 00 00 00 00  8    0         7    WB (Wi3/0/1:5)    Y Y
```

次の例に示すように **show cable dynamic-bonding-group summary** コマンドを使用して、動的に作成されたボンディング グループを確認します。

```
Router# show cable dynamic-bonding-group summary
Dynamic bonding group: Enable
BG ID BG Name   BG Size CMs ServFlows Create Time         Create Client       BG State
RFid list
24834 Wi3/0/1:1 8       11  11        Sep 14 14:36:35.194 MODEM_ONLINE        OPERATIONAL
24832-24839
24836 Wi3/0/1:3 32      6    6        Sep 14 14:43:24.144 MODEM_ONLINE        OPERATIONAL
24832-24863
24835 Wi3/0/1:2 8       7    7        Sep 14 17:20:37.115 MODEM_ONLINE        OPERATIONAL
24840-24847
24837 Wi3/0/1:4 8       7    7        Sep 14 17:21:37.723 STATIC_LOAD_BALANCE OPERATIONAL
24856-24863
24838 Wi3/0/1:5 8       7    7        Sep 14 17:21:39.761 STATIC_LOAD_BALANCE OPERATIONAL
24848-24855
```

表 *54*：動的ボンディング グループのステータス

CREATE_WAITING_SUP	ライン カードがDBGの作成要求を送信し、SUPによりボンディング グループが作成されるのを待機します。
HOLD	SUP により DBG が作成されたか、またはボンディング グループが回収されて使用可能な状態に復帰しています。
OPERATIONAL	HOLD 状態がタイムアウトになった後、ボンディング グループでモデムが使用されている場合、DBG状態はOPERATIONALに変化します。
RECLAIM_HOLD	回収可能な状態。 ボンディング グループでモデムが1つも使用されていないか、2 分間にわたり回収状態に一致すると、ボンディングボンディング グループが回収されます。DBG 状態が RECLAIM_HOLD に変化します。
RECLAIM_MODEM_MOVING	回収可能な状態。 モデムはボンディング グループの外に移動されます。
RECLAIM_WAITING_SUP	ライン カードが DBG 回収要求を送信し、SUP により BG が回収されるのを待機します。

動的ボンディング グループの詳細なチャネル リスト情報を表示するには、**show derived-config interface wideband** コマンドを使用します。

```
Router# show derived-config interface wideband-Cable 3/0/1:1
Building configuration...
Derived configuration: 113 bytes
!
interface Wideband-Cable3/0/1:1
  cable bundle 255
  cable rf-channels channel-list 0-7 bandwidth-percent 1
end
```

ボンディング グループ リソースの使用状況を確認するには、**show cable dynamic-bonding-group quota summary | slot | controller** コマンドを使用します。

```
Router# show cable dynamic-bonding-group quota controller 3/0/1
slot/subslot/ctrlr: 3/0/1
Total BG number: 128
Used BG number (static/dynamic): 6(1/5) Available BG number: 122
Available BG list port: 0, 6-29, 31-127
```

（注） 1 つのコントローラで 128 個の BG を設定できますが、CLC ごとにサポートされる BG は 896 個のみです。すべてのコントローラが 896 個の BG リソースを共有します。

回収されたボンディング グループを確認するには、**show cable dynamic-bonding-group reclaim-history summary** コマンドを使用します。

```
Router# show cable dynamic-bonding-group reclaim-history summary
BG ID BG Name   BG Size Create Time     Create Client Reclaim Time    Reclaim Client RFid
list
24835 Wi3/0/1:2 16      Sep 14 14:40:27 MODEM_ONLINE  Sep 14 14:44:27 DBG_INTERNAL
24832-2484
```

静的ロード バランシング設定の確認

静的ロード バランシングが設定されているかどうかを確認するには、次のようにします。

すべてのプライマリ チャネルの負荷を確認するために、**show cable load-balance docsis-group fn 1 md cable load | in In** コマンドを使用します。

```
Router# show cable load-balance docsis-group fn 1 md c3/0/1 load | in In
Interface           State   Group      Utilization Rsvd NBCM WB/UB Weight
In3/0/1:0(573 MHz)  initial 2147557888 0%(0%/0%)   0%   0    17    37
In3/0/1:4(597 MHz)  initial 2147557888 0%(0%/0%)   0%   0    17    37
In3/0/1:8(621 MHz)  initial 2147557888 0%(0%/0%)   0%   0    13    37
In3/0/1:12(645 MHz) initial 2147557888 0%(0%/0%)   0%   0    13    37
In3/0/1:16(669 MHz) initial 2147557888 0%(0%/0%)   0%   0    13    37
In3/0/1:20(693 MHz) initial 2147557888 0%(0%/0%)   0%   0    13    37
In3/0/1:24(717 MHz) initial 2147557888 0%(0%/0%)   0%   0    13    37
In3/0/1:28(741 MHz) initial 2147557888 0%(0%/0%)   0%   0    13    37
```

このコマンドの出力にすべてのプライマリ チャネルが一覧表示され、それらのチャネルで使用しているケーブル モデムの数が示されます。NBCM はチャネルで使用しているナロー バンド モデムの数、WBCM（WB/UB）はチャネルで使用しているワイドバンド モデムの数です。WBCM 合計数が、すべてのチャネルで均等に分散されているはずです。

任意の 2 つのチャネル間の WBCM 合計数の違いは、負荷の最小しきい値以下になります。デフォルトでは、負荷の最小しきい値は 5 です。

すべてのRFチャネルの負荷を確認するには、**show cable load-balance docsis-group fn 1 md rfch-util** コマンドを使用します。

```
Router# show cable load-balance docsis-group fn 1 md c3/0/1 rfch-util
Interface  Pstate Pending-In Pending-Out Throughput(Kbps) Util NBCM WBCM
In3/0/1:0  up     No         No          0                0%   0    17
In3/0/1:1  NA     No         No          0                0%   0    17
In3/0/1:2  NA     No         No          0                0%   0    17
In3/0/1:3  NA     No         No          0                0%   0    17
In3/0/1:4  up     No         No          0                0%   0    17
In3/0/1:5  NA     No         No          0                0%   0    17
In3/0/1:6  NA     No         No          0                0%   0    17
In3/0/1:7  NA     No         No          0                0%   0    17
In3/0/1:8  up     No         No          0                0%   0    13
In3/0/1:9  NA     No         No          0                0%   0    13
In3/0/1:10 NA     No         No          0                0%   0    13
In3/0/1:11 NA     No         No          0                0%   0    13
In3/0/1:12 up     No         No          0                0%   0    13
In3/0/1:13 NA     No         No          0                0%   0    13
In3/0/1:14 NA     No         No          0                0%   0    13
In3/0/1:15 NA     No         No          0                0%   0    13
…….
Average: 0.0
Variance: 0.0
```

このコマンドにより、プライマリチャネルとセカンダリチャネルの負荷に関する情報が一覧表示されます。WBCMは、チャネルで使用されているワイドバンドモデムの数です。

ロードバランシングでのケーブルモデムの内部状態を確認するには、**show cable load-balance docsis-group fn 1 md modem-list wideband** コマンドを使用します。

```
Router# show cable load-balance docsis-group fn 1 md c3/0/1 modem-list wideband
Codes: M - Multicast, U - UGS, P - PCMM, F - Max-Failures, X - eXcluded
       L - L2vpn, R - RSVP, S - DS-Resiliency
Primary WB   MAC Address           Primary DS   RCC-ID  Priority        MUPFXLRS State
Wi3/0/1:0    (3)
             c8fb.2631.0e56        In3/0/1:20   41      0        ------ LB_CM_HOLD_EXPIRE_IN
 36
             c8fb.26a6.c3dc        In3/0/1:16   41      0        ------ LB_CM_HOLD_EXPIRE_IN
 37
             c8fb.2631.0d7e        In3/0/1:16   41      0        ------ LB_CM_HOLD_EXPIRE_IN
 43
Wi3/0/1:1 (9)
             c8fb.2631.0c80         In3/0/1:0    32      0        ------ LB_CM_STATIC_MOVING
             c8fb.2631.0cae         In3/0/1:0    32      0        ------ LB_CM_STATIC_READY
             c8fb.2631.0db0         In3/0/1:24   42      0        ------ LB_CM_STATIC_MOVING
             c8fb.2631.0c10         In3/0/1:28   42      0        ------ LB_CM_STATIC_MOVING
             c8fb.2631.0d80         In3/0/1:16   41      0        ------ LB_CM_STATIC_MOVING
             c8fb.2631.0d26         In3/0/1:24   41      0        ------ LB_CM_STATIC_MOVING
             a4a2.4a2d.b4aa         In3/0/1:20   41      0        ------ LB_CM_STATIC_MOVING
             c8fb.2631.0e5c         In3/0/1:0    32      0        ------ LB_CM_STATIC_MOVING
             c8fb.2631.0cb0         In3/0/1:0    32      0        ------ LB_CM_STATIC_MOVING
Wi3/0/1:2 (3)
             c8fb.2631.0d2a        In3/0/1:12   34      0        ------ LB_CM_HOLD_EXPIRE_IN
 27
             c8fb.2631.0e5a         In3/0/1:12   34      0        ------ LB_CM_STATIC_MOVING
             c8fb.2631.0bfe         In3/0/1:8    34      0        ------ LB_CM_STATIC_MOVING
Wi3/0/1:3 (2)
             4800.33ea.54be         In3/0/1:28   33      0        ------ LB_CM_DYNAMIC_READY
```

```
            4800.33ee.ebe6         In3/0/1:20   33      0        ------ LB_CM_HOLD_EXPIRE_IN
 1
Wi3/0/1:4 (2)
            c8fb.2631.0e44         In3/0/1:24   42      0        ------ LB_CM_HOLD_EXPIRE_IN
 40
            c8fb.2631.0a44         In3/0/1:28   42      0        ------ LB_CM_HOLD_EXPIRE_IN
 42
```

表 *55*：ケーブル モデムの状態

CM の状態	説明
LB_CM_STATIC_READY	モデムは静的ロードバランシングによる移動に対応できる状態です。
LB_CM_STATIC_MOVING	モデムの移動が静的 LB によってトリガーされて進行中です。
LB_CM_HOLD_EXPIRE_IN	モデムは次の移動に備えて保留中です。デフォルトの保留時間は 600 秒です。
LB_CM_DYANMIC_READY	モデムは動的ロードバランシングによる移動に対応できる状態です。
LB_CM_DYANMIC_MOVING	モデムの移動が動的 LB によってトリガーされて進行中です。
LB_CM_DISABLED	モデムは移動に対応できません。モデムの移動失敗カウントが max-failure しきい値に達すると、以降の移動を避けるためにモデムが LB_CM_DISABLED に設定されます。

動的ロード バランシング設定の確認

すべての RF チャネルの使用状況を確認するには、**show cable load-balance docsis-group fn 320 md rfch-util** コマンドを使用します。

```
Router# show cable load-balance docsis-group fn 320 md c3/0/0 rfch-util
Interface Pstate   Pending-In   Pending-Out   Throughput(Kbps) Util   NBCM   WBCM
Do3/0/0:0  up      No           No            11754            31%    0      308
Do3/0/0:1  up      No           No            11754            31%    0      296
Do3/0/0:2  up      No           No            11754            31%    0      333
Do3/0/0:3  up      No           No            11754            31%    0      296
Do3/0/0:4  up      No           No            11754            31%    0      297
Do3/0/0:5  up      No           No            11754            31%    0      331
Do3/0/0:6  up      No           No            11754            31%    0      299
Do3/0/0:7  up      No           No            11753            31%    0      268
Do3/0/0:8  up      No           No            11754            31%    0      302
Do3/0/0:9  up      No           No            11754            31%    0      331
Do3/0/0:10 up      No           No            11753            31%    0      308
Do3/0/0:11 up      No           No            11754            31%    0      305
Do3/0/0:12 NA      No           No            12862            34%    0      258
Do3/0/0:13 NA      No           No            12862            34%    0      258
Do3/0/0:14 NA      No           No            12862            34%    0      258
```

```
…….
Average: 30.416
Variance: 1.701
```

任意の 2 つの RF チャネルの使用率の差が負荷しきい値を下回っている場合、すべての RF チャネル間のトラフィックは平衡化されていると見なされます。負荷しきい値のデフォルト値は10% です。

送信元ボンディング グループごとの潜在的ターゲット ボンディング グループを確認するには、**show cable load-balance docsis-group fn md cable target dbg** および **show cable load-balance docsis-group fn md** target wide コマンドを使用します。

```
Router# show cable load-balance docsis-group fn 320 md c3/0/0 target dbg
Interface    Bg-Id     Size     Group         Target
Wi3/0/0:0    24577     4        2147557695
Wi3/0/0:3    24580     4        2147557695
Wi3/0/0:4    24581     8        2147557695
Wi3/0/0:5    24582     8        2147557695
Wi3/0/0:6    24583     24       2147557695    33% [24576, 24584-24587, 24589-24607]
Wi3/0/0:7    24584     16       2147557695    30% [24576, 24586-24587, 24595-24607]
Wi3/0/0:8    24585     16       2147557695
Wi3/0/0:9    24586     32       2147557695
Wi3/0/0:10   24587     24       2147557695    33% [24576, 24584-24587, 24589-24607]
Wi3/0/0:11   24588     8        2147557695
Wi3/0/0:12   24589     8        2147557695    27% [24596-24603]
Wi3/0/0:13   24590     8        2147557695
Wi3/0/0:14   24591     4        2147557695

Router# show cable load-balance docsis-group fn 5 md c1/0/4 target wide
Interface     Bg-Id     State     Group         Target
Wi1/0/4:2     9219      up        2147510276    Wi1/0/4:4
Wi1/0/4:3     9220      up        2147510276
Wi1/0/4:4     9221      up        2147510276
```

ターゲット ボンディング グループが 1 つも表示されない場合、RF チャネル間のトラフィックを平衡化するためのボンディング グループは作成されません。

次に、しきい値が 14% に設定された DOCSIS 3.1 モデムでの出力例を示します。DOCSIS 3.1 モデム上で使用率ベースのロード バランシングが開始するには、OFDM チャネルが 100% 使用され、しかもトラフィックがSC-QAM上を流れている必要があります。使用率ベースのロードバランシングでは、D31 モデムの SC-QAM チャネル上のトラフィック フローが平衡化されます。

```
Router# show cable load-balance docsis-group fn 5 md c1/0/4 rfch-util
Interface   Pstate Pending-In Pending-Out Throughput(Kbps) Util NBCM WBCM
In1/0/4:0   up     No         No          10632            28%  0    45
In1/0/4:1   NA     No         No          11226            29%  0    41
In1/0/4:2   NA     No         No          11225            29%  0    41
In1/0/4:3   NA     No         No          11225            29%  0    41
In1/0/4:4   down   No         No          11225            29%  0    41
In1/0/4:5   down   No         No          11225            29%  0    41
In1/0/4:6   down   No         No          11225            29%  0    41
In1/0/4:7   down   No         No          11225            29%  0    41
In1/0/4:8   up     No         No          10620            28%  0    43
....
....
In1/0/4:35   NA    No         No          6646             17%  0    6
In1/0/4:36   NA    No         No          6646             17%  0    6
In1/0/4:37   NA    No         No          6647             17%  0    6
In1/0/4:38   NA    No         No          6646             17%  0    6
In1/0/4:39   NA    No         No          6647             17%  0    6
In1/0/4:40   up    No         No          6088             16%  0    6
In1/0/4:41   NA    No         No          6648             17%  0    6
In1/0/4:42   NA    No         No          6647             17%  0    6
In1/0/4:43   NA    No         No          6647             17%  0    6
In1/0/4:44   NA    No         No          6646             17%  0    6
In1/0/4:45   NA    No         No          6646             17%  0    6
In1/0/4:46   NA    No         No          6647             17%  0    6
```

```
In1/0/4:47   NA    No          No          6648             17%  0    6
In1/0/4:48   NA    No          No          6648             17%  0    6
In1/0/4:49   NA    No          No          6648             17%  0    6
In1/0/4:50   NA    No          No          6646             17%  0    6
In1/0/4:51   NA    No          No          6648             17%  0    6
In1/0/4:52   NA    No          No          6647             17%  0    6
In1/0/4:53   NA    No          No          6648             17%  0    6
In1/0/4:54   NA    No          No          6647             17%  0    6
In1/0/4:55   NA    No          No          6648             17%  0    6
In1/0/4:56   NA    No          No          6647             17%  0    6
In1/0/4:57   NA    No          No          6647             17%  0    6
In1/0/4:58   NA    No          No          6646             17%  0    6
In1/0/4:59   NA    No          No          6645             17%  0    6
In1/0/4:60   NA    No          No          6646             17%  0    6
In1/0/4:61   NA    No          No          6646             17%  0    6
In1/0/4:62   NA    No          No          6647             17%  0    6
In1/0/4:63   NA    No          No          6647             17%  0    6
In1/0/4:159  NA    No          No          1819685          100% 0    47
```

動的ボンディング グループに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャセット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *56*：動的ボンディング グループについての機能情報

機能名	リリース	機能情報
動的ボンディング グループ	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに追加されました。

第 20 章

スペクトル管理と高度なスペクトル管理

この章では、Cisco ケーブル モデム終端システム（CMTS）ルータでサポートされるスペクトル管理機能について説明します。スペクトル管理サポートは、次の 2 つのグループに分けられます。

- ガイド型およびスケジュール型スペクトル管理機能（ソフトウェアでサポートされます）
- インテリジェント型および高度なスペクトル管理機能（ハードウェアの特定のケーブル インターフェイス上でのみサポートされます）

機能情報の確認

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載され

ている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *57* : ***Cisco cBR*** シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

スペクトル管理の前提条件

ネットワークで信頼性の高いブロードバンド データ伝送をサポートするように設計されていることを確認します。使用するネットワークには、少なくとも以下の要素が必要です。

- ケーブル モデムに IP アドレスを割り当てる Dynamic Host Configuration Protocol（DHCP）サーバまたは光同軸ハイブリッド（HFC）ネットワーク上のセットトップ ボックス。これは、DHCP サーバとして機能するように設定された Cisco CMTS ルータです。
- アップコンバータが搭載されたケーブル インターフェイス ライン カードを使用していない場合は、Cisco CMTS ルータとコンバイナの間に IF/RF 外部アップコンバータを取り付ける必要があります。

（注） 「コンバイナ」とは、Cisco CMTS ルータと HFC ネットワークを接続するヘッドエンドまたはケーブル分配装置にあるすべてのケーブル、増幅器、タップを指します。

- ルータのケーブル モデムとケーブル インターフェイス カード間のダウンストリーム RF パスに取り付けられたダイプレックス フィルタ。最大ブレード（60% + 40% ブレード）を利用でき、ダブル フォイルで、このケーブルに適正なコネクタを使用した RG-59 ヘッドエンド同軸ケーブル。
- アマチュア無線周波数帯や短波周波数帯など、流合の問題が判明している周波数を避けます。
- 20 MHz 未満の不適切なスペクトルを避けます。
- チャネル プランを作成するときには、周波数ホッピングのための予備の帯域を確保します。
- 受信電力レベルの設定によって、多少の等化調整を行います。
- CATV 技術の性質上、アップストリームの雑音管理が重要な問題です。『NCTA Supplement on Upstream Transport Issues』（National Cable and Telecommunications Association（https://www.ncta.com）から入手可能）に記載されている厳格な北米プラント メンテナンス手順に従って、リターンの増幅器およびレーザーを調整することを推奨します。

スペクトル管理の制約事項

この項では、次のスペクトル管理機能に関する制約事項について説明します。

共有スペクトル グループ

- 拡張スペクトル管理は、ライン カード間の共有スペクトル グループをサポートしません。
- ガイド型スペクトル管理は、ライン カード間の共有スペクトル グループをサポートします。

アップストリームの動的変調

- Cisco CMTS ルータには、事前設定された（プライマリ）変調プロファイルが 1 つあります。このプロファイルは 4 位相偏移変調（QPSK）変調の一般的なプロファイルを定義します。アップストリームの動的変調機能を使用するには、事前設定されたプロファイルより高位の変調方式を持つセカンダリ変調プロファイルを作成する必要があります。3 段階の動的変調機能では、第 3 の変調プロファイルを作成して使用することができます。ただし、第 3 の変調プロファイルはオプションです。
- アップストリーム変調プロファイルは、アップストリーム ポートに割り当てられ、そのアップストリーム ポート上のすべてのケーブル モデムに影響します。
- 変調プロファイルは、ケーブル ネットワークの物理層に影響します。つまり、Data-over-Cable Service Interface Specifications（DOCSIS）仕様を熟知した経験豊富な技術者だけが変調プロファイルを作成してください。
- Voice over IP（VoIP）サービスでアップストリームの動的変調機能を使用するときは、アップストリーム変調またはチャネル幅が頻繁に変更されると、音声コールの品質に短時間の影響を与える可能性があります。

高度なスペクトル管理による固定周波数スペクトル グループ

固定周波数スペクトル グループを設定するには、次を実行します。

```
Router(config)#controller upstream-cable 9/0/15
Router(config-controller)#us-channel 0 spectrum-group n
Router(config-controller)#us-channel 0 channel-width 1600000
```

PacketCable VoIP コールのアップストリーム変調パラメータの制限事項

PacketCable の動作および VoIP コールのアップストリームを設定する際は、1.6Mhz、3.2Mhz、または 6.4Mhz のチャネル幅を使用することを推奨します（DOCSIS チャネル幅とアップストリーム パラメータの全組み合わせは、サポートされてはいますが、VoIP の使用時には最適でありません）。

N+1 冗長性のサポート

N+1 冗長性は、現用および保護ケーブル インターフェイス ラインカードが同一であることを必要とします。これにより、保護インターフェイスと現用インターフェイスが同一の適切な設定をサポートすることが保証されます。

インテリジェント型および高度なスペクトル管理をサポートするカードを保護する際、スイッチオーバーはスペクトル管理の設定を保存し、保護インターフェイスはまず現用インターフェイスと同じアップストリーム周波数を使用します。システムが安定して不要な周波数ホッピングやチャネル幅変更が起きなくなるまでは、高度なスペクトル管理機能を使用する保護インターフェイスは開始されません。

インテリジェント型および高度なスペクトル管理のサポート

- ケーブル インターフェイスは標準 DOCSIS、EuroDOCSIS、および拡張された日本の周波数範囲（アップストリーム インターフェイスの場合 5 ～ 85 MHz）を使用して、インテリジェント型および高度なスペクトル管理機能をサポートします。
- インテリジェント型および高度なスペクトル管理機能は、DOCSIS 1.0 および DOCSIS 1.1 Time Division Multiple Access（TDMA）モードの動作でのみサポートされます。これらの機能は、ケーブル インターフェイスが DOCSIS 2.0 混合、Advanced TDMA（A-TDMA）、Synchronous Code Division Multiple Access（S-CDMA）モードで動作している場合は使用できません。同様に、これらの機能は、ケーブルインターフェイスが複数の論理チャネルを使用するよう設定されている場合、使用できません。ただし、これらの制限は、ガイド型スペクトル管理には適用されません。
- アップストリーム チャネルは、DOCSIS 仕様で規定された搬送波対ノイズ＋干渉比（CNiR [CNR]）および搬送波対イングレス パワー比の値と一致している必要があります。どちらのパラメータも、最小値は 5 ～ 65 MHz の周波数範囲で 25 dB です。
- インテリジェント型および高度なスペクトル管理機能は、ラインカード間の共有スペクトル グループをサポートしません。スペクトル管理機能には、異なるライン カードのアップストリーム ポートに独自の RF ドメイン（オーバーラップしない一意の周波数セット）が必要です。
- N+1 の冗長構成は、高度なスペクトル管理では通常、標準の構成ですが、スペクトル グループが定義されているケーブル インターフェイス ラインカードではサポートされません。
- インテリジェント型および高度なスペクトル管理機能は、組み込みのスペクトル アナライザを使用してスペクトル グループをカードに割り当てることによって起動します。

スペクトル管理の情報

スペクトル管理は、シスコ ケーブル モデム終端システム（CMTS）が、アップストリーム設備障害を検知し、それを管理エンティティに報告し、可能な限り自動的に修正できます。スペクトル機能は、スループット低下や遅延はなく、また無線周波数（RF）設備でパケット オーバーヘッドをさらに生じることなく、これらの機能を実行します。

特に、ルータのケーブルインターフェイスはアップストリームパケットを受信するため、アップストリーム伝送エラーを直接検出します。ルータは、「フラッピング」しているケーブル モデム（ステーション メンテナンス メッセージをミスしたモデムや、オフラインになってからオンラインに復帰したモデム）の数と周波数など、モデムの状態変化の記録を保持することで設備の状態を間接的にモニタすることもできます。

（注） ケーブル モデム フラッピングの詳細とケーブル モデム フラップ リストのモニタリング方法については、「Flap List Troubleshooting for the Cisco CMTS Routers」を参照してください。

スペクトル管理は、ケーブル設備のアップストリーム ノイズ障害による長期的なサービスの中断を防ぐことができます。また、ケーブル ネットワークの障害管理やトラブルシューティングに使用されます。ケーブルモデムがフラップディテクタによってオンラインやオフラインになったことが検出されると、ケーブル オペレータはフラップ リストとスペクトル テーブルを調べて、考えられる原因を判断できます。

ケーブルテレビ（CATV）技術の性質上、アップストリームの雑音管理が重要な問題です。QPSK および直交振幅変調（QAM）のデータの伝送をサポートするには、周波数帯域に十分な CNR（CNiR）および搬送波対イングレス パワー比が必要です。DOCSIS では、どちらの比にも 5 ～ 65 MHz の周波数範囲で 25 dB の最小値を設定します。ノイズのせいで CNR（CNiR）が特定のチャネルで 25 dB を下回ると、そのチャネルのケーブルモデムが低下し、光同軸ハイブリッド（HFC）ネットワークが悪化することがあります。

この概要の構成は、次のとおりです。

- スペクトル管理測定値, （418 ページ）：スペクトル管理で使用する基本的な概念と用語の概要を示します。
- アップストリーム信号チャネルの概要, （423 ページ）：信号を送信する方法、およびアップストリーム チャネルで変更が発生する方法を説明します。
- アップストリーム セグメントとコンバイナ グループ, （424 ページ）：スパースおよびデンス セグメント、およびコンバイナ グループについて説明します。
- 周波数管理ポリシー, （425 ページ）：ノイズ障害の種類、およびスペクトル グループと周波数ホッピングでイングレス ノイズに対処する方法を説明します。
- ガイド型およびスケジュール型スペクトル管理, （428 ページ）：ガイド型およびスケジュール型スペクトル管理機能の周波数ホッピング機能、アップストリームの動的変調（信号対雑音比ベース）、および入力レベルについて説明します。
- インテリジェント型および高度なハードウェアベースのスペクトル管理, （433 ページ）：オンボード スペクトル管理ハードウェアを搭載する多数のケーブル インターフェイス ライン カードでサポートされるスペクトル管理機能について説明します。このような機能には、リアルタイム スペクトル アナライザ、CNR ベースのプロアクティブな周波数ホッピング、堅牢なアップストリームの動的変調などが含まれます。
- 利点, （434 ページ）：Cisco CMTS ルータ プラットフォームで提供されるさまざまなスペクトル管理機能について説明します。

スペクトル管理測定値

ダウンストリームまたはアップストリーム信号の品質を決定するには、主に信号対雑音比（SNR（MER））と搬送波対雑音比（CNR（CNiR））を測定します。ここでは、これら 2 つの測定比について相違点を含めて説明します。また、役に立つと思われるその他の値についても説明します。

信号と搬送波の雑音比

変調誤差比（MER（SNR））およびダウンストリームまたはアップストリームの CNR（CNiR）を測定することは、信号の品質を判断し、誤差を修正するためにスペクトル管理を実行する必要があるかどうかを決定するための最初の手順となります。これらの 2 つの値について、以下で簡単に説明します。

- 変調誤差比（MER（SNR））：イングレス ノイズ キャンセルが実行された後のアップストリーム上の信号強度を評価します。つまり、MER（SNR）は、周波数応答の歪み（チャネル内の振幅の傾き、リップルなど）、グループ遅延、マイクロリフレクション、位相ノイズなど、さまざまな変調障害を考慮します。MER（SNR）は、トランスミッタ回路、レシーバ回路、伝送メディアがアップストリーム信号に及ぼす影響を含むため、ケーブル ネットワーク全体のエンドツーエンド品質の適切な尺度となります。
- 搬送波対雑音比（CNR）：アップストリーム上で（イングレス ノイズ キャンセルが実行される前に）測定された変調電力（単位：dB）のチャネル電力対ノイズ電力の比です。

  用語 CNiR は CableLabs の用語で CNR 測定を表します。したがって、これら 2 つの用語、CNR と CNiR は同じ意味で使用されます。

  CNR（CNiR）測定は、通常は外部スペクトル アナライザでのみ提供されますが、インテリジェントで高度なハードウェア スペクトル管理機能をサポートするケーブル インターフェイス ラインカードも CNR（CNiR）測定を提供します。

  Cisco CMTS では、次の 2 つのタイプの CNR（CNiR）測定がサポートされます。

  - 特定のアップストリームを測定対象とする CNR（CNiR）：1 つのアップストリーム上にある全ケーブル モデムを対象とする全体的な CNiR（CNR）です。ケーブル インターフェイスでアップストリーム レシーバの RF 出力を測定することによって決定されます。この値は常に、特定のアップストリームの特定の時点のみにおけるスナップショットです。ケーブル インターフェイスはケーブル モデムでバーストが予測されない特定の時点の RF 出力を測定しますが、信号問題を抱えているかまたは生成している少数のケーブル モデムが原因で、偏りが発生する可能性があります。
  - モデムごとの CNiR（CNR）：特定のケーブル モデムを対象とする CNR（CNiR）です。ケーブル インターフェイスのアップストリーム レシーバにあるモデムのバースト伝送の信号強度です。モデムごとの CNiR（CNR）測定は、特定のケーブル モデムの信号をきわめて正確に測定する測定手段ですが、1 つのモデムの CNR（CNiR）を使用してアップストリーム上の他のケーブルモデムまたはアップストリーム自体について想定することはできません。ただし、代表的な期間中の複数のケーブル モデムの CNR（CNiR）をポーリングすることで、アップストリームの信号品質を大まかに把握することができます。

ヒント　チャネル幅の変更は、CNR（CNiR）に直接影響を及ぼします。チャネル幅を 2 倍（たとえば 400 KHz から 800 KHz）にすると、アップストリームの CNR（CNiR）は約 3 dB 低下します。チャネル幅を半分（たとえば 3.2 MHz から 1.6 MHz）に減らすと、アップストリームの CNR（CNiR）は約 3 dB 上昇します。

MER（SNR）値と CNR（CNiR）値の違い

唯一の障害が加法性白色ガウス雑音（AWGN）であるテストラボのような完全なネットワークでは、CNR（CNiR）および MER（SNR）値が、許容できる電力レベルと周波数範囲のすべてと同等であることが期待できます。しかし、ライブネットワークでは、CNR（CNiR）電力測定によって考慮されないノイズ障害および歪みを考慮するため、MER（SNR）値は CNR（CNiR）値よりも数 dB 分低くなることが予想されます。

一般に、CNR（CNiR）値が 15 ～ 25 dB の範囲内である場合、MER（SNR）値が同程度の値になることが想定されます。MER（SNR）と CNR（CNiR）値の差は、CNR（CNiR）値が 15 ～ 25 dB の範囲外になると、より大きくなることが予想されます。

次の表に、MER（SNR）と CNR（CNiR）値の比較、およびライブ トラフィックが通過するアクティブ ネットワークで MER（SNR）および CNR（CNiR）値が異なる可能性がある主な理由を示します。

表 *58*：*DOCSIS* ケーブル ネットワークの *MER*（*SNR*）と *CNR*（*CNiR*）の比較

信号対雑音比（SNR）	搬送波対雑音比（CNR）
RF 信号の検出後測定値。	RF 信号の検出前測定値。
ベースバンド ドメインの測定値。	RF 周波数領域の測定値。

信号対雑音比（SNR）	搬送波対雑音比（CNR）
信号の信号歪みと障害の影響が含まれます。次の作業を行います。 • チャネルのグループ遅延（たとえばダイプレクサ帯域エッジ近くでの運用中に発生）。 • チャネルの振幅変動とエコー。 • データの衝突。 • マイクロリフレクション。 • チャネルのナロー バンド 入力。 • ケーブル設備の非直線性。 • 位相ノイズ。 • プリアンブルの誤選択。 • ケーブル モデムの伝送における低シンボル忠実度（MER（SNR）値は適切）。 • 回復不能なキャリアのオフセット。 • 回復不能なシンボル タイミング オフセット。	RF 変調キャリア電力とノイズ電力の比を測定します。
全体的なエンドツーエンド ネットワーク品質（トランスミッタ、レシーバ、および伝送メディアが信号に対して実行している処理）の指標を提供します。	ネットワーク パフォーマンス（伝送メディアまたはネットワークが信号に対して実行している処理）の指標を提供します。
現在のデータ トラフィック パターンにおける一定期間の平均。信号品質の長期傾向を追跡するときに便利です。	リアルタイム スペクトラム解析。
値の一部としてCNR（CNiR）値を反映します。	値の一部として MER（SNR）値を反映しません。
10,000 シンボル分で平均され、正確な読み取りには短期および長期認可が転送されている必要があります。	伝送されているトラフィックのタイプの影響は受けません。
値を決定するために、修正不可能FECエラーのあるパケットは使用しません。したがって、修正不可能エラーのバーストにより、MER（SNR）値が誤って高くなることがあります。	修正不可能FECパケットのバーストの影響は受けません。

信号対雑音比（SNR）	搬送波対雑音比（CNR）
DOCSIS 仕様では、アップストリームとダウンストリームの必須MER（SNR）値が定義されていません。	6 MHz 帯で 35 dB の最小ダウンストリーム CNR（8 MHz 帯では DOCSIS 2.0 で 44 dB） 25 dB の最小アップストリーム CNR（CNiR）。

その他の測定値

MER（SNR）および CNR（CNiR）値に加えて、以下の信号品質インジケータを認識しモニタする必要があります。

- MER：これは RF 信号品質の尺度（dB 単位）です。SNR に相当し、加法性白色ガウス雑音（AWGN）劣化下の CNR（CNiR）に似ています。ただし、MER にはアナログからデジタルへの変換、デジタルからアナログへの変換、丸め誤差、歪み、信号障害（位相ノイズ、グループ遅延、ジッターなど）など信号に影響を与える追加要因が含まれているため、MER はデータ ネットワークで優先されます。そのため DOCSIS 2.0 RF 仕様では、信号の最小 MER 値要件を追加することで、既存の CNR（CNiR）最小要件を補っています。

  アップストリームの MER 値を計算する簡単な方法は、次のとおりです。

  ```
  MER = 20 x log (RMS error magnitude / Average symbol magnitude)
  ```

  アップストリームでのノイズの割合としてあらわされる同等値を探すために、エラーベクトル変調（EVM）も計算できます。

  ```
  EVM = Average error magnitude / Max symbol magnitude * 100
  ```

  MER 値の計算方法と使用方法の詳細については、DOCSIS 2.0 の仕様を参照してください。

- FEC カウンタ：アップストリームで修正可能および修正不可能な FEC エラーが発生する回数を追跡するカウンタです。FEC エラー カウンタは、インパルス ノイズなど、通常は MER（SNR）または CNR（CNiR）値に反映されないファスト トランジェント（高速過渡現象）エラーを追跡するのに役立ちます。

  1% より大きい訂正可能なエラー数は、物理設備またはケーブル モデムに起こりうる発展可能な問題を警告するサインとして使用できます。1% より大きい訂正不可能なエラー数は、アップストリームでトラフィックをブロックしている既存の問題を示している可能性があります。インテリジェント型および高度なスペクトル管理機能をサポートするケーブル インターフェイスのライン カードでは、ノイズ問題を修正するためにアップストリームで頻度を変更する必要があるかどうかを決定するために、モニタするインジケータの 1 つとして FEC カウンタを使用できます。

- マイクロリフレクション：受信者に到着する信号の追加コピー。通常は到着タイミングが異なり減衰量が異なるため、受信者は着信信号の実際の位相や振幅を誤認します。通常、マイクロリフレクションは物理的なケーブル設備におけるインピーダンスの不一致によって引き起こされ、天候などの理由で低下した設備、または正しく取り付けられなかった設備を示す可能性があります。

アップストリーム信号チャネルの概要

アップストリーム チャネルは、CMTS に対して送信する多数のケーブル モデムによって特徴付けられます。これらの信号は、バーストモードの伝送で動作します。アップストリームチャネルの時間はスロットで構成されます。CMTS はタイム スロットを提供し、各アップストリーム インターバルの使用を制御します。CMTS は、すべてのケーブル モデムに対して、アップストリーム チャネル記述子（UCD）メッセージを定期的にブロードキャストします。UCD メッセージには、アップストリーム チャネルに関連付けられたアップストリーム周波数および伝送パラメータが含まれます。これらのメッセージは、アップストリーム周波数、シンボル レートおよび変調方式、前方誤り訂正（FEC）パラメータ、他の物理層値などのアップストリーム チャネル特性を定義します。

シスコでは、すべての DOCSIS エラー訂正エンコーディング、変調タイプおよび変調フォーマットをサポートします。アップストリーム信号は、QPSK または QAM を使用して復調されます。QPSK が信号搬送波の位相で情報を伝達するのに対し、QAM は位相と振幅の両方を使用して情報を伝達します。

アップストリーム方向でデータを確実に送信するのは困難です。アップストリーム スペクトルはケーブル設備ごとに大きく異なるので、使用するケーブル プラントのリターン パスに基づいてアップストリームパラメータを選択してください。帯域幅の効率とアップストリームチャネルの堅牢性との間に最良のトレードオフが得られるよう、アップストリームプロファイルを選択またはカスタマイズします。たとえば、QAM-16 は、QPSK と同じビット エラー レートを達成するには約 7 dB 高い CNR（CNiR）が必要ですが、QPSK の 2 倍の速度で情報を伝送できます。

（注） 上記の仕様は事前定義された周波数セットに基づきますが、任意の時点で十分なCNR（CNiR）が得られる場合と得られない場合があります。

アップストリーム周波数は、次のように割り当てることができます。

- 固定：スペクトル グループを設定すると、固定アップストリーム周波数設定が無効になります。
- 単一のサブバンド：CMTS 管理者は、アップストリーム搬送波の境界がサブバンド内にとどまるように、中心周波数およびシンボルレートを定義できます。周波数およびシンボル レートは、定義されたアップストリームパラメータに基づいて雑音のある回線状態に応じて境界内で変更できます。
- 複数のサブバンド：データ搬送波は、一定期間、特定のサブバンドにとどまり、その後、定義されたアップストリーム パラメータに基づいて次のサブバンドにホッピングすることができます。

ヒント　周波数割り当ての初期選択およびセットアップの手順に、スペクトル アナライザによる雑音電力レベルの測定を組み込む必要があります。導入初期、少なくとも、増幅器カスケード調整または設備修復が、アップストリーム ポートに接続されたノードに大きな影響を与えなくなる程度の回数に減るまでは、固定周波数設定を使用することを推奨します。

アップストリーム周波数変化

DOCSIS の無線周波数インタフェース（RFI）仕様に示されているように、RF チャネル移動またはアップストリーム周波数変化は、UCD メッセージの変更が全ケーブル インターフェイスにブロードキャストされたときに発生します。

UCDメッセージによるチャネル移動の速度は、一般に、20ミリ秒（ms）未満です。この間、ケーブル インターフェイスのトランスミッタが新しい周波数に対して調整されるまで、アップストリーム伝送は中断されます。データは、この間ケーブル インターフェイスのバッファに保存され、周波数ホッピングが完了すると送信されます。

モデム単位のキープアライブ ポーリングを実行するには、ステーション メンテナンス インターバルを使用します。CMTS は最低でも 30 秒に 1 回、デフォルトで 20 秒に 1 回、各ケーブル モデムにポーリングを実行します。イングレス ノイズにより全ケーブルインターフェイスのうちの設定可能な一定の割合でキープアライブ メッセージの損失が発生すると、ポーリングは失敗となり、アロケーションテーブルから新しい周波数が選択され、UCDが更新されます。移動時間は、あらゆるアップストリーム UCD 更新で 2 ミリ秒です。UCD が更新されると、ホッピングが発生します。システムが次にUCDを変更するには、ホッピングしきい値の時間間隔が経過するまで待機する必要があります。

アップストリーム セグメントとコンバイナ グループ

Cisco ルータはケーブル設備をダウンストリーム チャネルに分割します。ダウンストリーム チャネルにはアップストリーム セグメントが含まれます。各アップストリーム セグメントは通常、1 つまたは複数のファイバ ノードに対応します。アップストリームセグメントは、次のいずれかとして定義されます。

- スパース セグメント：1 つのアップストリーム セグメントに 1 つのアップストリーム チャネルが 含まれます。
- デンス セグメント：1 つのアップストリーム セグメントに複数のアップストリーム チャネルが含まれ、周波数はそれぞれ異なります。

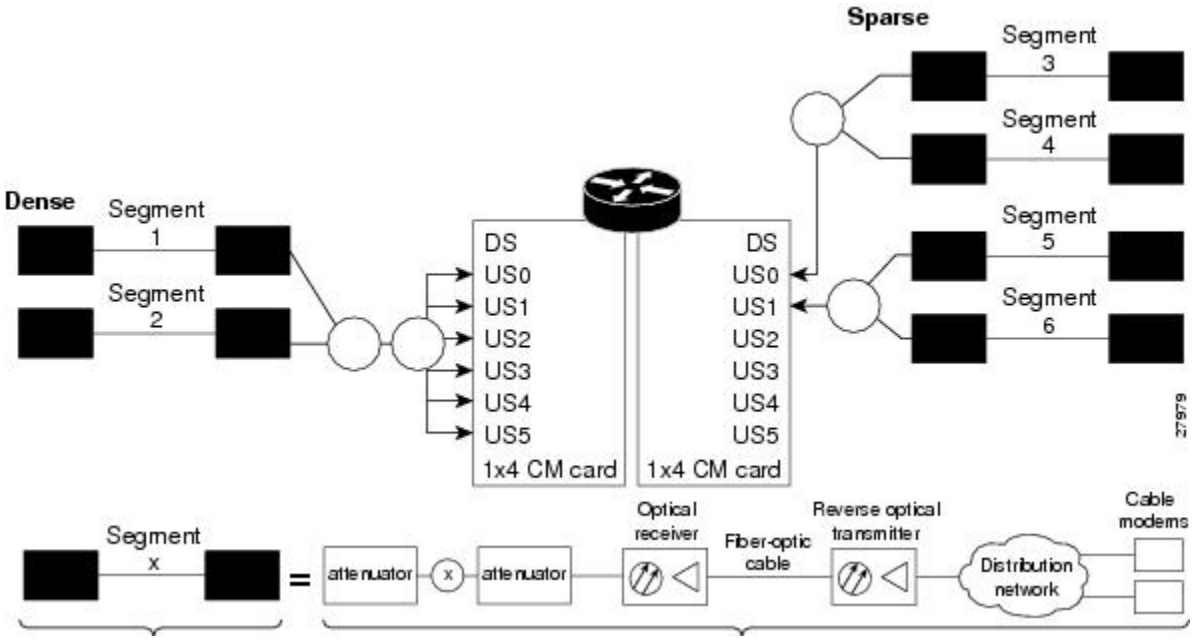
（注）　ケーブル インターフェイス ライン カードは、スパース セグメント、デンス セグメント、またはその両方をサポートできます。

スパース セグメントを定義すると、ケーブル オペレータは加入者の少ないファイバ ノード間でアップストリーム帯域幅を共有することができます。デンス セグメントを定義すると、ケーブル

オペレータは加入者の多いファイバ ノードにより多くのアップストリーム帯域幅を提供できます。

図に、スパース セグメントとデンス セグメントの違いを示します。

図 *17*：スパース セグメントおよびデンス セグメント



上の図に示すように、ダウンストリームセグメントには複数のアップストリームセグメントを含めることができます。2 つのファイバ ノードを 1 つのダウンストリーム セグメント内の異なるアップストリーム セグメントに配置することができます。

複数のファイバ ノードのリターン パスは、1 カ所で結合することによって、コンバイナ グループと呼ばれる単一 RF 周波数領域を形成できます。CMTS ソフトウェアによって、スペクトル グループと呼ばれる周波数ホッピング テーブルをコンバイナ グループに関連付けることができます。

（注） コンバイナ グループは、RF トポロジ ポイントを参照します。スペクトル グループはコンバイナ グループに関連付けられた周波数ホッピング テーブルを参照します。

周波数管理ポリシー

スペクトル管理では、共通の周波数管理ポリシーを一連のアップストリーム ポートに適用することで、そのデータがケーブル設備上で確実に配送されるようにします。ケーブル設備オペレータは、ノイズを測定し、ケーブル設備のスペクトル管理ポリシーを決定する必要があります。異なる変調方式、アップストリーム周波数技術、およびシンボル レートは、ケーブル設備特性およびシャーシのケーブル インターフェイス ライン カードに基づいて使用されます。

これらのトピックの詳細については、次のセクションを参照してください。

ノイズ障害

ケーブル ネットワーク上の信号劣化など、アップストリームのノイズ障害は、加入者のサービスに悪影響を及ぼす可能性があります。HFC ネットワークの場合は、双方向デジタルデータ信号のほうが、単方向の信号よりもストレスの影響を受けます。単方向のケーブル TV では、ビデオ信号の品質劣化は認識されない程度かもしれませんが、双方向デジタル信号とビデオ信号とでネットワークを共有する場合、次の原因によりデジタル信号が妨害されることがあります。

- インパルスおよび電気信号の流入：ノイズが住宅内の電源から、または CATV ケーブル付近の高圧ラインからネットワークに侵入することがあります。イングレス ノイズには、ブロードバンドとナローバンドの 2 種類があります。ブロードバンドのノイズは通常、周波数が低く（10 MHz 未満）、調波ロールオフが発生します。ナローバンドのノイズの方が、干渉源として深刻です。ケーブル機器およびインフラストラクチャは、アマチュア無線、市民ラジオ、高出力短波放送信号からノイズを拾うことがよくあります。信号漏洩保守プログラムを実装し、信号流入の発生場所を突き止め、対処してください。
- 増幅器のノイズ：増幅器によって HFC ネットワークのノイズが増します。ビデオ信号であれば普通は気付かない程度ですが、増幅器の設定に問題があると、デジタルデータ信号が劣化します。ネットワークの規模が大きいほど、増幅器のノイズが信号に影響する可能性は高まります。
- ノイズ ファンネリング：ヘッドエンドへのアップストリーム データ パスがネットワーク全体から干渉を受ける可能性があります。ノイズの性質として累積されるとヘッドエンドに集中するため、アップストリームのすべてのノイズは、最終的にヘッドエンドに集まります。RF レシーバを 1 台使用しているネットワークでは、ネットワークの規模が大きくなるほど、ノイズ ファンネリングが発生する確率が高くなります。
- 送信レベルの変動：温度は同軸ケーブルにおける信号損失に影響します。そのため、年間で 6 ～ 10 dB の変動が生じます。
- クリッピング：入力レベルが超過すると、光ファイバ トランスミッタのレーザー光により、光の伝送が中断することがあります。入力レベルが大きすぎると、アップストリーム伝送とダウンストリーム伝送の両方で、ビット エラーが発生します。レーザーが短時間（1 秒未満）超過しただけで、クリッピングが発生することがあります。

リターンの増幅器およびレーザーを調整するには、『NTSC Supplement on Upstream Transport Issues』または該当するケーブル設備規格に記載されている、厳密なプラント メンテナンス手順に従ってください。

スペクトル グループと周波数ホッピング

CMTS の管理者がアップストリーム周波数ホッピングを設定し、長期的なナローバンドノイズに対処することを推奨します。Cisco CMTS ルータは、ガイド型周波数ホッピングとタイム スケジュール型周波数ホッピングのコンビネーションをサポートします。

ノイズの混入を事前に回避するための周波数ホッピングは、周波数アジリティとも呼ばれます。周波数アジリティは、スペクトル グループを使用して設定し、アクティブにします。スペクトル管理は、多数のケーブル スペクトル グループの作成をサポートし、単一スペクトル グループ内

に複数のアップストリームポートを持つことを許可します。各スペクトルグループは、特定の周波数プランで使用する周波数のテーブルを定義します。アップストリーム周波数は、単一の固定周波数、単一の連続範囲の周波数（帯域）、または複数範囲（帯域）の周波数のいずれでもかまいません。

ケーブルインターフェイスは、スペクトルグループを設定して割り当てるか、または固定周波数を割り当てるかによって、アップストリームに周波数を割り当てるまで動作しません。スペクトルグループが優先されるため、スペクトルグループと固定周波数の両方をアップストリームに設定した場合、スペクトル グループが固定アップストリーム周波数の設定をオーバーライドします。

インターフェイスから見ると、スペクトル グループは、同じファイバ ノード グループに接続された1組のアップストリームでもあります。Ciscoルータのスペクトル管理ソフトウェアは、アップストリームに設定されているすべての RF パラメータを検査し、アップストリーム周波数をまとめて管理する必要があるかを判断します。たとえば、スペクトル グループに複数の固定周波数が設定されており、それらの周波数がすべて設定されたチャネル幅内である場合、スペクトル管理ソフトウェアはこれらの周波数を 1 つの帯域にまとめます。

アップストリーム ポートは、ノイズや他のパス障害に対応するために周波数ホッピングが必要な場合にどの周波数が有効かを、スペクトル グループを使って決定します。周波数ホッピング技法のタイプには、ガイド型、タイム スケジュール型、ガイド型とタイム スケジュール型のコンビネーションがあります。周波数ホッピング技法の詳細については、周波数ホッピング機能, （428 ページ）を参照してください。

（注） 各アップストリーム ポートに専用の RF ドメインがある場合、そのグループを非共有スペクトル グループと呼びます。複数のアップストリーム ポートで同じ RF ドメインを共用する場合には、そのグループを共有スペクトル グループと呼びます。

スペクトル管理のガイドライン

一般に、スペクトルを定義するときは、次のガイドラインを使用してください。

- アマチュア無線周波数帯や短波周波数帯など、流合の問題が判明している周波数を避けます。
- 20 MHz 未満の不適切なスペクトルを避けます。
- 周波数ホッピングに予備の帯域を許可します。
- 周波数帯域を作成するときには、可能なチャネル幅を考慮します。使用されている周波数の範囲は、アップストリームで設定されたチャネル幅を使用するときに少なくとも 2 つの周波数の間をホップできる必要があります。
- 共有スペクトル グループ内の同じコンバイナ グループにアップストリーム ポートを配置します。
- 受信電力レベルの設定によって、多少の等化調整を行います。

- 複数のアップストリーム ポートを組み合わせて広い帯域幅を提供する場合は、周波数帯域の重複を避ける必要があります。各ポートは、グループ内のその他のポートで使用されている帯域と重ならないような個別の周波数帯域を使用する必要があります。ある帯域の終了周波数と次の帯域の開始周波数の間に少なくとも 20 KHz を追加することを推奨します。これにより、帯域が重複しなくなります。

ガイド型およびスケジュール型スペクトル管理

ガイド型およびスケジュール型スペクトル管理は、現在サポートされているすべてのケーブル インターフェイス ライン カードにおける一連の基本機能を形成します。これらの機能が基本であるとみなされるのは、すべてのケーブル インターフェイスで使用可能であり、インテリジェント型および高度なスペクトル管理機能を構築するための基礎的で土台となる機能を構成するためです。

それぞれの機能の詳細については、以下の項を参照してください。

周波数ホッピング機能

コンシューマからサービス プロバイダーへのアップストリーム伝送ラインのノイズによって、加入者の自宅からのデータ送信が劣化することがあります。ノイズ障害がかなりの期間に及ぶ場合、ケーブルモデムとヘッドエンドファシリティとの通信が一時的に失われる可能性があります。危機管理計画として、マルチプル サービス オペレータ（MSO）は、加入者のために複数のチャネルまたはアップストリーム周波数を予約できます。あるチャネルで過剰な干渉が生じる場合、CMTS はケーブル モデムが別のチャネルに「ホップ」するように要求します。

周波数ホッピング機能を提供するため、Cisco CMTS ルータには未使用のアップストリーム チャネルのノイズを継続的にモニタするスペクトル マネージャが含まれます。特定のチャネルで CNR（CNiR）が許容できないレベルに達すると、スペクトル マネージャはそのチャネルを使用しているケーブル モデムに対して自動的に新しいアップストリーム チャネルを割り当てます。

Cisco CMTS ルータは、使用中の周波数帯域でノイズがないときにアップストリーム周波数ホッピングの次の手法をサポートします。

- ガイド型周波数ホッピング：ガイド型周波数ホッピング（ブラインドホッピングとも呼ばれます）では、ステーション メンテナンス（キープアライブ）メッセージの設定可能なしきい値が失敗すると、スペクトル マネージャは自動的に新しいアップストリーム チャネル周波数を割り当てます。失敗したステーション メンテナンス メッセージは、ノイズ、設備、または機器障害によるアップストリーム チャネル障害を表します。ガイド型周波数ホッピングでは、スペクトル グループで明示的な周波数サブ帯域および関連する入力電力レベルが割り当てられます。
- タイム スケジュール型周波数ホッピング：周波数の再割り当てが時刻または特定の曜日でスケジュールされます。
- ガイド型とタイム スケジュール型の周波数ホッピングの組み合わせ。

（注） 周波数ホッピングは、インパルス ノイズなどのブロードバンド ノイズ現象に対しては有効ではありません。

タイム スケジュール型とガイド型の手法は、独立した概念です。

- スペクトルは周波数テーブルではなくスクリプトによって制御されます。
- 使用可能なスペクトルは、オプションとしてタイム スケジュール型になります。
- ガイド型周波数ホッピングは、現在時刻の使用可能なスペクトルから選択されます。

スペクトル グループを使用して周波数ホッピングを設定およびアクティブ化できます。最大で40のケーブル スペクトル グループを作成でき、それぞれのグループには複数のアップストリーム ポートが含まれます。設定されたチャネル幅は、アップストリーム周波数ごとに使用されます。

ケーブル ネットワーク用に1つ以上のスペクトル グループを作成した後、グループに特性を追加でき、周波数の使用方法や周波数ホッピングをより完全に制御できます。

ホッピングしきい値を設定できます。たとえば、周波数ホップのしきい値の割合を設定する方法では、1 つの障害のあるケーブル モデムがその他の動作しているケーブル モデムへのサービスに影響を与えません。十分に高いしきい値が設定されていれば、1つのケーブルモデムでステーション メンテナンス（キープアライブ）メッセージの 90 パーセントに応答できなかったために、システムでホッピングが無限に発生することはありません。

また、周波数ホップの間の最小期間を設定できます。デフォルト設定は30秒です。宛先チャネルに障害があると予想される場合は、周波数ホップの間の最小期間を10秒などの小さな値に減らすことができます。これにより、クリア チャネルが見つかるまで周波数ホップをより迅速に継続できます。過剰な周波数ホップが問題である場合は、ホップ間の最小期間を増やすことができます。

周波数ホッピングのさまざまな手法を設定するには、スペクトル グループの作成と設定, （436 ページ）を参照してください。

（注） スペクトル管理機能は HFC ネットワーク上のアップストリーム パスに焦点を当てるため、単方向（Telco リターン）ケーブル モデムにはスペクトル管理がサポートされません。

（注） スペクトル帯域が変更された後、周波数を変更する前の周波数が新しいスペクトル帯域の範囲に属する場合は、スペクトル管理は各 US チャネルの周波数を再配置しないため、US 周波数は変更されません。前の周波数が新しいスペクトル帯域の範囲外である場合、US チャネルは周波数を取得しません。

タイム スケジュール型周波数ホッピング

設定された毎日または特定の曜日の時刻に基づいて、アップストリーム チャネル周波数の再割り当てを指定できます。ケーブル設備に 1 週間サイクルのアップストリーム雑音特性がある場合に

は、タイムスケジュール型スペクトル割り当てを使用します。タイムスケジュール型ポリシーにより、単一周波数がいつでも有効になります。

アップストリームの動的変調（MER [SNR] ベース）

このセクションでは、アップストリームのMER（SNR）の評価に基づくこの機能の動作について説明します。

（注） アップストリームの動的変調の高度なバージョンは、搬送波対雑音比（CNR [CNiR]）を使用し、インテリジェント型および高度なスペクトル管理をサポートするカードでサポートされます。

機能の概要

Cisco ケーブル インターフェイス ラインカードは、各アップストリーム ポートのアクティブなリターンパスにおけるMER（SNR）値と前方誤り訂正（FEC）カウンタをモニタします。アップストリームの動的変調機能は、アップストリーム チャネルの信号品質が設定された変調方式をサポートできるかどうかを判断し、必要に応じて最も堅牢な変調方式へと調整します。リターン パス条件が改善されると、この機能はアップストリーム チャネルを変調プロファイルが含まれるより高位の変調方式に戻します。

変調プロファイルは、アップストリームのモデム送信パラメータを設定するためにUCDメッセージで送信されるバースト プロファイルのコレクションです。アップストリームの動的変調機能は、アップストリームの信号品質に基づいてアップストリーム チャネルの変調プロファイルを調整します。

アップストリームの動的変調機能は、アップストリーム周波数が固定のインターフェイスで、またはスペクトル グループが割り当てられたインターフェイスで設定されます。

次の例は、2つおよび3つの変調プロファイルを使用する2つの異なるアップストリームの動的変調機能設定を示しています。

2つの変調プロファイルを使用するアップストリームの動的変調を示す例

次のプライマリおよびセカンダリ変調プロファイルを使って、CiscoCMTSルータ上でアップストリームの動的変調機能を設定できます。

- プライマリ変調プロファイルは、64-QAMまたは16-QAMを使用します。これは、帯域幅効率が高い変調方式であり、QPSKプロファイルよりもスループットが高くなります。
- セカンダリ変調プロファイルは、QPSKを使用します。これは、より堅牢な変調方式を使用しますが、帯域幅は効率的ではありません。

プライマリ プロファイルでは64-QAMまたは16-QAMを使用し、セカンダリではQPSKを使用することを推奨します。ただし、これはオプションであり、両方の変調プロファイルをQPSKまたはQAMにしてもかまいません。一方のプロファイルをQAM、他方をQPSKにすることは必須ではありませんが、変調プロファイルの切り替えはQAMおよびQPSKのしきい値に結び付いています。

3 つの変調プロファイルを使用するアップストリームの動的変調を示す例

次のプライマリ、セカンダリ、およびターシャリ変調プロファイルを使って、Cisco CMTS ルータ上でアップストリームの動的変調機能を設定できます。

- プライマリ変調プロファイルは、64-QAM を使用します。これは、帯域幅効率が高い変調方式であり、16-QAM プロファイルよりもスループットが高くなります。
- セカンダリ変調プロファイルは、16-QAM を使用します。これは、帯域幅効率が高い変調方式であり、QPSK プロファイルよりもスループットが高くなります。
- ターシャリ変調プロファイルは、QPSK を使用します。これは、より堅牢な変調方式を使用しますが、帯域幅は効率的ではありません。

プライマリ プロファイルでは 64-QAM 変調を使用し、セカンダリ プロファイルでは 16-QAM を使用し、ターシャリ プロファイルでは QPSK を使用することを推奨します。ただし、これはオプションであり、変調プロファイルを QPSK または QAM にしてもかまいません。1 つのプロファイルを QPSK、ほかの 2 つを QAM にすることは必須ではありませんが、変調プロファイルの切り替えは QAM および QPSK のしきい値に結び付いています。

変調プロファイルの切り替え条件

アップストリームの動的変調機能では、次の条件を使用して、プライマリ変調プロファイルからセカンダリ変調プロファイル（帯域幅効率は高いが堅牢性は劣るプロファイル）または（任意の）ターシャリ変調プロファイル（堅牢性は最も高いが帯域幅効率は劣るプロファイル）に切り替える必要があるかどうかを判別します。

プライマリ プロファイル（パフォーマンス高レベル）からセカンダリ プロファイル（パフォーマンス中レベル）への変調切り替えでは次の基準を使用します。

- アップストリーム MER（SNR）が MER（SNR）のしきい値 1 以下であること。さらに、修正可能 FEC（cFEC）エラーのパーセンテージが修正可能 FEC エラーのしきい値以下であるか、または修正不可能 FEC（uFEC）エラーのパーセンテージが修正不可能 FEC エラーのしきい値以上であること。

セカンダリ プロファイルからプライマリ プロファイルに戻る前に、次の条件が満たされる必要があります。

- アップストリーム MER（SNR）は MER（SNR）のしきい値 1 とヒステリシス値の合計以上であること。さらに、修正可能 FEC エラーのパーセンテージが修正可能 FEC エラーのしきい値以下であり、修正不可能 FEC エラーのパーセンテージが修正不可能 FEC エラーのしきい値以下であり、ホップ間隔がデフォルト値の 15 秒と等しいこと。

セカンダリ プロファイル（パフォーマンス中レベル）からターシャリ プロファイル（堅牢性最高）への変調切り替えでは次の基準を使用します。

- アップストリーム MER（SNR）が MER（SNR）のしきい値 2 以下であること。さらに、修正可能 FEC（cFEC）エラーのパーセンテージが修正可能 FEC エラーのしきい値以下であるか、または修正不可能 FEC（uFEC）エラーのパーセンテージが修正不可能 FEC エラーのしきい値以上であること。

ターシャリプロファイルからセカンダリプロファイルに戻る前に、次の条件が満たされる必要があります。

- アップストリーム MER（SNR）は MER（SNR）のしきい値 2 とヒステリシス値の合計以上であること。さらに、修正可能 FEC エラーのパーセンテージが修正可能 FEC エラーのしきい値以下であり、修正不可能 FEC エラーのパーセンテージが修正不可能 FEC エラーのしきい値以下であること。

プライマリプロファイルからターシャリプロファイルへの変調切り替えでは次の基準を使用します。

- アップストリーム MER（SNR）が MER（SNR）のしきい値 2 以下であること。さらに、修正可能 FEC（cFEC）エラーのパーセンテージが修正可能 FEC エラーのしきい値以下であるか、または修正不可能 FEC（uFEC）エラーのパーセンテージが修正不可能 FEC エラーのしきい値以上であること。

ターシャリプロファイルからプライマリプロファイルに戻る前に、次の条件が満たされる必要があります。

- ターシャリ プロファイルからプライマリ プロファイルへの変調切り替えは 2 つのステップからなるプロセスです。

  1. ターシャリ プロファイルからセカンダリ プロファイルへの変調切り替えは、アップストリーム MER（SNR）が MER（SNR）のしきい値 1 とヒステリシス値の合計以上である場合に発生します。
  2. その 15 秒後（構成不可能）、セカンダリプロファイルからプライマリプロファイルへの変調切り替えは、アップストリーム MER（SNR）が MER（SNR）のしきい値 1 とヒステリシス値の合計以上のままである場合に発生します。

アップストリームで多数の修正不可能なエラーが発生していることが唯一の問題であれば、ルータがプロファイルを切り替え続けているという状況が発生している可能性があります。修正不可能なエラーがプライマリプロファイルで発生したため、スイッチはセカンダリプロファイルに切り替えます。セカンダリプロファイルでは問題が発生しないため、ルータはプライマリプロファイルに戻します。しかし、修正不可能なエラーが再度発生し、ルータはセカンダリ プロファイルに戻します。このサイクルが際限なく続きます。

この問題を回避するため、ケーブル設備がプライマリ プロファイルで使用している変調方式（たとえば 64-QAM）に対応していることを確認してください。この変調方式を使用してアップストリームでの正常な動作を保証できない場合は、帯域幅効率の高いバースト パラメータを使用しているプライマリ プロファイル（QPSK など）を選択してください。Cisco IOS ソフトウェアには、プライマリ、セカンダリ、およびターシャリ プロファイルに使用できる事前定義された変調プロファイルがあります。

入力レベル

入力レベル *power-level-dBmV* は、**cable spectrum-group** コマンドのオプションです。このオプションにより、ケーブル モデムがある固定周波数から次の周波数に、またはある帯域から次の帯域に

ホッピングするときに、CMTS のアップストリーム レシーバで予期されるアップストリーム入力レベルを指定できます。アップストリームチャネルごとに、アップストリーム入力レベル（dBmV）が 1 つずつ対応付けられています。電力レベルは、アップストリーム周波数の変更が必要になったときに、各スペクトル グループが使用できるモデムの送信出力です。入力レベルは、周波数のホッピング時に設定できます。

入力レベルを指定することによって、ケーブル モデムがホッピングのたびに送信出力を上げ下げしなくて済むようにします。ケーブル オペレータは、周波数のファンクションとして、小さな電力等化を実行できます。有効範囲は -10 ～ +10 dBmV です。電力レベル値は、スペクトル管理の一部として電力レベルを変更しなければならない場合に限って変更してください。ケーブル設備によっては、日常のタイム スケジュールで変更するのは入力レベルのみに限定し、周波数は変更しないようにする必要があります。

インテリジェント型および高度なハードウェアベースのスペクトル管理

いくつかのインターフェイス ライン カードは、他の Cisco ケーブル インターフェイス ライン カードがサポートする基本機能を拡張する、ハードウェアベースのスペクトル管理機能を提供します。

インテリジェント型スペクトル管理の機能拡張

次に示す機能は、インテリジェント型スペクトル管理フィーチャ セットの一部になります。

- DOCSIS 周波数範囲の 5 ～ 42 MHz で常にアップストリーム スペクトル品質を分析するオンボード スペクトル アナライザが DOCSIS ケーブル インターフェイス ライン カードに組み込まれました。
- ハードウェア支援型の周波数ホッピング機能が組み込まれ、ソフトウェアのみのソリューションよりインテリジェントで高速な周波数選択が可能になりました。
- モデムのオフライン化を引き起こすことのあるイングレス ノイズに対する応答時間が短縮されました。
- ノイズがないことが判明しているチャネルへの周波数ホッピングを開始することによって、ブラインド周波数ホッピングが排除されました。
- パケットのドロップを排除し、その結果としてアップストリームでフル データ レートが維持されるように、周波数アジリティが改善されました。
- 共有スペクトル上で環境が結合される dense（密）モードで、周波数アジリティがサポートされるようになりました。
- 必要に応じて、個々の固定周波数からなるセットまたは周波数範囲に周波数ホッピングを限定できるようになりました。
- プラント環境および要件に応じて、周波数ホッピング条件をカスタマイズできるようになりました。
- 任意で既知の使用パターンまたはプラント条件を利用して、周波数ホッピングのスケジューリングが可能です。

- 任意でチャネル幅を動的に引き下げ、ノイズのあるアップストリームでも、ケーブルモデムをオンラインにしておくことができるようになりました。

利点

Cisco CMTS ルータ プラットフォームで提供されるスペクトル管理機能には、システム上の主な利点がいくつかあります。

- アップストリームのリターン パスに出現するイングレス ノイズ障害に対する応答時間を改善します。
- モデムがオンラインになる割合を押し上げます。
- サブスクライバ サービスへの入力の影響を軽減します。
- マイナー設備の停止をトラブルシューティングするときに、MSO担当者による時間と手間を削減します。
- ケーブル設備の信頼性を向上させます。
- スペクトル使用率を最大化します。

ガイド型およびスケジュール型スペクトル管理のメリット

次は、すべてのCisco CMTSルータ プラットフォームでサポートされるガイド型およびスケジュール型スペクトル管理の具体的なメリットをまとめたものです。

入力レベル

ケーブル設備オペレータは、周波数のファンクションとして、小さな電力レベル等化を実行できます。

周波数ホッピング機能

ケーブルモデムに新しいアップストリームチャネルを割り当てることによって、アップストリーム ノイズ障害を予防的に対策します。MSOは、アップストリーム周波数の搬送波対雑音比が最適値未満であるとき、またはケーブル設備がイングレス ノイズのランダムなバーストを示していて信頼性に影響するときに、特にこの機能を利用できます。

アップストリームの動的変調

- リターンパスにおけるQAM-16変調への移行に関連するリスクを軽減し、加入者がリターンパス障害時でもオンラインで接続状態を維持することを保証します。
- アクティブなアップストリームの信号品質が設定されている変調方式をサポートできるかどうかを確認し、必要に応じて、より堅牢な変調方式に予防的に調整します。
- プライマリ変調プロファイルからセカンダリ変調プロファイルへ自動的に切り替わることで、ケーブルモデムがオンラインを維持するためにチャネルをホップする必要性をなくします。

インテリジェント型および高度なスペクトル管理の利点

次に、サポート対象のケーブル インターフェイス ライン カードを使用した Cisco CMTS ルータでサポートされる、高度なスペクトル管理機能の利点について概要を説明します。

チャネル幅の動的変更

- ノイズ状態によって現在のチャネル幅が使用できない場合に、アップストリームで使用できる最大のチャネル幅を見つけて、DOCSIS アップストリーム チャネルのアベイラビリティを向上させます。
- 現在のプラント条件で最大の RF スペクトル使用効率を提供します。
- ノイズ問題に対応して使用できるチャネル幅の範囲をカスタマイズできます。

インテリジェント周波数ホッピング

- ノイズ状態が深刻になってケーブル モデムが強制的にオフラインにされないうちに、インターフェイスのアップストリーム周波数を予防的に変更します。
- 専用ハードウェアのインテリジェント周波数ホッピングが、新しいアップストリーム周波数を選択するために「先読み」を行い、安定したチャネルを見つけます。
- プライオリティを柔軟に設定できるので、個々のケーブル設備環境に合わせて、ホッピング決定条件を調整できます。
- プラント条件の変動にホッピング決定条件を合わせることによって、イングレス障害に対する感度を向上させます。
- モデム単位の確度で CNR（CNiR）の変動を絞り込み、問題のあるケーブル モデムを特定します。
- ユーザ側で設定できる予防的チャネル管理技法により、加入者がオンラインであるパーセンテージが維持または改善されます。

アップストリームの動的変調

- イングレス ノイズに対応するための、アップストリームにおける QPSK と QAM-16 変調間の切り替えに伴うリスクが軽減されるので、加入者はオンラインの接続を維持できます。
- 現在のアップストリーム信号を調べ、設定されている変調方式をサポートできるかどうかを確認します。必要に応じて、より堅牢なセカンダリ変調方式に予防的に調整します。
- DOCSIS アップストリーム チャネルのアベイラビリティを向上させ、最大の RF スペクトル使用効率を提供します。
- 現在割り当てられているアップストリームを使用しながら、ケーブルモデムをオンラインで維持できるような変調プロファイルに切り替えることによって、不要な周波数ホッピングを排除します。
- リターン パス障害が発生している間も、加入者はオンラインの状態が維持されます。

SNMP インターフェイス

- アップストリームの現在のノイズ状況をリモートで調べることができます。この情報はその後、サードパーティまたはカスタムのレポートアプリケーションやグラフィックアプリケーションに取り込むことができます。
- ポート単位で、搬送周波数のイングレス ノイズおよびインパルス ノイズを認識できます。
- 個々のケーブル モデムおよびセットトップ ボックス（STB）について、DOCSIS アップストリーム スペクトルのリアルタイム表示をリモートで収集するための、使いやすい分散方式が得られます。
- 各ヘッドエンドまたはハブで高価なスペクトル アナライザに依存する状況が軽減されます。
- 使いやすいインターフェイスにより、即座にスペクトル ビューが得られます。スペクトル アナライザの複雑な設定を行う必要はありません。
- エンジニアはスペクトル アナライザを使用する際に物理的に接続することなく、ネットワークのトラブルシューティングをリモートで実行できます。

ホッピングのデフォルト プライオリティ

インテリジェント型および高度なスペクトル管理機能では、ホッピングのデフォルト プライオリティは次のように設定されています。

- 周波数、変調、チャネル幅（スペクトル カード上でスペクトル グループを使用した場合）。
- 変調、ガイド型周波数ホッピング、チャネル幅（スペクトル グループによりアナライザ カードを使用した場合）。
- 変調のみ（スペクトル グループを使用しない場合 [固定周波数]）。

スペクトル管理の設定方法

ここでは、Cisco CMTS プラットフォームでスペクトル管理機能を使用する場合に最も一般的に実行する設定タスクについて説明します。ご使用のプラットフォームおよびケーブル インターフェイス ラインカードに適した設定タスクについては、次の項を参照してください。

ガイド型およびスケジュール型スペクトル管理の設定タスク

次のタスクにより、すべての Cisco CMTS プラットフォームでサポートされるガイド型およびスケジュール型スペクトル管理機能が設定されます。

スペクトル グループの作成と設定

スペクトル グループは、周波数ホッピングの実行時にアップストリームが使用できる周波数、および周波数ホッピングを制御する他のパラメータを定義します。スペクトル グループを作成および設定する場合、次のパラメータを指定できます。

- グループに割り当てられる周波数。ケーブルインターフェイスは次の周波数を使用して、周波数ホッピングが必要な場合に使用できる周波数を決定します。固定周波数のリストまたは周波数帯域、あるいはその両方を指定できます。スペクトル グループに周波数を追加する場合、Cisco CMTS は次のルールを使用します。
  - 固定周波数を指定する場合、Cisco CMTS は、その周波数がすべての利用可能なチャネル幅で動作するように、6.4 MHz のチャネル幅を持つ中心周波数だとします。たとえば、17,700,000 Hz の周波数を指定するのは、14,500,000 Hz ～ 20,900,000 Hz（6.4 MHz 幅の帯域）の周波数帯域を指定することと同等です。
  - 複数の固定周波数または重複する周波数帯域を設定する場合、スペクトル グループはその周波数を 1 つの帯域にまとめます。たとえば、17,700,000 Hz の固定周波数と 15,800,000 Hz ～ 25,200,000 Hz の帯域を指定すると、スペクトル グループは 14,500,000 Hz ～ 25,200,00 Hz の 1 つの帯域で設定されます。
  - スペクトル グループの周波数を制御する場合、必要なチャネル幅と同じ幅の周波数帯域を設定します。たとえば、3.2 MHz のチャネル幅で 17,700,000 Hz の中心周波数を使用する場合、16,100,000 ～ 19,300,000 Hz の帯域幅を指定します。重複しない帯域を設定するようにするには、帯域同士を最低 20 KHz 離します。

- アップストリームの入力電力レベル：（任意）新しい周波数へのホッピング時にアップストリームが使用すべき電力レベル（dBmV）。（ケーブル設備によっては、日常のタイム スケジュールで変更するのは入力レベルのみに限定し、周波数は変更しないようにする必要があります。）
- ホッピングのしきい値：（任意）周波数ホッピングの発生前に、ステーション メンテナンス メッセージを見落とし始めるケーブル モデムの割合。1 つの障害のあるケーブル インターフェイスが他の良好なケーブル インターフェイスのサービスに影響を与えないように、必要に応じてホッピングのしきい値の割合を設定します。これにより、1 つのケーブル モデムで 90 パーセントのエラーと 90 パーセントのトラフィックが生成されるため、システムでホッピングが無限に発生することはなくなります。
- ホッピングの間隔：（任意）周波数ホッピング間に経過すべき最短時間。これにより、別の周波数ホッピングの実行前に、アップストリームが安定するだけの十分な時間を指定できます。
- スケジュール型ホッピング時間：（任意）周波数ホッピングをスケジュール設定すべき時刻。

ヒント アップストリーム周波数（または周波数ホッピング テーブル）のリストを追加する前に、まずどのアップストリーム ポートをコンバイナ グループに割り当てるかを決定します。例については、例：コンバイナ グループに割り当てるアップストリーム ポートの特定，（465 ページ）を参照してください。

スペクトル グループを作成および設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cablespectrum-group** *group-number***time**[*day hh:mm:ss*] **frequency** *up-freq-Hz* [*power-level-dBmV*] 例： `Router(config)# cable spectrum-group 4 time Monday 12:00:00 frequency 40000000`	スペクトル グループ（まだ存在しない場合）を作成し、指定した固定周波数をこのグループに追加します。
ステップ 4	**cablespectrum-group** *group-number***time** [*day hh:mm:ss*] **band** *up-freq-Hz up-freq2-Hz [power-level-dBmV*] 例： `Router(config)# cable spectrum-group 4 band 20000000 24000000 13`	スペクトル グループ（まだ存在しない場合）を作成し、指定した周波数帯域をこのグループに追加します。 （注） 必要に応じて、このスペクトル グループに含めるそれぞれの固定周波数と周波数帯域についてステップ 4 とステップ 6 を繰り返します。周波数ホッピングが発生する前に、2 つ以上の固定周波数、または 2 つ以上の中心周波数を含む周波数帯域をスペクトル グループに割り当てる必要があります。
ステップ 5	**cablespectrum-group** *group-number***hopperiod** *seconds* 例： `Router(config)# cable spectrum-group 4 hop period 60`	周波数ホッピング間隔の最小時間を秒単位で指定します。 （注） Cisco uBR-MC5X20S/U/H BPE を使用する場合は 30 秒に設定することを推奨します。
ステップ 6	**cablespectrum-group** *group-number* **hopthreshold** [*percent*] 例： `Router(config)# cable spectrum-group 4 hop threshold 25`	スペクトル グループの周波数ホッピングのしきい値を指定します。 • **percent**：（任意）失われたステーション メンテナンス メッセージの割合としての周波数ホッピングのしきい値。有効な値は 1 ～ 100 パーセントです。デフォルトは 50 パーセントです。

	コマンドまたはアクション	目的
ステップ 7	**cablespectrum-group** *group-number* 例： `Router(config)# cable spectrum-group 4`	（任意）スペクトル グループのアップストリーム ポートで固有のアップストリーム周波数を使用することを指定します。
ステップ 8	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

1 つ以上のアップストリーム ポートへのスペクトル グループの割り当て

スペクトル グループの作成と設定が完了したら、グループの周波数スペクトルを周波数ホッピングに使用する前に、このスペクトル グループを 1 つ以上のアップストリーム ポートに割り当てます。

コントローラ インターフェイス上の 1 つまたはすべてのアップストリーム ポートにスペクトル グループを割り当てるには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**controller upstream-cable** *slot*/*subslot*/*port* 例： `Router(config)# controller upstream-cable 9/0/15`	コントローラ コンフィギュレーション モードを開始します。
ステップ 4	**us-channel** *us-channel_num* **spectrum-group** *spectrum-group-num* 例： `Router(config-controller)# us-channel 0 spectrum-group 1`	このコントローラ インターフェイス上のすべてのアップストリームに対して、指定したスペクトル グループをデフォルト グループとして割り当てます。

	コマンドまたはアクション	目的
ステップ 5	**us-channel** *us* *-channel_num***channel-width** *value* 例： `Router(config-controller)# us-channel 0 channel-width 1600000`	指定したアップストリーム チャネル スペクトル グループの channel-width を設定します。
ステップ 6	**end** 例： `Router(config-controller)# end`	コントローラ インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次の作業

ヒント　スペクトル グループ設定を確認するには、特権 EXEC モードで **showcablespectrum-group** コマンドを使用します。

DOCSIS 3.0 の共有スペクトル グループ（ファイバ ノード グループ）の設定

この機能は、Cisco CMTS ルータで複数のケーブル インターフェイス ライン カードを経由する共有スペクトル グループと、単一ケーブル インターフェイス ライン カード内の共有スペクトル グループをサポートします。

Cisco CMTS のファイバ ノード グループの設定に関する詳細については、次を参照してください。

- http://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_cbr_layer2_docsis/spectrum_management.html#task_1044164
- http://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_cbr_layer2_docsis/spectrum_management.html#task_4BF4590BA65D4CF1851A4DA0C8A9ADB2

アップストリームの動的変調の設定（MER [SNR] ベース）

MER（SNR）バージョンのアップストリームの動的変調機能のみをサポートするケーブル インターフェイス ライン カードでこの機能を使用するには、次の手順に従う必要があります。

1. プライマリ変調プロファイルを作成します。このプロファイルは通常、帯域幅の効率性に優れていますが、堅牢性はそれほどでもありません。
2. 必要に応じて、セカンダリ変調プロファイルを作成します。このプロファイルは通常、帯域幅の効率性には劣りますが、ある程度の堅牢性があります。
3. 必要に応じて、ターシャリ変調プロファイルを作成します。このプロファイルは通常、帯域幅の効率性には劣りますが、優れた堅牢性があります。

4 任意のケーブル インターフェイスとアップストリームにプロファイルを割り当てます。

ヒント 変調プロファイルを作成する場合は、各変調プロファイルのそれぞれのバースト パラメータを手動で指定する代わりに、定義済み変調プロファイルを使用することを推奨します。

制約事項

- アップストリームの動的変調機能は、高度なスペクトル管理用の DOCSIS 1.0 または DOCSIS 1.1 TDMA 専用の変調プロファイルのみでサポートされます。
- DOCSIS 2.0 混合モードまたは ATDMA 専用モードの変調プロファイルは、高度なスペクトル管理ではなく、基本的なスペクトル管理（MER [SNR] ベース）のみでサポートされます。
- 3 段階の動的変調機能では、基本的なスペクトル機能のみがサポートされます。CNR（CNiR）のしきい値および測定値に基づいて、変調プロファイルが変更されることはありません。
- アップストリームの動的変調機能は、単一の変調プロファイル設定では有効になりません。
- アップストリームの周波数ホッピングがスペクトル グループに割り当てられている場合、設定できる変調プロファイルは 2 つのみです。このスペクトル グループは、高度なスペクトル管理と、CNR（CNiR）の使用を示しています。
- 次の条件に基づいて、スペクトル グループの割り当て前に 3 つの変調プロファイルがアップストリーム インターフェイスに割り当てられている場合は、設定からプロファイルが 1 つ自動的に削除されます。
  - アップストリーム ポートが高性能なプロファイルを使用している場合、堅牢なプロファイルはドロップされます。
  - アップストリーム ポートが中程度または堅牢なプロファイルを使用している場合、高性能なプロファイルはドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**cablemodulation-profile** *profile* {**mixed**| **tdma** | **atdma** 例： `Router(config)# cable modulation-profile 3 mixed`	DOCSIS 1.0 または DOCSIS 1.1 TDMA あるいはA-TDMAアップストリームで使用するプライマリ変調プロファイルを作成します。 （注） DOCSIS 1.0 または DOCSIS 1.1 TDMA あるいは A-TDMA アップストリームで使用するセカンダリおよびターシャリプロファイルを作成するには、このコマンドを繰り返します。 （注） また、個別のバースト パラメータの値を設定することにより、**cablemodulation-profile** コマンドでカスタム変調プロファイルを作成することもできます。ただし、各パラメータの変更が DOCSIS MAC レイヤにどのような影響を与えるかを熟知していない場合は、このパラメータを変更しないでください。ケーブル設備の大部分には、デフォルトの定義済み変調プロファイルを使用することを推奨します。
ステップ 4	**controller upstream-cable** *slot*/*subslot*/*port* 例： `Router(config)# controller upstream-cable 9/0/15`	コントローラ コンフィギュレーション モードを開始します。
ステップ 5	**us-channel** *n***modulation-profile** *primary-profile-number*[*secondary-profile-number*] [*tertiary-profile-number*] 例： `Router(config-controller)# us-channel 0 modulation-profile 21 121 221`	プライマリ変調プロファイルと、オプションのセカンダリおよびターシャリ変調プロファイルを指定したアップストリーム ポートに割り当てます。
ステップ 6	次のいずれかのコマンドを使用します。 • **us-channel***n* **threshold snr-profiles** *threshold1-in-db threshold2-in-db*	（任意）MER（SNR）のしきい値をdBで指定します。

	コマンドまたはアクション	目的
	• **us-channel***n m***threshold snr-profiles** *threshold1-in-db threshold2-in-db* 例： `Router(config-controller)# us-channel 0 threshold snr-profiles 25 15`	
ステップ 7	次のいずれかのコマンドを使用します。 • **us-channel***n* **threshold corr-fec** *corr-fec* • **us-channel***n m* **threshold corr-fec** *corr-fec* 例： `Router(config-controller)# us-channel 0 threshold corr-fec 20`	（任意）アップストリームに修正可能なFECエラーの許容数を指定します。
ステップ 8	次のいずれかのコマンドを使用します。 • **us-channel***n* **threshold uncorr-fec** *uncorr-fec* • **us-channel***n m* **threshold uncorr-fec** *uncorr-fec* 例： `Router(config-controller)# us-channel 0 threshold uncorr-fec 10`	（任意）アップストリームに修正不可能な FEC エラーの許容数を指定します。
ステップ 9	**us-channel** *n* **threshold hysteresis** *hysteresis-in-db* 例： `Router(config-controller)# us-channel 0 threshold hysteresis 10`	（任意）動的変調アップグレードのしきい値と組み合わせて使用するヒステリシス値を指定します。
ステップ 10	**end** 例： `Router(config-controller)# end`	コントローラ インターフェイス コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

次の作業

ヒント　アップストリームの動的変調機能の詳細については、アップストリームの動的変調（MER [SNR] ベース），（430 ページ）を参照してください。

周波数ホッピングの確認

コマンドライン インターフェイス（CLI）を使用すると、CMTS の周波数ホッピングを確認できます。

CLI コマンドを使用した周波数ホッピングの確認

CLI コマンドを使用して周波数ホッピングを確認するには、次の手順を実行します。

手順

ステップ 1 特権 EXEC モードで **showinterfacescable** コマンドを使用して、テスト対象のインターフェイスが稼働していることを確認します。出力の最初の行には、インターフェイスとライン プロトコルの両方が稼働しているかどうかが表示されます。

例：

```
Router# show interfaces cable 9/0/0

Hardware is CMTS MD interface, address is c414.3c16.cf8f (bia c414.3c16.cf8f)
MTU 1500 bytes, BW 26000 Kbit/sec, DLY 1000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation MCNS, loopback not set
```

ステップ 2 **showinterfacescableupstream** コマンドを使用して、テスト対象のアップストリームが稼働していることを確認します。最初の行には、アップストリームが稼働しているかどうかが表示されます。

例：

```
Router# show interfaces cable 9/0/0 upstream 0

MAC domain upstream impairment report: 0x0
Cable9/0/0: Upstream 0 is up
Description: UC9/0/0:U0
Received 5 broadcasts, 0 multicasts, 26 unicasts
0 discards, 0 errors, 0 unknown protocol
31 packets input
Codewords: 348 good 0 corrected 0 uncorrectable
```

ステップ 3 アップストリームで現在使用している周波数を表示するには、**showcablehopupstream-cable** コマンドを使用します。

例：

```
Router# show cable hop upstream-cable 9/0/0

Upstream    Port       Poll Missed Min    Missed Hop   Hop     Corr    Uncorr
Port        Status     Rate Poll   Poll   Poll   Thres Period  FEC     FEC
                       (ms) Count  Sample Pcnt   Pcnt  (sec)   Errors  Errors
Cable6/0/U5 16.816 Mhz 1000 0      10         0%   20%  25     0       0
```

ステップ 4 **showcablehopupstream-cablehistory** コマンドを使用して、アップストリームの周波数の変更、変調の変更、チャネル幅の変更に関する操作履歴を表示します。

例：

```
Router# show cable hop upstream-cable 9/0/0 history

F = Frequency Hop, M = Modulation Change, C = Channel Width Change
Upstream     Action             Chg    Chg    Action
Port         Time          Code From   To     Reason
Ca7/0/0/U0   Sep 17 17:00:24 C  1.6    3.2    Configuration changed
             Sep 14 19:38:55 F  41.117 26.358 Interface state changed
             Sep 14 19:38:55 F   0.000 41.117 Interface state changed
             Sep 14 19:38:24 M  21     221    Configuration changed
```

ステップ 5 **showcablehopupstream-cablethreshold** コマンドを使用して、アップストリームのユーザ定義しきい値、現在の CNR、MER（SNR）、修正可能な FEC の割合、修正不可能な FEC の割合、適用されなかったステーション メンテナンスの割合の数値を表示します。

例：

```
Router# show cable hop upstream-cable 6/0/0 threshold

Upstream   SNR(dB)          CNR(dB)          CorrFEC%  UncorrFEC%       MissedSM%
Port       Val Thre1 Thre2 Val Thre1 Thre2 Pcnt Thre Pcnt Thre        Pcnt Thre

Ca6/0/0/U0 27   25   15    39   35   25    0    3    0    1           75   75
Ca6/0/0/U1 31   25   15    51   35   25    0    3    0    1           90   75
Ca6/0/0/U2 --   35   25    --   35   25    0    3    0    1           0    75
Ca6/0/0/U3 --   35   25    --   35   25    0    3    0    1           0    75
```

ステップ 6 **testcablehop** コマンドを使用して、該当するアップストリームで周波数ホッピングを強制的に実行します。コマンドを入力してから数秒後に、コンソール メッセージにホッピングの通知が表示されます。必要に応じてこのコマンドを繰り返し、アップストリームのスペクトル グループに割り当てられたすべての周波数でホッピングが行われていることを確認します。

例：

```
Router# test cable hop cable 6/0 upstream 5

2w0d: %UBR7200-5-USFREQCHG: Interface Cable6/0 Port U5, frequency changed to 15.760 MHz

Router# test cable hop cable 6/0 upstream 5

2w0d: %UBR7200-5-USFREQCHG: Interface Cable6/0 Port U5, frequency changed to 26.832 MHz
```

ステップ 7 **testcablechannel-width** コマンドを使用して、該当するアップストリームでチャネル幅の変更を強制的に実行します。テスト コマンドを投入してから数秒に、show cable hop コマンドを使用してチャネル幅の変更を確認します。

例：

```
Router# test cable channel-width cable 7/0/0 upstream 0

Channel width changed to 1600000 Hz for Cable7/0/0 U0

Router# *Sep 17 17:06:46.882: %UBR10000-5-USCWCHG: Interface Cable7/0/0 U0, channel width
changed to 1600 kHz SLOT 7/0: Sep 17 17:06:46.898: %UBR10000-5-USCWCHG: Interface Cable7/0/0
 U0, channel width changed to 1600 kHz

Router# Sep 17 17:06:46.898: %Interface Cable7/0/0 U0 With channel width 1600 kHz, the
minislot size is now changed to 4 ticks.
```

```
Router# show cable hop cable 7/0/0 upstream 0 history

F = Frequency Hop, M = Modulation Change, C = Channel Width Change
Upstream     Action             Chg    Chg    Action
Port         Time          Code From   To     Reason
Ca7/0/0/U0   Sep 17 17:06:46 C  3.2    1.6    Test command enforced
             Sep 17 17:06:02 M  222    221    SNR 36>=28 CFEC 0<=3 UnCFEC 0<=1
             Sep 17 17:06:00 M  221    222    Test command enforced
             Sep 17 17:03:21 M  222    221    SNR 36>=28 CFEC 0<=3 UnCFEC 0<=1
             Sep 17 17:03:19 M  221    222    Test command enforced
             Sep 17 17:01:44 F  26.358 19.742 Test command enforced
             Sep 17 17:01:17 F  21.528 26.358 Test command enforced
             Sep 17 17:00:24 C  1.6    3.2    Configuration changed
             Sep 14 19:38:55 F  41.117 21.528 Interface state changed
             Sep 14 19:38:55 F   0.000 41.117 Interface state changed
             Sep 14 19:38:24 M  21     221    Configuration changed
Router#
```

ステップ 8 **testcablefreq-hop** コマンドを使用して、該当するアップストリームで動的周波数の変更を強制的に実行します。テスト コマンドを発行してから数秒後に、 **show cable hop** コマンドを使用して周波数の変更を確認します。

例：

```
Router# test cable freq-hop cable 7/0/0 upstream 0

SLOT 7/0: Sep 17 17:01:44.650: %UBR10000-5-USFREQCHG: Interface Cable7/0/0 U0, changed to
Freq 19.742 MHz

Router# show cable hop cable 7/0/0 upstream 0 history

F = Frequency Hop, M = Modulation Change, C = Channel Width Change
Upstream     Action             Chg    Chg    Action
Port         Time          Code From   To     Reason
Ca7/0/0/U0   Sep 17 17:01:44 F  26.358 19.742 Test command enforced
             Sep 17 17:00:24 C  1.6    3.2    Configuration changed
             Sep 14 19:38:55 F  41.117 26.358 Interface state changed
             Sep 14 19:38:55 F   0.000 41.117 Interface state changed
             Sep 14 19:38:24 M  21     221    Configuration changed
```

ステップ 9 **testcablemodulation-change** コマンドを使用して、該当するアップストリームで動的変調の変更を強制的に実行します。テスト コマンドを発行してから数秒後に、 **show cable hop** コマンドを使用して変調の変更を確認します。

例：

```
Router# test cable modulation-change cable 7/0/0 upstream 0

SLOT 7/0: Sep 17 17:03:19.038: %UBR10000-5-USMODCHANGE: Interface Cable7/0/0 U0, dynamic
modulation changed to QPSK
SLOT 7/0: Sep 17 17:03:19.038: %UBR10000-6-PREAMLENADJUST: request burst's preamble length
 in mod profile 222 is adjusted to 38 bits.
SLOT 7/0: Sep 17 17:03:19.038: %UBR10000-6-PREAMLENADJUST: initial burst's preamble length
 in mod profile 222 is adjusted to 100 bits.
SLOT 7/0: Sep 17 17:03:19.038: %UBR10000-6-PREAMLENADJUST: station burst's preamble length
 in mod profile 222 is adjusted to 100 bits.

Router# show cable hop cable 7/0/0 upstream 0 history

F = Frequency Hop, M = Modulation Change, C = Channel Width Change
Upstream     Action             Chg    Chg    Action
Port         Time          Code From   To     Reason
Ca7/0/0/U0   Sep 17 17:03:19 M  221    222    Test command enforced
```

```
Sep 17 17:01:44 F  26.358 19.742 Test command enforced
Sep 17 17:01:17 F  21.528 26.358 Test command enforced
Sep 17 17:00:24 C  1.6    3.2    Configuration changed
Sep 14 19:38:55 F  41.117 21.528 Interface state changed
Sep 14 19:38:55 F   0.000 41.117 Interface state changed
Sep 14 19:38:24 M  21     221    Configuration changed
```

スペクトル グループ特性のトラブルシューティング

設定のトラブルシューティングでは、有効なスペクトル グループの番号、時間、周波数、および入力電力レベルを必ず入力します。また、スペクトルを定義するときは、次のガイドラインに従います。

- アマチュア無線周波数帯や短波周波数帯など、流合の問題が判明している周波数を避けます。
- 20 MHz 未満の不適切なスペクトルを避けます。
- 周波数ホッピングに予備の帯域を許可します。
- 共有スペクトル グループ内の同じコンバイナ グループにアップストリーム ポートを配置します。
- 受信電力レベルの設定によって、多少の等化調整を行います。

インテリジェント型および高度なスペクトル管理の設定タスク

ここでは、シスコのケーブルインターフェイスラインカードで使用できるインテリジェント型および高度なスペクトル管理機能対応の Cisco uBR7200 シリーズまたは Cisco uBR10012 ユニバーサル ブロードバンド ルータを設定するために必要な設定タスクについて説明します。

スペクトル グループの設定と割り当て

インテリジェント型および高度なスペクトル管理機能を使用する前に、スペクトル グループを作成および設定する必要があります。この手順は、ガイド型およびスケジュール型スペクトル管理で使用する手順と同じで、次のセクションに記載されています。

- http://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_cbr_layer2_docsis/spectrum_management.html#task_1044164
- http://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_cbr_layer2_docsis/spectrum_management.html#task_4BF4590BA65D4CF1851A4DA0C8A9ADB2

スペクトル グループを設定し、アップストリームに割り当てたら、Cisco IOS ソフトウェアでは、このソフトウェアをサポートするケーブル インターフェイス ライン カードで高度な周波数ホッピング アルゴリズムが自動的に使用されます。

（注） インテリジェント型および高度なスペクトル管理機能を効率的に使用するには、スペクトル グループを作成するときに、固定周波数ではなく、周波数帯域のみを設定することを推奨します。スペクトル グループでは、周波数ホッピングが発生する前に設定したチャネル幅で少なくとも 2 つの中心周波数を見つけられるように、ケーブル インターフェイスに十分な周波数帯域幅を設定する必要があります。

アップストリームの動的変調の設定（CNR ベース）

CNR ベース バージョンのアップストリームの動的変調機能の設定は、この機能の MER（SNR）バージョンの設定に似ています。

1. プライマリ変調プロファイルを作成します。このプロファイルは通常、帯域幅の効率性に優れていますが、堅牢性はそれほどでもありません。
2. セカンダリ変調プロファイルを作成します。このプロファイルは通常、帯域幅の効率性には劣りますが、優れた堅牢性があります。

ヒント 変調プロファイルを作成する場合は、各変調プロファイルのそれぞれのバースト パラメータを手動で指定する代わりに、定義済み変調プロファイルを使用することを推奨します。

3. 任意のケーブル インターフェイスとアップストリームにプロファイルを割り当てます。

変調プロファイルを作成し、アップストリームに割り当てたら、Cisco IOS ソフトウェアでは、このソフトウェアをサポートするケーブル インターフェイス ライン カードで CNR ベース バージョンのアップストリームの動的変調機能が自動的に使用されます。

制約事項

- アップストリームの動的変調機能は、DOCSIS 1.0 または DOCSIS 1.1 TDMA 専用の変調プロファイルのみでサポートされます。DOCSIS 2.0 混合モードまたは A-TDMA 専用モードの変調プロファイルではサポートされません。
- 3 段階の動的変調は、CNR ベース バージョンのアップストリームの動的変調ではサポートされません。
- CNR ベースのアップストリームの動的変調機能は、A-TDMA 変調プロファイルをサポートしていません。ただし、A-TDMA は、MER（SNR）ベースのアップストリームの動的変調機能でサポートされています。

アップストリームにプライマリおよびセカンダリ プロファイルを割り当てるには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cablemodulation-profile** *profile* {**mix**| **qam-16** | **qpsk** | **robust-mix**} 例： `Router(config)# cable modulation-profile 3 mix`	DOCSIS 1.0 または DOCSIS 1.1 TDMA アップストリームで使用するプライマリ変調プロファイルを作成します。 通常、プライマリ プロファイルは **qam-16** または **mix** のどちらかです。 （注） DOCSIS 1.0 または DOCSIS 1.1 TDMA アップストリームで使用するセカンダリ プロファイルを作成するには、このコマンドを繰り返します。通常、セカンダリ プロファイルは **robust-mix** または **qpsk** のどちらかです。 （注） また、個別のバースト パラメータの値を設定することにより、**cablemodulation-profile** コマンドでカスタム変調プロファイルを作成することもできます。ただし、各パラメータの変更が DOCSIS MAC レイヤにどのような影響を与えるかを熟知していない場合は、このパラメータを変更しないでください。ケーブル設備の大部分には、デフォルトの定義済み変調プロファイルを使用することを推奨します。
ステップ 4	**controller upstream-cable** *slot*/*subslot*/*port* 例： `Router(config)# controller upstream-cable 9/0/15`	コントローラ コンフィギュレーション モードを開始します。
ステップ 5	**cableupstream** *n* **modulation-profile** *primary-profile-number secondary-profile-number*	プライマリ変調プロファイルと、オプションのセカンダリ変調プロファイルを指定したアップストリーム ポートに割り当てます。

	コマンドまたはアクション	目的
	例： `Router(config-controller)# cable upstream 0 modulation-profile 3 4`	
ステップ 6	**end** 例： `Router(config-controller)# end`	コントローラ インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

プロアクティブなチャネル管理

高度なスペクトル管理機能をサポートするケーブル インターフェイス ライン カードで次のパラメータを使用して設定すると、カードのアップストリームでプロアクティブなチャネル管理操作を微調整できます。

- アップストリームのノイズが変調プロファイルのしきい値を超えた場合に実行する修正措置の優先順位。
- アップストリームとその 2 つの変調プロファイルの CNR（CNiR）と MER（SNR）のしきい値および FEC 値。
- 周波数ホッピングまたは変調スイッチングでもアップストリームの問題を回避できない場合に使用できるチャネル幅の許容範囲。

次のすべてのパラメータにはデフォルト設定があるため、実際の設備の特性に合うようにパラメータを変更しない限りは、この手順を実行する必要はありません。

パラメータを設定するには、次の手順に従います。

プロアクティブなチャネル管理

Cisco CMTS ルータの 1 つの物理ポートで 2 つの論理チャネルを設定することができます。論理チャネルを設定すると、アップストリーム関連のコマンドが、物理ポート レベルと論理チャネル レベルの 2 つのグループに分類されます。

物理ポート レベル

物理ポート レベルのコマンドの形式は **cableupstream** *n* です。ここで、*n* は物理ポート番号を表します。

論理チャネル レベル

論理チャネル レベルのコマンドの形式は **cableupstream** *n m* です。ここで *n* は物理ポート番号を表し、*m* は論理チャネル インデックス番号（0 または 1）を表します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**controller upstream-cable** *slot*/*subslot*/*port* 例： `Router(config)# controller upstream-cable 9/0/0`	コントローラ コンフィギュレーション モードを開始します。
ステップ 4	**us-channel** *n***hopmodulationfrequencychannel-width** 例： `Router(config-controller)# us-channel 0 hop modulation frequency channel-width`	アップストリームのノイズが現在の変調プロファイルで指定したしきい値を超えた場合に実行する 3 種類の修正措置（**modulation**、**frequency**、および **channel-width**）の優先度を指定します。デフォルトの優先度は、**frequency**、**modulation**、**channel-width** です。 （注） **channel-width** オプションの位置は、必ず **frequency** オプションの後でなければなりません。
ステップ 5	**cableupstream** *n* **thresholdcnr-profiles** *threshold1-in-db threshold2-in-db* 例： `Router(config-controller)# cable upstream 2 threshold  cnr-profiles 23 14`	（任意）アップストリームとその 2 つの変調プロファイルの CNR（CNiR）のしきい値および FEC 値を指定します。 （注） プライマリとセカンダリの CNR（CNiR）のしきい値を両方とも回避するには、最初のパラメータ（*threshold1-in-db*）を 0 に設定します。これにより、2 つ目のパラメータ（*threshold2-in-db*）が拒否され、CNR（CNiR）の両方のしきい値が回避されます。
ステップ 6	次のいずれかのコマンドを使用します。 • **cableupstreamnupstreamthresholdsnr-profiles** *threshold1-in-db threshold2-in-db*	（任意）アップストリームとその 2 つの変調プロファイルの MER（SNR）のしきい値および FEC 値を指定します。

	コマンドまたはアクション	目的
	• • **cableupstream** *n* *m***upstreamthresholdsnr-profiles** *threshold1-in-db threshold2-in-db* • 例： `Router(config-controller)# cable upstream 2 threshold  snr-profiles 23 14`	（注） プライマリ MER（SNR）のしきい値（*threshold1-in-db*）を 0 に設定すると回避できます。ただし、2 つ目のパラメータ（*threshold2-in-db*）を入力する必要があります。
ステップ 7	**cableupstream** *n***thresholdhysteresis** *hysteresis-in-db* 例： `Router(config-controller)# cable upstream 2 threshold hysteresis 3`	（任意）動的変調アップグレードのしきい値と組み合わせて使用するヒステリシス値を指定します。 （注） この値を 0 に設定することで、**hysteresis** しきい値をバイパスできます。
ステップ 8	次のいずれかのコマンドを使用します。 • **cableupstream** *n* **threshold corr-fec** *corrfec-threshold* • **cableupstream** *n* *m***threshold corr-fec** *corrfec-threshold* 例： `Router(config-controller)# cable upstream 5 threshold  corr-fec 5`	（任意）アップストリームとその 2 つの変調プロファイルの CNR（CNiR）のしきい値および FEC 値を指定します。 （注） この値を 0 に設定することで、**corr-fec** しきい値をバイパスできます。
ステップ 9	次のいずれかのコマンドを使用します。 • **cableupstream** *n* **threshold uncorr-fec** *uncorrfec-threshold* • **cableupstream** *n* *m***threshold uncorr-fec** *uncorrfec-threshold* 例： `Router(config-controller)# cable upstream 5 threshold  uncorr-fec 1`	（任意）アップストリームとその 2 つの変調プロファイルの CNR（CNiR）のしきい値および FEC 値を指定します。 （注） この値を 0 に設定すると、un**corr-fec** しきい値を回避できます。 （注） 通常のプラントの使用では、チャネルに許容できない数のエラーが発生しないように、修正不可能な FEC のしきい値をデフォルトの 1 % のままにしておくことを推奨します。
ステップ 10	**cableupstream** *n* **channel-width** *first-choice-width* [*last-choice-width*]	

	コマンドまたはアクション	目的
	例： `Router(config-controller)# cable upstream 0 channel-width 800000 800000`	
ステップ 11	**end** 例： `Router(config-controller)# end`	コントローラインターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

スペクトル管理の設定の確認

スペクトル管理の設定を確認するには、次の手順に従います。

手順

ステップ 1 入力した設定値を確認するには、特権 EXEC モードで **showrunning-config** コマンドを実行します。

例：
```
Router# show running-config
```

ステップ 2 各変調プロファイルの設定を表示するには、特権 EXEC モードで **show cable modulation-profile** コマンドを実行します。

例：
```
Router# show cable modulation-profile
```

特定の変調プロファイルの設定を表示するには、特権 EXEC モードでプロファイル番号を **show cable modulation-profile** コマンドに追加します。

例：
```
Router# show cable modulation-profile 6
```

ステップ 3 各アップストリームのステータスおよび設定を表示するには、特権 EXEC モードで **showcontrollerscableupstream** コマンドを実行します。次の例に、ケーブル ライン カードのアップストリーム 0 の情報を示します。

例：
```
Router# show controller cable 8/1/14 upstream 0

 Cable8/1/14 Upstream 0 is up
  Frequency 19.504 MHz, Channel Width 3.200 MHz, Symbol Rate 2.560 Msps
  Modulations (64-QAM) - A-short 64-QAM, A-long 64-QAM, A-ugs 64-QAM
  Mapped to shared connector 18 and receiver 56
  Spectrum Group 8
  MC3Gx60  CNR measurement : 30 dB
```

```
US phy MER(SNR)_estimate for good packets - 32.5530 dB
Nominal Input Power Level 0 dBmV, Tx Timing Offset 1547
Ranging Backoff Start 3, Ranging Backoff End 6
US timing offset adjustment type 0, value 0
Ranging Insertion Interval automatic (60 ms)
US throttling off
Tx Backoff Start 3, Tx Backoff End 5
Modulation Profile Group 221
Concatenation is enabled
Fragmentation is enabled
part_id=0x3142, rev_id=0xC0, rev2_id=0x00
nb_agc_thr=0x0000, nb_agc_nom=0x0000
Range Load Reg Size=0x58
Request Load Reg Size=0x0E
Minislot Size in number of Timebase Ticks is = 2
Minislot Size in Symbols = 32
Bandwidth Requests = 0xEE3AF
Piggyback Requests = 0x6A24F
Invalid BW Requests= 0x76
Minislots Requested= 0xC33362
Minislots Granted  = 0x158609
Minislot Size in Bytes = 24
Map Advance (Dynamic) : 2581 usecs
Map Count Internal = 330309891
No MAP buffer= 0x0   No Remote MAP buffer= 0x0
Map Counts: Controller 8/1/0 = 1321230158
UCD Counts:
  Controller 8/1/0:0 = 336057
  Controller 8/1/0:1 = 336057
  Controller 8/1/0:2 = 336057
  Controller 8/1/0:3 = 336057

UCD procedures on lch 0
UCD ucd-succeeds(5) ucd-shut(0) init-state-err(0)
UCD init-tss-err(0) init-timeout(0) init-start-err(0)
UCD ucd-ccc-time(0) ucd-timeout(0) ucd-tss-err(0)
UCD ucd-state-err(0) ucd-process(0) ucd-retries(0)
UCD stale-tss(0)
ATDMA mode enabled
PHY: us errors 0  us recoveries 0 (enp 0)
MAC PHY TSS: tss error start 0  tss error end 0
MAC PHY Status: bcm3140 status 0  lookout status 0
PHY: TSS late 0  discontinuous 0
PHY: TSS mis-match 0  not-aligned 0
PHY: TSS missed snapshots from phy 0
MAP/UCD Replication Instructions:
  Controller 8/1/0 index = 477, bitmap = 0x000F
Dynamic Services Stats:
DSA: 0  REQs  0 RSPs  0 ACKs
0 Successful DSAs  0 DSA Failures
DSC: 0  REQs  0 RSPs  0 ACKs
0 Successful DSCs  0 DSC Failures
DSD:  0 REQs  0 RSPs
0 Successful DSDs  0 DSD Failures
Dropped MAC messages: (none)
```

ステップ 4　各アップストリームのホッピング間隔およびホッピングしきい値を表示するには、特権EXECモードで **showcablehop** コマンドを実行します。

例：

```
Router# show cable hop

 Upstream    Port       Poll Missed Min    Missed Hop   Hop     Corr    Uncorr
 Port        Status     Rate Poll   Poll   Poll   Thres Period  FEC     FEC
                        (ms) Count  Sample Pcnt   Pcnt  (sec)   Errors  Errors
Cable3/0/U0 20.800 Mhz 105  0      20         0%   25%  45     1       4
Cable3/0/U1 20.800 Mhz 105  0      48         0%   25%  45     2       19
Cable3/0/U2 23.120 Mhz 105  0      45         0%   25%  45     0       5
Cable3/0/U3 22.832 Mhz 105  0      26         0%   25%  45     0       6
```

```
Cable3/0/U4 22.896 Mhz 105  0      43         0%   25%  45     0       7
Cable3/0/U5 23.040 Mhz 105  0      54         0%   25%  45     1       3
Cable4/0/U0 22.896 Mhz 117  0      26         0%   25%  45     0       2
Cable4/0/U1 23.168 Mhz 117  0      87         0%   25%  45     4       2
Cable4/0/U2 22.896 Mhz 117  0      23         0%   25%  45     1       0
Cable4/0/U3 20.800 Mhz 117  0      54         0%   25%  45     0       0
Cable4/0/U4 22.928 Mhz 117  0      22         0%   25%  45     0       1
Cable4/0/U5 22.960 Mhz 117  0      0       -----   25%  45     0       0
```

ステップ 5 周波数、変調、チャネル幅について、時間や理由に関係なく、ある状態から別の状態への変化を表示するには、**show cable hop** コマンドの **history** オプションを使用します。

例：

```
Router# show cable hop c8/1/1 u0 history

F = Frequency Hop, M = Modulation Change, C = Channel Width Change
Upstream   Action             Chg    Chg    Action
Port       Time          Code From   To     Reason
C8/1/1 U0  Feb 20 12:21:29 M  142    141    SNR 28>=28 CFEC 0<=3 UnCFEC 0<=1
           Feb 20 12:09:08 F   0.000 24.000 Configuration changed
```

ステップ 6 MER（SNR）、CNR（CNiR）、およびFECのしきい値を表示するには、**show cable hop** コマンドの **threshold** オプションを使用します。

例：

```
Router# show cable hop c8/1/1 u0 threshold

Upstream   SNR(dB)          CNR(dB)          CorrFEC%  UncorrFEC%       MissedSM%
Port       Val Thre1 Thre2 Val Thre1 Thre2 Pcnt Thre Pcnt Thre        Pcnt Thre
C8/1/1 u0  33   23   14    60   25   15    0    1    0    2           0    50
```

ステップ 7 各スペクトル グループの割り当てを表示するには、特権EXECモードで**showcablespectrum-group** コマンドを実行します。

例：

```
Router# show cable spectrum-group

Group  Frequency      Upstream      Weekly Scheduled          Power   Shared
No.    Band           Port          Availability              Level   Spectrum
       (MHz)                        From Time:    To Time:    (dBmV)
1      42.967 [3.20]  UC2/0/4:U0                              -1      No
1      83.400 [3.20]  UC2/0/4:U1                              -1      No
1      80.200 [3.20]  UC2/0/4:U2                              -1      No
1      42.922 [3.20]  UC2/0/4:U3                              -1      No
1      17.677 [3.20]  UC2/0/5:U0                              -1      54
1      10.603 [3.20]  UC2/0/5:U1                              -1      54
```

上記の例では

- No：ファイバ ノードが設定されていません
- 54：ファイバ ノードの ID

ステップ 8 特定のケーブル モデムの現在の CNR（CNiR）値を表示するには、特権 EXEC モードで **showcablemodemcnr** コマンドを実行します。

例：

```
Router# show cable modem 5.100.1.94 cnr
```

```
MAC Address    IP Address      I/F         MAC         Prim  snr/cnr
                                           State       Sid   (dB)
0018.689c.17b8 5.100.1.94      C7/0/0/U1   online      428   36.12
```

スペクトル管理のモニタリング

Cisco CLI コマンドまたはSNMP のいずれかを使用して、Cisco CMTS でのスペクトル管理アクティビティをモニタリングできます。

詳細については、次の項を参照してください。

CLI コマンドの使用

次のコマンドは、アップストリームのスペクトルの状態に関する情報を表示します。

コマンド	目的
Router# **show cable hop**[**cable***x/y*] [**upstream** *usport*]	ルータのすべてのアップストリーム、1つのケーブル インターフェイス ライン カード上のすべてのアップストリーム、または1つのアップストリームについて、ホップ間隔、ホップのしきい値、FEC エラー カウンタが表示されます。
Router# **show cable hop** [**cable** *x/y[z]*] [**upstream** *n*][*thresholds*]	MER（SNR）の設定値と現在の値をdBで、CNR（CNiR）は dB で、CorrFEC はパーセントで、UncorrFEC はパーセントで、失われたステーション メンテナンスは指定したアップストリームのパーセントで表示されます。
Router# **show cable hop history**	1 CMTS 全体に対して **showcablehophistory** コマンドを使用すると、アクションごとの最新の変更が表示されます。 2 MAC ドメインに対して **showcablehophistory** コマンドを使用すると、アクションごとの最新の 3 件の変更が表示されます。 3 特定のアップストリームに対して **showcablehophistory** コマンドを使用すると、アクションごとの最新の 10 件の変更が表示されます。変更は新しい順に時系列で表示されます。
Router# **show cable hop** [**cable** *x/y[z]*] [**upstream** *n*][**summary**	1 時間ごと、1 日ごと、1 週間ごと、30 日の稼働平均、システムが起動されて以来の平均が、指定したアップストリームごとに表示されます。
Router# **show cable hop** [**cable** *x/y[z]*] [**upstream** *n*] **[history]**	周波数、変調、チャネル幅について、時間や理由に関係なく、ある状態から別の状態への変化が表示されます。
Router# **show cable modem** [*ip-address* | *interface* | *mac-address*] [*options*]	登録および未登録ケーブルモデムの情報がMER（SNR）値を含めて表示されます。
Router# **show cable modulation-profile** [*num*] [**initial** | **long** | **reqdata** | **request** | **short** | **station**]	

コマンド	目的
	すべての変調プロファイルについて、特定の変調プロファイルについて、または特定の変調プロファイルの特定のバーストタイプについて、設定情報が表示されます。
`Router# show cable spectrum-group[groupnum] [detail]`	設定済みのスペクトルグループ情報が表示されます。
`Router# show controllers cable x/y upstream n [ip-address | mac-address] start-freq end-freq res-freq`	現在の周波数、チャネル幅、変調レート、スペクトルグループを含めて、アップストリームの状況が表示されます。
`Router# show controllers cable x/y upstream n spectrum [ip-address | mac-address] start-freq end-freq res-freq`	特定のケーブル モデムの雑音レベル、またはアップストリーム全体のバックグラウンド雑音が表示されます。

（注） **showcableflap-list** コマンドを使用すると、CMTS ルータのフラップ リストが表示されます。フラップ リストから、アップストリームのケーブル モデムで問題が発生しているか、発生している場合はどのようなタイプの問題であるかといった補足情報が得られます。ケーブル モデム フラッピングの詳細とケーブル モデム フラップ リストのモニタリング方法については、「Flap List Troubleshooting for the Cisco CMTS Routers」を参照してください。

SNMP の使用

SNMP を使用すると、スペクトル管理アクティビティをモニタできます。SNMP マネージャは、CiscoView や Cable Broadband Troubleshooter（リリース 3.0 以降）のようにグラフィックベースです。

次の MIB 属性を使用して SNMP サポートを提供できるように、CISCO-CABLE-SPECTRUM-MIB が強化されています。

ccsSNRRequestTable

次の表に、ccsSNRRequestTable の属性を示します。この属性には、アップストリームで各ケーブル モデムのために行われた CNR（CNiR）の測定値が含まれます。

表 *59* : *ccsSNRRequestTable* 属性

属性	タイプ	説明
ccsSNRRequestIndex	Integer32	各テーブル エントリを特定する任意のインデックス。
ccsSNRRequestMacAddr	MacAddress	報告されたリモート オンライン ケーブル モデムの MAC アドレス。
ccsSNRRequestSNR	Integer32	MER（SNR）の測定値（dB）です。動作状況が [running] の場合、この値は 0 です。
ccsSNRRequestOperation	CCSRequestOperation	現在の動作を設定します。[start]、[pending]、[running]、または [abort]。
ccsSNRRequestOperState	CCSRequestOperState	現在の動作状態を報告します。[idle]、[pending]、[running]、[noError]、[aborted]、[notOnLine]、[invalidMac]、[timeOut]、[fftBusy]、[fftFailed] など。
ccsSNRRequestStartTime	Timestamp	MER（SNR）測定動作の開始時間が含まれます。
ccsSNRRequestStoppedTime	Timestamp	MER（SNR）測定動作の終了時間が含まれます。
ccsSNRRequestStatus	RowStatus	テーブル エントリの修正、作成、および削除を制御します。

ccsSpectrumRequestTable

次の表に、ccsSpectrumRequestTable の各エントリの属性を示します。この属性は、特定のケーブル モデムのスペクトル プロファイルの取得またはアップストリーム全体のバックグラウンド MER（SNR）の取得に使用されます。

表 *60*：*ccsSpectrumRequestTable* 属性

属性	タイプ	説明
ccsSpectrumRequestIndex	Integer32	各テーブル エントリを特定する任意のインデックス。
ccsSpectrumRequestIfIndex	InterfaceIndexOrZero	アップストリームを特定するインターフェイス。
ccsSpectrumRequestMacAddr	MacAddress	特定のケーブル モデムに MER（SNR）値を指定する MAC アドレス、またはスペクトル全体のバックグラウンド ノイズを示す 0000.0000.0000。
ccsSpectrumRequestUpperFreq	CCSFrequency	モニタする周波数範囲の上限周波数（5000 ～ 42000 KHz、デフォルトは 42000 KHz）。
ccsSpectrumRequestLowFreq	CCSFrequency	モニタする周波数範囲の下限周波数（5000 ～ 42000 KHz、デフォルトは 5000 KHz）。
ccsSpectrumRequestResolution	Integer32	サンプリングする周波数範囲の決定に必要な解像度（12 ～ 37000 KHz、デフォルトは 60 KHz）。
ccsSpectrumRequestStartTime	Timestamp	スペクトル測定の開始時間。
ccsSpectrumRequestStoppedTime	Timestamp	スペクトル測定の終了時間。
ccsSpectrumRequestOperation	CCSRequestOperation	新しいスペクトル管理要求を開始したり、現在の要求を中止します。
ccsSpectrumRequestOperState	CCSRequestOperState	現在のスペクトル管理要求の動作状態を表示します。
ccsSpectrumRequestStatus	RowStatus	テーブル エントリの修正、作成、および削除を制御します。

ccsSpectrumDataTable

以下の表に、ccsSpectrumDataTableの各エントリの属性を示します。この表にはスペクトル要求の結果が含まれます。

表 *61*：*ccsSpectrumDataTable* 属性

属性	タイプ	説明
ccsSpectrumDataFreq	CCSMeasuredFrequency	この電力測定の実行に必要な周波数（KHz）。
ccsSpectrumDataPower	INTEGER	特定の周波数（– 50 ～ 50 dBmV）で測定された受信電力。

（注） ccsSpectrumRequestTable 表と ccsSpectrumDataTable 表にある情報は、**showcontrollerscableupstreamspectrum** コマンドによって表示される情報と同じです。

ccsUpSpecMgmtTable

次の表に、ccsUpSpecMgmtTableの属性を示します。各周波数ホップを記述するエントリを示しています。

表 *62*：*ccsUpSpecMgmtEntry* 属性

属性	タイプ	説明
ccsUpSpecMgmtHopPriority	INTEGER	アップストリームの過剰なノイズに対応する措置を決める際に、周波数、変調プロファイル、およびチャネル幅の優先度を指定します（デフォルトは、周波数、変調プロファイル、およびチャネル幅の順です）。
ccsUpSpecMgmtSnrThres1	Integer32	変調プロファイル 1（5 ～ 35 dB、デフォルトは 25）の上位 MER（SNR）のしきい値を指定します。

属性	タイプ	説明
ccsUpSpecMgmtSnrThres2	Integer32	変調プロファイル 2（5 ～ 35 dB、デフォルトは 13）の上位 MER（SNR）のしきい値を指定しますが、ccsUpSpecMgmtSnrThres1 で指定したよりも低い値でなければなりません。
ccsUpSpecMgmtFecCorrectThres1	Integer32	変調プロファイル 1 の修正可能な FEC エラーしきい値を指定します（1 ～ 20%）。
ccsUpSpecMgmtFecCorrectThres2	Integer32	廃止されており、すでに使用されていません。
ccsUpSpecMgmtFecUnCorrectThres1	Integer32	変調プロファイル 1 の修正不可能な FEC エラーしきい値を指定します（1 ～ 20%）。
ccsUpSpecMgmtFecUnCorrectThres2	Integer32	廃止されており、すでに使用されていません。
ccsUpSpecMgmtSnrPollPeriod	Integer32	廃止されており、すでに使用されていません。
ccsUpSpecMgmtHopCondition	INTEGER	周波数ホップを引き起こす状況を報告します（MER [SNR] 値またはモデムのオフラインの割合）。
ccsUpSpecMgmtFromCenterFreq	CCSFrequency	最新の周波数ホップの前に中心周波数（KHz）を表示します。
ccsUpSpecMgmtToCenterFreq	CCSFrequency	最新の周波数ホップの後に現在の中心周波数（KHz）を表示します。
ccsUpSpecMgmtFromBandWidth	CCSFrequency	最新の周波数ホップの前にチャネル幅（KHz）を表示します。
ccsUpSpecMgmtToBandWidth	CCSFrequency	最新の周波数ホップの後に現在のチャネル幅（KHz）を表示します。

属性	タイプ	説明
ccsUpSpecMgmtFromModProfile	Integer32	最新の周波数ホップの前に変調プロファイル番号を表示します。
ccsUpSpecMgmtToModProfile	Integer32	最新の周波数ホップの後に現在の変調プロファイル番号を表示します。
ccsUpSpecMgmtSNR	Integer32	アップストリームの現在のMER（SNR）値（dB）を表示します。
ccsUpSpecMgmtCnrThres1	Integer32	変調プロファイル 1（5 ～ 35 dB、デフォルトは 25）の上位CNR（CNiR）のしきい値を指定します。
ccsUpSpecMgmtCnrThres2	Integer32	変調プロファイル 2（5 ～ 35 dB、デフォルトは 13）の上位CNR（CNiR）のしきい値を指定しますが、ccsUpSpecMgmtCnrThres1 で指定したよりも低い値でなければなりません。
ccsUpSpecMgmtCNR	Integer32	アップストリームの現在のCNR（CNiR）値（dB）を表示します。
ccsUpSpecMgmtMissedMaintMsgThres	Integer32	スペクトル グループで失われたステーション メンテナンス メッセージの割合で周波数ホップのしきい値を表示します。
ccsUpSpecMgmtHopPeriod	Integer32	周波数ホップの間隔の最小時間を秒単位で表示します。

ccsHoppingNotification

次の表に、各周波数ホップの後に送信された通知に含まれる属性を示します。

表 *63*：*ccsHoppingNotification* 属性

属性	タイプ	説明
ccsUpSpecMgmtHopCondition	INTEGER	周波数ホップを引き起こす状況を報告します（MER [SNR] 値またはモデムのオフラインの割合）。
ccsUpSpecMgmtFromCenterFreq	CCSFrequency	最新の周波数ホップの前に中心周波数（KHz）を表示します。
ccsUpSpecMgmtToCenterFreq	CCSFrequency	最新の周波数ホップの後に現在の中心周波数（KHz）を表示します。
ccsUpSpecMgmtFromBandWidth	CCSFrequency	最新の周波数ホップの前にチャネル幅（KHz）を表示します。
ccsUpSpecMgmtToBandWidth	CCSFrequency	最新の周波数ホップの後に現在のチャネル幅（KHz）を表示します。
ccsUpSpecMgmtFromModProfile	Integer32	最新の周波数ホップの前に変調プロファイル番号を表示します。
ccsUpSpecMgmtToModProfile	Integer32	最新の周波数ホップの後に現在の変調プロファイル番号を表示します。

設定例

ここでは、次の設定例について説明します。

スペクトル グループとコンバイナ グループの例

次の例により、スペクトルグループとコンバイナグループが設定され、アクティブになっているかを確認することができます。

例：スペクトル グループの作成の確認

スペクトル グループの作成が完了したことを確認するには、**showcablespectrum-group** コマンドを入力します。

```
Router# show cable spectrum-group
spectrum-group 1
spectrum-group 2
spectrum-group 3
```

例：タイム スケジュール型スペクトル グループ

ケーブル設備に 1 週間サイクルのアップストリーム雑音特性がある場合には、タイム スケジュール型スペクトル割り当てを使用します。

```
Router(config)# cable spectrum-group 1 time Mon 08:00:00 frequency 21600000
```

削除するには、**delete** キーワードを使用します。

```
Router(config)# cable spectrum-group 1 time Mon 18:00:00 delete frequency 21600000
```

例：スペクトル グループの設定の確認

スペクトル グループの設定と有効化が完了したかどうかを確認するには、**showcablespectrum-group** コマンドを入力します。次のコマンドにより、各スペクトル グループ、そのグループに割り当てられた周波数、グループが割り当てられるアップストリーム ポート、グループにスケジュールがあるかどうか、現在の測定電力レベル、共有スペクトル グループであるかどうかが表示されます。

```
Router# show cable spectrum-group

22:07:46: %SYS-5-CONFIG_I: Configured from console by console
Group  Frequency      Upstream     Weekly Scheduled            Power   Shared
No.    Band           Port         Availability                Level   Spectrum
       (Mhz)                       From Time:    To Time:      (dBmV)
1       5.000-15.000                                           0       Yes
1      12.000                                                  0       Yes
1      22.000         Cable6/0 U5                              7       Yes
2      29.000         Cable6/0 U4                              6       No
2      26.000                                                  0       No
3      35.000-41.000                                           0       No
3      16.000-19.000  Cable6/0 U3                              5       No
5*      5.000-10.000               Thu 21:50:00  Thu 21:45:00  0       Yes
```

例：コンバイナ グループに割り当てるアップストリーム ポートの特定

次に、コンバイナ グループ A ～ J が指定された CMTS のトポロジ例を示します。コンバイナ グループ C ～ E は、共有スペクトル グループで設定された複数のアップストリーム ポートを持ちます。他のアップストリームは、非共有スペクトル グループで設定する必要があります。

次の例では、3 つのスペクトル グループから 10 のコンバイナ グループが周波数ホッピング テーブルで使用されます。

```
Cable3/0
DS +------+ Upconverter +----- laser group 1
U0 +------ combiner group A
U1 +------ combiner group B
U2 +-------combiner group C
U3 +-------combiner group C
```

```
U4 +----- combiner group D
U5 +------combiner group E
Cable4/0
DS +-----+ Upconverter +----- laser group 2
U0 +------combiner group E
U1 +----- combiner group F
U2 +----- combiner group G
U3 +----- combiner group H
U4 +----- combiner group I
U5 +----- combiner group J
```

レーザー グループとは、同じダウンストリーム信号を共用する 1 組のファイバ ノードを意味します。ノードごとに個別のフィードを発生させるには、通常、光スプリッタを使用します。

ダウンストリーム方向で、6 MHz のチャネル スロットが 2 つ割り当てられています。コンバイナ グループ A ～ E のすべてのファイバ ノードには、Cable3/0 からのダウンストリーム信号が含まれるチャネル スロットが与えられる必要があります。コンバイナ グループ A ～ E は、レーザー グループ 1 に属していることになります。

コンバイナ グループ E ～ J のすべてのファイバ ノードには、Cable4/0 からのダウンストリーム信号が含まれるチャネル スロットが与えられる必要があります。コンバイナ グループ E ～ J は、レーザー グループ 2 に属していることになります。

コンバイナ グループ E は 2 つのレーザー グループに属しているので、Cable3/0 および Cable4/0 に対応する 2 種類のダウンストリーム チャネル スロットがあります。

例：コンバイナ グループ

次に、すべてのアップストリーム ポートのスペクトル管理を有効にし、すべてのコンバイナ グループで 20 ～ 26 MHz の周波数帯域を使用する例を示します。

```
CMTS01(config)# cable spectrum-group 1 band 20000000 26000000
CMTS01(config)# cable spectrum-group 2 shared
CMTS01(config)# cable spectrum-group 2 band 20000000 26000000
CMTS01(config)# cable spectrum-group 3 shared
CMTS01(config)# cable spectrum-group 3 band 20000000 26000000
CMTS01(config)# controller upstream-Cable 9/0/0
CMTS01(config-controller)# cable spectrum-group 1
CMTS01(config-controller)# cable upstream 2 spectrum-group 2
CMTS01(config-controller)# cable upstream 3 spectrum-group 2
CMTS01(config-controller)# cable upstream 5 spectrum-group 3
CMTS01(config-controller)# exit
CMTS01(config)# controller upstream-Cable 9/0/1
CMTS01(config-controller)# cable spectrum-group 1
CMTS01(config-controller)# cable upstream 0 spectrum-group 3
```

スペクトル グループ 1 ～ 3 の説明は次のとおりです。

- スペクトル グループ 1：これは非共有グループです。アップストリーム RF ドメインが、各メンバーのアップストリーム ポートごとに存在します。

```
Upstream Port   RF Domain
Cable3/0 U0     combiner group A
Cable3/0 U1     combiner group B
Cable3/0 U4     combiner group D
Cable4/0 U1     combiner group F
Cable4/0 U2     combiner group G
Cable4/0 U3     combiner group H
Cable4/0 U4     combiner group I
Cable4/0 U5     combiner group J
```

- スペクトル グループ 2：これは共有グループです。存在するアップストリーム RF ドメインは 1 つです。

```
Upstream Port   RF Domain
Cable3/0 U2     combiner group C
Cable3/0 U3     combiner group C
```

- スペクトル グループ 3：これは共有グループです。存在するアップストリーム RF ドメインは 1 つです。

```
Upstream Port   RF Domain
Cable3/0 U5     combiner group E
Cable4/0 U0     combiner group E
```

各 RF ドメインの 20 ～ 26 MHz 帯域に関して、スペクトルは各メンバー ポートのチャネル幅設定に従ってチャネル化されます。たとえば、Cable3/0 のポート U2 および U3 は、それぞれ 3.2 MHz および 1.6 MHz のチャネル幅に設定され、スペクトル グループ 2 では次のチャネル化が使用されます。

```
> Channel Width Start Stop Center
>           (Mhz) (Mhz) (Mhz) (Mhz)
> 1        3.2    20.0 23.2 21.6
> 2*       1.6    20.0 21.6 20.8
> 3*       1.6    21.6 23.2 22.4
> 4        1.6    23.2 24.8 24.0
```

（注） チャネル 2 および 3 は、チャネル 1 の使用中は利用できません。

グループが共用されるので、ポート U2 および U3 は、オーバーラップしないように、それぞれチャネル 1 および 4 が割り当てられます。

（注） 各ポートに代替周波数割り当てはなく、24.8～26.0 MHz の帯域幅は無駄になります。代替チャネルを作成するには、上限の境界を 26.0 MHz から 28.0 MHz に引き上げます。

```
> Channel  Width  Start Stop  Center
>           (Mhz)  (Mhz) (Mhz) (Mhz)
>  1        3.2    20.0  23.2  21.6
>  2        3.2    23.2  26.4  24.8
>  3        1.6    20.0  21.6  20.8
>  4        1.6    21.6  23.2  22.4
>  5        1.6    23.2  24.8  24.0
>  6        1.6    24.8  26.4  25.6
>  7        1.6    26.4  28.0  27.4
```

チャネル幅が小さい場合、スペクトル割り当てを引き下げてみてください。そうしないと、多数のアップストリームチャネルスロットが生じ、周波数ホッピングで雑音のないスロットを見つけるまでに数分かかる場合があります。

例：その他のスペクトル管理の設定

さまざまなスペクトル グループを設定するには、次の例を参照してください。

- アップストリーム帯域が 12,000,000 ～ 18,000,000 Hz でデフォルト電力レベルが 0 dBmV のスペクトル グループ 3 を設定するには、次の例を使用します。

```
Router(config)# cable spectrum-group 3 band 12000000 18000000
```

- スペクトル グループ 3 で電力レベルが 13 dBmV に変更された有効帯域幅のリストに 20,000,000 ～ 24,000,000 Hz のアップストリーム帯域を追加するには、次の例を使用します。

```
Router(config)# cable spectrum-group 3 band 20000000 24000000 13
```

- デフォルト電力レベルが 0 dBmV のスケジュール型スペクトル グループ 4 で 5,000,004 ～ 40,000,000 Hz の継続帯域を設定するには、次の例を使用します。この帯域は、毎週月曜日の現地時間午後 12:00 に開始されるスペクトル グループで利用可能です。

```
Router(config)# cable spectrum-group 4 time Monday 12:00:00 band 5000004 40000000
```

- 有効周波数のリストに 9,500,000 Hz のアップストリーム周波数を追加し、公称電力レベルを 5 dBmV に変更するには、次の例を使用します。スペクトル マネージャは、毎日現地時間の午前 2:00 にこのグループの周波数および電力レベルを調整します。

```
Router(config)# cable spectrum-group 3 time 02:00:00 frequency 9500000 5
```

- 周波数ホップが発生するまでの最小期間を秒数で設定するには、次の例を使用します。

```
Router(config)# cable spectrum-group 3 hop period 800
```

- ルータが自動周波数ホップを開始する前に特定する「オフライン」モデム数のしきい値（割合で表示）を設定するには、次の例を使用します。

```
Router(config)# cable spectrum-group 3 hop threshold 40
```

- 特定のスペクトル グループを共有 RF スペクトル グループとして設定するには、次の例を使用します。特定のスペクトル グループを「共有」に指定するということは、アップストリーム ポートに割り当てられているアップストリーム周波数が、別のアップストリーム ポートに割り当てられないことをルータに通知しています。

```
Router(config)# cable spectrum-group 3 shared
```

- 現在の設定から指定したスペクトル グループを削除するには、次の例を使用します。

```
Router(config)# no cable spectrum-group 3
```

アップストリームの動的変調の例

次の例では、**show cable modulation-profile** コマンドにより変調プロファイル情報を表示する方法と、**cable modulation-profile** コマンドにより変調プロファイルを定義する方法を示します。

設定の確認

手順

ステップ 1 入力した設定値を確認するには、特権 EXEC モードで **showrunning-config** コマンドを入力します。

例：
```
Router# show running-config
```

設定の変更を検討する場合は、特権 EXEC モードで **showstartup-config** コマンドを使用すると、NVRAM に保存されている情報を表示できます。

ステップ 2 変調プロファイル グループ情報を表示するには、特権 EXEC モードで **show cable modulation-profile** コマンドを使用します。

例：
```
Router# show cable modulation-profile[profile][iuc-code]
```

このコマンドでは、次の構文が使用されます。

- *profile*：（任意）プロファイル番号。有効値は 1 ～ 8 です。
- *iuc-code*：（任意）内部使用コード。

  有効なオプションは次のとおりです。

  - **initial**：初期レンジング バースト
  - **long**：長期認可バースト
  - **request**：要求バースト
  - **short**：短期認可バースト
  - **station**：ステーション レンジング バースト

例：変調プロファイル

Cisco CMTS には、メモリ内に QPSK 変調の一般的なプロファイルを定義する設定済み変調プロファイルが 1 つ常駐します。アップストリームの動的変調機能を使用するには、最初のプロファイルとは異なり、通常はより堅牢な変調方式を提供する 2 つ目のプロファイルを作成する必要があります。

次に、QAM-16 の変調プロファイルの例を示します。初期要求およびステーション メンテナンス メッセージが QPSK として送信され、short および long のデータ パケットが QAM-16 として送信されます。QAM-16 変調は QPSK よりも帯域幅効率に優れていますが、QPSK は QAM-16 よりも堅牢です。

（注） アップストリーム要求およびステーション メンテナンス メッセージは、QPSK で 640K、1280K、および 2560K シンボル/秒に設定すると、ケーブル ネットワーク上では短時間で送信されます。そのため、これらのメッセージを QPSK モードで使用すると、実際は効率が上がり、信頼性に優れたモデム接続を実現します。アップストリームの初期メンテナンス メッセージは、設定に関係なく、ケーブル ネットワーク上で送信する時間はまったく同じです。システムを QPSK 用に設定すると、初期メンテナンス中にモデムをより高速で接続でき、電力調整の作業が軽減されます。

```
Router# configure terminal
Router(config)# cable modulation-profile 2 request 0 16 1 8 qpsk scrambler 152 no-diff 64
fixed uw16
Router(config)# cable modulation-profile 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128
 fixed uw16
Router(config)# cable modulation-profile 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128
 fixed uw16
Router(config)# cable modulation-profile 2 short 6 75 6 8 16qam scrambler 152 no-diff 72
fixed uw16
Router(config)# cable modulation-profile 2 long 8 220 0 8 16qam scrambler 152 no-diff 160
fixed uw16
```

次の例では、すべてのメッセージ タイプが QAM-16 変調によって伝送されます。QAM-16 変調では、5 つすべてのメッセージ タイプに同じ変調方式が適用されますが、ステーション メンテナンス メッセージと帯域要求メッセージについては、QAM-16 プリアンブルの長さが追加されるので、MAC データ メッセージの帯域効率向上の利点はもたらされません。

```
Router# configure terminal
Router(config)# cable modulation-profile 2 request 0 16 1 8 16qam scrambler 152 no-diff 128
 fixed uw16
Router(config)# cable modulation-profile 2 initial 5 34 0 48 16qam scrambler 152 no-diff
256 fixed uw16
Router(config)# cable modulation-profile 2 station 5 34 0 48 16qam scrambler 152 no-diff
256 fixed uw16
Router(config)# cable modulation-profile 2 short 5 75 6 8 16qam scrambler 152 no-diff 144
fixed uw16
Router(config)# cable modulation-profile 2 long 8 220 0 8 16qam scrambler 152 no-diff 160
fixed uw16
```

（注） DOCSIS と 16-QAM または混合シンボル レートを併用する場合、CMTS を short および long の両方のデータ バースト プロファイルのプリアンブルで固有ワード 16（「uw16」）に設定します。

cableupstream*port-number***modulation-profile** *primary profile-number secondary profile-number* コマンドを該当するインターフェイスに追加します。この例では、変調プロファイル 2 に QAM-16 変調、変調プロファイル 1 に QPSK 変調が設定されています。

```
Router# configure terminal
Router(config)# controller upstream-Cable 6/0/0
Router(config-controller)# cable upstream 0 modulation-profile 2 1
```

例：入力レベル

次の例では、24.8 MHz でのモデム送信電力が 1 dBmV 単位でアップストリームに調整され、28.0 MHz でのモデム送信電力が 2 dBmV 単位でアップストリームに調整されます。

```
CMTS01(config)# cable spectrum-group 1 frequency 21600000
CMTS01(config)# cable spectrum-group 1 frequency 24800000 1
CMTS01(config)# cable spectrum-group 1 frequency 28000000 2
```

高度なスペクトル管理の設定例

ここでは、次の一般的な設定を示します。

例：Cisco cBR シリーズ ルータ用の高度なスペクトル管理

ここでは、ケーブル インターフェイス ライン カードを使用した Cisco cBR ルータの一般的な設定例の抜粋を示します。この設定では次の作業を行います。

- 4 つのスペクトル グループのホップ間隔を 30 秒に設定します。
- QPSK 変調プロファイルを作成し、スロット 6/1/0 の シスコ ケーブル インターフェイス ライン カードの 4 つのアップストリームに割り当てます。
- 4 つのアップストリームそれぞれにスペクトル グループを割り当てます。
- 各アップストリームにデフォルトの CNiR（CNR）および FEC のしきい値を設定します。

```
cable modulation-profile 21 qpsk
interface Cable6/1/0
cable bundle 1
cable downstream annex B
cable downstream modulation 256qam
cable downstream interleave-depth 32
! upstream 0
cable upstream 0 spectrum-group 1
cable upstream 0 modulation-profile 21
cable upstream 0 threshold cnr-profiles 16 0
cable upstream 0 threshold Corr-Fec 3
cable upstream 0 threshold Uncorr-Fec 1
no cable upstream 0 shutdown ! upstream 1
cable upstream 1 spectrum-group 2
cable upstream 1 modulation-profile 21
cable upstream 1 threshold cnr-profiles 16 0
cable upstream 1 threshold Corr-Fec 3
cable upstream 1 threshold Uncorr-Fec 1
no cable upstream 1 shutdown ! upstream 2
cable upstream 2 spectrum-group 3
cable upstream 2 modulation-profile 21
cable upstream 2 threshold cnr-profiles 16 0
cable upstream 2 threshold Corr-Fec 3
cable upstream 2 threshold Uncorr-Fec 1
no cable upstream 2 shutdown ! upstream 3
cable upstream 3 spectrum-group 4
cable upstream 3 modulation-profile 21
cable upstream 3 threshold cnr-profiles 16 0
cable upstream 3 threshold Corr-Fec 3
cable upstream 3 threshold Uncorr-Fec 1
no cable upstream 3 shutdown
```

その他の参考資料

ここでは、Cisco CMTS ルータのスペクトル管理と高度なスペクトル管理に関連する資料を紹介します。

関連資料

関連項目	マニュアル タイトル
CMTS コマンド リファレンス	『Cisco Broadband Cable Command Reference Guide』

標準および RFC

標準	タイトル
SP-RFIv1.1-I09-020830	『Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1』
SP-RFIv2.0-I03-021218	『Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 2.0』
SP-OSSIv2.0-I03-021218	『Data-over-Cable Service Interface Specifications Operations Support System Interface Specification, version 2.0』
SP-BPI+-I09-020830	『Data-over-Cable Service Interface Specifications Baseline Privacy Plus Interface Specification, version 2.0』

MIB

MIB	MIB のリンク
CISCO-CABLE-SPECTRUM-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 https://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	https://www.cisco.com/cisco/web/support/index.html

スペクトル管理と高度なスペクトル管理に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャセット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

機能名	リリース	機能情報
スペクトル管理と高度なスペクトル管理	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 21 章

アップストリーム スケジューラ モード

このマニュアルでは、アップストリーム（US）スケジューラ モードをオプションで設定する方法を説明します。

この機能を使用すると、非送信請求許可サービス（UGS）、リアルタイム ポーリング サービス（rtPS）、非リアルタイム ポーリング サービス（nrtPS）スケジューリング タイプのいずれか、およびパケットベースと時分割多重（TDM）ベースのスケジューリングのいずれかを選択できます。低遅延キューイング（LLQ）は、DOCSIS の TDM インフラストラクチャでパケットモードに似た動作をエミュレートします。これにより、この機能はパケットと TDM の典型的なトレードオフを提供します。LLQ を使用すると、UGS、rtPS、または nrtPS のサービス パラメータをより柔軟に定義できますが、delay や jitter などのパラメータについては（統計分布以外の）保証がありません。

機能情報の確認

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載され

ている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *64*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

アップストリーム スケジューラ モードの制限事項

- 正しく動作させるには、インターフェイスベースのアドミッション制御を有効にする必要があります。LLQオプションを有効にすると、アップストリームパスが大量のコールでいっぱいになって使えなくなり、許容できない音声品質になってしまいます。インターフェイスベースのアドミッション制御を使用してコール数を制限し、音声品質を許容できるものにする必要があります。また、音声トラフィック以外のトラフィックを確保する必要もあります。
- インターフェイスベースのアドミッション制御を有効にしていない場合でも、一定のコール数に達するとデフォルト（DOCSIS）のスケジューリング モードがトラフィックをブロックします。
- UGS with Activity Detection（UGS-AD）は、LLQ スケジューラ モードではサポートされませんが、デフォルト DOCSIS スケジューラ モードでは引き続きサポートされます。

Cisco CMTS ルータのアップストリーム スケジューラ モードに関する情報

UGS を使用すると、固定サイズのフレームで定期的な伝送機会をケーブル モデムに与えることで、ケーブル モデムが保証されたレートと保証されたレベルのジッターで固定サイズのデータ バーストを送信できるサービス フローが作成されます。このタイプのサービス フローは、特に VoIP アプリケーションに適しています。

rtPS を使用すると、帯域幅要求に対してすべてのケーブル モデムではなく単一のケーブル モデムをポーリングすることで、ケーブル モデムがデータを送信する権限を要求するような定期的な機会を提供するサービス フローが作成されます。これは、リアルタイムのデータ送信の要求を持つアプリケーションを満たし、ケーブルモデムがさまざまな長さのデータ バーストを送信できるようにします。このタイプのサービス フローは、特に MPEG VoIP に適しています。

rtPS 要求はデフォルトで優先度 7 として内部的に扱われます。これはすべてのベスト エフォート型トラフィックで最高の優先度です。この高優先度により、輻輳時の rtPS トラフィックの遅延を低減します。

nrtPS を使用すると、帯域幅要求に対してすべてのケーブル モデムではなく単一のケーブル モデムをポーリングすることで、ケーブル モデムがデータを送信する権限を要求するような定期的な機会を提供するサービスフローが作成されます。データバーストは、さまざまな長さになる可能性があります。このタイプのサービスフローは、特に非インタラクティブサービス（ファイル転送など）に適しています。

アップストリーム スケジューラ モードの設定方法

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	次のいずれかのコマンドを使用します。 • **interface cable** *slot/subslot/port* • **interface cable** *slot/port* 例： `Router(config)# interface cable 7/0/1`	指定したケーブル インターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**cable upstream** *n* **scheduling type ugs mode** [**llq** |**docsis**] 例： `Router(config-if)# cable upstream 4 scheduling type ugs mode llq`	UGS サービスの LLQ タイプ（パケットベース）スケジューリングをイネーブルにします。 （注） **ugs**、**rtps**、**nrtps**、**llq**、および **docsis** の任意の組み合わせが可能です。デフォルト値は **docsis** のみです。
ステップ 5	**cable upstream** *n* **schedulingtype rtps mode** [**llq** |**docsis**] 例： `Router(config-if)# cable upstream 4 scheduling type rtps mode docsis`	rtPS サービスの標準 DOCSIS（TDM ベース）スケジューリングをイネーブルにします。 （注） **ugs**、**rtps**、**nrtps**、**llq**、および **docsis** の任意の組み合わせが可能です。デフォルト値は **docsis** のみです。
ステップ 6	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次の作業

スケジューラが DOCSIS モードで動作しているかどうかを確認するには、 **show interface cable mac-scheduler** コマンドを使用します。

```
Router# show interface cable 7/0/1 mac-scheduler 0
     DOCSIS 1.1 MAC scheduler for Cable7/0/1/U0 : rate 30720000
     wfq:None
     us_balance:OFF
     fairness:OFF
     Queue[Rng Polls] flows 0
     Queue[CIR Grants] flows 0
     Queue[BE(07) Grants] flows 0
     Queue[BE(06) Grants] flows 0
     Queue[BE(05) Grants] flows 0
     Queue[BE(04) Grants] flows 0
     Queue[BE(03) Grants] flows 0
     Queue[BE(02) Grants] flows 0
     Queue[BE(01) Grants] flows 0
     Queue[BE(00) Grants] flows 0
     Req Slots 2601578997, Req/Data Slots 4484512
     Init Mtn Slots 38265829, Stn Mtn Slots 78753
     Short Grant Slots 0, Long Grant Slots 0
     Adv Phy Short Grant Slots 412, Adv Phy Long Grant Slots 5519087
     Adv Phy UGS Grant Slots 0
     Avg upstream channel utilization : 1%
     Avg percent contention slots : 98%
     Avg percent initial ranging slots : 1%
     Avg percent minislots lost on late MAPs : 0%

     MAP TSS: lch_state 9, init_retries 0
              late_initial_maps 0, late_ucd_maps 0
              mac-phy tss errors 0, missed ccc 0
```

その他の参考資料

ここでは、Cisco CMTS ルータに関連する参考資料を示します。

関連資料

関連項目	マニュアル タイトル
Cisco CMTS コマンド リファレンス	『*Cisco CMTS Cable Command Reference*』 http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html

標準

規格	タイトル
DOCSIS	『Data-Over-Cable Service Interface Specifications, DOCSIS 2.0, Radio Frequency Interface Specification, CM-SP-RFIv2.0-I08-050408』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

アップストリーム スケジューラ モードに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *65* : アップストリーム スケジューラ モードに関する機能情報

機能名	リリース	機能情報
アップストリーム スケジューラ モード	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 22 章

総称ルーティング カプセル化

このマニュアルでは、Generic Routing Encapsulation（GRE）機能について説明します。この機能は、IP トンネル内のさまざまなプロトコル パケット タイプをカプセル化し、IP インターネットワークを使用して、リモート ポイントの Cisco ルータへの仮想ポイントツーポイント リンクを作成することを可能にする、トンネリング プロトコルです。

機能情報の確認

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *66*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

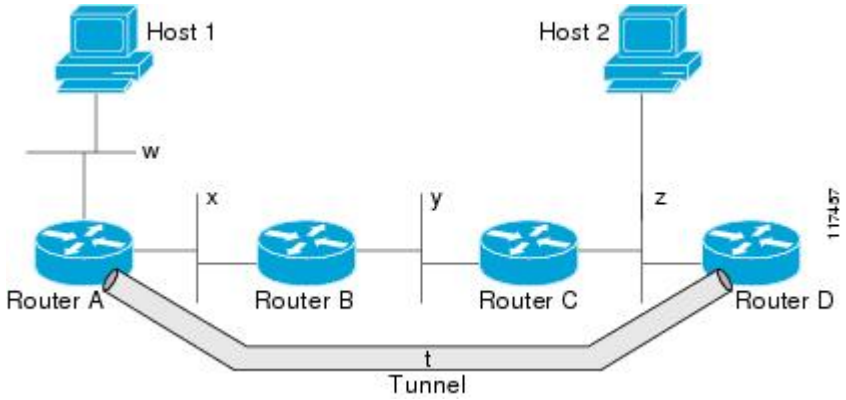
Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

トンネル実装の制約事項

- トンネル プロトコルにファイアウォールとアクセス コントロール リスト（ACL）チェックのパススルーを許可することが必要です。
- トンネルインターフェイスで帯域幅が正しく設定されていない場合、複数のポイントツーポイント トンネルがルーティング情報を使用して物理リンクを飽和させる可能性があります。
- トンネルは単一のホップ リンクに似ており、ルーティング プロトコルはマルチホップ物理パスを経由するトンネルを優先することがあります。トンネルは単一ホップ リンクであるかどうかに関係なく、マルチ ホップ リンクよりも低速パスを通過する場合があります。トンネルは、実際に通過するリンクと同様に堅牢で高速であったり、信頼性が低く低速であったりします。ホップ カウントだけに基づいて決定を行うルーティング プロトコルは、物理リンクのセットを経由するトンネルを優先することが多くなります。トンネルは、1 つのホッ

プのポイントツーポイントリンクで、パスのコストが最も低いように思われますが、代替物理トポロジと比較した場合、遅延の観点から見ると実際にはコストがかかる場合があります。たとえば、以下の図に示すトポロジでは、ホスト 1 からのパケットは、w、x、y、z の 4 つのパスを使用する代わりに、トンネルのホップ カウントがより短いと思われるネットワーク w、t、および z を通過してホスト 2 へ送信されると考えられます。ただし実際には、トンネルを通って送信されるパケットは、ルータ A、B、C を通過して、さらにルータ D まで移動してからルータ C に戻る必要があります。

図 *18*：トンネルに関する注意事項：ホップ カウント



- ルーティングが正しく設定されていない場合、トンネルに再帰ルーティングの問題がある可能性があります。トンネル宛先への最良パスはトンネル自身です。そのため再帰ルーティングによってトンネルインターフェイスがフラップします。再帰ルーティングの問題を回避するには、次の方法を使用して、常にコントロールプレーン ルーティングをトンネル ルーティングとは別個にします。
  - 異なる自律システム番号またはタグを使用する。
  - 異なるルーティング プロトコルを使用する。
  - スタティック ルートを使用して最初のホップ（ルーティング ループがないかどうか監視）をオーバーライドします。

次のエラーは、再帰ルーティングがトンネルの宛先にあるときに表示されます。

```
%TUN-RECURDOWN Interface Tunnel 0
temporarily disabled due to recursive routing
```

GRE IPv6 トンネルの制約事項

- GRE トンネル キープアライブ パケットはサポートされません。
- マルチポイント GRE（mGRE）IPv6 トンネリングはサポートされていません。

- Virtual Routing and Forwarding（VRF）ではトンネル トランスポートのサポートが限られています。VRF での限定サポートは、トンネル保護を使用しない Ipv6 ポイントツーポイント GRE に適用できます。

トンネル実装に関する情報

トンネリングとカプセル化

トンネルがどのように動作するかを理解するには、カプセル化とトンネリングの概念を区別できる必要があります。カプセル化は、特定のプロトコル スタックの各レイヤでデータにヘッダーを追加するプロセスです。開放型システム間相互接続（OSI）参照モデルは、ネットワークの機能について説明します。1 個のホスト（PC など）からネットワーク上の別のホストにデータ パケットを送信するには、カプセル化を使用して、プロトコル スタックの各レイヤで、データ パケットの前にヘッダーを降順で追加します。ヘッダーには、現在のレイヤのすぐ上にあるレイヤでカプセル化されているデータのタイプを示すデータ フィールドが含まれていることが必要です。ネットワークの受信側でパケットがプロトコル スタックを上っていくと、カプセル化された各ヘッダーは逆順に削除されます。

トンネリングでは、別のプロトコル内の 1 つのプロトコルからデータ パケットをカプセル化し、外部ネットワーク上のパケットを転送します。トンネリングは、カプセル化とは異なり、より低いレイヤのプロトコルと同じレベルのレイヤのプロトコルが、トンネルを通って送信されるようにします。トンネル インターフェイスは仮想（または論理）インターフェイスです。トンネリングは、次の 3 種類の主要コンポーネントから構成されます。

- パッセンジャ プロトコル：カプセル化の対象となるプロトコル。たとえば、IPv4 プロトコルや IPv6 プロトコルなどです。
- キャリア プロトコル：カプセル化するプロトコル。たとえば、総称ルーティング カプセル化（GRE）やマルチプロトコル ラベル スイッチング（MPLS）などです。
- トランスポート プロトコル：カプセル化したプロトコルを伝送するプロトコル。主なトランスポート プロトコルは IP です。

Tunnel ToS

Tunnel タイプ オブ サービス（ToS）により、ネットワーク トラフィックをトンネリングして、すべてのパケットを同じ ToS バイト値に分類できます。ToS バイト値および存続可能時間（TTL）のホップ カウント値は、ルータの IP トンネル インターフェイス向けのトンネル パケットのカプセル化 IP ヘッダーに設定できます。Tunnel ToS 機能は、Cisco Express Forwarding（旧称：CEF）、高速スイッチング、およびプロセス スイッチングでサポートされます。

ToS および TTL バイト値は、RFC 791 で定義されています。RFC 791 に定義されているとおり、RFC 2474 および RFC 2780 では ToS バイトの使用を廃止しています。RFC 791 では、ToS バイトのビット 6 と 7（最初の 2 つの最下位ビット）は将来使用するために予約されており、0 に設定する必要があることが指定されています。

Path MTU Discovery

Path MTU Discovery（PMTUD）は、GRE または IP-in-IP トンネル インターフェイスでイネーブルにできます。トンネル インターフェイスで PMTUD（RFC 1191）がイネーブルの場合、ルータは GRE（または IP-in-IP）トンネル IP パケットに対して PMTUD 処理を実行します。ルータは、トンネルに入ってくる元のデータの IP パケットに対して常に PMTUD 処理を実行します。PMTUD がイネーブルの場合、Don't Fragment（DF）ビットがすべてのパケットに設定されるため、トンネルを通過するパケットに対してはパケットのフラグメンテーションは許可されません。トンネルに入ったパケットがそのパケットの MTU 値よりも小さい MTU 値を持つリンクを検出すると、パケットは廃棄され、パケットの送信元にインターネット制御メッセージプロトコル（ICMP）メッセージが返されます。このメッセージには、フラグメンテーションが要求されたこと（しかし許可されなかったこと）と、パケットがドロップされる原因となったリンクの MTU が含まれています。

（注） トンネル インターフェイスの PMTUD は、トンネル エンドポイントがトンネルのパスでルータによって生成される ICMP メッセージを受信できることを要求します。ファイアウォール接続を通じて PMTUD を使用する前に、ICMP メッセージが受信できることを確認してください。

トンネルのパケットで PMTUD を有効にするには、**tunnelpath-mtu-discovery** コマンドを使用し、トンネルの PMTUD パラメータを確認するには、**showinterfacestunnel** コマンドを使用します。PMTUD が動作するトンネル インターフェイスは現在、GRE および IP-in-IP だけです。

トンネル用 QoS オプション

トンネル インターフェイスは、物理インターフェイスとしてさまざまな Quality of Service（QoS）機能をサポートします。QoS により、ミッション クリティカルなトラフィックのパフォーマンスを確実に受け入れ可能なレベルにする方法が提供されます。トンネル用 QoS オプションでサポートされる項目には、Generic Traffic Shaping（GTS）のトンネル インターフェイスへの直接適用や、Modular QoS CLI（MQC）を使用したクラス ベースのシェーピングなどが含まれます。またトンネル インターフェイスは、クラス ベースのポリシングもサポートしますが、専用アクセス レート（CAR）はサポートしません。

GRE トンネルでは、ルータは、ToS バイトの IP precedence ビット値をトンネルまたは内部パケットをカプセル化している GRE IP ヘッダーにコピーできます。トンネルのエンドポイント間の中間ルータは、IP precedence 値を使用して、QoS 機能（ポリシー ルーティング、重み付け均等化キューイング（WFQ）、重み付けランダム早期検出（WRED）など）向けにパケットを分類できます。

トンネルまたは暗号化ヘッダーによってパケットがカプセル化されている場合、QoS 機能は元のパケットのヘッダーを調べてパケットを正しく分類することができません。同じトンネルを通過するパケットは、同じトンネル ヘッダーを持つため、物理インターフェイスが輻輳している場合、パケットは同等に扱われます。ただし、トンネルのパケットはトンネリング前に分類でき、ユーザがトンネル インターフェイス上またはクリプト マップ上で QoS の事前分類機能を適用する際に暗号化を行うことができます。

（注） クラス ベースのシェーピング内の Class-based WFQ（CBWFQ）は、マルチポイント インターフェイスではサポートされません。

トンネル インターフェイス上に一部の QoS 機能を導入する方法については、トンネル インターフェイスでの QoS オプションの設定：例, （501 ページ）を参照してください。

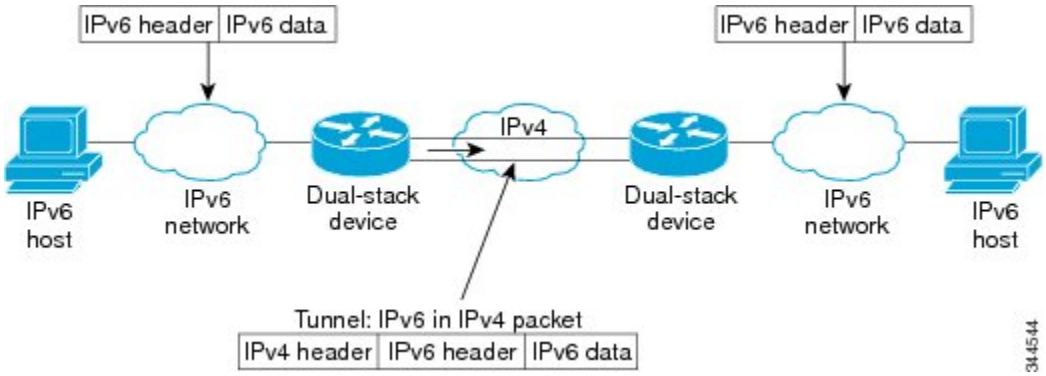
IPv4 GRE トンネルを介する IPv6 に関する情報

Ipv6 用オーバーレイ トンネル

オーバーレイ トンネリングでは、IPv4 パケット内で IPv6 パケットをカプセル化して、IPv4 インフラストラクチャ（コア ネットワークまたは以下の図）へ伝送します。オーバーレイ トンネルを使用することで、孤立した IPv6 ネットワークと通信できます。このとき、孤立した複数の IPv6 ネットワーク間にある IPv4 インフラストラクチャをアップグレードする必要はありません。オーバーレイ トンネルは、境界デバイス間、または境界デバイスとホスト間に設定できますが、両方のエンドポイントが IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。IPv6 では、次のタイプのオーバーレイ トンネリング メカニズムをサポートしています。

- 手動
- 総称ルーティング カプセル化（GRE）
- IPv4 互換
- 6to4
- Intrasite Automatic Tunnel Addressing Protocol（ISATAP）

図 *19* : オーバーレイ トンネル



（注） オーバーレイ トンネルにより、インターフェイスの最大伝送単位（MTU）が 20 オクテット減少します（ただし、基本 IPv4 パケット ヘッダーにオプション フィールドが含まれていないことを前提とします）。オーバーレイ トンネルを使用するネットワークは、トラブルシューティングが困難です。したがって、独立した IPv6 ネットワークに接続するオーバーレイ トンネルは、最終的な IPv6 ネットワーク アーキテクチャと見なしてはいけません。オーバーレイ トンネルの使用は、IPv4 と IPv6 の両方のプロトコル スタック、または IPv6 プロトコル スタックだけをサポートするネットワークへの移行方法と見なす必要があります。

以下の表は、IPv4 ネットワーク上での IPv6 パケットの伝送にどのトンネル タイプを設定すればよいかを決定する場合に役立ちます。

表 *67*：*IPv4* ネットワーク上で *IPv6* パケットを伝送するトンネル タイプの推奨される使用方法

トンネリング タイプ	推奨される使用方法	使用方法
手動	サイト内またはサイト間で使用可能な、単純なポイントツーポイント トンネル	IPv6 パケットだけを伝送できます。
GRE および IPv4 互換	サイト内またはサイト間で使用可能な、単純なポイントツーポイント トンネル	IPv6、コネクションレス型ネットワーク サービス（CLNS）、およびその他の多数のタイプのパケットを伝送できます。
IPv4 互換	ポイントツーマルチポイント トンネル	::/96 プレフィックスを使用します。このトンネル タイプの使用は推奨しません。
6to4	独立した IPv6 サイトへの接続に使用可能なポイントツーマルチポイント トンネル	サイトでは、2002::/16 プレフィックスからのアドレスを使用します。
6RD	IPv6 サービスは、IPv4 に IPv6 のカプセル化を使用することで IPv4 ネットワーク上のユーザに提供されます。	プレフィックスは、SP 自身のアドレス ブロックから割り当てることができます。
ISATAP	サイト内のシステムへの接続に使用可能なポイントツーマルチポイント トンネル	サイトでは、任意の IPv6 ユニキャスト アドレスを使用できます。

個々のトンネル タイプについて、このマニュアルで詳しく説明しています。実装する特定のトンネル タイプに関する情報を確認および理解することを推奨します。必要なトンネル タイプに精通

している場合は、以下の表で、有用と思われるトンネル設定パラメータの概要を参照してください。

表 *68*：トンネリング タイプ別のトンネル設定パラメータ

トンネリングタイプ	トンネル設定パラメータ			
トンネル モード	トンネルの送信元	トンネルの宛先	インターフェイスプレフィックスまたはアドレス	
手動	ipv6ip	IPv4アドレス、またはIPv4が設定されたインターフェイスへの参照。	IPv4 アドレス。	IPv6 アドレス。
GRE/IPv4	gre ip		IPv4 アドレス。	IPv6 アドレス。
IPv4 互換	ipv6ip auto-tunnel		不要。これらはすべて、ポイントツーマルチポイントのトンネリングタイプです。IPv4宛先アドレスは、パケット単位で、IPv6宛先から計算されます。	不要。インターフェイスアドレスは、::*tunnel-source*/96として生成されます。
6to4	ipv6ip 6to4			IPv6アドレス。プレフィックスは、トンネル送信元のIPv4アドレスを埋め込む必要があります。
6RD	ipv6ip 6rd			IPv6 アドレス。
ISATAP	ipv6ip isatap			変更された eui-64 形式での IPv6 プレフィックス。IPv6アドレスは、プレフィックスおよびトンネル送信元 IPv4 アドレスから生成されます。

IPv6 トラフィック用の GRE IPv4 トンネル サポート

IPv6 トラフィックは、標準的なポイントツーポイントのカプセル化スキームの実装にサービスを提供するように設計されている標準 GRE トンネリング技術を使用して、IPv4 GRE トンネルを介

して伝送できます。GREトンネルは、手動で設定されたIPv6トンネルと同様、リンクごとに個別のトンネルが設定された 2 つのポイント間のリンクです。これらのトンネルは、特定のパッセンジャまたはトランスポートプロトコルに結合されていませんが、この場合、GREを使用するパッセンジャ プロトコルとしてIPv6を伝送し、トランスポート プロトコルとしてIPv4またはIPv6を伝送します。

GRE トンネルは、2 つのエッジ デバイス間またはエッジ デバイスとエンド システム間に定期的でセキュアな通信を必要とする安定した接続のために主に使用されます。エッジ デバイスとエンド システムは、デュアル スタック実装である必要があります。

GRE IPv6 トンネルに関する情報

GRE IPv6 トンネルの概要

GRE IPv6 トンネル機能は、他のプロトコルから IPv6 ネットワークを介したパケット配信を有効にして、グローバルにルーティングされたIPv6アドレスのパブリック ネットワークを介したプライベート ネットワーク間で、IPv6 パケットのルーティングが可能になります。

ポイントツーポイント GRE トンネルでは、各トンネル インターフェイスは、設定時にトンネル送信元IPv6アドレスおよびトンネル宛先のIPv6アドレスを必要とします。すべてのパケットは、外部 IPv6 ヘッダーと GRE ヘッダーでカプセル化されます。

トンネルの実装方法

トンネル タイプの決定

トンネルを設定する前に、作成するトンネルのタイプを決定する必要があります。

手順

ステップ 1 パッセンジャ プロトコルを決定します。パッセンジャ プロトコルはカプセル化の対象となるプロトコルです。

ステップ 2 必要に応じて、**tunnelmode** コマンド キーワードを決定します。
次の表に **tunnelmode** コマンドで使用する適切なキーワードを設定する例を示します。

表 *69*：トンネル モードのコマンド キーワードの決定

キーワード	目的
dvmrp	ディスタンスベクターマルチキャストルーティング プロトコルのカプセル化の使用を指定するには、**dvmrp** キーワードを使用します。

キーワード	目的
greip	IP での GRE カプセル化の使用を指定するには、**gre** キーワードおよび **ip** キーワードを使用します。
greipv6	IPv6 での GRE カプセル化の使用を指定するには、**gre** キーワードおよび **ipv6** キーワードを使用します。
ipip [**decapsulate-any**]	IP-in-IP カプセル化の使用を指定するには、**ipip** キーワードを使用します。オプションの **decapsulate-any** キーワードは、あるトンネル インターフェイスの任意の数の IP-in-IP トンネルを終了させます。このトンネルは発信トラフィックを伝送しませんが、任意の数のリモート トンネル エンドポイントは、設定されたトンネルを宛先として使用できることに注意してください。
ipv6	IPv6 での汎用パケット トンネリングの使用を指定するには、**ipv6** キーワードを使用します。
ipv6ip	IPv6 をパッセンジャー プロトコルとして使用し、IPv4 をキャリア（カプセル化）プロトコルおよびトランスポートプロトコルとして使用することを指定するには、**ipv6ip** キーワードを使用します。追加のキーワードを使用しない場合は、手動 IPv6 トンネルが設定されます。追加のキーワードを使用して、IPv4 互換、6to4、または ISATAP トンネルを指定できます。
mpls	トラフィック エンジニアリング（TE）トンネルの設定に MPLS の使用を指定するには、**mpls** キーワードを使用します。

IPv4 GRE トンネルの設定

GRE トンネルを設定するには、この作業を実行します。トンネルインターフェイスを使用して、通常プロトコルをサポートしないネットワークへプロトコル トラフィックを通過させます。トンネルを構築するには、トンネル インターフェイスを 2 つのルータそれぞれで定義し、そのトンネ

ルインターフェイスが互いを参照することが必要です。各ルータでは、トンネルインターフェイスはレイヤ 3 アドレスを使用して設定する必要があります。トンネルのエンドポイント、トンネル送信元、およびトンネル宛先を定義して、トンネルのタイプを選択する必要があります。オプションの手順を実行して、トンネルをカスタマイズできます。

必ずトンネルの両側にルータを設定するようにしてください。トンネルの片方の端だけが設定されている場合、（キープアライブが設定されていない限り）トンネル インターフェイスはアップした状態になっていますが、トンネルに入ったパケットはドロップされます。

GRE トンネル キープアライブ

キープアライブ パケットは、IP カプセル化された GRE トンネルを介して送信されるよう設定できます。キープアライブが送信されるレートと、インターフェイスが非アクティブになるまでデバイスが応答なしでキープアライブ パケットの送信を続行する回数を指定できます。GREキープアライブ パケットは、トンネルの両側または片側のみのどちらでも送信できます。

はじめる前に

この作業でトンネルの送信元として使用する物理インターフェイスがアップしており適切なIPアドレスを使用して設定されていることを確認します。ハードウェアに関する技術的な説明およびインターフェイスのインストールに関する情報については、ご使用の製品のハードウェアのインストールおよび設定マニュアルを参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface** *type number* 例： `Router(config)# interface tunnel 0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。 • トンネルを設定するには、*type* 引数に **tunnel** を使用します。
ステップ 4	**bandwidth** *kb/s* 例： `Router(config-if)# bandwidth 1000`	インターフェイスに対する現在の帯域幅を設定し、上位レベル プロトコルと通信します。 • パケットの送信に使用されるトンネル帯域幅を指定します。

	コマンドまたはアクション	目的
		• 帯域幅をキロビット/秒単位（kb/s）で設定するには、*kb/s* 引数を使用します。 （注） これはルーティング パラメータにすぎないため、物理インターフェイスには影響を及ぼしません。トンネル インターフェイスのデフォルトの帯域幅設定は 9.6 kb/s です。トンネルの帯域幅を適切な値に設定する必要があります。
ステップ 5	**keepalive**[*period* [*retries*]] 例： `Router(config-if)# keepalive 3 7`	（任意）トンネルインターフェイス プロトコルがダウン状態になるまで、デバイスが応答なしでキープアライブ パケットの送信を続行する回数を指定します。 • GRE キープアライブ パケットは、トンネルの片側または両側のどちらででも設定できます。 • GREキープアライブをトンネルの両側で設定した場合、リンクの各側の *period* 引数と *retries* 引数は異なる値に設定できます。 （注） このコマンドがサポートされるのは、GRE ポイントツーポイント トンネルだけです。 （注） GREトンネルのキープアライブ機能は、VRF トンネルでは設定しないでください。機能のこの組み合わせはサポートされていません。
ステップ 6	**tunnelsource**{*ip-address* | *interface-type interface-number*} 例： `Router(config-if)# tunnel source TenGigabitEthernet 4/1/0`	トンネル送信元を設定します。 （注） トンネルの送信元 IP アドレスと宛先の IPアドレスは、2つの個別のデバイス上で定義する必要があります。
ステップ 7	**tunneldestination**{*hostname* | *ip-address*} 例： `Router(config-if)# tunnel destination 10.0.2.1`	トンネル宛先を設定します。 （注） トンネルの送信元と宛先の IP アドレスは、2つの個別のデバイス上で定義する必要があります。

	コマンドまたはアクション	目的
ステップ 8	**tunnelkey** *key-number* 例： `Router(config-if)# tunnel key 1000`	（任意）トンネル インターフェイスの ID キーをイネーブルにします。 （注） このコマンドがサポートされるのは、GRE トンネル インターフェイスだけです。セキュリティ目的でこのキーに依存することは推奨しません。
ステップ 9	**tunnelmodegre** {**ip** |**multipoint**} 例： `Device(config-if)# tunnel mode gre ip`	トンネルで使用されるカプセル化プロトコルを指定します。
ステップ 10	**ipmtu** *bytes* 例： `Device(config-if)# ip mtu 1400`	（任意）各インターフェイスで送信される IP パケットの MTU サイズを設定します。 • インターフェイスに設定されている MTU を IP パケットが超過した場合、DF ビットが設定されていなければ Cisco ソフトウェアは DF ビットをフラグメント化します。 • 物理メディアのすべてのデバイスが動作するには、同じプロトコル MTU を持っている必要があります。 • IPv6 パケットに対しては、**ipv6mtu** コマンドを使用します。 （注） **tunnelpath-mtu-discovery** コマンドが有効になっている場合、このコマンドを設定しないでください。
ステップ 11	**iptcpmss** *mss-value* 例： `Device(config-if)# ip tcp mss 250`	（任意）ルータ上で生成または終了する TCP 接続に対して、最大セグメント サイズ（MSS）を指定します。
ステップ 12	**tunnelpath-mtu-discovery**[**age-timer** {*aging-mins* | **infinite**}] 例： `Device(config-if)# tunnel path-mtu-discovery`	（任意）GRE または IP-in-IP トンネル インターフェイスで PMTUD をイネーブルにします。 • トンネル インターフェイスで PMTUD がイネーブルの場合、PMTUD は GRE IP トンネル パケット用に動作し、トンネル エンドポイント間のパス内のフラグメンテーションを最低限に抑えます。

	コマンドまたはアクション	目的
ステップ 13	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次の作業

「トンネルの設定と動作の確認」の項に進みます。

6to4 トンネルの設定

はじめる前に

6to4 トンネルでは、トンネルの宛先は、境界ルータの IPv4 アドレスによって決定されます。このアドレスは、プレフィックス 2002::/16 と連結されて 2002:*border-router-IPv4-address* ::/48 という形式になります。6to4 トンネルの両端の境界ルータは、IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。

（注） IPv4 互換トンネル 1 つだけの設定、および 6to4 IPv6 トンネル 1 つだけの設定が、1 台のルータ上でサポートされます。同じルータで両方のトンネル タイプの設定を選択する場合は、シスコは、これらが同じ送信元を共有しないようにすることを強く推奨します。

6to4 トンネルと IPv4 互換トンネルが同じインターフェイスを共有できない理由は、これらがともに NBMA「ポイントツーマルチポイント」アクセス リンクであり、多重化されたパケット ストリームからのパケットを着信インターフェイスの単一パケット ストリームに再度配列するために、トンネルの送信元しか使用できないためです。IPv4 プロトコル タイプが 41 のパケットがインターフェイスに到着すると、このパケットは IPv4 アドレスに基づいて、IPv6 トンネル インターフェイスにマッピングされます。ただし、6to4 トンネルと IPv4 互換トンネルが同じ送信元インターフェイスを共有している場合、ルータは、着信パケットを割り当てるべき IPv6 トンネル インターフェイスを区別できません。

手動で設定された IPv6 トンネルの場合、手動トンネルは「ポイントツーポイント」リンクであり、トンネルの IPv4 送信元と IPv4 宛先が両方とも定義されているため、同じ送信元インターフェイスを共有できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacetunnel** *tunnel-number* 例： `Router(config)# interface tunnel 0`	トンネル インターフェイスおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6 address** *ipv6-prefix*/*prefix-length* [**eui-64**] 例： `Router(config-if)# ipv6 address 2002:c0a8:6301:1::1/64`	インターフェイスに割り当てられた IPv6 アドレスを指定し、インターフェイスでの IPv6 処理をイネーブルにします。 • 最初の 2002::/16 プレフィックスに続く 32 ビットは、トンネル送信元に割り当てられた IPv4 アドレスに対応します。 （注） IPv6 アドレスの設定の詳細については、「Configuring Basic Connectivity for IPv6」モジュールを参照してください。
ステップ 5	**tunnelsource**{*ip-address* | *interface-type interface-number*} 例： `Router(config-if)# tunnel source TenGigabitEthernet 4/1/0`	トンネル インターフェイスの送信元 IPv4 アドレスまたは送信元インターフェイス タイプと番号を指定します。 （注） **tunnelsource** コマンドで指定したインターフェイスのタイプおよび番号は、IPv4 アドレスを使用して設定する必要があります。
ステップ 6	**tunnelmodeipv6ip6to4** 例： `Router(config-if)# tunnel mode ipv6ip 6to4`	6to4 アドレスを使用する IPv6 オーバーレイ トンネルを指定します。

	コマンドまたはアクション	目的
ステップ 7	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**ipv6route** *ipv6-prefix* / *prefix-length* **tunnel** *tunnel-number* 例： `Router(config)# ipv6 route 2002::/16 tunnel 0`	指定したトンネル インターフェイスへのスタティック ルートを設定します。 （注） 6to4 オーバーレイ トンネルを設定する場合は、6to4 トンネル インターフェイスに IPv6 6to4 プレフィックス 2002::/16 のスタティック ルートを設定する必要があります。 • **ipv6route** コマンドで指定したトンネル番号は、**interfacetunnel** コマンドで指定したトンネル番号と同じである必要があります。
ステップ 9	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次の作業

「トンネルの設定と動作の確認」の項に進みます。

トンネルの設定と動作の確認

以下の手順にある **show** コマンドおよび **ping** コマンドは、任意の順序で実行できます。次のコマンドは、GRE トンネル、IPv6 手動設定トンネル、および IPv4 GRE トンネルを介する IPv6 に使用できます。

手順

ステップ 1 **enable**
特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

例：
```
Device> enable
```

ステップ 2 **showinterfacestunnel** *number*[**accounting**]

2 台のルータがトンネルのエンドポイントとして設定されます。デバイス A では、IPv4 アドレスが 10.0.0.1、IPv6 プレフィックスが 2001:0DB8:1111:2222::1/64 のトンネル インターフェイス 0 に対する送信元として、TenGigabit イーサネット インターフェイス 4/1/0 が設定されています。デバイス B では、IPv4 アドレスが 10.0.0.2、IPv6 プレフィックスが 2001:0DB8:1111:2222::2/64 のトンネル インターフェイス 1 に対する送信元として、TenGigabit イーサネット インターフェイス 4/1/0 が設定されています。

トンネル送信元およびトンネル宛先のアドレスが設定されていることを確認するには、**showinterfacestunnel** コマンドをデバイス A で使用します。

例：

```
Device A# show interfaces tunnel 0

Tunnel0 is up, line protocol is up
  Hardware is Tunnel
  MTU 1514 bytes, BW 9 Kbit, DLY 500000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation TUNNEL, loopback not set
  Keepalive not set
  Tunnel source 10.0.0.1 (TenGigabitEthernet4/1/0), destination 10.0.0.2, fastswitch TTL
255
  Tunnel protocol/transport GRE/IP, key disabled, sequencing disabled
  Tunnel TTL 255
  Checksumming of packets disabled,  fast tunneling enabled
  Last input 00:00:14, output 00:00:04, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     4 packets input, 352 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     8 packets output, 704 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

ステップ 3 **ping** [*protocol*]*destination*

ローカルエンドポイントが設定され、動作していることをチェックするには、デバイス A で **ping** コマンドを使用します。

例：

```
DeviceA# ping 2001:0DB8:1111:2222::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:0DB8:1111:2222::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms
```

ステップ 4 **showiproute**[*address* [*mask*]]

リモート エンドポイント アドレスへのルートが存在することを確認するには、**showiproute** コマンドを使用します。

例：

```
DeviceA# show ip route 10.0.0.2
```

```
Routing entry for 10.0.0.0/24
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via TenGigabitEthernet4/1/0
      Route metric is 0, traffic share count is 1
```

ステップ 5 **ping** [*protocol*]*destination*

リモート エンドポイント アドレスに到着できることを確認するには、**ping** コマンドをデバイス A で使用します。

（注） フィルタリングが原因で、**ping** コマンドを使用してリモート エンドポイント アドレスに到着できない場合がありますが、トンネル トラフィックは依然としてその宛先に到着している場合があります。

例：

```
DeviceA# ping 10.0.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/28 ms
```

リモート IPv6 トンネル エンドポイントが到着可能であることを確認するには、再度デバイス A で **ping** コマンドを使用します。また、前の手順内のフィルタリングに関する注意事項はこの例にも適用されます。

例：

```
DeviceA# ping 2001:0DB8:1111:2222::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/20/20 ms
```

これらの手順は、トンネルのもう一方のエンドポイントで繰り返すことができます。

トンネル実装の設定例

例：GRE IPv4 トンネルの設定

GRE トンネリングの単純な設定例を次に示します。10 ギガビット イーサネット 4/1/0 は、ルータ A のトンネル送信元であり、ルータ B のトンネル宛先です。10 ギガビット イーサネット インターフェイス 4/1/1 は、ルータ B のトンネル送信元であり、ルータ A のトンネル宛先です。

ルータ A

```
interface Tunnel 0
 ip address 10.1.1.2 255.255.255.0
```

```
 tunnel source TenGigabitEthernet 4/1/0
 tunnel destination 192.168.3.2
 tunnel mode gre ip
!
interface TenGigabitEthernet 4/1/0
 ip address 192.168.4.2 255.255.255.0
```

ルータ B

```
interface Tunnel 0
 ip address 10.1.1.1 255.255.255.0
 tunnel source TenGigabitEthernet 4/1/1
 tunnel destination 192.168.4.2
 tunnel mode gre ip
!
interface TenGigabitEthernet 4/1/1
 ip address 192.168.3.2 255.255.255.0
```

次に、ルータ A とルータ B との間で IS-IS および IPv6 トラフィックをともに送出する GRE トンネルを設定する例を示します。

ルータ A

```
ipv6 unicast-routing
clns routing
!
interface Tunnel 0
 no ip address
 ipv6 address 2001:0DB8:1111:2222::1/64
 ipv6 router isis
 tunnel source TenGigabitEthernet 4/1/0
 tunnel destination 10.0.0.2
 tunnel mode gre ip
!
interface TenGigabitEthernet 4/1/0
 ip address 10.0.0.1 255.255.255.0
!
router isis
 network 49.0000.0000.000a.00
```

ルータ B

```
ipv6 unicast-routing
clns routing
!
interface Tunnel 0
 no ip address
 ipv6 address 2001:0DB8:1111:2222::2/64
 ipv6 router isis
 tunnel source TenGigabitEthernet 4/1/0
 tunnel destination 10.0.0.1
 tunnel mode gre ip
!
interface TenGigabitEthernet 4/1/0
 ip address 10.0.0.2 255.255.255.0
!
router isis
 network 49.0000.0000.000b.00
 address-family ipv6
 redistribute static
 exit-address-family
```

トンネル インターフェイスでの QoS オプションの設定：例

次の設定例は、トンネルインターフェイスのGTSに直接適用されます。この例では、設定によりトンネル インターフェイスが総出力レート 500 kb/s にシェーピングされます。

```
interface Tunnel 0
 ip address 10.1.2.1 255.255.255.0
 traffic-shape rate 500000 125000 125000 1000
 tunnel source 10.1.1.1
 tunnel destination 10.2.2.2
```

次の設定例では、MQC コマンドを使用して同じシェーピング ポリシーをトンネル インターフェイスに適用する方法を示しています。

```
policy-map tunnel
 class class-default
 shape average 500000 125000 125000
!
interface Tunnel 0
 ip address 10.1.2.1 255.255.255.0
 service-policy output tunnel
 tunnel source 10.1.35.1
 tunnel destination 10.1.35.2
```

ポリシングの例

インターフェイスが混雑しており、パケットのキューイングを開始した場合、送信待ちのパケットにキューイング方式を適用できます。論理インターフェイス（この例に挙げているトンネル インターフェイス）では本来、輻輳状態はサポートされておらず、キューイング方式を適用するサービス ポリシーの直接適用はサポートされていません。代わりに、階層型ポリシーを適用します。**priority** コマンドを使用した低遅延キューイングや、**bandwidth** コマンドを使用したキューイング メカニズムを設定する「子」ポリシー、つまり下位ポリシーを作成します。

```
policy-map child
 class voice
 priority 512
```

クラスベース シェーピングを適用する「親」またはトップレベルのポリシーを作成します。子クラスのアドミッション制御は親クラスのシェーピング比率に従って実行されるので、親ポリシー下で子ポリシーをコマンドとして適用します。

```
policy-map tunnel
 class class-default
 shape average 2000000
 service-policy child
```

親ポリシーをトンネル インターフェイスに適用します。

```
interface tunnel 0
 service-policy tunnel
```

次の例では、トンネル インターフェイスは、シェーピングを行わないキューイングを適用するサービス ポリシーを使用して設定されます。この設定がサポートされないことを通知するログ メッセージが表示されます。

```
Router(config)# interface tunnel1
Router(config-if)# service-policy output child
Class Based Weighted Fair Queueing not supported on this interface
```

IPv4 GRE トンネルを介した IPv6 の実装方法

GRE/IPv6 トンネルの設定

GRE トンネルは、IPv6 ネットワーク層を介して送出し、IPv6 トンネルで IPv4 パケットと IPv6 パケットを転送するように設定できます。

はじめる前に

GRE IPv6 トンネルが設定されている場合、IPv6 アドレスは、トンネル送信元およびトンネル宛先に割り当てられます。トンネル インターフェイスは、割り当て済みの IPv4 アドレスまたは IPv6 アドレスを持つことができます（ここでは説明していません）。設定されたトンネルの両端にあるホストまたはデバイスは、IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**interface tunnel** *tunnel-number* 例： `Device(config)# interface tunnel 0`	トンネル インターフェイスおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	次のいずれかのコマンドを入力します。 • **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} • **ipv6 address** *ipv6-prefix*/*prefix-length* [**eui-64**]	インターフェイスに割り当てられている IPv6 ネットワークを指定し、インターフェイスで IPv6 処理をイネーブルにします。 • **eui-64** キーワードを指定すると、ソフトウェアは、インターフェイスの IPv6 アドレスを設定し、アドレスの下位 64 ビットの EUI-64 インターフェイス ID を使用してインターフェイスで IPv6 処理を有効にします。

	コマンドまたはアクション	目的
	例： `Device(config-if)# ipv6 address 3ffe:b00:c18:1::3/127`	
ステップ 5	**tunnel source** {*ip-address* | *ipv6-address* | *interface-type interface-number*} 例： `Device(config-if)# tunnel source Tengigabitethernet 4/1/0`	送信元 IPv4 アドレス、IPv6 アドレスまたは送信元インターフェイス タイプおよびトンネル インターフェイスの番号を指定します。 • インターフェイスが指定されている場合、そのインターフェイスは IPv4 アドレスを使用して設定されている必要があります。
ステップ 6	**tunnel destination** {*hostname* | *ip-address* | *ipv6-address*} 例： `Device(config-if)# tunnel destination 2001:DB8:1111:2222::1/64`	トンネル インターフェイスの宛先 IPv4 アドレス、IPv6 アドレスまたはホスト名を指定します。
ステップ 7	**tunnel mode** {**aurp** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ipv6** | **ipip** [**decapsulate-any**] | **iptalk** | **ipv6** | **mpls** | **nos**} 例： `Device(config-if)# tunnel mode gre ipv6`	GRE IPv6 トンネルを指定します。 （注） **tunnel mode gre ipv6** コマンドでは、GRE をトンネルのカプセル化プロトコルとして指定します。
ステップ 8	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。

IPv4 GRE トンネルを介した IPv6 の設定例

例：IS-IS および IPv6 トラフィックを実行する GRE トンネル

次に、ルータ A とルータ B との間で IS-IS および IPv6 トラフィックをともに送出する GRE トンネルを設定する例を示します。

ルータ A の設定

```
ipv6 unicast-routing
clns routing
!
interface tunnel 0
 no ip address
 ipv6 address 3ffe:b00:c18:1::3/127
 ipv6 router isis
 tunnel source TenGigabitEthernet 4/1/0
 tunnel destination 2001:DB8:1111:2222::1/64
 tunnel mode gre ipv6
!
interface TenGigabitEthernet4/1/0
 ip address 10.0.0.1 255.255.255.0
!
router isis
 net 49.0000.0000.000a.00
```

ルータ B の設定

```
ipv6 unicast-routing
clns routing
!
interface tunnel 0
 no ip address
 ipv6 address 3ffe:b00:c18:1::2/127
 ipv6 router isis
 tunnel source TenGigabitEthernet 4/1/0
 tunnel destination 2001:DB8:1111:2222::2/64
 tunnel mode gre ipv6
!
interface TenGigabitEthernet4/1/0
 ip address 10.0.0.2 255.255.255.0
!
router isis
 net 49.0000.0000.000b.00
 address-family ipv6
 redistribute static
 exit-address-family
```

例：IPv6 トンネルのトンネル宛先アドレス

```
Router(config)#interface Tunnel0
Router(config-if)#ipv6 address 2001:1:1::1/48
Router(config-if)#tunnel source TenGigabitEthernet 4/1/0
Router(config-if)#tunnel destination 10.0.0.2
Router(config-if)#tunnel mode gre ipv6
Router(config-if)#exit
!
Router(config)#interface TenGigabitEthernet4/1/0
Router(config-if)#ip address 10.0.0.1 255.255.255.0
Router(config-if)#exit
!
Router(config)#ipv6 unicast-routing
Router(config)#router isis
Router(config)#net 49.0000.0000.000a.00
```

GRE IPv6 トンネルの設定方法

GRE IPv6 トンネルの設定

IPv6ネットワーク上でGREトンネルを設定するには、次の作業を実行します。GREトンネルは、IPv6 ネットワーク層を介して送出し、IPv6 トンネルを介して IPv6 パケットと IPv4 パケットを転送するように設定できます。

（注） IPv6 を有効にしたり、トンネルの出力インターフェイスの IPv6 MTU サイズを 1500 以上に設定したりして、警告メッセージを受信しないようにする必要があります。

はじめる前に

GRE IPv6トンネルが設定されている場合、IPv6アドレスは、トンネル送信元およびトンネル宛先に割り当てられます。トンネル インターフェイスは、IPv4 または IPv6 アドレスのいずれかにすることができます（このことは、以降の作業では示されていません）。設定されたトンネルの両端にあるホストまたはデバイスは、IPv4 プロトコル スタックと IPv6 プロトコル スタックの両方をサポートしている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**interfacetunnel** *tunnel-number* 例： `Device(config)# interface tunnel 0`	トンネル インターフェイスおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**tunnelsource**{*ipv6-address* | *interface-type interface-number*} 例： `Device(config-if)# tunnel source ethernet 0`	送信元 IPv6 アドレスまたは送信元インターフェイス タイプおよびトンネル インターフェイスの番号を指定します。 • インターフェイスのタイプと番号が指定されている場合、そのインターフェイスはIPv6アドレスを使用して設定する必要があります。

	コマンドまたはアクション	目的
		（注） このコンテキストで使用される構文だけが表示されます。詳細については、『IPv6 Command Reference』を参照してください。
ステップ 5	**tunneldestination** *ipv6-address* 例： `Device(config-if)# tunnel destination 2001:0DB8:0C18:2::300`	トンネル インターフェイスの宛先 IPv6 アドレスを指定します。 （注） このコンテキストで使用される構文だけが表示されます。詳細については、『IPv6 Command Reference』を参照してください。
ステップ 6	**tunnelmode greipv6** 例： `Device(config-if)# tunnel mode gre ipv6`	GRE IPv6 トンネルを指定します。 （注） **tunnelmodegreipv6** コマンドでは、GRE をトンネル インターフェイスのカプセル化プロトコルとして指定します。このコンテキストで使用される構文だけが表示されます。詳細については、『IPv6 Command Reference』を参照してください。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

GRE IPv6 トンネルの設定例

例：GRE IPv6 トンネルの設定

IPv6 トランスポートで GRE トンネルを設定する方法の例を次に示します。この例では、イーサネット 0/0 は IPv6 アドレスを備えており、これがトンネル インターフェイスが使用する送信元アドレスとなります。トンネルの宛先 IPv6 アドレスは直接指定されます。この例では、トンネルは IPv4 トラフィックおよび IS-IS トラックの両方を伝送します。

```
interface Tunnel0
 ip address 10.1.1.1 255.255.255.0
 ip router isis
 tunnel source Ethernet0/0
 tunnel destination 2001:DB8:1111:2222::1
 tunnel mode gre ipv6
!
interface Ethernet0/0
 no ip address
 ipv6 address 2001:DB8:1111:1111::1/64
!
router isis
 net 49.0001.0000.0000.000a.00
```

その他の参考資料

ここでは、GRE 機能に関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
CMTS コマンド リファレンス	次の URL にある『Cisco CMTS Cable Command Reference』。http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html
ケーブルを介した GRE トンネルの設定	次の URL にある『Configuring GRE Tunnel over Cable』。http://www.cisco.com/en/US/tech/tk86/tk89/technologies_configuration_example09186a008011520d.shtml

標準

規格	タイトル
SP-RFIv1.1-I09-020830	『Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1』（http://www.cablemodem.com）

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFC

RFC	タイトル
RFC 1701	『Generic Routing Encapsulation (GRE)』
RFC 1702	『Generic Routing Encapsulation over IPv4 networks』

RFC	タイトル
RFC 1853	『IP in IP Tunneling』
RFC 2003	『IP Encapsulation within IP』
RFC 2784	『Generic Routing Ecapsulation (GRE)』
RFC 2890	『Key and Sequence Number Extensions to GRE』

シスコのテクニカル サポート

説明	リンク
シスコのテクニカルサポートおよびドキュメンテーション Web サイトでは、製品、テクノロジー、ソリューション、テクニカル ティップス、ツールへのリンクなど、技術的なコンテンツを検索可能な形で大量に提供しています。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/cisco/web/support/index.html

Generic Routing Encapsulation に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *70*：*Generic Routing Encapsulation* に関する機能情報

機能名	リリース	機能情報
総称ルーティング カプセル化	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 23 章

Transparent LAN Service over Cable

このマニュアルでは、既存のワイドエリア ネットワーク（WAN）サポートを強化して、ハイブリッド ファイバ同軸ケーブル（HFC）ネットワーク上の複数のインターネット サービス プロバイダー（ISP）へのより柔軟なマネージド アクセスを提供する、Transparent LAN Service（TLS）over Cable について説明します。この機能により、サービス プロバイダーは、アップストリーム サービス ID（SID）を IEEE 802.1Q の仮想ローカル エリア ネットワーク（VLAN）にマッピングすることでレイヤ 2 トンネルを作成できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

- Transparent LAN Service over Cable に関する機能情報, 523 ページ

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *71*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

Transparent LAN Service over Cable の前提条件

- IEEE 802.1Q VLAN にマップされたケーブル モデムのハードウェア（MAC）アドレスを知る必要があります。
- すべての顧客宅内機器（CPE）からのトラフィックが集約されて同じ 802.1Q トンネルにグループ化されるように、レイヤ 2 ブリッジ アグリゲータ上にそれぞれの顧客別ブリッジ グループを作成する必要があります。

Transparent LAN Service over Cable の制限事項

- 特定のケーブル モデムに対して 802.1Q を設定すると、ルータでは以前のケーブル モデム設定がすべて削除されます。
- TLS over Cable は、その環境でベースライン プライバシー インターフェイス（BPI）がイネーブルになっているときのみ使用することを強くお勧めします。BPI がイネーブルになっていない状態で TLS 機能を使用すると、トラフィックは、複数のバーチャル プライベート ネットワーク（VPN）間を流れることができ、サービス妨害攻撃やスヌーピングに対して脆弱になる可能性があります。また、BPI がイネーブルでない場合は、ゲートウェイまたはファイアウォール ルータによってリモート ネットワークを分離することをお勧めします。

TLS 機能をレイヤ 2 VPN とともに使用する場合、関与するケーブル モデムのベースライン プライバシー インターフェイス（BPI）セキュリティ機能を必ずイネーブルにしてください。そうしない場合、そのレイヤ 2 トラフィックはアップストリームまたはダウンストリームで Cisco CMTS によりドロップされます。

- パケットはレイヤ 2 情報（ケーブル モデムの MAC アドレスとプライマリ SID）のみに基づいてレイヤ 2 トンネルにマッピングされます。パケットはトンネルを介して送信されるため、アクセス リスト、IP アドレスの source-verify、IP QoS などのレイヤ 3 サービスはサポートされません。
- ケーブル モデムからのトラフィックはすべて、同じレイヤ 2 トンネルにマッピングされます。ケーブルモデムの背後にあるさまざまな顧客宅内機器（CPE）デバイスからのトラフィックを区別することはできません。
- Transparent LAN Service over Cable 機能を使用しているときには CPE 学習を使用することはできません。ケーブル モデムがレイヤ 2 トンネルにマッピングされる場合、**showinterfacecablemodem** コマンドでは CPE デバイスの IP アドレスが「unavailable」と表示されます。
- DOCSIS QoS のレイヤ 2 トンネル間でのサポートは、プライマリ SID にのみ基づきます。セカンダリ サービスを使用しているトラフィックは、プライマリ SID と同じレイヤ 2 トンネルを使用します。
- この機能を使用しているデバイス（ケーブル モデム、その CPE デバイス、エンドポイント CPE デバイス）ではスパニング ツリー プロトコル（STP）を使用できません。特に、スパニ

ング ツリー プロトコルを VLAN ブリッジ アグリゲータとエンドポイントの顧客のデバイス間で使用することはできません。

- イーサネット IEEE 802.1Q VLAN インターフェイス上のレイヤ 2 トンネルには次の制限が適用されます。
  - IEEE 802.1Q トンネルは 10 ギガビット イーサネット インターフェイスでのみサポートされます。
  - Cisco CMTS ルータは最大 4095 の VLAN ID をサポートしますが、ブリッジ アグリゲータとして機能するスイッチがこれより少ない VLAN ID をサポートしている場合があります。この場合、ブリッジ アグリゲータ スイッチがサポートする VLAN の最大数までで Cisco CMTS を設定する必要があります。

Transparent LAN Service over Cable の情報

この項の構成は、次のとおりです。

機能の概要

Transparent LAN Service over Cable 機能は、サービス プロバイダーがケーブル モデムに対するトラフィックにレイヤ 2 トンネルを提供できるようにします。これにより、複数のサイトにある任意の数のケーブル モデムを使用して独自の仮想ローカル エリア ネットワーク（VLAN）を作成することができます。

Cisco CMTS で、各ケーブル モデムを適切な VLAN に（その MAC アドレスに基づき）マッピングします。このとき CMTS は、VLAN へのケーブル モデムのこの 1 対 1 のマッピングの内部データベースを作成し、これを適切な VLAN にパケットをカプセル化するために使用します。

CMTS はマップされたケーブル モデムからの CPE トラフィックを次の方法を使用してカプセル化します。

- IEEE 802.1Q マッピング：ケーブル モデムの MAC アドレスは、特定の 10 ギガビット イーサネット インターフェイスの IEEE 802.1Q VLAN にマッピングされ、ケーブル モデムからのすべてのトラフィックが指定された VLAN ID でタグ付けされます。

このグループのケーブル モデムに出入りするトラフィックはブリッジ アグリゲータによって 1 つの論理ネットワーク（VLAN）にブリッジされ、その特定のグループのケーブル モデム用のセキュアなバーチャル プライベート ネットワーク（VPN）を作成します。外部ルータによって特別に実行しない限り、特定の VLAN 上のトラフィックを他の VLAN に送信することはできません。

レイヤ 2 ブリッジ アグリゲータとして機能するスイッチは、適切な宛先にトラフィックを転送するために VLAN タギングを使用します。これにより、サービス プロバイダーは、顧客のネットワークのアドレッシング、ルーティング、およびトポロジの詳細を理解する必要がなくなります。

Transparent LAN Service とレイヤ 2 バーチャル プライベート ネットワーク

さらに、サービス プロバイダーは、プロバイダーのルータでの最小限の設定変更によってレイヤ 2 VPN を提供することができます。サービス加入者がプライベート ネットワークまたはケーブル モデムを変更する必要はなく、また、サービス プロバイダーがこの機能を有効にするために特別な DOCSIS コンフィギュレーション ファイルを提供する必要もありません。

レイヤ 2 VPN による TLS 機能に関しては、

- TLS 機能をレイヤ 2 VPN とともに使用する場合、関与するケーブル モデムのベースライン プライバシー インターフェイス（BPI）セキュリティ機能を必ずイネーブルにしてください。そうしない場合、そのレイヤ 2 トラフィックはアップストリームまたはダウンストリームで Cisco CMTS によりドロップされます。
- 顧客宅内機器（CPE）に関する情報は、**showcablemodem** コマンドの出力に表示されません。

IEEE 802.1Q マッピング

ここでは、Transparent LAN Service over Cable 機能で使用可能な、IEEE 802.1Q VLAN へのケーブル モデムのマッピングを説明します。

概要

Transparent LAN Service over Cable 機能は、サービス プロバイダーが IEEE 802.1Q 規格のタグを使用してイーサネット ネットワーク上のレイヤ 2 トンネルを提供できるようにします。これにより、異なるサイトにある任意の数のケーブル モデムを使用して独自の仮想ネットワークを作成することができます。

Cisco CMTS で、各ケーブル モデムを適切な VLAN に（その MAC アドレスに基づき）マッピングします。このとき CMTS は、VLAN へのケーブル モデムのこの 1 対 1 のマッピングの内部データベースを作成し、これを適切な VLAN にパケットをカプセル化するために使用します。

CMTS は、IEEE 802.1Q-1993, IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks で定義されているように、VLAN タグを使用してマップされたケーブル モデムから CPE トラフィックをカプセル化します。レイヤ 2 ブリッジ アグリゲータとして機能するスイッチは、適切な宛先にパケットを転送するために VLAN タギングを使用します。

このグループのケーブル モデムに出入りするトラフィックはブリッジ アグリゲータによって 1 つの論理ネットワークにブリッジされ、その特定のグループのケーブル モデム用のセキュアなバーチャル プライベート ネットワーク（VPN）を作成します。外部ルータによって特別に実行しない限り、特定の VLAN 上のトラフィックを他の VLAN に送信することはできません。

IEEE 802.1Q マッピングの詳細

IEEE 802.1Q VLAN を使用して Transparent LAN Service over Cable 機能を実装するには、サービス プロバイダーは次の構成手順を実行する必要があります。

1. IEEE 802.1Q VLAN にマッピングする必要があるケーブル モデムと MAC アドレスを特定します。
2. ブリッジ アグリゲータとして動作しているルータで、必要な VLAN を作成します。
3. Cisco CMTS 上のレイヤ 2 マッピングを有効にし、その Cisco CMTS 上の各ケーブル モデムを適切な VLAN にマッピングします。

Transparent LAN Service over Cable 機能が有効になって IEEE 802.1Q マッピングを使用するように構成された後、Cisco CMTS は、関連付けられたケーブル モデムと VLAN との間のトラフィック マッピングをただちに開始します。効率的にマッピングを行うため、Cisco CMTS は、各ケーブル モデムのプライマリ サービス フロー ID（SFID）およびサービス ID（SID）を適切な VLAN とイーサネット インターフェイスにリンクする内部データベースを保持します。これにより、ケーブル モデムからのすべてのサービス フローが正しくルーティングされます。

Cisco CMTS は、アップストリームでパケットを受信すると、SID を検索して、VLAN にマッピングされていることを確認します。そうである場合、パケットの送信元 MAC アドレスがケーブル モデムの MAC アドレスでないならば、Cisco CMTS は適切な IEEE 802.1Q VLAN タグをパケットのヘッダーに挿入し、そのパケットを適切なイーサネット インターフェイスに転送します。パケットがマッピングされていない場合、またはパケットがケーブル モデムから発信された場合、Cisco CMTS は通常のレイヤ 3 プロセスを使用してパケットをルーティングします。

Cisco CMTS が IEEE 802.1Q VLAN タグでカプセル化された WAN インターフェイスからパケットを受信すると、パケットの SID を検索して、マッピングされているケーブル モデムにそのパケットが属しているかどうかを調べます。そうである場合、Cisco CMTS は VLAN タグを削除し、適切な DOCSIS ヘッダーを追加し、適切なダウンストリーム インターフェイス上でパケットを送信します。パケットがマッピングされていない場合、Cisco CMTS は通常のレイヤ 3 プロセスを続行します。

利点

Transparent LAN Service over Cable 機能では、ケーブル サービス プロバイダーとそのパートナーおよびカスタマーに次の利点があります。

- レイヤ 2 レベルのマッピングを提供します。これは、レイヤ 3 のプロトコルとサービスに対して透過的です。つまり、サービス プロバイダーはカスタマーのネットワーク トポロジ、ルーティング プロトコル、または IP アドレッシングについてその詳細を知る必要はありません。
- サービス プロバイダーは、既存のイーサネット WAN ネットワークの使用率を最大化できます。複数のカスタマーを同じ発信インターフェイス上にまとめることができますが、トンネル上を送信されるため、各カスタマーのネットワークはプライベート状態が引き続き保証されます。
- 複数のカスタマーに高い柔軟性のあるスケーラブル ソリューションを提供します。サービス プロバイダーは、VPN ごとにブリッジ グループを 1 つだけ作成する必要があり、ケーブル モデムごとに VLAN マッピング 1 つのみがその VPN トンネルに参加する必要があります。
- カスタマーは自社のプライベート ネットワークを引き続きフル コントロールできる一方で、サービス プロバイダーはケーブル モデム、およびケーブル ネットワークや WAN ネットワー

クの残りの部分を引き続きフル コントロールできます。ケーブル モデムからの CPE トラフィックのみが L2VPN トンネルにマッピングされ、ケーブル モデムから発信されるトラフィックはサービス プロバイダーのネットワークによって通常どおり処理され続けます。

- サービス プロバイダーは、同じ DOCSIS ケーブル ネットワーク上でトンネル型と非トンネル型のケーブル モデムを混在させることができます。
- カスタマーは、複数のサイト用にイーサネット レイヤ 2 接続による単一のセキュアな仮想ネットワークを作成できます。
- 帯域幅やその他のネットワーク リソースを最大限に活用するために、さまざまなカスタマーやエンドポイントからの複数のトンネルを単一のブリッジに集約できます。
- マルチプロトコル ラベル スイッチング（MPLS）VPN などのレイヤ 3 ソリューションの場合と同様に、（単なる IP レイヤ 3 サービスではなく）複数のレイヤ 3 非 IP プロトコルのトンネリングをサポートします。
- すべての DOCSIS サービス（BPI+ 暗号化と認証を含む）は、すべてのケーブル モデムで引き続きサポートされます。

Transparent LAN Service over Cable の設定方法

この項の構成は、次のとおりです。

IEEE 802.1Q VLAN マッピングの設定

ここでは、Cisco CMTS でレイヤ 2 マッピングをイネーブルにする方法と、その後、特定のケーブルを IEEE 802.1Q VLAN にマッピングする方法を説明します。

IEEE 802.1Q マッピングのレイヤ 2 トンネリングの有効化と設定

ここでは、Cisco CMTS でレイヤ 2 マッピングをイネーブルにする方法、10 ギガビット イーサネット インターフェイスで IEEE 802.1Q VLAN に特定のケーブル モデムをマッピングする方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cablel2-vpn-servicexconnectnsidot1q** 例： `Router(config)# cable l2-vpn-service xconnect nsi dot1q`	IEEE 802.1Q VLAN マッピングでレイヤ 2 トンネリングをイネーブルにします。 （注） Cisco CMTS で VLAN トランキングを設定する必要はありません。VLAN トランキングはサポートされていますが、VLAN トランキングが Cisco CMTS に与える影響を認識してください。
ステップ 4	**cabledot1q-vc-map***mac-address ethernet-interface vlan-id* [*cust-name*] 例： `Router(config)# cable dot1q-vc-map 0000.0C04.0506 TenGigabitEthernet4/1/0 10`	ケーブル モデムの指定した MAC アドレスを、表示された VLAN および 10 ギガビット イーサネットインターフェイスにマッピングします。 （注） IEEE 802.1Q VLAN にマップされる各ケーブル モデムでこのコマンドを繰り返します。
ステップ 5	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IEEE 802.1Q VLAN ブリッジ グループの作成

ここでは、Cisco ルータの設定に必要な最小構成について説明します。これは、IEEE 802.1Q VLAN ブリッジ アグリゲータとして機能するため、Transparent LAN Service over Cable 機能で使用されている VLAN を終了できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal` 例：	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	**interface TenGigabitEthernet** *slot/subslot/port* 例： `Router(config)# interface TenGigabitEthernet4/1/0`	10 ギガビット イーサネット インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipaddress** *ip-address mask* 例： `Router(config-if)# ip address 10.10.10.85 255.255.255.0`	指定した IP アドレスとサブネット マスクでインターフェイスを設定します。
ステップ 5	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーションを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface TenGigabitEthernet** *slot/subslot/port.y* 例： `Router(config)# interface TenGigabitEthernet4/1/0.10`	10 ギガビット イーサネット インターフェイスでサブインターフェイスを作成します。 （注） ネットワーク管理を簡単にするには、このサブインターフェイスを使用する VLAN ID（この場合は 10）と同じ値にサブインターフェイス番号を設定します。 （注） サブインターフェイスを作成する手順は、フレームの dot1q タギングには必要ありませんが、推奨されています。
ステップ 7	**bridgegroup** *number* 例： `Router(config-if)# bridge group 20`	指定したブリッジ グループに属するようにこのサブインターフェイスを設定します。 （注） 作成およびブリッジするサブインターフェイス単位で、ステップ 5 ～ステップ 7 を繰り返します。
ステップ 8	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

Transparent LAN Service over Cable の設定例

この項では、ブリッジアグリゲータとして動作するCMTSルータおよびCiscoルータへのTransparent LAN Service over Cable 機能の設定例を示します。

例：IEEE 802.1Q VLAN マッピングの設定

次の設定の一部は、2 つの異なる IEEE 802.1Q VLAN にマッピングされた多くのケーブル モデムを表示する一般的な設定です。

```
cable l2-vpn-service xconnect nsi dot1q
! Customer 1
cable dot1q-vc-map 000C.0e03.69f9 TenGigabitEthernet 4/1/0 10 Customer1
cable dot1q-vc-map 0010.7bea.9c95 TenGigabitEthernet 4/1/0 11 Customer1
cable dot1q-vc-map 0010.7bed.81c2 TenGigabitEthernet 4/1/0 12 Customer1
cable dot1q-vc-map 0010.7bed.9b1a TenGigabitEthernet 4/1/0 13 Customer1
! Customer 2
cable dot1q-vc-map 0002.fdfa.137d TenGigabitEthernet 4/1/0 20 Customer2
cable dot1q-vc-map 0006.28f9.9d19 TenGigabitEthernet 4/1/0 21 Customer2
cable dot1q-vc-map 000C.7b6b.58c1 TenGigabitEthernet 4/1/0 22 Customer2
cable dot1q-vc-map 000C.7bed.9dbb TenGigabitEthernet 4/1/0 23 Customer2
cable dot1q-vc-map 000C.7b43.aa7f TenGigabitEthernet 4/1/0 24 Customer2
cable dot1q-vc-map 0050.7302.3d83 TenGigabitEthernet 4/1/0 25 Customer2
...
```

例：IEEE 802.1Q ブリッジ アグリゲータの設定

次に、IEEE 802.1Q タギング機能を使用して、同じ 10 ギガビット イーサネット インターフェイス間で VLAN を送信するブリッジ アグリゲータとして使用されるルータの例を示します。

```
!
interface TenGigabitEthernet4/1/0
 ip address 10.10.10.31 255.255.255.0
 duplex full
 speed auto
!
interface TenGigabitEthernet4/1/0.10
 description Customer1-site10
 encapsulation dot1Q 10
 bridge-group 200
interface TenGigabitEthernet4/1/0.11
 description Customer1-site11
 encapsulation dot1Q 11
 bridge-group 200
interface TenGigabitEthernet4/1/0.12
 description Customer1-site12
 encapsulation dot1Q 12
 bridge-group 200
interface TenGigabitEthernet4/1/0.13
 description Customer1-site13
 encapsulation dot1Q 13
 bridge-group 200
!-----------------------------------
interface TenGigabitEthernet4/1/0.20
 description Customer2-site20
 encapsulation dot1Q 20
 bridge-group 201
interface TenGigabitEthernet4/1/0.21
 description Customer2-site21
 encapsulation dot1Q 21
```

```
 bridge-group 201
interface TenGigabitEthernet4/1/0.22
 description Customer2-site22
 encapsulation dot1Q 22
 bridge-group 201
interface TenGigabitEthernet4/1/0.23
 description Customer2-site23
 encapsulation dot1Q 23
 bridge-group 201
interface TenGigabitEthernet4/1/0.24
 description Customer2-site24
 encapsulation dot1Q 24
 bridge-group 201
interface TenGigabitEthernet4/1/0.25
 description Customer2-site25
 encapsulation dot1Q 25
 bridge-group 201
!
bridge 200 protocol ieee
bridge 201 protocol ieee
...
```

Transparent LAN Service over Cable の設定の確認

- **show cable l2-vpn xconnect dot1q-vc-map** ：IEEE 802.1Q VLAN にケーブル モデムをマッピングする際の情報を表示します。

  次に、コマンドの出力例を示します。

  ```
  Router# show cable l2-vpn xconnect dot1q-vc-map

  MAC Address    Ethernet Interface      VLAN ID   Cable Intf  SID  Customer Name/VPNID
  38c8.5cac.4a62 TenGigabitEthernet4/1/2     56    Cable3/0/0  4    Customer2
  38c8.5cfe.f6fa TenGigabitEthernet4/1/2     34    Cable3/0/0  3    Customer1
  602a.d083.2e1c TenGigabitEthernet4/1/4     43    Cable3/0/0  5    Customer3
  ```

- **show cable l2-vpn xconnect dot1q-vc-map customer** *name*：指定した顧客名に関して IEEE 802.1Q VLAN にケーブル モデムをマッピングする際の情報を表示します。

  次に、コマンドの出力例を示します。

  ```
  Router# show cable l2-vpn xconnect dot1q-vc-map customer Customer1

  MAC Address    Ethernet Interface      VLAN ID   Cable Intf  SID  Customer Name/VPNID
  38c8.5cfe.f6fa TenGigabitEthernet4/1/2     34    Cable3/0/0  3    Customer1
  ```

- **show cable l2-vpn xconnect dot1q-vc-map** *mac-address*：指定した MAC アドレスに関して IEEE 802.1Q VLAN にケーブル モデムをマッピングする際の情報を表示します。

  次に、コマンドの出力例を示します。

  ```
  Router# show cable l2-vpn xconnect dot1q-vc-map 38c8.5cac.4a62

  MAC Address    Ethernet Interface      VLAN ID   Cable Intf  SID  Customer Name/VPNID
  38c8.5cac.4a62 TenGigabitEthernet4/1/2     56    Cable3/0/0  4    Customer2
  ```

- **show cable l2-vpn xconnect dot1q-vc-map** *mac-address***verbose**：アップストリームおよびダウンストリームで受信するパケット数やバイト数など、レイヤ 2 マッピングの詳細情報を表示します。

次に、コマンドの出力例を示します。

```
Router# show cable l2-vpn xconnect dot1q-vc-map 38c8.5cac.4a62 verbose

MAC Address                          : 38c8.5cac.4a62
Customer Name                        : Customer2
Prim Sid                             : 4
Cable Interface                      : Cable3/0/0
Ethernet Interface                   : TenGigabitEthernet4/1/2
DOT1Q VLAN ID                        : 56
Total US pkts                        : 1
Total US bytes                       : 342
Total DS pkts                        : 4
Total DS bytes                       : 512
```

その他の参考資料

標準

標準	タイトル
SP-RFIv1.1-I08-020301	『Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification』
IEEE 802.1Q の 1998 年版	『IEEE Standards for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks』

RFC

RFC[2]	タイトル
RFC 1163	『A Border Gateway Protocol』
RFC 1164	『Application of the Border Gateway Protocol in the Internet』
RFC 2233	『DOCSIS OSSI Objects Support』
RFC 2283	『Multiprotocol Extensions for BGP-4』
RFC 2665	『DOCSIS Ethernet MIB Objects Support』
RFC 2669	『Cable Device MIB』

2 サポートされている RFC がすべて記載されているわけではありません。

シスコのテクニカル サポート

説明	リンク
Technical Assistance Center（TAC）ホーム ページ：多数の技術関連の記事と、製品、テクノロジー、ソリューション、テクニカル ティップス、ツールへのリンクを提供する Web サイトです。必要な記事は検索して見つけることができます。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/cisco/web/support/index.html

Transparent LAN Service over Cable に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *72*：アップストリーム チャネル ボンディングに関する機能情報

機能名	リリース	機能情報
Transparent LAN Service over Cable	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 24 章

バッテリ バックアップ モードでのチャネル ボンディングのダウングレード

Cisco CMTS は、バッテリ バックアップ モードのケーブル モデムとメディア ターミナル アダプタ（MTA）のチャネル ボンディングのダウングレードをサポートします。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *73*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

バッテリ バックアップ モードでのチャネル ボンディングのダウングレードの前提条件

- ケーブル モデムが DOCSIS3.0 に準拠し、バッテリバックアップ機能を備えている必要があります。
- 少なくとも 1 つのダウンストリーム チャネルを含むダウンストリーム チャネル ボンディング グループが使用可能である必要があります。
- 少なくとも 1 つのアップストリーム チャネルを含むアップストリーム チャネル ボンディング グループが使用可能である必要があります。

バッテリ バックアップ モードでのチャネル ボンディングのダウングレードの制限事項

- ケーブル モデムが CM-STATUS イベント 9 および 10 をサポートしない場合、バッテリバックアップ モードのケーブル モデムでチャネル ボンディングはダウングレードされません。

（注） MAC ドメイン内の各プライマリ チャネルに個別の動的ボンディング グループを設定することを推奨します。

- ケーブルモデムがアクティブな音声コールを持つ場合、バッテリバックアップ モードのケーブル モデムでチャネル ボンディングはダウングレードされません。
- ケーブル モデムが保護ラインカードで動作しているときに、そのプライマリ チャネルが動的ボンディング グループに含まれていない場合、チャネル ボンディングはダウングレードされません。
- ケーブル モデムがバッテリバックアップ モードに入るかまたはバッテリバックアップ モードを終了するときにラインカードがスイッチオーバーすると、そのケーブルモデムはオフラインになる場合があります。

バッテリ バックアップ モードでのチャネル ボンディングのダウングレードの情報

この機能がイネーブルの場合、ケーブルモデムがバッテリバックアップモードに入ると、チャネル ボンディングは 1 つのダウンストリーム チャネルと 1 つのアップストリーム チャネル（バッテリ バックアップ 1x1 モード）にダウングレードします。この機能により、ケーブル モデムがバッテリ バックアップで稼働しているときの電力使用量が減ります。ケーブル モデムが AC 電源

モードに戻ると、チャネル ボンディングは元の設定に戻ります。この機能は、グローバルでも各 MAC ドメインでも設定できます。

（注） この機能を、グローバルおよび各 MAC ドメインでイネーブルにすることを推奨します。

ケーブル モデムでは、次の CM-STATUS イベントを使用して、電源ステータスを Cisco CMTS に示します。

- 9：ケーブル モデムがバッテリバックアップ モードで動作していることを示します。
- 10：ケーブル モデムが AC 電源モードに戻ったことを示します。

この機能がディセーブルの場合、バッテリ バックアップでの稼働中も、ケーブルモデムはチャネル ボンディングをダウングレードすることができません。

バッテリ バックアップ モードでのチャネル ボンディングのダウングレードの設定方法

この項の構成は、次のとおりです。

バッテリバックアップモードでのチャネルボンディングのダウングレードのグローバル設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 reduction-mode mta-battery enable** 例： `Router(config)# cable reduction-mode mta-battery enable`	バッテリ バックアップ モードのケーブル モデムのチャネルボンディングのダウングレードをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**cable reduction-mode mta-battery dampen-time** *seconds* 例： `Router(config)# cable reduction-mode mta-battery dampen-time 40`	（任意）ケーブルモデムでチャネルボンディング ダウングレード 1x1 モードの開始または終了を延期するには、減衰の時間を秒単位で設定します。
ステップ 5	**cable reduction-mode mta-battery ranging-init-technique** *us-ranging-init-technique* 例： `Router(config)# cable reduction-mode mta-battery ranging-init-technique 3`	（任意）init-ranging 方法を設定します。
ステップ 6	**cable reduction-mode mta-battery dynamic-channel-percent** *percent* 例： `Router(config)# cable reduction-mode mta-battery dynamic-channel-percent 10`	（任意）バッテリ バックアップ モードで動的チャネル帯域幅の上限と初回の割合を設定します。 （注） 新しく作成された動的ボンディング グループに参加するときに動的チャネル帯域幅を割り当てられるように、プライマリ チャネルに十分な帯域幅を残すようにします。
ステップ 7	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。

バッテリ バックアップ モードでの MAC ドメイン向けチャネル ボンディングのダウングレードの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacewideband-cable** *slot/subslot/port:wideband-channel* 例： `Router(config)# interface wideband-cable 1/0/0:7`	ワイドバンド ケーブル インターフェイスを設定します。
ステップ 4	**cableds-resiliency** 例： `Router(config-if)# cable ds-resiliency`	ライン カードまたはコントローラごとの使用に合わせて、復元力のボンディング グループまたは WB インターフェイスを予約します。
ステップ 5	**exit** 例： `Router(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**interface cable** *slot/subslot/port* 例： `Router(config)# interface cable 9/0/0`	ルータでケーブル インターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**cable reduction-mode mta-battery enable** 例： `Router(config-if)# cable reduction-mode mta-battery enable`	各MACドメインに対してバッテリ バックアップ モードのケーブル モデムのチャネル ボンディングのダウングレードをイネーブルにします。
ステップ 8	**cable cm-status enable 9** 例： `Router(config-if)# cable cm-status enable 9`	MAC ドメインの CM-STATUS イベント 9 をイネーブルにします。値 9 は、ケーブル モデムがバッテリ バックアップ モードで動作していることを示します。
ステップ 9	**cable cm-status enable 10** 例： `Router(config-if)# cable cm-status enable 10`	MAC ドメインの CM-STATUS イベント 10 をイネーブルにします。値10は、ケーブル モデムがAC電源モードに戻ったことを示します。
ステップ 10	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。

バッテリ バックアップ モードでのチャネル ボンディングのダウングレード設定の確認

- **show cable modem**：ケーブル モデムがバッテリ バックアップ モードで実行している場合の情報を表示します。

  次に、コマンドの出力例を示します。

```
Router# show cable modem

  D
MAC Address    IP Address      I/F           MAC               Prim  RxPwr  Timing Num
 I
                                              State             Sid   (dBmv) Offset CPE
 P
f45f.d4a1.b75a ---             C6/1/0/UB     p-online(pt)       846  !-3.50  1475   0
  N
c427.9551.3489 30.154.1.12     C6/1/0/UB     w-online(pt)       930   -0.50  1579   2
  Y
f45f.d4a1.b762 30.55.223.253   C6/1/0/UB     w-online           1770  0.00   1503   0
  Y
0016.925e.661a 30.55.230.136   C6/1/0/U0     online(pt)         825   -0.50  1467   1
  N
4458.2945.458a 30.0.7.72       C6/1/0/UB     w-online           3916  0.00   1511   2
  Y
4458.2945.401e ---             C6/1/0/UB     w-online(pt)       847   -0.50  1473   1
  N
4458.2945.20c6 ---             C6/1/0/UB     w-online(pt)(bm)   895   0.00   1481   0
  N
```

- **show cable modem reduction-mode mta-battery**：バッテリ バックアップ モードのケーブル モデムのチャネル ボンディングのダウングレード情報を表示します。

  次に、コマンドの出力例を示します。

```
Router# show cable modem reduction-mode mta-battery

                              Orig BG                        Curr BG
I/F     MAC Address    ID      I/F       RFs     ID          I/F        Upstream
------- -------------- ------------------------------------------------------
C7/0/0  0025.2eaf.843e 897  Wi7/0/0:0     4      252         Wi7/0/0:1      US0
C7/0/0  0025.2eaf.8356 897  Wi7/0/0:0     4      252         Wi7/0/0:1      US0
C7/0/0  0015.d176.5199 897  Wi7/0/0:0     4      252         Wi7/0/0:1      US0
```

次に、MAC アドレスを指定した場合のケーブル モデムに対するコマンドの出力例を示します。

```
Router# show cable modem 0025.2eaf.843e reduction-mode mta-battery

                              Orig BG                        Curr BG
I/F     MAC Address    ID      I/F       RFs     ID          I/F        Upstream
------- -------------- ------------------------------------------------------
C7/0/0  0025.2eaf.843e 897  Wi7/0/0:0     4      252         Wi7/0/0:1      US0
```

次に、IPアドレスを指定した場合のケーブルモデムに対するコマンドの出力例を示します。

```
Router# show cable modem 90.18.0.9 reduction-mode mta-battery

                              Orig BG                        Curr BG
I/F     MAC Address    ID      I/F       RFs     ID          I/F        Upstream
```

```
------- -------------- ------------------------------------------------------------
C7/0/0  0025.2eaf.843e 897  Wi7/0/0:0     4      252        Wi7/0/0:1      US0
```

次に、IPv6 アドレスを指定した場合のケーブル モデムに対するコマンドの出力例を示します。

```
Router# show cable modem 2001:18::9 reduction-mode mta-battery

                              Orig BG                        Curr BG
I/F     MAC Address    ID      I/F       RFs     ID          I/F        Upstream
------- -------------- ------------------------------------------------------------
C7/0/0  0025.2eaf.843e 897  Wi7/0/0:0     4      252        Wi7/0/0:1      US0
```

- **show cable modem verbose**：ケーブル モデムの詳細情報を示します。

次に、コマンドの出力例を示します。

```
Router# show cable modem 54d4.6ffb.30fd verbose

MAC Address                          : 54d4.6ffb.30fd
IP Address                           : 40.4.58.14
IPv6 Address                         : 2001:40:4:58:741A:408D:7E4B:D7C8
Dual IP                              : Y
Prim Sid                             : 9
Host Interface                       : C7/0/0/UB
MD-DS-SG / MD-US-SG                  : 1 / 1
MD-CM-SG                             : 0x3C0101
Primary Wideband Channel ID          : 897 (Wi7/0/0:0)
Primary Downstream                   : In7/0/0:2 (RfId : 722)
Wideband Capable                     : Y
RCP Index                            : 3
RCP ID                               : 00 10 00 00 08
Downstream Channel DCID RF Channel : 99    7/0/0:2
Downstream Channel DCID RF Channel : 97    7/0/0:0
Downstream Channel DCID RF Channel : 98    7/0/0:1
Downstream Channel DCID RF Channel : 100   7/0/0:3
Multi-Transmit Channel Mode          : Y
Extended Upstream Transmit Power     : 0dB
Upstream Channel                     : US0        US1
Ranging Status                       : sta        sta
Upstream SNR (dB)                    : 36.12      32.55
Upstream Data SNR (dB)               : --         --
Received Power (dBmV)                : 0.00       0.00
Reported Transmit Power (dBmV)       : 25.25      26.00
Peak Transmit Power (dBmV)           : 54.00      54.00
Phy Max Power (dBmV)                 : 54.00      54.00
Minimum Transmit Power (dBmV)        : 24.00      24.00
Timing Offset              (97.6 ns): 1226       1226
Initial Timing Offset                : 1229       973
Rng Timing Adj Moving Avg(0.381 ns): -1         0
Rng Timing Adj Lt Moving Avg         : -7         0
Rng Timing Adj Minimum               : -768       0
Rng Timing Adj Maximum               : 0          64768
Pre-EQ Good                          : 0          0
Pre-EQ Scaled                        : 0          0
Pre-EQ Impulse                       : 0          0
Pre-EQ Direct Loads                  : 0          0
Good Codewords rx                    : 515        472
Corrected Codewords rx               : 0          0
Uncorrectable Codewords rx           : 0          0
Phy Operating Mode                   : atdma*     atdma*
sysDescr                             :
Downstream Power                     : 0.00 dBmV (SNR = ----- dB)
MAC Version                          : DOC3.0
QoS Provisioned Mode                 : DOC1.1
Enable DOCSIS2.0 Mode                : Y
Modem Status                         : {Modem= w-online, Security=disabled}
Capabilities                         : {Frag=N, Concat=N, PHS=Y}
Security Capabilities                : {Priv=, EAE=Y, Key_len=}
L2VPN Capabilities                   : {L2VPN=N, eSAFE=N}
Sid/Said Limit                       : {Max US Sids=16, Max DS Saids=15}
```

```
Optional Filtering Support          : {802.1P=N, 802.1Q=N, DUT=N}
Transmit Equalizer Support          : {Taps/Symbol= 1, Num of Taps= 24}
Number of CPE IPs                   : 0(Max CPE IPs = 16)
CFG Max-CPE                         : 200
Flaps                               : 0()
Errors                              : 0 CRCs, 0 HCSes
Stn Mtn Failures                    : 0 aborts, 0 exhausted
Total US Flows                      : 1(1 active)
Total DS Flows                      : 1(1 active)
Total US Data                       : 7 packets, 2006 bytes
Total US Throughput                 : 0 bits/sec, 0 packets/sec
Total DS Data                       : 5 packets, 1202 bytes
Total DS Throughput                 : 0 bits/sec, 0 packets/sec
LB group ID assigned (index)        : 2151416065 (48131)
LB group ID in config file (index)  : N/A (N/A)
LB policy ID                        : 0
LB policy ID in config file         : 0
LB priority                         : 0
Tag                                 :
Required DS Attribute Mask          : 0x0
Forbidden DS Attribute Mask         : 0x0
Required US Attribute Mask          : 0x0
Forbidden US Attribute Mask         : 0x0
Service Type ID                     :
Service Type ID in config file      :
Active Classifiers                  : 2 (Max = NO LIMIT)
CM Upstream Filter Group            : 0
CM Downstream Filter Group          : 0
CPE Upstream Filter Group           : 0
CPE Downstream Filter Group         : 0
DSA/DSX messages                    : permit all
Voice Enabled                       : NO
CM Energy Management Capable        : Y
CM Enable Energy Management         : Y
CM Enter Energy Management          : No
Battery Mode                        : Yes
Battery Mode Status                 : BATTERY_MODE / AC_POWER_MODE
DS Change Times                     : 0
Boolean Services                    : 2
Number of Multicast DSIDs Support   : 16
MDF Capability Mode                 : 2
IGMP/MLD Version                    : MLDv2
FCType10 Forwarding Support         : Y
Features Bitmask                    : 0x0
Total Time Online                   : 2h12m   (2h12m    since last counter reset)
CM Initialization Reason            : NO_PRIM_SF_USCHAN
CFG Max IPv6 CPE Prefix             : 16 (-1 used)
```

（注） *Battery Mode* は、ケーブル モデムがバッテリ バックアップ モードまたは AC 電源モードのどちらであるかを示します。

Battery Mode Status は、ケーブル モデムのステータスを示します。

- ケーブル モデムのステータスが AC_POWER_MODE/BATTERY_MODE の場合は、安定状態です。
- ケーブル モデムのステータスが AC_POWER_PENDING/BATTERY_PENDING の場合は、転送状態です。
- ケーブル モデムのステータスが AC_POWER_HOLD/BATTERY_HOLD の場合は、減衰の時間が切れるまで最後に受信したイベントのステータスを更新しています。

- **show cable modem cm-status**：ケーブル モデム CM-STATUS のイベント情報を表示します。

次に、コマンドの出力例を示します。

```
Router# show cable modem e448.c70c.9d80 cm-status

I/F       MAC Address    Event              TID   Count Error Dups  Time
C6/0/3/UB e448.c70c.9d80 Battery backup     14     1    0     0     Apr 2 22:17:29
          e448.c70c.9d80 A/C power          1      1    0     0     Apr 2 22:43:52
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
CMTS コマンド	『Cisco CMTS Cable Command Reference』

標準および RFC

標準/RFC	タイトル
CM-SP- MULPIv3.1-I01-131029	『Data-Over-Cable Service Interface Specifications, DOCSIS 3.1, MAC and Upper Layer Protocols Interface Specification』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

バッテリ バックアップ モードでのチャネル ボンディングのダウングレードに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *74* : バッテリ バックアップ モードでのチャネル ボンディングのダウングレードに関する機能情報

機能名	リリース	機能情報
バッテリ バックアップ 1x1 モード	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に導入されました。

第 25 章

D-PON のアップストリーム ボンディング サポート

DOCSIS 受動光ネットワーク（D-PON）アーキテクチャ（RF over Glass：RFoG とも呼ばれる）は、ケーブル オペレータがファイバ ツー ホーム マーケット スペースに入って DOCSIS インフラストラクチャを効率的に利用するうえで役立ちます。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *75*：***Cisco cBR*** シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

D-PON のアップストリーム ボンディング サポートの前提条件

- DOCSIS 3.0 ケーブル モデム（CM）
- DOCSIS 2.0 対応セットトップ ボックス（STB）
- 非 D-PON 参照アップストリーム チャネルに関する追加のブロードキャスト初期レンジング機会の使用を防止するには、**cable upstream ranging-init-technique 2** コマンドを設定する必要があります。

D-PON のアップストリーム ボンディング サポートの制限事項

- 複数の CM を同時に機能させることはできません。CM ごとに異なるタイムスロットでアップストリーム データ伝送を行う必要があります。D-PON を設定すると、アップストリーム スケジューラがデータ伝送を許可する CM は常に 1 つだけとなります。
- 個々の MAC ドメインの D-PON を有効/無効にすることができます。
- MAC ドメインで D-PON を有効にするときには、**shutdown** および **noshutdown** コマンドを使用して、MAC ドメインを手動でシャットダウンしてから有効にする必要があります。
- MAC ドメインのすべての周波数で、次の項目を同じ設定にする必要があります。
  - ミニスロット サイズ
  - チャネル幅
  - 変調プロファイル
- ATDMA DOCSIS モードだけがサポートされます。
- D-PON 用に設定された MAC ドメインでは、次の機能がサポートされません。
  - ロード バランシング
  - スペクトル管理
  - アップストリーム設定（アップストリーム設定を変更するには、MAC ドメインをシャットダウンする必要があります）
  - S-CDMA 論理チャネル
  - 変調プロファイルの低減（D-PON では 16 QAM および 64 QAM 変調プロファイルのみを使用します）
  - 3.2 MHz および 6.4 MHz 以外のチャネル幅
  - インサービス ソフトウェア アップグレード（ISSU）
  - 同じ MAC ドメインでの D-PON および HFC の混在
  - ソフトウェア ライセンス

D-PON のアップストリーム ボンディング サポートについて

D-PON は一種のネットワーキングであり、光ネットワークを介して CMTS が RF 信号を送信できるようにします。この技術により、ケーブルオペレータは光同軸ハイブリッド（HFC）ネットワークで RF 技術を使用することができます。

CMTS からのダウンストリーム データはハブで他の RF 信号と結合されて、トランスミッタに送信されます。トランスミッタからの信号は、複数の PON を対象とします。各 PON が、単一ファイバからの 32 個のホームに対応します。

光ネットワーク ターミナル（ONT）からのアップストリームデータはスプリッタで結合されてハブに送信され、そこから光レシーバ（RX）にルーティングされます。複数の光レシーバからのアップストリーム データが結合されて、CMTS に送信されます。

CMTS へのアップストリーム データには、複数の PON からの信号が含まれます。複数の DOCSIS アップストリーム ソース（複数のモデムおよび DSG ターミナル）を含むことができる各 PON に、それぞれ専用のアップストリーム光レシーバが対応します。

同軸ネットワークに応じて、さまざまな方法でPONを構成できます。これらの構成は、次のカテゴリに大別されます。

- 内部制御型構成：この構成では、ONT の内部 CM がレーザーを制御します。アップストリーム信号は CM のイーサネット インターフェイスに送信され、ONT はアップストリームのタイミングを制御できます。このタイプの構成を使用するデバイスは、Digital Audio Visual Council（DAVIC）セット トップ端末（STT）です。
- 外部制御型構成：この構成では、ONT アップストリーム入力での RF の存在によってレーザーがアクティブ化されます。このタイプの構成を使用するデバイスは、DOCSIS セットトップ ゲートウェイ（DSG）デバイスです。
- デュアル制御型構成：この構成では、ONT が格納されているホームと内部 CM が、その他の DOCSIS アップストリーム ソース（DSG など）と連動してレーザーを制御します。RF プレゼンス ディテクタまたは内部 CM 制御回線が、アップストリーム信号を検出してアップストリーム レーザーをアクティブ化します。

アップストリームでの D-PON のスケジューリング

D-PON 実装では、CMTS のネイティブ アップストリーム スケジューリング ソフトウェアがアップストリーム データ伝送のタイミングを制御します。アップストリームの周波数割り当てに関わらず、アップストリーム データを伝送できる PON レシーバ ドメイン（PRD）は常に 1 つに限られます。これは、PRD の ONT からのレーザを 2 つ同時に使用すると光ビート干渉（OBI）が発生するためです。さらに、アップストリーム信号伝送に周波数変調（FM）を使用する場合、PON内の複数の ONT が同時に伝送すると PHY エラーが発生します。

D-PON 環境内の DOCSIS 3.0 CM がアップストリーム チャネルで初期レンジングに失敗しないように、すべてのアップストリーム チャネルで初期メンテナンス領域がスケジュールされます。D-PON 用に設定された MAC ドメイン内でレンジング要求を受信するとき、CM は D-PON リファレンス チャネル（US0）に対するアップストリーム チャネル オーバーライドを受け取ります。

D PON のこの実装では、アップストリーム周波数とは関係なく、アップストリームデータを伝送するためのタイムスロットが PRD 内の DOCSIS デバイスに与えられます。したがって、アップストリーム チャネル ボンディング機能を使用せずに MAC ドメイン内で複数のアップストリームを使用する利点はありません。

D-PON 機能は、次のサービス タイプをサポートします。

- 最大 4 つの周波数を同時使用するベストエフォート（BE）3.0
- 単一周波数のみを使用する BE 2.0
- 単一周波数のみを使用する非送信請求許可サービス（UGS）
- 単一周波数のみを使用するリアルタイム ポーリング サービス（RTPS）
- 単一周波数のみを使用する非リアルタイム ポーリング サービス（nRTPS）

D-PON のアップストリーム ボンディング サポートの設定方法

ここでは、Cisco cBR ルータ上で MAC ドメインの D-PON を有効にする方法を説明します。（デフォルトでアップストリーム チャネル 0 に設定される）リファレンス チャネルがボンディング グループに含まれる必要があります。

（注） USCB では、次の組み合わせで、RFOG MAC ドメイン内の US チャネルを最大 4 個サポートできます。

- US0
- US0、US1
- US0、US1、US2
- US0、US1、US2、US3

すべての US チャネルに、同じ数のミニスロット、チャネル幅（3.2 MHz または 6.4 MHz のみサポート）、DOCSIS モード（ATDMA のみサポート）、および変調プロファイルが設定されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**interface cable** *slot/subslot/cable-interface-index* 例： `Router(config)# interface cable 8/0/0`	指定したケーブル インターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**cableupstreamdpon** 例： `Router(config-if)# cable upstream dpon`	MAC ドメインに関する D-PON を有効にします。
ステップ 5	**shutdown** 例： `Router(config-if)# shutdown`	インターフェイスをシャットダウンします。
ステップ 6	**noshutdown** 例： `Router(config-if)# no shutdown`	インターフェイスをイネーブルにします。
ステップ 7	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

DOCSIS 3.0 ケーブル モデムのアップストリーム ボンディングが部分的ボンディング状態になる

スイッチオーバー後に元の CLC に復帰する間、アップストリーム ボンディングが部分的ボンディング状態になることがあります。

次の例では、スロット 1 と 0 の CLC 間でスイッチオーバーが行われます。スロット 1 の CLC に復帰すると、C1/0/3/UB が C1/0/3/p になります。次の出力では、この変化を強調表示しています。

```
Router# show cable modem
Load for five secs: 1%/0%; one minute: 2%; five minutes: 2% Time source is NTP, 13:00:25.570
 UTC Thu Feb 18 2016

                                                                                  D
MAC Address    IP Address      I/F           MAC               Prim  RxPwr  Timing Num I
                                             State             Sid   (dBmv) Offset CPE P
4844.8789.e0fc 10.78.100.6     C1/0/0/UB     w-online          6     -0.50  1787   0   N
c8fb.2639.33d0 10.78.100.7     C1/0/1/UB     w-online          1     -1.00  1793   0   N
4844.8789.e10e 10.78.100.10    C1/0/2/UB     w-online          1     -0.50  1784   0   N
602a.d0a2.9b3e 10.78.100.11    C1/0/3/p      w-online          4      1.50   1789   0   N
0025.2ecf.f922 10.78.100.8     C1/0/4/UB     w-online          1     -1.00  1788   0   N
```

この部分的ボンディングを回復させるには、コントローラで関連するアップストリーム ポートに対して **shutdown** コマンドと **no shutdown** コマンドを使用します。以下に設定例を示します。

```
Router(config)# controller Upstream-Cable 1/0/3
```

```
Router(config-controller)# us-channel 0 shutdown
Router(config-controller)# no us-channel 0 shutdown
```

D-PON のアップストリーム ボンディング サポートの確認

D-PON を使って設定された MAC ドメインのアップストリーム スケジューラ出力を確認するには、**showinterfacecablemac-scheduler** コマンドを使用します。

（注） D-PON リファレンス チャネル US0（US channel-id 1）MAP は、MAC ドメイン内の他の MAP を生成するためのテンプレートとして機能します。したがって、アップストリーム スケジューリングに関する統計情報の一部は、D-PON リファレンス チャネルを除く他のチャネルには該当しません。

```
Router# show interface cable 8/0/0 mac-scheduler 1
     DOCSIS 1.1 MAC scheduler for Cable8/0/0/U1 : rate 30720000
     wfq:None
     us_balance:OFF
     dpon_mode:ON
     fairness:OFF
     Queue[Rng Polls] flows 0
     Queue[CIR Grants] flows 0
     Queue[BE(07) Grants] flows 0
     Queue[BE(06) Grants] flows 0
     Queue[BE(05) Grants] flows 0
     Queue[BE(04) Grants] flows 0
     Queue[BE(03) Grants] flows 0
     Queue[BE(02) Grants] flows 0
     Queue[BE(01) Grants] flows 0
     Queue[BE(00) Grants] flows 0
     Req Slots 1824595508, Req/Data Slots 10640906
     Init Mtn Slots 89924653, Stn Mtn Slots 989543
     Short Grant Slots 0, Long Grant Slots 0
     Adv Phy Short Grant Slots 538, Adv Phy Long Grant Slots 219831
     Adv Phy UGS Grant Slots 0
     Avg upstream channel utilization : 0%
     Avg percent contention slots : 98%
     Avg percent initial ranging slots : 1%
     Avg percent minislots lost on late MAPs : 0%
     MAP TSS: lch_state 9, init_retries 0
     late_initial_maps 0, late_ucd_maps 0
     mac-phy tss errors 0, missed ccc 0
```

その他の参考資料

ここでは、D-PON 機能のアップストリーム ボンディング サポートに関する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
Prisma D-PON	『Cisco Prisma D-PON』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

D-PON のアップストリーム ボンディング サポートに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *76*：*D-PON* のアップストリーム ボンディング サポートに関する機能情報

機能名	リリース	機能情報
D-PON のアップストリーム ボンディング サポート	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 26 章

エネルギー管理モード

Data-over-Cable Service Interface Specifications（DOCSIS）ケーブル モデム（CM）および CMTS は、エネルギー管理 1x1 (EM) モードと呼ばれる省電力モードをサポートしています。アイドル時のユーザのデータ レート需要が、単一の割り当て済みアップストリーム/ダウンストリーム チャネル ペアで使用可能な容量に収まる場合、CM はエネルギー管理 1x1 (EM) モードに切り替わります。単一のチャネル ペアで確実に提供できるよりも多いデータ レートを CM が必要とする場合、CMTS は、より大きな送受信チャネル セットに戻るよう CM に指示します。

目次

エネルギー管理モードについて

エネルギー管理モードの詳細については、次の各項で説明します。

動的ダウンストリーム ボンディング グループ

エネルギー管理 1x1（EM）モード機能をサポートするために、CMTS は CM 用のアップストリームおよびダウンストリーム チャネル ペアを選択します。CM に割り当てられるアップストリーム チャネルとダウンストリーム チャネルが使用可能でなければなりません。使用可能でないチャネルを CMTS が選択すると、ダウンストリーム ボンディング チャネルに障害が発生する可能性があります。

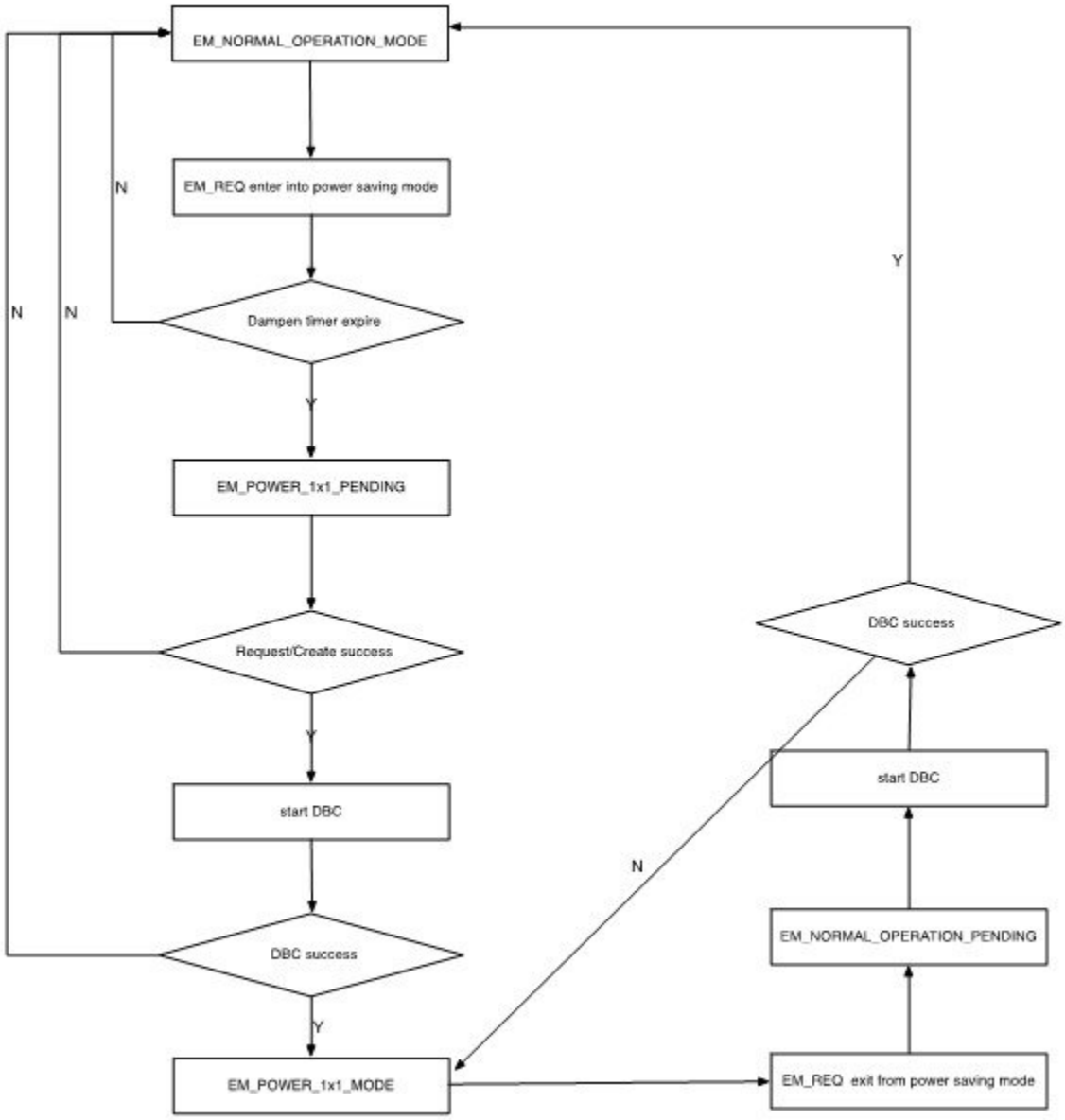
プロセスを簡素化するために、CMTS は次の規則に従って CM 用の 1 X 1 ボンディング グループを選択します。

- アップストリームの場合、CM で現在使用されているアップストリーム チャネルの中から、実帯域幅が最も利用しやすいチャネルを選択します。
- ダウンストリームの場合、CMTS は、CM で使用されている現在のプライマリ ダウンストリーム チャネルを選択します。
- チャネル ボンディング 1xN または Nx1 を使ってオンラインになっている CM が EM モードの開始を要求した場合、元のチャネル ボンディングが 1 で、Quality of Service（QoS）パラメータが更新されなければ、CMTS はアップストリーム チャネルとダウンストリーム チャネルを変更しません。
- CMTS は既存の動的ボンディング グループ（DBG）をすべて調べて、ターゲット チャネルでの完全一致を探します。
  - 見つかった場合、CMTS はこのボンディング グループを使用して、EM モードを開始するよう CM に指示します。
  - 利用可能な DBG がなく、未使用の DBG がある場合、CMTS はその未使用 DBG にプライマリ チャネルを追加して、EM モードを開始するよう CM に指示します。
  - 利用可能な DBG も未使用 DBG もない場合、CMTS は、新しい DGB を設定する必要があることを通知する警告をログに記録します。

CM 電源状態のフロー チャート

次の図に、CM 電源状態のフロー チャートを示します。

図 *20*：ケーブル モデムの電源状態のフロー チャート



バッテリ モードとの相互作用

エネルギー管理モードとバッテリ モードはどちらも、電力を節約するために 1x1 モードに入ります。ただし、これらのモードが 1x1 モードに入る目的は互いに異なるので、両者の動作にはいく

つかの違いがあります。エネルギー管理（EM）モードの目的はトラフィックが少ないときに電力を節約することであり、通常のサービスに与える影響は最小限です。バッテリ モードの目的は音声サービス（特に緊急通報サービス）を保証することであり、そのために必要に応じて他のサービスをドロップすることがあります。

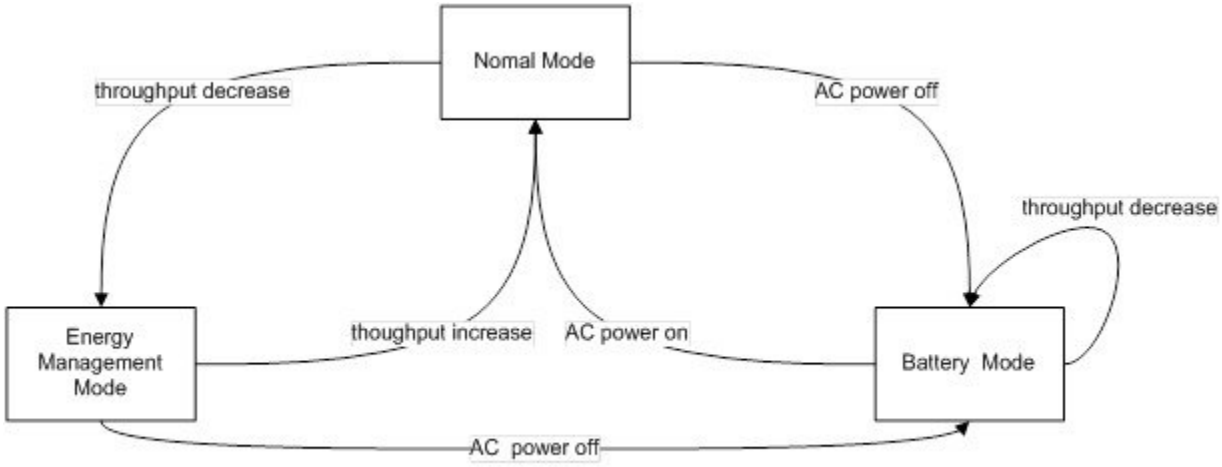
次の表に、エネルギー管理モードとバッテリ モードの動作の違いをまとめます。

	エネルギー管理（EM）モード	バッテリ モード（BM）
QoS	200k までの最小予約レート サービス。	最小予約レートなし。
マルチキャスト	• IGMP 要求が保証されます。 • CM が Internet Group Management Protocol（IGMP）グループに参加している場合、CMTS は EM モード開始要求を拒否し、CM を IGMP グループ内に保持します。 • CM が EM モードになっているときに IGMP 参加要求を受信した場合、CMTS は EM モードを終了するよう CM に指示します。	• CM が IGMP グループに参加しているときにコード 9 の CM-STATUS イベントを CMTS が受信した場合、CMTS は CM を IGMP グループから脱退させます。 • CM が BM の場合、CMTS は CM からの IGMP 参加要求を拒否します。

BM には EM モードより高い優先度が与えられます。CM がすでに EM モードになっているときに電源オフが発生すると、CM は BM になります。電源が復元されると CM は通常モードに戻り、トラフィックがしきい値を下回っていれば、再び EM モードに入ります。CM が BM から EM モードに直接切り替わることはありません。

次の図に、バッテリ モードとエネルギー管理モードの間の相互作用を示します。

図 *21*：*BM* および *EM* モードの相互作用



1. CM が通常モードのときに CMTS が EM モード開始要求を受信すると、CMTS は、ダウンストリーム ボンディング チャネル（DBC）で EM モードに入るよう CM に指示します。
2. CM が EM モードのときに CMTS が EM モード終了要求を受信すると、CMTS は、DBC で EM モードを終了して通常モードに入るよう CM に指示します。
3. CM が通常モードのときに、「CM がバッテリ バックアップで動作している」というメッセージを CMTS が受信した場合、CMTS は、DBC で EM モードに入るよう CM に指示します。
4. CM が BM モードのときに、「CM が AC 電源で動作している」というメッセージを CMTS が受信した場合、CMTS は、DBC で BM モードを終了して通常モードに入るよう CM に指示します。
5. CM が EM モードのときに、「CM がバッテリ バックアップで動作している」というメッセージを CMTS が受信した場合、CMTS は、サービス フロー再管理で BM モードに入るよう CM に指示します。
6. CM が BM モードのときに CMTS が EM モード開始要求を受信すると、CMTS は「CM が AC 電源で動作している」というメッセージを受信するまで待機します。これを受信した後、通常モードに戻るよう CM に指示します。

エネルギー管理要求の負荷の処理

勤務時間の始まりや終わりに多数の CM が同時に EM 要求を送信すると、非常に短時間にトラフィックが急激に増加または減少して、CMTS に大きな負荷がかかります。このような CMTS の負荷急増を回避するために、スロットル メカニズムが導入されています。

ライン カード EM プロセスでは、プロセスで現在処理中のトランザクションを示す変数が定義されます。エネルギー管理要求の受信時にトランザクションの最大数に達していなければ、CMTS はこの要求を処理し、現在のトランザクション数のカウンタを更新します。トランザクションの

最大数に達した場合は、CMTS は一時的な拒否応答を送信します。トランザクションが完了した後、または CM がオフラインになると、現在のトランザクション数のカウンタが更新されます。

スーパーバイザ ハイ アベイラビリティとライン カード スイッチオーバー

エネルギー管理機能は、制限付きでスーパーバイザ ハイ アベイラビリティとライン カード スイッチオーバーをサポートします。

アクティブなスーパーバイザまたはライン カードは、CM が安定した EM 状態になると、CM の EM モード データをスタンバイ SUP または保護ライン カードに同期します。DBS プロセスの続行中に CM が EM モードを開始または終了すると、スーパーバイザ ハイ アベイラビリティまたはライン カード スイッチオーバーによって CM がオフラインまたはオンライン ステータスになります。

エネルギー管理モードに関する前提条件

エネルギー管理モードを有効にするには、復元力ボンディング グループ（RBG）と動的ボンディング グループを設定する必要があります。

エネルギー管理モードの制限事項

CMTS ハイ アベイラビリティの制約事項

- 利用可能な DBG がない場合、CMTS は保護ライン カード上で新しい DBG を作成できず、CM は EM モードを開始できません。
- CM が通常モードから EM モードに移る時点、または EM モードから通常モードに戻る時点でのライン カードのスイッチオーバーはサポートされていません。
- EM モードの動作を削減するために、EM ステータスに関する情報は保護ライン カードに同期されません。そのため、ライン カード ハイ アベイラビリティの適用後に EM ステータスがクリアされます。

動的ボンディング グループの制限事項

EM 機能をサポートするために、CMTS は各 MAC ドメイン内のプライマリ チャネルごとに個別の DBG を設定します。たとえば、MAC ドメインに 8 つのプライマリ チャネルがある場合、この MAC ドメイン用に 8 つの DBG が作成されます。これにより、DBG 不足により EM が失敗することがなくなります。

CMTS と他の機能の相互作用に関する制限事項

以降の項で、CMTS と他の機能の相互作用に関する制限事項について説明します。

音声

音声コールが進行中の場合、CMTS は EM モードを開始するよう CM に指示しません。

EM モードの CM が音声コールを受信すると、動的な非送信請求許可サービス（UGS）サービス フローまたはアクティビティ検出による UGS（UGS-AD）サービス フローを追加します。音声コールが進行している間は、トラフィックのフローとは無関係に、CM は EM モードを終了しません。音声サービスが最優先されます。

動的ボンディング変更と動的チャネル変更、および関連するアプリケーション

D2.0 および D3.0 のロード バランシング（静的および動的）では、EM モードの CM がロード バランシングによって移動されることはありません。

RF 適応では、EM モードの CM が RF 適応によって代替論理チャネルに再配置されることはありません。

マルチキャスト

- CM がマルチキャスト グループに参加している場合、CMTS は、ボンディング マルチキャストと非ボンディング マルチキャストのどちらの場合も EM 要求を拒否します。
- CM が EM 状態のときにマルチキャスト参加要求を受信すると、CMTS はこの参加要求を破棄し、CM の EM モードを強制終了させます。
- CM が EM 状態で音声コールが進行中のときに新しいマルチキャスト参加要求を受信した場合、CMTS はこの参加要求を破棄しますが、音声コールが進行中であるため、CM の EM モードを強制終了させません。
- 現在処理中のトランザクション数に関するしきい値が存在します。マルチキャスト参加が要求されたときに、最大トランザクション数のしきい値にすでに達している場合、CMTS は EM モードを終了するよう CM に指示できません。また、CM が EM モードを終了できるようになるまで、マルチキャスト参加は拒否されます。
- EM モードの CM が PacketCable Multimedia（PCMM）マルチキャストに参加する必要がある場合、ゲートを正常にセットアップするには GateSet 要求を 2 回送信する必要があります。最初の GateSet 要求では単にモデムの EM モードが強制終了するだけで、ゲートのセットアップは行われません。

認定情報レート

最小予約レート サービス フローの QoS パラメータで 200 Kbps を超える QoS が定義されている場合、CM が EM モードになると、CMTS は最小予約レートとして 200 Kbps だけを割り当てます。最小予約レートが 200 Kbps 未満の場合、CM が EM モードになると、CMTS はサービス フロー設定に応じて最小予約レートをスケジュールします。

CM が EM モードになった時点で、CMTS は最小予約レートサービス フロー QoS パラメータを記録します。CM が EM モードを終了すると、CMTS は元のパラメータを使用します。

CM は EM モードに入るときに CM アップストリーム チャネルの 1 つを選択します。サービス フローが完全にそのアップストリーム チャネル上に収まっている限り、サービス フロー パラメータは変更されません。このように動作する理由は、サービス フローが DBC 操作に移されず、サービス フロー パラメータを変更する利点がないためです。

アドミッション コントロール

EM モードの終了要求を受信した際に、アドミッション コントロールの失敗により元のワイドバンド インターフェイスへのリカバリが制限されている場合、CMTS は CM が EM モードのままにならないよう、強制的に CM をオフラインにして再登録します。この場合、CMTS は警告メッセージをログに記録します。

バッテリ モード

バッテリ電源で動作する CM ステータスを CMTS が受信すると、CMTS は BM を開始するよう CM に指示します。受信した指示を CM が拒否した場合、CMTS はモデムを通常のステータスに維持します。

CM が BM のときに、A/C 電源で動作する CM ステータスを CMTS が受信すると、CMTS は BM を終了するよう CM に指示します。受信した指示を CM が拒否した場合、CMTS は、CM がバッテリ モードのままにならないよう CM を強制的にオフラインにします。この場合、CMTS は警告メッセージをログに記録します。

属性マスク

エネルギー管理モード用のアップストリームまたはダウンストリームのチャネル ペアを選択する際に、CMTS は、対応する CM の既存のサービス フローに関する属性マスクの要件を満たすチャネルを選択します。

場合によっては、エネルギー管理モードの処理用にアップストリームおよびダウンストリーム チャネルペアを選択する際に、サービス フロー属性に基づく割り当てを順守できないことがあります。この競合を解決する目的で、CMTS は次の方法のいずれか、または両方をサポートします。

1. CMTS は、必須の属性マスクや禁止された属性マスクに厳密に従うという要件を課すことができ、MD-CM-SG 内の個々の使用可能なチャネルがこれらのマスクを満たさない場合には、EM モードの開始を拒否できます。
2. 属性マスクのすべての条件が満たされなくても、CMTS は CM が EM モードに入ることを許可できます。この場合、CMTS は、属性マスクが保持されていないことを通知する警告イベントをログに記録します。

次の場合、CMTS は 2 番目の方法をサポートします。

EM モードに入るよう CM が指示されたとき、選択されたターゲット アップストリームおよびダウンストリーム チャネルがサービス フロー属性マスクに従っていない。この競合では、CMTS は EM モードを開始するようモデムに指示します。また、CMTS はこの競合を通知するために警告メッセージをログに記録します。

動的なサービス追加

CM が EM モードになっている場合、要求された属性が単一のチャネルに適合しないとしても、DSA 要求をセットアップできます。音声サービスに影響を与えないよう、CM の EM モードは強制的に終了されません。

設定変更およびインターフェイス シャットダウンの制限事項

1. **アップストリーム チャネルのシャットダウン**：アップストリーム チャネルのシャットダウンにより、MD-US-SG-ID が再計算されて新しい MD-US-SG-ID が割り当てられます。この場合、CM はオフラインにならず、CM インスタンスの内部データ構造は更新されません。DBC 運用では MD-US-SG-ID が検査されるため、CM が EM モードに入ると、CM 上の MD-US-SD-ID と新しい MD-US-SG-ID との間で不一致が生じます。したがって、DBC は失敗し、CM は EM モードを開始できません。
2. **アップストリーム サービス グループに変更を加えると、EM モードの CM がオフラインになる**：US-SG 設定が変更されると、DBC の動作がブロックされて、CM が EM モードのままになります。このシナリオを回避するために、（アップストリームチャネルのシャットダウンまたは非シャットダウンなどの）変更がアップストリーム サービス グループ（US-SG）で生じると、CMTS は CM をオフラインにします。この場合、複数のチャネルを含むワイドバンドチャネル ボンディングを使用する通常の CM として CM が再登録されます。
3. **元のワイドバンド インターフェイスの変更**：CM が EM モードになっているときに、CM 上の元のワイドバンド インターフェイス チャネルが変更されると、CM がオフラインになり、通常の CM として再登録されます。
4. **機能の無効化または有効化**：この機能を無効にしても、CM が要求を送信しない限り、CMTS は強制的に CM の EM モードを終了させません。CLI から EM 機能が無効にされた後、CMTS は EM 要求を受け入れません。

エネルギー管理モードの設定方法

ここでは、Cisco cBR-8 上にエネルギー管理機能を設定する方法を説明します。

目次

エネルギー管理モードの有効化

エネルギー管理モードを有効にするには、次の手順に従います。

configure terminal
cable reduction-mode energy-management enable

エネルギー管理モードの確認

- CM が EM モードになっているかどうかを確認するには、**show cable modem** コマンドを使用します。ケーブル モデムがエネルギー管理モードで動作している場合、MAC 状態は「em」フラグ付きで表示されます。

  show cable modem

```
                                                                  D
MAC Address    IP Address      I/F                MAC               Prim  RxPwr
  Timing Num   I
                                                                       State
          Sid   (dBmv) Offset  CPE    P
7cb2.1b0f.ea72 40.4.58.4       C7/0/0/UB     w-online(em)              2      0.00
     1231     1         Y
54d4.6ffb.2f6b 40.4.58.24      C7/0/0/UB     w-online                  3     -0.50
    1241     0         Y
0025.2ed9.9a22 40.4.58.3       C7/0/0/UB     w-online                  4      0.50
    1240     0         Y
```

- どの CM が EM モードになっているかを確認し、元のワイドバンドおよびアップストリーム チャネルの情報を取得するには、**show cable modem reduction-mode energy-management-mode** コマンドを使用します。

  show cable modem reduction-mode energy-management-mode

```
                                Orig BG     Orig US                    Curr BG
I/F     MAC Address    ID        I/F        bitmap   RFs     ID          I/F
Upstream
------- -------------- ---------------- --------
-----------------------------------------
C7/0/0  0025.2eaf.843e 897  Wi7/0/0:0     0x3B     4      252         Wi7/0/0:1
US0
C7/0/0  0025.2eaf.8356 897  Wi7/0/0:0     0x3B     4      252         Wi7/0/0:1
US0
C7/0/0  0015.d176.5199 897  Wi7/0/0:0     0x3B     4      252         Wi7/0/0:1
US0
```

MAC ドメインごとのエネルギー管理モードの有効化

CMTS は、EM 機能がグローバルに有効にされる場合も、MAC ドメインごとに有効にされる場合も、これをサポートします。MAC ドメインごとにエネルギー管理機能を有効にするには、次の手順に従います。

MAC ドメインごとに EM モードを有効にするには、次の手順に従います。

configure terminal
interface cable *slot/subslot/cable-interface-index*

cable reduction-mode energy-management enable

動的ボンディング チャネルでの初期レンジング手法の設定

初期レンジング手法のデフォルト値は 1 に設定され、有効な値の範囲は 1 ～ 4 です。

初期レンジングの手法を設定するには、次の手順に従います。

configure terminal
cable reduction-mode energy-management ranging-init-technique*value*

動的チャネル帯域幅のパーセンテージの設定

新しく作成された DBG に参加する際にプライマリ チャネルが動的チャネル帯域幅を割り当てることができるよう、プライマリ チャネル用に十分な帯域幅を残してください。デフォルトのパーセンテージ値は 5 に設定されます。有効な範囲は 1 ～ 96 です。

動的チャネル帯域幅のパーセンテージを設定するには、次の手順に従います。

configure terminal
cable reduction-mode energy-management dynamic-channel-percent *value*

エネルギー管理のキュー サイズの設定

キュー サイズのデフォルト値は 150 で、有効範囲は 50 ～ 10000 です。

エネルギー管理要求のキュー サイズを設定するには、次の手順に従います。

configure terminal
cable reduction-mode energy-management process-queue-size `value`
-

エネルギー管理モードの確認

ここでは、EM モードを確認する方法について説明します。

目次

エネルギー管理受信要求に関する基本的な統計情報の表示

特定の CM のすべてのエネルギー管理受信要求イベントに関する基本的な統計情報を表示するには、**show cable modem <cable if | mac_addr | ip_addr> reduction-mode energy-management-status** コマンドを使用します。

show cable modem c8/0/0 reduction-mode energy-management-status

```
I/F    MAC Address    Event          TID Count Error Dups   Time
C8/0/0 54d4.6ffb.2e21 Enter EM mode   1   1     0     1    Jul 16 21:38:18
                      Exit EM mode    1   1     0     0    Jul 16 21:38:39
C8/0/0 602a.d07c.4ec6 Enter EM mode   1   1     0     0    Jul 16 21:40:57
                      Exit EM mode    1   1     0     0    Jul 16 21:41:17
```

指定した CM のすべての EM_REQ イベントに関する基本的な受信統計情報をクリアするには、**clear cable modem <cable if | mac_addr | ip_addr> em-status** コマンドを使用します。

設定パラメータの確認

CM コンフィギュレーション ファイルで使われる設定パラメーターを確認するには、**show cable modem <mac address> reduction-mode energy-management-param** コマンドを使用します。

show cable modem 54d4.6ffb.2e21 reduction-mode energy-management-param

```
Energy Management feature enable : Y
DS entry bitrate threshold(bps)  : 100000
DS entry time threshold(s)       : 120
DS exit bitrate threshold(bps)   : 200000
DS exit time threshold(s)        : 2
US entry bitrate threshold(bps)  : 100000
US entry time threshold(s)       : 120
US exit bitrate threshold(bps)   : 200000
US exit time threshold(s)        : 2
cycle period(s)                  : 300
```

ケーブル モデムに関する情報の表示

CM に関するすべての情報を表示するには、**show cable modem** *mac address* **verbose** コマンドを使用します。

show cable modem *54d4.6ffb.30fd* **verbose**

```
MAC Address                          : 54d4.6ffb.30fd
IP Address                           : 40.4.58.14
IPv6 Address                         : 2001:40:4:58:741A:408D:7E4B:D7C8
Dual IP                              : Y
Prim Sid                             : 9
Host Interface                       : C7/0/0/UB
MD-DS-SG / MD-US-SG                  : 1 / 1
MD-CM-SG                             : 0x3C0101
Primary Wideband Channel ID          : 897 (Wi7/0/0:0)
Primary Downstream                   : In7/0/0:2 (RfId : 722)
Wideband Capable                     : Y
RCP Index                            : 3
RCP ID                               : 00 10 00 00 08
Downstream Channel DCID RF Channel : 99    7/0/0:2
Downstream Channel DCID RF Channel : 97    7/0/0:0
Downstream Channel DCID RF Channel : 98    7/0/0:1
Downstream Channel DCID RF Channel : 100   7/0/0:3
Multi-Transmit Channel Mode          : Y
Extended Upstream Transmit Power     : 0dB
Upstream Channel                     : US0        US1
Ranging Status                       : sta        sta
Upstream SNR (dB)                    : 36.12      32.55
Upstream Data SNR (dB)               : --         --
Received Power (dBmV)                : 0.00       0.00
Reported Transmit Power (dBmV)       : 25.25      26.00
Peak Transmit Power (dBmV)           : 54.00      54.00
Phy Max Power (dBmV)                 : 54.00      54.00
Minimum Transmit Power (dBmV)        : 24.00      24.00
Timing Offset              (97.6 ns): 1226       1226
Initial Timing Offset                : 1229       973
Rng Timing Adj Moving Avg(0.381 ns): -1         0
Rng Timing Adj Lt Moving Avg         : -7         0
Rng Timing Adj Minimum               : -768       0
Rng Timing Adj Maximum               : 0          64768
Pre-EQ Good                          : 0          0
Pre-EQ Scaled                        : 0          0
Pre-EQ Impulse                       : 0          0
Pre-EQ Direct Loads                  : 0          0
Good Codewords rx                    : 515        472
Corrected Codewords rx               : 0          0
Uncorrectable Codewords rx           : 0          0
Phy Operating Mode                   : atdma*     atdma*
sysDescr                             :
Downstream Power                     : 0.00 dBmV (SNR = ----- dB)
MAC Version                          : DOC3.0
QoS Provisioned Mode                 : DOC1.1
Enable DOCSIS2.0 Mode                : Y
Modem Status                         : {Modem= w-online(em), Security=disabled}
Capabilities                         : {Frag=N, Concat=N, PHS=Y}
Security Capabilities                : {Priv=, EAE=Y, Key_len=}
```

```
L2VPN Capabilities                  : {L2VPN=N, eSAFE=N}
Sid/Said Limit                      : {Max US Sids=16, Max DS Saids=15}
Optional Filtering Support          : {802.1P=N, 802.1Q=N, DUT=N}
Transmit Equalizer Support          : {Taps/Symbol= 1, Num of Taps= 24}
Number of CPE IPs                   : 0(Max CPE IPs = 16)
CFG Max-CPE                         : 200
Flaps                               : 0()
Errors                              : 0 CRCs, 0 HCSes
Stn Mtn Failures                    : 0 aborts, 0 exhausted
Total US Flows                      : 1(1 active)
Total DS Flows                      : 1(1 active)
Total US Data                       : 7 packets, 2006 bytes
Total US Throughput                 : 0 bits/sec, 0 packets/sec
Total DS Data                       : 5 packets, 1202 bytes
Total DS Throughput                 : 0 bits/sec, 0 packets/sec
LB group ID assigned (index)        : 2151416065 (48131)
LB group ID in config file (index) : N/A (N/A)
LB policy ID                        : 0
LB policy ID in config file         : 0
LB priority                         : 0
Tag                                 :
Required DS Attribute Mask          : 0x0
Forbidden DS Attribute Mask         : 0x0
Required US Attribute Mask          : 0x0
Forbidden US Attribute Mask         : 0x0
Service Type ID                     :
Service Type ID in config file      :
Active Classifiers                  : 2 (Max = NO LIMIT)
CM Upstream Filter Group            : 0
CM Downstream Filter Group          : 0
CPE Upstream Filter Group           : 0
CPE Downstream Filter Group         : 0
DSA/DSX messages                    : permit all
Voice Enabled                       : NO
DS Change Times                     : 0
Boolean Services                    : 2
CM Energy Management Capable        : Y
CM Enable Energy Management         : Y
CM Enter Energy Management          : YES
Number of Multicast DSIDs Support   : 16
MDF Capability Mode                 : 2
IGMP/MLD Version                    : MLDv2
FCType10 Forwarding Support         : Y
Features Bitmask                    : 0x0
Total Time Online                   : 2h12m    (2h12m     since last counter reset)
CM Initialization Reason            : NO_PRIM_SF_USCHAN
CFG Max IPv6 CPE Prefix             : 16 (-1 used)
```

エネルギー管理モードに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *77* : バッテリ バックアップ モードでのチャネル ボンディングのダウングレードに関する機能情報

機能名	リリース	機能情報
エネルギー管理モード	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 IV 部

レイヤ 2 および DOCSIS 3.1 構成

第 27 章

DOCSIS 3.1 OFDM チャネルの設定

このドキュメントでは、Cisco cBR シリーズ コンバージド ブロードバンド ルータ上で OFDM チャネルを設定する方法について説明します。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *78*：***Cisco cBR*** シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

OFDM チャネルの設定について

OFDM チャネル

DOCSIS 3.1 は、スループットおよびスペクトル効率を高めるためのモードを導入する一方で、DOCSIS 3.0 との後方互換性も維持しています。OFDM チャネル サポートでは、チャネル帯域幅 24 Mhz ～ 192 MHz で、ポートごとに 1 つの OFDM チャネルが含まれます。

各 OFDM チャネルは 1 つの制御プロファイル、1 つの NCP プロファイル、および最大 5 つのデータ プロファイルをサポートします。プロファイルは 1 つ以上の変調をサポートします。

Cisco IOS-XE リリース 3.18.1SP 以降、コマンド **guardband-override** を使用して ODFM チャネルのガードバンドを設定することにより、ある程度のパフォーマンスマージンを潜在的に相殺でき

ます。デフォルトで、Cisco cBR-8 ルータは、OFDM チャネル プロファイル内のロールオフと間隔に基づくデフォルト ガード バンドを使用します。

また、DOCSIS 3.1 OFDM サポートにより、ユーザは MAC ドメインで RF チャネル 158 ～ 162 をプライマリ チャネルとして設定することもできます。

（注） OFDM チャネルは、ワイドバンド グループに含まれるセカンダリ チャネルとしてのみ使用可能です。プライマリ チャネルは通常の DOCSIS 3.0 プライマリ RF チャネルとして設定される必要があります。

チャネル プロファイル

グローバルに設定される OFDM チャネル プロファイルには、チャネルのパラメータと、コントロール、NCP、およびデータ プロファイルに関連付けられる変調または変調プロファイルが格納されます。

各 OFDM チャネルの設定で、OFDM チャネル プロファイルを指定する必要があります。

変調プロファイル

グローバルに設定される OFDM 変調プロファイルは、さまざまなサブキャリア範囲または個別のサブキャリアのリストに対して異なる変調を割り当てます。

チャネルプロファイル内で、コントロール、NCP、またはデータ プロファイルに変調プロファイルを割り当てることができます。

OFDM チャネル除外バンド

ポート上のすべての OFDM チャネルから特定の周波数の範囲を除外するには、**ofdm-freq-excl-band** コマンドを使用します。

OFDM チャネルの設定方法

OFDM 変調プロファイルの設定

OFDM 変調プロファイルを設定するには、次の手順に従います。

enable
configure terminal
cable downstream ofdm-modulation-profile *id*
description *text*
subcarrier-spacing *value*
width *value*
start-frequency *value*

assign {**modulation-default** *mod_prof_id* | **modulation** *mod_prof_id* {**list-subcarriers** {**freq-abs** | **freq-offset**} *value* | **range-subcarriers** {**freq-abs** | **freq-offset**} *value* **width** *value*}}

（注） サブキャリアの間隔は、それが設定されている各チャネル プロファイルのサブキャリア間隔と一致する必要があります。

OFDM 変調プロファイル設定の確認

OFDM 変調プロファイルの設定を表示するには、次の例に示すように **show cable ofdm-modulation-profiles** コマンドを使用します。

```
Router# show cable ofdm-modulation-profile 10

**** OFDM Modulation Profile Configuration ****

Prof  FFT  Width     Start-freq Modulations
ID    KHz  Hz        Hz
10    50   96000000  627000000  64   default
                                512  freq-abs  709050000 width   12000000
                                2048 freq-abs  629000000 width    6000000

Profile Subcarrier Modulations
  Modulation: Start-freq-abs[start-sc] - End-freq-abs[end-sc] Width-freq[num-sc]
  64  : 572600000[   0] -  626950000[1087]    54400000[1088]
  64  : 627000000[1088] -  628950000[1127]     2000000[  40]
  2048: 629000000[1128] -  634950000[1247]     6000000[ 120]
  64  : 635000000[1248] -  709000000[2728]    74050000[1481]
  512 : 709050000[2729] -  721000000[2968]    12000000[ 240]
  64  : 721050000[2969] -  722950000[3007]     1950000[  39]
  64  : 723000000[3008] -  777350000[4095]    54400000[1088]

**** OFDM Modulation Profile Assigned Channel Profiles ****

Prof  Channel
ID    Profiles
10    30
```

OFDM 変調プロファイルと OFDM チャネル プロファイルの関連付けを表示するには、次の例に示すように **channel-profiles** オプションを指定した **show cable ofdm-modulation-profile** コマンドを使用します。

```
Router# show cable ofdm-modulation-profile channel-profiles

**** OFDM Modulation Profile Assigned Channel Profiles ****

Prof  Channel
ID    Profiles
8     None
9     28
10    30
192   192
```

OFDM 変調プロファイルの設定を表示するには、次の例のように **configuration** オプションを指定した **show cable ofdm-modulation-profile** コマンドを使用します。

```
Router# show cable ofdm-modulation-profile configuration

**** OFDM Modulation Profile Configuration ****

Prof  FFT  Width     Start-freq Modulations              Description
ID    KHz  Hz        Hz                                  (Limited to 20)
8     50   192000000 NA         2048 default
```

```
                                        512  freq-off   48000000
                                             width      24000000
9      50   96000000   627000000       512  default              512-1k-4k
                                        1024 freq-abs  635000000
                                             width      74050000
                                        4096 freq-abs  629000000
                                             width       6000000
10     50   96000000   627000000       64   default
                                        512  freq-abs  709050000
                                             width      12000000
                                        2048 freq-abs  629000000
                                             width       6000000
```

OFDM チャネル プロファイルの設定

OFDM チャネル プロファイルを設定するには、次の手順に従います。

enable
configure terminal
cable downstream ofdm-chan-profile *id*
description *text*
cyclic-prefix *value*
guardband-override *value*
interleaver-depth *value*
pilot-scaling *value*
roll-off *value*
subcarrier-spacing *value*
profile-ncp modulation-default *mod_prof_id*
profile-control {**modulation-default** *mod_prof_id* | **modulation-profile** *mod_prof_id*}
profile-data *channel_data_prof_id* {**modulation-default** *mod_prof_id* | **modulation-profile** *mod_prof_id*}

OFDM チャネル プロファイル設定の確認

OFDM チャネル プロファイルの詳細を表示するには、次の例に示すように **show cable ofdm-chan-profiles** コマンドを使用します。

```
Router# show cable ofdm-chan-profile 21
**** OFDM Channel Profile Configuration ****

Prof  Cycl  Roll  Guardband  FFT  Intr   Pilot  Modulation (D-Default, P-Profile)

ID    Prfx  Off   Override   KHz  Depth  Scale  Cntrl   NCP     Data Profiles (count = 0)
                                                             1       2       3       4
      5
21    1024  128   2400000    50   16     48     D:1024  D:16    NA      NA      NA      NA
      NA

**** OFDM Channel Profile Assigned Channels ****

Prof  Admin  Controller:channels
ID
21    Up     6/0/4:158
```

OFDM チャネル プロファイルと OFDM チャネルの関連付けを表示するには、次の例に示すように **channels** オプションを指定した **show cable ofdm-chan-profiles** コマンドを使用します。

```
Router# show cable ofdm-chan-profile channels

**** OFDM Channel Profile Assigned Channels ****

Prof  Admin  Controller:channels
```

```
ID
20    Up     3/0/1:158              3/0/2:158              3/0/3:158              3/0/5:158

             3/0/6:158              3/0/7:158
30    Up     3/0/4:158
101   Up     3/0/0:158
```

OFDMチャネルプロファイルの設定を表示するには、次の例のように**configuration**オプションを指定した **show cable ofdm-chan-profiles** コマンドを使用します。

```
Router# show cable ofdm-chan-profile configuration

**** OFDM Channel Profile Configuration ****

Prof  Cycl  Roll  Guardband  FFT  Intr   Pilot  Modulation (D-Default, P-Profile)

ID    Prfx  Off   Override   KHz  Depth  Scale  Cntrl   NCP     Data Profiles
             (Limited to 20)                                    1       2       3       4
      5
0     1024  128   NA         50   16     48     D:256   D:16    D:1024  NA      NA      NA
      NA
1     1024  128   NA         50   16     48     D:256   D:16    D:2048  D:1024  NA      NA
      NA
2     1024  128   NA         50   16     48     D:256   D:16    D:4096  D:2048  D:1024  NA
      NA
3     1024  128   NA         50   16     48     D:256   D:16    P:0     D:4096  D:2048
D:1024  NA
4     1024  128   NA         50   16     48     D:256   D:16    D:512   P:0     D:4096
D:2048  D:1024
5     1024  128   NA         25   16     48     D:256   D:16    D:1024  NA      NA      NA
      NA
6     1024  128   NA         25   16     48     D:256   D:16    D:2048  D:1024  NA      NA
      NA
7     1024  128   NA         25   16     48     D:256   D:16    D:4096  D:2048  D:1024  NA
      NA
8     1024  128   NA         25   16     48     D:256   D:16    P:1     D:4096  D:2048
D:1024  NA
9     1024  128   NA         25   16     48     D:256   D:16    D:512   P:1     D:4096
D:2048  D:1024
20    1024  128   NA         50   16     48     D:1024  D:16    NA      NA      NA      NA
      NA
21    1024  128   1000000    50   16     48     D:1024  D:16    NA      NA      NA      NA
      NA
```

プライマリ チャネルとしての OFDM チャネルの設定

MAC ドメインで RF チャネルを OFDM プライマリ チャネルとして設定するには、次のコマンドを使用します。

```
enable
configure terminal
interface cable <slot/subslot/port> downstream Integrated-Cable <slot/subslot/port>
rf-channel <ofdm-channel-number: 158-162>
end
```

OFDM プライマリ チャネル設定の確認

OFDM チャネルがプライマリ チャネルとなっている場合、その OFDM チャネル設定の詳細を表示するには、次の例に示すコマンドを使用します。

```
Router#sh run int c3/0/3
Building configuration...

Current configuration : 539 bytes
```

```
!
interface Cable3/0/3
 load-interval 30
 downstream Integrated-Cable 3/0/3 rf-channel 0
 downstream Integrated-Cable 3/0/3 rf-channel 158
 upstream 0 Upstream-Cable 3/0/6 us-channel 0
 upstream 1 Upstream-Cable 3/0/6 us-channel 1
 upstream 2 Upstream-Cable 3/0/6 us-channel 2
 upstream 3 Upstream-Cable 3/0/6 us-channel 3
 cable upstream bonding-group 1
  upstream 0
  upstream 1
  upstream 2
  upstream 3
  attributes 80000000
 cable bundle 1
 cable cm-status enable 3 6-11 16-18 20-27
 cable privacy accept-self-signed-certificate
end
```

また、次の例に示すコマンドを使用して、CFDM プライマリ チャネル設定の詳細を表示することもできます。

```
Router#sh cable mac-domain c3/0/3 cgd-associations
CGD Host  Resource  DS Channels            Upstreams    (ALLUS)   Active DS
Ca3/0/3   3/0/3     0                      0-3          Yes        0
                    158                    0-3          Yes        158
```

次の例のように、**show cable mac-domain Cable <slot>/<subslot>/<port> mdd** コマンドも CFDM プライマリ チャネル設定の詳細を表示します。

```
...
Downstream Active Channel List
        Channel ID:             159
        Frequency:              836000000Hz
        Primary Capable:        Primary-Capable
        CM-STATUS Event Bitmask:0x36
                                MDD Timeout
                                QAM FEC failure
                                MDD Recovery
                                QAM FEC recovery
        MAP/UCD Transport Indicator:  Can carry MAPs and UCDs
        OFDM PLC Params Bitmask:
               Tukey raised cosine window: 0.625
               Cyclic Prefix: 5.0
               Sub carrier spacing: 50
```

RF チャネルはゼロから始まる番号方式を使用する一方、ダウンストリーム チャネル ID は 1 から番号が付けられます。したがって、RF チャネル 158 はチャネル ID 159 に相当します。この例でのチャネル ID は 159 です。`MAP/UCD Transport Indicator` は、MAP と UCD がプライマリ チャネルでのみ送信されていることを意味します。

ポート/コントローラとチャネルの設定

ポート/コントローラとチャネルを設定するには、次の手順に従います。

enable
configure terminal
controller integrated-cable *slot/subslot/port*
max-ofdm-spectrum *value*
ofdm-freq-excl-band start-frequency *value* **width** *value*
rf-chan *start_id* [*end_id*]
ofdm channel-profile *id* **start-frequency** *value* **width** *value* [**plc** *value*]

（注） OFDM チャネル設定での *start_id* の範囲は 158 ～ 162 です。

OFDM チャネルに最大 OFDM スペクトルが割り当てられ、CMTS はこれを使用してデフォルト ポート基本電力を計算します。

ofdm-freq-excl-band コマンドを使用すると、すべての OFDM チャネルから特定の周波数の範囲を除外できます。

ポート/コントローラとチャネルの設定の確認

RF ポートの詳細を表示するには、次の例に示すように、**rf-port** オプションを指定した **show controller integrated-cable** コマンドを使用します。

```
Router# show controller integrated-cable 3/0/0 rf-port

Admin:  UP  MaxCarrier: 128  BasePower: 33 dBmV  Mode: normal
  Rf Module 0: UP
  Free freq block list has 3 blocks:
    45000000  - 107999999
    624000000 - 644999999
    837000000 - 1217999999
  Rf Port Status: UP
  MaxOfdmSpectrum:  192000000   Equivalent 6MHz channels: 32
  UsedOfdmSpectrum: 192000000   AvailOfdmSpectrum:        0
  DefaultBasePower: 33 dBmV     Equivalent 6MHz channels: 160
  OFDM frequency exclusion bands: None
```

OFDM チャネルのサマリー情報を表示するには、次の例に示すように、**rf-channel** オプションを指定した **show controller integrated-cable** コマンドを使用します。

```
Router# show controller integrated-cable 3/0/0 rf-channel 158

Chan State Admin Mod-Type  Start       Width     PLC        Profile-ID    dcid  power
output
                           Frequency
 158   UP   UP   OFDM      627000000   96000000  663000000       20       159   34
NORMAL
```

OFDM チャネルの詳細情報を表示するには、次の例に示すように、**rf-channel** および **verbose** オプションを指定した **show controller integrated-cable** コマンドを使用します。

```
Router# show controller integrated-cable 3/0/0 rf-channel 158 verbose

Chan State Admin Mod-Type  Start       Width     PLC        Profile-ID    dcid  power
output
                           Frequency
 158   UP   UP   OFDM      627000000   96000000  663000000       30       159   32
NORMAL
 Resource status:   OK
 License: granted <17:02:35 EDT May 18 2016>
 OFDM channel license spectrum width: 92200000
 OFDM modulation license (spectrum width): 2K (6000000)
 OFDM config state: Configured

 OFDM channel details: [3/0/4:158]
----------------------------------------
 OFDM channel frequency/subcarrier range     : 627000000[1088] - 722999999[3007]
 OFDM spectrum frequency/subcarrier range    : 572600000[   0] - 777399999[4095]
 Active spectrum frequency/subcarrier range  : 628900000[1126] - 721049999[2969]
 OFDM channel center frequency/subcarrier    : 675000000[2048]
 PLC spectrum start frequency/subcarrier     : 663000000[1808]
 PLC frequency/subcarrier                    : 665800000[1864]
```

```
Channel width                                  : 96000000
Active Channel width                           : 92200000
OFDM Spectrum width                            : 204800000
Chan prof id                                   : 30
Cyclic Prefix                                  : 1024
Roll off                                       : 128
Interleave depth                               : 16
Spacing                                        : 50KHZ
Pilot Scaling                                  : 48
Control modulation profile                     : 10
NCP modulation default                         : 16
Data modulation default                        : None
Data modulation profile                        : None
Lower guardband width in freq/subcarriers      : 1900000[38]
Upper guardband width in freq/subcarriers      : 1900000[38]
Licensed 4K modulation spectrum width          : 0
Licensed 2K modulation spectrum width          : 6000000

PLC spectrum frequencies [subcarriers]             :
 663000000[1808] - 668999999[1927]

PLC channel frequencies [subcarriers]                :
 665800000[1864] - 666199999[1871]   Size: 8 subcarriers

Excluded frequencies [subcarriers]                 :
 572600000[   0] - 628899999[1125]     721100000[2970] - 777399999[4095]
 Count: 2252

Pilot frequencies [subcarriers]                    :
 *:PLC pilots
 630700000[1162]   634300000[1234]   637900000[1306]   641500000[1378]
 645100000[1450]   648700000[1522]   652300000[1594]   655900000[1666]
 659500000[1738]   663450000[1817]*  664050000[1829]*  664600000[1840]*
 665050000[1849]*  666900000[1886]*  667350000[1895]*  667900000[1906]*
 668500000[1918]*  669100000[1930]   672700000[2002]   676300000[2074]
 679900000[2146]   683500000[2218]   687100000[2290]   690700000[2362]
 694300000[2434]   697900000[2506]   701500000[2578]   705100000[2650]
 708700000[2722]   712300000[2794]   715900000[2866]   719500000[2938]
 Count: 32

Active frequencies [subcarriers]                   :
 628900000[1126] - 721099999[2969]
 Count: 1844

Data frequencies [subcarriers]                     :
 628900000[1126] - 630699999[1161]     630750000[1163] - 634299999[1233]
 634350000[1235] - 637899999[1305]     637950000[1307] - 641499999[1377]
 641550000[1379] - 645099999[1449]     645150000[1451] - 648699999[1521]
 648750000[1523] - 652299999[1593]     652350000[1595] - 655899999[1665]
 655950000[1667] - 659499999[1737]     659550000[1739] - 663449999[1816]
 663500000[1818] - 664049999[1828]     664100000[1830] - 664599999[1839]
 664650000[1841] - 665049999[1848]     665100000[1850] - 665799999[1863]
 666200000[1872] - 666899999[1885]     666950000[1887] - 667349999[1894]
 667400000[1896] - 667899999[1905]     667950000[1907] - 668499999[1917]
 668550000[1919] - 669099999[1929]     669150000[1931] - 672699999[2001]
 672750000[2003] - 676299999[2073]     676350000[2075] - 679899999[2145]
 679950000[2147] - 683499999[2217]     683550000[2219] - 687099999[2289]
 687150000[2291] - 690699999[2361]     690750000[2363] - 694299999[2433]
 694350000[2435] - 697899999[2505]     697950000[2507] - 701499999[2577]
 701550000[2579] - 705099999[2649]     705150000[2651] - 708699999[2721]
 708750000[2723] - 712299999[2793]     712350000[2795] - 715899999[2865]
 715950000[2867] - 719499999[2937]     719550000[2939] - 721099999[2969]
 Count: 1804

Profiles:
 Number of profiles: 2
 CTRL profile (Profile A): rate: 461916 kbps, usable rate: 368000 kbps
 Active frequencies [subcarriers]:
 Modulation:Start-freq[start-subcarrier] - End-freq[end-subcarrier]
 ---------------------------------------------------------------------
 64   :628900000[1126] - 628950000[1127]     2048 :629000000[1128] - 630650000[1161]
 2048 :630750000[1163] - 634250000[1233]     2048 :634350000[1235] - 634950000[1247]
 64   :635000000[1248] - 637850000[1305]     64   :637950000[1307] - 641450000[1377]
```

```
 64   :641550000[1379] - 645050000[1449]     64   :645150000[1451] - 648650000[1521]
 64   :648750000[1523] - 652250000[1593]     64   :652350000[1595] - 655850000[1665]
 64   :655950000[1667] - 659450000[1737]     64   :659550000[1739] - 663400000[1816]
 64   :663500000[1818] - 664000000[1828]     64   :664100000[1830] - 664550000[1839]
 64   :664650000[1841] - 665000000[1848]     64   :665100000[1850] - 665750000[1863]
 64   :666200000[1872] - 666850000[1885]     64   :666950000[1887] - 667300000[1894]
 64   :667400000[1896] - 667850000[1905]     64   :667950000[1907] - 668450000[1917]
 64   :668550000[1919] - 669050000[1929]     64   :669150000[1931] - 672650000[2001]
 64   :672750000[2003] - 676250000[2073]     64   :676350000[2075] - 679850000[2145]
 64   :679950000[2147] - 683450000[2217]     64   :683550000[2219] - 687050000[2289]
 64   :687150000[2291] - 690650000[2361]     64   :690750000[2363] - 694250000[2433]
 64   :694350000[2435] - 697850000[2505]     64   :697950000[2507] - 701450000[2577]
 64   :701550000[2579] - 705050000[2649]     64   :705150000[2651] - 708650000[2721]
 64   :708750000[2723] - 709000000[2728]     512  :709050000[2729] - 712250000[2793]
 512  :712350000[2795] - 715850000[2865]     512  :715950000[2867] - 719450000[2937]
 512  :719550000[2939] - 721000000[2968]     64   :721050000[2969] - 721050000[2969]
 Active subcarrier count: 1804, ZBL count: 0
 Discontinuity time [days:hours:mins:secs]: 00:00:54:32 [16:15:02 EDT May 18 2016]

 NCP profile:
 Active frequencies [subcarriers]:
 Modulation:Start-freq[start-subcarrier] - End-freq[end-subcarrier]
 ------------------------------------------------------------------
 16   :628900000[1126] - 630650000[1161]     16   :630750000[1163] - 634250000[1233]
 16   :634350000[1235] - 637850000[1305]     16   :637950000[1307] - 641450000[1377]
 16   :641550000[1379] - 645050000[1449]     16   :645150000[1451] - 648650000[1521]
 16   :648750000[1523] - 652250000[1593]     16   :652350000[1595] - 655850000[1665]
 16   :655950000[1667] - 659450000[1737]     16   :659550000[1739] - 663400000[1816]
 16   :663500000[1818] - 664000000[1828]     16   :664100000[1830] - 664550000[1839]
 16   :664650000[1841] - 665000000[1848]     16   :665100000[1850] - 665750000[1863]
 16   :666200000[1872] - 666850000[1885]     16   :666950000[1887] - 667300000[1894]
 16   :667400000[1896] - 667850000[1905]     16   :667950000[1907] - 668450000[1917]
 16   :668550000[1919] - 669050000[1929]     16   :669150000[1931] - 672650000[2001]
 16   :672750000[2003] - 676250000[2073]     16   :676350000[2075] - 679850000[2145]
 16   :679950000[2147] - 683450000[2217]     16   :683550000[2219] - 687050000[2289]
 16   :687150000[2291] - 690650000[2361]     16   :690750000[2363] - 694250000[2433]
 16   :694350000[2435] - 697850000[2505]     16   :697950000[2507] - 701450000[2577]
 16   :701550000[2579] - 705050000[2649]     16   :705150000[2651] - 708650000[2721]
 16   :708750000[2723] - 712250000[2793]     16   :712350000[2795] - 715850000[2865]
 16   :715950000[2867] - 719450000[2937]     16   :719550000[2939] - 721050000[2969]
 Active subcarrier count: 1804, ZBL count: 0

CCCs:
  OCD CCC: 2
  DPD CCCs:
    Control profile  (Profile A) CCC: 2
        NCP profile  CCC: 2
Resource config time taken: 2286 msecs


JIB channel number: 776
Chan Pr EnqQ  Pipe  RAF   SyncTmr DqQ ChEn   RAF Pipe Phy0 Phy1 Tun# SessId 0[TkbRt MaxP]
    1[TkbRt MaxP]
 776  0   384     1   725       0 384 0100 13032    1    0    1    2      0 479610000 4485120
 383688000 4485120
 776  1   384     1  4786       0 384 0100  2190    1    0    1    2      0 479610000 4485120
 383688000 4485120
 776  2   384     1  4786       0 384 0100  2190    1    0    1    2      0 479610000 4485120
 383688000 4485120
 776  3   384     1  4786       0 384 0100  2190    1    0    1    2      0 479610000 4485120
 383688000 4485120
 776  4   384     1  4786       0 384 0100  2190    1    0    1    2      0 479610000 4485120
 383688000 4485120
 776  5   384     1  4786       0 384 0100  2190    1    0    1    2      0 479610000 4485120
 383688000 4485120
 776  6   384     1  4786       0 384 0100  2190    1    0    1    2      0 479610000 4485120
 383688000 4485120
 776  7   384     1     0       0 384 0100     0    1    0    1    2      0 479610000 4485120
 383688000 4485120

Chan   Qos-Hi   Qos-Lo    Med-Hi   Med-Lo    Low-Hi   Low-Lo
 776   368640   245760    368640   245760    614400   368640
Chan  Med Low TB-neg Qos_Exc  Med_Xof  Low_Xof  Qdrops(H-M-L)  Pos    Qlen(Hi-Med-lo) Fl
```

```
Tgl_cnt Rdy_sts
  776   0   0      0       0        0        0    0    0    0  Y      0      0      0  0
      0 ff
Chan       Rate   Neg   Pos    LastTS  CurrCr  Pos  [PLC Rate Neg Pos]
 776   10485750 65535 65535 116199669 268431360   Y [MM 86 128 1114][EM 87 128 6204][TR 2
9 3102]
DSPHY Info:
 Local rf port 0 , rf chan 158 pic loss 123
 non short CWs: = 235681130, shorts = 0, stuff bytes = 235639172 bch 235681130
 NCP msgs: = 453809753, PLC encodings = 16902476
 flow0 rcv 70203 flow1 rcv 3 flow0 drops 0 flow1 drops 0
```

設定例

このセクションでは、OFDM チャネルの設定例を示します。

例 1：**OFDM チャネルの設定**

（注） OFDM チャネル プロファイルを設定する前に、それが参照する OFDM 変調プロファイルを設定する必要があります。

次の例では、OFDM チャネルの設定方法を示します。

enable
configure terminal
cable downstream ofdm-modulation-profile *9*
description *512-1k-4k*
subcarrier-spacing *50KHz*
width *96000000*
start-frequency *627000000*
assign modulation-default *512-QAM*
assign modulation *1024-QAM* **range-subcarriers freq-abs** *635000000* **width** *74050000*
assign modulation *4096-QAM* **range-subcarriers freq-abs** *629000000* **width** *6000000*
exit
configure terminal
cable downstream ofdm-chan-profile *20*
description *Data profiles: 2 single mod, 1 mixed mod*
cyclic-prefix *192*
interleaver-depth *16*
pilot-scaling *48*
roll-off *128*
subcarrier-spacing *50KHz*
profile-ncp modulation-default *16-QAM*
profile-control modulation-default *256-QAM*
profile-data *1* **modulation-default** *1024-QAM*
profile-data *2* **modulation-default** *2048-QAM*
profile-data *3* **modulation-profile** *9*
exit
configure terminal
controller integrated-cable *3/0/0*
max-ofdm-spectrum *96000000*
ofdm-freq-excl-band start-frequency *683000000* **width** *10000000*
rf-chan *158*

power-adjust *0*
docsis-channel-id *159*
ofdm channel-profile *20* **start-frequency** *627000000* **width** *96000000* **plc** *663000000*

例 **2**：**MAC** ドメインでの **OFDM** プライマリ チャネルの設定

enable
configure terminal
```
Enter configuration commands, one per line.  End with CNTL/Z.
```
interface cable *3/0/0*
downstream Integrated-Cable *3/0/3* **rf-channel** *158*
end

その他の参考資料

関連資料

マニュアル タイトル	リンク
Cisco cBR Converged Broadband Routers Layer 2 and DOCSIS 3.0 Configuration Guide	http://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_cbr_layer2_docsis30.html

MIB

MIB	MIB のリンク
DOCS-IF31-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

DOCSIS 3.1 OFDM チャネル設定に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *79* : *DOCSIS 3.1 OFDM* チャネル設定に関する機能情報

機能名	リリース	機能情報
DOCSIS 3.1 OFDM チャネルのサポート	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。
完全なスペクトル 108-1218 MHz サポート	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

機能名	リリース	機能情報
DOCSIS 3.1 OFDM プライマリチャネルのサポート	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズコンバージド ブロードバンドルータに統合されました。
サブキャリア間隔、除外バンド、およびLCPR のサポートの強化	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズコンバージド ブロードバンドルータに統合されました。

第 28 章

OFDM チャネルの電力プロファイル

OFDM チャネル電力プロファイル機能は、DOCSIS 3.1 ダウンストリーム OFDM チャネルで 6 Mhz バンドの電力レベルを調整する際に役立ちます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *80*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

OFDM チャネルの電力プロファイルについて

OFDM 電力プロファイルは、電力レベルをより細かい粒度で補正することにより、ケーブル モデムの出力電力レベルを安定化させます。また OFDM チャネルの帯域幅でケーブル損失量の差異を低減します。

この機能により、 Cisco cBR シリーズ コンバージド ブロードバンド ルータはケーブルによる伝送損失を出荷時に修正できます。

OFDM 電力プロファイル（ofdm-power-profile）は、OFDM チャネルの送信電力レベルを 6 Mhz ごとに調整します。OFDM チャネル幅は 24 Mhz ～ 192 Mhz の範囲になるため、プロファイルでのバンド数は 4 ～ 32 となります。

各 6 MHz のバンドは、ゼロで始まるバンドインデックス（band-index）で参照されます。192 MHz OFDM チャネルでは最大バンド範囲が 0 ～ 31 になります。OFDM チャネル内のバンドごとに、

固有の電力レベルを設定できます。OFDM 電力プロファイルで可能なバンド調整範囲は合計 8 dB です。OFDM チャネルのダウンストリーム コントローラのベース チャネル電力が DRFI 仕様の最大電力レベルを超えて設定されている場合、特定の条件下では OFDM 電力プロファイルの調整範囲が最大 9 dB になることもあります。

電力プロファイルでは、電力レベル（power-adjust-default）をデフォルト値に設定できます。このデフォルト値は、他の方法で設定されていないバンドすべてに適用されます。

バンド電力レベルを設定する方法には 2 通りあります。1 つはパワー チルト設定（power-tilt-linear）で、もう 1 つはバンド/バンド範囲の電力レベルの設定（band-index）です。1 つの OFDM 電力プロファイル内で、この 2 つの方法を同時に使用してバンド電力レベルを設定できます。

パワー チルト設定は、バンド インデックス 0 に適用される `power-adjust-default` 値と、プロファイルの最大バンド インデックスに適用される power-tilt-linear 調整値との間で線形に power-adjust 値を適用します。たとえば、96 Mhz の OFDM 電力プロファイルで power-tilt-linear が 4dB に設定され、power-adjust-default が 0 dB に設定されているとします。プロファイルには 0 ～ 15 までの 16 個のバンドがあり、バンド インデックス 0 は +0 dB、バンド インデックス 15 は +4 dB です。バンド 1 ～ 14 の電力レベル設定では、バンド 0 ～ バンド 15 までの dB 値が 1/10 刻みで線形に割り当てられます。

band-index 設定は、指定したバンドに特定の値を適用します。band-index 設定では単一のバンドまたは複数バンドの範囲を指定できます。power-adjust 設定を使用して、バンドの電力レベル（dB）値を 1/10 刻みで指定します。

パワー チルトとバンド インデックスの両方を同時に使用できます。この場合、band-index が最後に適用されます。この両方を使用する場合、band-index power-adjust 値を使用して power-tilt-linear 値をオーバーライドできます。

Cisco cBR ルータには、番号 1 ～ 64 までの最大 64 個の OFDM 電力プロファイルを設定できます。設定時の検証テストに合格する限り、複数のライン カードにわたる複数のコントローラ OFDM チャネルに単一の OFDM 電力プロファイルを適用できます。設定エラーまたは警告が発生した場合は、それを示すエラー メッセージがルータのコンソールに表示されます。

OFDM 電力プロファイルの設定に関する制限事項

OFDM 電力プロファイルの設定には、次の制限事項が適用されます。

- OFDM 電力プロファイルは、DOCSIS 3.1 システムでのみ設定できます。
- 電力プロファイルは、ダウンストリーム コントローラの OFDM チャネル（RF チャネル 158 ～ 162）にのみ適用可能です。

OFDM チャネル電力プロファイルの設定方法

（注） このモジュールで参照されているコマンドの詳細については、「Cisco IOS Master Command List」を参照してください。

バンドインデックスを使用した OFDM 電力プロファイルの設定

次のコマンドをバンドインデックス設定と併せて使用して電力プロファイルを設定すると、バンドインデックス値がオーバーライドとして機能します。

```
enable
configure terminal
cable downstream ofdm-power-profile <profile_id>
  power-adjust-default -2.1
  band-index 0 7
    power-adjust -1.0
  band-index 8 15
    power-adjust -0.5
  band-index 16 23
    power-adjust 0.5
  band-index 24 31
    power-adjust 1.5

controller Integrated-Cable {slot}/{subslot}/{port}
rf-channel {158 - 162 }
power-profile {ofdm-power-profile-id}
```

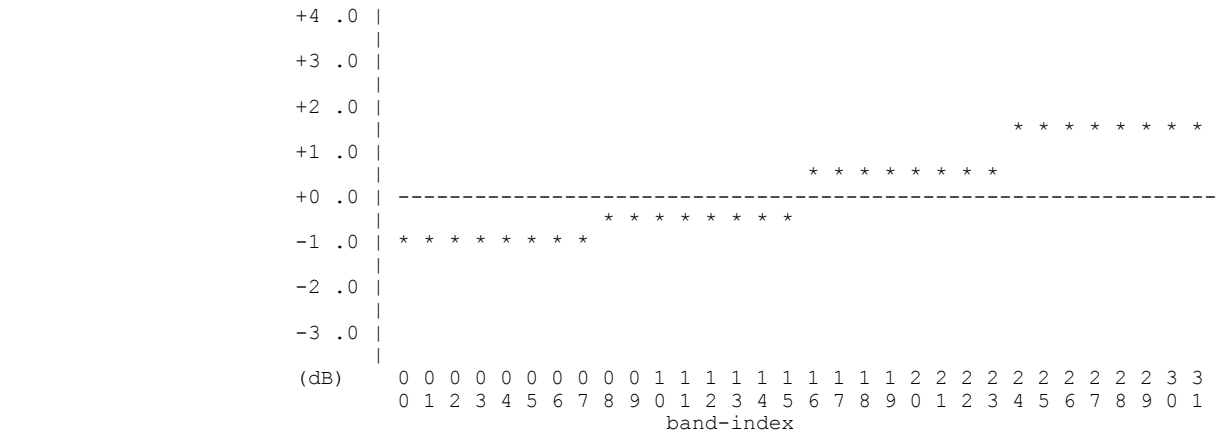
電力プロファイル設定の確認

電力プロファイル設定の詳細を表示するには、次の例に示すように **show cable ofdm-power-profile** コマンドを使用します。また、このコマンドにより、プロファイルで設定されている実際のパワーバンド電力レベルも表示されます。

```
Router> show cable ofdm-power-profile 3
OFDM Power Profile 3

Power-Adjust-Default(*): -2.1

Power-Band:
[00-07]   -1.0   -1.0   -1.0   -1.0   -1.0   -1.0   -1.0   -1.0
[08-15]   -0.5   -0.5   -0.5   -0.5   -0.5   -0.5   -0.5   -0.5
[16-23]    0.5    0.5    0.5    0.5    0.5    0.5    0.5    0.5
[24-31]    1.5    1.5    1.5    1.5    1.5    1.5    1.5    1.5
```



線形パワー チルトを使用した OFDM 電力プロファイルの設定

線形パワー チルトとバンド インデックス オーバーライドを使用して OFDM 電力プロファイルを設定するには、次のコマンドを使用します。

```
enable
configure terminal
cable downstream ofdm-power-profile <profile_id>
  power-adjust-default 0.0
  power-tilt-linear 3.5
  band-index 0
  power-adjust 4.0
```

show controller コマンドを使用した電力プロファイルの確認

電力プロファイルで設定された絶対パワーバンド レベルを表示するには、**show controller** コマンドを使用します。電力プロファイルがコントローラに適用されている場合、実際の送信電力レベル（dBmV 単位）が電力レベルとして表示されます。

```
Router>show controller Integrated-Cable 3/0/0 rf-channel 158 verbose
Chan State Admin Mod-Type  Start  Width     PLC        Profile-ID    dcid  power  output
                           Frequency
 158   UP   UP   OFDM      849000000   96000000  856000000       20       159   33.0
NORMAL
 Resource status:   OK
 License: granted <09:23:14 EDT Aug 1 2016>
 OFDM channel license spectrum width: 92200000
 OFDM config state: Configured

 OFDM Power Profile: 3
Power-Band:
[00-07]   32.0   32.0   32.0   32.0   32.0   32.0   32.0   32.0
[08-15]   32.5   32.5   32.5   32.5   32.5   32.5   32.5   32.5
[16-23]   33.5   33.5   33.5   33.5   33.5   33.5   33.5   33.5
[24-31]   34.5   34.5   34.5   34.5   34.5   34.5   34.5   34.5

OFDM channel details: [3/0/0:158]
-----------------------------------------
```

OFDM 電力プロファイルの設定例

ここでは、OFDM 電力プロファイルの設定例を記載します。

例：線形パワー チルトを使用した OFDM 電力プロファイルの設定

```
enable
configure terminal
cable downstream ofdm-power-profile 3
  power-adjust-default 0.0
  power-tilt-linear 3.5
  band-index 0
  power-adjust 4.0
```

OFDM チャネルの電力プロファイルに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。

Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *81*：*OFDM* チャネルの電力プロファイルに関する機能情報

機能名	リリース	機能情報
OFDM チャネルの電力プロファイル	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 29 章

DOCSIS 3.1 パス選択

このドキュメントでは、Cisco cBR シリーズ コンバージド ブロードバンド ルータ上でパス選択を設定する方法について説明します。

パス選択について

DOCSIS 3.1 パス選択機能が強化されて、OFDM ダウンストリーム チャネルおよび OFDMA アップストリーム チャネルをサポートするようになりました。RCC 選択プロセスが強化されて、OFDM チャネルを含むようになりました。TCC 選択プロセスが強化されて、OFDMA チャネルを含むようになりました。

パス選択の設定方法

OFDM チャネルを使用したダウンストリーム ボンディング グループの設定

OFDM チャネルを使用してダウンストリーム ボンディング グループを設定するには、以下の手順に従います。

enable
configure terminal
interface wideband-cable *slot/subslot/bay:wideband-channel*
description *text*
cable bundle *id*
cable rf-channels channel-list *grouplist* **bandwidth-percent** *percentage-bandwidth*

（注） チャネル 158 ～ 162 が OFDM チャネルとして指定されます。

OFDM チャネルを使用したダウンストリーム ボンディング グループ設定の確認

OFDMチャネルを使用したダウンストリームボンディング グループの詳細を表示するには、次の例に示すように **show running-config interface** コマンドを使用します。

```
Router# show running-config interface wideband-cable 3/0/0:13

Building configuration...

Current configuration : 212 bytes
!
interface Wideband-Cable3/0/0:13
 description D31-DSBG: 1 SC-QAM plus 1 OFDM
 cable bundle 1
 cable rf-channels channel-list 8 bandwidth-percent 30
 cable rf-channels channel-list 158 bandwidth-percent 25
end
```

OFDMA チャネルを使用したアップストリーム ボンディング グループの設定

OFDMA チャネルを使用してアップストリーム ボンディング グループを設定するには、次の手順に従います。

enable
configure terminal
interface cable *slot/subslot/bay*
cable upstream bonding-group *id*
upstream *id*

OFDMA チャネルを使用したアップストリーム ボンディング グループ設定の確認

OFDMA チャネルを使用したアップストリーム ボンディング グループの詳細を表示するには、次の例に示すように **show running-config interface** コマンドを使用します。

```
Router# show running-config interface cable 6/0/3
Building configuration...

Current configuration : 212 bytes
!
interface Cable6/0/3
 load-interval 30
 downstream Integrated-Cable 6/0/1 rf-channel 158
 upstream 0 Upstream-Cable 1/0/0 us-channel 0
 upstream 1 Upstream-Cable 1/0/0 us-channel 1
 upstream 2 Upstream-Cable 1/0/0 us-channel 2
 upstream 3 Upstream-Cable 1/0/0 us-channel 3
 upstream 6 Upstream-Cable 1/0/0 us-channel 12
 cable upstream balance-scheduling
 cable upstream bonding-group 2
  upstream 0
  upstream 1
  upstream 2
  upstream 3
  upstream 6
```

```
  attributes 80000000
 cable bundle 1
 cable privacy accept-self-signed-certificate
!
```

パス選択ステータスの確認

ケーブル モデムのパス選択ステータスを表示するには、次の例に示すように **show cable modem path-sel** コマンドを使用します。

```
router#show cable modem 38c8.5cfe.efa6 path-sel

CM 38c8.5cfe.efa6 Path-Sel Info: 07:20

RCS Filter Result: Succeed
Candidate RCS List: 2
  RCC-Id   Owner-Id   Preliminary  RCP      TLV-56   LBG      SF-Attr   CM-Attr
  1        1 :12289   Pass         Pass      --      Pass     Pass      Pass
  2        1 :12290   Pass         Pass      --      Pass     Pass      Pass

TCS Filter Result: Succeed
TCS Info:
  TCS in CGD            : 0x7         UCID: 1 2 3
  TCS in Freq Range     : 0x7         UCID: 1 2 3
  TCS Impaired          : 0x0
TCS Passed filters:
  Preliminary           : 0x7         UCID: 1 2 3
  LB Group              : 0x7         UCID: 1 2 3
  SF Attr Mask          : 0x7         UCID: 1 2 3
  CM Attr Mask          : 0x7         UCID: 1 2 3

Candidate US-BG List: 4
  UBG-Id   Chan-Mask    Preliminary  TLV-56   LBG      SF-Attr   CM-Attr
  1        0x7          Pass          --      Pass     Pass      Pass
  65537    0x2          Pass          --      Pass     Pass      Pass
  65538    0x4          Pass          --      Pass     Pass      Pass
  65536    0x1          Pass          --      Pass     Pass      Pass

Primary DS Chan Result: Skipped
Candidate Primary DS Chan List: 0

Primary US Chan Result: Skipped
Candidate Primary US Chan List: 0
```

パス選択ステータスのクリア

すべての CM のパス選択ステータスをクリアするには、次の例に示すように **clear cable modem all path-sel** コマンドを使用します。

```
Router# clear cable modem all path-sel

Router# show cable modem c8fb.26a6.c46a path-sel

CM c8fb.26a6.c46a Path-Sel Info: N/A
Path-Sel status has been cleared after register online.
```

RCC 設定の確認

ケーブル インターフェイス上のランタイム RCC を確認するには、次の例に示すように **show cable mac-domain rcc** コマンドを使用します。

```
Router# show cable mac-domain cable 7/0/0 rcc

RCC-ID   RCP               RCs MD-DS-SG CMs   WB/RCC-TMPL      D3.0 D3.1
4        00 00 00 00 00    16  0        1     WB (Wi7/0/0:0)   Y    Y
5        00 00 00 00 00    25  0        2     WB (Wi7/0/0:1)   N    Y
6        00 10 00 00 08    8   0        0     RCC-TMPL(3:1)    Y    N
7        00 00 00 00 00    4   0        0     WB (Wi7/0/0:4)   Y    Y
```

DOCSIS 3.1 対応の RCC に関する情報のみを表示するには、次の例に示すように **show cable mac-domain rcc simplified** コマンドを使用します。

```
router#show cable mac-domain cable 7/0/0 rcc 5 simplified

RCC ID                  : 5
Created Via             : Wideband - Wi7/0/0:1
CM attribute mask       : 0x80000000

Primary Receive Channel List:
  Chan Idx   RF Chan         DCID  Freq
  1          In7/0/0:0       1     453000000

Non-Primary Receive Channel List:
  Chan Idx   RF Chan         DCID  Freq
  2          In7/0/0:1       2     459000000
  3          In7/0/0:2       3     465000000
  4          In7/0/0:3       4     471000000
  5          In7/0/0:4       5     477000000
  6          In7/0/0:5       6     483000000
  7          In7/0/0:6       7     489000000
  8          In7/0/0:7       8     495000000
  9          In7/0/0:8       9     501000000
  10         In7/0/0:9       10    507000000
  11         In7/0/0:10      11    513000000
  12         In7/0/0:11      12    519000000
  13         In7/0/0:12      13    525000000
  14         In7/0/0:13      14    531000000
  15         In7/0/0:14      15    537000000
  16         In7/0/0:15      16    543000000
  17         In7/0/0:16      17    549000000
  18         In7/0/0:17      18    555000000
  19         In7/0/0:18      19    561000000
  20         In7/0/0:19      20    567000000
  21         In7/0/0:20      21    573000000
  22         In7/0/0:21      22    579000000
  23         In7/0/0:22      23    585000000
  24         In7/0/0:23      24    591000000
  25         In7/0/0:158     159   663000000

OFDM Receive Channel List:
  Chan Idx   RF Chan         DCID  PLC-Freq        Profiles
  25         In7/0/0:158     159   663000000       0 1 2
```

その他の参考資料

関連資料

マニュアル タイトル	リンク
Cisco cBR Converged Broadband Routers Layer 2 and DOCSIS 3.0 Configuration Guide	http://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_cbr_layer2_docsis30.html

MIB

MIB	MIB のリンク
• DOCS-IF31-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

DOCSIS 3.1 パス選択に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *82* : ***DOCSIS 3.1*** パス選択に関する機能情報

機能名	リリース	機能情報
DOCSIS 3.1 パス選択	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。
DOCSIS 3.1 アップストリーム パスの選択	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 30 章

DOCSIS 3.1 ダウンストリーム プロファイルの選択

初版：2016 年 7 月 13 日

DOCSIS 3.1 では、OFDM チャネル用のダウンストリーム プロファイルの概念が導入されています。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *83*：***Cisco cBR*** シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

ダウンストリーム プロファイルについて

プロファイルとは、OFDM チャネル内のサブキャリアごとに定義される変調次数のリストです。CMTS では、サブキャリアごとに異なる変調次数を割り当てた複数のプロファイルを定義し、それらのプロファイルを 1 つの OFDM チャネルで使用することができます。

プロファイルを表示するには、次のコマンドを使用します。

- ケーブル モデム（CM）に関連付けられているプロファイルを表示するには、**show cable modem** *[ip-address| mac-address| cable| {slot | subslot | cable-interface-index}]***phy ofdm-profile** コマンドを使用します。
- 特定のケーブル モデルに関連付けられている詳細なプロファイル管理データを表示するには、**show cable modem** *[ip-address| mac-address]***prof-mgmt** コマンドを使用します。

CMTS では、さまざまな CM グループに異なるプロファイルを割り当てることができます。

デフォルトのデータ プロファイル

初めて CM を登録すると、デフォルトのデータ プロファイルがそれに割り当てられます。デフォルトのデータ プロファイルは「profile-data 1」です。「profile-data 1」が設定されていない場合は、「profile-control」が CM に割り当てられます。

（注） プロファイル ID 0 が設定されたプロファイル A は、制御プロファイルとも呼ばれます。

推奨されるプロファイル

cable modem *ip***opt0** コマンドを使用してモデムから収集される Receive Modulation Error Ratio（RxMER）値と、バックグラウンドで自動的かつ定期的に収集される RxMER 値に基づき、CMTS は既存のプロファイルの中から、許容されるエラーでモデムがコード ワードを受信するための十分な信号対雑音比（SNR）マージンを持つ、最も高速なプロファイルを予想して見つけます。このプロファイルは、その CM に関する推奨プロファイルと呼ばれます。**show cable modem phy ofdm-profile** コマンドは、CM ごとの推奨プロファイルを表示します。

各推奨プロファイルには、ユーザ設定可能な有効期間が関連付けられ、次のようにそれを設定できます。

```
Router (config)#cable downstream ofdm-prof-mgmt recommend-profile-age age-in-minutes
```

推奨プロファイルがこの有効期間を超えると、その CM に対して有効でなくなります。

不適合プロファイル

CMTS が CM-STATUS イベント 16（DS OFDM プロファイル失敗）を受信すると、CM-STATUS メッセージで示されているプロファイルが、このモデムに対する「不適合プロファイル」としてマークされます。

各不適合プロファイルには、ユーザ設定可能な最大有効期間が関連付けられ、次のようにそれを設定できます。

```
Router (config)#cable downstream ofdm-prof-mgmt unfit-profile-age age-in-minutes
```

モデムの不適合プロファイルがこの有効期間を経過すると、無効になります。

プロファイルの設定方法

プロファイル ダウングレードの設定

CM は、DS OFDM プロファイルの障害を示すために CM-STATUS イベント 16 メッセージを送信します。CMTS はこの指標を受け取ると、次のコマンドで表示されるプロファイル順序に従い、より低いプロファイルにモデムをダウングレードするためのアクションを直ちに実行します。

```
Router# show controllers integrated-Cable 2/0/3 rf-channel 158 prof-order
```

[DOCSIS 3.1 MULPI] からの抜粋である次の表は、プロファイル ダウングレードをトリガーする CM-STATUS イベントを示しています。

表 *84*：表：プロファイル ダウングレード用の *CM-STATUS* イベント

イベント タイプ	イベント条件	ステータス レポート イベント		CM から報告されるパラメータ	
		「on」へのトリガー イベント	「off」へのトリガー イベント	DCID	プロファイル ID
16	DS OFDM プロファイル失敗	チャネルに割り当てられたダウンストリーム OFDM プロファイルのいずれかで FEC ロック損失が発生した	その OFDM プロファイルに関する FEC ロックの再設定 または プライマリ チャネル MDD のアクティブ チャネル リストからチャネルが削除された または DBC-REQ を介して設定された CM の受信チャネルからチャネルが削除された	はい	はい

自動プロファイル ダウングレードを無効にするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

```
Router (config)#no cable downstream ofdm-prof-mgmt prof-dwngrd-auto
```

RxMER とビット ロードのマッピングの設定

Receive Modulation Error Ratio（RxMER）値をビット ロード値にマップするには、さまざまな方法があります。シスコでは、DOCSIS 3.1 OSSI で推奨されている次のマッピングをベースライン マッピングとして使用します。

RxMER（¼ DB 単位）	QAM	ビット ロード
60	16	4
84	64	6
96	128	7
108	256	8
122	512	9
136	1024	10
148	2048	11
164	4096	12
184	8192	13
208	16384	14

- RxMER からビット ロードへのマッピングを調整するためのマージンを設定するには、次のコマンドを使用します。
  ```
  Router(config)# cable downstream ofdm-prof-mgmt mer-margin-qdb interval-in-minutes
  ```
  上記のマッピング表が使用される前に、この設定値（*quarter-DB*）が、CMTS で収集された RxMER 値に加算されます。こうして、ユーザは推奨プロファイルを選択する際により適切に制御できます。
- 推奨プロファイルの計算で無視できるサブキャリアのパーセンテージを指定するには、次のコマンドを使用します。
  ```
  Router(config)# cable downstream ofdm-prof-mgmt exempt-sc-pct percent
  ```
  これは、外れ値を無視できるエクステントを指定する方法になります。
- RxMER ポーリング間隔を設定するには、次のコマンドを使用します。
  ```
  Router(config)# cable downstream ofdm-prof-mgmt rxmer-poll-interval interval-in-minutes
  ```
  初期 CM 登録後、CMTS は bit-0 オプションを指定した OPT メッセージを使って CM から RxMERデータを収集し、以降も定期的にこれを行います。収集されたRxMERデータを使用して、各 CM の推奨プロファイルが計算されます。

その他の参考資料

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

ダウンストリーム プロファイルの選択機能について

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *85*：ダウンストリーム プロファイルの選択機能について

機能名	リリース	機能情報
ダウンストリーム プロファイルの選択	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 31 章

アップストリーム SC QAM に対する DOCSIS 3.1 規定電力

このガイドでは、Cisco cBR ルータ上のアップストリーム SC-QAM に対する規定電力について説明します。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *86*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

アップストリーム SC QAM に対する規定電力機能について

UpStream Single Carrier Quadrature Amplitude Modulation（US SC-QAM）に対する規定電力機能は、レンジング中に DOCSIS 3.1 ケーブル モデムの送信電力レベルを動的に設定するための新しい方法をサポートします。

アップストリームの新しい規定電力レベルを表示するには、次のコマンドを使用します。

```
Router# show cable modem [ ip-address | mac-address | cable {slot /subslot
/cable-interface-index}] verbose
```

（注） DOCSIS 3.1 規定電力機能は、デフォルトで有効です。

機能 TLV

US SC-QAM に対する規定電力の影響を受ける TLV

次の表に、アップストリーム SC-QAM に関する DOCSIS 3.1 レンジング応答（RNG-RSP）規定電力が適用される TVL を記載します。

名前	タイプ	DOCSIS 3.1 の値
Power Level Adjust	2	送信電力のオフセット調整（符号付き 8 ビット、1/4 dB 単位）
Power Offset	12.4.4	送信電力のオフセット調整（符号付き 8 ビット、1/4 dB 単位）
Dynamic Range Window Upper Edge	14	最大許容設定値（Phi）を下回る、ダイナミック レンジ ウィンドウの上限（1/4 dB 単位）（DOCSIS PHYv3.0）。
Commanded Power	17	この TLV には、ダイナミック レンジ ウィンドウ値、P1.6load_min_set、および CM の伝送チャネルセットの各チャネルの送信電力レベル（1/4 dB 単位）が含まれます。

規定電力のサブ TLV

次の表に、DDOCSIS 3.1 規定電力のサブ TLV を記載します。

名前	タイプ（1 バイト）	長さ（1 バイト）	値（可変長）
Commanded Power	17	5 + 3*N	
Dynamic Range Window	17.1	1	ケーブル モデムの伝送チャネルセットに含まれる複数のトランスミッタ間の 1.6 Mhz での最大電力差の範囲（dB 単位）。

名前	タイプ（1 バイト）	長さ（1 バイト）	値（可変長）
List of Upstream Channel IDs and Corresponding Transmit Power Levels	17.2	3*N	TCS 内のチャネルごとの値： • ビット 23 ～ 16：UCID • ビット 15 ～ 0：送信電力レベル（1/4 dBmV）

その他の参考資料

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

US SC-QAM に対する規定電力の機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *87*：規定電力に関する機能情報

機能名	リリース	機能情報
US SC-QAM に対する DOCSIS 3.1 規定電力	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 32 章

OFDM チャネルの DOCSIS3.1 ダウンストリーム復元力

このドキュメントでは、Cisco cBR シリーズ コンバージドブロードバンドルータ上で OFDM チャネルの DOCSIS3.1 ダウンストリーム復元力を設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *88*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

OFDM チャネルの DOCSIS3.1 ダウンストリーム復元力について

DOCSIS3.1 CM が SCQAM または OFDM チャネルの非プライマリ RF チャネル障害を報告した場合にダウンストリーム復元力モジュールが行うアクションは、DOCSIS3.0 CM の場合と同じです。つまり、RF チャネル障害が復元力しきい値を下回っている場合は、CM サービス フローが復元力ボンディング グループ（RBG）またはナロー バンド（NB）インターフェイスに移動されます。RF チャネル障害が復元力しきい値を上回っている場合は、障害が発生した RF チャネルが一時的にボンディング グループから削除されます。

次の表に、OFDM チャネルに関する CM-STATUS イベントと、ダウンストリーム復元力モジュールが行うアクションを要約します。

表 *89* : *OFDM* チャネルに関する *CM-STATUS* イベント

イベント タイプ コード	イベントの説明	DS 復元力モジュールのアクション
1	MDD タイムアウト	CM のサービス フローを RBG/NB に移動するか、RF チャネルを BG から一時的に削除します。
2	FEC ロック失敗	CM のサービス フローを RBG/NB に移動するか、RF チャネルを BG から一時的に削除します。
4	MDD リカバリ	CM のサービス フローを元の BG に移動します。
5	FEC ロック リカバリ	CM のサービス フローを元の BG に移動します。
16	DS OFDM プロファイル失敗。チャネルに割り当てられたいずれかのダウンストリーム OFDM プロファイルで FEC ロック損失が発生した。	DS OFDM プロファイル マネージャがこのイベントを処理してアクションを実行します。
20	NCP プロファイル失敗。NCP での FEC ロック損失	イベントが記録されて、show コマンドで表示されます。
21	PLC での FEC ロック損失	イベントが記録されて、show コマンドで表示されます。
22	NCP プロファイル リカバリ。	イベントが記録されて、show コマンドで表示されます。
23	PLC チャネルでの FEC リカバリ	イベントが記録されて、show コマンドで表示されます。
24	OFDM プロファイルでの FEC リカバリ	イベント 16 で報告された障害のリカバリ。DS OFDM プロファイル マネージャがこのイベントを処理してアクションを実行します。

OFDM チャネルの DOCSIS3.1 ダウンストリーム復元力の設定方法

OFDM チャネルの DOCSIS3.1 ダウンストリーム復元力の設定

ダウンストリーム復元力機能を有効にするには、コマンド **cable rf-change-trigger percent** を設定する必要があります。

OFDM RF 障害に固有のトリガーしきい値を設定するには、次の手順に従います。

enable
configure terminal
cable ofdm-rf-change-trigger percent *value* **counter** *number*
これら 2 つのトリガーしきい値は、NP OFDM RF チャネルにグローバルに適用されます。このコマンドが設定されない場合、コマンド **cable rf-change-trigger percent** で設定されたトリガーしきい値が NP OFDM チャネルに使用されます。

（注） この新しいコマンドはオプションです。これを設定すると、トリガーしきい値が NP OFDM チャネルにのみ適用されます。

OFDM の特定の CM-STATUS イベントの表示

OFDM の特定の CM-STATUS イベントの統計情報を表示するには、次の例に示すように **show cable modem wideband rcs-status** コマンドを使用します。

```
router#show cable modem 4800.33ea.7072 wideband rcs-status verboseCM   : 4800.33ea.7072
RF  : 3/0/0 0
  Status                    : UP
  FEC/QAM Failure           : 0
  Dup FEC/QAM Failure       : 0
  FEC/QAM Recovery          : 0
  Dup FEC/QAM Recovery      : 0
  MDD Failure               : 0
  Dup MDD Failure           : 0
  MDD Recovery              : 0
  Dup MDD Recovery          : 0
  Flaps                     : 0
  Flap Duration             : 00:00
RF  : 3/0/0 1
  Status                    : UP
  FEC/QAM Failure           : 0
  Dup FEC/QAM Failure       : 0
  FEC/QAM Recovery          : 0
  Dup FEC/QAM Recovery      : 0
  MDD Failure               : 0
  Dup MDD Failure           : 0
  MDD Recovery              : 0
  Dup MDD Recovery          : 0
  Flaps                     : 0
  Flap Duration             : 00:00
RF  : 3/0/0 159
  Status                    : UP
  FEC/QAM Failure           : 0
  Dup FEC/QAM Failure       : 0
  FEC/QAM Recovery          : 0
  Dup FEC/QAM Recovery      : 0
```

```
MDD Failure               : 0
Dup MDD Failure           : 0
MDD Recovery              : 0
Dup MDD Recovery          : 0
NCP PROF Failure          : 2          May 8  15:14:24
Dup NCP PROF Failure      : 0
NCP PROF Recovery         : 1          May 8  15:15:18
Dup NCP PROF Recovery     : 0
PLC Lock Failure          : 1          May 8  15:14:47
Dup PLC Lock Failure      : 0
PLC Lock Recovery         : 1          May 8  15:15:46
Dup PLC Lock Recovery     : 0
Flaps                     : 0
Flap Duration             : 00:00
OFDM Profile Id : 2
Status                    : UP
Profile Failure           : 1          May 8  15:16:18
DUP Profile Failure       : 0
Profile Recovery          : 1          May 8  15:16:44
DUP Profile Recovery      : 0
```

OFDM チャネルの DOCSIS3.1 ダウンストリーム復元力に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *90* : *OFDM* チャネルの *DOCSIS3.1* ダウンストリーム復元力に関する機能情報

機能名	リリース	機能情報
OFDM チャネルの DOCSIS3.1 ダウンストリーム復元力	Cisco IOS XE Everest 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 33 章

DOCSIS 3.1 OFDMA チャネルの設定

このドキュメントでは、Cisco cBR シリーズ コンバージド ブロードバンド ルータ上で OFDMA チャネルを設定する方法について説明します。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *91*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

OFDMA チャネルの設定について

OFDMA チャネル

DOCSIS 3.1 は、スループットおよびスペクトル効率を高めるためのモードを導入する一方で、DOCSIS 3.0 との後方互換性も維持しています。Orthogonal Frequency Division Multiple Access（OFDMA）チャネルには次の特徴があります。

- 最大 80 Mhz の周波数範囲
- アップストリーム スペクトル 5 ～ 85 MHz
- 50 kHz のサブキャリア間隔

- 25 kHz のサブキャリア間隔

所定のサブキャリア間隔での OFDMA チャネルのサブキャリア数は、チャネル幅によって異なります。

チャネル幅	50kHz	25kHz
48MHz	960	1920
96MHz	1920	3840

（注） 同じポート ペアで SC-QAM と OFDMA を設定する場合、ポートごとに 45 Mhz 以下の OFDMA（Cisco IOS XE Everest リリース 16.6.1 ではポート ペアごとに 90 Mhz 以下）を設定することを推奨します。

変調プロファイル

グローバルに設定される OFDMA 変調プロファイルは、さまざまな間隔使用コード（IUC）に関する変調次数とパイロット パターンを定義します。また、変調プロファイルは、初期レンジングと詳細レンジングのパラメータを割り当てるためにも使用されます。

OFDMA チャネル除外バンド

ポート上のすべての OFDMA チャネルから特定の周波数の範囲を除外するには、**ofdma-frequency-exclusion-band** コマンドを使用します。

除外および未使用バンドは、OFDMA チャネルだけに適用されます。OFDMA チャネルは除外バンド内の周波数をまったく使用しません。そのため、このバンドにレガシー SC-QAM チャネルを配置できます。OFDMA チャネルは、 **ofdma-frequency-unused-band** コマンドで設定された未使用バンドの周波数をデータ トラフィックには使用しませんが、これらの周波数でプローブを送信することはできます。

OFDMA チャネルの設定方法

OFDMA 変調プロファイルの設定

OFDMA 変調プロファイルは、初期レンジング、詳細レンジング、およびデータ IUC のパラメータを設定するために使用されます。OFDMA チャネルに適用する OFDMA 変調プロファイルを定義するには、次の手順に従います。

enable
configure terminal

cable mod-profile-ofdma *id*
subcarrier-spacing *value*
initial-rng-subcarrier *value*
fine-rng-subcarrier *value*
data-iuc *id* **modulation** *value* **pilot-pattern** *value*
設定例は次のとおりです。

```
Router# enable
Router# configure terminal
Router(config)# cable mod-profile-ofdma 466
Router(config-ofdma-mod-profile)# subcarrier-spacing 50KHz
Router(config-ofdma-mod-profile)# initial-rng-subcarrier 64
Router(config-ofdma-mod-profile)# fine-rng-subcarrier 128
Router(config-ofdma-mod-profile)# data-iuc 13 modulation 1024-QAM pilot-pattern 2
Router(config-ofdma-mod-profile)# exit
Router(config)# cable mod-profile-ofdma 423
Router(config-ofdma-mod-profile)# subcarrier-spacing 25KHz
Router(config-ofdma-mod-profile)# initial-rng-subcarrier 64
Router(config-ofdma-mod-profile)# fine-rng-subcarrier 128
Router(config-ofdma-mod-profile)# data-iuc 6 modulation 1024-QAM pilot-pattern 8
Router(config-ofdma-mod-profile)# data-iuc 9 modulation 1024-QAM pilot-pattern 8
Router(config-ofdma-mod-profile)# data-iuc 10 modulation 512-QAM pilot-pattern 8
Router(config-ofdma-mod-profile)# data-iuc 11 modulation 256-QAM pilot-pattern 8
Router(config-ofdma-mod-profile)# data-iuc 12 modulation 128-QAM pilot-pattern 9
Router(config-ofdma-mod-profile)# data-iuc 13 modulation 64-QAM pilot-pattern 9
```

（注） サブキャリアの間隔は、それが設定されている各チャネル プロファイルのサブキャリア間隔と一致する必要があります。

OFDMA 変調プロファイルの設定の確認

OFDMA 変調プロファイルの設定を表示するには、次の例に示すように **show cable modulation-profile ofdma** コマンドを使用します。

```
Router# show cable modulation-profile ofdma
Mod  Subc     IUC type   Act  Preamble  Bit       Pilot
     Spacing             subc Symbols   Loading   Pattern
421  25KHz    3  (IR)    64      4
              4  (FR)    192     1
              13 (data)                 16-QAM    8

423  25KHz    3  (IR)    64      4
              4  (FR)    128     1
              6  (data)                 1024-QAM  8
              10 (data)                 512-QAM   8
              11 (data)                 256-QAM   8
              12 (data)                 128-QAM   9
              13 (data)                 64-QAM    9

461  50KHz    3  (IR)    32      4
              4  (FR)    192     1
              13 (data)                 16-QAM    1

466  50KHz    3  (IR)    64      4
              4  (FR)    128     1
              13 (data)                 1024-QAM  2
```

OFDMA チャネルの設定

OFDMA チャネルを設定するには、次の手順に従います。

enable
configure terminal
controller Upstream-Cable *slot/subslot/port*
us-channel *id* **docsis-mode ofdma**
us-channel *id* **subcarrier-spacing** *value*
us-channel *id* **frequency-range** *start-value end-value*
us-channel *id* **modulation-profile** *id*
us-channel *id* **cyclic-prefix** *value* **roll-off-period** *value*
us-channel *id* **symbols-per-frame** *value*
us-channel *id* **data-iuc** *id* **band** *start-value end-value* **modulation** *value* **pilot-pattern** *value*
設定例は次のとおりです。

```
Router# enable
Router# configure terminal
Router(config)# controller Upstream-Cable 1/0/4
Router(config-controller)# us-channel 12 docsis-mode ofdma
Router(config-controller)# us-channel 12 subcarrier-spacing 25KHz
Router(config-controller)# us-channel 12 frequency-range 40000000 85000000
Router(config-controller)# us-channel 12 modulation-profile 423
Router(config-controller)# us-channel 12 cyclic-prefix 640 roll-off-period 224
Router(config-controller)# us-channel 12 symbols-per-frame 9
Router(config-controller)# us-channel 12 data-iuc 9 band 50000000 60000000 modulation 512-QAM
 pilot-pattern 8
Router(config-controller)# no us-channel 12 shutdown
```

（注）

- OFDMA は us-channel 12 ～ 15 を使用します。
- OFDMA 設定オプションを有効にするには、docsis-mode を **ofdma** に変更します。us-channel 12 ～ 15 では、これらのオプションがデフォルトで有効になります。
- OFDMA チャネルが存在する場合、設定するアクティブ SC QAM の数を 4 つ以下にすることをお勧めします。
- コントローラごとに設定できる OFDMA チャネルの数は 1 つだけです。
- OFDMA チャネルは 40 ～ 85 Mhz の間でなければなりません。
- 多くの場合、オプションの値は互いに依存します。ある値を変更すると、他の値が変更されたり無効になったりする場合があります。
- 最初にサブキャリアの間隔と周波数範囲を設定することを推奨します。周波数の範囲は 50 kHz 刻みで設定する必要があります。
- 現在、C-QAM と OFDMA の周波数をオーバーラップさせることはできません。

OFDMA チャネル設定の確認

OFDMA チャネル設定を表示するには、次の例に示すように **show controllers upstream-Cable us-channel** コマンドを使用します。

```
Router# show controllers upstream-Cable 1/0/4 us-channel 12
USPHY OFDMA support: FULL


Controller 1/0/4 upstream 12  AdminState:UP OpState: UP
  ofdma mode enabled
  Channel Freq Range 35.500 MHz to 79.500 MHz
  Channel Subcarrier Index Range Cfg: 74, 953 Op: 74, 953
  Channel SC0 Freq Cfg: 31.800 MHz Op: 31.800 MHz
  #Excl bands: 2
  (   0,   73), ( 954, 2047),
  #Unused bands: 0
  Cyclic Prefix Size 96,  Rolloff Period Size 64
  Subcarrier Spacing 50KHz,  Symbols Per Frame 18 Subcarrier Per Minislot: 8

  Modulation Profile (ID 466, Subcarrier Spacing 50KHz)
    IUC type   Cfg   Act  Preamble Bit       Pilot
               subc  subc Symbols  Loading   Pattern
    3  (IR)    64    64      4       -         -
    4  (FR)    128   128     1       -         -
    13 (data)  -     -       -     1024-QAM    2
  Calculated Data burst profile:
  IUC  Group   Bit       Pilot   Start  Consec
               Loading   Pattern Mslot  Mslot
  13   0       1024-QAM  2       0       109

  #Total mslots:110 #Fine Rng capable:95 #Initial Rng capable:103
   Initial Rng - Freq 50.000MHz mslotOffset:36 #mslot in frame:8
  Minislot mapping:  mslot#(start_sc start_freq(Mhz) end_sc end_freq(Mhz)
   mslot type(E-Edge; B-Body; S-Share with SCQAM;
   I-Initial rng capable; F-Fine rng capable)
   (next Fine Rng capable minislot if current is not capable))
  0  (  74, 35.500,   81, 35.850, EIF ( - )), 1  (  82, 35.900,   89, 36.250, BIF ( - )),
  2  (  90, 36.300,   97, 36.650, BIF ( - )), 3  (  98, 36.700,  105, 37.050, BIF ( - )),
  4  ( 106, 37.100,  113, 37.450, BIF ( - )), 5  ( 114, 37.500,  121, 37.850, BIF ( - )),
  6  ( 122, 37.900,  129, 38.250, BIF ( - )), 7  ( 130, 38.300,  137, 38.650, BIF ( - )),
  8  ( 138, 38.700,  145, 39.050, BIF ( - )), 9  ( 146, 39.100,  153, 39.450, BIF ( - )),
  10 ( 154, 39.500,  161, 39.850, BIF ( - )), 11 ( 162, 39.900,  169, 40.250, BIF ( - )),
  12 ( 170, 40.300,  177, 40.650, BIF ( - )), 13 ( 178, 40.700,  185, 41.050, BIF ( - )),
  14 ( 186, 41.100,  193, 41.450, BIF ( - )), 15 ( 194, 41.500,  201, 41.850, BIF ( - )),
  16 ( 202, 41.900,  209, 42.250, BIF ( - )), 17 ( 210, 42.300,  217, 42.650, BIF ( - )),
  18 ( 218, 42.700,  225, 43.050, BIF ( - )), 19 ( 226, 43.100,  233, 43.450, BIF ( - )),
  20 ( 234, 43.500,  241, 43.850, BIF ( - )), 21 ( 242, 43.900,  249, 44.250, BIF ( - )),
  22 ( 250, 44.300,  257, 44.650, BIF ( - )), 23 ( 258, 44.700,  265, 45.050, BIF ( - )),
  24 ( 266, 45.100,  273, 45.450, BIF ( - )), 25 ( 274, 45.500,  281, 45.850, BIF ( - )),

  26 ( 282, 45.900,  289, 46.250, BIF ( - )), 27 ( 290, 46.300,  297, 46.650, BIF ( - )),
  28 ( 298, 46.700,  305, 47.050, BIF ( - )), 29 ( 306, 47.100,  313, 47.450, BIF ( - )),
  30 ( 314, 47.500,  321, 47.850, BIF ( - )), 31 ( 322, 47.900,  329, 48.250, BIF ( - )),
  32 ( 330, 48.300,  337, 48.650, BIF ( - )), 33 ( 338, 48.700,  345, 49.050, BIF ( - )),
  34 ( 346, 49.100,  353, 49.450, BIF ( - )), 35 ( 354, 49.500,  361, 49.850, BIF ( - )),
  36 ( 362, 49.900,  369, 50.250, BIF ( - )), 37 ( 370, 50.300,  377, 50.650, BIF ( - )),
  38 ( 378, 50.700,  385, 51.050, BIF ( - )), 39 ( 386, 51.100,  393, 51.450, BIF ( - )),
  40 ( 394, 51.500,  401, 51.850, BIF ( - )), 41 ( 402, 51.900,  409, 52.250, BIF ( - )),
  42 ( 410, 52.300,  417, 52.650, BIF ( - )), 43 ( 418, 52.700,  425, 53.050, BIF ( - )),
  44 ( 426, 53.100,  433, 53.450, BIF ( - )), 45 ( 434, 53.500,  441, 53.850, BIF ( - )),
  46 ( 442, 53.900,  449, 54.250, BIF ( - )), 47 ( 450, 54.300,  457, 54.650, BIF ( - )),
  48 ( 458, 54.700,  465, 55.050, BIF ( - )), 49 ( 466, 55.100,  473, 55.450, BIF ( - )),
  50 ( 474, 55.500,  481, 55.850, BIF ( - )), 51 ( 482, 55.900,  489, 56.250, BIF ( - )),
  52 ( 490, 56.300,  497, 56.650, BIF ( - )), 53 ( 498, 56.700,  505, 57.050, BIF ( - )),
  54 ( 506, 57.100,  513, 57.450, BIF ( - )), 55 ( 514, 57.500,  521, 57.850, BIF ( - )),
  56 ( 522, 57.900,  529, 58.250, BIF ( - )), 57 ( 530, 58.300,  537, 58.650, BIF ( - )),
  58 ( 538, 58.700,  545, 59.050, BIF ( - )), 59 ( 546, 59.100,  553, 59.450, BIF ( - )),
  60 ( 554, 59.500,  561, 59.850, BIF ( - )), 61 ( 562, 59.900,  569, 60.250, BIF ( - )),
  62 ( 570, 60.300,  577, 60.650, BIF ( - )), 63 ( 578, 60.700,  585, 61.050, BIF ( - )),
```

```
64 ( 586, 61.100,  593, 61.450, BIF ( - )), 65 ( 594, 61.500,  601, 61.850, BIF ( - )),
66 ( 602, 61.900,  609, 62.250, BIF ( - )), 67 ( 610, 62.300,  617, 62.650, BIF ( - )),
68 ( 618, 62.700,  625, 63.050, BIF ( - )), 69 ( 626, 63.100,  633, 63.450, BIF ( - )),
70 ( 634, 63.500,  641, 63.850, BIF ( - )), 71 ( 642, 63.900,  649, 64.250, BIF ( - )),
72 ( 650, 64.300,  657, 64.650, BIF ( - )), 73 ( 658, 64.700,  665, 65.050, BIF ( - )),
74 ( 666, 65.100,  673, 65.450, BIF ( - )), 75 ( 674, 65.500,  681, 65.850, BIF ( - )),
76 ( 682, 65.900,  689, 66.250, BIF ( - )), 77 ( 690, 66.300,  697, 66.650, BIF ( - )),
78 ( 698, 66.700,  705, 67.050, BIF ( - )), 79 ( 706, 67.100,  713, 67.450, BIF ( - )),
80 ( 714, 67.500,  721, 67.850, BIF ( - )), 81 ( 722, 67.900,  729, 68.250, BIF ( - )),
82 ( 730, 68.300,  737, 68.650, BIF ( - )), 83 ( 738, 68.700,  745, 69.050, BIF ( - )),
84 ( 746, 69.100,  753, 69.450, BIF ( - )), 85 ( 754, 69.500,  761, 69.850, BIF ( - )),
86 ( 762, 69.900,  769, 70.250, BIF ( - )), 87 ( 770, 70.300,  777, 70.650, BIF ( - )),
88 ( 778, 70.700,  785, 71.050, BIF ( - )), 89 ( 786, 71.100,  793, 71.450, BIF ( - )),
90 ( 794, 71.500,  801, 71.850, BIF ( - )), 91 ( 802, 71.900,  809, 72.250, BIF ( - )),
92 ( 810, 72.300,  817, 72.650, BIF ( - )), 93 ( 818, 72.700,  825, 73.050, BIF ( - )),
94 ( 826, 73.100,  833, 73.450, BIF ( - )), 95 ( 834, 73.500,  841, 73.850, BI  (0  )),
96 ( 842, 73.900,  849, 74.250, BI  (0  )), 97 ( 850, 74.300,  857, 74.650, BI  (0  )),
98 ( 858, 74.700,  865, 75.050, BI  (0  )), 99 ( 866, 75.100,  873, 75.450, BI  (0  )),
100( 874, 75.500,  881, 75.850, BI  (0  )), 101( 882, 75.900,  889, 76.250, BI  (0  )),
102( 890, 76.300,  897, 76.650, BI  (0  )), 103( 898, 76.700,  905, 77.050, B   (0  )),
104( 906, 77.100,  913, 77.450, B   (0  )), 105( 914, 77.500,  921, 77.850, B   (0  )),
106( 922, 77.900,  929, 78.250, B   (0  )), 107( 930, 78.300,  937, 78.650, B   (0  )),
108( 938, 78.700,  945, 79.050, B   (0  )), 109( 946, 79.100,  953, 79.450, B   (0  )),

Mapped to connector 4 and receiver 108

Bind to Cable1/0/4 US4
MER(SNR) - Unknown - no modems online.
Spectrum Group is unassigned
Nominal Input Power Level 0 dBmV

UCD procedures on lch 0
UCD ucd-proxy-timeout   (0   ) ucd-proxy-wrong-ack (0   )
```

除外/未使用バンドの設定

OFDMA チャネルは除外バンド内の周波数をまったく使用しません。OFDMA プローブは、未使用バンド内の周波数で送信されます。したがって、SC-QAM チャネルとの干渉を防ぐために除外バンドを使用する必要があります。除外/未使用バンドを設定するには、次の手順に従います。

enable
configure terminal
controller Upstream-Cable *slot/subslot/port*
cable ofdma-frequency-exclusion-band *start-value end-value*
cable ofdma-frequency-unused-band *start-value end-value*
設定例は次のとおりです。

```
Router# enable
Router# configure terminal
Router(config)# controller Upstream-Cable 1/0/2
Router(config-controller)# cable ofdma-frequency-exclusion-band 48000000 54200000
Router(config-controller)# cable ofdma-frequency-unused-band 50000000 52000000
Router(config-controller)# us-channel 12 docsis-mode ofdma
Router(config-controller)# us-channel 12 subcarrier-spacing 25KHz
Router(config-controller)# us-channel 12 modulation-profile 423
Router(config-controller)# us-channel 12 frequency-range 45000000 70000000
Router(config-controller)# us-channel 12 cyclic-prefix 96 roll-off-period 64
Router(config-controller)# us-channel 12 symbols-per-frame 18
```

除外/未使用バンドの確認

除外/未使用バンドの設定を表示するには、次の例に示すように **show controllers upstream-Cable us-channel** コマンドを使用します。

```
Router# show controllers upstream-Cable 1/0/2 us-channel 12
USPHY OFDMA support: FULL

Controller Exclusion Freq List:
( 40.000 MHz, 44.200 MHz),
Controller Unused Freq List:
( 50.000 MHz, 52.000 MHz),

Controller 1/0/9 upstream 12 AdminState:UP OpState: UP
ofdma mode enabled
Channel Freq Range 28.500 MHz to 69.500 MHz
Channel Subcarrier Index Range Cfg: 148, 1787 Op: 148, 1787
Channel SC0 Freq Cfg: 24.800 MHz Op: 24.800 MHz
#Excl bands: 3
( 0, 147), ( 608, 776), (1788, 4095),
#Unused bands: 3
( 596, 607), (1001, 1088), (1777, 1787),
```

チャネルごとの OFDMA プロファイルのオーバーライド

次のコマンドで示されているように、特定の OFDMA チャネル上の特定の IUC で使用する変調とパイロット パターンをオーバーライドできます。

enable
configure terminal
controller Upstream-Cable *slot/subslot/port*
us-channel *id* **data-iuc** *id* **band** *start-value end-value* **modulation** *value* **pilot-pattern** *value*
設定例は次のとおりです。

```
Router# enable
Router# configure terminal
Router(config)# controller Upstream-Cable 1/0/2
Router(config-controller)# us-channel 12 docsis-mode ofdma
Router(config-controller)# us-channel 12 subcarrier-spacing 25KHz
Router(config-controller)# us-channel 12 modulation-profile 423
Router(config-controller)# us-channel 12 frequency-range 28000000 70000000
Router(config-controller)# us-channel 12 cyclic-prefix 96 roll-off-period 64
Router(config-controller)# us-channel 12 symbols-per-frame 18
Router(config-controller)# us-channel 12 data-iuc 6 band 60000000 65000000 modulation 128-QAM
 pilot-pattern 9
Router(config-controller)# no us-channel 12 shutdown
```

（注） サブキャリア間隔の変更により変調プロファイルが変更される場合を含め、変調プロファイルが変更されると、オーバーライド値が US チャネルから削除されます。

オーバーライド設定の確認

オーバーライド設定を表示するには、次の例に示すように **show controllers upstream-Cable us-channel** コマンドを使用します。

```
Router# show controllers upstream-Cable 1/0/2 us-channel 12
 .....
   Modulation Profile (ID 423, Subcarrier Spacing 25KHz)
    IUC type    Cfg   Act  Preamble Bit       Pilot
                subc  subc Symbols  Loading   Pattern
    3   (IR)    64    64     4       -         -
    4   (FR)    128   128    1       -         -
    6   (data)  -     -      -     1024-QAM    8
    10  (data)  -     -      -     512-QAM     8
    11  (data)  -     -      -     256-QAM     8
    12  (data)  -     -      -     128-QAM     9
    13  (data)  -     -      -     64-QAM      9
  Overwrite Data Profile:
  IUC  Start      End        Start   End    Bit       Pilot
       Freq(MHz)  Freq(MHz)  Subc    Subc   Loading   Pattern
  6      60.0      65.0      1408    1608   128-QAM   9

  Calculated Data burst profile:
  IUC  Group   Bit        Pilot   Start  Consec
               Loading    Pattern Mslot  Mslot
  6    0       1024-QAM   8       0      61
  6    1       128-QAM    9       62     11
  6    2       1024-QAM   8       74     10
  10   0       512-QAM    8       0      84
  11   0       256-QAM    8       0      84
  12   0       128-QAM    9       0      84
  13   0       64-QAM     9       0      84
 ......
```

ケーブル インターフェイスへの OFDMA アップストリームの適用

アップストリーム チャネルに MAC ドメインを関連付けてアップストリーム ボンディングを設定するには、次の手順に従います。

enable
configure terminal
interface Cable *slot/subslot/interface*
cable upstream bonding-group *id*
upstream *id*
attributes *value*
cable bundle *id*

設定例は次のとおりです。

```
Router# enable
Router# configure terminal
Router(config)# interface Cable 1/0/4
Router(config-if)# downstream Integrated-Cable 1/0/4 rf-channel 0
Router(config-if)# downstream Integrated-Cable 1/0/4 rf-channel 16
Router(config-if)# upstream 0 Upstream-Cable 1/0/0 us-channel 0
Router(config-if)# upstream 1 Upstream-Cable 1/0/0 us-channel 1
Router(config-if)# upstream 2 Upstream-Cable 1/0/0 us-channel 2
Router(config-if)# upstream 3 Upstream-Cable 1/0/0 us-channel 3
Router(config-if)# upstream 6 Upstream-Cable 1/0/0 us-channel 12
Router(config-if)# cable upstream bonding-group 1
Router(config-upstream-bonding)# upstream 0
Router(config-upstream-bonding)# upstream 1
```

```
Router(config-upstream-bonding)# upstream 2
Router(config-upstream-bonding)# upstream 3
Router(config-upstream-bonding)# attributes 80000000
Router(config-upstream-bonding)# exit
Router(config-if)# cable upstream bonding-group 2
Router(config-upstream-bonding)# upstream 0
Router(config-upstream-bonding)# upstream 1
Router(config-upstream-bonding)# upstream 2
Router(config-upstream-bonding)# upstream 3
Router(config-upstream-bonding)# upstream 6
Router(config-upstream-bonding)# attributes 80000000
Router(config-upstream-bonding)# exit
Router(config-if)# cable bundle 1
```

DOCSIS 3.1 ケーブル モデムおよび OFDMA アップストリームを使用するケーブル モデムの判別

DOCSIS 3.1 ケーブル モデムを表示するには、次の例に示すように **show cable modem docsis version d31-capable** コマンドを使用します。

```
Router# show cable modem docsis version d31-capable
MAC Address    I/F            MAC              Reg Oper DSxUS DS   RCC    US
                              State            Ver Ver        OFDM ID     OFDMA
4800.33ea.7012 C1/0/0/UB      w-online(pt)     3.1 3.1  33x4  1    5      1
203d.66ae.4169 C1/0/0/UB      w-online(pt)     3.1 3.1  33x4  1    5      1
```

ケーブル モデムの DOCSIS PHY レイヤの情報を表示するには、次の例に示すように **show cable modem phy** コマンドを使用します。

```
Router# show cable modem 5039.5584.5bbe phy
MAC Address    I/F        Sid   USPwr  USMER Timing DSPwr  DSMER  Mode   DOCSIS
                                 (dBmV) (SNR) Offset (dBmV) (SNR)         Prov
                                        (dB)                (dB)
5039.5584.5bbe C1/0/0/U0  15    38.75  ----- 2282   0.00   -----  ofdma  1.1
```

OFDMA アップストリームを使用するケーブル モデムを表示するには、次の例に示すように **show cable modem phy** コマンドを使用します。

```
Router# show cable modem phy | include ofdma
5039.5584.5bbe C1/0/0/U0     15    38.75  ----- 2282    0.00  -----  ofdma  1.1
0895.2a9b.26f1 C1/0/0/U0     16    28.00  ----- 2146    0.00  -----  ofdma  1.1
```

OFDMA チャネルのキャパシティと使用状況を表示するには、次の例に示すように **show interface cable mac-scheduler** コマンドを使用します。

```
Router# show interfaces cable 1/0/2 mac-scheduler 6
     DOCSIS 1.1 MAC scheduler for Cable1/0/2/U6 : rate 279807192
     Max potential performance for each configured IUC type
     IUC: 6     rate: 279807192
     IUC: 10    rate: 263104848
     IUC: 11    rate: 233779840
     IUC: 12    rate: 203019328
     IUC: 13    rate: 173899376
     wfq:None
     us_balance:OFF
     dpon_mode:OFF
     fairness:OFF
     Queue[Rng Polls] flows 0
     Queue[CIR Grants] flows 0
     Queue[BE(07) Grants] flows 0
     Queue[BE(06) Grants] flows 0
     Queue[BE(05) Grants] flows 0
     Queue[BE(04) Grants] flows 0
     Queue[BE(03) Grants] flows 0
     Queue[BE(02) Grants] flows 0
     Queue[BE(01) Grants] flows 0
     Queue[BE(00) Grants] flows 0
     Req Slots 38510548
```

```
Req/Data Slots 1275
Init Mtn Slots 47832
Stn Mtn Slots 0
IUC 5 Slots 0
IUC 6 Slots 6378
IUC 9 Slots 0
IUC 10 Slots 254923830
IUC 11 Slots 220
IUC 12 Slots 4006
IUC 13 Slots 251213508
Avg upstream channel utilization : 0%
Avg upstream channel utilization in 30 sec : 0%
Avg percent contention slots : 96%
Avg percent initial ranging slots : 0%
Avg percent minislots lost on late MAPs : 0%

MAP TSS: lch_state 10, init_retries 0
         late_initial_maps 0, late_ucd_maps 0
         mac-phy tss errors 0, missed ccc 0
```

DOCSIS3.0 ATDMA チャネルでの DOCSIS3.1 アップストリーム OFDMA チャネル ボンディングの確認

Cisco IOS XE Everest 16.6.1 リリース以降、DOCSIS3.1 アップストリーム OFDMA チャネルを DOCSIS3.0 ATDMA チャネルとボンディングできるようになっています。ユーザがベストエフォート フロー以外のフローを使用する場合、OFDMA チャネルを 1 つ以上の ATDMA チャネルとボンディングすることを推奨します。Cisco IOS XE Everest 16.6.1 リリースでボンディングできるのは、最大 1 つの 1 OFDMA チャネルと最大 4 つの ATDMA チャネルであることに注意してください。

次の出力例には、OFDMA（チャネル 12）と ATDMA チャンネル（チャネル 0、1、2、3）の両方が含まれるボンディング グループ 8 が示されています。

```
interface Cable6/0/0
downstream Integrated-Cable 6/0/0 rf-channel 1
downstream Integrated-Cable 6/0/0 rf-channel 158
upstream 0 Upstream-Cable 6/0/0 us-channel 0
upstream 1 Upstream-Cable 6/0/0 us-channel 1
upstream 2 Upstream-Cable 6/0/0 us-channel 2
upstream 3 Upstream-Cable 6/0/0 us-channel 3
upstream 6 Upstream-Cable 6/0/0 us-channel 12
cable upstream bonding-group 1
  upstream 0
  upstream 1
  upstream 2
  upstream 3
  attributes 80000000
cable upstream bonding-group 8
  upstream 0
  upstream 1
  upstream 2
  upstream 3
  upstream 6
  attributes 80000000
cable bundle 1
cable privacy accept-self-signed-certificate
end
```

DOCSIS 3.1 OFDMA チャネル設定に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *92* : ***DOCSIS 3.1 OFDMA*** チャネル設定に関する機能情報

機能名	リリース	機能情報
DOCSIS 31 US 16 OFDMA チャネル サポート（ライン カードごと）	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。
DOCSIS 3.1 US OFDMA チャネル ボンディング（DOCSIS 3.0 ATDMA チャネル全体）	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 34 章

Time and Frequency Division Multiplexing の設定

このドキュメントでは、DOCSIS 3.1 アップストリーム チャネルの Time and Frequency Division Multiplexing（TaFDM）機能に関する Cisco cBR-8 シリーズ ルータのサポートについて説明します。

TaFDM サポートについて

Time and Frequency Division Multiplexing（TaFDM）方式を使用すると、DOCSIS 3.1 でオーバーラップ可能な OFDMA チャネルと SCQAM チャネルは、異なる時間にアップストリームを使用することもできます。TaFDM の実装では、OFDMA と SC QAM の両方が別々の周波数で同時に動作できます。また、同じ周波数で異なる時間に動作することもできます。

TaFDM はレガシー DOCSIS SC-QAM チャネルとの後方互換性を維持しながら、スペクトル全体で DOCSIS 機能を有効にします。

通常、TaFDM はコントローラ レベルで設定されます。ただし、実装されるのは MAC ドメイン レベルです。オーバーラップする複数のチャネルを異なる MAC ドメインにバインドすることはできません。

TaFDM を使用して、オーバーラップする SC-QAM チャネルと OFDMA チャネルをバインドすることができます。ただし、モデムが UGS フローでプロビジョニングされ、別の非オーバーラップ SC-QAM が使用可能でない場合にのみ、このようなボンディングを推奨します。

オーバーラップ SC-QAM チャネルでの UGS フローのパフォーマンスを向上させるには、OFDMA チャネルの設定でサブキャリア間隔 50kHz を指定し、フレームあたりのシンボル数と循環プレフィックスを低く設定してください。

OFDMA チャネル トラフィックのスループットを向上させるには、OFDMA チャネルの設定でサブキャリア間隔 25kHz を指定し、パイロット パターンを高く設定してください。

TaFDM サポートの設定に関する前提条件

TaFDM 構成を設定する際には、次の前提条件が適用されます。

- 同じポート上のすべてのオーバーラップ SC QAM チャネルおよび OFDMA チャネルを、同じ MAC ドメインにバインドする必要があります。
- OFDMA チャネル IM ゾーンで使用する、良好な信号品質の最小 0.8 ～ 3.2 MHz の OFDMA 専用スペクトルを予約しておきます。

TaFDM をサポートする cBR の設定方法

（注） このモジュールで参照されているコマンドの詳細については、「Cisco IOS Master Command List」を参照してください。

TaFDM 変調プロファイルの設定

TaFDM変調プロファイルは、初期レンジング、詳細レンジング、およびデータ IUC のパラメータを設定するために使用されます。TaFDM 変調プロファイルを定義するには、次の例に示すコンフィギュレーション コマンドを実行します。

```
cable mod-profile-ofdma 450
  subcarrier-spacing 25KHz
  initial-rng-subcarrier 64
  fine-rng-subcarrier 192
  data-iuc 9 modulation 1024-QAM pilot-pattern 11
  data-iuc 10 modulation 512-QAM pilot-pattern 11
  data-iuc 11 modulation 256-QAM pilot-pattern 8
  data-iuc 12 modulation 128-QAM pilot-pattern 8
  data-iuc 13 modulation 64-QAM pilot-pattern 8

cable mod-profile-ofdma 470
  subcarrier-spacing 50KHz
  initial-rng-subcarrier 64
  fine-rng-subcarrier 192
  data-iuc 9 modulation 1024-QAM pilot-pattern 1
  data-iuc 10 modulation 512-QAM pilot-pattern 1
  data-iuc 11 modulation 256-QAM pilot-pattern 1
  data-iuc 12 modulation 128-QAM pilot-pattern 1
  data-iuc 13 modulation 64-QAM pilot-pattern 1
```

TaFDM の I/O コントローラの設定

次の設定例では、SC-QAM アップストリーム チャネルのエリア内に共有領域を定義します。

```
controller Upstream-Cable slot/subslot/port
  us-channel 0 frequency 35800000
```

```
 us-channel 0 channel-width 6400000 6400000
 us-channel 0 docsis-mode atdma
 us-channel 0 minislot-size 2
 us-channel 0 modulation-profile 221
 us-channel 0 equalization-coefficient
 no us-channel 0 shutdown
 us-channel 1 frequency 29400000
 us-channel 1 channel-width 6400000 6400000
 us-channel 1 docsis-mode atdma
 us-channel 1 minislot-size 2
 us-channel 1 modulation-profile 221
 us-channel 1 equalization-coefficient
 no us-channel 1 shutdown
 us-channel 2 frequency 23000000
 us-channel 2 channel-width 6400000 6400000
 us-channel 2 docsis-mode atdma
 us-channel 2 minislot-size 2
 us-channel 2 modulation-profile 221
 us-channel 2 equalization-coefficient
 no us-channel 2 shutdown
 us-channel 3 frequency 16600000
 us-channel 3 channel-width 6400000 6400000
 us-channel 3 docsis-mode atdma
 us-channel 3 minislot-size 2
 us-channel 3 modulation-profile 221
 us-channel 3 equalization-coefficient
 no us-channel 3 shutdown
```

OFDMA チャネル スループットの強化

次に、OFDMA チャネル スループットを強化する例を示します。

```
controller Upstream-Cable 1/0/0
  …
  us-channel 12 docsis-mode ofdma
  us-channel 12 subcarrier-spacing 25KHz
  us-channel 12 modulation-profile 450
  us-channel 12 frequency-range 10000000 85000000    #Overlap with SC-QAM channels
  us-channel 12 initial-rng-frequency-start 50000000    # Specify the preferred start
frequency for IM zone
  us-channel 12 cyclic-prefix 96 roll-off-period 64
  us-channel 12 symbols-per-frame 9
  no us-channel 12 shutdown
```

SC-QAM チャネル UGS フローのパフォーマンス強化

次に、SC-QAM チャネルの UGS フローのパフォーマンスを強化する例を示します。

```
controller Upstream-Cable 1/0/0
  …
  us-channel 12 docsis-mode ofdma
  us-channel 12 subcarrier-spacing 50KHz
  us-channel 12 modulation-profile 470
  us-channel 12 frequency-range 10000000 85000000    #Overlap with SC-QAM channels
  us-channel 12 initial-rng-frequency-start 50000000   #Specify the preferred frequency for
 IM zone
  us-channel 12 cyclic-prefix 96 roll-off-period 64
  us-channel 12 symbols-per-frame 8
  no us-channel 12 shutdown
```

ケーブル インターフェイス MAC ドメインの設定

次に、MAC ドメインのケーブル インターフェイスを設定する例を示します。

```
interface Cable1/0/0
  load-interval 30

  upstream 0 Upstream-Cable 1/0/0 us-channel 0
  upstream 1 Upstream-Cable 1/0/0 us-channel 1
  upstream 2 Upstream-Cable 1/0/0 us-channel 2
  upstream 3 Upstream-Cable 1/0/0 us-channel 3
  upstream 6 Upstream-Cable 1/0/0 us-channel 12
  cable upstream bonding-group 1
    upstream 0
    upstream 1
    upstream 2
    upstream 3
    attributes 80000000
  cable upstream bonding-group 2
    upstream 0
    upstream 1
    upstream 2
    upstream 3
    upstream 6
    attributes 80000000
  cable bundle 1
  cable sid-cluster-group num-of-cluster 2     #Maximize single modem throughput
  cable sid-cluster-switching max-request 4
  cable cm-status enable 3 6-11 16-18 20-27
  cable privacy accept-self-signed-certificate
```

サービス クラスの設定

次に、サービス クラスを設定する例を示します。

```
cable service class 198 name mega_up
cable service class 198 upstream
cable service class 198 max-concat-burst 16384
cable service class 198 max-rate 1000000000    # Maximize single modem throughput
cable service class 198 max-burst 250000
cable service class 198 priority 0
cable service class 198 peak-rate 0
```

TaFDM からの周波数帯域の除外

SC-QAM に特定の周波数範囲だけを使用させるには、次の例のようなコマンドを使用して、特定のバンドを除外するように Cisco cBR を設定します。

```
controller Upstream-Cable slot/subslot/port
 cable frequency-exclusion-band 18700000 22100000
```

TaFDM 設定の確認

次に、TaFDM 設定を確認する例を示します。

```
# show controllers upstream-Cable slot/subslot/port us-channel uschan-number-in-controller

#show controllers upstream-Cable slot/subslot/port us-channel uschan-number-in-controller
cdm-ump

# show interfaces cable slot/subslot/port mac-scheduler uschan-number-in-mac-domain
```

設定例

TaFDM 設定

```
controller Upstream-Cable 1/0/0
  us-channel 0 frequency 15000000
  us-channel 0 channel-width 3200000 3200000
  us-channel 1 frequency 22000000
  us-channel 1 channel-width 6400000 6400000
  us-channel 2 frequency 29000000
  us-channel 2 channel-width 6400000 6400000
  us-channel 3 frequency 36000000
  us-channel 3 channel-width 6400000 6400000
  us-channel 4 frequency 11000000
  us-channel 4 channel-width 1600000 1600000
  us-channel 12 frequency-range 5000000 85000000
```

TaFDM 設定に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *93* : *TaFDM* 設定についての機能情報

機能名	リリース	機能情報
TaFDM 設定	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに追加されました。

第 35 章

DOCSIS 3.1 アップストリーム プロファイルの選択

DOCSIS 3.1 では、OFDMA チャネル用のアップストリーム プロファイルの概念が導入されています。このドキュメントでは、Cisco cBR シリーズ コンバージド ブロードバンド ルータ上で DOCSIS 3.1 アップストリーム プロファイルの選択機能を設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *94* : ***Cisco cBR*** シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

アップストリーム プロファイルについて

変調プロファイルとは、OFDMAチャネルに定義された間隔使用コード（IUC）のリストのことです。IUC ごとに、変調次数とパイロット パターンが指定されています。変調プロファイルに含まれる複数の IUC に、同じ OFDMA チャネル上の異なる変調次数を設定できます。CMTS では、ミニスロットごとに異なる変調次数を割り当てた複数のプロファイルを定義し、それらのプロファイルを 1 つの OFDMA チャネルで使用することができます。

プロファイルを表示するには、次のコマンドを使用します。

- ケーブル モデム（CM）に関連付けられているプロファイルを表示するには、**show cable modem** *[ip-address| mac-address| cable| {slot | subslot | cable-interface-index}]***phy ofdm-profile upstream** コマンドを使用します。

- 特定のケーブル モデルに関連付けられている詳細なプロファイル管理データを表示するには、**show cable modem***[ip-address| mac-address]***prof-mgmt upstream** コマンドを使用します。

CMTS では、さまざまな CM グループに異なるデータ IUC を割り当てることができます。

DOCSIS 3.1 CM が 1 つのチャネルで使用できるアクティブな OFDMA アップストリーム データ プロファイル IUC は 2 つだけです。

デフォルトのデータ IUC

データ IUC 13 は最も堅牢な IUC であり、すべてのケーブル モデムでこれを使用できます。

推奨される間隔使用コード（IUC）

アップストリームのプロービング中に定期的に収集される Receive Modulation Error Ratio（RxMER）値に基づき、CMTS は既存の IUC の中から、許容されるエラー レートで CMTS がコード ワードを受信できる十分な信号対雑音比（SNR）マージンを持つ、最も高速な IUC を最大で 2 つ見つけます。**show cable modem phy ofdm-profile upstream** コマンドは、CM ごとに 1 つまたは 2 つの推奨 IUC を表示します。

Cisco IOS XE Everest 16.6.1 リリースでは、データ IUC 13 は CM に割り当てられたいずれかの IUC になります。

自動プロファイル ダウングレードを無効にするには、グローバル コンフィギュレーション モードで **no cable upstream ofdma-prof-mgmt prof-upgrade-auto** コマンドを使用します。

アップストリーム プロファイルの設定方法

RxMER とビット ロードのマッピングの設定

Receive Modulation Error Ratio（RxMER）値をビット ロード値にマップするには、さまざまな方法があります。シスコでは、DOCSIS 3.1 OSSI で推奨されている次のマッピングをベースライン マッピングとして使用します。

RxMER（¼ DB 単位）	QAM	ビット ロード
60	16	4
84	64	6
96	128	7
108	256	8
122	512	9

RxMER（¼ DB 単位）	QAM	ビット ロード
136	1024	10
148	2048	11
164	4096	12
184	8192	13
208	16384	14

- RxMER からビット ロードへのマッピングを調整するためのマージンを設定するには、次のコマンドを使用します。
  `Router(config)# cable upstream ofdma-prof-mgmt mer-margin-qdb interval-in-minutes`
  上記のマッピング表が使用される前に、この設定値（*quarter-DB*）が、CMTS で収集された RxMER 値に加算されます。こうして、ユーザは推奨プロファイルを選択する際により適切に制御できます。
- 推奨プロファイルの計算で無視できる、ミニスロット平均 RxMER のパーセンテージを指定するには、次のコマンドを使用します。
  `Router(config)# cable upstream ofdma-prof-mgmt exempt-mslot-pct percent`
  これは、外れ値を無視できるエクステントを指定する方法になります。
- RxMER ポーリング間隔を設定するには、次のコマンドを使用します。
  `Router(config)# cable upstream ofdma-prof-mgmt rxmer-poll-interval interval-in-minutes`
  CMTS はアップストリーム プロービングを使用して、CM ごとの RxMER データを収集します。これは登録時だけでなく、登録後も定期的に行われます。収集された RxMER データでミニスロットあたりの平均が算出され、各 CM の推奨 IUC を計算するためにそれが使用されます。

アップストリーム プロファイルの選択機能について

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *95* : アップストリーム プロファイルの選択機能について

機能名	リリース	機能情報
DOCSIS3.1 US プロファイル選択	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 36 章

ダウンストリーム パワー チルト

ダウンストリーム パワー チルト機能は、ヘッドエンドのケーブル損失を修正して、コントローラ ポート上のすべてのチャネルでパワー スペクトルを一定にするために使用されます。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *96*：***Cisco cBR*** シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

ダウンストリーム パワー チルトについて

ダウンストリームパワーチルト機能は、ヘッドエンドのケーブル損失を修正して、コントローラポート上のすべてのチャネルでパワー スペクトルを一定にするために使われます。

（注） この機能を有効にすると、フェイルオーバー パス（ラインカード スイッチオーバーの後）でノイズ レベル劣化が発生することがあります。

ダウンストリーム電力プロファイルの設定に関する制限事項

ダウンストリーム パワー チルト機能と OFDM 電力プロファイル機能は相互排他的です。この 2 つを同時に設定することはできません。

ダウンストリーム パワー チルトの設定方法

ダウンストリーム パワー チルトの設定

ダウンストリーム パワー チルトはダウンストリームのすべての SCQAM チャネルまたは OFDM チャネルに適用されます。コントローラ ポートのダウンストリーム パワー チルトを設定するには、ダウンストリーム コントローラ ポートで power-tilt コンフィギュレーション コマンドを使用します。

enable
configure terminal
controller Integrated-Cable *slot/subslot/port*
max-ofdm-spectrum *value*
max-carrier *value*
base-channel-power *value*
power-tilt *mode loss* **max-frequency** *freq-max*
rf-chan *start_id* [*end_id*]
type *value*
rf-output *value*
power-adjust *value*
qam-profile*id*
docsis-channel-id*id*
ofdm channel-profile *id* **start-frequency** *value* **width** *value* [**plc** *value*]
次に例を示します。

```
controller Integrated-Cable 3/0/0
  max-ofdm-spectrum 192000000
  max-carrier 32
  base-channel-power 34
  power-tilt linear 4.0 max-frequency 696000000
  rf-chan 0 31
    type DOCSIS
    frequency 261000000
    rf-output NORMAL
    power-adjust -2.0
    qam-profile 1
    docsis-channel-id 1
  rf-chan 158
    power-adjust 0
    docsis-channel-id 159
    ofdm channel-profile 20 start-frequency 600000000 width 96000000 plc 645000000
```

上記の設定手順で使用されるコマンド **power-tilt** *mode loss* **max-frequency** *freq-max* の中で、*mode* は、*freq-max* における損失が既知である場合、周波数 F での同軸ケーブルの損失を計算する式を表します。次の 2 つのオプションから選択できます。

- linear：$loss_F = loss_{freq\text{-}max} * (F / freq\text{-}max)$
- cable-loss-approx：$loss_F = loss_{freq\text{-}max} * SQRT((freq\text{-}max - F) / freq\text{-}max)$

loss は、*freq-max* で測定されるケーブル損失です（1/10 dB 単位で指定）。

ダウンストリーム パワー チルトの設定の確認

ダウンストリーム パワー チルトの詳細を表示するには、次の例に示すように **show cable controller integrated-cable** コマンドを使用します。このコマンドにより、DS パワー チルト コマンドによって設定された実際の SCQAM および OFDM チャネル電力レベルが表示されます。OFDM チャネルの場合、表示される電力レベルは中心周波数 6 MHz バンドの電力レベルを表します。

```
Router# show controller Integrated-Cable 1/0/1 rf-chan 0-162
Chan State Admin Frequency Type   Annex Mod srate Interleaver dcid power output
0    UP    UP    261000000 DOCSIS B     256 5361  I32-J4      1    29.9  NORMAL
1    UP    UP    267000000 DOCSIS B     256 5361  I32-J4      2    30.0  NORMAL
2    UP    UP    273000000 DOCSIS B     256 5361  I32-J4      3    30.0  NORMAL
3    UP    UP    279000000 DOCSIS B     256 5361  I32-J4      4    30.0  NORMAL
4    UP    UP    285000000 DOCSIS B     256 5361  I32-J4      5    30.1  NORMAL
5    UP    UP    291000000 DOCSIS B     256 5361  I32-J4      6    30.1  NORMAL
6    UP    UP    297000000 DOCSIS B     256 5361  I32-J4      7    30.2  NORMAL
7    UP    UP    303000000 DOCSIS B     256 5361  I32-J4      8    30.2  NORMAL
8    UP    UP    309000000 DOCSIS B     256 5361  I32-J4      9    30.2  NORMAL
9    UP    UP    315000000 DOCSIS B     256 5361  I32-J4      10   30.3  NORMAL
10   UP    UP    321000000 DOCSIS B     256 5361  I32-J4      11   30.3  NORMAL
11   UP    UP    327000000 DOCSIS B     256 5361  I32-J4      12   30.3  NORMAL
12   UP    UP    333000000 DOCSIS B     256 5361  I32-J4      13   30.4  NORMAL
13   UP    UP    339000000 DOCSIS B     256 5361  I32-J4      14   30.4  NORMAL
14   UP    UP    345000000 DOCSIS B     256 5361  I32-J4      15   30.4  NORMAL
15   UP    UP    351000000 DOCSIS B     256 5361  I32-J4      16   30.5  NORMAL
16   UP    UP    357000000 DOCSIS B     256 5361  I32-J4      17   30.5  NORMAL
17   UP    UP    363000000 DOCSIS B     256 5361  I32-J4      18   30.5  NORMAL
18   UP    UP    369000000 DOCSIS B     256 5361  I32-J4      19   30.6  NORMAL
19   UP    UP    375000000 DOCSIS B     256 5361  I32-J4      20   30.6  NORMAL
20   UP    UP    381000000 DOCSIS B     256 5361  I32-J4      21   30.6  NORMAL
21   UP    UP    387000000 DOCSIS B     256 5361  I32-J4      22   30.7  NORMAL
22   UP    UP    393000000 DOCSIS B     256 5361  I32-J4      23   30.7  NORMAL
23   UP    UP    399000000 DOCSIS B     256 5361  I32-J4      24   30.7  NORMAL
24   UP    UP    405000000 DOCSIS B     256 5361  I32-J4      25   30.8  NORMAL
25   UP    UP    411000000 DOCSIS B     256 5361  I32-J4      26   30.8  NORMAL
26   UP    UP    417000000 DOCSIS B     256 5361  I32-J4      27   30.8  NORMAL
27   UP    UP    423000000 DOCSIS B     256 5361  I32-J4      28   30.9  NORMAL
28   UP    UP    429000000 DOCSIS B     256 5361  I32-J4      29   30.9  NORMAL
29   UP    UP    435000000 DOCSIS B     256 5361  I32-J4      30   30.9  NORMAL
30   UP    UP    441000000 DOCSIS B     256 5361  I32-J4      31   30.9  NORMAL
31   UP    UP    447000000 DOCSIS B     256 5361  I32-J4      32   31.0  NORMAL

Chan State Admin Mod-Type Start     Width    PLC       Profile-ID dcid power output Frequency

158  UP    UP    OFDM     600000000 96000000 645000000 22         159  33.9         NORMAL
```

ダウンストリーム パワー チルトに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *97*：ダウンストリーム パワー チルトに関する機能情報

機能名	リリース	機能情報
ダウンストリーム パワー チルト	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に導入されました。

第 37 章

コントローラ プロファイルの設定

このドキュメントでは、Cisco cBR シリーズ コンバージドブロードバンドルータ上でコントローラ プロファイルを設定する方法について説明します。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *98*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

コントローラ プロファイル設定に関する情報

同じデバイス内で CMTS 機能と UEQAM 機能がマージされて密度が高くなると、現在のコントローラ設定方法では過度に複雑かつ困難になります。設定の中で同じ行があまりに多くなります。

コントローラの設定を単純化するために、コントローラ プロファイルと呼ばれる新しい概念が導入されました。コントローラ プロファイルは、ダウンストリームとアップストリームのコントローラに適用する設定パラメータからなるグループで、次のような利点があります。

- 迅速な導入
- cBR-8 の展開、設定、トラブルシューティングの簡素化
- ノード/地域間で共通の設定
- 共通機能に関するシスコ製品全体での一貫性

コントローラ プロファイルの設定方法

I-CMTS コントローラを設定するには、デフォルトでレガシー コントローラ コンフィギュレーション コマンドが使用されます。I-CMTS コントローラ プロファイルを使用する場合には、最初に **cable controller-profile I-CMTS enable** コマンドを使用してそのプロファイルを有効にする必要があります。

（注）

- プロファイルを使用してコントローラを設定する場合、統合ケーブル コントローラとアップストリーム ケーブル コントローラでレガシー コマンドがまったく設定されていない状態の「クリーン」なCMTSで設定を開始することを推奨します。レガシー設定とプロファイルとを切り替えないでください。
- コントローラ プロファイルに変更を加えると、関連するすべてのコントローラが変更されます。したがって、特定のコントローラを設定する場合（たとえばコントロールのベース チャネル電力を変更する場合）、このコントローラを他のコントローラとともにプロファイルにバインドしないでください。
- I-CMTS コントローラ プロファイルが有効になっている場合、レガシー コントローラ コンフィギュレーション コマンドはサポートされません。
- I-CMTS コントローラ プロファイルが有効になっている場合、running-config でレガシー コントローラの設定を表示することはできません。

ダウンストリーム コントローラ プロファイルの設定

ダウンストリーム コントローラ プロファイルを設定するには、次の手順に従います。

enable
configure terminal
cable downstream controller-profile *id* **[RPHY|I-CMTS]**
base-channel-power *value*
max-carrier *value*
freq-profile *id*
max-ofdm-spectrum *value*
ofdm-freq-excl-band start-frequency *value* **width***value*
rf-chan *start_id* [*end_id*]
type *value*
rf-output *value*
power-adjust *value*
qam-profile*id*
docsis-channel-id*id*
power-profile *id*
ofdm channel-profile *id* **start-frequency** *value* **width** *value* [**plc** *value*]

enable
configure terminal

controller integrated-cable *slot/subslot/port*
profile *id*
次に例を示します。

```
cable downstream controller-profile 0 I-CMTS
 max-carrier 32
 base-channel-power 34
 rf-chan 0 3
  type DOCSIS
  frequency 111000000
  rf-output NORMAL
  qam-profile 1
  docsis-channel-id 1

controller integrated-cable 2/0/0
 profile 0
```

（注）

- 新しい I-CMTS コントローラ プロファイルを設定する場合は、キーワード I-CMTS が必要です。RPHY と入力した場合、またはキーワードを入力しない場合、システムは RPHY コントローラ プロファイルであると見なします。プロファイル タイプ（RPHY/I-CMTS）を設定した後は、タイプを変更できなくなります。
- プロファイルを更新すると、バインドされているすべてのコントローラが影響を受けます。コントローラにバインドされているプロファイルを削除するには、その前に、すべてのコントローラをアンバインドする必要があります。コントローラがアンバインドされると、コントローラ内の RF チャネル設定がすべて削除されます。

ダウンストリーム コントローラ プロファイルの設定の確認

ダウンストリーム コントローラ プロファイルの設定を確認するには、**show cable downstream controller-profile** コマンドを使用します。

```
Router# show cable downstream controller-profile 0
Downstream controller-profile 0, type I-CMTS
Description:
Downstream controller-profile 0 is being used by controller Integrated-Cable:
  2/0/0,
  Admin:  UP
  MaxOfdmSpectrum: 192000000
  MaxCarrier: 128
  BasePower: 33.0 dBmV
  Mode: normal
  Frequency profile: unconfigured
  DS Splitting: No
  OFDM frequency exclusion bands: None

Configured RF Channels:
Chan Admin Frequency  Type        Annex Mod  srate Qam-profile  dcid  power output
 0    UP   213000000  DOCSIS       B    256   5361  1           1     33.0  NORMAL
 1    UP   219000000  DOCSIS       B    256   5361  1           2     33.0  NORMAL
 2    UP   225000000  DOCSIS       B    256   5361  1           3     33.0  NORMAL
 3    UP   231000000  DOCSIS       B    256   5361  1           4     33.0  NORMAL
 4    UP   237000000  DOCSIS       B    256   5361  1           5     33.0  NORMAL
 5    UP   243000000  DOCSIS       B    256   5361  1           6     33.0  NORMAL
```

上記の出力では、integrated-cable 2/0/0 にプロファイル 0 が関連付けられています。したがって、**show controllers integrated-Cable 2/0/0 rf-channel 0 5** の出力は上記の出力と一致するはずです。次の例を参照してください。

```
Router# show controllers integrated-cable 2/0/0 rf-channel 0-5
...
Chan Admin Frequency  Type        Annex Mod  srate Qam-profile  dcid  power output
 0    UP   213000000  DOCSIS       B    256   5361  1           1     33.0  NORMAL
 1    UP   219000000  DOCSIS       B    256   5361  1           2     33.0  NORMAL
 2    UP   225000000  DOCSIS       B    256   5361  1           3     33.0  NORMAL
 3    UP   231000000  DOCSIS       B    256   5361  1           4     33.0  NORMAL
 4    UP   237000000  DOCSIS       B    256   5361  1           5     33.0  NORMAL
 5    UP   243000000  DOCSIS       B    256   5361  1           6     33.0  NORMAL
```

プロファイル内のパラメータが設定済みパラメータと一致するかどうかを確認するには、次の例に示すように **show running-config [all] | section cable downstream controller-profile** コマンドを使用します。

```
Router# show running-config | section downstream controller-profile
cable downstream controller-profile 0 I-CMTS
 max-carrier 32
 base-channel-power 34
 rf-chan 0 3
  type DOCSIS
  frequency 111000000
  rf-output NORMAL
  qam-profile 1
  docsis-channel-id 1
```

アップストリーム コントローラ プロファイルの設定

アップストリーム コントローラ プロファイルを設定するには、次の手順に従います。

enable
configure terminal
cable upstream controller-profile *id* **[RPHY|I-CMTS]**
us-channel *id* {**chan-class-id** *id* | **channel-width** {*first-choice-width* [*last-choice-width*]} | **docsis-mode** {**atdma| tdma| tdma-atdma**} | **equalization-coefficient** | **frequency***value* | **hop-priority** {**frequency modulation channel-width| modulation frequency channel-width| frequency channel-width modulation**} | **ingress-nosie-cancellation** *interval* | **maintain-psd** | **max-logical-chans** *id* | **minislot-size** *value* | **modulation-profile** *primary-profile-number* [*secondary-profile-number*] [*tertiary-profile-number*] | **power-level** *value* | **rng-holdoff** *priority* | **specsvl error-adaptive-profile** *id* | **spectrum-group** *id* | **threshold** {**cnr-profiles** *value* [*value*] | **corr-fec** *value* | **hysteresis** *value* | **snr-profiles** *value* [*value*] | **corr-fec** *value*}

enable
configure terminal
controller upstream-cable *slot/subslot/port*
profile *id*

（注）
- 新しい I-CMTS コントローラ プロファイルを設定する場合は、キーワード I-CMTS が必要です。RPHY と入力した場合、またはキーワードを入力しない場合、システムは RPHY コントローラ プロファイルであると見なします。プロファイル タイプ（RPHY/I-CMTS）を設定した後は、タイプを変更できなくなります。
- プロファイルを更新すると、バインドされているすべてのコントローラが影響を受けます。コントローラにバインドされているプロファイルを削除するには、その前に、すべてのコントローラをアンバインドする必要があります。
- OFDMA は、このリリースではプロファイルの使用をサポートしていません。

アップストリーム コントローラ プロファイルの設定の確認

アップストリーム コントローラ プロファイルの設定を確認するには、**show cable upstream controller-profile** コマンドを使用します。

```
Router# show cable upstream controller-profile 0
Upstream controller-profile 0, type I-CMTS
Description:
Upstream controller-profile 0 is being used by controller Upstream-Cable:
9/0/0

Controller Upstream-Cable
    ...
  Upstream-channel 0
    chan-class-id                  : 0x0
    channel-width                  : 1600000 1600000
    docsis-mode                    : atdma
    equalization-coefficient       : TRUE
    frequency                      : 5000000
    ...
    modulation-profile             : 221
    ...
    shutdown                       : FALSE
    ...
```

上記の出力では、upstream-cable 9/0/0 にプロファイル 0 が関連付けられています。したがって、**show controllers upstream-Cable 9/0/0 us-channel 0** の出力は上記の出力と一致するはずです。次の例を参照してください。

```
Router# show controllers upstream-Cable 9/0/0 us-channel 0
...
Controller 9/0/0 upstream 0  AdminState:UP OpState: UP
  atdma mode enabled
  Frequency 5.000 MHz, Channel Width 1.600 MHz, Symbol Rate 1.280 Msps
  Modulation Profile Group 221
```

プロファイル内のパラメータが設定済みパラメータと一致するかどうかを確認するには、次の例に示すように **show running-config [all] | section cable upstream controller-profile** コマンドを使用します。

```
Router# show running-config | s cable upstream controller-profile 0
cable upstream controller-profile 0 I-CMTS
 us-channel 0 channel-width 1600000 1600000
 us-channel 0 docsis-mode atdma
 us-channel 0 minislot-size 4
 us-channel 0 modulation-profile 221
```

```
us-channel 0 shutdown
...
```

コントローラ プロファイル設定に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *99*：コントローラ プロファイル設定に関する機能情報

機能名	リリース	機能情報
SG ベース コンフィギュレーション（OpSimp）フェーズ 2	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に導入されました。

第 38 章

AC 電源モジュール モード コントロールの電圧しきい値

このドキュメントでは、AC 電源モジュール（PSM）のモードを切り替えるための電圧しきい値の設定方法を説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *100* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

AC PSM モード コントロールの電圧しきい値について

電圧しきい値を設定すると、ACPSMで提供される電力バジェットが現場交換可能ユニット（FRU）に十分な電源を供給できない場合に、さまざまなモードを切り替えることができます。

AC PSM モード コントロールの電圧しきい値の概要

AC PSM は、120V または 220V のいずれかのモードで動作できます。

70V ～ 197V の入力電圧では、PSM は 120V モード、電力容量 1300W で動作します。入力電圧が 85V を下回ると、PSM は完全にオフになって電力容量が 0W になります。

入力電圧が 197V を上回ると、PSM は 220V モード、電力容量 3000W で動作します。入力電圧が 190V を下回ると、PSM は 120V モードに切り替わり、その電力容量は 1300W に低下します。

ユーザがモードの切り替えを設定できるよう、2 つの新しいヒステリシスしきい値 Voff_3000W および Von_3000W が提供されています。PSM がモードを切り替える条件を定義するこれらのヒステリシスしきい値は、CLI コマンドを使用して設定できます。

たとえば、*Voff_3000W* が 180V と設定される場合、入力電圧が 180V を下回ると、PSM が 120V モードに切り替わり、その電力容量は 1300W になります。*Von_3000W* が 200V と設定されている場合、入力電圧が 200V を上回ると PSM が 220V モードに切り替わります。.

表 *101*：モード コントロールの電圧しきい値

しきい値	デフォルト値	設定可能な範囲
Voff_3000W	190V	Voff_3000W に設定できる値は 170V 以上です。 Von_3000W に設定できる値は 200V 以下です。 Voff_3000W の値を Von_3000W の値より小さくする必要があります。
Von_3000W	197V	

AC PSM モード コントロールの電圧しきい値の設定方法

AC PSM モード コントロールの電圧しきい値の設定

電圧しきい値を設定するには、次のように **platform power protection ac220v voff von** コマンドを実行します。

```
Router# configure terminal
platform power protection ac220v voff von
```

デフォルトの電圧しきい値を使用するには、次のように **no platform power protection ac220v** コマンドを実行します。

```
Router# configure terminal
no platform power protection ac220v
```

（注） デフォルトでは、サービス停止を回避するために電源保護アクションが無効にされています。保護アクションが無効にされていると、電力バジェットが不足してもオンライン FRU の電源はオフになりませんが、新しくインストールされたライン カードの電源がオンになりません。

電源保護アクションを有効にするには、**platform power protection action shutdown linecard** コマンドを実行します。

```
Router# configure terminal
platform power protection action shutdown linecard
```

AC PSM モード コントロールの電圧しきい値の検証

電圧しきい値の設定を確認するには、次の例に示すように **sh run** コマンドを使用します。

```
Router# configure terminal
Router (config)# sh run | i protection
platform power protection ac220v 180 200
```

設定例

ここでは、電圧しきい値機能の設定例を記載します。

例：AC PSM モード コントロールの電圧しきい値の設定

次に、電圧しきい値を設定する例を示します。

```
Router# configure terminal
platform power protection ac220v 180 200
```

次に、DPS を無効にする例を示します。

```
Router# configure terminal
no platform power protection ac220v
```

AC PSM モード コントロールの電圧しきい値に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *102* : ***AC PSM*** モード コントロールの電圧しきい値に関する機能情報

機能名	リリース	機能情報
AC PSM モード コントロールの電圧しきい値	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に導入されました。

第 V 部

レイヤ 2 およびレイヤ 3 の VPN 構成

第 39 章

L2VPN Support over Cable

Cisco CMTS の Layer 2 VPN（L2VPN）Support over Cable は、Business Services over DOCSIS（BSOD）Cable Labs 仕様のサポートに、ポイントツーポイント Transparent LAN Service（TLS）を提供します。

L2VPN Support over Cable 機能は以下をサポートします。

- この機能は、IEEE 802.1q VLAN ID に基づくさまざまなケーブル モデム（CM）およびサービス フロー（SF）のサポートにおいて、イーサネット トランキング インターフェイスを使用して複数の L2VPN トンネルにトラフィックを転送します。従来型 TLS サービスでは、プライマリのアップストリームまたはダウンストリーム SF しか使用できません。新しい L2VPN Support over Cable 機能では、プライマリとセカンダリ両方の SF を使用できます。
- TLS 機能では、CLI を使用してサービスをプロビジョニングします。L2VPN Support over Cable では、CM コンフィギュレーション ファイルを使用してサービスをプロビジョニングし、単一の CLI を使用してデフォルトのイーサネット ネットワーク システム インターフェイス（NSI）を特定します。
- ダウンストリーム トラフィックは CM 単位で転送され、アップストリーム トラフィックは SF 単位で転送されます。L2VPN Support over Cable では、同じ L2VPN のアップストリーム トラフィックは複数のアップストリーム サービス フローを使用でき、ダウンストリーム トラフィックはさまざまなダウンストリーム サービス フローを使用できます。

機能情報の確認

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *103* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

L2VPN Support over Cable の前提条件

- 暗号化サポートされたイメージを使用する必要があります。
- ケーブル モデムは、BPI+ をサポートするように設定する必要があります。

L2VPN Support over Cable の制限事項

L2VPN Support over Cable 機能には、次の一般的な制限事項があります。

- DOCSIS 1.0 CM はサポートされません。
- ロード バランシングおよび動的チャネル変更（DCC）は、L2VPN サポートがイネーブルの CM でサポートされません。

- DSx メッセージ（動的サービス追加（DSA）、動的サービス変更（DSC）、動的サービス削除（DSD））は、L2VPN プロビジョニングされた CM でサポートされます。ただし、L2VPN のタイプ、長さ、値（TLV）を伴う DSx はサポートされません。
- マルチポイント L2VPN はサポートされません。また、マルチポイント L2VPN 用のシンプルネットワーク管理プロトコル（SNMP）MIB はすべてサポートされません。
- eSAFE（組み込み型サービス/アプリケーション機能エンティティ）DHCP スヌーピングはサポートされません（L2VPN サブタイプ 43.5.3）。
- 1 つの MAC ドメインで最大 1024 の L2VPN がサポートされます。
- 1 つの L2VPN サービスで最大 8 のアップストリーム SF がサポートされます。
- 1 つの L2VPN サービスで最大 8 のダウンストリーム分類子がサポートされます。
- eSAFE の除外は 1 つの eSAFE ホストに対してのみサポートされます。対応 CM の REG-REQ メッセージが複数の eSAFE ホストを指定している場合は、Cisco CMTS ルータにより除外される eSAFE ホストとして eMTA（ifIndex 16）が選択されます。CM 機能の一部に eMTA が含まれていない場合、CM 機能の最初の eSAFE ホストが除外用に選択されます。
- ケーブル モデム インターフェイス マスク（CMIM）の最大長は 4 バイトです。
- Business Services over DOCSIS（BSOD）レイヤ 2 バーチャル プライベート ネットワーク仕様で、サポートされない領域は次のとおりです。
  - 必須 VPN ID および NSI カプセル化 サブタイプを置き換えるためのベンダー固有の L2VPN エンコーディングはサポートされません。
  - IEEE 802.1s が指定するような NSI ポート送信トラフィック クラスに対するイーグレス ユーザ プライオリティのマッピングはサポートされません。
  - ベンダー固有の設定によるゼロ以外のデフォルト ユーザ プライオリティ値での転送はサポートされていません。
  - 同じ VPN ID を持つ複数のダウンストリーム分類子 L2VPN エンコーディングを受け入れてパケットをさまざまなサービス フローに分類することはサポートされません。
  - 同じ CM 上の同じ L2VPN に複数の SAID を割り当てることはサポートされません。プライマリ SAID がすべてのダウンストリーム トラフィックの暗号化に使用されます。
  - 同じグループ レベルの L2VPN SAID を、同じ L2VPN ID が付けられた同じ MAC ドメイン内のさまざまな CM に割り当てることはサポートされません。
  - DOCSIS スパニング ツリー プロトコル（DSTP）を導入し、L2VPN 動作について設定されたすべての NSI および RF インターフェイスで DSTP BPDU 送信を実行することはサポートされません。
  - すべての L2VPN CM の顧客宅内機器（CPE）ポートへの DSTP 転送専用に DSTP SAID を導入することはサポートされません。

VPN ID の制限事項

- 各 CM で最大 4 つの VPN ID がサポートされます。
- CM 内の複数の SF が同じ L2VPN に属することができますが、CM 内の各 SF に関連付けることができる VPN ID は最大 1 つです。
- 1 つの Cisco CMTS ルータあたり、最大 4093 の固有の VPN ID がサポートされます。
- VPN ID の最大長は 16 バイトです。
- アップストリーム分類子エンコーディングを除くすべての L2VPN エンコーディングに VPN ID を含める必要があります。

L2VPN Support over Cable に関する情報

L2VPN Support over Cable には、Cisco CMTS ルータに関する次の利点と機能があります。

- ポイントツーポイント L2VPN 転送モードをサポートします。
- CM ごとに 4 つの VPN ID までサポートします。
- 1 つ以上の SF が同じ VPN ID に属する状態で、CM ごとに複数のアップストリーム SF をサポートします。
- Cisco CMTS ルータで 1 つ以上の L2VPN トンネル用のトランキング ポートとして動作する単一のイーサネット NSI をサポートします。
- CM のプライマリ SAID を使用した BPI+ 暗号化をサポートします。
- CM コンフィギュレーション ファイルと CM 登録における L2VPN エンコーディングをサポートします（L2VPN エンコーディングによる REG-REQ）。
- CM ごとおよび SF ごとの転送をサポートするために、アップストリーム L2VPN トンネルをサポートします。
- SUP NSF/SSO および N+1 ライン カードの冗長スイッチオーバーにおける L2VPN データベースとアップストリームおよびダウンストリーム SF の同期およびリカバリをサポートします。
- アップストリームおよびダウンストリームの QoS をサポートします。
- スタック構成の IEEE 802.1q タグをサポートします。
- 単一 Embedded Service/Application Functional Entity（eSAFE）ホスト用の L2VPN トンネルからのトラフィック除外をサポートします。
- CMIM および IEEE 802.1p プライオリティ ビットによるレイヤ 2 分類子をサポートします。
- プロビジョニング エラー（CM 全体で重複する VLAN ID、使用中の VLAN ID など）の検出をサポートし、対応するエラー メッセージで CM をオフラインに移行します。
- 同じ RF MAC ドメイン上の L2VPN および非 L2VPN トラフィックと、およびその他のトンネル トラフィックから分離された非 L2VPN トラフィックとの共存をサポートします。

- L2VPNプロビジョニングされたCMからの音声コールをサポートします。ただし、音声コールは L2VPN の一部ではありません。
- BSOD VLAN 冗長性機能をサポートします。この機能を使用すると、プライマリ WAN インターフェイスの他にバックアップ WAN インターフェイスを設定することができます。プライマリ WANインターフェイスがダウンした場合、L2VPN トラフィックはバックアップ WAN インターフェイスを使用して送受信されます。
- VLAN 冗長性機能の手動スイッチオーバーをサポートします。これにより、両方のアップリンク ポートが稼働している場合、アクティブなアップリンク ポートを現在のポートから別のポートに手動で切り換えることができます。
- 2000 バイトのレイヤ 2 MTU をサポートします。

ポイントツーポイント L2VPN 転送モード

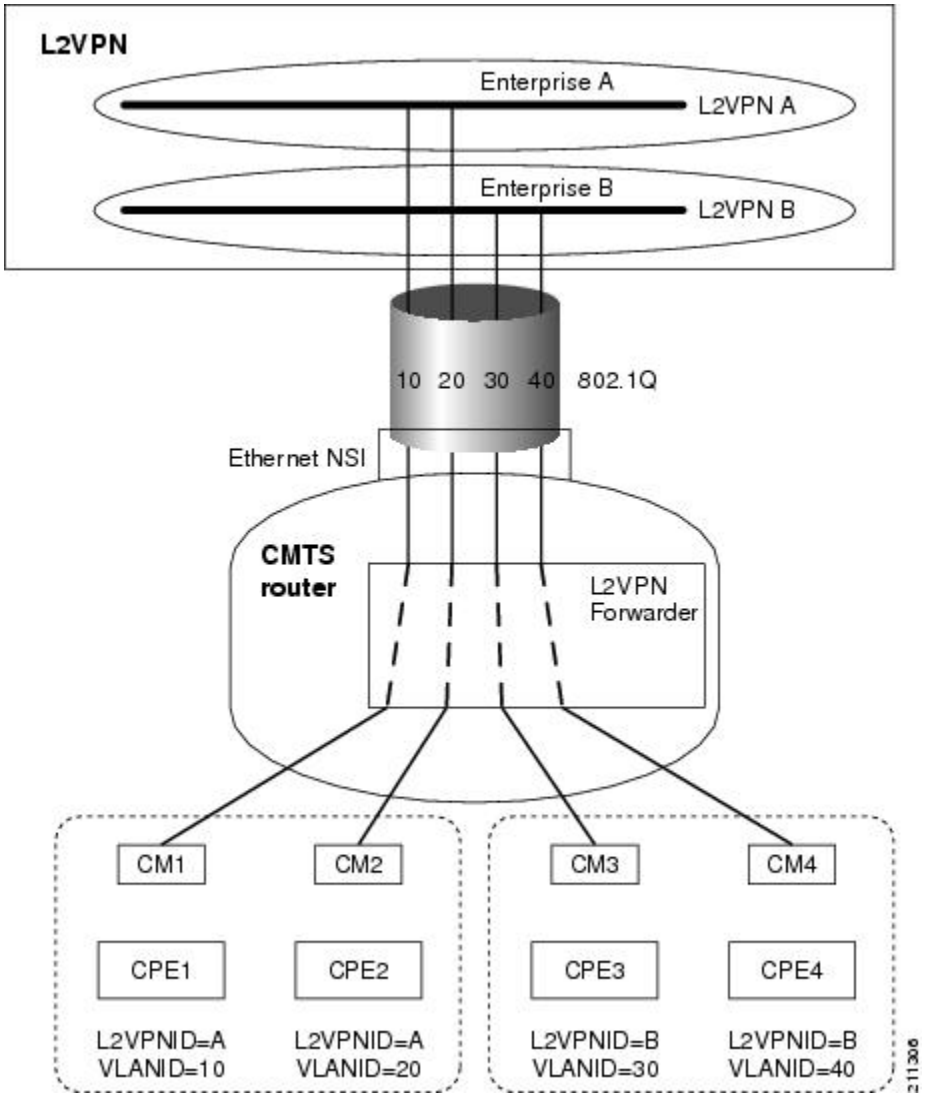
Cisco CMTS ルータは、BSOD 仕様に記載されたポイントツーポイント L2VPN 転送モードをサポートします。Cisco CMTS ルータの接続回線（SF または CM）はそれぞれ NSI カプセル化の値が指定されており、IEEE 802.1q VLAN ID により設定されています。

Cisco CMTS ルータ の L2VPN フォワーダは、転送の決定に MAC アドレス ラーニングを使用せずに、ルータ上の NSI ポートと接続回線間のアップストリーム トラフィックおよびダウンストリーム トラフィックを転送します。ケーブル オペレータのバックボーン ネットワーク上の L2VPN ブリッジが MAC アドレス ラーニングを実行して、VLAN ID 間でパケットをブリッジングします。

次の図に、IEEE 802.1q NSI カプセル化を使用したポイントツーポイント L2VPN ネットワークの例を示します。この例では、4 つの CM が 4 つの異なる VLAN ID（10、20、30、40）に関連付けられています。CM の L2VPN エンコーディングには L2VPN の論理 ID（この例では A または B）、

および関連付けされた VLAN ID を含む IEEE 802.1q 対応 NSI カプセル化サブタイプが含まれています。

図 *22*：ポイントツーポイント *L2VPN* ネットワーク構成図



L2VPN の論理 ID により、特定の VLAN ID に対して個別のブロードキャスト ドメインを作成することができます。図では、CM1 と CM2 からは VLAN 10 と VLAN 20 のトラフィックを企業 A のネットワークに送信し、CM3 と CM4 からは VLAN 30 と VLAN 40 のトラフィックを企業 B のネットワークに送信することができます。

CM コンフィギュレーション ファイルでの L2VPN エンコーディング

CM コンフィギュレーション ファイルには、Cisco CMTS がアップストリームおよびダウンストリーム CPE パケットの L2VPN 転送を処理する方法を制御する一連の L2VPN エンコーディングが含まれます。BSOD 仕様により、L2VPN エ

ンコーディングは、タイプ コード 43 およびサブタイプ 5（43.5）、ならびに予約済みベンダー ID 0xFFFFFF を使用する一般拡張情報（GEI）を使用してカプセル化されます。

L2VPN は次のタイプのエンコーディングを定義します。

- CM ごとの L2VPN エンコーディング：CM コンフィギュレーション ファイルの最上位に表示されるエンコーディング。
- SF ごとの L2VPN エンコーディング：アップストリーム サービス フロー エンコーディング（タイプ 24）のサブタイプとして表示されるエンコーディング。
- アップストリーム分類子 L2VPN エンコーディング：アップストリーム パケット分類コンフィギュレーション設定（タイプ 22）に表示されるエンコーディング。
- ダウンストリーム分類子 L2VPN エンコーディング：ダウンストリーム パケット分類コンフィギュレーション設定（タイプ 23）に表示されるエンコーディング。

最も単純な CM コンフィギュレーション ファイルは、プライマリ アップストリーム SF 定義内に 1 つの SF ごとの L2VPN エンコーディング、およびその L2VPN の NSI カプセル化サブタイプを含む 1 つの CM ごとの L2VPN エンコーディングを含みます。

（注） L2VPN 設定に BSOD（CM コンフィギュレーション ファイル）が使用され、Cisco CMTS WAN インターフェイスに QoS ポリシー マップの設定が適用されている場合、パケットは QoS ポリシー マップに一致しません。L2VPN 設定に CLI モードが使用され、Cisco CMTS WAN インターフェイスに QoS ポリシー マップ設定が適用されている場合、パケットは QoS ポリシー マップに一致します。

（注） Cisco CMTS では、2 つのイーサネット ネットワーク側インターフェイス（NSI）設定とバックアップ WAN インターフェイスのサポートにより、BSOD VLAN 冗長性機能をサポートしています。アクティブな NSI WAN インターフェイスがダウンすると、L2VPN トラフィックはバックアップ WAN インターフェイスを通過します。

サポートされる L2VPN のエンコーディング

ここでは、Cisco CMTS ルータでサポートされている CM コンフィギュレーション ファイルでサポートされる L2VPN のエンコーディングについて説明します。

- Cisco CMTS ルータは次の CM 機能をサポートします。
  - L2VPN の機能（5.17）
  - eSAFE ホスティング機能（5.18）
  - ダウンストリーム非暗号化トラフィック（DUT）のフィルタリング（5.19）
- Cisco CMTS ルータは、次のトップレベルのエンコーディングをサポートします。

- VPN 識別子（43.5.1）
- CMIM（43.5.4）：提供されている場合、L2VPN トンネルに関連付けられたすべてのアップストリーム SF に適用されます。1 つの eSAFE ホストのみをサポートします。
- IEEE 802.1q（43.5.2.2）のフォーマット コード 2 による NSI カプセル化（43.5.2）
- DUT フィルタリングのエンコーディング

• Cisco CMTS ルータは、次の SF ごとのエンコーディングをサポートします。

- VPN 識別子（43.5.1）
- イングレス ユーザ プライオリティ（43.5.8）

• Cisco CMTS ルータは、次のダウンストリーム分類子エンコーディングをサポートします。

- VPN 識別子（43.5.1）
- CMIM（43.5.4）および（22/23.13）
- ユーザ プライオリティ範囲（43.5.9）

CM コンフィギュレーション ファイルと L2VPN エンコーディングについての詳細は、「Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks」仕様を参照してください。

Cisco CMTS でコンフィギュレーション ファイル ジェネレータを使用する方法については「DOCSIS Internal Configuration File Generator for the Cisco CMTS」のドキュメントを参照してください。

L2VPN CM での音声コールのサポート

L2VPN CM では音声コールがサポートされます。この機能により、Cisco CMTS ルータは、L2VPN プロビジョニングされたケーブル モデム上の動的サービス フローをサポートして、非 L2VPN CPE からの音声コールを許可することができます。

L2VPN CM で音声コールをサポートするには、ケーブル モデム コンフィギュレーション ファイルを使用して適切な分類子を設定し、2 つの静的サービス フロー（プライマリおよびセカンダリ）を作成する必要があります。eMTA が、eSAFE ホストとして設定された組み込み型 CPE と共に L2VPN を構成できる場合は、1 つのサービス フローで十分です。適切な CMIM ビットが設定されている場合、Cisco CMTS は eSAFE ホストから L2VPN にパケットを送信しません。

L2VPN は、プライマリまたはセカンダリ サービス フローで設定することができますが、同じサービス フロー上の eMTA とは共存できません。eMTA は、常に、L2VPN とは異なるサービス フローを使用する必要があります。トラフィックを誘導する分類子も、L2VPN および eMTA が使用しているサービス フローに基づいている必要があります。上記の設定がされていれば、音声コールが開始されるたびに動的サービス フローが自動的に作成されます。

L2VPN Support over Cable の設定方法

ここでは、次の手順について説明します。

イーサネット ネットワーク システム インターフェイスの設定

L2VPN Support over Cable 機能を設定するには、L2VPN トラフィックのトランキング インターフェイスとして動作するようにイーサネット NSI を指定する必要があります。Cisco CMTS ルータでコマンドを使用して NSI を設定する必要があります。CM コンフィギュレーション ファイルを使用して設定することはできません。

はじめる前に

次のインターフェイス タイプは、L2VPN Support over Cable の NSI として設定できます。

- Cisco cBR シリーズ コンバージド ブロードバンド ルータ：GigabitEthernet と TenGigabitEthernet

（注） Cisco CMTS ルータは、CMTS ごとに 1 つの L2VPN NSI の設定のみをサポートします。
>

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cablel2-vpn-servicexconnectnsi dot1qinterface***ethernet-intf***[backup-interface ethernet-intf]** 例： `Router(config)# cable l2-vpn-service xconnect nsi dot1q interface Te4/1/0 backup-interface Te4/1/4`	DOT1Q L2VPN の WAN インターフェイスを設定します。 （任意）バックアップ インターフェイス：バックアップ インターフェイスが設定される場合、BSoD VLAN 冗長性機能が有効になっていることを意味します。

L2VPN サポート用 DOCSIS コンフィギュレーション ファイルの準備

L2VPN をサポートするには、DOCSIS コンフィギュレーション ファイルを適切なエンコーディングで設定する必要があります。Cisco CMTS ルータでサポートされるエンコーディングについては、CM コンフィギュレーション ファイルでの L2VPN エンコーディング，（659 ページ）を参照してください。

手動スイッチオーバー コマンドライン インターフェイス

BSoD VLAN 冗長性機能では、両方のアップリンクが稼働中であれば、コマンドライン インターフェイスを使用してアクティブアップリンク ポートを別のポートに手動で切り替えることができます。手動スイッチオーバーを実行するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**cable l2-vpn dot1q-nsi-redundancy force-switchover from** *active-nsi-interface* 例： `Router# cable l2-vpn dot1q-nsi-redundancy force-switchover from Te4/0/1`	アクティブ アップリンク ポートを、現在のアクティブ ポートから指定のポートに切り替えます。

dot1q L2VPN アップリンク冗長性の情報を表示するには、次の例に示すように **show cable l2-vpn dot1q-nsi-redundancy** を使用します。

```
Router# show cable l2-vpn dot1q-nsi-redundancy
Primary-NSI Backup-NSI Active-NSI Elapsed-after-SW
Te4/1/0       Te4/0/4    Te4/1/0    31m9s
Te4/1/2       Te4/0/5    Te4/1/2    59s
```

L2VPN Support over Cable の確認

Cisco CMTS ルータに関する L2VPN 情報を確認するには、**show cable l2-vpn xconnect dot1q-vc-map** コマンドを使用します。

手順

ステップ 1 すべてのケーブル モデムの VLAN 情報を表示するには、次の例に示すように **showcablel2-vpnxconnect dot1q-vc-map** コマンドを使用します。

例：

```
Router# show cable l2-vpn xconnect dot1q-vc-map
MAC Address    Ethernet Interface      VLAN ID   Cable Intf  SID  Customer Name/VPN ID
0014.f8c1.fd66 GigabitEthernet4/0/0        68    Cable6/0/0  3    0234560001
```

ステップ 2 特定の L2VPN ID または顧客の VLAN 情報を表示するには、次の例に示すように **showcablel2-vpnxconnectdot1q-vc-mapcustomer** 形式のコマンドを使用します。

例：

```
Router# show cable l2-vpn xconnect dot1q-vc-map customer 0234560001

MAC Address    Ethernet Interface      VLAN ID   Cable Intf  SID  Customer Name/VPNID
0014.f8c1.fd66 GigabitEthernet4/0/0        68    Cable6/0/0  3    0234560001
```

ステップ 3 特定のケーブル モデムの特定の L2VPN ID に関する情報を表示するには、次の例に示すように、ケーブル モデムの MAC アドレスを指定した **showcablel2-vpnxconnect dot1q-vc-mapvpn** 形式のコマンドを使用します。

例：

```
Router# show cable l2-vpn xconnect dot1q-vc-map 0014.f8c1.fd66 vpn 0234560001

MAC Address    Ethernet Interface      VLAN ID   Cable Intf  SID  Customer Name/VPNID
0014.f8c1.fd66 GigabitEthernet4/0/0        68    Cable6/0/0  3    0234560001
```

ステップ 4 特定のケーブル モデムの特定の L2VPN ID に関する詳細情報を表示するには、次の例に示すように、ケーブル モデムの MAC アドレスを指定した **showcablel2-vpnxconnectdot1q-vc-mapvpnverbose** 形式のコマンドを使用します。

例：

```
Router# show cable l2-vpn xconnect dot1q-vc-map 0014.f8c1.fd66 vpn 0234560001 verbose
MAC Address                    : 0014.f8c1.fd66
Prim Sid                       : 3
Cable Interface                : Cable6/0/0
VPN ID                         : 0234560001
L2VPN SAID                     : 12294
Upstream SFID                  : 23
Downstream CFRID[SFID]         : 2[24]
CMIM                           : 0x60
Ethernet Interface             : GigabitEthernet4/0/0
DOT1Q VLAN ID                  : 68
Total US pkts                  : 1372
Total US bytes                 : 500226
Total US pkt Discards          : 0
Total US byte Discards         : 0
Total DS pkts                  : 1248
Total DS bytes                 : 415584
Total DS pkt Discards          : 0
Total DS byte Discards         : 0
```

ステップ 5 特定のケーブル モデムの詳細情報と現在の冗長性に関する情報を表示するには、次の例に示すように、ケーブル モデムの MAC アドレスを指定した **showcablel2-vpnxconnectdot1q-vc-mapverbose** 形式のコマンドを使用します。

例：

```
Router# show cable l2-vpn xconnect dot1q-vc-map 0014.f8c1.fd66 verbose
MAC Address                    : 5039.5589.4302
```

```
Prim Sid                              : 45
Cable Interface                       : Cable6/0/2
L2VPNs provisioned                    : 1
DUT Control/CMIM                      : Disable/0x8000FFFF

VPN ID                                : 000234560001
L2VPN SAID                            : 45
Upstream SFID Summary                 : 77
Upstream SFID [77   ]                 : SID 45
Downstream CFRID[SFID] Summary        : Primary SF
CMIM                                  : 0x60
Primary Ethernet Interface            : GigabitEthernet4/0/0
Backup  Ethernet Interface            : GigabitEthernet4/0/1
Active  Ethernet Interface            : GigabitEthernet4/0/0
DOT1Q VLAN ID                         : 207
Total US pkts                         : 151269
Total US bytes                        : 211755224
Total DS pkts                         : 150502
Total DS bytes                        : 210463324
```

ステップ 6 dot1q L2VPN アップリンク冗長性の情報を表示するには、次の例に示すように **show cable l2-vpn dot1q-nsi-redundancy** を使用します。

例：

```
Router# show cable l2-vpn dot1q-nsi-redundancy
Primary-NSI Backup-NSI Active-NSI Elapsed-after-SW
Te4/1/0       Te4/0/4    Te4/1/0    31m9s
Te4/1/2       Te4/0/5    Te4/1/2    59s
```

L2VPN CM での音声コールの有効化

SID と VPN 間のマッピング ケーブル モデムのコンフィギュレーション ファイル（MPLS または 802.1q）を使用してケーブル モデムを登録すると、L2VPN CM で音声コール サポート機能をイネーブルにできます。

- L2VPN がプライマリ サービス フロー上にある場合は、静的セカンダリ サービス フローでケーブル モデムのコンフィギュレーション ファイルを使用し、分類子を L2VPN 以外のパケットのセカンダリ サービス フロー用に設定する必要があります。
- L2VPN がセカンダリ サービス フロー上にある場合は、分類子を L2VPN パケット用に設定する必要があります。

（注） ケーブル モデムのコンフィギュレーション ファイル ベースの L2VPN 設定には、プライマリまたはセカンダリ サービス フローで L2VPN を設定できるだけの柔軟性があります。ただし、セカンダリ サービス フローで L2VPN を設定し、プライマリ サービス フローはデフォルト トラフィック用に使用することを推奨します。

（注） CLI ベースの L2VPN 設定では、L2VPN はプライマリ サービス フロー上にあるため、静的セカンダリ サービス フローは eMTA で使用する必要があります。

動的サービス フローの確認

Cisco CMTS ルータで動的に作成したサービス フローを確認するには、**showinterfacecableservice-flow** コマンドを使用します。

（注） PacketCable の運用情報を確認するには、**showpacketcable** コマンドを使用します。

```
Router# show interface cable 5/1/0 service-flow
Sfid : 30191
Mac Address : 000a.739e.140a
Type : Secondary(Dynamic)
Direction : Upstream
Current State : Active
Current QoS Indexes [Prov, Adm, Act] : [0, 24, 24]
Active Time : 00:55
Sid : 7140
Admitted QoS Timeout : 200 seconds
Active QoS Timeout : 0 seconds
Packets : 1824
Bytes : 466944
Rate Limit Delayed Grants : 0
Rate Limit Dropped Grants : 0
Current Throughput : 68356 bits/sec, 32 packets/sec
Classifiers:
Classifier Id : 41
Service Flow Id : 30191
CM Mac Address : 000a.739e.140a
Direction : upstream
Activation State : active
Classifier Matching Priority : 128
PHSI : 1
Number of matches : -
IP Classification Parameters:
IP Source Address : 10.8.230.3
Source IP Address Mask : 255.255.255.255
Destination IP Address : 172.16.2.35
Destination IP Address Mask : 255.255.255.255
IP Protocol Type : 17
Source Port Low : 53456
Source Port High : 53456
Destination Port Low : 7052
Destination Port High : 7052
```

L2VPN Support over Cable の設定例

ここでは、L2VPN Support over Cable 機能の設定例を示します。

例：イーサネット NSI インターフェイスの指定

イーサネット NSI を CM コンフィギュレーション ファイル内で指定することも、以下の例に示すように **cable l2-vpn-service xconnect** グローバル コンフィギュレーション コマンドを使って指定することもできます。

```
cable l2-vpn-service xconnect nsi {dot1q|mpls}
```

例：MPLS L2VPN での音声コール サポートの有効化

次に、MPLS L2VPN の音声コール サポートを有効にするケーブル モデム コンフィギュレーション ファイルの例を示します。この例では、L2VPN がプライマリ サービス フローに適用されています。

```
03 (Net Access Control)          = 1
18 (Maximum Number of CPE)       = 16
43 (Vendor Specific Options)
   S08 (Vendor ID)       = ff ff ff
   S005 (Unknown sub-type)       = 01 04 32 30 32 30 02 07 04 05 01 0a 4c 02 01 2b 06 26 04
 00 00 01 90
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)            = 2
   S03 (Service Flow Reference)          = 2
   S09 (IP Packet Encodings)
       T03 (IP Source Address)           = 050 001 005 000
       T04 (IP Source Mask)              = 255 255 255 000
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)            = 3
   S03 (Service Flow Reference)          = 2
   S10 (Ethernet LLC Packet Classification Encodings)
       T02 (Source MAC Address)          = 00 e0 f7 5a c9 21
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)            = 21
   S03 (Service Flow Reference)          = 21
   S05 (Rule Priority)                   = 5
   S09 (IP Packet Encodings)
       T05 (IP Destination Address)      = 050 001 005 000
       T06 (IP Destination Mask)         = 255 255 255 000
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)            = 22
   S03 (Service Flow Reference)          = 21
   S05 (Rule Priority)                   = 5
   S10 (Ethernet LLC Packet Classification Encodings)
       T01 (Destination MAC Address)     = 00 e0 f7 5a c9 21 ff ff ff ff ff ff
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)          = 1
   S06 (QoS Parameter Set Type)          = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID)  = ff ff ff
       T005 (Unknown sub-type)  = 01 04 32 30 32 30
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)          = 2
   S06 (QoS Parameter Set Type)          = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)          = 20
   S06 (QoS Parameter Set Type)          = 7
   S07 (Traffic Priority)                = 0
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)          = 21
   S06 (QoS Parameter Set Type)          = 7
   S07 (Traffic Priority)                = 1
29 (Privacy Enable)              = 1
```

例：802.1q L2VPN での音声コール サポートの有効化

次に、802.1q L2VPN の音声コール サポートを有効にするケーブル モデム コンフィギュレーション ファイルの例を示します。この例では、L2VPN がセカンダリ サービス フローに適用されています。

```
03 (Net Access Control)          = 1
43 (Vendor Specific Options)
   S08 (Vendor ID)       = ff ff ff
```

```
   S005 (Unknown sub-type)      = 01 05 02 34 56 00 01 02 04 02 02 00 44
18 (Maximum Number of CPE)      = 16
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 2
   S03 (Service Flow Reference)         = 2
   S10 (Ethernet LLC Packet Classification Encodings)
       T02 (Source MAC Address)         = 00 e0 14 e3 23 1c
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 4
   S03 (Service Flow Reference)         = 4
   S43 (Vendor Specific Options)
       T08 (Vendor ID)  = ff ff ff
       T005 (Unknown sub-type)  = 01 05 02 34 56 00 01
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T01 (IEEE 802.1P UserPriority)   = 00 07
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 1
   S06 (QoS Parameter Set Type)         = 7
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 2
   S06 (QoS Parameter Set Type)         = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID)  = ff ff ff
       T005 (Unknown sub-type)  = 01 05 02 34 56 00 01 08 01 01
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 3
   S06 (QoS Parameter Set Type)         = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 4
   S06 (QoS Parameter Set Type)         = 7
```

例：CLI ベース L2VPN での音声コール サポートの有効化

次に、CLI を使用して設定された L2VPN の音声コール サポートを有効にするケーブル モデム コンフィギュレーション ファイルの例を示します。CLI を使用して設定された L2VPN は、プライマリ サービス フローに常に適用されます。

```
03 (Net Access Control)         = 1
18 (Maximum Number of CPE)      = 16
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 2
   S03 (Service Flow Reference)         = 2
   S09 (IP Packet Encodings)
       T03 (IP Source Address)          = 050 001 005 000
       T04 (IP Source Mask)             = 255 255 255 000
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 3
   S03 (Service Flow Reference)         = 2
   S10 (Ethernet LLC Packet Classification Encodings)
       T02 (Source MAC Address)         = 00 e0 f7 5a c9 21
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 21
   S03 (Service Flow Reference)         = 21
   S05 (Rule Priority)                  = 5
   S09 (IP Packet Encodings)
       T05 (IP Destination Address)     = 050 001 005 000
       T06 (IP Destination Mask)        = 255 255 255 000
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)           = 22
   S03 (Service Flow Reference)         = 21
   S05 (Rule Priority)                  = 5
   S10 (Ethernet LLC Packet Classification Encodings)
       T01 (Destination MAC Address)    = 00 e0 f7 5a c9 21 ff ff ff ff ff ff
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 1
   S06 (QoS Parameter Set Type)         = 7
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)         = 2
```

```
   S06 (QoS Parameter Set Type)          = 77
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)          = 20
   S06 (QoS Parameter Set Type)          = 7
   S07 (Traffic Priority)                = 0
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)          = 21
   S06 (QoS Parameter Set Type)          = 7
   S07 (Traffic Priority)                = 1
29 (Privacy Enable)              = 1
```

その他の参考資料

ここでは、L2VPN Support over Cable 機能の関連資料について説明します。

標準

規格	タイトル
CM-SP-BPI+-I12-050812	『*Baseline Privacy Plus Interface Specification*』 http://www.cablelabs.com/wp-content/uploads/specdocs/CM-SP-BPI+-C01-081104.pdf
CM-SP-L2VPN-I03-061222	『*Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks*』 http://www.cablelabs.com/wp-content/uploads/specdocs/CM-SP-L2VPN-I12-131120.pdf
CM-SP-RFIv2.0-I11-060602	『*Radio Frequency Interface Specification*』 http://www.cablelabs.com/wp-content/uploads/specdocs/CM-SP-RFIv2.0-C02-090422.pdf
IEEE 802.1ad	『*IEEE 802.1ad-2005 IEEE Standards for Local and metropolitan area networks*— Virtual Bridged Local Area Networks』 http://www.ieee.org
IEEE 802.1q	『*IEEE Std 802.1Q Virtual Bridged Local Area Networks*』 http://www.ieee.org

MIB

MIB	MIB のリンク
DOCS-L2VPN-MIB	選択したプラットフォーム、Cisco IOS-XE リリース、およびフィーチャセットに関する MIB を見つけてダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFC

RFC	タイトル
RFC 2685	『Virtual Private Networks Identifier』 http://www.ietf.org/rfc/rfc2685.txt
RFC 4364	『*BGP/MPLS IP Virtual Private Networks (VPNs)*』 http://www.ietf.org/rfc/rfc4364.txt

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

L2VPN Support over Cable に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャセット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *104* : ***L2VPN Support over Cable*** に関する機能情報

機能名	リリース	機能情報
L2VPN Support over Cable	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 40 章

L2VPN over Port-Channel

Layer 2 VPN（L2VPN）over Port-Channel 機能は、IEEE 802.1（dot1q）L2VPN WAN インターフェイス port-channel をサポートします。この機能を使用すると、port-channel アップリンクを通過するように dot1q L2VPN トラフィックを設定できます。

目次

L2VPN over Port-Channel 機能について

Cisco cBR-8 では、ケーブル モデムからのイーサネット フレームが特定の LAN インターフェイスに相互接続される L2VPN がサポートされています。挿入される VLAN ID が指定されます。L2VPN over Port-Channel 機能により、port-channel アップリンク インターフェイスおよび 10 GB アップリンク インターフェイスをサポートできるようになりました。

TLS L2VPN

Transparent LAN Service（TLS）L2VPN では、ケーブル モデムの MAC アドレス、VLAN ID、およびアウトバウンド インターフェイスが dot1q マップに含まれます。特定のケーブル モデムから受信したトラフィックに VLAN ID タグが付けられた後、アップリンク インターフェイスから送信されます。

DOCSIS L2VPN

Data-over-Cable Service Interface Specifications（DOCSIS）L2VPN では、ケーブル モデム（CM）コンフィギュレーション ファイルに CM 用とサービス フロー用の両方の L2VPN エンコーディング

が保持されます。CMTS レベルで、デフォルト port-channel ネットワーク側インターフェイス（NSI）を指定する必要があります。L2VPN エンコーディングは、登録時に CM によって CMTS に渡されます。CMTS は登録時に渡された情報に基づいて、DOCSIS サービス フロー VLAN マッピングをインストールします。アップストリーム トラフィックの場合、CMTS は dot1q VLAN でタグ付けされたトラフィックをアップリンク インターフェイスから送出します。ダウンストリームでは、CMTS は dot1q でタグ付けされたトラフィックをアグリゲータから受信します。CMTS は、VLAN ヘッダーを、対応するサービス フローへの DOCSIS ヘッダーに置き換えます。

L2VPN over Port-Channel の利点

dot1q L2VPN を使用することで、単一の 10 Gb ポートの代わりに port-channel インターフェイス機能を利用できます。

L2VPN over Port-Channel の制限事項

CMTS dot1q L2VPN は、顧客宅内機器とネットワークの間の相互トラフィックをサポートするように意図されています。CMTS L2VPN NSI ポートについては、port-channel インターフェイスは VLAN 冗長性をサポートしません。

L2VPN over Port-Channel の設定方法

ここでは、Cisco cBR-8 上で L2VPN over Port-Channel を設定する方法を説明します。

TLS L2VPN の port-channel アップリンク ポートの設定

TLS L2VPN には、全体的な enable CLI および dot1q マップを設定する必要があります。dot1q マップで、port-channel アップリンク ポートを指定する必要があります。

TLS L2VPN の port-channel アップリンク ポートを設定するには、次の手順に従います。

cable l2-vpn-service xconnect nsi dot1q
cable dot1q-vc-map *mac address* **port-channel** *number vlan id custom name*

DOCSIS L2VPN の port-channel アップリンク ポートの設定

DOCSIS L2VPN には、port-channel アップリンク ポートを指定した全体的な enable CLI のみを設定する必要があります。L2VPN 関連の他のパラメータは、CM コンフィギュレーション ファイルの type-length-value 解析によって設定されます。

DOCSIS L2VPN の port-channel アップリンク ポートを設定するには、次の手順に従います。

configure terminal
cable l2-vpn-service xconnect nsi dot1q interface port-channel *number*

port-channel 設定の確認

port-channel マッピングの確認

port-channel マッピングを確認するには、次の例に示すように **show cable l2-vpn xconnect dot1q-vc-map** コマンドを使用します。

show cable l2-vpn xconnect dot1q-vc-map

```
MAC Address    Ethernet Interface      VLAN ID   Cable Intf  SID  Customer Name/VPNID
c8fb.26a5.551c Port-channel64            1200    Cable6/0/0  17   Topgun
```

port-channel インターフェイスの表示

port-channel インターフェイスを表示するには、次の例に示すように **show cable l2-vpn xconnect dot1q-vc-map verbose** コマンドを使用します。

show cable l2-vpn xconnect dot1q-vc-map c8fb.26a5.551c verbose

```
MAC Address                          : c8fb.26a5.551c
Customer Name                        : ats
Prim Sid                             : 17
Cable Interface                      : Cable6/0/0
Ethernet Interface                   : Port-channel64
DOT1Q VLAN ID                        : 1200
Total US pkts                        : 189
Total US bytes                       : 18200
Total DS pkts                        : 615
Total DS bytes                       : 39360
```

L2VPN over Port-Channel に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *105*：*L2VPN over Port-Channel* に関する機能情報

機能名	リリース	機能情報	
L2VPN over Port-Channel	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。	

第 41 章

ケーブル L2VPN 用 MPLS 擬似回線

ケーブル レイヤ 2 バーチャル プライベート ネットワーク（L2VPN）用マルチプロトコル ラベル スイッチング（MPLS）擬似回線機能により、サービス プロバイダーは、単一の収束されたインターネット プロトコル（IP）/MPLS ネットワーク インフラストラクチャを使用して、2 つまたはそれ以上の VPN の顧客サイトにイーサネット データリンク層（レイヤ 2）を提供できるようになります。

機能情報の確認

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *106*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

ケーブル L2VPN 用 MPLS 擬似回線の前提条件

- ベースライン プライバシー インターフェイス プラス（BPI+）をイネーブルにして、ケーブル ネットワーク上のデータに、ケーブル モデムで送受信されるデータを保護するための単純なデータ暗号化方式を提供します。
- Cisco Express Forwarding（CEF）をイネーブルにしてネットワーク パフォーマンスを最適化します。
- リモート プロバイダー エッジ（PE）ルータのプライマリおよびバックアップ擬似回線が Cisco ケーブル モデム終端システム（CMTS）と同じ擬似回線タイプであることを確認します。
- CMTS が擬似回線タイプとして VLAN を使用している場合は、リモート PE のインターワーキングとして VLAN に pw-class を使用してリモート擬似回線を作成します。

ケーブル L2VPN 用 MPLS 擬似回線の制限事項

ケーブル L2VPN 用 MPLS 擬似回線の一般的な制限事項は次のとおりです。

- 1 つの RFC 4448 あたり、1 つの Ethernet over MPLS（EoMPLS）擬似回線のみがサポートされます。
- ポイントツーポイント転送のみをサポートします。イーサネット スイッチングはサポートされません。
- DOCSIS 2.0 および 3.0 認定ケーブル モデム（CM）が必要です。この機能は DOCSIS 1.0 認定ケーブル モデムではサポートされません。
- 1 ケーブル モデムあたり最大 4 VPN をサポートします。
- 最大 8 のアップストリーム サービス フローと 8 のダウンストリーム分類子をサポートします。
- 1 つの Cisco CMTS ルータで 最大 16000 の EoMPLS 擬似回線をサポートします。
- Cisco CMTS がスイッチオーバーするには、リモート PE にバックアップ擬似回線が設置されている必要があります。
- プライマリ擬似回線に障害が発生した場合のみ、バックアップ擬似回線が Cisco CMTS でアクティブになる必要があります。

（注） CLI ベース（静的プロビジョニング）L2VPN は、プライマリ アップストリームおよびダウンストリーム サービス フローのみの VPN へのトラフィック転送をサポートします。したがって、ケーブル モデムのコンフィギュレーション ファイルでは、プライマリ アップストリームおよびダウンストリーム サービス フローのみを設定する必要があります。

ケーブル L2VPN 用 MPLS 擬似回線の情報

ケーブル L2VPN 用 MPLS 擬似回線機能では、擬似回線（PW）上でレイヤ 2 プロトコル データ ユニット（PDU）をカプセル化して送信することにより、MPLS ネットワーク上でイーサネット ベースのレイヤ 2 VPN サービスを実現します。この機能を使用すると、サービス プロバイダーは自社の業務や企業や官公庁のお客様にサイト間接続を提供することができます。

MPLS ネットワーク上でエミュレートされるレイヤ 2 サービスは、MPLS ベースの L2VPN、または MPLS L2VPN と呼ばれます。さらに、MPLS ネットワーク上でエミュレートされるイーサネット サービスは、Ethernet over MPLS（EoMPLS）サービスと呼ばれます。

ケーブル L2VPN 用 MPLS 擬似回線機能は、CableLabs Business Services over DOCSIS（BSOD）L2VPN 仕様に完全に準拠しており、Cisco CMTS ルータでサポートされる既存の DOCSIS L2VPN 機能を拡張したものです。

ケーブル L2VPN 用 MPLS 擬似回線機能は、次の機能を提供します。

- MPLS ネットワーク上でイーサネット フレームを送信します。
- DOCSIS サービス フローを EoMPLS 擬似回線にマッピングされた接続回線として処理します。
- Cisco CMTS ルータが MPLS プロバイダー エッジ（PE）ルータとして機能できるようにします。
- DOCSIS 上の（CM と Cisco CMTS ルータの間の）イーサネット フレームを MPLS に（そこからさらにメトロポリタン エリア ネットワークまたはワイドエリア ネットワークに）転送できるようにします。
- MPLS ネットワーク上でサポートされるレイヤ 2 トラフィック タイプをカプセル化して送信するための共通フレームワークを提供します。

ケーブル L2VPN 用 MPLS 擬似回線機能は、802.1q ベースの L2VPN（L2VPN Support over Cable）のような既存の DOCSIS L2VPN 機能とは異なります。ケーブル L2VPN 用 MPLS 擬似回線機能では IP/MPLS ネットワークを使用してレイヤ 2 プロトコル データ ユニット（PDU）を送信しますが、802.1q ベースの L2VPN 機能ではレイヤ 2 イーサネット ネットワークを使用して PDU を送信します。

MPLS によるレイヤ 2 パケットの転送方法

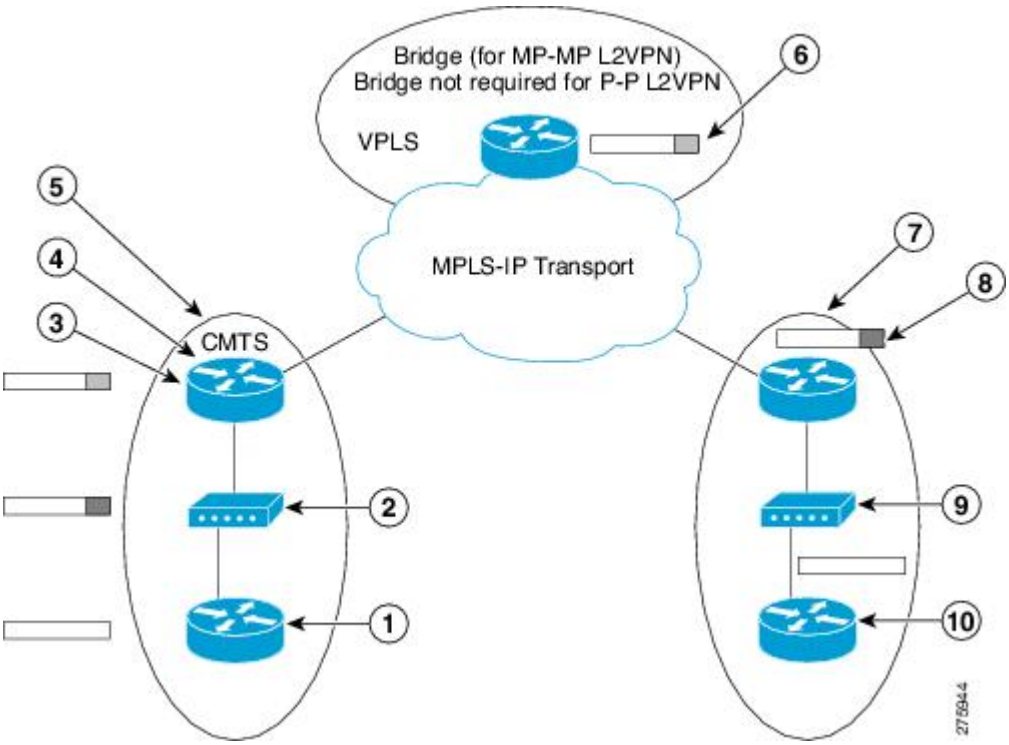
MPLS サブシステムは、レイヤ 2 イーサネット フレームの DOCSIS カプセル化を除去して、入力プロバイダー エッジ（PE）Cisco CMTS ルータで MPLS ラベルを追加します。その後、MPLS サブシステムは、擬似回線のもう一方の端にある対応する PE ルータに対して、得られた MPLS パケットを送信します。PE ルータは、2 つの PE ルータ間で IP/MPLS パケットを正常に送信できるように設定する必要があります。

ケーブル モデムは、アップストリーム分類子を使用して、アップストリーム方向の顧客宅内機器（CPE）からのイーサネット フレームを分類します。次に、これらのフレームに DOCSIS ヘッダーが追加され、特定のアップストリーム サービス フローで異なるサービス識別子を使用して送信されます。Cisco CMTS ルータでは、ケーブル インターフェイスおよびサービス識別子に基づき、アップストリーム パケットが L2VPN パケットとして分類されます。Cisco CMTS ルータは DOCSIS ヘッダーを取り除き、MPLS ヘッダーを追加します。MPLS ヘッダーには 2 つの MPLS ラベルが含まれます。リモートの PE ルータに対応する外部ラベルと、擬似回線ラベルに対応する内部ラベルです。Cisco CMTS ルータは、MPLS パケットを MPLS ネットワークを介して PE ルータ（擬似回線のもう一方の端）に転送します。

ダウンストリーム方向では、Cisco CMTS ルータは MPLS ヘッダーを 1 つのみ含む MPLS パケットを受信します。この MPLS ヘッダーには、Cisco CMTS ルータが対応する EoMPLS 擬似回線に対して以前に割り当てたラベルが含まれています。Cisco CMTS ルータは、いずれかの L2VPN ケーブル モデムを特定するために MPLS ラベルを使用します。次に Cisco CMTS ルータは、受信した MPLS パケットの MPLS ヘッダー内にある MPLS Experimental（MPLS-EXP）ビットに基づき、L2VPN ダウンストリーム分類子を使用して MPLS パケットを分類してから、MPLS ヘッダーを削除します。その後、Cisco CMTS ルータは DOCSIS ヘッダーを追加することで分類されたダウンストリーム サービス フロー上でパケットを送信します。ケーブル モデムは、DOCSIS ヘッダーを取り除き、CPE にイーサネット フレームを配送します。

ケーブル モデム MAC アドレス、VPN ID（CM コンフィギュレーション ファイル内に存在する場合）、ピア IP アドレス、および仮想回線 ID（VCID）の独自の組み合わせにより、Cisco CMTS ルータにおける MPLS 擬似回線を識別します。

図 *23*：レイヤ *2* パケットの転送



DOCSIS ベースのケーブル コミュニケーション システムで MPLS がレイヤ 2 パケットを転送する方法について、次の表で説明します。

1	ルータは、タグなしイーサネット フレームを送信します。	6	MPLS パケットは、ラベル スイッチドです。
2	CM は、フレームに DOCSIS ヘッダーを追加します。	7	Cisco CMTS ルータは、MPLS パケットを受信し、MPLS ヘッダー内のラベル値を使用して MPLS 転送テーブルを検索します。

3	Cisco CMTS ルータは、フレームから DOCSIS ヘッダーを取り除きます。	8	Cisco CMTS ルータは、MPLS ヘッダーを DOCSIS ヘッダー（適切な SID 値を含む）に置き換えます。
4	Cisco CMTS ルータは、DOCSIS ヘッダーから SID 値を使用してサービス ID（SID）データベースを検索し、MPLS ヘッダーを探します。	9	DOCSIS ヘッダーが削除されます。
5	Cisco CMTS ルータは、フレームに MPLS ヘッダーを追加します。	10	イーサネット フレームはタグなしで配送されます。

UNI でサポートされるイーサネット カプセル化

イーサネット ユーザ ネットワーク インターフェイス（UNI）は、ケーブル モデムとルータやスイッチなどの顧客宅内機器間の接続です。サービス プロバイダーは、UNI でカプセル化を使用している場合としていない場合があります。

ケーブル L2VPN 用 MPLS 擬似回線機能は、イーサネット UNI で次の転送タイプをサポートします。

- ポートベースの UNI（VLAN に非依存）：ポートベースの UNI は、Metro Ethernet Forum（MEF）で定義されているイーサネット プライベート回線（EPL）サービスを提供します。この転送タイプでは、MPLS 擬似回線はイーサネット ポートにマッピングされます。
- VLAN ベースの UNI：802.1q カプセル化を使用するイーサネット VLAN（スタック構成の VLAN を含む）。VLAN ベースの UNI は、MEF で定義されているイーサネット バーチャル プライベート回線（EVPL）サービスを提供します。この転送タイプでは、MPLS 擬似回線は 802.1q VLAN にマッピングされます。

（注） イーサネット UNI はケーブル モデムのイーサネット ポートに接続する必要があります。

この機能を設定する前に、次の概念を理解する必要があります。

MPLS 擬似回線

擬似回線は 2 つの PE ルータ間のポイントツーポイント レイヤ 2 接続です。ケーブル L2VPN 機能の MPLS 擬似回線は、次の擬似回線タイプをサポートします。

- タイプ 4 擬似回線：VLAN タグ付きレイヤ 2 イーサネット フレームの転送にのみ使用されます。
- タイプ 5 擬似回線：VLAN タグ付きとタグなしのレイヤ 2 イーサネット フレームの転送に使用されます。これがデフォルトの擬似回線タイプです。

bundle254 インターフェイス

bundle254（Bu254）インターフェイスは、すべての MPLS 擬似回線の回線識別子として使用される、Cisco CMTS ルータ上の内部バンドルインターフェイスです。この内部バンドルインターフェイスは、**cable l2-vpn-service xconnect** コマンドを使用して MPLS 擬似回線機能を有効にすると、Cisco CMTS ルータ上で自動的に作成されます。Cisco CMTS ルータで使用可能なすべての MPLS 擬似回線を処理するために作成される Bu254 インターフェイスは 1 つのみです。

show xconnect or show cable l2-vpn xconnect command displays コマンドの出力には、Cisco CMTS ルータがすべての MPLS 疑似回線用に作成した回線識別子が表示されます。.

イングレス プロセス

Cisco CMTS ルータのケーブル インターフェイスから受信したアップストリーム パケットがケーブル モデム インターフェイスおよびサービス ID（SID）に基づく L2VPN パケットであることが識別されると、パケットはイングレスプロセスに進みます。イングレスプロセスで、パケットは DOCSIS ヘッダーを削除されて MPLS 擬似回線設定に従う MPLS ラベル ヘッダーを追加され、Cisco CMTS ルータのイーサネット インターフェイスから送信されます。イングレス プロセスは、ラベル インポジション プロセスとしても知られています。

イーグレス プロセス

Cisco CMTS ルータのイーサネット インターフェイスから受信したダウンストリーム パケットが最深部の MPLS ラベルに基づいて L2VPN パケットであることが識別されると、パケットはイーグレス プロセスに進みます。イーグレス プロセスでは、MPLS ラベル ヘッダーがパケットから削除され、DOCSIS ヘッダーがこのパケットに追加されるようにします。その後、パケットは Cisco CMTS ルータのケーブル インターフェイスから送信されます。イーグレス プロセスは、ラベル ディスポジション プロセスとしても知られています。

MPLS 擬似回線コントロール プレーン プロセス

L2VPN 準拠 CM を Cisco CMTS ルータに登録し、ルータに L2VPN 関連パラメータを伝送すると、ルータは標準のラベル配布プロトコル（LDP）手順に従い、リモートの PE ルータを使用して Ethernet over MPLS 擬似回線をセットアップします。L2VPN 準拠 CM がオフラインになると、Cisco

CMTS ルータにより擬似回線もダウンします。Cisco CMTS ルータに L2VPN 準拠 CM が登録されていない場合は、ルータはリモートの PE ルータでターゲット LDP セッションを切断します。

L2VPN 疑似回線冗長化

L2VPN 擬似回線冗長性機能を使用して、PE ルータが擬似回線の障害を検出し、サービスの提供を続行できるバックアップ擬似回線にレイヤ 2 サービスを再ルーティングするようにできます。擬似回線冗長性は、Cisco CMTS ルータまたは PE ルータとしての汎用ルータに実装できます。プライマリ擬似回線が障害から回復すると、L2VPN 擬似回線冗長性機能はレイヤ 2 サービスをプライマリ擬似回線に戻すオプションを提供します。

各プライマリ擬似回線には、一意のプライオリティを持つバックアップ擬似回線を最大 3 つ設定できます。たとえば、バックアップ リスト中の 2 つの異なる擬似回線にプライオリティ 1 を設定することはできません。プライマリ擬似回線がダウンすると、Cisco CMTS は、最もプライオリティが高いバックアップ擬似回線にトラフィックを送信します。サービス転送を成功させるには、バックアップ擬似回線のリモート状態がすでに「up」であることが必要です。モデムが BPI オンラインの場合、アクティブな擬似回線のローカル状態のみが「up」となります。同様に、バックアップ擬似回線が使用中である場合、そのバックアップ擬似回線のみのローカル状態が「up」となります。

アクティブなバックアップ擬似回線がダウンすると、Cisco CMTS は、次にプライオリティが高くリモート状態が「up」のバックアップ擬似回線を使用します。ただし、最もプライオリティの高いバックアップ擬似回線が「up」になっている場合は、Cisco CMTS は低プライオリティの擬似回線からの高プライオリティの擬似回線へのスイッチオーバーを行いません。これは、バックアップ擬似回線間の不要なスイッチオーバーを防ぐためです。

プライマリ擬似回線が障害から回復すると、L2VPN 擬似回線冗長性機能は backup delay コマンドを使用して、設定された期間を待機した後、プライマリ擬似回線にサービスを戻します。プライマリ擬似回線が確立されると、アクティブなバックアップ擬似回線のローカル状態は「down」としてマーキングされます。

MPLS 擬似回線のプロビジョニング方法

ケーブル L2VPN 機能の MPLS 擬似回線は、次の擬似回線のプロビジョニング方法をサポートします。

（注） MPLS 擬似回線の静的または動的プロビジョニングを実行する前に、Cisco CMTS ルータで MPLS を有効にする必要があります。MPLS を有効にするために必要なタスクの詳細については、「Cisco CMTS ルータでの MPLS を有効にする方法」を参照してください。

MPLS 擬似回線の静的プロビジョニング方法

静的プロビジョニング方法では、コマンド ライン インターフェイス（CLI）を使用して、MPLS 擬似回線を CMTS で静的にプロビジョニングする必要があります。このタイプのプロビジョニングでは、CM コンフィギュレーション ファイルが BSOD L2VPN 準拠の TLV を使用する必要はありません。MPLS 擬似回線の静的プロビジョニング方法の詳細については、『*Static Provisioning of MPLS Pseudowires*』を参照してください。

MPLS 擬似回線の動的プロビジョニング方法

動的プロビジョニング方法は、CM コンフィギュレーション ファイル ベースのプロビジョニング方法であり、MPLS 擬似回線を作成するための推奨プロビジョニング方法です。MPLS 擬似回線を動的にプロビジョニングする方法の詳細については、MPLS 擬似回線の動的プロビジョニング, （699 ページ）を参照してください。

擬似回線を動的にプロビジョニングする利点は次のとおりです。

- CM コンフィギュレーション ファイルでは複数の VPN を指定でき、擬似回線は VPN ごとにプロビジョニングできます。
- 複数のアップストリーム サービス フローおよびダウンストリーム分類子を各 VPN に関連付けることができます。
- 各アップストリーム サービス フローは出力 WAN トラフィックの MPLS Experimental（EXP）レベルにタグ付けできます。
- ダウンストリームの入力 WAN トラフィックはダウンストリーム分類子ごとに指定されるダウンストリーム MPLS-EXP 範囲に基づいて分類できます。
- Cisco CMTS ルータは、ケーブル インターフェイスおよび WAN インターフェイス上で MPLS Quality of Service（QoS）を詳細に制御します。

MPLS 擬似回線の動的プロビジョニングでは、Trivial File Transfer Protocol（TFTP）サーバに保存されている L2VPN 準拠の CM コンフィギュレーション ファイルを使用します。CM コンフィギュレーション ファイルを作成するには、CableLabs Config File Editor などの一般的な CM コンフィギュレーション ファイル エディタ、または Broadband Access Center for Cable（BACC）などの高度なプロビジョニング バックエンド システムを使用します。

このプロビジョニング方法は、CM コンフィギュレーション ファイル内のタイプ、長さ、値（TLV）オブジェクトなど、CableLabs で定義された L2VPN エンコーディングを使用することが必要です。これらの L2VPN エンコーディングは、アップストリームおよびダウンストリーム イーサネット フレームの L2VPN 転送を制御します。

L2VPN エンコーディングは次の方法で指定できます。

- CM ごと
- ダウンストリーム分類子ごと
- サービス フローごと

- アップストリーム分類子ごと

（注） CM L2VPN エンコーディングは必須です。

CM L2VPN エンコーディングには多くの TLV が含まれます。そのうち最も重要な 2 つの TLV は、VPN 識別子および NSI カプセル化です。MPLS 擬似回線を設定するには、NSI カプセル化を MPLS に設定します。その他の TLV は、Source Attachment Individual Identifier（SAII）、Target Attachment Individual Identifier（TAII）、および Attachment Group Identifier（AGI）の形式で擬似回線識別子を指定するために使用されます。

L2VPN エンコーディング パラメータは、CM コンフィギュレーション ファイルの一般拡張情報（GEI）パラメータとしてエンコードされます。これは、ベンダー ID（0xFFFFFF）を使用したベンダー固有情報タイプパラメータのサブタイプとしてパラメータがエンコードされることを示します。

ケーブル L2VPN 用 MPLS 擬似回線機能用に CM コンフィギュレーション ファイルの最上位で使用される、CableLabs で定義された重要な TLV を次の表に示します。*CableLabs* で定義された *TLV* の完全なリストについては、CableLabs の BSOD 仕様『*Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks*』を参照してください。

表 *107*：*CableLabs* で定義された *L2VPN TLV*

TLV 名	タイプ	長さ	値と説明
ダウンストリーム非暗号化トラフィック（DUT）制御	45.1	1	ビット 0 DUT フィルタリング DUT フィルタリング＝0：無効（デフォルト） DUT フィルタリング＝1：DUT フィルタリング有効
ダウンストリーム非暗号化トラフィック（DUT）CMIM	45.2	N	DUT CMIM（任意） DUT トラフィックの発信インターフェイスを制限する CM インターフェイス マスク（CMIM）。DUT CMIM が省略されると、デフォルト値には eCM とすべての実装された eSAFE インターフェイスが含まれますが、CPE インターフェイスは含まれません。

TLV 名	タイプ	長さ	値と説明
VPN 識別子	43.5.1	1 対 N	L2VPN を特定する不透明オクテット文字列。N はベンダー固有であり、有効な範囲は 6 ～ 255 です。
NSI カプセル化のサブタイプ	43.5.2	n	単一 NSI カプセル化形式のコード/長さ/値のタプル。この TLV は、次のいずれかの値を使用します。 NSI カプセル化 = 0：その他 NSI カプセル化 = 1：IEEE 802.1Q（VLAN ID を指定） NSI カプセル化 = 2：IEEE 802.1AD（Q-in-Q を指定） NSI カプセル化 = 3：MPLS ピア（IPv4 または IPv6 アドレスを指定） MPLS 擬似回線を確実に使用するには、値を 3 に設定する必要があります。このアドレスは（ループバック インターフェイスに割り当てられた IP アドレスによって）リモート PE を特定する必要があります。
Attachment Group ID	43.5.5	0 ～ 16	IETF レイヤ 2 VPN シグナリング プロトコルの接続回線として CM または SF を特定する不透明バイト文字列。
Source Attachment Individual ID	43.5.6	0 ～ 16	IETF レイヤ 2 VPN シグナリング プロトコルの SAII 回線としてシグナリングされる不透明バイト文字列。
Target Attachment Individual ID	43.5.7	0 ～ 16	IETF レイヤ 2 VPN シグナリング プロトコルの接続回線として CM または SF を特定する不透明バイト文字列。

TLV 名	タイプ	長さ	値と説明
イングレス ユーザ プライオリティ	43.5.8	1	最下位 3 ビットで符号化される 0 ～ 7 の範囲のイングレス IEEE 802.1 ユーザ プライオリティ値。値が大きいほど、プライオリティが高いことを意味します。
ユーザ プライオリティの範囲	43.5.9	2	ユーザ プライオリティ範囲で低いユーザ プライオリティ値は、1バイト目の最下位 3 ビットでエンコードされます。範囲で高い値は、2 バイト目の最下位 3 ビットでエンコードされます。

Cisco 専用 L2VPN TLV

CableLabs で定義される L2VPN TLV は MPLS 擬似回線の、ダイナミック プロビジョニングに十分ですが、CMTS オペレータは追加機能を有効にするために CM コンフィギュレーション ファイルのトップレベルで Cisco 専用 TLV を使用できます。

この表は、ケーブル L2VPN 機能用に MPLS 擬似回線向けに定義された新しい Cisco 専用 TLV を示しています。

表 *108*：*Cisco* 専用 *L2VPN TLV*

TLV 名	タイプ	長さ	値	説明
MPLS-PW-TYPE	43.5.43.36	1	• 4 = タイプ 4 イーサネット VLAN • 5 = タイプ 5 イーサネット ポート	Cisco CMTS ルータは、このサブタイプを MPLS 擬似回線タイプ（タイプ 4 またはタイプ 5）であると解釈します。この TLV 値を指定しない場合、ルータはタイプ 5 のデフォルト値（5）を受け入れます。

TLV 名	タイプ	長さ	値	説明
MPLS-VCID	43.5.43.38	4	4 バイトの符号なし数 = MPLS VCID	このサブタイプは MPLS VCID であると解釈されます。 次の条件が満たされる場合、この TLV は無視され、TAII の値が擬似回線用の VCID として使用されます。 • CableLabs BSOD 仕様準拠 TLV、SAII、および TAII が CM コンフィギュレーション ファイル内にあること。 • 両方の長さが 4 バイトであること。 • SAII の値が TAII と同じであること。
MPLS-PEERNAME	43.5.43.39	N	ASCII エンコードされたデータ	Cisco CMTS ルータは、ASCII エンコードされたデータでこのオプションのサブタイプを MPLS ピア名として解釈します。

この表は、L2VPN 擬似回線冗長性機能向けに定義された新しいシスコ専用タイプ、長さ、値（TLV）を示しています。

表 *109*：擬似回線冗長性向けの *Cisco* 専用 *L2VPN TLV*

TLV 名	タイプ	長さ	値	説明
BACKUP-PW	45.5.43.40	N	バックアップ擬似回線関連パラメータ	Cisco CMTS ルータは、このサブタイプを MPLS バックアップ擬似回線の関連パラメータとして解釈します。この TLV は、新しいバックアップ擬似回線の開始を示します。
BACKUP-PEERIP	43.5.43.40.1	4	バックアップ ピアの IP アドレスです（IPv4）。	Cisco CMTS ルータは、このオプションのサブタイプを MPLS バックアップ擬似回線のピア IP アドレスとして解釈します。この TLV は IPv4 アドレスです。
BACKUP-PEERNAME	43.5.43.40.2	N	ASCII エンコードされたデータ	Cisco CMTS ルータは、ASCII エンコードされたデータでこのオプションのサブタイプを MPLS バックアップピア名として解釈します。 この TLV は DNS によって IPv4 アドレスに解決されます。

TLV 名	タイプ	長さ	値	説明
BACKUP-MPLS-VCID	43.5.43.40.3	4	4 バイトの符号なし数 = バックアップ擬似回線の MPLS VCID	Cisco CMTS ルータは、このサブタイプをバックアップ擬似回線の VCID として解釈します。 次の条件が満たされる場合、この TLV は無視され、TAII の値が擬似回線用の VCID として使用されます。 • CableLabs BSOD 仕様準拠 TLV、SAII、および TAII が CM コンフィギュレーション ファイル内にあること。 • SAII と TAII の長さが 4 バイトであること。 • SAII の値が TAII と同じであること。
BACKUP-MPLS-PRIORITY	43.5.43.40.4	1	1 バイトの符号なし数 = バックアップ擬似回線のプライオリティ	Cisco CMTS ルータは、このサブタイプを MPLS プライオリティとして解釈します。 各プライマリ擬似回線には、一意のプライオリティを持つバックアップ擬似回線を最大 3 つ設定できます。プライオリティは、プライマリ ピアがダウンしているときに CMTS がバックアップ ピアに切り替える順序を示します。

TLV 名	タイプ	長さ	値	説明
BACKUP-ENABLE-DELAY	43.5.43.41	1	1 バイトの符号なし数 = 秒数	Cisco CMTS ルータは、このサブタイプをプライマリ擬似回線がダウンしてからバックアップ擬似回線が引き継ぐまで待機する秒数として解釈します。 この TLV 値を指定しない場合、ルータはデフォルト値の 0 秒を使用します。
BACKUP-DISABLE-DELAY	43.5.43.42	1	1 バイトの符号なし数 = 秒数	Cisco CMTS ルータは、このサブタイプをプライマリ擬似回線のリモート状態が起動してからプライマリ擬似回線が引き継ぐまで待機する秒数として解釈します。 この TLV 値を指定しない場合、ルータはデフォルト値の 0 秒を使用します。
BACKUP-DISABLE-NEVER	43.5.43.43	1	1 バイトの符号なし数 = バックアップ擬似回線を無効化しない	Cisco CMTS ルータは、このサブタイプをプライマリ擬似回線が起動した後であってもバックアップ擬似回線を無効にしてはいけないことを示すフラグとして解釈します。 この TLV が存在しない場合、ルータはプライマリ擬似回線に戻すというデフォルトのアクションを実行します。

Cisco CMTS ルータでの MPLS を有効にする方法

Cisco CMTS ルータで MPLS を有効にするには、次のタスクを順序通りに実行します。

（注） MPLS 擬似回線の静的または動的プロビジョニングを実行する前に、Cisco CMTS ルータで MPLS を有効にする必要があります。

LDP ルータ ID の設定

mplsldprouter-id コマンドを使用すると、LDP ルータ ID としてインターフェイス IP アドレスを割り当てることができます。

LDP ルータ ID を決定する通常のプロセスは次のとおりです。

1. ルータは、すべての動作インターフェイスのすべての IP アドレスを考慮します。
2. これらのアドレスにループバック インターフェイス アドレスが含まれている場合、ルータは最大のループバック アドレスを選択します。ループバック アドレスの状態は変わらないため、ループバック アドレスを設定すると、ルータに安定した LDP ID を確保できます。ただし、各ルータでループバック インターフェイスと IP アドレスを設定する必要はありません。

次のような場合、ループバック IP アドレスは、ローカル LDP ID のルータ ID とは考えられません。

1. ループバック インターフェイスが明示的にシャットダウンされた場合
2. **mplsldprouter-id** コマンドで、別のインターフェイスを LDP ルータ ID として使用するように指定し場合
3. ループバック インターフェイスを使用する場合は、ループバック インターフェイスの IP アドレスが /32 ネットワーク マスクで設定されていることを確認します。さらに、使用中のルーティング プロトコルが対応する /32 ネットワークをアドバタイズするように設定されていることを確認します。それ以外の場合、ルータは最大のインターフェイスアドレスを選択します。

ルータは、特定の状況で使用できないルータ ID を選択する場合があります。たとえば、ルータは、ルーティング プロトコルがネイバー ルータにアドバタイズできない IP アドレスを選択する場合があります。ルータは、次回 LDP ルータ ID の選択が必要になったときにルータ ID を実装します。**mplsldprouter-id** コマンドの効果は、LDP ルータ ID の選択が必要になる時点までは反映されません。これは次回にインターフェイスがシャットダウンされるか、またはアドレスが設定解除されるときです。

mplsldprouter-id コマンドで **force** キーワードを使用すると、ルータ ID の効果がより素早く表れます。ただし、ルータ ID の実装は、指定したインターフェイスの現在の状態に応じて、次のように異なります。

- インターフェイスがアップ状態（動作中）の場合、およびその IP アドレスが現在 LDP ルータ ID ではない場合、LDP ルータ ID は、強制的にそのインターフェイスの IP アドレスに変更されます。LDP ルータ ID のこの強制的な変更によって、既存の LDP セッションが切断さ

れ、LDPセッションを通じて学習されたラベルバインディングが解放されます。また、バインディングに関連付けられていた MPLS 転送アクティビティが中断されます。

- インターフェイスがダウンしている場合、インターフェイスがアップ状態に移行すると、LDP ルータ ID は、強制的にそのインターフェイスの IP アドレスに変更されます。LDP ルータ ID のこの強制的な変更によって、既存の LDP セッションが切断され、LDP セッションを通じて学習されたラベルバインディングが解放されます。また、バインディングに関連付けられていた MPLS 転送アクティビティが中断されます。

はじめる前に

LDP ルータ ID として指定する前に、指定したインターフェイスが動作していることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**mplsip** 例： `Router(config)# mpls ip`	指定したギガビットイーサネットインターフェイスで動的MPLS転送機能をイネーブルにします。
ステップ 4	**mplsldprouter-idloopback**interface-number [**force**] 例： `Router(config)# mpls ldp router-id loopback 2030 force`	LDP ルータ ID としてのループバックインターフェイスの IP アドレスを指定します。
ステップ 5	**exit** 例： `Router(config)# exit`	グローバルコンフィギュレーションモードを終了し、特権EXECモードを開始します。

ギガビット イーサネット インターフェイスでの MPLS の設定

MPLS 転送およびラベル配布プロトコルは、ルータがリモート PE ルータに対して MPLS ラベルスイッチド パス（LSP）を確立できるように、Cisco CMTS ルータの 1 ポートまたは 10 ポート GE インターフェイスで有効にする必要があります。このセクションでは、ギガビット イーサネット インターフェイスで MPLS 転送および LDP を有効にする方法について説明します。

（注） 設定手順は、1 ポートおよび 10 ポート GE インターフェイスの場合と似ています。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacegigabitethernet** slot/subslot/port 例： `Router(config)# interface gigabitethernet 3/0/0`	インターフェイス ケーブル コンフィギュレーション モードを開始し、ギガビット イーサネット インターフェイスを指定します。
ステップ 4	**mplsip** 例： `Router(config-if)# mpls ip`	指定したギガビット イーサネット インターフェイスで動的 MPLS 転送機能をイネーブルにします。
ステップ 5	**end** 例： `Router(config-if)# end`	インターフェイス ケーブル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

MPLS ラベル配布プロトコルの設定

MPLS ラベル配布プロトコル（LDP）により、複数のサービス レベルをサポートする、拡張性と柔軟性に優れた IP VPN の構築を実現します。このセクションでは、ギガビット イーサネット インターフェイスで MPLS ラベル配布プロトコルを設定する方法について説明します。

また、LDP セッションの中断後に L2VPN トラフィック リカバリを高速化できるように、MPLS LDP のグレースフル リスタートを設定できる場合もあります。詳細については、『MPLS LDP Graceful Restart』ガイドを参照してください。

（注） MPLS ラベル配布プロトコルを設定する前に **showipinterfacebrief** コマンドを使用して、IP アドレスを持つループバック インターフェイスが各 PE ルータ上にあることを確認します。このループバック インターフェイスは、擬似回線のピア IP アドレスとして Cisco CMTS ルータを特定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacegigabitethernet** slot/subslot/port 例： `Router(config)# interface gigabitethernet 3/0/0`	インターフェイス ケーブル コンフィギュレーション モードを開始し、ギガビット イーサネット インターフェイスを指定します。
ステップ 4	**mplslabelprotocolldp** 例： `Router(config-if)# mpls label protocol ldp`	指定したギガビット イーサネット インターフェイスで MPLS LDP パラメータを有効にします。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Router(config-if)# end`	インターフェイス ケーブル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ケーブル L2VPN 用 MPLS 擬似回線の Cisco CMTS サポートの有効化

Cisco CMTS ルータで MPLS 擬似回線の設定をサポートするには、インターフェイスのネットワーク側で MPLS トンネル トラフィックをイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cablel2-vpn-servicexconnectnsimpls** 例： `Router(config)# cable l2-vpn-service xconnect nsi mpls`	次の場合に MPLS トンネル トラフィックをイネーブルにします。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

MPLS 擬似回線のプロビジョニング方法

MPLS 擬似回線は、次の方法でプロビジョニングできます。

（注） MPLS 擬似回線の静的または動的プロビジョニングを実行する前に、Cisco CMTS ルータで MPLS を有効にする必要があります。

MPLS 擬似回線の動的プロビジョニング

動的プロビジョニング方法は、次のタイプの構成をサポートします。

- BSOD 仕様ベースの MPLS 擬似回線のプロビジョニング
- CM コンフィギュレーション ファイルを使用するタイプ 4 MPLS 擬似回線のプロビジョニング
- CM コンフィギュレーション ファイルを使用するタイプ 5 MPLS 擬似回線のプロビジョニング

CM コンフィギュレーション ファイルを使用する動的プロビジョニング方法については、『Configuration Examples for Dynamic Provisioning of MPLS Pseudowires』を参照してください。

（注） MPLS擬似回線用に静的プロビジョニング方法ではなく動的プロビジョニング方式を使用することを推奨します。

MPLS 擬似回線の静的プロビジョニング方法

静的プロビジョニング方法では、コマンド ライン インターフェイス（CLI）を使用して、MPLS 擬似回線を CMTS で静的にプロビジョニングする必要があります。このタイプのプロビジョニングでは、CM コンフィギュレーション ファイルが BSOD L2VPN 準拠の TLV を使用する必要はありません。MPLS擬似回線の静的プロビジョニング方法の詳細については、『*Static Provisioning of MPLS Pseudowires*』を参照してください。

L2VPN 擬似回線冗長性の設定方法

L2VPN擬似回線冗長性機能により、プライマリ擬似回線に障害が発生した場合、バックアップ擬似回線に切り替えることができます。また、この機能により、CiscoCMTSはプライマリ擬似回線が回復したらこれに操作を再開させることができます。

バックアップ擬似回線の設定

プライマリ擬似回線に最大 3 つのバックアップ擬似回線を設定できます。各バックアップ擬似回線のプライオリティは異なる必要があります。

バックアップ擬似回線は、IPアドレスまたはホスト名とVCIDを組み合わせて独自に指定します。バックアップ ピアで設定できるのは、IP アドレスまたはホスト名と VCID のみで、残りのパラメータはプライマリ擬似回線と同じです。

バックアップ擬似回線は、DOCSIS コンフィギュレーション ファイルを使用して設定することもできます。

バックアップ擬似回線を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cablel2vpn***mac-address* 例： `Router(config)# cable l2vpn 0011.0011.0011`	L2VPN MAC アドレスを指定し、L2VPN コンフィギュレーション モードを開始します。
ステップ 4	**serviceinstance***id service-type* 例： `Router(config-l2vpn)# service instance 1 ethernet`	サービス インスタンス ID を指定し、イーサネット サービス コンフィギュレーション モードを開始します。
ステップ 5	**xconnect** *peer-ip-address vc-id* **encapsulation mpls** 例： `Router(config-ethsrv)# xconnect 10.2.2.2 22 encapsulation mpls`	トンネリング方式を指定してMPLS擬似回線でデータをカプセル化し、xconnectコンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**backuppeer** *peer-ip-address vc-id* [priority value] 例： `Router(config-xconn)# backup peer 10.3.3.3 33 priority 2`	バックアップ擬似回線とそのプライオリティを指定します。設定するバックアップ擬似回線が 1 つのみの場合は、プライオリティ キーワードは任意です。複数のバックアップ擬似回線を設定する場合は必須です。
ステップ 7	**end** 例： `Router(config-xconn)# end`	xconnect コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

バックアップ遅延の設定

プライマリ擬似回線がダウンしてから、バックアップ擬似回線に引き継ぐまでの待機時間を設定するには、次の手順を実行します。また、プライマリ擬似回線がアクティブになった後、バックアップ擬似回線から引き継ぐまでの待機時間を指定することもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cablel2vpn***mac-address* 例： `Router(config)# cable l2vpn 0011.0011.0011`	L2VPN MAC アドレスを指定し、L2VPN コンフィギュレーション モードを開始します。 • *mac-address*：CM の MAC アドレス。

	コマンドまたはアクション	目的
ステップ 4	**serviceinstance***id service-type* 例： `Router(config-l2vpn)# service instance 1 ethernet`	サービス インスタンス ID を指定し、イーサネット サービス コンフィギュレーション モードを開始します。 • *id*：サービス インスタンス ID。 • service-type：インスタンスのサービス タイプ。
ステップ 5	**xconnect** *peer-ip-address vc-id* **encapsulation mpls** 例： `Router(config-ethsrv)# xconnect 10.2.2.2 22 encapsulation mpls`	トンネリング方式を指定して MPLS 擬似回線でデータをカプセル化し、xconnect コンフィギュレーション モードを開始します。 • *peer-ip-address*：リモート PE ルータの IP アドレス。リモート ルータ ID は、到達可能であるかぎり任意の IP アドレスです。 • *vc-id*：PE ルータ間の仮想回線の 32 ビット識別子。 • **encapsulationmpls**：MPLS をトンネリング方式として指定します。

ステップ 6	次のいずれかを実行します。
	• **backupdelay**enable-delay-period {disable-delay-period | never}
	•
	
	例：
	`Router(config-xconn)# backup delay 10 10`
	
	例：
	`Router(config-xconn)# backup delay 10 never`
		バックアップ擬似回線を有効または無効にするまでの待機時間を指定します。
		• *enable-delay-period*：プライマリ擬似回線がダウンしてから、バックアップ擬似回線に引き継ぐまでに待機する秒数を指定します。有効な範囲は、0 ～ 180 秒です。デフォルト値は 0 です。
		• *disable-delay-period*：プライマリ擬似回線がアクティブになった後、バックアップ擬似回線から引き継ぐまでに待機する秒数を指定します。有効な範囲は、0 ～ 180 秒です。デフォルト値は 0 です。
		• **never**：バックアップ擬似回線に移行したら、プライマリ擬似回線を再びアクティブ化しないように指定します。

ステップ 7	**end** 例： `Router(config-xconn)# end`	xconnect コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

手動による切り替え

プライマリまたはバックアップ擬似回線に手動で切り替えるには、次の手順を実行します。また、**xconnectbackupforce-switchover** コマンドを使用すると、プライマリ リモート ピアの計画停電用のバックアップ擬似回線に強制的に切り替えることができます。

（注） 手動切り替えは、冗長グループで利用可能なメンバーに対してのみ実行できます。コマンドで指定した擬似回線が利用できない場合は、このコマンドは拒否されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例**： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**xconnectbackupforce-switchoverpeer10.10.1.1123** **例**： `Router# xconnect backup force-switchover peer 10.10.1.1 123`	ルータをバックアップ疑似回線またはプライマリ疑似回線に切り替えることを指定します。

トラブルシューティングのヒント

次のコマンドは、不適切な MPLS 擬似回線設定のトラブルシューティングに役立ちます。

- **showipinterface brief**：IP アドレスを持つループバック インターフェイスが各 PE ルータに存在するかを確認するのに役立ちます。
- **show mpls l2transport vc**：ルータ上でレイヤ 2 パケットをルーティングするためにイネーブルにされているプライマリおよびバックアップ擬似回線に関する情報の確認に役立ちます。
- **show xconnect all**：すべての xconnect 接続回線とプライマリおよびバックアップ擬似回線に関する情報の確認に役立ちます。
- **show cable l2-vpn xconnect mpls-vc-map**：プライマリおよびバックアップ擬似回線が正しく設定されていることを確認するのに役立ちます。

ケーブル L2VPN 用 MPLS 擬似回線の設定例

ここでは、静的および動的なプロビジョニング方法における MPLS 擬似回線の設定例を示します。

MPLS 擬似回線の静的プロビジョニングの設定例

次の例は、CLI ベースの MPLS 擬似回線のプロビジョニングを示しています。

```
Router> enable
Router# configure terminal
Router(config)# cable l2vpn 0000.396e.6a68 customer2
Router(config-l2vpn)# service instance 2000 ethernet
Router(config-ethsrv)# xconnect 101.1.0.2 221 encapsulation mpls pw-type 4
Router(config-ethsrv)# cable set mpls-experimental 7
```

MPLS 擬似回線の動的プロビジョニングの設定例

ここでは、CM コンフィギュレーション ファイルを使用した BSOD CableLabs 仕様、タイプ 4、およびタイプ 5 の TLV に基づく MPLS 擬似回線プロビジョニングの例を示します。

BSOD 仕様ベースの MPLS 擬似回線のプロビジョニング例

次に、BSOD CableLabs の仕様に基づいた MPLS 擬似回線の設定例を示します。

```
03 (Net Access Control) = 1
43 (Vendor Specific Options)
   S08 (Vendor ID) = ff ff ff
   S005 (L2VPN sub-type)
 =
        T01 (VPN Id) = 02 34 56 00 02 # VPNID=0234650002
        T02 (NSI) = 04 05 01 0a 4c 01 01# [04=mpls] [05=len][01=ipv4][IP=10.76.1.1]
        T05 (AGI) = 01 01 07 d1 # AGI = 0x010107d1
        T06 (SAII) = 00 00 07 d1 # SAII = TAII = VCID = 0x7d1 = 2001
        T07 (TAII) = 00 00 07 d1
18 (Maximum Number of CPE) = 16
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 1
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type)  =
            S01 (VPNID) =   02 34 56 00 02
            S08 (UserPrio) = 01

24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 2
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type) =
            S01 (VPNID) = 02 34 56 00 02
            S08 (UserPrio) = 04
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 3
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type) =
            S01 (VPNID) =   02 34 56 00 02
```

```
            S08 (UserPrio) = 05
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 4
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type) =
            S01 (VPNID) = 02 34 56 00 02
            S08 (UserPrio) = 06
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 2
   S03 (Service Flow Reference) = 2
   S05 (Rule Priority) = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask) = 00 20 ff
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 3
   S03 (Service Flow Reference) = 3
   S05 (Rule Priority) = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask) = 21 40 ff
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 4
   S03 (Service Flow Reference) = 4
   S05 (Rule Priority) = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)  = 41 ff ff
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 11
   S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 12
   S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 13
   S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 14
   S06 (QoS Parameter Set Type) = 7
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 12
   S03 (Service Flow Reference) = 12
   S05 (Rule Priority) = 3
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T01 (IEEE 802.1P UserPriority)   = 00 02
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type)

              S01 (VPNID) = 02 34 56 00 02
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 13
   S03 (Service Flow Reference) = 13
   S05 (Rule Priority) = 3
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T01 (IEEE 802.1P UserPriority) = 03 04
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type)
              S01 (VPNID) = 02 34 56 00 02
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 14
   S03 (Service Flow Reference) = 14
   S05 (Rule Priority) = 3
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T01 (IEEE 802.1P UserPriority) = 05 06
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T005 (L2VPN sub-type)
              S01 (VPNID) = 02 34 56 00 02
```

CM コンフィギュレーション ファイルを使用したタイプ 4 MPLS 擬似回線のプロビジョニング

次の例では、タイプ 4 MPLS 擬似回線の CM コンフィギュレーション ファイルベースのプロビジョニングを示します。

```
03 (Net Access Control) = 1
43 (Vendor Specific Options)
   S08 (Vendor ID) = ff ff ff
   S005 (L2VPN Options) =
T001 (VPN ID) = 02 34 56 00 02 # VPN-ID = "0234560002"
T043 (Cisco Vendor Specific) = 2b 16
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO
S036 (MPLSPWTYPE) = 24 01 04 # MPLSPWTYPE= Type4 - Ethernet-vlan Type
S039 (MPLSPEERNAME) = 27 06 63 37 36 30 30 32 MPLSPEERNAME= "c76002" in ascii
S038 (MPLSVCID) = 26 04 00 00 07 d1 = 2001 VCID
43 (Vendor Specific Options)
   S08 (Vendor ID) = ff ff ff
   S005 (L2VPN Options) =
T001 (VPN ID) = 02 34 56 00 03 # VPN-ID = "0234560003"
T043 (Cisco Vendor Specific) =  2b 16
S008 (Vendor ID) = 00 00 0c Vendor ID = "00 00 0C" - CISCO
S036 (MPLSPWTYPE) = 24 01 04 MPLSPWTYPE= Type4 - Ethernet-vlan Type
S039 (MPLSPEERNAME) = 27 06 63 37 36 30 30 32 # MPLSPEERNAME= "c76002" in ascii
S038 (MPLSVCID) = 26 04 00 00 0b b9 # = 3001 VCID
43 (Vendor Specific Options)
   S08 (Vendor ID) = ff ff ff
   S005 (L2VPN Options) =
T001 (VPN ID) = 02 34 56 00 04 # VPN-ID = "0234560004"
T043 (Cisco Vendor Specific) = 2b 16
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO
S036 (MPLSPWTYPE) = 24 01 04 # MPLSPWTYPE= Type4 - Ethernet-vlan Type
S039 (MPLSPEERNAME) = 27 06 63 37 36 30 30 32 # MPLSPEERNAME= "c76002" in ascii
S038 (MPLSVCID) = 26 04 00 00 0f a1 # = 4001 VCID
18 (Maximum Number of CPE) = 16
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 1
   S06 (QoS Parameter Set Type) = 7
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 2
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) = 02 34 56 00 02
       T043 (Cisco Vendor Specific) = 2b 0A
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO

S034 (MPLS-EXP-SET) = 22 05 # MPLSEXP-INGRESS= 5
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 3
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) = 02 34 56 00 03
       T043 (Cisco Vendor Specific) =  2b 0A
S008 (Vendor ID) = 00 00 0c
# Vendor ID = "00 00 0C" - CISCO

S034 (MPLS-EXP-SET) = 22 06

# MPLSEXP-INGRESS= 6
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 4
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) = 02 34 56 00 04
       T043 (Cisco Vendor Specific) = 2b 0A
S008 (Vendor ID) = 00 00 0c
# Vendor ID = "00 00 0C" - CISCO
```

```
S034 (MPLS-EXP-SET) = 22 04

# MPLSEXP-INGRESS= 4
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 2
   S03 (Service Flow Reference) = 2
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T02 (IEEE 802.1Q VLAN ID) = 7d 00
   S05 (Rule Priority) = 2
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 3
   S03 (Service Flow Reference) = 3
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T02 (IEEE 802.1Q VLAN ID) = bb 80
   S05 (Rule Priority) = 3
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 4
   S03 (Service Flow Reference) = 4
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T02 (IEEE 802.1Q VLAN ID) = fa 00
   S05 (Rule Priority) = 4
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 11
   S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 12
   S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 13
   S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 14
   S06 (QoS Parameter Set Type) = 7
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 12
   S03 (Service Flow Reference) = 12
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T02 (IEEE 802.1Q VLAN ID) = 7d 00
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) = 02 34 56 00 02
       T043 (Cisco Vendor Specific) = 2b 0B
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO
S035 (MPLS-EXP_RANGE) = 23 02  03 # MPLSEXP-EGRESS_RANGE= 2 - 3
   S05 (Rule Priority) = 2
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 13
   S03 (Service Flow Reference) = 13
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T02 (IEEE 802.1Q VLAN ID) = bb 80
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) =  02 34 56 00 03
       T043 (Cisco Vendor Specific) = 2b 0B
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO

S035 (MPLS-EXP-RANGE) = 23 04  05 # MPLSEXP-EGRESS_RANGE= 4 - 5
   S05 (Rule Priority = 3
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference) = 14
   S03 (Service Flow Reference) = 14
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
       T02 (IEEE 802.1Q VLAN ID) = fa 00
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) = 02 34 56 00 04
       T043 (Cisco Vendor Specific) = 2b 0B
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO

S035 (MPLS-EXP-RANGE) = 23 00  01 # MPLSEXP-EGRESS_RANGE= 0 - 1
   S05 (Rule Priority) = 4
```

CM コンフィギュレーション ファイルを使用したタイプ 5 MPLS 擬似回線のプロビジョニング例

次の例では、タイプ 5 MPLS 擬似回線の CM コンフィギュレーション ファイルベースのプロビジョニングを示します。

```
03 (Net Access Control) = 1
43 (Vendor Specific Options)
   S08 (Vendor ID) = ff ff ff
   S005 (L2VPN Options) =
T001 (VPN ID) = 02 34 56 00 02 # VPN-ID = "0234560002"
T043 (Cisco Vendor Specific) = 2b 16
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO
S036 (MPLSPWTYPE) = 24 01 05 # MPLSPWTYPE= Type5 - Ethernet-Port Type
S039 (MPLSPEERNAME) = 27 06 63 37 36 30 30 32 # MPLSPEERNAME= "c76002" in ascii
S038 (MPLSVCID) = 26 04 00 00 07 d1 # = 2001 VCID
45 (L2VPN CMIM) = 02 04 ff ff ff ff 01 01 01
18 (Maximum Number of CPE) = 16
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference) = 1
   S06 (QoS Parameter Set Type) = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID) = ff ff ff
       T001 (VPN ID) = 02 34 56 00 02 # VPN-ID = "0234560002"
       T043 (Cisco Vendor Specific) = 2b 0A
S008 (Vendor ID) = 00 00 0c # Vendor ID = "00 00 0C" - CISCO
S034 (MPLS-EXP-SET) = 22 04 # MPLS-EXP-SET at INGRESS= 4
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference) = 12
   S06 (QoS Parameter Set Type) = 7
```

L2VPN 擬似回線冗長性の設定例

ここでは、CM コンフィギュレーション ファイルを使用した、L2VPN 擬似回線冗長性機能の設定例を示します。

例：バックアップ擬似回線ピアと VC ID の設定

次に、CM 設定に基づいてファイルベースのバックアップ ピア ルータをプロビジョニングする方法について説明します。

PE ルータ 1

```
cable l2vpn 0025.2e2d.7252
 service instance 1 ethernet
  encapsulation default
  xconnect 10.76.2.1 400 encapsulation mpls
   backup peer 10.76.2.1 600 priority 4
```

PE ルータ 2

```
cable l2vpn 0011.0011.0011
 service instance 1 ethernet
  encapsulation default
  xconnect 10.2.2.2 22 encapsulation mpls
   backup peer 10.3.3.3 33 priority 2
   backup delay 10 10
```

例：バックアップ遅延の設定

次に、一時回線ステータスの変更後、二次回線ステータスが変更されるまでの時間を決定するため、バックアップ遅延の設定方法について説明します。

```
cable l2vpn 0011.0011.0011
 service instance 1 ethernet
  encapsulation default
  xconnect 10.2.2.2 22 encapsulation mpls
   backup delay 10 10
```

例：CM コンフィギュレーション ファイルを使用した L2VPN バックアップ MPLS 擬似回線のプロビジョニング

次に、CM コンフィギュレーション ファイルに基づいて L2VPN バックアップ MPLS 擬似回線をプロビジョニングする方法について説明します。

```
03 (Net Access Control)          = 1
18 (Maximum Number of CPE)       = 3
43 (Vendor Specific Options)
   S08 (Vendor ID)       = ff ff ff
   S005 (Unknown sub-type)       = 01 04 32 30 32 30 02 07 04 05 01 0a 4c 02 01 2b 15 26 04
 00 00 00 14 28 10 01 05 01 0a 4c 02 01 03 04 00 00 07 08 04 01 05 28 0d 01 05 01 0a 4c 02
 03 03 04 00 00 00 15 28 10 01 05 01 0a 4c 02 01 03 04 00 00 b1 8e 04 01 01 29 01 03 2a 01
 01
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)          = 4
   S06 (QoS Parameter Set Type)          = 7
   S08 (Max Sustained Traffic Rate)      = 2000000
   S09 (Max Traffic Burst)               = 3200
   S15 (Service Flow Sched Type)         = 2
   S43 (Vendor Specific Options)
       T08 (Vendor ID)       = ff ff ff
       T005 (Unknown sub-type)       = 01 04 32 30 32 30
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)          = 2
   S06 (QoS Parameter Set Type)          = 7
   S08 (Max Sustained Traffic Rate)      = 3000000
   S09 (Max Traffic Burst)               = 250000
29 (Privacy Enable)              = 1
```

MPLS 擬似回線の設定の確認

次の **show** コマンドを使用すると、MPLS 擬似回線の設定を確認できます。

- **showmplsldpdiscovery**
- **showcablel2-vpnxconnect**
- **showxconnect**
- **showmplsl2transportvc**

すべてのケーブル モデムの MPLS 擬似回線と仮想回線間のマッピングを確認するには、次の例に示すように **showcablel2-vpnxconnect** コマンドを使用します。

```
Router# show cable l2-vpn xconnect mpls-vc-map
```

```
MAC Address     Peer IP Address VCID Type Prio CktID      Cable Intf  SID Customer Name/VPNID
0023.bee1.eb48  123.1.1.1       30   Prim*     Bu254:4101 Cable3/0/0  3
38c8.5cac.4a62  123.1.1.1       20   Prim*     Bu254:4100 Cable3/0/0  4   customer1
602a.d083.2e1c  123.1.1.1       60   Prim*     Bu254:4102 Cable3/0/0  5
```

擬似回線冗長性が設定されていない場合、すべてのケーブル モデムの MPLS 擬似回線と仮想回線間のマッピングを確認するには、次の例に示すように **showcablel2-vpnxconnectmpls-vc-map** コマンドを使用します。

```
Router# show cable l2-vpn xconnect mpls-vc-map
MAC Address    Peer IP Address VCID Type  Prio CktID      Cable Intf SID Customer Name/VPNID
0025.2e2d.7252 10.76.2.1       400  Prim*      Bu254:400  Cable8/0/3 1
0014.f8c1.fd46 10.2.3.4        1000 Prim*      Bu254:1000 Cable8/0/0 1   2020
0014.f8c1.fd46 10.76.2.1       1800 Prim*      Bu254:1800 Cable8/0/0 1   2021
```

擬似回線冗長性が設定されている場合、すべてのケーブル モデムの MPLS 擬似回線と仮想回線間のマッピングを確認するには、次の例に示すように **showcablel2-vpnxconnectmpls-vc-map** コマンドを使用します。

```
Router# show cable l2-vpn xconnect mpls-vc-map
MAC Address    Peer IP Address VCID Type  Prio CktID      Cable Intf SID Customer Name/VPNID
602a.d083.2e1c 123.1.1.1       60   Prim*      Bu254:4102 Cable3/0/0 5
38c8.5cac.4a62 123.1.1.1       20   Prim*      Bu254:4103 Cable3/0/0 4   000232303230
               156.1.3.1       30   Bkup  3    Bu254:4103
               123.1.1.1       50   Bkup  8    Bu254:4103
38c8.5cac.4a62 156.1.3.1       56   Prim*      Bu254:4104 Cable3/0/0 4   000232303231
               123.1.1.1       40   Bkup  1    Bu254:4104
```

擬似回線冗長性が設定されていない場合、MPLS 擬似回線に関連付けられたすべての仮想回線の状態を取得するには、次の例に示すように **showcablel2-vpnxconnectmpls-vc-mapstate** コマンドを使用します。

```
Router# show cable l2-vpn xconnect mpls-vc-map state
MAC Address      Peer IP Address VCID Type Prio State Customer Name/VPNID State
602a.d083.2e1c   123.1.1.1       60   Prim*     UP                       UP
38c8.5cac.4a62   123.1.1.1       20   Prim*     UP    000232303230       UP
38c8.5cac.4a62   156.1.3.1       56   Prim*     UP    000232303231       UP
```

擬似回線冗長性が設定されている場合、MPLS 擬似回線に関連付けられたすべての仮想回線の状態を取得するには、次の例に示すように **showcablel2-vpnxconnectmpls-vc-mapstate** コマンドを使用します。

```
Router# show cable l2-vpn xconnect mpls-vc-map state
MAC Address      Peer IP Address VCID Type   Prio State Customer Name/VPNID State
602a.d083.2e1c   123.1.1.1       60   Prim*       UP                       UP
38c8.5cac.4a62   123.1.1.1       20   Prim*       UP    000232303230       UP
                 156.1.3.1       30   Bkup   3    UP    000232303230       STDBY
                 123.1.1.1       50   Bkup   8    DOWN  000232303230       STDBY
38c8.5cac.4a62   156.1.3.1       56   Prim*       UP    000232303231       UP
                 123.1.1.1       40   Bkup   1    UP    000232303230       STDBY

When the local state of the modem is DOWN, the L2VPN is not configured on the WAN interface
 and the remote state of the L2VPN will be shown as OFF.

Router#show cable l2-vpn xconnect mpls-vc-map state
MAC Address     Peer IP Address VCID Type   Prio State Customer Name/VPNID State
602a.d083.2e1c  123.1.1.1       60   Prim*       OFF                DOWN
38c8.5cac.4a62  123.1.1.1       20   Prim*       UP    000232303230 UP
38c8.5cac.4a62  156.1.3.1       56   Prim*       UP    000232303231 UP
```

擬似回線冗長性が設定されている場合、CM の特定の MAC アドレスについて MPLS 擬似回線マッピングの情報を確認するには、次の例に示すように **showcablel2-vpnxconnectmpls-vc-map** コマンドを使用します。

```
Router# show cable l2-vpn xconnect mpls-vc-map 0025.2e2d.7252
MAC Address    Peer IP Address VCID Type  Prio CktID     Cable Intf SID Customer Name/VPNID
0025.2e2d.7252 10.76.2.1       400  Prim*      Bu254:400 Cable8/0/3 1
               10.76.2.1       600  Bkup  4    Bu254:600
```

擬似回線冗長性が設定されている場合、CM の MPLS 擬似回線マッピングの詳細情報を確認するには、次の例に示すように **showmplsl2-vpnxconnectmpls-vc-mapverbose** コマンドを使用します。

次の例では、バックアップピアコマンドを使用して設定した擬似回線のモデムの情報を示しています。

```
Router# show cable l2-vpn xconnect mpls-vc-map 0025.2e2d.7252 verbose
MAC Address                         : 0025.2e2d.7252
Customer Name                       :
Prim Sid                            : 1
Cable Interface                     : Cable8/0/3
MPLS-EXP                            : 0
PW TYPE                             : Ethernet
Backup enable delay                 : 0 seconds
Backup disable delay                : 0 seconds
Primary peer
Peer IP Address (Active)            : 10.76.2.1
XConnect VCID                       : 400
Circuit  ID                         : Bu254:400
Local State                         : UP
Remote State                        : UP
Backup peers
Peer IP Address                     : 10.76.2.1
XConnect VCID                       : 600
Circuit  ID                         : Bu254:600
Local State                         : STDBY
Remote State                        : UP
Priority                            : 4
Total US pkts                       : 0
Total US bytes                      : 0
Total US pkts   discards            : 0
Total US bytes  discards            : 0
Total DS pkts                       : 0
Total DS bytes                      : 0
Total DS pkts   discards            : 0
Total DS bytes  discards            : 0
```

次の例では、モデムコンフィギュレーションファイルを使用して作成した擬似回線のモデムの情報を示しています。

```
Router# show cable l2-vpn xconnect mpls-vc-map 0014.f8c1.fd46 verbose
MAC Address                         : 0014.f8c1.fd46
Prim Sid                            : 3
Cable Interface                     : Cable8/0/0
L2VPNs provisioned                  : 1
DUT Control/CMIM                    : Disable/0x8000FFFF
VPN ID                              : 2020
L2VPN SAID                          : 12289
Upstream SFID Summary               : 15
Downstream CFRID[SFID] Summary      : Primary SF
CMIM                                : 0x60
PW TYPE                             : Ethernet
MPLS-EXP                            : 0
Backup enable delay                 : 3 seconds
Backup disable delay                : 1 seconds
Primary peer
Peer IP Address (Active)            : 10.2.3.4
```

```
XConnect VCID                       : 1000
Circuit  ID                         : Bu254:1000
Local State                         : UP
Remote State                        : UP

Backup peers
Peer IP Address                     : 10.2.3.4
XConnect VCID                       : 21
Circuit  ID                         : Bu254:21
Local State                         : STDBY
Remote State                        : DOWN
Priority                            : 2
Peer IP Address                     : 10.76.2.1
XConnect VCID                       : 1800
Circuit  ID                         : Bu254:1800
Local State                         : STDBY
Remote State                        : DOWN
Priority                            : 5
Peer IP Address                     : 10.76.2.1
XConnect VCID                       : 45454
Circuit  ID                         : Bu254:45454
Local State                         : STDBY
Remote State                        : DOWN
```

オンライン モデムのすべての接続回線および擬似回線の情報を確認するには、次の例に示すように **showxconnect** コマンドを使用します。

```
Router# show xconnect all
Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  RV=Recovering      NH=No Hardware
XC ST  Segment 1                         S1 Segment 2                          S2
------+--------------------------------+--+--------------------------------+--
UP     ac   Bu254:2001(DOCSIS)           UP mpls 10.76.1.1:2001               UP
UP     ac   Bu254:2002(DOCSIS)           UP mpls 10.76.1.1:2002               UP
UP     ac   Bu254:2004(DOCSIS)           UP mpls 10.76.1.1:2004               UP
DN     ac   Bu254:22(DOCSIS)             UP mpls 101.1.0.2:22                 DN
```

Cisco CMTS ルータ上のレイヤ 2 パケットのルーティングが有効になっている MPLS 仮想回線と静的擬似回線の情報を確認するには、次の例に示すように **showmplsl2transportvc** コマンドを使用します。

```
Router# show mpls l2transport vc
Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Bu254          DOCSIS 2002                10.76.1.1       2002       UP
Bu254          DOCSIS 2003                10.76.1.1       2003       UP
Bu254          DOCSIS 2004                10.76.1.1       2004       DOWN
Bu254          DOCSIS 2017                10.76.1.1       2017       UP
Bu254          DOCSIS 2018                10.76.1.1       2018       UP
Bu254          DOCSIS 2019                10.76.1.1       2019       UP
```

その他の参考資料

標準

規格	タイトル
CM-SP-L2VPN-I08-080522	『*Business Services over DOCSIS (BSOD) Layer 2 Virtual Private Networks*』

規格	タイトル
L2VPN-N-10.0918-2	『*L2VPN MPLS Update*』

MIB

MIB	MIB のリンク
• DOCS-L2VPN-MIB • CISCO-IETF-PW-MIB • CISCO-CABLE-L2VPN-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFC

RFC	タイトル
RFC 3985	『*Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture*』
RFC 4385	『*Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN*』
RFC 4446	『*IANA Allocations for Pseudowire Edge-to-Edge Emulation (PWE3)*』
RFC 4447	『*Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*』
RFC 4448	『*Encapsulation Methods for Transport of Ethernet over MPLS Networks*』
RFC 5085	『*Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ケーブル L2VPN 用 MPLS 擬似回線に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *110*：ケーブル *L2VPN* 用 *MPLS* 擬似回線に関する機能情報

機能名	リリース	機能情報
ケーブル L2VPN 用 MPLS 擬似回線	Cisco IOS XE Everest 16.6.1	この機能は、 Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 42 章

MPLS VPN ケーブルの機能拡張

この機能モジュールでは、マルチプロトコル ラベル スイッチング バーチャル プライベート ネットワーク（MPLS VPN）と、ケーブル インターフェイス バンドリング機能について説明します。MPLS プロトコル、ケーブル インターフェイス、バンドル インターフェイス、およびサブバンドル インターフェイスを使用して VPN を作成する方法を説明します。VPN はさまざまなプロトコルを使用して多くの方法で作成できます。

機能情報の確認

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *111* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

機能の概要

MPLS VPN テクノロジーを使用して、サービス プロバイダーは共有光同軸ハイブリッド（HFC）ネットワークとインターネット プロトコル（IP）インフラストラクチャを使用してスケーラブルかつ効率的にプライベート ネットワークを作成できます。

ケーブルの MPLS VPN ネットワークは、次の要素で構成されます。

- ケーブルおよびIPバックボーンを介してトラフィックを伝送するためにインターネット サービス プロバイダー（ISP）の VPN を作成し、物理インフラストラクチャを持つマルチプル サービス オペレータ（MSO）またはケーブル会社。
- HFC ネットワークおよび IP インフラストラクチャを使用して、ケーブル カスタマーにインターネット サービスを提供する ISP。

各 ISP は、MSO の物理ネットワーク インフラストラクチャを通じて加入者の PC と ISP のネットワークとの間でトラフィックを転送します。MPLS VPN は、レイヤ 3 で作成され、VPN のルートの振り分けをそのネットワークに属するルータだけに制限することで、プライバシーとセキュリティを提供します。したがって、各 ISP の VPN は同じ MSO インフラストラクチャを使用する他の ISP から絶縁されています。

MPLS VPN は、各 VPN に固有の VPN ルーティングおよび転送（VRF）インスタンスを割り当てます。VRF インスタンスは、1 つの IP ルーティング テーブル、取得された転送テーブル、フォワーディング テーブルを使用する一連のインターフェイス、および転送テーブルの内容を決定する一連のルールとルーティング プロトコルで構成されています。

各 PE ルータは 1 つ以上の VRF テーブルを維持します。適切な VRF テーブルでパケットの IP 宛先アドレスを検索するのは、パケットがそのテーブルに関連付けられたインターフェイスから直接到着した場合だけです。

MPLS VPN は BGP と IP アドレス解決の組み合わせを使用してセキュリティを保証します。「*Configuring Multiprotocol Label Switching*」を参照してください。

表はケーブル MPLS VPN ネットワークを示しています。ネットワーク内のルータは以下のとおりです。

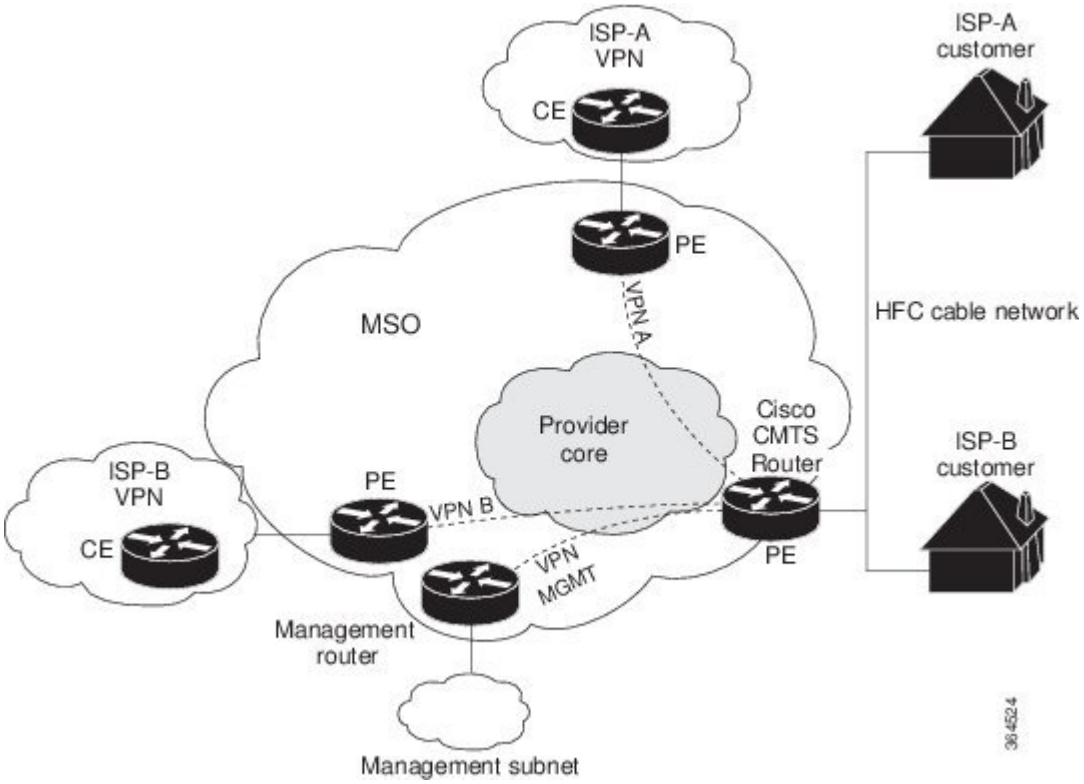
- プロバイダー（P）ルータ：プロバイダー ネットワークのコア内のルータ。P ルータは MPLS スイッチングを実行し、ルーティングされるパケットに VPN ラベル（PE ルータによって割り当てられた、各ルート内の MPLS ラベル）を付加しません。VPN ラベルは、データ パケットを正しい出力ルータに誘導するために使用されます。
- プロバイダーエッジ（PE）ルータ：着信パケットが受信されるインターフェイスまたはサブインターフェイスに基づいて、着信パケットに VPN ラベルを追加するルータ。PE ルータは、CE ルータに直接接続します。MPLS-VPN 手法では、それぞれの Cisco CMTS ルータが PE ルータとして動作します。
- カスタマー（C）ルータ：ISP または企業ネットワークのルータ。
- カスタマー エッジ（CE）ルータ：MSO のネットワークの PE ルータに接続する ISP のネットワークのエッジ ルータ。CE ルータは、PE ルータとインターフェイスする必要があります。

MPLS ネットワークには固有の VPN があり、この VPN は排他的に MSO デバイスを管理するため、管理 VPN と呼ばれます。その他の VPN がアクセスできるデバイス、およびサーバが含まれます。管理 VPN は、Cisco Network Registrar（CNR）サーバや Time-of-Day（ToD）サーバなどの管理サーバに接続する PE ルータに対して Cisco CMTS ルータを接続します。PE ルータは、管理サーバに接続し、管理 VPN の一部です。属する ISP に関係なく、管理サーバは PC やケーブル モ

デムから受信する Dynamic Host Configuration Protocol（DHCP）、DNS（ドメイン ネーム システム）、および TOD 要求を処理します。

（注） MPLS VPN を設定する場合、管理 VPN の一部として作成された最初のサブインターフェイスを設定する必要があります。

図 *24*：*MPLS VPN* ネットワーク



ケーブル VPN 設定には、次のものがあります。

- 各企業ネットワークへの直接ピアリングが必要な MSO ドメイン（ISP）、個人用および商用の加入者向けプロビジョニング サーバ、商用ユーザ向けのダイナミック DNS。MSO は、ケーブル インターフェイス IP アドレッシング、Data-over-Cable Service Interface Specifications（DOCSIS）のプロビジョニング、CM ホスト名、ルーティングの修正、特権レベル、およびユーザ名とパスワードを管理します。
- 加入者または在宅勤務者のホスト デバイス用の DHCP サーバ、MSO アドレス空間内のエンタープライズ ゲートウェイ、および在宅勤務者のサブネットに戻るスタティック ルートがある、ISP またはエンタープライズ ドメイン。

（注） シスコは、MSOでエンドユーザデバイスとゲートウェイインターフェイスにすべてのアドレスを割り当てることを推奨します。MSO では分割管理を使用して ISP でトンネルとセキュリティを設定できるようにすることもできます。

MPLS VPN 設定では、MSO は次を設定する必要があります。

- CMTS
- P ルータ
- PE ルータ
- CE ルータ
- すべてのケーブル モデム顧客について ISP DOCSIS サーバあたり 1 つの VPN。MSO は管理 VPN に DOCSIS サーバを接続し、認識されるようにする必要があります。

MSO は、ISP、およびその ISP に接続するリモート PE ルータを VPN の PE ルータとして機能させるような Cisco CMTS ルータを設定する必要があります。

MSO は、すべてのケーブル モデムのプライマリ IP アドレス範囲を決定する必要があります。

ISP は、加入者 PC のセカンダリ IP アドレス範囲を決定する必要があります。

セキュリティ違反を減らし、VPN または特定の ISP 管理でケーブル モデムからの DHCP 要求を区別するために、MSO は Cisco IOS-XE ソフトウェアの **cablehelper-address** コマンドを使用できます。MSO は、ISP の VPN でのみアクセスできるようにホスト IP アドレスを指定できます。これにより、ISP はその DHCP サーバを使用して IP アドレスを割り当てることができるようになります。ケーブル モデム IP アドレスは、管理 VPN からアクセスできることが必要です。

個々の ISP またはお客様に対して VPN を作成する MPLS VPN の手法では、サブインターフェイスを仮想バンドル インターフェイスに設定する必要があります。各 ISP には 1 つのサブインターフェイスが必要です。サブインターフェイスは、それぞれの ISP の VPN ルーティングおよび転送（VRF）テーブルに関連付けられます。最初のサブインターフェイスは、管理VPNにバインドされたケーブル インターフェイス上で作成する必要があります。

CNR からの応答をケーブル モデムにルーティングするには、CNR に接続する PE ルータが管理 VPN への ISP VPN のルートをインポートする必要があります。同様に、管理要求（CNR への DHCP 更新など）をケーブル モデムに転送するには、ISP VPN が適切な管理 VPN ルートをエクスポートおよびインポートする必要があります。

各ルータに必要なサブネットが 1 つだけになるように Cisco CMTS ルータ上のすべてのケーブル インターフェイスを単一バンドルにグループ化できます。ケーブル インターフェイスをグループ化すると、別のIPサブネットまたは個々のケーブルインターフェイスは不要です。このグループ化により、特に多くの加入者のためのサブネットを管理するブリッジング ソリューションを使用する際のパフォーマンス、メモリ、およびセキュリティの問題が回避されます。

サブインターフェイスを使用して、トラフィックを単一の物理インターフェイスで区別し、複数の VPN に割り当てることができます。複数のサブインターフェイスを設定し、各サブインターフェイスに MPLS VPN を関連付けることができます。1 つの物理インターフェイス（ケーブル設備）を複数のサブインターフェイスに分割できます。この場合、各サブインターフェイスは特定

の VPN に関連付けられます。各 ISP は、物理インターフェイス上でアクセスすることが必要で、各自のサブインターフェイスが与えられます。管理サブインターフェイスを作成して、ISP からのケーブル モデムの初期化をサポートしてください。

特定の VPN の（および ISP）加入者に関連付けられた各サブインターフェイスを使用して、加入対象のサービスを提供する ISP を反映する論理サブインターフェイスに接続します。適切に設定されると、加入者トラフィックは適切なサブインターフェイスと VPN に入ります。

利点

- MPLS VPN は、ケーブル MSO および ISP に、ケーブル設備への複数のアクセスをサポートする管理可能な方法を提供します。サービス プロバイダーは、ネットワークのコア全体でスケーラブルで効率的な VPN を作成できます。MPLS VPN を使用するシステムは、ケーブル転送インフラストラクチャと管理における拡張性をサポートします。
- 各 ISP は、加入者の PC から MSO の物理ケーブル設備を経由して ISP のネットワークに至るインターネット アクセス サービスをサポートできます。
- MPLS VPN により、MSO は ISP を介して付加価値のあるサービスを提供できるようになるため、より広い範囲の潜在顧客に接続を提供できます。MSO は ISP と連携して複数の ISP から複数のサービスを配信し、VPN 技術を使用して MSO の独自のネットワーク内の値を追加できます。
- 加入者はさまざまなサービス プロバイダーからのサービスを組み合わせて選択できます。
- サービスを確保するために CMTS DOCSIS 1.0 および DOCSIS 1.0 拡張にビルドされた MPLS VPN ケーブル機能セットは信頼でき、ケーブル設備を介して配信するのが最適です。MPLS VPN は、システム サポートのドメイン選択、加入者ごとの認証、QoS の選択、ポリシーベース ルーティング、および QoS と課金のためにケーブル モデムの背後にある加入者エンド デバイスに到達する機能を提供し、同時にセッション スプーフィングを防止しています。
- MPLS VPN テクノロジーは、共有ケーブル インフラストラクチャ全体にわたるセキュアなアクセスとサービスの整合性の両方を実現します。
- ケーブル インターフェイスのバンドリングにより、各ケーブル インターフェイス上での IP サブネットの必要がなくなります。代わりに、IP サブネットは各ケーブル インターフェイス バンドルにのみ必要です。Cisco CMTS ルータのすべてのケーブル インターフェイスを 1 つのバンドルに追加できます。

制限事項

- CMTS の各サブインターフェイスは、ISP および MSO によるアドレス範囲を必要とします。これら 2 つの範囲は重複してはならず、拡張性に関しては加入者の増加をサポートするために拡張可能である必要があります。

（注） このマニュアルでは、MSO および ISP IP アドレスのアドレス割り当てと管理については記載していません。この情報については、「*Configuring Multiprotocol Label Switching*」を参照してください。

- **cablesource-verifydhcp** コマンドにより、CMTS から DHCP サーバへの Dynamic Host Control Protocol（DHCP）のリースクエリ プロトコルが有効になります。これにより、アップストリーム トラフィックの IP アドレスを確認して、MSO の顧客が承認されない、スプーフィングされた、または盗難された IP アドレスを使用するのを防ぐことができます。
- MPLS VPN のみを使用している場合、仮想バンドルにサブインターフェイスを作成して IP アドレスを割り当て、各 ISP に VRF 設定を提供します。サブインターフェイスを作成して MPLS VPN のみを設定している場合、ケーブル インターフェイス バンドリング機能は MPLS VPN と無関係に動作します。
- ケーブル インターフェイス バンドリングを使用する場合は、次の手順を行ってください。
  - 仮想バンドル インターフェイスを定義し、仮想バンドルにいずれかの物理ケーブル インターフェイスを関連付けます。
  - 仮想バンドル インターフェイスで、すべての汎用 IP ネットワーク情報（IP アドレス、ルーティング プロトコル、スイッチング モードなど）を指定します。バンドル スレーブ インターフェイスで汎用 IP ネットワーク情報を指定しないでください。
  - サブインターフェイスが定義されたインターフェイスは、バンドルの一部にできません。
  - source-verify や ARP 処理など、汎用（ダウンストリームまたはアップストリームに関係しない）ケーブル インターフェイス設定を仮想バンドル インターフェイスで指定します。バンドル スレーブ インターフェイスで汎用設定を指定しないでください。
- インターフェイス バンドルは、コマンド ライン インターフェイス（CLI ベースの HTML 設定を含む）の使用によってのみ設定できます。

前提条件

IP ベース VPN を設定する前に、次の作業を実行します。

- ネットワークで信頼性の高いブロードバンドデータ伝送がサポートされていることを確認します。使用する設備は、National Television Standards Committee（NTSC）または該当する国際ケーブル設備勧告に基づいて、クリーンに保たれ、安定化され、認定を受けている必要があります。使用するプラントがすべての DOCSIS または European Data-over-Cable Service Interface Specifications（EuroDOCSIS）ダウンストリームおよびアップストリーム RF 要件を満たしていることを確認します。
- 『Hardware Installation Guide』および『Regulatory Compliance and Safety Information guide』の手順に従って Cisco ルータが設置されていることを確認します。

- Cisco ルータが基本動作用に設定されていることを確認します。
- シャーシには、少なくともバックボーン接続を提供する 1 つのポート アダプタと、RF ケーブル TV インターフェイスとして動作する 1 つの Cisco ケーブル モデム カードが搭載されている必要があります。

その他の重要情報

- その他の必要なヘッドエンドまたは配線ハブ ルーティングおよびネットワーク インターフェイス装置がすべて設置され、設定され、サポートされているサービスに基づいて動作できる状態になっていることを確認します。これには、すべてのルータ、サーバ（DHCP、TFTP、ToD）、ネットワーク管理システム、その他の設定または課金システムやバックボーン、VPN をサポートする他の機器が含まれます。
- DHCP および DOCSIS コンフィギュレーション ファイルが作成され、各ケーブル モデムなどの適切なサーバに転送されて、初期化時に、DHCP 要求の送信、IP アドレスの受信、TFTP および ToD サーバ アドレスの取得、ネットワーク内の DOCSIS コンフィギュレーション ファイルのダウンロードが可能であることを確認します。ISP の VPN に接続できるように各サブインターフェイスを設定します。
- DOCSIS サーバが管理 VPN に表示されることを確認します。
- 適切な周波数を割り当てるために、チャネル計画について理解しておく必要があります。使用するヘッドエンドまたは配線ハブに該当する場合、バンドリングまたは VPN のおおまかなセットアップ方針を作成します。必要に応じて、パスワード、IP アドレス、サブネット マスク、デバイス名を入手します。
- 仮想バンドル インターフェイスのサブインターフェイスを作成します。ISP のネットワークに接続できるように各サブインターフェイスを設定します。

MPLS VPN 設定手順の前提条件は次のとおりです。

- IP アドレッシングがすでに定義されており、特定のサブインターフェイスに対して MSO および ISP ネットワークの範囲が割り当てられている。
- MSO で CNR を使用し、（**cablehelper-address** コマンドを使って）ケーブル モデム MAC アドレスに基づいてケーブル モデムに適切な IP アドレスを付与するように設定済みである。CMTS は、**cablehelper-address** 設定に基づいて CNR に DHCP 要求を転送します。CNR サーバは、client-class 機能を使用してケーブル モデムを割り当てる IP アドレスを決定します。これにより、CNR は MAC アドレスに基づいたデバイスに特定のパラメータを割り当てられます。
- ISP CE ルータが、（**cablehelper-address** コマンドを使用して）該当する IP アドレス範囲を VPN に適切にルーティングできるように設定されている。
- P および PE ルータで Cisco Express Forwarding（CEF）をすでに実行している。
- MPLS が、インターフェイス コンフィギュレーション モードで **tagswitchingip** コマンドを使用して送信 VPN 上で設定されている。

設定作業

MPLS VPN を設定するには、次のタスクを実行します。

各 VPN 用の VRF の作成

各 VPN の VRF を作成するには、まずルータ コンフィギュレーション モードで次の手順を実行します。

（注） CMTS のみに論理サブインターフェイスがあるため、他の PE デバイスの VRF は特定の物理インターフェイスに割り当てられます。

手順

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **vrf definition** *mgmt-vpn*	VRF コンフィギュレーション モード (config-vrf)# を開始し、VRF テーブルを VPN（*mgmt-vpn* で指定）にマッピングします。管理 VPN は最初に設定した VPN です。
ステップ 2	Router(config-vrf)# **rd** *mgmt-rd*	ルート識別子を管理VPNに割り当て、ルーティングと転送のテーブルを作成します。
ステップ 3	Router(config-vrf)# **route-target**{**export**| **import**| **both**} *mgmt-rd*	管理VPNのルート識別子についてすべてのルートをエクスポートおよびインポートします。これにより、VRF内で共有するルートが決まります。
ステップ 4	Router(config-vrf)# **route-targetimport** isp1-vpn-rd	VPN（*isp1-vpn*）ルート識別子のすべてのルートをインポートします。
ステップ 5	Router(config-vrf)# **route-targetimport** isp2-vpn-rd	VPN（*isp2-vpn*）ルート識別子のすべてのルートをインポートします。
ステップ 6	Router(config-vrf)# **vrf definition** isp1-vpn	ルート識別子を管理*isp1-vpn*に割り当て、ルーティングと転送のテーブルを作成します。
ステップ 7	Router(config-vrf)# **rd** *mgmt-rd*	ルート識別子（mgmt-rd）を管理 VPN（mgmt-vpn）に割り当て、ルーティングと転送のテーブルを作成します。
ステップ 8	Router(config-vrf)# **route-targetexport** isp1-vpn-rd	VPN（*isp1-vpn*）ルート識別子のすべてのルートをエクスポートします。

	コマンドまたはアクション	目的
ステップ 9	Router(config-vrf)# **route-targetimport** isp1-vpn-rd	VPN（*isp1-vpn*）ルート識別子のすべてのルートをインポートします。
ステップ 10	Router(config-vrf)# **route-targetimport** mgmt-vpn-rd	VPN（*mgmt-vpn*）ルート識別子のすべてのルートをエクスポートします。
ステップ 11	Router(config-vrf)# **vrf definition** isp2-vpn	ルート識別子を管理 *isp2-vpn* に割り当て、ルーティングと転送のテーブルを作成します。
ステップ 12	Router(config-vrf)# **route-targetexport** isp2-vpn-rd	VPN（*isp2-vpn*）ルート識別子のすべてのルートをエクスポートします。
ステップ 13	Router(config-vrf)# **route-targetimport** isp2-vpn-rd	VPN（*isp2-vpn*）ルート識別子のすべてのルートをインポートします。
ステップ 14	Router(config-vrf)# **route-targetimport** mgmt-vpn-rd	VPN（*mgmt-vpn*）ルート識別子のすべてのルートをインポートします。

仮想バンドル インターフェイスのサブインターフェイスの定義と VRF の割り当て

論理ケーブル サブインターフェイスを作成するには、まずグローバル コンフィギュレーション モードで次の手順を実行します。各 VPN（1 つの ISP に 1 つ）にサブインターフェイスを 1 つ作成します。作成した最初のサブインターフェイスは、管理VPNの一部として設定する必要があります（サブインターフェイス最小番号を付与）。

手順

	コマンドまたはアクション	目的
ステップ 1	Router# **configureterminal**	コンフィギュレーション モードに入ります。
ステップ 2	Router(config)# **interfacebundlen.***x*	仮想バンドルインターフェイス コンフィギュレーション モードを開始し、サブインターフェイス最小番号が付与された最初の（Management）サブインターフェイスを定義します。
ステップ 3	Router(config-subif)# **description** *string*	サブインターフェイスを管理サブインターフェイスとして特定します。

	コマンドまたはアクション	目的
ステップ 4	Router(config-subif)# **vrfforwarding** *mgmt-vpn*	サブインターフェイスを管理 VPN（顧客にサービスを提供する MSO で使用される MPLS VPN）に割り当てます。
ステップ 5	Router(config-subif)# **ipaddress** *ipaddress mask*	サブインターフェイスに IP アドレスおよびサブネット マスクを割り当てます。
ステップ 6	Router(config-subif)# **cablehelper-address** *ip-address* **cable-modem**	ケーブル モデムからリスト内の IP アドレスに DHCP 要求を転送します。
ステップ 7	Router(config-subif)# **cablehelper-address** *ip-address* **host**	ホストからリスト内の IP アドレスに DHCP 要求を転送します。
ステップ 8	Router(config-if)# **interfacebundlen.***x*	ISP の追加サブインターフェイスを定義します（isp1 など）。
ステップ 9	Router(config-subif)# **description** *string*	サブインターフェイス（*isp1-vpn* のサブインターフェイスなど）を特定します。
ステップ 10	Router(config-subif)# **vrfforwarding** *isp1-vpn*	サブインターフェイスを *isp1-vpn* VPN に割り当てます。
ステップ 11	Router(config-subif)# **ipaddress** *ipaddress mask*	サブインターフェイスに IP アドレスおよびサブネット マスクを割り当てます。
ステップ 12	Router(config-subif)# **cablehelper-address** *ip-address* **cable-modem**	ケーブル モデムからリスト内の IP アドレスに DHCP 要求を転送します。
ステップ 13	Router(config-subif)# **cablehelper-address** *ip-address* **host**	ホストからリスト内の IP アドレスに DHCP 要求を転送します。
ステップ 14	Router(config-if)# **interfacebundlen.***x*	ISP の追加サブインターフェイスを定義します（isp2 など）。
ステップ 15	Router(config-subif)# **description** *string*	サブインターフェイス（*isp2-vpn* のサブインターフェイスなど）を特定します。
ステップ 16	Router(config-subif)# **vrfforwarding** *isp2-vpn*	サブインターフェイスを *isp2-vpn* VPN に割り当てます。
ステップ 17	Router(config-subif)# **ipaddress** *ipaddress mask*	サブインターフェイスに IP アドレスおよびサブネット マスクを割り当てます。
ステップ 18	Router(config-subif)# **cablehelper-address** *ip-address* **cable-modem**	ケーブル モデムからリスト内の IP アドレスに DHCP 要求を転送します。

	コマンドまたはアクション	目的
ステップ 19	Router(config-subif)# **cablehelper-address** *ip-address* **host**	ホストからリスト内の IP アドレスに DHCP 要求を転送します。
ステップ 20	Router(config)# **exit**	コンフィギュレーション モードに戻ります。

ケーブル インターフェイス バンドルの設定

ケーブル インターフェイスをバンドルに割り当てるには、まずインターフェイス コンフィギュレーション モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	Router(config)# **interface cable** *slot/port*	ケーブル インターフェイス コンフィギュレーション モードを開始します。 IP アドレスはこのインターフェイスに割り当てられていません。このインターフェイス内で作成された論理サブインターフェイスに割り当てられます。
ステップ 2	Router(config-if)# **cablebundle***bundle-number*	インターフェイスをバンドル インターフェイスに定義します。
ステップ 3	Router(config)# **interface cable** *slot/subslot/port*	別のケーブル インターフェイスに対してケーブル インターフェイス コンフィギュレーション モードを開始します。 IP アドレスはこのインターフェイスに割り当てられていません。このインターフェイス内で作成された論理サブインターフェイスに割り当てられます。
ステップ 4	Router(config-if)# **cablebundle** *bundle-number*	*bundle-number* で指定されたバンドルにインターフェイスを追加します。

仮想バンドル インターフェイスでのサブインターフェイスと MPLS VPN の設定

仮想バンドル インターフェイスでサブインターフェイスを設定し、各サブインターフェイスにレイヤ 3 設定を割り当てる方法は、次のとおりです。

ケーブル インターフェイス バンドルを設定します。

仮想バンドル インターフェイスでサブインターフェイスを定義し、各サブインターフェイスにレイヤ 3 設定を割り当てます。

各顧客の VPN に 1 つ（ISP ごとに 1 つ）のサブインターフェイスを作成します。

プロバイダー コアにある P ルータの MPLS の設定

プロバイダー コアの P ルータで MPLS を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	Router# **configureterminal**	コンフィギュレーション モードに入ります。
ステップ 2	Router(config)#**ipcef**	Cisco Express Forwarding（CEF）の動作を有効にします。 CEF設定およびコマンド構文の詳細については、Cisco Express Forwarding の概要と設定を参照してください。
ステップ 3	Router(config)#**interfaceTengigabitethernet** *slot/subslot/port*	GigabitEthernet インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	Router(config-if)#**ipaddress** *ip-address mask*	インターフェイスのプライマリ IP アドレス範囲を定義します。
ステップ 5	Router(config-if)#**mplsip**	MPLSパケットに転送されるようにインターフェイスを有効にします。
ステップ 6	Router(config-if)#**exit**	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	Router(config)#**mpls label-protocol ldp**	ラベル配布プロトコル（LDP）を有効にします。 LDP と MPLS の詳細については、「Configuring Multiprotocol Label Switching」を参照してください。
ステップ 8	Router(config)# **exit**	コンフィギュレーション モードに戻ります。

MPLS VPN 設定の確認

PE ルータ上の MPLS VPN の動作を確認するには、次のコマンドを使用します。MPLS VPN の検証コマンドの詳細については、「Configuring Multiprotocol Label Switching」を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	Router# **showipvrf**	VRF とインターフェイスを表示します。
ステップ 2	Router# **showiproutevrf[vrf-name]**	VRF の IP ルーティング テーブルを表示します。
ステップ 3	Router# **showipprotocolsvrf[vrf-name]**	VRF に対応するルーティング プロトコル情報を表示します。
ステップ 4	Router# **show ip route vrf** *vrf-name*	PE ルーティング テーブル内にあるローカルおよびリモートの CE デバイスを表示します。
ステップ 5	Router# **show mpls forwarding-table**	VPN ルーティング/転送インスタンスのエントリを表示します。

次の作業

検証説明の詳細については、『MPLS: Layer 3 VPNs Configuration Guide』を参照してください。

設定例

ここでは、次の設定例について説明します。

VRF 定義設定

```
vrf definition Basketball
 rd 100:2
 route-target export 100:2
 route-target import 100:0
 route-target import 100:2
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
vrf definition Football
 rd 100:1
 route-target export 100:1
 route-target import 100:0
 route-target import 100:1
```

```
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
vrf definition MGMT
 rd 100:0
 route-target export 100:0
 route-target import 100:0
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
vrf definition Mgmt-intf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
vrf definition Tennis
 rd 100:4
 route-target export 100:4
 route-target import 100:0
 route-target import 100:4
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
vrf definition Volleyball
 rd 100:3
 route-target export 100:3
 route-target import 100:0
 route-target import 100:3
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
```

ケーブル バンドル サブインターフェイスの設定

```
interface Bundle255
 description Bundle Master Interface
 no ip address
 cable arp filter request-send 3 2
 cable arp filter reply-accept 3 2

interface Bundle255.1
 description Management Interface
 vrf forwarding MGMT
 ip address 112.51.0.1 255.255.0.0
 cable helper-address 20.11.0.162
 ipv6 address 2001:100:112:B001::1/64

interface Bundle255.2
 vrf forwarding Basketball
 ip address 112.54.0.1 255.255.0.0 secondary
 ip address 112.53.0.1 255.255.0.0
 cable helper-address 20.11.0.62
 cable helper-address 20.11.0.162
 ipv6 address 2001:100:112:B003::1/64
 ipv6 address 2001:100:112:B004::1/64
```

```
interface Bundle255.3
 vrf forwarding Football
 ip address 112.56.0.1 255.255.0.0 secondary
 ip address 112.55.0.1 255.255.0.0
 cable helper-address 20.11.0.62
 cable helper-address 20.11.0.162
 ipv6 address 2001:100:112:B005::1/64
 ipv6 address 2001:100:112:B006::1/64

interface Bundle255.4
 vrf forwarding Volleyball
 ip address 112.58.0.1 255.255.0.0 secondary
 ip address 112.57.0.1 255.255.0.0
 cable helper-address 20.11.0.62
 cable helper-address 20.11.0.162
 ipv6 address 2001:100:112:B007::1/64
 ipv6 address 2001:100:112:B008::1/64

interface Bundle255.5
 vrf forwarding Tennis
 ip address 112.61.0.1 255.255.0.0 secondary
 ip address 112.60.0.1 255.255.0.0 secondary
 ip address 112.59.0.1 255.255.0.0
 cable helper-address 20.11.0.162
 ipv6 address 2001:100:112:B009::1/64
 ipv6 address 2001:100:112:B00A::1/64
```

PE WAN インターフェイスの設定

```
mpls label protocol ldp
mpls ldp nsr
mpls ldp graceful-restart

interface TenGigabitEthernet4/1/1
 description WAN connection to cBR8
 mtu 4470
 ip address 100.6.120.5 255.255.255.252
 ip router isis hub
 ipv6 address 2001:100:6:120::5:1/112
 ipv6 enable
 mpls ip
 mpls traffic-eng tunnels
 cdp enable
 isis circuit-type level-1
 isis network point-to-point
 isis csnp-interval 10
 hold-queue 400 in
 ip rsvp bandwidth 1000000
end
```

PE BGP の設定

```
router bgp 100
 bgp router-id 100.120.120.120
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 timers bgp 5 60
 neighbor 100.100.4.4 remote-as 100
 neighbor 100.100.4.4 ha-mode sso
 neighbor 100.100.4.4 update-source Loopback0
 neighbor 100.100.4.4 ha-mode graceful-restart
 !
 address-family ipv4
```

```
 redistribute connected
 redistribute static route-map static-route
 redistribute rip
 neighbor 100.100.4.4 activate
 neighbor 100.100.4.4 send-community extended
 neighbor 100.100.4.4 next-hop-self
 neighbor 100.100.4.4 soft-reconfiguration inbound
 maximum-paths ibgp 2
exit-address-family
!
address-family vpnv4
 neighbor 100.100.4.4 activate
 neighbor 100.100.4.4 send-community extended
exit-address-family
!
address-family ipv6
 redistribute connected
 redistribute rip CST include-connected
 redistribute static metric 100 route-map static-route-v6
 neighbor 100.100.4.4 activate
 neighbor 100.100.4.4 send-community extended
 neighbor 100.100.4.4 send-label
exit-address-family
!
address-family vpnv6
 neighbor 100.100.4.4 activate
 neighbor 100.100.4.4 send-community extended
exit-address-family
!
address-family ipv4 vrf Basketball
 redistribute connected
exit-address-family
!
address-family ipv6 vrf Basketball
 redistribute connected
 redistribute static metric 100
exit-address-family
!
address-family ipv4 vrf Football
 redistribute connected
exit-address-family
!
address-family ipv6 vrf Football
 redistribute connected
 redistribute static metric 100
exit-address-family
!
address-family ipv4 vrf MGMT
 redistribute connected
exit-address-family
!
address-family ipv6 vrf MGMT
 redistribute connected
exit-address-family
!
address-family ipv4 vrf Tennis
 redistribute connected
 redistribute static route-map static-route
 redistribute rip
exit-address-family
!
address-family ipv6 vrf Tennis
 redistribute connected
 redistribute rip CST include-connected
 redistribute static metric 100 route-map static-route-v6
exit-address-family
!
address-family ipv4 vrf Volleyball
 redistribute connected
 redistribute static route-map static-route
 redistribute rip
exit-address-family
!
```

```
address-family ipv6 vrf Volleyball
 redistribute connected
 redistribute rip CST include-connected
 redistribute static metric 100 route-map static-route-v6
exit-address-family
```

その他の参考資料

標準

規格	タイトル
DOCSIS 1.0	*DOCSIS 1.0*

MIB

MIB	MIB のリンク
CISCO-DOCS-REMOTE-QUERY.my	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://tools.cisco.com/ITDIT/MIBS/servlet/index

RFC

RFC	タイトル
RFC 1163	『A Border Gateway Protocol』
RFC 1164	『Application of the Border Gateway Protocol in the Internet』
RFC 2283	『Multiprotocol Extensions for BGP-4』
RFC 2547	『BGP/MPLS VPNs』
RFC 2233	『DOCSIS OSSI Objects Support』
RFC 2669	『Cable Device MIB』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

MPLS VPN ケーブルの拡張に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *112* : *MPLS VPN* ケーブルの拡張に関する機能情報

機能名	リリース	機能情報
マルチプロトコル ラベル スイッチング バーチャル プライベート ネットワーク（MPLS VPN）	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 43 章

マルチキャスト VPN と DOCSIS 3.0 マルチキャストの QoS サポート

CMTS の拡張されたマルチキャストの新機能は DOCSIS 3.0 仕様に適合しており、次の機能を含みます。

- 拡張されたマルチキャスト エコー。ここで、レイヤ 3 マルチキャスト スイッチング パスは、Cisco Packet Processor（CPP）の Parallel Express Forwarding マルチキャスト ルーティング テーブルを使用します。
- 拡張されたマルチキャスト サービス品質（MQoS）フレームワーク。マルチキャスト アドレス、ルール プライオリティ、それに関連するマルチキャスト VPN（MVPN）のセッション範囲を定義するグループ設定（GC）を指定します。
- マルチキャスト サービス フローを含むインテリジェント型マルチキャスト アドミッション制御。
- 拡張されたマルチキャスト VPN 機能。マルチプロトコル ラベル スイッチング（MPLS）VPN 環境でマルチキャスト トラフィックを設定およびサポートします。

機能情報の確認

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *113* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

マルチキャスト VPN と DOCSIS 3.0 マルチキャストの QoS サポートに関する制限事項

タイプ オブ サービス（TOS）パラメータは、Cisco cBR シリーズ ルータでは認識されません。

40000 個のマルチキャスト セッションを利用するには、各 LC に少なくとも 1 つのバンドルが必要です。

マルチキャスト VPN と DOCSIS 3.0 マルチキャストの QoS サポートに関する情報

IP マルチキャスト（複数のケーブル ネットワーク受信者への同一情報の送信）は、帯域幅の効率を向上させ、サービス プロバイダーがトラフィックの種類に応じて異なる Quality of Service を提供できるようにします。拡張されたマルチキャストにより、DOCSIS 3.0 仕様を実装するうえで要求されるマルチキャストの改良が実装されます。

（注） DOCSIS 3.0 規格は、DOCSIS 2.0 マルチキャスト動作モードへの下位互換性を保持します。

Cisco cBR ルータはシャーシごとに 40000 個の DSG マルチキャスト セッションをサポートします。

CMTS の拡張されたマルチキャストの利点は次のとおりです。

高度な QoS

新しいマルチキャスト QoS（MQoS）フレームワークで、マルチキャスト アドレス、ルール プライオリティ、それに関連するマルチキャスト VPN（MVPN）のセッション範囲を定義するグループ設定（GC）を指定できます。すべての GC にグループ QoS 設定（GQC）とグループ暗号化ルールがあります。

セッション範囲、ルール プライオリティ、および MVPN に基づいて、マルチキャスト サービス フローは GC で許可され、関連する GQC とグループ暗号化ルールがフローに適用されます。MQoS 実装では、ケーブル固有のマルチキャストの現在の実装で IGMP バージョン 2 をサポートしますが、IGMP バージョン 3 はサポートしていないため、マルチキャスト セッションの送信元アドレスがチェックされません。ダウンストリーム サービス フロー、サービス ID（SID）、および MAC 書き換え文字列は、新しい IGMP 加入（またはインターフェイス上の静的マルチキャスト グループ CLI）時に作成され、MQoS は新しいマルチキャスト グループ加入に適用されます。

高度な QoS の利点は次のとおりです。

- グループ分類子は、ケーブル インターフェイス レベルおよびバンドル インターフェイス レベルでも適用できる。
- グループ サービス フロー（GSF）は、サービス クラス名に基づいて定義される。GSF は個別のサービス フローと類似しており、通常はサービス クラスの最小レートと最大レートのパラメータが含まれる。GSF は、同じグループ分類子ルール（GCR）に一致する特定のダウンストリーム チャネル セット（DCS）上のすべてのケーブル モデムで共有されます。デフォルトのサービス フローは、どの GCR にも一致しないマルチキャスト フローに使用されます。GSF は常にアクティブ状態です。
- CMTS はマルチキャスト パケットを複製し、そのパケットを分類する。
- 一段階複製と二段階複製がサポートされている。
- 高度な QoS は、DOCSIS Set-top Gateway（DSG）に対応および統合されている。

インテリジェント型マルチキャスト アドミッション制御

アドミッション制御を使用すると、サービス フローをバケットに分類することができます。分類例としては、サービス フローを作成するためのサービス クラス名、サービス フロー プライオリティ、またはサービスフロータイプ（非送信請求許可サービス（UGS）など）があります。各バケットの帯域幅限度も定義できます。たとえば、バケット 1 を高プライオリティのパケット ケーブル サービス フローに定義して、リンク帯域幅の最小 30 パーセント、最大 50 パーセントをバケット 1 に与えるように指定できます。

インテリジェント型マルチキャスト アドミッション制御は、GSF 概念を使用したマルチキャスト サービス フローの組み込みなどの追加の機能を含みます。GSF は GQC テーブルで定義されたルールに基づいて作成されます。このルールによって、セッション範囲を通じてマルチキャスト ストリームが GSF に関連付けられます。このルールにおけるサービス クラス名が、その GSF の QoS を定義します。さらに、他の属性が、ルールおよびグループ コンフィギュレーション テーブルに追加され、各 GSF が属しているアプリケーション タイプが指定されます。この方法では、各 GSF に関連付けられた QoS は GSF のバケット カテゴリに依存しません。

インテリジェント型マルチキャスト アドミッション制御の利点は次のとおりです。

- 各マルチキャスト セッションの確立を明示的に確認できます。
- アドミッション制御では、最初のフローが確立された後は、マルチキャスト フローに帯域幅をさらに消費することはありません。
- マルチキャスト セッションが切断されるとサービス フローはクリーンアップされます。

マルチキャスト セッション制限のサポート

マルチキャスト ビデオ環境では、特定のサービス フローに許可するマルチキャスト セッションの数を制限できます。マルチキャスト QoS インフラストラクチャの最上位に機能を追加するマルチキャスト セッション制限機能により、特定のサービス フローで許可されるマルチキャスト セッションの数を指定できます。現在のセッション数が定義された制限に達した場合、新しいセッションは転送されますが、いずれかのセッションが終了して新しいセッション用のスロットが解放されるまで、それらはデフォルトのマルチキャスト サービス フローを使用することになります。

マルチキャスト バーチャル プライベート ネットワーク

新しいマルチキャスト VPN（MVPN）機能を使用すると、マルチプロトコル ラベル スイッチング（MPLS）VPN 環境でマルチキャスト トラフィックを設定およびサポートすることができます。この機能は、個々の VPN Virtual Routing and Forwarding（VRF）インスタンスのマルチキャスト パケットのルーティングおよび転送をサポートし、さらにサービス プロバイダーのバックボーン全体に VPN マルチキャスト パケットを転送するメカニズムも提供します。

MVPN により、レイヤ 3 またはレイヤ 2 VPN上で複数のリモート サイトやデバイスを接続することができます。レイヤ 3 VPN は、VPN 内のトラフィックのルーティングを可能にします。レイヤ 2 VPN は、顧客に属するリモート サイト間のトラフィックにブリッジング転送メカニズムを提供します。レイヤ 3 VPN上でのマルチキャストをサポートするため、各 VPN は、プロバイダー エッ

ジ（PE）ルータにより維持される関連の MVPN ルーティングおよび転送（mVRF）テーブルを含む個別のマルチキャスト ドメインを受け取ります。ケーブル環境では、PE ルータはルーティング CMTS です。プロバイダー ネットワークは、関連するすべての mVRF イネーブル PE ルータ間の各 VPN に対し、デフォルトのマルチキャスト配信ツリー（デフォルト MDT）を構築します。このツリーは、すべての PE ルータにマルチキャスト トラフィックを分散するのに使用されます。

VPN 環境で最大のセキュリティとデータ プライバシーを実現するため、CMTS は、異なる VPN に属する同じダウンストリーム インターフェイス上のマルチキャスト セッションを区別します。異なる VPN 間のマルチキャスト トラフィックを区別するために、CMTS には VRF サブインターフェイスごとの BPI+ が有効なマルチキャスト セキュリティ アソシエーション ID（MSAID）割り当て機能が実装されています。MSAID は各サブインターフェイスの各ケーブル バンドル グループに割り当てられます。マルチキャスト グループには、それぞれの VRF インスタンス専用の MSAID が設定されます。

マルチキャスト VPN と DOCSIS 3.0 マルチキャストの QoS サポートの設定方法

ここでは、次の手順について説明します。

マルチキャスト グループの QoS プロファイルの設定

QoS グループの設定に適用できる QoS プロファイルを設定するには、**cablemulticastgroup-qos** コマンドを使用します。QoS プロファイルを QoS マルチキャスト グループに追加するには、QoS プロファイルを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cablemulticastgroup-qos** *number***scn** *service-class-name* **control**{ **single** | **aggregate** [**limit** *max-sessions*]}	マルチキャスト QoS グループに適用できる QoS プロファイルを設定します。

	コマンドまたはアクション	目的
	例： `Router(config)#: cable multicast group-qos 2 scn name1 control single`	（注） 番号が指定されていない場合は、デフォルト QoS プロファイルが適用されます。デフォルトのグループ QoS 設定では、マルチキャスト セッションがインターフェイス上の GC のどの分類子とも一致しない場合に使用される各ケーブル インターフェイスのデフォルトのマルチキャスト サービス フローを作成します。

マルチキャスト QoS グループの設定

マルチキャストアドレス、ルールプライオリティ、それに関連するマルチキャスト VPN（MVPN）のセッション範囲を定義するグループ設定（GC）を指定できます。すべての GC にグループ QoS 設定とグループ暗号化ルールがあります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cablemulticastgroup-qos** *number* **scn** *service-class-name***control** {**single** |**aggregate** [limit *max-sessions*]} 例： `Router(config-mqos)# cable multicast group-qos 5 scn name1 control single`	（任意）マルチキャスト QoS グループに適用できる QoS プロファイルを設定します。 （注） 番号が指定されていない場合は、デフォルト QoS プロファイルが適用されます。デフォルトのグループ QoS 設定では、マルチキャスト セッションがインターフェイス上の GC のどの分類子とも一致しない場合に使用される各ケーブル インターフェイスのデフォルトのマルチキャスト サービス フローを作成します。

	コマンドまたはアクション	目的
ステップ 4	**cablemulticastqosgroup** *id* **priority** *value* [**global**] 例： `Router(config)# cable multicast qos group 2 priority 6`	マルチキャスト QoS グループを設定し、マルチキャスト QoS コンフィギュレーション モードを開始します。
ステップ 5	**session-range** *ip-address ip-mask* 例： `Router(config-mqos)# session-range 224.10.10.10 255.255.255.224`	マルチキャスト QoS グループの IP アドレスと IP マスクのセッション範囲を指定します。複数のセッション範囲を設定できます。
ステップ 6	**tos** *low-byte high-byte mask* 例： `Router(config-mqos)# tos 1 6 15`	（任意）マルチキャスト QoS グループの、タイプ オブ サービス（ToS）最小データ バイト数、ToS 最大データ バイト数、マスクを指定します。
ステップ 7	**vrf***name* 例： `Router(config-mqos)# vrf name1`	（任意）Virtual Routing and Forwarding（VRF）インスタンスの名前を指定します。 （注） マルチキャスト QoS（MQoS）グループがこの VRF で定義されていない場合は、エラー メッセージが表示されます。各 VRF に特定の MQoS グループを定義するか、一致する MQoS グループが見つからない状況で割り当てられたデフォルトの MQoS グループを定義する必要があります。VRF のデフォルト マルチキャスト QoS グループの設定、（742 ページ）を参照してください。
ステップ 8	**application-id***number* 例： `Router(config-mqos)# application-id 25`	（任意）マルチキャスト QoS グループのアプリケーション ID 番号を指定します。マルチキャスト QoS グループに対してアドミッション制御を有効にするように、この値を設定します。

VRF のデフォルト マルチキャスト QoS グループの設定

定義した Virtual Routing and Forwarding（VRF）インスタンスのそれぞれが、VRF 間のマルチキャスト ストリーム クロストークを回避するために、定義した MQoS グループと一致する必要があります。潜在的なクロストークを回避するには、VRF のマルチキャスト トラフィックが MQoS の既

存のグループと一致しない場合にVRFに割り当てられるデフォルトのMQoSグループを定義します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cablemulticastgroup-qos***number* **scn***service-class-name* **control** {**single** | **aggregate** [**limit** *max-sessions*]} 例： `Router(config-mqos)# cable multicast group-qos 5 scn name1 control single`	（任意）マルチキャスト QoS グループに適用できる QoS プロファイルを設定します。
ステップ 4	**cablemulticastqosgroup** *id***priority255global** 例： `Router(config)# cable multicast qos group 2 priority 255 global`	デフォルトのマルチキャスト QoS グループを設定し、マルチキャストQoSコンフィギュレーション モードを開始します。
ステップ 5	**session-range 224.0.0.0 224.0.0.0** 例： `Router(config-mqos)# session-range 224.0.0.0 224.0.0.0`	デフォルトのマルチキャスト QoS グループのセッション範囲のIPアドレスとIPマスクを指定します。IPアドレスとIPマスクに224.0.0.0と入力して、考えられるすべてのマルチキャスト セッションに対応します。
ステップ 6	**vrf***name* 例： `Router(config-mqos)# vrf name1`	VRF インスタンスの名前を指定します。
ステップ 7	**application-id***number* 例： `Router(config-mqos)# application-id 5`	（任意）マルチキャスト QoS グループのアプリケーション ID 番号を指定します。マルチキャスト QoS グループに対してアドミッション制御を有効にするように、この値を設定します。

	コマンドまたはアクション	目的

マルチキャスト VPN と DOCSIS 3.0 マルチキャストの QoS サポートの設定の確認

マルチキャスト VPN および DOCSIS 3.0 マルチキャスト QoS サポート機能の設定を確認するには、次に示す **show** コマンドを使用します。

- 特定のバンドルのマルチキャストセッションの設定パラメータを確認するには、次の例に示すように **showinterfacebundle** *number***multicast-sessions** コマンドを使用します。

```
Router# show interface bundle 1 multicast-sessions
Multicast Sessions on Bundle1
 Group            Interface    GC  SAID SFID  GQC GEn RefCount GC-Interface State
 234.1.1.45       Bundle1.1    1   8193  ---   1   5   1        Bundle1     ACTIVE
 234.1.1.46       Bundle1.1    1   8193  ---   1   5   1        Bundle1     ACTIVE
 234.1.1.47       Bundle1.1    1   8193  ---   1   5   1        Bundle1     ACTIVE
Aggregate Multicast Sessions on Bundle1
 Aggregate Sessions for SAID 8193 GQC 1 CurrSess 3
 Group            Interface    GC  SAID SFID AggGQC GEn RefCount GC-Interface
 234.1.1.45       Bundle1.1    1   8193  ---   1      5   1        Bundle1
 234.1.1.46       Bundle1.1    1   8193  ---   1      5   1        Bundle1
 234.1.1.47       Bundle1.1    1   8193  ---   1      5   1        Bundle1
```

- 特定のケーブルのマルチキャストセッションの設定パラメータを確認するには、次の例に示すように **showinterfacecable** *ip-addr***multicast-sessions** コマンドを使用します。

```
Router# show interface cable 7/0/0 multicast-sessions
Default Multicast Service Flow 3 on Cable7/0/0
Multicast Sessions on Cable7/0/0
 Group            Interface    GC  SAID SFID  GQC GEn RefCount GC-Interface State
 234.1.1.45       Bundle1.1    1   8193 24     1   5   1        Bundle1     ACTIVE
 234.1.1.46       Bundle1.1    1   8193 24     1   5   1        Bundle1     ACTIVE
 234.1.1.47       Bundle1.1    1   8193 24     1   5   1        Bundle1     ACTIVE
Aggregate Multicast Sessions on Cable7/0/0
 Aggregate Sessions for SAID 8193 SFID 24 GQC 1 CurrSess 3
 Group            Interface    GC  SAID SFID AggGQC GEn RefCount GC-Interface
 234.1.1.45       Bundle1.1    1   8193 24     1      5   1        Bundle1
 234.1.1.46       Bundle1.1    1   8193 24     1      5   1        Bundle1
 234.1.1.47       Bundle1.1    1   8193 24     1      5   1        Bundle1
```

- MSAID マルチキャスト グループ サブインターフェイスのマッピングを表示するには、次の例に示すように **showinterfacecable** *address***modem** コマンドを使用します。

```
Router# show interface cable 6/1/0 modem
SID   Priv Type      State          IP address      method  MAC address     Dual
      bits                                                                  IP
9     11   modem     online(pt)     101.1.0.6       dhcp    0006.28f9.8c79  N
9     11   host      unknown        111.1.1.45      dhcp    0018.1952.a859  N
10    10   modem     online(pt)     101.1.0.5       dhcp    0006.5305.ac19  N
10    10   host      unknown        111.1.0.3       dhcp    0018.1952.a85a  N
13    10   modem     online(pt)     101.1.0.3       dhcp    0014.f8c1.fd1c  N
8195  10   multicast unknown        224.1.1.51      static  0000.0000.0000  N
8195  10   multicast unknown        224.1.1.49      static  0000.0000.0000  N
8195  10   multicast unknown        224.1.1.50      static  0000.0000.0000  N
```

マルチキャスト VPN と DOCSIS 3.0 マルチキャストの QoS サポートの設定例

ここでは、次の設定例について説明します。

例：グループ QoS とグループ暗号化プロファイルの設定

（注） QoS グループにグループ QoS とグループ暗号化プロファイルを追加するには、QoS グループを設定する前に、各プロファイルを最初に設定する必要があります。

次の例では、QoS プロファイル 3 および暗号化プロファイル 35 が設定されています。

```
configure terminal
cable multicast group-qos 3 scn name1 control single
cable multicast group-encryption 35 algorithm 56bit-des
```

例：QoS グループの設定

次の例では、QoS グループ 2 が、優先度 6 のグローバル アプリケーションとして設定されています。QoS グループ 2 に対しては、QoS プロファイル 3 および暗号化プロファイル 35 が適用されます。他のパラメータは、アプリケーション タイプ、セッション範囲、ToS、および VRF を含む QoS グループ 2 に設定されます。

```
cable multicast qos group 2 priority 6 global
group-encryption 35
group-qos 3
session-range 224.10.10.01 255.255.255.254
tos 1 6 15
vrf vrf-name1
application-id 44
```

その他の参考資料

ここでは、マルチキャスト VPN と DOCSIS 3.0 マルチキャスト QoS サポートに関連する参考資料について説明します。

関連資料

関連項目	マニュアル タイトル
CMTS ケーブル コマンド	『*Cisco CMTS Cable Command Reference*』 http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref.html

標準

規格	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2236	『*Internet Group Management Protocol, Version 2*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

マルチキャスト VPN と DOCSIS3.0 マルチキャストの QoS サポートに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *114*：マルチキャスト *VPN* と *DOCSIS3.0* マルチキャストの *QoS* サポートに関する機能情報

機能名	リリース	機能情報
マルチキャスト VPN と DOCSIS 3.0 マルチキャストの QoS サポート	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.5.1 に統合されました。

第 44 章

Cisco CMTS 用 EtherChannel

このマニュアルでは、Cisco ケーブル モデム終端システム（CMTS）の Cisco EtherChannel テクノロジーの機能、利点、および設定について説明します。

EtherChannel は、複数の物理的 Ethernet 接続を設定および集約して、より高帯域幅の単一論理ポートを形成するテクノロジーです。Cisco CMTS で最初に設定した EtherChannel ポートが、デフォルトで EtherChannel のバンドル マスターとして機能し、各スレーブ インターフェイスは、EtherChannel のバンドル マスターの MAC アドレスを使用してネットワークと通信します。

EtherChannel ポートはルーティングまたはブリッジングのエンドポイントに常駐します。ルータまたはスイッチは、EtherChannel を使用して半二重または全二重モードで帯域幅利用を増やし、複数の物理接続間でトラフィックのロード バランシングを行います。

Cisco CMTS の EtherChannel は、複数のデバイス、標準による VLAN 間ルーティング、および Cisco cBRルータでの 10 ギガビット EtherChannel（GEC）をサポートします。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *115*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

Cisco CMTS の EtherChannel の制約事項

- Cisco CMTS の EtherChannel は、ネットワーク レイヤ 3 機能に制限され、他の特定のシスコ製品のプラットフォームとは異なり、データリンク レイヤ 2 EtherChannel 機能はサポートしません。
- Port Aggregation Protocol（PAgP）は、他のシスコ製品のプラットフォーム（CatOS スイッチなど）とは異なり、Cisco CMTS ではサポートされません。
- Cisco CMTS では、IEEE 802.1Q トランキング プロトコルのみサポートされます。ATM トランキングは、Cisco cBR シリーズ ルータではサポートされません。
- 1 バンドルあたり最大 8 つのリンクがサポートされます。
- Cisco CMTS の EtherChannel は、同じ速度を持つインターフェイスまたは物理ポートのみをサポートします。
- Cisco cBR シリーズ ルータ上の EtherChannel は MQC QOS をサポートしません。EtherChannel の代わりに Equal Cost Multi Path（ECMP）ロード バランシングを使用できます。
- EtherChannel のメンバー インターフェイス上のレイヤ 3 設定はサポートされません。
- MAC アドレス アカウンティング機能はポート チャネルでサポートされません。

Cisco CMTS の EtherChannel に関する情報

この項の構成は、次のとおりです。

Cisco CMTS への EtherChannel の導入

EtherChannel は実績のある業界標準技術に基づいています。Cisco CMTS がサポートする EtherChannel には次のような利点があります。

- Cisco CMTS の EtherChannel は、サブセカンド コンバージェンス時間をサポートします。
- EtherChannel を使って 2 つのスイッチ装置を接続したり、ルータとスイッチを接続することができます。
- 2 台の装置を 1 つの EtherChannel で接続すると高帯域がサポートされます。
- どちらかの Cisco CMTS プラットフォームに論理ポート チャネルが備わっている場合、ルータ、スイッチ、サーバ間のリンクがフォールトトレラントで高速になります。
- EtherChannel により、Cisco CMTS に冗長性とハイ アベイラビリティが実現されます。一方の側で接続エラーが発生すると、スイッチまたはルータは EtherChannel の相手側の接続でロード バランシングを行います。

- Cisco CMTS のロード バランシングはダイナミック リンクの追加および削除をサポートしますが、トラフィックは中断しません。
- EtherChannel は VLAN 間トランキングをサポートします。トランキングは、複数の VLAN のトラフィックを 2 つの装置間のポイントツーポイント リンクに伝送します。ネットワークの VLAN 間通信では、Cisco CMTS ルータと 1 台のスイッチまたは複数のスイッチの間のトランキングが行われます。キャンパス ネットワークではトランキングが EtherChannel リンクに設定され、複数の VLAN 情報を高帯域チャネルで送信します。

Cisco cBR シリーズ ルータでの Cisco 10 ギガビット EtherChannel

Cisco 10 ギガビット EtherChannel（GEC）は、ギガビット/秒の伝送レートを実現する高性能なイーサネット技術です。スイッチ、ルータ インターフェイス、およびサーバの各リンクにわたって、レジリエンシー（復元力）とロード シェアリング機能を備えた柔軟でスケーラブルな帯域幅を提供します。

Cisco cBR シリーズ ルータ上の 10 GEC には、次の EtherChannel 機能があります。

- VLAN 間ネットワークで IEEE 802.1Q カプセル化をサポートします。
- 最大 8 の物理的 10 ギガビット イーサネット ポートの 1 つの論理 EtherChannel リンクへの統合をサポートします。
- 統合された合計が最大 80 Gbps（全二重）になる、最大 40 Gbps（半二重）の帯域幅をサポートします。

Cisco CMTS の EtherChannel の設定方法

この項の構成は、次のとおりです。

Cisco CMTS の 10 ギガビット EtherChannel の設定

はじめる前に

- 10 ギガビット イーサネットのケーブル配線を完了し、ルータおよびネットワークで稼働します。
- LAN インターフェイスを設定し、IP アドレスとサブネット マスクを指定して、ルータおよびネットワークで稼働します。

（注）
- Cisco cBR シリーズ ルータは、1 つの論理 10 GEC ポートとして設定される最大 8 つの物理コネクタをサポートします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface port-channel** *n* 例： `Router(config)# interface port-channel 1`	EtherChannel インターフェイスを作成します。最初に設定した EtherChannel インターフェイスは、EtherChannel グループ内のすべてのポートのバンドル マスターになります。最初の EtherChannel インターフェイスの MAC アドレスは、グループ内のすべての EtherChannel インターフェイスの MAC アドレスになります。 EtherChannel グループから EtherChannel インターフェイスを削除するには、このコマンドの **no** 形式を使用します。 グループ内の最初の EtherChannel インターフェイスが後で削除された場合、デフォルトでは、グループ内の 2 番目の EtherChannel インターフェイスがバンドル マスターになります。 10 GEC グループにバンドルされた EtherChannel ポートごとにこの手順を繰り返します。この設定は、EtherChannel グループの設定前に、すべての EtherChannel インターフェイスで有効にする必要があります。
ステップ 4	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**interface tengigabitethernet** *slot/subslot/port* 例： `Router# interface gigabitethernet 4/1/0`	EtherChannel バンドルにメンバー EtherChannel リンクとして追加する 10 ギガビット イーサネット インターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
		（注） Cisco CMTS EtherChannel を EtherChannel のメンバーとして設定する前に、Cisco CMTS EtherChannel に追加しているリンクをシャットダウンすることを推奨します。この手順の次のステップを実行する直前に、インターフェイス コンフィギュレーション モードで **shutdown** コマンドを使用します。
ステップ 6	**shutdown** 例： `Router(config-if)# shutdown`	ステップ 5 で選択したインターフェイスを EtherChannel のメンバーとして設定する前にシャットダウンします。

ステップ 7	次のいずれかのコマンドを使用します。
	• 静的 10 GEC 設定の場合、**channel-group** *number* コマンドを使用します。
	• 動的 10 GEC 設定の場合、**channel-group** *number***mode** {**active** | **passive**} コマンドを使用します。
	
	例：
	`Router(config-if)# channel-group 1`
	or
	`Router(config-if)# channel-group 1 mode active`
		EtherChannel グループに 10 ギガビット イーサネット インターフェイスを追加し、そのインターフェイスと EtherChannel リンクを関連付けます。
		Cisco CMTS から EtherChannel グループおよび関連するポートを削除するには、このコマンドの **no** 形式を使用します。

ステップ 8	**no shutdown** 例： `Router(config-if)# no shutdown`	EtherChannel を設定するインターフェイスを有効にします。
ステップ 9	**end** 例： `Router(config# end`	特権 EXEC モードに戻ります。 上記のステップを完了すると、ネットワークの IP トラフィックが表示されるようになります。

トラブルシューティングのヒント

前の手順でインターフェイスの動作を確認し、次の手順で EtherChannel 設定を確認しても EtherChannel リンクに障害が発生する場合は、ネットワークの VLAN 間または IP 間ルーティング、または帯域幅の使用量が非常に高いことが関係している可能性があります。

次の作業

追加の IP アクセス リスト、VLAN 間またはロード バランシングの設定が Cisco CMTS に作成される場合があり、これらの変更は、EtherChannel からのサービスを中断することなく、実行中の EtherChannel 設定でサポートされます。

Cisco CMTS の EtherChannel の確認

リンクは、トラフィックを中断することなく EtherChannel インターフェイスに対して追加または削除を行うことができます。EtherChannel 内のイーサネット リンクで障害が発生すると、それまでその障害リンクで伝送されていたトラフィックが EtherChannel 内の残りのリンクに切り替えられます。コマンドを使用したリンクの追加または削除や、リンク障害のシミュレーションとリカバリ（（no）シャットダウン リンクと同様）など、リンクの追加または削除の要因となるイベントが数多くあります。

Cisco EtherChannel は、Cisco CMTS シャーシの現場で交換可能なユニット（FRU）の活性挿抜（OIR）をサポートしています。1 つの FRU の OIR 中にアクティブ状態を維持するポートは、サービスを中断せずにトラフィックの帯域幅要件を引き継いでサポートします。ただし、ここでは OIR については説明しません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show interface port-channel** *n* 例： `Router# show interface port-channel 1`	選択した EtherChannel グループの Cisco CMTS の EtherChannel 設定を確認します。

Cisco CMTS の EtherChannel の設定例

次の例では、ポートチャネル インターフェイス 2 の 10 ギガビット EtherChannel 情報を示します。

この設定は、次の 3 つの 10 ギガビット GEC ポート チャネルで構成されています。

- メンバー 0 は 10 ギガビット GEC インターフェイス バンドル マスターです。
- メンバー 2 はこの 10 ギガビット GEC グループの最後のスレーブ インターフェイスです。
- この 3 つのポート チャネル インターフェイス（メンバー）は、ネットワーク上の 10 ギガビット GEC ピアで設定された 1 つの 10 ギガビット GEC グループで構成されています。

```
Router# show interface port-channel 2
Port-channel2 is up, line protocol is up
  Hardware is GEChannel, address is 8888.8888.8888 (bia 0000.0000.0000)
  Internet address is 101.101.101.1/16
  MTU 1500 bytes, BW 3000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of members in this channel: 3
    No. of configured  members in this channel: 3
    No. of passive members in this channel: 0
    No. of active members in this channel: 3
        Member 0 : TenGigabitEthernet4/1/0 , Full-duplex, 1000Mb/s
        Member 1 : TenGigabitEthernet4/1/1 , Full-duplex, 1000Mb/s
        Member 2 : TenGigabitEthernet4/1/2 , Full-duplex, 1000Mb/s
    No. of Non-active members in this channel: 0
  Last input 00:00:02, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/225/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/120 (size/max)
  30 second input rate 17292000 bits/sec, 9948 packets/sec
  30 second output rate 17315000 bits/sec, 9935 packets/sec
     866398790 packets input, 3324942446 bytes, 0 no buffer
     Received 2 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     866394055 packets output, 3323914794 bytes, 0 underruns
     0 output errors, 0 collisions, 0 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
シスコ製品用の EtherChannel	• Cisco EtherChannel ホームページ http://www.cisco.com/warp/public/cc/techno/lnty/etty/fsetch/index.shtml • Cisco EtherChannel テクノロジー ホワイト ペーパー http://www.cisco.com/en/US/tech/tk389/tk213/technologies_white_paper09186a0080092944.shtml
EtherChannel 用の追加デバイスの設定	• 『*Configuring EtherChannel and 802.1Q Trunking Between a Catalyst 2950 and a Router (inter-VLAN Routing)*』 http://www.cisco.com/c/en/us/support/docs/switches/catalyst-2950-series-switches/24042-158.html • 『*Configuring EtherChannel and 802.1Q Trunking Between Catalyst 2900XL/3500XL and Catalyst 2940, 2950/2955, and 2970 Switches*』 http://www.cisco.com/c/en/us/support/docs/switches/catalyst-2900-xl-series-switches/21041-131.html

標準および **RFC**

標準	タイトル
IEEE Std 802.1Q の 2003 年版	IEEE Std 802.1Q の 2003 年版（IEEE Std 802.1Q-1998、IEEE Std 802.1u-2001、IEEE Std 802.1v-2001、IEEE Std 802.1s-2002 を含む） http://ieeexplore.ieee.org/xpl/tocresult.jsp?isNumber=27089

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support

Cisco CMTS 上の EtherChannel に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *116*：*Cisco CMTS* 上の *EtherChannel* に関する機能情報

機能名	リリース	機能情報
Cisco CMTS 上の EtherChannel	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 45 章

フローベースのポートチャネルごとのロード バランシング

フローベースのポートチャネルごとのロード バランシング機能を使用すると、10 ギガビット EtherChannel（GEC）インターフェイス経由のトラフィックのさまざまなフローをパケット ヘッダーに基づいて識別し、ポート チャネルの異なるメンバー リンクにマッピングすることができます。この機能により、特定のポート チャネルへのフロー ベースのロード バランシングおよび手動 VLAN ロード バランシングを適用することができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

- その他の参考資料，767 ページ
- フローベースのポートチャネルごとのロード バランシングに関する機能情報，768 ページ

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *117*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

フローベースのポートチャネルごとのロードバランシングの制約事項

- 最大で 64 の Ten GEC インターフェイスをサポートします。
- 1 つの Ten GEC インターフェイスあたり最大で 8 つのメンバー リンクをサポートします。

フローベースのポートチャネルごとのロードバランシングに関する情報

フローベースのロード バランシング

フローベースのロードバランシングは、データ パケットのキー フィールドに基づいてトラフィックのさまざまなフローを識別します。フローを識別するために、たとえば、IPv4 送信元および宛先 IP アドレスを使用できます。次に、さまざまなデータ トラフィックがポート チャネルの異なるメンバー リンクにマッピングされます。マッピングが完了したら、フローのデータ トラフィックは、割り当てられたメンバー リンクを通じて送信されます。フロー マッピングは動的で、フローが割り当てられたメンバー リンクの状態が変わったときに変更されます。フローのマッピングは、メンバー リンクが GEC インターフェイスに追加または削除された場合にも変更されます。複数のフローは、各メンバー リンクにマッピングできます。

フローベースのロード バランシング用のバケット

ロード バランシングは、バケットの概念によって、Ten GEC インターフェイスのメンバー リンクへのトラフィック フローを動的にマッピングします。多様な定義済みトラフィック フローがバケットにマップされ、バケットはメンバー リンク間で均等に配分されます。各ポート チャネルで 16 のバケットが維持され、各バケットに 1 つのアクティブ メンバー リンクが関連付けられます。バケットにマッピングされたすべてのトラフィック フローは、バケットが割り当てられたメンバー リンクを使用します。

ルータは、ポート チャネルにフローベースのロードバランシングを適用するときに、バケットからメンバーへのリンク マッピングを作成し、ポート チャネルには少なくとも 1 つのアクティブ メンバー リンクが作成されます。マッピングは、最初のメンバー リンクが追加または起動されるときにも作成され、ロードバランシング メソッドがフローベースに設定されます。

メンバー リンクがダウンするか、またはポート チャネルから削除されると、そのメンバー リンクに関連付けられたバケットはラウンドロビン方式で他のアクティブ メンバー リンク間で再配布されます。メンバー リンクが起動するまたはポート チャネルに追加されると、他のリンクに関連付けられたバケットの一部がこのリンクに割り当てられます。

ロードバランシング メソッドを変更する場合、フローベースのロードバランシング用のバケットからメンバーへのリンク マッピングは削除されます。マッピングは、ポート チャネルが削除されるか、またはポート チャネルの最後のメンバー リンクが削除されるまたはダウンした場合にも削除されます。

ポート チャネルのロード バランシング

GEC インターフェイスは、動的なフローベースのロード バランシングまたは手動 VLAN ロード バランシングを使用できます。すべてのポート チャネルに対してグローバルにロードバランシング メソッドを設定するか、特定のポートチャネルに直接設定するかを設定できます。グローバル コンフィギュレーションは、ロードバランシングが明示的には設定されていないポートチャネルだけに適用されます。ポートチャネルの設定はグローバル コンフィギュレーションを上書きします。

フローベースのロード バランシングは、グローバル レベルでデフォルトでイネーブルになります。VLAN ロード バランシングを明示的に設定しないと、ロードバランシング メソッドは、フローベースになります。

次の表は、設定に基づいてポートチャネルに適用されるロードバランシング メソッドをリストします。

表 *118*：フローベースのロード バランシングの設定オプション

グローバル設定	ポートチャネルの設定	適用されるロード バランシング
未設定	未設定	フローベース
	フローベース	フローベース
	手動 VLAN	手動 VLAN
手動 VLAN	未設定	手動 VLAN
	フローベース	フローベース
	手動 VLAN	手動 VLAN

次の表に、グローバル ロードバランシング メソッドを変更した場合の設定結果を示します。

表 *119*：グローバル コンフィギュレーションが変更された場合の結果

ポートチャネルの設定	グローバル設定		ポートチャネルで実行されるアクション
—	遷移元	目的	—
未設定	未設定	手動 VLAN	フローベースから手動 VLAN への変更
	手動 VLAN	未設定	手動 VLAN からフローベースへの変更

ポートチャネルの設定	グローバル設定		ポートチャネルで実行されるアクション
設定済み	いずれか（Any）	いずれか（Any）	変更なし

次の表に、ポートチャネル ロードバランシング メソッドが変更された場合の設定結果を示します。

表 *120*：ポートチャネルの設定が変更された場合の結果

ポートチャネルの設定	グローバル設定		ポートチャネルで実行されるアクション
—	遷移元	目的	—
未設定	未設定	手動 VLAN	フローベースから手動 VLAN への変更
	未設定	フローベース	アクションなし
	手動 VLAN	フローベース	手動 VLAN からフローベースへの変更
	手動 VLAN	未設定	手動 VLAN からフローベースへの変更
	フローベース	手動 VLAN	フローベースから手動 VLAN への変更
	フローベース	未設定	アクションなし
設定済み	未設定	手動 VLAN	アクションなし
	未設定	フローベース	手動 VLAN からフローベースへの変更
	手動 VLAN	フローベース	手動 VLAN からフローベースへの変更
	手動 VLAN	未設定	アクションなし
	フローベース	手動 VLAN	フローベースから手動 VLAN への変更
	フローベース	未設定	フローベースから手動 VLAN への変更

フローベースのポートチャネルごとのロードバランシングをイネーブルにする方法

ポート チャネルのロード バランシングの設定

ポートチャネルにロードバランシングを設定するには、次の手順を実行します。各GECインターフェイスに対してこの手順を繰り返して行います。

はじめる前に

すでに任意のロードバランシング メソッドをグローバルに設定していて、すべてのポートチャネルにその方式を使用する場合は、次のタスクを実行する必要はありません。ロードバランシングをグローバルに設定するには、**port-channel load-balancing vlan-manual** コマンドを使用します。グローバル コマンドを設定していない場合、フローベースのロードバランシングがすべてのポート チャネルに適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfaceport-channel** *channel-number* 例： `Router(config)# interface port-channel 1`	インターフェイス コンフィギュレーション モードを開始し、ポートチャネルとしてインターフェイスを定義します。
ステップ 4	**load-balancing** {**flow** | **vlan**} 例： `Router(config-if)# load-balancing flow`	特定のポート チャネルにロードバランシング メソッドを適用します。 • このコマンドを設定しない場合、ポートチャネルは、**port-channel load-balancing vlan-manual** コマンドで設定されたグローバ

	コマンドまたはアクション	目的
		ル ロードバランシング方式を使用します。グローバルデフォルトはフローベースです。
ステップ 5	**end** 例： `Router(config-if)# end`	設定モードを終了します。

10 GEC インターフェイス上のロード バランシング設定の確認

- **showrunning-configinterfaceport-channel** *channel-number*：ポート チャネル設定を表示します。

  次に、このコマンドの出力例を示します。

```
Router# show running-config interface port-channel 62
Building configuration...

Current configuration : 108 bytes
!
interface Port-channel62
 ip address 12.1.1.1 255.255.255.0
 ipv6 address 2001:12:1:1::1/64
 mpls
```

- **showetherchannelload-balancing**：各ポート チャネルに適用されるロード バランシング メソッドを表示します。

  次に、このコマンドの出力例を示します。

```
Router# show etherchannel load-balancing

EtherChannel Load-Balancing Method:
Global LB Method: flow-based

  Port-Channel:                        LB Method
    Port-channel62                  :  flow-based
    Port-channel63                  :  flow-based
```

- **showinterfaces port-channel** *channel-number* **etherchannel**：現在使用中のバケットの分散を表示します。

  次に、ロードバランシングがフローベースに設定されているインターフェイスの出力例を示します。

```
Router(config)# show interface port-channel 62 etherchannel

 All IDBs List contains 8 configured interfaces
  Port: TenGigabitEthernet4/1/0 (index: 0)
  Port: TenGigabitEthernet4/1/1 (index: 1)
  Port: TenGigabitEthernet4/1/2 (index: 2)
  Port: TenGigabitEthernet4/1/3 (index: 3)
  Port: TenGigabitEthernet4/1/4 (index: 4)
```

```
 Port: TenGigabitEthernet4/1/5 (index: 5)
 Port: TenGigabitEthernet4/1/6 (index: 6)
 Port: TenGigabitEthernet4/1/7 (index: 7)

Active Member List contains 8 interfaces
 Port: TenGigabitEthernet4/1/0
   LACP Mode: Active

 Port: TenGigabitEthernet4/1/1
   LACP Mode: Active

 Port: TenGigabitEthernet4/1/2
   LACP Mode: Active

 Port: TenGigabitEthernet4/1/3
   LACP Mode: Active

 Port: TenGigabitEthernet4/1/4
   LACP Mode: Active

 Port: TenGigabitEthernet4/1/5
   LACP Mode: Active

 Port: TenGigabitEthernet4/1/6
   LACP Mode: Active

 Port: TenGigabitEthernet4/1/7
   LACP Mode: Active

Passive Member List contains 0 interfaces
Load-Balancing method applied: flow-based

Bucket Information for Flow-Based LB:
Interface:                                Buckets
   TenGigabitEthernet4/1/0:
                           Bucket 0 , Bucket 1
   TenGigabitEthernet4/1/1:
                           Bucket 2 , Bucket 3
   TenGigabitEthernet4/1/2:
                           Bucket 4 , Bucket 5
   TenGigabitEthernet4/1/3:
                           Bucket 6 , Bucket 7
   TenGigabitEthernet4/1/4:
                           Bucket 8 , Bucket 9
   TenGigabitEthernet4/1/5:
                           Bucket 10, Bucket 11
   TenGigabitEthernet4/1/6:
                           Bucket 12, Bucket 13
   TenGigabitEthernet4/1/7:
                           Bucket 14, Bucket 15
```

フローベースのポートチャネルごとのロード バランシングの設定例

例：フローベースのロード バランシング

次に、フローベースのロード バランシングがポートチャネル 2 で設定され、VLAN 手動方式がグローバルに設定されている設定の例を示します。

```
!
no aaa new-model
port-channel load-balancing vlan-manual
ip source-route
.
.
```

```
.
interface Port-channel2
 ip address 10.0.0.1 255.255.255.0
 no negotiation auto
 load-balancing flow
!
interface Port-channel2.10
 ip rsvp authentication key 11223344
 ip rsvp authentication
!
interface Port-channel2.50
 encapsulation dot1Q 50
!
interface TenGigabitEthernet4/1/0
 no ip address
 negotiation auto
 cdp enable
 channel-group 2
!
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

フローベースのポートチャネルごとのロードバランシングに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *121*：フローベースのポートチャネルごとのロード バランシングに関する機能情報

機能名	リリース	機能情報
フローベースのポートチャネルごとのロード バランシング	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 46 章

非 L2VPN サービス フローの TLV による MPLS QoS

非 L2VPN サービス フローの TLV による MPLS QoS 機能により、MPLS L3VPN インポジション パケットの TC ビットをマークし、ベンダー固有の TLV を使用して MPLS のディスポジション パケットの TC ビットに基づいてダウンストリーム パケットを分類することができます。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *122* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

非 L2VPN サービス フローの TLV による MPLS QoS の制限事項

- この機能は IPv4 のみをサポートします。IPv6 はサポートしません。
- この機能は SNMP をサポートしません。
- この機能は動的サービス フローをサポートしません。
- 1 CM あたり 4 つの VPN および 8 つのアップストリーム サービス フローのみ設定できます。
- VPN では、最大 8 つの DS 分類子（0 ～ 7 の TC ビットを使用）を設定できます。
- VPN で TC ビット ダウンストリーム分類子が設定されている場合、VPN に属するダウンストリーム MPLS パケットは TC ビット分類でのみ処理されます。一般的な IP ヘッダー フィールド分類は処理されません。

非 L2VPN サービス フローでの TLV による MPLS QoS に関する情報

非 L2VPN サービス フローでの TLV による MPLS QoS の機能は QoS の拡張であり、MPLS L3VPN 用 MPLS トラフィック クラス（TC）ビットに基づきます。以前、MPLS TC ビットは MPLS EXP ビットと呼ばれていました。RFC 5462 により、MPLS EXP フィールドは MPLS TC フィールドに名前が変更されました。

アップストリーム サービス フローのエンコーディングでは、Cisco 独自の TLV を使用して MPLS インポジション パケットに TC ビット値を設定します。ダウンストリーム分類子のエンコーディングでは、Cisco 独自の TLV を使用して MPLS ディスポジション パケットの TC ビットに基づいてダウンストリームの分類を導入します。

非 L2VPN サービス フローの TLV による MPLS QoS の設定

（注） この機能は、ケーブル モデム コンフィギュレーション ファイルを使用して設定され、L3VPN の一般設定に応じて異なります。

ここでは、MPLS インポジション パケットと MPLS ディスポジション パケットの設定方法、および AToM L2VPN および MPLS L3VPN によりベンダー固有の TLV を使用する方法を説明します。

MPLS インポジション パケットのトラフィック クラス

次の表に、MPLS インポジション パケットの TC ビットを設定するために、ケーブル モデム コンフィギュレーション ファイルに含めるべきベンダー固有の TLV を示します。MPLS-TC-SET TLV はアップストリームで定義され、アップストリーム サービス フローのエンコーディングで VPN RD と関連付けられます。

表 *123*：*MPLS* インポジション パケットの *TC* ビットを設定するための *TLV*

TLV 名	サブタイプ	長さ	値
MPLS-TC-SET TLV	43.5.43.34	1	インポジション MPLS-TC-SET ビット

MPLS ディスポジション パケットのトラフィック分類

次の表に、MPLS ディスポジション パケットの TC ビットに基づく DS パケットを分類するために、ケーブル モデム コンフィギュレーション ファイルに含めるべきベンダー固有の TLV を示します。

MPLS-TC-RANGE TLV は、DS 分類子の符号化でのみ定義されます。これは、ダウンストリーム分類子エンコーディングで VPN RD に関連付けられている同じ MPLS L3VPN に属する CM の複数のダウンストリーム フローをサポートします。

表 *124*：*MPLS* ディスポジション パケットの *TC* ビットを分類するための *TLV*

TLV 名	サブタイプ	長さ	値
MPLS-TC-RANGE	43.5.43.35	2	MPLS-TC-low および MPLS-TC-high

AToM L2VPN と MPLS L3VPN でのベンダー専用 TLV の使用

AToM L2VPN（L2 MPLS）と MPLS L3VPN（L3 MPLS）の両方が同じ一連の TLV（MPLS-TC-SET と MPLS-TC-RANGE）を使用している場合、それらを区別する必要があります。アップストリーム サービス フローのエンコーディングとダウンストリーム分類子のエンコーディングのための TLV を次のように設定します。

アップストリーム サービス フローのエンコーディング

- L2VPN 用に、MPLS-TC-SET（43.5.43.34）および L2VPN ID（43.5.1）を設定します。
- MPLS L3VPN 用に、MPLS-TC-SET（43.5.43.34）および VPN RD（43.5.1）を設定します。

（注） アップストリーム サービス フローのエンコーディングのために L2VPN と MPLS L3VPN の TLV を同時に設定しないでください。設定すると、TLV エラーが発生します。

ダウンストリーム分類子のエンコーディング

- L2VPN：MPLS-TC-RANGE（43.5.43.35）および L2VPN ID（43.5.1）を設定します。
- MPLS L3VPN：MPLS-TC-RANGE（43.5.43.35）および VPN RD（43.5.1）を設定します。

設定例

ここでは、次の設定例について説明します。

例：アップストリームサービス フロー マーキング TLV

次に、MPLS インポジション パケットの TC ビットをプロビジョニングするための CM 設定 TLV の例を示します。

```
24 (Upstream Service Flow Encoding)
```

```
   S01 (Service Flow Reference)         = 2
   S06 (QoS Parameter Set Type)         = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID)  = 00 00 0c
       T004 (VPN Route Distinguisher) = xx xx xx xx xx xx xx xx
            S005 (Vendor specific L2VPN TLV)
            S043 (Cisco Vendor Specific)
       T034 (MPLS-TC-SET) = 04 # MPLSTC-SET = 4
```

例：ダウンストリーム パケット分類 TLV

次に、MPLS ディスポジション パケットの TC ビットに基づいてダウンストリーム パケットを分類するための CM 設定 TLV の例を示します。

```
23 (Downstream Packet Classification Encoding)
   S01 (Classifier Reference)           = 13
   S03 (Service Flow Reference)         = 13
   S11 (IEEE 802.1P/Q Packet Classification Encodings)
   S43 (Vendor Specific Options)
       T08 (Vendor ID)  = 00 00 0c
       S004 (VPN Route Distinguisher) = xx xx xx xx xx xx xx xx
       S005 (Vendor specific L2VPN TLV)
           S043 (Cisco Vendor Specific)
           S035 (MPLS-TC-RANGE)   = 04  05      # MPLSTC-EGRESS_RANGE= 4 - 5
```

例：MPLS QoS コンフィギュレーション ファイル

次の例では、MPLS L3VPN インポジション パケットの TC ビットをマークし、ベンダー固有の TLV を使用して MPLS L3VPN のディスポジション パケットの TC ビットに基づいてダウンストリーム パケットを分類するように設定されているケーブル モデムを示します。

```
CM-CONFIG
=========
03 (Net Access Control)                      = 1
18 (Maximum Number of CPE)       = 16
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 2
   S03 (Service Flow Reference)        = 2
   S05 (Rule Priority)                             = 2
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 00 20 ff
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 3
   S03 (Service Flow Reference)        = 3
   S05 (Rule Priority)                             = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 40 80 ff
22 (Upstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 4
   S03 (Service Flow Reference)        = 4
   S05 (Rule Priority)                             = 4
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = a0 e0 ff
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 12
   S03 (Service Flow Reference)        = 12
   S05 (Rule Priority)                             = 2
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)             = 00 00 0c
       T004 (Unknown sub-type)         = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)         = 2b 09 08 03 00 00 0c 23 02 01 01
23 (Downstream Packet Classification Encoding Block)
```

```
   S01 (Classifier Reference)              = 13
   S03 (Service Flow Reference)        = 13
   S05 (Rule Priority)                             = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)          = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)          = 2b 09 08 03 00 00 0c 23 02 02 02
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 14
   S03 (Service Flow Reference)        = 14
   S05 (Rule Priority)                             = 4
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)          = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)          = 2b 09 08 03 00 00 0c 23 02 03 03
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 1
   S06 (QoS Parameter Set Type)     = 7
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 2
   S06 (QoS Parameter Set Type)     = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)          = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)          = 2b 08 08 03 00 00 0c 22 01 04
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 3
   S06 (QoS Parameter Set Type)     = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)          = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)          = 2b 08 08 03 00 00 0c 22 01 05
24 (Upstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 4
   S06 (QoS Parameter Set Type)     = 7
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)          = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)          = 2b 08 08 03 00 00 0c 22 01 06
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 11
   S06 (QoS Parameter Set Type)     = 7
   S07 (Traffic Priority)                          = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 12
   S06 (QoS Parameter Set Type)     = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 13
   S06 (QoS Parameter Set Type)     = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 14
   S06 (QoS Parameter Set Type)     = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 15
   S06 (QoS Parameter Set Type)     = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 16
   S06 (QoS Parameter Set Type)     = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 17
   S06 (QoS Parameter Set Type)     = 7
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 18
   S06 (QoS Parameter Set Type)     = 7
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 19
   S03 (Service Flow Reference)        = 19
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 00 ff ff
```

```
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)         = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)         = 2b 09 08 03 00 00 0c 23 02 00 00
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 15
   S03 (Service Flow Reference)        = 15
   S05 (Rule Priority)                             = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)         = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)         = 2b 09 08 03 00 00 0c 23 02 04 04
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 16
   S03 (Service Flow Reference)        = 16
   S05 (Rule Priority)                             = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)         = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)         = 2b 09 08 03 00 00 0c 23 02 05 05
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 17
   S03 (Service Flow Reference)        = 17
   S05 (Rule Priority)                             = 3
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)         = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)         = 2b 09 08 03 00 00 0c 23 02 06 06
23 (Downstream Packet Classification Encoding Block)
   S01 (Classifier Reference)              = 18
   S03 (Service Flow Reference)        = 18
   S09 (IP Packet Encodings)
       T01 (IP Type of Srv Rng & Mask)             = 00 ff ff
   S43 (Vendor Specific Options)
       T08 (Vendor ID)           = 00 00 0c
       T004 (Unknown sub-type)         = 00 00 00 01 00 00 00 01
       T005 (Unknown sub-type)         = 2b 09 08 03 00 00 0c 23 02 07 07
25 (Downstream Service Flow Encodings)
   S01 (Service Flow Reference)        = 19
   S06 (QoS Parameter Set Type)     = 7
#<EOF>
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

非 L2VPN サービス フローの TLV による MPLS QoS に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *125*：非 *L2VPN* サービス フローの *TLV* による *MPLS QoS* に関する機能情報

機能名	リリース	機能情報
非 L2VPN サービス フローの TLV による MPLS QoS	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

機能名	リリース	機能情報
非 L2VPN サービス フローの TLV による MPLS QoS	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 VI 部

レイヤ 3 の設定

第 47 章

CMTS ルータの DHCP、ToD、TFTP サービス

（注） Cisco IOS-XE リリース 16.5.1 では、Cisco CMTS ルータでのこの機能のサポートが統合されています。

このドキュメントでは、Data-over-Cable Service Interface Specifications（DOCSIS）ネットワーク用に Dynamic Host Configuration Protocol（DHCP）、Time of Day（ToD）、および Trivial File Transfer Protocol（TFTP）サービスを提供するオンボード サーバをサポートするよう、Cisco ケーブル モデム終端システム（CMTS）プラットフォームを設定する方法について説明します。また、外部 DHCP サーバで使用可能なオプション設定についてもこのドキュメントで説明します。

DHCP、ToD、TFTP サービスの前提条件

Cisco CMTS をスタンドアロンもしくは外部の他の ToD サーバと共に ToD サーバとして使用できるようにするには、ケーブル モデムで有効な ToD サーバ（DHCP オプション 4）の 1 つとして Cisco CMTS の IP アドレスを提供するよう DHCP サーバを設定する必要があります。

DHCP、ToD、TFTP サービスの制限事項

- ToD サーバは、DOCSIS 仕様に準拠するためには UDP プロトコルを使用する必要があります。
- DOCSIS ネットワーク（特に BPI+ 暗号化および認証を使用する DOCSIS 1.1 ネットワーク）を適切に動作させるには、Cisco CMTS のシステム クロックを正確に設定する必要があります。これを行うには、**setclock** コマンドを使用して手動で設定するか、Network Time Protocol（NTP）または Simple Network Time Protocol（SNTP）を使用するように CMTS を設定します。
- Cisco cBR シリーズ ルータは内蔵 DHCP サーバをサポートしていません。

DHCP、ToD、TFTP サービスに関する情報

ここでは、DHCP、ToD、TFTP サービス機能とその個々のコンポーネントに関する次の情報を示します。

機能の概要

すべての Cisco CMTS プラットフォームは、DOCSIS ケーブル ネットワークで使用するために DHCP、ToD、および TFTP プロキシ サービスを提供するオンボード サーバをサポートします。これらのサーバは、DOCSIS 1.0 および 1.1 対応ケーブル モデムで必要な登録サービスを提供します。

- 外部 DHCP サーバ：DHCP サービスを提供します。外部 DHCP サーバは、通常、大規模ケーブル ネットワークの管理により適した統合型プロビジョニング システムに含まれます。
- Time-of-Day サーバ：RFC 868 準拠 ToD サービスを提供し、ケーブル モデムが登録プロセス中に現在の日付と時刻を取得できるようにします。ケーブルモデムは、IP アドレス、および DHCP が提供するその他の IP パラメータを取得した後で、ToD サーバに接続します。

ケーブル モデムはオンラインになる前に ToD 要求を正常に完了する必要はありませんが、これにより、イベント ログに正確なタイムスタンプを追加でき、これらのログが CMTS で使用されているクロックへと調整されます。また、ケーブルモデムがベースライン プライバシー インターフェイス プラス（BPI+）暗号化および認証への登録を試みている場合、正確な日付と時刻を取得することは必須です。

- 外部 TFTP サーバ：ケーブル モデムに DOCSIS コンフィギュレーション ファイルをダウンロードします。DOCSIS コンフィギュレーション ファイルには、ケーブル モデムの動作パラメータが含まれています。ケーブル モデムは ToD サーバに接続してから DOCSIS コンフィギュレーション ファイルをダウンロードします。

（注） たくさんの方法で追加のサーバを追加できます。たとえば、ほとんどのケーブル オペレータは、Cisco Network Registrar（CNR）を使用して DHCP と TFTP サーバを提供しています。ToD サーバは、ほとんどのワークステーションや PC で無料で使用できます。追加サーバは、1 台のワークステーションまたはPCにインストールすることも、異なるワークステーションやPCにインストールすることもできます。

外部 DHCP サーバ

Cisco CMTS ルータは、DOCSIS ケーブル ネットワークで使用中の外部 DHCP サーバの運用とセキュリティを強化することができる、次のオプション設定を提供します。

ケーブル ソース確認機能

サービス不正使用攻撃に対抗するには、Cisco CMTS ルータのケーブル インターフェイスで **cablesource-verify** コマンドを有効にできます。この機能では、CMTS がケーブル インターフェイスで受信する IP パケットの正当性を確認し、3 つの保護レベルを提供するために、ルータの内部データベースを使用します。

- 最も基本的な保護レベルでは、ケーブル ソース確認機能は各 IP アップストリーム パケットを検査して、重複する IP アドレスがケーブル ネットワークに現れないようにします。競合が発生すると、Cisco CMTS は DHCP サーバから IP アドレスが割り当てられたデバイスからのパケットのみを認識します。アドレスが重複するデバイスは、ネットワーク アドレスが許容されません。また、IP アドレスがその特定ケーブル セグメントで不正なネットワーク アドレスであるデバイスからのトラフィックも認識を拒否します。
- コマンド **cablesource-verify** にオプション **dhcp** を追加すると、ユーザが現在未使用の IP アドレスをデバイスに静的に割り当てることができなくなるため、より包括的な保護レベルを提供できます。Cisco CMTS はケーブル インターフェイスで未知の IP アドレスのパケットを受信すると、パケットをドロップしますが、そのデバイスの IP および MAC アドレスに関する情報を DHCP サーバへクエリする DHCP LEASEQUERY メッセージを発行します。DHCP サーバがデバイスに関する情報を返さない場合、CMTS はそのデバイスのネットワーク アクセスをブロックし続けます。
- **dhcp** オプションを使用するときは、**leasetimer** オプションも有効にできます。このオプションは、内部 CPE データベースでリース期間が終了した IP アドレスがあるかどうかを定期的に確認するよう Cisco CMTS に指示します。期限切れの IP アドレスを使用している CPE デバイスは、有効な DHCP サーバから IP アドレスを更新するまで、ネットワークへの今後のアクセスを拒否されます。これにより、ユーザが DHCP で割り当てられた IP アドレスをスタティック アドレスとして自分の CPE デバイスに割り当てることを防止できます。
- dhcp オプションに加えて、cable source-verify group コマンドを使用して Cisco CMTS でプレフィックス ベースの送信元アドレス確認（SAV）を構成することもできます。CM は、SAV グループに属する静的な IPv4 または IPv6 プレフィックスを構成することもできます。SAV プレフィックス処理が Cisco CMTS で有効な場合、CM からのパケットの送信元 IP アドレスは、（その CM 用に）構成されたプレフィックスと SAV グループに対して照合、確認され

ます。確認に失敗するとパケットはドロップされます。そうでない場合、パケットは転送されてさらに処理されます。SAV プレフィックス処理と SAV プレフィックス構成の詳細については、プレフィックスベースの送信元アドレス確認,（784ページ）および以下を参照してください。 プレフィックスベースの送信元アドレス確認の設定,（796 ページ）

プレフィックス ベースの送信元アドレス確認

送信元アドレス確認（SAV）機能により、アップストリーム パケットの送信元 IP アドレスを確認して SID/MAC と IP の一貫性を確認できます。DOCSIS 3.0 のセキュリティ仕様には、すべての CM に静的 IPv4 または IPv6 プレフィックスを設定できるプレフィックス ベースの SAV が導入されています。これらのプレフィックスは CMTS で事前設定されているか、または、CM 登録時に CMTS に通知されます。Cisco CMTS は、これらの設定されたプレフィックスを使用して、CM 経由で着信されるすべてのパケットの送信元 IP アドレスを確認します。

SAV グループはプレフィックスの集合体です。プレフィックスは、IPv4 または IPv6 サブネット アドレスです。グローバル コンフィギュレーション モードで cable source-verify group コマンドを使用して、SAV グループを設定できます。CMTS は合計 255 の SAV グループをサポートします。各 SAV グループは最大 4 つのプレフィックスを含むことができます。プレフィックスは prefix コマンドを使用して設定できます。

CM は、その登録時に、設定済みの静的プレフィックスを 2 つの TLV（43.7.1 と 43.7.2）を使用して CMTS に通知します。TLV 43.7.1 は CM が属する SAV プレフィックス グループの名前を指定し、TLV 43.7.2 は実際の IPv4 または IPv6 プレフィックスを指定します。各 CM には最大 4 つのプレフィックスを設定できます。Cisco CMTS はこれらの TLV を受信すると、まず、指定の SAV グループとプレフィックスが Cisco CMTS ですでに設定されているかどうかを確認します。設定されている場合、Cisco CMTS は登録中の CM にそれらを関連付けます。設定されていない場合、Cisco CMTS は指定の SAV グループとプレフィックスを自動作成し、それらを登録中の CM に関連付けます。

これらの TLV によって提供される SAV グループ名とプレフィックスは、Cisco CMTS によって有効とみなされます。TLV によって指定されたプレフィックスに属する送信元 IP アドレスにより（CM を経由して）受信されたパケットは承認済みと見なされます。たとえば、ある CM の SAV プレフィックスが 10.10.10.0/24 に設定されている場合、この CM（または CM の背後の CPE）を経由して受信されるパケットは、その送信元のサブネットのアドレスが 10.10.10.0/24 であれば承認済みと見なされます。

SAV グループおよびプレフィックスの設定方法の詳細については、プレフィックスベースの送信元アドレス確認の設定,（796 ページ）を参照してください。

スマート リレー機能

Cisco CMTS は、スマート リレー機能（**ip dhcp smart-relay** コマンド）をサポートします。これは、プライマリ サーバの IP アドレスがなくなったり IP アドレスでの応答ができなくなった場合に、自動的にケーブル モデムや CPE デバイスをセカンダリ DHCP サーバやアドレス プールに切り換える機能です。リレー エージェントは、プライマリ サーバへの DHCP 要求の転送を 3 回試みます。3 回の試行でプライマリからの応答を得られないと、リレー エージェントは自動的にセカンダリ サーバに切り換えます。

cable dhcp-giaddr policy コマンドを使用して、ケーブル インターフェイスのセカンダリ アドレスに対応したセカンダリ DHCP プールを CPE デバイスで使用するように指定した場合、スマート リレーエージェントは、使用可能なアドレスプールが見つかるまで、使用可能なセカンダリをラウンド ロビン式で自動的に循環させます。これにより、クライアントは、特定のプールが使い果たされることでネットワークから締め出されることがなくなります。

GIADDR フィールド

ケーブル モデムと CPE デバイスで別々の IP アドレス プールを使用する場合は、**cabledhcp-giaddrpolicy** コマンドを使用できます。これにより、ケーブル モデムでプライマリ プールからのアドレスを使用し、CPE デバイスはセカンダリ プールからのアドレスを使用するように指定できます。デフォルトでは、CMTS はすべての DHCP 要求をプライマリ DHCP サーバに送信し、セカンダリ サーバはプライマリ サーバが応答しないときに限り使用されます。異なる DHCP サーバを指定するには、**cablehelper** コマンドを使用します。

DHCP リレー エージェントのサブオプション

DHCP リレー エージェント情報サブオプション（DHCP オプション 82、サブオプション 9）強化は、CPE デバイスのプロビジョニングを簡素化します。ケーブル オペレータはこのサブオプションを使用して、適切な IP アドレスを取得するために CPE のサービス クラスまたは QoS 情報を DHCP サーバにリレーできます。

CPE をプロビジョニングするには、DHCP サーバが CPE のサービス クラスまたは QoS 情報を認識している必要があります。DHCP サーバはこの情報を取得するために DHCP DISCOVER メッセージを使用します。このメッセージには、CPE が背後に存在する CM のサービス クラスまたは QoS 情報が含まれます。

プロビジョニング プロセス中に、Cisco CMTS は DHCPv4 リレー エージェント情報サブオプションを使用して、CM のサービス クラスまたは QoS プロファイルに関する情報を DHCP サーバにアドバタイズします。適切な IP アドレスを取得するために、同じ手法を使用して CPE 情報が DHCP サーバにリレーされます。

サービス クラス オプションを有効にするには、CM コンフィギュレーション ファイルで指定されたサービス クラス名が Cisco CMTS で構成されている必要があります。これを行うには、 **cable dhcp-insert service-class** コマンドを使用します。

（注） サービス クラスのリレー エージェント情報オプションを DHCP DISCOVER メッセージに挿入するには、バンドル インターフェイスで **ipdhcprelayinformationoption-insert** コマンドが設定されている必要があります。

Time-of-Day サーバ

Cisco CMTS は、ケーブル インターフェイスに接続されたケーブル モデムや他の顧客宅内機器（CPE）デバイスに現在の日付と時刻を提供する ToD サーバとして機能することができます。これにより、ケーブル モデムと CPE デバイスは、シンプル ネットワーク管理プロトコル（SNMP）

メッセージおよびエラー ログ エントリに正確なタイムスタンプを提供することができ、また、ケーブルネットワーク内のすべてのシステム クロックを確実に同一システム時間に同期することができます。

DOCSIS 1.0 および 1.1 仕様では、すべての DOCSIS ケーブル モデムが初期電源投入プロビジョニング中に送信する DHCP 要求で次の時間関連フィールドを要求することを必要とします。

- タイム オフセット（オプション 2）：ケーブル モデムまたは CPE デバイスのタイム ゾーンを、装置のタイムスタンプがグリニッジ標準時（GMT）からずれている秒数の形式で指定します。
- タイム サーバ オプション（オプション 4）：ToD サーバの 1 つまたは複数の IP アドレスを指定します。

ケーブル モデムは、正常に DHCP リース時間を取得した後、DHCP サーバから提供されるリストにある ToD サーバの 1 つに接続しようとします。接続できた場合、ケーブル モデムは ToD サーバから受信したタイム オフセットおよびタイムスタンプを使用して、システム クロックを更新します。

ToD サーバにアクセスできなかった場合、または応答がなかった場合、ケーブル モデムは最終的にタイムアウトし、CMTS に失敗がログされ、初期化プロセスを続けます。ケーブル モデムは ToD サーバの応答を受信しなくてもオンラインになることができますが、ToD 応答を正常に受信できるまで定期的に（少なくとも 5 分に 1 回）ToD サーバにアクセスする必要があります。ToD サーバに接続できるまで、ケーブル モデムはシステム クロックを 1970 年 1 月 1 日の午前 0 時（GMT）に初期化する必要があります。

（注） DOCSIS 1.0 仕様の最初のバージョンでは、ケーブル装置は ToD サーバから有効な応答を得ないかぎり、初期化プロセスを続けることができないと規定されていました。この要件は、リリース済みの DOCSIS 1.0 仕様および DOCSIS 1.1 仕様では削除されています。ただし、最初の DOCSIS 1.0 仕様に準拠した古いファームウェアで動作しているケーブル装置の場合、ToD サーバからの応答を受信できないと、オンラインにならないものがあります。

応答を受信するまでケーブル モデムは ToD サーバへの接続を繰り返し再試行するため、ヘッドエンドに 1 つまたは複数の他の ToD サーバがある場合も、Cisco CMTS で ToD サーバをアクティブにすることを考慮してください。これにより、ネットワークの輻輳によって他のサーバがダウンしたり接続できなくても、オンラインのケーブル モデムが常に Cisco CMTS にある ToD サーバへ確実に接続できるようになり、その結果、ToD 要求を繰り返し送信しなくなります。

ヒント Cisco CMTS を ToD サーバとして使用できるようにするには、DHCP サーバを設定して、ケーブル モデムの有効な ToD サーバ（DHCP オプション 4）の 1 つとして IP アドレスを Cisco CMTS に提供する必要があります。

さらに、DOCSIS 仕様ではケーブル モデムがオンラインになる前に ToD サーバの応答を正常に取得する必要はありませんが、タイムスタンプを取得しないとケーブル モデムは次の状況でオンラインになれません。

- DOCSIS コンフィギュレーション ファイルがタイムスタンプを取得している場合、ケーブル モデムがファイルをキャッシュしてそれに応答することを防ぐには、ケーブル モデムおよび CMTS のクロックを同期する必要があります。同期しない場合、ケーブル モデムは DOCSIS コンフィギュレーション ファイルが適切なタイムスタンプを持っているかどうかを判別できません。
- ケーブル モデムがベースライン プライバシー インターフェイス プラス（BPI+）認証および暗号化を使用して登録している場合、ケーブル モデムおよびCMTS のクロックは同期している必要があります。これは、BPI+ 認証では CMTS およびケーブル モデムが認証で使用されるデジタル証明書のタイムスタンプを確認することを必要とするためです。CMTS およびケーブル モデムのタイムスタンプが同期していない場合、ケーブル モデムは BPI+ 暗号化を使用してオンラインになることができません。

（注） DOCSIS ケーブル モデムは、RFC 868 互換 ToD サーバを使用して現在のシステム時間を取得する必要があります。この目的のために、Network Time Protocol（NTP）サービスや Simple Network Time Protocol（SNTP）サービスを使用することはできません。ただし、Cisco CMTS は、NTP または SNTP サーバを使用して自身のシステム クロックを設定し、その後それを ToD サーバで使用することができます。そうしない場合、CMTS が起動するたびに **clockset** コマンドを使用して手動で CMTS のクロックを設定しなければなりません。

ヒント ケーブル ヘッドエンドにインストールされているワークステーションや PC から追加のサーバを提供することができます。通常、UNIX および Solaris システムには、オペレーティング システムの一部として ToD サーバが含まれており、適切な行を inetd.conf ファイルに配置することでイネーブルにできます。Windows システムでは、Greyware や Tardis などのシェアウェア サーバを使用できます。DOCSIS 仕様では、ToD サーバは、パケットに対して TCP プロトコルの代わりにユーザ データグラム プロトコル（UDP）を使用する必要があります。

TFTP サーバ

すべての Cisco CMTS プラットフォームは、次のタイプのファイルを DOCSIS ケーブル モデムに提供できる TFTP サーバを提供するように設定できます。

- DOCSIS コンフィギュレーション ファイル：DOCSIS ケーブル モデムが DHCP リースを取得して ToD サーバの接続を試行した後、ケーブル モデムは TFTP を使用して承認済みの TFTP サーバから DOCSIS コンフィギュレーション ファイルをダウンロードします。DHCP サーバには、DOCSIS コンフィギュレーション ファイルの名前と TFTP サーバの IP アドレスをケーブル モデムに提供する役割があります。
- ソフトウェア アップグレード ファイル：DOCSIS コンフィギュレーション ファイルで、ケーブル モデムが特定のバージョンのソフトウェアを実行しなければならないと指定されていて、ケーブル モデムがまだそのソフトウェアを実行していない場合、ケーブル モデムはそのソフトウェア ファイルをダウンロードする必要があります。セキュリティ上の理由から、

ケーブル オペレータはDOCSISコンフィギュレーション ファイルと新しいソフトウェア ファイルのダウンロードにそれぞれ別の TFTP サーバを使用することができます。

- Cisco IOS-XE コンフィギュレーション ファイル：Cisco ケーブル装置用の DOCSIS コンフィギュレーションファイルでは、ケーブルモデムがコマンドラインインターフェイス（CLI）コンフィギュレーション コマンドを含む Cisco IOS-XE 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定することもできます。通常、音声ポートや IPSec 暗号化などのプラットフォーム固有の機能を設定するためにこれを実行します。

（注） DOCSIS コンフィギュレーション ファイルと Cisco IOS-XE コンフィギュレーション ファイルとを混同しないでください。DOCSIS コンフィギュレーション ファイルはDOCSIS仕様で指定された特定のフォーマットのバイナリ ファイルで、各 DOCSIS ケーブル モデムはオンラインになる前に有効なファイルをダウンロードする必要があります。これに対して、Cisco IOS-XE コンフィギュレーション ファイルは ASCII テキスト ファイルで、1 つまたは複数の Cisco IOS-XE CLI コンフィギュレーション コマンドがこれに含まれています。Cisco ケーブル装置のみが Cisco IOS-XE ファイルをダウンロードできます。

すべての Cisco CMTS プラットフォームは、これらのファイルをケーブル モデムにアップロードできる TFTP サーバとして設定できます。ファイルは有効な装置内に常駐できますが、通常 Cisco CMTS のフラッシュ ディスク スロットに挿入されているフラッシュ メモリ デバイスにコピーされます。

利点

- Cisco CMTS は、すべてのケーブル モデムがオンラインになる前に適切な日時で同期するように、プライマリまたはバックアップ ToD サーバとして動作できます。これにより、ToD のタイムアウト期間を待ってからオンラインになる必要がないため、ケーブルモデムは迅速にオンラインになることができます。
- Cisco CMTS 上の ToD サーバは、ケーブル ネットワークに接続されたすべてのデバイスが同じシステム クロックを使用するようにします。このため、多数のケーブル モデム、CPE デバイス、Cisco CMTS などのサービスによって生成されたデバッグ出力とエラー ログを解析するときに、システムの問題をより簡単にトラブルシューティングできます。
- Cisco CMTS は DOCSIS コンフィギュレーション ファイル、ソフトウェア アップグレード ファイル、および Cisco IOS コンフィギュレーション ファイル用の TFTP サーバとして機能できます。

ToD および TFTP サービスの設定方法

Cisco CMTS で Time of Day サービスおよび TFTP サービスを設定するために必要な次の設定タスクを参照してください。

Time-of-Day サービスの設定

ここでは、Cisco CMTS ルータで Time of Day（ToD）サーバを有効または無効にする手順について説明しています。

前提条件

Cisco CMTS を ToD サーバとして使用できるようにするには、DHCP サーバを設定して、ケーブル モデムの有効な ToD サーバ（DHCP オプション 4）の 1 つとして IP アドレスを Cisco CMTS に提供する必要があります。

Time-of-Day サービスの有効化

Cisco CMTS で ToD サーバを有効にするには、まず EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的

ステップ 1	**enable**
	
	例：
	
	`Router> enable`
	`Router#`
		特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

ステップ 2	**configureterminal**
	
	例：
	
	`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	**serviceudp-small-servers max-serversno-limit**
	
	例：
	
	`Router(config)# service udp-small-servers max-servers no-limit`
	`Router(config)#`
		UDP プロトコル（ToD、echo、chargen、discard など）を使用するマイナー サーバを使用できるようにします。
		
		max-servers no-limit オプションを指定すると、ケーブル障害または停電によって多数のケーブル モデムがオフラインになった場合でも、多数のケーブル モデムが一度に ToD サーバを取得できます。問題の解決後、即座にケーブル モデムを再接続できます。

ステップ 4	**cabletime-server**
	
	例：
	
	`Router(config)# cable time-server`
	`Router(config)#`
		Cisco CMTS で ToD サーバを有効にします。

	コマンドまたはアクション	目的

ステップ 5	**exit**
	
	例：
	
	`Router(config)# exit`
	`Router#`
		グローバル コンフィギュレーション モードを終了します。

Time-of-Day サービスの無効化

ToD サーバを無効にするには、まず EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的

ステップ 1	**enable**
	
	例：
	
	`Router> enable`
	`Router#`
		特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

ステップ 2	**configureterminal**
	
	例：
	
	`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	**nocabletime-server**
	
	例：
	
	`Router(config)# cable time-server`
	`Router(config)#`
		Cisco CMTS で ToD サーバを無効にします。

ステップ 4	**noserviceudp-small-servers**
	
	例：
	
	`Router(config)# no service udp-small-servers`
	`Router(config)#`
		（任意）すべてのマイナー UDP サーバの使用を無効にします。
		
		（注） 他の DHCP または TFTP サーバも有効にする場合は、マイナー UDP サーバを無効にしないでください。

ステップ 5	**exit**
	
	例：
	
	`Router(config)# exit`
	`Router#`
		グローバル コンフィギュレーション モードを終了します。

TFTP サービスの設定

CMTS が TFTP サーバとして動作し、ケーブル モデムに 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場合に Cisco CMTS の TFTP サービスを設定するには、次のステップを実行します。

- 選択した DOCSIS コンフィギュレーション エディタを使用して、DOCSIS コンフィギュレーション ファイルを作成します。
- Cisco CMTS のフラッシュ メモリ デバイスに任意のファイル（DOCSIS コンフィギュレーション ファイル、ソフトウェア アップグレード ファイル、Cisco IOS コンフィギュレーション ファイル）をすべてコピーします。通常これは、まず外部 TFTP サーバにファイルを配置し、TFTP コマンドを使用してルータのフラッシュ メモリにこのファイルを転送することで行われます。
- **tftp-server** コマンドを使用して、Cisco CMTS 上の TFTP サーバを有効にします。

オプションと記載されていない限り、各設定タスクは必須です。

手順

ステップ 1 **showfilesystems** コマンドを使用すると、CMTS で利用できるフラッシュ メモリ カードとともに、各カードの空き領域および各カードへのアクセスに使われる適切なデバイス名が表示されます。Cisco CMTS プラットフォームのほとんどの設定で線形フラッシュ メモリ カードとフラッシュ ディスク メモリ カードの両方がサポートされます。線形フラッシュ メモリにアクセスするには、**slot0**（または **flash**）および **slot1** デバイス名を使用します。フラッシュ ディスク メモリにアクセスするには、**disk0** および **disk1** デバイス名を使用します。

たとえば、次のコマンドにより、2 つのリニア フラッシュ メモリ カードを搭載した Cisco uBR7200 シリーズ ルータが表示されます。カードにアクセスするには、**slot0**（または **flash**）および **slot1** デバイス名を使用できます。

例：

```
Router# show file systems

File Systems:
     Size(b)     Free(b)      Type  Flags  Prefixes
    48755200    48747008     flash     rw   slot0: flash:
    16384000    14284000     flash     rw   slot1:
    32768000    31232884     flash     rw   bootflash:
*          -           -      disk     rw   disk0:
           -           -      disk     rw   disk1:
           -           -    opaque     rw   system:
           -           -    opaque     rw   null:
           -           -   network     rw   tftp:
      522232      507263     nvram     rw   nvram:
           -           -   network     rw   rcp:
           -           -   network     rw   ftp:
```

```
          -           -   network     rw   scp:
Router#
```

次に、2 つのフラッシュ ディスク カードを搭載した Cisco uBR10012 ルータの例を示します。これらのカードにアクセスするには、**disk0** および **sec-disk0** デバイス名を使用できます。

例：

```
Router# show file systems

File Systems:
     Size(b)     Free(b)      Type  Flags  Prefixes
           -           -     flash     rw   slot0: flash:
           -           -     flash     rw   slot1:
    32768000    29630876     flash     rw   bootflash:
*  128094208    95346688      disk     rw   disk0:
           -           -      disk     rw   disk1:
           -           -    opaque     rw   system:
           -           -     flash     rw   sec-slot0:
           -           -     flash     rw   sec-slot1:
*  128094208    95346688      disk     rw   sec-disk0:
           -           -      disk     rw   sec-disk1:
    32768000    29630876     flash     rw   sec-bootflash:
           -           -     nvram     rw   sec-nvram:
           -           -    opaque     rw   null:
           -           -   network     rw   tftp:
      522232      505523     nvram     rw   nvram:
           -           -   network     rw   rcp:
           -           -   network     rw   ftp:
           -           -   network     rw   scp:
Router#
```

ステップ 2 任意のフラッシュ メモリ カードに、CMTS にコピーするすべてのファイルに十分な空き領域があることを確認します。

ステップ 3 **ping** コマンドを使用して、任意のファイルを含むリモート TFTP サーバにアクセス可能であることを確認します。次に、IP アドレス 10.10.10.1 の外部 TFTP サーバに対して **ping** コマンドを使用する場合の例を示します。

例：

```
Router# ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/6/6 ms
```

ステップ 4 **copytftp** *devname* コマンドを使用して、外部 TFTP サーバから CMTS の適切なフラッシュ メモリ カードに各ファイルをコピーします。ここで、*devname* は接続先のフラッシュ メモリ カードのデバイス名です。外部 TFTP サーバの IP アドレスおよび転送するファイルのファイル名の入力が求められます。

次に、IP アドレス 10.10.10.1 の外部 TFTP サーバから最初のフラッシュ メモリ ディスク（disk0）に転送される docsis.cm ファイルの例を示します。

例：

```
Router# copy tftp disk0
Address or name of remote host []? 10.10.10.1

Source filename []? config-files/docsis.cm

Destination filename [docsis.cm]?
```

```
Accessing tftp://10.10.10.1/config-file/docsis.cm......
Loading docsis.cm from 10.10.10.1 (via Ethernet2/0): !!!
[OK - 276/4096 bytes]
276 bytes copied in 0.152 secs
Router#
```

ステップ 5 必要に応じてステップ 4, （792 ページ）を繰り返し、外部 TFTP サーバから Cisco CMTS のフラッシュ メモリ カードにすべてのファイルをコピーします。

ステップ 6 **dir** コマンドを使用して、転送したすべてのファイルがフラッシュ メモリ カードに含まれていることを確認します。

例：

```
Router# dir disk0:

Directory of disk0:/
    1  -rw-    10705784   May 30 2002 19:12:46  ubr10k-p6-mz.122-2.8.BC
    2  -rw-        4772   Jun 20 2002 18:12:56  running.cfg.save
    3  -rw-         241   Jul 31 2002 18:25:46  gold.cm
    4  -rw-         225   Jul 31 2002 18:25:46  silver.cm
    5  -rw-         231   Jul 31 2002 18:25:46  bronze.cm
    6  -rw-          74   Oct 11 2002 21:41:14  disable.cm
    7  -rw-     2934028   May 30 2002 11:22:12  ubr924-k8y5-mz.bin
    8  -rw-     3255196   Jun 28 2002 13:53:14  ubr925-k9v9y5-mz.bin
128094208 bytes total (114346688 bytes free)
Router#
```

ステップ 7 **configureterminal** コマンドを使用して、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。

例：

```
Router# configure terminal

Router(config)#
```

ステップ 8 **tftp-server** コマンドを使用して、Cisco CMTS 上の TFTP サーバによって特定のどのファイルを転送できるかを指定します。また、**alias** オプションを使用して、DHCP サーバが参照用に使用する別のファイル名を指定することもできます。たとえば、次のコマンドは、コンフィギュレーション ファイルおよびソフトウェア アップグレード ファイルの TFTP 転送を有効にします。

例：

```
Router(config)# tftp-server disk0:gold.cm alias gold.cm

Router(config)# tftp-server disk0:silver.cm alias silver.cm

Router(config)# tftp-server disk0:bronze.cm alias bronze.cm

Router(config)# tftp-server disk0:ubr924-k8y5-mz.bin alias ubr924-codefile

Router(config)# tftp-server disk0:ubr925-k9v9y5-mz.bin alias ubr925-codefile

Router(config)#
```

（注） また、**tftp-server** コマンドではオプションでアクセス リストを指定することにより、特定のファイルへのアクセスを、アクセス リストに一致する IP アドレスに限定できます。

ステップ 9 （任意）次のコマンドを使用すると、UDP スモール サーバの使用を有効にして、一度に任意の数の接続を許可できます。これにより、ケーブルまたは電源の障害が原因でオフラインになっていた多くのケーブル モデムは、すぐにオンラインに復帰します。

例：

```
Router(config)# service udp-small-servers max-servers no-limit
Router(config)#
```

外部 DHCP サーバの使用の最適化

Cisco CMTS は、DOCSIS ケーブル ネットワークでの外部 DHCP サーバの運用を最適化できるさまざまなオプションを提供します。詳細については、次の各項を参照してください。すべての手順は、ネットワークとアプリケーション サーバの必要性に応じて任意で実行します。

ケーブル ソース確認オプションの設定

外部 DHCP サーバを使用する際のセキュリティを向上するには、次の手順を使用してケーブル ソース確認機能を必要に応じて設定できます。

制約事項

- ケーブル ソース確認機能は、外部 DHCP サーバのみをサポートします。内部 DHCP サーバと一緒に使用することはできません。

手順

	コマンドまたはアクション	目的

ステップ 1	**enable**
	例：
	`Router> enable`
	`Router#`
		特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

ステップ 2	**configureterminal**
	例：
	`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	**interfacecable** *x/y*
	例：
	`Router(config)# interface cable 4/0`
	`Router(config-if)#`
		指定したケーブル インターフェイスに対してケーブル インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 4	**cablesource-verify** [**dhcp** | **leasetimer** *value*]
	
	例：
	
	`Router(config-if)# cable source-verify dhcp`
	
	例：
	
	`Router(config-if)# cable source-verify leasetimer 30`
	
	`Router(config-if)#`
		（任意）DHCP サーバがこのケーブル インターフェイスのデバイスに発行した IP アドレスに対してのみ、CMTS がネットワーク アクセスを許可していることを確認します。CMTS はケーブル インターフェイスを通過する DHCP パケットを検査し、どのインターフェイスでどの IP アドレスが有効であるかについてデータベースを構築します。
		
		• **dhcp** =（任意）不明な IP アドレスを持つすべてのデバイスからのトラフィックをドロップしますが、CMTS はデバイスの情報について DHCP サーバにもクエリを送信します。デバイスに有効な IP アドレスが設定されていると、DHCP サーバが CMTS に通知すると、CMTS はネットワーク上のデバイスを許可します。
		
		• **leasetimer** *value*=（任意）リース時間が満了した IP アドレスについて、ルータが内部 CPE データベースをチェックする頻度を分単位で指定します。これにより、ユーザが DHCP で割り当てられた IP アドレスをスタティック アドレスとして自分の CPE デバイスに割り当てることを防止できます。値の有効範囲は 1 ～ 240 分で、デフォルト値はありません。
		
		（注） **leasetimer** オプションは、インターフェイスで **dhcp** オプションもまた使用される場合にのみ適用されます。

ステップ 5	**nocablearp**
	
	例：
	
	`Router(config-if)# no cable arp`
	`Router(config-if)#`
		（任意）ケーブル ネットワークのデバイスから発信された Address Resolution Protocol（ARP）要求をブロックします。このコマンドを **cablesource-verifydhcp** コマンドとともに使用して、IP アドレスの乗っ取りやスプーフィングを行おうとする特定のタイプのサービス不正使用攻撃をブロックします。
		
		（注） それぞれの任意のケーブル インターフェイスでステップ 3, （794 ページ）～ステップ 5, （795 ページ）を繰り返します。

ステップ 6	**exit**
	
	例：
	
	`Router(config-if)# exit`
	`Router(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的

ステップ 7	**ipdhcprelayinformationoption**
	
	例：
	
	`Router(config)# ip dhcp relay information option`
	`Router(config)#`
		（任意）リレーしている DHCP パケットへの DHCP リレー情報（DHCP オプション 82）の挿入を CMTS で有効にします。これにより、DHCP サーバはどの CPE デバイスがどのケーブル モデムを使用しているかについての正確な情報を保存することができます。**cablesource-verifydhcp** コマンドを使用している場合は、このコマンドも一緒に使用する必要があります。

ステップ 8	**exit**
	
	例：
	
	`Router(config)# exit`
	`Router#`
		グローバル コンフィギュレーション モードを終了します。

プレフィックスベースの送信元アドレス確認の設定

外部 DHCP サーバ使用時のセキュリティを強化するために、グローバル コンフィギュレーション（Config）モードを開始してから、次の手順を使用してプレフィックスベースの SAV を設定できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**enable**
	
	例：
	
	`Router> enable`
	`Router#`
		特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

ステップ 2	**configureterminal**
	
	例：
	
	`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 source-verify enable-sav-static
	
	例：
	
	`Router# cable source-verify enable-sav-static`
	`Router(config)#`
		Cisco CMTS で SAV プレフィックス処理を有効にします。

	コマンドまたはアクション	目的
ステップ 4	**cablesource-verifygroup** *groupname* 例： `Router(config)# cable source-verify group sav-1`	SAV グループ名を設定します。 *groupname*：最大 16 文字の SAV グループ名。

ステップ 5	**prefix** [**ipv4_prefix/ipv4_prefix_length**|**ipv6_prefix/ipv6_prefix_length**]
	
	例：
	
	`Router(config-sav)# prefix 10.10.10.0/24`
	`Router(config-sav)#`
		SAV グループに関連する IPv4 または IPv6 プレフィックスを設定します。
		
		• *ipv4_prefix*：SAV グループに関連し、X.X.X.X/X 形式で指定された IPv4 プレフィックス。
		
		• ipv4_prefix_length：IPv4 プレフィックスの長さ。有効な範囲は 0 ～ 32 です。
		
		• ipv6_prefix：特定の SAV グループに関連し、X:X:X:X::/X で指定された IPv6 プレフィックス。
		
		• ipv6_prefix_length：IPv6 プレフィックスの長さ。有効な範囲は 0 ～ 128 です。
		
		1 つの SAV グループに最大 4 つのプレフィックスを設定できます。これらのプレフィックスは、IPv4 と IPv6 のいずれか、またはその両方を組み合わせることができます。

ステップ 6	**exit** 例： `Router(config-sav)# exit`	SAV コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 7	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

DHCP オプション パラメータの設定

外部 DHCP サーバを使用する場合、Cisco CMTS は特定のアプリケーションでケーブル ネットワークの運用を高めるオプションを数多くサポートします。これらのオプションを設定するには、まず EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的

ステップ 1	**enable**
	
	例：
	
	`Router> enable`
	`Router#`
		特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

ステップ 2	**configureterminal**
	
	例：
	
	`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	**ipdhcpsmart-relay**
	
	例：
	
	`Router(config)# ip dhcp smart-relay`
	`Router(config)#`
		（任意）プライマリ DHCP サーバが要求に 3 つ連続で応答しない場合、CMTS の DHCP リレー エージェントが、ケーブル モデムまたは CPE デバイスをセカンダリ DHCP サーバまたはアドレス プールに自動的に切り替えられるようにします。複数のセカンダリ サーバが定義されている場合は、リレー エージェントが DHCP 要求をセカンダリ サーバにラウンド ロビン形式で転送します。

ステップ 4	**ipdhcppingpacket0**
	
	例：
	
	`Router(config)# ip dhcp ping packet 0`
	`Router(config)#`
		（任意）DHCP サーバが、クライアントが該当する IP アドレスを現在すでに使用しているかどうかをテストするために、まず ICMP ping を送信するのではなく、そのプールから IP アドレスを割り当てるように指示します。ping オプションを無効にすると、数多くのモデムが同時に接続しようとした場合にアドレスの割り当てを高速化できます。ただし、ping オプションを無効にすると、ユーザが未承認の

	コマンドまたはアクション	目的
		静的 IP アドレスを CPE デバイスに割り当てる場合、割り当てられる IP アドレスが重複することもあります。 （注） DHCP サーバはデフォルトで、要求しているクライアントに特定のアドレスを割り当てる前に、1 つのプールアドレスに ping を 2 回送信します。ping の応答がない場合、DHCP サーバは、このアドレスが未使用であると見なして、要求しているクライアントにアドレスを割り当てます。

ステップ 5	**ipdhcprelayinformationcheck**
	例：
	`Router(config)# ip dhcp relay information check`
	`Router(config)#`
		（任意）転送された BOOTREPLY メッセージ内のリレーエージェント情報オプションを DHCP サーバが検証するように設定します。無効なメッセージはドロップされます。
		（注） **ipdhcprelayinformation** コマンドには、DHCP パケットの特殊な処理に役立つその他のオプションがいくつか含まれています。詳細については、Cisco IOS-XE のマニュアルのコマンド リファレンス ページを参照してください。

ステップ 6	**interfacecable** *x/y*
	例：
	`Router(config)# interface cable 4/0`
	`Router(config-if)#`
		指定したケーブル インターフェイスに対してケーブル インターフェイス コンフィギュレーション モードを開始します。

ステップ 7	**cabledhcp-giaddrpolicy** [**host**| **stb**| **mta**| **ps**] *giaddr*
	例：
	`Router(config-if)# cable dhcp-giaddr policy mta 172.1.1.10`
	`Router(config-if)#`
		DHCP 要求パケットの DHCP GIADDR フィールドを、ケーブル モデムの場合はプライマリ アドレスに、CPE デバイスの場合はセカンダリ アドレスに設定します。これにより、異なるクライアントごとに個別のアドレス プールを使用できます。
		• **host**：ホストに GIADDR を指定します。
		• **mta**：MTA に GIADDR を指定します。
		• **ps**：PS に GIADDR を指定します。
		• **stb**：STB に GIADDR を指定します。
		• *giaddr*：バンドル インターフェイスのセカンダリ インターフェイスの IP アドレス。

	コマンドまたはアクション	目的
		（注） **cabledhcp-giaddr** コマンドでは **primary** オプションもサポートされます。**primary** オプションは、すべてのデバイス タイプで GIADDR としてプライマリ インターフェイス IP アドレスのみを使用するように強制します。プライマリ アドレスが失敗してもセカンダリ アドレスには移行しません。

ステップ 8	**cablehelper-address** *address* [**cable-modem** | **host**|**mta**|**stb**]
	
	例：
	
	`Router(config-if)# cable helper-address 10.10.10.13`
	
	`Router(config-if)#`
		（任意）ケーブル インターフェイスまたはサブインターフェイスに応じたそれぞれの DHCP サーバを指定して、ケーブル モデムおよび CPE デバイスからの DHCP 要求のロード バランシングを有効にします。また、ケーブル モデムおよび CPE デバイスに個別のサーバを指定することもできます。
		
		• *address*：UDP ブロードキャスト パケットがユニキャスト パケット経由で送信された DHCP サーバの IP アドレス。
		
		• **cable-modem** ：このサーバがケーブル モデム パケットのみを受け入れるように指定します（任意）。
		
		• **host** ：このサーバが CPE デバイス パケットのみを受け入れるように指定します（任意）。
		
		• **mta**：このサーバが MTA パケットのみを受け入れるように指定します（任意）。
		
		• **stb**：このサーバが STB パケットのみを受け入れるように指定します（任意）。
		
		（注） オプションを指定しない場合、helper-address はすべてのケーブル デバイスをサポートし、関連する DHCP サーバはすべてのケーブル デバイス クラスから DHCP パケットを受け入れます。
		（注） オプションを 1 つのみ指定する場合、その他の種類のデバイス（ケーブル モデム、ホスト、mta、stb）は DHCP サーバに接続できません。それぞれのコマンドで任意の各オプションを指定する必要があります。
		
		ヒント 各ケーブル インターフェイスで複数のヘルパー アドレスを指定するには、このコマンドを繰り返します。16 個以上のヘルパー アドレスを指定できますが、Cisco IOS ソフトウェアが使用するのは有効な最初の 16 個のアドレスのみです。

	コマンドまたはアクション	目的
		ヒント　バンドル内の異なるサブバンドルでさまざまなヘルパー アドレスを設定する場合、ケーブル モデムがオンラインにならないことがあります。バンドル内のすべてのサブバンドルに同じヘルパー アドレスを使用することを推奨します。 （注）　**iphelper-address** コマンドは **cablehelper-address** と同様の機能を実行しますが、非ケーブル インターフェイスに対してこのコマンドを使用する必要があります。**cablehelper-address** コマンドは DOCSIS ネットワーク上の DHCP 要求の処理用として最適化されているため、ケーブルインターフェイスでこれを使用する必要があります。
ステップ 9	**cabledhcp-giaddrpolicy** 例： `Router(config-if)# cable dhcp-giaddr policy`	プライマリ アドレスがケーブル モデムで使用され、セカンダリ アドレスがホストと他の顧客宅内機器（CPE）デバイスで使用されるように、制御ポリシーを選択します。この設定は、ケーブルモデムとホストが異なるサブネットで IP アドレスを使用できるように、インターフェイスの CM をルーティング モードで設定する場合に通常使用されます。

ステップ 10	**exit**
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 11	**exit**
	例：
	`Router(config)# exit`
	`Router#`
		グローバル コンフィギュレーション モードを終了します。

ToD および TFTP サービスの設定方法

Cisco CMTS で Time of Day サービスおよび TFTP サービスを設定するために必要な次の設定タスクを参照してください。

設定例

ここでは、次の設定例を示します。

ToD サーバの例

次に、一般的な ToD サーバ設定の例を示します。

```
service udp-small-servers max-servers no-limit
cable time-server
```

ToD サーバの有効化に必要なコマンドはこれだけです。

TFTP サーバの例

次の行は、TFTP サーバを含む設定の例です。**tftp-server** コマンドを使用してシステム上の特定のファイルと一致するファイルを一覧して変更します。

```
! Enable the user of unlimited small servers
 service udp-small-servers max-servers no-limit
!
...
! Enable the TFTP server and specify the files that can be
!   downloaded along with their aliases
 tftp-server disk0:gold.cm alias gold.cm
 tftp-server disk0:silver.cm alias silver.cm
 tftp-server disk0:bronze.cm alias bronze.cm
 tftp-server disk0:ubr924-k8y5-mz.bin alias ubr924-codefile
 tftp-server disk0:ubr925-k9v9y5-mz.bin alias ubr925-codefile
```

その他の参考資料

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

CMTS ルータの DHCP、ToD、TFTP サービスに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *126*：ダウンストリーム インターフェイスの設定に関する機能情報

機能名	リリース	機能情報
DHCP、ToD、およびTFTPサービス	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 48 章

仮想インターフェイスのバンドル

仮想インターフェイスのバンドルにより、Cisco cBR シリーズ ルータの複数のケーブル インターフェイスを単一の論理バンドルに組み合わせることができ、これにより、IP アドレス空間を節約し、ネットワーク運用を簡素化することができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *127* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

仮想インターフェイスのバンドルに関する情報

この項の構成は、次のとおりです。

仮想インターフェイスのバンドルの概要

（注） すべてのケーブル バンドルが仮想インターフェイス バンドルとして自動的に変換および設定されます。スタンドアロン ケーブル インターフェイスは、正常に動作させるために、手動で仮想バンドルに設定する必要があります。

仮想インターフェイス バンドリングは以下をサポートします。

- 仮想インターフェイスのバンドルでは、マスターインターフェイスとスレーブ インターフェイスの代わりにバンドル インターフェイスとバンドル メンバーが使用されます。
- 仮想バンドル インターフェイスは、IP ループバック アドレスのように仮想的に定義されます。
- 仮想インターフェイスのバンドル情報を表示するには、複数の **show** コマンドを使用できます。

仮想インターフェイス バンドリングは、物理インターフェイスにエラーが発生した場合、バンドル内の 1 ライン カードの活性挿抜（OIR）に問題がある場合、またはマスター インターフェイスでの設定削除にエラーがあった場合に、接続が失われないようにします。

仮想インターフェイス バンドリングは、バンドル メンバー インターフェイスで、次のレイヤ 3 設定をサポートおよび管理します。

- IP アドレス
- IP ヘルパー アドレス
- source-verify 機能および lease-timer 機能
- cable dhcp-giaddr（giaddr フィールドは DHCP クライアントの IP アドレスに設定されています）
- プロトコルに依存しないマルチキャスト（PIM）
- アクセス コントロール リスト（ACL）
- サブインターフェイス
- IPv6
- 1982 バイトのレイヤ 3 MTU。

（注） お客様が CMTS から DOCSIS 3.1 モデムに ping を発行して 1982 バイト MTU をテストすることを希望する場合は、**cable mtu-override** コマンドを設定する必要があります。テストが完了したら、**no cable mtu-override** コマンドを使用して、この設定を削除してください。デフォルトでは、バンドルインターフェイスで no cable mtu-override は設定されていません。

（注） このバンドルの仮想インターフェイスを必ずオンのままにしておく必要があります（**noshutdown** を使って有効化されます）。

仮想インターフェイスのバンドルのガイドライン

次のガイドラインでは、仮想インターフェイスのバンドルについて説明します。

- 最初の仮想バンドル メンバーの初期設定によって、仮想バンドル インターフェイスが自動的に作成されます。
- すべてのケーブル バンドルは、ソフトウェア イメージのロード後に自動的に変換され、仮想バンドル内に配置されるように設定されます。
- スタンドアロン ケーブル インターフェイスは、正常に動作させるために、手動で仮想バンドルに設定する必要があります。
- 仮想バンドル インターフェイスはメンバーからのカウンタを累積します。メンバー リンクのカウンタは、バンドルに追加されてもクリアされません。バンドル専用のカウンタが必要な場合は、バンドルに追加する前に、またはイメージをロードする前に、メンバーのバンドル カウンタをクリアします。
- この機能では、1 ～ 255 の数値範囲で最大 40 の仮想インターフェイス バンドルをサポートします。
- バンドル内のすべてのメンバーが削除された場合でも、仮想バンドルインターフェイスは具体的に削除しない限り設定されたままになります。
- この機能は、仮想バンドル インターフェイスのサブインターフェイスをサポートします。
- バンドル認識型の設定は、仮想バンドル インターフェイスでサポートされます。
- バンドル非認識型の設定は、各仮想バンドル メンバーでサポートされます。
- 仮想バンドル インターフェイスを作成するとき、以前の Cisco IOS リリースでバンドル インターフェイスが存在した場合は、以前のケーブル設定がアップグレード後に再出現します。
- サブバンドルを使用する場合、すべてのレイヤ 3 構成をメイン バンドルではなくサブバンドルで設定する必要があります。

仮想インターフェイスのバンドル認識型とバンドル非認識型のサポート

仮想インターフェイス バンドリングでは、2 つの設定（仮想バンドル自体と、バンドル メンバーとして知られる仮想バンドルのインターフェイス）が使用されます。仮想インターフェイス バンドルとバンドル メンバーは、バンドルを認識している場合とバンドルを認識していない場合があります。

- バンドル認識型の機能は仮想バンドルで保持されます。次の作業を行います。

- IP アドレス
- IP ヘルパー、ケーブル ヘルパー
- DHCP giaddr
- Sub-interface
- 送信元確認
- リース クエリ
- Address Resolution Protocol（ケーブル ARP フィルタリング（ケーブル インターフェイスもバンドリング）および Proxy ARP）
- ケーブル マッチ
- アクセス コントロール リスト（ACL）
- プロトコルに依存しないマルチキャスト（PIM）
- ケーブル代行受信

• バンドル非認識型の機能は仮想バンドル メンバーで保持されます。次の作業を行います。

- DS/US 設定
- HCCP 冗長機能
- ロード バランシング
- DMIC、tftp-enforce、shared-secret
- スペクトル管理
- アドミッション制御
- 代行受信

仮想インターフェイスのバンドルの設定

仮想インターフェイス バンドルをイネーブルにして、必要に応じて Cisco CMTS のインターフェイス情報を再設定するには、まず仮想インターフェイス バンドルを設定し、指定した仮想バンドルの他のバンドル メンバーを追加します。すべての仮想インターフェイス バンドルの必要に応じて、各インターフェイスで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacebundle** *n* 例： `Router(config-if)# interface bundle 1`	選択したインターフェイスを仮想バンドルに追加します。これが仮想バンドルを設定する最初のインターフェイスの場合は、このコマンドは、指定したインターフェイスのバンドルをイネーブルにします。 Cisco CMTS で設定できるのは、最大 40 の仮想インターフェイス バンドルです。数値 ID の範囲は 1 ～ 255 です。
ステップ 4	**ipaddress** *address mask* 例： `Router(config-if)# ip address 7.7.7.7 255.255.255.0`	必要に応じて、Cisco IOS アップグレードを使用します。 指定したインターフェイスおよび仮想バンドルの IP アドレスを設定します。
ステップ 5	**cable helper-address address** [**cable-modem** | **host** | **mta** | **ps** | **stb**] 例： `Router(config-if)# cable helper-address 10.10.10.13`	（任意）IPv4 DHCP サーバ アドレスを指定します。
ステップ 6	**cable dhcp-giaddr** {**primary** | **policy** [**host** | **stb** | **mta** | **ps** | **strict**]} 例： `Router(config-if)# cable dhcp-giaddr policy host`	DHCP 要求パケットの DHCP GIADDR フィールドを設定します。
ステップ 7	**cable source-verify dhcp** 例： `Router(config-if)# cable source-verify dhcp`	（任意）DHCP サーバがこのケーブル インターフェイスのデバイスに発行した IP アドレスに対してのみ、Cisco CMTS がネットワーク アクセスを許可していることを確認します。Cisco CMTS はケーブル インター

	コマンドまたはアクション	目的
		フェイスを通過するDHCPパケットを検査し、どのインターフェイスでどのIPアドレスが有効であるかについてデータベースを構築します。不明なIPアドレスを持つすべてのデバイスからのトラフィックをドロップしますが、Cisco CMTSはデバイスの情報についてDHCPサーバにもクエリを送信します。デバイスに有効なIPアドレスが設定されていると、DHCPサーバがCisco CMTSに通知すると、CMTSはネットワーク上のデバイスを許可します。
ステップ8	**no cable arp** 例： `Router(config-if)# no cable arp`	（任意）静的IPv4 CPEがオンラインにならないようにブロックします。ケーブルネットワークのデバイスに送信するAddress Resolution Protocol（ARP）プロセスもブロックします。 （注） Cisco CMTSでサービス妨害（DoS）を発生させる特定の種類のスキャニング攻撃をブロックするには、このコマンドを**cable source-verify dhcp**コマンドとともに使用します。
ステップ9	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、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10	**interfacecable** *slot /subslot/port* 例： `Router(config)# interface cable 3/0/0`	仮想インターフェイスバンドルをイネーブルにする選択インターフェイスでインターフェイス コンフィギュレーション モードを開始します。
ステップ11	**cablebundle** *n* 例： `Router(config-if)# cable bundle 1`	インターフェイスバンドルに属するケーブルインターフェイスを設定します。ここで、*n*はバンドル番号です。
ステップ12	**nocableupstream** *n***shut** 例： `Router(config-if)# no cable upstream 4 shut`	必要に応じて、Cisco IOSアップグレードを使用します。 ケーブル インターフェイスは、指定したケーブル インターフェイスでno shutdownコマンドを使用してイネーブルにする必要があります。 *n*：ケーブル インターフェイスで仮想バンドルを有効にするように指定します。

	コマンドまたはアクション	目的
ステップ 13	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。

次の作業

インターフェイスから仮想バンドルを削除するには、インターフェイス コンフィギュレーション モードで **nointerfacebundle** コマンドを使用します。ここで、*n* はバンドル ID を示します。

nointerfacebundle *n*

バンドルからメンバーを削除する場合、バンドル自体が個別に削除されるまで、バンドルはインターフェイス（空だとしても）上に残ります。

バンドル インターフェイスの IPv6 パラメータの設定に関する詳細については、『*IPv6 on Cable*』機能ガイドを参照してください。

仮想インターフェイスのバンドルの設定の確認

- **show ip interface brief**：インターフェイスの概要を表示します。

  次に、このコマンドの出力例を示します。

```
Router# show ip interface brief

Interface              IP-Address      OK? Method Status                Protocol
Cable3/0/0             Bundle1         YES unset  up                    up
GigabitEthernet0       10.86.3.175     YES NVRAM  administratively down down
Bundle1                100.1.2.1       YES manual up                    up
Bundle2                100.1.3.1       YES NVRAM  up                    up
Dti4/1/0               unassigned      YES unset  administratively down down
Dti5/1/0               unassigned      YES unset  administratively down down
Dti4/1/1               unassigned      YES unset  administratively down down
Dti5/1/1               unassigned      YES unset  administratively down down
Loopback1              1.2.3.4         YES NVRAM  up                    up
Tunnel0                unassigned      YES unset  up                    up
```

- **show running-config interface bundle** *n*：指定したバンドルに関する情報を表示します。

  次に、このコマンドの出力例を示します。

```
Router# show running-config interface Bundle 1

Current configuration : 696 bytes
!
interface Bundle2
 ip address 100.1.3.1 255.255.255.0
 no cable nd
 cable arp filter request-send 3 2
 cable arp filter reply-accept 3 2
 no cable arp
 cable ipv6 source-verify dhcp
 cable source-verify dhcp
 cable dhcp-giaddr primary
```

```
 cable helper-address 10.10.0.53
 ipv6 address 2001:420:3800:910::1/64
 ipv6 enable
 ipv6 nd reachable-time 3600000
 ipv6 nd cache expire 65536
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 nd ra interval msec 2000
 no ipv6 redirects
 ipv6 dhcp relay destination 2001:420:3800:800:250:56FF:FEB2:F11D
 ipv6 dhcp relay destination vrf vrfa 2001:420:3800:800:250:56FF:FEB2:F11D
 ipv6 dhcp relay source-interface Bundle2
 arp timeout 2147483
```

- **show ip interface brief | include bundle**：バンドル インターフェイスの情報を表示します。

  次に、このコマンドの出力例を示します。

```
Router# show ip interface brief | include Bundle

Bundle1 unassigned YES unset up up
Bundle1.1 100.1.2.1 YES NVRAM up up
Bundle2 100.1.3.1 YES NVRAM up up
```

- **show running-config interface bundle** *n.n*：指定したバンドルのサブインターフェイスの情報を表示します。

  次に、このコマンドの出力例を示します。

```
Router# show running-config interface bundle 1.1

Current configuration : 1415 bytes
!
interface Bundle1.1
ip address 100.1.2.1 255.255.255.0
ip pim sparse-mode
ip rip send version 2
ip rip receive version 2
ip rip authentication mode md5
ip rip authentication key-chain ubr-rip
ip igmp static-group 239.1.4.1 source 115.255.0.100
ip igmp static-group 239.1.3.1 source 115.255.0.100
ip igmp static-group 239.1.2.1 source 115.255.0.100
ip igmp static-group 232.1.4.1 source 115.255.0.100
ip igmp static-group 232.1.3.1 source 115.255.0.100
ip igmp static-group 232.1.2.1 source 115.255.0.100
ip igmp static-group 232.1.1.1 source 115.255.0.100
ip igmp static-group 230.1.4.1
ip igmp static-group 230.1.3.1
ip igmp static-group 230.1.2.1
ip igmp static-group 224.1.4.1
ip igmp static-group 224.1.3.1
ip igmp static-group 224.1.2.1
ip igmp static-group 224.1.1.1
ip igmp version 3
ip igmp query-interval 20
no cable arp
cable ipv6 source-verify dhcp
cable source-verify dhcp
cable dhcp-giaddr primary
cable helper-address 10.10.0.53
ipv6 address 2001:420:3800:909::1/64
ipv6 enable
ipv6 nd reachable-time 3600000
ipv6 nd cache expire 65536
ipv6 nd prefix default no-advertise
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 nd ra interval msec 2000
no ipv6 redirects
```

```
ipv6 dhcp relay destination 2001:420:3800:800:250:56FF:FEB2:F11D link-address
2001:420:3800:909::1
ipv6 dhcp relay source-interface Bundle1
ipv6 rip CST enable
arp timeout 2147483
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
CMTS コマンド リファレンス	『Cisco IOS CMTS Cable Command Reference Guide』

標準および **RFC**

標準	タイトル
SP-RFIv1.1-I09-020830	『Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1』
SP-RFIv2.0-I03-021218	『Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 2.0』
SP-OSSIv2.0-I03-021218	『Data-over-Cable Service Interface Specifications Operations Support System Interface Specification, version 2.0』
SP-BPI+-I09-020830	『Data-over-Cable Service Interface Specifications Baseline Privacy Plus Interface Specification, version 2.0』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

仮想インターフェイスのバンドルに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *128*：仮想インターフェイスのバンドルに関する機能情報

機能名	リリース	機能情報
仮想インターフェイスのバンドル	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 49 章

IPv6 対応ケーブル

Cisco cBR シリーズ コンバージド ブロードバンド ルータは、完全な IPv6 機能をサポートします。

Cisco IOS ソフトウェアと Cisco CMTS ルータで使用可能な IPv6 機能サポートは広範囲に及びます。このマニュアルでは、Cisco CMTS ルータでサポートされるすべての IPv6 機能の概要とその制限事項について説明します。

ただし、このマニュアルではそれぞれの機能の詳細は説明しません。このマニュアルで説明する Cisco CMTS ルータでの IPv6 プロトコルのサポート領域は、プラットフォーム非依存、プラットフォーム固有の機能サポートで分類されます。

- プラットフォーム非依存の IPv6 機能：Cisco IOS ソフトウェアで他のいくつかのシスコ プラットフォーム用にサポートされる IPv6 機能。一般に、Cisco CMTS ルータ間でプラットフォーム固有の動作や設定の違いがありません。
- これらのプラットフォーム非依存の機能の制約事項については、「IPv6 対応ケーブルの制約事項」を参照してください。
- これらの機能の詳細、たとえば概念情報やタスクベースの設定情報については、この機能とは別の項、および Cisco IOS ソフトウェアに関するマニュアルで解説しています。Cisco IOS ソフトウェアに関するマニュアルでこの関連情報を得るための詳細情報は、「IPv6 対応ケーブルに関する機能情報」に示しています。

プラットフォーム固有の IPv6 機能：ケーブルの技術領域に固有の IPv6 機能。サポート対象の Cisco CMTS ルータにのみ適用されます。ケーブル固有の IPv6 機能サポートには、IPv6 をサポートする新規または変更されたケーブル機能、および CMTS ルータ プラットフォーム上の既存の（従来型）ケーブル機能における IPv6 プロトコルの透過的なサポートが含まれます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *129*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

IPv6 対応ケーブルの制約事項

マルチキャストの制約事項

IPv6 マルチキャストには、Cisco CMTS ルータ上での動作について次の制限があります。

- パケットが同じ CM の背後にある別の CPE 宛に送信されている場合、ICMP リダイレクトは発信元ホストに送信されません。すべての CPE 間トラフィックは Cisco CMTS ルータにより処理されます。
- IPv6 マルチキャスト転送は Parallel Express Forwarding（PXF）ではサポートされていません。したがって、IPv6 マルチキャスト転送のパフォーマンスは、ルート プロセッサ（RP）によって制限されます。

IPv6 マルチキャストの次の領域は Cisco CMTS ルータでサポートされません。

- Multiprotocol Border Gateway Protocol（MBGP）のアドレス ファミリ サポート
- Bidirectional Protocol Independent Multicast（PIM）
- ブートストラップ ルータ（BSR）
- DOCSIS 3.0 暗号化マルチキャスト
- 受信側の明示的トラッキング
- IPv6 マルチキャスト エコー
- Multicast Forwarding Information Base（MFIB）表示の強化
- マルチキャスト使用認証およびプロファイル サポート
- PIM 組み込みランデブー ポイント
- Protocol Independent Multicast Sparse Mode（PIM-SM）で受け入れる登録機能
- ブートストラップルータ（BSR）パケットのリバースパスフォワーディング（RPF）フラッディング
- ルーティング可能アドレスの hello オプション
- Multicast Listener Device（MLD）バージョン 1 SSM の Source Specific Multicast（SSM）マッピング

QoS 制約事項

Cisco IOS-XE リリース 16.5.1 では、次のフィールドが IPv6 ダウンストリーム分類でサポートされます。

- IPv6 宛先アドレス
- ipv6 送信元アドレス
- IPv6 次ヘッダー
- IPv6 トラフィック クラス

（注） IPv6 フロー ラベル フィールドはサポートされません。

DOCSIS QoS の次の領域は Cisco CMTS ルータでサポートされません。

- アップストリーム IPv6 のタイプ オブ サービス（TOS）の上書き
- ダウンストリーム IPv6 の分類

（注） ToS 上書き、DOCSIS 分類、ギガビット イーサネット上のモジュラ QoS CLI（MQC）がサポートされます。

IPv6 対応ケーブルに関する情報

この項では、次のトピックについて取り上げます。

サポートされている機能

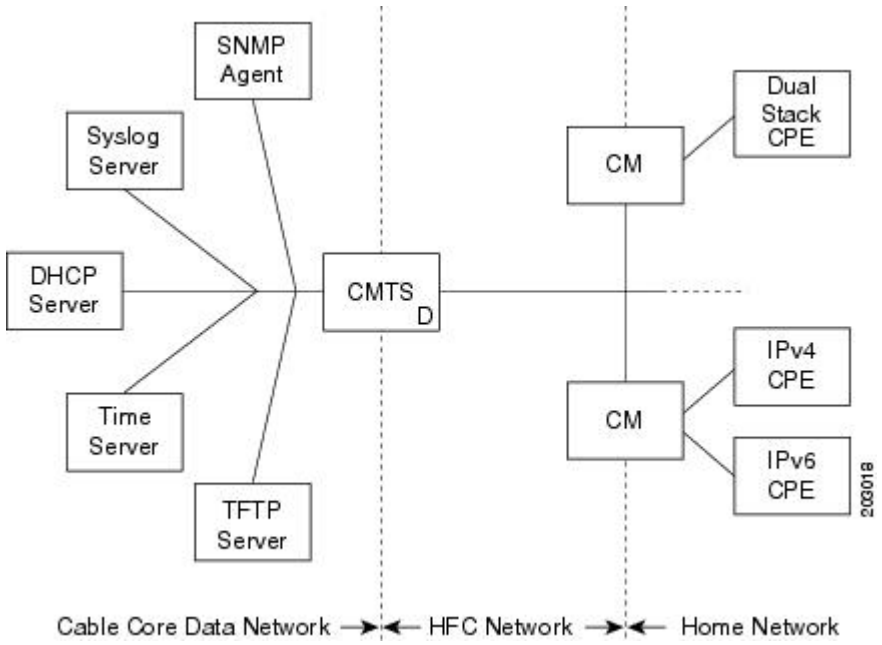
次の機能が Cisco CMTS ルータでサポートされています。

- PXF の IPv6 パケットの送信元検証
- PXF の ACL サポート
- ToS の上書き
- DOCSIS の分類
- ギガビット イーサネット上のモジュラ QoS CLI（MQC）
- IPv6 DOCSIS RP および LC HA と DCC
- IPv6 パケットの MAC タッピング
- バックホール宛ての IPv6 パケットの等コスト ルート ロード バランシング
- IPv6 over IPv4 GRE トンネル
- CM と CPE への異なるプレフィックスの割り当て
- MPLS-VPN 経由の DHCPv6
- DHCPv6 リレー プレフィックス委任 VRF の認識
- CPE ごとに単一アドバタイズの複数の IAPD 割り当て
- CM の背後にある複数の CPE への複数の IA_NA および IAPD の割り当て
- 各ケーブル モデムの IA_NA および IAPD の組み合わせのデフォルトの最大数は 16（リンク ローカル アドレスを含む）です。
- IPv6 ダウンストリーム ToS の上書き
- DHCPv6 クライアントのリンク層アドレス オプション（RFC 6939）
- Voice over IPv6この機能を使用する前に PacketCable Multimedia を有効にする必要があります。詳細については、http://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_pktcbl_pktcblmm/packetcable_and_packetcable_multimedia.html を参照してください。

IPv6 をサポートする DOCSIS 3.0 ネットワーク モデルの概要

次の図に、『*DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification*』で説明されているネットワーク モデルを示します。

図 *25*：*DOCSIS 3.0* ネットワーク モデル



このモデルでは、さまざまな装置が次の機能とサービスをサポートしています。

- 顧客宅内機器（CPE）：IPv4、IPv6、またはデュアル スタック動作をサポートします。

（注） Cisco cBR ルータは、デュアル スタック動作用にプロビジョニングされた CPE デバイスをサポートします。

- ケーブル モデム（CM）：ブリッジング装置として機能し、IPv4、IPv6、またはデュアル スタック動作をサポートします。
- ケーブルモデム終端システム（CMTS）ルータ：ハイブリッドファイバ同軸ケーブル（HFC）ネットワーク上で CM と連動して、プロビジョニング サーバおよび CMTS ルータ背後のコア データ ネットワークへの IPv4 および IPv6 ネットワーク接続を提供します。

CMTS ルータは、IPv6 アドレス割り当て、ルーティング、および IPv6 マルチキャストおよびユニキャスト パケットの転送をサポートします。

（注） Cisco cBR ルータは、1 つのクライアント ケーブル モデムか、または CPE あたり 1 個の DHCPv6 IPv6 アドレスのみをサポートします。この制限は、DHCPv6 プレフィックス委任のプレフィックスにも適用されます。1 台のクライアントに対して 2 個以上の DHCPv6 アドレスまたはプレフィックスをブロックする理由は、エンドツーエンド ネットワークにはソース アドレス選択（SAS）が必要であり、エンドツーエンドネットワークのノードすべてが正しい SAS をサポートしない可能性があるためです。さらに、SAS 仕様（RFC 3484）は、正しい SAS 動作を定義するために、IETF によって変更されています。

- シンプル ネットワーク管理プロトコル（SNMP）エージェント：ネットワーク上でデバイスを設定および照会するための管理ツールを提供します。
- Syslog サーバ：CM からメッセージを収集してその機能をサポートします。
- Dynamic Host Control Protocol（DHCP）サーバ：DOCSIS 3.0 ネットワーク モデルは、IP アドレスの割り当てを制御するための DHCPv4 と DHCPv6 の両サーバをサポートします。
- タイム サーバ：CM に現在の時刻を提供します。
- 簡易ファイル トランスポート プロトコル（TFTP）サーバ：CM コンフィギュレーション ファイルを提供します。

ケーブル モデム IPv6 アドレス プロビジョニングの概要

ケーブル モデムが CMTS ルータに登録される際、それに先立ち CMTS ルータは、サポートする IP プロビジョニング モードに関する情報をケーブル モデムに提供するために MAC Domain Descriptor（MDD）メッセージを送信します。CMTS ルータのプロビジョニング モードを設定するには、**cableip-init** インターフェイス コンフィギュレーション コマンドを使用します。詳細については、ケーブル インターフェイスとバンドルへの IPv6 アドレッシングと基本接続の実装，（834 ページ）を参照してください。

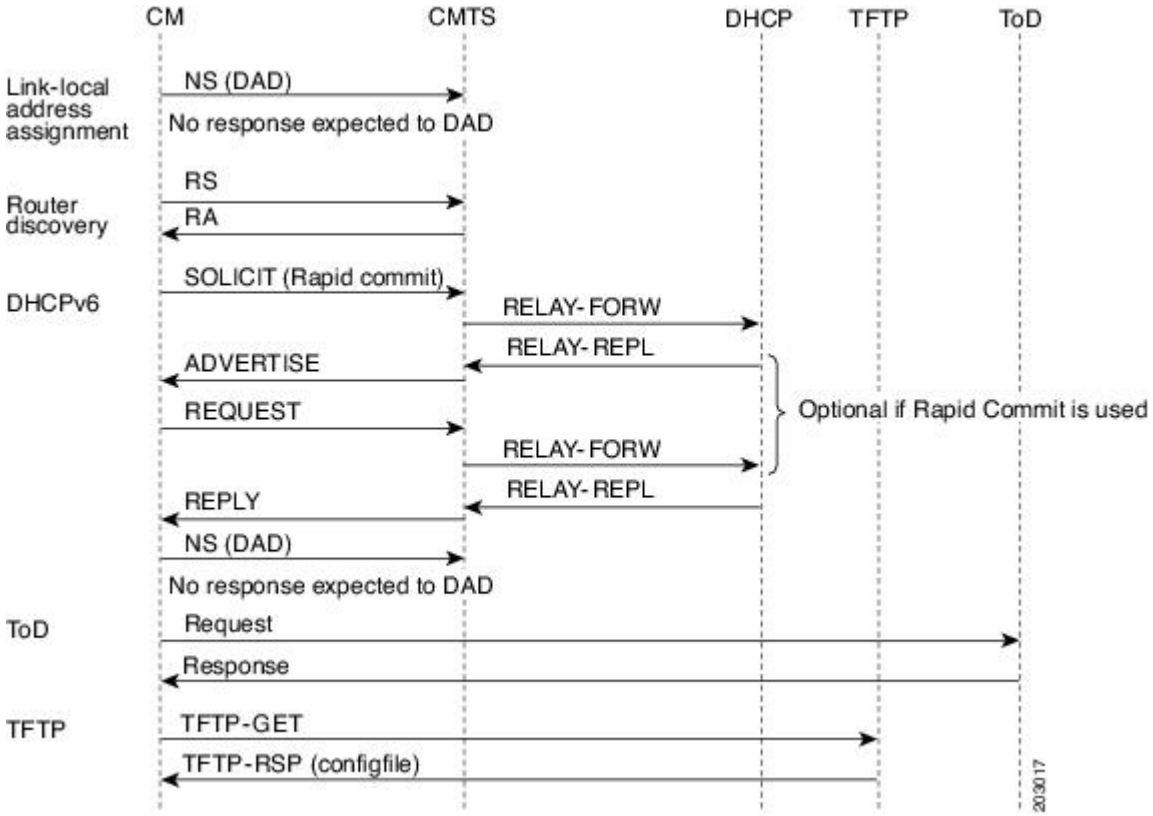
MDD には、IP バージョン、管理および代替プロビジョニング モード、ならびにダウンストリーム トラフィック フィルタリングが可能なケーブル モデムで使用される事前登録ダウンストリーム サービス ID（DSID）を定義する IP 初期化パラメータ（TLV：タイプ、長さ、値）が含まれます。

（注） Cisco CMTS ルータは、代替プロビジョニング モードおよび事前登録 DSID をサポートしません。

MULPIv3.0 I04 以降のバージョンの *DOCSIS 3.0 MAC and Upper Layer Protocols InterfaceSpecification* をサポートするには、ケーブル モデムは第一に IPv6 アドレスの取得を試みる必要があります。

次の図は、ケーブルモデムがIPv6アドレスを要求しているときの、ケーブルモデム、CMTSルータ、DHCP サーバ間のメッセージ フローを示しています。

図 *26*：*DHCP IPv6* アドレス割り当てにおける *CM* プロビジョニングのメッセージ フロー



1. リンクローカル アドレス割り当て：ケーブル モデムはリンクローカル アドレス（LLA）を使用してネイバー要請（NS）メッセージを CMTS ルータに送信します。これにより、その LLA に対する重複アドレス検出（DAD）プロセスが開始されます。この NS メッセージに対し、ケーブル モデムに応答は返されません。
2. ルータの検出：定期的なルータ アドバタイズ（RA）メッセージを検出するために、ケーブル モデムはダウンストリームをリスニングします。RA メッセージが検出されると、ケーブル モデムは RA メッセージのデータを使用してデフォルト ルートを設定します。RA が指定期間内に検出されない場合、ケーブルモデムはルータ要請（RS）メッセージを送信して、リンク（全ノードのマルチキャスト）上のルータを探索します。CMTS ルータは、M および O ビットが 1 に設定された状態のルータ アドバタイズ（RA）メッセージを用いて応答し、ステートフルなアドレス設定を行うよう CM に指示します。

（注） Cisco CMTS ルータは SLAAC アドレス割り当てをサポートしません。

- DHCPv6：ケーブル モデムは CMTS ルータに IPv6 アドレスを要求する DHCPv6 Solicit メッセージを送信します。CMTS ルータはこのメッセージを DHCPv6 サーバにリレーします。DHCPv6 サーバは、サーバの可用性を示すアドバタイズ メッセージを送信します。

ケーブル モデムで Rapid-Commit オプションが使用されていない場合、ケーブル モデムはアドバタイズ メッセージへの応答として、CMTS ルータが DHCPv6 サーバへのリレーに経由するサーバを選択するよう要求メッセージを送信します。Rapid-Commit オプションが使用されている場合、同じ CPE に異なるアドレスを割り当てる可能性がある、複数の DHCPv6 サーバは使用できません。

ケーブル モデムは DAD プロセスを開始します。この中では、DHCPv6 サーバにより割り当てられる IPv6 アドレスの一意性を確認します。

- TFTP および Time-of-Day（ToD）：IP 接続が確立されると、CM は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 TFTP サーバに要求を送信するとともに、起動プロセスを完了するために ToD サーバに現在時刻を要求します。

CMTS での IPv6 デュアル スタック CPE サポート

家庭で導入されるオペレーティング システム（OS）のほとんどはデュアル スタック動作をサポートします。Cisco CMTS は、CPE 上で IPv4 アドレッシングかつ IPv6 アドレッシングなデュアル スタックをサポートします。

サブインターフェイス上の IPv6 の概要

Cisco CMTS は、バンドル サブインターフェイス上で IPv6 をサポートします。バンドル サブインターフェイス上で IPv6 を設定する方法については、ケーブル インターフェイスとバンドルへの IPv6 アドレッシングと基本接続の実装，（834 ページ）を参照してください。CMTS のバンドル コンフィギュレーションの例については、例：サブインターフェイス経由の IPv6，（851 ページ）を参照してください。

サブインターフェイスで IPv6 をイネーブルにするには、バンドルでなくバンドル サブインターフェイスで IPv6 を設定します。サブインターフェイスを設定したら、CM をリセットします。

（注） IPv6 に対するサブインターフェイス上の MPLS VPN はサポートされません。

IPv6 での高可用性の概要

Cisco cBR シリーズ ルータはスーパーバイザ カード用に IPv6 HA をサポートします。

（注） IPv6 DOCSIS HA および HCCP は、Cisco CMTS ルータでサポートされます。

Cisco CMTS ルータでの IPv6 HA 機能のサポートには、次の機能が含まれます。

- DOCSIS PRE HA
- DOCSIS ライン カード HA
- 動的チャネル変更（DCC）

DOCSIS PRE HA

DOCSIS PRE HA には、Cisco CMTS ルータに関する次の動作制限と前提条件があります。

- CM と CPE は、PRE がスイッチオーバーした後でオフラインになってはいけません。
- IPv6 CM と CPE のデータ構造は、PRE のスイッチオーバー前に、スタンバイの PRE と同期されている必要があります。動的と一括の両方の同期がサポートされます。
- シングル スタック、デュアル スタック、および APM は、CM 用にサポートされます。
- シングル スタックおよびデュアル スタックのプロビジョニング モードが CPE でサポートされます。
- PRE のスイッチオーバー後、スタンバイ PRE でネイバー探索（ND）メッセージを使用して IPv6 ネイバー エントリが再構築されます。IPv6 ルートはルーティング プロトコルが収束した後で再構築されます。

DOCSIS ライン カード HA

DOCSIS ライン カード HA には、Cisco CMTS ルータに関する次の動作制限と前提条件があります。

- IPv6 CM と CPE のデータ構造は、ライン カードのスイッチオーバー前に、スタンバイのライン カードと同期されている必要があります。動的と一括の両方の同期がサポートされます。
- CM と CPE は、ライン カードがスイッチオーバーして復帰した後でオフラインになってはいけません。CM と CPE は、スイッチオーバー前と同様に動作する必要があります。
- DOCSIS ライン カード HA は、4+1 と 7+1 の両方の冗長性をサポートします。
- IPv6 でのトラフィック停止は長引く可能性があります。これは、ルーティング プロトコルが収束した後のみトラフィックのリカバリが発生するためです。

動的チャネル変更

動的チャネル変更（DCC）機能は、Cisco CMTS ルータでサポートされます。

（注） シングル スタック IPv6 CM と CPE またはデュアル スタック CM と CPE の DCC の動作は、シングル スタック IPv4 CM と CPE の場合と同じです。

IPv6 および IPv4 DCC 機能には、Cisco CMTS ルータに関する次の動作制限と前提条件があります。

ナローバンド ケーブル モデム

- CM の送信元と宛先 MAC ドメインが同じライン カード上にある場合、CM とその関連 CPE をアップストリームまたはダウンストリーム間で移動するために、または CM と CPE をアップストリームとダウンストリームの組み合わせ間で移動するために、DCC 初期化テクニック 0、1、2、3、および 4 が使用されます。
- CM の送信元と宛先 MAC ドメインが異なるライン カード上にある場合は、CM とその関連 CPE をライン カード間で移動するために、DCC 初期化テクニック 0 のみを使用できます。

ワイドバンド ケーブル モデム

- CM の送信元と宛先 MAC ドメインが同じライン カード上にある場合、CM とその関連 CPE をアップストリーム間で移動するために、DCC 初期化テクニック 0、1、2、3、および 4 が使用されます。
- CM のプライマリ ダウンストリームが DCC 後に変更される場合は、CM とその関連 CPE をライン カード間で移動するために、DCC 初期化テクニック 0 のみを使用できます。

IPv6 VPN over MPLS の概要

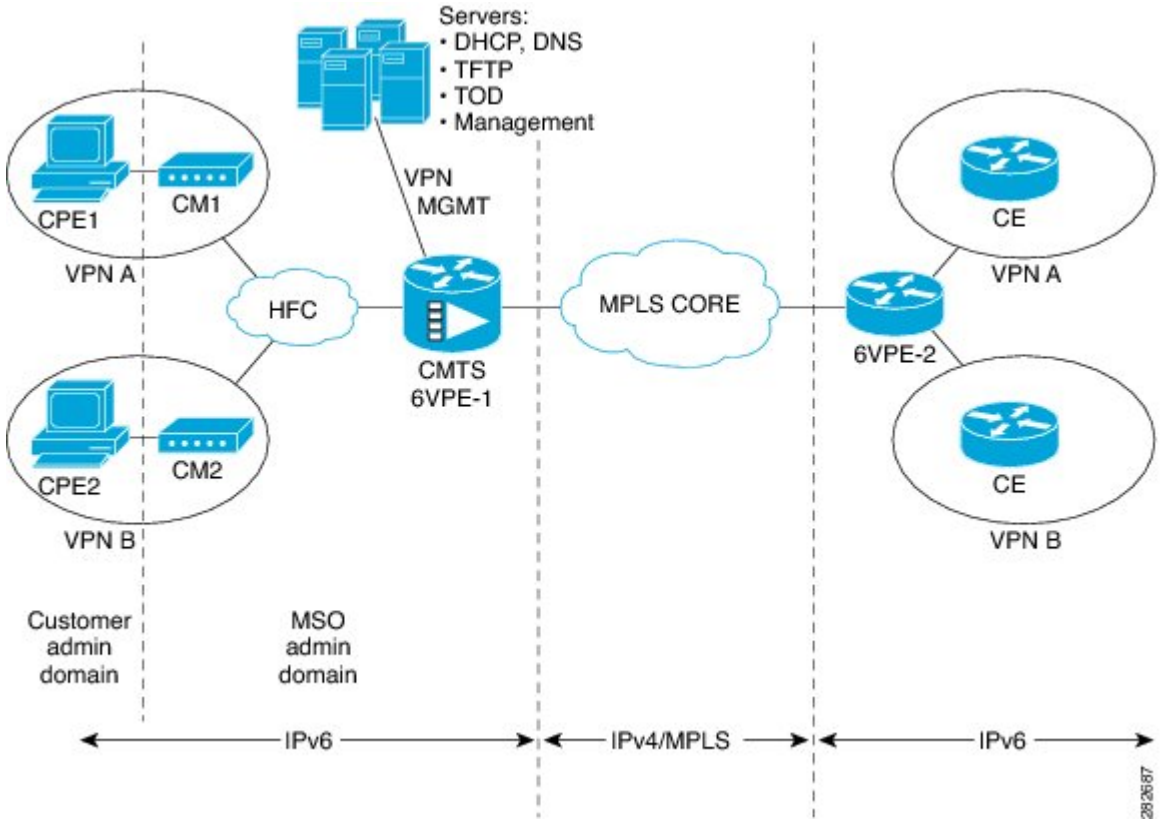
マルチプロトコル ラベル スイッチング（MPLS）の VPN 機能は、プロバイダー エッジ（PE）ベースの VPN モデルの実装を表します。このマニュアルでは、IPv6 VPN over MPLS（6VPE）機能について説明します。

6VPE 機能により、サービス プロバイダーは IPv4 MPLS コアでの PE ルータのアップグレードや再設定をしなくても IPv6 VPN サービスを提供することができます。この結果、IPv6 VPN サービスの設定と動作は現行の IPv4 VPN サービスとほとんど同じになります。

原則として、IPv4 VPN と IPv6 VPN との間に相違点はありません。IPv4 と IPv6 のどちらにおいても、マルチプロトコル BGP が MPLS VPN for IPv6（VPNv6）アーキテクチャのコアとなります。サービス プロバイダー バックボーンを介して IPv6 ルートを配布するために使用され、同じ手順を使用して、重複するアドレス、再配布ポリシー、およびスケーラビリティの問題が処理されます。

次の図に、6PE/6VPE リファレンス アーキテクチャの概略図を示します。

図 *27* : *6PE/6VPE* リファレンス アーキテクチャ



ケーブル モニタ

Cisco CMTS ルータ用のケーブル モニタおよび傍受機能では、ケーブル ネットワークから着信するトラフィックのモニタリングおよび傍受のソフトウェア ソリューションを提供します。これらの機能は、サービス プロバイダーが合法的傍受機能を提供します。

詳細については、『Cable Monitor and Intercept Features for the Cisco CMTS Routers』ガイドを参照してください。

Cisco CMTS での IPv6 CPE ルータ サポートの概要

IPv6 CPE ルータ サポートが Cisco CMTS で提供されています。IPv6 CPE ルータは、主に、エンドユーザ ネットワークをサービス プロバイダー ネットワークに接続する家庭および小規模オフィス向けノードです。ホーム ルータとも呼ばれます。

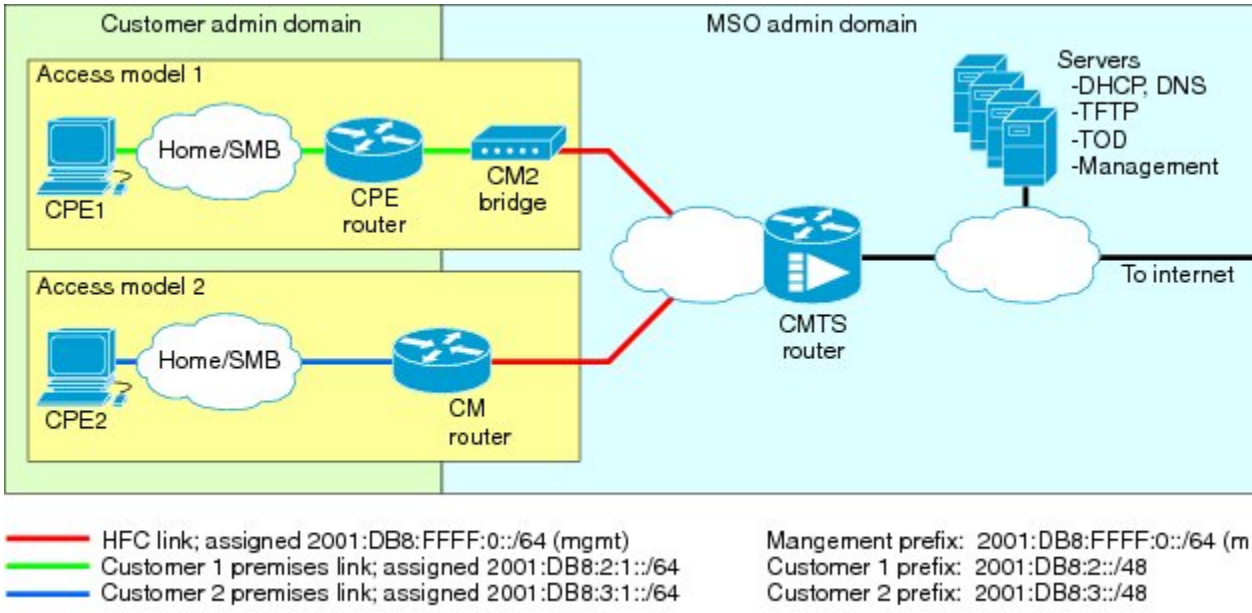
IPv6 CPE ルータは、IPv6 ルーティングの実行を担います。つまり、IPv6 CPE ルータは、そのルーティングテーブルで IPv6 宛先アドレスを検索し、どのインターフェイスにパケットを送信する必要があるかを決定します。

IPv6 CPE ルータでは次の機能が実行されます。

- WAN インターフェイスを自動的にプロビジョニングします。
- LAN インターフェイスのプロビジョニング用の IP アドレス空間を取得します。
- サービス プロバイダー ネットワークからの他の設定情報を取得します。

次の図に、CM が IPv6 アドレスを要求しているときの、CPE ルータ、CMTS、DHCPv6 サーバ（CNR）間の CPE ルータ リファレンス アーキテクチャの概略図を示します。

図 *28*：*IPv6 CPE* ルータ リファレンス アーキテクチャ



IPv6 CPE ルータ サポート機能の一部として、次の拡張機能が導入されています。

- IPv6 ルータ デバイスへのサポート。
- IPv6 プレフィックス委任（PD）の高可用性。
- IPv6 ケーブルの source-verify、ケーブル DOCSIS フィルタ コード、およびパケット傍受でのプレフィックス認識のサポート。

CMTS での IPv6 プレフィックス安定性の概要

Cisco CMTS での IPv6 プレフィックス安定性は、DOCSIS 3.0 MULPI CM SP MULPIv3.0 I15 110210 規格で指定されているようにサポートされます。IPv6 プレフィックス安定性により、IPv6 ホームルータは同じプレフィックスを維持しながら、ある Cisco CMTS から別の Cisco CMTS に移動できます。

マルチプル サービス オペレータ（MSO）は、この機能を使用することで、（IPv6 ルータを所有する）顧客がノード分割をしても同じ IPv6 プレフィックスを保持できるようにすることができます。

設定可能な DHCPv6 リレー アドレス

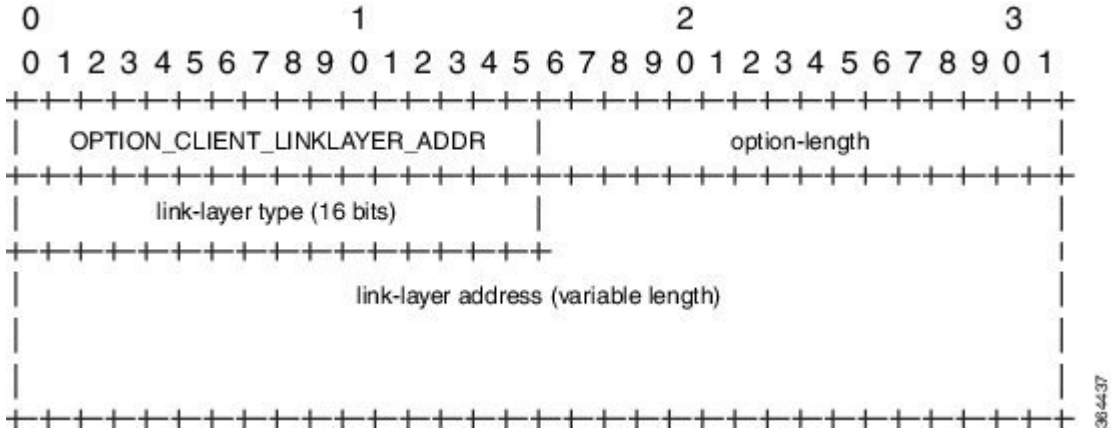
Cisco CMTS ルータ上の DHCPv6 Cisco IOS リレー エージェントは、発信元アドレスからのすべての設定済みリレー宛先へ relay-forward メッセージを送信します。発信元アドレスは、ネットワーク インターフェイスでプロビジョニングされた IPv6 アドレス、または Cisco CMTS WAN IPv6 アドレスです。リレー宛先は、サーバまたは別のリレーエージェントのユニキャストアドレス、またはマルチキャストアドレスにすることができます。relay-forward メッセージには、特定の DHCPv6 リンク アドレスが含まれます。

DHCP リレー エージェントは、クライアントとサーバ間のメッセージを中継するために使用されます。クライアントは、リンクスコープを持つ予約済みのマルチキャスト アドレスを使用して DHCP サーバを探します。

DHCPv6 クライアントのリンク層アドレス オプション（RFC 6939）

Cisco IOS-XE リリースでは、DHCPv6 クライアントのリンク層アドレス オプション（RFC 6939）をサポートしています。これは、ファーストホップ DHCPv6 リレー エージェント（クライアントと同じリンクに接続されたリレー エージェント）がサーバに送信されている DHCPv6 メッセージでクライアントのリンク層アドレスを提供できるようにするためのオプションのメカニズムと関連の DHCPv6 オプションを定義します。

DHCPv6 クライアントのリンク層アドレス オプションの形式は次のとおりです。



名前	説明
option-code	OPTION_CLIENT_LINKLAYER_ADDR (79)
option-length	2 + MAC アドレス長

名前	説明
link-layer type	CPE または CM MAC アドレスのタイプ。リンク層のタイプは、RFC0826 の説明に従い IANA によって割り当てられた有効なハードウェアの種類である必要があります。
link-layer address	CPE または CM の MAC アドレス。

（注） RFC6939 はデフォルトで有効になります。CLI コマンドでは有効/無効にできません。

Cisco CMTS バンドル サブインターフェイスで DHCPv6 リレー アドレスを設定するには、DHCPv6 リレー エージェントの設定, （847 ページ）セクションを参照してください。

DHCPv6 のクライアント、サーバ、またはリレー エージェント機能の詳細については、『IPv6 Implementation Guide, Cisco IOS XE Release 3S』の「Implementing DHCP for IPv6」の章を参照してください。

単一アドバタイズでの複数の IAPD のサポート

CM の背後にある CPE への複数の IA_NA および IAPD の割り当てが、Cisco CMTS ルータでサポートされます。この機能には、リンクローカル アドレス、IA_NA および IAPD に対するサポートが含まれます。ただし、1 つの CM に割り当てることができるのは、1 つの IA_NA のみです。この IA_NA には、静的または DHCP 割り当てが可能です。

CM の背後にある CPE は、複数の DHCPv6 IA_NA および IAPD を要求できます。各 CPE には単一のアドバタイズ/応答メッセージで複数の IA_NA および IAPD が割り当てられます。IA_NA および IAPD の各 CPE 要求は、個別のアドバタイズ/応答メッセージとして処理されます。

IPv6 ネイバー探索グリーニング

IPv6 ネイバー探索（ND）グリーニング機能を使用して、失効した IPv6 CPE アドレスの回復と Cisco CMTS 加入者データベースの CPE レコードの更新が、Cisco CMTS ルータによって自動的に行われるようにすることができます。Cisco CMTS ルータは、アップストリーム方向に送信されている要請されたネイバー アドバタイズメント（NA）メッセージのみをグリーニングします。IPv6 ND グリーニングは、IPv4 CPE リカバリに使用される Address Resolution Protocol（ARP）グリーニングに似ています。

IPv6 ND グリーニング機能は、Cisco CMTS ルータにデフォルトで設定されています。この機能を無効にするには、バンドル インターフェイス コンフィギュレーション モードで **cable nd** コマンドの **no** 形式を使用します。**cable nd** コマンドは、Cisco CMTS サブスクライバ データベースに CPE（ケーブル モデム背後のホスト）を追加します。このコマンドは、ルータの IPv6 ND プロトコルの動作には影響しません。

（注） IPv6 ND グリーニング機能は、ダウンストリーム方向で送信された NA メッセージのグリーニングはサポートしません。

IPv6 対応ケーブルの設定方法

ここでは、次の作業について説明します。

IPv6 スイッチング サービスの設定

CMTS ルータは、Cisco Express Forwarding for IPv6（CEFv6）または distributed CEFv6（dCEFv6）のいずれかを使用して、ユニキャストおよびマルチキャストの IPv6 トラフィックの転送をサポートします。

- CEFv6：すべての CMTS プラットフォーム
- dCEFv6：Cisco uBR10012 ユニバーサル ブロードバンド ルータのみ

また、CMTS ルータは、ルータ上で Cisco Express Forwarding スイッチングまたは distributed Cisco Express Forwarding スイッチングをグローバルに有効にする限り、ユニキャスト リバース パス フォワーディング（RPF）もサポートします。シスコ エクスプレス フォワーディング スイッチングの入力インターフェイスを設定する必要はありません。シスコ エクスプレス フォワーディングがルータ上で実行されているかぎり、個々のインターフェイスは他のスイッチング モードで設定できます。

CMTS ルータで Cisco Express Forwarding または（Cisco uBR10012 ユニバーサル ブロードバンド ルータ上でのみサポートされる）distributed Cisco Express Forwarding を使用して IPv6 トラフィックの転送を設定するには、**ipv6unicast-routing** グローバル コンフィギュレーション コマンドを使用して IPv6 ユニキャスト データグラムの転送を設定し、**ipv6address** コマンドを使用してバンドル インターフェイス上に IPv6 アドレスを設定する必要があります。

showipv6cefplatform コマンドは、Cisco CMTS プラットフォームでサポートされます。**showipv6cefplatform** コマンドは、デバッグの目的で使用できます。

はじめる前に

- Cisco Express Forwarding v6 または distributed Cisco Express Forwarding v6 の設定前に、**ipcef** または **ipcefdistributed** コマンドを使用して、ルータで Cisco Express Forwarding for IPv4 をグローバルに有効にする必要があります。

（注） デフォルトでは、**ipcef** コマンドはすべての Cisco CMTS ルータで有効です。そのため、無効にされている場合のみ有効にする必要があります。ただし、IPv4 または IPv6 用の分散型 CEF スイッチング サービスを実行する場合は、Cisco uBR10012 ユニバーサル ブロードバンド ルータで **ipcefdistributed** コマンドを明示的に設定する必要があります。

- **ipv6unicast-routing** グローバル コンフィギュレーション コマンドを使用して、IPv6 ユニキャスト データグラムの転送を設定する必要があります。
- ケーブル バンドル インターフェイスで IPv6 アドレッシングを設定する必要があります。
- CEF スイッチングは、ユニキャスト RPF を機能させるために必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	次のいずれかを実行します。
	• **ipcef**
	• **ipcefdistributed**
	例：
	`Router(config)# ip cef`
	or
	`Router(config)# ip cef distributed`
		Cisco Express Forwarding をイネーブルにします。
		または
		distributed Cisco Express Forwarding for IPv4 データグラムを有効にします。
		（注） CMTS ルータの場合、distributed Cisco Express Forwarding は Cisco uBR10012 ユニバーサル ブロードバンド ルータでのみサポートされます。

ステップ 4	次のいずれかを実行します。
	• **ipv6cef**
	• **ipv6cefdistributed**
	例：
	`Router(config)# ipv6 cef`
	or
	`Router(config)# ipv6 cef distributed`
		Cisco Express Forwarding v6 を有効にします。
		または
		distributed Cisco Express Forwarding v6 for IPv6 データグラムを有効にします。
		（注） CMTS ルータの場合、distributed Cisco Express Forwarding v6 は Cisco uBR10012 ユニバーサル ブロードバンド ルータでのみサポートされます。

	コマンドまたはアクション	目的
ステップ 5	**ipv6unicast-routing** 例： `Router(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。

次の作業

- （任意）グローバル コンフィギュレーション モードで **ipv6multicast-routing** コマンドを使用して IPv6 マルチキャスト ルーティングを有効にし、他のマルチキャスト機能を設定します。

ケーブル インターフェイスとバンドルへの IPv6 アドレッシングと基本接続の実装

ケーブル仮想バンドル インターフェイスの設定

ケーブル ライン カード インターフェイスで唯一必要な IPv6 設定は IP プロビジョニング モードです。IPv6 機能の残りの部分は、設定する特定のケーブル ライン カード インターフェイスに関連付けられた仮想バンドル インターフェイスで設定されます。

インターフェイス コンフィギュレーション モードでサポートされる IPv6 機能のほとんどは（ケーブル固有の IPv6 機能とプラットフォームに依存しない IPv6 機能の両方）、ケーブル バンドル インターフェイスで設定されます。

Cisco CMTS ルータは、バンドル インターフェイスで IPv6 ルーティングをサポートし、パケットを転送するために、IPv6 ユニキャストとマルチキャスト アドレスの両方をケーブル バンドル転送テーブルにマッピングします。

各バンドル インターフェイスには、IPv6 の有効時にリンク ローカル トラフィックをサポートする独自のリンク ローカル アドレス（LLA）があります。Cisco CMTS ルータは、最大 40 のアクティブなバンドル インターフェイスをサポートし、最大 40 のアクティブな IPv6 対応バンドル インターフェイスにも変換できます。

IPv6 のコマンドは、複数のバンドル サブインターフェイスで設定することができます。

はじめる前に

cableipv6source-verify コマンドと **cablend** コマンドは、Cisco IOS リリース 12.2(33)SCE 以降では互いに両立しません。DHCPv6 および SAV ベースの CPE だけがルータでトラフィックを送信できるようにするには、**cableipv6source-verify** コマンドを使用する前に、**no** 形式の **cable nd** コマンドを使って IPv6 ND グリーニングを無効にする必要があります。

制約事項　すべてのマルチキャスト トラフィックはバンドル メンバー インターフェイスにフラッディングします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacebundle** *n* 例： `Router(config)# interface bundle 1`	ケーブル バンドル インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。*n* はバンドル インターフェイスの数を指定します。
ステップ 4	**ipv6address***ipv6-prefix*/*prefix-length* [**eui-64**] 例： `Router(config-if)# ipv6 address 2001:DB8::/32 eui-64`	インターフェイスに割り当てられている IPv6 ネットワークを指定し、インターフェイスで IPv6 処理をイネーブルにします。ipv6 address eui-64 コマンドを指定して、IPv6 アドレスの下位 64 ビットにインターフェイス識別子（ID）を持つサイトローカルおよびグローバル IPv6 アドレスを設定します。このアドレスに 64 ビット ネットワーク プレフィックスのみを指定する必要があります。下位 64 ビットはインターフェイス ID から自動的に計算されます。
ステップ 5	**ipv6address***ipv6-prefix*/*prefix-length* **link-local** 例： `Router(config-if)# ipv6 address 2001:DB8::/32 link-local`	（任意）インターフェイスに割り当てられている IPv6 アドレスを指定し、そのインターフェイスで IPv6 処理をイネーブルにします。**ipv6addresslink-local** コマンドは、（**ipv6enable** コマンドを使用して）インターフェイスで IPv6 が有効になるときに自動設定されるリンクローカル アドレスの代わりに使用されるリンクローカル アドレスをインターフェイス上に設定します。

	コマンドまたはアクション	目的
ステップ 6	**ipv6enable** 例： `Router(config-if)# ipv6 enable`	インターフェイスで IPv6 リンクローカル アドレスを自動的に設定し、インターフェイスで IPv6 処理もイネーブルにします。リンクローカル アドレスは、同じリンク上のノードとの通信にだけ使用できます。
ステップ 7	cable ipv6 source-verify 例： `Router(config-if)# cable ipv6 source-verify`	（任意）Cisco CMTS ルータのケーブル インターフェイス アップストリームで受信した MAC アドレスの MD-SID-IPv6 アドレス バインディング パケットの送信元検証を有効にします。

次の作業

- ネイバー探索機能と DHCPv6 機能など、バンドルインターフェイスでプラットフォームに依存しない任意の IPv6 機能を設定します。
- ケーブル インターフェイス上に IP プロビジョニング モードとバンドルを設定します。

ケーブル インターフェイスの IP プロビジョニング モードとバンドルの設定

CMTS ルータを使用すると、IPv4 と IPv6 の両方のアドレッシング サポート（「デュアル スタック」とも呼ばれる）、IPv4 アドレッシングのみ、または IPv6 アドレッシングのみにプロビジョニングされるケーブルモデムをサポートするケーブルインターフェイスを設定できます。ケーブルモデム登録の前に、CMTS ルータは、ケーブル モデムにサポート対象のプロビジョニング モードを MDD メッセージで送信します。

ケーブルインターフェイスでのプロビジョニング モードの設定に加えて、ケーブルインターフェイスとケーブルバンドルも関連付ける必要があります。他の IPv6 機能設定のほとんどはバンドルインターフェイスで実行します。

（注） ここでは、CMTS ルータでの IPv6 サポートの確立に関連するコマンドのみを説明します。アップストリーム機能とダウンストリーム機能の設定など、必要に応じて適用する他のケーブル インターフェイス コマンドについて説明しません。

はじめる前に

バンドル インターフェイスは設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacecable**{*slot* / *port* | *slot* / *subslot* /*port* } 例： `Router(config)# interface cable 5/0/1`	ここでケーブル インターフェイス ライン カードを指定します。 これらの引数の有効値は、CMTSルータとケーブル インターフェイス ライン カードに応じて異なります。サポート対象のスロットおよびポート番号については、ルータ シャーシとケーブル インターフェイス ライン カードのハードウエア マニュアルを参照してください。
ステップ 4	**cableip-init** {**apm** | **dual-stack** | **ipv4** | **ipv6**} 例： `Router(config-if)# cable ip-init ipv6`	ここでケーブル インターフェイスでサポートされる IP プロビジョニング モードを指定します。
ステップ 5	**cablebundle***n* 例： `Router(config)# cable bundle 1`	ケーブル インターフェイスと設定済み仮想バンドル インターフェイスを関連付けます。*n* はバンドル インターフェイスの数を指定します。

次の作業

- アップストリーム機能とダウンストリーム機能など、サポートするその他のケーブル インターフェイス機能の設定に進みます。他のケーブル インターフェイス機能の詳細については、『*Cisco IOS CMTS Cable Software Configuration Guide*』を参照してください。
- 他の IPv6 ケーブル オプション機能の設定に進みます。

IPv6 ケーブル フィルタ グループの設定

Cisco CMTS ルータは、IPv6 ケーブル フィルタ グループの機能および IPv6 フィルタリング オプションをサポートします。

IPv6 ケーブル フィルタ グループの設定

Cisco CMTS ルータは、IPv6 ケーブル フィルタ グループの機能および IPv6 フィルタリング オプションをサポートします。

ケーブル フィルタ グループと DOCSIS サブスクライバ管理 MIB

ケーブル サブスクライバ管理の仕様は DOCSIS 1.1 で、次の設定方法を使用して確立できます。

- CMTS ルータ設定（CLI 経由）
- SNMP コンフィギュレーション
- DOCSIS 1.1 コンフィギュレーション ファイル（TLV 35、36、および 37）

ここでは、IPv6 ケーブル フィルタ グループで CMTS ルータのコンフィギュレーション コマンドを使用し、DOCSIS サブスクライバ管理 MIB（DOCS-SUBMGMT-MIB）のパケット フィルタリング部分をサポートすることについて説明します。この IPv6 ケーブル フィルタ グループのサポートは、CM および CPE トラフィックの IPv6 アドレス オプションまでフィルタ分類子を拡大していますが、サービス フローとパケットの一致に使用される DOCSIS IPv6 分類子とは無関係です。

CMTS ルータで IPv6 ケーブル フィルタ グループを設定する場合は、次のガイドラインに従ってサポートされます。

- 1 つのケーブル フィルタ グループは、同じグループ ID を共有する一連の **cablefiltergroup** コマンドから成ります。
- 個別のインデックスを使用して、同じグループ ID の異なるフィルタ セットを定義できます。これを使用すると、同じフィルタ グループで IPv4 と IPv6 の両方のフィルタを定義できます。
- CM は、1 つのアップストリームと 1 つのダウンストリームのフィルタ グループに関連付けることができます。
  - アップストリーム トラフィック：CM から送信されるすべてのトラフィックは、**cablesubmgmtdefaultfilter-groupcmupstream** コマンドで設定された割り当て済みアップストリーム フィルタ グループに照らして評価されます。
  - ダウンストリーム トラフィック：CM に送信されるすべてのトラフィックは、**cablesubmgmtdefaultfilter-groupcmdownstream** コマンドで設定された割り当て済みダウンストリーム フィルタ グループに照らして評価されます。
- CPE は、1 つのアップストリームと 1 つのダウンストリームのフィルタ グループに関連付けることができます。

- アップストリーム トラフィック：CPE から送信されるすべてのトラフィックは、**cablesubmgmtdefaultfilter-groupcpeupstream** コマンドで設定された割り当て済みアップストリーム フィルタ グループに照らして評価されます。
- ダウンストリーム トラフィック：CPE に送信されるすべてのトラフィックは、**cablesubmgmtdefaultfilter-groupcpedownstream** コマンドで設定された割り当て済みダウンストリーム フィルタ グループに照らして評価されます。

（注） TLV 35、36、および 37 は DOCSIS 1.0 CM コンフィギュレーション ファイルに適用されないため、DOCSIS 1.0 CM のケーブル サブスクライバ管理を実現する唯一の方法は、Cisco CMTS ルータでそれを明示的に設定し、**cablesubmgmtdefaultactive** グローバル コンフィギュレーション コマンドを使って有効化することです。

はじめる前に

ケーブル フィルタ グループを作成してから、CM または CPE のアップストリームまたはダウンストリームに割り当てる必要があります。

制約事項

- 結合した IPv6 ヘッダーはサポートされません。
- 個別のフィルタ グループ インデックスは、IPv4 と IPv6 の両方のバージョンを同時にサポートするように設定することはできません。同じフィルタ グループで IPv4 および IPv6 フィルタをサポートする必要がある場合、同じフィルタ グループ ID を持つ別のインデックス番号を使用し、1 つのインデックスを **ip-versionipv4**、もう 1 つのインデックスを **ip-versionipv6** として設定する必要があります。
- CM トラフィックに割り当てることができるのは、アップストリームとダウンストリームのフィルタ グループをそれぞれ 1 つのみです。
- CM 内のすべての CPE が共通のフィルタ グループを共有するように、CM に追加した CPE に割り当てることができるのは、アップストリームとダウンストリームのフィルタ グループをそれぞれ 1 つのみです。
- CM で動作するフィルタ グループについては、CMTS ルータでフィルタ グループを設定してから、CM を再登録する必要があります。
- Parallel Express Forwarding（PXF）を Cisco uBR10012 ルータで設定する場合は、**cablefiltergroup** コマンドまたはインターフェイス ACL（**ipaccess-list**）コマンドのいずれかを設定できます。
- DOCSIS CM コンフィギュレーション ファイルで TLV 35、36、および 37 をプロビジョニングしない場合は、CMTS ルータで **cablesubmgmtdefaultactive** グローバル コンフィギュレーション コマンドを指定して機能を有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cablefiltergroup***group-id***index***index-num***dest-port***port-num* 例： `Router(config)# cable filter group 1 index 1 dest-port 69`	（任意）一致させる必要のある TCP/UDP 宛先ポート番号を指定します。有効な範囲は 0 ～ 65535 です。デフォルト値は、TCP/UDP のすべてのポート番号に一致します（IPv4 と IPv6 フィルタ）。
ステップ 4	**cablefiltergroup** *group-id* **index** *index-num* **ip-proto** *proto-type* 例： `Router(config)# cable filter group 1 index 1 ip-proto 17`	（任意）一致させる必要のある IP プロトコル タイプ番号を指定します。有効な範囲は 0 ～ 256 です。デフォルト値は 256 で、すべてのプロトコルに一致します（IPv4 と IPv6 フィルタ）。 一般的に使用される値は次のとおりです。
ステップ 5	**cablefiltergroup** *group-id* **index** *index-num***ip-tos** *tos-mask tos-value* 例： `Router(config)# cable filter group 1 index 1 ip-tos 0xff 0x80`	（任意）一致させる ToS マスクと値を指定します（IPv4 と IPv6 フィルタ）。 *tos-mask* は、*tos-value* と論理的に AND 結合され、*tos-mask* とパケットの実際の ToS 値の AND 演算結果と比較されます。2 つの値が同じ場合、フィルタはこれらが一致していると見なします。 両方のパラメータのデフォルト値はすべての ToS 値と一致します。

	コマンドまたはアクション	目的
ステップ 6	**cablefiltergroup** *group-id* **index** *index-num* **ip-versionipv6** 例： `Router(config)# cable filter group 1 index 1 ip-version ipv6`	このフィルタ グループが IPv6 フィルタ グループであることを指定します。
ステップ 7	**cablefiltergroup** *group-id* **index** *index-num***match-action** {**accept**| **drop**} 例： `Router(config)# cable filter group 1 index 1 match-action drop`	（オプション）このフィルタに一致するパケットに対して行うアクションを指定します（IPv4 および IPv6）。
ステップ 8	**cablefiltergroup** *group-id* **index** *index-num***src-port***port-num* 例： `Router(config)# cable filter group 1 index 1 src-port 50`	（任意）一致させる必要のある TCP/UDP 送信元ポート番号を指定します。有効な範囲は 0 ～ 65535 です。デフォルト値は、TCP/UDP のすべてのポート番号に一致します（IPv4 と IPv6 フィルタ）。
ステップ 9	**cablefiltergroup** *group-id* **index** *index-num***status** {**active**| **inactive**} 例： `Router(config)# cable filter group 1 index 1 status inactive`	（任意）フィルタを有効/無効にします（IPv4 と IPv6 フィルタ）。 （注） このコマンドを使用してフィルタを有効または無効にするには、他のオプションを 1 つ以上使用してフィルタ グループを作成する必要があります。
ステップ 10	**cablefiltergroup** *group-id* **index** *index-num***tcp-flags***flags-mask flags-value* 例： `Router(config)# cable filter group 1 index 1 tcp-flags 0 0`	（オプション）一致させる TCP フラグのマスクと値を指定します（IPv4 および IPv6）。
ステップ 11	**cablefiltergroup** *group-id* **index** *index-num***v6-dest-address***ipv6-address* 例： `Router(config)# cable filter group 1 index 1 v6-dest-address 2001:DB8::/32`	（オプション）一致する必要がある IPv6 宛先アドレスを、X:X:X:X::X の形式で指定します（IPv6 フィルタのみ）。

	コマンドまたはアクション	目的
ステップ 12	**cablefiltergroup** *group-id* **index** *index-num***v6-dest-pfxlen***prefix-length* 例： `Router(config)# cable filter group 1 index 1 v6-dest-pfxlen 64`	（任意）IPv6 宛先アドレスのネットワーク部分の長さを指定します。有効な範囲は 0 ～ 128 です。
ステップ 13	**cablefiltergroup** *group-id* **index** *index-num***v6-src-address***ipv6-address* 例： `Router(config)# cable filter group 1 index 1 v6-src-address 2001:DB8::/32`	（オプション）一致する必要がある IPv6 発信元アドレスを、X:X:X:X::X の形式で指定します（IPv6 フィルタのみ）。
ステップ 14	**cablefiltergroup** *group-id* **index** *index-num***v6-src-pfxlen***prefix-length* 例： `Router(config)# cable filter group 1 index 1 v6-src-pfxlen 48`	（任意）IPv6 送信元アドレスのネットワーク部分の長さを指定します。有効な範囲は 0 ～ 128（IPv6 フィルタのみ）です。
ステップ 15	**cablesubmgmtdefaultfilter-group** {**cm**| **cpe**} {**downstream**| **upstream**} *group-id* 例： `Router(config)# cable submgmt default filter-group cm upstream 1`	ダウンストリームまたはアップストリームのトラフィックについて、CM またはその CPE デバイスに定義したフィルタ グループを（*group-id* を指定して）適用します。
ステップ 16	**cablesubmgmtdefaultactive** 例： `Router(config)# cable submgmt default active`	（DOCSIS 1.1 CM コンフィギュレーション ファイルで TLV 35、36、および 37 をプロビジョニングしていない場合は必須） フィルタを有効にして、特定の CM の CPE デバイスを管理します（docsSubMgtCpeActiveDefault 属性を TRUE に設定）。

次の例では、ID 254 とインデックス番号 128 の IPv6 フィルタ グループを作成する方法について説明します。IPv6 フィルタ グループを作成するにはキーワード **ip-versionipv6** を設定する必要があります。設定しない場合、デフォルトで IPv4 フィルタ グループが作成されます。

```
configure terminal
cable filter group 254
 index 128 v6-src-address 2001:DB8::/32
cable filter group 254
 index 128 v6-src-pfxlen 48
```

```
cable filter group 254
 index 128 v6-dest-address 2001:DB8::/32
cable filter group 254
 index 128 v6-dest-pfxlen 64
cable filter group 254
 index 128 ip-version ipv6
cable filter group 254
 index 128 match-action drop
cable submgmt default filter-group cm upstream 254
```

このグループは CM アップストリーム トラフィックをフィルタリングし、IPv6 アドレス 2001:DB8::/32（ネットワーク プレフィックス 128）宛ての IPv6 送信元アドレス 2001:33::20B:BFFF:FEA9:741F（ネットワーク プレフィックス 128）を持つパケットをドロップします。

すべての **cablefiltergroup** コマンドは、グループ ID 254（およびインデックス 128）で関連付けられます。**cablesubmgmtdefaultfilter-group** コマンドは、対応するフィルタ グループ ID 254 を CM アップストリーム トラフィックに適用します。

ケーブル フィルタ グループ設定をモニタするには、次の例に示す形式の **showcablefilter** コマンドを使用します。これらの出力例では、コマンド **showcablefilter**、**showcablefiltergroup254**、および **showcablefiltergroup254index128** からのすべての出力で同じ情報が表示されます。これは、現在、1 つのフィルタ グループとインデックスだけが定義されているためです。

（注） SrcAddr/mask フィールドと DestAddr/Mask フィールドの出力領域に文字列「Use Verbose」が表示されます。これは、**showcablefiltergroupverbose** 形式のコマンドを使って IPv6 アドレス全体を表示するように提案しています。

```
Router# show cable filter
Filter    SrcAddr/Mask       DestAddr/Mask      Prot ToS  SPort DPort TCP   Action Status
Grp Id v6                                                              Flags
254 128Y  Use Verbose
        Use Verbose
                                  drop   active
Router# show cable filter group 254
Filter    SrcAddr/Mask       DestAddr/Mask      Prot ToS  SPort DPort TCP   Action Status
Grp Id v6                                                              Flags
254 128Y  Use Verbose        Use Verbose                                     drop   active
Router# show cable filter group 254 index 128
Filter    SrcAddr/Mask       DestAddr/Mask      Prot ToS  SPort DPort TCP   Action Status
Grp Id v6                                                              Flags
254 128Y  Use Verbose        Use Verbose                                     drop   active
Router# show cable filter group 254 index 128 verbose
Filter Group                          : 254
Filter Index                          : 128
Filter Version                        : IPv6
Matches                               : 0
    Source IPv6 address               : 2001:DB8::/32
    Destination IPv6 address          : 2001:DB8::/32
    Match action                      : drop
    Status                            : active
```

トラブルシューティングのヒント

cable filter group コマンドを設定してから、**cable submgmt default filter-group** コマンドを使用してフィルタ グループを適用してください。これをしないと、次のメッセージが表示され、未定義のフィルタ グループへのアソシエーションが実行されます。

```
Router(config)# cable submgmt default filter-group cm upstream 100
Default value set to a nonexistent filter-group 100.
```

IPv6 ドメイン名サービス

Cisco CMTS ルータ上で IPv6 アドレッシングを使用するデバイスに対するドメイン ネーム サービス（DNS）機能が、Cisco IOS リリースでサポートされています。

DNS は、ホスト名としばしば複雑になる 128 ビット IPv6 アドレスを組み合わせたものを関連付けることで、ケーブルデバイスの識別を簡単にします。ホスト名の使用をサポートする CMTS ルータ CLI 内の IPv6 アドレスの代わりに、ホスト名を使用できます。

CMTS ルータには 2 つの独立した DNS キャッシュがあります。IOS DNS キャッシュ、および CM と CPE の CMTS ルータで学習した IPv6 アドレスを保存するケーブル固有の DNS キャッシュです。

ケーブルの IPv6 DNS サービスのこの段階で、**showcablemodemdomain-name** コマンドの使用時に必要なドメイン名情報について DNS サーバに照会します。このコマンドを使用する場合、次のアクションが実行されます。

1. CMTS ルータは、CM がオンラインであるかを確認します。CM がオンラインになると、CMTS ルータは、CM に割り当てられた対応する IPv6 アドレスを使用し、IOS DNS キャッシュでそのドメイン名を検索します。
2. 何も一致しない場合は、CMTS ルータが CM の IPv6 アドレスを持つ DNS クエリ メッセージを DNS サーバに送信し、ドメイン名を解決しようとします。
3. DNS 応答を受信すると、CMTS ルータは、各 IPv6 アドレスの IOS DNS キャッシュにドメイン名を保存します。
4. また、CMTS ルータは、ケーブル固有の DNS キャッシュに DNS サーバで応答する完全修飾ドメイン名（FQDN）を保存します。

（注） **no ip domain lookup** コマンドを実行すると、DNS 解決が無効になります。

ケーブルに IPv6 DNS の CMTS ルータでホスト名を使用する場合、次のプラットフォーム非依存 Cisco IOS-xe ソフトウェア コマンドがサポートされます。

- **connect**
- **pingipv6**
- **showhosts**
- **telnet**
- **traceroute**

はじめる前に

- DNS サーバを設定する必要があります。
- ホスト名を特定して、IPv6 アドレスに割り当てる必要があります。Cisco DNS サーバを使用している場合は、**iphost** グローバル コンフィギュレーション コマンドを使用してホスト名を IP アドレスにマッピングします。
- サポート対象のコマンドで DNS ホスト名（またはドメイン）が利用可能になる前に、**ipname-server** グローバル コンフィギュレーション コマンドを使用して DNS サーバを設定する必要があります。
- ケーブル コマンドの一部としてドメイン名を使用するには、その前に、CMTS ルータのルート プロセッサ（RP）で **showcablemodemdomain-name** コマンドを実行する必要があります。

制約事項

- IPv4 アドレッシングを使用するケーブル デバイスの DNS はサポートされません。
- コマンドライン インターフェイス（CLI）内の列のサイズが制限されているため、ドメイン名の表示も 32 文字に制限されています。そのため、CMTS ルータのコマンド出力結果には、ドメイン名全体は常に表示されません。
- DHCPv6 または IPv6（ND）プロセスを経由した IPv6 アドレスの取得など、IPv6 アドレス ラーニングが行われるケーブル デバイスのみがサポートされます。
- ケーブル固有の DNS キャッシュは、ルート プロセッサ（RP）で **showcablemodemdomain-name** コマンドを使用した場合にのみ更新されます。DNS クエリはこのコマンドを使用して RP でのみ送信されるため、ライン カード コンソールで **showcablemodemdomain-name** コマンドを使用しても、DNS キャッシュは更新できません。出力は RP のみで表示されます。
- ケーブル固有の DNS キャッシュでは、FQDN のみが保存され、一部が修飾されたドメイン名は保存されません。
- ケーブル固有の DNS キャッシュは、IOS DNS キャッシュに適用するタイムアウトには関連付けられていません。そのため、そのデバイスで IOS DNS キャッシュ タイムアウトが発生しても、ケーブル固有の DNS キャッシュ エントリは削除されません。ケーブル固有の DNS キャッシュは、**showcablemodemdomain-name** コマンドを使用した場合にのみ更新されます。
- CMTS ルータは、ケーブル固有の DNS キャッシュ内の IPv6 アドレスごとにドメイン名を 1 つのみ保存できるようにサポートします。
- リンク ローカル アドレスのドメイン名はサポートされていません。
- **noipdomain-name** コマンドは、DNS ルックアップを無効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**ipname-server** [**vrf** *vrf-name*] *server-address1* [*server-address2...server-address6*] 例： `Router(config)# ip name-server 2001:DB8::/32`	名前とアドレスの解決に使用する 1 つまたは複数のネーム サーバのアドレスを指定します。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 5	**showcablemodemdomain-name** 例： `Router# show cable modem domain-name`	ケーブル固有の DNS キャッシュが更新され、CM 内のすべての CM と CPE デバイスのドメイン名が表示されます。

IPv6 ソース検証の設定

通常、IPv6 ソース検証機能はケーブル バンドル インターフェイスで有効になっています。そこから、設定を取得するためにケーブル インターフェイスが仮想バンドル インターフェイスに関連付けられます。

ケーブル ライン カード インターフェイスで IPv6 ソース検証を有効にすると、ソース検証ルーチンはパケットの MAC アドレス MD SID IP バインディングを確認します。送信元検証が成功すると、パケットが転送されます。この検証に失敗すると、パケットはドロップされます。

CM がブリッジ モデム デバイスとして動作しているときは、CMTS ルータはその CM に関連するすべての IPv6 アドレス、およびその CM の背後にある CPE を確認します。

cableipv6source-verify コマンドは、IPv6 パケットのソース検証のみを制御します。IPv4 ベースのソース検証では、**cablesource-verify** コマンドを使用します。このコマンドも、さまざまなオプションをサポートします。

バンドルインターフェイスでのIPv6ソース検証の構成方法の詳細については、ケーブル仮想バンドル インターフェイスの設定, （834 ページ）を参照してください。

制限事項

IPv6パケットのソース検証は、ルートプロセッサ（RP）のプロセススイッチングされたパケットのみで発生します。

IPv6 VPN over MPLS の設定

Cisco CMTS ルータは、IPv6 VPN over MPLS（6VPE）機能をサポートします。この機能の実装には、次の設定タスクが含まれます。

- IPv6 の VRF インスタンスの構成
- インターフェイスへの VRF のバインド
- サブインターフェイスの作成
- PE から CE へのルーティング用のスタティック ルートの設定
- eBGP の PE から CE へのルーティング セッションの設定
- iBGP 用の IPv6 VPN アドレス ファミリの設定
- スケーラビリティ向上のためのルート リフレクタの設定
- インターネット アクセスの設定

設定例の詳細については、IPv6 対応ケーブルの設定例, （851 ページ）を参照してください。

（注） （CM の接続先である）サブバンドル インターフェイスの IPv6 アドレスは、CPE DHCPv6 要求の DHCPv6 リレー パケットで使用します。DHCPv6 パケットが VRF インターフェイス間を移動する必要がある場合、接続を確立するために各 VRF インターフェイスの IPv6 アドレスが Cisco CMTS 上で構成される必要があります。

DHCPv6 リレー エージェントの設定

Cisco CMTS ルータでは、特定の送信元アドレスからクライアント リレー宛先にリレー転送メッセージを転送する DHCPv6 リレー エージェントをサポートします。

DHCPv6 リレー エージェント機能をイネーブルにし、インターフェイス上でリレー宛先アドレスを指定するには、次の作業を実行します。

はじめる前に

リレー転送メッセージには、特定の送信元 IPv6 アドレスを含める必要があります。Cisco CMTS DHCPv6 リレー エージェントと DHCPv6 サーバの間で導入されたファイアウォールが、1 つの

Cisco CMTS バンドル インターフェイスに設定される送信元アドレスは 1 つのみだと考えているため、これが必要になります。

制約事項

ipv6dhcprelaydestination コマンドの 1 つ以上のパラメータを変更する場合、**no** 形式を使ってコマンドを無効にする必要があります。その後、変更したパラメータを使ってコマンドを再び実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacetype** *number* 例： `Router(config)# interface ethernet 4/2`	インターフェイスのタイプと番号を指定し、ルータをインターフェイス コンフィギュレーション モードにします。
ステップ 4	**ipv6dhcprelaydestination** *ipv6-address*[*interface*] [**link-address** *link-address*] [**source-address** *source-address*] 例： `Router(config-if) ipv6 dhcp relay destination 2001:db8:1234::1 ethernet 4/2 link-address 2001:db8::1 source-address 2001:db8::2`	クライアント パケットを転送する宛先アドレスを指定し、インターフェイスに対して DHCPv6 リレー サービスをイネーブルにします。
ステップ 5	**end** 例： `Router(config-if) end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

構成可能な DOCSIS CMTS 機能の DHCPv6 フィールド

DOCSIS 3.1 仕様では、CMTS が DOCSIS 3.0 のケーブル モデムと機能をサポートする必要があります。DOCSIS バージョンの後方互換性をサポートするには、DHCPv6 ベンダー オプションを 30 から 31 に変更する必要があります。

現在、**cable docsis-ver [major version | minor version]** コマンドを使用して、任意の DOCSIS バージョンにアップグレードできるようになりました。

このコマンドのデフォルト値は **cable docsis-ver 3 1** です。

IPv6 ND グリーニングの設定

DHCPv6 リースクエリを使用して IPv6 送信元検証を設定する前に、IPv6 ND グリーニングをディセーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacebundle** *bundle-no* 例： `Router(config)# interface bundle 1`	バンドルインターフェイス番号を指定し、バンドル インターフェイス コンフィギュレーション モードを開始します。 • *bundle-no*：バンドル インターフェイス番号。有効な範囲は 1 ～ 255 です。
ステップ 4	**nocablend** 例： `Router(config-if) no cable nd`	Cisco CMTS ルータで IPv6 ND グリーニングをディセーブルにします。
ステップ 5	**end** 例： `Router(config-if) end`	特権 EXEC モードに戻ります。

IPv6 デュアル スタック CPE サポートの設定

ここでは、**show** コマンドを使用して、CMTS 機能での IPv6 デュアル スタック CPE サポートの設定を確認する方法を説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

ステップ 2	**showcablemodem**[*ip-address* | *mac-address*] **ipv6**[**cpe** | **prefix** | **registered**|**unregistered]**
	
	例：
	
	`Router# show cable modem ipv6 registered`
	
	例：
	
	`Router# show cable modem 0019.474a.c14a ipv6 cpe`
		Cisco CMTS ルータの CM 内で指定した CM と CPE に関する IPv6 情報を表示します。次のオプションを指定できます。

ステップ 3	**showcablemodem**[ip-address | mac-address] **registered** 例： `Router# show cable modem 0019.474e.e4DF registered`	Cisco CMTS に登録された CM のリストを表示します。次のオプションを指定できます。
ステップ 4	**showcablemodem** {ip-address | mac-address} **cpe** 例： `Router# show cable modem 0019.474a.c14a cpe`	特定の CM を介してケーブル インターフェイスにアクセスする CPE デバイスを表示します。次のオプションを指定できます。

例

showcablemodemipv6 コマンドを使用してデュアル スタック CPE の IPv6 部分を表示し、**showcablemodemcpe** コマンドを使用してデュアル スタック CPE の IPv4 モードを表示します。

showcablemodemipv6registered コマンドと **showcablemodemregistered** コマンドはどちらも、デュアル スタック CPE に関して CPE カウントを 1 と表示します。

次に、**showcablemodemipv6** コマンドの出力例を示します。

```
Router# show cable modem ipv6 registered
Interface   Prim Online       CPE IP Address                                MAC Address
            Sid  State
C4/0/U2     1    online       0   ---                                       0019.474a.c18c
C4/0/U2     3    online(pt)   1   2001:420:3800:809:EDA4:350C:2F75:4779   0019.474a.c14a
Router# show cable modem 0019.474a.c14a ipv6 cpe
MAC Address    IP Address                          Domain Name
0005.0052.2c1d 2001:420:3800:809:48F7:3C33:B774:9185
```

次に、**showcablemodemipv6** コマンドの出力例を示します。

```
Router# show cable modem
 0023.bed9.4c8e ipv6 cpe
Load for five secs: 0%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *06:37:20.439 UTC Thu Aug 2 2012
MAC Address    IP Address
0023.bed9.4c91 2001:40:3:4:200:5EB7:BB6:C759
2001:40:3:4:210:D73B:7A50:2D05
```

次に、**showcablemodemregistered** コマンドの出力例を示します。

```
Router# show cable modem registered
Interface   Prim Online      Timing Rec   QoS CPE IP address      MAC address
            Sid  State       Offset Power
C4/0/U2     3    online      1022   0.00  2   1   50.3.37.12      0019.474a.c14a
```

次に、**showcablemodemcpe** コマンドの出力例を示します。

```
Router# show cable modem 0019.474a.c14a cpe

IP address        MAC address      Dual IP
 50.3.37.3 0005.0052.2c1d Y
```

IPv6 対応ケーブルの設定例

ここでは、次の設定例について説明します。

例：サブインターフェイス経由の IPv6

次に、サブインターフェイスで使用できる CMTS バンドル コンフィギュレーションの例を示します。

```
Router# show cable modem ipv6
Device Type: B - CM Bridge, R - CM Router
IP Assignment Method: D - DHCP
MAC Address    Type Interface    Mac State    D/IP IP Address
0019.474a.c18c B/D  C4/0/U2      online        Y  2001:420:3800:809:4C7A:D518:91
C6:8A18
Router# show run interface bundle2
Building configuration...
Current configuration : 138 bytes
!
interface Bundle2
 no ip address
 cable arp filter request-send 3 2
 cable arp filter reply-accept 3 2
 no cable ip-multicast-echo
end
```

```
Router#

show run interface bundle2.1
Building configuration...
Current configuration : 382 bytes
!
interface Bundle2.1
 ip address 50.3.37.1 255.255.255.0
 no cable ip-multicast-echo
 cable helper-address 10.10.0.12
 ipv6 address 2001:DB8::/32
 ipv6 enable
 ipv6 nd prefix default no-advertise
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 nd ra interval msec 2000
 ipv6 dhcp relay destination 2001:420:3800:800:203:BAFF:FE11:B644
 arp timeout 240
end
```

例：基本的な IPv6 ケーブル フィルタ グループ

次に、ケーブル ルータ内の特定の IPv6 ホスト（発信元アドレス 2001:DB8::1/48）のトラフィックをネットワーク上の IPv6 ホスト（宛先アドレス 2001:DB8::5/64）にドロップする IPv6 フィルタ グループの設定例を示します。

```
configure terminal
!
! Specify the filter group criteria using a common group ID
!
cable filter group 254 index 128 v6-src-address 2001:DB8::1
cable filter group 254 index 128 v6-src-pfxlen 128
cable filter group 254 index 128 v6-dest-address 2001:DB8::5
cable filter group 254 index 128 v6-dest-pfxlen 128
!
! Specify that the filter group is IP version 6
!
cable filter group 254 index 128 ip-version ipv6
!
! Specify the drop action for matching packets
!
cable filter group 254 index 128 match-action drop
!
! Apply the filter group with ID 254 to all CM upstream traffic
!
cable submgmt default filter-group cm upstream 254
```

例：IPv6 を使用した完全なケーブル構成

次に、ケーブルの完全な構成例を示します。IPv4 と IPv6 の両方と、フィルタ定義と同一の ID を関連付ける個別のインデックスを使用して、複数のケーブル フィルタ グループの設定も表示します。

```
Router# show running-config
Building configuration...
Current configuration : 15010 bytes
!
! Last configuration change at 08:32:14 PST Thu Nov 8 2007
!
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
```

```
no service password-encryption
service internal
service compress-config
!
hostname router
!
boot-start-marker
boot-end-marker
!
enable password password1
!
no aaa new-model
clock timezone PST -9
clock summer-time PDT recurring
clock calendar-valid
facility-alarm core-temperature major 53
facility-alarm core-temperature minor 45
facility-alarm core-temperature critical 85
facility-alarm intake-temperature major 49
facility-alarm intake-temperature minor 40
facility-alarm intake-temperature critical 67
!
!
card 1/0 2jacket-1
card 1/0/0 24rfchannel-spa-1
card 5/0 5cable-mc520h-d
cable admission-control preempt priority-voice
cable modem vendor 00.18.68 SA-DPC2203
cable modem vendor 00.19.47 SA-DPC2505
no cable qos permission create
no cable qos permission update
cable qos permission modems
!
cable filter group 1 index 1 src-ip 0.0.0.0
cable filter group 1 index 1 src-mask 0.0.0.0
cable filter group 1 index 1 dest-ip 0.0.0.0
cable filter group 1 index 1 dest-mask 0.0.0.0
cable filter group 2 index 1 src-ip 0.0.0.0
cable filter group 2 index 1 src-mask 0.0.0.0
cable filter group 2 index 1 dest-ip 0.0.0.0
cable filter group 2 index 1 dest-mask 0.0.0.0
cable filter group 3 index 1 src-ip 0.0.0.0
cable filter group 3 index 1 src-mask 0.0.0.0
cable filter group 3 index 1 dest-ip 0.0.0.0
cable filter group 3 index 1 dest-mask 0.0.0.0
cable filter group 4 index 1 src-ip 0.0.0.0
cable filter group 4 index 1 src-mask 0.0.0.0
cable filter group 4 index 1 dest-ip 0.0.0.0
cable filter group 4 index 1 dest-mask 0.0.0.0
cable filter group 5 index 1 src-ip 0.0.0.0
cable filter group 5 index 1 src-mask 0.0.0.0
cable filter group 5 index 1 dest-ip 0.0.0.0
cable filter group 5 index 1 dest-mask 0.0.0.0
cable filter group 6 index 1 src-ip 0.0.0.0
cable filter group 6 index 1 src-mask 0.0.0.0
cable filter group 6 index 1 dest-ip 0.0.0.0
cable filter group 6 index 1 dest-mask 0.0.0.0
cable filter group 7 index 1 src-ip 0.0.0.0
cable filter group 7 index 1 src-mask 0.0.0.0
cable filter group 7 index 1 dest-ip 0.0.0.0
cable filter group 7 index 1 dest-mask 0.0.0.0
cable filter group 8 index 1 src-ip 0.0.0.0
cable filter group 8 index 1 src-mask 0.0.0.0
cable filter group 8 index 1 dest-ip 0.0.0.0
cable filter group 8 index 1 dest-mask 0.0.0.0
cable filter group 9 index 1 src-ip 0.0.0.0
cable filter group 9 index 1 src-mask 0.0.0.0
cable filter group 9 index 1 dest-ip 0.0.0.0
cable filter group 9 index 1 dest-mask 0.0.0.0
cable filter group 10 index 1 src-ip 0.0.0.0
cable filter group 10 index 1 src-mask 0.0.0.0
cable filter group 10 index 1 dest-ip 0.0.0.0
cable filter group 10 index 1 dest-mask 0.0.0.0
```

```
cable filter group 12 index 1 src-ip 0.0.0.0
cable filter group 12 index 1 src-mask 0.0.0.0
cable filter group 12 index 1 dest-ip 0.0.0.0
cable filter group 12 index 1 dest-mask 0.0.0.0
cable filter group 16 index 1 src-ip 0.0.0.0
cable filter group 16 index 1 src-mask 0.0.0.0
cable filter group 16 index 1 dest-ip 0.0.0.0
cable filter group 16 index 1 dest-mask 0.0.0.0
ip subnet-zero
ip domain name cisco.com
ip host host1 239.192.254.254
ip host host2 239.192.254.253
ip name-server 10.39.26.7
ip name-server 2001:0DB8:4321:FFFF:0:800:20CA:D8BA
!
!
!
!
ipv6 unicast-routing
ipv6 cef
packetcable multimedia
packetcable
!
!
!
redundancy
 mode sso
!
!
controller Modular-Cable 1/0/0
 annex B modulation 64qam 0 23
 ip-address 10.30.4.175
 modular-host subslot 5/0
 rf-channel 0 cable downstream channel-id 24
 rf-channel 1 cable downstream channel-id 25
 rf-channel 2 cable downstream channel-id 26
 rf-channel 3 cable downstream channel-id 27
 rf-channel 4 cable downstream channel-id 28
 rf-channel 5 cable downstream channel-id 29
 rf-channel 6 cable downstream channel-id 30
 rf-channel 7 cable downstream channel-id 31
 rf-channel 8 cable downstream channel-id 32
 rf-channel 9 cable downstream channel-id 33
 rf-channel 10 cable downstream channel-id 34
 rf-channel 11 cable downstream channel-id 35
 rf-channel 12 cable downstream channel-id 36
 rf-channel 13 cable downstream channel-id 37
 rf-channel 14 cable downstream channel-id 38
 rf-channel 15 cable downstream channel-id 39
 rf-channel 16 cable downstream channel-id 40
 rf-channel 17 cable downstream channel-id 41
 rf-channel 18 cable downstream channel-id 42
 rf-channel 19 cable downstream channel-id 43
 rf-channel 20 cable downstream channel-id 44
 rf-channel 21 cable downstream channel-id 45
 rf-channel 22 cable downstream channel-id 46
 rf-channel 23 cable downstream channel-id 47
!
!
policy-map foo
policy-map 1
policy-map cos
policy-map qpolicy
policy-map shape
policy-map dscp
!
!
!
!
!
!
interface Loopback0
 ip address 127.0.0.1 255.255.255.255
```

```
!
interface FastEthernet0/0/0
 ip address 10.39.21.10 255.255.0.0
 speed 100
 half-duplex
 ipv6 address 2001:DB8::/32
 ipv6 enable
!
interface Wideband-Cable1/0/0:0
 no cable packet-cache
 cable bonding-group-id 1
!
interface Wideband-Cable1/0/0:1
 no cable packet-cache
 cable bonding-group-id 2
!
interface Wideband-Cable1/0/0:2
 no cable packet-cache
 cable bonding-group-id 3
!
interface Wideband-Cable1/0/0:3
 no cable packet-cache
 cable bonding-group-id 4
!
interface Wideband-Cable1/0/0:4
 no cable packet-cache
 cable bundle 1
 cable bonding-group-id 5
 cable rf-channel 1 bandwidth-percent 60
!
interface Wideband-Cable1/0/0:5
 no cable packet-cache
 cable bundle 1
 cable bonding-group-id 6
 cable rf-channel 0 bandwidth-percent 40
 cable rf-channel 2
 cable rf-channel 3
!
interface Wideband-Cable1/0/0:6
 no cable packet-cache
 cable bonding-group-id 7
!
interface Wideband-Cable1/0/0:7
 no cable packet-cache
 cable bonding-group-id 8
!
interface Wideband-Cable1/0/0:8
 no cable packet-cache
 cable bonding-group-id 9
!
interface Wideband-Cable1/0/0:9
 no cable packet-cache
 cable bonding-group-id 33
!
interface Wideband-Cable1/0/0:10
 no cable packet-cache
 cable bonding-group-id 34
!
interface Wideband-Cable1/0/0:11
 no cable packet-cache
 cable bonding-group-id 35
!
interface Cable5/0/0
 no cable packet-cache
 cable bundle 1
 cable downstream channel-id 119
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream frequency 99000000
 no cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 0
```

```
 cable upstream 0 frequency 6000000
 cable upstream 0 ingress-noise-cancellation 200
 cable upstream 0 docsis-mode tdma
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 no cable upstream 0 shutdown
 cable upstream 1 connector 1
 cable upstream 1 ingress-noise-cancellation 200
 cable upstream 1 docsis-mode tdma
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 2
 cable upstream 2 ingress-noise-cancellation 200
 cable upstream 2 docsis-mode tdma
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 3
 cable upstream 3 ingress-noise-cancellation 200
 cable upstream 3 docsis-mode tdma
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
!
interface Cable5/0/1
 cable ip-init ipv6
 no cable packet-cache
 cable bundle 1
 cable downstream channel-id 120
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 705000000
 no cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 4
 cable upstream 0 frequency 6000000
 cable upstream 0 ingress-noise-cancellation 200
 cable upstream 0 docsis-mode tdma
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 no cable upstream 0 shutdown
 cable upstream 1 connector 5
 cable upstream 1 ingress-noise-cancellation 200
 cable upstream 1 docsis-mode tdma
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 6
 cable upstream 2 ingress-noise-cancellation 200
 cable upstream 2 docsis-mode tdma
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 7
 cable upstream 3 ingress-noise-cancellation 200
 cable upstream 3 docsis-mode tdma
 cable upstream 3 channel-width 1600000 1600000
```

```
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
!
interface Cable5/0/2
 no cable packet-cache
 cable downstream channel-id 121
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 8
 cable upstream 0 ingress-noise-cancellation 200
 cable upstream 0 docsis-mode tdma
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 cable upstream 0 shutdown
 cable upstream 1 connector 9
 cable upstream 1 ingress-noise-cancellation 200
 cable upstream 1 docsis-mode tdma
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 10
 cable upstream 2 ingress-noise-cancellation 200
 cable upstream 2 docsis-mode tdma
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 11
 cable upstream 3 ingress-noise-cancellation 200
 cable upstream 3 docsis-mode tdma
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
!
interface Cable5/0/3
 no cable packet-cache
 cable downstream channel-id 122
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 12
 cable upstream 0 ingress-noise-cancellation 200
 cable upstream 0 docsis-mode tdma
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 cable upstream 0 shutdown
 cable upstream 1 connector 13
 cable upstream 1 ingress-noise-cancellation 200
 cable upstream 1 docsis-mode tdma
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 14
 cable upstream 2 ingress-noise-cancellation 200
 cable upstream 2 docsis-mode tdma
```

```
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 15
 cable upstream 3 ingress-noise-cancellation 200
 cable upstream 3 docsis-mode tdma
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
!
interface Cable5/0/4
 no cable packet-cache
 cable downstream channel-id 123
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream rf-shutdown
 cable upstream max-ports 4
 cable upstream 0 connector 16
 cable upstream 0 ingress-noise-cancellation 200
 cable upstream 0 docsis-mode tdma
 cable upstream 0 channel-width 1600000 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 modulation-profile 21
 cable upstream 0 shutdown
 cable upstream 1 connector 17
 cable upstream 1 ingress-noise-cancellation 200
 cable upstream 1 docsis-mode tdma
 cable upstream 1 channel-width 1600000 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 range-backoff 3 6
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 18
 cable upstream 2 ingress-noise-cancellation 200
 cable upstream 2 docsis-mode tdma
 cable upstream 2 channel-width 1600000 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 range-backoff 3 6
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 19
 cable upstream 3 ingress-noise-cancellation 200
 cable upstream 3 docsis-mode tdma
 cable upstream 3 channel-width 1600000 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 range-backoff 3 6
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
!
interface Bundle1
 ip address 10.46.2.1 255.255.0.0 secondary
 ip address 10.46.1.1 255.255.0.0
 cable arp filter request-send 3 2
 cable arp filter reply-accept 3 2
 cable dhcp-giaddr policy strict
 cable helper-address 10.39.26.8
 ipv6 address 2001:DB8::/32
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 nd ra interval 5
 ipv6 dhcp relay destination 2001:0DB8:4321:FFFF:0:800:20CA:D8BA
!
ip default-gateway 10.39.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 10.39.26.12
ip route 192.168.254.253 255.255.255.255 10.39.0.1
```

```
ip route 192.168.254.254 255.255.255.255 10.39.0.1
!
!
no ip http server
no ip http secure-server
!
logging cmts cr10k log-level errors
cpd cr-id 1
nls resp-timeout 1
cdp run
!
tftp-server bootflash:docs10.cm alias docs10.cm
tftp-server bootflash:rfsw_x373.bin alias rfsw_x373.bin
snmp-server community private RW
snmp-server enable traps cable
snmp-server manager
!
!
control-plane
!
!
line con 0
 logging synchronous
 stopbits 1
line aux 0
line vty 0 4
 password lab
 login
!
!
cable fiber-node 1
  downstream Modular-Cable 1/0/0 rf-channel 1
  upstream Cable 5/0 connector 0
!
cable fiber-node 2
  downstream Modular-Cable 1/0/0 rf-channel 0 2-3
  upstream Cable 5/0 connector 4
!
end
```

例：6VPE の BGP 設定

次に、CMTS 6VPE の BGP 設定の例を示します。

```
Router# router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 11.1.1.5 remote-as 1
 neighbor 11.1.1.5 update-source Loopback1
 no auto-summary
 !
 address-family vpnv6              --- Enable vpnv6 AF
  neighbor 11.1.1.5 activate      --- Activate neighbor 6VPE-2
  neighbor 11.1.1.5 send-community extended
 exit-address-family
 !
 address-family ipv6 vrf vrf_mgmt
  redistribute connected            ---- Publish directly connected route
  redistribute static
  no synchronization
 exit-address-family
!
 address-family ipv6 vrf vrfa   --- Enable IPv6 vrf AF for each VRF
  redistribute connected
  no synchronization
 exit-address-family
 !
 address-family ipv6 vrf vrfb --- Enable IPv6 vrf AF for each VRF
  redistribute connected
```

```
  no synchronization
 exit-address-family
!
```

例：6VPE のサブインターフェイス設定

次の例では、仮想バンドル インターフェイス 1 のサブインターフェイスを定義する方法について説明します。

IPv6 VPN を設定する場合、管理 VRF の一部として作成された最初のサブインターフェイスを設定する必要があります。次の例では、バンドル 1.10 が最初のサブインターフェイスで、管理 VRF に設定されています。CNR サーバが管理 VRF にアクセス可能であることを確認します。

```
interface Bundle1.10                --- Management VRF
 vrf forwarding vrf_mgmt
 cable dhcp-giaddr primary
 ipv6 address 2001:40:3:110::1/64
 ipv6 enable
 ipv6 nd managed-config-flag
 ipv6 nd other-config-flag
 ipv6 dhcp relay destination 2001:10:74:129::2
interface Bundle1.11          --- VRF A
 vrf forwarding vrfa
 cable dhcp-giaddr primary
 ipv6 address 2001:40:3:111::1/64
 ipv6 enable
 ipv6 dhcp relay destination 2001:10:74:129::2
interface Bundle1.12          --- VRFB
 vrf forwarding vrfb
 cable dhcp-giaddr primary
 ipv6 address 2001:40:3:112::1/64
 ipv6 enable
 ipv6 dhcp relay destination 2001:10:74:129::2
```

例：ケーブル インターフェイスのバンドル

次に、物理インターフェイスのグループのバンドルの方法例を示します。

```
int C5/0/4 and int c5/0/3 are bundled.
int c5/0/4
cable bundle 1
int c5/0/3
cable bundle 1
```

例：6VPE の VRF 設定

次の例では、各 VPN の VRF を作成する方法を示します。

```
vrf definition vrf_mgmt
 rd 1:1
 !
 address-family ipv4
 route-target export 1:1
 route-target import 1:1
 route-target import 2:2
 route-target import 2:1
 exit-address-family
 !
 address-family ipv6
 route-target export 1:1
```

```
 route-target import 1:1
 route-target import 2:1  -- import route of vrfa
 route-target import 2:2  -- import route of vrfb
 exit-address-family
```

IPv6 対応ケーブルの確認

ここでは、IPv6 対応ケーブルの設定を確認する方法について説明します。この項の内容は次のとおりです。

IPv6 VRF 設定の確認

IPv6 VRF 設定を確認するには、特権 EXEC モードで show vrf ipv6 コマンドを使用します。

```
Router# show vrf ipv6 vrfa
  Name                             Default RD          Protocols   Interfaces
  vrfa                             2:1                 ipv4,ipv6   Bu1.11
Router# show vrf ipv6 interfaces
Interface              VRF                              Protocol   Address

Bu1.10                 vrf_mgmt                         up         2001:40:3:110::1

Fa0/0/0                vrf_mgmt                         up         2001:20:4:1::38

Bu1.11                 vrfa                             up         2001:40:3:111::1

Bu1.12                 vrfb                             up         2001:40:3:112::1

CMTS#
```

IPv6 BGP ステータスの確認

IPv6 BGP ステータスを確認するには、特権 EXEC モードで show ip bgp コマンドを使用します。

```
Router# show ip bgp vpnv6 unicast all neighbors

BGP neighbor is 11.1.1.5,  remote AS 1, internal link
  BGP version 4, remote router ID 11.1.1.5
  Session state = Established, up for 00:35:52
  Last read 00:00:37, last write 00:00:14, hold time is 180, keepalive interval is 60 seconds

  BGP multisession with 2 sessions (2 established), first up for 00:40:07
  Neighbor sessions:
    2 active, is multisession capable
  Neighbor capabilities:
    Route refresh: advertised and received(new) on session 1, 2
    Address family IPv4 Unicast: advertised and received
    Address family VPNv6 Unicast: advertised and received
......
```

MPLS 転送テーブルの確認

MPLS 転送テーブルの出力を確認するには、特権 EXEC モードで show mpls forwarding-table コマンドを使用します。

```
Router# show mpls forwarding-table
```

```
Local  Outgoing      Prefix            Bytes Label   Outgoing   Next Hop
Label  Label or VC   or Tunnel Id      Switched      interface
......
19     No Label      2001:40:3:110::/64[V]   \                              ---Route in
vrf_mgmt
                                       0             aggregate/vrf_mgmt
21     No Label      2001:40:3:111::/64[V]   \                              ---Route in
vrfa
                                       0             aggregate/vrfa
22     No Label      2001:40:3:112::/64[V]   \                              ---Route in
vrfb
                                       0             aggregate/vrfb
......
```

IPv6 ケーブル モデムとホスト状態の確認

ケーブルモデムおよびCPEのIPv6アドレスと接続ホストの状態を確認するには、特権EXECモードで **showinterfacecablemodem** コマンドを使用します。

```
Router# show interface cable 7/0/0 modem ipv6
SID  Type State         IPv6 Address                            M MAC address
11   CM  online         2001:420:3800:809:3519:5F9C:B96A:D31    D 0025.2e2d.743a
11   CPE unknown        2001:420:3800:809:3DB2:8A6C:115F:41D8   D 0011.2544.f33b
```

単一アドバタイズでの複数の IAPD の確認

ネットワーク上のデバイスに割り当てられた複数の IPv6 プレフィックスを確認するには、特権 EXEC モードで show cable modem ipv6 prefix コマンドを使用します。

```
Router# show cable modem ipv6 prefix
Load for five secs: 1%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *06:36:53.075 UTC Thu Aug 2 2012
Device Type: B - CM Bridge, R - CM Router
IP Assignment Method: D - DHCP
MAC Address    Type IPv6 prefix
0023.bed9.4c91 R/D  2001:40:1012::/64
               R/D  2001:40:2012:1::/64
0000.002e.074c R/D  2001:40:1012:8::/64
               R/D  2001:40:2012:1D::/64
0000.002e.074b R/D  2001:40:1012:23::/64
               R/D  2001:40:2012:1C::/64
0000.002e.074a R/D  2001:40:1012:22::/64
               R/D  2001:40:2012:1B::/64
```

特定の MAC アドレスを持つ CM の背後の CPE に割り当てられている複数の IPv6 プレフィックスを確認するには、特権 EXEC モードで **showcablemodem** *mac-address***ipv6prefix** コマンドを使用します。

```
Router# show cable modem 0023.bed9.4c8e ipv6 prefix
Load for five secs: 0%/0%; one minute: 1%; five minutes: 1%
Time source is hardware calendar, *06:37:22.335 UTC Thu Aug 2 2012
Device Type: B - CM Bridge, R - CM Router
IP Assignment Method: D - DHCP
MAC Address    Type IPv6 prefix
0023.bed9.4c91 R/D  2001:40:1012::/64
               R/D  2001:40:2012:1::/64
```

特定のMACアドレスを持つCM内のCPEのIPv6情報を確認するには、特権EXECモードでshow cable modem *mac-address* ipv6 **cpe** コマンドを使用します。

```
Router# show cable modem 0023.bed9.4c8e ipv6 cpe
Load for five secs: 0%/0%; one minute: 1%; five minutes: 1%
```

```
Time source is hardware calendar, *06:37:20.439 UTC Thu Aug 2 2012
MAC Address    IP Address
0023.bed9.4c91 2001:40:3:4:200:5EB7:BB6:C759
               2001:40:3:4:210:D73B:7A50:2D05
```

サポートされている MIB

CISCO-DOCS-EXT-MIB

CISCO-DOCS-EXT-MIB には、Data-over-Cable Service Interface Specifications（DOCSIS）インターフェイス MIB（DOCS-IF-MIB）への拡張をサポートするオブジェクトが含まれています。

- CdxBundleIpHelperEntry：バンドル インターフェイスおよびサブバンドル インターフェイス上のケーブル ヘルパー エントリのリストを提供します。
- CdxBundleIPv6DHCPRelayEntry：バンドル インターフェイスおよびサブバンドル インターフェイス上の IPv6 DHCP リレー オプション、IPv6 DHCP リレー送信元インターフェイス詳細、および IPv6 DHCP リレー トラスト構成が含まれています。
- CdxBundleIPv6DHCPRelayDestEntry：ケーブル バンドル インターフェイスおよびサブバンドル インターフェイス上の IPv6 DHCP リレー送信先エントリのリストが含まれています。

その他の参考資料

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 対応ケーブルに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *130*：ダウンストリーム インターフェイスの設定に関する機能情報

機能名	リリース	機能情報
構成可能な DOCSIS CMTS 機能の DHCPv6 フィールド	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータで導入されました。
IPv6 対応ケーブル	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 50 章

ケーブル DHCP リースクエリ

このドキュメントでは、Cisco Cable Modem Termination System（CMTS）ルータでの Dynamic Host Configuration Protocol（DHCP）リースクエリ機能について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *131* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

ケーブル DHCP リースクエリの前提条件

- Cisco CMTS ルータで DHCP リースクエリを有効にするには、その前に **cablesource-verifydhcp** コマンドおよび **nocablearp** コマンドを使用してケーブル インターフェイスを設定する必要があります。リースクエリは DHCP サーバまたは設定済みの代替サーバに送信されます。

DHCP リースクエリを特定のサーバに転送するには、Cisco CMTS ルータで DHCP リースクエリを有効にする前に、cable **source-verifydhcpserver** ipaddress コマンドおよび **nocablearp** コマンドを使用する必要があります。設定できる代替サーバは 1 つだけです。

- Cisco CMTS ルータ上に IPv6 顧客宅内機器（CPE）ルータが導入される場合は、**ipv6 route** コマンドを設定する必要があります。

ケーブル DHCP リースクエリの制限事項

- 代替サーバが設定されていない限り、リースクエリは DHCP サーバに送信されます。
- 設定できる代替サーバは 1 つだけです。
- DHCP サーバと設定済みの代替サーバを同期する責任はユーザにあります。
- 設定済みの代替サーバで障害が発生したとしても、リースクエリ要求の送信先は DHCP サーバに戻されません。
- クライアントごとにサポートされる IA_IADDR は 1 つだけです。リースクエリが複数の結果を返した場合、クエリに一致する IA_ADDR だけが Cisco CMTS サブスクライバ データベースに追加されます。
- Cisco CMTS は、CPE の IPv6 リンク ローカル アドレスのソースを検証しません。

ケーブル DHCP リースクエリについて

ウィルス、サービス妨害（DoS）攻撃、サービス不正使用攻撃により、未使用のアドレスを探し出すために IP アドレス範囲のスキャンが開始された場合、問題が発生することがあります。Cisco CMTS ルータが不明な IP アドレスを検証しているときに、この種のスキャンによって大量の DHCP リースクエリが生成されて、次の問題が発生する可能性があります。

- Cisco CMTS ルータ PRE カードによる CPU 使用率が高くなる。
- DHCP サーバの使用率が高くなり、応答が遅くなったり無応答になったりする。
- Cisco CMTS ルータまたは DHCP サーバ（あるいは設定済みの代替サーバ）によってパケットがドロップされる。
- ケーブル インター フェースで他の顧客が利用できる帯域幅がなくなる。

このような大量のリースクエリ要求がケーブル インターフェイスで発生しないようにするには、アップストリームインターフェイス、ダウンストリームインターフェイス、またはその両方で、これらの要求のフィルタリングを有効にできます。ケーブル DHCP リースクエリ機能を有効にすると、Cisco CMTS は、設定された期間中、サービス ID（SID）ごとに特定の数の DHCP リースクエリ要求だけをインターフェイスで許可します。ある SID が最大許容数を超えるリースクエリを生成すると、ルータは次の設定期間が始まるまで、最大許容数を超える過剰な要求をドロップします。

DHCPサーバ（または設定済みの代替サーバ）とケーブルネットワークの機能に合わせて、DHCPリースクエリ要求の許容数と間隔を設定できます。

DHCP リースクエリ要求を DHCP サーバに送信するように Cisco CMTS ルータを設定するには、**cablesource-verifydhcp** and**nocablearp** コマンドを使用します。ケーブルインターフェイス上でケーブルモデムを使用する顧客宅内機器（CPE）デバイスのパケット内で不明なIPアドレスが見つかると、それが検証されます。この IP アドレスが割り当てられている CPE デバイスが存在する場合、そのデバイスの DHCP リレー情報とリース情報を含む DHCP ACK メッセージが DHCP サーバから返されます。

cablesource-verifydhcp コマンドと **nocablearp** コマンドが設定されている場合、ケーブル バンドルインターフェイスで設定されているIPアドレス範囲内の不明なIPアドレスを検証するために、ダウンストリーム パケットに関する DHCP リースクエリが送信されます。

DHCP リースクエリがダウンストリーム方向で機能するためには、Cisco Network Registrar（CNR）が DHCP Option 82 を認識する必要があります。CMTS で CPE IP アドレスを正しい CM にマッピングするためには、これが必要です。これを行うには、DHCP DISCOVER メッセージの中にサービス クラス リレー エージェント オプションを挿入するよう、バンドル インターフェイスで **ipdhcprelayinformationoption** コマンドを設定します。このように設定すると、DHCP DISCOVER 実行中に DHCP Option 82 の値が CNR によりキャッシュに入れられ、その IP アドレスに関する後続の DHCP リースクエリでこの値が CMTS に返されます。

DHCP リースクエリ要求を DHCP サーバ以外のサーバに送るように Cisco CMTS ルータを設定するには、**cablesource-verifydhcpserveripaddress**and**nocablearp** コマンドを使用します。

Cisco CMTS では、シスコの標準に従った DHCP リースクエリ、および RFC 4388 標準準拠の DHCP リースクエリの 2 種類の DHCP リースクエリ実装がサポートされます。これらの 2 つの標準の主な違いは、クエリまたは DHCP サーバへの応答で使用される識別子です。DHCP サーバでサポートされている標準に応じて、いずれかの実装を選択できます。

Cisco モードまたは RFC 4388 標準モードで Cisco CMTS を設定するには、**ipdhcpcompatibility lease-query client** {**cisco** | **standard**} コマンドを使用します。

DHCP MAC アドレス除外リスト

この機能により、Cisco CMTS の標準的な DHCP 送信元検証から、信頼できる MAC アドレスを除外することができます。DHCP MAC アドレス除外リスト機能により、標準的な DHCP 送信元検証では拒否されるようなパケットでも、信頼できる MAC アドレスからのパケットであれば通過できます。この機能は、指定した MAC アドレスに対する Cisco CMTS での cable source-verify コマンドをオーバーライドしますが、標準的な有効化された DHCP 送信元検証プロセスのサポートを完全に維持します。この機能は、Cisco cBR ルータ シャーシ上のパフォーマンス ルーティング エンジン 1（PRE1）、PRE2、および PRE4 モジュールでサポートされます。

送信元検証チェックを行わずに、DHCP で信頼できる送信元 MAC アドレスからのパケットを通過させるには、グローバル コンフィギュレーション モードで cable trust コマンドを使用します。信頼できる MAC アドレスを MAC 除外リストから削除するには、このコマンドの no 形式を使用します。除外リストから MAC アドレスを削除すると、その送信元からのすべてのパケットが標準の DHCP 送信元検証の対象になります。

cable trust コマンドの詳細については、『Cisco IOS CMTS Cable Command Reference Guide』を参照してください。

統一 DHCPv6 リースクエリ

この機能は、アップストリーム IPv6 ソース検証用に Cisco CMTS ルータで統一 DHCPv6 リースクエリ プロトコル（RFC 5007）をサポートします。このプロトコルは、家庭や小規模なオフィスのケーブル展開の背後にある IPv6 CPE の信頼性を検証します。

ルータで IPv6 ソース検証が失敗した場合、バンドルインターフェイスまたはサブインターフェイスで **cableipv6source-verifydhcp** and **nocablend** コマンドが設定されていれば、Cisco CMTS は Cisco Network Registrar（CNR）に対して統一 DHCPv6 リースクエリをトリガーします。有効なリースクエリ応答が CNR から受信される場合、Cisco CMTS は CPE をサブスクライバ データベースに追加し、その CPE に関する以降のトラフィックを許可します。

Cisco CMTS ルータでの統一 DHCPv6 リースクエリ プロトコルの主な用途は、プレフィックス委任（PD）ルートを含む CPE のデータ損失を回復することです。Cisco CMTS からの IPv6 CPE データが損失する場合はいくつかあります。たとえば、Cisco CMTS リロード中に PD ルート損失が発生することがあります。

統一 DHCPv6 リースクエリ プロトコルでは、次のものもサポートされます。

- DHCPv6 リースクエリ プロトコル
- ソース検証が失敗したクライアントに関する不正クライアント データベース
- DHCPv6 リースクエリ フィルタ
- 特定の DHCPv6 サーバに対する DHCPv6 リースクエリ

ケーブル DHCP リースクエリ要求のフィルタリングの設定方法

Cisco CMTS のダウンストリームとアップストリームで DHCP リースクエリ要求のフィルタリングを設定するには、次の手順に従います。

ダウンストリームでの DHCP リースクエリ フィルタリングの有効化

ケーブル インターフェイスのすべてのダウンストリームで DHCP リースクエリのフィルタリングを開始するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権EXECモードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cablesource-verifyleasequery-filterdownstream** *threshold interval* 例： `Router(config)# cable source-verify leasequery-filter downstream 5 10`	指定されたバンドル インターフェイスに対し、指定のしきい値および間隔の値を使用して、すべてのダウンストリームでリースクエリ フィルタリングを有効にします。
ステップ 4	**end** 例： `Router(config)# end`	コンフィギュレーション モードを終了し、特権EXECモードに戻ります。

アップストリームでの DHCP リースクエリ フィルタリングの有効化

バンドル インターフェイスのすべてのアップストリームでDHCPリースクエリのフィルタリングを開始するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacebundle** *bundle-no* 例： `Router(config)# interface bundle 1`	指定したバンドル インターフェイスに関するインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**cablesource-verifyleasequery-filterupstream** *threshold interval* 例： `Router(config-if)# cable source-verify leasequery-filter upstream 2 5`	指定されたバンドル インターフェイスに対し、指定のしきい値および間隔の値を使用して、すべてのアップストリームでリースクエリ フィルタリングを有効にします。 （注） **cablesource-verifyleasequery-filterupstream** コマンドはバンドル インターフェイスでのみ設定できます。 （注） ステップ 3 とステップ 4 を繰り返して、他のバンドルインターフェイスに対してアップストリームでの DHCP リースクエリのフィルタリングを有効にします。ケーブルバンドル内のマスターとスレーブのインターフェイスは個別に設定する必要があります。
ステップ 5	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

統一 DHCPv6 リースクエリ フィルタリングの設定

IPv6 CPE の信頼性を検証するために DHCP サーバにリースクエリを送信するよう Cisco CMTS ルータを設定するには、次の手順に従います。また、バンドル インターフェイスでのリースクエリ要求の数量を抑えるために、これらの要求のフィルタリングを有効にすることもできます。同様に、許容されるリースクエリ要求の数と間隔を設定することもできます。

（注） リースクエリ タイマが満了すると、IPv4 静的 CPE のみがホスト データベースから削除されます。

はじめる前に

- 統一 DHCPv6 リースクエリ プロトコルを設定する前に、バンドルインターフェイス コンフィギュレーション モードで **no** 形式の **cablend** コマンドを使用して IPv6 ネイバー探索（ND）収集機能を無効にしてください。IPv6 ND 収集の詳細については、IPv6 対応ケーブル機能ガイドを参照してください。
- 統一 DHCPv6 リースクエリ プロトコルを有効にするには、Cisco CMTS バンドルまたはバンドル サブインターフェイスで **cableipv6source-verifydhcp** コマンドを設定します。
- 単一の DHCP サーバに対しては **cableipv6source-verifydhcp** [**server** *ipv6-address]* コマンドを使用します。
- 複数の *DHCP* サーバに対しては **cableipv6source-verifydhcpcommandwithoutanykeywords** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacebundle** *bundle-no* 例： `Router(config)# interface bundle 1`	指定したバンドルインターフェイスに関するインターフェイス コンフィギュレーション モードを開始します。

ステップ 4	**cableipv6source-verify** または **cableipv6source-verifydhcp** [server ipv6-address]
	
	例：
	`Router(config-if)# cable ipv6 source-verify`
	`or`
	`Router(config-if)# cable ipv6 source-verify dhcp server 2001:DB8:1::1`
		指定したバンドルインターフェイスでのリースクエリ フィルタリングを有効にし、複数の DHCPv6 サーバで IP アドレスを検証します。または、指定したバンドルインターフェイスでのリースクエリ フィルタリングを有効にし、指定した DHCPv6 サーバで IP アドレスを検証します。

	コマンドまたはアクション	目的
ステップ 5	**cableipv6source-verifyleasetimer** *value* 例： `Router(config-if)# cable ipv6 source-verify leasetimer 200`	Cisco CMTS の内部 CPE データベースを検査してリース時間が満了した IPv6 アドレスを調べるために、指定したバンドル インターフェイスでのリースクエリ タイマーを有効にします。
ステップ 6	**cableipv6source-verifyleasequery-filter** *threshold interval* 例： `Router(config-if)# cable ipv6 source-verify leasetimer 5 10`	IPv6 リースクエリ要求のフィルタリングを有効にします。
ステップ 7	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権EXECモードに戻ります。

ダウンストリームでの DHCPv6 リースクエリ フィルタリングの有効化

ケーブル インターフェイスのすべてのダウンストリームで DHCP リースクエリのフィルタリングを開始するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**cableipv6source-verifyleasequery-filterdownstream** *threshold interval* 例： `Router(config-if)# cable ipv6 source-verify leasetimer 5 10`	指定されたバンドル インターフェイスに対し、特定のしきい値および間隔の値を使用して、すべてのダウンストリームでリースクエリ フィルタリングを有効にします。
ステップ 4	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DHCP リースクエリのフィルタリングの設定例

ここでは、DHCP リースクエリのフィルタリング機能を設定する例を記載します。

例：DHCP リースクエリのフィルタリング

次の例に、アップストリーム/ダウンストリームの両方のインターフェイスでDHCP リースクエリ要求をフィルタリングするようにバンドル インターフェイスを設定する場合の、一般的な設定を抜粋します。

（注） リースクエリ要求を受信する代替サーバがすでに設定されている場合、以下の **cablesource-verifydhcp** コマンドの代わりに **cablesource-verifydhcpserver** *ipaddress* コマンドが表示されます。

```
.
.
.
cable source-verify leasequery-filter downstream 5 20
.
.
.
interface bundle 1
.
.
.
 cable source-verify dhcp
 cable source-verify leasequery-filter upstream 1 5
 no cable arp
.
.
```

例：統一 DHCPv6 リースクエリのフィルタリング

次に、Cisco IOS リリース 12.2(33)SCF1 のルータでフィルタリングされた DHCPv6 リースクエリ要求の総数を表示する例を示します。

```
Router# show cable leasequery-filter
IPv4 Lease Query Filter statistics for Unknown Sid
  Requests Sent : 0 total. 0 unfiltered, 0 filtered
IPv6 Lease Query Filter statistics for Unknown Sid
  Requests Sent : 0 total. 0 unfiltered, 0 filtered
```

その他の参考資料

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

ケーブル DHCP リースクエリに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *132*：ケーブル *DHCP* リースクエリに関する機能情報

機能名	リリース	機能情報
ケーブル DHCP リースクエリ	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 51 章

レイヤ 3 CPE モビリティ

レイヤ 3 CPE モビリティ機能は、モビリティ CPE デバイスができる限りトラフィックを中断せずにケーブル モデム間を移動できるよう導入されました。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *133* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

レイヤ 3 CPE モビリティの前提条件

レイヤ 3 CPE モビリティ機能を使用するために、特別な装置やソフトウェアは必要ありません。

レイヤ 3 CPE モビリティの制限事項

- レイヤ 3 CPE モビリティ機能を使用すると、CPE デバイスの移動範囲を同じバンドル内またはサブバンドル インターフェイス内に制限することができます。
- モビリティを設定する IPv4 または IPv6 サブネットは、バンドルまたはサブバンドル インターフェイスですでに設定されている IPv4 または IPv6 サブネットと一致する必要があります。そうでない場合は設定は受け入れられず、次のメッセージが表示されます。

```
Please remove the previous online CPEs or reset CMs,
```

- バンドルまたはサブバンドル インターフェイスで IPv4 または IPv6 アドレスを削除すると、関連のモビリティ サブネットも同時に削除されます。
- マルチキャスト パケットは、レイヤ 3 CPE モビリティ機能をトリガーしません。
- バンドルまたはサブバンドル インターフェイスで設定された VRF は、CPE モビリティ機能がサポートされません。
- レイヤ 3 CPE モビリティ機能では、同時に移動する CPE デバイスの数やシステムの負荷状態によっては、モビリティ時のパケット ロスタイム期間は予測不能となります。
- 複数の IPv4 または IPv6 アドレスを持つ CPE デバイスでは、すべての IPv4 または IPv6 アドレスは新しい送信元情報により再構築されます。
- レイヤ 3 CPE モビリティは、ラインカード HA または SUP HA の間に失敗する場合があり、トリガー アップストリーム パケットがドロップします。
- CPE モビリティがオンになると、モビリティの動作はケーブル IPv4 または IPv6 の送信元検証前に有効になります。
- レイヤ 3 CPE モビリティがイネーブルの場合、モビリティ サブネットが CPE デバイスを迅速に移動できるよう、一部のセキュリティ チェックがスキップされます。

レイヤ 3 CPE モビリティの情報

レイヤ 3 CPE モビリティ機能では、IPv4 または IPv6 のユニキャスト アップストリーム パケットをトリガーとして、CPE デバイスがケーブル モデム間を移動できます。

各ケーブルモデムは事業拠点のホットスポットに置かれます。CPEデバイスは、サービスプロバイダーもヘッドエンド CMTS も同じである事業拠点間を移動します。このモビリティは選択した IP サブネットで許可されます。

モビリティを設定するIPv4またはIPv6サブネットは、バンドルまたはサブバンドルインターフェイスですでに設定されている IPv4 または IPv6 サブネットと一致する必要があります。そうでない場合は設定は受け入れられず、次のメッセージが表示されます。

```
Please remove the previous online CPEs or reset CMs,
```

バンドルまたはサブバンドル インターフェイスでモビリティ サブネットを削除すると、モビリティ サブネットが設定または削除された後で次の警告メッセージが表示されます。

```
Warning: Please remove the previous online CPEs or reset CMs, to make the mobility scope
change works for every device !!!
```

（注） サブネットのモビリティ設定が有効な場合、既存のオンライン CPE デバイスはモビリティ サブネットを認識するように更新されますが、その間は CPU 使用率が高くなります。したがって、CM および CPE がオンラインになる前にモビリティ サブネットを設定することをお勧めします。

レイヤ 3 CPE モビリティ機能を有効にすると、特定の状況でパントされたパケットが過剰に発生する可能性があります。デフォルトでは、送信元ベースのレート制限（SBRL）機能がこのようなパントされたパケットをレート制限して、CPU のオーバーロードを回避します。

レイヤ 3 CPE モビリティの利点

この機能は、IP アドレスを変更せずにケーブル モデム間で CPE デバイスを移動でき、確立された TCP または UDP セッションは維持されます。

レイヤ 3 モビリティの設定方法

CPE モビリティの設定

ここでは、インターフェイスまたはサブインターフェイスバンドルで特定の IP サブネットのモビリティを有効にする方法について説明します。

はじめる前に

モビリティのサブネットは、バンドルまたはサブバンドルインターフェイスで設定した IPv4 または IPv6 のアドレスと一致する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacebundlebundlenumber|bundle-subif-number**
	
	例：
	
	`Router(config)# interface bundle 1`
	`or`
	`Router(config)# interface Bundle 1.1`
		インターフェイス コンフィギュレーションまたはサブインターフェイス モードを開始します。

ステップ 4	**cablel3-mobility** *IP-address mask* | *IPv6 prefix*
	
	例：
	
	`Router(config-if)# cable l3-mobility 2001:DB:22:1::1/64`
	
	例：
	
	`Router(config-subif)# cable l3-mobility 192.0.3.1 255.255.255.0`
	
	例：
	
	`Router(config-subif)#cable l3-mobility 2001:DB:22:1::1/64`
		特定の IPv4 または IPv6 サブネットのモビリティをイネーブルにします。
		
		（注） このコマンドは、インターフェイスまたはサブインターフェイス バンドルで設定できます。

ステップ 5	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

次の作業

トラブルシューティングのヒント

モビリティの IP アドレスがモビリティのサブネットと一致しない場合は、次の警告メッセージが表示されます。

```
Mobility IP should match the IDB subnet!
```

インターフェイスから IPv4 または IPv6 アドレスを削除すると、その IP アドレスのモビリティ範囲が削除され、次の警告メッセージが表示されます。

```
IPv6 2001:DBB:3:111::1 removed from Mobility subnets on Bundle1
。
```

L3 モビリティの送信元ベースのレート制限（SBRL）の設定

ここでは、L3 モビリティ機能の送信元ベースのレート制限（SBRL）を設定する方法について説明します。この手順はオプションであり、設定しない場合はデフォルトの SBRL 設定が適用されます。

（注） L3 モビリティの SBRL はデフォルトで有効のため、この設定はオプションです。

加入者側の SBRL には、パント要因ごとのグローバル コンフィギュレーションがあります。L3 モビリティ パントは、パント要因ごとの設定のみの対象です。トラフィック ストリームは、パント要因と発信元 MAC アドレスのハッシュ値で識別されます。この値は、レート制限のインデックスとして使用されます。ハッシュ衝突に対する特別な処理がないため、ハッシュ衝突ストリームが同じストリームであるかのように処理されます。

L3 モビリティのデフォルトのレートは 4 パケット/秒です。

はじめる前に

（注） パントされたすべてのパケットは、CoPP とパント ポリサーの対象です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**platform punt-sbrl subscriber punt-cause** *punt-cause***rate** *rate* 例： `Router(config)# platform punt-sbrl subscriber punt-cause 99 rate 8`	加入者 MAC アドレス SBRL を設定します。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Router(config-if)# exit`	グローバル コンフィギュレーション モードを終了します。

CPE モビリティの無効化

ここでは、特定の IP サブネットでモビリティをディセーブルにする方法について説明します。

はじめる前に

次の手順を完了する前に、CPE モビリティを特定の IP サブネットでイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacebundle** *bundle number* | *bundle-subif-number*
	
	例：
	
	`Router(config)# interface bundle 1`
	or
	`Router(config)# interface Bundle 1.1`
		インターフェイス コンフィギュレーション またはサブインターフェイス モードを開始します。

	コマンドまたはアクション	目的

ステップ 4	**nocablel3-mobility** *IP-address mask* | *IPv6 prefix*
	
	例：
	
	`Router(config-if)# cable l3-mobility 192.0.3.1 255.255.255.0`
	
	`Router(config-if)# cable l3-mobility 2001:DB:22:1::1/64`
		特定の IPv4 または IPv6 サブネットのモビリティをディセーブルにします。
		
		（注） このコマンドは、インターフェイスまたはサブインターフェイスバンドルで設定できます。

ステップ 5	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

レイヤ 3 モビリティ設定の確認

レイヤ 3 モビリティ設定を確認するには、**showcablebundle** コマンドを使用します。

レイヤ 3 モビリティの設定例

ここでは、次の設定例について説明します。

例：CPE レイヤ 3 モビリティの設定

次に、インターフェイス バンドルのレイヤ 3 CPE モビリティを設定する方法について説明します。

```
Router#show running interface bundle 10
Building configuration...
Current configuration : 1247 bytes
!
interface Bundle10
ip address 192.0.3.1 255.255.255.0 secondary
ip address 192.2.21.1 255.255.255.0 secondary
ip address 192.3.23.1 255.255.255.0
ip pim sparse-dense-mode
ip igmp static-group 231.1.1.1
no cable arp filter request-send
no cable arp filter reply-accept
cable l3-mobility 192.0.3.1 255.255.255.0
cable l3-mobility 192.2.21.1 255.255.255.0
cable l3-mobility 192.3.23.1 255.255.255.0
cable l3-mobility 2001:DB:26:1::1/64
cable l3-mobility 2001:DB:27:1::1/96
cable dhcp-giaddr primary
cable helper-address 20.1.0.3
ipv6 address 2001:DB:26:1::1/64
ipv6 address 2001:DB:27:1::1/96
ipv6 enable
```

```
ipv6 nd reachable-time 3600000
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 dhcp relay destination 2001:DB:1:1:214:4FFF:FEA9:5863
end
```

例：L3 モビリティの SBRL の設定

次に、L3 モビリティの SBRL の設定方法について説明します。

```
Router# show run | i punt-sbrl
platform punt-sbrl subscriber punt-cause 99 rate 8
```

その他の参考資料

ここでは、Cisco CMTS ルータのレイヤ 3 CPE モビリティ機能に関連する資料を紹介します。

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

レイヤ 3 CPE モビリティに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *134*：レイヤ *3 CPE* モビリティに関する機能情報

機能名	リリース	機能情報
レイヤ 3 モビリティ	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 52 章

DOCSIS 3.0 マルチキャスト サポート

Cisco cBR シリーズ ルータは、Data-over-Cable Service Interface Specifications（DOCSIS）3.0 に基づくマルチキャストの改良をサポートします。DOCSIS 3.0 マルチキャスト サポートにより、帯域幅の効率が向上し、サービス プロバイダーはトラフィックの種類に応じて異なる Quality of Service を提供することができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *135*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

DOCSIS 3.0 マルチキャスト サポートの前提条件

- DOCSIS 3.0 対応の Cisco CMTS と、DOCSIS 3.0 イネーブルのケーブル モデムが必要です。
- Cisco CMTS はデフォルトで MDF イネーブルである必要があります。
- サービス品質（QoS）パラメータは、さまざまなマルチキャスト セッション用に設定されている必要があります。

DOCSIS 3.0 マルチキャスト サポートの制約事項

- 明示的トラッキングはディセーブルにできません。
- マルチキャスト QoS のために、3 つのオブジェクトおよびテンプレート、サービス クラス、Group-QoS-Config（GQC）、および Group-Config を定義し、それらを特定のバンドルまたは転送インターフェイスに関連付ける必要があります。
- オブジェクトとテンプレートを定義する前に、デフォルトのサービス クラスと GQC を定義する必要があります。
- 静的マルチキャスト機能は常にイネーブルであり、ディセーブルにすることはできません。
- グループ設定がデフォルトの転送インターフェイスで設定されている場合、サービス フロー属性ベースの選択は無視されます。
- マルチキャスト DSID 機能は DOCSIS 3.0 準拠のケーブル モデムでのみサポートされます。
- cable multicast mdf-disable wb-incapable-cm コマンドは、ケーブル モデムのマルチキャスト ダウンストリーム サービス ID（DSID）転送機能を無効にします。これにより、Cisco CMTS とケーブル モデム間の DSID 機能が影響を受けます。
- CPE へのマルチキャスト トラフィックは、アクティブ セッション中にマルチキャスト QoS 設定やサービス フロー属性を変更した後、2 倍に増大します。トラフィックの複製は、デフォルトのセッション タイムアウト期間（180 秒）まで続きます。セッション タイムアウト後、マルチキャスト DSID は Cisco CMTS と CM から削除され、通常のマルチキャスト トラフィック フローが再開されます。
- DOCSIS 3.0 マルチキャスト サポート機能が正しく機能するには、CPE と CM が同じ Virtual Routing and Forwarding（VRF）インターフェイス上にある必要があります。

DOCSIS 3.0 マルチキャスト サポートに関する情報

ネットワーク アプリケーション内蔵のテクノロジーである IP マルチキャストは、複数の受信者に同じ情報を転送します。ケーブル ネットワークを含むネットワーク アプリケーションはいずれも、マルチキャスト テクノロジーの帯域幅の効率化を利用することができます。2 つの新しいテクノロジー、チャネル ボンディングと Single Source Multicast（SSM）により、マルチキャストの導入が大幅に加速されることが予想されます。

チャネル ボンディングと SSM テクノロジーにより、既存の光同軸ハイブリッド（HFC）ネットワークの運用効率が劇的に向上します。ケーブル オペレータはマルチキャストの改良を使用して、ビデオ オン デマンド（VoD）、インターネット プロトコル テレビジョン（IPTV）などの高度なサービスをシームレスに提供したり、インタラクティブなビデオと音声、およびデータ サービスを促進することができます。

次の項では、DOCSIS 3.0 マルチキャスト サポートの利点について説明します。

マルチキャスト DSID 転送

DOCSIS 3.0 マルチキャスト サポートにより、幅広いマルチキャスト プロトコルをサポートする柔軟性と拡張性を提供するための集中制御が Cisco CMTS に実装されています。これは、DOCSIS 1.1 および 2.0 モデルに含まれていた Internet Group Management Protocol（IGMP）バージョン 2 スヌーピング インフラストラクチャに代わるものです。ここで Cisco CMTS は、すべてのマルチキャスト ストリームを特定するために、一意のダウンストリーム サービス ID（DSID）を割り当てます。これらの DSID は CM に送信され、マルチキャスト トラフィックのフィルタリングおよび CPE への転送に使用されます。

マルチキャスト DSID 転送（MDF）には次の利点があります。

- MAC ドメイン内のボンディング グループにわたって、パケット ストリームを一意に認識します。
- マルチキャスト チャネルごとに、Any-Source Multicast（ASM）または Source Specific Multicast（SSM）のいずれかにパケット ストリームを指定します。
- マルチキャスト DSID 管理はルート プロセッサ（RP）上に実装されているため、スタンドアロンで動作します。
- Cisco CMTS による全アップストリーム信号制御パケットのスヌーピングにより、マルチキャスト DSID 転送（MDF）イネーブルの CM 上の顧客宅内機器（CPE）を検出し、プールから DSID が割り当てられます。
- 割り当てられた DSID は、Dynamic Bonding Change（DBC）メッセージにより CM に送信されます。
- マルチキャスト セッションを組み合わせて、同ボンディング グループ内の他の MDF イネーブル CM で DSID を再利用します。
- マルチキャスト セッションがイベントを終了すると、Cisco CMTS による DBC メッセージによって DSID は CM から削除されます。
- 最後のメンバーがボンディング グループを離れると、Cisco CMTS により DSID はプールに解放されます。
- 次の DSID は各プライマリ ダウンストリーム（モジュラおよび組み込みケーブル インターフェイス）に事前に割り当てられており、一般クエリ メッセージを転送します。これらの DSID はマルチキャスト グループのシグナリング プロトコルの一部を形成します。他のマルチキャスト グループはこれらの DSID を使用しません。
  - IGMPv2 一般クエリ（IPv4）

- IGMPv3 一般クエリ（IPv4）
- MLDv1 一般クエリ（IPv6）
- MLDv2 一般クエリ（IPv6）
- DSID（IPv6）の事前登録

- DSID の割り当てにより、DOCSIS 3.0 の MDF イネーブル CM でのバーチャル プライベート ネットワーク（VPN）間トラフィック分離が保証されます。たとえば、同じマルチキャストを組み合わせた 2 つの VPN からの 2 つのクライアントは、2 つの個別の DSID を取得します。

ボンディングされた CM でのマルチキャスト転送

DOCSIS 3.0 イネーブル CM へのマルチキャスト パケットは、セカンダリ マルチキャスト ボンディング グループがディセーブルの場合、プライマリ ボンディング グループに DSID 拡張ヘッダーを含むボンディング パケットとして送信されます。MDF ディセーブルまたは DOCSIS 3.0 以前の CM へのマルチキャスト パケットは、DSID 拡張ヘッダーを含まない未ボンディング状態で送信されます。この機能の詳細については、マルチキャスト セカンダリ ボンディング グループ, （893 ページ）を参照してください。

MDF イネーブル CM のみ、または MDF ディセーブル CM のみが存在するネットワークでは、トラフィックはフィールド タイプを使用して分離されます。MDF イネーブル CM はフィールド タイプを持つフレームを転送しますが、MDF ディセーブル CM はこれをドロップします。DSID のラベル付けにより、MDF イネーブル CM はマルチキャスト セッションのコピーを確実に取得して「クロス トーク」を回避します。

フィールド タイプ転送をサポートしないハイブリッド CM（MDF イネーブル CM と MDF ディセーブル CM）では、トラフィックを確実に分離するには、暗号化またはセキュリティ アソシエーション ID（SAID）による分離をセッションごとに設定する必要があります。DOCSIS 3.0 では、ハイブリッド CM がフィールド タイプのフレームの転送に失敗した場合、Cisco CMTS はマルチキャスト セキュリティ アソシエーション ID（MSAID）による分離を使用することになっています。この分離は、一方をボンディングされた CM に、他方を未ボンディングの CM またはハイブリッド CM にというように、異なる MSAID を各複製に割り当てることで達成されます。これにより、CM が重複するトラフィックを受信することを回避できます。

TLV の静的転送

DOCSIS 3.0 仕様により、Cisco CMTS は静的マルチキャストをサポートする必要があります。CM が Cisco CMTS に登録を試みると、Cisco CMTS は静的マルチキャスト エンコーディングが CM コンフィギュレーション ファイルに存在するかどうかをチェックします。静的マルチキャスト エンコーディングが存在する場合、Cisco CMTS は、登録応答（REG-RSP）メッセージで各静的マルチキャスト チャネルに対応する DSID を送信します。

マルチキャスト DSID 管理はスーパーバイザに置かれています。インターフェイス カードは、適切な DSID 割り当てを得るためにはに問い合わせる必要があります。また、後続の静的マルチキャ

ストエンコーディングでスーパーバイザと通信する必要を省くために、インターフェイス カードはスーパーバイザからの応答をキャッシュします。

明示的なトラッキング

Cisco CMTS は、IGMPv3 サポートを使用して明示的なトラッキングを実行できます。IGMPv3 は IGMPv2 仕様に関連するレポート抑制機能を排除するため、Cisco CMTS がセッション情報およびホスト情報の詳細を取得できるようになります。これは、CM ごとの IGMP 高速脱退処理と DSID 管理に役立ちます。

特定のマルチキャスト セッションに参加するホスト（IP/MAC）を追跡するには、ホストまたはセッション データベースを使用します。ホストから、SID とケーブル ダウンストリーム インターフェイスに基づいて CM を追跡できます。また、このデータベースは、マルチキャスト セッションが終了したときに Cisco CMTS が特定の CM から DSID を削除する必要があるかどうかを判断するのにも役立ちます。

マルチキャスト サービス品質の拡張

DOCSIS 3.0 では、CMTS はセッション制限を超えるフローを許可しません。現行のマルチキャスト QoS（MQoS）のセッション制限はセッションは許可しますが、セッション制限を超えたセッションに QoS を提供しません。

（注） マルチキャスト QoS 機能がディセーブルの場合は、デフォルトのグループ サービス フロー（GSF）がマルチキャスト パケットの送信に使用されます。

マルチキャスト QoS の DOCSIS 3.0 要件として、Group Classifier Rules（GCR）のサポートがあります。Cisco CMTS は、セッション範囲がマルチキャスト グループ アドレスに一致している一連のグループ コンフィギュレーション（GC）を決定します。SSM の場合は、一致する GC を特定するために、送信元アドレスも使用されます。一致する GC にはそれぞれ 1 つの GCR が作成され、GCR はマルチキャスト セッションに関連付けられます。また、GCR には一意の ID、SAID、およびグループ サービス フロー（GSF）が割り当てられます。

GC エントリの選択には、次の条件が使用されます。

- 複数の GC エントリが一致する場合、最高ルール プライオリティを持つ GC が選択されます。
- 複数の GC が同じ最高ルール プライオリティを持つ場合、すべての一致する GC エントリが選択されます。

GCR 分類は、タイプ オブ サービス（TOS）フィールドに基づいて行われます。複数の GCR が単一のマルチキャスト セッションに一致している場合、GCR 中の TOS 指定子の使用により、正しい GCR が選択されます。

（注） 2 つのマルチキャスト グループ コンフィギュレーション（GC）のセッション範囲とコンフィギュレーションが（グローバルまたはバンドル コンフィギュレーションで）同じである場合は、同じ転送インターフェイスの選択は保証されません。

非IPマルチキャストおよびブロードキャスト パケットはGSFを使用します。これらは個々のサービス フローに似ており、同じ GCR に一致する特定のデジタル コマンド シグナル（DCS）についてすべての CM により共有されます。単一の GSF は、同様の GQC の集合を使用して異なる GC に一致するマルチキャスト セッションで使用されます。

マルチキャスト セカンダリ ボンディング グループ

DOCSIS 3.0 対応 CM は、CMTS の MDF サポートを使用して非プライマリ（またはボンディングされた）チャネルからマルチキャスト パケットを受信できます。

マルチキャスト セカンダリ ボンディング グループは、光分割によって 1 つ以上のファイバ ノードにフィードする共有ボンディング グループまたは RF チャネル として定義されます。これにより、異なるプライマリ ボンディング グループおよびチャネルの CM は、1 つまたは複数の共有セットをリスニングできるようになります。マルチキャスト パケットは共有ダウンストリーム チャネル セットにのみ複製され、そのためダウンストリーム帯域幅が節約されます。

DOCSIS 3.0 は属性ベースのサービス フロー作成を定義しています。これにより、Cisco CMTS は、ユニキャストおよびマルチキャスト転送のためのボンディング グループまたは個々のチャネルの選択において、より「インテリジェント」な決定ができます。

マルチキャスト セカンダリ ボンディング グループには次の利点があります。

- マルチキャスト セカンダリ ボンディング グループ用の、新しい MQoS および属性ベース転送。
- プライマリ ダウンストリーム インターフェイスはナローバンド CM に対して転送インターフェイスとして機能します。
- ワイドバンド CM の転送インターフェイスを選択するために、以下のアルゴリズムが使用されます。
  - セッションに一致する group-config がプライマリ ボンディング グループに存在する場合、そのプライマリ ボンディング グループが選択されます。MQoS パラメータは group-config から取得されます。
  - group-config がバンドル レベルでもグローバル レベルでも存在しない場合、プライマリ ボンディング グループが選択されます。
  - バンドル レベルまたはグローバル レベルで検索された group-config を使用して、Group-QoS-Config（GQC）、さらには属性および禁止されたビット マスクが検索され、次いでそれらを使用してインターフェイスが検索されます。
  - バンドル レベルの group-config またはグローバル レベルの group-config が設定されている場合、バンドル内のすべてのワイドバンド ケーブル モデム（WCM）は同一のセカンダリ ボンディング グループを使用します。

- 特定の送信元アドレスが一致するインターフェイスが見つからなかった場合、IGMP レポートは送信元を無視します。
  - 一致するインターフェイスが見つかると、そのインターフェイスが転送に使用され、転送インターフェイス、バンドル インターフェイス、またはグローバル レベルの一致する group-config から MQoS パラメータが取得されます。
  - 一致するインターフェイスが見つからない場合、IGMP レポートは無視されます。
- 静的結合の場合は、属性ベースの転送はサポートされず、プライマリ ダウンストリームだけが使用されます。

ロード バランシング

ロードバランシング機能では、特定の CM でマルチキャスト ストリームが配信されている間、その CM はロードバランシングの対象になりません。この機能には明示的トラッキング データベースが使用され、これを達成するのに必要な CM 加入に関する全情報がそこに保持されます。

マルチキャスト DSID 転送ディセーブル モード

ケーブル モデムが IGMP スヌーピングを実行する必要があるアプリケーションでは、そのケーブル モデムの MDF をディセーブルにする必要があります。Cisco CMTS により MDF イネーブル モードで登録されているケーブル モデムは、MDF 転送が DSID フィルタリングに基づくため、IGMP スヌーピングを実行しません。**cablemulticastmdf-disable** コマンドは、ケーブル モデムの MDF 機能を無効にします。

このコマンドはルートプロセッサに設定され、コンフィギュレーション更新によってケーブルラインカードにダウンロードされます。この設定により、Cisco CMTS 転送のメカニズムや DSID 割り当てが変更することはありません。Cisco CMTS により DSID が割り当てられ、マルチキャスト パケットが DSID ヘッダーでカプセル化されます。これは、MDF ディセーブルのケーブル モデム上のトラフィック転送には影響しません。DOCSIS 3.0 仕様により、DOCSIS 2.0 以前または MDF ディセーブルのケーブル モデムは、DSID ヘッダーを無視し、IGMP スヌーピング グループからの Group Media Access Control（GMAC）に基づいてマルチキャスト転送を継続します。ケーブル モデムが MDF ディセーブル モードで動作しているときは IGMPv2 のみがサポートされ、IGMPv3 および MLD メッセージはドロップされます。

IGMP SSM マッピングが使用されている場合、BPI+ に基づくマルチキャスト暗号化は、非 MDF ケーブル モデムではサポートされません。非 MDF ケーブル モデムとは、DOCSIS 3.0 以前のケーブル モデム、または MDF ディセーブル モードで動作している DOCSIS 3.0 ケーブル モデムです。

DOCSIS 2.0 ハイブリッド ケーブル モデムの MDF1 サポート

Cisco CMTS ルータは、DOCSIS 2.0 ハイブリッド ケーブル モデム、IPv6、および MDF 機能をアドバタイズして IPv6 パケット転送を可能にする他のケーブル モデムで MDF 機能をイネーブルにします。**cable multicast mdf-disable** コマンドにおける **wb-incapable-cm** キーワードは、DOCSIS

Set-Top Gateway（DSG）ハイブリッド組み込みケーブル モデムを含むすべての DOCSIS 2.0 ハイブリッド ケーブル モデムで MDF を無効にして、IGMP スヌーピングをサポートします。

ハイブリッド STB の DSG 無効化

wb-incapable-cm キーワードを指定した **cablemulticastmdf-disable** コマンドは、MDF サポートを無効にするだけでなく、すべての DOCSIS 2.0 DSG 組み込みケーブル モデムが DSG マルチキャスト トラフィックを受信することを防止します。

wb-incapable-cm キーワードによって非 DSG DOCSIS 2.0 ハイブリッド ケーブル モデムでのみ MDF 機能が無効になります。すべての DSG 組み込みケーブル モデム（DOCSIS 3.0 DSG および DOCSIS 2.0 DSG ハイブリッド）で MDF 機能を無効にするために、新しいキーワード DSG が導入されました。

（注） MDF 機能を無効にした後で、**clearcablemodemreset** コマンドを実行し、すべての DSG 組み込みケーブル モデムをオンラインにする必要があります。

MDF1 サポートの利点

- 異なる既知のケーブル モデムのファームウェアで IPv6 をサポートします。
- Cisco CMTS での MDF 機能を無効にします。
- インサービス ソフトウェア アップグレード（ISSU）とライン カードの高可用性をサポートします。

動的マルチキャスト レプリケーション セッション

ユーザがパフォーマンスを向上させるために Cisco cBR ルータで IPTV サービスを有効にすると、Cisco cBR で次の機能がサポートされるようになります。

- バンドル インターフェイスごとに 8000 個の SID をサポートします。

  それぞれの MQoS はマルチキャスト セッションごとに 1 つの SID を必要とするので、Cisco cBR はバンドルごとに 8000 個の SID をサポートします。

- IP Communicator メッセージを高速化かつ効率化します。
- マルチキャスト転送を高速化します。
- 動的マルチキャスト セッションのキャッシングを有効にします。

マルチキャスト レプリケーション セッションのキャッシュ

新しいマルチキャスト レプリケーション セッションを作成する場合、使用される CPU サイクルは、既存のマルチキャスト レプリケーション セッションに参加する場合よりも大幅に増えます。

セッションが終了した後、マルチキャストレプリケーションセッションに関連するリソースの大部分をキャッシュすることができます。

したがって、後で新しい IGMP 参加要求を受け取ったときに、これらのリソースを再利用できます。

マルチキャストレプリケーション セッションのキャッシュは、アクティブな SUP でのみ有効です。SUPSOが発生すると、キャッシュされたすべてのセッションが失われ、IGMP/MLD参加要求の受信時に新しいアクティブ SUP でセッションが再作成されます。

LCSOが発生すると、このLCのキャッシュされたすべてのセッションがクリアされ、IGMP/MLD参加要求の受信時に新しいアクティブ LC でセッションが再作成されます。

DOCSIS 3.0 マルチキャスト サポートの設定方法

ここでは、Cisco CMTS ルータに DOCSIS 3.0 マルチキャスト サポートを導入するために必要な次のタスクについて説明します。

基本的なマルチキャスト転送の設定

DOCSIS 3.0 マルチキャスト設定に適用できる基本的なマルチキャスト転送プロファイルを設定するには、**ipmulticast-routing** コマンドを使用します。マルチキャスト グループの作業を続行する前に、マルチキャスト ルーティングのプロファイルを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**IPmulticast-routing**[**vrf**] 例： `Router(config)# IP multicast-routing vrf`	グローバルに、または特定の Virtual Routing and Forwarding（VRF）インターフェイスでマルチキャスト ルーティングを有効にします。

	コマンドまたはアクション	目的
ステップ 4	**interfacebundle** *number* 例： `Router(config)# interface bundle 1`	インターフェイスバンドルを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	**IPpimsparse-mode** 例： `Router(config-if)# IP pim sparse-mode`	スパース動作モードを設定します。 （注） Cisco CMTS ルータは、PIM スパースモード用に設定した Protocol Independent Multicast（PIM）のランデブー ポイント（RP）が必要です。スーパーバイザは、 **ip pim rp-address** コマンドまたはAuto-スーパーバイザ設定プロトコルを使用して設定されます。
ステップ 6	**IPpimsparse-dense-mode** 例： `Router(config-if)# IP pim sparse-dense-mode`	マルチキャスト グループが動作するモードに応じて、スパース動作モードまたはデンス動作モードのいずれかのインターフェイスを設定します。
ステップ 7	**IPigmpversionversion-number** 例： `Router(config-if)# IP igmp version 3`	IGMP バージョン 3 を使用できるようにインターフェイスを設定します。
ステップ 8	**IPigmpv3-query-max-response-time** *response_time* 例： `Router(config-if)# IP igmp v3-query-max-response-time 500`	IGMP バージョン 3 の最大クエリ応答時間を設定します。

マルチキャスト DSID 転送の設定

マルチキャスト DSID 転送機能は、デフォルトでイネーブルになっています。この機能は設定できません。

明示的なトラッキングの設定

明示的なトラッキング機能は、デフォルトで有効になっています。ユーザが構成することはできません。

マルチキャスト QoS の設定

DOCSIS 3.0 設定に適用できるマルチキャスト QoS プロファイルを設定するには、**cablemulticastgroup-qos** コマンドを使用します。マルチキャスト QoS プロファイルを QoS マルチキャスト グループに追加するには、マルチキャスト QoS プロファイルを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権EXECモードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cableserviceclass** *class-index***name** *service-class-name* 例： `Router(config)# cable service class 1 name MQOS_DEFAULT`	ケーブル サービス クラスの名前を設定します。
ステップ 4	**cableserviceclass** *class-index***downstream** 例： `Router(config)# cable service class 1 downstream`	ケーブル サービス クラスのダウンストリームを設定します。
ステップ 5	**cableserviceclass** *class-index***max-rate** *maximum-bandwidth-allowed* 例： `Router(config)# cable service class 1 max-rate 10000000`	ケーブル サービス クラスの最大許容帯域幅を設定します。

	コマンドまたはアクション	目的
ステップ 6	**cableserviceclass** *class-index***min-rate** *cir* 例： `Router(config)# cable service class 1 min-rate 1000000`	ケーブル サービス クラスの最小認定情報レートを設定します。
ステップ 7	**cablemulticastgroup-qosdefaultscn** *service-class-name***aggregate** 例： `Router(config)# cable multicast group-qos default scn MQOS_DEFAULT aggregate`	QoS プロファイルのデフォルトのサービス クラス名を指定します。
ステップ 8	**cablemulticastqosgroup** *number***priority** *value* 例： `Router(config)# cable multicast qos group 20 priority 1`	マルチキャスト QoS グループを設定し、マルチキャストQoSコンフィギュレーション モードを開始して、ケーブル マルチキャスト QoS グループのプライオリティを指定します。
ステップ 9	**application-id** *app-id* 例： `Router(config-mqos)# application-id 10`	マルチキャストQoSグループのアプリケーション ID 番号を指定します。マルチキャスト QoS グループに対してアドミッション制御を有効にするように、この値を設定します。
ステップ 10	**session-rangeip-addressip-mask** 例： `Router(config-mqos)# session-range 230.0.0.0 255.0.0.0`	マルチキャスト QoS グループの IP アドレスと IP マスクのセッション範囲を指定します。複数のセッション範囲を設定できます。
ステップ 11	**cablemulticastqosgroup** *number priority value* [**global**] 例： `Router(config)#cable multicast qos group 20 priority 63 global`	マルチキャスト QoS グループ ID を指定します。

サービス フロー属性ベースの転送インターフェイスの選択

サービス フロー属性機能により、ボンディングされた CM は、複数のボンディング グループをリスニングし、インターフェイス固有のビットマスクを使用して、マルチキャストトラフィックを受信する最適なルートを選択できます。

サービス フロー属性機能を使用すると、「サービス フロー属性マスク」と名付けられた DOCSIS 3.0 構造に基づいて転送インターフェイスを選択できます。すべてのインターフェイスには、そのインターフェイスの属性を表す属性ビット マスクがあります。グループ QoS 設定で指定したマルチキャスト サービス クラスには、必須属性と禁止属性のビット マスクが含まれます。ボンディングされた CM が複数のボンディング グループ（ワイドバンド インターフェイス）をリスニングする場合、サービス クラスとボンディング グループの固有のビット マスクを使用して、マルチキャスト トラフィックの転送用にこれらのボンディング グループのいずれかを選択できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cableserviceclass** *class-index***name** *name* 例： `Router(config)# cable service class 10 name mcast10`	サービス クラス名を設定します。
ステップ 4	**cableserviceclass** *class-index***downstream** 例： `Router(config)# cable service class 10 downstream`	選択したサービス クラスのダウンストリームを設定します。
ステップ 5	**cableserviceclass** *class-index***max-rate** *maximum-rate* 例： `Router(config)# cable service class 10 max-rate 1000000`	選択したサービスクラスの最大レートを設定します。
ステップ 6	**cableserviceclass** *class-index***min-rate** *minimum-rate* 例： `Router(config)#  cable service class 10 min-rate 100000`	選択したサービスクラスの最小レートを設定します。

	コマンドまたはアクション	目的
ステップ 7	**cableserviceclass** *class-index***req-attr-mask** *required-attribute-mask* 例： `Router(config)# cable service class 10 req-attr-mask 8000000F`	選択したサービス クラスの必須属性マスクを設定します。
ステップ 8	**cableserviceclass** *class-index***forb-attr-mask** *forbidden-attribute-mask* 例： `Router(config)# cable service class 10 forb-attr-mask 7FFFFFF0`	選択したサービス クラス名の禁止属性マスクを設定します。
ステップ 9	**cablemulticastgroup-qos** *number***scn** *service-class-name***aggregate** 例： `Router(config)# cable multicast group-qos 1 scn 10 mcast10 aggregate`	ケーブル マルチキャスト グループ QoS ID、サービス クラス名、およびマルチキャスト値を設定します。
ステップ 10	**cablemulticastqosgroup** *group***priority** *priority* 例： `Router(config)# cable multicast qos group 1 priority 1`	ケーブルMQoSグループを設定し、MQoSコンフィギュレーション モードを開始します。
ステップ 11	**session-range** *session-range mask* 例： `Router(config-mqos)# session-range 230.1.1.1 255.255.255.255`	セッション範囲を指定します。
ステップ 12	**group-qos** *qos* 例： `Router(config-mqos)# group-qos 1`	グループ QoS を指定します。
ステップ 13	**exit** 例： `Router(config-mqos)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 14	**interfacebundle** *number* • **ipaddress** *ip mask*	IP アドレス、ヘルパー アドレス、およびMQoSグループを指定したインターフェイス バンドルを設定します。

	コマンドまたはアクション	目的

	• **ippimsparse-mode**
	• **iphelper-address** *helper-address*
	• **cablemulticast-qosgroup** *group*
	
	例：
	`Router(config)# interface Bundle1`
	`Router(config-if)#ip address 40.1.1.1 255.255.255.0`
	`Router(config-if)#ip pim sparse-mode`
	`Router(config-if)#ip helper-address 2.39.16.1`
	`Router(config-if)#cable multicast-qos group 1`	

ステップ 15	**exit** 例： `Router(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。

ステップ 16	**interfacewideband-cable** *slot*/*subslot*/*port*:*wideband-channel*
	• **description** *description*
	• **cablebundle** *number*
	• **cable rf-channel channel-list** *grouplist***bandwidth-percent** *bw-percent*
	• **cabledownstreamattribute-maskattribute-***mask*
	
	例：
	`Router(config)# interface Wideband-Cable1/0/0:0`
	`Router(config-if)# description cable rf-channels channel-list 0-7 bandwidth-percent 20`
	`Router(config-if)# cable bundle 1`
	`Router(config-if)# cable rf-channels channel-list 0-7 bandwidth-percent 20`
	`Router(config-if)# cable downstream attribute-mask 8000000F`
		サービス クラスおよびワイドバンドインターフェイスで指定したビット マスクに基づいて転送するインターフェイスを選択します。

ステップ 17	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。

マルチキャスト DSID 転送ディセーブル モードの設定

ケーブル モデムの MDF を無効にするには、グローバル コンフィギュレーション モードで **cablemulticastmdf-disable** コマンドを使用します。

（注） IGMP SSM マッピングが使用されている場合、BPI+ に基づくマルチキャスト暗号化は、非 MDF ケーブル モデムではサポートされません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cablemulticastmdf-disable[wb-incapable-cm]** 例： `Router(config)# cable multicast mdf-disable`	ケーブル モデムの MDF 機能をディセーブルにします。

ステップ 4	exit
	例：
	`Router(config)# exit`
	`Router#`
		グローバル コンフィギュレーション モードを終了します。

マルチキャスト レプリケーション セッションのグローバル設定

次のコマンドを使用してマルチキャスト レプリケーションセッションの最大数をグローバルに設定し、L2 転送インターフェイスごとに値を設定します。

オペレータが最大数の値を設定しない場合、すべてのL2転送インターフェイスに対してデフォルトで値0が設定され、キャッシュ機能が無効になります。Cisco cBR はマルチキャスト レプリケーション セッションをキャッシュしません。

たとえば、値が 10 から 0 に変更されると、現行のキャッシュがすべてクリアされます。値の範囲は、0 ～ 500 です。

次に、キャッシュの最大数を 0 に設定する例を示します。

```
enable
configure terminal
cable multicast ses-cache 0
```

次に、現在の値を変更する例を示します。

```
enable
configure terminal
 [no|default] cable multicast ses-cache <0-500>
```

転送インターフェイスのマルチキャスト レプリケーション セッションの設定

L2転送インターフェイスごとにマルチキャスト レプリケーションセッションを有効にするには、次の手順に従います。

最大数の値の範囲は 0 ～ 500 です。たとえば、値が 10 から 0 に変更されると、現行のキャッシュがすべてクリアされます。

インターフェイスに設定されている値がシステムの値よりも優先されます。次に、転送インターフェイスでセッション キャッシュを設定し、Cisco cBR にシステムの値を使用させる例を示します。

```
enable
configure terminal
interface wideband-Cable {slot /subslot /controller :wideband-channel}
[no|default] cable multicast ses-cache
```

次に、インターフェイスのキャッシュの最大数を設定する例を示します。

```
enable
configure terminal
interface integrated-Cable {slot/subslot/port:rf-channel}
cable multicast ses-cache 500
```

次に、インターフェイスに対して値 0 を設定する例を示します。

```
enable
configure terminal
interface integrated-Cable {slot/subslot/port:rf-channel}
no cable multicast ses-cache
```

マルチキャスト レプリケーションのキャッシュのクリア

すべて、または特定の L2 転送インターフェイスのマルチキャスト レプリケーション セッションをクリアするには、次のコマンドを使用します。システムにより、すべてのL2転送インターフェイスまたは特定の L2 インターフェイスに関する現行のキャッシュ エントリがすべて削除されます。

```
enable
clear cable multicast ses-cache [interface xxx | all | counter]
```

DOCSIS 3.0 マルチキャスト サポートのモニタリング方法

DOCSIS 3.0 マルチキャスト サポート機能をモニタリングするには、次の手順を使用します。

基本的なマルチキャスト転送の確認

基本的なマルチキャスト転送の設定パラメータを確認するには、次の例のように **showipmroute** コマンドを使用します。

```
Router# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       V - RD & Vector, v - Vector
Outgoing interface flags: H - Hardware switched, A - Assert winner
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 230.1.1.1), 00:00:03/00:02:55, RP 30.1.1.1, flags: S
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Bundle1, Forward/Sparse, 00:00:03/00:02:55, H
(*, 224.0.1.40), 00:12:02/00:02:19, RP 30.1.1.1, flags: SJCL
  Incoming interface: Null, RPF nbr 0.0.0.0
  Outgoing interface list:
    Bundle1, Forward/Sparse, 00:12:02/00:02:19
```

IGMPv3 に基づいて指定した仮想インターフェイス バンドルのマルチキャスト情報を確認するには、次の例のように **showcablebundlemulticast** コマンドを使用します。

```
Router# show cable bundle 1 multicast

CableBundle Interface Source IP  Multicast IP    MAC Address
1    Bundle1.1 *       230.1.1.1    0100.5e00.0001
```

IGMPv3 に基づいて指定した仮想インターフェイス バンドルの MAC 転送テーブルを確認するには、次の例のように **showcablebundleforwarding** コマンドを使用します。

```
Router# show cable bundle 1 forwarding

MAC address Interface Flags Location link sublink
00c0.5e01.0203 Cable8/0/0 3 64E5BF60 0 64E5BE00
00c0.5e01.0203 Cable7/0/0 3 64E5BE00 0 0
00c0.5e01.0101 Cable8/0/0 3 64E5BEE0 0 64E5BE40
```

マルチキャスト DSID 転送の確認

DSID データベースの内容をすべて確認するには、次の例に示すように **showcablemulticastdsid** コマンドを使用します。

```
Router# show cable multicast dsid
Multicast Group    : 230.1.2.3
         Source    : *
```

```
        IDB       : Bu2          Interface: Mo1/1/0:0   Dsid: 0x1F078
        StatIndex : 2            SAID: DEFAULT
Multicast Group   : 230.1.2.3
        Source    : *
        IDB       : Bu2          Interface: Mo1/1/0:0   Dsid: 0x1F078
        StatIndex : 3            SAID: 8196
Multicast Group   : 230.1.2.3
        Source    : *
        IDB       : Bu2          Interface: Mo1/1/0:0   Dsid: 0x1F078
```

StatIndex:4SAID:8197

データベースの内容をすべて確認するには、次の例に示すように **showcablemulticastdb** コマンドを使用します。

Router# **showcablemulticastdb**

```
interface : Bundle1
Session (S,G) : (*,230.1.1.1)
Fwd Intfc Sub Intfc Host Intfc CM Mac Hosts
Wi1/1/0:0 Bundle1 Ca5/0/0 0018.6852.8056 1
```

登録済み CM および未登録 CM の情報を確認するには、次の例に示すように **show cable modem verbose** コマンドを使用します。

Router# **showcablemodem0010.7bb3.fcd1verbose**

```
MAC Address : 00C0.7bb3.fcd1
IP Address : 10.20.113.2
Prim Sid : 1
QoS Profile Index : 6
Interface : C5/0/U5
sysDescr : Vendor ABC DOCSIS 2.0 Cable Modem
Upstream Power : 0 dBmV (SNR = 33.25 dBmV)
Downstream Power : 0 dBmV (SNR = ----- dBmV)
Timing Offset : 1624
Initial Timing Offset : 2812
Received Power : 0.25
MAC Version : DOC1.0
Qos Provisioned Mode : DOC1.0
Enable DOCSIS2.0 Mode : Y
Phy Operating Mode : atdma
Capabilities : {Frag=N, Concat=N, PHS=N, Priv=BPI}
Sid/Said Limit : {Max Us Sids=0, Max Ds Saids=0}
Optional Filtering Support : {802.1P=N, 802.1Q=N}
Transmit Equalizer Support : {Taps/Symbol= 0, Num of Taps= 0}
Number of CPE IPs : 0(Max CPEs = 1)
CFG Max-CPE : 1
Flaps : 373(Jun 1 13:11:01)
Errors : 0 CRCs, 0 HCSes
Stn Mtn Failures : 0 aborts, 3 exhausted
Total US Flows : 1(1 active)
Total DS Flows : 1(1 active)
Total US Data : 1452082 packets, 171344434 bytes
Total US Throughput : 0 bits/sec, 0 packets/sec
Total DS Data : 1452073 packets, 171343858 bytes
Total DS Throughput : 0 bits/sec, 0 packets/sec
Active Classifiers : 0 (Max = NO LIMIT)
DSA/DSX messages : reject all
Dynamic Secret : A3D1028F36EBD54FDCC2F74719664D3F
Spoof attempt : Dynamic secret check failed
Total Time Online : 16:16
```

明示的なトラッキング機能の確認

明示的なトラッキング情報を確認するには、次の例に示すように **showcablemulticastdb** コマンドを使用します。

Router# **showcablemulticastdb**

```
Interface : Bundle1
Session (S,G) : (*,230.1.1.1)
Fwd Intfc  Sub Intfc  Host Intfc   CM Mac           Hosts
Mo1/1/0:0  Bundle1    Ca5/0/0      0018.6852.8056       1
```

マルチキャスト QoS 機能の確認

ケーブル MQoS の詳細を確認するには、次の例に示すように **showcablemulticastqos** コマンドを使用します。

```
Router# show cable multicast qos ?
group-config Display Multicast Group Config information
group-encryption Display Multicast Group Encryption information
group-qos Display Multicast Group QOS information
Router# show cable multicast qos group-config
Multicast Group Config 1 : Priority 1
Group QOS - 1
Group Encryption - 1
Session Range - Group Prefix 230.0.0.0 Mask 255.0.0.0 Source Prefix 0.0.0.0 Mask 0.0.0.0
Router# show cable multicast qos group-encryption
Multicast Group Encryption 1 : Algorithm 56bit-des
Router# show cable multicast qos group-qos
Group QOS Index Service Class Control Igmp Limit Override
DEFAULT MQOS_DEFAULT Aggregate NO-LIMIT 1 MQOS Aggregate NO-LIMIT
```

特定のケーブル インターフェイスの DOCSIS サービス フローを確認するには、次の例に示すように **showinterfaceservice-flow** コマンドを使用します。

```
Router# show interface cable 6/0 service-flow

Sfid  Sid   Mac Address     QoS Param Index Type    Dir    Curr   Active
BG/CH
                            Prov  Adm  Act                State  Time
4     8193  ffff.ffff.ffff   3     3    3   sec(S)  DS     act    21h57m
5     8196  ffff.ffff.ffff   4     4    4   sec(S)  DS     act    00:17
```

サービス フロー属性の確認

サービス クラス設定でサービス フロー属性の設定を確認するには、次の例のように show cable service-class verbose コマンドを使用します。

```
Router# show cable service-class 10 verbose
Index:                                  10
Name:                                   mcast10
Direction:                              Downstream
Traffic Priority:                       0
Maximum Sustained Rate:                 1000000 bits/sec
Max Burst:                              3044 bytes
Minimum Reserved Rate:                  1000000 bits/sec
Minimum Packet Size                     0 bytes
Admitted QoS Timeout                    200 seconds
Active QoS Timeout                      0 seconds
Required Attribute Mask                 8000000F
Forbidden Attribute Mask                7FFFFFF0
Scheduling Type:                        Undefined
Max Latency:                            0 usecs
Parameter Presence Bitfield:            {0x3148, 0x0}
```

ワイドバンド インターフェイス設定の SF 属性の設定を確認するには、次の例に示すように **show running-config interface** コマンドを使用します。

```
Router# show running-config interface Wideband-Cable 1/0/0:2
interface Wideband-Cable1/0/0:2
 cable bundle 1
 cable bonding-group-id 3
 cable rf-channel 3
 cable downstream attribute-mask 8000000F
end
```

マルチキャスト グループ分類子の確認

グループ分類子ルールの詳細を確認するには、次の例に示すように **showinterfacewideband-cablemulticast-gcr** コマンドを使用します。

```
Router# show interface wideband-cable 1/1/0:0 multicast-gcr
Group Classifier Rules on Wideband-Cable1/1/0:0:
Classifier_id  Group_id  Group_Qos_id  Sid   SFID   ref_count
7              1         1             8196  10     1
8              2         1             8197  11     1
```

トラブルシューティングのヒント

マルチキャスト トラフィックの転送用に選択されたワイドバンドインターフェイスで指定されている RF 周波数を、CM がリスニングできることを確認します。

現行のキャッシュの表示

L2 転送インターフェイスを基準に現在のマルチキャスト レプリケーション セッションを表示するには、このコマンドを使用します。

- インターフェイスを指定しない場合、このコマンドは現行の L2 転送インターフェイスの要約を表示します。要約にはキャッシュ番号が含まれます。
- インターフェイスを指定すると、このコマンドはそのインターフェイスの要約を表示します。キャッシュに関するより詳細な情報を表示するには、verbose オプションを追加します。

```
Router#show cable multicast ses-cache global summary

Global Cache Config: 20
---------------------------------------------------------------------
Fwd             Cache      Cache     Cache      Cache
Intfc           Config     Used      Missed     Hitted
Wi7/0/0:1        10         4          4           12
---------------------------------------------------------------------
Total                            4             4              12

Router# show cable multicast ses-cache global

Fwd Intfc          Sub Intfc              Session (S,G)
Wi7/0/0:0          Bundle1               (30.30.30.30,227.0.0.20)
                   Bundle1               (30.30.30.30,227.0.0.22)

Wi7/0/0:1          Bundle1               (30.30.30.30,226.0.0.20)
                   Bundle1               (30.30.30.30,226.0.0.22)
                   Bundle1               (30.30.30.30,226.0.0.23)
                   Bundle1               (30.30.30.30,226.0.0.21)
```

```
Router#show cable multicast ses-cache interface wi7/0/0:1

Fwd Intfc          Sub Intfc              Session (S,G)
Wi7/0/0:1          Bundle1                (30.30.30.30,226.0.0.20)
                   Bundle1                (30.30.30.30,226.0.0.22)
                   Bundle1                (30.30.30.30,226.0.0.23)
                   Bundle1                (30.30.30.30,226.0.0.21)


Router# show cable multicast ses-cache interface wi7/0/0:1 summary

Global Cache Config: 20
-------------------------------------------------
Fwd             Cache       Cache    Cache      Cache
Intfc             Config      Used     Missed    Hitted
Wi7/0/0:1    10              4           4              12


Router# show cable multicast ses-cache wi8/0/0:0 verbose

Multicast Group    : 232.10.0.8

         Source    : 100.0.0.2

         Act GCRs  : 1

         Interface : Bu255 State: A GI: Bu255  RC: 0

         GCR       : GC   SAID    SFID    Key   GQC    GEn

                     10   8858    24      0     1      0


Multicast Group    : 232.10.0.16

         Source    : 100.0.0.2

         Act GCRs  : 1

         Interface : Bu255  State: A  GI: Bu255  RC: 0

         GCR       : GC   SAID    SFID    Key   GQC    GEn

                     10   8859    25      0     1      0

Total session cache num: 2
```

Cache Missed の値は、キャッシュされたエントリを再利用できないときに新しい参加要求を受け取るたびに増加します。

DOCSIS 3.0 マルチキャスト サポートの設定例

ここでは、次の設定例について説明します。

例：基本的なマルチキャスト転送の設定

（注） 次に、Cisco CMTS がマルチキャスト パケットを転送するのに必要なコマンドを示します。ただし、マルチキャスト QoS および認証機能は、マルチキャスト パケットを適切に転送するためのオプションです。

次の例では、基本的なマルチキャスト転送プロファイルが設定されています。

```
ip multicast-routing
interface TenGigabitEthernet4/1/0
  ip pim sparse-dense-mode
interface Bundle 1
  ip pim sparse-mode
  ip igmp version 3
```

例：マルチキャスト QoS の設定

（注） デフォルトのサービス クラスおよびGQCは、マルチキャスト QoS の設定前に定義する必要があります。

次の例では、マルチキャスト QoS を設定しています。3 つのオブジェクトとテンプレートを定義し、特定のバンドルまたは転送インターフェイスと関連付ける必要があります。オブジェクトには、サービス クラス、グループ QoS 設定（GQC）、グループ設定があります。

```
cable service class 1 name MQOS_DEFAULT
cable service class 1 downstream
cable service class 1 max-rate 10000000
cable service class 1 min-rate 1000000
cable multicast group-qos default scn MQOS_DEFAULT aggregate
cable multicast group-qos 10 scn MQOS single
cable multicast qos group 20 priority 1
application-id 10
session-range 230.0.0.0 255.0.0.0
tos 1 6 15
vrf name1
cable multicast qos group 20 priority 63 global
```

例：サービス フロー属性ベースの転送インターフェイス選択の設定

次の例では、サービス フローの属性ベースの転送インターフェイス選択を設定します。グループ 230.1.1.1 のマルチキャスト トラフィックを送信するには、インターフェイス W6/0/0:0 を選択します。マルチキャスト QoS パラメータはグループ qos 1（サービス クラス「mcast10」から効果的に）から取得します。

```
cable service class 10 name mcast10
cable service class 10 downstream
cable service class 10 max-rate 1000000
cable service class 10 min-rate 1000000
cable service class 10 req-attr-mask 8000000F
cable service class 10 forb-attr-mask 7FFFFFF0
cable multicast group-qos 1 scn mcast10 aggregate
```

```
cable multicast qos group 1 priority 1
session-range 230.1.1.1 255.255.255.255
 group-qos 1
interface Bundle1
 ip address 40.1.1.1 255.255.255.0
 ip pim sparse-mode
 ip helper-address 2.39.16.1
 cable multicast-qos group 1
end
interface Wideband-Cable6/0/0:0
cable bundle 10
cable rf-channels channel-list 0-7 bandwidth-percent 20
cable downstream attribute-mask 8000000F
end
```

例：マルチキャスト レプリケーション セッションの設定

次の例は、L2 転送インターフェイスごとにマルチキャスト レプリケーション セッションを有効にする方法を示しています。

```
enable
conf t
interface xxx

[no|default] cable multicast ses-cache
 cable multicast ses-cache 3
```

その他の参考資料

次に、CMTS ルータでの DOCSIS 3.0 マルチキャスト サポートに関連する資料を説明します。

関連資料

関連項目	マニュアル タイトル
CMTS ケーブル コマンド	http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html『Cisco IOS CMTS Cable Command Reference』
マルチキャスト VPN と DOCSIS 3.0 マルチキャストの QoS	『Multicast VPN and DOCSIS 3.0 Multicast QoS Support』
DOCSIS 3.0 QoS サポート	『DOCSIS WFQ Scheduler on the Cisco CMTS Routers』

標準

規格	タイトル
CM-SP-CMCIv3-I01-080320	『Cable Modem to Customer Premise Equipment Interface Specification』

規格	タイトル
CM-SP-MULPIv3.0-I08-080522	『MAC and Upper Layer Protocols Interface Specification』
CM-SP-OSSIv3.0-I07-080522	『Operations Support System Interface Specification』
CM-SP-PHYv3.0-I07-080522	『Physical Layer Specification』
CM-SP-SECv3.0-I08-080522	『Security Specification』

MIB

MIB[3]	MIB のリンク
• DOCS-MCAST-AUTH-MIB • DOCS-MCAST-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

[3] サポートされている MIB がすべて記載されているわけではありません。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

DOCSIS 3.0 マルチキャスト サポートに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *136*：*DOCSIS 3.0* マルチキャスト サポートに関する機能情報

機能名	リリース	機能情報
DOCSIS 3.0 マルチキャスト サポート	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。
動的マルチキャスト レプリケーション セッション	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 53 章

Cisco cBR での IPv6 セグメント ルーティング

Cisco コンバージド ブロードバンド ルータでは、IPv6 アドレス設定のサブモードとして IPv6 セグメント ルーティングを使用できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *137* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

IPv6 セグメント ルーティングについて

IPv6 セグメント ルーティング（SR）とは、IPv6 転送をサポートする SDN 技術です。SR では、送信元ルータまたはエッジ ルータがトラフィックの送信元ルーティングを実行し、それをセグメ

ント リストとして IPv6 ルーティング拡張ヘッダーにエンコードします。ネットワークがアプリケーションごと、またはフローごとの状態を維持する必要はありません。

ネットワーク内の任意の IPv6 対応ノードは、IPv6 セグメント ルーティング（SRv6）をサポートしなくても、セグメント リスト内の最初のセグメントに SR 拡張ヘッダー付きで IPv6 トラフィックを転送できます。

セグメント リスト内の現行セグメントをホストするノードで、SR 拡張ヘッダーを含むトラフィックの宛先アドレスを変更するように SRv6 が設定され、そのセグメント ID が宛先になります。SRv6 の最終処理の一環として、SR 拡張ヘッダー内の次のセグメント ID がパケットの宛先アドレスに書き込まれ、この新しい宛先アドレスにトラフィックを転送するためにルックアップが実行されます。

セグメント リスト内の最後のセグメントが削除されてトラフィックが最終的な宛先に配信されるまで、SR 拡張ヘッダー内のセグメント ID をホストするノードでこの転送と SRv6 最終処理が続行されます。

IPv6 セグメント ルーティングの設定に関する制限事項

同じインターフェイス上で重複する IPv6 アドレスを設定することは許可されていません。

IPv6 セグメント ルーティングの設定方法

（注） このモジュールで参照されているコマンドの詳細については、「Cisco IOS Master Command List」を参照してください。

cBR での IPv6 セグメント ルーティングの設定

IPv6 セグメント ルーティングを設定するには、次の手順に従います。

1 インタ フェースで IPv6 アドレスを設定する際に、セグメント ルーティング サブモードを開始します。

```
enable
configure terminal
interface type [slot_#/]port_#
ipv6 address ipv6_address_prefix/prefix_length
ipv6 address ipv6_address_prefix/prefix_length segment-routing
```

2 ローカル プレフィックスを SID として定義します。

```
ipv6-sr prefix-sid
exit
```

IPv6 セグメント ルーティングの設定の確認

次に、IPv6 の設定を確認する例を示します。

```
Router#sh run
*Oct 17 13:13:23.975: %SYS-5-CONFIG_I: Configured from console by console
Router#sh run | sec Ether
interface Ethernet0/0
 no ip address
 shutdown
 ipv6 address 2001::2001/64 segment-routing >>>>>>>
  ipv6-sr prefix-sid >>>>>>>
```

セグメント ルーティング用の複数の IPv6 アドレスの設定

同じインターフェイスで SRv6 に対して複数の IPv6 アドレスを設定するには、次のコマンドを使用します。

1. インタ フェースで IPv6 アドレスを設定する際に、セグメント ルーティング サブモードを開始します。

   ```
   enable
   configure terminal
   interface type [slot_#/]port_#
   ipv6 address ipv6_address_prefix/prefix_length segment-routing
   ```

2. ローカル プレフィックスを、SID として定義します。

   ```
   ipv6-sr prefix-sid
   exit
   ```

複数の Ipv6 アドレスでの IPv6 セグメント ルーティング設定の確認

次に、複数の IPv6 アドレスについて SRv6 設定を確認する例を示します。

```
Router#sh run | sec Ether
interface Ethernet0/0
 no ip address
 shutdown
 ipv6 address 2001:db8:110::/64 segment-routing  >>> submode 1
  ipv6-sr prefix-sid
 ipv6 address 2001:db9:111::/64 segment-routing  >>> submode 2
  ipv6-sr prefix-sid
interface Ethernet0/1
 no ip address
 shutdown
interface Ethernet0/2
 no ip address
 shutdown
interface Ethernet0/3
 no ip address
 shutdown
interface Ethernet1/0
 no ip address
 shutdown
interface Ethernet1/1
 no ip address
 shutdown
interface Ethernet1/2
```

プレフィックス SID の無効化

セグメント ID に関連付けられているローカル プレフィックス SID を無効にするには、次のコマンドを使用します。

```
enable
configure terminal
interface type [slot_#/]port_#
ipv6 address ipv6_address_prefix/prefix_length segment-routing
no ipv6-sr prefix-sid
end
```

プレフィックス SID が無効化されているかどうかの確認

次に、プレフィックス SID が無効化されているかどうかを確認する例を示します。

```
Router#sh run | sec Ether
interface Ethernet0/0
 no ip address
 shutdown
 ipv6 address 110::110/64 segment-routing >>> "ipv6-sr prefix sid" is no longer present
ipv6 address 111::111/64 segment-routing
ipv6-sr prefix-sid
```

プレフィックス SID に関する SRv6 の無効化

IPv6 アドレスの SRv6 設定を無効にして IPv6 アドレスを削除するには、次のコマンドを使用します。

```
enable
configure terminal
interface type [slot_#/]port_#
no ipv6 address ipv6_address_prefix/prefix_length segment-routing
end
```

SRv6 が無効化されてプレフィックス SID が削除されているかどうかの確認

次に、SRv6が無効化されてプレフィックスSIDが削除されているかどうかを確認する例を示します。

```
Router#sh run |
*Oct 17 13:17:51.523: %SYS-5-CONFIG_I: Configured from console by console
Router#sh run | sec Ether
interface Ethernet0/0
 no ip address
 shutdown
 ipv6 address 110::110/64 segment-routing
ipv6 address 111::111/64 segment-routing is entirely removed from ethernet0/0
```

設定例

ここでは、IPv6 セグメント ルーティングの例を記載します。

例：Cisco cBR での IPv6 セグメント ルーティングの設定

```
Router#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Router(config)#inter Ether0/0
Router(config-if)#ipv6 address 110::110/64 ?
  anycast
  eui-64
  segment-routing
  <cr>
Router(config-if)#ipv6 address 110::110/64 segment-routing
Router(config-if-sr-ipv6)#?
ipv6 address segment-routing mode configuration commands:
  default  Set a command to its defaults
  exit     Exit from SR submode
  ipv6-sr  Request options specific to IPV6 segment-routing
  no       Negate a command or set its defaults
Router(config-if-sr-ipv6)#ipv6-sr ?
  prefix-sid  Set host prefix as IPv6 SR identifier prefix-sid
Router(config-if-sr-ipv6)#ipv6-sr prefix-sid
Router(config-if-sr-ipv6)#exit
Router(config-if)#exit
Router(config)#exit
Router#
```

例：SRv6 用の複数の IPv6 アドレスの設定

```
Router#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#inter Ether 0/0
Router(config-if)# ipv6 address 110::110/64 segment-routing
Router(config-if)# ipv6 address 111::111/64 segment-routing
Router(config-if-sr-ipv6)#ipv6-sr prefix-sid
Router(config-if-sr-ipv6)#end
```

例：プレフィックス SID の無効化

```
Router#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#inter Ether0/0
Router(config-if)#inter Ether0/0
Router(config-if)#ipv6 address 110::110/64 segment-routing
Router(config-if-sr-ipv6)#no ipv6-sr prefix-sid
Router(config-if-sr-ipv6)#end
```

例：アクティブなプレフィックス SID を持つ SR の無効化

```
Router#conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#inter Ether0/0
Router(config-if)#no ipv6 address 111::111/64 segment-routing
Router(config-if)#end
```

IPv6 セグメント ルーティングの機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *138* : *IPv6* セグメント ルーティングの機能情報

機能名	リリース	機能情報
IPv6 セグメント ルーティング	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 VII 部

レイヤ 3 構成：IP アクセス コントロール リスト

- ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張, 1093 ページ

第 54 章

IP アクセス コントロール リスト

アクセス コントロール リスト（ACL）は、パケット フィルタリングを実行して、ネットワークを介して移動するパケットと移動先を制御します。パケット フィルタリングによって、ネットワーク トラフィックを制限し、ユーザおよびデバイスのネットワークに対するアクセスを制限し、トラフィックがネットワークから外部に送信されるのを防ぐことで、セキュリティを実現します。IP アクセス リストによって、スプーフィングやサービス妨害攻撃の可能性を軽減し、ファイアウォールを介した動的で一時的なユーザ アクセスが可能になります。

また、IP アクセス リストは、セキュリティ以外の用途にも使用できます。たとえば、帯域幅制御、ルーティング アップデートのコンテンツの制限、ルートの再配布、ダイヤルオンデマンド（DDR）呼び出しのトリガー、デバッグ出力の制限、Quality of Service（QoS）機能のトラフィックの識別と分類などです。このモジュールでは、IP アクセス リストの概要について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *139* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

IP アクセス リストに関する情報

IP アクセス リストの利点

アクセスコントロールリスト（ACL）は、ネットワークを通過するパケットのフローを制御するためにパケットフィルタリングを実行します。パケットフィルタリングによってユーザおよびデバイスのネットワークに対するアクセスを制限し、セキュリティの手段として利用できます。アクセスリストによってトラフィック数を減らすことで、ネットワークリソースを節約できます。アクセス リストを使用した場合の利点は次のとおりです。

- 着信 rsh および rcp 要求を認証する：アクセス リストは、デバイスへのアクセスを制御するように構成された認証データベース内のローカル ユーザ、リモート ホスト、およびリモート ユーザの識別を簡素化できます。Cisco ソフトウェアは認証データベースを使用して、リモート シェル（rsh）およびリモート コピー（rcp）プロトコルの着信要求を受け取ることができます。
- 不要なトラフィックまたはユーザをブロックする：アクセス リストを使用すると、インターフェイス上の着信パケットまたは発信パケットをフィルタできるため、送信元アドレス、宛先アドレス、またはユーザ認証に基づいてネットワークへのアクセスを制御できます。また、アクセス リストを使用して、デバイス インターフェイスで転送またはブロックするトラフィックの種類を決定することもできます。たとえば、電子メール トラフィックはネットワークでルーティングすることを許可し、すべての Telnet トラフィックはネットワークに入ることをブロックするようにアクセス リストを使用できます。
- vty へのアクセスを制御する：インバウンド vty（Telnet）でのアクセス リストは、デバイスへの回線にアクセスできるユーザを制御できます。アウトバウンド vty でのアクセス リストは、デバイスからの回線が到達可能な宛先を制御できます。
- QoS 機能のトラフィックを特定または分類する：アクセス リストは、Weighted Random Early Detection（WRED）および専用アクセス レート（CAR）の IP プレシデンスを設定することで、輻輳回避を提供します。また、クラスベース均等化キューイング（CBWFQ）、プライオリティ キューイング、カスタム キューイングのために輻輳管理を提供します。
- debug コマンド出力を制限する：アクセス リストは、IP アドレスやプロトコルに基づいて debug 出力を制限できます。
- 帯域幅制御を提供する：低速リンクでのアクセスリストはネットワークでの過剰なトラフィックを防止できます。
- NAT 制御を提供する：アクセス リストによって、ネットワーク アドレス変換（NAT）が変換するアドレスを制御できます。
- DoS 攻撃の可能性を低減する：アクセス リストは、サービス妨害（DoS）攻撃の可能性を低減させます。ホストからのトラフィック、ネットワーク、またはネットワークにアクセスするユーザを制御するように IP 発信元アドレスを指定します。TCP インターセプト機能を設定することで、接続に関する要求でサーバにフラッディングが発生しないようにすることができます。

- ルーティング アップデートの内容を制限する：アクセス リストによって、ネットワーク内で送信、受信、または再配布されるルーティング アップデートを制御できます。
- ダイヤルオンデマンド コールをトリガーする：アクセス リストによって、ダイヤルおよび切断条件を適用できます。

アクセス リストを使用する必要がある境界ルータおよびファイアウォール ルータ

アクセス リストを設定する理由は多数あります。たとえば、アクセス リストを使用して、ルーティングアップデートのコンテンツを制限したり、トラフィック フローを制御したりできます。アクセス リストを設定する最も重要な理由の 1 つは、ネットワークに対するアクセスを制御することで、ネットワークに基本レベルのセキュリティを提供することです。ルータでアクセス リストを設定しない場合、ルータを通過するすべてのパケットは、ネットワークのすべての部分で許可される可能性があります。

アクセス リストで、ネットワークの一部に対してアクセスを許可するホストと、同じ領域に対してアクセスを禁止するホストを設定できます。以下の図では、適切なアクセス リストをルータのインターフェイスに適用することで、ホスト A は Human Resources ネットワークに対するアクセスが許可され、ホスト B は Human Resources ネットワークに対するアクセスが禁止されます。

ファイアウォールルータにはアクセスリストを使用する必要があります。多くの場合、ファイアウォール ルータは内部ネットワークと外部ネットワーク（インターネット）の間に配置されます。また、ネットワークの 2 つの部分の間に配置されたルータにアクセス リストを使用して、内部ネットワークの特定の部分に発着信するトラフィックを制御できます。

アクセス リストのセキュリティ上の利点を実現するために、場合によっては、少なくとも境界ルータでアクセス リストを設定する必要があります。境界ルータとは、ネットワークのエッジにあるルータです。このようなアクセス リストは、外部ネットワークから、または内部ネットワークのあまり制御されていない領域から、内部ネットワークの機密性が高い領域に対する基本的なバッファとして機能します。このような境界ルータでは、ルータ インターフェイスに設定されている各ネットワーク プロトコルに合わせてアクセスリストを設定する必要があります。インバウンドトラフィック、アウトバウンドトラフィック、またはその両方がインターフェイスでフィルタされるように、アクセス リストを設定できます。

アクセスリストは個々のプロトコルベースで定義されます。つまり、各プロトコルのトラフィック フローを制御する場合、インターフェイスでイネーブルにするプロトコルごとにアクセスリストを定義する必要があります。

アクセス リストの定義

アクセスコントロールリスト（ACL）は、ネットワークを通過するパケットの動きを制御するためにパケットフィルタリングを実行します。パケットフィルタリングは、ネットワークへのトラフィックのアクセスを限定し、ユーザおよびデバイスのネットワークに対するアクセスを制限し、トラフィックがネットワークから流出するのを防ぐことで、セキュリティを提供します。IP アクセス リストによって、スプーフィングやサービス妨害攻撃の可能性を軽減し、ファイアウォールを介した動的で一時的なユーザ アクセスが可能になります。

また、IP アクセス リストは、セキュリティ以外の用途にも使用できます。たとえば、帯域幅制御、ルーティング アップデートのコンテンツの制限、ルートの再配布、ダイヤルオンデマンド（DDR）呼び出しのトリガー、デバッグ出力の制限、Quality of Service（QoS）機能のトラフィックの識別と分類などです。

アクセス リストは、少なくとも 1 つの **permit** ステートメント、および任意の 1 つまたは複数の **deny** ステートメントで構成される順次リストです。IP アクセス リストの場合、これらのステートメントは IP アドレス、上位層の IP プロトコルなどの IP パケットのフィールドに適用できます。

アクセス リストは名前または番号で識別および参照されます。アクセス リストはパケット フィルタとして動作し、各アクセス リストに定義されている条件に基づいてパケットがフィルタされます。

アクセス リストを構成した後でアクセス リストを有効にするには、アクセス リストをインターフェイスに適用するか（**ipaccess-group** コマンドを使用）、vty に適用するか（**access-class** コマンドを使用）、またはアクセス リストを許容するあらゆるコマンドでアクセス リストを参照する必要があります。複数のコマンドから同じアクセス リストを参照できます。

次の構成では、branchoffices という名前の IP アクセス リストが 10 ギガビット イーサネット インターフェイス 4/1/0 上で構成され、着信パケットに適用されます。発信元アドレスとマスクのペアで指定されているネットワーク以外は、10 ギガビット イーサネット インターフェイス 4/1/0 にアクセスできません。ネットワーク 172.16.7.0 上の送信元から発信されるパケットの宛先に、制限はありません。ネットワーク 172.16.2.0 上の送信元から発信されるパケットの宛先は、172.31.5.4 にする必要があります。

```
ip access-list extended branchoffices
 10 permit 172.16.7.0 0.0.0.3 any
 20 permit 172.16.2.0 0.0.0.255 host 172.31.5.4
!
interface tengigabitethernet 4/1/0
 ip access-group branchoffices in
```

アクセス リストのルール

アクセス リストには、次のルールが適用されます。

- 1 つのインターフェイス、1 つのプロトコル、1 つの方向につき、許可されるアクセス リストは 1 つだけです。
- アクセス リストには少なくとも 1 つの **permit** ステートメントが含まれる必要があります。そうしないと、ネットワークに入るすべてのパケットが拒否されます。
- アクセス リスト条件または一致基準の構成順序は重要です。パケットを転送するかブロックするかを決定するときに、Cisco ソフトウェアは、それぞれの条件ステートメントに対してステートメントの作成順にパケットをテストします。一致が見つかると、条件ステートメントはそれ以上チェックされません。同じ **permit** または **deny** ステートメントでも、順序が異なる場合、ある状況では通過し、別の状況では拒否されるパケットが生じる可能性があります。
- アクセス リストを名前によって参照したときに、そのアクセス リストが存在しない場合は、すべてのパケットが通過します。インターフェイスまたはコマンドに空のアクセス リストを適用すると、ネットワークに対するすべてのトラフィックが許可されます。

- 標準のアクセス リストと拡張のアクセス リストの名前は同じにできません。
- パケットが発信インターフェイスにルーティングされる前に、着信アクセス リストがパケットを処理します。ネットワークへのパケット アクセスを拒否するフィルタ条件がある着信アクセス リストは、ルーティング ルックアップ時のオーバーヘッドを削減します。構成されたフィルタ基準に基づいてネットワークへのアクセスを許可されたパケットはルーティング処理されます。着信アクセス リストの場合、**permit** ステートメントを構成するとパケットは受信後に処理され、**deny** ステートメントを構成するとパケットは破棄されます。
- 発信アクセス リストの場合、パケットの処理後にデバイスから送信されます。着信パケットは発信インターフェイスにルーティングされてから、発信アクセス リストで処理されます。発信アクセス リストの場合、**permit** ステートメントを構成するとパケットは出力バッファに送信され、**deny** ステートメントを構成するとパケットは破棄されます。
- アクセス リストで、デバイスに到達するトラフィック、またはデバイス経由で送信されるトラフィックは制御できますが、デバイスが送信元のトラフィックは制御できません。

IP アクセス リストを作成する際に役立つヒント

意図しない結果を回避し、より効率的で有効なアクセス リストを作成するために役立つヒントを紹介します。

- アクセス リストを作成してから、インターフェイス（または別の対象）に適用します。その理由は、存在しないアクセス リストをインターフェイスに適用してから、アクセス リストを設定すると、最初のステートメントが有効になり、それに続く暗黙の **deny** ステートメントによって即時のアクセスに問題が発生するおそれがあるためです。
- アクセス リストを設定してから適用するもう 1 つの理由は、空のアクセス リストが適用されたインターフェイスはすべてのトラフィックを許可するためです。
- すべてのアクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。そうでない場合、すべてのパケットは拒否され、トラフィックはまったく通過しません。
- まだ拒否されていないその他のパケットすべてを許可する場合、ステートメント **permitanyany** を使用します。ステートメント **permitanyany** を使用すると、実質的に、アクセス リストの末尾にある暗黙の deny ステートメントでその他すべてのパケットが拒否されることを防ぎます。最初のアクセス リスト エントリは、**permitanyany** にしないでください。すべてのトラフィックが通過し、以降のテストに到達するパケットがなくなります。**permitanyany** を指定すると、まだ拒否されていないすべてのトラフィックが通過します。
- すべてのアクセス リストは、暗黙の **deny** ステートメントで終わりますが、明示的な **deny** ステートメント（たとえば、**denyipanyany** など）を使用することを推奨します。ほとんどのプラットフォームでは、**showaccess-list** コマンドを発行して拒否されるパケット数を表示し、アクセス リストが許可していないパケットに関する詳細情報を調査できます。明示的な **deny** ステートメントで拒否されたパケットのみがカウントされます。これは、明示的な **deny** ステートメントによって、より詳細なデータが生成されるためです。
- アクセス リストの作成中、または作成後に、エントリを削除する場合があります。

- 番号付きアクセスリストからはエントリを削除できません。削除しようとすると、アクセス リスト全体が削除されます。エントリを削除する必要がある場合、アクセス リスト全体を削除してから最初から作り直す必要があります。
- 名前付きアクセス リストからはエントリを削除できます。**nopermit** または **nodeny** コマンドを使用して、該当するエントリを削除します。

- 個々のステートメントの用途をひと目で確認および理解しやすくするために、**remark** コマンドを使用して、ステートメントの前後に役立つ注記を書き込むことができます。
- 特定のホストまたはネットワークに対するアクセスを拒否し、そのネットワークまたはホストの誰かがアクセスしようとしたかどうかを検出する場合、対応する **log** ステートメントを指定した **deny** キーワードを含めます。それによって、その送信元からの拒否されたパケットがログに記録されます。
- このヒントは、アクセスリストの配置に適用されます。リソースを保存しようとすると、着信アクセス リストでは常にフィルタ条件を適用した後に、ルーティング テーブルの検索を行います。発信アクセス リストではフィルタ条件を適用する前に、ルーティング テーブルの検索を行います。

名前付きまたは番号付きアクセス リスト

すべてのアクセスリストは、名前または番号で識別されます。名前付きアクセスリストは、番号付きアクセス リストよりも便利です。タスクを思いだしやすく関連性がある、わかりやすい名前を指定できるためです。名前付きアクセス リストでは、ステートメントの順序を変更したり、ステートメントを追加したりできます。

名前付きアクセスリストは、番号付きアクセスリストではサポートされない次の機能をサポートします。

- IP オプションのフィルタリング
- 非隣接ポート
- TCP フラグ フィルタリング
- **nopermit** または **nodeny** コマンドでのエントリの削除

（注） 番号付きアクセス リストを受け入れるコマンドの中には、名前付きアクセス リストを受け入れないコマンドがあります。たとえば、vty には番号付きアクセス リストだけを使用します。

標準または拡張アクセス リスト

すべてのアクセス リストは、標準アクセス リストまたは拡張アクセス リストです。送信元アドレスのみをフィルタする予定の場合、より簡易な標準アクセス リストで十分です。送信元アドレス以外のアドレスをフィルタする場合、拡張アクセス リストが必要です。

- 名前付きアクセス リストは、**standardextendedipaccess-list** コマンド構文内の standard または extended に基づいて、標準か拡張として指定されます。
- 番号付きアクセス リストは、**access-list** コマンド構文に基づいて、標準か拡張として指定されます。標準 IP アクセス リストには 1 ～ 99 または 1300 ～ 1999 の番号が付けられ、拡張 IP アクセス リストには 100 ～ 199 または 2000 ～ 2699 の番号が付けられます。標準 IP アクセス リストの範囲は、当初は 1 ～ 99 のみでしたが、1300 ～ 1999 の範囲に拡張されました（間の番号は他のプロトコルに割り当てられました）。拡張アクセス リストの範囲も同様に拡張されました。

標準アクセス リスト

標準アクセス リストは、パケットの送信元アドレスのみをテストします（ただし 2 つの例外があります）。標準アクセス リストは送信元アドレスをテストするため、宛先の近くでトラフィックをブロックする際には効率的です。標準アクセス リストのアドレスが送信元アドレスではない例外が 2 つあります。

- アウトバウンド VTY アクセス リストでは、誰かが Telnet を実行しようとすると、アクセス リストエントリのアドレスは、送信元アドレスではなく宛先アドレスとして使用されます。
- ルートをフィルタする場合、送信元アドレスではなくアドバタイズされたネットワークがフィルタされます。

拡張アクセス リスト

拡張アクセス リストは、任意の場所のトラフィックをブロックするために適しています。拡張アクセス リストは、送信元アドレス、宛先アドレス、およびその他の IP パケット データをテストします。たとえば、プロトコル、TCP または UDP ポート番号、タイプ オブ サービス（ToS）、優先順位、TCP フラグ、IP オプションなどです。また、拡張アクセス リストには、次のように標準アクセス リストにはない機能があります。

- IP オプションのフィルタリング
- TCP フラグのフィルタリング
- パケットの非初期フラグメントのフィルタリング（「Refining an IP Access List」モジュールを参照してください）

（注） 拡張アクセス リストの対象となるパケットは、自律的に切り替えられません。

アクセスを制御するためにフィルタできる IP パケット フィールド

拡張アクセス リストを使用すると、IP パケットに含まれる次の任意のフィールドについてフィルタできます。送信元アドレスおよび宛先アドレスは、アクセス リストの基礎として最もよく指定される 2 つのフィールドです。

- 送信元アドレス - 特定のネットワーキング デバイスまたはホストから送信されるパケットを制御するために、送信元アドレスを指定します。
- 宛先アドレス - 特定のネットワーキング デバイスまたはホストに対して送信されるパケットを制御するために、宛先アドレスを指定します。
- プロトコル -- キーワード **eigrp**、**gre**、**icmp**、**igmp**、**ip**、**ipinip**、**nos**、**ospf**、**tcp**、または **udp** によって示される、または 0～255 の範囲の整数（インターネット プロトコルを表します）によって示されたIPプロトコルを指定します。トランスポート層プロトコル（**icmp**、**igmp**、**tcp**、または **udp**）を指定すると、コマンドは、固有の構文になります。
  - ポートおよび非隣接ポート - ポート名またはポート番号で TCP または UDP ポートを指定します。ポート番号に非隣接ポート番号は指定できません。ポート番号は、Telnet トラフィックや HTTP トラフィックなどをフィルタする際に有効です。
  - TCP フラグ - TCP パケットに設定された任意のフラグまたはすべてのフラグにパケットが一致することを指定します。特定のフラグについてフィルタすることで、不正な同期パケットを回避できます。
- IP オプション - IP オプションを指定します。IP オプションに基づいてフィルタする理由の 1 つは、IP オプションを含む偽造パケットでルータが飽和状態にならないようにするためです。

アクセス リストのアドレスに対するワイルドカード マスク

アドレス フィルタリングでは、アクセス リスト エントリ内のアドレス ビットとアクセス リストに送信されるパケットを比較するときに、対応するIPアドレスを確認するか無視するかをソフトウェアに示すために、ワイルドカードマスクを使用します。注意してワイルドカードマスクを設定することで、許可または拒否テストのために 1 つまたは複数の IP アドレスを指定できます。

IP アドレス ビット用のワイルドカード マスクでは、数値 1 と数値 0 を使用して、対応する IP アドレス ビットをどのように扱うかを指定します。1 と 0 は、サブネット（ネットワーク）マスクで意味する内容が対照的なため、ワイルドカード マスクは逆マスクとも呼ばれます。

- ワイルドカード マスク ビット 0 は、対応するビット値を確認することを示します。ビット値は一致する必要があります。
- ワイルドカード マスク ビット 1 は、対応するビット値を無視することを示します。ビット値が一致する必要はありません。

アクセス リスト ステートメントの送信元アドレスまたは宛先アドレスでワイルドカード マスクを指定しない場合、0.0.0.0（すべての値が一致する必要があることを示します）という暗黙的なワイルドカード マスクが想定されます。

サブネット マスクでは、ネットワークとサブネットを示す隣接ビットをマスクにする必要がありますが、それとは異なり、ワイルドカード マスクではマスクに非隣接ビットを使用できます。

次の表に、アクセスリストのIPアドレスおよびマスクと、それに一致すると見なされる対応するアドレスの例を示します。

表 *140* : *IP* アドレス、ワイルドカード マスク、および一致する結果の例

アドレス	ワイルドカード マスク	一致する結果
0.0.0.0	255.255.255.255	すべてのアドレスはアクセス リスト条件に一致します
172.18.0.0/16	0.0.255.255	ネットワーク 172.18.0.0
172.18.5.2/16	0.0.0.0	ホスト 172.18.5.2 のみが一致します
172.18.8.0	0.0.0.7	サブネット 172.18.8.0/29 のみが一致します
172.18.8.8	0.0.0.7	サブネット 172.18.8.8/29 のみが一致します
172.18.8.15	0.0.0.3	サブネット 172.18.8.15/30 のみが一致します
10.1.2.0	0.0.252.255（マスクの非隣接ビット）	10.1.2.0 ～ 10.1.254.0 に含まれる偶数のネットワークに一致します

アクセス リストのシーケンス番号

IP アクセス リスト エントリにシーケンス番号を適用する機能によって、アクセス リストの変更が簡易になります。IP アクセス リスト エントリ シーケンス番号機能の前には、アクセス リスト内のエントリの位置を指定する方法はありませんでした。以前は、既存のリストの途中にエントリを挿入する場合、目的の位置の後にあるすべてのエントリを削除してから、新しいエントリを追加し、削除したすべてのエントリを再入力する必要がありました。これは手間がかかり、エラーが起こりやすい方法です。

この新しい機能を使用すると、アクセスリストエントリにシーケンス番号を追加し、順序を変更することができます。新しいエントリを追加する場合、アクセス リストの目的の位置に挿入されるようにシーケンス番号を指定します。必要に応じて、アクセス リストの現在のエントリを並べ替えて、新しいエントリを挿入できる場所を作成できます。

アクセス リストのロギング

Cisco IOS ソフトウェアには、単一の標準または拡張 IP アクセス リスト エントリで許可または拒否されたパケットに関するロギング メッセージ機能があります。つまり、パケットがエントリに一致する場合は常に、パケットに関する情報を提供するロギング メッセージがコンソールに送信

されます。コンソールに記録されるメッセージのレベルは、**loggingconsole** グローバル コンフィギュレーション コマンドで制御されます。

アクセス リスト エントリをトリガーする最初のパケットによって、即時にロギング メッセージが作成され、表示またはロギングされるまで、以降のパケットは 5 分間隔で収集されます。ログ メッセージにはアクセス リスト番号、パケットの許可または拒否に関する状況、パケットの送信元 IP アドレス、および直前の 5 分間に許可または拒否された送信元からのパケット数が示されます。

ただし、**ipaccess-listlog-update** コマンドを使用して、アクセス リストに一致する場合（さらに許可または拒否される場合）に、システムでログ メッセージを生成するパケットの数を設定できます。この手順を実行するのは、5 分間隔よりも短い頻度でログ メッセージを受信する場合です。

注意 *number-of-matches* 引数を 1 に設定すると、ログ メッセージはキャッシングされずにただちに送信されます。この場合、アクセス リストに一致するパケットごとにログ メッセージが発生します。大量のログ メッセージでシステムが過負荷になる可能性があるため、1 に設定することは推奨されません。

ipaccess-listlog-update コマンドを使用する場合でも、5 分タイマーは有効なままなので、各キャッシュ内のメッセージ数に関係なく、5 分が経過すると各キャッシュは空になります。ログ メッセージを送信するタイミングに関係なく、しきい値が指定されていない場合と同様に、ログ メッセージのキャッシュは消去され、カウントは 0 にリセットされます。

（注） ロギング メッセージが多すぎて処理できない場合、または 1 秒以内に処理する必要があるロギング メッセージが複数ある場合、ロギング設備ではロギング メッセージ パケットの一部をドロップすることがあります。この動作によって、ロギング パケットが多すぎてルータがクラッシュすることを回避します。そのため、課金ツールや、アクセス リストと一致する数の正確な情報源としてロギング設備を使用しないでください。

アクセス リスト ロギングの代替方法

ログ オプションを使用した ACL 内のエントリのパケット マッチングは代替のプロセスです。ACL でログ オプションを使用することは推奨されません。Null0 の宛先インターフェイスで NetFlow エクスポートおよびマッチングを使用することを推奨します。これは CEF パスで実行されます。Null0 の宛先インターフェイスは、ACL によってドロップされるすべてのパケット用に設定されます。

その他の IP アクセス リスト機能

標準または拡張アクセス リストを作成する基本手順以外に、次のようにアクセス リストを強化できます。これらの各方法の詳細については、「Refining an Access List」モジュールを参照してください。

- 拡張アクセス リスト内の **permit** または **deny** ステートメントが有効になる日時を指定し、アクセス リストを細かくし、絶対的または定期的な期間に限定することができます。
- 名前付きアクセス リストの作成後は、エントリを追加したり、エントリの順序を変更したりできます（これはアクセス リストのシーケンス番号再割り当てとも呼ばれます）。
- パケットの非初期フラグメントについてフィルタすることで、パケットをフィルタするときにより細かい精度を達成できます。

アクセス リストを適用する場所

アクセス リストは、デバイスの着信または発信インターフェイスに適用できます。アクセス リストを着信インターフェイスに適用すると、インターフェイスで着信するトラフィックが制御され、アクセス リストを発信インターフェイスに適用すると、インターフェイスから発信されるトラフィックが制御されます。

ソフトウェアは、着信インターフェイスでパケットを受信すると、アクセス リストで設定されているステートメントに対してパケットを検査します。アクセス リストがアドレスを許可している場合は、ソフトウェアはパケットを処理します。着信パケットをフィルタリングするためにアクセス リストを適用すると、フィルタリングされたパケットはデバイスに到達する前に廃棄されるため、デバイスのリソースを節約できます。

発信インターフェイスでは、アクセス リストはインターフェイスから転送（送信）されたパケットをフィルタリングします。発信インターフェイスで Rate-Based Satellite Control Protocol（RBSCP）の TCP アクセス コントロール リスト（ACL）を使用して、発信インターフェイスで TCP 確認応答（ACK）を受けるパケットの種類を制御できます。

debug コマンドを使用してアクセス リストを参照し、デバッグ ログの量を制限できます。たとえば、アクセスリストのフィルタリング基準または一致基準に基づいて、デバッグ ログを送信元または宛先のアドレスまたはプロトコルに制限できます。

アクセス リストを使用して、ルーティング アップデート、ダイヤルオンデマンド（DDR）、および Quality of Service（QoS）機能を制御することができます。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IP アクセス リスト コマンド：コマンド構文、コマンドモード、コマンド履歴、デフォルト設定、使用に関する注意事項および例	『Cisco IOS IP Addressing Services Command Reference』

関連項目	マニュアル タイトル
送信元アドレス、宛先アドレス、またはプロトコルに基づくフィルタリング	『ICreating an IP Access List and Applying It to an Interface』モジュール
IP オプション、TCP フラグ、非隣接ポート、または TTL に基づくフィルタリング	『Creating an IP Access List to Filter IP Options, TCP Flags, or Noncontiguous Ports』モジュール

標準

標準と RFC	タイトル
なし	—

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IP アクセス リストに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *141* : *IP* アクセス リストに関する機能情報

機能名	リリース	機能情報
IP アクセス リスト	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 55 章

IP アクセス リストの作成とインターフェイスへの適用

IP アクセス リストには、ネットワークを保護し、Quality of Service（QoS）係数の設定や **debug** コマンド出力の制限などのセキュリティ以外の目標を達成する際に多数の利点があります。ここでは、標準、拡張、名前付き、および番号付き IP アクセス リストの作成方法について説明します。アクセス リストは、名前または番号で参照できます。標準アクセス リストは、IP パケットの送信元アドレスのみに基づいてフィルタできます。拡張アクセス リストは、IP パケットの送信元アドレス、宛先アドレス、および他のフィールドに基づいてフィルタできます。

アクセス リストの作成後に有効にするには、何かに適用する必要があります。ここでは、アクセス リストをインターフェイスに適用する方法について説明します。ただし、アクセス リストにはその他にも多数の用途があり、このモジュールで言及していますが、他のモジュールでも説明しています。多様なテクノロジーについては、他のコンフィギュレーション ガイドを参照してください。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *142*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

IP アクセス リストの作成とインターフェイスへの適用に関する情報

IP アクセス リストを作成する際に役立つヒント

- アクセス リストを作成してから、インターフェイス（または別の対象）に適用します。その理由は、存在しないアクセス リストをインターフェイスに適用してから、アクセス リストを設定すると、最初のステートメントが有効になり、それに続く暗黙の **deny** ステートメントによって即時のアクセスに問題が発生するおそれがあるためです。
- アクセス リストを設定してから適用するもう 1 つの理由は、空のアクセス リストが適用されたインターフェイスはすべてのトラフィックを許可するためです。
- すべてのアクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。そうでない場合、すべてのパケットは拒否され、トラフィックはまったく通過しません。
- ネットワークまたはサブネットのより具体的な参照が、より全般的な参照よりも前に出現するように、アクセス リストを構成します。
- パケットは、ACL の最初の ACE に一致します。したがって、**permitipanyany** はすべてのパケットに一致し、以降のすべての ACES は無視されます。
- すべてのアクセス リストは、暗黙の **deny** ステートメントで終わりますが、明示的な **deny** ステートメント（たとえば、**denyipanyany** など）を使用することを推奨します。ほとんどのプラットフォームでは、**showaccess-list** コマンドを発行して拒否されるパケット数を表示し、アクセス リストが許可していないパケットに関する詳細情報を調査できます。明示的な **deny** ステートメントで拒否されたパケットのみがカウントされます。これは、明示的な **deny** ステートメントによって、より詳細なデータが生成されるためです。
- アクセス リストの作成中、または作成後に、エントリを削除する場合があります。名前付きアクセス リストからはエントリを削除できます。**nopermit** または **nodeny** コマンドを使用して、該当するエントリを削除します。
- 個々のステートメントの用途をひと目で確認および理解しやすくするために、**remark** コマンドを使用して、ステートメントの前後に役立つ注記を書き込むことができます。
- 特定のホストまたはネットワークに対するアクセスを拒否し、そのネットワークまたはホストの誰かがアクセスしようとしたかどうかを検出する場合、対応する **log** ステートメントを指定した **deny** キーワードを含めます。それによって、その送信元からの拒否されたパケットがログに記録されます。
- このヒントは、アクセス リストの配置に適用されます。リソースを保存しようとすると、着信アクセス リストでは常にフィルタ条件を適用した後に、ルーティング テーブルの検索を行います。発信アクセス リストではフィルタ条件を適用する前に、ルーティング テーブルの検索を行います。

アクセス リストの注釈

任意のIPアクセスリストのエントリについて、コメントまたは注釈を含めることができます。アクセス リストの注釈は、アクセス リスト エントリの前後にあるオプションの注釈です。エントリの内容がわかるので、エントリの目的を解釈する必要はありません。各注釈の長さは 100 文字に制限されます。

コメントは、**permit** または **deny** ステートメントの前後どちらにでも配置できます。注釈を追加する場所には一貫性があるようにしてください。注釈が関連する **permit** または **deny** ステートメントの前にある場合と後にある場合とが混在すると、ユーザが混乱する可能性があります。

後続の **deny** ステートメントの機能を説明する注釈の例を次に示します。

```
ip access-list extended telnetting
 remark Do not allow host1 subnet to telnet out
 deny tcp host 172.16.2.88 any eq telnet
```

その他の IP アクセス リスト機能

標準または拡張アクセスリストを作成する基本手順以外に、次のようにアクセスリストを強化できます。これらの各方法の詳細については、『*Refining an IP Access List module*』を参照してください。

- 拡張アクセス リスト内の **permit** または **deny** ステートメントが有効になる日時を指定し、アクセス リストを細かくし、絶対的または定期的な期間に限定することができます。
- 名前付きまたは番号付きアクセスリストの作成後は、エントリを追加したり、エントリの順序を変更したりできます（これはアクセスリストのシーケンス番号再割り当てとも呼ばれます）。
- パケットの非初期フラグメントについてフィルタすることで、パケットをフィルタするときにより細かい精度を達成できます。

IP アクセス リストの作成とインターフェイスへの適用方法

ここでは、名前または番号を使用して、標準または拡張アクセス リストを作成する一般的な方法について説明します。アクセス リストには高い柔軟性があります。この作業では、単純に 1 つの **permit** コマンドと 1 つの **deny** コマンドを使用して、それぞれのコマンド構文を指定します。後は、必要な **permit** および **deny** コマンドの数とその順番を決めるだけです。

（注） このモジュールの最初の 2 つの作業として、1 つのアクセス リストを作成します。適切に機能するように、アクセス リストを適用する必要があります。インターフェイスにアクセス リストを適用する場合は、「インターフェイスへのアクセス リストの適用」タスクを実行します。

送信元アドレスに基づいてフィルタする標準アクセス リストの作成

送信元アドレスのみに基づいてフィルタする場合、簡易な標準アクセス リストで十分です。標準アクセス リストには名前付きと番号付きという 2 種類があります。名前付きアクセス リストを使用すると、番号よりも直感的な名前を使用してアクセス リストを特定できます。また、番号付きアクセス リストよりもサポートする機能が多数です。

送信元アドレスに基づいてフィルタする名前付きアクセス リストの作成

送信元アドレスのみに基づいてフィルタする必要がある場合、標準の名前付きアクセス リストを使用します。この作業では、1 つの **permit** ステートメントと 1 つの **deny** ステートメントを使用しますが、使用する実際のステートメントとその順序は、フィルタまたは許可する内容によって変わります。フィルタリングの目標を達成するように、**permit** および **deny** ステートメントを定義します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**ip access-list standard** *name* 例： `Device(config)# ip access-list standard R&D`	名前を使用して標準 IP アクセス リストを定義し、標準名前付きアクセス リストのコンフィギュレーション モードを開始します。
ステップ 4	**remark** 注記 例： `Device(config-std-nacl)# remark deny Sales network`	（任意）アクセス リスト エントリに関してユーザにわかりやすいコメントを追加します。 • 注釈はアクセス リスト エントリの前または後に指定できます。 • この例の注釈では、後続のエントリがインターフェイスに対する Sales ネットワークのアクセスを拒否することをネットワーク管理者に示しています（こ

	コマンドまたはアクション	目的
		のアクセスリストは後でインターフェイスに適用される想定です）。
ステップ 5	**deny** {*source* [*source-wildcard*] | **any**} [**log**] 例： `Device(config-std-nacl)# deny 172.16.0.0 0.0.255.255 log`	（任意）送信元アドレスおよびワイルドカードマスクに基づいて、指定した送信元を拒否します。 • *source-wildcard* を省略すると、0.0.0.0 というワイルドカードマスクが想定されます（つまり、すべての送信元アドレスに一致します）。 • 必要に応じて、*source source-wildcard* の代わりにキーワード **any** を使用して、送信元および 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。 • この例では、ネットワーク 172.16.0.0 のすべてのホストは、アクセスリストへの合格が拒否されます。 • この例では、送信元アドレスを明示的に拒否し、**log** キーワードを指定しているため、その送信元からのパケットが拒否されるとロギングされます。これは、ネットワークまたはホスト上の誰かがアクセスしようとしたことを通知する方法の 1 つです。
ステップ 6	**remark** 注記 例： `Device(config-std-nacl)# remark Give access to Tester's host`	（任意）アクセスリストエントリに関してユーザにわかりやすいコメントを追加します。 • 注釈はアクセス リスト エントリの前または後に指定できます。 • この注釈は、後続のエントリがインターフェイスに対する Tester のホスト アクセスを許可することをネットワーク管理者に示します。
ステップ 7	**permit** {*source* [*source-wildcard*] | **any**} [**log**] 例： `Device(config-std-nacl)# permit 172.18.5.22 0.0.0.0`	送信元アドレスおよびワイルドカード マスクに基づいて、指定した送信元を許可します。 • 各アクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。ただし、最初のエントリにする必要はありません。 • *source-wildcard* を省略すると、0.0.0.0 というワイルドカードマスクが想定されます（つまり、すべての送信元アドレスに一致します）。

	コマンドまたはアクション	目的
		• 必要に応じて、*source source-wildcard* の代わりにキーワード **any** を使用して、送信元および 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。 • この例では、ホスト 172.18.5.22 がアクセス リストに合格できます。
ステップ 8	アクセス リストの基礎とする送信元の指定が完了するまで、ステップ 4 ～ 7 の手順を繰り返します。	明示的に許可されていないすべての送信元は、アクセス リストの末尾にある暗黙的な **deny** ステートメントで拒否されます。
ステップ 9	**end** 例： `Device(config-std-nacl)# end`	標準の名前付きアクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 10	**showipaccess-list** 例： `Device# show ip access-list`	（任意）現在の IP アクセス リストすべてのコンテンツが表示されます。

送信元アドレスに基づいてフィルタする番号付きアクセス リストの作成

送信元アドレスのみに基づいてフィルタする必要があり、名前付きアクセス リストを使用しない場合、標準の番号付きアクセス リストを設定します。

IP 標準アクセス リストには、1 ～ 99 または 1300 ～ 1999 の番号を付けます。この作業では、1 つの **permit** ステートメントと 1 つの **deny** ステートメントを使用しますが、使用する実際のステートメントとその順序は、フィルタまたは許可する内容によって変わります。フィルタリングの目標を達成するように、**permit** および **deny** ステートメントを定義します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**access-list** *access-list-number permit* {*source* [*source-wildcard*] | **any**} [**log**] 例： `Device(config)# access-list 1 permit 172.16.5.22 0.0.0.0`	送信元アドレスおよびワイルドカードマスクに基づいて、指定した送信元を許可します。 • 各アクセス リストには、少なくとも 1 つの permit ステートメントが必要です。ただし、最初のエントリにする必要はありません。 • 標準 IP アクセス リストには、1 ～ 99 または 1300 ～ 1999 の番号を付けます。 • source-wildcard を省略すると、0.0.0.0 というワイルドカード マスクが想定されます（つまり、すべての送信元アドレスに一致します）。 • 必要に応じて、source source-wildcard の代わりに、キーワード any を使用して、送信元と 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。 • この例では、ホスト 172.16.5.22 がアクセス リストに合格できます。
ステップ 4	**access-list** *access-list-number***deny** {*source* [*source-wildcard*] | **any**} [**log**] 例： `Device(config)# access-list 1 deny 172.16.7.34 0.0.0.0`	送信元アドレスおよびワイルドカードマスクに基づいて、指定した送信元を拒否します。 • *source-wildcard* を省略すると、0.0.0.0 というワイルドカード マスクが想定されます（つまり、すべての送信元アドレスに一致します）。 • 必要に応じて、*source source-wildcard* の代わりに省略形 **any** を使用すると、送信元と 0.0.0.0 255.255.255.255 の送信元ワイルドカードを指定できます。

	コマンドまたはアクション	目的
		• この例では、ホスト 172.16.7.34 はアクセス リストへの合格が拒否されます。
ステップ 5	アクセス リストの基礎とする送信元の指定が完了するまで、ステップ 3 ～ 6 の手順を繰り返します。	明示的に許可されていないすべての送信元は、アクセス リストの末尾にある暗黙的な **deny** ステートメントで拒否されます。
ステップ 6	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 7	**showipaccess-list** 例： `Device# show ip access-list`	（任意）現在の IP アクセス リストすべてのコンテンツが表示されます。

拡張アクセス リストの作成

送信元アドレス以外の要素に基づいてフィルタする場合、拡張アクセス リストを作成する必要があります。拡張アクセス リストには名前付きと番号付きという 2 種類があります。名前付きアクセスリストを使用すると、番号よりも直感的な名前を使用してアクセスリストを特定できます。また、サポートする機能が多数です。

送信元アドレスまたは宛先アドレス以外の要素をフィルタする方法の詳細については、コマンド リファレンス マニュアルの構文の説明を参照してください。

名前付き拡張アクセス リストの作成

送信元アドレス、宛先アドレス、またはアドレスと他の IP フィールドの組み合わせをフィルタする場合、名前付き拡張アクセス リストを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**ip access-list extended** *name* 例： `Device(config)# ip access-list extended acl1`	名前を使用して拡張 IP アクセス リストを定義し、拡張名前付きアクセス リストのコンフィギュレーション モードを開始します。
ステップ 4	**deny***protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# deny ip 172.18.0.0 0.0.255.255 host 172.16.40.10 log`	（任意）ステートメントに指定されたすべての条件に一致するすべてのパケットを拒否します。 • *source-wildcard* または *destination-wildcard* を省略すると、0.0.0.0 のワイルドカード マスクが想定されます。つまり、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。 • 必要に応じて、*source source-wildcard* または *destination destination-wildcard* の代わりにキーワード **any** を使用して、アドレスおよび 0.0.0.0 255.255.255.255 のワイルドカードを指定できます。 • 必要に応じて、キーワード **host** *source* を使用して *source* 0.0.0.0 の送信元および送信元ワイルドカードを示すか、省略形 **host** *destination* を使用して *destination* 0.0.0.0 の宛先および宛先ワイルドカードを示します。 • この例では、すべての送信元のパケットは、宛先ネットワーク 172.18.0.0 へのアクセスが拒否されます。アクセス リストによって許可または拒否されるパケットに関するロギング メッセージは、**loggingfacility** コマンドで設定された機能に送信されます（たとえば、コンソール、端末、syslog）。つまり、パケットがアクセス リストに一致する場合は常に、パケットに関する情報を提供するロギング メッセージが設定された設備に送信されます。コンソールに記録されるメッセージのレベルは **loggingconsole** コマンドで制御されます。
ステップ 5	**permit** *protocol source* [*source-wildcard*] *destination* [*destination-wildcard*] [**option**	ステートメントに指定されたすべての条件に一致するすべてのパケットを許可します。

	コマンドまたはアクション	目的
	option-name] [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# permit tcp any any`	• 各アクセス リストには、少なくとも 1 つの permit ステートメントが必要です。 • *source-wildcard* または *destination-wildcard* を省略すると、0.0.0.0 のワイルドカード マスクが想定されます。つまり、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。 • 必要に応じて、*source source-wildcard* または *destination destination-wildcard* の代わりにキーワード **any** を使用して、アドレスおよび 0.0.0.0 255.255.255.255 のワイルドカードを指定できます。 • この例では、任意の送信元から任意の宛先への TCP パケットが許可されています。 • **log-input** キーワードを使用して、ロギング出力に入力インターフェイス、送信元 MAC アドレス、または仮想回線を含めます。
ステップ 6	アクセス リストの基礎とするフィールドと値の指定が完了するまで、ステップ 4 ～ 7 の手順を繰り返します。	明示的に許可されていないすべての送信元は、アクセス リストの末尾にある暗黙的な **deny** ステートメントで拒否されます。
ステップ 7	**end** 例： `Device(config-ext-nacl)# end`	標準の名前付きアクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。
ステップ 8	**showipaccess-list** 例： `Device# show ip access-list`	（任意）現在の IP アクセス リストすべてのコンテンツが表示されます。

番号付き拡張アクセス リストの作成

送信元アドレス、宛先アドレス、またはアドレスと他の IP フィールドの組み合わせに基づいてフィルタし、名前を使用しない場合、番号付き拡張アクセス リストを作成します。拡張 IP アクセス リストには、100 ～ 199 または 2000 ～ 2699 の番号を付けます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**access-list** *access-list-number* **remark***remark* 例： `Device(config)# access-list 107 remark allow Telnet packets from any source to network 172.69.0.0 (headquarters)`	（任意）アクセス リスト エントリに関してユーザにわかりやすいコメントを追加します。 • 最大 100 文字の注釈をアクセス リスト エントリの前または後に指定できます。
ステップ 4	**access-list***access-list-number* **permit** *protocol*{*source* [*source-wildcard*] | **any**} {*destination* [*destination-wildcard*] | **any**} [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config)# access-list 107 permit tcp any 172.69.0.0 0.0.255.255 eq telnet`	ステートメントに指定されたすべての条件に一致するすべてのパケットを許可します。 • 各アクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。ただし、最初のエントリにする必要はありません。 • 拡張 IP アクセス リストには、100 ～ 199 または 2000 ～ 2699 の番号を付けます。 • *source-wildcard* または *destination-wildcard* を省略すると、0.0.0.0 のワイルドカード マスクが想定されます。つまり、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。 • 必要に応じて、*source source-wildcard* または *destination destination-wildcard* の代わりにキーワード **any** を使用すると、アドレスおよび 0.0.0.0

	コマンドまたはアクション	目的
		255.255.255.255 のワイルドカードを指定できます。 • TCP と他のプロトコルでは、その他の構文も使用できます。複雑な構文の場合、コマンド リファレンスの **access-list** コマンドを参照してください。
ステップ 5	**access-list***access-list-number* **remark***remark* 例： `Device(config)# access-list 107 remark deny all other TCP packets`	（任意）アクセス リスト エントリに関してユーザにわかりやすいコメントを追加します。 • 最大 100 文字の注釈をアクセス リスト エントリの前または後に指定できます。
ステップ 6	**access-list***access-list-number* **deny***protocol* {*source* [*source-wildcard*] | **any**} {*destination* [*destination-wildcard*] | **any**} [**precedence** *precedence*] [**tos** *tos*] [**established**] [**log** | **log-input**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config)# access-list 107 deny tcp any any`	ステートメントに指定されたすべての条件に一致するすべてのパケットを拒否します。 • *source-wildcard* または *destination-wildcard* を省略すると、0.0.0.0 のワイルドカード マスクが想定されます。つまり、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。 • 必要に応じて、*source source-wildcard* または *destination destination-wildcard* の代わりにキーワード **any** を使用すると、アドレスおよび 0.0.0.0 255.255.255.255 のワイルドカードを指定できます。
ステップ 7	アクセス リストの基礎とするフィールドと値の指定が完了するまで、ステップ 3 ～ 6 の手順を繰り返します。	明示的に許可されていないすべての送信元は、アクセス リストの末尾にある暗黙的な **deny** ステートメントで拒否されます。
ステップ 8	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
ステップ 9	**showipaccess-list** 例： `Device# show ip access-list`	（任意）現在の IP アクセス リストすべてのコンテンツが表示されます。

インターフェイスへのアクセス リストの適用

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**interface** *type number* 例： `Device(config)# interface TenGigabitEthernet4/1/0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipaccess-group** {*access-list-number* | *access-list-name*} {**in** | **out**} 例： `Device(config-if)# ip access-group acl1 in`	指定したアクセス リストをインバウンド インターフェイスに適用します。 • 送信元アドレスをフィルタリングするには、インバウンド インターフェイスにアクセス リストを適用します。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPアクセスリストの作成とインターフェイスへの適用に関する設定例

例：ホスト送信元アドレスでのフィルタリング

次の例では、user1 に属するワークステーションが 10 ギガビット イーサネット インターフェイス 4/1/0 へのアクセスを許可され、user2 に属するワークステーションはアクセスを許可されていません。

```
interface TenGigabitEthernet4/1/0
 ip access-group workstations in
!
ip access-list standard workstations
 remark Permit only user1 workstation through
 permit 172.16.2.88
 remark Do not allow user2 workstation through
 deny 172.16.3.13
```

例：サブネット送信元アドレスでのフィルタリング

次の例では、user1 サブネットは 10 ギガビット イーサネット インターフェイス 4/1/0 へのアクセスが許可されていませんが、Main サブネットはアクセスが許可されています。

```
interface TenGigabitEthernet4/1/0
 ip access-group prevention in
!
ip access-list standard prevention
 remark Do not allow user1 subnet through
 deny 172.22.0.0 0.0.255.255
 remark Allow Main subnet
 permit 172.25.0.0 0.0.255.255
```

例：送信元と宛先のアドレスおよび IP プロトコルでのフィルタリング

次の設定例は、2 つのアクセス リストを持つインターフェイスを示します。一方のリストは発信パケット、もう一方のリストは着信パケットに適用されます。Internet-filter という標準アクセス リストは、送信元アドレスに基づいて発信パケットをフィルタします。インターフェイスから発信が許可されるパケットは、送信元が 172.16.3.4 である必要があります。

marketing-group という拡張アクセス リストは、着信パケットをフィルタします。このアクセス リストは、任意の送信元からネットワーク 172.26.0.0 への Telnet パケットを許可し、その他すべての TCP パケットを拒否します。また、ICMP パケットはすべて許可します。1024 未満のポート番号を使用する、任意の送信元からネットワーク 172.26.0 0 への UDP パケットは拒否します。最後に、このアクセスリストはその他すべてのIPパケットを拒否し、そのエントリによって許可または拒否されるパケットのロギングを実行します。

```
interface TenGigabitEthernet4/1/0
 ip address 172.20.5.1 255.255.255.0
 ip access-group Internet-filter out
 ip access-group marketing-group in
!
ip access-list standard Internet-filter
 permit 172.16.3.4
```

```
ip access-list extended marketing-group
 permit tcp any 172.26.0.0 0.0.255.255 eq telnet
 deny tcp any any
 permit icmp any any
 deny udp any 172.26.0.0 0.0.255.255 lt 1024
 deny ip any any
```

例：番号付きアクセス リストを使用した送信元アドレスでのフィルタリング

次の例では、ネットワーク 10.0.0.0 は Class A ネットワークで、2 番目のオクテットでサブネットを指定します。つまり、サブネット マスクは 255.255.0.0 です。ネットワーク 10.0.0.0 アドレスの 3 番目および 4 番目のオクテットで特定のホストを指定します。Cisco IOS-XE ソフトウェアは、アクセス リスト 2 を使用して、サブネット 48 上の 1 つのアドレスを受け入れ、そのサブネット上のその他のアドレスはすべて拒否します。最後の行は、その他すべてのネットワーク 10.0.0.0 サブネット上のアドレスを受け入れることを示します。

```
interface TenGigabitEthernet4/1/0
 ip access-group 2 in
!
access-list 2 permit 10.48.0.3
access-list 2 deny 10.48.0.0  0.0.255.255
access-list 2 permit 10.0.0.0  0.255.255.255
```

例：サブネットへの Telnet アクセスの防止

次の例では、user1 サブネットは、10 ギガビット イーサネット インターフェイス 4/1/0 から Telnet にアクセスできません。

```
interface TenGigabitEthernet4/1/0
 ip access-group telnetting out
!
ip access-list extended telnetting
 remark Do not allow user1 subnet to telnet out
 deny tcp 172.20.0.0 0.0.255.255 any eq telnet
 remark Allow Top subnet to telnet out
 permit tcp 172.33.0.0 0.0.255.255 any eq telnet
```

例：ポート番号を使用した TCP および ICMP に基づくフィルタリング

次の例では、acl1 という名前の拡張アクセス リストの最初の行で、1023 よりも大きい宛先ポートを持つ着信 TCP 接続を許可しています。2 行目で、ホスト 172.28.1.2 の Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）ポートへの着信 TCP 接続を許可しています。最後の行では、エラー フィードバックのための着信 ICMP メッセージを許可しています。

```
interface TenGigabitEthernet4/1/0
 ip access-group acl1 in
!
ip access-list extended acl1
 permit tcp any 172.28.0.0 0.0.255.255 gt 1023
 permit tcp any host 172.28.1.2 eq 25
 permit icmp any 172.28.0.0 255.255.255.255
```

例：SMTP 電子メールと確立済み TCP 接続の許可

インターネットに接続されているネットワークがあり、イーサネット上のホストでインターネット上の任意のホストに対してTCP接続を構成するとします。ただし、専用のメールホストのメール（SMTP）ポートを除き、IP ホストから 10 ギガビット イーサネット上のホストに対する TCP 接続を構成できないようにします。

SMTP は、接続の一端では TCP ポート 25、もう一端ではランダムなポート番号を使用します。接続の存続中は、この同じ 2 つのポート番号が使用されます。インターネットから着信するメールパケットは、25 という宛先ポートを持ちます。アウトバウンドパケットは、ポート番号が予約されています。ルータの背後にあるセキュア システムは、ポート 25 でメール接続を常に受け入れるため、着信および発信サービスを個別に制御できます。アウトバウンド インターフェイスまたはインバウンド インターフェイスで、アクセス リストを設定できます。

次の例で、10 ギガビット イーサネット ネットワークはアドレスが 172.18.0.0 の Class B ネットワークで、メール ホストのアドレスは 172.18.1.2 です。**established** キーワードを使用するのは、TCP プロトコルで確立済み接続を指定する場合のみです。TCP データグラムに ACK または RST ビットが設定されている場合に一致が発生します。これは、パケットが既存の接続に属することを示します。

```
interface TenGigabitEthernet4/1/0
 ip access-group 102 in
!
access-list 102 permit tcp any 172.18.0.0 0.0.255.255 established
access-list 102 permit tcp any host 172.18.1.2 eq 25
```

例：ポート名に基づくフィルタによる Web へのアクセス回避

次の例では、w1 および w2 ワークステーションは Web アクセスが許可されていません。ネットワーク 172.20.0.0 上のその他のホストは Web アクセスが許可されています。

```
interface TenGigabitEthernet4/1/0
 ip access-group no-web out
!
ip access-list extended no-web
 remark Do not allow w1 to browse the web
 deny host 172.20.3.85 any eq http
 remark Do not allow w2 to browse the web
 deny host 172.20.3.13 any eq http
 remark Allow others on our network to browse the web
 permit 172.20.0.0 0.0.255.255 any eq http
```

例：送信元アドレスでのフィルタリングとパケットのロギング

次の例では、アクセス リスト 1 および 2 を定義します。いずれのリストもロギングが有効です。

```
interface TenGigabitEthernet4/1/0
 ip address 172.16.1.1 255.0.0.0
 ip access-group 1 in
 ip access-group 2 out
!
access-list 1 permit 172.25.0.0 0.0.255.255 log
access-list 1 deny 172.30.0.0 0.0.255.255 log
!
```

```
access-list 2 permit 172.27.3.4 log
access-list 2 deny 172.17.0.0 0.0.255.255 log
```

インターフェイスが 172.25.7.7 から 10 パケットを受信し、172.17.23.21 から 14 パケットを受信する場合、最初のログは次のようになります。

```
list 1 permit 172.25.7.7 1 packet
list 2 deny 172.17.23.21 1 packet
```

5 分後、コンソールは次のログを受信します。

```
list 1 permit 172.25.7.7 9 packets
list 2 deny 172.17.23.21 13 packets
```

例：デバッグ出力の制限

次の例では、アクセス リストを使用して、**debug** コマンド出力を制限します。**debug** 出力を制限すると、対象へのデータ量が制限され、時間とリソースの節約につながります。

```
Device(config)# ip access-list acl1
Device(config-std-nacl)# remark Displays only advertisements for LDP peer in acl1
Device(config-std-nacl)# permit host 10.0.0.44

Device# debug mpls ldp advertisements peer-acl acl1

tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.17.0.33
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.16.0.31
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.22.0.33
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.0.1
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.0.3
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.1.33
```

IPアクセスリストの作成とインターフェイスへの適用に関する追加参照資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

関連項目	マニュアル タイトル
• アクセス リスト エントリの順序 • 日または週の時刻に基づくアクセス リスト エントリ • 非初期フラグメントを使用するパケット	Refining an IP Access List
IP オプション、TCP フラグ、または非隣接ポートに基づくフィルタリング	『Creating an IP Access List for Filtering』
ロギング関連のパラメータの制御	『Understanding Access Control List Loggingl』

標準および RFC

標準/RFC	タイトル
この機能によりサポートされる新規または変更された標準や RFC はありません。またこの機能による既存の標準や RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPアクセスリストの作成とインターフェイスへの適用に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートす

る特定のソフトウェア リリース、フィーチャセット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *143* : *IP* アクセス リストの作成とインターフェイスへの適用に関する機能情報

機能名	リリース	機能情報
IP アクセス リスト	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 56 章

IP オプション、TCP フラグ、非隣接ポートをフィルタする IP アクセス リストの作成

ここでは、IP アクセス リストを使用して、特定の IP オプション、TCP フラグ、非隣接ポートを含む IP パケットをフィルタする方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

- IP オプション、TCP フラグ、非隣接ポート、TTL 値をフィルタする IP アクセス リストの作成に関する機能情報，981 ページ

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *144*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

IP オプション、TCP フラグ、非隣接ポートをフィルタする IP アクセス リストの作成に関する前提条件

このモジュールのいずれかのタスクを実行する前に、次のモジュールの情報を把握しておく必要があります。

- 『IP アクセス リストの概要』
- 『IP アクセス リストの作成とインターフェイスへの適用』

IP オプション、TCP フラグ、非隣接ポートをフィルタする IP アクセス リストの作成に関する情報

IP オプション

IP は、サービスを提供するときに、タイプ オブ サービス、存続可能時間、オプション、およびヘッダー チェックサムという 4 つの主要メカニズムを使用します。

オプションは一般的に IP オプションと呼ばれ、一部の状況で必要な制御機能のために用意されていますが、ほとんどの一般的な通信では不要です。IP オプションには、タイム スタンプ、セキュリティ、および特殊なルーティングに関する条件が含まれます。

IP オプションはデータグラムに含まれる場合と含まれない場合があります。IP オプションはすべての IP モジュール（ホストとゲートウェイ）で実装する必要があります。オプションというのは、実装ではなく、任意の指定したデータグラムでの送信を指します。環境によっては、セキュリティ オプションがすべてのデータグラムで必要です。

オプション フィールドは長さが可変です。オプションの個数はゼロ個以上です。IP オプションには、次の 2 つの形式のいずれかを使用できます。

- 形式 1：単一オクテットの option-type
- 形式 2：1 つの option-type オクテット、option-length オクテット、および実際の option-data オクテット

option-length オクテットは、option-type オクテット、option-length オクテット、および option-data オクテットの数をカウントします。

option-type オクテットには、1 ビットのコピー済みフラグ、2 ビットのオプション クラス、および 5 ビットのオプション番号という 3 つのフィールドがあります。これらのフィールドは、オプション タイプ フィールドの 8 ビット値を構成します。IP オプションは、一般的にその 8 ビット値で参照されます。

IP オプションの詳細な一覧と説明については、次の URL の RFC 791『*Internet Protocol*』を参照してください。http://www.faqs.org/rfcs/rfc791.html

IP オプションをフィルタする利点

- ネットワークからのIPオプションを含むパケットをフィルタすることで、ダウンストリームのデバイスとホストにかかるオプション パケットの負荷が軽減されます。
- また、この機能によって、分散型システムでRoute Processor（RP）処理が必要なIPオプションを含むパケットについて、RP への負荷が最小限になります。以前は、パケットは常に RP CPU でルーティングまたは処理されていました。パケットをフィルタすることで、パケットの RP への影響を回避できます。

TCP フラグに基づいてフィルタする利点

ACL TCP フラグ フィルタリング機能には、TCP フラグに基づいてフィルタする柔軟なメカニズムが用意されています。以前は、パケットのいずれかの TCP フラグがアクセス コントロール エントリ（ACE）で指定されたフラグに一致する限り、着信パケットは一致していました。すべてのフラグが設定されたパケットがアクセスコントロールリスト（ACL）を通過する可能性があるため、この動作ではセキュリティの抜け穴を考慮しています。ACL TCP フラグ フィルタリング機能では、フィルタするフラグの任意の組み合わせを選択できます。設定されているフラグ、および設定されていないフラグに基づいてマッチングする機能によって、TCP フラグに基づくフィルタリングの制御性が向上するため、セキュリティが強化されます。

TCP パケットは偽造の同期パケットとして送信され、それがリスニング ポートで受け入れられる可能性があるため、ファイアウォールデバイスの管理者は、偽造のTCPパケットをドロップするフィルタリング ルールを設定することを推奨します。

アクセスリストを構成するACEを設定し、特定のグループのTCPフラグが設定されているパケットのみ、または設定されていないパケットのみを許可することで、不正なTCPパケットを検出およびドロップできます。ACL TCP フラグ フィルタリング機能によって、次のようにパケット フィルタリングの制御性が向上します。

- フィルタする TCP パケットについて、TCP フラグの任意の組み合わせを選択できます。
- 設定されているフラグと設定されていないフラグに基づいてマッチングできるように、ACE を設定できます。

TCP フラグ

次の表は TCP フラグの一覧です。詳細については、RFC 793『*Transmission Control Protocol*』を参照してください。

表 *145* : *TCP* フラグ

TCP フラグ	目的
ACK	Acknowledge フラグ：セグメントの acknowledgment フィールドが、このセグメントの送信元が受信を予測している番号の次のシーケンス番号を指定することを示します。
FIN	Finish フラグ：接続をクリアするために使用されます。
PSH	Push フラグ：呼び出しのデータを受信ユーザに対してただちにプッシュする必要があることを示します。
RST	Reset フラグ：受信者が以降のやり取りなしで接続を削除する必要があることを示します。
SYN	Synchronize フラグ：接続の確立に使用されます。
URG	Urgent フラグ：urgent フィールドが重要で、セグメントシーケンス番号に追加する必要があることを示します。

アクセスコントロールエントリ機能での非隣接ポートに関する名前付きACLサポートを使用する利点

この機能によって、同じ送信元アドレス、宛先アドレス、およびプロトコルに関して複数のエントリを処理するために、アクセス コントロール リストで必要なアクセス コントロール エントリ（ACE）の数が大幅に削減されます。大量の ACE を保守している場合、可能な限り、新しいアクセス リスト エントリを作成するときは、この機能を使用して既存のアクセス リスト エントリのグループを統合します。非隣接ポートを使用するアクセスリストエントリを設定すると、保守するアクセス リスト エントリ数が少なくなります。

TTL 値のフィルタリング方法

IP は、拡張名前付きおよび番号付きアクセス リストは、インターフェイスを発着信するパケットの TTL 値でフィルタリングできます。有効な TTL 値 0 ～ 255 のパケットを許可または拒否できます（フィルタリング）。その他のフィールド（送信元または宛先アドレスなど）でのフィルタリングと同様に、**ipaccess-group** コマンドは **in** または **out** を指定します。これにより、アクセス リストの入力または出力が行われ、それぞれ着信または発信パケットに適用されます。TTL 値は、アクセスリストエントリで指定したプロトコル、アプリケーション、およびその他の設定とともにチェックされ、すべての条件を満たす必要があります。

入力インターフェイスに到達した TTL 値 0 または 1 のパケットに対する特別な処理

分散型シスコ エクスプレス フォワーディング（dCEF）、CEF、ファスト スイッチング、プロセス スイッチングなどのソフトウェア スイッチング パスは、通常、アクセス リスト ステートメントに基づいてパケットを許可または廃棄します。ただし、入力インターフェイスに到達したパケットの TTL 値が 0 または 1 であるときには、特別な処理が必要です。TTL 値が 0 または 1 のパケットは、CEF、dCEF、またはファスト スイッチング パスで入力アクセス リストがチェックされる前に、プロセス レベルに送信されます。入力アクセス リストは、TTL 値が 2 ～ 255 であるパケットに適用され、許可または拒否の決定が行われます。

TTL 値が 0 または 1 のパケットは、デバイスから外部に転送されることがないため、プロセス レベルに送信されます。プロセス レベルでは、各パケットがそのデバイス宛であるかどうか、および Internet Control Message Protocol（ICMP）TTL 値期限切れメッセージを返送する必要があるかどうかをチェックする必要があります。つまり、TTL が 0 または 1 のパケットをドロップする意図で TTL 値 0 または 1 のフィルタリングを設定した ACL が入力インターフェイスで設定されている場合でも、高速なパスではパケットのドロップが発生しないということです。代わりに、プロセスが ACL を適用するときに、プロセス レベルで発生します。これはハードウェア スイッチング プラットフォームについてもあてはまります。TTL 値が 0 または 1 のパケットはルート プロセッサ（RP）またはマルチレイヤ スイッチ フィーチャ カード（MSFC）のプロセス レベルに送信されます。

出力インターフェイスでは、TTL 値でのアクセス リスト フィルタリングは、その他のアクセス リスト機能と同じように動作します。チェックはデバイスで有効な最も高速なスイッチング パスで行われます。これは、より高速なスイッチング パスは出力インターフェイスですべての TTL 値（0 ～ 255）を均等に処理するためです。

TTL 値 0 と 1 でフィルタリングするためのコントロール プレーン ポリシング

TTL 値が 0 または 1 のパケットに対する特別な動作によって、デバイスの CPU 使用率が高くなります。0 または 1 の TTL 値 でフィルタリングする場合は、CPU が過負荷になることを防ぐためにコントロール プレーン ポリシング（CPP）を使用してください。CPP を活用するには、TTL 値 0 および 1 をフィルタリングすることに特化したアクセス リストを設定し、CPP を通じてそのアクセス リストを適用する必要があります。このアクセス リストは、その他のインターフェイス アクセス リストとは別のアクセス リストにします。CPP は個々のインターフェイスにおいてではなくシステム全体に対して機能するため、そのようなアクセス リストはデバイス全体に対して 1 つのみ設定する必要があります。このタスクは、セクション「TTL 値 0 と 1 でフィルタリングするコントロール プレーン ポリシングの有効化」で説明しています。

TTL 値に基づいてフィルタする利点

- 存続可能時間（TTL）値でのフィルタリングは、デバイスに到達できるパケット、またはデバイスに到達できないパケットを制御する方法を提供します。ネットワーク レイアウトを確認することで、特定のデバイスからのパケットをホップ数に基づいて許可するか拒否するかを選択できます。たとえば、小規模ネットワークでは、ホップ数が 3 より大きい場所からのパケットを拒否する可能性があります。TTL 値でのフィルタリングでは、トラフィックがネイバー デバイスから発信されたかどうかを検証できます。たとえば特定プロトコルの初期

TTL 値より 1 小さい TTL 値のパケットのみを受け入れることで、1 ホップで自分に到達するパケットのみを受け入れることができます。

- 多くのコントロール プレーン プロトコルはネイバーのみと通信しますが、パケットを誰からも受信します。TTL でフィルタリングするアクセス リストを受信側ルータに適用すると、不要なパケットをブロックできます。
- Cisco ソフトウェアが送信するすべてのパケットは、プロセス レベルに対して TTL 値が 0 または 1 です。デバイスは、Internet Control Message Protocol（ICMP）TTL 値期限切れメッセージを送信元に送信する必要があります。TTL 値が 0 ～ 2 であるパケットをフィルタリングすることで、プロセス レベルでの負荷を削減できます。

IP オプション、TCP フラグ、非隣接ポートをフィルタする IP アクセス リストの作成方法

IP オプションを含むパケットのフィルタリング

アクセス リストを設定して、IP オプションを含むパケットをフィルタし、アクセス リストが適切に設定されていることを確認するには、次の手順を完了します。

（注）

- IP オプションのフィルタリングに関する ACL のサポート機能は、名前付きの拡張 ACL でのみ使用できます。
- この機能を設定する場合、リソース予約プロトコル（RSVP）マルチプロトコル ラベル スイッチング トラフィック エンジニアリング（MPLS TE）、Internet Group Management Protocol バージョン 2（IGMPV2）、および IP オプション パケットを使用するその他のプロトコルは、ドロップまたは無視モードでは機能しない可能性があります。
- ほとんどの Cisco デバイスでは、IP オプションを含むパケットはハードウェアではスイッチされませんが、処理するコントロール プレーン ソフトウェアが必要です（主に、オプションを処理し、IP ヘッダーを書き直す必要があるため）。結果として、IP オプションを含むすべての IP パケットは、ソフトウェアでフィルタとスイッチが行われます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**ipaccess-list extended** *access-list-name* 例： `Device(config)# ip access-list extended mylist1`	名前で IP アクセス リストを指定し、名前付きアクセス リストのコンフィギュレーション モードを開始します。
ステップ 4	[*sequence-number*] **deny** *protocol source source-wildcard destination destination-wildcard* [**option** *option-value*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# deny ip any any option traceroute`	（任意）名前付き IP アクセス リスト モードで **deny** ステートメントを指定します。 • このアクセス リストでは、**deny** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**permit** ステートメントが最初に使用される可能性もあります。 • **option** キーワードおよび *option-value* 引数を使用して、特定の IP オプションを含むパケットをフィルタします。 • この例では、traceroute IP オプションを含むすべてのパケットが除外されます。 • エントリを削除するには、このコマンドの **no** *sequence-number* 形式を使用します。
ステップ 5	[*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* [**option** *option-value*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# permit ip any any option security`	名前付き IP アクセス リスト モードで **permit** ステートメントを指定します。 • この例では、セキュリティ IP オプションを含むすべてのパケット（まだフィルタされていないパケット）が許可されます。 • エントリを削除するには、このコマンドの **no** *sequence-number* 形式を使用します。
ステップ 6	必要に応じて、ステップ 4 またはステップ 5 を繰り返します。	アクセス リストは変更できます。
ステップ 7	**end** 例： `Device(config-ext-nacl)# end`	（任意）名前付きアクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 8	**showipaccess-lists** *access-list-name* 例： `Device# show ip access-lists mylist1`	（任意）IP アクセス リストの内容を表示します。

次の作業

アクセスリストをインターフェイスに適用するか、アクセスリストを受け入れるコマンドから参照します。

（注） IP オプションを含むすべてのパケットを効率的に除去するには、グローバル **ip options drop** コマンドを設定することを推奨します。

TCP フラグを含むパケットのフィルタリング

この作業では、アクセス リストを設定して、TCP フラグを含むパケットをフィルタし、アクセスリストが適切に設定されていることを確認します。

（注）
- TCP フラグのフィルタリングを使用できるのは、名前付きの拡張 ACL のみです。
- ACL TCP フラグ フィルタリング機能は、Cisco ACL の場合にのみサポートされます。
- 事前に、次のコマンドラインインターフェイス（CLI）形式を使用して、TCP フラグチェック メカニズムを設定できます。

permittcpanyanyrst 同じ ACE を表す **permittcpanyanymatch-any+rst** 形式を使用できるようになりました。どちらの CLI 形式も可能ですが、新しいキーワード **match-all** または **match-any** を使用する場合、その後に、「+」または「-」というプレフィックスで始まる新しいフラグを続ける必要があります。単一の ACL では、古い形式のみ、または新しい形式のみを使用することを推奨します。CLI の古い形式と新しい形式の混在やマッチングを行うことはできません。

注意 新しい構文形式の ACE を持つデバイスを、ACL TCP フラグ フィルタリング機能をサポートしないシスコ ソフトウェアの以前のバージョンでリロードすると、ACE は適用されないため、セキュリティの抜け穴が発生する可能性があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**ipaccess-list extended** *access-list-name* 例： `Device(config)# ip access-list extended kmd1`	名前で IP アクセス リストを指定し、名前付きアクセス リストのコンフィギュレーション モードを開始します。
ステップ 4	[*sequence-number*] **permittcp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established**|{**match-any** | **match-all**} {+ | -} *flag-name*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# permit tcp any any match-any +rst`	名前付き IP アクセス リスト モードで **permit** ステートメントを指定します。 • このアクセス リストでは、**permit** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。 • **permit** コマンドの TCP コマンド構文を使用します。 • RST TCP ヘッダー フラグが設定されたすべてのパケットは一致し、ステップ 3 で名前付きアクセス リスト kmd1 に合格できます。
ステップ 5	[*sequence-number*] **denytcp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established**|{**match-any** | **match-all**} {+ | -} *flag-name*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]	（任意）名前付き IP アクセス リスト モードで **deny** ステートメントを指定します。 • このアクセス リストでは、**permit** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。

	コマンドまたはアクション	目的
	例： `Device(config-ext-nacl)# deny tcp any any match-all -ack -fin`	• **deny** コマンドの TCP コマンド構文を使用します。 • ACK フラグが設定されず、FIN フラグも設定されていないパケットは、ステップ 3 で名前付きアクセス リスト kmd1 に合格しません。 • 上位層プロトコル（ICMP、IGMP、TCP、および UDP）を許可するその他のコマンド構文については、**deny**（IP）コマンドを参照してください。
ステップ 6	必要に応じてステップ 4 またはステップ 5 を繰り返し、計画したシーケンス番号でステートメントを追加します。エントリを削除するには **no** *sequence-number* コマンドを使用します。	アクセス リストは変更できます。
ステップ 7	**end** 例： `Device(config-ext-nacl)# end`	（任意）コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 8	**showipaccess-lists** *access-list-name* 例： `Device# show ip access-lists kmd1`	（任意）IP アクセス リストの内容を表示します。 • 出力を見直して、アクセス リストに新しいエントリが含まれることを確認します。

非隣接ポートを使用するアクセス コントロール エントリの設定

非隣接 TCP または UDP ポート番号を使用するアクセス リスト エントリを作成するには、次の作業を実行します。この作業では 、TCP ポートを使用しますが、**permit** および **deny** コマンドの UDP 構文を使用して、非隣接 UDP ポートをフィルタすることもできます。

この作業では、**permit** コマンドを最初に使用していますが、フィルタリングの目標に合わせた順序で、**permit** および **deny** コマンドを使用できます。

（注） ACL：アクセス コントロール エントリでの非隣接ポートに関する名前付き ACL サポート機能を使用できるのは、名前付きの拡張 ACL のみです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**ipaccess-list extended** *access-list-name* 例： `Device(config)# ip access-list extended acl-extd-1`	名前で IP アクセス リストを指定し、名前付きアクセス リストのコンフィギュレーション モードを開始します。
ステップ 4	[*sequence-number*] **permittcp** *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established** {**match-any** | **match-all**} {**+** | **-**} *flag-name*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# permit tcp any eq telnet ftp any eq 450 679`	名前付きアクセス リスト コンフィギュレーション モードで **permit** ステートメントを指定します。 • 演算子には、**lt**（より小さい）、**gt**（より大きい）、**eq**（等しい）、**neq**（等しくない）、および **range**（包含範囲）が含まれます。 • 演算子が source および source-wildcard 引数の後にある場合、送信元ポートに一致する必要があります。演算子が destination および destination-wildcard 引数の後にある場合、宛先ポートに一致する必要があります。 • **range** 演算子には 2 つのポート番号が必要です。**eq** および **neq** 演算子の後には、最大 10 個のポートを設定できます。他のすべての演算子は 1 つのポート番号が必要です。 • UDP ポートをフィルタするには、このコマンドの UDP 構文を使用します。

	コマンドまたはアクション	目的
ステップ 5	[*sequence-number*] **denytcp** *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established** {**match-any** | **match-all**} {**+** | **-**} *flag-name*] [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# deny tcp any neq 45 565 632`	（任意）名前付きアクセス リスト コンフィギュレーション モードで **deny** ステートメントを指定します。 • 演算子には、**lt**（より小さい）、**gt**（より大きい）、**eq**（等しい）、**neq**（等しくない）、および **range**（包含範囲）が含まれます。 • 演算子が *source* および *source-wildcard* 引数の後にある場合、送信元ポートに一致する必要があります。演算子が *destination* および *destination-wildcard* 引数の後にある場合、宛先ポートに一致する必要があります。 • **range** 演算子には 2 つのポート番号が必要です。**eq** および **neq** 演算子の後には、最大 10 個のポートを設定できます。他のすべての演算子は 1 つのポート番号が必要です。 • UDP ポートをフィルタするには、このコマンドの UDP 構文を使用します。
ステップ 6	必要に応じてステップ 4 またはステップ 5 を繰り返し、計画したシーケンス番号でステートメントを追加します。エントリを削除するには、**no** *sequence-number* コマンドを使用します。	アクセス リストは変更できます。
ステップ 7	**end** 例： `Device(config-ext-nacl)# end`	（任意）名前付きアクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 8	**showipaccess-lists** *access-list-name* 例： `Device# show ip access-lists kmd1`	（任意）アクセス リストの内容を表示します。

非隣接ポートを使用する複数アクセス リスト エントリの 1 つのアクセス リスト エントリへの統合

非隣接ポートを使用するアクセス リスト エントリ グループを 1 つのアクセス リスト エントリに統合するには、次の作業を実行します。

この作業では 、TCP ポートを使用しますが、**permit** および **deny** コマンドの UDP 構文を使用して、非隣接 UDP ポートをフィルタすることもできます。

この作業では、**permit** コマンドを最初に使用していますが、フィルタリングの目標に合わせた順序で、**permit** および **deny** コマンドを使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showipaccess-lists** *access-list-name* 例： `Device# show ip access-lists mylist1`	（任意）IP アクセス リストの内容を表示します。 • 出力を見直して、アクセス リスト エントリを統合できるかどうかを確認します。
ステップ 3	**configure terminal** 例： `Device# configure terminal`	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 4	**ipaccess-list extended** *access-list-name* 例： `Device(config)# ip access-list extended mylist1`	名前で IP アクセス リストを指定し、名前付きアクセスリストのコンフィギュレーション モードを開始します。
ステップ 5	**no** [*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard*[**option** *option-name*] [**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# no 10`	統合できる重複するアクセス リスト エントリを削除します。 • このステップを繰り返して、ポート番号のみが異なるために統合できるエントリを削除します。 • このステップを繰り返して、たとえばアクセス リスト エントリ 20、30、および 40 を削除した後は、1 つの **permit** ステー

	コマンドまたはアクション	目的
		トメントに統合されるため、これらのエントリは削除されます。 • *sequence-number* が指定された場合、その他のコマンド構文は任意です。
ステップ 6	[*sequence-number*] **permit** *protocol source source-wildcard*[*operator port*[*port*]] *destination destination-wildcard*[*operator port*[*port*]] [**option** *option-name*] [**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# permit tcp any neq 45 565 632 any eq 23 45 34 43`	名前付きアクセス リスト コンフィギュレーション モードで **permit** ステートメントを指定します。 • このインスタンスでは、非隣接ポートを使用するアクセス リスト エントリ グループは、1 つの **permit** ステートメントに統合されました。 • **eq** および **neq** 演算子の後には、最大 10 個のポートを設定できます。
ステップ 7	必要に応じてステップ 5 と 6 を繰り返し、**permit** または **deny** ステートメントを追加して、可能な場合はアクセス リスト エントリを統合します。エントリを削除するには、**no** *sequence-number* コマンドを使用します。	アクセス リストは変更できます。
ステップ 8	**end** 例： `Device(config-std-nacl)# end`	（任意）名前付きアクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 9	**showipaccess-lists** *access-list-name* 例： `Device# show ip access-lists mylist1`	（任意）アクセス リストの内容を表示します。

次の作業

アクセスリストをインターフェイスに適用するか、アクセスリストを受け入れるコマンドから参照します。

TTL 値に基づいたパケットのフィルタリング

アクセス リストは柔軟性に優れているため、TTL 値に基づいてパケットをフィルタリングする **permit** および **deny** コマンドの組み合わせ 1 つだけでは定義することができません。次のタスクでは、TTL フィルタリングを実行する例を 1 つだけ示します。独自のフィルタリング プランを満たす **permit** および **deny** ステートメントを適切に設定します。

（注） デバイスで使用する Cisco のソフトウェア リリースに応じて、アクセス リストで演算子 EQ または NEQ を指定する場合、アクセス リストでは最大 10 個の TTL 値を指定できます。TTL 値の数は、シスコのソフトウェア リリースによって異なります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**ipaccess-list extended** *access-list-name* 例： `Device(config)# ip access-list extended ttlfilter`	IP アクセス リストを名前で定義します。 • TTL 値でフィルタリングするアクセス リストは、拡張アクセス リストである必要があります。
ステップ 4	[*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard*[**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# permit ip host 172.16.1.1 any ttl lt 2`	パケットが名前付き IP アクセス リストを通過できる条件を設定します。 • 各アクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。 • この例では、送信元 172.16.1.1 から TTL 値が 2 未満の接続先へのパケットが許可されています。

	コマンドまたはアクション	目的
ステップ 5	**permit** または **deny** ステートメントを続けて追加し、必要なフィルタリングを実現します。	--
ステップ 6	**exit** 例： `Device(config-ext-nacl)# exit`	コンフィギュレーション モードを終了して、コマンドライン インターフェイス（CLI）モード階層で次に高いレベルのモードを開始します。
ステップ 7	**interface** *type number* 例： `Device(config)# interface TenGigabitEthernet4/1/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 8	**ipaccess-group** *access-list-name* {**in** | **out**} 例： `Device(config-if)# ip access-group ttlfilter in`	アクセス リストをインターフェイスに適用します。

TTL 値 0 と 1 でフィルタリングするコントロール プレーン ポリシングの有効化

TTL 値 0 または 1 に基づいて IP パケットをフィルタリングしたり、CPU の過負荷を防止したりするには、次のタスクを実行します。このタスクでは、TTL 値 0 と 1 で分類用のアクセス リストを設定し、モジュラ QoS コマンドライン インターフェイス（CLI）（MQC）を設定して、ポリシーマップをコントロールプレーンに適用します。アクセスリストを通過するパケットはドロップされます。この特別なアクセスリストは、他のインターフェイスアクセスリストとは異なります。

アクセス リストは柔軟性に優れているため、TTL 値に基づいてパケットをフィルタリングする **permit** および **deny** コマンドの組み合わせ 1 つだけでは定義することができません。次のタスクでは、TTL フィルタリングを実行する例を 1 つだけ示します。独自のフィルタリング プランを満たす **permit** および **deny** ステートメントを適切に設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**ipaccess-list extended** *access-list-name* 例： `Device(config)# ip access-list extended ttlfilter`	IP アクセス リストを名前で定義します。 • TTL 値でフィルタリングするアクセス リストは、拡張アクセス リストである必要があります。
ステップ 4	[*sequence-number*] **permit** *protocol source source-wildcard destination destination-wildcard* **ttl** *operator* value 例： `Device(config-ext-nacl)# permit ip host 172.16.1.1 any ttl lt 2`	パケットが名前付き IP アクセス リストを通過できる条件を設定します。 • 各アクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。 • この例では、送信元 172.16.1.1 から TTL 値が 2 未満の接続先へのパケットが許可されています。
ステップ 5	**permit** または **deny** ステートメントを続けて追加し、必要なフィルタリングを実現します。	アクセス リストを通過するパケットはドロップされます。
ステップ 6	**exit** 例： `Device(config-ext-nacl)# exit`	コンフィギュレーション モードを終了して、CLI モード階層で次に高いレベルのモードを開始します。
ステップ 7	**class-map** *class-map-name* [**match-all** | **match-any**] 例： `Device(config)# class-map acl-filtering`	指定したクラスへのパケットのマッチングに使用するクラス マップを作成します。

	コマンドまたはアクション	目的
ステップ 8	**matchaccess-group** {*access-group* | **name** *access-group-name*} 例： `Device(config-cmap)# match access-group name ttlfilter`	指定したアクセス コントロール リストに基づいて、クラス マップの一致基準を設定します
ステップ 9	**exit** 例： `Device(config-cmap)# exit`	コンフィギュレーション モードを終了して、CLI モード階層で次に高いレベルのモードを開始します。
ステップ 10	**policy-map** *policy-map-name* 例： `Device(config)# policy-map acl-filter`	1 つ以上のインターフェイスに付加できるポリシー マップを作成または変更し、サービス ポリシーを指定します。
ステップ 11	**class**{*class-name*|**class-default**} 例： `Device(config-pmap)# class acl-filter-class`	作成または変更するポリシーのクラス名を指定するか、ポリシーを指定する前にデフォルト クラス（一般に class-default クラスといいます）を指定します。
ステップ 12	**drop** 例： `Device(config-pmap-c)# drop`	特定のクラスに属するパケットを廃棄するトラフィック クラスを設定します。
ステップ 13	**exit** 例： `Device(config-pmap-c)# exit`	コンフィギュレーション モードを終了して、CLI モード階層で次に高いレベルのモードを開始します。
ステップ 14	**exit** 例： `Device(config-pmap)# exit`	コンフィギュレーション モードを終了して、CLI モード階層で次に高いレベルのモードを開始します。
ステップ 15	**control-plane** 例： `Device(config)# control-plane`	デバイスのコントロール プレーンに関連する属性またはパラメータを関連付けたり、変更したりします。

	コマンドまたはアクション	目的
ステップ 16	**service-policy**{**input** | **output**} *policy-map-name* 例： `Device(config-cp)# service-policy input acl-filter`	集約コントロール プレーン サービスのためにポリシー マップをコントロール プレーンに適用します。

IP オプション、TCP フラグ、非隣接ポートのフィルタリングの設定例

例：IP オプションを含むパケットのフィルタリング

次の例は、アクセス リスト エントリ（ACE）に指定されている IP オプションが含まれる場合にのみ、TCP パケットを許可するように設定された ACE を含む、mylist2 という拡張アクセス リストを示します。

```
ip access-list extended mylist2
 10 permit ip any any option eool
 20 permit ip any any option record-route
 30 permit ip any any option zsu
 40 permit ip any any option mtup
```

一致し、それによって許可されたパケットの数を示すため、**show access-list** コマンドが入力されました。

```
Device# show ip access-list mylist2
Extended IP access list test
10 permit ip any any option eool (1 match)
20 permit ip any any option record-route (1 match)
30 permit ip any any option zsu (1 match)
40 permit ip any any option mtup (1 match)
```

例：TCP フラグを含むパケットのフィルタリング

次のアクセス リストでは、TCP フラグ ACK および SYN が設定され、FIN フラグが設定されていない場合にのみ、TCP パケットを許可します。

```
ip access-list extended aaa
 permit tcp any any match-all +ack +syn -fin
 end
```

ACL を表示するために、 **show access-list** コマンドが入力されました。

```
Device# show access-list aaa

Extended IP access list aaa
 10 permit tcp any any match-all +ack +syn -fin
```

例：非隣接ポートを使用するアクセス リスト エントリの作成

eq および **neq** 演算子の後に最大 10 ポートを入力できるため、次のアクセス リスト エントリを作成できます。

```
ip access-list extended aaa
 permit tcp any eq telnet ftp any eq 23 45 34
 end
```

show access-lists コマンドを入力して、新しく作成されたアクセス リスト エントリを表示します。

```
Device# show access-lists aaa

Extended IP access list aaa
 10 permit tcp any eq telnet ftp any eq 23 45 34
```

例：既存の複数のアクセス リスト エントリと非隣接ポートを使用する 1 つのアクセス リスト エントリの統合

showaccess-lists コマンドは、abc と名付けられたアクセス リストに対して、アクセス リスト エントリのグループを表示するのに使用されます。

```
Device# show access-lists abc
Extended IP access list abc
 10 permit tcp any eq telnet any eq 450
 20 permit tcp any eq telnet any eq 679
 30 permit tcp any eq ftp any eq 450
 40 permit tcp any eq ftp any eq 679
```

エントリはすべて同じ **permit** ステートメントに対してであり、異なるポートを示すだけのため、1 つのアクセス リスト エントリに統合できます。次の例では、重複するアクセス リスト エントリを削除し、以前に表示されていたアクセス リスト エントリ グループを統合する新しいアクセス リスト エントリを作成します。

```
ip access-list extended abc
 no 10
 no 20
 no 30
 no 40
 permit tcp any eq telnet ftp any eq 450 679
 end
```

show access-lists コマンドを再入力すると、統合されたアクセス リスト エントリが表示されます。

```
Device# show access-lists abc
Extended IP access list abc
 10 permit tcp any eq telnet ftp any eq 450 679
```

例：TTL 値のフィルタリング

次のアクセス リストは、存続可能時間（TTL）の値が 10 と 20 でタイプ オブ サービス（ToS）レベルが 3 の IP パケットをフィルタリングします。また、TTL が 154 を超える IP パケットをフィルタリングし、その規則を先頭以外のフラグメントにも適用します。フラッシュの優先レベルと

1 以外の TTL 値を持つ IP パケットを許可し、そのようなパケットのログ メッセージをコンソールに送信します。他のすべてのパケットは拒否されます。

```
ip access-list extended incomingfilter
 deny ip any any tos 3 ttl eq 10 20
 deny ip any any ttl gt 154 fragments
 permit ip any any precedence flash ttl neq 1 log
!
interface TenGigabitEthernet4/1/0

ip access-group incomingfilter in
```

例：TTL 値 0 と 1 でフィルタリングするコントロール プレーン ポリシング

次の例では、acl-filter と呼ばれるポリシー マップで使用するために、acl-filter-class と呼ばれるトラフィック クラスを設定します。アクセス リストは、存続可能時間（TTL）値が 0 または 1 の送信元からの IP パケットを許可します。アクセスリストに一致するパケットがドロップされます。ポリシー マップはコントロール プレーンに結合されます。

```
ip access-list extended ttlfilter

 permit ip any any ttl eq 0 1

class-map acl-filter-class


 match access-group name ttlfilter


policy-map acl-filter

 class acl-filter-class

 drop

control-plane

 service-policy input acl-filter
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
noipoptions コマンドを使用した、IP オプションを含むパケットをドロップまたは無視するためのデバイスの設定。	『ACL IP Options Selective Drop』
アクセス リストに関する概要情報	『IP Access List Overview』

関連項目	マニュアル タイトル
IP アクセス リストの作成とインターフェイスへの適用に関する情報	『Creating an IP Access List and Applying It to an Interface』
QoS コマンド	『*Cisco IOS Quality of Service Solutions Command Reference*』

RFC

RFC	タイトル
RFC 791	*Internet Protocol*（インターネット プロトコル） http://www.faqs.org/rfcs/rfc791.html http://www.faqs.org/rfcs/rfc791.html
RFC 793	『*Transmission Control Protocol*』
RFC 1393	『*Traceroute Using an IP Option*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IP オプション、TCP フラグ、非隣接ポート、TTL 値をフィルタする IP アクセス リストの作成に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *146*：*IP* オプション、*TCP* フラグ、非隣接ポート、*TTL* 値をフィルタする *IP* アクセス リストの作成に関する機能情報

機能名	リリース	機能情報
IP アクセス リスト	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 57 章

IP アクセス リストの精緻化

アクセス リストを作成している間、または作成した後に、アクセス リストを精緻化するにはいくつかの方法があります。アクセス リストのエントリの順序を変更したり、アクセス リストにエントリを追加したりできます。また、アクセス リスト エントリを日または週の特定の時間帯に制限したり、パケットの非初期フラグメントをフィルタリングすることでパケットをフィルタリングするときにより細かく設定することができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *147* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

IP アクセス リストの精緻化に関する情報

アクセス リストのシーケンス番号

IP アクセス リスト エントリにシーケンス番号を適用する機能によって、アクセス リストの変更が簡易になります。IP アクセス リスト エントリ シーケンス番号機能の前には、アクセス リスト内のエントリの位置を指定する方法はありませんでした。以前は、既存のリストの途中にエントリを挿入する場合、目的の位置の後にあるすべてのエントリを削除してから、新しいエントリを追加し、削除したすべてのエントリを再入力する必要がありました。これは手間がかかり、エラーが起こりやすい方法です。

シーケンス番号を使用して、ユーザはアクセス リスト エントリを追加し、それを並べ替えることができるようになりました。新しいエントリを追加する場合、アクセス リストの目的の位置に挿入されるようにシーケンス番号を指定します。必要に応じて、アクセス リストの現在のエントリを並べ替えて、新しいエントリを挿入できる場所を作成できます。

アクセス リスト シーケンス番号の利点

アクセス リスト シーケンス番号は、アクセス リストで **permit** または **deny** コマンドを開始する番号です。シーケンス番号により、エントリがアクセス リストに表示される順序が決定されます。IP アクセス リスト エントリにシーケンス番号を適用する機能によって、アクセス リストの変更が簡易になります。

シーケンス番号を設定する前に、アクセス リストの末尾にアクセス リスト エントリを追加できるため、アクセス リスト全体の再設定が必要になるリストの末尾以外の位置では、ステートメントの追加が必要になります。アクセス リスト内でのエントリの位置を指定する方法はありません。以前は、既存のリストの途中にエントリ（ステートメント）を挿入する場合、目的の位置の後にあるすべてのエントリを削除してから、新しいエントリを追加し、削除したすべてのエントリを再入力する必要がありました。これは手間がかかり、エラーが起こりやすい方法です。

この新しい機能を使用すると、アクセスリストエントリにシーケンス番号を追加し、順序を変更することができます。新しいエントリを追加するとき、アクセス リストの目的の位置に配置されるように、シーケンス番号を選択します。必要に応じて、アクセス リストの現在のエントリを並べ替えて、新しいエントリを挿入できる場所を作成できます。シーケンス番号により、アクセス リストの変更を簡単に実行できるようになりました。

シーケンス番号の動作

- 以前のリリースとの下位互換性を保つため、シーケンス番号のないエントリが適用された場合には、最初のエントリにはシーケンス番号 10 が割り当てられます。連続してエントリを追加すると、シーケンス番号は 10 ずつ増分されます。最大シーケンス番号は 2147483647 です。生成したシーケンス番号がこの最大値を超えると、次のメッセージが表示されます。

```
Exceeded maximum sequence number.
```

- シーケンス番号のないエントリを入力すると、アクセス リストの最後のシーケンス番号に 10 を加えたシーケンス番号が割り当てられ、リストの末尾に配置されます。
- （シーケンス番号以外が）既存のエントリに一致するエントリを入力すると、何も変更されません。
- 既存のシーケンス番号を入力すると、次のエラー メッセージが表示されます。

```
Duplicate sequence number.
```

- グローバル コンフィギュレーション モードで新しいアクセス リストを入力すると、そのアクセス リストのシーケンス番号が自動的に生成されます。
- シーケンス番号が不揮発性生成（NVGEN）されることはありません。つまり、シーケンス番号自体は保存されません。システムのリロード時には、設定されたシーケンス番号はデフォルトのシーケンス開始番号と増分に戻されます。この機能は、シーケンス番号をサポートしないソフトウェア リリースとの下位互換性を保つために提供されています。
- この機能は、名前付きおよび番号付きの標準および拡張 IP アクセス リストと連動します。

時間範囲の利点

時間範囲の利点および可能な使用法として、次のことが挙げられます。

- ネットワーク管理者は、リソースへのユーザアクセスの許可または拒否の制御をより強化できます。これらのリソースとして、アプリケーション（IP アドレス/マスク ペアとポート番号によって特定されます）、ポリシー ルーティング、またはオンデマンド リンク（ダイヤラへの関連トラフィックとして認識されます）があります。
- ネットワーク管理者は、次に示すような、時刻ベースのセキュリティ ポリシーを設定できます。
  - アクセス リストを使用した境界セキュリティ
  - IP セキュリティ プロトコル（IPsec）を使用したデータの機密性保持
- プロバイダーのアクセス レートが一日の時間帯によって異なるときは、トラフィックは自動的にコスト効率よく再ルーティングすることが可能です。
- ネットワーク管理者は、ロギング メッセージを制御できます。アクセス リスト エントリは、一日の特定の時間帯にトラフィックをロギングすることはできますが、常にロギングすることはできません。したがって、管理者はピーク時間中に生成された多くのログを分析することなく、単にアクセスを拒否できます。

パケットの非初期フラグメントをフィルタリングする利点

パケットの初期フラグメントにとどまらず、より多くのトラフィックをブロックするには、拡張アクセス リストを使用してパケットの非初期フラグメントをフィルタリングします。まず、次の概念を理解しておく必要があります。

フラグメントを拒否する追加の IP アクセス リスト エントリで **fragments** キーワードが使用されている場合、フラグメント制御機能を使用すると、次のような利点があります。

追加のセキュリティ

パケットの初期フラグメントにとどまらず、より多くのトラフィックをブロックできます。不要なフラグメントは、受信側にリアセンブリ タイムアウトになるまで残りません。これは、このようなフラグメントは受信側に送信される前にブロックされるためです。不要なトラフィックを大量にブロックすることで、セキュリティが高まり、ハッカーから攻撃を受けるリスクが軽減されます。

コスト削減

パケットの不要な非初期フラグメントをブロックすると、ブロックしたいトラフィックに注意を払う必要がなくなります。

使用ストレージの削減

パケットの不要な非初期フラグメントが受信側に届かないようにブロックすることで、宛先はリアセンブリ タイムアウトになるまでフラグメントを保存する必要がなくなります。

予期される動作

非初期フラグメントは、初期フラグメントと同様に扱われます。予期されないポリシー ルーティング結果や、ルーティングされるべきでないパケットのフラグメントが生じる可能性も低くなります。

フラグメントのアクセス リスト処理

fragments キーワードを使用する場合と、使用しない場合に関するアクセス リスト エントリの動作は、次のようにまとめることができます。

アクセス リスト エントリの状態...	結果

fragments キーワードがなく（デフォルト）、すべてのアクセス リスト エントリの情報が一致している	レイヤ 3 情報のみを含むアクセス リスト エントリの場合：
	• エントリは、非フラグメント パケット、先頭フラグメント、先頭以外のフラグメントに適用されます。
	
	レイヤ 3 およびレイヤ 4 情報を含むアクセス リスト エントリの場合：
	• エントリは、非フラグメント パケットと先頭フラグメントに適用されます。
	  • エントリが **permit** ステートメントであると、パケットまたはフラグメントは許可されます。
	  • エントリが **deny** ステートメントであると、パケットまたはフラグメントは拒否されます。
	• エントリは、次の方法で先頭以外のフラグメントにも適用されます。非初期フラグメントにはレイヤ 3 情報のみが含まれているため、アクセス リスト エントリのレイヤ 3 の部分のみが適用されます。アクセス リスト エントリのレイヤ 3 の部分が一致し、
	  • エントリが **permit** ステートメントであると、非初期フラグメントは許可されます。
	  • エントリが **deny** ステートメントであると、次のアクセス リスト エントリが処理されます。
	
	（注） 非初期フラグメントと、非フラグメントまたは初期フラグメントの場合では、**deny** ステートメントの処理方法は異なります。

fragments キーワードが指定され、すべてのアクセス リスト エントリ情報が一致している	アクセス リスト エントリは、非初期フラグメントにのみ適用されます。 レイヤ 4 情報を含むアクセスリスト エントリには、**fragments** キーワードは設定できません。

すべてのアクセス リスト エントリに **fragments** キーワードを追加することはできません。IP パケットの最初のフラグメントは非フラグメントとして見なされ、以降のフラグメントとは独立して扱われるためです。初期フラグメントは、アクセス リストの **permit** キーワードが設定された **deny** または **fragments** エントリとは一致しません。パケットは、**fragments** キーワードが設定されていないアクセス リスト エントリによって許可または拒否されるまで、次のアクセス リスト エントリと比較されます。したがって、**deny** エントリごとに、2 つのアクセス リスト エントリが必要になる場合があります。ペアの最初の **deny** エントリには、**fragments** キーワードは含まれず、初期フラグメントに適用されます。ペアの 2 番目の **deny** エントリは、**fragments** キーワードを含んでおり、以降のフラグメントに適用されます。同じホストに対する複数の **deny** エントリがあるが、レイヤ 4 ポートが異なる場合は、そのホストで **fragments** キーワードが設定された 1 つの **deny** アクセスリストエントリを追加する必要があります。このように、パケットのすべてのフラグメントは、アクセス リストによって同様に扱われます。

IP データグラムのパケット フラグメントは個々のパケットと見なされ、それぞれ、アクセス リスト アカウンティングとアクセス リストの違反カウントの 1 つのパケットとして個別にカウントされます。

IP アクセス リストを精緻化する方法

このモジュールで説明する作業では、アクセス リストを精緻化するためのさまざまな方法を示します（アクセスリストを作成するときに精緻化しなかった場合に利用できます）。アクセスリストエントリの順序変更、アクセスリストへのエントリの追加、日または週の特定の時間帯でのアクセスリストエントリの制限などを実行できます。また、パケットの非初期フラグメントをフィルタリングすることでパケットをフィルタリングするときにより細かく設定することができます。

シーケンス番号を使用したアクセス リストの変更

既存のアクセス リストへのエントリの追加、エントリの順序変更、または（将来の変更に対応するための）アクセス リストのエントリの番号付けを行うには、次の手順を実行します。

（注） アクセス リストからエントリを削除するには、単にこのコマンドの **nodeny** 形式または **nopermit** 形式を使用するだけです。あるいは、ステートメントにすでにシーケンス番号がある場合は **no** *sequence-number* コマンドも使用できます。

（注）

- アクセス リスト シーケンス番号は、ダイナミック、リフレクシブ、またはファイアウォールのアクセス リストをサポートしていません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**ipaccess-listresequence** *access-list-name starting-sequence-number increment* 例： `Router(config)# ip access-list resequence kmd1 100 15`	開始シーケンス番号と、シーケンス番号の増分を使用して、指定した IP アクセス リストを並べ替えます。 • この例では、kmd1 という名前のアクセス リストを並べ替えます。開始シーケンス番号は 100、増分は 15 です。
ステップ 4	**ipaccess-list**{**standard**| **extended**} *access-list-name* 例： `Router(config)# ip access-list standard xyz123`	名前で IP アクセス リストを指定し、名前付きアクセス リストのコンフィギュレーション モードを開始します。 • **standard** を指定する場合は、標準アクセス リスト構文を使用して、**permit** および **deny** ステートメント（場合によっては両方）を指定します。 • **extended** を指定する場合は、拡張アクセス リスト構文を使用して、**permit** および **deny** ステートメント（場合によっては両方）を指定します。
ステップ 5	次のいずれかを実行します。 • *sequence-number* **permit** *source source-wildcard* • *sequence-number* **permit** *protocol source source-wildcard destination destination-wildcard*[**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**]	名前付き IP アクセス リスト モードで permit ステートメントを指定します。 • このアクセス リストでは、**permit** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。 • 上位層プロトコル（ICMP、IGMP、TCP、および UDP）を許可するその他のコマンド構文に

	コマンドまたはアクション	目的
	例： `Router(config-std-nacl)# 105 permit 10.5.5.5 0.0.0.255`	ついては、**permit**（IP）コマンドを参照してください。 • エントリを削除するには、**no** *sequence-number* コマンドを使用します。 • プロンプトに示されるとおり、このアクセス リストは標準アクセス リストでした。ステップ 4 で **extended** を指定した場合は、このステップのプロンプトは Router(config-ext-nacl)# となり、拡張 **permit** コマンド構文を使用します。
ステップ 6	次のいずれかを実行します。 • *sequence-number* **deny** *source source-wildcard* • *sequence-number* **deny** *protocol source source-wildcard destination destination-wildcard*[**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Router(config-std-nacl)# 110 deny 10.6.6.7 0.0.0.255`	（任意）名前付き IP アクセス リスト モードで deny ステートメントを指定します。 • このアクセス リストでは、**permit** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。 • 上位層プロトコル（ICMP、IGMP、TCP、および UDP）を許可するその他のコマンド構文については、**deny**（IP）コマンドを参照してください。 • エントリを削除するには、**no** *sequence-number* コマンドを使用します。 • プロンプトに示されるとおり、このアクセス リストは標準アクセス リストでした。ステップ 4 で **extended** を指定した場合は、このステップのプロンプトは Router(config-ext-nacl)# となり、拡張 **deny** コマンド構文を使用します。
ステップ 7	必要に応じてステップ 5 とステップ 6 を繰り返し、目的とするシーケンス番号順にステートメントを追加します。エントリを削除するには、**no** *sequence-number* コマンドを使用します。	アクセス リストは変更できます。
ステップ 8	**end** 例： `Router(config-std-nacl)# end`	（任意）コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**showipaccess-lists** *access-list-name* 例： `Router# show ip access-lists xyz123`	（任意）IP アクセス リストの内容を表示します。 • 出力を見直して、アクセス リストに新しいエントリが含まれることを確認します。

例

この出力例は、**xyz123** アクセス リストを指定した場合の **showipaccess-lists** コマンドの出力例を示します。

```
Router# show ip access-lists xyz123
Standard IP access list xyz123
100 permit 10.4.4.0, wildcard bits 0.0.0.255
105 permit 10.5.5.5, wildcard bits 0.0.0.255
115 permit 10.0.0.0, wildcard bits 0.0.0.255
130 permit 10.5.5.0, wildcard bits 0.0.0.255
145 permit 10.0.0.0, wildcard bits 0.0.0.255
```

日または週の特定の時間帯でのアクセス リスト エントリの制限

デフォルトで、アクセスリストステートメントは適用されたときに実行されます。ただし、時間範囲を定義し、各アクセス リスト ステートメントにおいて名前ごとに時間範囲を参照することで、**permit** または **deny** ステートメントが有効になる日または週の時間帯を定義できます。IP および Internetwork Packet exchange（IPX）名前付きまたは番号付きの拡張アクセス リストは、時間範囲に対応します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**ipaccess-listextended** *name* 例： `Router(config)# ip access-list extended rstrct4`	名前を使用して拡張 IP アクセス リストを定義し、拡張名前付きアクセス リストのコンフィギュレーション モードを開始します。
ステップ 4	[*sequence-number*] **deny** *protocol source*[*source-wildcard*] [*operator port*[*port*]] *destination*[*destination-wildcard*] [*operator port*[*port*]] 例： `Router(config-ext-nacl)# deny ip any 172.20.1.1`	（任意）ステートメントに指定されたすべての条件に一致するすべてのパケットを拒否します。 • このステートメントは、非フラグメントパケットと初期フラグメントに適用されます。
ステップ 5	[*sequence-number*] **deny** *protocol source*[*source-wildcard*][*operator port*[*port*]] *destination*[*destination-wildcard*] [*operator port*[*port*]] **fragments** 例： `Router(config-ext-nacl)# deny ip any 172.20.1.1 fragments`	（任意）ステートメントに指定されたすべての条件に一致するすべてのパケットを拒否します。 • このステートメントは、非初期フラグメントに適用されます。
ステップ 6	[*sequence-number*] **permit** *protocol source*[*source-wildcard*] [*operator port*[*port*]] *destination*[*destination-wildcard*] [*operator port*[*port*]] 例： `Router(config-ext-nacl)# permit tcp any any`	ステートメントに指定されたすべての条件に一致するすべてのパケットを許可します。 • 各アクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。 • *source-wildcard* または *destination-wildcard* を省略すると、0.0.0.0 のワイルドカードマスクが想定されます。つまり、それぞれ送信元アドレスまたは宛先アドレスの全ビットへの一致を意味します。 • 必要に応じて、**any** キーワードを、*source source-wildcard* または *destination destination-wildcard* の代わりに使用してアドレスと 0.0.0.0 255.255.255.255 のワイルドカードを指定します。

	コマンドまたはアクション	目的
ステップ 7	アクセス リストの基本となる値を指定するまで、ステップ 4 ～ 6 を適宜組み合わせて繰り返します。	明示的に許可されていないすべての送信元は、アクセス リストの末尾にある暗黙的な **deny** ステートメントで拒否されます。
ステップ 8	**end** 例： `Router(config-ext-nacl)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 9	**showipaccess-list** 例： `Router# show ip access-list`	（任意）現在の IP アクセス リストすべてのコンテンツが表示されます。

次の作業

アクセスリストをインターフェイスに適用するか、アクセスリストを受け入れるコマンドから参照します。

（注） IP オプションを含むすべてのパケットを効率的に除去するには、グローバル **ip options drop** コマンドを設定することを推奨します。

IP アクセス リストの精緻化の設定例

例：アクセス リストのエントリの並べ替え

次に、並べ替える前と後のアクセス リストの例を示します。開始値は 1、増分値は 2 です。後続のエントリはユーザ指定の増分値に基づいて並べられています。範囲は 1 ～ 2147483647 です。

シーケンス番号のないエントリが入力されると、デフォルトで、アクセス リストの最後のエントリのシーケンス番号に 10 を加えたシーケンス番号が割り当てられます。

```
Router# show access-list carls
Extended IP access list carls
    10 permit ip host 10.3.3.3 host 172.16.5.34
    20 permit icmp any any
    30 permit tcp any host 10.3.3.3
    40 permit ip host 10.4.4.4 any
    50 Dynamic test permit ip any any
    60 permit ip host 172.16.2.2 host 10.3.3.12
    70 permit ip host 10.3.3.3 any log
```

```
    80 permit tcp host 10.3.3.3 host 10.1.2.2
    90 permit ip host 10.3.3.3 any
    100 permit ip any any
Router(config)# ip access-list extended carls
Router(config)# ip access-list resequence carls 1 2
Router(config)# end
Router# show access-list carls
Extended IP access list carls
    1 permit ip host 10.3.3.3 host 172.16.5.34
    3 permit icmp any any
    5 permit tcp any host 10.3.3.3
    7 permit ip host 10.4.4.4 any
    9 Dynamic test permit ip any any
    11 permit ip host 172.16.2.2 host 10.3.3.12
    13 permit ip host 10.3.3.3 any log
    15 permit tcp host 10.3.3.3 host 10.1.2.2
    17 permit ip host 10.3.3.3 any
    19 permit ip any any
```

例：シーケンス番号を指定したエントリの追加

次の例では、新しいエントリ（シーケンス番号 15）がアクセス リストに追加されます。

```
Router# show ip access-list
Standard IP access list tryon
2 permit 10.4.4.2, wildcard bits 0.0.255.255
5 permit 10.0.0.44, wildcard bits 0.0.0.255
10 permit 10.0.0.1, wildcard bits 0.0.0.255
20 permit 10.0.0.2, wildcard bits 0.0.0.255
Router(config)# ip access-list standard tryon
Router(config-std-nacl)# 15 permit 10.5.5.5 0.0.0.255
Router# show ip access-list
Standard IP access list tryon
2 permit 10.4.0.0, wildcard bits 0.0.255.255
5 permit 10.0.0.0, wildcard bits 0.0.0.255
10 permit 10.0.0.0, wildcard bits 0.0.0.255
15 permit 10.5.5.0, wildcard bits 0.0.0.255
20 permit 10.0.0.0, wildcard bits 0.0.0.255
```

例：シーケンス番号を指定しないエントリの追加

次に、シーケンス番号が指定されていないエントリをアクセス リストの末尾に追加する方法を示します。シーケンス番号のないエントリを追加すると、自動的にシーケンス番号が割り当てられ、アクセス リストの末尾に配置されます。デフォルトの増分値は 10 であるため、エントリには、既存のアクセス リストの最後のエントリのシーケンス番号に 10 を加えたシーケンス番号が割り当てられます。

```
Router(config)# ip access-list standard resources
Router(config-std-nacl)# permit 10.1.1.1 0.0.0.255
Router(config-std-nacl)# permit 10.2.2.2 0.0.0.255
Router(config-std-nacl)# permit 10.3.3.3 0.0.0.255
Router# show access-list
Standard IP access list resources
10 permit 10.1.1.1, wildcard bits 0.0.0.255
20 permit 10.2.2.2, wildcard bits 0.0.0.255
30 permit 10.3.3.3, wildcard bits 0.0.0.255
Router(config)# ip access-list standard resources
Router(config-std-nacl)# permit 10.4.4.4 0.0.0.255
Router(config-std-nacl)# end
Router# show access-list
Standard IP access list resources
10 permit 10.1.1.1, wildcard bits 0.0.0.255
20 permit 10.2.2.2, wildcard bits 0.0.0.255
```

```
30 permit 10.3.3.3, wildcard bits 0.0.0.255
40 permit 10.4.4.4, wildcard bits 0.0.0.255
```

例：IP アクセス リスト エントリに適用された時間範囲

次の例では、月曜日から金曜日の 午前 8 時から午後 6 時の間の、no-http と呼ばれる時間範囲を作成します。この時間帯は、**deny** ステートメントに適用されるため、月曜日から金曜日の午前 8 時から午後 6 時の HTTP トラフィックが拒否されます。

udp-yes と呼ばれる時間範囲は、正午から午後 8 時までの週末を定義します。この時間範囲は、**permit** ステートメントに適用されるため、土曜日から日曜日の正午から午後 8 時の UDP トラフィックのみが許可されます。両方のステートメントを含むアクセス リストは、10 ギガビット イーサネット インターフェイス 4/1/0 のインバウンド パケットに適用されます。

```
time-range no-http
 periodic weekdays 8:00 to 18:00
!
time-range udp-yes
 periodic weekend 12:00 to 20:00
!
ip access-list extended strict
 deny tcp any any eq http time-range no-http
 permit udp any any time-range udp-yes
!
interface TenGigabitEthernet4/1/0
 ip access-group strict in
```

例：IP パケット フラグメントのフィルタリング

次のアクセス リストでは、最初のステートメントはホスト 172.16.1.1 を宛先とする非初期フラグメントのみを拒否します。2 番目のステートメントは、ホスト 172.16.1.1 の TCP ポート 80 を宛先とする残りの非フラグメントと初期フラグメントのみを許可します。3 番目のステートメントは、その他のすべてのトラフィックを拒否します。すべての TCP ポートで非初期フラグメントをブロックするため、ホスト 172.16.1.1 のポート 80 をはじめとするすべての TCP ポートで非初期フラグメントをブロックする必要があります。つまり、非初期フラグメントにはレイヤ 4 ポート情報は含まれないため、指定のポートで該当するトラフィックをブロックするには、すべてのポートのフラグメントをブロックする必要があります。

```
access-list 101 deny ip any host 172.16.1.1 fragments
access-list 101 permit tcp any host 172.16.1.1 eq 80
access-list 101 deny ip any any
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

関連項目	マニュアル タイトル
time-range コマンドを使用した時間帯の確立	『*Cisco IOS XE Network Management Configuration Guide*』の「Performing Basic System Management」章
ネットワーク管理コマンドの説明	『*Cisco IOS Network Management Command Reference*』

標準

規格	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IP アクセス リストの精緻化に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *148* : *IP* アクセス リストの精緻化に関する機能情報

機能名	リリース	機能情報
IP アクセス リスト	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 58 章

IP 名前付きアクセス コントロール リスト

アクセス コントロール リスト（ACL）は、ネットワークを通過するパケットの動きを制御するためにパケット フィルタリングを実行します。パケット フィルタリングは、ネットワークへのトラフィックのアクセスを限定し、ユーザおよびデバイスのネットワークに対するアクセスを制限し、トラフィックがネットワークから流出するのを防ぐことで、セキュリティを提供します。IP アクセス リストによって、スプーフィングやサービス妨害攻撃の可能性を軽減し、ファイアウォールを介した動的で一時的なユーザ アクセスが可能になります。

IP 名前付きアクセス コントロール リスト機能により、ネットワーク管理者は、管理するアクセス リストを識別するための名前を使用することができます。

このモジュールでは、IP 名前付きアクセス コントロール リスト、およびその設定方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

- IP 名前付きアクセス コントロール リストに関する機能情報，1009 ページ

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *149*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

IP 名前付きアクセス コントロール リストに関する情報

アクセス リストの定義

アクセスコントロールリスト（ACL）は、ネットワークを通過するパケットの動きを制御するためにパケットフィルタリングを実行します。パケットフィルタリングは、ネットワークへのトラフィックのアクセスを限定し、ユーザおよびデバイスのネットワークに対するアクセスを制限し、トラフィックがネットワークから流出するのを防ぐことで、セキュリティを提供します。IP アクセス リストによって、スプーフィングやサービス妨害攻撃の可能性を軽減し、ファイアウォールを介した動的で一時的なユーザ アクセスが可能になります。

また、IP アクセス リストは、セキュリティ以外の用途にも使用できます。たとえば、帯域幅制御、ルーティング アップデートのコンテンツの制限、ルートの再配布、ダイヤルオンデマンド（DDR）呼び出しのトリガー、デバッグ出力の制限、Quality of Service（QoS）機能のトラフィックの識別と分類などです。

アクセス リストは、少なくとも 1 つの **permit** ステートメント、および任意の 1 つまたは複数の **deny** ステートメントで構成される順次リストです。IP アクセス リストの場合、これらのステートメントは IP アドレス、上位層の IP プロトコルなどの IP パケットのフィールドに適用できます。

アクセス リストは名前または番号で識別および参照されます。アクセス リストはパケット フィルタとして動作し、各アクセス リストに定義されている条件に基づいてパケットがフィルタされます。

アクセス リストを構成した後でアクセス リストを有効にするには、アクセス リストをインターフェイスに適用するか（**ipaccess-group** コマンドを使用）、vty に適用するか（**access-class** コマンドを使用）、またはアクセスリストを許容するあらゆるコマンドでアクセスリストを参照する必要があります。複数のコマンドから同じアクセス リストを参照できます。

次の構成では、branchoffices という名前の IP アクセス リストが 10 ギガビット イーサネット インターフェイス 4/1/0 上で構成され、着信パケットに適用されます。発信元アドレスとマスクのペアで指定されているネットワーク以外は、10 ギガビット イーサネット インターフェイス 4/1/0 にアクセスできません。ネットワーク 172.16.7.0 上の送信元から発信されるパケットの宛先に、制限はありません。ネットワーク 172.16.2.0 上の送信元から発信されるパケットの宛先は、172.31.5.4 にする必要があります。

```
ip access-list extended branchoffices
 10 permit 172.16.7.0 0.0.0.3 any
 20 permit 172.16.2.0 0.0.0.255 host 172.31.5.4
!
interface TenGigabitEthernet4/1/0
 ip access-group branchoffices in
```

名前付きまたは番号付きアクセス リスト

すべてのアクセスリストは、名前または番号で識別されます。名前付きアクセスリストは、番号付きアクセス リストよりも便利です。タスクを思いだしやすく関連性がある、わかりやすい名前を指定できるためです。名前付きアクセス リストでは、ステートメントの順序を変更したり、ステートメントを追加したりできます。

名前付きアクセスリストは、番号付きアクセスリストではサポートされない次の機能をサポートします。

- IP オプションのフィルタリング
- 非隣接ポート
- TCP フラグ フィルタリング
- **nopermit** または **nodeny** コマンドでのエントリの削除

（注） 番号付きアクセス リストを受け入れるコマンドの中には、名前付きアクセス リストを受け入れないコマンドがあります。たとえば、vty には番号付きアクセス リストだけを使用します。

IP アクセス リストの利点

アクセスコントロールリスト（ACL）は、ネットワークを通過するパケットのフローを制御するためにパケットフィルタリングを実行します。パケットフィルタリングによってユーザおよびデバイスのネットワークに対するアクセスを制限し、セキュリティの手段として利用できます。アクセスリストによってトラフィック数を減らすことで、ネットワークリソースを節約できます。アクセス リストを使用した場合の利点は次のとおりです。

- 着信 rsh および rcp 要求を認証する：アクセス リストは、デバイスへのアクセスを制御するように構成された認証データベース内のローカル ユーザ、リモート ホスト、およびリモート ユーザの識別を簡素化できます。Cisco ソフトウェアは認証データベースを使用して、リモート シェル（rsh）およびリモート コピー（rcp）プロトコルの着信要求を受け取ることができます。
- 不要なトラフィックまたはユーザをブロックする：アクセスリストを使用すると、インターフェイス上の着信パケットまたは発信パケットをフィルタできるため、送信元アドレス、宛先アドレス、またはユーザ認証に基づいてネットワークへのアクセスを制御できます。また、アクセス リストを使用して、デバイス インターフェイスで転送またはブロックするトラフィックの種類を決定することもできます。たとえば、電子メール トラフィックはネットワークでルーティングすることを許可し、すべての Telnet トラフィックはネットワークに入ることをブロックするようにアクセス リストを使用できます。
- vty へのアクセスを制御する：インバウンド vty（Telnet）でのアクセス リストは、デバイスへの回線にアクセスできるユーザを制御できます。アウトバウンド vty でのアクセス リストは、デバイスからの回線が到達可能な宛先を制御できます。
- QoS 機能のトラフィックを特定または分類する：アクセス リストは、Weighted Random Early Detection（WRED）および専用アクセス レート（CAR）の IP プレシデンスを設定することで、輻輳回避を提供します。また、クラスベース均等化キューイング（CBWFQ）、プライオリティ キューイング、カスタム キューイングのために輻輳管理を提供します。
- debug コマンド出力を制限する：アクセス リストは、IP アドレスやプロトコルに基づいて debug 出力を制限できます。

- 帯域幅制御を提供する：低速リンクでのアクセス リストはネットワークでの過剰なトラフィックを防止できます。
- NAT 制御を提供する：アクセス リストによって、ネットワーク アドレス変換（NAT）が変換するアドレスを制御できます。
- DoS 攻撃の可能性を低減する：アクセス リストは、サービス妨害（DoS）攻撃の可能性を低減させます。ホストからのトラフィック、ネットワーク、またはネットワークにアクセスするユーザを制御するようにIP発信元アドレスを指定します。TCPインターセプト機能を設定することで、接続に関する要求でサーバにフラッディングが発生しないようにすることができます。
- ルーティング アップデートの内容を制限する：アクセス リストによって、ネットワーク内で送信、受信、または再配布されるルーティング アップデートを制御できます。
- ダイヤルオンデマンド コールをトリガーする：アクセス リストによって、ダイヤルおよび切断条件を適用できます。

アクセス リストのルール

アクセス リストには、次のルールが適用されます。

- 1 つのインターフェイス、1 つのプロトコル、1 つの方向につき、許可されるアクセス リストは 1 つだけです。
- アクセス リストには少なくとも 1 つの **permit** ステートメントが含まれる必要があります。そうしないと、ネットワークに入るすべてのパケットが拒否されます。
- アクセス リスト条件または一致基準の構成順序は重要です。パケットを転送するかブロックするかを決定するときに、Cisco ソフトウェアは、それぞれの条件ステートメントに対してステートメントの作成順にパケットをテストします。一致が見つかると、条件ステートメントはそれ以上チェックされません。同じ **permit** または **deny** ステートメントでも、順序が異なる場合、ある状況では通過し、別の状況では拒否されるパケットが生じる可能性があります。
- アクセス リストを名前によって参照したときに、そのアクセス リストが存在しない場合は、すべてのパケットが通過します。インターフェイスまたはコマンドに空のアクセス リストを適用すると、ネットワークに対するすべてのトラフィックが許可されます。
- 標準のアクセス リストと拡張のアクセス リストの名前は同じにできません。
- パケットが発信インターフェイスにルーティングされる前に、着信アクセス リストがパケットを処理します。ネットワークへのパケット アクセスを拒否するフィルタ条件がある着信アクセス リストは、ルーティング ルックアップ時のオーバーヘッドを削減します。構成されたフィルタ基準に基づいてネットワークへのアクセスを許可されたパケットはルーティング処理されます。着信アクセス リストの場合、**permit** ステートメントを構成するとパケットは受信後に処理され、**deny** ステートメントを構成するとパケットは破棄されます。
- 発信アクセス リストの場合、パケットの処理後にデバイスから送信されます。着信パケットは発信インターフェイスにルーティングされてから、発信アクセス リストで処理されます。

発信アクセス リストの場合、**permit** ステートメントを構成するとパケットは出力バッファに送信され、**deny** ステートメントを構成するとパケットは破棄されます。

- アクセス リストで、デバイスに到達するトラフィック、またはデバイス経由で送信されるトラフィックは制御できますが、デバイスが送信元のトラフィックは制御できません。

IP アクセス リストを作成する際に役立つヒント

意図しない結果を回避し、より効率的で有効なアクセス リストを作成するために役立つヒントを紹介します。

- アクセス リストを作成してから、インターフェイス（または別の対象）に適用します。その理由は、存在しないアクセス リストをインターフェイスに適用してから、アクセス リストを設定すると、最初のステートメントが有効になり、それに続く暗黙の **deny** ステートメントによって即時のアクセスに問題が発生するおそれがあるためです。
- アクセス リストを設定してから適用するもう 1 つの理由は、空のアクセス リストが適用されたインターフェイスはすべてのトラフィックを許可するためです。
- すべてのアクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。そうでない場合、すべてのパケットは拒否され、トラフィックはまったく通過しません。
- 最初に（**permit** または **deny** ステートメントに対する）一致が見つかった後は条件のテストが終了するため、パケットが一致する可能性の高いステートメントをアクセス リストの先頭に配置すると処理にかかる時間とリソースが削減されます。最も頻繁に発生する条件を発生頻度の低い条件より前に配置します。
- ネットワークまたはサブネットのより具体的な参照が、より全般的な参照よりも前に出現するように、アクセス リストを構成します。
- まだ拒否されていないその他のパケットすべてを許可する場合、ステートメント **permit any any** を使用します。ステートメント **permit any any** を使用すると、実質的に、アクセス リストの末尾にある暗黙の deny ステートメントでその他すべてのパケットが拒否されることを防ぎます。最初のアクセス リスト エントリは、**permit any any** にしないでください。すべてのトラフィックが通過し、以降のテストに到達するパケットがなくなります。**permit any any** を指定すると、まだ拒否されていないすべてのトラフィックが通過します。
- すべてのアクセス リストは、暗黙の **deny** ステートメントで終わりますが、明示的な **deny** ステートメント（たとえば、**deny ip any any** など）を使用することを推奨します。ほとんどのプラットフォームでは、**show access-list** コマンドを発行して拒否されるパケット数を表示し、アクセス リストが許可していないパケットに関する詳細情報を調査できます。明示的な **deny** ステートメントで拒否されたパケットのみがカウントされます。これは、明示的な **deny** ステートメントによって、より詳細なデータが生成されるためです。
- アクセス リストの作成中、または作成後に、エントリを削除する場合があります。
  - 番号付きアクセス リストからはエントリを削除できません。削除しようとすると、アクセス リスト全体が削除されます。エントリを削除する必要がある場合、アクセス リスト全体を削除してから最初から作り直す必要があります。

- 名前付きアクセス リストからはエントリを削除できます。**no permit** または **no deny** コマンドを使用して、該当するエントリを削除します。

- 個々のステートメントの用途をひと目で確認および理解しやすくするために、**remark** コマンドを使用して、ステートメントの前後に役立つ注記を書き込むことができます。
- 特定のホストまたはネットワークに対するアクセスを拒否し、そのネットワークまたはホストの誰かがアクセスしようとしたかどうかを検出する場合、対応する **log** ステートメントを指定した **deny** キーワードを含めます。それによって、その送信元からの拒否されたパケットがログに記録されます。
- このヒントは、アクセス リストの配置に適用されます。リソースを保存しようとすると、着信アクセス リストでは常にフィルタ条件を適用した後に、ルーティング テーブルの検索を行います。発信アクセス リストではフィルタ条件を適用する前に、ルーティング テーブルの検索を行います。

アクセス リストを適用する場所

アクセスリストは、デバイスの着信または発信インターフェイスに適用できます。アクセスリストを着信インターフェイスに適用すると、インターフェイスで着信するトラフィックが制御され、アクセス リストを発信インターフェイスに適用すると、インターフェイスから発信されるトラフィックが制御されます。

ソフトウェアは、着信インターフェイスでパケットを受信すると、アクセス リストで設定されているステートメントに対してパケットを検査します。アクセス リストがアドレスを許可している場合は、ソフトウェアはパケットを処理します。着信パケットをフィルタリングするためにアクセス リストを適用すると、フィルタリングされたパケットはデバイスに到達する前に廃棄されるため、デバイスのリソースを節約できます。

発信インターフェイスでは、アクセス リストはインターフェイスから転送（送信）されたパケットをフィルタリングします。発信インターフェイスで Rate-Based Satellite Control Protocol（RBSCP）の TCP アクセス コントロール リスト（ACL）を使用して、発信インターフェイスで TCP 確認応答（ACK）を受けるパケットの種類を制御できます。

debug コマンドを使用してアクセス リストを参照し、デバッグ ログの量を制限できます。たとえば、アクセスリストのフィルタリング基準または一致基準に基づいて、デバッグ ログを送信元または宛先のアドレスまたはプロトコルに制限できます。

アクセス リストを使用して、ルーティング アップデート、ダイヤルオンデマンド（DDR）、および Quality of Service（QoS）機能を制御することができます。

IP 名前付きアクセス コントロール リストの設定方法

IP 名前付きアクセス リストの作成

IP 名前付きアクセス リストを作成すると、発信元アドレスと宛先アドレス、またはアドレスと他の IP フィールドの組み合わせをフィルタリングすることができます。名前付きアクセスリストにより、分かりやすい名前の付いたアクセス リストを特定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**ip access-list extended** *name* 例： `Device(config)# ip access-list extended acl1`	名前を使用して拡張 IP アクセス リストを定義し、拡張名前付きアクセス リストのコンフィギュレーション モードを開始します。
ステップ 4	**remark** *remark* 例： `Device(config-ext-nacl)# remark protect server by denying sales access to the acl1 network`	（任意）アクセス リスト ステートメントに説明を追加します。 • 注釈は IP アクセス リスト エントリの前または後に指定できます。 • この例では、**remark** コマンドは、ステップ 5 で設定された **deny** コマンドがインターフェイスに対する Sales ネットワーク アクセスを拒否することをネットワーク管理者に示します。
ステップ 5	**deny** *protocol* [*source source-wildcard*] {**any** | **host** {*address* | *name*} {*destination* [*destination-wildcard*] {**any** | **host** {*address* | *name*} [**log**]	（任意）注釈で指定されたすべての条件に一致するパケットをすべて拒否します。

	コマンドまたはアクション	目的
	例： `Device(config-ext-nacl)# deny ip 192.0.2.0 0.0.255.255 host 192.0.2.10 log`	
ステップ 6	**remark** *remark* 例： `Device(config-ext-nacl)# remark allow TCP from any source to any destination`	（任意）アクセス リスト ステートメントに説明を追加します。 • 注釈は IP アクセス リスト エントリの前または後に指定できます。
ステップ 7	**permit** *protocol* [*source source-wildcard*] {**any** | **host** {*address* | *name*} {*destination* [*destination-wildcard*] {**any** | **host** {*address* | *name*} [**log**] 例： `Device(config-ext-nacl)# permit tcp any any`	ステートメントで指定されたすべての条件に一致するパケットをすべて許可します。
ステップ 8	アクセス リストにステートメントをさらに指定するには、ステップ 4 ～ 7 を繰り返します。	（注） ステートメントによって明示的に許可されていないすべての送信元アドレスは、アクセス リストの末尾にある暗黙的な deny ステートメントで拒否されます。
ステップ 9	**end** 例： `Device(config-ext-nacl)# end`	拡張名前付きアクセス リストのコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 10	**show ip access-lists** 例： `Device# show ip access-lists`	現在のすべての IP アクセス リストの内容を表示します。

例：

以下は、 **show ip access-lists** コマンドの出力例です。

```
Device# show ip access-lists acl1

Extended IP access list acl1
   permit tcp any 192.0.2.0 255.255.255.255 eq telnet
   deny tcp any any
   deny udp any 192.0.2.0 255.255.255.255 lt 1024
   deny ip any any log
```

インターフェイスへのアクセス リストの適用

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**interface** *type number* 例： `Device(config)# interface TenGigabitEthernet4/1/0`	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipaccess-group** {*access-list-number* | *access-list-name*} {**in** | **out**} 例： `Device(config-if)# ip access-group acl1 in`	指定したアクセス リストをインバウンド インターフェイスに適用します。 • 送信元アドレスをフィルタリングするには、インバウンド インターフェイスにアクセス リストを適用します。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IP 名前付きアクセス コントロール リストの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IP 名前付きアクセス コントロール リストに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *150* : *IP* 名前付きアクセス コントロール リストに関する機能情報

機能名	リリース	機能情報
IP アクセス リスト	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 59 章

IPv4 ACL チェーニング サポート

マルチアクセス コントロール リストとも呼ばれる ACL チェーニングにより、アクセス コントロール リスト（ACL）を分割することができます。このモジュールでは、IPv4 ACL チェーニング サポートによって ACL を共通 ACL とユーザ専用 ACL に明示的に分割する方法、および両 ACL をデバイスでのトラフィック フィルタリングのためにバインドする方法について説明します。この方法では、Ternary Content Addressable Memory（TCAM）内の共通 ACL は複数のターゲットにより共有され、これによりリソース使用量が削減されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *151* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

IPv4 ACL チェーニング サポートの制限事項

- 単一のアクセス コントロール リスト（ACL）を、同じ方向の同じターゲットに対する共通、標準の両 ACL に使用することはできません。

- ACL チェーニングはセキュリティ ACL にのみ適用されます。サービス品質（QoS）、ファイアウォール サービス モジュール（FW）、ポリシーベース ルーティング（PBR）などのフィーチャ ポリシーではサポートされません。
- 共通 ACL ではターゲットごとの統計情報はサポートされません。

IPv4 ACL チェーニング サポートに関する情報

ACL チェーニングの概要

パケット フィルタリング プロセスは、1 つのインターフェイスの 1 つの方向および 1 つのプロトコルごとに適用される単一のアクセス コントロール リスト（ACL）のみをサポートします。そのため、多数のインターフェイスに共通ACLエントリが必要な場合、管理性と拡張性の問題が生じます。そのようなインターフェイスにはすべて重複アクセス コントロール エントリ（ACE）が設定されており、共通 ACE の変更はすべての ACL で行われる必要があります。

インターネット サービス プロバイダー（ISP）のエッジ ボックスの典型的な ACL には次の 2 組の ACE が含まれます。

- 共通 ISP 専用 ACE
- 顧客/インターフェイス専用 ACE

これらのアドレス ブロックは、ISP の保護されたインフラストラクチャ ネットワークへのアクセスを拒否するため、および顧客の送信元アドレス ブロックのみを許可することでスプーフィングを防ぐために行われます。この結果、インターフェイスごとに一意のACLが設定され、ほとんどの ACE がデバイス上のすべての ACL で共通になります。ACL をプロビジョニングし、変更するのは非常に面倒ですが、ACE を変更すれば全ターゲットに影響を及ぼすことができます。

IPv4 ACL チェーニング サポート

IPv4 ACL チェーニング サポートを使用して、アクセス コントロール リスト（ACL）を共通 ACL と顧客専用 ACL に分割したり、両 ACL を共通セッションにアタッチすることができます。この方法では、共通 ACL を 1 コピーのみ Ternary Content Addressable Memory（TCAM）にアタッチしこれを全ユーザで共有することで、共通 ACE の維持が簡略化されます。

IPv4 ACL チェーニング機能により、次の 2 つの IPv4 ACL を 1 方向ごとに 1 つのインターフェイスでアクティブにできます。

- 共通
- 標準
- 共通と標準

（注） 1 つのインターフェイスで共通と標準の両 ACL を設定している場合、共通 ACL が標準 ACL に優先されます。

IPv4 ACL チェーニング サポートの設定方法

ACL チェーニングは、**ip traffic filter** コマンドによってサポートされています。

ip traffic filter コマンドは積み上げ可能ではありません。このコマンドを使用すると、このコマンドの以前のインスタンスが置き換えられます。

詳細については、『Security Configuration Guide: Access Control Lists Configuration Guide』の「*IPv6 ACL Chaining with a Common ACL*」セクションを参照してください。

共通 ACL を受け入れるインターフェイスの設定

このタスクを実行すると、インターフェイス固有の ACL とともに、共通のアクセス コントロール リスト（ACL）を受け入れるようにインターフェイスを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**interface** *type number* 例： `Device(config)# interface TenGigabitEthernet4/1/0`	インターフェイスを設定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipaccess-group** {**common** {*common-access-list-name* {*regular-access-list* | **acl**}}{**in** | **out**}} 例： `Device(config-if)# ipv4 access-group common acl-p acl1 in`	インターフェイス固有の ACL とともに、共通 ACL を受け入れるようにインターフェイスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-if)# end`	（任意）コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPv4 ACL チェーニング サポートの設定例

ここでは、共通アクセス コントロール リスト（ACL）の設定例を示します。

例：共通 ACL を受け入れるインターフェイスの設定

次に、ACL を明示的に削除しないでインターフェイスで設定したアクセス コントロール リスト（ACL）を交換する方法例を示します。

```
interface TenGigabitEthernet4/1/0
ipv4 access-group common  C_acl ACL1 in
end
replace interface acl ACL1 by ACL2
interface TenGigabitEthernet4/1/0
ipv4 access-group common  C_acl ACL2 in
end
```

次に、インターフェイスから共通 ACL を明示的に削除しないと、共通 ACL をインターフェイスで交換できない理由を示します。

```
interface TenGigabitEthernet4/1/0
ipv4 access-group common  C_acl1 ACL1 in
end
change the common acl to C_acl2
interface TenGigabitEthernet4/1/0
no ipv4 access-group common  C_acl1  ACL1 in
end
interface TenGigabitEthernet4/1/0
ipv4 access-group common  C_acl2  ACL1 in
end
```

（注） 共通 ACL を再設定すると、ライン カードの他のインターフェイスが共通 ACL に取り付けられないことを確認する必要があります。

（注） 共通 ACL とインターフェイス ACL の両方をインターフェイスに取り付け、その一方をインターフェイスで再構成すると、他は自動的に削除されます。

次に、インターフェイス ACL の削除方法を示します。

```
interface TenGigabitEthernet4/1/0
ipv4 access-group common C_acl1 ACL1 in
end
```

IPv4 ACL チェーニング サポートの追加参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 ACL チェーニング サポート	『Security Configuration Guide: Access Control Lists』
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv4 ACL チェーニング サポートに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *152*：*IPv4 ACL* チェーニング サポートに関する機能情報

機能名	リリース	機能情報
IP アクセス リスト	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 60 章

共通 ACL による IPv6 ACL チェーニング

マルチアクセス コントロール リストとも呼ばれる ACL チェーニングにより、ACL を分割することができます。このマニュアルでは、IPv6 ACL チェーニング サポートによって ACL を共通 ACL とユーザ専用 ACL に明示的に分割する方法、および両 ACL をデバイスでのトラフィック フィルタリングのためにバインドする方法について説明します。この方法では、Ternary Content Addressable Memory（TCAM）内の共通 ACL は複数のターゲットにより共有され、これによりリソース使用量が削減されます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *153* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

共通 ACL による IPv6 ACL チェーニングに関する情報

ACL チェーニングの概要

パケット フィルタリング プロセスは、1 つのインターフェイスの 1 つの方向および 1 つのプロトコルごとに適用される単一のアクセス コントロール リスト（ACL）のみをサポートします。そのため、多数のインターフェイスに共通ACLエントリが必要な場合、管理性と拡張性の問題が生じます。そのようなインターフェイスにはすべて重複アクセス コントロール エントリ（ACE）が設定されており、共通 ACE の変更はすべての ACL で行われる必要があります。

インターネット サービス プロバイダー（ISP）のエッジ ボックスの典型的な ACL には次の 2 組の ACE が含まれます。

- 共通 ISP 専用 ACE
- 顧客/インターフェイス専用 ACE

これらのアドレス ブロックは、ISP の保護されたインフラストラクチャ ネットワークへのアクセスを拒否するため、および顧客の送信元アドレス ブロックのみを許可することでスプーフィングを防ぐために行われます。この結果、インターフェイスごとに一意のACLが設定され、ほとんどの ACE がデバイス上のすべての ACL で共通になります。ACL をプロビジョニングし、変更するのは非常に面倒ですが、ACE を変更すれば全ターゲットに影響を及ぼすことができます。

共通 ACL による IPv6 ACL チェーニング

IPv6 ACL チェーニングを使用して、トラフィック フィルタを次の ACL とチェーニングできます。

- 共通 ACL
- 専用 ACL
- 共通 ACL と専用 ACL

各アクセス コントロール リスト（ACL）は順に照合されます。たとえば、共通 ACL と専用 ACL の両方を指定している場合、パケットはまず共通ACLに対して照合され、一致が見つからなければ専用 ACL に対して照合されます。

（注） 任意の IPv6 ACL を共通または専用 ACL としてトラフィック フィルタで設定できます。ただし、同じ ACL を同じトラフィック フィルタで共通と専用の両方として指定することはできません。

共通 ACL による IPv6 ACL チェーニングの設定方法

はじめる前に

IPv6 ACL のチェーニングは、既存の IPv6 traffic-filter コマンド：**ipv6 traffic-filter** [**common** *common-acl*] [*specific-acl*] [**in** | **out**] の拡張機能を使用して、インターフェイス上で設定します。

（注） 次のいずれかを設定できます。

- 共通 ACL のみ。例：**ipv6 traffic-filter common** *common-acl*
- 特定の ACL のみ。例：**ipv6 traffic-filter** *common-acl*
- 両方の ACL。例：**ipv6 traffic-filter common** *common-acl specific-acl*

ipv6 traffic-filter コマンドは追加式ではありません。このコマンドを使用すると、このコマンドの以前のインスタンスが置き換えられます。たとえば、コマンド シーケンス **ipv6 traffic-filter** [**common** *common-acl*] [*specific-acl*] **in ipv6 traffic-filter** [*specific-acl*] **in** は共通 ACL をトラフィック フィルタにバインドし、共通 ACL を削除して、特定の ACL をバインドします。

インターフェイスへの IPv6 ACL の設定

このタスクを実行すると、インターフェイス固有の ACL とともに、共通のアクセス コントロール リスト（ACL）を受け入れるようにインターフェイスを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**interface** *type number* 例： `Device(config)# interface TenGigabitEthernet4/1/0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**ipv6traffic filter** {*common-access-list-name* {**in** | **out**}} 例： `Device(config)# ipv6 traffic-filter outbound out`	指定したIPv6アクセスリストを、前のステップで指定したインターフェイスに適用します。
ステップ 5	**end** 例： `Device(config-if)# end`	（任意）コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

共通 ACL による IPv6 ACL チェーニングの設定例

特定の順序でなくても、次の組み合わせを設定できます。

- 共通 ACL、たとえば： **ipv6 traffic-filter common** *common-acl* **in**
- 特定の ACL、たとえば： **ipv6 traffic-filter** *specific-acl* **in**
- 両方の ACL、たとえば： **ipv6 traffic-filter common** *common-acl specific-acl* **in**

例：共通 ACL を受け入れるインターフェイスの設定

次に、ACL を明示的に削除しないでインターフェイスで設定したアクセス コントロール リスト（ACL）を交換する方法例を示します。

```
interface TenGigabitEthernet4/1/0
ipv6 access-group common  C_acl ACL1 in
end
replace interface acl ACL1 by ACL2
interface TenGigabitEthernet4/1/0
ipv6 access-group common  C_acl ACL2 in
end
```

次の例では、共通ACLをインターフェイスから削除する方法を示します。インターフェイスから共通 ACL を明示的に削除しないと、共通 ACL をインターフェイスで交換できません。

```
interface TenGigabitEthernet4/1/0
ipv6 access-group common  C_acl1 ACL1 in
end
change the common acl to C_acl2
interface TenGigabitEthernet4/1/0
no ipv6 access-group common  C_acl1  ACL1 in
end
interface TenGigabitEthernet4/1/0
ipv6 access-group common  C_acl2  ACL1 in
end
```

（注） 共通 ACL を再設定すると、ライン カードの他のインターフェイスが共通 ACL に取り付けされないことを確認する必要があります。

（注） 共通 ACL とインターフェイス ACL の両方をインターフェイスに取り付け、その一方をインターフェイスで再構成すると、他は自動的に削除されます。

次に、インターフェイス ACL を削除する方法を示します。

```
interface TenGigabitEthernet4/1/0
ipv6 access-group common C_acl1 ACL1 in
end
```

共通 ACL による IPv6 ACL チェーニングの追加情報

関連資料

関連項目	マニュアル タイトル
IPv4 ACL チェーニング サポート	『Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

共通 ACL による IPv6 ACL チェーニングに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *154*：共通 *ACL* による *IPv6 ACL* チェーニングに関する機能情報

機能名	リリース	機能情報
IPv6 アクセス リスト	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 61 章

注釈付きの IP アクセス リスト エントリ

注釈付きの IP アクセス リスト エントリ機能により、**deny** または **permit** 条件に関するコメントや備考をどの IP アクセスリストにも含めることができます。これらの注釈は、ネットワーク管理者がアクセス リストを理解するのを容易にします。各注釈の長さは 100 文字に制限されます。

このモジュールは、注釈付きの IP アクセス リスト エントリ機能に関する情報を提供します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *155* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

注釈付き IP アクセス リスト エントリに関する情報

IP アクセス リストの利点

アクセスコントロールリスト（ACL）は、ネットワークを通過するパケットのフローを制御するためにパケットフィルタリングを実行します。パケットフィルタリングによってユーザおよびデバイスのネットワークに対するアクセスを制限し、セキュリティの手段として利用できます。アクセスリストによってトラフィック数を減らすことで、ネットワークリソースを節約できます。アクセス リストを使用した場合の利点は次のとおりです。

- 着信 rsh および rcp 要求を認証する：アクセス リストは、デバイスへのアクセスを制御するように構成された認証データベース内のローカル ユーザ、リモート ホスト、およびリモート ユーザの識別を簡素化できます。Cisco ソフトウェアは認証データベースを使用して、リモート シェル（rsh）およびリモート コピー（rcp）プロトコルの着信要求を受け取ることができます。
- 不要なトラフィックまたはユーザをブロックする：アクセス リストを使用すると、インターフェイス上の着信パケットまたは発信パケットをフィルタできるため、送信元アドレス、宛先アドレス、またはユーザ認証に基づいてネットワークへのアクセスを制御できます。また、アクセス リストを使用して、デバイス インターフェイスで転送またはブロックするトラフィックの種類を決定することもできます。たとえば、電子メール トラフィックはネットワークでルーティングすることを許可し、すべての Telnet トラフィックはネットワークに入ることをブロックするようにアクセス リストを使用できます。
- vty へのアクセスを制御する：インバウンド vty（Telnet）でのアクセス リストは、デバイスへの回線にアクセスできるユーザを制御できます。アウトバウンド vty でのアクセス リストは、デバイスからの回線が到達可能な宛先を制御できます。
- QoS 機能のトラフィックを特定または分類する：アクセス リストは、Weighted Random Early Detection（WRED）および専用アクセス レート（CAR）の IP プレシデンスを設定することで、輻輳回避を提供します。また、クラスベース均等化キューイング（CBWFQ）、プライオリティ キューイング、カスタム キューイングのために輻輳管理を提供します。
- debug コマンド出力を制限する：アクセス リストは、IP アドレスやプロトコルに基づいて debug 出力を制限できます。
- 帯域幅制御を提供する：低速リンクでのアクセスリストはネットワークでの過剰なトラフィックを防止できます。
- NAT 制御を提供する：アクセス リストによって、ネットワーク アドレス変換（NAT）が変換するアドレスを制御できます。
- DoS 攻撃の可能性を低減する：アクセス リストは、サービス妨害（DoS）攻撃の可能性を低減させます。ホストからのトラフィック、ネットワーク、またはネットワークにアクセスするユーザを制御するように IP 発信元アドレスを指定します。TCP インターセプト機能を設定することで、接続に関する要求でサーバにフラッディングが発生しないようにすることができます。

- ルーティング アップデートの内容を制限する：アクセス リストによって、ネットワーク内で送信、受信、または再配布されるルーティング アップデートを制御できます。
- ダイヤルオンデマンド コールをトリガーする：アクセス リストによって、ダイヤルおよび切断条件を適用できます。

アクセス リストの注釈

任意のIPアクセスリストのエントリについて、コメントまたは注釈を含めることができます。アクセス リストの注釈は、アクセス リスト エントリの前後にあるオプションの注釈です。エントリの内容がわかるので、エントリの目的を解釈する必要はありません。各注釈の長さは 100 文字に制限されます。

コメントは、**permit** または **deny** ステートメントの前後どちらにでも配置できます。注釈を追加する場所には一貫性があるようにしてください。注釈が関連する **permit** または **deny** ステートメントの前にある場合と後にある場合とが混在すると、ユーザが混乱する可能性があります。

後続の **deny** ステートメントの機能を説明する注釈の例を次に示します。

```
ip access-list extended telnetting
 remark Do not allow host1 subnet to telnet out
 deny tcp host 172.16.2.88 any eq telnet
```

注釈付き IP アクセス リスト エントリの設定方法

名前付きまたは番号付きアクセス リストへの注釈の書き込み

名前付きまたは番号付きアクセスリスト設定を使用できます。作業する設定用にアクセスリストを作成したら、アクセス リストをインターフェイスまたは端末回線に適用する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例**： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** **例**： `Device# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**ip access-list** {**standard** | **extended**} {*name* | *number*} 例： `Device(config)# ip access-list extended telnetting`	名前または番号でアクセス リストを特定し、拡張名前付きアクセス リスト コンフィギュレーション モードを開始します。
ステップ 4	**remark** *remark* 例： `Device(config-ext-nacl)# remark Do not allow host1 subnet to telnet out`	名前付き IP アクセス リストのエントリに注釈を追加します。 • 注釈は、**permit** または **deny** ステートメントの目的を示します。
ステップ 5	**deny** *protocol* **host** *host-address* **any eq** *port* 例： `Device(config-ext-nacl)# deny tcp host 172.16.2.88 any eq telnet`	パケットを拒否する名前付き IP アクセス リストの条件を設定します。
ステップ 6	**end** 例： `Device(config-ext-nacl)# end`	拡張名前付きアクセス リスト コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

注釈付き IP アクセス リスト エントリの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

注釈付き IP アクセス リスト エントリに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *156*：注釈付き *IP* アクセス リスト エントリに関する機能情報

機能名	リリース	機能情報
IP アクセス リスト	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 62 章

標準 IP アクセス リストのロギング

標準 IP アクセス リストのロギング機能は、標準 IP アクセス リストによって許可または拒否されるパケットに関するメッセージをロギングする機能を提供します。アクセス リストに一致するパケットによって、デバイス コンソールにあるパケットに関する情報メッセージがロギングされます。

このモジュールは、標準 IP アクセス リスト ロギングに関する情報を提供します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *157* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

標準 IP アクセス リストのロギングに関する制限事項

IP アクセス リスト ロギングは、ルーティング インターフェイスまたはルータ アクセス コントロール リスト（ACL）でのみサポートされます。

標準 IP アクセス リストのロギングに関する情報

標準 IP アクセス リストのロギング

標準 IP アクセス リストのロギング機能は、標準 IP アクセス リストによって許可または拒否されるパケットに関するメッセージをロギングする機能を提供します。アクセス リストに一致するパケットによって、デバイス コンソールに送信されるパケットに関する情報ロギング メッセージが生成されます。デバイス コンソールに印刷されるメッセージのログ レベルは、**logging console** コマンドによって制御されます。

アクセス リストが最初に検査したパケットがアクセス リストをトリガーし、デバイス コンソールにメッセージをロギングします。後続のパケットは、5 分間隔で収集された後、表示またはロギングされます。ログ メッセージには、アクセス リスト番号、パケットの送信元 IP アドレス、その送信元からの、直前の 5 分間隔に許可または拒否されたパケットの数、およびパケットが許可されたか拒否されたかに関する情報が含まれます。特定のアクセス リストによって許可または拒否された複数のパケットについて、各パケットの送信元アドレスなどをモニタすることができます。

標準 IP アクセス リストのロギングの設定方法

番号を使用した標準 IP アクセス リストの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**access-list** *access-list-number* {**deny** | **permit**} **host** *address* [**log**] 例： `Device(config)# access-list 1 permit host 10.1.1.1 log`	送信元アドレスとワイルドカードを使用して、標準の名前付き IP アクセス リストを定義し、デバイス コンソールでアクセス リスト エントリと一致したパケットに関する情報メッセージのロギングを設定します。

	コマンドまたはアクション	目的
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} **any** [**log**] 例： `Device(config)# access-list 1 permit any log`	送信元の省略形および送信元マスク 0.0.0.0 255.255.255.255 を使用して、標準の 名前付き IP アクセス リストを定義します。
ステップ 5	**interface** *type number* 例： `Device(config)# interface TenGigabitEthernet4/1/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ip access-group** *access-list-number* {**in** | **out**} 例： `Device(config-if)# ip access-group 1 in`	指定した番号付きアクセス リストを着信または発信インターフェイスに適用します。 • 送信元アドレスに基づいてフィルタする場合、一般的に、着信インターフェイスにアクセス リストを適用します。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

名前を使用した標準 IP アクセス リストの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**ip access-list standard** *name* 例： `Device(config)# ip access-list standard acl1`	標準の IP アクセス リストを定義して、標準の名前付きアクセス リスト コンフィギュレーション モードを開始します。
ステップ 4	{**deny** | **permit**} {**host** *address* | **any**} **log** 例： `Device(config-std-nacl)# permit host 10.1.1.1 log`	パケットがネットワークに入らないように拒否したり、パケットがネットワークに入ることを許可したりする名前付き IP アクセス リストで条件を設定し、デバイス コンソールでアクセス リスト エントリと一致するパケットに関する情報メッセージのロギングを設定します。
ステップ 5	**exit** 例： `Device(config-std-nacl)# exit`	標準の名前付きアクセス リスト コンフィギュレーション モードを終了し、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 6	**interface** *type number* 例： `Device(config)# interface TenGigabitEthernet4/1/0`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**ip access-group** *access-list-name* {**in** | **out**} 例： `Device(config-if)# ip access-group acl1 in`	指定したアクセス リストを着信または発信インターフェイスに適用します。 • 送信元アドレスに基づいてフィルタする場合、一般的に、着信インターフェイスにアクセス リストを適用します。
ステップ 8	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

標準 IP アクセス リストのロギングの設定例

例：デバッグ出力の制限

次の例では、アクセス リストを使用して、**debug** コマンド出力を制限します。**debug** 出力を制限すると、対象へのデータ量が制限され、時間とリソースの節約につながります。

```
Device(config)# ip access-list acl1
Device(config-std-nacl)# remark Displays only advertisements for LDP peer in acl1
Device(config-std-nacl)# permit host 10.0.0.44

Device# debug mpls ldp advertisements peer-acl acl1

tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.17.0.33
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.16.0.31
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 172.22.0.33
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.0.1
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.0.3
tagcon: peer 10.0.0.44:0 (pp 0x60E105BC): advertise 192.168.1.33
```

標準 IP アクセス リストのロギングに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

標準 IP アクセス リストのロギングに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *158*：標準 *IP* アクセス リストのロギングに関する機能情報

機能名	リリース	機能情報
IP アクセス リスト	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 63 章

IP アクセス リスト エントリ シーケンス番号

IP アクセス リスト エントリ シーケンス番号機能により、**permit** または **deny** ステートメントにシーケンス番号を適用したり、名前付き IP アクセス リストでそのようなステートメントを順序変更、追加、削除することができます。IP アクセス リスト エントリ シーケンス番号機能を使用すると、IP アクセス リストを非常に簡単に変更することができます。この機能以前は、アクセス リストの末尾にしかアクセス リスト エントリを追加できませんでした。そのため、名前付き IP アクセス リストの末尾以外のどこかにステートメントを追加する必要がある場合、アクセス リスト全体の再設定が必要でした。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

- その他の参考資料，1053 ページ
- IP アクセス リスト エントリ シーケンス番号に関する機能情報，1053 ページ

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *159*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

IP アクセス リストのエントリ シーケンス番号に関する制約事項

- この機能は、ダイナミック アクセス リスト、再帰アクセス リスト、またはファイアウォール アクセス リストをサポートしていません。
- また、名前付きアクセス リストよりも古くから存在する、旧式のスタイルで番号付けされたアクセス リストもサポートしていません。アクセス リストは番号で指定できるため、標準または拡張名前付きアクセス リスト（NACL）コンフィギュレーション モードでは番号を入力することができます。

IP アクセス リストのエントリ シーケンス番号に関する情報

IP アクセス リストの目的

アクセスリストは、パケットフィルタリングを実行して、ネットワークを介して移動するパケットとその場所を制御します。この処理は、ネットワーク トラフィックを制限し、ユーザやデバイスによるネットワークへのアクセスを制限するのに役立ちます。アクセス リストの用途は多様なので、多くのコマンドの構文でアクセスリストが参照されます。アクセスリストを使用して、次のようなことを実行できます。

- インターフェイスでの着信パケットのフィルタリング
- インターフェイスでの発信パケットのフィルタリング
- ルーティング アップデートの内容の制限
- アドレスまたはプロトコルに基づくデバッグ出力の制限
- 仮想端末回線アクセスの制御
- 輻輳回避、輻輳管理、プライオリティおよびカスタムキューイングなどの高度な機能に使用されるトラフィックの特定または分類
- ダイヤルオンデマンド ルーティング（DDR）呼び出しのトリガー

IP アクセス リストの機能

アクセス リストは、permit ステートメントと deny ステートメントで構成される順次リストです。これらのステートメントは、IP アドレス、場合によっては上位層 IP プロトコルに適用されます。アクセスリストには、参照に使用される名前があります。多くのソフトウェア コマンドは、構文の一部としてアクセス リストを受け取ります。

アクセスリストを設定して名前を付けることは可能ですが、アクセスリストを受け取るコマンドによってアクセス リストが参照されるまで、有効にはなりません。複数のコマンドから同じアクセスリストを参照できます。アクセスリストで、デバイスに到達するトラフィック、またはデバ

イス経由で送信されるトラフィックは制御できますが、デバイスが送信元のトラフィックは制御できません。

IP アクセス リストのプロセスとルール

- アクセス リストの条件に対してフィルタリングされる各パケットの送信元アドレスや宛先アドレス、またはプロトコルがテストされます。一度に 1 つの条件（**permit** または **deny** ステートメント）がテストされます。
- パケットがアクセス リストのステートメントに一致しないと、そのパケットはリスト内の次のステートメントに対してテストされます。
- パケットとアクセス リスト ステートメントが一致すると、リスト内の残りのステートメントはスキップされ、パケットは一致したステートメントに指定されたとおりに許可または拒否されます。パケットが許可されるか拒否されるかは、パケットが一致する最初のエントリによって決まります。つまり、一致すると、それ以降のエントリは考慮されません。
- アクセス リストでアドレスまたはプロトコルが拒否されると、パケットは廃棄され、インターネット制御メッセージ プロトコル（ICMP）ホスト到達不能メッセージが返されます。
- 一致する条件がない場合は、パケットはドロップされます。これは、各アクセス リストは暗黙の **deny** ステートメントで終了するためです。言い換えると、パケットが各ステートメントに対してテストされたときまでに許可されないと、このパケットは拒否されます。
- 最初に一致が見つかった後は条件のテストが終了するため、条件の順序は重要です。同じ **permit** または **deny** ステートメントでも、順序が異なる場合、ある状況では通過し、別の状況では拒否されるパケットが生じる可能性があります。
- コマンドでアクセス リストを名前によって参照したときに、そのアクセス リストが存在しない場合は、すべてのパケットが通過します。
- 1 つのインターフェイス、1 つのプロトコル、1 つの方向につき、許可されるアクセス リストは 1 つだけです。
- インバウンド アクセス リストは、デバイスに到達するパケットを処理します。着信パケットの処理後に、アウトバウンドインターフェイスへのルーティングが行われます。インバウンド アクセス リストが効率的なのは、フィルタリング テストで拒否されたことでパケットが廃棄される場合、ルーティング検索のオーバーヘッドが抑えられるためです。パケットがテストで許可されると、そのパケットに対してルーティングの処理が実施されます。インバウンド リストの場合、**permit** とは、インバウンド インターフェイスで受信したパケットを引き続き処理することを意味します。**deny** とは、パケットを破棄することです。
- 発信アクセス リストの場合、パケットの処理後にデバイスから送信されます。着信パケットはアウトバウンド インターフェイスにルーティングされてから、アウトバウンド アクセス リストで処理されます。アウトバウンド リストの場合、**permit** とは、出力バッファに対して送信されることを示し、**deny** とは、パケットが廃棄されることを示します。

IP アクセス リストを作成する際に役立つヒント

意図しない結果を回避し、より効率的で有効なアクセス リストを作成するために役立つヒントを紹介します。

- アクセス リストを作成してから、インターフェイス（または別の対象）に適用します。その理由は、存在しないアクセス リストをインターフェイスに適用してから、アクセス リストを設定すると、最初のステートメントが有効になり、それに続く暗黙の **deny** ステートメントによって即時のアクセスに問題が発生するおそれがあるためです。
- アクセス リストを設定してから適用するもう 1 つの理由は、空のアクセス リストが適用されたインターフェイスはすべてのトラフィックを許可するためです。
- すべてのアクセス リストには、少なくとも 1 つの **permit** ステートメントが必要です。そうでない場合、すべてのパケットは拒否され、トラフィックはまったく通過しません。
- 最初に（**permit** または **deny** ステートメントに対する）一致が見つかった後は条件のテストが終了するため、パケットが一致する可能性の高いステートメントをアクセス リストの先頭に配置すると処理にかかる時間とリソースが削減されます。最も頻繁に発生する条件を発生頻度の低い条件より前に配置します。
- ネットワークまたはサブネットのより具体的な参照が、より全般的な参照よりも前に出現するように、アクセス リストを構成します。
- まだ拒否されていないその他のパケットすべてを許可する場合、ステートメント **permit any any** を使用します。ステートメント **permit any any** を使用すると、実質的に、アクセス リストの末尾にある暗黙の deny ステートメントでその他すべてのパケットが拒否されることを防ぎます。最初のアクセス リスト エントリは、**permit any any** にしないでください。すべてのトラフィックが通過し、以降のテストに到達するパケットがなくなります。**permit any any** を指定すると、まだ拒否されていないすべてのトラフィックが通過します。
- すべてのアクセス リストは、暗黙の **deny** ステートメントで終わりますが、明示的な **deny** ステートメント（たとえば、**deny ip any any** など）を使用することを推奨します。ほとんどのプラットフォームでは、**show access-list** コマンドを発行して拒否されるパケット数を表示し、アクセス リストが許可していないパケットに関する詳細情報を調査できます。明示的な **deny** ステートメントで拒否されたパケットのみがカウントされます。これは、明示的な **deny** ステートメントによって、より詳細なデータが生成されるためです。
- アクセス リストの作成中、または作成後に、エントリを削除する場合があります。
  - 番号付きアクセス リストからはエントリを削除できません。削除しようとすると、アクセス リスト全体が削除されます。エントリを削除する必要がある場合、アクセス リスト全体を削除してから最初から作り直す必要があります。
  - 名前付きアクセス リストからはエントリを削除できます。**no permit** または **no deny** コマンドを使用して、該当するエントリを削除します。
- 個々のステートメントの用途をひと目で確認および理解しやすくするために、**remark** コマンドを使用して、ステートメントの前後に役立つ注記を書き込むことができます。

- 特定のホストまたはネットワークに対するアクセスを拒否し、そのネットワークまたはホストの誰かがアクセスしようとしたかどうかを検出する場合、対応する **log** ステートメントを指定した **deny** キーワードを含めます。それによって、その送信元からの拒否されたパケットがログに記録されます。
- このヒントは、アクセス リストの配置に適用されます。リソースを保存しようとすると、着信アクセス リストでは常にフィルタ条件を適用した後に、ルーティング テーブルの検索を行います。発信アクセス リストではフィルタ条件を適用する前に、ルーティング テーブルの検索を行います。

送信元アドレスと宛先アドレス

IP パケットの送信元アドレスと宛先アドレスのフィールドは、アクセス リストの基礎となる典型的な 2 つのフィールドです。送信元アドレスを指定して、特定のネットワーキング デバイスまたはホストから送信されるパケットを制御します。宛先アドレスを指定して、特定のネットワーキング デバイスまたはホストに送信されるパケットを制御します。

ワイルドカード マスクと暗黙のワイルドカード マスク

アドレス フィルタリングでは、アクセス リスト エントリ内のアドレス ビットとアクセス リストに送信されるパケットを比較する際、対応する IP アドレス ビットを確認するか無視するかを決定するために、ワイルドカードマスクが使用されます。管理者は、ワイルドカードマスクを慎重に設定することにより、許可または拒否のテストに 1 つまたは複数の IP アドレスを選択できます。

IP アドレス ビット用のワイルドカード マスクでは、数値 1 と数値 0 を使用して、対応する IP アドレス ビットをどのように扱うかを指定します。1 と 0 は、サブネット（ネットワーク）マスクで意味する内容が対照的なため、ワイルドカード マスクは逆マスクとも呼ばれます。

- ワイルドカード マスク ビット 0 は、対応するビット値を確認することを示します。
- ワイルドカード マスク ビット 1 は、対応するビット値を無視することを示します。

アクセス リスト ステートメントの送信元アドレスまたは宛先アドレスでワイルドカード マスクを指定しない場合、0.0.0.0 というデフォルトのワイルドカード マスクが想定されます。

サブネット マスクでは、ネットワークとサブネットを示す隣接ビットをマスクにする必要がありますが、それとは異なり、ワイルドカード マスクではマスクに非隣接ビットを使用できます。

トランスポート層の情報

トランスポート層の情報（パケットが TCP、UDP、Internet Control Message Protocol（ICMP）または Internet Group Management Protocol（IGMP）パケットであるか、などの情報）に基づいてパケットをフィルタできます。

利点：IP アクセス リスト エントリ シーケンス番号

IP アクセス リスト エントリにシーケンス番号を適用する機能によって、アクセス リストの変更が簡易になります。IP アクセス リスト エントリ シーケンス番号機能の前には、アクセス リスト内のエントリの位置を指定する方法はありませんでした。既存のリストの途中にエントリ（ステートメント）を挿入するには、目的の位置の後ろにあるすべてのエントリを削除する必要がありました。次に、新しいエントリを追加したら、先に削除したすべてのエントリを再入力する必要がありました。これは手間がかかり、エラーが起こりやすい方法です。

IP アクセス リスト エントリ シーケンス番号機能を使用すると、アクセス リスト エントリにシーケンス番号を追加し、リスト内のエントリを並べ替えることができます。新しいエントリを追加する場合、アクセス リストの目的の位置にエントリが挿入されるようにシーケンス番号を選択できます。必要に応じて、アクセス リストの現在のエントリを並べ替えて、新しいエントリを挿入できる場所を作成できます。

シーケンス番号の動作

- 以前のリリースとの下位互換性を保つため、シーケンス番号のないエントリが適用された場合には、最初のエントリにはシーケンス番号 10 が割り当てられます。連続してエントリを追加すると、シーケンス番号は 10 ずつ増分されます。最大シーケンス番号は 2147483647 です。生成したシーケンス番号がこの最大値を超えると、次のメッセージが表示されます。

```
Exceeded maximum sequence number.
```

- シーケンス番号のないエントリを 1 つ入力すると、アクセス リストの最後のシーケンス番号に 10 を加えたシーケンス番号が割り当てられ、リストの末尾に配置されます。
- （シーケンス番号以外が）既存のエントリに一致するエントリを入力すると、何も変更されません。
- 既存のシーケンス番号を入力すると、次のエラー メッセージが表示されます。

```
Duplicate sequence number.
```

- グローバル コンフィギュレーション モードで新しいアクセス リストを入力すると、そのアクセス リストのシーケンス番号が自動的に生成されます。
- ルート プロセッサ（RP）のエントリとラインカード（LC）のエントリのシーケンス番号を常に同期できるように、分散機能がサポートされています。
- シーケンス番号が不揮発性生成（NVGEN）されることはありません。つまり、シーケンス番号自体は保存されません。システムのリロード時には、設定されたシーケンス番号はデフォルトのシーケンス開始番号とその番号からの増分に戻されます。この機能は、シーケンス番号をサポートしないソフトウェア リリースとの下位互換性を保つために提供されています。

- IP アクセス リスト エントリ シーケンス番号機能では、名前付き標準アクセス リストと拡張 IP アクセス リストが使用されます。アクセス リストの名前を番号として指定できるため、番号も使用できます。

IP アクセス リストでのシーケンス番号の使用法

アクセス リスト エントリの順序付けとアクセス リストの変更

ここでは、名前付きIPアクセスリストのエントリにシーケンス番号を割り当てる方法と、アクセス リストに対するエントリの追加または削除を行う方法を説明します。この作業を実行する場合は、次の点に注意してください。

- アクセス リスト エントリの並べ替えは任意です。この作業での並べ替えのステップは、機能の目的の 1 つであり、またその機能の説明が必要と思われることから、必要に応じて説明します。
- 次の手順で、**permit** コマンドはステップ 5 に、**deny** コマンドはステップ 6 に記載されています。ただし、その順番を入れ替えることもできます。設定のニーズに合わせた順番を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**ipaccess-listresequence** *access-list-name starting-sequence-number increment* 例： `Device(config)# ip access-list resequence kmd1 100 15`	開始シーケンス番号と、シーケンス番号の増分を使用して、指定した IP アクセス リストを並べ替えます。

	コマンドまたはアクション	目的
ステップ 4	**ipaccess-list**{**standard**| **extended**} *access-list-name* 例： `Device(config)# ip access-list standard kmd1`	名前で IP アクセス リストを指定し、名前付きアクセス リストのコンフィギュレーション モードを開始します。 • **standard** を指定する場合は、標準アクセス リスト構文を使用して、**permit** または **deny** ステートメント（場合によっては両方）を指定します。 • **extended** を指定する場合は、拡張アクセス リスト構文を使用して、**permit** または **deny** ステートメント（場合によっては両方）を指定します。
ステップ 5	次のいずれかを実行します。 • *sequence-number* **permit** *source source-wildcard* • *sequence-number* **permit** *protocol source source-wildcard destination destination-wildcard*[**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-std-nacl)# 105 permit 10.5.5.5 0.0.0 255`	名前付き IP アクセス リスト モードで permit ステートメントを指定します。 • このアクセス リストでは、**permit** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。 • プロンプトに示されるとおり、このアクセス リストは標準アクセスリストでした。ステップ 4 で **extended** を指定した場合は、このステップのプロンプトは Device(config-ext-nacl) となり、拡張 **permit** コマンド構文を使用します。
ステップ 6	次のいずれかを実行します。 • *sequence-number* **deny** *source source-wildcard* • *sequence-number* **deny** *protocol source source-wildcard destination destination-wildcard*[**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-std-nacl)# 105 deny 10.6.6.7 0.0.0 255`	（任意）名前付き IP アクセス リスト モードで deny ステートメントを指定します。 • このアクセス リストでは、**permit** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。 • プロンプトに示されるとおり、このアクセス リストは標準アクセスリストでした。ステップ 4 で **extended** を指定した場合は、このステップのプロンプトは Device(config-ext-nacl) となり、拡張 **deny** コマンド構文を使用します。

	コマンドまたはアクション	目的
ステップ 7	次のいずれかを実行します。 • *sequence-number* **permit** *source source-wildcard* • *sequence-number* **permit** *protocol source source-wildcard destination destination-wildcard*[**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# 150 permit tcp any any log`	名前付き IP アクセス リスト モードで permit ステートメントを指定します。 • このアクセス リストでは、**permit** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。 • 上位層プロトコル（ICMP、IGMP、TCP、および UDP）を許可するその他のコマンド構文については、permit（IP）コマンドを参照してください。 • エントリを削除するには、**no** *sequence-number* コマンドを使用します。
ステップ 8	次のいずれかを実行します。 • *sequence-number* **deny** *source source-wildcard* • *sequence-number* **deny** *protocol source source-wildcard destination destination-wildcard*[**precedence** *precedence*][**tos** *tos*] [**log**] [**time-range** *time-range-name*] [**fragments**] 例： `Device(config-ext-nacl)# 150 deny tcp any any log`	（任意）名前付き IP アクセス リスト モードで deny ステートメントを指定します。 • このアクセス リストでは、**permit** ステートメントを最初に使用していますが、必要なステートメントの順序に応じて、**deny** ステートメントが最初に使用される可能性もあります。 • 上位層プロトコル（ICMP、IGMP、TCP、および UDP）を許可するその他のコマンド構文については、deny（IP）コマンドを参照してください。 • エントリを削除するには、**no** *sequence-number* コマンドを使用します。
ステップ 9	必要に応じてシーケンス番号ステートメントを追加するには、ステップ 5 とステップ 6 を繰り返します。	アクセス リストは変更できます。
ステップ 10	**end** 例： `Device(config-std-nacl)# end`	（任意）コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 11	**showipaccess-lists** *access-list-name* 例： `Device# show ip access-lists kmd1`	（任意）IPアクセス リストの内容を表示します。

例

アクセス リストに新しいエントリが含まれていることを確認するには、**showipaccess-lists** コマンドの出力を確認します。

```
Device# show ip access-lists kmd1

Standard IP access list kmd1
100 permit 10.4.4.0, wildcard bits 0.0.0.255
105 permit 10.5.5.0, wildcard bits 0.0.0.255
115 permit 10.0.0.0, wildcard bits 0.0.0.255
130 permit 10.5.5.0, wildcard bits 0.0.0.255
145 permit 10.0.0.0, wildcard bits 0.0.0.255
```

IP アクセス リスト エントリ シーケンス番号の設定例

例：アクセス リストのエントリの並べ替え

次に、アクセス リストを並べ替える例を示します。開始値は 1、増分値は 2 です。後続のエントリは指定の増分値に基づいて並べられています。範囲は 1 ～ 2147483647 です。

シーケンス番号のないエントリが入力されると、デフォルトで、アクセス リストの最後のエントリのシーケンス番号に 10 を加えたシーケンス番号が割り当てられます。

```
Device# show access-list 150

Extended IP access list 150
    10 permit ip host 10.3.3.3 host 172.16.5.34
    20 permit icmp any any
    30 permit tcp any host 10.3.3.3
    40 permit ip host 10.4.4.4 any
    50 Dynamic test permit ip any any
    60 permit ip host 172.16.2.2 host 10.3.3.12
    70 permit ip host 10.3.3.3 any log
    80 permit tcp host 10.3.3.3 host 10.1.2.2
    90 permit ip host 10.3.3.3 any
    100 permit ip any any

Device(config)# ip access-list extended 150
Device(config)# ip access-list resequence 150 1 2
Device(config)# exit

Device# show access-list 150

Extended IP access list 150
    1 permit ip host 10.3.3.3 host 172.16.5.34
```

```
3 permit icmp any any
10 permit tcp any any eq 22 log
5 permit tcp any host 10.3.3.3
7 permit ip host 10.4.4.4 any
9 Dynamic test permit ip any any
11 permit ip host 172.16.2.2 host 10.3.3.12
13 permit ip host 10.3.3.3 any log
15 permit tcp host 10.3.3.3 host 10.1.2.2
17 permit ip host 10.3.3.3 any
19 permit ip any any
```

例：シーケンス番号を持つエントリの追加

次に、指定のアクセス リストに新しいエントリを追加する例を示します。

```
Device# show ip access-list

Standard IP access list tryon
2 permit 10.4.4.2, wildcard bits 0.0.255.255
5 permit 10.0.0.44, wildcard bits 0.0.0.255
10 permit 10.0.0.1, wildcard bits 0.0.0.255
20 permit 10.0.0.2, wildcard bits 0.0.0.255

Device(config)# ip access-list standard tryon
Device(config-std-nacl)# 15 permit 10.5.5.5 0.0.0.255
Device(config-std-nacl)# exit
Device(config)# exit
Device# show ip access-list

Standard IP access list tryon
2 permit 10.4.0.0, wildcard bits 0.0.255.255
5 permit 10.0.0.0, wildcard bits 0.0.0.255
10 permit 10.0.0.0, wildcard bits 0.0.0.255
15 permit 10.5.5.0, wildcard bits 0.0.0.255
20 permit 10.0.0.0, wildcard bits 0.0.0.255
```

例：シーケンス番号のないエントリ

次に、シーケンス番号が指定されていないエントリをアクセス リストの末尾に追加する方法を示します。シーケンス番号のないエントリを追加すると、自動的にシーケンス番号が割り当てられ、アクセス リストの末尾に配置されます。デフォルトの増分値は 10 であるため、エントリには、既存のアクセス リストの最後のエントリのシーケンス番号に 10 を加えたシーケンス番号が割り当てられます。

```
Device(config)# ip access-list standard 1
Device(config-std-nacl)# permit 10.1.1.1 0.0.0.255
Device(config-std-nacl)# permit 10.2.2.2 0.0.0.255
Device(config-std-nacl)# permit 10.3.3.3 0.0.0.255
Device(config-std-nacl)## exit
Device# show access-list

Standard IP access list 1
10 permit 0.0.0.0, wildcard bits 0.0.0.255
20 permit 0.0.0.0, wildcard bits 0.0.0.255
30 permit 0.0.0.0, wildcard bits 0.0.0.255

Device(config)# ip access-list standard 1
Device(config-std-nacl)# permit 10.4.4.4 0.0.0.255
Device(config-std-nacl)# end
Device(config-std-nacl)## exit
Device# show access-list

Standard IP access list 1
```

```
10 permit 0.0.0.0, wildcard bits 0.0.0.255
20 permit 0.0.0.0, wildcard bits 0.0.0.255
30 permit 0.0.0.0, wildcard bits 0.0.0.255
40 permit 0.0.0.0, wildcard bits 0.0.0.255
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
IP アクセス リスト コマンド	『*Cisco IOS Security Command Reference*』
IP アクセス リストの設定	『Creating an IP Access List and Applying It to an Interface』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IP アクセス リスト エントリ シーケンス番号に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *160* : *IP* アクセス リスト エントリ シーケンス番号に関する機能情報

機能名	リリース	機能情報
IP アクセス リスト	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータに統合されました。

第 64 章

ACL IP オプションの選択的ドロップ

ACL IP オプションの選択的ドロップ機能を使用すると、Cisco ルータが IP オプションが設定されたパケットをフィルタしたり、ルータまたはダウンストリーム ルータ上での IP オプションの影響を軽減したりすることができるようになります。これは、これらのパケットをドロップするか、IP オプションの処理を無視することによって行われます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *161* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

ACL IP オプションの選択的ドロップの制約事項

リソース予約プロトコル（RSVP）（マルチプロトコル ラベル スイッチング トラフィック エンジニアリング（MPLS TE））、Internet Group Management Protocol バージョン2（IGMPv2）、および

IP オプション パケットを使用するその他のプロトコルは、ドロップまたは無視モードでは機能しない可能性があります。

ACL IP オプションの選択的ドロップに関する情報

ACL IP オプションの選択的ドロップの使用

ACL IP オプションの選択的ドロップ機能を使用すると、IP オプションが設定されたパケットをルータでフィルタできるようになります。これにより、これらのパケットのルータまたはダウンストリーム ルータへの影響を軽減し、次の手順を実行できます。

- 受信した IP オプション パケットをすべてドロップし、オプションがネットワークの奥深くまで入り込まないようにします。
- そのルータ宛ての IP オプション パケットを無視し、IP オプションが設定されていないものとして扱います。

多くのユーザにとっては、パケットのドロップが最善策であると言えます。ただし、正規の IP オプションが存在する可能性のある環境では、ルータ上のパケットのロード処理を減らすだけで十分です。したがって、ルータ上のオプション処理をスキップしたうえで、ピュア IP であるかのようにパケットを転送することができます。

ACL IP オプションの選択的ドロップを使用する利点

- ドロップ モードでは、ネットワークからのパケットをフィルタすることで、オプション パケットからロードするというダウンストリーム ルータおよびホストの負荷を軽減できます。
- ドロップ モードでは、分散システム上でのルート プロセッサ（RP）処理が必要となるオプションの RP へのロードが最小限に抑えられます。以前は、パケットは常に RP CPU でルーティングまたは処理されていました。現在は、無視またはドロップすることで、パケットが RP パフォーマンスに影響を及ぼすことを回避できます。

ACL IP オプションの選択的ドロップの設定方法

ACL IP オプションの選択的ドロップの設定

ここでは、ACL IP オプションの選択的ドロップ機能を設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**ipoptions** {**drop** | **ignore**} 例： `Router(config)# ip options drop`	ルータに送信された IP オプション パケットをドロップまたは無視します。
ステップ 4	**exit** 例： `Router(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**showiptraffic** 例： `Router# show ip traffic`	（任意）IP トラフィックの統計情報を表示します。

ACL IP オプションの選択的ドロップの設定例

例：ACL IP オプションの選択的ドロップの設定

次に、ネットワークに入ったすべてのオプション パケットをドロップするように、ルータ（およびダウンストリーム ルータ）を設定する例を示します。

```
Router(config)# ip options drop
% Warning:RSVP and other protocols that use IP Options packets may not function in drop or
 ignore modes.
end
```

例：ACL IP オプションの選択的ドロップの確認

以下は、**ip options drop** コマンドを使用した後の出力例です。

```
Router# show ip traffic
IP statistics:
  Rcvd:  428 total, 323 local destination
         0 format errors, 0 checksum errors, 0 bad hop count
         0 unknown protocol, 0 not a gateway
         0 security failures, 0 bad options, 0 with options
  Opts:  0 end, 0 nop, 0 basic security, 0 loose source route
         0 timestamp, 0 extended security, 0 record route
         0 stream ID, 0 strict source route, 0 alert, 0 cipso, 0 ump
         0 other, 30 ignored
  Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
         0 fragmented, 0 fragments, 0 couldn't fragment
  Bcast: 0 received, 0 sent
  Mcast: 323 received, 809 sent
  Sent:  809 generated, 591 forwarded
  Drop:  0 encapsulation failed, 0 unresolved, 0 no adjacency
         0 no route, 0 unicast RPF, 0 forced drop, 0 unsupported-addr
         0 options denied, 0 source IP address zero
```

IP アクセス リスト エントリ シーケンス番号の追加情報

ここでは、IP アクセス リストに関する関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
IP アクセス リストの設定	『Creating an IP Access List and Applying It to an Interface』
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
IP アクセス リスト コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

ACL IP オプションの選択的ドロップに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *162* : *ACL IP* オプションの選択的ドロップに関する機能情報

機能名	リリース	機能情報
IP アクセス リスト	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 65 章

ACL Syslog 相関

アクセス コントロール リスト（ACL）Syslog 相関機能では、アクセス コントロール エントリ（ACE）Syslog エントリにタグ（ユーザ定義の Cookie またはデバイスが生成した MD5 ハッシュ値）を追加します。このタグは Syslog エントリを生成した ACL 内で ACE を一意に特定します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *163* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

ACL Syslog 相関の前提条件

ACL Syslog 相関機能を設定する前に、「IP アクセス リストの概要」モジュールでその概念を理解する必要があります。

ACL Syslog 相関機能は、ユーザ定義の cookie またはデバイスで生成されるハッシュ値を syslog 内の ACE メッセージに追加します。ログ オプションが ACE に対してイネーブルになっている場合、これらの値は ACE メッセージにのみ追加されます。

ACL Syslog 相関に関する情報

ACL Syslog 相関タグ

ACL Syslog 相関機能では、アクセス コントロール エントリ（ACE）Syslog エントリにタグ（ユーザ定義の Cookie またはデバイスが生成した MD5 ハッシュ値）を追加します。このタグは Syslog エントリを生成した ACE を一意に特定します。

ネットワーク管理ソフトウェアでは、どの ACE が特定の Syslog イベントを生成したかを特定するためにタグを使用できます。たとえば、ネットワーク管理者はネットワーク管理アプリケーションで ACE 規則を選択し、次にその ACE ルールに対応する Syslog イベントを表示できます。

Syslog メッセージにタグを追加するには、Syslog イベントを生成する ACE でログ オプションが有効になっている必要があります。システムは各メッセージに 1 つのタイプのタグ（ユーザ定義の Cookie またはデバイスで生成した MD5 ハッシュ値）のみを追加します。

ユーザ定義の Cookie タグを指定するには、ユーザは ACE ログ オプションを構成する際に Cookie 値を入力する必要があります。Cookie は英数字形式である必要があります。64 文字以上にはできず、16 進数表記（0x など）で始めることはできません。

デバイスで生成した MD5 ハッシュ値タグを指定するには、ハッシュ生成機能をデバイスで有効にする必要があります。また、ACE ログ オプションを構成するときにユーザは Cookie 値を入力してはいけません。

ACE Syslog メッセージ

パケットが ACL 内のアクセス コントロール エントリ（ACE）と一致すると、そのイベントのログ オプションが有効になっているかどうかシステムでチェックされます。ログ オプションが有効な場合、ACL Syslog 相関機能がデバイスで構成されていると、システムは syslog メッセージにタグを付けます。タグは、標準情報に加えて syslog メッセージの最後に表示されます。

次は、ユーザ定義の Cookie タグを示すサンプル syslog メッセージです。

```
Jun 5 12:55:44.359: %SEC-6-IPACCESSLOGP: list logacl permitted tcp 192.168.16.1(38402) ->
192.168.16.2(23), 1 packet [User_permiited_ACE]
```

次は、ハッシュ値タグを示すサンプル syslog メッセージです。

```
Jun 5 12:55:44.359: %SEC-6-IPACCESSLOGP: list logacl permitted tcp 192.168.16.1(38402) ->
192.168.16.2(23), 1 packet [0x723E6E12]
```

ACL Syslog 相関の設定方法

デバイスでのハッシュ値生成の有効化

ユーザ定義 Cookie を使用して設定されていないシステム内でログをイネーブルにした各アクセスコントロール エントリ（ACE）の MD5 ハッシュ値を生成するデバイスを設定するには、このタスクを実行します。

ハッシュ値生成設定をイネーブルにすると、システムは既存のすべての ACE をチェックし、ハッシュ値を必要とする各 ACE のハッシュ値を生成します。ハッシュ値生成の設定をディセーブルにすると、これまでに生成されたすべてのハッシュ値がシステムから削除されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**ipaccess-listlogginghash-generation** 例： `Device(config)# ip access-list logging hash-generation`	デバイスでハッシュ値生成を有効にします。 • ログを有効にした ACE があり、ハッシュ値を必要とする場合、デバイスは自動的に値を生成し、コンソールでその値を表示します。
ステップ 4	**end** 例： `Device(config)# end`	（任意）グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	次のいずれかを実行します。 • **showipaccess-list** *access-list-number*	（任意）番号付きまたは名前付き IP アクセス リストの内容を表示します。 • ログをイネーブルにした ACE のアクセス リストに生成したハッシュ値が含まれることを確認するには、出力を見直します。

	コマンドまたはアクション	目的

	• **showipaccess-list** *access-list-name*
	
	例：
	`Device# show ip access-list 101`
	
	例：
	`Device# show ip access-list acl`	

デバイスでのハッシュ値生成の無効化

デバイスでのハッシュ値生成をディセーブルにするには、このタスクを実行します。ハッシュ値生成の設定をディセーブルにすると、これまでに生成されたすべてのハッシュ値がシステムから削除されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**noipaccess-listlogginghash-generation** 例： `Device(config)# no ip access-list logging hash-generation`	デバイスでのハッシュ値生成をディセーブルにします。 • これまでに作成されたハッシュ値がシステムから削除されます。
ステップ 4	**end** 例： `Device(config)# end`	（任意）グローバルコンフィギュレーション モードを終了し、特権EXECモードに戻ります。

	コマンドまたはアクション	目的

ステップ 5	次のいずれかを実行します。
	• **showipaccess-list** *access-list-number*
	• **showipaccess-list** *access-list-name*
	
	例：
	`Device# show ip access-list 101`
	
	例：
	`Device# show ip access-list acl`
		（任意）IPアクセスリストの内容を表示します。
		• ログをイネーブルにした ACE のアクセス リストに生成したハッシュ値が含まれないことを確認するには、出力を見直します。

ユーザ定義 Cookie を使用した ACL Syslog 相関の設定

syslog メッセージタグとしてユーザ定義の Cookie クッキーを使用し、特定のアクセス リストのデバイス上の ACL syslog 相関機能を設定するには、このタスクを実行します。

このセクションでは、番号付きアクセス リストのユーザ定義の Cookie を使用して、ACL Syslog 相関機能を設定する方法について例を示します。ただし、番号付きおよび名前付きアクセス リストの両方、標準および拡張アクセスリストの両方について、ユーザ定義の Cookie を使用し、ACL Syslog 相関機能を設定できます。

（注） 次の制限事項は、ユーザ定義の Cookie 値を選択する場合に適用されます。

- 最大文字数は 64 です。
- Cookie は 16 進表記（0x など）で始めることはできません。
- Cookie は、**reflect**、**fragment**、**time-range** キーワードと同じまたはその一部を使用することはできません。たとえば、reflect と ref は無効な値です。ただし、これらのキーワードを先頭に使用することはできます。たとえば、reflectedACE と fragment_33 は有効な値です。
- Cookie に設定できるのは英数字のみです。

>

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**access-list** *access-list-number* **permit** *protocol source destination* **log** *word* 例： `Device(config)# access-list 101 permit tcp host 10.1.1.1 host 10.1.1.2 log UserDefinedValue`	拡張 IP アクセス リストとユーザ定義の Cookie 値を定義します。 • Cookie 値の引数として *word* を入力します。
ステップ 4	**end** 例： `Device(config)# end`	（任意）グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**showipaccess-list** *access-list-number* 例： `Device# show ip access-list 101`	（任意）IP アクセス リストの内容を表示します。 • 出力を見直して、アクセス リストにユーザ定義の Cookie 値が含まれることを確認します。

例

以下は、ユーザ定義 Cookie 値に対する **showipaccess-list** コマンドの出力例です。

```
Device# show ip access-list
101
Extended IP access list 101
30 permit tcp host 10.1.1.1 host 10.1.1.2 log (tag = UserDefinedValue)
```

ハッシュ値を使用した ACL Syslog 相関の設定

syslog メッセージ タグとしてデバイスで生成されたハッシュ値を使用し、特定のアクセス リストのデバイス上の ACL Syslog 相関機能を設定するには、このタスクを実行します。

このセクションでは、番号付きアクセス リストのデバイスで生成されたハッシュ値を使用して、ACL Syslog 相関機能を設定する方法についてステップを示します。ただし、番号付きおよび名前付きアクセスリストの両方、標準および拡張アクセスリストの両方について、デバイスで生成されたハッシュ値を使用し、ACL Syslog 相関機能を設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**ipaccess-listlogginghash-generation** 例： `Device(config)# ip access-list logging hash-generation`	デバイスでハッシュ値生成を有効にします。 • ログを有効にした ACE があり、ハッシュ値を必要とする場合、デバイスは自動的に値を生成し、コンソールでその値を表示します。
ステップ 4	access-list *access-list-number* **permit** *protocol source destination* **log** 例： `Device(config)# access-list 102 permit tcp host 10.1.1.1 host 10.1.1.2 log`	拡張 IP アクセス リストを定義します。 • アクセス リストのログ オプションを有効にしますが、Cookie 値は指定しないでください。 • デバイスが、新たに定義したアクセス リストのハッシュ値を自動的に生成します。
ステップ 5	**end** 例： `Device(config)# end`	（任意）グローバル コンフィギュレーション モードを終了し、特権EXECモードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**showipaccess-list** *access-list-number* 例： `Device# show ip access-list 102`	（任意）IP アクセス リストの内容を表示します。 • 出力を見直して、アクセスリストにルータが生成したハッシュ値が含まれることを確認します。

例

以下は、device-generated ハッシュ値を有するアクセス リストに対する **showipaccess-list** コマンドの出力例です。

```
Device# show ip access-list
102
Extended IP access list 102
10 permit tcp host 10.1.1.1 host 10.1.1.2 log (hash = 0x7F9CF6B9)
```

ACL Syslog 相関タグ値の変更

ユーザ定義の Cookie の値を変更したり、ユーザ定義の Cookie とデバイスで生成したハッシュ値を置き換えたりするには、このタスクを実行します。

この手順は、番号付きアクセス リストの ACL Syslog 相関タグ値を変更する方法について示しています。ただし、番号付きおよび名前付きアクセスリストの両方と、標準および拡張アクセスリストの両方について、ACL Syslog 相関タグ値を変更できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	show access-list 例： `Device(config)# show access-list`	（任意）アクセス リストの内容を表示します。

	コマンドまたはアクション	目的
ステップ 3	**configure terminal** 例： `Device# configure terminal`	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 4	access-list *access-list-number* **permit** *protocol source destination* **log** *word*
	
	例：
	
	`Device(config)# access-list 101 permit tcp host 10.1.1.1 host 10.1.1.2 log NewUDV`
	
	例：
	
	`OR`
	
	例：
	
	例：
	
	`Device(config)# access-list 101 permit tcp any any log replacehash`
		Cookie を修正したり、ハッシュ値を Cookie に変更したりします。
		
		• アクセス リスト コンフィギュレーション コマンド全体を入力し、前のタグ値を新しいタグ値で置き換える必要があります。

ステップ 5	**end** 例： `Device(config)# end`	（任意）グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**showipaccess-list** *access-list-number* 例： `Device# show ip access-list 101`	（任意）IP アクセス リストの内容を表示します。 • 変更を確認するために出力結果を見直します。

トラブルシューティングのヒント

アクセス リストのデバッグ**debugipaccess-listhash-generation** ip access-list のハッシュ生成コマンドを使用します。次は、**debug** コマンド出力の例になります。

```
Device# debug ip access-list hash-generation
 Syslog hash code generation debugging is on
Device# show debug
```

```
IP ACL:
 Syslog hash code generation debugging is on
Device# no debug ip access-list hash-generation

 Syslog hash code generation debugging is off
Device# show debug
Device#
```

ACL Syslog 相関の設定例

例：ユーザ定義 Cookie を使用した ACL Syslog 相関の設定

次に、ユーザ定義 Cookie を使用して、デバイス上で ACL Syslog 相関機能を設定する方法について説明します。

```
Device#
Device# debug ip access-list hash-generation
Syslog MD5 hash code generation debugging is on
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# access-list 33 permit 10.10.10.6 log cook_33_std
Device(config)# do show ip access 33
Standard IP access list 33
10 permit 10.10.10.6 log (tag = cook_33_std)
Device(config)# end
```

例：ハッシュ値を使用した ACL Syslog 相関の設定

次の例では、デバイスで生成されたハッシュ値を使用して、デバイス上で ACL Syslog 相関機能を設定する方法について説明します。

```
Device# debug ip access-list hash-generation
Syslog MD5 hash code generation debugging is on
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# access-list 33 permit 10.10.10.7 log
Device(config)#
*Nov 7 13:51:23.615: %IPACL-HASHGEN: Hash Input: 33 standard permit 10.10.10.7
Hash Output: 0xCE87F535
Device(config)#
do show ip access 33

Standard IP access list 33
    10 permit 10.10.10.6 log (tag = cook_33_std)
    20 permit 10.10.10.7 log (hash = 0xCE87F535)
```

例：ACL Syslog 相関タグ値の変更

次に、既存のアクセス リストのユーザ定義 Cookie と新しい Cookie 値を交換する方法と、デバイス生成ハッシュ値とユーザ定義 Cookie 値を交換する方法について示します。

```
Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# do show ip access-list 101
Extended IP access list 101
    10 permit tcp host 10.1.1.1 host 10.1.1.2 log (tag = MyCookie)
```

```
    20 permit tcp any any log (hash = 0x75F078B9)
Device(config)# access-list 101 permit tcp host 10.1.1.1 host 10.1.1.2 log NewUDV
Device(config)# do show access-list
Extended IP access list 101
    10 permit tcp host 10.1.1.1 host 10.1.1.2 log (tag = NewUDV)
    20 permit tcp any any log (hash = 0x75F078B9)
Device(config)# access-list 101 permit tcp any any log replacehash
Device(config)# do show access-list
Extended IP access list 101
    10 permit tcp host 10.1.1.1 host 10.1.1.2 log (tag = NewUDV)
    20 permit tcp any any log (tag = replacehash)
```

IPv6 IOS ファイアウォールの追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『Cisco IOS Security Command Reference: Commands A to C』 • 『Cisco IOS Security Command Reference: Commands D to L』 • 『Cisco IOS Security Command Reference: Commands M to R』 • 『Cisco IOS Security Command Reference: Commands S to Z』
IPv6 コマンド	『Cisco IOS IPv6 Command Reference』
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	*IPv6 RFCs*

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ACL Syslog 相関に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャセット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *164* : *ACL Syslog* 相関に関する機能情報

機能名	リリース	機能情報
IP アクセス リスト	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 66 章

IPv6 アクセス コントロール リスト

アクセス リストによって、デバイス インターフェイスでブロックされるトラフィックおよび転送されるトラフィックが決定され、送信元アドレスと宛先アドレスに基づくトラフィックのフィルタリング、および特定のインターフェイスへの着信および発信トラフィックのフィルタリングを行うことができます。標準の IPv6 ACL 機能が拡張されて、IPv6 オプション ヘッダー、および任意でより細かい制御を行うための上位層プロトコル タイプ情報に基づくトラフィック フィルタリングがサポートされています。標準の IPv6 ACL 機能が拡張されて、IPv6 オプション ヘッダー、および任意でより細かい制御を行うための上位層プロトコル タイプ情報に基づくトラフィック フィルタリングがサポートされています。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *165* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

IPv6 アクセス コントロール リストに関する情報

IPv6 トラフィック フィルタリングのアクセス コントロール リスト

IPv6 での標準の ACL 機能は、IPv4 での標準の ACL に似ています。アクセス リストによって、デバイス インターフェイスでブロックされるトラフィックおよび転送されるトラフィックが決定され、送信元アドレスと宛先アドレスに基づいて、特定のインターフェイスへの着信と発信をフィルタリングできます。各アクセス リストの末尾には、暗黙的な deny 文があります。グローバル コンフィギュレーション モードで **deny** および **permit** キーワードで **ipv6access-list** コマンドを使用して、IPv6 ACL を定義し、拒否および許可条件を設定します。

IPv6 で拡張された ACL では標準 IPv6 ACL 機能を強化して、IPv6 オプション ヘッダー、および任意でより細かい制御を行うための上位層プロトコル タイプ情報に基づくトラフィック フィルタリングがサポートされています（IPv4 における拡張 ACL に類似した機能です）。

IPv6 パケット インスペクション

ヘッダー フィールド（トラフィック クラス、フロー ラベル、ペイロード長、次ヘッダー、ホップ リミット、および送信元 IP アドレスや宛先 IP アドレス）は、IPv6 インスペクション用に使用されます。IPv6 ヘッダー フィールドの詳細および説明については、RFC 2474 を参照してください。

IPv6 でのアクセス クラス フィルタリング

IPv6 ACL に基づく、デバイスとの間の着信接続と発信接続のフィルタリングは、ライン コンフィギュレーション モードで **ipv6access-class** コマンドを使用して実行されます。**ipv6access-class** コマンドは、IPv6 ACL が名前で定義される点を除き、**access-class** コマンドに似ています。IPv6 ACL が着信トラフィックに適用される場合、ACL 内の送信元アドレスは、着信接続の送信元アドレスと照合され、ACL 内の宛先アドレスは、インターフェイス上のローカル デバイス アドレスと照合されます。IPv6 ACL が発信トラフィックに適用される場合、ACL 内の送信元アドレスは、インターフェイス上のローカル デバイス アドレスと照合され、ACL 内の宛先アドレスは、発信接続の送信元アドレスと照合されます。ユーザが任意の接続を試行できるように、すべての仮想端末回線で同じ制限を設定することを推奨します。

IPv6 アクセス コントロール リストの設定方法

IPv6 トラフィック フィルタリングの設定

トラフィック フィルタリング用の IPv6 ACL の作成および設定

（注） Cisco cBR ルータの IPv6 ACL には暗黙の許可ルールは含まれません。IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク層サービスを使用します。したがって、IPv6 ネイバー探索をイネーブルにするには、IPv6 ネイバー探索パケットのインターフェイス上での送受信が許可されるように IPv6 ACL を追加する必要があります。IPv4 では、IPv6 ネイバー探索プロセスと同等のアドレス解決プロトコル（ARP）は、別のデータリンク層プロトコルを使用します。したがってデフォルトでは、IPv4 ACL により、ARP パケットのインターフェイス上での送受信が暗黙的に許可されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**ipv6access-list** *access-list-name* 例： `Device(config)# ipv6 access-list inbound`	IPv6 ACL を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。 • *access-listname* 引数は、IPv6 ACL の名前を指定します。IPv6 ACL の名前にスペースまたは引用符を含めることはできません。また、先頭を数字にすることはできません。

	コマンドまたはアクション	目的

ステップ 4	次のいずれかを実行します。
	• **permitprotocol** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix / prefix-length* | **any** | **host** *destination-ipv6-address*} [**operator** [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
	• **deny** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**
	例：
	`Device(config-ipv6-acl)# permit tcp 2001:DB8:0300:0201::/32 eq telnet any`
	例：
	`Device(config-ipv6-acl)# deny tcp host 2001:DB8:1::1 any log-input`
		IPv6 ACL の許可条件または拒否条件を指定します。

インターフェイスへの IPv6 ACL の適用

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**interface** *type number* 例： `Device(config)# interface TenGigabitEthernet4/1/0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ipv6traffic-filter** *access-list-name*{**in**|**out**} 例： `Device(config-if)# ipv6 traffic-filter outbound out`	指定したIPv6アクセス リストを、前のステップで指定したインターフェイスに適用します。

vty へのアクセスの制御

IPv6 ACL の作成によるアクセス クラス フィルタリングの提供

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**ipv6access-list** *access-list-name* 例： `Device(config)# ipv6 access-list cisco`	IPv6 ACL を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかを実行します。
	• **permitprotocol** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [*operator* [*port-number*]] {*destination-ipv6-prefix / prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*
	• **deny** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address*} [*operator port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [*operator* [*port-number*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**
	
	例：
	`Device(config-ipv6-acl)# permit ipv6 host 2001:DB8:0:4::32 any`
	
	例：
	`Device(config-ipv6-acl)# deny ipv6 host 2001:DB8:0:6::6 any`
		IPv6 ACL の許可条件または拒否条件を指定します。

仮想端末回線への IPv6 ACL の適用

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**line**[**aux**| **console**| **tty**| **vty**] *line-number*[*ending-line-number*] 例： `Device(config)# line vty 0 4`	設定する特定の回線を識別し、ライン コンフィギュレーション モードを開始します。 • この例では、**vty** キーワードを使用して、リモート コンソール アクセス用の仮想端末回線を指定します。
ステップ 4	**ipv6access-class** *ipv6-access-list-name*{**in**| **out**} 例： `Device(config-line)# ipv6 access-class cisco in`	IPv6 ACL に基づいて、デバイスとの間の着信接続と発信接続をフィルタリングします。

IPv6 アクセス コントロール リストの設定例

例：IPv6 ACL 設定の確認

この例では、**show ipv6 access-list** コマンドを使用して、IPv6 ACL が正しく構成されているかを確認します。

```
Device> show ipv6 access-list

IPv6 access list inbound
    permit tcp any any eq bgp (8 matches) sequence 10
    permit tcp any any eq telnet  (15 matches) sequence 20
    permit udp any any  sequence 30

IPv6 access list Virtual-Access2.1#427819008151 (per-user)
```

```
permit tcp host 2001:DB8:1::32 eq bgp host 2001:DB8:2::32 eq 11000 sequence 1
permit tcp host 2001:DB8:1::32 eq telnet host 2001:DB8:2::32 eq 11001 sequence 2
```

例：IPv6 ACL の作成と適用

次に、HTTP アクセスを日中の特定の時間に制限し、許可されていない時間のアクティビティを記録する方法について例を示します。

```
Device# configure terminal
Device(config)# time-range lunchtime
Device(config-time-range)# periodic weekdays 12:00 to 13:00
Device(config-time-range)# exit
Device(config)# ipv6 access-list INBOUND
Device(config-ipv6-acl)# permit tcp any any eq www time-range lunchtime
Device(config-ipv6-acl)# deny tcp any any eq www log-input
Device(config-ipv6-acl)# permit tcp 2001:DB8::/32 any
Device(config-ipv6-acl)# permit udp 2001:DB8::/32 any
Device(config-ipv6-acl)# end
```

例：vty へのアクセスの制御

次の例では、仮想端末回線 0 ～ 4 に着信する接続は、acl1 という名前の IPv6 アクセス リストに基づいてフィルタリングされます。

```
ipv6 access-list acl1
 permit ipv6 host 2001:DB8:0:4::2/32 any
!
line vty 0 4
 ipv6 access-class acl1 in
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
IP アクセス リスト コマンド	『*Cisco IOS Security Command Reference*』
IP アクセス リストの設定	『Creating an IP Access List and Applying It to an Interface』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 アクセス コントロール リストに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *166* : *IPv6* アクセス コントロール リストに関する機能情報

機能名	リリース	機能情報
IPv6 アクセス リスト	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 67 章

IPv6 テンプレート ACL

ベンダー固有属性（VSA）の Cisco AV ペアを使用してユーザ プロファイルが設定されている場合は、類似した 1 ユーザ単位の IPv6 ACL を 1 つのテンプレート ACL で置き換えることができます。つまり、1 つの ACL で多数の類似した ACL を表します。IPv6 テンプレート ACL を使用することで、ACL をサポートするために必要なメモリおよび Ternary Content Addressable Memory（TCAM）リソースを最小限に抑えながら、1ユーザあたりのACLの合計数を増やすことができます。

IPv6 テンプレート ACL 機能では、次の ACL フィールドを使用してテンプレートを作成します。

- IPv6 の送信元アドレスおよび宛先アドレス
- すべての関連ポート（0 ～ 65535）を含む TCP および UDP
- ICMP ネイバー探索アドバタイズメントおよび要請
- 指定した DSCP 値による IPv6 DSCP

この機能により、ACL の名前はたとえば次のように動的に生成されます。

- 6Temp_#152875854573 - 親 ACL のテンプレートとして動的に生成されたテンプレート名の例
- Virtual-Access2.32135#152875854573 - 子 ACL またはテンプレートの一部とされていない ACL の例。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://

tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *167*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

IPv6 ACL に関する情報：テンプレート ACL

IPv6 テンプレート ACL

ベンダー固有属性（VSA）の Cisco AV ペアを使用してユーザ プロファイルが設定されている場合は、類似した 1 ユーザ単位の IPv6 ACL を 1 つのテンプレート ACL で置き換えることができます。つまり、1 つの ACL で多数の類似した ACL を表します。IPv6 テンプレート ACL を使用することで、ACL をサポートするために必要なメモリおよび Ternary Content Addressable Memory（TCAM）リソースを最小限に抑えながら、1 ユーザあたりの ACL の合計数を増やすことができます。

IPv6 テンプレート ACL 機能では、次の ACL フィールドを使用してテンプレートを作成します。

- IPv6 の送信元アドレスおよび宛先アドレス

- すべての関連ポート（0 ～ 65535）を含む TCP および UDP
- ICMP ネイバー探索アドバタイズメントおよび要請
- 指定した DSCP 値による IPv6 DSCP

この機能により、ACL の名前はたとえば次のように動的に生成されます。

- 6Temp_#152875854573 - 親 ACL のテンプレートとして動的に生成されたテンプレート名の例
- Virtual-Access2.32135#152875854573 - 子 ACL またはテンプレートの一部とされていない ACL の例。

IPv6 ACL を有効にする方法：テンプレート ACL

IPv6 テンプレートの処理の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**access-listtemplate** [*number-of-rules*] 例： `Router(config)# access-list template 50`	テンプレート ACL の処理をイネーブルにします。 • このタスクの例では、50 以下のルールを設定した ACL がテンプレート ACL ステータスとして見なされるように指定しています。 • *number-of-rules* 引数のデフォルトは 100 です。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了して、ルータを特権 EXEC モードにします。

	コマンドまたはアクション	目的
ステップ 5	**showaccess-listtemplate** {**summary** | *aclname* | **exceed** *number* | **tree**} 例： `Router# show access-list template summary`	ACL テンプレートの情報を表示します。

IPv6 ACL の設定例：テンプレート ACL

例：IPv6 テンプレート ACL の処理

この例では、内容は同じでも、名前が ACL1 と ACL2 で異なります。

```
ipv6 access-list extended ACL1 (PeerIP: 2001:1::1/64)
permit igmp any                  2003:1::1/64
permit icmp 2002:5::B/64         any
permit udp  any                  host 2004:1::5
permit udp  any                  host 2002:2BC::a
permit icmp host 2001:BC::7      host 2003:3::7
ipv6 access-list extended ACL2 (PeerIP: 2007:2::7/64)
permit igmp any                  2003:1::1/64
permit icmp 2002:5::B/64         any
permit udp  any                  host 2004:1::5
permit udp  any                  host 2002:2BC::a
permit icmp host 2001:BC::7      host 2003:3::7
```

これらの ACL のテンプレートは次のとおりです。

```
ipv6 access-list extended Template_1
permit igmp any                  2003:1::1/64
permit icmp 2002:5::B/64         any
permit udp  any                  host 2004:1::5
permit udp  any                  host 2002:2BC::a
permit icmp host 2001:BC::7      host 2003:3::7
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

関連項目	マニュアル タイトル
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	*IPv6 RFCs*

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IPv6 テンプレート ACL に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *168* : *IPv6* テンプレート *ACL* に関する機能情報

機能名	リリース	機能情報
IPv6 アクセス リスト	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 68 章

ホップバイホップフィルタリングに対応するための IPv6 ACL の拡張

ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張機能により、ホップ バイ ホップ拡張ヘッダーを含む可能性がある IPv6 トラフィックを制御することができます。アクセス コントロール リスト（ACL）を設定して、すべてのホップ バイ ホップ トラフィックを拒否するか、またはプロトコルに基づいて選択的にトラフィックを許可することができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

- ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張に関する機能情報, 1098 ページ

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *169* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張に関する情報

ACL およびトラフィック転送

IPv6 アクセス コントロール リスト（ACL）は、デバイス インターフェイスでブロックされるトラフィックと転送されるトラフィックを決定します。ACL を使用すると、特定のインターフェイスへの着信および発信を、送信元アドレスと宛先アドレスに基づいてフィルタリングできます。**ipv6 access-list** コマンドを使用して、IPv6 ACL を定義し、**deny** および **permit** コマンドを使用してその条件を構成します。

ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張機能は、上位層プロトコル タイプでのトラフィック フィルタリングをサポートするために RFC 2460 を実装します。

ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張の設定方法

ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**ipv6access-list** *access-list-name* 例： `Device(config)# ipv6 access-list hbh-acl`	IPv6 ACL を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 4	**permit** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host**	IPv6 ACL の許可条件を設定します。

	コマンドまたはアクション	目的
	destination-ipv6-address | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*header-number* | *header-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] 例： `Device(config-ipv6-acl)# permit icmp any any dest-option-type`	
ステップ 5	**deny** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** |**host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** |**host** *destination-ipv6-address* | **auth**} [*operator* [*port-number*]] [**dest-option-type** [*header-number* | *header-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**hbh**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**] 例： `Device(config-ipv6-acl)# deny icmp any any dest-option-type`	IPv6 ACL の拒否条件を設定します。
ステップ 6	**end** 例： `Device (config-ipv6-acl)# end`	特権 EXEC コンフィギュレーション モードに戻ります。

ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張の設定例

例：ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張

```
Device(config)# ipv6 access-list hbh_acl
Device(config-ipv6-acl)# permit tcp any any hbh
Device(config-ipv6-acl)# permit tcp any any
Device(config-ipv6-acl)# permit udp any any
Device(config-ipv6-acl)# permit udp any any hbh
Device(config-ipv6-acl)# permit hbh any any
Device(config-ipv6-acl)# permit any any
Device(config-ipv6-acl)# hardware statistics
```

```
Device(config-ipv6-acl)# exit

! Assign an IP address and add the ACL on the interface.

Device(config)# interface TenGigabitEthernet4/1/0
Device(config-if)# ipv6 address 1001::1/64
Device(config-if)# ipv6 traffic-filter hbh_acl in
Device(config-if)# exit
Device(config)# exit
Device# clear counters
Clear "show interface" counters on all interfaces [confirm]
Device#

! Verify the configurations.

Device# show running-config interface TenGigabitEthernet4/1/0

Building configuration...

Current configuration : 114 bytes
!
interface TenGigabitEthernet4/1/0
no switchport
ipv6 address 1001::1/64
ipv6 traffic-filter hbh_acl
end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
IPv6 アドレッシングと接続	『*IPv6 Configuration Guide*』
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
IPv6 コマンド	『*Cisco IOS IPv6 Command Reference*』
Cisco IOS IPv6 機能	『Cisco IOS IPv6 Feature Mapping』

標準および RFC

標準/RFC	タイトル
IPv6 に関する RFC	*IPv6 RFCs*

MIB

MIB	MIB のリンク
	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *170*：ホップ バイ ホップ フィルタリングに対応するための *IPv6 ACL* の拡張に関する機能情報

機能名	リリース	機能情報
IPv6 アクセス リスト	Cisco IOS XE Fuji 16.7.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Fuji 16.7.1 に統合されました。

第 VIII 部

アプリケーション：音声とビデオの設定

第 69 章

Unique Device Identifier の取得

Unique Device Identifier（UDI）の取得機能は、この ID 情報を保存したシスコ製品から UDI 情報を取得および表示するための機能を提供します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *171* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

Unique Device Identifier の概要

識別可能な各製品は、エンティティ MIB（RFC-2737）およびそのサポート ドキュメントで定義されたエンティティです。シャーシなどの一部のエンティティには、スロットのようなサブエンティティがあります。イーサネット スイッチは、スタックなどのスーパーエンティティのメンバであ

る場合があります。注文可能なシスコ製品のエンティティは、そのほとんどが UDI を割り当てられて出荷されます。UDI 情報は、ラベルに印字され、ハードウェア デバイスに物理的に貼付されます。また、簡単にリモート検索できるよう、デバイス内に電子的に保存されます。

UDI は、次の要素で構成されています。

- 製品 ID（PID）
- バージョン ID（VID）
- シリアル番号（SN）

PIDは製品を発注するための名前で、従来は「製品名」または「部品番号」と呼ばれていました。これは、正しい交換部品を発注するために使用される ID です。

VID は製品のバージョンです。製品が改訂されるたびに、VID は増加します。VID は、製品変更の通知を管理する業界のガイドラインである、Telcordia GR-209-CORE から取得された厳格なプロセスに従って増加されます。

SNはベンダー固有の製品の通し番号です。それぞれの製造済み製品には、現場では変更できない固有のシリアル番号が工場で割り当てられます。この番号は、製品の特定のインスタンスを個々に識別するための手段です。

Unique Device Identifier の取得機能の利点

- ネットワーク内の個別のシスコ製品を識別します。
- シスコ製品をシンプルに、クロスプラットフォームで、一貫して識別することで、資産管理の運用経費が削減されます。
- 交換可能な製品の PID を識別します。
- リコールまたはリビジョン対象の製品を容易に特定できます。
- シスコ製品のインベントリを自動化します（設備および資産管理）。
- 修理や交換サービスのためにシスコ製品のエンタイトルメント レベルを決定するためのメカニズムを提供します。

ケーブル製品の製品品目記述子

製品品目記述子（PID）の詳細については、Cisco.comにある製品ハードウェアインストールガイドを参照してください。

Unique Device Identifier の取得

UDI 取得を使用するには、使用中の Cisco 製品の UDI が有効になっている必要があります。UDI 対応のシスコ製品では、5 つの必須エンティティ MIB オブジェクトがサポートされます。5 つのエンティティ MIB v2（RFC-2737）オブジェクトは次のとおりです。

- entPhysicalName

- entPhysicalDescr
- entPhysicalModelName
- entPhysicalHardwareRev
- entPhysicalSerialNum

show inventory コマンドを使用できる場合もありますが、UDI 対応ではないデバイスに対してこのコマンド使用すると、出力が生成されない可能性があります。

PID、VID、および SN が割り当てられているネットワーキング デバイスに取り付けられているすべてのシスコ製品についての情報を取得および表示するには、**show inventory** コマンドを入力します。シスコ エンティティに PID が割り当てられていない場合、そのエンティティは取得または表示されません。

```
Router# show inventory

NAME: "Chassis", DESCR: "Cisco cBR-8 CCAP Chassis"
PID: CBR-8-CCAP-CHASS  , VID: V01, SN: FXS1739Q0PR

NAME: "clc 3", DESCR: "Cisco cBR CCAP Line Card"
PID: CBR-CCAP-LC-40G   , VID: V01, SN: TEST1234567

NAME: "Cable PHY Module", DESCR: "CLC Downstream PHY Module 3/0"
PID: CBR-D30-DS-MOD    , VID: V01, SN: CAT1725E1BZ

NAME: "Cable PHY Module", DESCR: "CLC Downstream PHY Module 3/1"
PID: CBR-D30-DS-MOD    , VID: V01, SN: CAT1725E1AT

NAME: "Cable PHY Module", DESCR: "CLC Upstream PHY Module 3/2"
PID: CBR-D30-US-MOD    , VID: V01, SN: CAT1717E0FF

NAME: "sup 1", DESCR: "Cisco cBR CCAP Supervisor Card"
PID: CBR-CCAP-SUP-60G  , VID: V01, SN: CAT1824E0MT

NAME: "harddisk 5/1", DESCR: "Hard Disk"
PID: UGB88RTB100HE3-BCU-DID, VID:    , SN: 11000066829

NAME: "sup-pic 5/1", DESCR: "Cisco cBR CCAP Supervisor Card PIC"
PID: CBR-SUP-8X10G-PIC , VID: V01, SN: CAT1720E0F4

NAME: "SFP+ module 5/1/0", DESCR: "iNSI xcvr"
PID: SFP+ 10GBASE-SR   , VID: A   , SN: FNS172720X6

NAME: "SFP+ module 5/1/1", DESCR: "iNSI xcvr"
PID: SFP+ 10GBASE-LR   , VID: A   , SN: UGT085P

NAME: "SFP+ module 5/1/2", DESCR: "iNSI xcvr"
PID: SFP+ 10GBASE-LR   , VID: A   , SN: UGT087Z

NAME: "SFP+ module 5/1/3", DESCR: "iNSI xcvr"
PID: SFP+ 10GBASE-SR   , VID: G4.1, SN: AVD1729A38T

NAME: "SFP+ module 5/1/7", DESCR: "iNSI xcvr"
PID: 10GE ZR           , VID: A   , SN: FNS11300AUH

NAME: "Power Supply Module 0", DESCR: "Cisco cBR CCAP AC Power Supply"
PID: PWR-3KW-AC-V2     , VID: V02, SN: DTM17370345

NAME: "Power Supply Module 2", DESCR: "Cisco cBR CCAP AC Power Supply"
PID: PWR-3KW-AC-V2     , VID: V02, SN: DTM173702KF
```

診断のために、**show inventory** コマンドで **raw** キーワードを使用すると、PID、UDI、その他の物理 ID がないエンティティを含む、すべての RFC 2737 エンティティが表示されます。

（注） **raw** キーワードオプションの主な目的は、**show inventory** コマンド自体の問題をトラブルシューティングすることです。

```
Router# show inventory raw

NAME: "Chassis", DESCR: "Cisco cBR-8 CCAP Chassis"
PID: CBR-8-CCAP-CHASS  , VID: V01, SN: FXS1739Q0PR

NAME: "slot 0/0", DESCR: "Chassis Slot"
PID:                   , VID:    , SN:

NAME: "slot 0/1", DESCR: "Chassis Slot"
PID:                   , VID:    , SN:

NAME: "slot 1/0", DESCR: "Chassis Slot"
PID:                   , VID:    , SN:

NAME: "slot 1/1", DESCR: "Chassis Slot"
PID:                   , VID:    , SN:

NAME: "slot 2/0", DESCR: "Chassis Slot"
PID:                   , VID:    , SN:

NAME: "slot 2/1", DESCR: "Chassis Slot"
PID:                   , VID:    , SN:

NAME: "slot 3/0", DESCR: "Chassis Slot"
PID:                   , VID:    , SN:

NAME: "clc 3", DESCR: "Cisco cBR CCAP Line Card"
PID: CBR-CCAP-LC-40G   , VID: V01, SN: TEST1234567

NAME: "12_CUR: Sens 3/0", DESCR: "12_CUR: Sens"
PID:                   , VID:    , SN:

NAME: "12_CUR: Vin 3/1", DESCR: "12_CUR: Vin"
PID:                   , VID:    , SN:

NAME: "12_CUR: ADin 3/2", DESCR: "12_CUR: ADin"
PID:                   , VID:    , SN:

NAME: "G0_CUR: Sens 3/3", DESCR: "G0_CUR: Sens"
PID:                   , VID:    , SN:

NAME: "G0_CUR: Vin 3/4", DESCR: "G0_CUR: Vin"
PID:                   , VID:    , SN:

NAME: "G0_CUR: ADin 3/5", DESCR: "G0_CUR: ADin"
PID:                   , VID:    , SN:

NAME: "G1_CUR: Sens 3/6", DESCR: "G1_CUR: Sens"
PID:                   , VID:    , SN:

NAME: "G1_CUR: Vin 3/7", DESCR: "G1_CUR: Vin"
PID:                   , VID:    , SN:

NAME: "G1_CUR: ADin 3/8", DESCR: "G1_CUR: ADin"
PID:                   , VID:    , SN:

NAME: "LB_CUR: Sens 3/9", DESCR: "LB_CUR: Sens"
PID:                   , VID:    , SN:

NAME: "LB_CUR: Vin 3/10", DESCR: "LB_CUR: Vin"
PID:                   , VID:    , SN:

NAME: "LB_CUR: ADin 3/11", DESCR: "LB_CUR: ADin"
PID:                   , VID:    , SN:
```

```
NAME: "Temp: CAPRICA 3/12", DESCR: "Temp: CAPRICA"
PID:                    , VID:    , SN:

NAME: "Temp: BASESTAR 3/13", DESCR: "Temp: BASESTAR"
PID:                    , VID:    , SN:

NAME: "Temp: RAIDER 3/14", DESCR: "Temp: RAIDER"
PID:                    , VID:    , SN:

NAME: "Temp: CPU 3/15", DESCR: "Temp: CPU"
PID:                    , VID:    , SN:

NAME: "Temp: INLET 3/16", DESCR: "Temp: INLET"
PID:                    , VID:    , SN:

NAME: "Temp: OUTLET 3/17", DESCR: "Temp: OUTLET"
PID:                    , VID:    , SN:

NAME: "Temp: DIGITAL 3/18", DESCR: "Temp: DIGITAL"
PID:                    , VID:    , SN:

NAME: "Temp: UPX 3/19", DESCR: "Temp: UPX"
PID:                    , VID:    , SN:
```

トラブルシューティングのヒント

いずれかのシスコ製品に PID が割り当てられていない場合は、出力で誤った PID と VID が表示され、SN 要素が次の例のとおり足りない場合があります。

```
NAME: "POS3/0/0", DESCR: "Skystone 4302 Sonet Framer"

PID: FastEthernet, VID: , SN:

NAME: "Serial1/0", DESCR: "M4T"

PID: M4T                , VID:    , SN:
```

出力例では、PID は製品説明とまったく同じです。UDI は、PID が割り当てられた新しいシスコ製品とともに使用するように設計されています。シスコの旧製品の UDI 情報は常に信頼できるとは限りません。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
コンフィギュレーション ファイルの管理についての情報	『Cisco IOS Configuration Fundamentals Configuration Guide』
インターフェイス統計を表示するコマンド	『Cisco IOS Interface Command Reference』

標準および RFC

標準/RFC	タイトル
RFC 2737	『*Entity MIB (Version 2)*』

MIB

MIB	MIB のリンク
CISCO-ENTITY-ASSET-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Unique Device Identifier の取得に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *172* : ***Unique Device Identifier*** の取得に関する機能情報

機能名	リリース	機能情報
Unique Device Identifier の取得	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 70 章

Cisco CMTS ルータ用拡張モード DOCSIS セットトップ ゲートウェイ 1.2

拡張モード DOCSIS セットトップ ゲートウェイ（A-DSG）Issue 1.2 には、CableLabs™ による最新の DOCSIS セットトップ仕様へのサポートが導入されています。次の機能拡張が含まれます。

- *DOCSIS* セットトップ ゲートウェイ（*DSG*）インターフェイスの仕様
- A-DSG 1.2 による DOCS-DSG-IF MIB のサポートの導入。

Cisco A-DSG 1.2 は CableLabs™ によって認定された最新の業界イノベーションをサポートする強力なツールです。A-DSG 1.2 はブロードバンド ケーブル環境の拡張された DOCSIS の実装に多大なサポートを提供します。セットトップ ボックス（STB）は、MAC アドレス、トラフィック管理ルール、分類子を含む、Cisco CMTS ルータの環境全体を動的に学習します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *173* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

拡張モード DSG Issue 1.2 の前提条件

拡張モード DSG Issue 1.2 機能を使用するために、特別な装置やソフトウェアは必要ありません。

拡張モード DSG Issue 1.2 の制限事項

ここでは、Cisco CMTS ルータでの A-DSG 1.2 特有の制限事項について説明します。

DSG コンフィギュレーション ファイル転送操作

DSG 1.2 では、TFTP サーバ、ファイル システム、またはブートフラッシュから実行コンフィギュレーションにDSG コンフィギュレーション ファイルをコピーすることをサポートしていません。

マルチキャスト設定の制約事項

A-DSG 1.2 が正常に動作するように IP マルチキャストを設定する必要があります。具体的には、IP マルチキャスト ルーティングをグローバル コンフィギュレーションで設定する必要があります。また、マルチキャスト トラフィックを伝送するケーブル インターフェイスのすべてのバンドル インターフェイスで、IP PIM を設定する必要があります。

DSG をサポートするマルチキャストの追加情報およびグローバル コンフィギュレーションについては、デフォルトのマルチキャスト QoS の設定, （1117 ページ）およびIP マルチキャスト動作の設定, （1125 ページ）を参照してください。

DSG ユニキャスト専用マッピングのための NAT

DSG 1.2 はマルチキャスト IP アドレスをサポートしています。他方、ユニキャスト IP 宛先アドレスもサポートします。Cisco cBR-8 ルータでの DSG 1.2 サポートは、ルータ上のネットワーク アドレス変換（NAT）の設定とともに提供されます。これには次の設定が含まれます。

- WAN インターフェイスは **ipnatoutside** コマンドで設定されます。
- ケーブル インターフェイスは、**ipnatinside** コマンドで設定されます。
- 各マッピングの追加設定として、送信元スタティック マルチキャスト IP アドレスとユニキャスト IP アドレスがあります。

ユニキャスト IP アドレスは、Cisco CMTS ルータに到着する DSG パケットのユニキャスト宛先 IP アドレスです。マルチキャスト IP アドレスは、1 つまたは一連の DSG トンネルにマッピングするよう設定された新しい宛先 IP アドレスです。

マルチキャストでの PIM および SSM

Source Specific Multicast（SSM）操作を A-DSG 1.2 と組み合わせて使用する場合は、次のシステム全体のコンフィギュレーション コマンドを指定する必要があります。

- **ip pim ssm**

IP マルチキャスト動作の設定, （1125 ページ）を参照してください。

サブインターフェイス

A-DSG 1.2 は Cisco CMTS ルータのサブインターフェイスをサポートします。

拡張モード DSG Issue 1.2 に関する情報

A-DSG 1.2 は、これらの新機能や強化機能を提供します。

- A-DSG クライアントおよびエージェント モード

- DSG 1.2 をサポートする拡張モード MIB（DOCS-DSG-IF-MIB を含む）
- セキュリティを強化した拡張モード トンネル
- 仮想インターフェイス バンドリングによるケーブル インターフェイス バンドリング
- ダウンストリーム チャネル記述子
- IP マルチキャストのサポート
- Quality of Service（QoS）

DSG 1.2 クライアントおよびエージェント

A-DSG 1.2 では、CableLabs™ の *DOCSIS Set-top Gateway (DSG) Interface Specification*（CM-SP-DSG-I05-050812）に記述されている DSG クライアントおよびエージェント機能をサポートします。

FQDN サポート

グローバル コンフィギュレーション モードで **cabledsgcfr** コマンドを使用して、A-DSG 分類子のマルチキャスト グループの完全修飾ドメイン名（FQDN）または IP アドレスと送信元アドレスを指定できます。ネットワークの変更を実装するときは、マルチキャスト グループと送信元アドレスの変更を回避するために FQDN を使用することを推奨します。

この機能では、**cabledsgcfr** コマンドを使用して、送信元 IP アドレスの代わりにホスト名（FQDN）を使用できます。たとえば、2 つの場所に 2 つの A-DSG トンネル サーバがあり、マルチキャスト トラフィックを同じマルチキャスト アドレスに送信しているとします。このシナリオでは、送信元 IP アドレスにホスト名を指定し、マルチキャスト トラフィックを送信している送信元を DNS サーバで判断させることができます。

ホスト名を使用して A-DSG 分類子を設定する場合、Cisco CMTS ルータは、そのホスト名がローカル ホスト キャッシュを使用して IP アドレスに解決できるかどうかをただちに確認します。確認できない場合、ルータはホスト名が解決されるまでその分類子を有効にしません。ホスト名をローカルで解決できない場合、ルータは DSG 分類子を確認するために DNS クエリを実行します。

FQDN 形式では、Cisco CMTS ルータで開始される静的 Internet Group Management Protocol（IGMP）参加要求をサポートしません。A-DSG 設定時にバンドル インターフェイスで自動的に作成される IGMP 静的グループの IP アドレスは、**showrunning-configinterface** コマンドの出力には表示されません。バンドル インターフェイスで設定されている A-DSG 静的グループを表示するには、特権 EXEC モードで **showcabledsgstatic-groupbundle** コマンドを使用します。

DSG 名プロセスと DNS クエリ

それぞれの DNS レコードには、サーバ管理者が設定する存続可能時間（TTL）値が含まれます。この値は数秒から数週間までとさまざまです。DSG 名プロセスは、TTL 値条件より優先して、Cisco CMTS ルータの A-DSG 分類子を更新します。

DSG 名プロセスにより、Cisco CMTS ルータは、DNS サーバを照会して分類子更新を高速化できます。Cisco CMTS ルータが A-DSG 分類子検証のために DNS クエリを実行できるようにするには、グローバル コンフィギュレーション モードで **ipname-server** コマンドを使用して 1 つ以上の DNS サーバを設定する必要があります。また、グローバル コンフィギュレーション モードで **cabledsgname-update-interval** コマンドを使用して DNS クエリ間隔を指定できます。

Cisco IOS ソフトウェアのリロード時またはルート プロセッサのスイッチオーバー時にインターフェイスが停止している場合は、DNS サーバのクエリに失敗する可能性があります。また、**cabledsgname-update-interval** コマンドを使用して指定した間隔を待機せずに DNS クエリを実行する可能性もあります。このとき、未解決のホスト名に対して、ルータはシステム定義（15 秒）の間隔に基づいて自動的に DNS クエリを実行し、DSG 分類子の高速な更新を促します。システム定義の間隔は変更できません。

プライマリ チャネルでの A-DSG 転送

プライマリ対応インターフェイスごとに A-DSG 転送を無効にすることができます。そうするには、インターフェイス コンフィギュレーション モードで **cabledownstreamdsgdisable** コマンドを使用します。プライマリ対応インターフェイスには、モジュラ式の統合ケーブル インターフェイス、および Cisco cBR-8 CCAP ケーブル インターフェイスが含まれます。

たとえばケーブル インターフェイス 7/1/1 が A-DSG 対応であり、4 つのモジュラ チャネルが接続されているとします。ただし、この 4 つのモジュラ チャネルのうち 2 つだけで A-DSG 転送を有効にしたいとします。選択したチャネルを除外するには、cable downstream dsg disable コマンドを使用できます。モジュラ チャネルを無効にする方法の詳細については、プライマリ チャネルの A-DSG 転送の無効化, （1134 ページ）を参照してください。

（注） A-DSG ダウンストリーム転送がプライマリ対応インターフェイスで無効になると、ルータはプライマリ対応インターフェイスでマルチキャスト サービス フローを作成せず、ダウンストリーム チャネル ディスクリプタ（DCD）メッセージの送信を停止しません。

DOCSIS 3.0 DSG MDF サポート

DOCSIS 3.0 DSG マルチキャスト DSID 転送（MDF）のサポートが導入されました。MAC ドメイン記述子（MDD）メッセージで DSG DA-to-DSID Association Entry のタイプ、長さ、値（TLV 13）を使用して、ダウンストリーム サービス識別子（DSID）と DSG トンネル トラフィックに使用されるグループ MAC アドレスとの間の関連付けを通信します。これは Cisco CMTS ルータで自動的にサポートされます。

DOCSIS 2.0 ハイブリッド CM と DOCSIS 3.0 CM は Dynamic Bonding Change（DBC）を使用して Cisco CMTS ルータから DSID 情報を取得しますが、DOCSIS 2.0 DSG ハイブリッド組み込み CM と DOCSIS 3.0 DSG 組み込み CM は MDD メッセージを通じて Cisco CMTS ルータから DSID 情報を取得します。

すべての DSG 組み込みケーブル モデム（DOCSIS 3.0 DSG および DOCSIS 2.0 DSG ハイブリッド モデムを含む）で MDF 機能を無効にするには、グローバル コンフィギュレーション モードで cable multicast mdf-disable コマンドを使用し、dsg キーワードを指定します。

Source Specific Multicast マッピング

Source Specific Multicast（SSM）は、ブロードキャスト アプリケーションとしても知られる 1 対多アプリケーションをサポートする最善のデータグラム配信モデルです。SSM は、オーディオおよびビデオのブロードキャスト アプリケーション環境を対象としたシスコの IP マルチキャスト ソリューションの中核的なネットワーキング テクノロジーです。

次の 2 つの Cisco IOS コンポーネントは共に SSM の実装をサポートします。

- Protocol Independent Multicast Source-Specific Mode（PIM-SSM）
- インターネット グループ管理プロトコル バージョン 3（IGMPv3）

Cisco CMTS ルータで SSM マッピングを設定できます。

Cisco CMTS ルータで SSM マッピングを設定する方法については、『Source Specific Multicast (SSM) Mapping』機能ガイドを参照してください。

拡張モード DSG Issue 1.2 の設定方法

拡張モード DSG Issue 1.2 を使用するには、DSG トンネル設定へのサポート、マルチキャストのサポートにグローバル、WAN 側およびインターフェイス レベルの設定が含まれている必要があります。

デフォルトのマルチキャスト QoS の設定

DOCSIS 3.0 によると、MQoS を使用する場合はデフォルトのマルチキャスト サービス品質（MQoS）を設定する必要があります。また、これは DSG にも適用されます。サービス クラス名とトンネルを関連付けることで MQoS を使用します。

デフォルトの MQoS を設定していない場合、DSG トンネル サービス クラス設定は拒否されます。同様に、MQoS を使用する DSG トンネルがない場合、デフォルトの MQoS を削除するように求められます。

デフォルトの MQoS が設定されており、MQoS グループ設定に何も一致しない場合、CMTS はプライマリ ダウンストリーム チャネルを選択してマルチキャスト トラフィックを転送します。それ以外の場合、マルチキャスト トラフィックの転送にはワイドバンド インターフェイスが使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

ステップ 2	**configure terminal**
	
	例：
	`Router# configure terminal`
	
	例：
	`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	**cablemulticastgroup-qosdefaultscn** *service-class-name* **aggregate** 例： `Router(config)# cable multicast group-qos default scn name1 aggregate`	QoS プロファイルのサービス クラス名を設定します。
ステップ 4	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。

次の作業

（注） CMTS によるマルチキャスト トラフィックの送信中にデフォルトの MQoS を設定または削除すると、重複したトラフィックが約 3 分間（またはクエリ間隔の 3 倍）生成されます。

拡張モード DSG 1.2 のグローバル トンネル グループ設定の構成

この手順では、DSG トンネル グループを有効にするために Cisco CMTS ルータでグローバルおよびインターフェイス レベルのコマンドを構成します。DSG トンネル グループは、複数の DSG チャネルをバンドルし、MAC ドメイン インターフェイスに関連付けるために使用します。

グローバル A-DSG 1.2 トンネルの設定

この手順では、A-DSG 1.2 クライアントとエージェントの両方をサポートするグローバル コンフィギュレーションを設定してイネーブルにします。追加の手順には、クライアントおよびエージェントに関する追加設定が含まれます。

はじめる前に

DOCSIS Set-top Gateway（DSG）でトンネルのサービス品質（QoS）を指定するように設定する場合は、デフォルトのマルチキャスト QoS（MQoS）も設定します。詳細については、デフォルトのマルチキャスト QoS の設定，（1117 ページ）を参照してください。

（注） DSG トンネル サービス クラスの設定は、デフォルトの MQoS が設定されていないと拒否されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

ステップ 2	**configure terminal**
	
	例：
	
	`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	**cabledsgtg***group-id* [**channel***channel-id* |**priority***DSG-rule-priority*] [**enable**|**disable**] 例： `Router(config)# cable dsg tg 1 channel 1 priority 1 enable`	コマンドにより、トンネル グループと Cisco CMTS 上の 1 つ以上のダウンストリーム インターフェイスを関連付けられます。
ステップ 4	**cabledsgtg***group-id* [**channel** *channel-id* [**ucid** *ID1*]] 例： `Router(config)# cable dsg tg 1 channel 1 ucid 1`	DSG 1.2 トンネルが適用されるアップストリーム チャネルまたはチャネルを設定します。

	コマンドまたはアクション	目的
ステップ 5	**cabledsgtg** *group-id* [**channel** *channel-id* [**vendor-param** *vendor-group-id*]] 例： `Router(config)# cable dsg tg 1 channel 1 vendor-param 1`	アップストリーム DSG 1.2 チャネルにベンダー固有のパラメータを設定します。
ステップ 6	**cabledsgvendor-param** *group-id* **vendor** *vendor-index* **oui** *oui* **value** *value-in-TLV* 例： `Router(config)# cable dsg vendor-param 1 vendor 1 oui ABCDEA value 0101AB`	A-DSG 1.2 にベンダー固有のパラメータを設定します。Cisco CMTS からこの設定を削除するには、このコマンドの no 形式を使用します。
ステップ 7	**cabledsgchan-list** *list-index* **index** *entry-index* **freq** *freq* 例： `Router(config)# cable dsg chan-list 1 index 1 freq 47000000`	A-DSG 1.2 ダウンストリーム チャネル リストを設定します。このチャネル リストは、セットトップ ボックスがその動作に適した DSG トンネルを探すのに検索できる DSG チャネル（ダウンストリーム周波数）のリストです。A-DSG 1.2 チャネル リストを Cisco CMTS から削除するには、このコマンドの no 形式を使用します。
ステップ 8	**cabledsg timer inde** [**Tdsg1** *Tdsg1*]	[**Tdsg2** *Tdsg2*]	[**Tdsg3** *Tdsg3*]	[**Tdsg4** *Tdsg4*] 例： `Router(config)# cable dsg timer 1 Tdsg1 1 Tdsg2 2 Tdsg3 3 Tdsg4 4`	ダウンストリーム チャネルと関連付け、ダウンストリーム チャネル ディスクリプタ（DCD）メッセージにエンコードされるように、A-DSG 1.2 タイマー エントリを設定します。Cisco CMTS からケーブル DSG タイマーを削除するには、このコマンドの no 形式を使用します。
ステップ 9	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。

次の作業

トラブルシューティングのヒント

拡張モード DOCSIS セットトップ ゲートウェイ機能のモニタリングおよびデバッグ方法, （1134 ページ）に記載されている **debug** および **show** コマンドを参照してください。

サブインターフェイスへの DSG トンネル グループの追加

この手順では、cable dsg tg group-id コマンドを使用してサブインターフェイスに DSG トンネル グループを追加します。サブインターフェイスに DSG トンネル グループを追加したら、ダウンストリーム DSG が設定されている場合は、適切な IP Internet Group Management Protocol（IGMP）の静的結合が作成され、DSG トラフィックの転送が開始されます。

はじめる前に

IGMP の静的結合には、ダウンストリーム DSG が必要です。

制約事項

DSG トンネル グループを関連付けられるのは、同じバンドル インターフェイス内のサブインターフェイス 1 つだけです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

ステップ 2	**configureterminal**
	例：
	`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	**interfacebundle***bundle-subif-number*
	例：
	`Router(config)# interface bundle 11.2`
	`Router(config-subif)#`
		インターフェイス バンドルを指定し、サブインターフェイス コンフィギュレーション モードを開始します。

ステップ 4	**cabledsgtg***group-id* 例： `Router(config-subif)# cable dsg tg 1`	サブインターフェイスに DSG トンネル グループを追加します。
ステップ 5	end 例： `Router(config-subif)# end`	特権 EXEC モードに戻ります。

拡張モード DSG 1.2 用の DSG クライアントの設定

グローバル コンフィギュレーションおよび DSG クライアント コンフィギュレーションを Cisco CMTS の DSG 1.2 に設定したら、DSG 1.2 クライアント コンフィギュレーションを続行するには、次の手順を実行します。

制約事項 **in-dcdignore** オプションは、DSG-IF-MIBS 仕様ではサポートされません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cabledsgclient-list** *client-list-id* **id-index** *id* {**application-id** *app-id* | **ca-system-id** *sys-id* | **mac-addr** *mac-addr* | **broadcast** [*broadcast-id*]} 例： `Router(config)# cable dsg client-list 1 id-index 1 mac-addr abcd.abcd.abcd`	DSG クライアント パラメータを設定します。このコマンドは以前の Cisco IOS リリースから変更されており、DSG 1.2 では、このコマンドはクライアント ID ブロードキャスト タイプとベンダー固有のパラメータ インデックスにオプションのブロードキャスト ID を指定します。
ステップ 4	**cabledsgclient-list** *client-list-id* **id-index** *id* [**vendor-param** *vendor-group-id*] 例： `Router(config-if)# cable dsg client-list 1 id-index 1 vendor-param 1`	DSG クライアントにベンダー固有のパラメータを設定します。
ステップ 5	**cabledsgtunnel** *tunnel id* **mac_addr** *mac addr* **tg** *tunnel-group* **clients** *client-list-id* [**enable** | **disable**]	このコマンドは、トンネル グループとクライアント リスト ID を DSG トンネルに関連付けるように変更されています。また、オプショ

	コマンドまたはアクション	目的
	例： `Router(config)# cable dsg tunnel mac-addr abcd.abcd.abcd tg 1 clients 1 enable`	ンの QoS サービス クラス名をこのトンネルに関連付けることもできます。 （注） Cisco CMTS ルータでケーブル サービス クラスと A-DSG トンネルを関連付けるには、グローバル コンフィギュレーション モードで cable dsg tunnel srv-class コマンドを使用します。
ステップ 6	**cabledsgcfr** *cfr index* [**dest-ip** {*ipaddr |hostname}]* [**tunnel** *tunnel-index*][**dest-port** *start end*]| [**priority** *priority*][**src-ip**{*ipaddr |hostname}* [**src-prefix-len** *length*]] [**enable**|**disable**] [**in-dcd**{**yes**	**no**|**ignore**}] 例： `Router(config)# cable dsg cfr 1 dest-ip 224.225.225.225 tunnel 1 dest-port 40 50 priority 2 src-ip ciscovideo.com src-prefix-len 24 enable`	DCD パラメータのオプション サポートで DSG 分類子インデックスを指定し、DCD メッセージにこの分類子を含めるかどうかを表します。 （注） **ignore** オプションを使用すると、DSG 分類子が DCD メッセージに含まれません。

ステップ 7	**end**
	例：
	`Router(config)# end`
	`Router#`
		特権 EXEC モードに戻ります。

次の作業

トラブルシューティングのヒント

拡張モード DOCSIS セットトップ ゲートウェイ機能のモニタリングおよびデバッグ方法, （1134 ページ）に記載されている **debug** および **show** コマンドを参照してください。

拡張モード DSG 1.2 用のダウンストリーム DSG 1.2 の設定

グローバルおよびクライアント コンフィギュレーションが Cisco CMTS の DSG 1.2 に設定されている場合、DSG 1.2 ダウンストリーム コンフィギュレーションを続行するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**interfacecable** {*slot* /*port* |*slot* /*subslot*/*port* } 例： `Router(config)# interface cable 8/1/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**cabledownstreamdsgtg** *group-id* **[channel** *channel-id]* 例： `Router(config-if)# cable downstream dsg tg 1 channel 1`	DSG トンネル グループとダウンストリーム インターフェイスを関連付けます。この設定を削除するには、このコマンドの **no** 形式を使用します。
ステップ 5	**cabledownstreamdsgchan-list** *list-index* 例： `Router(config-if)# cable downstream dsg chan-list 2`	DCD メッセージに含めるように、A-DSG チャネル リスト エントリとダウンストリーム チャネルを関連付けます。この設定を削除するには、このコマンドの **no** 形式を使用します。
ステップ 6	**cabledownstreamdsgtimer** *timer-index* 例： `Router(config-if)# cable downstream dsg timer 3`	DCD メッセージに含めるように、DSG タイマ エントリとダウンストリーム チャネルを関連付けます。この設定を削除するには、このコマンドの no 形式を使用します。
ステップ 7	**cabledownstreamdsgvendor-param** *vsif-grp-id* 例： `Router(config-if)# cable downstream dsg vendor-param 2`	DCD メッセージに含めるように、A-DSG ベンダー パラメータとダウンストリームを関連付けます。Cisco CMTS からこの設定を削除するには、このコマンドの no 形式を使用します。

	コマンドまたはアクション	目的
ステップ 8	**cabledownstreamdsg**[**dcd-enable**| **dcd-disable**] 例： `Router(config-if)# cable downstream dsg dcd-enable`	DCD メッセージがダウンストリーム チャネルで送信できるようにします。このコマンドは、Cisco CMTS の A-DSG に現在有効なルールまたはトンネルがない場合に使用されます。DCD メッセージを無効にするには、このコマンドの **disable** 形式を使用します。
ステップ 9	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。

IP マルチキャスト動作の設定

ここでは、Cisco CMTS のケーブル インターフェイスおよび WAN インターフェイスで IP マルチキャスト伝送の動作を設定する方法について説明します。DSG トラフィックで使用されている各ケーブル インターフェイス、および IP マルチキャスト トラフィックを転送しているネットワーク コントローラまたはコンディショナル アクセス（CA）サーバに接続された各 WAN インターフェイスに対して、次の設定を実行する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Router# configure terminal`	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 2	**ipmulticast-routing** 例： `Router(config)# ip multicast-routing`	ルータでマルチキャスト ルーティングを有効にします。
ステップ 3	**ip pim ssm** {**default** | **range***{access-list* | *word* }} 例： `Router(config)# ip pim ssm range 4`	IP マルチキャスト アドレスの Source Specific Multicast（SSM）範囲を定義します。SSM 範囲を無効にするには、このコマンドの no 形式を使用します。

	コマンドまたはアクション	目的
		（注） IP マルチキャスト アドレスの SSM 範囲を **ippimssm** コマンドで定義すると、SSM 範囲内で承認および発信される Multicast Source Discovery Protocol（MSDP）の送信元アクティブ（SA）メッセージがなくなります。
ステップ 4	ip cef distributed 例： `Router(config)# ip cef distributed`	ルート プロセッサ カードで Cisco Express Forwarding（CEF）を有効にします。CEF を無効にするには、このコマンドの no 形式を使用します。 **ipcef** コマンドのその他の情報については、Cisco.com 上の次のドキュメントを参照してください。 • 『*Cisco IOS Switching Services Command Reference*, Release 12.3』 http://www.cisco.com/en/US/docs/ios/12_3/switch/command/reference/swtch_r.html
ステップ 5	**interfacebundle** *bundle-number* 例： `Router(config)# interface bundle 10`	DSG トラフィックに使用される各インターフェイス バンドルのインターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ippim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**} 例： `Router(config-if)# ip pim dense-mode`	ケーブル インターフェイスで、DSG 機能の使用に必要な Protocol Independent Multicast（PIM）を有効にします。 （注） マルチキャスト トラフィックを転送する各インターフェイスでこのコマンドを設定する必要があります。
ステップ 7	DSG トラフィックで使用する各ケーブル インターフェイスに対して、ステップ 5, （1126 ページ）およびステップ 6, （1126 ページ）を繰り返します。また、DSG ネットワーク コントローラおよびコンディショナル アクセス（CA）サーバから IP マルチキャスト トラフィックを転送する各 WAN インターフェイスに対して、次のステップを繰り返します。	

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DNS クエリと DSG 名プロセスの有効化

DSG 名プロセスにより、Cisco CMTS ルータは、DNS サーバを照会して分類子更新を高速化できます。

はじめる前に

グローバル コンフィギュレーション モードで **ipdomain-lookup** コマンドを使用して、IP DNS ベースのホスト名/アドレス変換が Cisco CMTS ルータで設定されていることを確認します。デフォルトでは設定されていますが、ステータスは実行コンフィギュレーションに表示されません。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Router# configure terminal`	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 2	**ipdomain-name** *name* 例： `Router(config)# ip domain-name cisco.com`	Cisco IOS ソフトウェアで使用する IP ドメイン名を設定し、不完全なホスト名のドメインを補完します。
ステップ 3	r **ipname-serve***server-address*[**multiple-server-addresses**] 例： `Router(config)# ip name-server 131.108.1.111`	サーバの IP アドレスを設定します。
ステップ 4	**cabledsgname-update-interva**l*minutes* 例： `Router(config)# cable dsg name-update-interval 10`	DNS サーバの FQDN 分類子に変更がないかを確認する間隔を設定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。

ユニキャスト メッセージをサポートする NAT の設定

ここでは、DSG メッセージングで IP ユニキャスト アドレスを使用できるようにするために、ネットワーク アドレス変換（NAT）について Cisco CMTS ルータを設定する方法について説明します。これにより、Cisco CMTS ルータは、DSG トラフィックに適した IP マルチキャスト アドレスに受信 IP ユニキャスト アドレスを変換できます。

Cisco cBR-8 ルータの場合、A-DSG 1.2 はユニキャスト メッセージをサポートする Cisco CMTS に近い外部ルータを使用できます。この場合、近接ルータは NAT をサポートし、Cisco CMTS にアドレス変換されたマルチキャスト IP パケットを送信する必要があります。

ヒント　拡張モード DSG の設定例, （1137 ページ）で説明しているようにケーブル インターフェイスを DSG の動作に合わせて設定してから、この手順を実行する必要があります。

（注）　Cisco CMTS ルータが「IP Plus」（-i-）Cisco IOS ソフトウェア イメージを実行している場合のみ、NAT がサポートされます。イメージの可用性と要件の詳細については、Cisco IOS リリースのリリース ノートを参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Router# configure terminal`	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 2	**interface** *wan-interface* 例： `Router(config)# interface FastEthernet0/0`	指定した WAN インターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipnatoutside** 例： `Router(config-if)# ip nat outside`	「外部」（パブリック）NATインターフェイスとして WAN インターフェイスを設定します。
ステップ 4	**interfacebundle** *bundle-number* 例： `Router(config-if)# interface bundle 10`	指定したインターフェイス バンドルのインターフェイス コンフィギュレーション モードを開始します。 （注） このインターフェイス バンドルは、DSG の動作に合わせて設定しておく必要があります。
ステップ 5	**ipaddress** *ip-address mask* **secondary** 例： `Router(config-if)# ip address 192.168.18.1 255.255.255.0 secondary`	DSG トラフィックで使用されるユニキャスト アドレスと一致する IP アドレスおよびサブネットを使用して、ケーブル インターフェイスを設定します。この IP アドレスとそのサブネットは、ケーブル ネットワーク内の他のケーブル インターフェイス、ケーブルモデム、その他の種類のトラフィックで使用しないでください。
ステップ 6	**ipnatinside** 例： `Router(config-if)# ip nat inside`	「内部」（プライベート）NATインターフェイスとしてケーブルインターフェイスを設定します。
ステップ 7	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**ipnatinsidesourcestatic** *ip-multicast-address cable-ip-address* 例： `Router(config)# ip nat inside source static 224.3.2.1 192.168.18.2`	ケーブル インターフェイスに割り当てられるユニキャスト IP アドレスを DSG トラフィックで使用されるマルチキャスト アドレスにマッピングします。
ステップ 9	DSG ユニキャスト トラフィックに合わせて構成する各ケーブル インターフェイスについて、ステップ 2, （1128 ページ）およびステップ 8, （1129 ページ）を繰り返します。	

	コマンドまたはアクション	目的
ステップ 10	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

マルチキャスト運用に対応する WAN インターフェイスの設定

他のドキュメントで説明されているような Cisco CMTS における基本的な WAN インターフェイス設定に加えて、A-DSG 1.2 で IP マルチキャスト運用をサポートするために、必要に応じて次の WAN インターフェイス コマンドを Cisco CMTS で設定する必要があります。

- **ippim**
- **ippimssm**
- **ipcef**

これらのコマンドは、IP マルチキャスト動作の設定, （1125 ページ）、および Cisco.com 上の次のドキュメントで説明されています。

ippim コマンドのその他の情報については、Cisco.com 上の次のドキュメントを参照してください。

- 『*Cisco IOS IP Command Reference, Volume 3 of 4*: Multicast, Release 12.3』

http://www.cisco.com/en/US/docs/ios/12_3/ipmulti/command/reference/iprmc_r.html

ippimssm コマンドのその他の情報については、Cisco.com 上の次のドキュメントを参照してください。

- 『*Cisco IOS IP Command Reference, Volume 3 of 4: Multicast* , Release 12.3 T』

http://www.cisco.com/en/US/docs/ios/12_3t/ip_mcast/command/reference/ip3_i2gt.html

ipcef コマンドのその他の情報については、Cisco.com 上の次のドキュメントを参照してください。

- 『*Cisco IOS Switching Services Command Reference*, Release 12.3』

http://www.cisco.com/en/US/docs/ios/12_3/switch/command/reference/swtch_r.html

パケット フィルタリング用の標準 IP アクセス リストの設定

ここでは、承認されたトラフィックのみがケーブル インターフェイスで許可されるように、標準 IP アクセス リストを設定する方法について説明します。

ヒント　この手順では、アクセスが許可された IP アドレスの範囲を決定するために、アクセス リストが IP アドレスとビットマスクをどのように使用するかについて基本的な知識を把握していることを前提としています。アクセス リストの設定に関する詳細については、その他の参考資料, （1141 ページ）に記載されたマニュアルを参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Router# configure terminal`	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 2	**access-list** *access-list* **permit** *group-ip-address* [*mask*] 例： `Router(config)# access-list 90 permit 228.1.1.1`	指定した *group-ip-address* と *mask* に一致する特定のマルチキャスト アドレスへのアクセスを許可するアクセス リストを作成します。
ステップ 3	**access-list** *access-list* **deny** *group-ip-address* [*mask*] 例： `Router(config)# access-list 90 deny 224.0.0.0 15.255.255.255`	指定した *group-ip-address* と *mask* に一致するマルチキャストアドレスへのアクセスを拒否するアクセスリストを設定します。
ステップ 4	**access-list** *access-list* **denyany** 例： `Router(config)# access-list 90 deny any`	事前に設定した IP アドレス以外からのアクセスが拒否されるように、アクセス リストを設定します。
ステップ 5	**interfacebundle** *bundle-number* 例： `Router(config)# interface bundle 10`	指定したインターフェイス バンドルのインターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ipaccess-group** *access-list* 例： `Router(config-if)# ip access-group 90`	（オプションですが推奨）パケットがインターフェイスで許可される前にアクセス リストでフィルタリングされるように、アクセス リストを使用してインターフェイスを設定します。

	コマンドまたはアクション	目的
		（注） 標準アクセス リストで許可されるのは、前のステップで指定したアドレス 1 つのみです。拒否されたトンネルのマルチキャスト アドレスのみが含まれるアウトバウンド アクセス リストを適用すると、DSG トラフィックの通過は許可されません。 （注） Cisco cBR-8 ルータでは、ケーブル インターフェイスの受信アクセス リストがマルチキャスト トラフィックには適用されないため、ここでも適用されません。その結果、Cisco cBR-8 では、ネットワーク上のケーブル モデムまたは CPE デバイスから発信されるパケット、およびマルチキャスト グループに送信されるパケットの発信方向でブロックされる拡張アクセス リストを使用する必要があります。マルチキャスト グループには、インターフェイスで有効化された A-DSG 1.1 ルールに関連する分類子が含まれます。
ステップ 7	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

マルチキャスト グループ フィルタリング用の標準 IP アクセス リストの設定

ここでは、DSG セットトップ ボックスなどの DOCSIS 以外のデバイスが、承認済みのマルチキャスト グループ アドレスと DSG トンネルにのみアクセスできるように、標準 IP アクセス リストを設定する方法について説明します。

ヒント この手順では、アクセスが許可された IP アドレスの範囲を決定するために、アクセス リストが IP アドレスとビットマスクをどのように使用するかについて基本的な知識を把握していることを前提としています。アクセス リストの設定に関する詳細については、その他の参考資料, （1141 ページ）に記載されたマニュアルを参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Router# configure terminal`	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 2	**access-list** *access-list* **permit** *group-ip-address* [*mask*] 例： `Router(config)# access-list 90 permit 228.1.1.1`	指定した *group-ip-address* と *mask* に一致する特定のマルチキャスト アドレスへのアクセスを許可するアクセス リストを作成します。
ステップ 3	**access-list** *access-list* **deny** *group-ip-address* [*mask*] 例： `Router(config)# access-list 90 deny 224.0.0.0 15.255.255.255`	指定した *group-ip-address* と *mask* に一致するマルチキャスト アドレスへのアクセスを拒否するアクセス リストを設定します。
ステップ 4	**access-list** *access-list* **denyany** 例： `Router(config)# access-list 90 deny any`	事前に設定した IP アドレス以外からのアクセスが拒否されるように、アクセス リストを設定します。
ステップ 5	**interfacecable** *interface* 例： `Router(config)# interface cable 3/0`	指定したケーブル インターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 6	**ipigmpaccess-group** *access-list* [*version*] 例： `Router(config-if)# ip igmp access-group 90`	（オプションですが推奨）承認済みのデバイスのみが DSG トンネルにアクセスできるように、関連するアクセス リストのみからトラフィックを受け入れるインターフェイスを設定します。
ステップ 7	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

プライマリ チャネルの A-DSG 転送の無効化

プライマリ対応インターフェイスごとに A-DSG 転送を無効にできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Router# configure terminal`	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 2	**interfacemodular-cable** *slot* /*subslot*/*port* :*interface-number* 例： `Router(config)# interface modular-cable 1/0/0:0`	モジュラ ケーブル インターフェイスを指定し、ケーブル インターフェイス コンフィギュレーション モードを開始します。このコマンドの変数は、Cisco CMTS ルータおよび Cisco IOS-XE ソフトウェア リリースに応じて異なる場合があります。
ステップ 3	**cabledownstreamdsgdisable** 例： `Router(config-if)# cable downstream dsg disable`	プライマリ対応インターフェイスで A-DSG 転送および DCD メッセージを無効にします。
ステップ 4	**end** 例： `Router(config-if)# end`	特権 EXEC モードに戻ります。

拡張モード DOCSIS セットトップ ゲートウェイ機能のモニタリングおよびデバッグ方法

ここでは、拡張モード DOCSIS セットトップ ゲートウェイ機能に関する情報をモニタリングおよび表示するのに使用できる次のコマンドについて説明します。

拡張モード DSG 1.2 のグローバル設定の表示

次のコマンドは、グローバルに設定された、またはインターフェイス レベルでの DSG 設定、ステータス、統計情報、および複数タイプの DSG 1.2 トンネル情報を表示します。

showcabledsgcfr

分類子の状態、送信元、宛先 IP アドレスなど、すべての DSG 分類子の詳細を確認するには、**showcabledsgcfr** コマンドを使用します。

特定の DSG 分類子の詳細を確認するには、**showcabledsgcfr** *cfr-id* コマンドを使用します。

すべての DSG 分類子の詳細な出力を確認するには、**showcabledsgcfrverbose** コマンドを使用します。

単一の DSG 分類子の詳細な出力を確認するには、**showcabledsgcfr** *cfr-id***verbose** コマンドを使用します。

showcabledsghost

Cisco CMTS ルータの DSG ホスト名および IP アドレスのマッピングを確認するには、**showcabledsghost** コマンドを使用します。

Cisco CMTS ルータの DSG ホスト名および IP アドレスのマッピングの詳細な出力を確認するには、**showcabledsghostverbose** コマンドを使用します。

show cable dsg tunnel

トンネル MAC アドレス、状態、トンネル グループ ID、トンネルとその状態に関連する分類子を表示するには、特権 EXEC モードで **showcabledsgtunnel** コマンドを使用します。また、このコマンドは、トンネルが関連付けられたインターフェイスの数、関連するクライアント、すべての設定済みトンネルの QoS サービス クラス名の数も表示します。

特定の DSG トンネルの情報を表示するには、情報を表示するトンネルを指定した **showcabledsgtunnel** *tunnel-id* コマンドを使用します。

showcabledsgtunnel *tunnel-id* [**cfr** | **clients** | **interfaces** | **statistics** | **verbose**]

- **cfr**：DSG トンネルの分類子を表示します。
- **clients**：DSG トンネルのクライアントを表示します。
- **interfaces**：DSG トンネルのインターフェイスを表示します。
- **statistics**：DSG トンネルの統計情報を表示します。
- **verbose**：DSG トンネルの詳細情報を表示します。

show cable dsg tg

すべての DSG トンネル グループの設定済みパラメータを表示するには、**showcabledsgtg** コマンドを使用します。

（注） **showcabledsgtg** コマンド出力の **Chan state** 列に、トンネル グループに属するチャネルが有効または無効のどちらに設定されているかが示されます。トンネル グループが有効になっていても、そのトンネル グループ内の特定のチャネルが無効になっている可能性があります。

指定したトンネル グループの設定済みパラメータを表示するには、**showcabledsgtg** *tg-id***channel** *channel-id* コマンドを使用します。

指定したトンネル グループの詳細情報を表示するには、**showcabledsgtg** *tg-id***channel** *channel-id***verbose** コマンドを使用します。

showrunning-configinterface

サブインターフェイスに接続するトンネル グループを表示するには、次の例に示すように特権 EXEC モードで **showrunning-configinterface** コマンドを使用します。

```
Router# show running-config interface bundle 11.2
!
interface Bundle11.2
 ip address 4.4.2.1 255.255.255.0
 no ip unreachables
 ip pim sparse-mode
 ip igmp static-group 230.1.1.30
 no cable ip-multicast-echo
 cable dsg tg 61
end
```

（注） DSG 設定時に自動的に作成される IGMP 静的グループの IP アドレスは、**showrunning-configinterface** コマンド出力には表示されません。

showcabledsgstatic-groupbundle

バンドル インターフェイスで設定されているすべての DSG 静的グループを確認するには、特権 EXEC モードで **showcabledsgstatic-groupbundle** コマンドを使用します。

拡張モード DSG 1.2 のインターフェイスレベル設定の表示

次の **show** コマンドは、A-DSG 1.2 のインターフェイス レベルの設定を表示します。

show cable dsg tunnel interfaces

関連するトンネルのすべてのインターフェイスと DSG ルールを表示するには、特権 EXEC モードで **showcabledsgtunnelinterfaces** コマンドを使用します。

showcabledsgtunnel （*tunnel-id*） **interfaces**

show interfaces cable dsg downstream

DSG ダウンストリーム インターフェイス設定情報を表示して、DSG トンネル、分類子、クライアント、ベンダー固有のパラメータを含めるには、特権 EXEC モードで **showinterfacescabledsgdownstream** コマンドを使用します。

show interfaces cable dsg downstream dcd

特定のダウンストリームの DCD 統計情報を表示するには、特権 EXEC モードで **showinterfacescabledsgdownstreamdcd** コマンドを使用します。このコマンドでは DCD タイプ/長さ/値の情報のみが表示されます（以前に **debugcabledsg** コマンドを有効にした場合）。

show interfaces cable dsg downstream tg

DSG トンネル グループ パラメータと、トンネル グループに適用されるルール情報を表示して、トンネルとトンネルの状態、分類子、クライアント情報を含めるには、特権 EXEC モードで **showinterfacescabledsgdownstreamtg** コマンドを使用します。指定した場合は、特定のトンネルの情報を表示できます。

show interfaces cable dsg downstream tunnel

ダウンストリームに関連付けられている DSG トンネルの情報を表示するには、特権 EXEC モードで **showinterfacescabledsgdownstreamtunnel** コマンドを使用します。

拡張モード DSG のデバッグ

Cisco CMTS ルータでの A-DSG のデバッグをイネーブルにするには、特権 EXEC モードで debug cable dsg コマンドを使用します。

拡張モード DSG の設定例

ここでは、次のコンポーネントを搭載する DSG ネットワーク例を示します。

- Cisco ユニバーサル ブロードバンド ルータ 2 台
- 各 DSG の実装用の IP マルチキャスト
- 各 Cisco CMTS 用の DSG クライアント 2 台
- DSG サーバ（各 Cisco CMTS に 1 台ずつ）2 台

各 Cisco CMTS を次のように設定します。このトピックの後半では、このアーキテクチャに適用する設定例について説明します。

CMTS ヘッドエンド 1

- DSG サーバ #1：DSG サーバの IP アドレスを 12.8.8.1 に設定し、IP マルチキャストを経由して Cisco CMTS に接続
- Cisco CMTS の宛先 IP アドレス：228.9.9.1
- DSG トンネル アドレス：0105.0005.0005
- 2 台の DSG クライアントをサポートするダウンストリーム #1：
  - DSG クライアント #1：ID 101.1.1
  - DSG クライアント #2：ID 102.2.2

CMTS ヘッドエンド 2

- DSG サーバ #2：DSG サーバの IP アドレスを 12.8.8.2 に設定し、IP マルチキャストを経由して Cisco CMTS に接続
- Cisco CMTS の宛先 IP アドレス：228.9.9.2
- DSG トンネル アドレス：0106.0006.0006
- 2 台の DSG クライアントをサポートするダウンストリーム #2：
  - DSG クライアント #1：ID 101.1.1
  - DSG クライアント #2：ID 102.2.2

MAC DA 代替による 2 つの DSG トンネルの例

この設定では、上述の 2 種類の Cisco CMTS ヘッドエンドの場合、次の 2 つの DSG ルール セットがあり、それぞれが各自の方法で Cisco CMTS に適用されます。

次の設定が DSG #1 と 2 つのダウンストリームに適用されます。

- DSG ルール ID 1
- DSG クライアント ID 101.1.1
- DSG トンネル アドレス 105.5.5

次の設定は DSG ルール #2 と 2 つのダウンストリームに適用されます。

- DSG ルール ID 1
- DSG クライアント ID 102.2.2
- DSG トンネル アドレス 106.6.6

ダウンストリームごとに地域化した DSG の例

この設定内容で、かつ上述の 2 種類の Cisco CMTS ヘッドエンドの場合、このアーキテクチャで設定できるダウンストリーム ルールは次の 2 つです。

- ダウンストリーム ルール #1
  - DSG ルール ID #1
  - DSG クライアント ID：101.1.1
  - DSG トンネル アドレス：105.5.5
- ダウンストリーム ルール #2
  - DSG ルール ID #2
  - DSG クライアント ID：102.2.2
  - DSG トンネル アドレス：106.6.6

アップストリームごとに地域化した DSG の例

この設定では、上述の 2 種類の Cisco CMTS ヘッドエンドの場合、このアーキテクチャで設定できるアップストリーム ルールは次の 2 つです。

- アップストリーム ルール #1
  - DSG ルール ID #1
  - DSG クライアント ID：101.1.1
  - DSG UCID 範囲：0 ～ 2
  - DSG トンネル アドレス：105.5.5
- アップストリーム ルール #2
  - DSG ルール ID #2
  - DSG クライアント ID：102.2.2
  - DSG UCID 範囲：3 ～ 5
  - DSG トンネル アドレス：106.6.6

すべての分類子と MAC DA 代替による 2 つの DSG トンネルの例

この設定では、上述の 2 種類の Cisco CMTS ヘッドエンドの場合、次の 2 つの DSG ルール セットがあり、それぞれが各自の方法で Cisco CMTS に適用されます。

次の設定が DSG #1 に適用されます。

- DSG ルール ID 1

- ダウンストリーム 1 と 2
- DSG クライアント ID 101.1.1
- DSG トンネル アドレス 105.5.5
- DSG 分類子 ID：10
- IP SA：12.8.8.1
- IP DA：228.9.9.1
- UDP DP：8000

次の設定が DSG ルール #2 に適用されます。

- DSG ルール ID 2
- ダウンストリーム 1 と 2
- DSG クライアント ID 102.2.2
- DSG トンネル アドレス 106.6.6
- DSG 分類子 ID：20
- IP SA：12.8.8.2
- IP DA：228.9.9.2
- UDP DP：8000

複数の DSG サーバから IP マルチキャストをサポートする 1 つの DSG トンネルの例

この設定内容で、かつ上述の 2 種類の Cisco CMTS ヘッドエンドの場合、IP マルチキャストをサポートする複数の DSG サーバの DSG トンネルの例は次の 1 つです。

- DSG ルール ID 1
- ダウンストリーム 1 と 2
- DSG クライアント ID 101.1.1 と 102.2.2
- DSG トンネル アドレス 105.5.5
- DSG 分類子 ID：10
    - IP SA：12.8.8.1
    - IP DA：228.9.9.1
    - UDP DP：8000
- DSG 分類子 ID：20
    - IP SA：12.8.8.2
    - IP DA：228.9.9.2

° UDP DP：8000

例：DNS クエリの有効化

次の例では、Cisco CMTS ルータで DNS クエリを有効にする方法について説明します。

```
Router# configure terminal
Router(config)# ip domain-lookup
Router(config)# ip domain-name cisco.com
Router(config)# ip name-server 131.108.1.111
Router(config)# cable dsg name-update-interval 10
Router(config)# end
```

例：プライマリ チャネルの A-DSG 転送の無効化

次の例では、Cisco CMTS ルータのプライマリ対応モジュラ インターフェイスの A-DSG 転送を無効にする方法を示します。

```
Router# configure terminal
Router(config)# interface modular-cable 1/0/0:0
Router(config-if)# cable downstream dsg disable
Router(config-if)# end
```

その他の参考資料

ここでは、A-DSG 1.2 に関連する参照資料を示します。

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco CMTS ルータの拡張モード DSG 1.2 に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャセット、またはプラットフォームを確認できます。

Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *174*：*Cisco CMTS* ルータの *DOCSIS* セットトップ ゲートウェイと *A-DSG* に関する機能情報

機能名	リリース	機能情報
Cisco CMTS ルータの DOCSIS セットトップ ゲートウェイ	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 71 章

Cisco CMTS ルータ用 Cisco Network Registrar

この章は、Cisco Network Registrar（CNR）のマニュアルを捕捉するものであり、Cisco ユニバーサル ブロードバンド ルータをネットワークのヘッドエンドの CMTS として使用して光同軸ハイブリッド（HFC）ネットワークをプロビジョニングする場合の追加のケーブルについて説明します。

（注） CNR サーバでの IPv6 プロビジョニングについては、「IPv6 on Cable」を参照してください。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *175* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

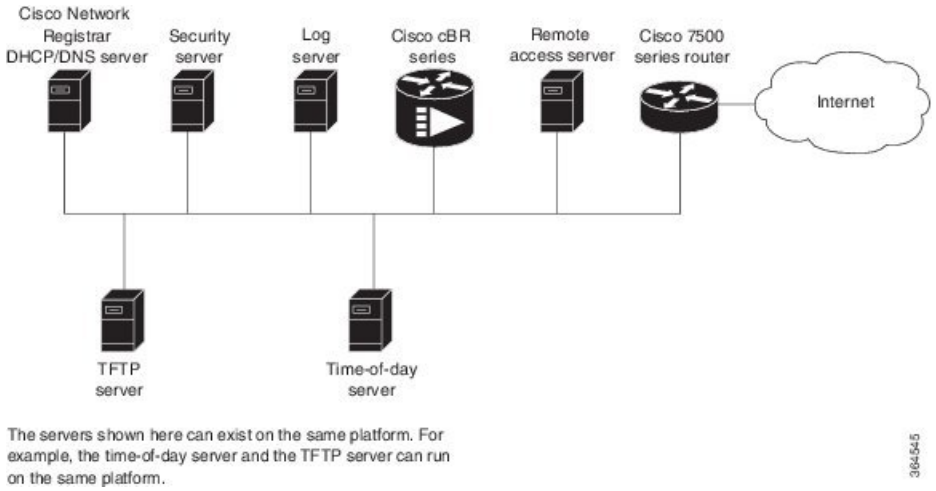
Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

HFC ネットワークに必要なサーバ

HFC ネットワークでの双方向データ ケーブル モデムをサポートするには、TFTP サーバ、DHCP サーバ、および Time-of-day（TOD）サーバが必要です。これらのサーバを使用できない場合、ケーブル モデムはブートしません。ログ サーバとセキュリティ サーバは、ケーブル モデムの設

定と動作に必要ありません。ログサーバまたはセキュリティサーバが存在しない場合、ケーブルモデムは警告メッセージを生成しますが、正常にブートして機能し続けます。

図 *29*：双方向 *HFC* ネットワークに必要なサーバ



このプロビジョニング モデルでは、TOD および TFTP サーバは RFC 868 および RFC 1350 仕様の標準的なインターネット実装です。UNIX ベースのオペレーティング システムを実行するコンピュータにはたいてい、標準的なソフトウェア機能として TOD サーバおよび TFTP サーバが搭載されています。通常、TOD サーバは UNIX *inetd* に組み込まれており、追加設定は必要ありません。TFTP サーバは標準ソフトウェアで通常ディセーブルになっていますが、ユーザがイネーブルにすることができます。Microsoft NT のサーバ ソフトウェアには、サービス コントロール パネルによりイネーブル化できる TFTP サーバが含まれています。Microsoft NT に TOD サーバは含まれません。Microsoft NT の TOD サーバのパブリック ドメイン バージョンは複数のサイトからダウンロードできます。

上の図に示された DHCP およびドメイン ネーム システム（DNS）サーバは、Cisco Network Registrar バージョン 2.0 以降で利用可能な DHCP/DNS サーバである必要があります。CNR は IP アドレスのポリシーベースの割り当てを実施する唯一の DHCP サーバです。ヘッドエンドは、Cisco cBR-8 コンバージド ブロードバンド ルータである必要があります。リモート アクセス サーバは、単方向（ダウンストリームのみ）の通信に制限された HFC ネットワークでのみ必要です。一方向 HFC ネットワークでは、PC からヘッドエンドを経由したインターネットへのアップストリーム データは、ダイヤルアップ接続により伝送されます。アップストリーム データのこのダイヤルアップ接続は、Telco リターンと呼ばれます。単純化するため、モデルにはログ サーバとセキュリティ サーバは含まれません。『*CiscoNetworkRegistrarUserManual*』で説明しているように、ケーブル モデムのポリシーに適切な DHCP オプションを含めることにより、ログ サーバとセキュリティ サーバを使用するようにケーブル モデムを設定できます。

Cisco Network Registrar について

CNR は、Windows または Solaris上で動作するダイナミック IP アドレス管理システムであり、Dynamic Host Configuration Protocol（DHCP）を使用してブロードバンド ネットワーク上のケーブ

ル インターフェイス、PC、およびその他のデバイスに IP アドレスを割り当てます。CNR ツールには、ケーブル システム管理者が個々の DHCP オプションの定義と表示、ネットワーク上のデバイスの ID またはタイプの定義、および事前定義されたクラスまたはグループへのデバイス割り当てを実行できるスクリプト拡張が含まれています。

ケーブル システム管理者は、CNR ツールを使って以下を提供するポリシーを指定できます。

- 統合された DHCP サーバおよびドメイン ネーム サーバ（DNS）サービス
- ネットワークのサイズに基づく Time-of-Day（ToD）および Trivial File Transfer Protocol（TFTP）サーバ
- DHCP セーフ フェールオーバーおよびダイナミック DNS 更新

（注） これは、CNR 3.0 以上でのみ使用可能です。

スクリプトの概要, （1154 ページ）のセクションで示されている CNR ツールおよび拡張スクリプトを使用すると、ケーブル システム管理者は、各加入者サイトでサポートするサービスと構成に基づいて、ネットワークおよび各ケーブル インターフェイスの範囲、ポリシー、およびオプションを指定できます。

（注） 範囲とは、TCP/IP アドレスの管理グループを指します。範囲内にあるすべての IP アドレスは同じサブネットにある必要があります。

ケーブル システム管理者は、すべての標準オプションのシステム デフォルト ポリシーを定義し、特定のサブネットに関連するオプション（ケーブル インターフェイスなど）について範囲固有のポリシーを使用します。これにより、DHCP は IP アドレスを使用して情報を送信できます。

スクリプトには 7 つのエントリ ポイントがあります。

- post-packet-decode
- pre-client-lookup
- post-client-lookup：クライアント クラス プロセスの結果を検査して対処し、データ項目を pre-packet-encode 拡張ポイントで使用する環境ディクショナリ内に配置します（DHCP リレー オプションを含む）
- check-lease-acceptable
- pre-packet-encode
- post-sent-packet
- pre-dns-add-forward

DHCP を使用する CNR の概要

Cisco Network Registrar（CNR）は、Dynamic Host Configuration Protocol（DHCP）を使用してサービス クラスなどの事前定義されたポリシー セットに基づいてネットワーク上の PC や他の装置に IP アドレスを割り当てる、ダイナミック IP アドレス管理システムです。CNR は、要求側装置の ID またはタイプと適用されているポリシーに基づき、アドレス プールから使用可能な IP アドレスを割り当てます。たとえば、CNR は登録済みの装置と未登録の装置、および特定のサービス クラスに割り当てられている登録済み装置を判別できます。

また、CNR にはプログラムまたはスクリプトによるカスタマイズ可能な拡張機能が提供され、これにより、個々の DHCP オプションを表示したり、オプションの内容に基づいて装置の ID またはタイプを決定したり、事前定義されたクラスまたはグループに装置を割り当てたりできるようになります。これらの拡張機能を使用して、PC とケーブル モデムを区別して、それらに異なるアドレス プールからの IP アドレスを割り当てることができます。

典型的な Data-over-Cable 環境では、サービス プロバイダーは、加入者の顧客宅内装置（CPE）について収集する必要がある情報の量を低減するプロビジョニングの簡略化に関心があります。現行のプロビジョニング モデルをサポートするためには、加入者の住居や職場に現場技術者を派遣してケーブル モデムを設置および設定する必要があります。技術者は現場訪問中に顧客のアカウントのデータベースにケーブル モデムのシリアル番号と MAC アドレスを登録することになる場合があります。ケーブル モデムを再設置するためには現場技術者が加入者サイトに実際に赴く必要があるため、プロバイダーはモデムの情報を容易に追跡できます。

困難なのは、ケーブル加入者の PC に関する情報を手動で登録、追跡することです。加入者が新しい PC を購入したり、ネットワーク インターフェイス カード（NIC）を交換していても、その変更を知らせてこない場合があります。CNR による自動プロビジョニングは、顧客の機器を追跡するのに必要なカスタマー サービスの介入を減らします。このマニュアルで説明するプロビジョニング モデルを使用するために、ケーブル モデムのシリアル番号と MAC アドレスの追跡は依然として必要ですが、加入者サイトに設置された PC または NIC カードに関する情報を追跡する必要はありません。

このマニュアルの残りの部分では、このモデルをサポートするための CNR の設定方法について説明します。以下の項では、ケーブルヘッドエンドに必要な機器とサーバについて説明し、DOCSIS 互換ケーブル モデムと Cisco ユニバーサル ブロードバンド ルータ間のインタラクションの概要を示します。また、このプロビジョニング モデルをサポートするための CNR の設定方法に関する手引きを提供します。

Cisco コンバージド ブロードバンド ルータとケーブル モデムの動作

Cisco コンバージド ブロードバンド ルータとケーブル モデムは、Data Over Cable Service Interface Specification（DOCSIS）標準規格に基づいています。これらの標準規格は、Multimedia Cable Network Systems, Ltd.（MCNS）と呼ばれるケーブル サービス プロバイダーのコンソーシアムによって作成され、そのケーブル ヘッドエンドとさまざまなベンダーが製造するケーブルモデム機器が相互運用することを目的にしています。主な DOCSIS 標準規格では、ケーブル モデムが任意のヘッドエンド機器と通信したり、ヘッドエンド機器が任意のケーブル モデムと通信したりするための基盤を提供します。

アクティビティが複数のチャネルに分散されるように、ケーブルモデムは特定のケーブルチャネル上で動作するように割り当てられます。ヘッドエンドに取り付けられた各 Cisco cBR-8 ルータは、特定のチャネルを処理します。ネットワーク計画の一環として、各ケーブル モデムが使用できるチャネルを決定してください。

ケーブル モデムは、次のイベントが発生するまでネットワークに接続できません。

- ケーブルモデムは初期化して、ヘッドエンドと通信するために使用できる最初の周波数が見つかるまで使用可能な周波数の範囲を調べます。ケーブル モデムは別のベンダーの DOCSIS 互換デバイスの可能性があり、ヘッドエンドは Cisco cBR-8 ルータが取り付けられている可能性があります。初期接続のこの時点では、ケーブルモデムは、適切なチャネルで通信しているかどうかを判断できません。
- ケーブルモデムが DHCP サーバプロセスを実行し、サーバからコンフィギュレーション ファイルを受信します。
- コンフィギュレーション ファイル内のいずれかのパラメータで、使用できるチャネルをケーブル モデムに通知します。
- 割り当てられたチャネルがケーブル モデムに現在接続されている Cisco cBR-8 ルータで使用できない場合、ケーブル モデムは自身をリセットし、割り当てられたチャネルで起動します。
- この 2 回目の DHCP プロセス中に、モデムは正しい CMTS に接続されます。今度はコンフィギュレーション ファイルがロードされます。DOCSIS 互換ケーブル モデムがネットワークにアクセスするには、DHCP サーバに 2 回、2 つの異なるネットワークを介してアクセスすることになります。そのため、クライアントあたり 1 リースの IP アドレッシングが重要です。

ケーブル モデムの DHCP フィールドとオプション

DHCP オプションおよびパケット フィールドは、ケーブル モデムが正常に起動して動作するために必要です。以下の表は、必須の DHCP オプションとフィールドを示しています。

表 *176*：必須の *DHCP* フィールドとオプション

必須フィールド/オプション	Cisco Network Registrar のフィールド/オプション	値および説明
フィールド		

必須フィールド/オプション	Cisco Network Registrar のフィールド/オプション	値および説明
giaddr	-	[IP Address]。DHCP パケットがリレー エージェントを DHCP サーバにパススルーするときに、リレー エージェントは一意の IP アドレスをパケットに指定してこのフィールドに保存します。リレー エージェントは、iphelper 属性が定義されている cBR-8 ルータです。
subnet-mask	-	giaddr フィールドに保存されている IP アドレスのサブネット マスク。この値は、リレーエージェントによってDHCPパケットにも保存されます。
file	Packet-file-name	TFTP サーバから読み取られるケーブル モデム コンフィギュレーション ファイルの名前。
siaddr	Packet-siaddr	コンフィギュレーション ファイルが保存されている TFTP サーバの IP アドレス。
オプション		
Time-servers	-	RFC 868 標準で指定されたタイム サーバを実行しているホストのリスト。
Time-offset	-	ケーブル モデムの内部クロックの協定世界時（UTC）からのタイムオフセット。この値は、エラー ログにタイムスタンプを付けるときに保存される現地時刻を計算するためにケーブル モデムによって使用されます。
MCNS-security-server	-	セキュリティ サーバの IP アドレス。これはセキュリティが必要になったときに設定してください。詳細については、RFC 1533 を参照してください。

Cisco Network Registrar の構成例

テスト構成で Cisco Network Registrar を設定するために、次の情報を使用できます。この構成は、DHCP 関連の設定のみを説明します。DNS の設定やダイナミック DNS（DDNS）の設定については扱いません。範囲、プライマリ範囲、セカンダリ範囲、範囲選択タグ、クライアント クラス、CNR ポリシーなど、重要な CNR の概念を理解しておく必要があります。これらの概念の詳細については、『Using Network Registrar』パブリケーションを参照してください。

テスト構成では、次の操作を実行するように CNR を構成できます。

- 複数のネットワーク番号をサポートするポートを介して、HFC ネットワーク上のケーブル モデムや PC から DHCP 要求を受信します。ヘッドエンドの Cisco cBR-8 ルータをフォワーダとして設定する必要があります（iphelper が構成されます）。
- net-10 ネットワーク（インターネットへのルーティング不可能）と net-24 ネットワーク（インターネットへのルーティング可能）という 2 つのネットワークで IP アドレスを提供します。
- デバイスの MAC アドレスに基づいてケーブル モデムと PC との違いを通知し、net-24 アドレスを PC へ、および net-10 アドレスをケーブル モデムへ提供します。
- 認識されていない MAC アドレスへ IP アドレスの提供を拒否します。

これらのオプションを実行するには、次の CNR の構成項目を実装する必要があります。

- 2 つの範囲選択タグを作成します。1 つは PC 用、もう 1 つはケーブル モデム用です。
- 2 つのクライアント クラスを作成します。1 つは PC 用、もう 1 つはケーブル モデム用です。
- ケーブル モデム デバイスに適したリース ポリシーを作成します。
- PC デバイスに適したリース ポリシーを作成します。
- クラス A net-24（ルーティング可能）アドレスが含まれる範囲を作成します。
- クラス A net-10（ルーティング不可能）アドレスが含まれる範囲を作成します。
- net-24 アドレスが含まれる範囲をプライマリ範囲として識別し、net-10 アドレスが含まれる別の範囲を net-24 範囲に対するセカンダリとして構成します。

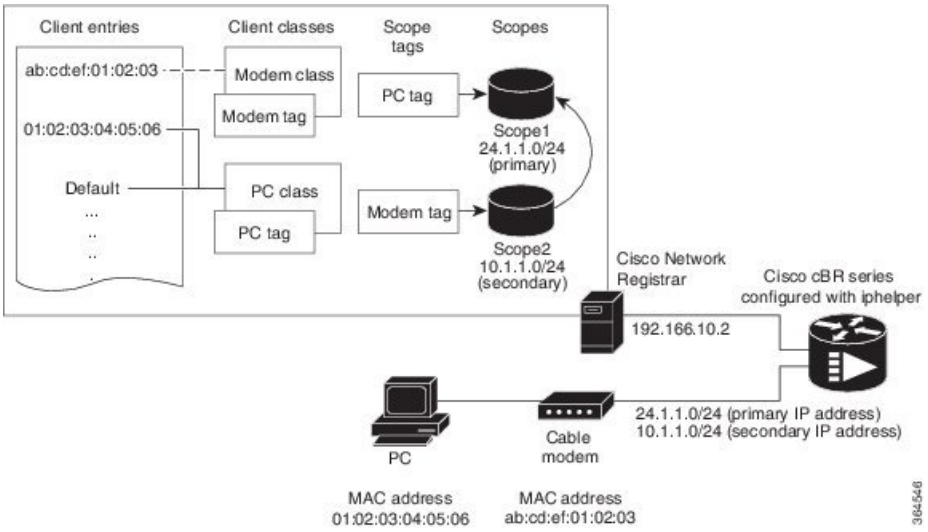
（注） Cisco cBR-8 ルータのアップストリーム ポートは、net-24 ネットワーク上のプライマリ ネットワーク アドレスで構成する必要があります（24.1.1.1 など）。

- 適切な範囲にポリシーを割り当てます。
- ケーブル モデムと PC の MAC アドレスをクライアント エントリ リストに追加します。
- ルーティング可能なアドレスを含む範囲と PC タグを関連付けます。

- ルーティング不可能なアドレスを含む範囲とケーブル モデム タグを関連付けます。
- ケーブル モデム クライアント クラスとケーブル モデム タグを関連付けます。
- PC クライアント クラスと PC タグを関連付けます。
- PC クラスに PC MAC を割り当てます。
- ケーブル モデム クラスにケーブル モデム MAC を割り当てます。
- クライアント クラス処理を有効にします。

次の図は、HFC ネットワークにおけるテスト CNR 構成を示しています。

図 *30*：*HFC* ネットワークにおけるテスト構成



これらの構成項目とその関連付けは、CNR 管理グラフィカル ユーザ インターフェイス（GUI）またはコマンドライン インターフェイス（CLI）を使用して作成できます。次のサンプル スクリプトは、サンプル サーバの DHCP を構成します。

```
File: cabledemo.rc
Command line: nrcmd -C <cluster> -N <user name> -P <password> -b < cabledemo.rc
-------------------------------------------------------------------------------
scope-selection-tag tag-CM create
scope-selection-tag tag-PC create
client-class create class-CM
client-class class-CM set selection-criteria=tag-CM
client-class create class-PC
client-class class-PC set selection-criteria=tag-PC
policy cmts-cisco create
policy cmts-cisco setleasetime 1800
policy cmts-cisco setoption domain-name-servers 192.168.10.2
policy cmts-cisco setoption routers 10.1.1.1
policy cmts-cisco setoption time-offset  604800
policy cmts-cisco setoption time-servers 192.168.10.20
policy cmts-cisco set packet-siaddr=192.168.10.2
policy cmts-cisco setoption log-servers 192.168.10.2
policy cmts-cisco setoption mcns-security-server 192.168.10.2
policy cmts-cisco set packet-file-name=golden.cfg
policy cmts-cisco set dhcp-reply-options=packet-file-name,packet-siaddr,mcns-security-server
policy pPC create
```

```
policy pPC set server-lease-time 1800
policy pPC setleasetime 1800
policy pPC setoption domain-name-servers 192.168.10.2
policy pPC setoption routers 24.1.1.1
scope S24.1.1.0 create 24.1.1.0 255.255.255.0
scope S24.1.1.0 addrange 24.1.1.5 24.1.1.254
scope S24.1.1.0 set policy=pPC
scope S24.1.1.0 set selection-tags=tag-PC
scope S10.1.1.0 create 10.1.1.0 255.255.255.0
scope S10.1.1.0 addrange 10.1.1.5 10.1.1.254
scope S10.1.1.0 set policy=cmts-cisco
scope S10.1.1.0 set selection-tags=tag-CM
scope S10.1.1.0 set primary-scope=S24.1.1.0
client 01:02:03:04:05:06 create client-class-name=class-PC
client ab:cd:ef:01:02:03 create client-class-name=class-CM
client default create action=exclude
dhcp enable client-class
dhcp enable one-lease-per-client
save
dhcp reload
```

DHCP サーバの設定に加えて、パケット トレースを有効にできます。パケット トレースを有効にすると、サーバは要求と応答の両方を分析してからログに追加します。トレースを有効にすると、パフォーマンスに悪影響が生じ、ログがすぐにロールオーバーします。

パケット トレースを設定するには、次の nrcmd コマンドを使用します。

DHCP set log-settings=incoming-packet-detail,outgoing-packet-detail

ケーブル モデム DHCP 応答フィールド

ブロードバンド ネットワークの各ケーブル インターフェイスには、DHCP 応答で次のフィールドが必要です。

- CM の IP アドレス
- CM のサブネット マスク

（注） ネットワークの経験が少ないケーブル オペレータは、ネットワーク番号に基づく推測を入力し、IP ネットワークの分割方法を示すことができます。

- ケーブル インターフェイス用に意図された、TFTP サーバの DOCSIS コンフィギュレーション ファイルの名前
- ケーブル インターフェイスの協定世界時（UTC）からのタイム オフセット。エラー ログにタイムスタンプを付けるときに、現地時刻を計算するためにケーブルインターフェイスで使用されます
- ケーブル インターフェイスが現在時刻を取得する元になるタイム サーバ アドレス

DOCSIS DHCP のフィールド

DOCSIS DHCP オプションの要件は次のとおりです。

- TFTPブートストラッププロセスで使用される次のサーバのIPアドレス。これはsiaddrフィールドで返されます
- ケーブル インターフェイスが TFTP サーバからダウンロードする DOCSIS コンフィギュレーション ファイル

（注） リレーエージェントを使用する別のネットワーク上にDHCPサーバがある場合は、リレーエージェントが DHCP 応答のゲートウェイ アドレス フィールドを設定する必要があります。

- セキュリティが必要な場合は、セキュリティ サーバの IP アドレスを設定する必要があります

DHCP リレー オプション（DOCSIS オプション 82）

DOCSIS Option82 は、DHCPDISCOVER パケットを修正して、ケーブル インターフェイスと CPE デバイスまたはそれらの背後にある「クライアント」とを区別します。DOCSIS Option82 は次の 2 つのサブオプションで構成されます。

- サブオプション 1、回路 ID：

```
Type 1 (1 byte)
Len 4 (1 byte)
Value (8 bytes)
<bit 31,30,.....................0)
<xYYYYYYYYYYYYYYYYYYYYYYYYYYYYYY>
```

MSB は、接続されたデバイスがケーブル インターフェイスであるかどうかを示します。

x=1 ケーブル モデム REQ

x=0 CPE デバイス（サブオプション 2 に示すケーブル インターフェイスの MAC アドレスが設定されたケーブル インターフェイスの背後）

残りのビットは、CMTS インターフェイスに対する SNMP インデックスを構成します。

Y=0xYYYYYYY は、CMTS インターフェイスに対する SNMP インデックスです。

- サブオプション 2、ケーブル インターフェイスの MAC アドレス：

```
Type 2 (1 byte)
Len 6 (1 byte)
Value xxxx.xxxx.xxxx (6 bytes)
```

スクリプトの概要

ここでは、ケーブル インターフェイス設定に適用できるスクリプトを示します。

双方向ケーブル モデムのスクリプト

加入者サイトでの双方向設定をサポートするには、次のスクリプトを使用します。

- **Relay.tcl**
- **SetRouter.tcl**

Telco リターン ケーブル モデムのスクリプト

同じケーブル インターフェイス カードまたはシャーシ上の Telco リターンおよび双方向ケーブル インターフェイス設定をサポートするには、次のスクリプトを使用します。

- **PostClientLookup.tcl**
- **PrePacketEncode.tcl**

スクリプトの配置

Windows NT の場合

Windows NT 上で稼働している CNR の場合は、適切なスクリプトを次のディレクトリに置いてください。

```
\program files\network registrar\extensions\dhcp\scripts\tcl
```

Solaris

Solaris 上で稼働している CNR の場合は、適切なスクリプトを次のディレクトリに置いてください。

```
/opt/nwreg2/extensions/dhcp/scripts/tcl
```

Cisco Network Registrar でのスクリプトの有効化

適切なディレクトリにスクリプトを配置したら、このスクリプトを次のように有効化します。

手順

ステップ 1 テキスト エディタを開きます。

ステップ 2 nrcmd> コマンド プロンプトでスクリプトの 1 つを開きます。

ステップ 3 拡張ポイントを作成し、このポイントをシステムに追加します。

（注） 最も簡単な方法は、スクリプトからコマンド ラインを切り取り、nrcmd> コマンド ラインに貼り付けるだけです。

ステップ 4 拡張ポイントを作成して追加したら、dhcp をリロードします。
スクリプトが有効化されます。

スクリプトを使用するための Cisco CMTS ルータの設定

各ケーブル インターフェイスは、BOOTP フォワーダとして設定し、リレー オプションを有効にする必要があります。各ケーブル インターフェイスのプライマリおよびセカンダリ IP アドレスは、CNR ツールと同期する必要があります。

システムでスクリプトと正しく通信するために、Cisco CMTS ルータで次のコマンドを使用します。

- オプション 82 を有効にするには、**ipdhcprelayinfooption** コマンドを使用します。
- 転送される BOOTREPLY メッセージ内の DHPC リレー エージェント情報の検証を無効にするには、**noipdhcprelayinformationoptioncheck** コマンドを使用します。

（注） パケットが DHCP サーバに転送される前にリレー IP アドレスを提供するために、ケーブル インターフェイス コンフィギュレーション モードで cable dhcp giaddr コマンドを使用して DHCPDISCOVER および DHCPREQUEST パケットの GIADDR フィールドを変更できます。このコマンドを使用して、プライマリ アドレスが CM に使用され、セカンダリ アドレスが CM の背後にあるホストに使用されるように「policy」オプションを設定します。

システム デフォルト ポリシーの構成

以下のためにシステム デフォルト ポリシーにこれらのオプションを追加します。

- ケーブル モデムがネットワークでサポートされるようにするため
- PC がネットワークの各ケーブル インターフェイスの背後でサポートされるようにするため

ケーブル モデム

CNR ツール ドキュメントに従ってこれらの設定を定義します。

- BOOTP を使用するケーブル インターフェイスの TFTP サーバ（IP アドレス）
- タイム サーバ（IP アドレス）
- タイム オフセット（16 進数値、東部標準時間の場合は 1440）

- packet-siaddr（CNR の IP アドレス）
- ルータ（0.0.0.0 に設定）
- boot-file（BOOTP を使用するケーブル インターフェイスの .cm ファイル名）
- packet-file-name（.cm ファイル名）

PC

CNR ツール ドキュメントに従ってこれらの設定を定義します。

- ドメイン名
- ネーム サーバ（DNS サーバの IP アドレス）

選択タグのスコープの作成

全般

範囲選択タグを作成する場合：

手順

ステップ 1 範囲選択タグ作成コマンドをスクリプトから切り取り、nrcmd> コマンドラインに貼り付けます。
（注） この名前は、スクリプトに記載された名前と完全に一致する必要があります。

ステップ 2 次に選択タグを適切なスクリプトに追加します。
例：

```
CM_Scope tagCablemodem
PC_Scope tagComputer
```

Cisco cBR-8 ルータの Telco リターン

はじめる前に

（注） telco リターンで prepacketencode および postclientlookup .tcl スクリプトを使用する場合、telco リターン範囲には、この範囲に関連する選択タグが含まれます。

手順

ステップ 1 Telcocablemodem をプライマリ ケーブル インターフェイス範囲に配置し、その代わりにプールからアドレスを取得します。

ステップ 2 上記と同じ手順を実行しますが、telco 固有のコマンドが設定された別の .cm ファイルを含む telco リターン ポリシーを使用します。

ネットワーク範囲の作成

次に、ネットワークの範囲を作成する例を示します。この例では、2 つの場所に 2 台の Cisco cBR-8 コンバージド ブロードバンド ルータがあり、1 台の Cisco cBR-8 上に Telco リターン用のケーブル インターフェイス カードが 1 つ構成されています。

```
cm-toledo1_2-0 10.2.0.0 255.255.0.0 assignable 10.2.0.10-10.2.254.254 tagCablemodem
tagTelcomodem Default GW=10.2.0.1 (assigned by scripts)
cm-toledo1_3-0 10.3.0.0 255.255.0.0 assignable 10.3.0.10-10.3.254.254 tagCablemodem
tagTelcomodem Default GW=10.3.0.1 (assigned by scripts)
pc-toledo1_2-0 208.16.182.0 255.255.255.248 assignable 208.16.182.2-208.16.182.6 tagComputer
 Default GW=208.16.182.1 (assigned by scripts)
pc-toledo1_3-0 208.16.182.8 255.255.255.248 assignable 208.16.182.10-208.16.182.14 tagComputer
 Default GW=208.16.182.9 (assigned by scripts)
telco_return_2-0 192.168.1.0 255.255.255.0 (No assignable addresses, tag was put on cable
modem primary scope to force telco-return cable modem to pull address from primary scope)
cm-arlington1_2-0 10.4.0.0 255.255.0.0 assignable 10.4.0.10-10.4.254.254 tagCablemodem
Default GW=10.4.0.1 (assigned by scripts)
cm-arlington1_3-0 10.5.0.0 255.255.0.0 assignable 10.5.0.10-10.5.254.254 tagCablemodem
Default GW=10.5.0.1 (assigned by scripts)
pc-arlington1_2-0 208.16.182.16 255.255.255.248 assignable 208.16.182.17-208.16.182.22
tagComputer Default GW=208.16.182.17 (assigned by scripts)
pc-toledo1_3-0 208.16.182.24 255.255.255.248 assignable 208.16.182.2-208.16.182.30 tagComputer
 Default GW=208.16.182.25 (assigned by scripts)
```

（注） .248 サブネット範囲で最後の有効なアドレスがブロードキャスト アドレスであることに注意してください。このアドレスは使用しないでください。

サービス クラスのポリシーまたはケーブル モデムの Cisco IOS イメージのアップグレードのためのポリシーの作成

サービス クラス（CoS）をサポートするには、次を定義します。

- 範囲選択タグ：範囲設定タイプを定義する ID

（注） これは Option82 で必須です。

- クライアント クラス：クライアント グループに関連付けられているクラス

（注） 範囲選択タグは、クライアント クラスから除外またはクライアント クラスに追加されます。

- クライアント：特定の DHCP クライアントと、そのクライアントが属する定義済みクラス

CoS を割り当てたり、Option82 を使用したりするには、MAC アドレスを使用してクライアント エントリを作成し、適切なポリシーを指定します。クライアントベースの MAC プロビジョニングを使用するには、クライアント エントリ「default - exclude」を追加し、クライアント タブですべてのデバイス（たとえば、ケーブル インターフェイスと PC）の MAC アドレスを入力して、適切なタグなど、使用するポリシーを選択します。

サブインターフェイスをサポートする CNR 手順

サブインターフェイスを設定している場合は、CNR の設定方法が異なります。次に例を示します。Cisco cBR-8 ルータで 2 つの ISP サブインターフェイスと 1 つの管理サブインターフェイスを設定している場合は、この管理サブインターフェイスが設定する最初のサブインターフェイスであることを確認します。ケーブル インターフェイス 3（c3/0/0）を使用している場合、3 つのサブインターフェイスとして、c3/0/0.1、c3/0/0.2、および c3/0/0.3 を作成し、最初のサブインターフェイスである c3/0/0.1 を管理インターフェイスとして設定します。

（注） Cisco cBR-8 ルータには、初回の初期化時に CM から DHCP パケットをルーティングするために管理インターフェイスが必要です。それは、CNR から DHCP 応答メッセージをグリーニングして IP アドレスが割り当てられるまで、Cisco cBR-8 ルータの属するサブインターフェイスが分からないためです。

CNR でそのような設定を行うには、次の手順を実行してください。

手順

ステップ 1 2 つのスコープ選択タグ isp1-cm-tag と isp2-cm-tag を作成します。

ステップ 2 たとえば、mgmt-scope、isp1-cm-scope、isp2-cm-scope のように 3 つのスコープを設定し、isp1-cm-scope と isp2-cm-scope のそれぞれでプライマリ スコープに設定する mgmt-scope を定義します。

ステップ 3 また、isp1-pc-scope と isp2-pc-scope の 2 つのスコープを各 ISP の PC にも設定します。スコープ isp1-cm-scope の場合、isp1-cm-tag をスコープ選択タグに設定します。スコープ isp2-cm-scope の場合、isp2-cm-tag をスコープ選択タグに設定します。

ステップ 4 isp1-client-class と isp2-client-class などの 2 つのクライアント クラスを設定します。

ステップ 5 ISP1 に属する CM の MAC アドレスを持つクライアント エントリを作成し、そのエントリを isp1-client-class に割り当てます。また、スコープ選択タグ isp1-cm-tag も割り当てます。

ステップ 6 ISP2 に属する CM のクライアント クラスを作成し、そのクラスを isp2-client-class に割り当てます。また、スコープ選択タグ isp2-cm-tag も割り当てます。

ステップ 7 scope-selection-tag ウィンドウでクライアント クラス処理を有効にします。
ソフトウェアは DHCP 応答が実際に属するサブインターフェイスを見つけるために DHCP 応答をグリーニングするため、これらのサブインターフェイスで重複するアドレス範囲を設定することはできません。CNR では重複するアドレス範囲スコープを設定できますが、CNR を使用してこれらのスコープからアドレスを割り当てることはできません。

その他の参考資料

次に、Cisco CMTS ルータを使用する場合の Cisco Network Registrar に関連する資料を紹介します。

シスコのテクニカル サポート

説明	リンク
Technical Assistance Center（TAC）ホーム ページ：多数の技術関連の記事と、製品、テクノロジー、ソリューション、テクニカル ティップス、ツールへのリンクを提供する Web サイトです。必要な記事は検索して見つけることができます。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/cisco/web/support/index.html

第 IX 部

PacketCable および PacketCable Multimedia の構成

第 72 章

PacketCable と PacketCable Multimedia

このマニュアルでは、既存の DOCSIS（1.1 以降）ネットワーク上での PacketCable および PacketCable Multimedia 運用のための Cisco CMTS の設定方法について説明します。

機能情報の確認

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *177* : ***Cisco cBR*** シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

PacketCable 運用の制限事項

- 音声コールのパケット ドロップを防ぐには、Cisco CMTS でデフォルトのトークン バケット設定（**cabledownstreamrate-limittoken-bucketshaping**）を使用する必要があります。**shaping** オプションが使用されない場合（**cabledownstreamrate-limittoken-bucket**）、パケット ドロップが確実に発生します。
- 組み込み型マルチメディア ターミナル アダプタ（E-MTA）クライアントのみサポートします。スタンドアロン MTA（S-MTA）クライアントはサポートされません。
- PacketCable 運用は HCCP N+1 冗長性と同時に設定できますが、PacketCable のステートは現用インターフェイスと保護インターフェイス間で同期化されません。スイッチオーバーが発生した場合、既存の音声発信は続行されますが、ユーザが電話を切ると、保護インターフェ

イスは以前の発信状態を認識しないため、PacketCable イベント メッセージは生成されません。ただし、新規の音声コールは通常の方法で作成および処理されます。

- PacketCable の音声コールをサポートするアップストリームや、非送信請求許可サービス（UGS）またはアクティビティ検出による UGS（UGS-AD）を使用するアップストリームでは、200,000 Hz のチャネル幅は使用できません。音声および他の UGS/UGS-AD サービス フローでこのような狭いチャネル幅を使用すると、「DSA MULTIPLE ERRORS」が原因でコールが拒否されます。

PacketCable 運用の情報

ここでは、PacketCable の運用、PacketCable ネットワークのコンポーネント、および DOCSIS ケーブル ネットワークの他のコンポーネントとの連携に関する概要とその他の情報について説明します。

機能の概要

PacketCable は Cablelabs とその関連ベンダーが提供するプログラム イニシアチブであり、光同軸ハイブリッド（HFC）ケーブル ネットワーク上でパケット ベースのリアルタイム ビデオおよびその他のマルチメディア トラフィックを提供する標準的な方法を確立します。PacketCable 仕様は Data-over-Cable System Service Interface Specifications（DOCSIS）1.1 に基づき構築されていますが、インターネットや公衆電話交換網（PSTN）などの非ケーブル ネットワーク上で使用するためにその他のプロトコルで DOCSIS プロトコルを拡張しています。

これにより PacketCable は、ケーブル ネットワークで発着信されるトラフィックのためのエンドツーエンドのソリューションになっており、異なるネットワークとメディア タイプで構成されるインフラストラクチャ上でマルチメディア サービスを提供するタスクを簡略化します。また、エンドツーエンドのコール シグナリング、プロビジョニング、Quality of Service（QoS）、セキュリティ、請求、およびネットワークの管理の統合アプローチも提供します。

Emergency 911 機能

PacketCable Emergency 911 ケーブル インターフェイス ラインカードの優先順位付け

PacketCable Emergency 911 ケーブル インターフェイス ラインカードの優先順位付け機能により、HCCP スイッチオーバー イベントの場合でも、Emergency 911 コールをサポートするケーブル インターフェイス ラインカードを、非緊急音声コールをサポートするケーブル インターフェイス ラインカードよりも自動的に優先させることができます。このような場合、現用 HCCP ケーブル インターフェイス ラインカードが停止すると、保護 HCCP ラインカード インターフェイスは Emergency 911 音声コールへのサービスを自動的に優先させます。この機能はデフォルトでイネーブルになっており、手動でディセーブルに設定することはできません。

（注） Emergency 911 ケーブル インターフェイス ラインカードの優先順位付けは、PacketCable 音声コールにのみ適用されます。

HCCP スイッチオーバー イベント中、ケーブル モデムは次の順序で復旧します。

1. Emergency 911 音声トラフィックをサポートするケーブル モデム
2. 非緊急音声トラフィックをサポートするケーブル モデム
3. サービスが停止する T4 タイムアウト イベントに近づいているケーブル モデム
4. 残りのケーブル モデム

Emergency 911 音声イベントおよびケーブル インターフェイス ラインカードの優先順位付けについての情報を表示するには、特権 EXEC モードで show cable calls コマンドおよび show hccp event-history コマンドを使用します。

PacketCable Emergency 911 のサービス リストおよび履歴

Cisco CMTS ルータでの PacketCable Emergency 911 コールへの拡張情報サポートには、次の情報および関連する履歴が含まれています。

- アクティブな Emergency 911 コール
- 最近の緊急 911 コール
- 通常の音声コール
- 最近の Emergency 911 コールのあとに行われた音声コール

この機能は、次のコンフィギュレーションおよびshowコマンドによりイネーブル化およびサポートされます。

- cable high-priority-call-window
- **showcablecalls**
- **showcablemodem calls**

Cisco CMTS ルータが Emergency 911 コールの記録を保持するコール ウィンドウ（分）を設定するには、グローバル コンフィギュレーション モードで cable high-priority-call-window コマンドを使用します。Cisco CMTS ルータから通話ウィンドウ設定を削除するには、このコマンドの **no** 形式を使用します。

PacketCable ネットワーク コンポーネント

PacketCable ネットワークには複数のコンポーネントが含まれます。一部のコンポーネントは DOCSIS 1.1 ネットワークに存在するコンポーネントと同じですが、他のコンポーネントは新規のもので、PacketCable ネットワークがコールを確立する必要があるエンドツーエンドのインフラストラクチャを構築します。PacketCable のコンポーネントおよびプロトコルは、実装および相互運

用性を容易にするために、可能な限り既存のプロトコルやインフラストラクチャ上に構築されています。

- ケーブル モデム：DOCSIS 1.0 または DOCSIS 1.1 ケーブル ネットワークに接続する顧客宅内機器（CPE）。DOCSIS のケーブル モデムはすべて、インターネットへの高速データ接続を提供しますが、他のケーブル モデムは電話接続などの機能を提供できます。
- ケーブル モデム終端システム（CMTS）：DOCSIS ケーブル ネットワークを IP バックボーン ネットワークに接続するヘッドエンドベースのルータ。CMTS は DOCSIS 1.1 の MAC レイヤを制御し、ケーブル オペレータが加入者に対して保証するサービス品質（QoS）の制限を強化します。標準的な CMTS では、数百 ～ 数千のケーブル モデムが使用できます。

（注） ケーブル モデムおよび CMTS の動作については、DOCSIS 1.1 仕様書を参照してください。

- マルチメディア ターミナル アダプタ（MTA）：電話および他のエンド ユーザ デバイスを PacketCable ネットワークに接続する CPE デバイス。PacketCable 仕様では、2 つの MTA タイプ（組み込み型 MTA（E-MTA）およびスタンドアロン MTA（S-MTA））が定義されています。E-MTA は DOCSIS 1.1 ケーブル モデムに統合された MTA です。S-MTA は単独の MTA で、DOCSIS 1.1 ケーブル モデムをケーブル ネットワークに接続する必要があります。
- コール管理サーバ（CMS）：中心部に配置されるサーバで、MTA がネットワーク上でコールを確立できるようにシグナリング機能を提供します。CMS はネットワーク ベースのコール シグナリング（NCS）プロトコルを使用して、認証、許可、コール ルーティング、および 3 ウェイ コーリングなどの特殊な機能のサポートを可能にします。PacketCable ネットワークは、ネットワークの規模と複雑さに応じて、複数の CMS サーバを含むことができます。

（注） CMS は Common Open Policy Service（COPS）プロトコルの上部に複数のプロトコルを実装して、PacketCable ネットワークの他の部分と通信します。

- ゲート コントローラ（GC）：PacketCable ネットワーク内でゲートの確立を制御するサーバ。ゲートとは、CMTS 内の論理的なエンティティです。サービス フローが要求している QoS 機能に対して許可されるようにします。個別のゲートがサービス フローのアップストリームおよびダウンストリームの方向性を制御します。コールが確立すると、GC は CMTS にそれぞれのゲートを作成するように指示し、各ゲートに一連の許可パラメータを提供します。各ゲートは CMTS が MTA がコールに対して作成している QoS 要求を許可するために使用します。また、GC はコールが許可および確立されるようにコールの両端に 2 組のゲートを作成する調整役でもあります。

（注） PacketCable ネットワークには複数の GC を含めることができますが、一時に特定のコールを制御するサーバは 1 つだけです。通常、同一のワークステーションが CMS と GC サーバの両方を兼ねます。

- 記録保持サーバ（RKS）：各コールの生成時にその情報を収集する課金サーバ。RKS は Remote Authentication Dial-In User Service（RADIUS）プロトコルを使用して、CMTS および他の PacketCable サーバから課金データを収集します。RKS は各コールのコール データ レコード（CDR）を作成し、その後の処理のためにサービス プロバイダーのデータ処理センターの適切なアプリケーション サーバにその情報を転送します。

DQoS（Dynamic Quality of Service）

PacketCable ネットワークの主要機能とは、DOCSIS 1.1 で提供される動的サービスに似ている Dynamic Quality of Service（DQoS）機能です。ただし、DOCSIS 1.1 DQoS は、ケーブル ネットワーク内でのみサービスを承認およびプロビジョニングし、ネットワーク全体でエンドポイント間でコールを伝達するために必要なリソースを確保しません。

PacketCable DQoS はネットワーク全体で DOCSIS 1.1 サービスを拡張し、リソースをエンドポイント間で動的に承認およびプロビジョニングできるようにします。これにより、サービス不正使用攻撃の可能性を防ぎ、使用が承認されているサービスを顧客に保証します。

（注） PacketCable 1.0 では、E-MTA クライアント用にケーブル ネットワーク内のリソース予約で DOCSIS 1.1 が使用される必要があります。

二段階式リソース予約プロセス

PacketCable の DQoS モデルは二段階式のリソース予約プロセスを使用しており、リソースは最初に予約され、その後コミットされます。これにより、双方向での予約プロセスが可能になり、実際に電話をかける前に接続の両方のエンドポイントでリソースを使用することが保証されます。

MTA がコール要求を行うと、ローカル CMTS はゲート コントローラと通信して、コールのリソースを許可します。リソースが許可されると、CMTS はローカルのリソースを予約し、一方、リモート エンドで必要なリソースに関してリモート エンドとネゴシエートします。

（注） CMTS は DOCSIS 1.1 動的サービス追加（DSA）メッセージを使用してリソースを予約し、次に動的サービス変更（DSC）メッセージを使用してリソースにコミットします。

必要なリソースがすべて使用できるようになると、ローカル CMTS およびリモート CMTS はリソースにコミットし、トラフィックを流します。使用量のアカウンティングおよび課金は、リモート MTA により検出されてコールが実際に進行するまで開始されません。

DQoS モデルでは、コールの両方のエンドポイント、さらにバックボーン ネットワークで同じ帯域幅が予約され、帯域幅はコールの進行中にのみ予約されます。コールが終了すると、ネットワークのすべての部分がコールのリソースを解放し、他のユーザがそれを使用できるようになります。

DQoS を使用したコールの作成

DOCSIS 1.1 ネットワークはサービス フローを使用してさまざまな QoS ポリシーを実行しますが、サービス フローはケーブル ネットワークの内側だけに存在します。サービス フローを制御してネットワーク全体に広げるために、PacketCable ネットワークは「ゲート」を作成し、維持します。

ゲートは接続の両側の CMTS 上で作成される論理エンティティで、特定の DQoS トラフィック フローの許可と確立を行います。CMTS はゲート コントローラと通信して、接続の両側でマッチング ゲートの作成を行います。

ゲートは単一方向なので、ダウンストリームとアップストリームのトラフィック フローには別のゲートが必要です。ただし、1 つのコールのダウンストリーム ゲートとアップストリーム ゲートには、通常、同じゲート ID が使用されます。各 CMTS はそれぞれ固有のゲート セットを保持するので、双方向のトラフィック フローではゲートを 4 つ（ローカル CMTS とリモート CMTS にそれぞれ 2 つ）作成する必要があります。

標準的なコールの場合、ゲートは次の各段階を経て、DQoS トラフィック フローが作成されます。

1. ローカル MTA がコール要求を作成し、ゲート コントローラは CMTS に Gate-Allocation コマンドを送信します。これに応じてゲートが作成され、Allocated ステートになります。
2. コール管理サーバ（ゲート コントローラと同一サーバの場合あり）はコールの要求を分析して、宛先の電話番号を適切な宛先ゲートウェイに変換します。
3. ゲート コントローラはコールを要求する MTA が必要なリソースに対して許可されていることを確認し、Gate-Set コマンドを CMTS に送信し、ゲートを Authorized ステートにします。
4. 接続の両側の CMTS はコールに必要なローカル リソースを予約し、ゲートを Reserved ステートにします。
5. リモート CMTS およびローカル CMTS はゲート調整を行うと、それぞれのゲートが Local_Committed ステートおよび Remote_Committed ステートになります。
6. 両側が必要なリソースをすべて予約すると、各 CMTS はそのゲートを Committed ステートにして、トラフィックを流します。

DQoSLite ベースの IPv6 音声サポート

DQoSLite は、IPv4 アドレス空間を回収するために、ゲートの概念を使わずに IPv6 で個人用音声サービスを検証して提供するモデム中心型ソリューションです。CMTS は、リソースの予約と認証には参加しません。

DQoSLite は PacketCable 2.0 の要素を利用します。SIP に基づく、PacketCable 2.0 と同様のプロビジョン メカニズムを使用する DQoSLite を、ISP 用の IP Multimedia Subsystem（IMS）インフラストラクチャに統合することができます。

この新しい DQoSLite インフラストラクチャに IPv6 音声ソリューションを導入する主な要因は次のとおりです。

- SIP または IMS に基づいています。
- 広範なマルチメディア サービスをサポートします。

• IPv4 アドレス空間の一部を回収できます。

この機能は、次のコンフィギュレーションおよびshowコマンドによりイネーブル化およびサポートされます。

- **packetcale authorize vanilla-docsis-mta**
- **show cable modem**{*ip-address*|*mac-address*}**qos**
- **show cable modem**{*ip-address*|*mac-address*}**service-flow**
- **show interface cable** *slot*/*subslot*/*cable-interface-index* **sid** *sid*
- **showinterface cable** *slot*/*subslot*/*cable-interface-index* **service-flow** *sfid*

動的サービス トランザクション ID サポート

DOCSIS 2.0 はトランザクション間で一意のトランザクション ID（TAID）が必須です。TAID は一意で、増加しない必要があります。TAID は送信者によって割り当てられます。TAID タイムアウトは、送信者と受信者の間で一致しないことがあります。これは TAID の一意性に影響します。

TAID は送信者がトランザクションを完了したら再利用できます。同様に、DOCSIS では受信者が SFID なしでも TAID でトランザクションを特定できます。これら 2 つの要件が組み合わさると、DSD トランザクションと DSA/DSC 割り込みトランザクションで問題が発生します。

相互運用性の問題を解決するために、TAIDの一意性が保証される必要があります。これは、同じ TAID を再利用するために CMTS を T10 まで待機させることで行われます。この要件を満たすために、新しい TAID 割り当てアルゴリズムが使用されます。

既存の 16 ビット カウンタを置き換えるために TAID プールを作成します。この TAID プールは、TAIDの有効期限を追跡するためにタイマーによってモニタされます。可用性を示すために、プール内の各 TAID にフラグが割り当てられます。新しい TAID が要求されると、動的サービス プロセスは TAID の可用性をチェックします。TAID が使用可能な場合は、新しいサービス フローに割り当てられますが、それ以外の場合は要求が拒否されます。

TAID が割り当てられると、タイマーが有効期限 T10 で開始し、TAID の非可用性を示すために TAID フラグが false に設定されます。動的サービス プロセスはタイマーを追跡します。この時間が期限切れになると、タイマーが停止し、TAID の可用性を示すためにフラグが TRUE に設定されます。

TAID プールはプロセスの初期化時に割り当てられ、初期化されます。TAID に関連付けられたすべてのタイマーは、リーフ タイマーとしてプロセスの親タイマーに追加されます。

PacketCable サブスクライバ ID のサポート

PacketCable サブスクライバ ID 機能は、すべてのゲート コントロール メッセージにサブスクライバ ID を追加して、Cisco CMTS ルータから返されるエラー コードを強化します。

以前は、ゲート ID が個々の CMTS システムに一意にあるのみで、CMS の代わりに CMTS 接続を管理する中央デバイスによって、CMS のすべてのゲート コントロール メッセージの処理がプロキシされていました。CMS は単一の Common Open Policy Service（COPS）でプロキシ デバイスに

関連付けられていました。したがって、複数の CMTS システムを使用している場合、ゲート ID が重複する可能性がありました。

各ゲート コントロール メッセージにサブスクライバ ID が追加されて、CMS とプロキシデバイス間のゲート ID のあいまいさが解消されています。サブスクライバ ID パラメータは、次の COPS メッセージに追加されています。

- GATE-INFO
- GATE-DELETE
- GATE-OPEN
- GATE-CLOSE

サブスクライバ ID は CMS で取得され、Gate-Set メッセージで使用されます。また、CMTS またはそのプロキシから返されるエラー コードは、ゲート動作障害に関するより具体的な情報を含むように強化されています。

この機能を有効にするには、グローバル コンフィギュレーション モードで **packetcablegatesend-subscriberID** コマンドを使用します。

利点

PacketCable 機能は、サービス プロバイダーとそのカスタマーに次の利点を提供します。

ケーブル ネットワーク上の統合サービス

PacketCable を使用すると、ケーブル オペレータは、ネットワーク全体で、データ接続に加えて、マルチメディアのリアルタイム サービスを提供できます。これらのサービスには、ライフラインをサポートする基本的なテレフォニー、および競争力の高い拡張コーリング サービスを提供するテレフォニーが含まれます。オペレータは、既存のネットワーク インフラストラクチャを広く活用しながら、新しいサービスを導入できます。

現在のデータ ネットワークの標準的な伝送メカニズムとして IP は普及しています。このため、マルチメディア電子メール、リアルタイム チャット、ストリーミング メディア、（音楽やビデオなど）、ビデオ会議といった高度なインターネット アプリケーションを数多く実現できます。PacketCable イニシアチブは、ケーブル オペレータ向けにネットワーク アーキテクチャを提供することで、これらのサービスを迅速かつ経済的に実現します。

標準化されたプロビジョニング

PacketCable の仕様では均一でオープン、かつ相互運用可能なネットワークを定義できるため、PacketCable は個々の加入者に IP サービスをプロビジョニングする標準化された効率的な方法を提供します。ケーブル オペレータには、標準化されたプロビジョニングおよびそれに関連する導入コストの低下が保証されます。

相互運用性

顧客宅内機器（CPE）デバイスは、ケーブル設備の VoIP ソリューション導入における設備投資の大部分を占めています。PacketCable の仕様では、ベンダーはケーブル オペレータが導入を計画し

ている音声とその他のサービスをサポートするMTAクライアントを構築できます。これらのCPEデバイスは既存の DOCSIS 準拠ケーブル モデムに基づくため、開発の時間とコストは最小限に抑えられます。

仕様に対して各種の標準規格に準拠したアプローチを取るため、PacketCable ネットワークのその他のコンポーネントとの相互運用性も保証されます。どの PacketCable 認定コンポーネントも、PacketCable の標準に準拠したネットワーク内で相互運用できます。

セキュアなアーキテクチャ

PacketCable は DOCSIS 1.1 で利用できるセキュリティ機能を基に構築されているため、一般的なサービス不正使用攻撃を防止する高いセキュリティ標準によって、ケーブル オペレータはエンドツーエンドでセキュアなネットワークが保証されます。包括的で各種の標準規格に準拠した PacketCableの仕様は、公衆電話交換網（PSTN）と同程度にセキュアなネットワークを構築するように設計されています。

CALEA サポート

PacketCable アーキテクチャは、1994 年の Communications Assistance for Law Enforcement Act（CALEA）に対応するように設計されました。CALEA では、通信キャリアに対して、裁判所が命じた電子的監視を実施する際に法執行機関に協力することを要求しています。PacketCable ネットワークでは、裁判所命令のタイプに応じて、キャリアに提供義務のある 2 種類の情報を提供できます。

- コール識別情報：キャリアは傍受ターゲットとのコールに関するコール識別情報を提供する必要があります。通話では、この情報にターゲットからコールした電話番号やターゲットをコールした電話番号が含まれます。
- コールの内容：キャリアは傍受ターゲットとのコールの内容を提供する必要があります。通話では、このリアルタイム コンテンツは音声による対話です。

PacketCable 運用の設定方法

ここでは、PacketCable 機能を設定するためのタスクについて説明します。オプションと記載されていない限り、各タスクは必須です。

PacketCable 運用の有効化

PacketCable 運用をイネーブルにするには、まずユーザ EXEC モードで次のコマンドを実行します。この手順は必須です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**packetcable** 例： `Router(config)# packetcable`	すべてのケーブル インターフェイスで PacketCable 運用をイネーブルにします。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

PacketCable 運用の無効化

PacketCable 運用をディセーブルにするには、まずユーザ EXEC モードで次のコマンドを実行します。この手順は、Cisco CMTS で PacketCable シグナリングのサポートを止める場合にのみ必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**nopacketcable** 例： `Router(config)# no packetcable`	すべてのケーブル インターフェイスで PacketCable 運用をディセーブルにします。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

PacketCable 運用の設定

PacketCable の運用に影響するさまざまなパラメータを設定するには、ユーザ EXEC モードで次のコマンドを使用します。各パラメータは一般的な PacketCable 運用に適したデフォルト値に設定されているため、これらすべての手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**packetcableelement-id** *n* 例： `Router(config)# packetcable element-id 23`	Cisco CMTS のイベント メッセージ要素 ID を設定します。要素 ID を手動で設定しない場合、PacketCable 運用が有効になると、CMTS は、0 ～ 99,999 の範囲のランダムな値をデフォルト値に設定します。
ステップ 4	**packetcablegatemaxcount** *n* 例： `Router(config)# packetcable gate maxcount 524288`	Cisco CMTS のゲート データベースに割り当てるゲート ID の最大数を設定します。

	コマンドまたはアクション	目的
ステップ 5	**packetcabletimerT0** *timer-value* 例： `Router(config)# packetcable timer T0 40000`	T0 タイマーをミリ秒で設定します。
ステップ 6	**packetcabletimerT1** *timer-value* 例： `Router(config)# packetcable timer T1 300000`	T1 タイマーをミリ秒で設定します。
ステップ 7	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

PacketCable と PacketCable 以外の UGS サービス フローの有効化

デフォルトでは、**packetcable** コマンドを使って PacketCable の運用を有効にすると、非送信請求許可サービス（UGS）サービス フローを要求するときにケーブル モデムが PacketCable プロトコルに従う必要があります。これにより、PacketCable の運用をサポートしない DOCSIS ケーブル モデムが、DOCSIS スタイル UGS サービス フローを使用できなくなります。

PacketCable および PacketCable 以外の両方の DOCSIS CM が混在するネットワークがある場合、両方のタイプの UGS サービス フローを有効にするには、**packetcableauthorizevanilla-docsis-mta** コマンドを使用できます。これはオプションの手順です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**packetcable** 例： `Router(config)# packetcable`	PacketCable の運用をイネーブルにします。
ステップ 4	**packetcableauthorizevanilla-docsis-mta** 例： `Router(config)# packetcable authorize vanilla-docsis-mta`	DOCSIS スタイル UGS サービス フロー要求を使用できるようにします。
ステップ 5	**cable dsx authorization** 例： `Router(config)# cable dsx authorization`	DSX 認証を有効にします。
ステップ 6	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

次の作業

ヒント　PacketCable 以外の UGS サービス フローが有効になっているかどうかを表示するには、**showpacketcableglobal** コマンドを使用します。

PacketCable サブスクライバ ID サポートの有効化

GATE-OPEN と GATE-CLOSE ゲート コントロール メッセージにサブスクライバ ID を追加するには、グローバル コンフィギュレーション モードで **packetcablegatesend-subscriberID** コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**packetcable** 例： `Router(config)# packetcable`	PacketCable の運用をイネーブルにします。
ステップ 4	**packetcablegatesend-subscribeID** 例： `Router(config)# packetcable gate send-subscriberID`	ゲート コントロールのサブスクライバ ID 情報を使用できるようにします。
ステップ 5	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

RKS サーバ用の RADIUS アカウントの設定

RADIUS プロトコルを使用して Cisco CMTS ルータと記録保持サーバ（RKS サーバ）との通信をイネーブルにするには、次のコマンドを使用します。この手順は必須です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**aaanew-model** 例： `Router(config)# aaa new-model`	認証、許可、アカウンティング（AAA）アクセスコントロールモデルをイネーブルにします。
ステップ 4	**aaagroupserverradius** *group-name* 例： `Router(config)# aaa group server radius packetcable`	認証用に RADIUS サーバのグループを作成し、RADIUS グループ コンフィギュレーション モードを開始します。*group-name* は固有の値で、このグループを識別する任意の文字列です。
ステップ 5	**server** {*hostname* | *ip-address*} [**auth-port** *udp-port*] [**acct-port** *udp-port*] 例： `Router(config-sg-radius)# server radius-server1`	RKS サービスを提供している RADIUS サーバのホスト名または IP アドレスを指定します。 （注） 複数の RADIUS サーバを開始するには、必要に応じてこのコマンドを繰り返します。Cisco CMTS は、このコマンドで指定した順番にサーバを使用します。
ステップ 6	**exit** 例： `Router(config-sg-radius)# exit`	RADIUS グループ コンフィギュレーション モードを終了します。
ステップ 7	**aaaaccountingnetworkdefaultstart-stopgroupradiusgroup** *group-name* 例： `Router(config)# aaa accounting network default start-stop group radius group packetcable`	前に作成したグループで定義した RADIUS サーバ グループを使用して、AAA サービスをイネーブルにします。*group-name* パラメータは、ステップ 4 で指定したのと同じ名前にする必要があります。
ステップ 8	**radius-serverhost** {*hostname* | *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*] [**timeout** *seconds*] [**retransmit** *retries*] **key0000000000000000** 例： `Router(config)# radius-server host radius-server1 key 0000000000000000`	RADIUS ホストを指定します。*hostname* または *ip-address* には、ステップ 5 で指定したサーバのいずれかと同じ値を使用します。また、ステップ 5 で **auth-port** または **acct-port** の値を指定した場合は、ここでも同じように指定する必要がありま

	コマンドまたはアクション	目的
		す。**key** 値は必須で、次に示すように 16 個の ASCII ゼロを指定する必要があります。 （注） ステップ 5 で入力した各 RADIUS サーバでこのコマンドを繰り返します。
ステップ 9	**radius-servervsasendaccounting** 例： `Router(config)# radius-server vsa send accounting`	アカウンティング関連のベンダー固有属性（VSA）を認識して使用できるように Cisco CMTS を設定します。
ステップ 10	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

次の作業

トラブルシューティングのヒント

PacketCable CMS と Cisco CMTS ルータ間の接続が完全に確立されておらず、PacketCable CMS が TCP FIN メッセージを送ってセッションを正しく終了しない場合は、接続に関する **showcopsserver** コマンドの出力に COPS サーバが示されます。

PacketCable クライアント承認タイムアウト

PacketCable クライアント承認タイムアウト機能は、Cisco CMTS ルータで PacketCable の COPS をサポートします。また、この機能を使用すると、Cisco CMTS ルータでの COPS Telnet 接続のタイムアウト値と COPS Telnet セッションのクリアのタイムアウト値も設定できます。

ネットワークまたは Cisco CMTS ルータ上の Telnet のエラーが原因で、不完全な COPS セッションが作成される場合があります。この問題を解決するために、タイムアウト タイマーは、Cisco CMTS ルータ上の古い COPS Telnet セッションに割り当てられたリソースをクリアしてクリーニングできるようにします。

タイムアウト タイマーは、Cisco CMTS ルータの各 COPS Telnet 接続に適用されます。このタイムアウト設定が期限切れになると、Telnet セッションが終了し、Cisco CMTS ルータのサポート リソースがクリアされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**packetcable timer** {**T0** *timer-value*| **T1** *timer-value* | **multimedia T1** *timer-value*}
	
	例：
	`Router(config)# packetcable timer T0 300000`
	
	例：
	`Router(config)# packetcable timer T1 400000`
	
	例：
	`Router(config)# packetcable timer multimedia T1 400000`
		PacketCable タイマー値を設定します。

ステップ 4	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。

次の作業

トラブルシューティングのヒント

PacketCable CMS と Cisco CMTS ルータ間の接続が完全に確立されておらず、PacketCable CMS が TCP FIN メッセージを送ってセッションを正しく終了しない場合は、接続に関する **showcopsserver** コマンドの出力に COPS サーバが示されます。

PacketCable の設定例

ここでは、PacketCable の設定例を示します。

例：PacketCable の通常設定

ここでは、デフォルト パラメータを使用して、PacketCable の運用に合わせて設定された Cisco CMTS ルータの一般的な設定を示します。この設定を使用するには、ネットワーク内のサーバのアドレスと一致するように、RADIUS と RKS の各サーバの IP アドレスを変更する必要があります。

```
!
version 15.5
no parser cache
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
service internal
service udp-small-servers max-servers no-limit
service tcp-small-servers max-servers no-limit
!
hostname Router
!
no logging rate-limit
aaa new-model
!
!
aaa group server radius a
 server 10.9.62.12 auth-port 1813 acct-port 1812
 server 10.9.62.13 auth-port 1813 acct-port 1812
!
aaa accounting network default start-stop group radius group a
aaa session-id common
enable password <delete>
!
cable modulation-profile 2 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cable modulation-profile 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 short 6 75 6 8 16qam scrambler 152 no-diff 144 shortened uw8
cable modulation-profile 2 long 8 220 0 8 16qam scrambler 152 no-diff 160 shortened uw8
cable modulation-profile 5 request 0 16 2 8 qpsk scrambler 152 no-diff 64 fixed uw16
cable modulation-profile 5 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 5 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 5 short 6 78 7 8 16qam scrambler 152 no-diff 144 shortened uw16
cable modulation-profile 5 long 8 220 0 8 16qam scrambler 152 no-diff 160 shortened uw16
cable qos profile 5 max-burst 1200
cable qos profile 5 max-downstream 2000
cable qos profile 5 max-upstream 128
cable qos profile 5 priority 5
cable qos profile 5 privacy
cable qos profile 7 guaranteed-upstream 87
cable qos profile 7 max-upstream 87
cable qos profile 7 privacy
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable qos permission enforce 5
cable time-server
no cable privacy accept-self-signed-certificate
ip subnet-zero
!
!
no ip domain-lookup
```

```
ip domain-name cisco.com
ip host tftp 10.8.8.8
ip host cnr 10.9.62.17
!
packetcable
packetcable element-id 12456
!
!
!
interface Tunnel0
 ip address 10.55.66.3 255.255.255.0
 load-interval 30
 tunnel source TenGigabitEthernet 4/1/0
 tunnel destination 172.27.184.69
!
interface Tunnel10
 ip address 10.0.1.1 255.255.0.0
!
interface TenGigabitEthernet 4/1/0
 ip address 10.9.60.10 255.255.0.0
 no ip redirects
 no ip mroute-cache
 full-duplex
!
interface TenGigabitEthernet 4/1/0
 ip address 172.22.79.44 255.255.254.0
 no ip redirects
 no ip mroute-cache
 full-duplex
!
interface Cable3/0
 ip address 10.3.1.33 255.255.255.0 secondary
 ip address 10.4.1.1 255.255.255.0 secondary
 ip address 10.4.1.33 255.255.255.0 secondary
 ip address 10.3.1.1 255.255.255.0
 ip helper-address 10.9.62.17
 load-interval 30
 no keepalive
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 55500000
 cable upstream 0 modulation-profile 2
 no cable upstream 0 shutdown
 cable upstream 1 frequency 12000000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
 cable upstream 1 data-backoff automatic
 cable upstream 1 modulation-profile 2
 cable upstream 1 shutdown
 cable upstream 2 frequency 16000000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 3200000
 cable upstream 2 data-backoff automatic
 cable upstream 2 modulation-profile 2
 no cable upstream 2 shutdown
 cable upstream 3 frequency 20000000
 cable upstream 3 power-level 0
 cable upstream 3 channel-width 3200000
 cable upstream 3 data-backoff automatic
 cable upstream 3 modulation-profile 2
 no cable upstream 3 shutdown
 cable upstream 4 frequency 24000000
 cable upstream 4 power-level 0
 cable upstream 4 channel-width 3200000
 cable upstream 4 data-backoff automatic
 no cable upstream 4 shutdown
 cable upstream 5 frequency 28000000
 cable upstream 5 power-level 0
 cable upstream 5 channel-width 3200000
 cable upstream 5 data-backoff automatic
 cable upstream 5 modulation-profile 2
 no cable upstream 5 shutdown
```

```
 cable dhcp-giaddr policy
!
router eigrp 48849
 network 1.0.0.0
 network 10.0.0.0
 auto-summary
 no eigrp log-neighbor-changes
!
ip default-gateway 10.9.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 172.22.78.1
ip route 10.8.0.0 255.255.0.0 10.9.0.1
ip route 192.168.80.0 255.255.255.0 Tunnel0
ip route 192.168.80.0 255.255.255.0 172.27.184.69
ip route 10.255.254.254 255.255.255.255 10.9.0.1
no ip http server
ip pim bidir-enable
!
!
cdp run
!
!
radius-server host 10.9.62.12 auth-port 1813 acct-port 1812 key 0000000000000000
radius-server retransmit 3
radius-server vsa send accounting
!
line con 0
 exec-timeout 0 0
 privilege level 15
line aux 0
line vty 0 4
 session-timeout 33
 exec-timeout 0 0
 password <deleted>
!
ntp clock-period 17179976
ntp server 1.9.35.8
end
```

PacketCable 運用の確認

PacketCable 運用の情報を確認および維持するには、次のコマンドを 1 つ以上使用します。

- **showpacketcableglobal**
- **showpacketcablegate**
- **showpacketcablegateipv6**
- **showpacketcablegatedqos**
- **showpacketcablegatecountercommit**

PacketCable の設定、要素 ID の値、ゲートの最大数、および CMTS ベースのさまざまな DQoS タイマーを確認するには、特権 EXEC モードで **showpacketcableglobal** コマンドを使用します。

```
Router# show packetcable global
Packet Cable Global configuration:
Enabled   : Yes
Element-ID: 12456
Max Gates : 1048576
Allow non-PacketCable UGS
Default Timer value -
  T0      : 30000 msec
  T1      : 300000 msec
```

ゲート データベース内の 1 つまたは複数のゲートに関する情報を確認するには、次の例に示すように **showpacketcablegate** コマンドを使用します。

```
Router# show packetcable gate summary
GateID     i/f          SubscriberID   GC-Addr        State     Type  SFID(us) SFID(ds)
13582      Ca8/1/0      3.18.1.4       20.5.0.254     RECOVERY  Dqos  74
29962      Ca8/1/0      3.18.1.5       20.5.0.254     RECOVERY  Dqos  73
46354      Ca8/1/0      ------         20.5.0.254     RECOVERY  Dqos  72
62738      Ca8/1/0      ------         20.5.0.254     RECOVERY  Dqos           69
Total number of  gates = 4
Total Gates committed(since bootup or clear counter) = 8
```

ゲート データベース内の IPv6 サブスクライバ ID に関連する 1 つまたは複数の PacketCable ゲートの情報を確認するには、次の例に示すように **showpacketcablegateipv6** コマンドを使用します。

```
Router# show packetcable gate ipv6 summary
GateID     i/f                  SubscriberID                State   SFID(us) SFID(ds)
13582      Ca8/1/0      2001:40:1:42:C0B4:84E5:5081:9B5C       COMMIT    74
29962      Ca8/1/0      2001:40:1:42:C0B4:84E5:5081:9B5C       COMMIT    73
46354      Ca8/1/0      2001:40:1:42:C0B4:84E5:5081:9B5C       COMMIT    72
62738      Ca8/1/0      2001:40:1:42:C0B4:84E5:5081:9B5C       COMMIT              69

Total number of  gates = 4
Total Gates committed(since bootup or clear counter) = 8
```

ゲート データベース内の IPv4 サブスクライバ ID に関連する 1 つまたは複数の PacketCable ゲートの情報を確認するには、次の例に示すように **showpacketcablegatedqos** コマンドを使用します。

```
Router# show packetcable gate dqos summary
GateID     i/f          SubscriberID   GC-Addr        State     Type  SFID(us) SFID(ds)
13576      Ca8/1/0      40.1.43.60     10.74.58.5     COMMIT    DQoS  527      528
29956      Ca8/1/0      40.1.43.56     10.74.58.5     COMMIT    DQoS  525      526
Total number of DQOS gates = 2
Total Gates committed(since bootup or clear counter) = 346
```

Cisco CMTS ルータを最後にリセットしてから、またはカウンタを最後にクリアにしてから、このルータの状態が Committed に移行したゲートの総数を確認するには、次の例のような show packetcable gate counter commit コマンドを使用します。

```
Router# show packetcable gate counter commit
通知済みゲート総数（カウンタの起動またはクリア以降）= 132
```

緊急 911 コールの確認

ここでは、show cable calls および show cable modem calls コマンドを使用して緊急 911 コールに関連するさまざまなシナリオを確認する方法を、いくつかの例で示します。

次の例に、優先度の高いコールのウィンドウ設定時に Cisco CMTS ルータの Cable8/1/1 インターフェイスで実行される緊急 911 コールを示します。

```
Router# show cable calls
Interface   ActiveHiPriCalls  ActiveAllCalls  PostHiPriCallCMs  RecentHiPriCMs
C5/0/0      0                 0               0                 0
C5/0/1      0                 0               0                 0
C5/1/0      0                 0               0                 0
C5/1/1      0                 0               0                 0
C5/1/2      0                 0               0                 0
C5/1/3      0                 0               0                 0
C5/1/4      0                 0               0                 0
C6/0/0      0                 0               0                 0
C6/0/1      0                 0               0                 0
C7/0/0      0                 0               0                 0
```

```
C7/0/1      0                 0                 0                 0
C8/1/0      0                 0                 0                 0
C8/1/1      1                 1                 0                 0
C8/1/2      0                 0                 0                 0
C8/1/3      0                 0                 0                 0
C8/1/4      0                 0                 0                 0
Total       1                 1                 0                 0
```

次の例に、この緊急 911 コールが終了したときの Cisco CMTS ルータ上の変化を示します。

```
Router# show cable calls
Interface   ActiveHiPriCalls  ActiveAllCalls  PostHiPriCallCMs  RecentHiPriCMs
C5/0/0      0                 0               0                 0
C5/0/1      0                 0               0                 0
C5/1/0      0                 0               0                 0
C5/1/1      0                 0               0                 0
C5/1/2      0                 0               0                 0
C5/1/3      0                 0               0                 0
C5/1/4      0                 0               0                 0
C6/0/0      0                 0               0                 0
C6/0/1      0                 0               0                 0
C7/0/0      0                 0               0                 0
C7/0/1      0                 0               0                 0
C8/1/0      0                 0               0                 0
C8/1/1      0                 0               0                 1
C8/1/2      0                 0               0                 0
C8/1/3      0                 0               0                 0
C8/1/4      0                 0               0                 0
Total       0                 0               0                 1
```

次の例に、音声コールを同じ MTA から同じインターフェイス上の他の MTA に発信するときに使用可能な情報を示します。

```
Router# show cable calls
Interface   ActiveHiPriCalls  ActiveAllCalls  PostHiPriCallCMs  RecentHiPriCMs
C5/0/0      0                 0               0                 0
C5/0/1      0                 0               0                 0
C5/1/0      0                 0               0                 0
C5/1/1      0                 0               0                 0
C5/1/2      0                 0               0                 0
C5/1/3      0                 0               0                 0
C5/1/4      0                 0               0                 0
C6/0/0      0                 0               0                 0
C6/0/1      0                 0               0                 0
C7/0/0      0                 0               0                 0
C7/0/1      0                 0               0                 0
C8/1/0      0                 0               0                 0
C8/1/1      0                 2               1                 1
C8/1/2      0                 0               0                 0
C8/1/3      0                 0               0                 0
C8/1/4      0                 0               0                 0
Total       0                 2               1                 1
```

次の例に、同じ MTA から同じインターフェイス上の他の MTA に発信した音声コールが終了したときに使用可能な情報を示します。

```
Router# show cable calls
Interface   ActiveHiPriCalls  ActiveAllCalls  PostHiPriCallCMs  RecentHiPriCMs
C5/0/0      0                 0               0                 0
C5/0/1      0                 0               0                 0
C5/1/0      0                 0               0                 0
C5/1/1      0                 0               0                 0
C5/1/2      0                 0               0                 0
C5/1/3      0                 0               0                 0
C5/1/4      0                 0               0                 0
C6/0/0      0                 0               0                 0
C6/0/1      0                 0               0                 0
C7/0/0      0                 0               0                 0
C7/0/1      0                 0               0                 0
C8/1/0      0                 0               0                 0
C8/1/1      0                 0               0                 1
```

```
C8/1/2      0                0               0                0
C8/1/3      0                0               0                0
C8/1/4      0                0               0                0
Total       0                0               0                1
```

次の例に、Cisco CMTS ルータの cable modem calls コマンドの一定期間にわたる出力を示します（コール ステータス情報が変化しています）。コール情報は、コールが終了すると消えます。

```
Router# show cable modem calls
Cable Modem Call Status Flags:
H: Active high priority calls
R: Recent high priority calls
V: Active voice calls (including high priority)
MAC Address    IP Address      I/F       Prim  CMCallStatus  LatestHiPriCall
                                         Sid                    (min:sec)
0000.cab7.7b04 10.10.155.38    C8/1/1/U0 18    R                 0:39
Router# show cable modem calls
Cable Modem Call Status Flags:
H: Active high priority calls
R: Recent high priority calls
V: Active voice calls (including high priority)
MAC Address    IP Address      I/F       Prim  CMCallStatus  LatestHiPriCall
                                         Sid                    (min:sec)
```

次の例に、Cisco CMTS ルータ上の新規の緊急 911 コールを示します。

```
Router# show cable modem calls
Cable Modem Call Status Flags:
H: Active high priority calls
R: Recent high priority calls
V: Active voice calls (including high priority)
MAC Address    IP Address      I/F       Prim  CMCallStatus  LatestHiPriCall
                                         Sid                    (min:sec)
0000.cab7.7b04 10.10.155.38    C8/1/1/U0 18    HV                1:30
```

次の例に、Cisco CMTS ルータ上の緊急 911 コールの終了を示します。

```
Router# show cable modem calls
Cable Modem Call Status Flags:
H: Active high priority calls
R: Recent high priority calls
V: Active voice calls (including high priority)
MAC Address    IP Address      I/F       Prim  CMCallStatus  LatestHiPriCall
                                         Sid                    (min:sec)
0000.cab7.7b04 10.10.155.38    C8/1/1/U0 18    R                 0:3
```

次の例に、同じ MTA から Cisco CMTS ルータへの非緊急音声コールを示します。

```
Router# show cable modem calls
Cable Modem Call Status Flags:
H: Active high priority calls
R: Recent high priority calls
V: Active voice calls (including high priority)
MAC Address    IP Address      I/F       Prim  CMCallStatus  LatestHiPriCall
                                         Sid                    (min:sec)
0000.ca36.f97d 10.10.155.25    C8/1/1/U0 5     V                  -
0000.cab7.7b04 10.10.155.38    C8/1/1/U0 18    RV                0:30
```

次の例に、Cisco CMTS ルータ上の非緊急音声コールの終了を示します。

```
Router# show cable modem calls
Cable Modem Call Status Flags:
H: Active high priority calls
R: Recent high priority calls
V: Active voice calls (including high priority)
MAC Address    IP Address      I/F       Prim  CMCallStatus  LatestHiPriCall
                                         Sid                    (min:sec)
0000.cab7.7b04 10.10.155.38    C8/1/1/U0 18    R                 0:36
```

PacketCable Multimedia 運用の情報

PacketCable Multimedia（PCMM）機能は、PacketCable Multimedia 用 CableLabs® 規格の強力な実装です。DOCSIS（DOCSIS 1.1 以降のバージョン）ネットワークにより、PCMM は、マルチメディア アプリケーション、音声、帯域幅使用量の多いサービスに強化された QoS を提供します。

Cisco CMTS ルータでは、SIP ベースの電話や SIP テレビ電話、帯域幅オンデマンド アプリケーション、ネットワーク ベースのゲーム アプリケーション（すべて、ネットワーク上で広範な帯域幅を要求）に対し、DOCSIS QoS がサポートされます。

ここでは、Cisco CMTS ルータ用 PacketCable Multimedia について、特に、このマニュアルで後述する Cisco IOS コマンドライン インターフェイスで設定する PCMM コンポーネントに関する情報を提供します。

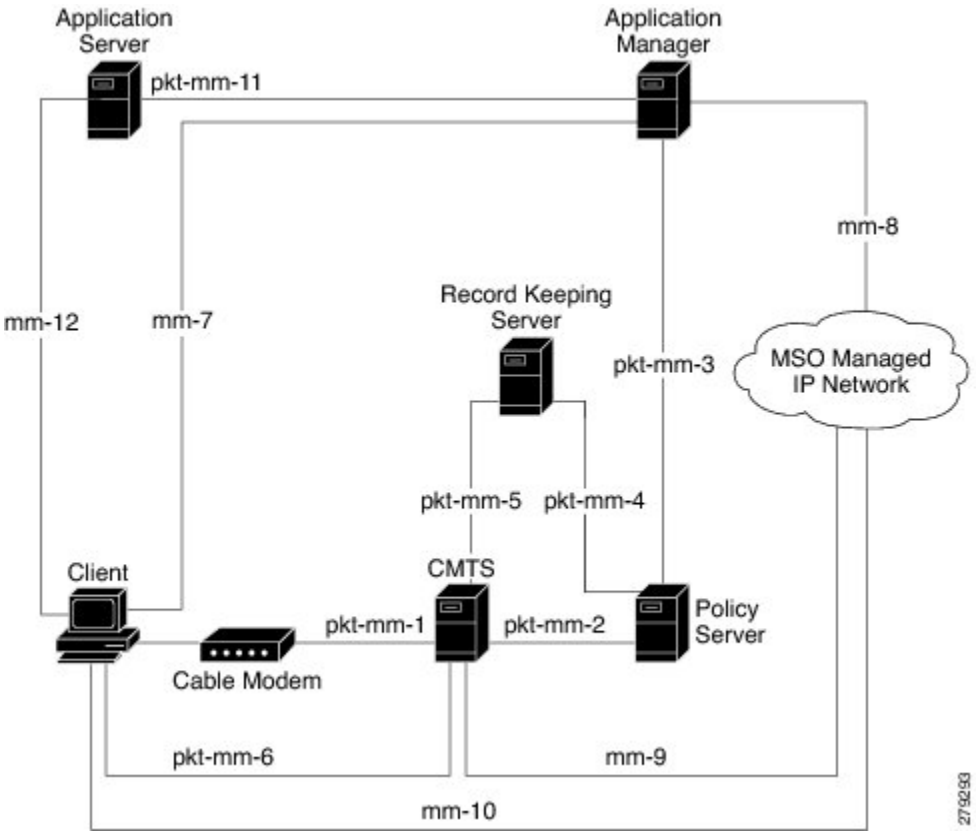
PCMM の概要

PCMM 機能をサポートするには次のネットワーク コンポーネントが必要です。

- アプリケーション サーバ：クライアント要求をアプリケーション マネージャに転送する中継役を担います。
- アプリケーションマネージャ：アプリケーションまたはセッション レベルの状態を管理し、セッション コントロール ドメイン（SCD）ポリシーを適用します。
- ポリシー サーバ：RCD ポリシーを適用し、アプリケーション マネージャと Cisco CMTS ルータ間の関係を管理します。
- Cisco CMTS ルータ：DOCSIS サービス フローを通じてアドミッション制御を実行し、ネットワーク リソースを管理します。

次の図に、PCMM 機能のアーキテクチャ概要を示します。

図 *31*：*PCMM* アーキテクチャ概要



PacketCable 1.x を介した PCMM の機能拡張

PacketCable Multimedia は、既存の PacketCable 1.x の展開と機能性をできるかぎり利用してサービス配信を行うための仕様です。さらに、PCMM は CLI を直接実装して VoIP サービス配信仕様を拡張し強化します。PCMM の主な拡張内容は次のとおりです。

- DOCSIS 1.1 サービス品質（QoS）メカニズムに基づく、時間と用量によるネットワーク リソース認証。
- イベントベースのネットワーク リソースの監査および管理機能
- すべてのインターフェイスを適切なレベルで保護するセキュアなインフラストラクチャ。
- PCMM ゲートのインストールと管理にサービス フローの作成、変更、削除機能が追加された PacketCable 1.x の事前許可モデル。ネットワークベースのセキュアな QoS も実現します。

Cisco CMTS ルータの PCMM および高可用性機能

Cisco CMTS ルータの高可用性は PCMM アプリケーションおよび PCCM ゲート用に作成されたサービス フローの同期のみに対応します。

PCMM ゲート

PCMM ゲートの概要と PCMM DQoS（Dynamic Quality of Service）

PacketCable 1.x ゲートは、QoS パラメータとポリシーに基づく加入者許可、およびネットワーク リソースの特別なエンベロープを定義します。また、PacketCable 1.x ゲートは、IP アドレスとポートを開始および終了するための分類子を保守します。

サブスクライバ ID は、ケーブル モデムまたはクライアント CPE のいずれかの IPv4 と IPv6 の両方のアドレスを識別できます。

PacketCable 1.x は事前許可モデルを定義します。PacketCable ゲートは、ネットワーク リソースの予約要求やアクティベーション要求よりも先に Cisco CMTS に作成されインストールされます。このプロセスはゲート コントロールと呼ばれ、COPS ベースのポリシー インターフェイスを通じて Cisco CMTS で 管理されます。

PCMM ではこの COPS ベースのインターフェイスが拡張され、QoS の寿命管理ができるようになりました。PCMM ゲートはサービス フローの作成、変更、削除機能を保守し、ネットワークベースの QoS を提供します。Cisco CMTS では指定の時間に複数の PCMM ゲートおよびサービス フロー ポリシーを保守することができ、これらの PCMM ゲートは PacketCable 1.x ゲートと完全に相互運用できます。

ケーブル モデムの加入者がネットワーク集中型アプリケーションの帯域を要求する場合、ネットワーク ポリシー サーバは Cisco CMTS ルータに Gate-Set メッセージを送信します。このメッセージには、QoS、サービス フロー、この加入者の課金情報が含まれています。このゲート プロファイル 情報は Cisco CMTS ルータで保守され、PCMM ゲート状態と PCMM 状態遷移を含みます。

Cisco CMTS ルータはケーブル モデムのサービス フローを開始し、Cisco CMTS での DOCSIS リソースの可用性を PCMM に特徴的な帯域幅使用量の多いサービス フローに合わせて最適化します。

制限事項

一部のアップストリーム パスで、一部のモデムにベスト エフォート サービス フローが認定情報レート（CIR）とともに設定されている場合があります。そのようなモデムで多数の帯域幅要求がキューイングされた場合は、少数の要求のみが CMTS に送信されます。これは、サービス フローの数に増えるとトラフィック量が増大して送信中の要求が輻輳状態になること、およびパケットのサイズが小さいことに起因します。このため、CMTS により少数のベスト エフォート サービス フロー要求のみが満たされます。

PCMM 永続ゲート

永続ゲートとは、オフラインになったケーブルモデムでPCMMゲート情報を保守する機能です。このゲート情報は、ケーブル モデムがオンラインに戻るとすぐにイネーブルになります。ケーブル モデムがオンラインに戻ると、Cisco CMTS ルータは保存されていた PCMM ゲートをスキャンし、それぞれの PCMM ゲートに応じてケーブル モデムへのサービスを開始します。イネーブルに戻ったサービスではそのゲートのトラフィック サポート プロファイルが保守され、新しいオンライン加入者に応じて DOCSIS リソースが割り当てられます。

PCMM インターフェイス

PCMM は、ケーブル インターフェイス ラインカードと Cisco CMTS ルータのルート プロセッサ（RP）との IPC ハンドシェイクを最適化します。また、PCMM インターフェイスの PacketCable 1.x からの変更には、COPS インターフェイスおよび分散ケーブル インターフェイス ラインカードの処理が含まれます。

PCMM と COPS の間のインターフェイス

PCMM は COPS セッションの処理が PacketCable 1.x と異なります。PCMM での COPS セッションでは、TCP ポート番号 3918 がデフォルトで使用されます。PacketCable は、TCP ポート要求と COPS セッションに DQoS 仕様を使用します。

PCMM モジュールを初めて初期化する場合、ケーブル インターフェイス ライン カードとルート プロセッサに PCMM レジストリが追加されます。PCMM モジュールには、PCMM COPS クライアントが Cisco CMTS ルータの COPS レイヤとともに登録されます。

PCMM と分散型ケーブル インターフェイス ラインカード

PacketCable 1.x では、PCMM は IPC メッセージを使って音声をサポートします。ネットワーク プロセッシング エンジン（NPE）やルート プロセッサ（RP）に PCMM ゲートが作成されると、PCMM ゲート パラメータがケーブル インターフェイス ライン カードに送信されます。IPC は NPE または RP とケーブル インターフェイス ライン カードの間の通信をすべて保守します。

PCMM ではイベント メッセージが使用され、Gate-Set メッセージに基づく課金情報をサポートします。DSX が正しく動作すると、分散型ケーブル インターフェイス ライン カードのイベント メッセージがライン カードから送信されます。

PCMM モジュールは PCMM COPS クライアントも COPS レイヤとともに登録します。

PCMM ユニキャストとマルチキャスト

ユニキャスト送信では、コンテンツは一意のユーザに送信されます。マルチキャスト送信では、コンテンツは複数のユーザに同時に送信されます。

PCMM マルチキャスト セッション範囲

PCMM マルチキャスト グループに対し IPv4 IP アドレスとマスクを指定することで PCMM マルチキャスト セッション範囲を設定できます。PCMM マルチキャスト セッション範囲により、Cisco CMTS ルータは PCMM ポリシー サーバから Gate-Set メッセージを受信できるようになります。PCMM マルチキャスト セッション範囲が設定されている場合、Cisco CMTS ルータで Internet Group Management Protocol（IGMP）および DOCSIS Set-Top Gateway（DSG）などの他のソースを使用してマルチキャスト セッションを作成することはできません。

PCMM 運用の設定方法

次に示すタスクにより、CMTS ルータで PCMM 運用をイネーブルにし、その関連機能を設定する方法について説明します。

Cisco CMTS ルータでの PCMM 運用の有効化

Cisco CMTS ルータで PCMM 運用をイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**packetcablemultimedia** 例： `Router(config)# packetcable multimedia`	Cisco CMTS ルータで PCMM 処理をイネーブルにして表示します。このコマンドは、PCMM ポリシー サーバから受信した PCMM COPS メッセージへの応答を、Cisco CMTS ルータが開始または停止できるようにします。

	コマンドまたはアクション	目的
ステップ 4	**packetcableauthorizevanilla-docsis-mta** 例： `Router(config)# packetcable authorize vanilla-docsis-mta`	非 DQoS MTA が DOCSIS DSX メッセージを送信するのを許可します。
ステップ 5	**packetcablegatemaxcount** *n* 例： `Router(config)# packetcable gate maxcount 890`	ゲート データベースの最大 PCMM ゲート数を設定します。
ステップ 6	**packetcabletimermultimediaT1** *timer-value* 例： `Router(config)# packetcable timer multimedia T1 300000`	PCMM ゲート処理で使用する T1 タイマーのタイムアウト値を設定します。
ステップ 7	**clearpacketcablegatecountercommit[dqos|multimedia]** 例： `Router(config)# clear packetcable gate counter commit multimedia`	（任意）指定した PCMM ゲート カウンタをクリアします。
ステップ 8	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。

PCMM マルチキャスト セッション範囲の設定

PCMM マルチキャスト セッション範囲により、Cisco CMTS ルータで PCMM マルチキャスト グループの IP アドレス範囲を使用できます。

はじめる前に

PCMM が、packetcable multimedia コマンドを使用して設定されていることを確認します。**packetcablemultimediacommand.**

（注）
- Cisco CMTS ルータで PCMM マルチキャスト グループのみを設定できます。1 つのマルチキャスト グループに最大 10 のマルチキャスト セッションを設定できます。
- PCMM マルチキャスト機能は、マルチキャスト DSID ベースの転送（MDF）に対応しているケーブル モデムでのみサポートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cablemulticastsourcepcmm** 例： `Router(config)# cable multicast source pcmm`	Cisco CMTS ルータの PCMM ベースのマルチキャスト サービスを有効にし、マルチキャスト セッション範囲コンフィギュレーション モードを開始します。
ステップ 4	**session-range** *ip-addressip-mask* 例： `Router(config)# session-range 229.0.0.0 255.0.0.0`	PCMM マルチキャスト グループのセッション範囲を設定します。
ステップ 5	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。

PacketCable Multimedia の設定例

ここでは、Cisco CMTS ルータでの PCMM 運用の設定例を示します。

例：Cisco CMTS ルータでの PCMM 運用の有効化

```
Router# configure terminal
Router(config)# packetcable multimedia
Router(config)# packetcable authorize vanilla-docsis-mta
Router(config)# packetcable gate maxcount 890
Router(config)# packetcable timer multimedia 30000
```

例：Cisco CMTS ルータでのマルチキャスト セッション範囲の有効化

```
Router# configure terminal
Router(config)# cable multicast source pcmm
Router(config)# session-range 229.0.0.0 255.0.0.0
```

PCMM 運用の確認

PCMM 運用を確認するには、次の **show** コマンドを使用します。

- **showpacketcablegatemultimedia**
- **showcablemulticastdb**
- **showinterfacewideband-cable**
- **showcablemulticastqos**

PCMMマルチキャスト ゲートを確認するには、次の例に示すように**showpacketcablegatemultimedia** コマンドを使用します。

```
Router# show packetcable gate multimedia multicast summary
GateID     i/f          SubscriberID   GC-Addr        State     Type  SFID(us) SFID(ds)
134        Ca5/0/0      60.1.1.202     2.39.26.19     COMMIT    MM             4
Total number of Multimedia-MCAST gates = 1
Total Gates committed(since bootup or clear counter) = 1
```

PCMM IPv6 ゲートを確認するには、次の例に示すように **show packetcable gate multimedia ipv6** コマンドを使用します。

```
Router# show packetcable gate multimedia ipv6 summary
Load for five secs: 10%/1%; one minute: 9%; five minutes: 9%
Time source is NTP, 03:29:42.153 EST Mon Nov 9 2015

GateID     i/f                     SubscriberID               State   SFID(us) SFID(ds)
409        Ca5/0/2      2001:420:2C7F:FC38:58AF:E36A:80:213A   COMMIT             1326

16789      Ca5/0/2      2001:420:2C7F:FC38:AC40:A49A:F80A:8D0B COMMIT    1321
33177      Ca5/0/2      2001:420:2C7F:FC38:DD49:72A3:2ECC:8770 COMMIT             1322

49577      Ca5/0/2      2001:420:2C7F:FC38:485:31DF:C88B:E315  COMMIT    1308
65953      Ca5/0/2      2001:420:2C7F:FC38:5AB:AA0B:34AD:ACCF  COMMIT    1336
82337      Ca5/0/2      2001:420:2C7F:FC38:5AB:AA0B:34AD:ACCF  COMMIT             1337

98721      Ca5/0/2      2001:420:2C7F:FC38:5570:EF2E:7565:D36A COMMIT             1316

115097     Ca5/0/2      2001:420:2C7F:FC38:6009:EF26:F573:7356 COMMIT             1318
```

```
131489     Ca5/0/2      2001:420:2C7F:FC38:7D4A:BC50:3FD:CA7   COMMIT    1312
147873     Ca5/0/2      2001:420:2C7F:FC38:E83E:8259:AEF6:5624 COMMIT    1332


Total number of Multimedia gates = 10
Total Gates committed(since bootup or clear counter) = 1024
```

マルチキャスト データベースで利用可能なすべての PCMM クライアント エントリを確認するには、次の例に示すように **show cable multicast db** コマンドを使用します。

```
Router# show cable multicast db client pcmm
Interface : Bundle1
Session (S,G) : (*,229.2.2.12)
Fwd Intf     Bundle Intf  Host Intf    CM MAC         CPE IP           Gate-ID SFID
Wi1/1/0:0    Bundle1      Ca5/0/0      0018.6852.8056 60.1.1.202       134 4
```

特定のワイドバンド ケーブル インターフェイスのマルチキャスト セッションを確認するには、次の例に示すように **showinterfacewideband-cable** コマンドを使用します。

```
Router# show interface wideband-cable 1/1/0:0 multicast-sessions
Default Multicast Service Flow 3 on Wideband-Cable1/1/0:0
Multicast Group    : 229.2.2.12
         Source    : N/A
         Act GCRs  : 1
         Interface : Bu1                    State: A      GI: Bu1         RC: 0
  GCR       : GC   SAID    SFID    Key   GQC    GEn
                   512  8196    4       0     512    0
```

特定のワイドバンド ケーブル インターフェイス上のサービス フローの属性ベースの割り当てを確認するには、次の例に示すように **showinterfacewideband-cable** コマンドを使用します。

```
Router# show interface wideband-cable 1/1/0:0
service-flow 4 verbose
Sfid                                  : 4
Mac Address                           : ffff.ffff.ffff
Type                                  : Secondary(Static)
Direction                             : Downstream
Current State                         : Active
Current QoS Indexes [Prov, Adm, Act]  : [4, 4, 4]
Active Time                           : 05:26
Required Attributes                   : 0x00000000
Forbidden Attributes                  : 0x00000000
Aggregate Attributes                  : 0x00000000
Multicast Sid                         : 8196
Traffic Priority                      : 0
Maximum Sustained rate                : 0 bits/sec
Maximum Burst                         : 3044 bytes
Minimum Reserved Rate                 : 250000 bits/sec
Minimum Packet Size                   : 0 bytes
Maximum Latency                       : 0 usecs
Peak Rate                             : 0 bits/sec
Admitted QoS Timeout                  : 200 seconds
Active QoS Timeout                    : 0 seconds
Packets                               : 0
Bytes                                 : 0
Rate Limit Delayed Packets            : 0
Rate Limit Dropped Packets            : 0
Current Throughput                    : 0 bits/sec, 0 packets/sec
Application Priority                  : 0
Low Latency App                       : No
Blaze/JIB3 DS Statistic Index         : 0
Forwarding Interface                  : Wi1/1/0:0
Classifiers: NONE
```

PCMM ベースの MQoS ゲート コントローラが正しいセッション範囲で作成されていることを確認するには、次の例に示すように **showcablemulticastqos** コマンドを使用します。

```
Router# show cable multicast qos group-qos
Group QOS Index    Service Class     Control    Igmp Limit    Override  App
 DEFAULT           mcast_default      Aggregate  NO-LIMIT
 1                 SDV_SD             Single      ---           No        CLI
 512               SDV_HD             Single      ---           No        PCMM
```

PacketCable と PacketCable Multimedia の高可用性ステートフル スイッチオーバー（SSO）

拡張型高可用性サポート機能により、Cisco CMTS ルータでのスイッチオーバー イベント時に PacketCable と PacketCable Multimedia（PCMM）のゲートを同期化できるようになります。この拡張機能はデフォルトで有効になっています。

この機能は、N+1 冗長性の場合に作業インターフェイスと保護インターフェイスを関連付けるために使用される、既存のインターフェイス単位の HCCP コマンドを使用します。

アドミッション制御による PacketCable と PCMM

PacketCable または PacketCable Multimedia ネットワークには、アドミッション制御 QoS の恩恵を受ける多数のコンポーネントが含まれます。アドミッション制御は PacketCable および PCMM の QoS を次の方法で管理し最適化します。

- 音声およびデータの QoS（DOCSIS 1.1 以降のバージョンに基づく）
- ケーブル モデム登録
- CMS
- ゲートウェイ コントローラ（GC）
- 記録保持サーバ（RKS）
- ビデオ テレフォニー

PacketCable または PCMM のいずれかでアドミッション制御を設定し、その恩恵を受けるには、PacketCable または PCMM が Cisco CMTS ヘッドエンドで十分に動作する必要があります。

音声 MGPI サポート

Multiple Grants Per Interval（MGPI）機能を使用すると、Cisco CMTS ルータは、同じケーブル モデムの UGS トラフィック プロファイルを使用して、単一の DOCSIS サービス フローに複数の PacketCable Multimedia ゲート（アプリケーション フロー）をマッピングすることができます。つまり、Cisco CMTS ルータでは、単一のサービス フローに基づく各アプリケーション フローの 1 間隔あたりの許可の数が増え、これにより 1 間隔あたりの複数許可が実現しています。

MGPI 機能は、CableLabs PacketCable 仕様（PKT-SP-MM-I05-091029）に基づくフロー集約音声の MGPI 機能をサポートします。フロー集約 MGPI 機能により、アプリケーション マネージャは UGS トラフィック プロファイルを使用して、1 間隔あたりの許可の数を明示的に設定し、単一ゲートに複数のアプリケーションフローを置くことができます。これにより、イベントメッセージ、ボリューム、および時間の使用制限が集約されたビューが表示されます。

DOCSIS 3.0 E-MTA での音声サポート

PacketCable および PCMM サービスが、組み込み型マルチメディア ターミナル アダプタ（E-MTA）でサポートされます。E-MTA は、物理的な音声デバイス、ネットワーク インターフェイス、および VoIP トランスポート、クラス機能シグナリング、QoS シグナリングに必要なすべてのシグナリングおよびカプセル化機能へのインターフェイスを含むネットワーク要素です。

PacketCable と PCMM コール トレース

シグナリング情報を効果的にキャプチャするため、この機能では設定された数の PacketCable または PCMM ゲートのシグナリングをバッファします。デフォルトで、10 のユーザ設定のゲート トレースだけがバッファに保存されます。指定した数に達したら、それ以降のゲート シグナリング情報はバッファされません。トレースされるゲートの 1 つが削除されると、新しいゲートのゲート シグナリングがバッファされます。

Cisco CMTS ルータでの PacketCable および PacketCable Multimedia ゲートのコール トレース機能を有効にするには、グローバル コンフィギュレーション モードで **cabledynamic-qostrace** コマンドを使用します。コール トレースをイネーブルにする必要がある加入者の数を指定する必要があります。

PacketCable と PCMM 統計情報の確認

次のコマンドを使用すると、Cisco CMTS ルータの PacketCable および PCMM の統計情報を確認できます。

- **showinterfacecabledynamic-servicestatistics**
- **showinterfacecablepacketcablestatistics**
- **showpacketcablecms**

ケーブル インターフェイスに基づいたダイナミックなサービスの統計情報を確認するには、次の例のように show interface cable dynamic-service statistics コマンドを使用します。

```
Router# show interface cable 7/1/0 dynamic-service statistics
  Upstream         Downstream
DSA REQ      0                5
DSA RSP      5                0
DSA ACK      0                5
DSC REQ      0                5
DSC RSP      5                0
DSC ACK      0                5
DSD REQ      0                0
DSD RSP      0                0
Retransmission counts
```

```
             Upstream        Downstream
DSA REQ      0               0
DSA RSP      0               0
DSA ACK      0               0
DSC REQ      0               5
DSC RSP      5               0
DSC ACK      0               0
DSD REQ      0               0
DSD RSP      0               0
```

ケーブル インターフェイスに基づいた PacketCable IPC の統計情報を確認するには、次の例のように show interface cable packetcable statistics コマンドを使用します。

```
Router# show interface cable 7/1/0 packetcable statistics
Packetcable IPC Statistics on RP
Msg   create     gate       gate       gate set   dsd
      gie        set        del        notify     notify
Sent  0          10         0          0          0
Rcvd  0          0          0          10         0
Packetcable IPC Statistics on LC
Msg   create     gate       gate       gate set   dsd
      gie        set        del        notify     notify
Sent  0          0          0          10         0
Rcvd  0          10         0          0          0
```

PacketCable クライアントに現在接続されているすべてのゲート コントローラを確認するには、次の例ように show packetcable cms コマンドを使用します。

```
Router# show packetcable cms
GC-Addr         GC-Port  Client-Addr    COPS-handle  Version PSID Key PDD-Cfg
1.100.30.2      47236    2.39.34.1      0x2FF9E268/1    4.0   0    0   0
2.39.26.19      55390    2.39.34.1      0x2FF9D890/1    1.0   0    0   2
```

PacketCable 接続がダウンした COPS サーバを含むすべてのゲート コントローラを確認するには、次の例に示すように **show packetcable cms** コマンドを使用します。

```
Router# show packetcable cms all
GC-Addr         GC-Port  Client-Addr    COPS-handle  Version PSID Key PDD-Cfg
1.100.30.2      47236    2.39.34.1      0x2FF9E268/1    4.0   0    0   0
2.39.26.19      55390    2.39.34.1      0x2FF9D890/1    1.0   0    0   2
1.10.30.22      42307    2.39.34.1      0x0       /0    4.0   0    0   0
```

ゲート コントローラの統計情報を確認するには、次の例に示すようにキーワード verbose を指定した **show packetcable cms** コマンドを使用します。

```
Router# show packetcable cms verbose
Gate Controller
     Addr         :     1.100.30.2
     Port         :     47236
     Client Addr  :     2.39.34.1
     COPS Handle  :     0x2FF9E268
     Version      :     4.0
     Statistics   :
        gate del =  0  gate del ack =  0   gate del err = 0
        gate info = 0  gate info ack = 0  gate info err = 0
        gate open =  0  gate report state = 0
        gate set =  0  gate set ack =  0   gate set err = 0
        gate alloc = 0 gate alloc ack = 0  gate alloc err = 0
        gate close =  0
Gate Controller
     Addr         :     2.39.26.19
     Port         :     55390
     Client Addr  :     2.39.34.1
     COPS Handle  :     0x2FF9D890
     Version      :     1.0
     Statistics   :
        gate del =  0  gate del ack =  0   gate del err = 0
        gate info = 0  gate info ack = 0  gate info err = 0
        gate open =  0  gate report state = 0
        gate set =  2  gate set ack =  2   gate set err = 0
```

```
        PCMM Timers Expired
        Timer T1 =  0  Timer T2 =  0 Timer T3 = 0 Timer T4 = 0
GC-Addr         GC-Port  Client-Addr    COPS-handle  Version PSID Key PDD-Cfg
1.100.30.2      47236    2.39.34.1      0x2FF9E268/1    4.0   0    0   0
2.39.26.19      55390    2.39.34.1      0x2FF9D890/1    1.0   0    0   2
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
CMTS コマンド	『*Cisco CMTS Cable Command Reference*』 http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html
N+1 冗長	『*N+1 Redundancy for the Cisco CMTS Routers*』 http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/cmts_nplus1_redun_ps2209_TSD_Products_Configuration_Guide_Chapter.html
NTP または SNTP の設定	システム クロックの設定に Network Time Protocol（NTP）または Simple Network Time Protocol（SNTP）を使用するように Cisco CMTS ルータを設定するには、『Cisco IOS Configuration Fundamentals Configuration Guide』の「System Management」セクションの「Performing Basic System Management」章を参照してください。

標準

標準[4]	タイトル
PKT-SP-MM-I06-110629	『PacketCable™ Specification Multimedia Specification』
ITU X.509 V3	『*International Telecommunications Union (ITU) X.509 Version 3.0* standard』
PKT-EM-I03-011221	『*PacketCable™ Event Message Specification*』

標準[4]	タイトル
PKT-SP-DQOS-I04-021018	『*PacketCable™ Dynamic Quality-of-Service Specification*』
PKT-SP-EC-MGCP-I04-011221	『*PacketCable™ Network-Based Call Signaling Protocol Specification*』
PKT-SP-ESP-I01-991229	『*PacketCable™ Electronic Surveillance Specification*』
PKT-SP-ISTP-I02-011221	『*PacketCable™ Internet Signaling Transport Protocol (ISTP) Specification*』
PKT-SP-PROV-I03-011221	『*PacketCable™ MTA Device Provisioning Specification*』

4 サポートされている標準がすべて記載されているわけではありません。

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1321	『*The MD5 Message-Digest Algorithm*』
RFC 1510	『*The Kerberos Network Authentication Service (V5)*』
RFC 2138	『*Remote Authentication Dial In User Service (RADIUS)*』
RFC 2205	『*Resource ReSerVation Protocol (RSVP)*』
RFC 2327	*SDP: Session Description Protocol*

RFC	タイトル
RFC 2748	『*The COPS (Common Open Policy Service) Protocol*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

PacketCable と PacketCable Multimedia に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

機能名	リリース	機能情報
PacketCable と PacketCable Multimedia ユニキャスト	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。
PacketCable と PacketCable Multimedia マルチキャスト	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

機能名	リリース	機能情報
DQoSLite ベースの IPv6 音声サポート	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 73 章

COPS エンジン操作

このマニュアルでは、Cisco CMTS ルータの Common Open Policy Service（COPS）エンジン機能について説明します。Cisco CMTS ルータは、COPS エンジンを搭載するアクセス コントロール リスト（ACL）もサポートします。

機能情報の確認

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *178* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

Cisco CMTS ルータの COPS エンジンの前提条件

- Cisco COPS QoS Policy Manager などの互換性のあるポリシー サーバをネットワークに接続する必要があります。

- Cisco CMTS ルータでこの機能を使用するには、Computer Assisted Law Enforcement Act（CALEA）またはその他の合法的傍受（LI）などの管理ポリシーに準拠している必要があります。

Cisco CMTS の COPS エンジンの制限事項

- リソース予約プロトコル（RSVP）は Cisco CMTS で設定されません。Cisco CMTS で COPS エンジンを設定できるのは、RSVP と COPS サーバが別々に設定され動作可能になっているネットワークに限定されます。

Cisco CMTS の COPS エンジンに関する情報

共通オープン ポリシー サービス（COPS）は、ネットワーク トラフィック ポリシー情報をネットワーク デバイスに伝達するためのプロトコルです。

COPS は、リソース予約プロトコル（RSVP）と協調して動作します。RSVP は、ネットワーク リソース（主に帯域幅）を予約して、インターネット上をエンドツーエンドで送信するアプリケーションが必要な速度と品質で動作することを保証するための手段です。RSVP は Cisco CMTS 上で設定されませんが、Cisco CMTS はその設定でネットワークに RSVP があることを前提としています。

RSVP 用 COPS の詳細については、その他の参考資料，（1214 ページ）を参照してください。

Cisco CMTS での COPS エンジンの設定方法

ここでは、Cisco CMTS の RSVP 用 COPS の設定タスクについて説明します。

Cisco CMTS で COPS エンジンを設定するには、次のタスクを実行します。

COPS TCP と DSCP マーキングの設定

この機能を使用すると、Cisco ルータで送信または受信する COPS メッセージの DiffServ コードポイント（DSCP）マーキングを変更できます。**copsipdscp** コマンドは、ケーブル ネットワーク内の Cisco ルータと COPS サーバ間の接続に関するデフォルトの IP パラメータを変更します。

DSCP 値は、Cisco ルータの Quality of Service（QoS）設定で DSCP と IP プレシデンスの関係を要約するために使用されます。このコマンドを使用すると、COPS で着信または発信接続のパケットをリマークできます。

発信接続のデフォルト設定は 0 です。デフォルトの着信接続では、COPS エンジンは TCP 接続を開始する COPS サーバから DSCP 値を取得します。

（注） この機能は、すべての COPS サーバを使用するすべての TCP 接続に影響を与えます。

- Cisco ルータによって送信されるメッセージの場合、デフォルトの DSCP 値は 0 です。
- Cisco ルータへの着信接続については、COPS エンジンは TCP 接続を開始する COPS サーバが使用する DSCP 値をデフォルトで取得します。
- **copsipdscp** コマンドを使用すると、Cisco ルータは着信接続または発信接続の COPS パケットをリマークできます。
- このコマンドは、すべての COPS サーバによるすべての TCP 接続に影響します。
- このコマンドは COPS サーバの既存の接続には影響しません。このコマンドを使用すると、この機能はそれ以降の新しい接続でのみサポートされます。

Cisco CMTS で COPS メッセージの DSCP マーキング オプションを有効にするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**copsipdscp** [<**0-63**> | **default** | **af11-af43** |**cs1-cs7**] 例： `Router(config)# cops ip dscp default`	Cisco ルータで送信される COPS メッセージのマーキングを指定します。 このコマンドの値は、COPS メッセージの送信で使用するマーキングを指定します。Cisco CMTS ルータでサポートされる値は次のとおりです。 • **0-63**：0 ～ 63 の DSCP 値。 • **af11**：AF11 dscp（001010）を使用 • **af12**：AF12 dscp（001100）を使用 • **af13**：AF13 dscp（001110）を使用 • **af21**：AF21 dscp（010010）を使用 • **af22**：AF22 dscp（010100）を使用 • **af23**：AF23 dscp（010110）を使用 • **af31**：AF31 dscp（011010）を使用

	コマンドまたはアクション	目的
		• **af32**：AF32 dscp（011100）を使用 • **af33**：AF33 dscp（011110）を使用 • **af41**：AF41 dscp（100010）を使用 • **af42**：AF42 dscp（100100）を使用 • **af43**：AF43 dscp（100110）を使用 • **cs1**：CS1 dscp（001000）[優先順位 1] を使用 • **cs2**：CS2 dscp（010000）[優先順位 2] を使用 • **cs3**：CS3 dscp（011000）[優先順位 3] を使用 • **cs4**：CS4 dscp（100000）[優先順位 4] を使用 • **cs5**：CS5 dscp（101000）[優先順位 5] を使用 • **cs6**：CS6 dscp（110000）[優先順位 6] を使用 • **cs7**：CS7 dscp（111000）[優先順位 7] を使用 • **default**：デフォルト dscp（000000）を使用 • **ef**：EF dscp（101110）を使用

ステップ 4	exit
	
	例：
	
	`Router(config)# exit`
	`Router#`
		特権 EXEC モードに戻ります。

COPS TCP ウィンドウ サイズの設定

この機能により、COPS プロセスで使用されるデフォルトの TCP 受信ウィンドウ サイズを変更できます。この設定を使用すると、COPS サーバが一度に大量のデータを送信できないようにすることができます。

Cisco CMTS で TCP ウィンドウ サイズを変更するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**copstcpwindow-size** *bytes* 例： `Router(config)# cops tcp window-size 64000`	Cisco CMTS のデフォルトの TCP 受信ウィンドウ サイズを変更します。TCP ウィンドウ サイズをデフォルト設定 4K に戻すには、このコマンドの **no** 形式を使用します。 （注） デフォルトの COPS TCP ウィンドウ サイズは 4000 バイトです。 （注） このコマンドは、COPS サーバへの既存の接続には影響しません。このコマンドを使用すると、この機能はそれ以降の新しい接続でのみサポートされます。 （注） このコマンドは、すべての COPS サーバを使用するすべての TCP 接続に影響を与えます。

ステップ 4	**exit**
	
	例：
	
	`Router(config)# exit`
	`Router#`
		特権 EXEC モードに戻ります。

COPS エンジンのアクセス コントロール リスト サポートの設定

Cisco CMTS で COPS ACL を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**copslistenersaccess-list**{ *acl-num* |*acl-name* } 例： `Router# cops listeners access-list 40`	Cisco CMTS のすべての COPS リスナー アプリケーションへの着信接続のためにアクセス コントロール リスト（ACL）を設定します。Cisco CMTS からこの設定を削除するには、このコマンドの **no** 形式を使用します。

ステップ 4	**exit**
	
	例：
	`Router(config)# exit`
	`Router#`
		特権 EXEC モードに戻ります。

次の作業

特権 EXEC モードで **showaccess-list** コマンドを使用すると、アクセス リストを表示できます。

特定のアクセス コントロール リストへの RSVP ポリシーの制限

Cisco CMTS ですでに設定された特定の ACL に対して RSVP ポリシーを制限するには、次の手順を実行します。

ACL 設定については、COPS エンジンのアクセス コントロール リスト サポートの設定, （1210 ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacecable** (*slot* /*subslot* /*port* }
	
	例：
	
	`Router(config)#interface cable 8/0/1`
	`Router(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 4	**ip rsvp policy cops** *ACL-1 ACL-2* **servers** *iP-addr1 IP-addr2* 例： `Router(config-if)# ip rsvp policy cops 40 160 servers 161.44.130.164 161.44.129.2`	指定した ACL と一致するメッセージに RSVP ポリシーを適用するようにルータに通知し、そのセッションで COPS サーバまたはサーバを指定します。

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

Cisco CMTS での COPS エンジン設定の表示と検証

Cisco CMTS で COPS を有効化して設定した後は、次の手順に従い、**show** コマンドの 1 つまたはすべてを使用して、設定を確認および追跡できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**showcopsservers** 例： `Router# show cops servers`	サーバアドレス、ポート、状態、キープアライブ、およびポリシー クライアント情報を表示します。

	コマンドまたはアクション	目的
ステップ 3	**showiprsvppolicycops** 例： `Router# show ip rsvp policy cops`	ポリシー サーバ アドレス、ACL ID、およびクライアント/サーバの接続状態を表示します。
ステップ 4	**show ip rsvppolicy** 例： `Router# show ip rsvp policy`	ACL ID および接続状態を表示します。

COPS エンジン情報の show コマンド

次に、Cisco ルータの COPS エンジンの設定例を 3 つ示します。それぞれの show コマンドで COPS エンジン設定を確認します。

ネットワークの COPS サーバの表示

この例では、ポリシー サーバ アドレス、状態、キープアライブ、およびポリシー クライアントの情報を表示します。

```
Router# show cops servers
COPS SERVER: Address: 161.44.135.172. Port: 3288. State: 0. Keepalive: 120 sec
Number of clients: 1. Number of sessions: 1.
    COPS CLIENT: Client type: 1.  State: 0.
```

ネットワークの COPS ポリシー情報の表示

この例では、ポリシー サーバ アドレス、ACL ID、およびクライアント/サーバ接続のステータスを表示します。

```
Router# show ip rsvp policy cops
COPS/RSVP entry. ACLs: 40 60
PDPs: 161.44.135.172
Current state: Connected
Currently connected to PDP 161.44.135.172, port 0
```

COPS の アクセス リストの表示

この例では、各 ACL ID の ACL ID 番号およびステータスを表示します。

```
Router# show ip rsvp policy
Local policy: Currently unsupported
COPS:
ACLs: 40 60 . State: CONNECTED.
ACLs: 40 160 . State: CONNECTING.
```

ケーブル用 COPS エンジンの設定例

ここでは、Cisco CMTS での RSVP 用 COPS の設定例を示します。

例：COPS サーバの指定

次の例は、COPS サーバを指定し、このサーバで RSVP 用 COPS を有効にします。 **ip rsvp policy cops** コマンドを使用することによって、両方の機能が実行されます。残りのすべての RSVP 用 COPS コマンドのデフォルト設定は、暗黙的に受け入れられます。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip rsvp policy cops servers 161.44.130.168 161.44.129.6
Router(config)# exit
```

例：COPS サーバの表示

次の例では、ルータの RSVP 設定用 COPS のビューを 3 種類表示します。これは、RSVP 設定用 COPS の確認に使用できます。

この例では、ポリシー サーバ アドレス、状態、キープアライブ、およびポリシー クライアントの情報を表示します。

```
Router# show cops servers
COPS SERVER: Address: 161.44.135.172. Port: 3288. State: 0. Keepalive: 120 sec
Number of clients: 1. Number of sessions: 1.
    COPS CLIENT: Client type: 1.  State: 0.
```

この例では、ポリシー サーバ アドレス、ACL ID、およびクライアント/サーバ接続のステータスを表示します。

```
Router# show ip rsvp policy cops
COPS/RSVP entry. ACLs: 40 60
PDPs: 161.44.135.172
Current state: Connected
Currently connected to PDP 161.44.135.172, port 0
```

この例では、各 ACL ID の ACL ID 番号およびステータスを表示します。

```
Router# show ip rsvp policy
Local policy: Currently unsupported
COPS:
ACLs: 40 60 . State: CONNECTED.
ACLs: 40 160 . State: CONNECTING.
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco CMTS コマンド	『Cisco CMTS Cable Command Reference』

関連項目	マニュアル タイトル
RSVP 用 COPS	• 『*Configuring COPS for RSVP*』 http://www.cisco.com/en/US/docs/ios-xml/ios/qos_rsvp/configuration/12-4t/cops_rsvp.html • 『*COPS for RSVP*』 http://www.cisco.com/en/US/docs/ios/12_1t/12_1t1/feature/guide/CopsRSVP.html

標準

規格	タイトル
PKT-SP-ESP-I01-991229	『PacketCable™ Electronic Surveillance Specification』（http://www.packetcable.com）

MIB

MIB	MIB のリンク
• この機能のサポートのために導入または強化された MIB はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
一般的な RFC リソース	• 『*RFC Index Search Engine*』 http://www.rfc-editor.org/rfcsearch.html • 『*SNMP: Frequently Asked Questions About MIB RFCs*』 http://www.cisco.com/en/US/tech/tk648/tk362/technologies_q_and_a_item09186a00800c2612.shtml

シスコのテクニカル サポート

説明	リンク
シスコのテクニカルサポートおよびドキュメンテーション Web サイトでは、製品、テクノロジー、ソリューション、テクニカル ティップス、ツールへのリンクなど、技術的なコンテンツを検索可能な形で大量に提供しています。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

COPS エンジン操作に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *179* : *COPS* エンジン操作に関する機能情報

機能名	リリース	機能情報
COPS エンジン操作	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 X 部

QoS の構成

第 74 章

動的帯域幅共有

Cisco cBR シリーズ ルータでは、内蔵ケーブル（IC）インターフェイスとワイドバンド（WB）ケーブル インターフェイス（DBS）での動的帯域幅共有が可能です。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *180* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

動的帯域幅共有に関する情報

内蔵およびワイドバンド ケーブル インターフェイスでの DBS

DOCSIS 3.0 の規格より前は、サービス フローは単一のケーブル インターフェイスに関連付けられていました。このインターフェイスはラインカード上の物理ダウンストリームに対応していました。DOCSIS 3.0 の規格では、ケーブル サービス フローを複数のダウンストリーム チャネルに関連付けることができます。

DBS は、同じダウンストリーム チャネルを共有する IC および WB ケーブル インターフェイス用の動的帯域幅割り当てです。IC、WB ケーブルのそれぞれ、またはナローバンド チャネルに使用できる帯域幅は固定値ではなく、IC または WB ケーブルの設定とトラフィックの負荷によって異なります。

DBS により DOCSIS 2.0 ケーブル モデムおよび DOCSIS 3.0 ケーブル モデムで高バースト レートが実現します。DBS 機能により、ラインカードおよびスーパーバイザのスイッチオーバーは機能を損なうことなく継続的に実行されます。

動的帯域幅共有の設定方法

動的帯域幅共有は、Cisco cBR ルータの内蔵ケーブ インターフェイスおよびワイドバンド ケーブル インターフェイスでデフォルトでイネーブルになっています。WB インターフェイスと IC インターフェイスの帯域幅割り当てを設定できます。

重要 Cisco cBR ルータでは動的帯域幅共有をディセーブルにすることはできません。

ここでは、次の手順について説明します。

ワイドバンド ケーブル インターフェイスの DBS の設定

ワイドバンドケーブルインターフェイスの帯域幅割り当てを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacewideband-cable** *slot/subslot/portwideband-channel* 例： `Router(config)# interface wideband-cable 1/0/0:0`	ワイドバンド ケーブル インターフェイスを設定します。
ステップ 4	**cablerf-channel channel-list** *grouplist* [**bandwidth-percent** *bw-percent*] 例： `Router(config-if)# cable rf-channel channel-list 10 bandwidth-percent 50`	ワイドバンド チャネル インターフェイスの帯域幅割り当てを設定します。

内蔵ケーブル インターフェイスの DBS の設定

内蔵ケーブル インターフェイスの帯域幅割り当てを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**interfaceintegrated-cable** *slot/subslot/portrf-channel* 例： `Router(config)# interface integrated-cable 1/0/0:0`	ケーブル インターフェイス モードを開始します。
ステップ 4	**cablerf-bandwidth-percent** *bw-percent* 例： `Router(config-if)# cable rf-bandwidth-percent 50`	内蔵ケーブルインターフェイスの帯域幅割り当てを設定します。

動的帯域幅共有設定の確認

動的帯域幅共有の情報を確認するには、次のコマンドを使用します。

- **show controllers Integrated-Cable** *slot/subslot/port***bandwidth rf-channel**：RF チャネルの帯域幅情報を表示します。

  次に、コマンドの出力例を示します。

```
Router# show controllers integrated-Cable 2/0/0 bandwidth rf-channel

Ctrlr    RF       IF           CIR(Kbps)    Guar(Kbps)
2/0/0    0        In2/0/0:0    7500         13750
                  Wi2/0/0:0    7500         13750
                  Wi2/0/0:1    3750         10000
2/0/0    1        In2/0/0:1    7500         13750
                  Wi2/0/0:0    7500         13750
                  Wi2/0/0:1    3750         10000
2/0/0    2        In2/0/0:2    7500         12500
                  Wi2/0/0:0    7500         12500
                  Wi2/0/0:1    7500         12500
2/0/0    3        In2/0/0:3    7500         12500
                  Wi2/0/0:0    7500         12500
                  Wi2/0/0:1    7500         12500
2/0/0    4        In2/0/0:4    7500         12500
                  Wi2/0/0:0    7500         12500
                  Wi2/0/0:1    7500         12500
2/0/0    5        In2/0/0:5    7500         12500
                  Wi2/0/0:0    7500         12500
                  Wi2/0/0:1    7500         12500
2/0/0    6        In2/0/0:6    7500         12500
                  Wi2/0/0:0    7500         12500
                  Wi2/0/0:1    7500         12500
2/0/0    7        In2/0/0:7    7500         12500
                  Wi2/0/0:0    7500         12500
                  Wi2/0/0:1    7500         12500
2/0/0    8        In2/0/0:8    7500         18750
                  Wi2/0/0:1    7500         18750
                  Wi2/0/0:2    7500         0
2/0/0    9        In2/0/0:9    7500         18750
                  Wi2/0/0:1    7500         18750
                  Wi2/0/0:2    7500         0
2/0/0    10       In2/0/0:10   7500         18750
```

```
                  Wi2/0/0:1    7500         18750
                  Wi2/0/0:2    7500         0
2/0/0    11       In2/0/0:11   7500         18750
                  Wi2/0/0:1    7500         18750
                  Wi2/0/0:2    7500         0
2/0/0    12       In2/0/0:12   7500         37500
                  Wi2/0/0:2    7500         0
                  Wi2/0/0:3    7500         0
2/0/0    13       In2/0/0:13   7500         37500
                  Wi2/0/0:2    7500         0
                  Wi2/0/0:3    7500         0
```

- **show controllers Integrated-Cable** *slot/subslot/port***bandwidth wb-channel**：ワイドバンドチャネルの帯域幅情報を表示します。

  次に、コマンドの出力例を示します。

```
Router# show controllers Integrated-Cable 2/0/0 bandwidth wb-channel

Ctrlr    WB       RF         CIR(Kbps)    Guar(Kbps)
2/0/0    0                   60000        102500
                  2/0/0:0    7500         13750
                  2/0/0:1    7500         13750
                  2/0/0:2    7500         12500
                  2/0/0:3    7500         12500
                  2/0/0:4    7500         12500
                  2/0/0:5    7500         12500
                  2/0/0:6    7500         12500
                  2/0/0:7    7500         12500
2/0/0    1                   82500        170000
                  2/0/0:0    3750         10000
                  2/0/0:1    3750         10000
                  2/0/0:2    7500         12500
                  2/0/0:3    7500         12500
                  2/0/0:4    7500         12500
                  2/0/0:5    7500         12500
                  2/0/0:6    7500         12500
                  2/0/0:7    7500         12500
                  2/0/0:8    7500         18750
                  2/0/0:9    7500         18750
                  2/0/0:10   7500         18750
                  2/0/0:11   7500         18750
                  2/0/0:32   0            0
                  2/0/0:33   0            0
                  2/0/0:34   0            0
                  2/0/0:35   0            0
2/0/0    2                   60000        0
                  2/0/0:8    7500         0
                  2/0/0:9    7500         0
                  2/0/0:10   7500         0
                  2/0/0:11   7500         0
                  2/0/0:12   7500         0
                  2/0/0:13   7500         0
                  2/0/0:14   7500         0
                  2/0/0:15   7500         0
                  2/0/0:64   0            0
                  2/0/0:65   0            0
                  2/0/0:66   0            0
                  2/0/0:67   0            0
```

- **show controllers Integrated-Cable** *slot/subslot/port***mapping rf-channel**：RF チャネルのマッピングを表示します。

  次に、コマンドの出力例を示します。

```
Router# show controllers integrated-Cable 2/0/0 mapping rf-channel

Ctrlr    RF       IC %       IC Rem     WB         WB %       WB Rem
2/0/0    0        20         1          2/0/0:0    20         1
```

```
                                        2/0/0:1     10        1
2/0/0     1         20          1       2/0/0:0     20        1
                                        2/0/0:1     10        1
2/0/0     2         20          1       2/0/0:0     20        1
                                        2/0/0:1     20        1
2/0/0     3         20          1       2/0/0:0     20        1
                                        2/0/0:1     20        1
2/0/0     4         20          1       2/0/0:0     20        1
                                        2/0/0:1     20        1
2/0/0     5         20          1       2/0/0:0     20        1
                                        2/0/0:1     20        1
2/0/0     6         20          1       2/0/0:0     20        1
                                        2/0/0:1     20        1
2/0/0     7         20          1       2/0/0:0     20        1
                                        2/0/0:1     20        1
2/0/0     8         20          1       2/0/0:1     20        1
                                        2/0/0:2     20        1
2/0/0     9         20          1       2/0/0:1     20        1
                                        2/0/0:2     20        1
2/0/0     10        20          1       2/0/0:1     20        1
                                        2/0/0:2     20        1
```

- **show controllers Integrated-Cable** *slot/port/interface-number***mapping wb-channel**：ワイドバンドチャネルのマッピングを表示します。

  次に、コマンドの出力例を示します。

```
Router# show controllers integrated-Cable 2/0/0 mapping wb-channel

Ctrlr     WB        RF          WB %    WB Rem
2/0/0     0         2/0/0:0     20      1
                    2/0/0:1     20      1
                    2/0/0:2     20      1
                    2/0/0:3     20      1
                    2/0/0:4     20      1
                    2/0/0:5     20      1
                    2/0/0:6     20      1
                    2/0/0:7     20      1
2/0/0     1         2/0/0:0     10      1
                    2/0/0:1     10      1
                    2/0/0:2     20      1
                    2/0/0:3     20      1
                    2/0/0:4     20      1
                    2/0/0:5     20      1
                    2/0/0:6     20      1
                    2/0/0:7     20      1
                    2/0/0:8     20      1
                    2/0/0:9     20      1
                    2/0/0:10    20      1
                    2/0/0:11    20      1
                    2/0/0:32    20      1
                    2/0/0:33    20      1
                    2/0/0:34    20      1
                    2/0/0:35    20      1
2/0/0     2         2/0/0:8     20      1
                    2/0/0:9     20      1
                    2/0/0:10    20      1
                    2/0/0:11    20      1
                    2/0/0:12    20      1
                    2/0/0:13    20      1
                    2/0/0:14    20      1
                    2/0/0:15    20      1
                    2/0/0:64    20      1
                    2/0/0:65    20      1
                    2/0/0:66    20      1
                    2/0/0:67    20      1
2/0/0     3         2/0/0:12    20      1
                    2/0/0:13    20      1
                    2/0/0:14    20      1
                    2/0/0:15    20      1
                    2/0/0:16    20      1
```

```
2/0/0:17    20      1
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco CMTS ケーブル コマンド	『*Cisco CMTS Cable Command Reference*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

動的帯域幅共有に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *181*：動的帯域幅共有に関する機能情報

機能名	リリース	機能情報
動的帯域幅共有	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 75 章

モジュラ Quality of Service コマンドライン インターフェイスの QoS

このモジュールでは、モジュラ Quality of Service（QoS）コマンドライン インターフェイス（CLI）（MQC）を使用した QoS 機能の適用に関する概念と、MQC の設定タスクについて説明します。MQC を使用すると、トラフィック クラスの定義、トラフィック ポリシー（ポリシー マップ）の作成、およびインターフェイスへのトラフィック ポリシーの適用が可能になります。トラフィック ポリシーには、トラフィック クラスに適用する QoS 機能が含まれます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。この

モジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *182*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

MQC を使用した QoS 機能の適用に対する制約事項

MQC ベースの QoS は、Internetwork Packet Exchange（IPX）、DECnet、AppleTalk などとは異なり、レガシー レイヤ 2 プロトコル パケットの分類をサポートしません。このタイプのパケットが一般的なレイヤ 2 トンネリング メカニズムによって転送されると、パケットは MQC により処理されますが、プロトコル分類はされません。その結果、レイヤ 2 トンネルのレガシー プロトコル トラフィックは、「match any」クラスまたは class-default によってのみ照合されます。

サポートされる QoS ポリシー マップとクラス マップの数は、プラットフォームとリリースにより異なります。

（注） ポリシーマップの制限は、適用されるポリシーマップのインスタンスの数ではなく、ポリシーマップの定義を参照します。

概要

MQC 構造

MQC（モジュラ QoS コマンドライン インターフェイス（CLI））では、QoS グループ値に基づいてパケット分類とマーキングを設定できます。MQC CLI では、トラフィック クラスおよびポリシーを作成し、QoS機能（パケット分類など）をイネーブルにして、それらのポリシーをインターフェイスに適用することができます。

MQC 構造では、エンティティ（トラフィック クラス、ポリシー マップ、サービス ポリシー）を開発する必要があります。

トラフィック クラスの要素

トラフィック クラスに含まれる 3 つの主な要素は、トラフィック クラス名、一連の **match** コマンド、およびトラフィック クラスで複数の **match** コマンドが使用される場合にそれらの **match** コマンドを評価する方法です。

match コマンドは、パケットを分類するために使用します。パケットがチェックされ、**match** コマンドで指定された条件を満たすかどうかが判断されます。パケットが指定された条件を満たしている場合、パケットはそのクラスのメンバーと見なされます。一致条件を満たしていないパケットは、デフォルト トラフィック クラスのメンバーとして分類されます。

利用可能な match コマンド

次の表に、MQC で使用できる **match** コマンドの一部を示します。使用可能な **match** コマンドは、Cisco IOS XE のリリースによって異なります。コマンドおよびコマンド シンタックスの詳細については、『*Cisco IOS Quality of Service Solutions* Command Reference』を参照してください。

表 *183* : *MQC* で使用可能な *match* コマンド

コマンド	目的
matchaccess-group	指定したアクセスコントロールリスト（ACL）に基づいて、クラスマップの一致基準を設定します。
matchany	すべてのパケットに対して適切に一致する基準となる、クラス マップの一致基準を設定します。
matchcos	レイヤ 2 サービス クラス（CoS）マーキングに基づいてパケットを照合します。
matchdestination-addressmac	宛先 MAC アドレスを一致条件として使用します。
matchdiscard-class	特定の廃棄クラスのパケットを照合します。
match [**ip**] **dscp**	特定の IP Diffserv コード ポイント（DSCP）値を一致条件として識別します。1 つの match 文に最大 8 つの DSCP 値を含めることができます。
matchinput-interface	指定された入力インターフェイスを一致基準として使用するクラス マップを設定します。
matchiprtp	Real-Time Transport Protocol（RTP）ポートを一致条件として使用するようにクラスマップを設定します。
matchmplsexperimental	指定されたマルチプロトコル ラベル スイッチング（MPLS）の EXP フィールドの値を一致基準として使用するクラスマップを設定します。
matchmplsexperimentaltopmost	最上位ラベル内の MPLS EXP 値を照合します。

コマンド	目的
matchnot	成功しない一致基準として使用する、1 つの一致基準値を指定します。 （注） **matchnot** コマンドは、一致基準として使用する特定の match パラメータを指定する代わりに、パケットがクラスのメンバーとして分類されるのを防ぐ一致基準を指定するために使用します。たとえば、トラフィック クラスの設定中に **matchnotqos-group6** コマンドを発行すると、QoS グループ 6 だけが、成功する一致基準として考慮されない QoS グループ値となります。他の QoS グループ値は成功する一致基準となります。
matchpacketlength	IP ヘッダー中のレイヤ 3 パケット長をクラスマップ中の一致条件として指定します。
matchport-type	トラフィックを、クラス マップのポート タイプに基づいて照合します。
match [ip] precedence	IP precedence 値を一致基準として識別します。
matchprotocol	指定されたプロトコルに基づいて、クラスマップの一致基準を設定します。 （注） 個別の **matchprotocol** (NBAR) コマンドを使用すると、Network-Based Application Recognition（NBAR）が認識しているプロトコル タイプでトラフィックを照合するように NBAR を設定できます。
matchprotocolfasttrack	FastTrack ピアツーピア トラフィックを照合するように NBAR を設定します。
matchprotocolgnutella	Gnutella ピアツーピア トラフィックを照合するように NBAR を設定します。
matchprotocolhttp	URL、ホスト、多目的インターネット メール拡張（MIME）タイプ、HTTP パケット ヘッダー内のフィールドによってハイパーテキスト転送プロトコル（HTTP）トラフィックを照合するように NBAR を設定します。

コマンド	目的
matchprotocolrtp	RTP トラフィックを照合するようにNBARを設定します。
matchqos-group	特定のQoSグループ値を一致基準として識別します。
matchsource-addressmac	送信元 MAC アドレスを一致基準として使用します。

1 つのトラフィック クラスでの複数の match コマンド

トラフィック クラスに複数の **match** コマンドが含まれている場合、それらの **match** コマンドの評価方法を指定する必要があります。指定するには、**class-map** コマンドの **match-any** キーワードまたは **match-all** キーワードを使用します。**match-any** キーワードと **match-all** キーワードついては、次の点に注意してください。

- **match-any** キーワードを指定した場合、トラフィック クラスによって評価されるトラフィックは、指定した基準の *1* つに一致する必要があります。
- **match-all** キーワードを指定した場合、トラフィック クラスによって評価されるトラフィックは、指定したすべての基準に一致する必要があります。
- どちらのキーワードも指定しない場合、トラフィック クラスによって評価されるトラフィックは、指定したすべての基準に一致する必要があります（つまり、**match-all** キーワードの動作が適用されます）。

トラフィック ポリシーの要素

トラフィック ポリシーには、トラフィック ポリシー名、トラフィック クラス（**class** コマンドで指定）、QoS 機能をイネーブルにするために使用するコマンドの 3 つの要素が含まれています。

ポリシー マップをインターフェイスに適用すると（**service-policy** コマンドを使用）、トラフィック ポリシー（ポリシー マップ）は、イネーブルにした QoS 機能をトラフィック クラスに適用します。

（注） パケットは、トラフィック ポリシー内のいずれかのトラフィック クラスだけに一致します。パケットがトラフィック ポリシー内の複数のトラフィック クラスに一致する場合、ポリシーで定義されている最初のトラフィック クラスが使用されます。

QoS 機能をイネーブルにするために使用するコマンド

QoS 機能をイネーブルにするために使用するコマンドは、Cisco IOS XE リリースごとに異なります。以下の表に、使用可能なコマンドとそれによってイネーブルになる QoS 機能の一部を示します。コマンド構文の詳細については、『*Cisco IOS QoS Command Reference*』を参照してください。

イネーブルにする特定の QoS 機能の詳細については、『Cisco IOS XE Quality of Service Solutions Configuration Guide』の適切なモジュールを参照してください。

表 *184*：*QoS* 機能をイネーブルにするために使用するコマンド

コマンド	目的
bandwidth	クラスの最小帯域幅保証を設定します。
bandwidthremaining	クラスの過剰重量を設定します。
fair-queue	トラフィック クラス内のフローベースのキューイング機能をイネーブルにします。
fair-queue pre-classify	**qos pre-classify** コマンドを設定し、それを均等化キューに使用できるかどうかを確認します。トンネル インターフェイスで **qos pre-classify** コマンドが有効にされた後、**fair-queue pre-classify** コマンドがポリシー マップ用に有効にされると、ポリシー マップはトンネル インターフェイスまたは物理インターフェイスのいずれかに関連付けられます。 均等化キューのハッシュ アルゴリズムには、トンネルの内部 IP ヘッダーが使用されます。
drop	指定したトラフィック クラスのパケットを廃棄します。
police	トラフィック ポリシングを設定します。
police(percent)	インターフェイスで利用可能な帯域幅の割合に基づいてトラフィック ポリシングを設定します。
police(tworates)	認定情報レート（CIR）と最大情報レート（PIR）の 2 つのレートを使用したトラフィック ポリシングを設定します。
priority	ポリシーマップに属するトラフィックのクラスにプライオリティを与えます。

コマンド	目的
queue-limit	ポリシーマップで設定されているクラスに対してキューが保持できるパケットの最大数を指定または変更します。
random-detect	重み付けランダム早期検出（WRED）をイネーブルにします。
random-detectdiscard-class	ポリシー マップ内のクラスの discard-class 値に対し、WRED パラメータを設定します。
random-detectdiscard-class-based	パケットの廃棄クラス値に基づく WRED を設定します。
random-detectexponential-weighting-constant	クラス用に予約されたキューの平均キューサイズ計算用の指数加重係数を設定します。
random-detectprecedence	ポリシーマップ内のクラスポリシーに対する、特定の IP precedence の WRED パラメータを設定します。
service-policy	一致基準として使用するトラフィック ポリシーの名前を指定します（トラフィック ポリシーを互いにネストさせるため（階層型トラフィック ポリシー））。
setatm-clp	ポリシーマップを設定するときのセル損失率優先度（CLP）ビットを設定します。
setcos	送信パケットのレイヤ 2 サービス クラス（CoS）値を設定します。
setdiscard-class	discard-class 値でパケットをマークします。
set[**ip**] **dscp**	タイプ オブ サービス（ToS）バイト内の DiffServ コード ポイント（DSCP）値を設定することでパケットをマークします。
setfr-de	インターフェイスから送信されるすべてのトラフィックに対し、フレームリレーフレームのアドレス フィールドの廃棄適性（DE）ビット設定を 1 に変更します。

コマンド	目的
setmplsexperimental	パケットが指定したポリシーマップに一致する場合に MPLS ビットを設定する値を指定します。
setprecedence	パケット ヘッダーに precedence 値を設定します。
setqos-group	後でパケットを分類するために使用できる QoS グループ ID を設定します。
shape	指定したアルゴリズムに従って、指示されたビット レートまでトラフィックをシェーピングします。

ネストしたトラフィック クラス

MQC では、必ずしも 1 つのトラフィック クラスだけを 1 つのトラフィック ポリシーに関連付ける必要はありません。

パケットが複数の一致基準を満たしているシナリオでは、MQC により複数のトラフィック クラスを 1 つのトラフィック ポリシー（ネストしたトラフィック クラスとも呼ぶ）に関連付けることができます。これを行うには、**matchclass-map** コマンドを使用します（これらをネストしたクラス マップまたは *MQC* 階層型クラス マップと呼びます）。 このコマンドで、1 つのトラフィック クラス内で match-any 特性と match-all 特性を組み合わせる唯一の方法が提供されます。これを実行することにより、1 つの一致基準評価命令（match-any と match-all のどちらか）を使用してトラフィック クラスを作成して、そのトラフィック クラスを別の一致基準タイプを使用するトラフィック クラス内に一致基準として使用できます。たとえば、match-any 命令を使用して作成したトラフィック クラスは match-all 命令を一致基準として使用して設定したクラスを使用する必要があり、その逆の場合も同様です。

考えられるシナリオは次のとおりです。A、B、C、および D が、すべて異なる一致基準であるとし、A、B、または C かつ D（A または B または（C かつ D））に一致するトラフィックをトラフィック クラスに属するものとして分類するとします。ネストしたトラフィック クラスがない場合、トラフィックがトラフィック クラスの一部であると見なされるためには、4 つの一致基準すべてに一致するか（A かつ B かつ C かつ D）、いずれかの一致基準に一致する必要があります（A または B または C または D）。「かつ」（match-all）文と「または」（match-any）文をトラフィック クラス内で組み合わせることはできないため、目的の設定を実現できません。

解決策：C と D に対して match-all を使用する 1 つのトラフィック クラスを作成し（これを条件 E と呼びます）、A、B、E を使用して新しい match-any トラフィック クラスを作成します。新しいトラフィック クラスの評価順序は正しくなります（A または B または E、つまり A または B または（C かつ D））。

class-map コマンドの match-all キーワードと match-any キーワード

トラフィック クラスを作成するときに使用するコマンドの 1 つが **class-map** コマンドです。**class-map** コマンドのコマンド シンタックスには、2 つのキーワード **match-all** と **match-any** が含まれています。**match-all** キーワードと **match-any** キーワードの指定が必要になるのは、トラフィック クラスで複数の一致条件を設定する場合だけです。これらのキーワードについて、次の点に注意してください。

- 指定したトラフィック クラスにパケットを分類するために、トラフィック クラス内のすべての一致基準に一致する必要がある場合、**match-all** キーワードを使用します。
- 指定したトラフィック クラスにパケットを分類するために、トラフィック クラス内の *1* つの一致基準だけに一致する必要がある場合に、**match-any** キーワードを使用します。
- **match-all** キーワードも **match-any** キーワードも指定しない場合、トラフィック クラスの動作は、**match-all** キーワードを指定した場合と同じになります。

service-policy コマンドの input および output キーワード

一般的な規則として、トラフィック ポリシーで設定する QoS 機能は、インターフェイスで受信されるパケットか、インターフェイスで送信されるパケットに適用できます。そのため、**service-policy** コマンドを使用する場合は、**input** キーワードまたは **output** キーワードを使用してトラフィック ポリシーの方向を指定する必要があります。

たとえば、**service-policyoutputpolicy-map1** コマンドは、トラフィック ポリシーの QoS 機能を出力方向のインターフェイスに適用します。インターフェイス（出力）から送信されるすべてのパケットが、policy-map1 という名前のトラフィック ポリシーで指定された基準に従って評価されます。

（注） Cisco のリリースでは、キューイング メカニズムは入力方向ではサポートされていません。非キューイング メカニズム（トラフィック ポリシングやトラフィック マーキングなど）は、入力方向でサポートされています。また、送信元 MAC アドレスに基づくトラフィックの分類（**matchsource-addressmac** コマンドを使用）は、入力方向でのみサポートされています。

MQC を使用して QoS 機能を適用することの利点

MQC 構造では、一度トラフィック ポリシー（ポリシー マップ）を作成すると、必要な数のトラフィック クラスに適用できます。また、トラフィック ポリシーを必要な数のインターフェイスに適用できます。

MQC を使用した QoS 機能の適用方法

トラフィック クラスの作成

トラフィック クラスを作成するには、**class-map** コマンドを使用してトラフィック クラス名を指定します。次に、1 つ以上の **match** コマンドを使用して、適切な一致基準を指定します。指定した基準に一致するパケットがトラフィック クラスに分類されます。class-map コマンドの **match-all** キーワードと **match-any** キーワードの詳細については、「class-map コマンドの match-all キーワードと match-any キーワード」の項を参照してください。

（注） **matchcos** コマンドはステップ 4 に記載されています。**matchcos** コマンドは、使用できる **match** コマンドの 1 つに過ぎません。他の利用可能な **match** コマンドについては、「class-map コマンドの match-all キーワードと match-any キーワード」の項を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**class-map** [**match-all**| **match-any**] *class-map-name* 例： `Router(config)# class-map match-any class1`	クラス マップで使用するクラスを作成し、クラス マップ コンフィギュレーション モードを開始します。 • クラスマップは、パケットを指定したクラスに照合するために使用します。 • クラス名を入力します。

	コマンドまたはアクション	目的
		（注） **match-all** キーワードは、すべての一致基準が満たされることが必要であることを指定します。**match-any** キーワードは、いずれかの一致条件が満たされることが必要であることを指定します。これらのキーワードは、複数の **match** コマンドを指定する場合にだけ使用します。
ステップ 4	**matchcos** *cos-number* 例： `Router(config-cmap)# match cos 2`	レイヤ 2 サービスクラス（CoS）番号に基づいてパケットを照合します。 • CoS 番号を入力します。 （注） **matchcos** コマンドは、使用できる **match** コマンドの一例です。他の利用可能な **match** コマンドについては、「class-map コマンドの match-all キーワードと match-any キーワード」の項を参照してください。
ステップ 5	必要に応じて追加の match コマンドを入力します。追加のコマンドが不要な場合はステップ 6 に進みます。	--
ステップ 6	**end** 例： `Router(config-cmap)# end`	（任意）QoS class-map コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トラフィック ポリシーの作成

（注） **bandwidth** コマンドはステップ 5 に記載されています。**bandwidth** コマンドは、QoS 機能を有効にするためにポリシー マップで使用できるコマンドの一例です（ここでは、クラスベース均等化キューイング（CBWFQ））。利用可能なその他のコマンドの詳細については、「トラフィック ポリシーの要素」セクションを参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**policy-map** *policy-map-name* 例： `Router(config)# policy-map policy1`	トラフィック ポリシーの名前を作成または指定し、QoS ポリシーマップ コンフィギュレーション モードを開始します。 • ポリシー マップ名を入力します。
ステップ 4	**class** {*class-name*| **class-default**} 例： `Router(config-pmap)# class class1`	トラフィック クラスの名前を指定し、QoSポリシーマップ クラス コンフィギュレーション モードを開始します。 （注） この手順により、トラフィック クラスがトラフィック ポリシーに関連付けられます。
ステップ 5	**bandwidth** {*bandwidth-kbps* | **percent** *percent*} 例： `Router(config-pmap-c)# bandwidth 3000`	（任意）トラフィック クラスに対する輻輳期間中の最小帯域幅保証を指定します。 • 最小帯域幅保証は、kb/s 単位か、使用可能な全帯域幅のパーセンテージで指定します。 （注） **bandwidth** コマンドを使用すると CBWFQ がイネーブルになります。**bandwidth** コマンドは、QoS 機能をイネーブルにするためにポリシーマップで使用できるコマンドの一例です。利用可能なその他のコマンドの詳細については、「トラフィック ポリシーの要素」セクションを参照してください。
ステップ 6	イネーブルにする追加の QoS 機能に対するコマンドを入力します。他に QoS 機能が必要ない場合は、ステップ 7 に進みます。	--

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Router(config-pmap-c)# end`	（任意）QoS ポリシーマップ クラス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

MQC を使用したインターフェイスへのトラフィック ポリシーの適用

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface** *type number* 例： `Router(config)# interface TenGigabitEthernet 4/1/0`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。 • インターフェイス タイプとインターフェイス番号を入力します。
ステップ 4	**service-policy**{**input** | **output**} *policy-map-name* 例： `Router(config-if)# service-policy input policy1`	ポリシー マップをインターフェイスに付加します。 • **input** キーワードまたは **output** キーワードとポリシー マップ名を入力します。
ステップ 5	**end** 例： `Router(config-if)# end`	（任意）インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

トラフィック クラスとトラフィック ポリシー情報の確認

ここで取り上げる show コマンドはいずれも任意で使用します。また、入力順も任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**showclass-map** 例： `Router# show class-map`	（任意）すべてのクラス マップとその一致条件を表示します。
ステップ 3	**showpolicy-map** *policy-map-name* **class** *class-name* 例： `Router# show policy-map policy1 class class1`	（任意）指定したポリシー マップの指定したクラスの設定を表示します。 • ポリシー マップ名とクラス名を入力します。
ステップ 4	**showpolicy-map** 例： `Router# show policy-map`	（任意）存在するすべてのポリシー マップのすべてのクラスの設定を表示します。
ステップ 5	**showpolicy-mapinterface** *type number* 例： `Router# show policy-map interface TengigabitEthernet 4/1/0`	（任意）インターフェイスに適用された入力ポリシーと出力ポリシーの統計情報と設定を表示します。 • インターフェイス タイプと番号を入力します。
ステップ 6	**exit** 例： `Router# exit`	（任意）特権 EXEC モードを終了します。

MQC を使用した QoS 機能の適用の設定例

トラフィック クラスの作成

次の例では、トラフィック クラスを作成し、一致基準を定義します。最初のトラフィック クラス（class1）では、アクセス コントロール リスト（ACL）101 を使用し、2 つめのトラフィック クラス（class2）では ACL 102 を使用します。パケットとこれらの ACL のコンテンツを照合し、そのクラスに属しているかどうかを判断します。

```
class-map class1
  match access-group 101
  exit
class-map class2
  match access-group 102
  end
```

ポリシー マップの作成

次の例では、class1 と class2 の 2 つのクラスに適用する QoS 機能を含むトラフィック ポリシー（policy1）を定義します。これらのクラスの一致基準は、トラフィック クラスの作成, （1244 ページ）ですでに定義されています。

class1 では、帯域幅割り当て要求と、そのクラス用に予約されるキューの最大パケット数の制限がポリシーに含まれています。class2 に対しては、帯域幅割り当て要求だけがポリシーで指定されています。

```
policy-map policy1
  class class1
    bandwidth 3000
    queue-limit 30
    exit
  class class2
    bandwidth 2000
    end
```

例：トラフィック ポリシーのインターフェイスへの適用

次に、既存のトラフィック ポリシーをインターフェイスに適用する例を示します。**policy-map** コマンドを使用してトラフィック ポリシーを定義した後、**service-policy** コマンドをインターフェイス コンフィギュレーション モードで使用して、1 つ以上のインターフェイスに適用できます。同じトラフィック ポリシーを複数のインターフェイスに割り当てることができますが、各インターフェイスには、入力方向と出力方向に対して、それぞれトラフィック ポリシーを 1 つだけ割り当てることができます。

```
Router(config)# interface TengigabitEthernet 4/1/0
Router(config-if)# service-policy output policy1
Router(config-if)# exit
Router(config)# interface TengigabitEthernet 4/1/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
```

match not コマンドの使用

matchnot コマンドを使用して、一致基準として使用していないQoSポリシー値を指定します。その QoS ポリシーの他のすべての値が成功する一致基準となります。たとえば、QoS クラスマップ コンフィギュレーション モードで **matchnotqos-group4** コマンドを発行すると、指定したクラスは、成功する一致基準として 4 を除くすべての QoS グループ値を受け入れます。

次のトラフィック クラスでは、IP 以外のすべてのプロトコルが成功する一致条件と見なされます。

```
class-map noip
  match not protocol ip
  end
```

デフォルト トラフィック クラスの設定

トラフィック クラスで指定された一致条件を満たさないトラフィック（つまり、未分類のトラフィック）は、デフォルト トラフィック クラスに属するものとして扱われます。

デフォルト クラスを設定しない場合でも、パケットはそのクラスのメンバーとして扱われます。デフォルトクラスにはイネーブルになっているQoS機能がないため、このクラスに属するパケットにはQoS機能がありません。そのようなパケットをテール ドロップが管理する先入先出（FIFO）キューに配置します。テールドロップは、すべてのトラフィックを等しく扱ってサービスクラス間での区別はせずに輻輳を回避する手段です。輻輳期間中はキューが一杯になります。出力キューが一杯でテール ドロップがアクティブな場合、輻輳が解消されてキューが一杯でなくなるまでパケットはドロップされます。

次の例では、次の特性を持つデフォルト クラス（常に class-default という名前になります）のポリシー マップ（policy1）を設定します。ポリシーがクラス ポリシー policy1 で定義されている他のクラスの一致基準を満たさないトラフィック用に 10 個のキューがあり、キューあたり 20 個のパケットを超えると、追加でキューに格納されるパケットを処理するためにテール ドロップが実施されます。

次の例では、次の特性を持つデフォルト クラス（常に class-default という名前になる）のポリシー マップ（policy1）を設定します。ポリシーがトラフィック ポリシー policy1 で定義されている他のクラスの一致基準を満たさないトラフィック用に 10 個のキューがあります。

```
policy-map policy1
  class class-default
    shape average 100m
```

「class-map match-any」コマンドと「class-map match-all」コマンドの違い

次に、複数の一致条件がある場合にパケットを評価する例を示します。この例で、**class-mapmatch-any** コマンドと **class-mapmatch-all** コマンドの違いを示します。トラフィック クラスのメンバーと見なされるためには、パケットが一致基準のすべて（**match-all**）を満たすか、または一致基準のいずれか 1 つ（**match-any**）を満たす必要があります。

次に、**class-map match-all** コマンドを使用してトラフィック クラスを設定する例を示します。

```
class-map match-all cisco1
  match qos-group 4
  match access-group 101
```

インターフェイス上に設定されているトラフィック クラス cisco1 を持つルータにパケットが到着した場合、そのパケットが IP プロトコル、QoS グループ 4、およびアクセス グループ 101 に一致するかどうかが評価されます。これらの一致基準がすべて満たされると、パケットはトラフィック クラス cisco1 のメンバーとして分類されます（論理 AND 演算子：IP プロトコル AND QoS グループ 4 AND アクセス グループ 101）。

```
class-map match-all vlan
  match vlan 1
  match vlan inner 1
```

次に、**class-map match-any** コマンドを使用する例を示します。パケットがトラフィック クラスのメンバーとして分類されるには、一致基準の 1 つのみを満たす必要があります（つまり、論理OR 演算子：プロトコル IP OR QoS グループ 4 OR アクセス グループ 101）。

```
class-map match-any cisco2
  match protocol ip
  match qos-group 4
  match access-group 101
```

トラフィック クラス cisco2 では、成功する一致が見つかるまで連続的に一致基準が評価されます。パケットは、まず IP プロトコルを一致基準として使用できるかどうかを判断するために評価されます。使用できる場合、パケットはトラフィック クラス cisco2 に一致します。使用できない場合、QoS グループ 4 は一致基準として評価され、以降も同様に評価されます。パケットが指定したどの条件にも一致しない場合、パケットはデフォルト トラフィック クラス（*class default-class*）のメンバーとして分類されます。

一致基準としてのトラフィック クラス（ネストしたトラフィック クラス）の確立

matchclass-map コマンドを使用する理由は 2 つあります。1 つの理由はメンテナンスです。現在大規模なトラフィック クラスが存在している場合、トラフィック クラス一致基準を使用するほうが、同じトラフィック クラス設定を再入力するよりも簡単です。2 つめのより一般的な理由としては、1 つのポリシー内で match-all と match-any の特性を組み合わせるためです。これにより、1 つの一致基準評価命令（match-any と match-all のどちらか）を使用したトラフィック クラスを作成し、このトラフィック クラスを、異なるタイプの一致基準を使用するトラフィック クラスで一致条件として使用します。

考えられるシナリオは次のとおりです。A、B、C、および D が、すべて異なる一致基準であるとし、A、B、または C かつ D（A または B または（C かつ D））に一致するトラフィックをトラフィック クラスに属するものとして分類するとします。ネストしたトラフィック クラスがない場合、トラフィックがトラフィック クラスの一部であると見なされるためには、4 つの一致基準すべてに一致するか（A かつ B かつ C かつ D）、いずれかの一致基準に一致する必要があります（A または B または C または D）。「かつ」（match-all）文と「または」（match-any）文をトラフィック クラス内で組み合わせることはできないため、目的の設定を実現できません。

解決策：C と D に対して match-all を使用する 1 つのトラフィック クラスを作成し（これを条件 E と呼びます）、A、B、E を使用して新しい match-any トラフィック クラスを作成します。新しいトラフィック クラスの評価順序は正しくなります（A または B または E、つまり A または B または（C かつ D））。

例：メンテナンスのためにネストされたトラフィック クラス

次の例で、トラフィック クラス class1 の特性は、トラフィック クラス class2 の特性とほぼ同じですが、トラフィック クラス class1 では、一致条件として宛先アドレスが追加されています。トラフィック クラス class1 をゼロから設定する代わりに、**matchclass-mapclass2** コマンドを入力できます。このコマンドを使用すると、トラフィック クラス class2 のすべての特性をトラフィック クラス class1 に取り込み、トラフィック クラスを再設定することなく、新しい宛先アドレスの一致基準を追加できます。

```
Router(config)# class-map match-any class2
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 3
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# class-map match-all class1
Router(config-cmap)# match class-map class2
Router(config-cmap)# match destination-address mac 0000.0000.0000
Router(config-cmap)# exit
```

例：match-any特性とmatch-all特性を1つのトラフィッククラスで組み合わせるためのネストしたトラフィック クラス

1 つのトラフィック クラスで match-any 特性と match-all 特性を使用するための唯一の方法は、**matchclass-map** コマンドを使用することです。1 つのクラスに match-any と match-all の特性を組み合わせるには、一致基準に match-all 命令を使用して設定されたクラスを使用するトラフィック クラスを作成する match-any 命令を使用します（**matchclass-map** コマンドを使用）。

次に、2 つのトラフィック クラスの特性を組み合わせる例を示します。1 つは match-any 特性を使用し、1 つは match-all 特性を使用しています。これを、**matchclass-map** コマンドで 1 つのトラフィック クラスとして設定します。その結果、パケットがトラフィック クラス class4 のメンバーと見なされるためには、次の 3 つの一致基準のいずれかを満たしている必要があります。IP プロトコルかつ QoS グループ 4、宛先 MAC アドレス 00.00.00.00.00.00、またはアクセス グループ 2。

この例で、トラフィック クラス class4 だけがトラフィック ポリシー policy1 と共に使用されています。

```
Router(config)# class-map match-all class3
Router(config-cmap)# match protocol ip
Router(config-cmap)# match qos-group 4
Router(config-cmap)# exit
Router(config)# class-map match-any class4
Router(config-cmap)# match class-map class3
Router(config-cmap)# match destination-address mac 00.00.00.00.00.00
Router(config-cmap)# match access-group 2
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
```

```
set-qos-transmit 4
Router(config-pmap-c)# end
```

例：QoS ポリシーとしてのトラフィック ポリシー（階層型トラフィック ポリシー）

QoS ポリシー マップ クラス コンフィギュレーション モードで **service-policy** コマンドを使用すると、トラフィック ポリシーを QoS ポリシー内に含めることができます。トラフィック ポリシーを含むトラフィック ポリシーは、階層型トラフィック ポリシーと呼びます。

階層型トラフィック ポリシーには、1 つの子ポリシーと 1 つの親ポリシーが含まれています。子ポリシーは、以前に定義したトラフィック ポリシーであり、**service-policy** コマンドを使用して新しいトラフィック ポリシーに関連付けられます。既存のトラフィック ポリシーを使用する新しいトラフィック ポリシーが親ポリシーです。ここに示す例では、トラフィック ポリシー child が子ポリシーであり、トラフィック ポリシー parent が親ポリシーです。

階層型トラフィック ポリシーはサブインターフェイスに追加できます。階層型トラフィック ポリシーを使用すると、1 つのトラフィック ポリシー（1 つの子ポリシー 1 つの親のポリシーを持つ）を使用して、サブインターフェイスのシェーピングと優先順位付けを行うことができます。

```
Router(config)# policy-map child
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 50
Router(config)# policy-map parent
Router(config-pmap)# class class-default
Router(config-pmap-c)# shape average 10000000
Router(config-pmap-c)# service-policy child
```

shape コマンドで使用する値は、サービス プロバイダーから通知された認定情報レート（CIR）値からプロビジョニングします。

port-channel インターフェイスの入力 MQC の設定方法

トラフィック フローを区別し、対応する「qos-group」機能を設定するために port-channel インターフェイス上で入力 MQC を設定するには、次に説明する手順に従います。

制約事項

- ポリシング、シェーピング、WRED、キューイングなどの QoS アクションはサポートされていません。
- ケーブルの物理インターフェイスで入力 MQC を設定することはできません。

トラフィック クラスの作成

トラフィック クラスを定義するには、**class-map** コマンドを使用します。トラフィック クラスに含まれる 3 つの主な要素は、名前、一連の **match** コマンド、そしてトラフィック クラスに複数の **match** コマンドが存在する場合に **match** コマンドを評価する方法です。

match コマンドは、パケット分類のためのさまざまな基準を指定するために使用します。パケットが検査されて、**match** コマンドで指定された基準に一致するかどうか判別されます。指定された基準にパケットが一致する場合、そのパケットはクラスのメンバーと見なされ、トラフィック

ポリシーで設定された QoS 仕様に従って転送されます。一致基準を満たさないパケットは、デフォルトのトラフィック クラスのメンバーとして分類されます。

トラフィック クラスを作成して一致基準を定義するには、次の手順に従います。

configure terminal
class-map *class*
match *type*

ポリシー マップの作成

トラフィック クラスの作成後にトラフィック ポリシーを設定すると、これらのクラス内の選択したトラフィックに特定のアクションを適用するためのマーキング機能を設定できます。

トラフィック ポリシーを作成するには、**policy-map** コマンドを使用します。トラフィック ポリシーの目的は、ユーザ指定のトラフィック クラスに分類されたトラフィックに関連付ける QoS 機能を設定することです。

（注） パケットは、トラフィック ポリシー内のいずれかのトラフィック クラスだけに一致します。パケットがトラフィック ポリシー内の複数のトラフィック クラスに一致する場合、ポリシーで定義されている最初のトラフィック クラスが使用されます。

トラフィック ポリシーを定義するには、次の手順を実行します。

configure terminal
policy-map *policy*
class *class*

ポリシー マップでの QoS アクションの定義

ポリシー マップでクラス モードからアクション コマンドを追加できます。

set アクション

set コマンドを使用してトラフィックにマークを付けると、転送パスにある他のネットワーク デバイスが、トラフィック フローに適用する適切なサービス クラスを迅速に判断できるようになります。

set アクションを定義するには、次の手順に従います。

configure terminal
policy-map *policy*
class *class*
set *option*

集約 port-channel インターフェイスの設定

port-channel インターフェイスを設定するには、次の手順に従います。

configure terminal
platform qos port-channel-aggregate *port_channel_number*
interface port-channel *port_channel_number*
ip address *ip musk*
interface *name*
channel-group *number*

トラフィック ポリシーのインターフェイスへの適用

policy-map コマンドを使用してトラフィック ポリシーを定義した後、**service-policy** コマンドをインターフェイス コンフィギュレーション モードで使用して、1 つ以上のインターフェイスに適用できます。同じトラフィック ポリシーを複数のインターフェイスに割り当てることができますが、各インターフェイスには、入力方向と出力方向に対して、それぞれトラフィック ポリシーを 1 つだけ割り当てることができます。

トラフィック ポリシーをインターフェイスに適用するには、次の手順をすべて行います。

configure terminal
interface port-channel *port_channel_number*
service-policy input *policy*

例：port-channel インターフェイスの入力 MQC の設定

以下に、port-channel インターフェイスの入力 MQC を設定する例を示します。

```
Router# configure terminal
Router(config)# class-map class1
Router(config-cmap)# match any
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# set dscp af11
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# platform qos port-channel-aggregate 2 Router(config)# interface port-channel
 2
Router(config-if)# ip address 192.168.0.1 255.255.255.0
Router(config-if)# no shut
Router(config-if)# interface tenGigabitEthernet 4/1/1
Router(config-if)# no ip address
Router(config-if)# no shut
Router(config-if)# channel-group 2
Router(config-if)# interface port-channel 2
Router(config-if)# service-policy input policy1
Device(config-if)# end
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
QoS コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco IOS Quality of Service Solutions Command Reference*』
パケット分類	「Classifying Network Traffic」モジュール
フレーム リレー フラグメンテーション（FRF）PVC	「FRF .20 Support」モジュール
選択的パケット廃棄	「IPv6 Selective Packet Discard」モジュール
スケーリングとパフォーマンスの情報	『Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide』の「Broadband Scalability and Performance」モジュール

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

モジュラ Quality of Service コマンドライン インターフェイスの QoS に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *185*：モジュラ *Quality of Service* コマンドライン インターフェイスの *QoS* に関する機能情報

機能名	リリース	機能情報
モジュラ Quality of Service コマンドライン インターフェイスの QoS	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。
port-channel インターフェイスでのサービス ポリシー	Cisco IOS XE Everest 16.6.1	この機能が Cisco IOS XE Everest 16.6.1上の Cisco cBR シリーズ コンバージド ブロードバンド ルータ に統合されました。

第 76 章

Cisco CMTS ルータ用の DOCSIS 1.1

このマニュアルでは、Data-over-Cable Service Interface Specifications（DOCSIS）1.1 の動作について、Cisco CMTS ルータを設定する方法について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *186* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

DOCSIS 1.1 動作の前提条件

DOCSIS 1.1 動作をサポートするには、ケーブル モデムが DOCSIS 1.1 フィーチャ セットをサポートする必要があります。さらに、Cisco CMTS の電源を投入して設定する前に、以下の点をチェックしてください。

- ネットワークで信頼性の高いブロードバンドデータ伝送がサポートされていることを確認します。使用するプラントは、NTSC または該当する国際ケーブル設備勧告に基づいて、点検され、調整され、認定を受けている必要があります。プラントがすべての DOCSIS ダウンストリームおよびアップストリーム RF 要件を満たしていることを確認します。
- Cisco CMTS が適切なハードウェア インストレーション ガイドの指示に従って設置されていることを確認します。シャーシには、少なくともバックボーン接続を提供する 1 つのポートアダプタと、RF ケーブル TV インターフェイスとして動作する 1 つの Cisco ケーブル ラインカードが搭載されている必要があります。
- その他の必要なヘッドエンドまたは配線ハブ ルーティングおよびネットワーク インターフェイス装置がすべて設置され、設定され、（サポートされているサービスに基づいて）動作できる状態になっていることを確認します。これには、すべてのルータ、サーバ（DHCP、TFTP、ToD）、ネットワーク管理システム、および他の設定または課金システムが含まれます。また、ゲートキーパやゲートウェイを含む IP テレフォニー機器、バーチャル プライベート ネットワーク（VPN）をサポートする場合はバックボーンやその他の機器、ダイヤルアップ アクセス サーバ、電話回線および接続、Telco リターンをサポートする場合はその他の機器なども含まれます。
- DHCP および DOCSIS のコンフィギュレーション ファイルが作成されて適切なサーバに適用され、各ケーブル モデムはその初期化時に DHCP 要求を伝送し、IP アドレスを受信して TFTP および ToD サーバ アドレスを取得し、DOCSIS コンフィギュレーション ファイルをダウンロードできるようになっていることを確認します。さらに任意で、サーバが更新されたソフトウェア イメージを DOCSIS 1.0 および DOCSIS 1.1 ケーブル モデムにダウンロードできることを確認します。
- 顧客宅内機器（CPE）（ケーブル モデムまたはセットトップ ボックス、PC、電話機、またはファクシミリ装置）がネットワークおよびサービスの要件を満たしていることを確認します。
- 適切な周波数を割り当てるために、チャネル計画について理解しておく必要があります。使用するヘッドエンドまたは配線ハブに該当する場合、バンドリングまたは VPN ソリューション セットのおおまかなセットアップ方針を作成します。VoIP サービスに H.323 を使用し、VoIP 対応のケーブル モデム コンフィギュレーション ファイルを設定する場合は、ダイヤル プランに関する情報が必要です。必要に応じて、パスワード、IP アドレス、サブネット マスク、およびデバイス名を取得してください。
- Cisco CMTS と Time-of-Day（ToD）サーバのシステム クロックが同期していることを確認します。同期していない場合、CM のクロックが Cisco CMTS のクロックと一致せず、BPI+ 動作に干渉する可能性があります。特に、ケーブル モデム（CM）のデジタル証明書を適切に検査できなくなります。

これらの前提条件が満たされたら、Cisco CMTS の設定を開始できます。最低限の作業として、Cisco CMTS にホスト名およびパスワードを設定し、ケーブル設備およびネットワーク バックボーン上で IP をサポートできるように Cisco CMTS を設定します。

注意 サービス クラス ベースのプロビジョニングを使用する場合は、ケーブル モデムで接続が試行される前に、Cisco CMTS でサービス クラスを設定する必要があります。サービス クラスを設定するには、**cableserviceclass** コマンドを使用します。

DOCSIS 1.1 動作の制限事項

DOCSIS 1.1 の動作には、次の制限事項があります。

ベースライン プライバシー インターフェイス プラスの要件

ケーブル モデムおよびCMTS の両方で、BPI+ 暗号化および認証がサポートされイネーブルになっている必要があります。さらに、ケーブル モデムには DOCSIS 1.1 および BPI+ 仕様に準拠するデジタル証明書が含まれている必要があります。

また、CMTS と Time-of-day（TOD）サーバのシステム クロックが同期していることを確認します。同期していない場合、CM のクロックが CMTS のクロックと一致せず、BPI+ 動作に干渉する可能性があります。特に、CM のデジタル証明書を適切に検査できなくなります。

（注） CMTS と Time-of-Day（ToD）サーバのシステム クロックが同期していることを確認します。同期していない場合、CM のクロックが CMTS のクロックと一致せず、BPI+ 動作に干渉する可能性があります。特に、CM のデジタル証明書を適切に検査できなくなります。

BPI+ 暗号化マルチキャストは Cisco cBR-8 ルータ上のバンドルされたサブインターフェイスでサポートされません

現在の Cisco IOS-XE リリースは、Cisco cBR-8 ルータ上のバンドルされたケーブル サブインターフェイスでBPI+暗号化マルチキャストの使用をサポートしません。暗号化マルチキャストは、バンドルされたケーブルインターフェイスまたはバンドルされていないケーブルサブインターフェイスでサポートされていますが、サブインターフェイスがCisco cBR-8 ルータでバンドルされている場合はサポートされません。

BPI+ はハイ アベイラビリティ設定でサポートされません

現在の Cisco IOS-XE リリースでは、インターフェイスが N+1（1:n）ハイ アベイラビリティまたは Remote Processor Redundancy Plus（RPR+）ハイ アベイラビリティ冗長性用にも構成されている場合、ケーブル インターフェイスで BPI+ 暗号化マルチキャストの使用をサポートしません。

さらに、BPI+暗号化を必要とするケーブルインターフェイス設定は、現用ケーブルインターフェイスと保護ケーブルインターフェイス間で自動的に同期しないので、現用ケーブルインターフェイスから保護ケーブル インターフェイスへスイッチオーバーした後に BPI+ は自動的にはサポートされません。これに対する回避策は、必要な設定を使用して保護ケーブル インターフェイスを手動で設定することです。

DOCSIS ルート証明書

Cisco CMTS でサポートする DOCSIS ルート CA 証明書は 1 つだけです。

最大バースト サイズ

以前は、無制限値を設定するために、最大連結バーストサイズパラメータをゼロに設定していました。DOCSIS 1.1 環境では、このパラメータは非ゼロ値に設定する必要があり、また DOCSIS 1.0 ケーブル モデム用の最大値は 1522 バイトになります。

ケーブル モデムが最大連結バースト サイズをゼロに登録しようとすると、DOCSIS 1.1 CMTS はケーブル モデムがオンラインになることを拒否します。これにより、DOCSIS 1.0 ケーブル モデムが大容量のデータ パケットを送信することでアップストリームの音声トラフィックに干渉することを防げます。DOCSIS 1.0 がフラグメンテーションをサポートしていない場合、そのようなデータ パケットの伝送により音声トラフィックに不要なジッタが発生する可能性があります。

さらに、DOCSIS 1.1 では、最大送信バースト サイズを 1522 バイトまたは最大連結バースト サイズのどちらか大きい方に設定する必要があります。DOCSIS 1.0 ケーブル モデムに対して、最大連結バースト サイズを 1522 バイトを超える値に設定しないでください。

（注） この変更により、最大連結バーストサイズにゼロ値を設定する DOCSIS コンフィギュレーション ファイルを変更する必要があります。フラグメンテーションがディセーブルでない限り、この制限は DOCSIS 1.1 ケーブル モデムには存在しません。

パフォーマンス

DOCSIS 1.0 ケーブル モデムには、非送信請求許可およびリアルタイム ポーリングなどの、拡張 DOCSIS 1.1 スケジューリング メカニズム用のスケジューリング パラメータを明示的に要求し提供する能力がありません。同じアップストリーム チャネルにある DOCSIS 1.1 ケーブル モデムは、拡張スケジューリング メカニズムの恩恵を受けます。また DOCSIS 1.1 CMTS は、DOCSIS 1.0 ケーブル モデムが同じアップストリーム チャネルにある場合でも、DOCSIS 1.1 ケーブル モデムからの音声トラフィックを適切にサポートできます。

プロビジョニング

DOCSIS 1.1 ケーブル モデム用の TFTP コンフィギュレーション ファイルのフォーマットおよび内容は、DOCSIS 1.0 ケーブル モデム用のファイルとは大きく異なります。DOCSIS 1.0 ケーブル モデム用の DOCSIS 1.0 スタイル コンフィギュレーション ファイル、および DOCSIS 1.1 ケーブル モデム用の DOCSIS 1.1 コンフィギュレーション ファイルを作成するのに、デュアルモード コンフィギュレーション ファイル エディタを使用します。

登録

DOCSIS 1.1 CMTS は、DOCSIS 1.0 ケーブル モデムからの既存の登録のタイプ/長さ/値（TLV）パラメータと、DOCSIS 1.1 ケーブル モデムからの新しいタイプの TLV を処理する必要があります。DOCSIS 1.0 および DOCSIS 1.1 ケーブル モデムは、正常に同じ DOCSIS 1.1 CMTS に登録できます。

DOCSIS 1.1 ケーブル モデムは、明示的にサービス クラス パラメータを要求せずに、CMTS に静的に定義されているサービス クラスの間接的なリファレンスを作成するように設定できます。DOCSIS 1.1 CMTS はこの登録要求を受信すると、登録応答で実際のサービス クラスのパラメータをエンコードして、ケーブル モデムからの DOCSIS 1.1 固有の登録確認応答 MAC メッセージを待機します。

DOCSIS 1.0 ケーブル モデムが DOCSIS 1.1 CMTS に登録する場合、登録要求では明示的に登録内のすべての非デフォルトサービスクラス パラメータが要求されます。間接サービス クラス リファレンスがないために、DOCSIS 1.1 TLV が不要となり、ローカル登録確認応答待機状態を確立する必要がなくなります。

DOCSIS 1.1 CMTS が DOCSIS 1.0 ケーブル モデムから登録要求を受信すると、DOCSIS 1.0 スタイルの登録応答で応答し、ケーブル モデムからの登録確認応答 MAC メッセージの送信を待機しません。

DOCSIS 1.1 に関する情報

DOCSIS 1.1 は、ケーブル ネットワーク用の初期 DOCSIS 1.0 規格の最初のメジャー リビジョンです。初期規格では同軸ケーブル ネットワークでの高品質なデータ トラフィックを提供していましたが、音声やビデオなどのリアルタイム トラフィックの要望により、DOCSIS 仕様に多くの変更が必要になりました。

DOCSIS 1.1 仕様は、DOCSIS 1.0 ネットワークに対して次の機能強化を提供しています。

ベースライン プライバシー インターフェイス プラス

DOCSIS 1.0 では、共有メディア ケーブル ネットワーク全体でユーザ データのプライバシーを保護するため、およびケーブル ネットワークで DOCSIS ベースのデータ転送サービスへの不正アクセスを防止するために、ベースラインプライバシーインターフェイス（BPI）が導入されました。BPI は、ケーブル モデムと CMTS の間を RF インターフェイス全体でトラフィックを暗号化するほか、認証、認可、およびアカウンティング（AAA）機能も含まれます。

BPI は、アクセス コントロール リスト（ACL）、トンネル、フィルタリング、スプーフィングに対する保護をサポートします。また、加入者が無効な送信元 IP アドレスを使用しないように RF サブネットで送信元 ソース IP フィルタリングを構成するコマンドもサポートします。DOCSIS 1.1 では BPI プラス（BPI+）でこれらのセキュリティ機能を強化しています。BPI+ での強化には次の点が含まれます。

- X.509 デジタル証明書はセキュアなユーザの識別および認証を提供します。Cisco CMTS では、自己署名された製造元の証明書と、DOCSIS ルート CA 証明書にチェーンされる証明書の両方をサポートします。
- キー暗号化では、最も重要なアプリケーションに適した 168 ビット Triple DES（3DES）暗号化を使用します。
- PKCS#1 バージョン 2.0 暗号化による 1024 ビット公開キー。
- 暗号化マルチキャストをサポートし、承認済みサービス フローのみが特定のマルチキャスト ブロードキャストを受信するようにします。

- セキュアなソフトウェア ダウンロードにより、サービス プロバイダーはケーブル モデムのソフトウェアをリモートでアップグレードでき、傍受、干渉、改変のリスクをなくします。

連結

連結を使用すると、ケーブルモデムは複数のアップストリームパケットに対して単一のタイムスライス要求を作成でき、アップストリームの単一大規模バーストですべてのパケットを送信できます。連結では、1つの大規模MACデータ フレームの一部として複数のアップストリーム パケットを送信できるため、連結された MAC フレーム全体に対してタイムスロット要求を 1 つのみ作成すればよく、アップストリーム チャネルでのパケット送信遅延を減らすことができます。これにより、TCP 確認応答パケットなど非常に小さなパケットを大量に送信するときに、アップストリーム帯域の浪費を避けることができます。

動的 MAC メッセージ

動的サービス MAC メッセージでは、ケーブル モデムでサービス フローをオン デマンドで動的に作成できます。これらのメッセージは、サービス フローを作成、切断、および変更する上位層メッセージの DOCSIS リンク層に相当します。

DOCSIS 1.1 動的サービス状態マシンは次のメッセージをサポートします。

- 動的サービス追加（DSA）：このメッセージは、新しいサービス フローを作成するために使用されます。
- 動的サービス変更（DSC）：このメッセージは、既存のサービス フローの属性を変更するために使用されます。
- 動的サービス削除（DSD）：このメッセージは、既存のサービス フローを削除するために使用されます。

（注） これらのメッセージは総称で DSX メッセージと呼ばれます。

高度な QoS

DOCSIS 1.1 では、音声やビデオなどのリアルタイム トラフィックを優先するために高度な QoS 機能を提供します。

- DOCSIS 1.0 QoS モデル（QoS プロファイルに関連付けられたサービス ID（SID））は、サービス フローおよびサービス クラス モデルに置き換えられました。これらは、QoS パラメータを異なるタイプへのトラフィックの割り当てや、帯域幅条件の変化に対応する場合に優れた柔軟性を実現します。
- ケーブル モデムごとに複数のサービス フローをサポートするため、1 つのケーブル モデムで、データ、音声、およびビデオの組み合わせをサポートできるようになります。

- 単一方向サービス フローを使用して、ケーブル モデムごとにいずれかの方向における、よりきめ細かい QoS を提供します。
- アップストリーム サービス フローには、使用するトラフィックとアプリケーションのタイプに応じて、次のいずれかの QoS スケジューリング タイプが割り当てられます。
  - Best-effort：品質非保証型のベスト エフォート ベースで送信されるデータ トラフィック。このタイプのサービス フローは、DOCSIS 1.0 ネットワークで使用する方式と類似しています。
  - Real-time polling（rtPS）：ユニキャストで可変サイズのパケットを一定間隔で作成する、ビデオなどのリアルタイムサービス フロー。
  - 非リアルタイム ポーリング サービス（nrtPS）：ケーブル モデムが可変長のデータ バーストを要求する定期的な機会を保証される点では rtPS タイプと類似していますが、ネットワークでのトラフィック量と輻輳量に応じて CMTS がケーブル モデムのポーリング間隔を変えることができる点で異なります。
  - Unsolicited grants（UGS）：固定間隔で固定サイズのパケットを送信するという特徴のある、音声などの固定ビット レート（CBR）または認定情報レート（CIR）トラフィックで、最小データ レートを保証します。
  - Unsolicited Grant with Activity Detection（USG-AD）：UGS と rtPS を組み合わせたもので、（サイレンス サプレッションを使用するような音声など）アクティブでない期間があるようなリアルタイム トラフィックに対応します。このサービス フローでは、アクティブの際に UGS 固定送信を行いますが、アクティブでない期間には rtPS ポーリングに切り替わって、未使用の帯域幅を無駄にしないようにします。

フラグメンテーション

DOCSIS フラグメンテーションでは、アップストリーム MAC スケジューラが UGS（音声スロット）間のスケジュール ギャップに収まるように大きなデータ要求をスライスできます。これにより、大きなデータ パケットが音声やビデオなどのリアルタイム トラフィックに影響を及ぼすのを防ぎます。

フラグメンテーションでは、大きなデータ認可が UGS スロットをプリエンプション処理するときに、UGS スロットで発生するランタイム ジッターが減少します。フラグメンテーションを無効にすると、ランタイム ジッターは増加しますが、フラグメント MAC フレームのフラグメンテーション リアセンブリのオーバーヘッドが低下します。

（注） DOCSIS フラグメンテーションを IP パケットのフラグメンテーションと混同しないでください。IP パケットのフラグメンテーションは、より小さい最大伝送ユニット（MTU）サイズのネットワーク セグメントに合わせるために実行されます。DOCSIS フラグメンテーションは、高優先順位のリアルタイム トラフィック（音声コールなど）に干渉せずに低優先順位のパケットを効率的に送信することを主に考慮したレイヤ2フラグメンテーションです。IP フラグメンテーションは、レイヤ 3 で実行され、異なる最大パケット サイズを使用するルータに対応することを主な目的としています。

相互運用性

DOCSIS 1.1 ケーブル モデムは DOCSIS 1.0 および 1.0+ ケーブル モデムと同一のネットワーク内に共存できます。Cisco CMTS は、各ケーブル モデムに適したサービス レベルを提供します。

ペイロード ヘッダー抑制

ペイロードヘッダー抑制（PHS）は、アップストリームおよびダウンストリームの両サービス フローで反復または冗長パケットヘッダーを抑制することによって、リンク レイヤの帯域幅を節約できます。PHS はサービス フロー単位でイネーブルまたはディセーブルにすることができ、各サービス フローは抑制するヘッダー部分を決定する PHS ルール セットを個別にサポートできます。これにより、各サービス フローおよび特定のタイプのアプリケーションに対して最も効率的な方法で PHS を実行できます。

ダウンストリーム ToS の上書き

ダウンストリーム ToS の上書きは DOCSIS 1.1 でサポートされます。この機能は IPv4 および IPv6 環境で使用できます。ダウンストリーム ToS の上書きを設定するには、CLI コマンド **cableserviceclass** *class-index***tos-overwrite** *and-mask or-mask* またはケーブル モデム コンフィギュレーション ファイルのいずれかを使用できます。

DOCSIS 1.1 QoS

DOCSIS 1.1 QoS フレームワークは次のオブジェクトに基づいています。

- サービス フロー：DOCSIS リンク上の単方向パケット シーケンス。別々のサービス フローがアップストリーム トラフィックとダウンストリーム トラフィックに使用され、そのトラフィックの QoS パラメータを定義します。
- サービス クラス： CMTS によって維持される設定のコレクション。そのサービス クラスに関連付けられたサービスフローが割り当てられたケーブル モデムに対し、特定の QoS サービス層を提供します。

- パケット分類子：分類子が属しているサービス フローへとパケットを分類するために使用される一連のパケット ヘッダー フィールド。CMTS はパケット分類子を使用して、パケットを適切なサービス フローに照合します。
- ペイロード ヘッダー抑制（PHS）ルール：リンク上で送信する前に送信側が抑制する一連のパケット ヘッダー フィールド。受信側は、ヘッダーが抑制されたフレーム伝送を受信した後で、復元します。PHS は、伝送前に繰り返しのあるパケット ヘッダーを削除することで、帯域幅の効率を向上させます。

これらのコンポーネントの詳細については、次の項を参照してください。

サービス フロー

DOCSIS 1.1 では、QoS の基本ユニットはサービス フローです。これは、ケーブル モデムと CMTS との間の RF インターフェイス上で送信されるパケットの単一方向シーケンスです。サービス フローは、遅延、ジッター、スループット保証などの QoS パラメータ セットを定義します。また、これらのパラメータはアップストリームおよびダウンストリーム トラフィック フローに対して個別に適用できます。これは、DOCSIS 1.0 ネットワークとの主な相違点で、1.0 では同一の QoS パラメータがダウンストリームおよびアップストリーム フローの両方に適用されます。

（注） DOCSIS 1.0 ネットワークでは、サービス ID（SID）を使用して特定のフローに設定された QoS パラメータを識別します。DOCSIS 1.1 ネットワークでは、サービス フロー ID（SFID）を使用して特定のアップストリームまたはダウンストリームに割り当てられたサービス フローを識別します。DOCSIS 1.1 ネットワークでも引き続き SID という用語を使用していますが、アップストリーム サービス フローにのみ適用されます。

すべてのケーブル モデムは、アップストリームおよびダウンストリーム フローに対して個別の SFID を持つ、アップストリームおよびダウンストリーム方向のプライマリ サービス フローを確立します。プライマリ フローは、ケーブル モデムと CMTS との接続を維持し、これにより CMTS は MAC 管理メッセージを常にケーブル モデムに送信できます。

さらに、DOCSIS 1.1 ケーブル モデムは複数のセカンダリ サービス フローを確立できます。セカンダリ サービス フローは、（ケーブル モデムにダウンロードされる DOCSIS コンフィギュレーション ファイルに設定することで）固定的に作成することも、音声コールなどのオンデマンド トラフィックのニーズに合うように動的に作成することもできます。固定サービス フローは使用されていなくても継続して有効ですが、動的サービス フローは必要でなくなると削除されます。

指定されたいずれの時点でも、サービス フローは、3 つのステート（[Provisioned]、[Admitted]、[Active]）のいずれかになります。アクティブ フローのみが DOCSIS ネットワークでトラフィックを通過させることができます。すべてのサービス フローは SFID で識別されますが、許可およびアクティブ ステートのアップストリーム サービス フローには、さらにこれらに関連したレイヤ 2 SID があります。SID は、異なるサービス フローにタイム スロット スケジューリングを指定する際に MAC スケジューラが使用する識別子です。

サービス クラス

各サービス フローは 1 つのサービス クラスに関連付けられます。サービス クラスは、サービス フローの最大帯域幅やトラフィックのプライオリティなど、特定のクラスのサービスやその QoS 特性を定義します。サービス クラス属性は、事前設定された CMTS ローカル サービス クラス（クラスベース フロー）から継承されるか、またはケーブル モデムが動的にサービス フローを要求して CMTS がそのサービス フローを作成する際に個別に指定できます。

DOCSIS 1.1 サービス クラスは、サービス フローの MAC レイヤ スケジューリング タイプも定義します。スケジューリング タイプは、ケーブル モデムが作成できるデータ バースト要求のタイプと、そのような要求を実行できる頻度を定義します。次のスケジューリング タイプがサポートされます。

- ベストエフォート（BE）：ケーブル モデムは他のケーブル モデムと帯域幅要求の作成において競合し、データを伝送する前に、CMTS がこれらの要求を認可するのを待機する必要があります。このタイプのサービス フローは、DOCSIS 1.0 ネットワークで使用する方式と類似しています。
- リアルタイム ポーリング サービス（rtPS）：ケーブル モデムは、他のケーブル モデムと競合せずに帯域幅要求を作成できる定期的なタイム スロットを与えられます。これにより、可変長のデータ バーストを持つリアルタイム伝送が可能になります。
- 非リアルタイム ポーリング サービス（nrtPS）：ケーブル モデムは、可変サイズのデータ バーストに対する帯域幅要求を定期的に作成する機会が提供されます。このタイプのフローは、ケーブル モデムが可変長のデータ バーストを要求する定期的な機会を保証される点では rtPS タイプと類似していますが、ネットワークでのトラフィック量と輻輳量に応じて CMTS がケーブル モデムのポーリング間隔を変えることができる点で異なります。
- 非送信請求許可サービス（UGS）：ケーブル モデムは、保証最小データ レートと保証最大ジッター レベルで固定データ バーストを伝送できます。このタイプのサービス フローは、Voice-over-IP（VoIP）コールなどの、認定情報レート（CIR）が必要なトラフィックに適しています。
- アクティビティ検出による非送信請求許可サービス（UGS-AD）：UGS タイプと類似していますが、（誰も話していないときの音声コールなど）ケーブル モデムがサービス フローを使用していないときに CMTS がトラフィックをモニタする点が異なります。CMTS がサービス フローで無音状態を検出すると、CMTS は一時的にサービス フローを rtPS タイプに切り換えます。ケーブル モデムが再びフローを使用し始めると、CMTS はフローを UGS タイプに戻します。これにより、CMTS が VoIP コールをより効率的にサポートできます。

各サービス フローは単一のサービス クラスを割り当てられますが、同じサービス クラスを複数のサービス フローに割り当てることもできます。また、ケーブル モデムに複数のサービス フローを割り当てることもできます。これにより、複数のトラフィック フロー が異なるサービス クラスを使用できるようになります。

パケット分類子

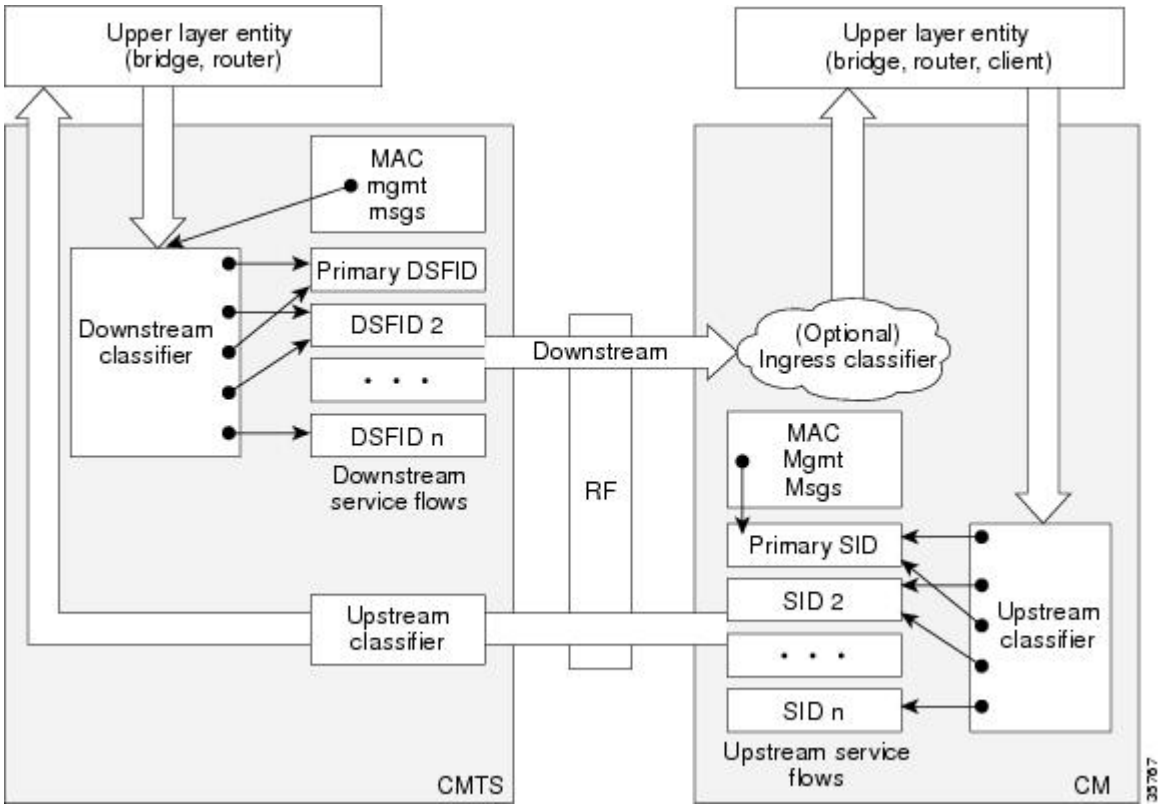
DOCSIS 1.0 ネットワークでは、ケーブル モデムはすべてのトラフィックに 1 つの QoS パラメータ セットのみを使用していたため、CMTS では適切なケーブル モデムで送受信されるパケットをルーティングすることのみが必要でした。しかし、DOCSIS 1.1 ネットワークでは、ケーブル モデムは複数のサービス フローを使用でき、各サービス フローにはさまざまなレベルのサービスが指定されるようになりました。アップストリームおよびダウンストリーム パケットを適切なサービス フローに迅速に割り当てるために、CMTS ではパケット分類子の概念が使用されます。

各パケット分類子は、送信元 MAC アドレス、宛先 IP アドレス、プロトコル タイプなど、1 つ以上のパケット ヘッダーの属性を指定します。分類子はまた、パケットがこの特定の組み合わせのヘッダーに一致したときに使用されるようサービス フローを指定します。ダウンストリームとアップストリームのサービス フローでは異なる分類子が使用されます。

CMTS は、ダウンストリーム パケットおよびアップストリーム パケットを受信すると、各パケットのヘッダーと各パケット分類子の内容を比較します。CMTS は、パケットを分類子に照合した後、パケットに適切な SFID を割り当て、パケットをケーブル モデムに送信するかまたはケーブル モデムから受信します。これにより、パケットは適切なサービス フローに、したがって、適切な QoS パラメータに割り当てられます。

次の図に、パケット分類子のマッピングを示します。

図 *32*：*MAC* レイヤ内の分類子



パケット ヘッダー抑制ルール

多くのデータやリアルタイム アプリケーションはパケット ヘッダー フィールドに固定値を使用する場合があるため、DOCSIS 1.1 は、セッション中にパケットのグループが伝送される際にパケットヘッダーの重複部分を抑制するための PHS をサポートしています。各サービス フローは、ヘッダーのどの部分を抑制するかを決定する個別の PHS ルール セットをサポートできます。

PHS が使用されている場合、送信 CMTS は、サービス フローのすべてのパケットの指定されたヘッダーを抑制します。次いで、受信 CMTS が、最終宛先にパケットを転送する前に、欠落したヘッダーを復元します。

PHS を適切に使用することで、特に、VoIP トラフィックなどの他のプロトコルでカプセル化されたリアルタイム データなどの、パケット化された伝送の効率が増加します。

QoS の比較

このセクションでは、DOCSIS 1.0、DOCSIS 1.0+、DOCSIS 1.1 ネットワーク間の QoS の相違点をまとめます。

（注） Cisco CMTS ルータは、DOCSIS 1.0、DOCSIS 1.0+ 拡張、または DOCSIS 1.1 を実行するケーブル モデムと透過的に相互運用することができます。ケーブル モデムがシステムの初期化時に DOCSIS 1.1 対応であることを表示している場合、Cisco CMTS ルータは DOCSIS 1.1 機能を使用します。ケーブル モデムが DOCSIS 1.1 対応ではなくても DOCSIS 1.0+ QoS 拡張をサポートしている場合、Cisco CMTS はケーブル モデムの動的サービス要求を自動的にサポートします。そうでない場合、ケーブル モデムは、DOCSIS 1.0 デバイスとして扱われます。

DOCSIS 1.0

DOCSIS 1.0 は、ケーブル モデムにダウンロードされている DOCSIS コンフィギュレーション ファイルに事前プロビジョニングされたサービス クラス（CoS）に基づく静的 QoS モデルを使用します。CoS は、アップストリーム方向とダウンストリーム方向の両方に適用される、双方向 QoS プロファイルであり、限定的な制御（いずれかの方向のピーク レート制限など）やアップストリームでの相対的な優先順位を持ちます。

DOCSIS 1.0 は、サービス識別子（SID）の概念を定義します。SID は、ネットワーク上での伝送が許可されているケーブル モデムを識別します。DOCSIS 1.0 ネットワークでは、各ケーブル モデムに対してアップストリーム方向とダウンストリーム方向の両方に割り当てられる SID は 1 つのみであり、ケーブル モデムと SID の間に 1 対 1 の対応関係が作成されます。ケーブル モデムを出入りするすべてのトラフィックは、その SID にマッピングされます。

通常、DOCSIS 1.0 ケーブル モデムには CoS が 1 つあり、すべてのトラフィックが同等に扱われるため、ケーブルモデム上のデータ トラフィックが進行中の音声コールの品質に干渉する可能性があります。ただし、CMTS には IP 参照元タイプ オブ サービス（ToS）ビットに基づいてダウンストリーム トラフィックに優先順位を付ける限定的な機能があります。

たとえば、音声コールが使用する IP プレシデンス ビットが高くなるほど、受け取るキューイング優先度が高くなります（ただしサービスの保証された帯域幅またはレートなし）。DOCSIS 1.0 ケーブル モデムを使用すると、音声コールの帯域幅を永続的に予約することにより音声コールの

品質が高まる可能性があります。ただし、音声コールが進行中ではないときには常にその帯域幅が無駄になります。

DOCSIS 1.0+

リアルタイム トラフィック（音声コールなど）の処理における DOCSIS 1.0 ネットワークの制限を踏まえ、シスコは DOCSIS 1.1+ で期待されていた重要な QoS 強化を提供するために、DOCSIS 1.0+ 拡張を作成しました。特に DOCSIS 1.0+ の強化により、DOCSIS リンク上で基本的な Voice over IP（VoIP）サービスを提供します。

シスコの DOCSIS 1.0+ 拡張には次の DOCSIS 1.1 機能が含まれます。

- ケーブル モデムごとに複数の SID。音声とデータ トラフィックに対して別々のサービス フローを作成します。CMTS およびケーブル モデムは音声トラフィックに高い優先順位を与えることができ、データ トラフィックが音声コールの品質に影響することを防ぎます。
- ケーブル モデムによって開始された動的 MAC メッセージ：動的サービス追加（DSA）と動的サービス削除（DSD）。これらのメッセージを使用すると動的 SID を必要に応じて作成および削除できるため、音声コールに必要な帯域幅をそのコールの発生時に割り当てて、コールが終了したらほかの用途のために解放することができます。
- アップストリームにおける非送信請求許可サービス（CBR スケジューリング）：Cisco uBR925 ケーブル アクセス ルータなどの統合テレフォニー ケーブル モデム（ITCM）からのアップストリーム VoIP パケット用に高品質なチャネルを提供できます。
- パケット内の IP プレシデンス値に基づく、特定のケーブル モデムに対する個別のダウンストリーム レートを提供する機能。同じ ITCM に送信される音声シグナリングとデータ トラフィックを分離して、レート シェーピングに対処できます。
- 連結により、ケーブル モデムは 1 つの大きなバーストで複数のパケットを送信できます。それぞれのパケットに個別の許可要求を行う必要はありません。

注意 すべての DOCSIS 1.0 拡張は、これらの拡張をサポートするケーブル モデムおよび CMTS を使用するときのみ使用できます。ケーブル モデムは、動的 MAC メッセージを送信することで、この拡張の使用を有効にします。DOCSIS 1.0 ケーブル モデムは、CMTS からの DOCSIS 1.0 処理を引き続き受信します。

DOCSIS ネットワークの各バージョンとの相互運用性

DOCSIS 1.1 ケーブル モデムは、以前の DOCSIS 1.0 および 1.0+ モデルに比べて機能が追加され、パフォーマンスも向上していますが、これら 3 つのモデルはすべて同じネットワーク上で共存できます。DOCSIS 1.0 および 1.0+ ケーブル モデムは、DOCSIS 1.1 CMTS のパフォーマンスに悪影響を与えず、DOCSIS 1.1 機能の動作に干渉しません。

次の表に、DOCSIS 1.1 CMTS と他のバージョンのケーブル モデムとの相互運用性を示します。

表 *187* : *DOCSIS 1.1* 相互運用性

対象コンフィギュレーション	結果
DOCSIS 1.1 CMTS と DOCSIS 1.0 ケーブル モデム	DOCSIS 1.0 ケーブル モデムは、DOCSIS 1.0 の機能と能力を発揮できます。可能な場合 BPI がサポートされて、CMTS でイネーブルになります。
DOCSIS 1.1 CMTS と DOCSIS 1.0+ ケーブル モデム	DOCSIS 1.0+ ケーブル モデムは、基本 DOCSIS 1.0 サポートを受けます。可能な場合 BPI がサポートされて、CMTS でイネーブルになります。また、DOCSIS 1.0+ ケーブル モデムは、次の DOCSIS 1.1 機能を発揮します。 • ケーブル モデムごとの複数の SID • ケーブルモデムから発信されたダイナミック サービス MAC メッセージング • アップストリームにおける非送信請求許可サービス（UGS、CBR スケジューリング） • IP プレシデンス値に基づく、特定のケーブル モデムに対する個別のダウンストリーム レート • 連結
DOCSIS 1.1 CMTS と DOCSIS 1.1 ケーブル モデム	DOCSIS 1.1 ケーブル モデムは、このマニュアルに記載されているすべての DOCSIS 1.1 機能を発揮します。可能な場合 BPI+ がサポートされて、CMTS でイネーブルになります。

DOCSIS 1.0 ケーブル モデムの拡張レート帯域幅割り当て（ERBA）サポート

DOCSIS 1.0 ケーブル モデムのダウンストリームで ERBA を定義するには、グローバル コンフィギュレーション モードで cable qos promax-ds-burst コマンドを使用します。

ERBA 機能には、次の拡張機能ごとに特徴があります。

- **cableds-max-burst** コンフィギュレーション コマンドを使用して、Cisco CMTS で [DOCSIS1.1 Downstream Maximum Transmit Burst] パラメータのサポートを有効にします。
- Cisco CMTS で DOCSIS1.0 モデムをマッピングして DOCSIS 1.1 QoS プロファイル パラメータを上書きすると、DOCSIS1.0 モデムで [DOCSIS1.1 Downstream Maximum Transmit Burst] パラメータをサポートできるようになります。

ERBA を使用すると、DOCSIS1.0 モデムは短時間だけ最大ライン レートまで伝送レートを一時的にバーストできます。この機能は、QoS プロファイルの既存のサービス レベルを変更せずに、インターネット ダウンロードの帯域幅要求など、瞬間的な帯域幅要求に対して高帯域幅を提供します。

この機能を使用すると、Cisco CMTS で DOCSIS 1.1 QoS プロファイル パラメータを上書きするようにマッピングして、DOCSIS 1.0 ケーブル モデムのバースト伝送を設定することができます。DOCSIS 1.0 ケーブル モデムは、一致する QoS プロファイルに登録する場合に DOCSIS 1.0 パラメータが必要です。この機能で、ダウンストリームの最大ライン レートをイネーブルにすると、ERBA 設定は、対応する QoS プロファイルに登録されるすべてのケーブル モデムに適用されます。

（注） QoS 定義は、この機能をサポートする Cisco CMTS ヘッドエンドにあらかじめ設定しておく必要があります。

DOCSIS 1.0 ケーブル モデムの ERBA は、次の新しいまたは拡張されたコマンドとキーワードによりサポートされます。

- cable qos pro max-ds-burst burst-size
- show cable qos profile n [verbose]

ERBA の DOCSIS 3.0 ダウンストリーム ピーク トラフィック レート TLV サポート

DOCSIS WFQ スケジューラでは、それぞれのサービス フローが 1 つの専用キューを持つことができます。サービス フローで ERBA が有効な場合、ピーク レートはスケジューラ内のキューシェープ レートとして実装されますが、最大持続レートはトークン バケットのリフィル レートとして設定されます。ERBA がオフのとき、バースト サイズおよびピーク レート値は使用されません。

最大トラフィック バースト パラメータは、サービス フローのバースト継続時間を制御するために使用されます。これにより、最大でチャネル ライン レートまで、または設定済みのピーク レートまで（最大許容バースト サイズ内にあるとき）バーストされます。Cisco cBR-8 コンバージド ブロードバンド ルータでは、この動作を明示的に制御するために **cableds-max-burst** コマンドを使用します。

ERBA 対応サービス フローが使用できるピーク レートを指定するために、*peak-rate* キーワードが導入されました。ピーク レート値は **cableds-max-burst** コマンドの設定後に作成された特定のサービス フローに適用されます。

サービス フローで DOCSIS 3.0 TLV 25.27 が指定されている場合、*peak-rate* 値は TLV 値として設定されます。ただし、ERBA がサービス フローでオンに設定されていない場合には *peak-rate* 値は無視されます。

モデムの登録または動的サービス追加（DSA）操作中、サービス クラス名 TLV 25.4 が送信されて、サービス クラス テンプレートに一致する静的または動的ダウンストリーム サービス フローが作成されます。これらのダウンストリーム サービス フローは、特定のピーク レートを使用して作成されます。

一部の DOCSIS 1.x および DOCSIS 2.0 ケーブル モデムは、DOCSIS 1.x または DOCSIS 2.0 に完全準拠しておらず、登録時に CMTS からダウンストリーム ピーク レート TLV 25.27 を受信したときにオンラインにならないことがあります。この障害を解決するために、DOCSIS1.x および DOCSIS 2.0 ケーブル モデムにピーク トラフィック レート TLV を送信することを制限するようにケーブル サービス属性の withhold-TLVs コマンドを設定します。ピーク レート TLV の抑制方法の詳細については、DOCSIS 3.0 以前のケーブル モデムのアップストリームとダウンストリームのピーク レート TLV の抑制，（1270 ページ）を参照してください。

（注） ERBA 機能は、高優先度のサービス フローおよびマルチキャスト サービス フローには適用できません。

次の表に、Cisco cBR-8 ルータの ERBA サポートを示します。

表 *188*：*Cisco cBR-8* ルータの拡張レート帯域幅割り当てサポート

	ポリサー レート	ポリサーの超過アクション	ポリサーのトークンバケットのサイズ	キュー シェープ レート
従来のサービス フロー	最大持続トラフィック レート（未使用）	送信	CMTS が内部で計算した値（未使用）	最大持続トラフィック レート
ERBA 対応サービス フロー	最大持続トラフィック レート	ドロップ	最大トラフィック バースト TLV	ピーク トラフィック レート

Cisco cBR-8 ルータでは、Cisco cBR-8 CCAP ライン カード上の ERBA をサポートするために、デュアル トークン バケット ベース シェーパーが使用されます（Cisco cBR-8 CCAP ライン カードでは、ERBA 機能は常に有効です）。デュアル トークン バケット シェーパーには、サービス フローごとに 2 つの独立したトークン バケットがあります。一方のバケットの最大レートは MSR に設定され、最大トークンは最大トラフィック バーストに設定されます。もう一方のバケットは、ピーク レートのリフィル レートで設定され、最大トークンはデフォルト レベルの 4 ミリ秒に設定されます。パケットは、2 つのバケットのいずれかが枯渇すると成形されます。

次の表に、Cisco cBR-8 ルータの ERBA デュアル トークン バケット設定を示します。

表 *189*：*ERBA* デュアル トークン バケット設定

	トークンバケット レート（1）	トークンバケット サイズ（1）	トークンバケット レート（2）	トークンバケット サイズ（2）
従来のサービス フロー	最大持続トラフィック レート	4ms * MSR	該当なし	該当なし

	トークンバケット レート（1）	トークンバケット サイズ（1）	トークンバケット レート（2）	トークンバケット サイズ（2）
ERBA 対応サービス フロー	最大持続トラフィック レート	最大トラフィック バースト または 4ms * MSR	ピーク レート	4ms * ピーク レート

DOCSIS 3.0 以前のケーブル モデムのアップストリームとダウンストリームのピーク レート TLV の抑制

DOCSIS 3.0 アップストリーム（US）のピーク レート TLV 24.27 とダウンストリーム（DS）のピーク レート TLV 25.27 は、ケーブル サービス クラス コマンドまたは CM コンフィギュレーション ファイルを使用して Cisco CMTS でイネーブルにします。DOCSIS 1.x と DOCSIS 2.0 の CM は次の TLV をサポートしていません。理想としては、DOCSIS 1.x または DOCSIS 2.0 の CM が登録時にピーク レート TLV を受信する場合、この TLV を無視し、登録を進める必要があります。ただし、古くて規格に準拠していない DOCSIS 3.0 以前の CM がいくつかあります。この CM は、Cisco CMTS からの登録応答でピーク レート TLV を受信すると、オンライン移行に失敗する場合があります。これを解決するために、Cisco CMTS は、DOCSIS 3.0 以前の CM に対して DOCSIS 3.0 ピーク レート TLV を抑制できるようにします。

DOCSIS 3.0 US および DS のピーク レート TLV を抑制するには、グローバル コンフィギュレーション モードで **cableserviceattributewithhold-TLVscommandwiththepeak-rate** コマンドを使用します。設定した場合、このコマンドは、Cisco CMTS が US と DS ピーク レート TLV を DOCSIS 1.x と DOCSIS 2.0 CM に送信するのを制限します。TLV を送信する決定は、登録時に受け取った CM の DOCSIS バージョンに基づいています。登録要求が DOCSIS 3.0 以前の CM から送られた場合、ピーク レート TLV は登録応答で送信されません。ただし、このコマンドにより、DOCSIS 3.0 CM への DOCSIS 3.0 ピーク レート TLV の送信が制限されることはありません。

MAC アドレスを使用したダウンストリーム分類の強化

ケーブル モデムのコンフィギュレーション ファイルで指定されるダウンストリーム分類子は、DOCSIS 仕様に基づいてパケットをサービス フローにマッピングするために使用されます。ダウンストリーム分類子と宛先 MAC アドレスとの新しい組み合わせがサポートされます。この強化により、サービス プロバイダーはダウンストリーム分類子に関連付けられた高優先度のサービス フローの管理を向上できます。たとえば、単一の User Datagram Protocol（UDP）ポートを高優先度のトラフィックと低優先度のトラフィックで共有できます。

ダウンストリーム分類は Cisco CMTS ルータで自動的に有効になります。ルータでサポートされるダウンストリーム分類子は次のとおりです。

組み合わせなし

- IP（IPv4）
- IPv6

- TCP および UDP
- 宛先 MAC

組み合わせあり

- IPv4 + TCP/UDP
- IPv6 + TCP/UDP
- 宛先 MAC + IPv4（宛先 IP アドレスを除く）
- 宛先 MAC + IPv6（宛先 IPv6 アドレスを除く）
- 宛先 MAC + TCP/UDP
- 宛先 MAC + IPv4 + TCP/UDP（宛先 IP アドレスを除く）
- 宛先 MAC + IPv6 + TCP/UDP（宛先 IPv6 アドレスを除く）

利点

DOCSIS 1.1 には、ケーブル ネットワーク上の各種トラフィック（音声、データ、ビデオ）について高度で柔軟な QoS 機能を実現する豊富な機能が用意されています。また、強化されたセキュリティ機能および認証機能を提供します。

ベースライン プライバシー インターフェイス プラスの強化

DOCSIS 1.1 におけるベースライン プライバシー インターフェイスのプラス（+）バージョン（BPI+）では、MAC サブレイヤ内でパフォーマンスおよびシステム セキュリティを高める拡張サービスを提供します。デジタル証明書は、MAC アドレスと IP アドレスに基づいて個人情報盗難を防ぐために、各ケーブルモデムにセキュア認証を提供します。高度な暗号化は、ケーブルモデムと CMTS の間でセキュアなチャネルを提供します。セキュアなソフトウェア ダウンロードは、サービス プロバイダーがケーブル モデム上のソフトウェアをアップグレードでき、ソフトウェア コードの傍受、干渉、改変という脅威がありません。

動的サービス フロー

サービス フローのダイナミックな作成、変更、削除により、レイヤ 2 の帯域幅リソースをオンデマンド予約できます。CMTS では、音声コールまたはビデオ セッション中に、特別な QoS をケーブルモデムに動的に提供できるようになりました。これはケーブルモデムの登録時にリソースを静的にプロビジョニングおよび予約することとは対照的です。これにより、使用可能な帯域幅をより効率的に使用できます。

連結

ケーブル モデムは、複数のアップストリーム パケットを 1 つの大きな MAC データ フレームへと連結します。このためケーブル モデムは、パケットごとにタイムスロットを要求する代わりに、連結された MAC フレーム全体に対するタイムスロット要求を 1 つだけ作成できます。これにより、パケット バースト アップストリーム転送時の遅延が軽減されます。

強化された QoS

CMTS およびケーブル モデムは、広範なスケジューリング パラメータを使用して QoS の要件を伝達し、サービス フロー レベルごとにより高度な QoS を実現できます。

さまざまな新しいタイムスロット スケジューリング分野は、要求アップストリームで保証される遅延とジッターの限界を確保するのに役立ちます。アクティビティ検出では非アクティブなサービス フローにはタイムスロットを発行しないことで、リンク帯域幅の節約に役立ちます。節約した帯域幅は、その他のベスト エフォート データ スロットに再利用できます。

パケット分類は、CMTS およびケーブル モデムがさまざまなタイプのトラフィックをさまざまな DOCSIS サービス フロー レベルまで分離するのに役立ちます。各フローは、CMTS から異なる QoS サービスを受信している可能性があります。

フラグメンテーション

フラグメンテーションは、大きなデータ パケットを分割して、UGS スロット間の短いタイムスロットに収めます。これにより、大きなデータパケットが共有アップストリームチャネル上で送信され、音声に使用されるUGSスロットをプリエンプション処理するときに、音声パケットで生じるジッターを軽減します。

SID ごとに複数のサブフロー

この機能では、ケーブルモデムで単一のハードウェア キューに複数のコールを設定できます。このアプローチは、音声コールごとにケーブルモデムで個別のSIDハードウェア キューが必要となる方法よりもスケーリングに優れています。

ペイロード ヘッダー抑制

ペイロードヘッダー抑制（PHS）では、CMTSとケーブルモデムがパケットヘッダー内で反復部分または冗長部分を抑制してから DOCSIS リンクで送信できます。このため、特に音声のようにヘッダーのサイズが実際のパケットのサイズと変わらなくなるようなタイプのトラフィックにおいて、リンク帯域幅が節約されます。

サービス クラス

DOCSIS 1.1 ネットワークにサービス クラスを使用すると、次の利点があります。

- オペレータは、サービス フローを構成する負担をプロビジョニング サーバから CMTS に移動できます。オペレータは、サービス クラス名を使用してモデムをプロビジョニングします。名前の実装はCMTSで構成されます。これにより、オペレータはモデムのプロビジョニングを変更せずに、特定のサービスの実装をローカル環境に変更できます。たとえば、2 つの異なるCMTSで同じサービスを提供するために、一部のスケジューリングパラメータを異なる設定にする必要がある可能性があります。別の例としては、サービス プロファイルを 1 日の時間に合わせて変更することができます。
- これにより、CMTS ベンダーは必要に応じてクラスベースのキューイングを提供できます。帯域幅に関して、サービスフローはそのクラス内で競争し、クラスは他のクラスと競争します。

- このため、上位層プロトコルではサービス クラス名ごとにサービス フローを作成できます。たとえば、テレフォニー シグナリングは、クラス G.711 の使用可能なプロビジョニングされたサービス フローのインスタンスを作成するようにケーブル モデムに指示できます。

（注） サービス クラスはオプションです。フロー スケジューリングの仕様は常に完全な状態で提供できます。サービス フローはどのサービス クラスにも属さない可能性があります。CMTS の実装では、そのようにクラスに属さないフローが、クラスに属し、同等のパラメータを使用するフローとは異なる処理になることがあります。

DOCSIS 1.1 動作用 Cisco CMTS の設定方法

DOCSIS 1.1 動作の設定タスクについては、次の項を参照してください。一覧内の各作業は、必須と任意に分けています。

（注） ここでは、DOCSIS 1.1 動作用の設定タスクについてのみ説明します。設定全体については、その他の参考資料, （1298 ページ）に示すソフトウェア設定ガイドを参照してください。

ベースライン プライバシー インターフェイスの設定

デフォルトでは、BPI+ 暗号化はすべてのケーブル インターフェイスの 56 ビットの DES 暗号化で有効です。BPI+ 暗号化がすでに無効の場合、または CMTS のケーブル インターフェイスで BPI+ 暗号化を再設定する場合は、次の手順を実行します。

（注） ケーブル インターフェイスの BPI+ 暗号化が無効の場合に、ケーブル モデムが BPI+ 暗号化を使用してそのインターフェイスで登録しようとすると、CMTS はその登録要求を拒否し、エラー メッセージ %CBR-4-SERVICE_PERMANENTLY_UNAVAILABLE を表示します。また、**showcablemodem** コマンドは、MAC ステータス reject(c) でこのケーブル モデムが拒否されたことを示します。

はじめる前に

BPI+ 暗号化は、そのファイル名に「k1」、「k8」、「k9」が含まれる場合、またはフィーチャ セットの説明に BPI が含まれる場合にすべての Cisco CMTS イメージでサポートされます。すべての BPI イメージで、40 ビットおよび 56 ビットの DES 暗号化がサポートされます。

デフォルトでは、BPI+ 暗号化は 56 ビットの DES 暗号化で有効になります。また、ケーブル モデムが DOCSIS 1.1 ソフトウェアを実行している場合、サービス プロバイダーが DOCSIS コンフィギュレーション ファイルの Privacy Enable フィールド（TLV 29）を 0 に設定して無効にしない限り、BPI+暗号化はデフォルトで有効になります。そのため、デフォルト設定を使用する場合は、BPI+ 暗号化を使用できるように CMTS とケーブル モデムの両方が設定されます。

手順

	コマンドまたはアクション	目的

ステップ 1	**enable**
	
	例：
	
	`Router> enable`
	`Router#`
		特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

ステップ 2	**configureterminal**
	
	例：
	
	`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	**interfacecable***slot /subslot /port*
	
	例：
	
	`Router(config)# interface cable 6/0/0`
	
	`Router(config-if)#`
		この特定のスロットでケーブル インターフェイス ライン カードのインターフェイス コンフィギュレーション モードを開始します。

ステップ 4	**cableprivacy**
	
	例：
	
	`Router(config-if)# cable privacy`
	`Router(config-if)#`
		（任意）ケーブル インターフェイス（デフォルト）で BPI+ 56 ビット DES 暗号化を有効にします。

ステップ 5	**cableprivacyaccept-self-signed-certificate**
	
	例：
	
	`Router(config-if)# cable privacy accept-self-signed-certificate`
	`Router(config-if)#`
		（任意）ケーブル モデムでは、DOCSIS ルート証明書と連鎖している製造元の証明書のみを許可するデフォルト設定に対して、自己署名された製造元の証明書を使用して登録できます。
		
		注意 DOCSIS BPI+ 証明書を回避するように上記のコマンドを慎重に使用します。そうしないと、自己署名証明書は、DOCSIS BPI+ 証明書に適合していないケーブル モデムに登録回避策を提供します。この機能は、短期間のトラブルシューティングまたはセキュリティ対策の追加で使用することを目的としています。

	コマンドまたはアクション	目的
		（注） デフォルトでは、CMTS は自己署名証明書を承認しません。デフォルト設定では、ケーブル モデムが自己署名証明書で登録しようとすると、CMTS はケーブルモデムによる登録を拒否します。

ステップ 6	**cableprivacy authorize-multicast**
	
	例：
	
	`Router(config-if)# cable privacy authorize-multicast`
	`Router(config-if)#`
		（任意）ケーブル インターフェイスで BPI+ 暗号化を有効にし、AAA プロトコルを使用して、すべてのマルチキャスト ストリーム（IGMP）参加要求を承認します。
		（注） このコマンドを使用してマルチキャストストリームを許可する場合は、**cableprivacyauthenticate-modem** コマンドを使用してケーブルインターフェイスでも AAA サービスを有効にする必要があります。

ステップ 7	**cableprivacy mandatory**
	
	例：
	
	`Router(config-if)# cable privacy mandatory`
	`Router(config-if)#`
		（任意）DOCSIS コンフィギュレーション ファイルで BPI/BPI+ を有効にしたすべての CM でベースライン プライバシーをアクティブにし、他の CM をオフラインにする必要があります。
		CM の DOCSIS コンフィギュレーション ファイルで BPI を有効にしていない場合は、CM は BPI なしでオンラインになることができます。

ステップ 8	**cableprivacy oaep-support**
	
	例：
	
	`Router(config-if)# cable privacy oaep-support`
	`Router(config-if)#`
		（任意）ケーブル インターフェイスで BPI+ 暗号化を有効にし、Optimal Asymmetric Encryption Padding（OAEP）を有効にします。このオプションは、デフォルトで有効です。このオプションを無効にすると、パフォーマンスに影響を与える可能性があります。

ステップ 9	**cableprivacykek** {**life-time** *seconds* }
	
	例：
	
	`Router(config-if)# cable privacy kek life-time 302400`
	`Router(config-if)#`
		（任意）すべてのケーブル インターフェイスで BPI+ 動作のキーの暗号化キー（KEK）に対する存続時間値を設定します。

	コマンドまたはアクション	目的

ステップ 10	**cableprivacytek** {**life-time** *seconds*}
	
	例：
	
	`Router(config-if)# cable privacy tek life-time 86400`
	`Router(config-if)#`
		（任意）すべてのケーブル インターフェイスで BPI+ 動作のトラフィックの暗号化キー（TEK）に対する存続時間値を設定します。

ステップ 11	**exit**
	
	例：
	
	`Router(config-if)# exit`
	`Router(config)#`
		インターフェイス コンフィギュレーション モードを終了します。
		
		（注） それぞれのケーブル インターフェイスでステップ 3, （1274 ページ）～ステップ 11, （1276 ページ）を繰り返します。

ステップ 12	**exit**
	
	例：
	
	`Router(config)# exit`
	`Router#`
		グローバル コンフィギュレーション モードを終了します。

次の作業

また、各ケーブル モデムの DOCSIS コンフィギュレーション ファイルで BPI+ 動作に次の追加タイマーを設定することもできます。一般的なルールとして、デフォルト値を変更する特別な理由がない限り、DOCSIS コンフィギュレーション ファイルでこれらのタイマーを指定する必要はありません。

表 *190*：各ケーブル モデムの *BPI+* タイマー値

タイマー	説明
許可待機タイムアウト	ケーブル モデムが KEK を最初にネゴシエートする場合に CMTS からの応答を待機する時間。
再許可待機タイムアウト	認証キー（KEK）の存続時間がほぼ満了しているため、ケーブル モデムが新しい KEK をネゴシエートする場合に CMTS からの応答を待機する時間。
許可拒否待機タイムアウト	KEK の最初のネゴシエーションを CMTS が拒否した場合、ケーブル モデムが新しい KEK をネゴシエートする前に待機する必要のある時間。

タイマー	説明
動作待機タイムアウト	ケーブル モデムが TEK を最初にネゴシエートする場合にCMTSからの応答を待機する時間。
キー再生成待機タイムアウト	TEKの存続時間がほぼ満了しているため、ケーブル モデムが新しい TEK をネゴシエートする場合に CMTS からの応答を待機する時間。

CMTS への DOCSIS ルート証明書のダウンロード

DOCSIS 1.1 により、ケーブル モデムは、DOCSIS ルート証明書に関連付けられた製造元の X.509 デジタル チェーン証明書を使用して自分自身を識別できます。DOCSIS ルート証明書は、CMTS ルータのブートフラッシュにすでにインストールされています。ただし、Euro-DOCSIS 証明書など、別のルート証明書をインストールする場合は、証明書をダウンロードし、ブートフラッシュに「euro-root-cert」として保存します。

ヒント Verisign が提供する DOCSIS ルート証明書の詳細については、次の URL の情報を参照してください。http://www.verisign.com/products-services/index.html

（注） DOCSIS ルート証明書と、EuroDOCSIS または PacketCable ルート証明書をロードすることが可能です。EuroDOCSIS PacketCable ルート証明書をブートフラッシュにコピーすることを推奨します。

ネットワーク上のケーブル モデムがチェーン証明書を使用している場合に必要となる、DOCSIS ルート証明書を Cisco CMTS にダウンロードするには、次の手順を実行します。

手順

ステップ 1 DOCSIS 証明書の署名者である Verisign から DOCSIS ルート証明書をダウンロードします。このマニュアルを発行した時点では、DOCSIS ルート証明書は以下の URL からダウンロードすることができます。http://www.verisign.com/products-services/index.html

ステップ 2 Verisign は、圧縮 Zip アーカイブ ファイルで DOCSIS ルート証明書を配布しています。アーカイブから DOCSIS ルート証明書を解凍して CMTS がアクセスできる TFTP サーバにコピーします。
ヒント 他の証明書との混同を避けるために、TFTP サーバに保存する際に、「CableLabs_DOCSIS.509」という名のファイル名をそのまま使用します。

ステップ 3 シリアル ポート接続または Telnet 接続のいずれかを使用して Cisco CMTS にログインします。**enable** コマンドとパスワードを入力して特権 EXEC モードを開始します。

例：

```
Router> enable

Password: <password>
Router#
```

ステップ 4 **dirbootflash** コマンドを使用して、ブートフラッシュにDOCSISルート証明書用の十分な空き容量（約 1,000 バイトのディスク容量）があることを確認します。

例：

```
Router# dir bootflash:

Directory of bootflash:/
    1  -rw-     3229188   Dec 30 2002 15:53:23
cbrsup-universalk9.2015-03-18_03.30_johuynh.SSA.bin
3407872 bytes total (250824 bytes free)
Router#
```

ヒント DOCSISルート証明書のスペースを確保するためにブートフラッシュからファイルを削除する場合、削除ファイルからの空きスペースを再利用するために **squeeze** コマンドを使用することを忘れないでください。

ステップ 5 **copytftpbootflash** コマンドを使用して、DOCSIS ルート証明書をルータのブートフラッシュ メモリにコピーします（ルート証明書として認識するために、ファイル名は CMTS のブートフラッシュで「root-cert」とします）。

例：

```
Router# copy tftp bootflash:

Address or name of remote host []? tftp-server-ip-address

Source filename []? CableLabs_DOCSIS.509

Destination filename [CableLabs_DOCSIS.509]? root-cert

Loading CableLabs_DOCSIS.509 from tftp-server-ip-address (via FastEthernet0/0): !
[OK - 996/1024 bytes]
996 bytes copied in 4.104 secs (249 bytes/sec)
Router#
```

ヒント ルート証明書を PCMCIA フラッシュ ディスク（disk0 または disk1）にもコピーできます。ただし、フラッシュ ディスクにはセキュリティがなくルータから簡単に取り外せるため、動作上およびセキュリティ上の理由からブートフラッシュのルート証明書を保持しておくことを推奨します。

ステップ 6 DOCSIS ルート証明書が正常にブートフラッシュ メモリにコピーされたことを確認します。

例：

```
Router# dir bootflash:

Directory of bootflash:/
    1  -rw-     3229188   Dec 30 2002 15:53:23
cbrsup-universalk9.2015-03-18_03.30_johuynh.SSA.bin
    2  -rw-         996   Mar 06 2002 16:03:46  root-cert
```

```
3408876 bytes total (248696 zxbytes free)
Router#
```

ステップ 7 （任意）BPI+ を使用して最初のケーブル モデムが登録された後、**showcryptocatrustpoints** コマンドを使用して、CMTS が学習したルート証明書を表示できます。

（注） 少なくとも 1 つのケーブル モデムが BPI+ 暗号化を使って CMTS に登録されるまで、**showcryptocatrustpoints** コマンドはルート証明書を表示しません。または、特権 EXEC モードでサポート対象外の **testcablegenerate** コマンドを使用して、強制的に CMTS にルート証明書を登録させることもできます。

例：

```
Router# show crypto ca trustpoints
Root certificate
  Status: Available
  Certificate Serial Number: D54BB68FE934324F6B8FD0E41A65D867
  Key Usage: General Purpose
  Issuer:
    CN = DOCSIS Cable Modem Root Certificate Authority
     OU = Cable Modems
     O = Data Over Cable Service Interface Specifications
     C = US
  Subject Name:
    CN = "BPI Cable Modem Root Certificate Authority "
     OU = DOCSIS
     O = BPI
     C = US
  Validity Date:
    start date: 07:00:00 UTC Mar 27 2001
    end   date: 06:59:59 UTC Jan 1 2007
```

次の作業

ヒント CMTS で学習したすべての証明書（ルート、製造元、CM）を表示するには、**showcryptocacertificates** コマンドを使用します。

信頼できる証明書としての製造元の証明書の追加

DOCSIS 仕様によると、信頼できるまたは信頼できないものとしてマークすることによって、各 CMTS で受け入れられる製造元の証明書と CM 証明書をオペレータが制御できます。次のセクションで説明するように、CLI コマンドまたは SNMP コマンドを使って、Cisco CMTS 上の信頼できる証明書のリストに証明書を追加できます。

（注） ケーブル モデムを構成するために SNMP を使用できない場合、または証明書の追加に CLI コマンドの使用が必要な特定のアプリケーションがある場合を除き、ケーブル モデムに証明書を追加するために SNMP の方法を使用する必要があります。

コマンド ライン インターフェイスを使用した信頼済み証明書としての証明書の追加

CMTS 上の信頼済み証明書のリストに製造元の証明書を追加するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的

ステップ 1	**enable**
	
	例：
	
	`Router> enable`
	`Router#`
		特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

ステップ 2	**configureterminal**
	
	例：
	
	`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	**cableprivacyadd-certificatemanufacturer** *serial-number*
	
	例：
	
	`Router(config)# cable privacy add-certificate manufacturer 000102`
	`Router(config)#`
		（任意）信頼済み証明書として追加する製造元の CA 証明書のシリアル番号を指定します。

ステップ 4	**exit**
	
	例：
	
	`Router(config)# exit`
	`Router#`
		グローバル コンフィギュレーション モードを終了します。

SNMP コマンドを使用した信頼できる証明書として証明書の追加

DOCS-BPI-PLUS-MIB でテーブルと属性を操作することで、証明書を作成して信頼できる証明書の CMTS リストに追加するために SNMP マネージャを使用できます。製造元の証明書を追加するには、docsBpi2CmtsCACertTable テーブルにエントリを追加します。各エントリで次の属性を指定します。

- docsBpi2CmtsCACertStatus：行エントリを作成するために 4 に設定します。
- docsBpi2CmtsCACert：実際の X.509 証明書の 16 進データ（X509Certificate 値）。
- docsBpi2CmtsCACertTrust：証明書の信頼状態を指定する 1 ～ 4 の整数値：1 = 信頼、2 = 非信頼、3 = チェーン、4 = ルート。信頼すべき証明書の場合は 1、ルート証明書で検証される必要があるチェーン証明書の場合は 3 を指定します。

同様に、CM 証明書を信頼できる証明書のリストに追加するには、docsBpi2CmtsProvisionedCmCertTable テーブルにエントリを追加します。各エントリで次の属性を指定します。

- docsBpi2CmtsProvisionedCmCertStatus：行エントリを作成するために 4 に設定します。
- docsBpi2CmtsProvisionedCmCert：実際の X.509 証明書の 16 進データ（X509Certificate 値）。
- docsBpi2CmtsProvisionedCmCertTrust：証明書の信頼状態を指定する 1 ～ 2 の整数値：1 = 信頼、2 = 非信頼。信頼すべき CM 証明書の場合は 1 を指定します。

ヒント　実際の証明書データをロードする前に CertStatus 属性を必ず設定してください。そうでないと、CMTS では証明書がチェーンされていると想定して、ただちに製造元証明書およびルート証明書で検証を試みます。

たとえば、Unix のコマンドライン SNMP ユーティリティを使用して IP アドレス 192.168.100.134 の CMTS 上にある信頼できる証明書のリストに製造元の証明書を追加するには、次のコマンドを入力します（<*index*>値のテーブル エントリを有効なインデックス ポインタで置き換えてください）。

```
% setany -v2c 192.168.100.134 private docsBpi2CmtsCACertStatus.
<index>
 -i 4
 docsBpi2CmtsCACert.
<index>
 -o
 '<hex_data>' docsBpi2CmtsCACertTrust.
<index>
 -i 1
```

CM 証明書で同様の処理を実行するには、次のコマンドを使用します。

```
% setany -v2c 192.168.100.134 private docsBpi2CmtsProvisionedCmCertStatus.
<index>
 -i 4 docsBpi2CmtsProvisionedCmCert.
<index>
 -o
 '<hex_data>' docsBpi2CmtsProvisionedCmCertTrust.
<index>
 -i 1
```

ヒント　ほとんどのオペレーティング システムでは、証明書を指定する 16 桁の 10 進数文字列を入力するために必要なだけの入力行数を受け入れられません。したがって、これらの属性を設定するには、グラフィカルな SNMP マネージャを使用する必要があります。大量の証明書がある場合は、スクリプト ファイルを使用すると便利です。

（注）　自己署名証明書を追加する場合は、CMTS が証明書を受け入れる前に、**cable privacy accept-self-signed-certificate** コマンドも使用する必要があります。

ホットリストへの製造元の証明書または CM 証明書の追加

DOCSIS 仕様によると、この証明書が受け入れられなくなったことを示すために、CMTS 上のホットリスト（別名証明書失効リスト（CRL））に製造元のデジタル証明書または CM デジタル証明書をオペレータが追加できます。これはケーブル モデムの盗難をユーザが報告するとき、またはサービス プロバイダーが特定の製造元のケーブルモデムをサポートしないことを決めたときに、実行できます。

SNMP コマンドを使用したホットリストへの証明書の追加

DOCS-BPI-PLUS-MIB でテーブルと属性を操作することで、証明書を作成してホットリストに追加するために SNMP マネージャを使用できます。製造元の証明書を追加するには、docsBpi2CmtsCACertTable テーブルにエントリを追加します。各エントリで次の属性を指定します。

- docsBpi2CmtsCACertStatus：行エントリを作成するために 4 に設定します。
- docsBpi2CmtsCACert：実際の X.509 証明書の 16 進データ（X509Certificate 値）。
- docsBpi2CmtsCACertTrust：証明書の信頼状態を指定する 1 ～ 4 の整数値：1 = 信頼、2 = 非信頼、3 = チェーン、4 = ルート。証明書をホットリストに追加する際は、この属性を非信頼の 2 に設定します。

同様に、CM 証明書をホットリストに追加するには、docsBpi2CmtsProvisionedCmCertTable テーブルにエントリを追加します。各エントリで次の属性を指定します。

- docsBpi2CmtsProvisionedCmCertStatus：行エントリを作成するために 4 に設定します。
- docsBpi2CmtsProvisionedCmCert：実際の X.509 証明書の 16 進データ（X509Certificate 値）。
- docsBpi2CmtsProvisionedCmCertTrust：証明書の信頼状態を指定する 1 ～ 2 の整数値：1 = 信頼、2 = 非信頼。証明書をホットリストに追加する際は、この属性を非信頼の 2 に設定します。

ヒント　実際の証明書データをロードする前に CertStatus 属性を必ず設定してください。そうでないと、CMTS では証明書がチェーンされていると想定して、ただちに製造元証明書およびルート証明書で検証を試みます。

（注）　この手順は、docsBpi2CmtsProvisionedCmCertTrust 属性は 1 ではなく 2 に設定される点を除き、SNMP コマンドを使用した信頼できる証明書として証明書の追加, （1280ページ）で信頼できる証明書として証明書を追加するための手順とまったく同じです。

たとえば、Unix のコマンドライン SNMP ユーティリティを使用して IP アドレス 192.168.100.113 の CMTS 上にあるホットリストに製造元の証明書を追加するには、次のコマンドを入力します（<*index*>値のテーブル エントリを有効なインデックス ポインタで置き換えてください）。

```
% setany -v2c 192.168.100.113 private docsBpi2CmtsCACertStatus.
<index>
 -i 4
 docsBpi2CmtsCACert.
<index>
 -o
 '<hex_data>' docsBpi2CmtsCACertTrust.
<index>
 -i 2
```

CM 証明書で同様の処理を実行するには、次のコマンドを使用します。

```
% setany -v2c 192.168.100.113 private docsBpi2CmtsProvisionedCmCertStatus.
<index>
 -i 4
 docsBpi2CmtsProvisionedCmCert.
<index>
 -o
 '<hex_data>' docsBpi2CmtsProvisionedCmCertTrust.
<index>
 -i 2
```

ヒント　ほとんどのオペレーティング システムでは、証明書を指定する 16 桁の 10 進数文字列を入力するために必要なだけの入力行数を受け入れられません。したがって、これらの属性を設定するには、グラフィカルな SNMP マネージャを使用する必要があります。大量の証明書がある場合は、スクリプト ファイルを使用すると便利です。

連結の有効化

ケーブル インターフェイスの 1 つ以上のアップストリームで連結をイネーブルにするには（これはデフォルト設定）、次の手順を実行します。

手順

	コマンドまたはアクション	目的

ステップ 1	**enable**
	
	例：
	
	`Router> enable`
	`Router#`
		特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

ステップ 2	**configureterminal**
	
	例：
	
	`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。

	コマンドまたはアクション	目的

ステップ 3	**interfacecable***slot* / *port*
	
	例：
	`Router(config)# interface cable 6/0`
	`Router(config-if)#`
		この特定のスロットでケーブルインターフェイス ライン カードのインターフェイス コンフィギュレーション モードを開始します。

ステップ 4	**cableupstream** *n***concatenation**
	
	例：
	`Router(config-if)# cable upstream 0 concatenation`
	`Router(config-if)# cable upstream 1 concatenation`
	`Router(config-if)#`
		ケーブルインターフェイスで指定したアップストリームの連結をイネーブルにします。
		（注） インターフェイスの各アップストリームに対してこのコマンドを繰り返します。

ステップ 5	**exit**
	
	例：
	`Router(config-if)# exit`
	`Router(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 6	**exit**
	
	例：
	`Router(config)# exit`
	`Router#`
		グローバル コンフィギュレーション モードを終了します。

DOCSIS フラグメンテーションの有効化

ケーブル インターフェイスの 1 つ以上のアップストリームで DOCSIS フラグメンテーションをイネーブルにするには（デフォルト設定）、次の手順を実行します。

手順

	コマンドまたはアクション	目的

ステップ 1	**enable**
	
	例：
	`Router> enable`
	
	例：
	`Router#`
		特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的

ステップ 2	**configureterminal**
	
	例：
	
	`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	**interfacecable***slot* /*port*
	
	例：
	
	`Router(config)# interface cable 6/0`
	`Router(config-if)#`
		この特定のスロットでケーブルインターフェイス ライン カードのインターフェイス コンフィギュレーション モードを開始します。

ステップ 4	**cableupstream***n* **fragmentation**
	
	例：
	
	`Router(config-if)# cable upstream 2 fragmentation`
	`Router(config-if)# cable upstream 3 fragmentation`
	`Router(config-if)#`
		ケーブルインターフェイスで指定したアップストリームのフラグメンテーションをイネーブルにします。
		
		（注） インターフェイスの各アップストリームに対してこのコマンドを繰り返します。

ステップ 5	**cableupstream** *n***unfrag-slot-jitter**[**limit***jitter* | **cac-enforce**]
	
	例：
	
	`Router(config-if)# cable upstream 0 unfrag-slot-jitter limit 2000 cac-enforce`
	`Router(config-if)#`
		（任意）フラグメント化不能スロットがあるため、アップストリームで許容可能なジッターの量を指定します。**limit** オプションは、許容可能なジッター制限をミリ秒で指定します（0 ～ 4,294,967,295）。**cac-enforce** オプションは、フラグメント化可能スロット ジッターよりも少ないジッターを要求するサービス フローを拒否できるようにアップストリームを設定します。
		
		（注） デフォルトでは、*jitter* は制限 0 ミリ秒に設定されており、**cac-enforce** オプションが有効です。

ステップ 6	**exit**
	
	例：
	
	`Router(config-if)# exit`
	`Router(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 7	**exit**
	
	例：
	
	`Router(config)# exit`
	`Router#`
		グローバル コンフィギュレーション モードを終了します。

次に示す **showcableqosprofile** コマンドの例は、最大ダウンストリーム バーストが定義済みで、管理により作成された QoS プロファイルであることを示します。

```
Router# show cable qos profile
ID  Prio Max       Guarantee Max         Max   TOS  TOS   Create  B     IP prec.
         upstream  upstream  downstream tx    mask value by      priv  rate
         bandwidth bandwidth bandwidth  burst                     enab  enab
1   0    0         0         0          0     0xFF 0x0   cmts(r) no    no
2   0    64000     0         1000000    0     0xFF 0x0   cmts(r) no    no
3   7    31200     31200     0          0     0xFF 0x0   cmts    yes   no
4   7    87200     87200     0          0     0xFF 0x0   cmts    yes   no
6   1    90000     0         90000      1522  0xFF 0x0   mgmt    yes   no
10  1    90000     0         90000      1522  0x1  0xA0  mgmt    no    no
50  0    0         0         96000      0     0xFF 0x0   mgmt    no    no
51  0    0         0         97000      0     0xFF 0x0   mgmt    no    no
```

次の例は、特権 EXEC モードで **showcableqosprofileverbose** コマンドを使用して表示されるサンプル QoS プロファイル 10 の最大ダウンストリーム バースト サイズを示します。

```
Router# show cable qos profile 10 verbose
Profile Index                           10
Name
Upstream Traffic Priority               1
Upstream Maximum Rate (bps)             90000
Upstream Guaranteed Rate (bps)          0
Unsolicited Grant Size (bytes)          0
Unsolicited Grant Interval (usecs)      0
Upstream Maximum Transmit Burst (bytes) 1522
Downstreamam Maximum Transmit Burst (bytes) 100000
IP Type of Service Overwrite Mask       0x1
IP Type of Service Overwrite Value      0xA0
Downstream Maximum Rate (bps)           90000
Created By                              mgmt
Baseline Privacy Enabled                no
```

Cisco cBR-8 ルータでの DOCSIS 1.1 ダウンストリーム最大送信バーストの有効化

Cisco cBR-8 ルータで ERBA を設定するには、次の手順を実行します。この手順および関連コマンドは、このマニュアルに記載されているガイドラインと制限事項の対象です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

ステップ 2	**configure terminal**
	
	例：
	
	`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。

	コマンドまたはアクション	目的
ステップ 3	[**no**] **cableds-max-burstburst-threshold** *threshold* 例： `Router(config)# cable ds-max-burst burst-threshold 2048`	DOCSIS 1.1 ダウンストリームの最大バーストをサポートします。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。
ステップ 4	**cableserviceclass** *class-index***peak-rate** *peak-rate* 例： `Router(config)# cable service class 1 peak-rate 1000`	特定のサービス クラスの peak-rate 値を設定します。

ステップ 5	**Ctrl^Z**
	
	例：
	
	`Router(config)# Ctrl^Z`
	`Router#`
		特権 EXEC モードに戻ります。

この機能をイネーブルにすると、バーストのしきい値よりも大きなバースト サイズの新しいサービス フローがサポートされます。ただし、既存のサービス フローは影響を受けません。

この機能を無効にすると、新しいサービス フローでは、**cableds-max-burst** コマンド設定 [Downstream Maximum Transmit Burst] パラメータが設定されません。ただし、既存のサービス フローは影響を受けません。

DOCSIS 動作のモニタリング

ここでは、DOCSIS ネットワークおよびそのケーブル モデム、CMTS の RF ネットワークとケーブル インターフェイス、および BPI+ の動作に関する情報を提供するコマンドについて説明します。

DOCSIS ネットワークのモニタリング

showcablemodem コマンドは、ケーブル モデムおよび DOCSIS ネットワークの現在の状態を表示するための主要なコマンドです。このコマンドには多くのオプションがあり、DOCSIS 動作のさまざまな側面の情報を提供します。

ケーブル モデムのステータスの表示

既知のケーブル モデムとそれらの現在のステータスのリストを表示するには、**show cable modem** コマンドを使用します。

また、**showcablemodem** コマンドで MAC アドレスまたは IP アドレスを指定して、特定のケーブル モデムを表示することもできます。CPE デバイスの MAC アドレスまたは IP アドレスを指定すると、このデバイスに関連付けられたケーブル モデムの情報が表示されます。

（注） CPE IP アドレスとケーブル モデムとの関連付けがすでに解除された場合、**showcablemodem** コマンドはケーブルモデムに関する情報を表示しない場合があります。ケーブルモデムの CPE デバイスの IP アドレスを表示するには、**clearcablehostip-address** コマンドを使ってルータ データベースからモデムの IP アドレスをクリアした後、**pingdocsismac-address** コマンドを入力します。このコマンドは、DOCSIS ping を CM に送信して MAC アドレスを解決します。

製造元別にソートしたケーブル モデムのリストを表示するには、**vendor** オプションを使用します。

各ケーブル モデムの MAC 状態フィールドには、ケーブル モデムの現在の状態が表示されます。

表 *191*：*MAC* の状態フィールドの説明

[MAC State] の値	説明
登録とプロビジョニングのステータス条件	
init(r1)	CM が初期の範囲設定を送信しました。
init(r2)	CM が範囲設定を実行しています。CMTS が CM から初期範囲設定を受信し、RF 電力、タイミング オフセット、および周波数調整を CM に送信しました。
init(rc)	レンジングが完了しました。
init(d)	DHCP 要求を受信しました。また、最初の IP ブロードキャスト パケットを CM から受信したことを示します。
init(i)	DHCP 応答を受信し、IP アドレスが割り当てられましたが、CM は IP パケットでまだ応答していません。

[MAC State] の値	説明
init(o)	CM が DHCP 応答の指定に従い、Trivial File Transfer Protocol（TFTP）を使用してオプションファイル（DOCSIS コンフィギュレーションファイル）のダウンロードを開始しました。CM がこの状態のままになる場合は、ダウンロードが失敗したことを示します。
init(t)	時刻（TOD）の交換が開始されました。
resetting	CM のリセット中です。登録プロセスが間もなく再開されます。
エラーのないステータス条件	
offline	CM はオフラインと見なされます（切断または電源オフ）。
online	CM は登録済みで、ネットワーク上でデータを渡すことができます。
online(d)	CM は登録されていますが、CM のネットワークアクセスが DOCSIS コンフィギュレーションファイルで無効になっています。
online(pk)	CM は登録済みで、BPI が有効になっており、KEK が割り当てられています。
online(pt)	CM は登録済みで、BPI が有効になっており、TEK が割り当てられています。BPI 暗号化が実行中です。
expire(pk)	CM は登録されており、BPI は有効で、KEK は割り当てられていますが、有効期限が切れています。
expire(pt)	CM は登録されており、BPI は有効で、TEK は割り当てられていますが、有効期限が切れています。
エラー ステータス条件	

[MAC State] の値	説明
reject(m)	CM が登録を試みましたが、メッセージ整合性チェック（MIC）の値が正しくないため、登録を拒否されました。さらに、これは、DOCSIS コンフィギュレーションファイルの共有秘密が **cableshared-secret** コマンドで CMTS に設定された値と一致しないことを示している可能性があります。 さらに、**cabletftp-enforce** コマンドを使用して、登録前に DOCSIS コンフィギュレーションファイルの TFTP ダウンロードを試みるよう CM に要求したが、CM がこれを実行しなかったことを示している可能性もあります。
reject(c)	CM が登録を試みましたが、いくつかのエラーが原因で登録を拒否されました。 • CM が **cableupstreamadmission-control** コマンドで設定された上限を超える最低保証アップストリーム帯域幅を登録しようとしました。 • セキュリティ違反のために CM が無効になっています。 • DOCSIS コンフィギュレーションファイルに含まれるサービス クラス（COS）の値が正しくありません。 • CM は新しい COS 設定を作成しようとしましたが、CMTS がそのような変更を許可しないように設定されています。
reject(pk)	KEK キーの割り当てが拒否され、BPI 暗号化は確立されませんでした。
reject(pt)	TEK キーの割り当てが拒否され、BPI 暗号化は確立されませんでした。

[MAC State] の値	説明
reject(ts)	CM が登録を試みましたが、CM 登録要求に含まれる TFTP サーバのタイムスタンプが CMTS によって保持されているタイムスタンプと一致しないため、登録は失敗しました。これは、CM が以前に登録を試みた際に使用した古いDOCSIS コンフィギュレーション ファイルを再利用して登録を試みたことを示す可能性があります。
reject(ip)	CM が登録を試みましたが、TFTP サーバが DOCSIS コンフィギュレーション ファイルを CM に送信した際に記録した IP アドレスと CM 要求に含まれるIPアドレスが一致しないため、登録は失敗しました。IP スプーフィングが発生するおそれがあります。
reject(na)	CM が登録を試みましたが、CMTS が送信した登録応答（REG-RSP）メッセージに対する応答として、CMが登録確認（REG-ACK）メッセージを送信しなかったため、登録は失敗しました。登録未確認（REG-NACK）と考えられます。

ケーブル モデムのサマリー レポートの表示

showcablemodem コマンドでは、**summary** オプションと **total** オプションを使用して、サマリー レポートを表示することもできます。

また、**summary** オプションと **total** オプションを使用して、1 つのインターフェイスまたはある範囲内の複数のインターフェイスの情報を表示することもできます。

ケーブル モデムの機能の表示

ケーブル モデムの機能と現在の DOCSIS プロビジョニングを表示するには、**mac** オプションを使用します。

ケーブル モデムとその機能のサマリー レポートを取得するには、**mac** オプションを **summary** および **total** オプションと併せて使用します。

特定のケーブル モデムに関する詳細情報の表示

show cable modem コマンドのいくつかのオプションにより、特定のケーブルモデム（各自のMAC アドレスで識別）の詳細情報が表示されます。**verbose** オプションにより、最も包括的な出力が表示されます。

また、**connectivity** および **maintenance** オプションにより、特定のケーブル モデムに関する問題のトラブルシューティングに役立つ情報が表示されます。

RF ネットワークおよびケーブル インターフェイスのモニタリング

showinterfacecable コマンドを使用して、CMTS の RF ネットワークおよびケーブル インターフェイスの動作に関する情報を表示できます。

ヒント　**showcableinterface** コマンドとそのオプションの詳細については、『*Cisco Broadband Cable Command Reference Guide*』の章「Cisco Cable Modem Termination System Commands」を参照してください（http://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_cmts_quality_of_services/docsis_1_1.html#ref_1239231を参照）。

複製されたケーブル モデムに関する情報の表示

複製されたケーブル モデムとして検出されたケーブル モデムのリストを表示するには、**privacyhotlist** オプションを指定した **showinterfacecable** コマンドを使用します。

ケーブル モデムへの RF アクセスの拒否

レンジングの際にケーブル モデムに関する無線周波数（RF）アクセスを拒否するには、**cableprivacyhotlistcm** *mac-address* コマンドを使用します。

次に、独自のMACアドレスを使用して複製したケーブルモデムをブロックする方法を示します。

```
Router(config)# cable privacy hotlist cm 00C0.0102.0304
Router(config)#
```

オペレータが、特定の CMTS に登録してはいけないモデムの MAC アドレスを特定したら、上記のコマンドを使用して CMTS にこの MAC アドレスを追加できます。このコマンドにより、このモデムは CMTS のあらゆるインターフェイスでオンラインになることができなくなります。

Mac スケジューラの情報の表示

各ケーブル インターフェイスで動作している DOCSIS MAC レイヤ スケジューラの情報を表示するには、**showcableinterface** コマンドで **mac-scheduler** オプションを使用します。インターフェイスのすべてのアップストリームまたはインターフェイスの 1 つのアップストリームに関する情報を表示できます。

QoS パラメータ セットの情報の表示

ケーブル インターフェイスで定義されている DOCSIS 1.1 QoS パラメータ セットに関する情報を表示するには、**qosparamset** オプションを指定した **showcableinterface** コマンドを使用します。

また、**verbose** オプションと一緒にそのサービス クラスのインデックス番号を指定して、特定のパラメータ セットの詳細情報を表示することもできます。

サービス フローの情報の表示

ケーブル インターフェイスで設定されるサービス フローとその QoS パラメータ セットを表示するには、**showinterfacecable** コマンドで **service-flow** オプションを使用します。

各サービス フローの主な QoS パラメータを表示するには、このコマンドに **qos** オプションを追加します。

特定のサービス フローの QoS パラメータをすべて表示するには、**qos** および **verbose** オプションを使用します。これらのオプションは個別または組み合わせて使用できます。

サービス ID の情報の表示

DOCSIS 1.1 ネットワークのアップストリームに対してのみ割り当てられるサービス ID（SID）の情報を表示するには、**showinterfacecable** コマンドで **sid** オプションを使用します。

各 SID に関連する主要な QoS パラメータを表示するには、**qos** オプションを追加します。

特定の SID とその QoS パラメータの詳細情報を表示するには、**qos** と **verbose** の両方のオプションを使用します。

BPI+ 動作のモニタリング

CMTS とそれに接続されたケーブル モデムでの BPI 動作のステータスのモニタリングについては、次の項を参照してください。

ケーブル モデムの現在の BPI+ の状態の表示

ケーブルモデムの現在の BPI+ 状態を表示するには、**showcablemodem** コマンドを使用します。このコマンドのオプションを何も設定せずに使用すると、すべてのインターフェイスのケーブル モデムのステータスが表示されます。また、CMTS の特定のケーブル インターフェイス、または特定のケーブル モデムの IP アドレスや MAC アドレスを指定することもできます。

```
Router# show cable modem
 [ip-address
 | interface
 | mac-address
```

showcablemodem コマンドの出力結果の MAC の状態列には、各ケーブル モデムの現在のステータスが表示されます。次に、このフィールドで考えられる BPI 関連の値を示します。

表 *192* : *show cable modem* による *BPI+* の考えられる状態

状態	説明
online	ケーブル モデムがオンラインに変わり、BPI+ の使用が設定されている場合は、セッションのプライバシー パラメータをネゴシエートしています。モデムが数分以上この状態の場合は、オンラインですが BPI+ は使用されていません。ケーブル モデムが DOCSIS 認定ソフトウェアを実行し、BPI+ を有効にする DOCSIS コンフィギュレーション ファイルを使用していることを確認します。
online(pk)	ケーブル モデムはオンラインで、CMTS とキーの暗号化キー（KEK）のネゴシエーションが完了しています。BPI+ ネゴシエーションが成功すると、この状態は online(pt) に変わります。
online(pt)	ケーブル モデムがオンラインで、CMTS とトラフィックの暗号化キー（TEK）のネゴシエーションが完了しています。BPI+ セッションが確立し、ケーブル モデムは、指定したプライバシー パラメータを使用して、CMTS ですべてのユーザ トラフィックを暗号化しています。
reject(pk)	主にケーブル モデムの認証に失敗したため、CMTS と KEK のネゴシエーションに失敗しました。ケーブル モデムが BPI+ 用に正しく設定されており、有効なデジタル証明書を使用していることを確認します。CMTS で BPI+ を登録する必要がある場合は、ケーブル モデムをオフラインにして、再登録する必要があります。ケーブル モデムが CMTS プロビジョニング システムに正しく登録されていることを確認します。 （注） ケーブル モデムで BPI+ の認証に失敗すると、次のようなメッセージが CMTS ログに表示されます `%CBR-5-UNAUTHSIDTIMEOUT: CMTS deleted BPI unauthorized Cable Modem 00c0.abcd.ef01`
reject(pt)	ケーブル モデムは、TEK と CMTS のネゴシエーションに失敗しました。CMTS で BPI+ を登録する必要がある場合は、ケーブル モデムで再登録する必要があります。

CMTS の BPI+ タイマー値の表示

特定のケーブル インターフェイスの KEK および TEK 存続時間タイマーの値を表示するには、**showinterfacecable** *x/y* **privacy** [**kek** | **tek**] コマンドを使用します。

CMTS の 証明書リストの表示

CMTS で既知の証明書のリストを表示するには、**showcryptcacertificates** コマンドを使用します。次に例を示します。

```
Router# show crypto ca certificates

Certificate
  Status: Available
  Certificate Serial Number: 7DBF85DDDD8358546BB1C67A16B3D832
  Key Usage: General Purpose
  Subject Name
    Name: Cisco Systems
  Validity Date:
    start date: 00:00:00 UTC Sep 12 2001
    end   date: 23:59:59 UTC Sep 11 2021
Root certificate
  Status: Available
  Certificate Serial Number: 5853648728A44DC0335F0CDB33849C19
  Key Usage: General Purpose
    CN = DOCSIS Cable Modem Root Certificate Authority
     OU = Cable Modems
     O = Data Over Cable Service Interface Specifications
     C = US
  Validity Date:
    start date: 00:00:00 UTC Feb 1 2001
    end   date: 23:59:59 UTC Jan 31 2031
```

DOCSIS 1.1 動作の設定例

ここでは、Cisco CMTS での DOCSIS 1.1 動作の設定例を示します。

例：Cisco cBR-8 ルータ（BPI+ 付き）用の DOCSIS 1.1 の設定

```
version 12.2
service timestamps log datetime msec localtime
service password-encryption
!
hostname cBR-8
!
redundancy
 main-cpu
  auto-sync standard
logging queue-limit 100
no logging buffered
no logging rate-limit
enable password my-enable-password
!
ipc cache 5000
card 1/1 2cable-tccplus
card 2/0 1gigethernet-1
card 2/1 2cable-tccplus
```

```
card 3/0 1gigethernet-1
card 4/0 1oc12pos-1
card 8/0 5cable-mc520s
card 8/1 5cable-mc520s
cable flap-list insertion-time 60
cable flap-list power-adjust threshold 4
cable flap-list aging 86400
cable modem vendor 00.50.F1 TI
cable spectrum-group 2 band 11000000 16000000
cable spectrum-group 21 band 17000000 25000000
cable spectrum-group 32 shared
cable spectrum-group 32 band 5000000 42000000
cable modulation-profile 2 request 0 16 0 8 qpsk scrambler 152 no-diff 64 fixed uw16
cable modulation-profile 2 initial 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 station 5 34 0 48 qpsk scrambler 152 no-diff 128 fixed uw16
cable modulation-profile 2 short 6 75 6 8 16qam scrambler 152 no-diff 144 shortened uw8
cable modulation-profile 2 long 8 220 0 8 16qam scrambler 152 no-diff 160 shortened uw8
cable modulation-profile 21 request 0 16 0 22 qpsk scrambler 152 no-diff 32 fixed
cable modulation-profile 21 initial 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 21 station 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 21 short 3 76 12 22 qpsk scrambler 152 no-diff 64 shortened
cable modulation-profile 21 long 7 231 0 22 qpsk scrambler 152 no-diff 64 shortened
cable modulation-profile 22 request 0 16 0 22 qpsk scrambler 152 no-diff 32 fixed
cable modulation-profile 22 initial 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 22 station 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 22 short 4 76 7 22 16qam scrambler 152 no-diff 128 shortened
cable modulation-profile 22 long 7 231 0 22 16qam scrambler 152 no-diff 128 shortened
cable modulation-profile 23 request 0 16 0 22 qpsk scrambler 152 no-diff 32 fixed
cable modulation-profile 23 initial 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 23 station 5 34 0 48 qpsk scrambler 152 no-diff 64 fixed
cable modulation-profile 23 short 4 76 7 22 16qam scrambler 152 no-diff 128 shortened
cable modulation-profile 23 long 7 231 0 22 16qam scrambler 152 no-diff 128 shortened
cable qos profile 5 max-downstream 10000
cable qos profile 5 max-upstream 1000
cable qos profile 5 priority 7
cable qos profile 5 tos-overwrite 0x3  0x0
cable qos profile 5 name cm_no_priority
cable qos profile 6 max-downstream 10000
cable qos profile 6 max-upstream 5000
cable qos profile 6 priority 7
cable qos profile 6 tos-overwrite 0x3  0x0
cable qos profile 6 name qos6
cable qos profile 7 max-downstream 128
cable qos profile 7 max-upstream 128
cable qos profile 7 priority 7
cable qos profile 8 max-downstream 10000
cable qos profile 8 max-upstream 1000
cable qos profile 8 priority 3
cable qos profile 8 tos-overwrite 0x3  0x0
cable qos profile 8 name qos8
no cable qos permission create
no cable qos permission update
cable qos permission modems
cable event syslog-server 10.10.10.131
ip subnet-zero
!
!
interface FastEthernet0/0/0
 ip address 10.10.32.21 255.255.0.0
 no cdp enable
!
interface GigabitEthernet2/0/0
 ip address 10.10.31.2 255.0.0.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 load-interval 30
 negotiation auto
 no cdp enable
!
interface GigabitEthernet3/0/0
 no ip address
 ip pim sparse-mode
```

```
 no ip route-cache cef
 load-interval 30
 shutdown
 negotiation auto
 no cdp enable
!
interface POS4/0/0
 no ip address
 crc 32
 no cdp enable
 pos ais-shut
!
!
interface Cable8/0/0
 ip address 10.10.10.28 255.255.255.0
 ip helper-address 1.10.10.133
 cable bundle 2 master
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 669000000
 cable downstream channel-id 0
 no cable downstream rf-shutdown
 cable downstream rf-power 45
 cable upstream 0 connector 0
 cable upstream 0 spectrum-group 32
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 data-backoff 0 6
 cable upstream 0 modulation-profile 23
 no cable upstream 0 rate-limit
 no cable upstream 0 shutdown
 cable upstream 1 connector 1
 cable upstream 1 spectrum-group 32
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 data-backoff 0 6
 cable upstream 1 modulation-profile 23
 no cable upstream 1 shutdown
 cable upstream 2 connector 2
 cable upstream 2 spectrum-group 32
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 data-backoff 3 6
 cable upstream 2 modulation-profile 23
 no cable upstream 2 shutdown
 cable upstream 3 connector 3
 cable upstream 3 spectrum-group 32
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 21
 no cable upstream 3 shutdown
 cable source-verify
 cable privacy kek life-time 300
 cable privacy tek life-time 180
 no keepalive
!
interface Cable8/0/1
 ip address 10.10.11.121
 cable bundle 2
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 453000000
 cable downstream channel-id 0
 no cable downstream rf-shutdown
 cable upstream max-ports 6
 cable upstream 0 connector 4
 cable upstream 0 spectrum-group 2
```

```
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 range-backoff 3 6
 cable upstream 0 data-backoff 0 6
 cable upstream 0 modulation-profile 23 21
 no cable upstream 0 rate-limit
 cable upstream 0 shutdown
 cable upstream 1 connector 5
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 6
 cable upstream 2 channel-width 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 7
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
 cable upstream 4 channel-width 1600000
 cable upstream 4 minislot-size 4
 cable upstream 4 modulation-profile 21
 cable upstream 4 shutdown
 cable upstream 5 channel-width 1600000
 cable upstream 5 minislot-size 4
 cable upstream 5 modulation-profile 21
 cable upstream 5 shutdown
 cable source-verify
 cable privacy kek life-time 300
 cable privacy tek life-time 180
 no keepalive
!
!
ip classless
ip http server
no ip http secure-server
!
!
no cdp run
snmp-server community public RW
snmp-server community private RW
snmp-server enable traps cable
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 exec-timeout 0 0
 password my-telnet-password
 login
 length 0
!
end
```

その他の参考資料

DOCSIS 1.1 の動作に関連する詳細情報については、次の参考資料を参照してください。

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Cisco CMTS ルータの DOCSIS 1.1 に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャセット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *193* : *Cisco CMTS* ルータの *DOCSIS 1.1* に関する機能情報

機能名	リリース	機能情報
Cisco CMTS ルータでの DOCSIS 1.1	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 77 章

デフォルト DOCSIS 1.0 ToS の上書き

このマニュアルでは、Cisco ケーブル モデム終端システム（CMTS）の DOCSIS 1.0 ToS の上書き機能について説明します。この機能により、すべての DOCSIS 1.0 ケーブル モデム（CM）によって作成されたプロファイルをデフォルト ToS の上書きにバインドすることで、タイプ オブ サービス（ToS）の上書きを実行するために複数の QoS プロファイルを作成する必要がなくなります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *194* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

デフォルト DOCSIS 1.0 ToS の上書きの制限事項

- デフォルト DOCSIS 1.0 ToS の上書き機能は DOCSIS バージョン 1.0 を稼働する CM のみに適用されます。

- デフォルト DOCSIS 1.0 ToS の上書き機能の設定後、設定を有効にするには、すべての CM をリセットする必要があります。
- デフォルト DOCSIS 1.0 ToS の上書き機能が設定されると、すべての CM で設定されたデフォルト値が表示されます。その後、QoS プロファイルを編集することによってのみ上書き値を変更できます。

デフォルト DOCSIS 1.0 ToS 上書きに関する情報

デフォルト DOCSIS 1.0 ToS 上書き機能を設定するには、次のトピックについて理解しておく必要があります。

デフォルト DOCSIS 1.0 ToS の上書きの概要

現在、ToSの上書きには静的ケーブルQoSプロファイルの作成が必要です。このプロファイルは、ToS フィールドに割り当てられ、その後 1.0 CM に関連付けられます。この実装は、いくつかの異なるサービス タイプのみ提供される場合に機能します。

ただし、多数のサービス タイプが存在する場合は、ToSの上書きを実行するためにそれぞれのサービス タイプが静的 QoS プロファイルを必要とするため、拡張性の問題が生じます。

デフォルト DOCSIS 1.0 ToS の上書き機能により、すべての DOCSIS 1.0 ケーブル モデム（CM）によって作成されたプロファイルをデフォルト ToS の上書きに自動でバインドすることで、タイプ オブ サービス（ToS）の上書きを実行するために複数の QoS プロファイルを作成する必要がなくなります。

DOCSIS

CableLabs によって作成された Data Over Cable Service Interface Specification（DOCSIS）は、ケーブル テレビ システム ネットワーク上での高速データ配信に関連するすべてのケーブル モデムにおけるインターフェイス規格と要件を定義します。

DOCSIS アーキテクチャは、次の 2 つのコンポーネントで構成されています。

- ケーブル モデム（CM）
- ケーブル モデム終端システム（CMTS）

これらの各コンポーネントは別々の場所に配置されますが、多くの場合、CM はカスタマーのサイトに、CMTS はサービス プロバイダーのサイトに配置されます。また、CM と CMTS の間の通信は、DOCSIS を介してケーブル上を伝送されます。

（注） 使用可能な DOCSIS のバージョンは複数ありますが、デフォルト DOCSIS 1.0 ToS の上書き機能は DOCSIS 1.0 を実行する CM のみに適用されます。

タイプ オブ サービス（ToS）

タイプ オブ サービス（ToS）のビット ID などのツールにより、使用中のアプリケーションのタイプによってネットワーク トラフィックを分離することができます。ToS機能をさらに拡張して、使用中のインターフェイス、ユーザ タイプと個々のユーザ ID、またはサイト アドレスにより、ネットワーク トラフィックを特定のブランドに分離することができます。

デフォルト DOCSIS 1.0 ToS 上書きの設定方法

この項に示すタスクにより、デフォルトの DOCSIS 1.0 ToS 上書き機能がイネーブルになります。

デフォルト DOCSIS 1.0 ToS の上書きの有効化

現在、DOCSIS 1.0 コンフィギュレーション ファイルが設定されたすべての CM には ToS の上書き機能があり、デフォルト値は tos-and: 0xff と tos-or: 0x00 に設定されています。DOCSIS 1.0 コンフィギュレーション ファイルにはこれまで ToS の上書き機能を指定する仕組みがなかったため、QoS プロファイルを作成し、デフォルトの ToS の上書き機能に割り当てていました。

次の手順を実行すると、デフォルトの DOCSIS 1.0 ToS の上書き機能がイネーブルになるため、CM で作成されたすべてのプロファイルにデフォルトの ToS の上書き機能を追加できます。

はじめる前に

この作業の前提条件はありません。

（注）
- デフォルト DOCSIS 1.0 ToS の上書き機能は DOCSIS バージョン 1.0 を稼働する CM のみに適用されます。
- デフォルト DOCSIS 1.0 ToS の上書き機能の設定後、設定を有効にするには、すべての CM をリセットする必要があります。
- デフォルト DOCSIS 1.0 ToS の上書き機能が設定されると、すべての CM で設定されたデフォルト値が表示されます。その後、QoS プロファイルを編集することによってのみ上書き値を変更できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cabledefault-tos-qos10tos-overwrite** *tos-and tos-or* 例： `Router(config)# cable default-tos-qos10 tos-overwrite 0x1F 0xE0`	CM に ToS の上書き機能のデフォルト値を設定します。このデフォルト値は、CM で今後作成されるすべてのプロファイルに追加されます。
ステップ 4	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次の作業

ToS 上書き機能のデフォルト値を設定した後、**clearcablemodemdelete** コマンドを使って CM をリセットすると、ToS 上書き機能の新しいデフォルト値が有効になります。

QoS プロファイルの編集

デフォルト DOCSIS 1.0 ToS 上書き機能を設定すると、QoS プロファイルを編集して、別の ToS 上書き値を変更することができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**cableqosprofile** {*groupnum* | *ip-precedence* | *guaranteed-upstream* | *max-burst* | *max-upstream* | *max-downstream* | *priority* | *tos-overwrite* | *value* 例： `Router(config)# cable qos profile 4 guaranteed-upstream 2`	QoS プロファイルを設定します。
ステップ 4	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

その他の参考資料

ここでは、デフォルト DOCSIS 1.0 ToS 上書きの機能の関連資料について説明します。

シスコのテクニカル サポート

説明	リンク
シスコのテクニカルサポートおよびドキュメンテーション Web サイトには、数千ページに及ぶ検索可能な技術情報があります。製品、テクノロジー、ソリューション、技術的なヒント、ツール、技術マニュアルへのリンクもあります。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/cisco/web/support/index.html

デフォルト DOCSIS 1.0 ToS 上書きに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *195*：デフォルト *DOCSIS 1.0 ToS* 上書きに関する機能情報

機能名	リリース	機能情報
デフォルト DOCSIS 1.0 ToS の上書き	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 78 章

Cisco CMTS ルータの DOCSIS WFQ スケジューラ

DOCSIS WFQ スケジューラは、WAN アップリンク インターフェイスと DOCSIS ダウンストリーム インターフェイスの両方で出力のスケジューリング サービスを提供する出力パケット スケジューラです。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *196* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

DOCSIS WFQ スケジューラの前提条件

DOCSIS WFQ スケジューラ機能を使用するために、特別な装置やソフトウェアは必要ありません。

DOCSIS WFQ スケジューラの制限事項

- DBS 機能は DOCSIS 3.0 ダウンストリーム チャネル ボンディングにのみ適用されます。

DOCSIS WFQ スケジューラに関する情報

DOCSIS WFQ スケジュール エンジンの使用により出力パケットのスケジューリング サービスが提供され、これには、Cisco cBR-8 コンバージド ブロードバンド ルータでの絶対プライオリティ キューイング、重み付け均等化キューイング、最小レート保証、トラフィック シェーピング、および DOCSIS ボンディング グループの動的帯域幅共有が含まれます。

DOCSIS WFQ スケジューラは、WAN アップリンク インターフェイスと DOCSIS ダウンストリーム インターフェイスの両方にサービスを提供します。WAN アップリンク インターフェイスのスケジューリング パラメータは、Modular QoS CLI（MQC）により設定されます。ケーブル ダウンストリーム インターフェイスの DOCSIS サービス フローのキューは、DOCSIS ダウンストリーム QoS のタイプ、長さ、値（TLV）で設定されているパラメータにより作成されます。

（帯域が 150 Mbps 超の）DOCSIS サービス フローのデフォルト キュー サイズは、ケーブル ダウンストリーム インターフェイスの帯域幅に基づきます（次の表を参照）。また、すべてのサービス フローのキュー限度を、**cablequeue-limit** コマンド、サービス クラスにおけるバッファ サイズ、またはダウンストリーム バッファ制御 TLV を使用して調整できます。

（注） デフォルト キュー サイズの変更と **cablequeue-limit** コマンドは、DOCSIS の高プライオリティ キューに影響しません。

次の表に、Annex B 256 QAM チャネルに基づくキュー サイズの例を示します。

表 *197*：帯域幅、キュー サイズ、キュー限度

チャネル	帯域幅（**Mbps**）	デフォルト キュー サイズ	キュー サイズ				
			1 ミリ秒	**20** ミリ秒	**30** ミリ秒	**40** ミリ秒	**200** ミリ秒
1	37.5	63	63	63	92	123	617
2	75	255	63	123	185	247	1235
3	112.5	255	63	185	277	370	1852
4	150	255	63	247	370	494	2470
5	187.5	319	63	308	463	617	3087
6	225	383	63	370	555	741	3705

チャネル	帯域幅（Mbps）	デフォルト キュー サイズ	キュー サイズ				
			1 ミリ秒	20 ミリ秒	30 ミリ秒	40 ミリ秒	200 ミリ秒
7	262.5	447	63	432	648	864	4323
8	300	511	63	494	741	988	4940
12	450	767	63	741	1111	1482	7411
14	525	895	63	864	1296	1729	8646
16	600	1023	63	988	1482	1976	9881

DOCSIS WFQ スケジューラを使用すると、キュー スケーリングの限度を大幅に拡張できます。

次の項では、DOCSIS WFQ スケジューラ機能について説明します。

キュー タイプ

DOCSIS WFQ スケジューラ機能は、次のキュー タイプをサポートします。

- プライオリティ キュー
- CIR キュー
- ベスト エフォート キュー

プライオリティ キュー

プライオリティ キューは他のすべてのキューよりも絶対最優先で処理されます。DOCSIS ダウンストリーム インターフェイスでは、プライオリティ キューは、パケット ケーブル音声サービス フローなどのプライオリティ サービス フローを要求する DOCSIS アプリケーションによって設定されます。WAN アップリンク インターフェイスでは、プライオリティ キューは MQC ポリシーマップによって設定されます。

プライオリティ キューには、次のような制約事項が適用されます。

- 1 つの WAN アップリンク インターフェイスに 1 つのプライオリティ キューのみ指定できます。
- 各 DOCSIS ダウンストリーム インターフェイス用に作成された低遅延サービス フローには、1 つのプライオリティ キューのみ指定できます。
- DOCSIS ダウンストリーム上のすべての低遅延フローは、単一のプライオリティ キューに集約されます。

CIR キュー

CIR キューは、少なくとも認定情報レート（CIR）を使用して処理されることが保証されます。CIR キューは、ゼロ以外の最小予約レートで DOCSIS サービス フローを処理するために使用されます。CIR キューにかかる負荷が CIR 値を超えると、超過トラフィックは、ベスト エフォート型トラフィックとして処理されます。

ベスト エフォート キュー

ベスト エフォート（BE）キューは、プライオリティ キューと CIR キューで使用されていないインターフェイス帯域幅を共有します。共有は各キューの過剰率に比例します。

BE キューには、次の条件が適用されます。

- DOCSIS ダウンストリーム インターフェイスでは、BE キューは最小予約レートを要求しない DOCSIS サービス フローによって作成されます。
- 最小予約レートを使用しない各 DOCSIS フローは、独自の BE キューを使用します。

DOCSIS QoS サポート

DOCSIS は、Quality of Service（QoS）パラメータを定義します。たとえば、トラフィックの優先度、最大持続トラフィック レート、最小予約トラフィック レート、最大トラフィック バースト、最大ダウンストリーム遅延、ピーク トラフィック レートがあります。

ダウンストリーム サービス フローは、目的の QoS を指定するために QoS パラメータを使用します。ダウンストリーム ポリサーとスケジューラは、トラフィック シェーピング、帯域幅プロビジョニング、トラフィックの優先順位付け、帯域幅保証などのサービスを提供します。

DOCSIS サービス フロー パラメータは、パケット キュー パラメータにマッピングされ、DOCSIS パラメータをサポートするためにパケット キューの適切な QoS サポートとともに提供されます。

次の DOCSIS QoS パラメータがサポートされています。

- トラフィック プライオリティ
- 最大持続トラフィック レート
- 最小予約トラフィック レート

（注） http://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_cmts_quality_of_services/docsis_wfq_scheduler.html#con_1085732で説明されているように、最大トラフィック バースト サイズおよびピーク トラフィック レートがサポートされます。

トラフィック プライオリティ

ベストエフォート型トラフィックに使用可能なダウンストリームチャネルの帯域幅、つまりチャネル帯域幅からプライオリティ トラフィックと CIR トラフィックが消費する分を除いた帯域幅が、その DOCSIS トラフィック プライオリティに比例してベスト エフォート サービス フローに割り当てられます。たとえば、特定の時点に同じダウンストリーム チャネルでパケットを送信するサービス フローが 3 つあり、DOCSIS トラフィック プライオリティがそれぞれ 0、1、3 である場合、それらは1:2:4でチャネル帯域幅を共有することになります。この帯域幅割り当てを達成するため、DOCSIS プライオリティから得られる過剰率と呼ばれる値が各サービス フローに割り当てられます。次の表に、DOCSISプライオリティの過剰率へのデフォルトマッピングを示します。

（注） フローのトラフィック プライオリティが明示的に指定されていない場合、DOCSIS仕様によりデフォルトのプライオリティ値 0 が使用されます。

表 *198*：過剰率に対する *DOCSIS* プライオリティのマッピング

DOCSIS トラフィック プライオリティ	過剰率
0	4
1	8
2	12
3	16
4	20
5	24
6	28
7	32

過剰率に対するカスタム *DOCSIS* プライオリティのマッピング

このオプションは、ダウンストリームサービスフローの過剰率に対するカスタムプライオリティのマッピングを構成するために導入されました。このオプションは、上の表にリストされたデフォルト マッピングを上書きするものです。

（注） 構成値は、構成の適用後に作成された新しいサービス フローに対してのみ使用されます。すべての既存サービス フローは、以前の過剰率の値を維持します。

過剰率に対するプライオリティのマッピングを構成するオプションは、ダウンストリーム転送インターフェイス単位で使用でき、レガシー ケーブル、ワイドバンドおよびモジュラ ケーブル、および統合ケーブル インターフェイスに適用できます。

cable downstream qos wfq weights コマンドは、マッピングを設定するために使用されます。

最大持続トラフィック レート

最大持続トラフィック レート（MSR）は、サービス フローの最大情報レートを指定します。サービス フローの MSR はパケット キューのシェープ レートにマッピングされます。最大持続トラフィック レートが指定されていないかまたはゼロに設定されている場合、そのトラフィック レートは DOCSIS 仕様で設定された物理チャネル容量のみに制限されます。

最小予約トラフィック レート

最小予約トラフィック レート（MRR）は、サービス フロー用に予約された最小レートを指定します。サービス フローの MRR はパケット キューの CIR にマッピングされ、これによりキューが輻輳時に取得する最小帯域幅量が保証されます。MRR が指定されていない場合、CIR は DOCSIS 仕様によりゼロに設定されます。

高優先度のトラフィック

高優先度のトラフィック フローは、データ転送インターフェイスの低遅延キュー（LLQ）にマッピングされます。LLQ 内のパケットは、同じインターフェイスのその他のキューよりも絶対最優先で処理されます。

次のサービス フローには高優先度のサービスが必要です。

- DOCSIS ダウンストリーム遅延 TLV がゼロより大きい値に設定されたサービス フロー。たとえば、PacketCable Multimedia Specification（PCMM）の音声コール。
- PacketCable ダウンストリーム サービス フロー。
- アップストリーム フローが非送信請求許可サービス（UGS）タイプ（非 PacketCable 音声コール）であるサービス フロー。

拡張レート帯域幅割り当て

DOCSIS WFQ スケジューラは、サービス フローの拡張レート帯域幅割り当て（ERBA）機能をサポートします。ERBA 機能を使用すると、ケーブル モデム（CM）は短時間だけ最大ライン レートまで伝送レートを一時的にバーストできます。この機能は、QoS プロファイルの既存のサービス レベルを変更せずに、瞬間的な帯域幅要求に対して高帯域幅を提供します。

DOCSIS WFQ スケジューラでは、それぞれのサービス フローが 1 つの専用キューを持つことができます。サービス フローで ERBA が有効な場合、ピーク レートはスケジューラ内のキュー シェープ レートとして実装されますが、最大持続レートはトークン バケットのリフィル レートとして設定されます。ERBA がオフのとき、バースト サイズおよびピーク レート値は使用されません。

最大トラフィック バースト パラメータは、サービス フローのバースト継続時間を制御するために使用されます。これにより、最大でチャネル ライン レートまで、または設定済みのピーク レートまで（最大許容バースト サイズ内にあるとき）バーストされます。Cisco cBR-8 コンバージド ブロードバンド ルータでは、この動作を明示的に制御するために **cableds-max-burst** コマンドを使用します。

（注） ERBA 機能は、高優先度のサービス フローおよびマルチキャスト サービス フローには適用できません。

次の表に、Cisco cBR-8 ルータの ERBA サポートを示します。

表 *199*：*Cisco cBR-8* ルータの拡張レート帯域幅割り当てサポート

	ポリサー レート	ポリサーの超過アクション	ポリサーのトークンバケットのサイズ	キュー シェープ レート
従来のサービス フロー	最大持続トラフィック レート（未使用）	送信	CMTS が内部で計算した値（未使用）	最大持続トラフィック レート
ERBA 対応サービス フロー	最大持続トラフィック レート	ドロップ	最大トラフィック バースト TLV	ピーク トラフィック レート

Cisco CMTS ルータでの ERBA サポートの詳細については、「DOCSIS 1.1 for the Cisco CMTS Routers」の「Using Enhanced Bandwidth Rate Allocation (ERBA) Support for DOCSIS 1.0 Cable Modems」を参照してください。

ピーク トラフィック レート

cableds-max-burst コマンドの *peak-rate* オプションにより、ERBA 対応サービス フローで使用できるピーク レートを指定できます。*peak-rate* 値はグローバル値であり、**cableds-max-burst** コマンドの設定後に作成されたすべてのサービス フローに適用されます。peak-rate のデフォルト値は 0 です。

サービス フローで DOCSIS 3.0 TLV 25.27 が指定されている場合、*peak-rate* 値は TLV 値として設定されます。ただし、ERBA がサービス フローでオンに設定されていない場合には *peak-rate* 値は無視されます。

peak-rate 値は、サービス クラス テンプレートの一部を形成するケーブル サービス クラスのコマンドでも設定できます。モデムの登録または動的サービス追加（DSA）操作中、サービス クラス名 TLV 25.4 が送信されて、サービス クラス テンプレートに一致する静的または動的ダウンストリーム サービス フローが作成されます。これらのダウンストリーム サービス フローは特定の *peak-rate* とともに作成されます。*peak-rate* が指定されない場合は、**cableds-max-burst** コマンドで指定した値が使用されます。

サービス フローにサービス クラスと TLV 25.27 の両方の定義による *peak-rate* がある場合、TLV で指定された *peak-rate* 値が使用されます。

DOCSIS 1.x または DOCSIS 2.0 に完全準拠しない DOCSIS 1.x、DOCSIS 2.0 ケーブル モデムが Cisco CMTS から TLV 25.27 を受信するとオンライン化に失敗する場合があります。これを回避するには、非 DOCSIS 3.0 ケーブル モデムにこの TLV が送信されるのを制限するために **cableserviceattributewithhold-TLVscommandwiththepeak-rate** キーワードを設定できます。

ボンディング グループの動的帯域幅共有を使用した DOCSIS 3.0 ダウンストリーム ボンディング サポート

DOCSIS 3.0 にはダウンストリーム チャネル ボンディングという概念が導入されています。各ボンディング グループ（BG）は、ダウンストリーム チャネルのコレクションで構成され、ダウンストリーム チャネルは 1 つ以上のボンディング グループによって使用できます。各ダウンストリームチャネルは、BG に属しながら、MAC ドメインでプライマリ チャネルとして動作して、未ボンディングのトラフィックを伝送することもできます。

DOCSIS 3.0 標準規格より前は、ダウンストリーム サービス フローは、単一のダウンストリーム インターフェイスに関連付けられていました。このダウンストリームインターフェイスは RF チャネル上の物理ダウンストリームに対応していました。DOCSIS 3.0 では、ダウンストリーム サービス フローはダウンストリーム ボンディング グループに関連付けられます。これらのボンディング グループは複数のダウンストリーム RF チャネルを使用できます。

DBS は、同じダウンストリーム チャネルを共有するワイドバンド（WB）インターフェイスおよび統合ケーブル（IC）インターフェイス用の動的帯域幅割り当てです。ボンディング グループのチャネル共有が原因で、ボンディング グループまたは未ボンディングのチャネルで使用可能な帯域幅は固定されません。帯域幅は、設定と WB または IC 上のトラフィック負荷によって異なります。

（注） ボンディング グループは WB インターフェイスとして、未ボンディングのチャネルは IC インターフェイスとして実装されます。

DBS モードでは、共有 RF チャネルの帯域幅は WB インターフェイスと IC インターフェイスの間で動的に割り当てられます。DBS は、高バースト トラフィックが存在する場合でも、基盤となる RF チャネル帯域幅の効率的な使用を可能にします。DBS は WB または IC インターフェイス レベルで設定されます。デフォルトでは、WB または IC チャネルの帯域幅は静的に割り当てられます（非 DBS）。

Cisco CMTS ルータでの DBS のサポートについては、「Dynamic Bandwidth Sharing on the Cisco CMTS Router」を参照してください。

DOCSIS WFQ スケジューラの設定方法

DOCSIS WFQ スケジューラ機能は自動的にロードされるため、設定することはできません。スケジュールに使用されるパラメータには、インターフェイス帯域幅とキュー パラメータが含まれます。

この項では、次の必須およびオプションの作業について説明します。

過剰率に対する DOCSIS プライオリティのマッピング

ここでは、ダウンストリーム サービス フローのカスタム過剰率に対して DOCSIS プライオリティをマッピングする方法について説明します。次のカスタムマッピングはデフォルトマッピングを上書きします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**interfacewideband-cable** *slot*/*subslot*/*port* :*wideband-channel* または **interfaceintegrated-cable** *slot*/*subslot*/*port* :*rf-channel* 例： `Router(config)# interface wideband-cable 2/0/0:0` or `Router(config)# interface integrated-cable 1/0/0:0`	指定したケーブル ダウンストリーム インターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**cabledownstreamqoswfqweigthts{weight1...weight8}** 例： `Router(config-if)# cable downstream qos wfq weights 10 20 30 40 50 60 70 80`	8 つのプライオリティにカスタム過剰率を設定します。 （注） カスタム値は、既存のサービス フローではなく、新しいサービス フローに対してのみ使用されます。
ステップ 5	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ダウンストリーム キュー情報の確認

モデムのダウンストリーム キュー情報を確認するには、**showcablemodem** [*mac-address* |*ip-address*]**service-flow** コマンドを使用します。

統合ケーブル インターフェイスまたはワイドバンド ケーブル インターフェイス上のすべてのキューの統計情報を確認するには、**showcabledpqueue** *interface* コマンドを使用します。

その他の参考資料

ここでは、DOCSIS WFQ スケジューラ 機能に関する参考資料について説明します。

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

DOCSIS WFQ スケジューラに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *200* : *DOCSIS WFQ* スケジューラに関する機能情報

機能名	リリース	機能情報
DOCSIS WFQ スケジューラ	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 79 章

DOCSIS インターフェイス間均等化

DOCSIS インターフェイス間均等化機能は、認定情報レート（CIR）フローには予約可能帯域幅を、ベストエフォート（BE）サービス フローには均等な帯域幅を隣接するボンディング グループ（BG）間で効率的に配布するための最適なメカニズムを導入します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *201*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

DOCSIS インターフェイス間均等化の前提条件

（注） このマニュアルで「ボンディング グループ（BG）」とは、DOCSIS インターフェイス間均等化機能の文脈におけるすべての組み込みケーブル（IC）とワイドバンドケーブル（WC）を表すために使用されています。IC インターフェイスは単一チャネル BG と見なされます。

DOCSIS インターフェイス間均等化の制約事項

- CIR フローで RF 帯域幅をすべて予約することはできません。CIR フローで予約できるのは、従来の CIR 帯域幅に加え、「bandwidth-percent」により静的に予約されていない RF 帯域幅の 90 パーセント[5] レガシー CIR 帯域幅に加えて、「bandwidth-percent」で静的に予約されていない RF 帯域幅の
- CIR 予約が従来の構成の「bandwidth-percent」で指定される静的予約可能な帯域幅を超えないようにするため、DOCSIS インターフェイス間均等化機能をディセーブルにする前に CIR 予約をクリアすることを推奨します。これは、DOCSIS インターフェイス間均等化機能をディセーブルにした後に CIR オーバーサブスクリプションが起きるのを防ぐためです。
- DOCSIS インターフェイス間均等化機能の効果はトポロジとフロー分散に依存します。特定のシナリオでは、DOCSIS インターフェイス間均等化機能を使用しても、BE の均等化も最大 CIR 使用率も達成されない場合があります。
- DOCSIS インターフェイス間均等化機能は、動的帯域幅共有（DBS）がイネーブルの IC および WB インターフェイスにのみ適用されます。

DOCSIS インターフェイス間均等化に関する情報

DOCSIS インターフェイス間均等化機能は、DOCSIS DOCSIS WFQ スケジューラ上の拡張機能です。ダウンストリーム CIR サービス フローが従来の構成で定義されたしきい値（つまり「bandwidth-percent」または「max-reserved-bandwidth」）を超えるインターフェイスで許可されます。たとえば、現在のパラメータが十分な帯域幅を保証できないときに、大規模な CIR フロー（マルチキャスト サービス フローなど）が許可されるようになります。しかしその成功率は、共通 RF チャネル内のケーブル インターフェイスの帯域幅の割り当てと予約によって異なります。

この機能は、共通 RF チャネルを使用するケーブル インターフェイス間でダウンストリーム BE サービス フローの均等な帯域幅も保証します。隣接 BG のすべてのアクティブなサービス フローにおけるフロー単位の帯域幅は、定期的に均等化されます。すべての BG の重み付け（DOCSIS トラフィック優先度（トラフィック優先度＋1））は、ダウンストリーム BE サービス フロー間で同

[5] CIR フローで予約可能な帯域幅は、静的部分と動的部分で構成されます。デフォルトで、帯域幅の静的部分は従来の構成から割り当てられます。帯域幅の動的な部分は、BE トラフィック用の各 RF チャネルに残っているヘッドルームから割り当てられます。

じです。帯域幅は、BE トラフィックに使用でき、追加の CIR フローを許可するために使用できます。

（注） DOCSIS トラフィック優先度については、『DOCSIS WFQ Scheduler on the Cisco CMTS Routers』ガイドを参照してください。

オンデマンド CIR の取得

RF チャネルの帯域幅が複数のボンディング グループで共有され、現行のボンディング グループの保証帯域幅が不十分の場合、この機能により、近くのボンディング グループの予約済みでない保証帯域幅を現行のボンディング グループの CIR 用に「借りる」ことができます。

この機能は、マルチキャスト サービス フローによってのみ使用されます。

ボンディング グループ間均等化

DOCSIS インターフェイス間均等化機能は、集約されたアクティブ フロー数の重み値（これは EIR 要求）を使用して、予約可能な帯域幅を定期的に再調整します。異なるボンディング グループで同じ重みのサービス フローは、ほとんど同じスループットになります。

OFDM チャネル

OFDM チャネル

DOCSIS 3.1 は、スループットおよびスペクトル効率を高めるためのモードを導入する一方で、DOCSIS 3.0 との後方互換性も維持しています。OFDM チャネル サポートでは、チャネル帯域幅 24 Mhz ～ 192 MHz でポートごとに 1 つの OFDM チャネルが含まれます。Cisco IOS-XE 16.5.1 では、SC-QAM および OFDM チャネルでボンディング グループを構成できます。1 つの OFDM チャネルに複数のプロファイルを設定し、各プロファイルに異なるレートを指定できます。使用されているプロファイルに応じて、OFDM チャネル レートは常に異なる可能性があります。OFDM チャネルの詳細については、『*OFDM Channel Configuration Guide*』を参照してください。

OFDM チャネル レート

1 つの OFDM チャネルに複数のプロファイルを設定し、各プロファイルに異なるレートを指定することができます。たとえば 96MHz の OFDM チャネルに、変調 1024-QAM のプロファイル A（制御プロファイル）、変調 2048-QAM のプロファイル B、変調 4096-QAM のプロファイル C を設定した場合、プロファイル A、B、C のプロファイル レートはそれぞれ 616Mbps、680Mbps、736Mbps となります。

Cisco IOS-XE 16.5.1 では、OFDM チャネルで制御プロファイル（プロファイル A）とデータ プロファイル（プロファイル B、C など）が設定されている場合、DOCSIS インターフェイス間均等化の計算には最小のデータ プロファイル レートが使用されます。それ以外の場合は、制御プロファイル レートが使用されます。

インターフェイス帯域幅

ワイドバンドケーブル（WB）インターフェイスにSC-QAMとOFDMチャネルの両方を含めることができます。OFDMチャネルが含まれる場合、インターフェイス帯域幅の計算で最大プロファイル レートが使用されます。

たとえば、96MHzのOFDMチャネルに、変調1024-QAMのプロファイルA、変調2048-QAMのプロファイルB、変調4096-QAMのプロファイルCを設定した場合、プロファイルA、B、Cのプロファイル レートはそれぞれ616Mbps、680Mbps、736Mbpsとなります。この場合、インターフェイス帯域幅の計算には736Mbpsが使用されます。

DOCSISインターフェイス間均等化の設定方法

ここでは、DOCSISインターフェイス間均等化機能を導入するために必要な次のタスクについて説明します。

DOCSISインターフェイス間均等化の設定

ここでは、ケーブル インターフェイスのDOCSISインターフェイス間均等化機能を有効にする方法について説明します。この設定は、ルータ上のすべてのWBまたはICインターフェイスに適用されます。

制約事項

CIR予約が従来の設定の「bandwidth-percent」で指定された静的予約可能帯域幅を超えないようにするために、DOCSISインターフェイス間均等化機能を無効にする前にCIR予約をクリアにすることを推奨します。

手順

	コマンドまたはアクション	目的
ステップ1	**enable** 例： `Router> enable`	特権EXECモードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ2	**configure terminal** 例： `Router# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**cableacfeenable** 例： `Router(config)# cable acfe enable`	ケーブルインターフェイスでDOCSISインターフェイス間均等化機能を有効にします。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

超過情報レート最大比率の設定

ここでは、隣接する BG 内の BE 帯域幅の超過情報レート（EIR）最大比率を設定する方法について説明します。

EIR 比率は、BG 間の EIR 帯域幅の最大差を維持するために使用されます。これにより、BG（アクティブ BE サービス フローがわずかしかない）の EIR 帯域幅が非常に狭くなったり、ゼロになることを防ぎます。そうしないと、これらの BG の EIR 帯域幅が非常に狭くなるだけで、CIR フローを許可できなくなります。

たとえば、同じ RF チャネルを共有する 2 つの BG 共有があり、BG1 には 1000 アクティブ BE サービス フローがあり、BG2 には何もないとします。「max-eir-ratio」を使用しないと、BG1 がすべての帯域幅を使用し、BG2 の帯域幅がなくなってしまいます。音声 CIR が BG2 の帯域幅を使用しようとすると、拒否されてしまいます。「max-eir-ratio」を 10 に設定すると、BG2 は、音声 CIR の許可に十分な QAM の約 10 パーセントを取得します。「max-eir-ratio」は、完全な均等化と CIR 使用率でトレードオフされます。つまり、一部の BG が他の BG に何も残らないようにすべての帯域幅を取得しないようにするために「フローの均等化」が低下します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**cableacfemax-eir-ratio** *eir-ratio* 例： `Router(config)# cable acfe max-eir-ratio 20`	隣接する BG 内の BE 帯域幅で EIR 最大比率を設定します。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

超過情報レート一定需要の設定

ここでは、ボンディング グループに関する一定の超過情報レート（EIR）需要を設定する方法を説明します。EIR 需要は、BG 間の相対帯域幅を決定するために使われる、単位のない値です。

DOCSIS 優先度 0 のアクティブな EIR フローには、ACFE モジュールで 1000 需要単位が割り当てられます。したがって、constant-eir-demand が 1 に設定された BG に与えられる帯域幅は、単一サービス フローの帯域幅の 1/1000 以下に限られます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 acfe constant-eir-demand** *value* 例： `Router(config)# cable acfe constant-eir-demand 20`	BG の EIR 一定需要として 20 を設定します。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

最大ボーナス帯域幅の設定

ここでは、BG で利用可能な最大ボーナス帯域幅を設定する方法について説明します。

ボーナス帯域幅とは、DOCSIS インターフェイス間均等化により、CIR 予約の各 BG に提供される追加の帯域幅です。デフォルトの最大ボーナス帯域幅設定では、1 つの BG で基盤となる RF 帯域幅をすべて予約できます。最大ボーナスを設定すると、スケジューラが帯域幅の増加を保証しても、AC モジュールはその設定値を超える CIR フローを許可しません。これにより、BG での CIR フローの枯渇を効果的に防ぎます。

（注） **cableacfemax-bonus-bandwidth** コマンドの設定は、新しく受信される CIR フローにのみ適用されます。これにより、**max-bonus-bandwidth** を超える既存の CIR フローが終了されることはありません。

制約事項 最大ボーナス帯域幅がインターフェイスの現在の CIR 予約を下回る場合、CIR 予約が最大ボーナス帯域幅設定を下回るまで、新しい CIR フローは何も許可されません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface** {**wideband-cable** | **interface-cable** }*slot*/*subslot* /*port* :*interface-num*	設定するインターフェイスを指定します。

	コマンドまたはアクション	目的
	例： `Router(config)# interface wideband-cable 1/0/0:0`	（注） 引数の有効値は、CMTSルータとケーブル インターフェイス ライン カードに応じて異なります。サポート対象の値については、ルータ シャーシとケーブル インターフェイス ライン カードのハードウエア マニュアルを参照してください。
ステップ 4	**cableacfemax-bonus-bandwidth** *bonus-bandwidth* 例： `Router(config-if)# cable acfe max-bonus-bandwidth 1000000`	BG で利用可能な最大ボーナス帯域幅を設定します。
ステップ 5	**end** 例： `Router(config)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

DOCSIS インターフェイス間均等化の確認

DOCSIS インターフェイス間均等化機能をモニタリングするには、次の手順を使用します。

予約可能帯域幅の確認

特定のインターフェイスの予約済み帯域幅と予約可能帯域幅を表示するには、次の例に示すように **showinterface{wideband-cable|modular-cable|integrated-cable}** コマンドを使用します。

```
Router# show interfaces wideband-cable 1/0/0:1 downstream
Total downstream bandwidth 1875 Kbps
Total downstream reserved/reservable bandwidth 20000/1500 Kbps
Total downstream guaranteed/non-guaranteed bonus bandwidth 20760/9741 Kbps
Router#
```

「予約可能帯域幅」は、従来の設定の保証帯域幅に含まれます。DOCSIS インターフェイス間均等化機能を無効にすると、「保証ボーナス帯域幅」と「非保証ボーナス帯域幅」の両方の値がゼロになります。この機能を有効にすると、「予約可能帯域幅」および「保証ボーナス帯域幅」は、インターフェイスで予約可能な最大 CIR を表示します。この制限を超えるユニキャスト CIR フローは拒否されます。「非保証ボーナス帯域幅」を追加すると、マルチキャスト CIR フローが AC モジュールを通過できます。ただし、帯域幅は共有プールから発生するため、サービス フローの作成に失敗する場合があります。

特定のインターフェイスの予約済み帯域幅と予約可能帯域幅を表示するには、次の例に示すように **showcableadmission-controlinterface** コマンドを使用します。

```
Router#show cable admission-control interface wideband-Cable 1/0/0:0

Interface Wi1/0/0:0
BGID: 28673

Resource - Downstream Bandwidth
--------------------------------
App-type    Name       Reservation/bps    Exclusive
1                      0                  Not configured
2                      0                  Not configured
3                      0                  Not configured
4                      0                  Not configured
5                      0                  Not configured
6                      0                  Not configured
7                      0                  Not configured
8                      20000000           Not configured
Max Reserved BW = 1500000 bps
Total Current Reservation = 20000000 bps
Guaranteed Bonus BW = 20760000 bps
Non-guaranteed Bonus BW = 9741000 bps
Subset BGs: In1/0/0:8 In1/0/0:9 In1/0/0:10 In1/0/0:11 In1/0/0:12
Superset BGs: N/A
Overlapping BGs: Wi1/0/0:8 Wi1/0/0:9 Wi1/0/0:10
Router#
```

Cisco IOS-XE リリース 3.18.0SP 以降、キャパシティ BW も表示されます。これは、このインターフェイスの RC チャネルのチャネル キャパシティの要約です。OFDM チャネルのキャパシティは、最小プロファイル レートを考慮して計算されます。

```
Router#show cable admission-control interface wideband-Cable 2/0/0:1

Interface Wi2/0/0:1
BGID: 8194

Resource - Downstream Bandwidth
--------------------------------
App-type    Name       Reservation/bps    Maximum        Rejected
1                      4000               90%            0
2                      0                  N/A            0
3                      0                  90%            0
4                      0                  N/A            0
5                      0                  N/A            0
6                      0                  90%            0
7                      0                  N/A            0
8                      0                  87%            0
Max Reserved BW = 11424000 bps
Total Current Reservation = 4000 bps
Guaranteed Bonus BW = 884352000 bps
Non-guaranteed Bonus BW = 225904000 bps
Capacity BW = 1428000000 bps
Subset BGs: In2/0/0:0 In2/0/0:1 In2/0/0:2 In2/0/0:3 In2/0/0:4 In2/0/0:5 In2/0/0:6 In2/0/0:7
 In2/0/0:158 Wi2/0/0:0
Superset BGs: N/A
```

DOCSIS インターフェイス間均等化のグローバル ステータスと統計情報の確認

DOCSISインターフェイス間均等化機能のグローバル ステータスおよび統計情報を表示するには、**showcableacfesummary** コマンドを使用します。

```
Router# show cable acfe summary
ACFE state: Enabled
EIR Rebalance period (secs): 5
```

```
EIR Rebalance invocations:   254
CIR Acquire rate/limit:      100/100
CIR Acquire invocations:     0
CIR Acquire throttled:       0
CIR Oversubscriptions:       0
Maximal EIR ratio:           10
Constant EIR demand:         2
```

コントローラ別 DOCSIS インターフェイス間均等化のステータスと統計情報の確認

各コントローラ インターフェイスのステータスおよび統計情報を表示するには、次の例に示すように **showcableacfecontroller** コマンドを使用します。

```
Router# show cable acfe controller integrated-Cable 1/0/0
EIR Rebalance invoked: 450963
Adaptive CIR granted: 20
Adaptive CIR rejected: 1
Total clusters: 9
RF FlexBW
8 36376
9 36376
10 32625
......
```

BG クラスタは複数のチャネル全体に広がり、基盤となる RF チャネル帯域幅を動的に共有する手段として使用されます。

show controllers integrated-Cable acfe cluster コマンドを使用すると、次のようなコントローラ別の統計情報とクラスタを表示して、帯域幅情報を確認できます。

```
Router# show controllers integrated-Cable 1/0/0 acfe cluster 0
Integrated-Cable 1/0/0 status:
Topology changed: No

========Cluster 0========
Number of RF: 2
RF FlexBW  WB  ExcessBW Quanta
0  35625   -   35438    35438
           0   187   187
1  35250   0  35250   35250

Number of BG: 2
Intf Demand CIR Max  CstrMin Alloc NBonus Ratio
WB0  1000  0  70875  35250  35437  35438  14855190400
IC0  1000  0  35625  0      35438  187    14855609600
```

インターフェイス別 DOCSIS インターフェイス間均等化のステータスと統計情報の確認

各インターフェイスのステータスおよび統計情報を表示するには、次の例に示すように **showcableacfeinterface** コマンドを使用します。

```
Router# show cable acfe interface wideband-cable 1/0/0:1
EIR Demand (raw/scale):   0/1
Per-Flow EIR BW (kbps):   19125
Guar Bonus BW (kbps):     19125
Non-guar Bonus BW (kbps): 38250
```

```
Reserved Bonus BW (kbps): 0
!
```

DOCSIS インターフェイス間均等化の設定例

ここでは、Cisco CMTS ルータでの DOCSIS インターフェイス間均等化の設定例の設定例を示します。

例：DOCSIS インターフェイス間均等化

次に、ルータ上で有効化された DOCSIS インターフェイス間均等化機能の例を示します。

```
Current configuration : 39682 bytes
!
! Last configuration change at 04:30:02 UTC Wed Jan 19 2
! NVRAM config last updated at 04:23:17 UTC Wed Jan 19 2
!
version 12.2
!
cable clock dti
cable acfe enable
!
.
.
.
```

例：超過情報レートの最大需要比率

次に、ルータで設定された超過情報レートの最大需要比率の例を示します。

```
Building configuration...
Current configuration : 54253 bytes
!
version 12.2
!
cable clock dti
cable acfe enable
cable acfe max-eir-ratio 20
!
```

cable acfe max-eir-ratio コマンドの効果を実際に示すために、シンプルな BG クラスタを使用します。

```
!
interface integrated-Cable1/0/0:0
cable bundle 1
 cable rf-bandwidth-percent 10
!
interface Wideband-Cable9/0/0:0
 cable bundle 1
  cable rf-channels channel-list 0
  bandwidth-percent 1
  end
!
```

この RF チャネルでは、大域幅の 20% が「bandwidth-percent」で予約されているため、DOCSIS インターフェイス間均等化機能で使用できるのは、27 Mbps（(100 - 20) * 90 * 37.5）です。

「max-eir-ratio」が 100 を超え、WB インターフェイスに 99 のアクティブ BE フローがあるけれども、IC インターフェイスの BE フローが 1 つしかない場合、IC インターフェイスで得られるのは

270 kbps（ボーナス大域幅の 1/(1+99)*27）のみです。BE トラフィックが完全に均等化されます。ただし、ボーナス帯域幅を超えるため、IC インターフェイスで 270 kbps を超えるユニキャスト CIR フローを許可することはできません。「max-eir-ratio」を 10 に設定すると、IC インターフェイスに 99/10 フローが付与されるため、割り当てられるボーナス帯域幅が大きくなります。「max-eir-ratio」は、完全な均等化と CIR 使用率でトレードオフされます。

例:：EIR の一定需要

次に、ルータでの EIR 一定需要の設定例を示します。

```
Building configuration...
Current configuration : 54253 bytes
!
version 12.2
!
cable clock dti
cable acfe enable
cable acfe max-eir-ratio 20
cable acfe constant-eir-demand 2
!

!
interface integrated-Cable1/0/0:0
cable bundle 1
 cable rf-bandwidth-percent 10
 cable acfe constant-eir-demand 2
!
interface Wideband-Cable9/0/0:0
 cable bundle 1
  cable rf-channels channel-list 0
  bandwidth-percent 1
  cable acfe constant-eir-demand 2
  end
!
```

例：最大ボーナス帯域幅

次に、ルータ上で有効化された最大ボーナス帯域幅の例を示します。

```
Building configuration...
Current configuration : 274 bytes
!
interface Wideband-Cable1/0/0:0
cable bundle 1
cable rf-channel 0 bandwidth-percent 10
cable acfe max-bonus-bandwidth 10000
end
!
```

このインターフェイス単位の設定では、DOCSIS インターフェイス間均等化機能が、WB インターフェイスに 10 Mbps 以上を保証しても、AC モジュールは、従来の保存可能な帯域幅を超える 10 Mbps 帯域幅を渡すことはありません。

```
!
.
.
.
```

その他の参考資料

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

DOCSIS インターフェイス間均等化に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *202*：ダウンストリーム インターフェイスの設定に関する機能情報

機能名	リリース	機能情報
DOCSISインターフェイス間均等化	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 80 章

サービス グループ アドミッション コントロール

このドキュメントでは、サービス グループ アドミッション コントロール機能について説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「Bug Search Tool」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *203* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

サービス グループ アドミッション コントロールに関する制限事項

- SGAC を設定するには、DOCSIS インターフェイス間均等化機能が有効になっている必要があります。

- SGAC は、ダウンストリームのみをサポートします。

サービス グループ アドミッション コントロールについて

概要

サービス グループ アドミッション コントロール（SGAC）とは、着信サービス要求の処理とサポートで 1 つ以上のリソースが利用不可の場合に、アドミッション要求に基づいてグレースフルにサービス グループを管理するメカニズムのことです。このようなメカニズムがないと、新しい要求が予期しない動作を伴って失敗するだけでなく、進行中のフローで品質に関する問題が発生する可能性もあります。SGAC はそのようなリソースを継続的にモニタリングし、リソースの可用性に基づいて要求を受け入れるか、拒否します。

SGAC により、コール アドミッション時に Quality of Service（QoS）に関するある程度の保証を加入者に提供できるとともに、リソース消費量がクリティカルなレベルに近づくとグレースフルにサービス レベルを低減できます。予測不可能なトラフィック需要によって加入者への QoS が低下するような状況でも、SGAC によってその影響を軽減できます。

（注） SGAC はモニタリング対象のリソースに応じて、クリティカルしきい値を超過した時点、または Cisco CMTS で帯域幅がほぼ使い果たされた時点のいずれかで、サービス レベルをグレースフルに低減させ始めます。

SGAC では、Cisco CMTS 上のリソースごとにしきい値を設定できます。これらのしきい値は、リソースの最大許容使用量に対する割合として表されます。所定のリソースのしきい値を超過するたびに、アラーム トラップを送信できます。

ダウンストリーム（DS）チャネルの場合、ファイバ ノードごとにしきい値を使用して帯域幅割り当てを設定できます。

SGAC とダウンストリーム帯域幅使用率

SGAC を使用すると、さまざまな DOCSIS トラフィック タイプまたはアプリケーション タイプに関して帯域幅の使用を制御できます。アプリケーション タイプを定義するには、ユーザが CLI を使用してサービス フローを分類します。

サービス フローの分類

SGAC 機能を使用すると、アプリケーションのタイプに基づいて帯域幅を割り当てることができます。フロー分類では、最大 8 つのアプリケーション タイプまたはバケットに帯域幅を分割できます。バケットの構成はコマンドライン インターフェイス（CLI）で定義され、それと同様にサービス フローをこれら 8 つのアプリケーション バケットのいずれか 1 つに分類するためのルールも CLI で定義されます。サービス フローのさまざまな属性を使用して、ルールを定義できます。

PacketCable で作成されたフローには、次の属性を使用できます。

- フローに関連付けられた PacketCable ゲートの優先度（高または標準）

PacketCable MultiMedia（PCMM）で作成されたフローには、次の属性を使用できます。

- ゲートの優先度（0 ～ 7）
- アプリケーション タイプ（0 ～ 65535）

すべてのフローは次の属性タイプを使用します。

- サービス クラス名

サービス フローが受け入れられる前に、分類ルールがそれに適用されます。サービス フローのさまざまな属性がユーザ設定のルールと比較されます。ルールとの一致に応じて、サービス フローにはアプリケーション タイプ (1 ～ 8）のラベルが付けられます。次に、アプリケーション タイプに従って帯域幅割り当てが行われます。

サービス フローが受け入れられる前に、その属性に基づいて分類されます。一度に 1 バケットずつ、フロー属性と CLI で設定されたルールが比較されます。いずれかのルールに一致した場合、そのバケットでサービス フローにラベルが付けられ、それ以上の検査は行われません。

バケット 1 のルールが最初にスキャンされ、バケット 8 のルールが最後にスキャンされます。2 つの異なるバケットの 2 つの異なるルールが同じサービス フローに一致した場合、そのフローは最初の一致に従って分類されます。一致が見つからない場合、そのフローはベスト エフォート（BE）として分類され、ベスト エフォート ルールを含むバケットのラベルがフローに付けられます。デフォルトでは、BE バケットはバケット 8 です。

ダウンストリーム帯域幅のしきい値

SGAC は、設定済みの最大予約帯域幅を使用して、ダウンストリーム帯域幅使用量をモニタリングします。サービス フローの最小レートがゼロ以外の値で、それによって予約帯域幅の合計が設定済みしきい値を超えることになる場合、SGAC はそのサービス フローを拒否します。

柔軟な帯域幅割り当て

さまざまなアプリケーション タイプに関する帯域幅割り当ての制限という問題に対処するには、標準優先度の音声フローと緊急音声フローの両方にアドミッション コントロールを適用できます。それには、しきい値を拡張して、ファイバノード内でアプリケーション タイプのグループを割り当てます。それぞれのダウンストリーム サービス フローは、引き続き単一のアプリケーション タイプに分類されます。ただし、アプリケーション タイプとしきい値の間の 1 対 1 のマッピングは存在しなくなります。

こうして、設定された各しきい値と、それに関連付けられたアプリケーション タイプ グループを 1 つの制約として扱うことができます。特定のアプリケーション タイプに分類されるサービス フローは、そのアプリケーション タイプに関連付けられたすべての制約を通過する必要があります。

ボンディング グループ アドミッション コントロールの概要

DOCSIS 3.0 で導入されたボンディング グループ（つまり束ねられたチャネル）を使用すると、単一のケーブル モデムが複数の RF チャネルを介してデータを送信でき、より高いスループットが実現します。これらのボンディング グループはアップストリームとダウンストリームの両方のチャネルに定義されます。ボンディング グループは、複数の RF チャネルを結合することによって作成されます。また、単一の RF チャネルを複数のボンディング グループで共有することもできます。

（注） Cisco IOS-XE 3.18.0SP リリース以降、DOCSIS 3.1 に従い、ボンディング グループに OFDM チャネルが含まれる場合、予約可能なボンディング グループ帯域幅合計（キャパシティ）は、最も効率の低い使用可能な OFDM プロファイルを使って計算されます。

ボンディング グループ SGAC 機能では、1 つのアプリケーション タイプに対する予約済み最大帯域幅を、利用可能な帯域幅の一部として定義できます。この帯域幅の一部は、予約可能な帯域幅合計に占めるパーセンテージ値として定義されます。

サービス グループ アドミッション コントロールの設定、モニタリング、およびトラブルシューティング方法

デフォルト設定がデフォルトで有効になっているため、設定手順はオプションです。ここでは、SGAC のデフォルト運用と非デフォルト運用の両方のために SGAC を非デフォルト設定、モニタリング、デバッグするための一連の手順を紹介します。

サービス フロー分類ルールの定義

この手順では、Cisco CMTS でサービス フロー分類ルールを定義する方法を説明します。この手順は柔軟で、**cableapplicationtypeinclude** コマンドのバリエーションを使用して、デフォルトのグローバル サービス フロー ルールを変更します。

Cisco CMTS 上で SGAC を設定/再設定する際は、ここで説明するステップやコマンドを、ほとんどあらゆる組み合わせで使用できます。

（注） SGAC 用のアプリケーション ルールはグローバルに設定され、さまざまなダウンストリーム帯域幅リソースが同じサービス フロー ルール セットを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cableapplication-type** *n* **include packetcable** { **normal** | **priority** } 例： `Router(config)# cable application-type 5 include packetcable priority`	PacketCable の場合、このコマンドにより PacketCable サービス フロー属性を指定のバケットにマッピングします。PacketCable サービス フローが PacketCable ゲートに関連付けられます。ゲートは標準または高優先度に指定できます。

ステップ 4	**cableapplication-type** *n* **include pcmm** {**priority** *gate-priority* / **app-id** *gate-app-id* }
	
	例：
	
	`Router(config)# cable application-type 2 include pcmm priority 7`
	`Router(config)# cable application-type 2 include pcmm app-id 152`
		PCMM の場合、このコマンドにより PCMM サービス フロー優先度またはアプリケーションを指定のバケットにマッピングします。PCMM ゲートは、優先度レベルおよびアプリケーション識別子によって特徴付けられます。

ステップ 5	**cable application-type** *n* **include service-class** *service-class-name* 例： `Router(config)# cable application-type 1 include service-class stream1`	サービス クラス パラメータの場合、このコマンドのバリエーションはサービス クラス名をサービス フローに適用し、対応する QoS パラメータを適用します。 サービス クラスの概念は、DOCSIS 1.1 で導入されました。サービス クラスはサービス クラス名で識別されます。サービス クラス名は、Cisco CMTS が QoS パラメータ セットに関連付ける文字列です。サービス クラスを使用する目的の 1 つは、上位レベルのプロトコルで適切な QoS パラメータ セットを使用してサービス フローを作成できるようにすることです。アプリケーションをサービス フローにバインドするには、サービス クラスを使用すると便利です。ルールが、このようなバインディングを実装するためのメカニズムとなります。

	コマンドまたはアクション	目的
		このステップでコマンドを使用する際には、次の要因に注意してください。 • サービス フローを定義するために **cableserviceclass** コマンドを使用して個別にサービス クラスを設定します。 • 名前付きサービス クラスは、任意のアプリケーションのタイプに分類できます。 • アプリケーション タイプごとに、最大 10 個のサービス クラス名を設定できます。10 個を超えるサービス クラスを設定しようとすると、エラー メッセージが出力されます。 • 新しいクラスを追加する前に、 **nocable traffic-type** コマンドを使用してサービス クラスの設定を削除する必要があります。
ステップ 6	**cable application-type** *n* **include BE** **例：** `Router# cable application-type 3 include BE`	ベスト エフォート サービス フローの場合、このコマンドのバリエーションはステップ 3 を拡張し、非ゼロの設定情報レート（CIR）を使ってベスト エフォート サービス フローのデフォルト バケット 8 を変更します。ケーブル モデムの登録時には、これらの BE サービス フローがしばしば作成されます。
ステップ 7	Ctrl-Z **例：** `Router(config)# Ctrl^Z`	特権 EXEC モードに戻ります。

以下に、高優先度の PacketCable サービス フローをアプリケーション バケット 5 にマッピングする例を示します。

```
Router(config)# cable application-type 5 include packetcable priority
```

以下に、標準優先度の PacketCable サービス フローをアプリケーション バケット 1 にマッピングする例を示します。

```
Router(config)# cable application-type 1 include packetcable normal
```

以下に、指定のバケット番号を、優先度 7 の PCMM サービス フローにマッピングした後、この同じバケット番号にアプリケーション ID 152 をマッピングする例を示します。

```
Router(config)# cable application-type 2 include pcmm priority 7
Router(config)# cable application-type 2 include pcmm app-id 152
```

以下に、ベスト エフォート CIR フローをバケット 3 にマッピングする例を示します。

```
Router(config)# cable application-type 3 include BE
```

アプリケーション バケット名の設定

この手順に従うことで、SGACがサポートする8つのアプリケーションバケットのうちの6つに、英数字からなる名前を割り当てることができます。デフォルトのバケット識別子は、1 ～ 8 の範囲です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cableapplication-type** *n***name** *bucket-name* 例： `Router(config)# cable application-type 7 name besteffort`	指定されたバケットに英数字の名前を割り当てます。 （注） サポートされる **show** および **debug** コマンドでは、このバケット名がデフォルトのバケット番号とともに表示されます。
ステップ 4	Ctrl-Z 例： `Router(config)# Ctrl^Z`	特権 EXEC モードに戻ります。

高優先度の緊急 911 コールのプリエンプション

高優先度の音声（911）トラフィックに排他的共有帯域幅が与えられるようにSGACルールとしきい値を設定できます。緊急911トラフィックの平均通話量はそれほど高くないため、緊急911コールに予約する帯域幅の割合は小さくてもかまいません。ただし、局地的な緊急事態が発生すると、緊急 911 コールの通話量が急増する可能性があります。その場合は、通常の音声トラフィックの一部をプリエンプション処理して、緊急 911 コールの急増に対応する必要が生じます。

Cisco CMTS ソフトウェアは、1 つ以上の標準優先度の音声フローをプリエンプション処理し、高優先度の音声フローに帯域幅を譲ります。SGAC には、このプリエンプション機能を有効または無効にするためのコマンドライン インターフェイス（CLI）が用意されています。

SGAC のプリエンプション ロジックは、次の手順に従います。

1. 最初のアドミッション コントロールで高優先度の PacketCable フローを許可できない場合、通常の PacketCable コール用に設定された別のバケットでそのフローを許可できるかどうか検査します（PacketCable 標準ルールと高優先度ルールがそれぞれ別のバケットに設定されている場合にのみ当てはまります）。帯域幅が使用可能な場合、コールは標準優先度のバケットで受け入れられます。
2. 標準優先度のバケットに余裕がない場合、標準優先度 PacketCable フローをプリエンプション処理し、低優先度フローがプリエンプションされたバケットで高優先度フローを受け入れます。
3. プリエンプション処理できる標準優先度フローがない場合、高優先度フローの受け入れを拒否します。通常は、標準優先度バケットと高優先度バケットの両方が 911 フローで満杯になっている場合にこれが発生します。

このプリエンプションは、PacketCable 高優先度フローにのみ適用されます。

ダウンストリームの低優先度サービス フローがプリエンプション対象として選択されると、反対方向でも対応する同じ音声コールのサービス フローがプリエンプション処理されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	[**no**] **cableadmission-controlpreemptpriority-voice** 例： `Router(config)# no cable admission-control preempt priority-voice`	Cisco CMTS のデフォルト緊急 911 コール プリエンプション機能を変更し、Cisco CMTS でその他のすべてのバケットに優先して、緊急 911 コールのスループットおよび帯域幅要件がサポートされるようにします。 このコマンドの **no** 形式はこのプリエンプションを無効にし、緊急 911 コールをサポートするバケットを Cisco CMTS で

	コマンドまたはアクション	目的
		のデフォルト設定および標準機能に戻します。

ステップ 4	**Ctrl-Z**
	
	例：
	`Router(config)# Ctrl^Z`
	`Router#`
		特権 EXEC モードに戻ります。

帯域幅利用率の計算

SGAC 機能は各 US/DS チャネルに対してカウンタを維持します。カウンタには現在の帯域幅予約が保持されます。新規サービス フローを作成するためのサービス リクエストが出されるたびに、SGAC は新規フローに必要な帯域幅を推定して、それをカウンタに加算します。推定帯域幅は次のように計算されます。

- DS サービス フローの場合、必要な帯域幅は、DOCSIS サービス フローの QoS パラメータで指定された最小予約レートです。

上記の各計算で、SGAC は PHY オーバーヘッドを考慮しません。DOCSIS オーバーヘッドは UGS フローと UGS-AD フローでのみ計上されます。利用可能な帯域幅部分を推定するための計算では、PHY オーバーヘッドと DOCSIS オーバーヘッドだけでなく、DOCSIS メンテナンス メッセージをスケジュール設定する際に発生するオーバーヘッドも考慮する必要があります。SGAC は補正係数（80 %）を raw データ レートに適用して、利用可能な帯域幅の合計を計算します。

（注） 束ねられたチャネルでの DS フローと US フローの場合、最大予約帯域幅は、SGAC しきい値に定義された帯域幅です。この値は Kbps 単位で示されます。

SGAC チェックの有効化

CMTS で設定したファイバ ノードには、HFC 設備で一致する物理ファイバ ノードが 1 つ以上表示されます。CMTS は、設備内の物理ファイバ ノードの DOCSIS ダウンストリーム サービス グループ（DS-SG）および DOCSIS アップストリーム サービス グループ（US-SG）を特定するのに、ファイバ ノード構成を使用します。MAC ドメイン内の MAC ドメイン ダウンストリームおよびアップストリームのサービス グループ（それぞれ MD-DS-SG と MD-US-SG）の計算が自動的に行われるように、サービス グループ情報は MAC ドメイン チャネル設定と比較されます。

アプリケーション タイプ、およびサービス グループに許可される指定のアプリケーション タイプのサービス フローに対して SGAC チェックを有効にするには、各光ファイバ ノードで次の手順に従います。

はじめる前に

予約帯域幅を柔軟に調整できるようにするには、DOCSIS インターフェイス間均等化機能を常に有効にして、各ボンディング グループに設定される帯域幅パーセンテージを最小限に維持してください。

制限事項

SGAC はダウンストリームでのみサポートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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 fiber-node** *id* 例： `Router(config)# cable fiber-node 1`	ケーブル ファイバ ノード コンフィギュレーション モードを開始し、ファイバ ノードを設定します。
ステップ 4	**admission-control application-type** *n***ds-bandwidth** *pct* 例： `Router(config-fiber-node)# admission-control application-type 1 ds-bandwidth 1`	指定したアプリケーション タイプに関する SGAC チェックを有効にします。 SGAC チェックを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 5	Ctrl-Z 例： `Router(config-if)# Ctrl^Z`	特権 EXEC モードに戻ります。

次の作業

アドミッション コントロールの設定を確認するには、**show cable admission-control fiber-node** を使用します。

SGAC の設定例

ここでは、Cisco CMTS での SGAC 機能のソリューション レベルの例を記載します。.デフォルトおよび非デフォルトの運用設定での SGAC の機能について説明します。

例：SGAC 設定コマンド

設定例のこのセクションでは、Cisco CMTS 上で次の SGAC パラメータを設定します。

- すべての PacketCable フローがバケット 1 にマップされます。
- BE サービス フローがバケット 8 にマップされます。

次の設定コマンドにより、これらの設定が有効になります：

- PacketCable 音声フローをマップするには、次のコマンドを使用します。

```
cable application-type 1 include packetcable normal
cable application-type 1 include packetcable priority
cable application-type 1 name PktCable
```

- BE フローをバケット 8 にマップするには、次のコマンドを使用します。

```
cable application-type 8 name HSD
cable application-type 8 include best-effort
```

- 上記の設定に従い、PCMM ストリーミング ビデオ アプリケーションへの帯域幅割り当てを制御することもできます。ストリーミング ビデオ アプリケーションは、PCMM アプリケーション ID 35 によって識別されます。次のコマンドが、この設定を実装します。

```
cable application-type 2 name PCMM-Vid
cable application-type 2 include pcmm app-id 35
```

- これらの設定を Cisco CMTS 上で確認するには、次の **show** コマンドを使用します。

```
Router# show cable application-type
For bucket 1, Name PktCable
     Packetcable normal priority gates
     Packetcable high priority gates
For bucket 2, Name PCMM-Vid
     PCMM gate app-id = 30
For bucket 3, Name Gaming
     PCMM gate app-id = 40
For bucket 4, Name
For bucket 5, Name
For bucket 6, Name
For bucket 7, Name
For bucket 8, Name HSD
     Best-effort (CIR) flows

Router# show cable admission-control fiber-node 1
App-type    Name       Exclusive
1                      N/A
2                      N/A
3           Normal     10%
```

```
4                       N/A
5                       N/A
6                       N/A
7           Emergency   N/A
8                       N/A

Router#show cable admission-control interface integrated-Cable 8/0/0:0

Interface In8/0/0:0
RFID 24576

Resource - Downstream Bandwidth
-------------------------------
App-type    Name        Reservation/bps    Exclusive      Rejected
1                       0                  N/A            0
2                       0                  N/A            0
3           Normal      0                  10%            0
4                       0                  N/A            0
5                       0                  N/A            0
6                       0                  N/A            0
7           Emergency   0                  N/A            0
8                       0                  N/A            0
Max Reserved BW = 300000 bps
Total Current Reservation = 0 bps
Guaranteed Bonus BW = 21055000 bps
Non-guaranteed Bonus BW = 7744000 bps
Superset BGs: Wi8/0/0:0 Wi8/0/0:4 Wi8/0/0:6


Router#show cable admission-control interface wideband-Cable 8/0/0:0

Interface Wi8/0/0:0
BGID: 24577

Resource - Downstream Bandwidth
-------------------------------
App-type    Name        Reservation/bps    Exclusive      Rejected
1                       0                  N/A            0
2                       0                  N/A            0
3           Normal      0                  10%            0
4                       0                  N/A            0
5                       0                  N/A            0
6                       0                  N/A            0
7           Emergency   0                  N/A            0
8                       0                  N/A            0
Max Reserved BW = 600000 bps
Total Current Reservation = 0 bps
Guaranteed Bonus BW = 21055000 bps
Non-guaranteed Bonus BW = 36844000 bps
Subset BGs: In8/0/0:0 In8/0/0:1
Superset BGs: Wi8/0/0:4 Wi8/0/0:6
Overlapping BGs: N/A
```

上記の設定例を省略または変更できますが、このセクションの残りの設定例では、これらの設定を前提としています。

例：ダウンストリーム トラフィックの SGAC

この例では、この項で最初に説明したコマンドに従ってルールを設定してあることを前提としています。

- すべての音声フローはバケット 1 に含まれます。
- すべての CIR データ フローは、バケット 8 に分類されます。

次の例は、ダウンストリーム トラフィックでの設定例または SGAC を示しています。この例では、音声トラフィックが占める帯域幅の割合が 30% に達すると、それ以上の音声フローは拒否されます。

- ダウンストリームのスループットの 30% が音声トラフィック専用に予約されます。

次のコマンドが、この設定を実装します。

```
Router(config-fiber-node)#admission-control application-type 1 ds-bandwidth 30
```

次に、柔軟な帯域幅割り当ての設定例を示します。この例では、通常の音声トラフィック（application-type 1）に 2 つのしきい値を関連付けます。通常の音声トラフィックだけの場合は、サービス グループのキャパシティの最大 40% を使用できます。一方、通常の音声トラフィックと緊急音声トラフィックの組み合わせでは、サービス グループのキャパシティの最大 50% を使用できます。つまり、通常の音声トラフィックが最大 40% の帯域幅割り当てをすべて使用する場合でも、緊急音声トラフィックはサービス グループのキャパシティの少なくとも 10% を使用できます。

```
Router(config-fiber-node)#admission-control application-type 1 ds-bandwidth 40
Router(config-fiber-node)#admission-control application-type 1-2 ds-bandwidth 50
```

値は次のとおりです。

- 1 は通常の音声アプリケーション タイプ
- 2 は緊急音声アプリケーション タイプ

その他の参考資料

以降のトピックには、Cisco CMTS 用の SGAC に関する参考資料が記載されています。

関連資料

関連項目	マニュアル タイトル
Cisco CMTS ケーブル コマンド	『Cisco CMTS Cable Command Reference』

標準

規格	タイトル
CableLabs™ DOCSIS 1.1 仕様	http://www.cablelabs.com/cablemodem/
CableLabs™ PacketCable 仕様	http://www.cablelabs.com/packetcable/
CableLabs™ PacketCable マルチメディア仕様	http://www.cablelabs.com/packetcable/specifications/multimedia.html

MIB

MIB	MIB のリンク
MIB	選択したプラットフォームの MIB を検索してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

サービス グループ アドミッション コントロールに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *204* : サービス グループ アドミッション コントロールに関する機能情報

機能名	リリース	機能情報
サービス グループ アドミッション コントロール	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 81 章

加入者トラフィック管理

このドキュメントでは、加入者トラフィック管理（STM）機能バージョン 1.3 について説明します。STM 機能では、DOCSIS 準拠のすべてのケーブル モデムがサポートされます。

サービス プロバイダーは STM 機能を使用することで、特定のサービス クラス（または Quality of Service（QoS）プロファイル）に関して一定期間にわたって適用する最大帯域幅しきい値を設定できます。この設定済みしきい値を超えた加入者を識別して、縮小された QoS をその加入者に割り当てることができます。STM は、Network-Based Application Recognition（NBAR）およびアクセス コントロール リスト（ACL）に代わる CPU 負荷の低い手法として機能します。ただし、STM を使用する場合に NBAR と ACL を無効にする必要があるわけではありません。STM を NBAR および ACL と併せて適用することができます。また、STM は Cisco Broadband Troubleshooter とともに、Cisco CMTS で追加のネットワーク管理/トラブルシューティング機能を提供します。

重要

このドキュメントで使われる QoS プロファイルという用語は、DOCSIS 1.1 ケーブル モデムのサービス クラスと同じ意味です。ただし、QoS プロファイルは DOCSIS 1.0 運用にのみ適用されます。DOCSIS1.1 運用で QoS プロファイルという用語が使用されている場合は、QoS プロファイルをサービス クラスとして扱ってください。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

- Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス，1354 ページ

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *205*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

Cisco CMTS ルータでの加入者トラフィック管理の制限事項

（注） このドキュメントで使われる QoS プロファイルという用語は、DOCSIS 1.1 ケーブル モデムのサービス クラスと同じ意味です。ただし、QoS プロファイルは DOCSIS 1.0 運用にのみ適用されます。DOCSIS 1.1 運用で QoS プロファイルという用語が使用されている場合は、QoS プロファイルをサービス クラスとして扱ってください。

STM 機能には次の制限があります。

- STM バージョン 1.1 では、サンプリング レートの範囲（期間）の計算に、STM 1.0 で使用される一定の範囲（10 ～ 30 分）ではなくモニタリング期間が使用されます。

- モニタリング期間が 1 日（1440 分）を超える場合、その期間のサンプル レートは [期間/100] として計算されます。
- モニタリング期間が 1 日未満の場合、サンプル レートの範囲は 10 ～ 30 分です。
- 期間 2 日、サンプル レート 20 分の STM 1.0 を使用している場合、STM 1.1 でその設定を復元しようとすると、有効な範囲が 28 ～ 86 分に変更されているため、コマンドが失敗します。

- DOCSIS1.0 では、強制ルールで指定された登録済み QoS プロファイルが、Cisco CMTS に存在する QoS プロファイルと正確に一致する必要があります。モデムで作成された QoS プロファイルを使用しているケーブル モデムを管理するには、まず、正確に同じ QoS プロファイルを Cisco CMTS 上に作成する必要があります。強制ルールでケーブル モデムを管理できるようになるには、その前に、QoS プロファイル内のすべてのパラメータが一致する必要があります。
- Cisco cBR シリーズ ルータは、特定の強制ルールを最大 40 個までサポートします。最大数の強制ルールを作成した後でさらにルールを作成するには、既存のルールを 1 つ削除する必要があります。
- 強制ルールの設定を変更すると、その強制ルールにマッピングされている加入者のバイト カウンタがすべて自動的にリセットされます。
- 登録済み QoS プロファイルにユーザが違反した場合に適用される強制 QoS プロファイルを指定する際は、最初にプロビジョニングされた QoS プロファイルおよび適用される QoS プロファイルの両方が Cisco CMTS で作成される必要があります。
- 加入者トラフィック管理機能は、稼働時間ではなく、ルータ上に設定されている時間に基づいて期間を計算します。したがって、**clockset** コマンドを使用してルータ上の時刻を変更すると、STM モニタリングの動作に影響が及ぶ可能性があります。
- 加入者トラフィック管理の最大周期は 31 日です。31 日の周期を選択する場合、設定できる最小サンプル レートは（31 日/100）分です。

Cisco CMTS ルータでの加入者トラフィック管理について

この項の内容は、次のとおりです。

機能の概要

サービス プロバイダーは STM 機能を使用することで、特定のサービス クラス（または QoS プロファイル）に対し、一定の期間にわたる最大帯域幅しきい値を設定できます。これにより、設定済みしきい値を超えた加入者を識別して、縮小した QoS をその加入者に割り当てることができます。この機能は現在の手法（NBAR、ACL など）を補足するもので、一部のユーザがケーブル ネットワークの帯域幅を占有するような事態を防ぎます。

現在の加入者制御方法（NBAR、ACL など）では、CMTS に届いたパケットをすべて検査します。これらの手法により、問題となるトラフィックの大半を食い止めることができますが、ネットワー

ク帯域幅を逼迫させる最新世代ピアツーピア ファイル共有アプリケーションにとっては効果が限定的です。

STM 機能を使用すると、ネットワーク パフォーマンスや他のユーザなどに影響を与えることなく、潜在的問題のある少数のユーザに焦点を絞ることができます。

STM 機能は次の 2 種類のモニタリングをサポートします。

- レガシーモニタリング：レガシーモニタリングでは、単一のモニタリング期間をセットアップできます。モニタリングを行う時間帯を選択することはできません。設定されたモニタリング パラメータは、一日を通して一定に保たれます。
- ピーク/オフピーク モニタリング：ピーク/オフピーク モニタリングでは、一日のうちトラフィック量が高くなる時間帯を最大 2 つ指定し、それ以外の（オフピーク）時間帯にもモニタリングを続行できます。ピーク時オプションを週末のモニタリングと組み合わせることにより、平日と週末でそれぞれ最大 2 つのピーク時を指定し、特定の加入者の帯域幅使用状況を識別して制限できます。

ケーブル モデムがオフラインになって 24 時間オフライン状態が続くと、Cisco CMTS ルータはサービス フロー ID を内部データベースから削除し、モデムのトラフィック カウンタも削除します。このため、ユーザが帯域幅制限を超えたとしても、いったんオフラインすることでカウンタをリセットできます。この種のサービス不正使用を阻止するには、加入者トラフィック管理機能で、サービス レベル契約（SLA）に違反しているケーブル モデムに対するペナルティ期間を実装すると役立ちます。その場合、ケーブル モデムがオフラインになってカウンタがリセットされたとしても、CMTS により引き続きペナルティ期間を適用できます。

機能リスト

加入者トラフィック管理機能では、次の運用機能を使用できます。

- 加入者トラフィック管理 1.1（STM 1.1）は、DOCSIS 1.1 運用に関して登録されたケーブル モデムをサポートします（サービス クラス/サービス フロー ID [SFID] モデルを使用）。
- ルータごとに、最大 40 個の強制ルールを作成できます。
- ダウンストリーム トラフィックとアップストリーム トラフィックに別々の強制ルールを使用できます。ただし、設定できる強制ルールの最大数の制限は、アップストリームのルールとダウンストリームのルールの合計数に対して適用されます。
- 各強制ルールでは、加入者の登録済み QoS プロファイルを使用して、DOCSIS1.0 ケーブル モデムでの過剰なトラフィックのモニタリング対象となるユーザを識別します。登録済み QoS プロファイルは Cisco CMTS 上に存在する必要があります。ケーブル モデムで作成された QoS プロファイルを使用しているケーブル モデムを管理するには、まず Cisco CMTS 上で、完全に同一の QoS パラメータを使って手動で QoS プロファイルを作成する必要があります。その後、手動で作成したプロファイルを使ってケーブルモデムがオンラインになるように設定する必要があります。
- それぞれの強制ルールは、指定したウィンドウ（時間枠）内でユーザが伝送できる最大キロバイト数を指定します。

- 強制ルールで指定された最大帯域幅を超えた加入者は、自動的に別の強制QoSプロファイルに切り替えられ、カスタマイズ可能なペナルティ期間にわたってネットワーク使用が制限されます。強制QoSプロファイルによってトラフィックの保証帯域幅や優先度などを変更できるため、サービス契約に違反した加入者に対してサービスプロバイダーが許容できる対応策が適用されます。
- ペナルティ期間が終了すると、加入者は登録済みQoSプロファイルに自動的に戻されます。また、ペナルティ期間が満了する前に、サービスプロバイダーのネットワーク オペレーション センター（NOC）の技術者が元の QoS プロファイルに切り替えることもできます。

（注） 手動でスイッチバックするには、ケーブル モデムをいったん削除して、再登録できるようにします。

- また、この機能でサポートされる **no-persistence** オプションを使用すると、ケーブル モデムが再起動した後に強制QoSプロファイルが無効になります。このオプションは、この機能を最初に実装したときに特に役立ちます。ユーザベース全体に大きな影響を与えることなく、問題がある加入者とアプリケーションを識別できます。繰り返し違反する加入者に対しては、ケーブル モデムの再起動後も強制 QoS ルールを適用し続ける強制ルールに切り替えることができます。
- 全加入者の使用統計は一覧表示できます。帯域幅を過剰に使用している加入者だけを一覧表示することもできます。
- ペナルティ期間はケーブルモデムの再起動後も継続されるため、加入者は、モデムをリセットしてケーブル ネットワークに再登録するという方法で強制 QoS プロファイルを回避することができません。このため、割り当てられた最大帯域幅を超過し続ける加入者に対して適切なペナルティを設定できます。また、ペナルティ対象に指定された CM をペナルティ期間から解除する時刻を指定することもできます。
- 過剰な帯域幅を使用している加入者がサービス レベルをアップグレードする場合は、プロビジョニング システムを再設定して、新しい QoS プロファイルをケーブル モデムに割り当てることができます。その後、ユーザがケーブルモデムを再起動してオンラインになると、新しいサービス レベルが適用されます。
- **cable modem service-class-name** コマンドを使用することで、特定のモデムで加入者サービスクラスを変更できます。
- 週末には、ピーク時/オフピーク時モニタリング ウィンドウなどさまざまな加入者モニタリング パラメータを設定できます。また、必要に応じて週のすべての曜日で同じモニタリング ウィンドウを設定したり、週末のモニタリングを完全に無効にしたりすることも可能です。

サービス フロー モニタリングのスライディング ウィンドウ

強制ルールを有効化すると、CMTS は定期的に、登録済み QoS プロファイルで指定された帯域幅よりも多くの帯域幅を消費している加入者がいないかどうかを確認するために、加入者が使用している帯域幅を検査します。CMTS は、サンプル レート間隔ごとに開始し、モニタリング期間に

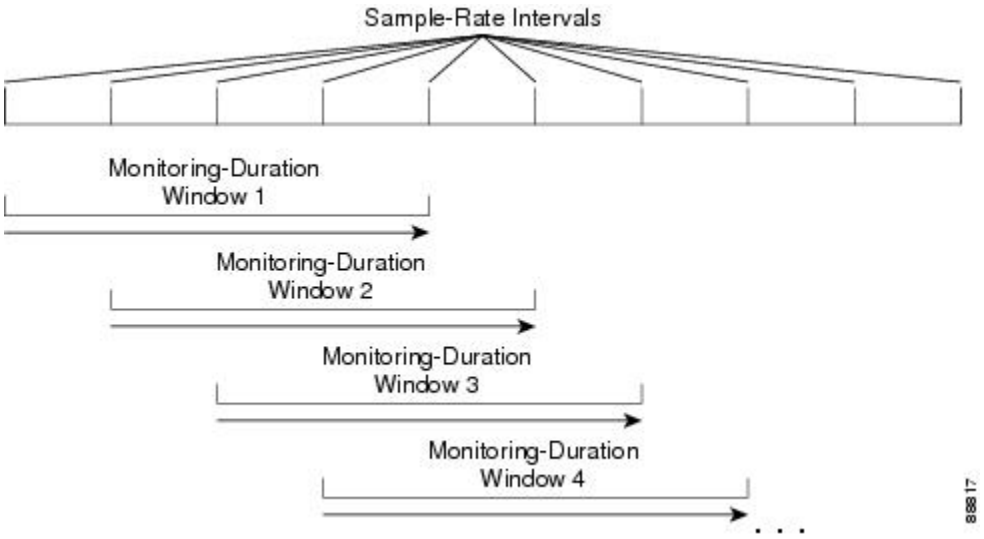
わたって継続されるスライディング ウィンドウ（時間枠）を使ってサブスクライバを追跡します。

サンプル レート間隔ごとに新しいスライディング ウィンドウ期間が開始し、CMTS はその期間に送信された合計バイト数を追跡します。各スライディング ウィンドウ期間の終了時に、CMTS はバイト カウンタを調べて、ネットワーク上の帯域幅を過剰に使用している加入者がいるかどうかを判断します。

たとえば、デフォルトサンプル レート間隔 15 分、デフォルト モニタリング期間 360 分（6 時間）が設定されている場合、CMTS は 15 分ごとに帯域幅の使用をサンプリングし、360 分のモニタリング期間が終了するたびに、送信された合計バイト数を判定します。したがって、CMTS は 6 時間にわたり、15 分間隔で各加入者の使用状況統計を確認することになります。

次の図に、このプロセスで各サンプル レート間隔の開始時に新しいスライディング ウィンドウを開始する仕組みを示します。

図 *33*：モニタリング期間ウィンドウ



週末のモニタリング

標準のレガシー モニタリング設定とピーク オフピーク モニタリング設定を使用すると、週末にも引き続きモニタリングが行われます。

STM バージョン 1.2 では、週末に対する異なるモニタリング条件を設定できます。週末のモニタリング オプションは、既存のモニタリング オプションで使用できるパラメータと同じものをサポートしますが、週末用の代替モニタリングを設定するための別個のコマンド セットを使用します。これには、週末のピーク時およびオフピーク時のモニタリング ウィンドウ（時間枠）の設定が含まれます。

さらに、CLI では週末の任意のモニタリングを無効にする機能や、週のすべての曜日に同じモニタリング条件を使用する機能がサポートされます。

SNMP トラップ通知

加入者が強制ルールに違反するたびに Simple Network Management Protocol（SNMP）トラップ通知を送信できます。SNMP トラップは CISCO-CABLE-QOS-MONITOR-MIB で定義され、**snmp-serverenabletrapscable** コマンドによって有効になります。

各 SNMP トラップ通知には、次の情報が含まれます。

- 加入者のケーブル モデムの MAC アドレス
- 加入者に適用されている強制ルールの名前
- モニタリング期間ウィンドウ（時間枠）で加入者が送信した合計バイト数
- 加入者のペナルティ期間が満了する時刻

CISCO-CABLE-QOS-MONITOR-MIB には、加入者トラフィック管理の設定について、および強制ルールに違反した加入者についての情報を提供する次のテーブルも含まれています。

- ccqmCmtsEnforceRuleTable：Cisco CMTS で現在設定されている強制ルールの属性が格納されます。
- ccqmEnfRuleViolateTable：モニタリング期間のスライディング ウィンドウ内で強制ルールに違反した加入者のスナップショット リストを提供します。

強制ルールでは、次のオブジェクトが使用されます。

- ccqmCmtsEnfRulePenaltyEndTime
- ccqmCmtsEnfRuleWkndOff
- ccqmCmtsEnfRuleWkndMonDuration
- ccqmCmtsEnfRuleWkndAvgRate
- ccqmCmtsEnfRuleWkndSampleRate
- ccqmCmtsEnfRuleWkndFirstPeakTime
- ccqmCmtsEnfRuleWkndFirstDuration
- ccqmCmtsEnfRuleWkndFirstAvgRate
- ccqmCmtsEnfRuleWkndSecondPeakTime
- ccqmCmtsEnfRuleWkndSecondDuration
- ccqmCmtsEnfRuleWkndSecondAvgRate
- ccqmCmtsEnfRuleWkndOffPeakDuration
- ccqmCmtsEnfRuleWkndOffPeakAvgRate
- ccqmCmtsEnfRuleWkndAutoEnforce
- ccqmCmtsEnfRuleFirstPeakTimeMin
- ccqmCmtsEnfRuleSecondPeakTimeMin

- ccqmCmtsEnfRuleWkndFirstPeakTimeMin
- ccqmCmtsEnfRuleWkndSecondPeakTimeMin
- ccqmCmtsEnfRulePenaltyEndTimeMin
- ccqmCmtsEnfRuleWkPenaltyPeriod
- ccqmCmtsEnfRuleWkndPenaltyPeriod
- ccqmCmtsEnfRuleRelTimeMonitorOn

強制ルール違反には、次のオブジェクトが使用されます。

- ccqmEnfRuleViolateID
- ccqmEnfRuleViolateMacAddr
- ccqmEnfRuleViolateRuleName
- ccqmEnfRuleViolateByteCount
- ccqmEnfRuleViolateLastDetectTime
- ccqmEnfRuleViolatePenaltyExpTime
- ccqmEnfRuleViolateAvgRate

ケーブル モデムと加入者トラフィック管理機能の相互作用

加入者トラフィック管理機能を使用すると、ケーブル モデムを再起動する（または設定を変更する）などの手口でQoS制約がバイパスされることを防げます。ただしサービス プロバイダーは、必要に応じてモデムのプロファイルなどの設定パラメータを変更できます。

加入者トラフィック管理機能が有効になっている場合は、次の動作が適用されます。

- ケーブル モデムが再起動しても、ダウンストリームおよびアップストリーム トラフィックのプライマリ サービス フロー カウンタは保持されます。ただし、サービス プロバイダーはカウンタをリセットできます。リセットするには、**cable modem qos profile** コマンドを使ってケーブル モデムの QoS プロファイルを変更し、ケーブル モデムをリセットします。
- セカンダリ サービス フロー カウンタは、ケーブル モデムが再起動するたびにリセットされます。これは強制ルールの設定とは無関係に行われます。
- 再起動後も、ケーブル モデムは現在のプライマリ ダウンストリームおよびアップストリーム サービス フローを保持します。ケーブル モデムが再起動したときに強制 QoS プロファイル ペナルティ期間中である場合、再起動後も強制 QoS プロファイルが使用されます。サービス プロバイダーは **cable modem qos profile** コマンドを使って新しい QoS プロファイルを割り当てることにより、手動でプロファイルを変更できます。

（注） **cable modem qos profile** コマンドを使用してケーブル モデムの QoS プロファイルを変更すると、ケーブル モデムの再起動後の強制ルールも変更されます。ケーブル モデムがオンラインに戻ると、モデムで新しく使用されている QoS プロファイルに一致する QoS プロファイルが登録された強制ルール（**qos-profile registered** コマンドを参照）に従ってモデムが動作し始めます。

- また、強制ルールの設定を変更することもできます。プロバイダーが強制ルールの設定を変更すると、次のようになります。
  - （**no enabled** コマンドを使用して）強制ルールを無効にした場合、そのルールで登録されている QoS プロファイルを使用するすべてのケーブル モデムは、加入者トラフィック管理機能の管理対象でなくなります。no enabled を設定すると強制ルールが非アクティブになり、ペナルティ状態のすべてのモデムが登録済み QoS に移行します。
  - （**qos-profile registered** コマンドを使用して）ルールの登録済み QoS プロファイルを変更した場合、以前の登録済み QoS プロファイルを使用するケーブル モデムは、加入者トラフィック管理機能の管理対象でなくなります。代わりに、新しい登録済み QoS プロファイルを使用するすべてのケーブルモデムが、このルールの管理対象になります。
  - （**qos-profile enforced** コマンドを使用して）ルールの強制 QoS プロファイルを変更した場合、ペナルティ期間中にあり、このルールを使用するケーブルモデムはすべて以前の強制 QoS プロファイルを引き続き使用します。ただし、この設定変更後にペナルティ期間に入ったケーブル モデムは、新しい強制 QoS プロファイルを使用します。
- 強制ルールは永続化させないこともできます。その場合、ケーブルモデムが再起動すると、強制 QoS プロファイルは適用されなくなります。その代わりとして、ケーブル モデムが再起動して Cisco CMTS に再登録される際に、モデムの DOCSIS コンフィギュレーション ファイルで指定された QoS プロファイルが CMTS によって割り当てられます。

Cisco CMTS ルータでの加入者トラフィック管理機能の設定方法

この項の内容は、次のとおりです。

強制ルールの作成および設定

モニタリング対象となるそれぞれのサービス クラス名に、強制ルールがリンクされます。強制ルールは、モニタリング期間、サンプル レート、ペナルティ期間、その強制ルールがリンクされている登録済みサービス クラス名および強制サービス クラス名を定義します。

強制ルールを作成して設定するには、次の手順に従います。強制ルールは、 **enabled** コマンドが実行されるまでアクティブになりません。

はじめる前に

- 強制ルールを作成する前に、そのルールで使用する登録済み Quality of Service（QoS）プロファイルと強制 QoS プロファイルを CMTS 上で作成する必要があります。モデムにより作成された QoS プロファイルを使用しているケーブル モデムを管理するには、あらかじめ CMTS 上で、モデム作成プロファイルと同じ QoS パラメータを持つ新しい QoS プロファイルを手動で作成しておく必要があります。その後、手動で作成したプロファイルを使ってモデムがオンラインになったら、この手順を開始します。
  - Cisco CMTS の Quality of Service（QoS）プロファイルを表示するには、特権 EXEC モードで show cable qos profile コマンドを使用します。
  - QoS プロファイルを設定するには、グローバル コンフィギュレーション モードで cable qos profile コマンドを使用します。特定の値をデフォルト値に設定する場合、または具体的なパラメータが設定されていないプロファイルを削除する場合は、このコマンドの no 形式を使用します。
- DOCSIS 1.1 ケーブル モデムをモニタリングする場合：
  - サービス クラス名で登録されている DOCSIS 1.1 モデムのみがモニタリングされます。
  - CM が再起動されても DOCSIS 1.1 サービス フロー カウンタを保持するには、**cableprimary-sflow-qos11keepall** グローバル コンフィギュレーション コマンドを設定します。
- プライマリ アップストリームおよびダウンストリーム サービス フローのみがサポートされます。

制約事項

- ピーク オフピーク モニタリングを設定する際には、1 日のうちのピーク期間を最大 2 つ定義できます。オフピーク期間を設定すると、ピーク時以外の残りの期間もモニタリングできます。最初のピーク時、2 番目のピーク時、およびオフピーク時に関してそれぞれ異なるモニタリング期間としきい値を設定できます。ただし、ピーク時またはオフピーク時のモニタリング期間として、1 日を超える値を設定することはできません。
- 名前付きサービス クラスで定義するパラメータは、CM 用の登録済みパラメータ セットのうち、互換性のあるサブセットでなければなりません。CMTS ルータ サービス クラスを使用して変更できるのは、**max-rate**, **priority**、**tos-overwrite** オプションなどの特定のオプションのみです。CMTS ルータの強制および登録済みサービス クラスの両方で、**max-burst** オプションの値が、登録済み DOCSIS コンフィギュレーション ファイル内の **max-burst** の値と正確に一致する必要があります。サービス クラスの値が一致しない場合、ケーブル モデム登録が reject-c 状態で失敗するか、強制クラスが失敗します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cableqosenforce-rule** *name* 例： `Router(config)# cable qos enforce-rule test`	指定した *name* を持つ強制ルールを作成し、強制ルール コンフィギュレーション モードを開始します。 （注） それぞれの強制ルールに名前を付けて作成できます。
ステップ 4	**monitoring-basics**{**legacy** | **peak-offpeak**}{**docsis10** | **docsis11**} 例： `Router(enforce-rule)# monitoring-basics peak-offpeak docsis11`	必要なモニタリングのタイプと、モニタリング対象のモデムのタイプを定義します。 デフォルトは レガシーおよび DOCSIS 1.0 です。
ステップ 5	次のいずれかの操作を行います。 • ステップ 4, （1364 ページ） で DOCSIS 1.0 ケーブル モデムを指定した場合は、次のコマンドを使用します。 1 **qos-profileregistered** *profile-id* 2 **qos-profileenforced** *profile-id* [**no-persistence**] • ステップ 4, （1364 ページ） で DOCSIS 1.1 ケーブル モデムを指定した場合は、**service-class**{**enforced**|**registered**} *name* コマンドを使用します。	• DOCSIS 1.0 ケーブルモデムの場合： 1 この強制ルールに使用する登録済み Quality of Service（QoS）プロファイルを指定します。 （注） モデムにより作成された QoS プロファイルを使用しているケーブルモデムを管理するには、あらかじめ CMTS 上で、モデム作成プロファイルと同じ QoS パラメータを持つ新しい QoS プロファイルを手動で作成しておく必要があります。その後、手動で作成したプロファイルを使ってモデムがオンラインになったら、このコマンドを使用します。

	コマンドまたはアクション	目的
	例： `Router(enforce-rule)# service-class enforced test`	2 DOCSIS 1.0 ケーブル モデムで、登録済み Quality of Service（QoS）プロファイルにユーザが違反した場合に適用する強制 QoS プロファイルを指定します。 • DOCSIS 1.1 以降のケーブル モデムの場合は、強制ルール内でケーブル モデム モニタリングの対象となる、指定した *name* を持つ特定のサービス クラスを識別します。
ステップ 6	**duration** *minutes* **avg-rate** *rate* **sample-interval** *minutes*[**penalty** *minutes*] {**downstream** | **upstream**} [**enforce**] 例： `Router(enforce-rule)# duration 10 avg-rate 500 sample-interval 10 penalty 120 downstream enforce`	レガシー モニタリングが設定されている場合（ステップ 4, （1364 ページ））、加入者をモニタリングする期間とサンプル レートを指定します。

ステップ 7	**peak-time1** {*hour* | *hour:minutes*}**duration** *minutes* **avg-rate** *rate* [**peak-time2** {*hour* | *hour:minutes*} **duration** *minutes* **avg-rate** *rate*][**duration** *offpeak-minutes* **avg-rate** *offpeak-rate*] **sample-interval** *minutes*[**penalty** *minutes*] {**downstream** | **upstream**}[**enforce**]
	例：
	`Router(enforce-rule)# peak-time1 6 duration 180 avg-rate 2 peak-time2 18 duration 180 avg-rate 2 duration 120 avg-rate 3 sample-interval 10 upstream enforce`
	`Router(enforce-rule)# peak-time1 6:30 duration 180 avg-rate 2 peak-time2 18:40 duration 180 avg-rate 2 duration 120 avg-rate 3 sample-interval 10 penalty 120 upstream enforce`
		ピーク オフピーク モニタリングが設定されている場合（ステップ 4, （1364 ページ））、ピーク時のモニタリング期間を指定します。

ステップ 8	**penalty-period** *minutes* [**time-of-day** {*hour*|*hour:minutes*}] [**monitoring-on**] 例： `Router(enforce-rule)# penalty-period 10`	（任意）登録済み QoS プロファイルに違反した加入者に対して強制 QoS プロファイルを適用する期間を指定します。

	コマンドまたはアクション	目的
ステップ 9	**enabled** 例： `Router(enforce-rule)# enabled`	（任意）強制ルールをアクティブにして、加入者トラフィック管理を開始します。
ステップ 10	**end** 例： `Router(enforce-rule)# end`	強制ルール コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

例

ここでは、いくつかの enforce-rule コマンドのヘルプ機能を含め、コマンドライン インターフェイス（CLI）の例を記載します。

例：レガシー モニタリングの設定

次に、レガシー モニタリングの強制ルールを設定する例を示します。

```
Router(config)# cable qos enforce-rule test
Router(enforce-rule)# monitoring-basics ?
  legacy        Enable legacy (same average rate for all day)  monitoring
  peak-offpeak  Enable peak-offpeak monitoring
Router(enforce-rule)# monitoring-basics legacy ?
  docsis10  Enforce-rule will map to docsis 1.0 modems
  docsis11  Enforce-rule will map to docsis 1.1 modems
Router(enforce-rule)# monitoring-basics legacy docsis11
Router(enforce-rule)# service-class ?
  enforced    Enforced service class
  registered  Registered service class
Router(enforce-rule)# service-class registered ?
  WORD  Registered service class name
Router(enforce-rule)# service-class registered BEUS
Router(enforce-rule)# service-class enforced test
Router(enforce-rule)# duration ?
  <10-10080>  Duration in minutes
Router(enforce-rule)# duration 10 ?
  avg-rate  Average rate for the duration in kbits/sec
Router(enforce-rule)# duration 10 avg-rate ?
  <1-4294967>  average rate in kbits/sec
Router(enforce-rule)# duration 10 avg-rate 2 ?
  sample-interval  Rate of sampling in Minutes
Router(enforce-rule)# duration 10 avg-rate 2 sample-interval ?
  <1-30>  Sampling rate in Minutes
Router(enforce-rule)# duration 10 avg-rate 2 sample-interval 10 ?
  downstream  downstream
  upstream    upstream
Router(enforce-rule)# duration 10 avg-rate 2 sample-interval 10 upstream ?
  enforce  enforce the qos-profile automatically
  <cr>
Router(enforce-rule)# duration 10 avg-rate 2 sample-interval 10 upstream enf
Router(enforce-rule)# $ avg-rate 2 sample-interval 10 upstream enforce
Router(enforce-rule)# enabled
Router(enforce-rule)# end
```

例：ピーク オフピーク モニタリングの設定

次に、ピーク オフピーク モニタリングの強制ルールを設定する例を示します。

```
Router(config)# cable qos enforce-rule test
Router(enforce-rule)# monitoring-basics peak-offpeak
Router(enforce-rule)# monitoring-basics peak-offpeak docsis10
Router(enforce-rule)# qos-profile ?
  enforced    Enforced qos profile
  registered  QoS profile index
Router(enforce-rule)# qos-profile registered ?
  <1-255>  Registered QoS profile index
Router(enforce-rule)# qos-profile registered 5
Router(enforce-rule)# qos-profile enforced 4
Router(enforce-rule)# peak-time1 6 ?
  duration  First peak duration
Router(enforce-rule)# peak-time1 6 duration ?
  <60-1440>  Duration in minutes
Router(enforce-rule)# peak-time1 6 duration 180 ?
  avg-rate  First peak average rate in kbits/sec
Router(enforce-rule)# peak-time1 6 duration 180 avg-rate ?
  <1-4294967>  Average rate in kbits/sec
Router(enforce-rule)# peak-time1 6 duration 180 avg-rate 2 ?
  duration         Off-peak duration
  peak-time2       Second peak time
  sample-interval  Rate of sampling in minutes

Router(enforce-rule)# peak-time1 6 duration 180 avg-rate 2 peak-time2 ?
  <10-1440>  Start of second peak time
Router(enforce-rule)# peak-time1 6 duration 180 avg-rate 2 peak-time2 18 ?
  duration  Second peak duration
Router(enforce-rule)# $6 duration 180 avg-rate 2 peak-time2 18 duration ?
  <10-1440>  Duration in minutes
Router(enforce-rule)# $6 duration 180 avg-rate 2 peak-time2 18 duration 240 ?
  avg-rate  Second peak average rate in kbits/sec
Router(enforce-rule)# $ 180 avg-rate 2 peak-time2 18 duration 240 avg-rate ?
  <1-4294967>  Average rate in kbits/sec
Router(enforce-rule)# $ 180 avg-rate 2 peak-time2 18 duration 240 avg-rate 3 ?
  duration         Off-peak duration
  sample-interval  Rate of sampling in minutes
Router(enforce-rule)# $ 180 avg-rate 2 peak-time2 18 duration 240 avg-rate 3 d
Router(enforce-rule)# $-time2 18 duration 240 avg-rate 3 duration 120 ?
  avg-rate  Off-peak average rate in kbits/sec
Router(enforce-rule)# $duration 240 avg-rate 3 duration 120 avg-rate 1 ?

  sample-interval  Rate of sampling in minutes
Router(enforce-rule)# $40 avg-rate 3 duration 120 avg-rate 1 sample-interval ?
  <1-30>  Sampling rate in Minutes
Router(enforce-rule)# $e 3 duration 120 avg-rate 1 sample-interval 10 ?

  downstream  downstream
  upstream    upstream
Router(enforce-rule)# $e 3 duration 120 avg-rate 1 sample-interval 10 upstream ?
  enforce  enforce the qos-profile automatically
  <cr>
Router(enforce-rule)# $on 120 avg-rate 1 sample-interval 10 upstream enforce
Router(enforce-rule)# enabled
Router(enforce-rule)# end
```

週末のモニタリングの設定

ここでは、Cisco CMTS 上で STM に対する週末モニタリングを設定するために必要なタスクについて説明します。

前提条件

週末のモニタリングを設定する前に、強制ルールの平日のモニタリング パラメータを設定する必要があります。強制ルールの作成および設定，（1362 ページ）を参照してください。

制限事項

- アップストリームとダウンストリームの設定でサポートされる強制ルールの数は、合計で最大 40 個です。
- SNMP を週末のモニタリングに使用する場合、SNMP GET および GETMANY 操作のみがサポートされます。

週末用の異なるレガシー モニタリング条件の設定

加入者の週末のアップストリームまたはダウンストリーム トラフィックに関して異なるレガシー モニタリング条件を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cableqosenforce-rule** *name* 例： `Router(config)# cable qos enforce-rule test`	指定した *name*（名前）の強制ルールにアクセスして、強制ルール コンフィギュレーション モードを開始します。
ステップ 4	**weekendduration** *minutes* **avg-rate** *rate* **sample-interval** *minutes* {**downstream** | **upstream**} [**penalty** *minutes*] [**enforce**] 例： `Router(enforce-rule)# weekend duration 15 avg-rate 500 sample-interval 10 penalty 120 downstream enforce`	週末の加入者モニタリングで使用する時間帯とサンプル レートを指定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Router(enforce-rule)# end`	強制ルール コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

週末用の異なるピーク オフピーク モニタリング条件の設定

加入者の週末のアップストリームまたはダウンストリーム トラフィックに関して異なるピーク/オフピーク モニタリング条件を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cableqosenforce-rule** *name* 例： `Router(config)# cable qos enforce-rule test`	指定した *name*（名前）の強制ルールにアクセスして、強制ルール コンフィギュレーション モードを開始します。
ステップ 4	**weekendpeak-time1**{*hour* | *hour*:*minutes*} **duration** *minutes* **avg-rate** *rate* [**peak-time2** *hour***duration** *minutes* **avg-rate** *rate*] [**duration** *offpeak-minutes***avg-rate** *offpeak-rate*] **sample-interval** *minutes*[**penalty** *minutes*] {**downstream**| **upstream**}[**enforce**] 例： `Router(enforce-rule)# weekend peak-time1 9 duration 180 avg-rate 2 peak-time2 16 duration 180 avg-rate 2 duration 120 avg-rate 3 sample-interval 10 upstream enforce`	週末のピーク時およびオフピーク時のモニタリング期間を指定します。

	コマンドまたはアクション	目的
	例： `Router(enforce-rule)# weekend peak-time1 9:30 duration 180 avg-rate 2 peak-time2 16:58 duration 180 avg-rate 2 duration 120 avg-rate 3 sample-interval 10 penalty 120 upstream enforce`	
ステップ 5	**end** 例： `Router(enforce-rule)# end`	強制ルール コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

週末のモニタリングの無効化

週末のモニタリング設定を無効にして平日だけモニタリングするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cableqosenforce-rule** *name* 例： `Router(config)# cable qos enforce-rule test`	指定した *name* を持つ強制ルールにアクセスして、強制ルール コンフィギュレーション モードを開始します。
ステップ 4	**weekendoff** 例： `Router(enforce-rule)# weekend off`	週末のモニタリングを無効にします。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Router(enforce-rule)# end`	強制ルール コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

週末のモニタリング条件を削除して毎日同じモニタリング基準を使用する

指定した週末モニタリング条件を削除して、（平日を含む）週全体で同じモニタリング基準を使用するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cableqosenforce-rule** *name* 例： `Router(config)# cable qos enforce-rule test`	指定した *name*（名前）の強制ルールにアクセスして、強制ルール コンフィギュレーション モードを開始します。
ステップ 4	**noweekend** 例： `Router(enforce-rule)# no weekend`	平日と週末に同じパラメータを使用して週末のモニタリングを実行します。
ステップ 5	**end** 例： `Router(enforce-rule)# end`	強制ルール コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

強制ルールの無効化

強制ルールを無効にするには、次の手順に従います。強制ルールは CMTS コンフィギュレーション ファイルに残りますが、この強制ルールを使用するすべての加入者トラフィック管理が終了します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cableqosenforce-rule***name* 例： `Router(config)# cable qos enforce-rule test`	指定した *name* を持つ強制ルールを作成し、強制ルール コンフィギュレーション モードを開始します。
ステップ 4	**noenabled** 例： `Router(enforce-rule)# no enabled`	強制ルールを無効にして、このルールの登録済み QoS プロファイルが適用されているユーザの加入者トラフィック管理を終了します。これにより、ペナルティ状態のすべてのモデムが登録済み QoS に移動されます。
ステップ 5	**end** 例： `Router(enforce-rule)# end`	強制ルール コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

強制ルールの削除

強制ルールを削除して CMTS コンフィギュレーション ファイルから除去するには、次の手順に従います。これにより、このルールを使用している加入者トラフィック管理も終了します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**nocableqosenforce-rule***name* 例： `Router(config)# no cable qos enforce-rule ef-rule`	指定した *name* を持つ強制ルールを削除します。この強制ルールとその設定が CMTS 設定から削除され、このルールを使用する加入者トラフィック管理が終了します。
ステップ 4	**end** 例： `Router(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

ケーブル モデム サービス クラスの変更

特定の DOCSIS 1.1 ケーブル モデムの QoS サービス クラスを変更するには、次の手順に従います。

制約事項

- このコマンドは、DOCSIS 1.1 CM プライマリ サービス フローでのみサポートされます。
- CM のオンライン状態が少なくとも 200 秒続いた後に、**cablemodemservice-class-name** コマンドを指定できます。
- 名前付きサービス クラスで定義するパラメータは、CM 用の登録済みパラメータ セットのうち、互換性のあるサブセットでなければなりません。CMTS ルータ サービス クラスを使用して変更できるのは、**max-rate**, **priority**、**tos-overwrite** オプションなどの特定のオプションのみです。CMTS ルータの強制および登録済みサービス クラスの両方で、**max-burst** オプションの値が、登録済み DOCSIS コンフィギュレーション ファイル内の **max-burst** の値と正確に一致する必要があります。サービス クラスの値が一致しない場合、CM 登録が reject-c 状態で失敗するか、強制クラスが失敗します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**cablemodem** {*ip-address* | *mac-address*} **service-class-name** *name* 例： `Router# cable modem aaaa.bbbb.cccc service-class-name test`	特定のケーブル モデムの QoS サービス クラスを変更します。
ステップ 3	**end** 例： `Router# end`	特権 EXEC モードを終了します。

Cisco CMTS ルータでの加入者トラフィック管理機能のモニタリング

ここで説明する次のタスクを使用して、加入者トラフィック管理機能をモニタリングすることができます。

現在定義されている強制ルールの表示

Cisco CMTS ルータで現在定義されているすべての強制ルール、または特定の強制ルールの定義を表示するには、特権 EXEC モードで **showcableqosenforce-rule** コマンドを使用します。

オフピーク モニタリングのモニタリング期間と、その時間帯に該当する平均レートの値を表示するには、**showcableqosenforce-rule** コマンドを使用します。モニタリングが行われない場合は、0 と表示されます。

次に、すべての設定済み強制ルールを表示する **showcableqosenforce-rule** コマンドの出力例を示します。

```
Router# show cable qos enforce-rule
            Name               Dur   Dir byte-cnt Auto rate  penalty Reg Enf Ena Persist
                              (min)      (kbytes) enf  (min) (min)   QoS QoS
 residential                   10    us  5        act  1     10080   5   10  Yes Yes
 ef-q11d                       30    ds  150      act  1     20      11  99  Yes Yes
 ef-q11u                       30    us  60       act  1     20      11  99  Yes Yes
 ef-q21                        720   us  60       act  1     10      21  81  Yes Yes
 ef-q21d                       300   ds  150      act  1     10      21  81  Yes Yes
 ef-q22                        720   us  60       act  1     10      22  82  Yes Yes
 ef-q22d                       300   ds  150      act  1     10      22  82  Yes No
```

```
 ef-q23                        720  us  60       act  1     10       23  83  Yes Yes
 ef-q23d                       300  ds  150      act  1     10       23  83  Yes Yes
 ef-q24                        720  us  60       act  1     10       24  84  Yes Yes
 ef-q24d                       300  ds  150      act  1     10       24  84  Yes Yes
 ef-q25                        720  us  60       act  1     10       25  85  Yes Yes
 ef-q25d                       300  ds  150      act  1     10       25  85  Yes Yes
 ef-q26                        720  us  60       act  1     10       26  86  Yes Yes
 ef-q26d                       300  ds  150      act  1     10       26  86  Yes Yes
 ef-q27                        720  us  60       act  1     10       27  87  Yes Yes
 ef-q27d                       300  ds  150      act  1     10       27  87  Yes Yes
 ef-q28                        720  us  60       act  1     10       28  88  Yes Yes
 ef-q28d                       300  ds  150      act  1     10       28  88  Yes No
 ef-q5d                        300  ds  150      act  1     10       5   99  Yes Yes
 ef-q5u                        720  us  600      act  1     10       5   99  Yes Yes
```

次に、「test」という名前の特定の強制ルールに対する **showcableqosenforce-rule** コマンドの出力例を示します。

```
Router# show cable qos enforce-rule test
     Name        Type Dur  Dir Avg-rate Auto rate     Reg        Enf      En Per
                      (min)    kbits/s  enf  (min)
test           p-off 120   us 1        act  10     255         4         Y  Y
```

次に、「test」という名前の強制ルールに対する **showcableqosenforce-ruleverbose** コマンドの出力例を示します。

```
Router# show cable qos enforce-rule test verbose
Name                          : test
Version                       : docsis11
Monitoring Type               : peak-offpeak
Registered                    : REG-DS
Enforced                      : ENF-DS
Monitoring Duration           : 70 (in minutes)
Sample-rate                   : 10 (in minutes)
Average-rate                  : 3 kbits/sec
Direction                     : downstream
Auto Enforce                  : Yes
Current Penalty Duration      : 10 (in minutes)
Default Penalty Duration      : 10 (in minutes)
Penalty End-time              : 23:0 (time of day)
Rule Enabled                  : Yes
Persistence                   : Yes
Weekend                       : No
Penalty Off                   : No
Monitor Weekend               : Yes
Monitoring after RelTime      : Off
First Peak Time               : 10:0
Duration                      : 60 (in minutes)
First Average-rate            : 1 kbits/sec
Second Peak Time              : 19:0
Duration                      : 65 (in minutes)
Second Average-rate           : 2 kbits/sec
Offpeak Duration              : 70 (in minutes)
Offpeak Average-rate          : 3 kbits/sec
Auto Enforce                  : Yes
Sample Rate                   : 10
Penalty-Period for week-days  : 0
Weekend First Peak Time       : 11:0
Weekend Duration              : 75 (in minutes)
Weekend First Average-rate    : 4 kbits/sec
Weekend Second Peak Time      : 20:0
Weekend Duration              : 80 (in minutes)
Weekend Second Average-rate   : 5 kbits/sec
Weekend Offpeak Duration      : 85 (in minutes)
Weekend Offpeak Average-rate  : 6 kbits/sec
Weekend Auto Enforce          : Yes
Weekend Sample Rate           : 12
Penalty-Period for week-ends  : 0
router#sh clock
*17:30:50.259 UTC Mon Apr 19 2010
```

次に、ピーク オフピーク週末モニタリング オプションが指定されている「test」という名前の特定強制ルールに対する **showcableqosenforce-ruleverbose** コマンドの出力例を示します。

```
Router# show cable qos enforce-rule test verbose
Name : test
Version : docsis10
Monitoring Type : peak-offpeak
Registered : 255
Enforced : 4
Monitoring Duration : 120 (in minutes)
Sample-rate : 10 (in minutes)
Average-rate : 1 kbits/sec
Direction : upstream
Penalty Time : 10080 (in minutes)
Penalty End-time : 23 (time of day in hrs)
Rule Enabled : Yes
Persistence : Yes
Week-end : Yes
First Peak Time : 6
Duration : 180 (in minutes)
First Average-rate : 2 kbits/sec
Second Peak Time : 18
Duration : 240 (in minutes)
Second Averate-rate : 3 kbits/sec
Offpeak Duration : 120 (in minutes)
Offpeak Average-rate : 1 kbits/sec
Auto-enforce : active
Weekend First Peak Time : 8
Weekend First Duration : 120 (in minutes)
Weekend First Average-rate : 2 kbits/sec
Weekend Second Peak Time : 18
Weekend Second Duration : 180 (in minutes)
Weekend Second Average-rate : 5 kbits/sec
Weekend Offpeak Duration : 240 (in minutes)
Weekend Offpeak Average-rate : 4 kbits/sec
Weekend Auto-enforce : active
```

現在の加入者使用状況の表示

ケーブル インターフェイス上のすべての加入者の使用状況を表示するには、特権 EXEC モードで、オプションを指定せずに show cable subscriber-usage コマンドを使用します。

登録済み Quality of Service（QoS）プロファイルに違反している加入者の使用状況だけを表示するには、このコマンドの show cable subscriber-usage over-consume 形式を使用します。

次に、特定のケーブル インターフェイスのすべての加入者に関する **showcablesubscriber-usage** コマンドを実行した場合の出力例を示します。

```
Router# show cable subscriber-usage cable 6/0/1
Sfid Mac Address   Enforce-rule Total-Kbyte    Last-detect    Last-penalty   Pen
                        Name        Count          time           time       Flag
3    0007.0e03.110d efrule-q5   121944817  Jan1  03:44:08  Jan1  03:54:08  Act
4    0007.0e03.110d efrule-q5d  1879076068 Jan1  03:35:05  Jan1  03:45:06  Act
5    0007.0e03.1431 efrule-q5   120052387  Jan1  03:44:18  Jan1  03:54:18  Act
6    0007.0e03.1431 efrule-q5d  1838493626 Jan1  03:34:55  Jan1  03:44:55  Act
7    0007.0e03.1445 efrule-q5   120919427  Jan1  03:44:08  Jan1  03:54:08  Act
8    0007.0e03.1445 efrule-q5d  1865955172 Jan1  03:35:06  Jan1  03:45:06  Act
9    0007.0e03.1225 efrule-q5   120200155  Jan1  03:44:18  Jan1  03:54:18  Act
10   0007.0e03.1225 efrule-q5d  1839681070 Jan1  03:34:55  Jan1  03:44:55   -
11   0007.0e03.0cb1 efrule-q5   122941643  Jan1  03:43:58  Jan1  03:53:58  Act
12   0007.0e03.0cb1 efrule-q5d  1889107176 Jan1  03:35:06  Jan1  03:45:06  Act
13   0007.0e03.1435 efrule-q5   119504795  Jan1  03:44:18  Jan1  03:54:18  Act
14   0007.0e03.1435 efrule-q5d  1835164034 Jan1  03:34:55  Jan1  03:44:55   -
```

デフォルトで、出力はサービス フロー ID（SFID）を基準にソートされて表示されます。加入者のバイト カウントを基準に表示内容をソートして、最大バイト カウントを最初にリストするには、**sort-byte-count** オプションを使用します。次に、このコマンドを **showcablesubscriber-usagesort-byte-count** 形式で実行した場合の出力例を示します。

（注） **sort-byte-count** オプションが **sort-avg-rate** オプションに置き換わりました。

```
Router# show cable subscriber-usage
 sort-byte-count

Sfid Mac Address   Enforce-rule Total-Kbyte  Last-detect    Last-penalty   Pen
                      Name        Count       time            time        Flag
7    0007.0e03.2cad test1       65157114   Feb24 11:36:34  Mar3  11:36:34  Act
9    0007.0e03.2c45 test1       16381014                                   -
5    0007.0e03.2c25 test1       13440960                                   -
```

Cisco CMTS ルータでの加入者トラフィック管理の設定例

ここでは、Cisco CMTS ルータでの加入者トラフィック管理機能の設定例を記載します。

例：DOCSIS コンフィギュレーション ファイルと STM サービス クラス

次に、DOCSIS コンフィギュレーション ファイルの例と、加入者トラフィック管理を実行するために Cisco CMTS ルータに定義できる登録済みの強制 WoS サービス クラスの例を示します。

DOCSIS コンフィギュレーション ファイルのオプション

この例には、DOCSIS コンフィギュレーション ファイル内でケーブル モデムに関して設定できる極めて基本的なオプション セットが示されています。これを使用することで、Cisco CMTS ルータ上で新しい QoS サービス クラスを適切に設定できます。

（注） いくつかの QoS パラメータについては、登録済み QoS パラメータ セットと新しいサービス クラスでの値を変更できません。たとえば、**max-burst** の値は、DOCSIS コンフィギュレーション ファイルで登録された元の値、さらに Cisco CMTS ルータ上の登録済み強制 QoS サービス クラスでの値と一致している必要があります。**max-burst** 値が登録済み CMTS サービス クラスと DOCSIS コンフィギュレーション ファイルでの値と異なる場合、CM は reject-c 状態になるか、強制クラスに障害が発生する可能性があります。

次に、アップストリームおよびダウンストリームの基本的なパラメータ セットを定義するための、DOCSIS コンフィギュレーション ファイル内の「BE-STM-US-1」および「BE-STM-DS-1」という 2 つのサービス クラスの設定例を示します。

```
03 (Net Access Control) = Yes
17 (Baseline Privacy Block)
S01 (Authorize Wait Timeout) = 10
18 (Maximum Number of CPE) = 10
24 (Upstream Service Flow Block)
S01 (Flow Reference) = 1
```

```
S04 (Service Class Name) = BE-STM-US-1
S06 (QoS Parameter Set Type) = 7
25 (Downstream Service Flow Block)
S01 (Flow Reference) = 2
S04 (Service Class Name) = BE-STM-DS-1
S06 (QoS Parameter Set Type) = 7
29 (Privacy Enable) = Yes
```

The following example shows sample **cable service class** commands on the Cisco CMTS router for configuration of subscriber traffic management that correspond to the service class names in the DOCSIS configuration file of "BE-STM-US-1" and "BE-STM-DS-1." These service classes correspond to the registered service classes configured by the **service-class registered** command for the QoS enforce-rules shown later in this example:

```
cable service class 2 name BE-STM-US-1
cable service class 2 upstream
cable service class 2 max-rate 2000000
cable service class 2 max-burst 3044
cable service class 2 max-concat-burst 8000
cable service class 3 name BE-STM-DS-1
cable service class 3 downstream
cable service class 3 max-rate 30000000
cable service class 3 max-concat-burst 8000
```

ケーブル モデムが最大の US スループットを達成できるよう、able service class コマンドの max-concat-burst キーワードには大きい値を指定してください。

次に示す、Cisco CMTS ルータに対する **cableserviceclass** コマンドの例は、識別された加入者に関して新しい QoS パラメータを設定し、**max-rate** パラメータを使って帯域幅を制限します。これらのサービス クラスは、この例の後の方に示されている **service-classenforced** コマンドによって QoS 強制ルールに関して設定される強制サービス クラスに対応します。

```
cable service class 102 name BEUS-1
cable service class 102 upstream
cable service class 102 max-rate 48888
cable service class 102 max-burst 3044
cable service class 102 max-concat-burst 8000
cable service class 103 name BEDS-1
cable service class 103 downstream
cable service class 103 max-rate 988888
cable service class 103 max-concat-burst 8000
```

次の例は、登録済み強制サービス クラスを識別する、アップストリームおよびダウンストリームのモニタリングに関する対応する強制ルールの設定を示しています。

```
cable qos enforce-rule US-1
  monitoring-basics legacy docsis11
  penalty-period 10
  service-class registered BE-STM-US-1
  service-class enforced BEUS-1
  duration 10 avg-rate 1 sample-interval 10 up enf
  enabled
!
cable qos enforce-rule DS-1
  monitoring-basics legacy docsis11
  penalty-period 10
  service-class registered BE-STM-DS-1
  service-class enforced BEDS-1
  duration 10 avg-rate 1 sample-interval 10 do enf
  enabled
```

例：ダウンストリームの設定

以下に、ダウンストリーム方向のトラフィックに対する標準的な強制ルールの設定例を示します。

```
!
cable qos enforce-rule downstream-rule
```

```
  monitoring-basics legacy docsis11
  penalty-period 10
  service-class registered class5
  service-class enforced class99
  duration 30 avg-rate 1 sample-interval 10 downstream enforce
  enabled
```

例：アップストリームの設定

以下に、アップストリーム方向のトラフィックに対する標準的な強制ルールの設定例を示します。

```
!
cable qos enforce-rule upstream-rule
  monitoring-basics legacy docsis11
  penalty-period 10
  service-class registered class5
  service-class enforced class99
  duration 30 avg-rate 1 sample-interval 10 upstream enforce
  enabled
```

例：ダウンストリームとアップストリームの設定

次に、ダウンストリームとアップストリーム両方の方向でのトラフィックに対する標準的な強制ルールの設定例を示します。同一の設定を使用した 2 つの別個のルールを作成します。ただし、**duration** コマンド内ではそれぞれキーワード **upstream**、**downstream** を使用します。

（注） アップストリーム方向とダウンストリーム方向の強制ルールでは、同一の設定を使用することも、それぞれに個別の設定を使用することもできます。

```
!
cable qos enforce-rule upstream-rule
  monitoring-basics legacy docsis11
  penalty-period 10
  service-class registered class5
  service-class enforced class99
  duration 30 avg-rate 5 sample-interval 10 upstream enforce
  enabled
cable qos enforce-rule downstream-rule
  monitoring-basics legacy docsis11
  penalty-period 10
  service-class registered class5
  service-class enforced class99
  duration 30 avg-rate 5 sample-interval 10 downstream enforce
  enabled
```

次に、アップストリーム方向のトラフィックに対する強制ルールの設定例を示します。アップストリームには固有の違反期間を設定します。違反リリース時刻を過ぎると、モニタリングが有効になります。

（注） アップストリーム方向では、固有の違反期間（120分）を設定します。この設定は、penalty-period コマンドを使用して設定された期間（60 分）に優先されます。違反リリース時刻（23:00）を過ぎると、トラフィック カウンタのすべてが 0 にリセットされ、モニタリングが新たに開始されます。

```
!
cable qos enforce-rule upstream_rule
  monitoring-basics peak-offpeak docsis10
  penalty-period 60 time-of-day 23:00 monitoring-on
  qos-profile registered 6
  qos-profile enforced 100
  peak-time1 10:30 duration 120 avg-rate 10 peak-time2 22:10 duration 60 avg-rate 10
sample-interval 10 penalty 120 upstream enforce
enabled
```

例：週末のモニタリングの設定

次に、DOCSIS 1.0 ケーブル モデムに対するピーク オフピーク週末モニタリングの設定例を示します。

```
cable qos enforce-rule monitoring
    monitoring-basics peak-offpeak docsis10
    penalty-period 60
    qos-profile registered 6
    qos-profile enforced 100
    peak-time1 10 duration 120 avg-rate 10 peak-time2 23 duration 60 avg-rate 10
sample-interval 10 upstream enforce
    weekend peak-time1 8 duration 60 avg-rate 100 peak-time2 20 duration 60 avg-rate 10000
 duration 90 avg-rate 20000 sample-interval 20 downstream enforce
    enabled
```

その他の参考資料

加入者トラフィック管理機能の詳細については、次の参考資料を参照してください。

関連資料

関連項目	マニュアル タイトル
ケーブル コマンド	『Cisco IOS CMTS Cable Command Reference』

標準

標準[6]	タイトル
SP-RFIv1.1-I09-020830	『*Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1*』（http://www.cablemodem.com）

標準[6]	タイトル
draft-ietf-ipcdn-docs-rfmibv2-06	『*Radio Frequency (RF) Interface Management Information Base for DOCSIS 2.0 Compliant RF Interfaces*』

6 サポートされている標準がすべて記載されているわけではありません。

MIB

MIB [7]	MIB のリンク
• CISCO-CABLE-QOS-MONITOR-MIB • DOSCIS-QOS-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

7 サポートされている MIB がすべて記載されているわけではありません。

RFC

RFC[8]	タイトル
RFC 2233	『DOCSIS OSSI Objects Support』
RFC 2665	『DOCSIS Ethernet MIB Objects Support』
RFC 2669	『Cable Device MIB』

8 サポートされている RFC がすべて記載されているわけではありません。

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

加入者トラフィック管理に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *206*：加入者トラフィック管理に関する機能情報

機能名	リリース	機能情報
加入者トラフィック管理	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 XI 部

セキュリティおよびケーブル モニタリング構成

第 82 章

動的共有秘密

このマニュアルでは、サービス プロバイダーが Data-over-Cable Service Interface Specifications（DOCSIS）ケーブル ネットワークに高度なセキュリティを提供することを可能にする動的共有秘密機能について説明します。この機能では、各ケーブル モデムにダウンロードされる DOCSIS コンフィギュレーション ファイルを検証するのに、ランダム化された単回使用の共有秘密を使用します。

動的共有秘密機能は、モデムごとに一意の DOCSIS 共有秘密を自動作成して、現在のセッションでのみ有効なワンタイム使用の DOCSIS コンフィギュレーション ファイルを作成します。これにより、1 つのケーブル モデムにダウンロードされた DOCSIS コンフィギュレーション ファイルを他のモデムで使用することはできなくなり、同じモデムが後でこのコンフィギュレーション ファイルを再利用することもできなくなります。

特許取得済みのこの機能は、登録されたすべてのモデムが、モデムの登録時にその特定のモデム用に DOCSIS プロビジョニング システムが指定した Quality of Service（QoS）パラメータのみを使用することを保証するために設計されています。この機能は、承認済みの DOCSIS 標準です。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *207* : ***Cisco cBR*** シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

動的共有秘密の前提条件

動的共有秘密機能の設定が Cisco CMTS ルータでサポートされていることが必要です。

動的共有秘密機能に必要なその他の重要な前提条件は次のとおりです。

- Cisco CMTS で Cisco IOS-XE 3.15.0S 以降が実行されている必要があります。
- 動的共有秘密機能が外部プロビジョニング サーバをサポートしていることが必要です。
- 動的共有秘密機能をイネーブルにする前に、ケーブル モデムを Cisco CMTS に登録する必要があります。
- 完全なセキュリティのため、DOCSIS コンフィギュレーション ファイルのファイル名は、少なくとも 5 文字以上の長さにする必要があります。

- ケーブル モデムのプロビジョニング時に最適なパフォーマンスを得るため、Cisco Network Registrar リリース 3.5 以降を使用することを推奨します。

（注） 動的共有秘密機能がデフォルト設定の使用によりイネーブルになっている場合、ケーブル モデムの診断 Web ページには DOCSIS コンフィギュレーション ファイルのスクランブルされた名前が表示されます。このファイル名は、ケーブル モデムが CMTS に登録されるたびにランダムに変更します。デフォルトの動作を変更するには、**cabledynamic-secret** コマンドで **nocrypt** オプションを使用します。

動的共有秘密の制限事項

動的共有秘密の一般的な制限事項

- 共有秘密とセカンダリ共有秘密は、動的共有秘密機能を使用して設定できません。
- マスター ケーブル インターフェイスで動的共有秘密機能を設定する場合は、対応するすべてのスレーブ ケーブル インターフェイスでもこの機能を設定する必要があります。
- 動的共有秘密機能では、CMTS に登録された各ケーブル モデムが DOCSIS で指定された手順を使用してサービス プロバイダーの認定 Dynamic Host Configuration Protocol（DHCP）および TFTP サーバで指定された DOCSIS コンフィギュレーション ファイルだけを使用できるようにします。
- 動的共有秘密機能は、すでにオンラインでプロビジョニングされたケーブル モデムに影響しません。ケーブル モデムがオンラインの場合は、リセットして再登録されるようにし、動的共有秘密機能に準拠させる必要があります。
- DMIC ロック モードは HCCP N+1 冗長性でのスイッチオーバー イベントで次の動作を使用します。過去にロック モードであったすべてのケーブル モデムは、スイッチオーバー イベントでオフラインになり、ロックされたモデムの以前の状態は失われます。過去にロックされたモデムが非準拠のままである場合、登録が 3 回失敗するとロック モードに戻ります。モデムが DOCSIS に準拠すると、通常の方法でオンラインに戻ります。DMIC ロック モードに関する詳細については、SNMP サポート，（1395 ページ）を参照してください。
- Broadband Access Center for Cable（BACC）プロビジョニング サーバが使用されている場合、デバイス プロビジョニング エンジン（DPE）TFTP サーバは、TFTP クライアントの IP アドレスが DOCSIS ケーブル モデムの IP アドレスと一致することを確認します。一致が検出されない場合は、要求はドロップされます。この機能は、CMTS DMIC 機能と互換性がありません。動的設定 TFTP 要求で要求元 IP アドレスの確認を無効にするには、すべての BACC DPE サーバで no tftp verify-ip コマンドを使用します。詳細については、http://www.cisco.com/c/en/us/td/docs/net_mgmt/broadband_access_center_for_cable/4-0/command/reference/DPECLIRef40.html にある『Cisco Broadband Access Centre DPE CLI Reference』を参照してください。

動的共有秘密のケーブル モデムの制限

Incognito サーバおよび Thomson ケーブル モデムにおける DHCP 制限

Dynamic Host Configuration Protocol（DHCP）は、TCP/IP ネットワーク上の DHCP ホストに構成情報を渡します。構成パラメータとそのほかの制御情報は、DHCP メッセージの options フィールドに保存されます。

Incognito DHCP サーバとともに DMIC を使用する場合、次の 2 つのオプションが DHCP メッセージで送信されないように Incognito サーバを再構成する必要があります。

- オプション *66*：DHCP ヘッダーの sname フィールドが DHCP オプションで使用された場合、TFTP サーバを特定するためにこのオプションが使用されます。オプション 66 は、DHCP メッセージの Options フィールドにおける可変長フィールドです。RFC 2132 によると「DHCP ヘッダーの「sname フィールド」が DHCP オプションで使用された場合に、TFTP サーバを特定するために使用されるオプション」であると説明されています。
- *sname* フィールド：sname フィールドは、DHCP メッセージのヘッダーにおける 64 オクテットのフィールドです。RFC2131 によると「オプションのサーバホスト名であり、ヌルで終了する文字列」であると説明されています。返されたパラメータがオプションに割り当てられている通常の領域を超えた場合に、DHCP サーバはこのオプションを挿入します。このオプションが存在する場合、クライアントは標準のオプション フィールドの解釈を完了したら、指定された追加のフィールドを解釈します。

（注） DHCP メッセージに両方のオプションを含めることは、DOCSIS に準拠していません。

以下に示す問題のあるパケット キャプチャは、sname とオプション 66 の両方が（この順序で）設定されている場合の DHCP オファーです。

```
0000  00 30 19 47 8f 00 00 d0 b7 aa 95 50 08 00 45 00
0010  01 4a 8f 50 00 00 80 11 46 30 ac 10 02 01 ac 10
0020  0a 01 00 43 00 43 01 36 0c 75 02 01 06 00 b0 a0
0030  25 01 00 00 00 00 00 00 00 00 ac 10 0a 53 00 00
0040  00 00 ac 10 0a 01 00 10 95 25 a0 b0 00 00 00 00
0050  00 00 00 00 00 00 5b 31 37 32 2e 31 36 2e 32 2e
(sname option immediately above)
0060  31 5d 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0090  00 00 00 00 00 00 00 64 65 66 61 75 6c 74 2e 63 66
00a0  67 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110  00 00 00 00 00 00 63 82 53 63 35 01 02 36 04 ac
0120  10 02 01 33 04 00 06 94 0d 01 04 ff ff ff 00 02
0130  04 ff ff b9 b0 03 08 ac 10 02 fe ac 10 0a 01 04
0140  04 ac 10 02 01 07 04 ac 10 02 01 42 0a 31 37 32
(option 66 immediately above)
0150  2e 31 36 2e 32 2e 31 ff
```

Incognito DHCP サーバおよび Thomson ケーブル モデムとともに DMIC を使用する場合、両方のオプションが DHCP オファーで送信されないようにする必要があります。これを実現するには、次の回避策のいずれかを使用します。

- 上記のように sname オプションが含まれないように Incognito DHCP サーバを変更します。
- 上記の例で示す問題のあるパケット キャプチャのように sname がオプション 66 よりも優先されないようにケーブル モデム コードを変更します。
- CNR のような準拠した DHCP および TFTP サーバに移行します。これは、パフォーマンスも大幅に優れています。

追加の DOCSIS DHCP 情報、またはオプションの DHCP MAC 除外については、以下のリソースを参照してください。

- 『*DHCP Options and BOOTP Vendor Extensions*』（*RFC 2132*）

http://www.ietf.org/rfc/rfc2132.txt

- 『*Filtering Cable DHCP Lease Queries on Cisco CMTS Routers*』

http://www.cisco.com/en/US/docs/cable/cmts/feature/cblsrcvy.html

DOCSIS 準拠

- ケーブル モデムは、DOCSIS 準拠であると見なされます。ケーブル モデムが完全な DOCSIS 準拠でない場合、まれに登録時に CMTS メッセージ整合性チェック（MIC）障害をトリガーすることがあります。ただし通常運用では、動的共有秘密機能から CMTS MIC チェックに失敗したケーブル モデムは、DOCSIS 準拠ではないか、または DOCSIS のセキュリティ機能を回避するためにエンド ユーザによってハッキングされる可能性があります。

OUI が以下のケーブル モデムの一部には、ハードウェアおよびソフトウェアのリビジョンに応じて、動的共有秘密機能に問題があると認識されています。

- ◦ 00.01.03
  ◦ 00.E0.6F
  ◦ 00.02.B2

これらのケーブル モデムは、init(o) MAC 状態でスタックしたままになることがあり、動的共有秘密機能が無効になるまでオンラインにできません。この問題が発生した場合は、ケーブル モデムのソフトウェアを完全に準拠したソフトウェア リビジョンにアップグレードすることを推奨します。

また、グローバル コンフィギュレーション モードで次のコマンドを使用して、これらのケーブル モデムを動的秘密機能から除外することもできます。

cable dynamic-secret exclude

ケーブル モデムを除外するということは、違反者が除外された OUI を使用するようにケーブル モデムを変更する場合、システムが保護されなくなる、ということです。#unique_1687を参照してください。

ヒント　プロバイダーがネットワーク内の DOCSIS 非準拠モデムを特定できるようにするため、動的共有秘密機能では「マークのみ」オプションをサポートします。マークのみモードでの動作時、ケーブル モデムはプロビジョニングされているサービス クラスよりも上位のクラスを正常に取得できる可能性がありますが、これらのケーブル モデムは、**show cable modem** コマンド（たとえば **!online** を指定）の出力で違反としてマークされます。このようなケーブル モデムは、**show cable modem rogue** コマンドでも表示されます。サービス プロバイダーは、そのケーブル モデムを DOCSIS 準拠ソフトウェアにアップグレードする必要があるかどうか、またはエンドユーザがサービス不正使用攻撃のためにケーブル モデムをハッキングしたかどうかを判断できます。

次に、違反したケーブル モデムが設置されている状態の Cisco CMTS に対する **cable dynamic-secret mark** コマンドの出力例を示します。これらのケーブル モデムは、**!online** ステータスに到達するまでの最大 3 回の登録サイクルに対して、簡潔に「reject(m)」として表示される可能性があります。

```
Router# show cable modem rogue
                                    Spoof TFTP
MAC Address    Vendor     Interface  Count Dnld Dynamic Secret
000f.0000.0133 00.0F.00   C4/0/U1    3     Yes  905B740F906B48870B3A9C5E441CDC67
000f.0000.0130 00.0F.00   C4/0/U1    3     Yes  051AEA93062A984F55B7AAC979D10901
000f.0000.0132 00.0F.00   C4/0/U2    3     Yes  FEDC1A6DA5C92B17B23AFD2BBFBAD9E1
vxr#scm | inc 000f
000f.0000.0133 4.174.4.101     C4/0/U1  !online       1     -7.00 2816    0   N
000f.0000.0130 4.174.4.89      C4/0/U1  !online       2     -6.50 2819    0   N
000f.0000.0132 4.174.4.90      C4/0/U2  !online       18    -7.00 2819    0   N
```

TFTP の制限事項

- 次の状況では、ケーブル モデムが TFTP 転送状態のままになる可能性があります（**showcablemodem** コマンドに init(o) として表示されます）。
  - **cabledynamic-secret** コマンドにより動的共有秘密機能がケーブル インターフェイスで有効になっている。この機能は、ケーブル モデムが不正なケーブル モデムであるか、ケーブル モデムが更新されていない初期の DOCSIS 1.0 ファームウェアを実行している DOCSIS 1.0 ケーブル モデムである場合に適用されます。この機能はまた、TFTP サーバが Cisco CMTS にケーブル モデムの TFTP コンフィギュレーション ファイルを提供できない場合にも適用されます。これはたとえば、BACC を使用していて、一致しない送信元 IP アドレスからの TFTP 要求を許可するようシステムを設定していない場合があてはまります。この障害は、**debugcabledynamic-secret** コマンドによっても示されます。
  - 同時に多数のケーブル モデムが登録されている。それらのケーブル モデムの一部またはすべては、Cisco CMTS ルータ上の複数の TFTP ポートを使用する複数の TFTP 転送を使用して DOCSIS コンフィギュレーション ファイルもダウンロードしている可能性があり、TFTP サーバは、システムによって生成される TFTP 要求のレートについて行くことができません。一部の TFTP サーバは、単位時間あたりの同じ送信元 IP アドレスに

より開始された同時 TFTP get 要求の数を制限されるか、またはケーブルの動的秘密が設定される前に新しいモデムの登録レートを処理できない可能性があります。**debugcabledynamic-secret** コマンドは、このような状況で一部のファイルを受信できなかったことを示します。

このスタック ケーブル モデムの状況により TFTP サーバで使用可能なポートが足りなくなり、その結果、TFTP ダウンロードの段階でケーブルが失敗する可能性があります。この状況が発生するのを防ぐには、ケーブル インターフェイス上の動的共有秘密機能を一時的にディセーブルにするか、または DOCSIS コンフィギュレーション ファイルのサイズを軽減します。

動的共有秘密に関する情報

DOCSIS 仕様では、ケーブル モデムが承認済み TFTP サーバから、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必要があります。この DOCSIS コンフィギュレーション ファイルは、ネットワーク セッションの Quality of Service（QoS）およびその他のパラメータを指定します。サービス不正使用攻撃では、承認済み DOCSIS コンフィギュレーション ファイルを傍受、変更、または置換したり、ローカル TFTP サーバからファイルをダウンロードしたりしようと頻繁に試みます。

サービス不正使用攻撃を防ぐため、DOCSIS 仕様ではサービス プロバイダーが共有秘密パスワードを使用して、すべての DOCSIS コンフィギュレーション ファイルに接続された CMTS メッセージ整合性チェック（MIC）フィールドを計算することを許可しています。CMTS MIC は、コンフィギュレーション ファイルで指定される DOCSIS タイプ/長さ/値（TLV）フィールドにわたって計算された MD5 ダイジェストです。共有秘密が使用されている場合は、共有秘密も MD5 の計算で使用されます。

ケーブル モデムは、登録要求に CMTS MIC の計算と、DOCSIS コンフィギュレーション ファイルのコンテンツを含める必要があります。ユーザが DOCSIS コンフィギュレーション ファイルのいずれかのフィールドを修正するか、または別の共有秘密値を使用する場合、ケーブル モデムの登録時に CMTS は CMTS MIC を確認できません。CMTS は、ケーブル モデムの登録を許可せず、そのケーブル モデムを「reject(m)」状態であるとマークして、CMTS MIC 障害を示します。

ただし、ユーザはこれまでさまざまな手法を使用してこのようなセキュリティ チェックを迂回してきました。そのため、プレミアム サービスを提供するコンフィギュレーション ファイルを取得してから、そのファイルを使用して自分自身により高位のサービス クラスを提供します。サービス プロバイダーは、共有秘密を変更し、DOCSIS タイムスタンプを実装し、モデム固有のコンフィギュレーション ファイルを使用することで、これに対抗してきました。しかしこれは、ネットワークのケーブル モデムごとに DOCSIS コンフィギュレーション ファイルを作成することに他なりません。さらに、このような対抗は、共有秘密が発見されるたびに繰り返さなければなりません。

動的共有秘密機能は、ネットワークのケーブル モデムごとに一意であり動的に生成された共有秘密を実装することで、このようなタイプの攻撃を防ぎます。また、動的共有秘密は現在のセッションに対してのみ有効であり、再利用はできません。こうすることで、「リプレイ アタック」の脅威を取り除き、変更および置換された DOCSIS コンフィギュレーション ファイルの再利用を防ぎます。

動作モード

動的共有秘密機能は、CMTS MIC 検証チェックに失敗したケーブル モデムに対してとるべき処置に応じて、次の 3 つの異なるモードで動作します。

- マーキング モード：**mark** オプションを使用すると、CMTS MIC 妥当性チェックに失敗した場合でも、CMTS はケーブル モデムをオンラインにします。ただし、CMTS はこの状況を調査できるようにするために、コンソールに警告メッセージを出力し、**show cable modem** コマンド内のこのケーブル モデムに感嘆符（!）のマークを付けます。
- ロッキング モード：**lock** オプションが使用されていると、CMTS は、2 回連続して MIC 妥当性チェックに失敗した CM に制限付き QoS 設定を割り当てます。ロックされたケーブル モデムに特定の QoS プロファイルを使用するよう指定できます。そうしない場合はデフォルトで、ダウンストリームおよびアップストリーム サービス フローの最大レートを 10 kbps に制限する特別な QoS プロファイルに設定されます。

顧客が CM をリセットするとその CM は再登録されますが、制限付きの QoS プロファイルがそのまま使用されます。ロックされた CM はオフラインになるまで、制限された QoS プロファイルを使い続け、そのまま 24 時間以上オフラインのままになります。その後、有効な DOCSIS コンフィギュレーション ファイルで再登録できるようになります。システム オペレータは、**clear cable modem lock** コマンドを使用して CM のロックを手動でクリアできます。

このオプションは、共有秘密鍵を推測しようとしたり、動的共有秘密セキュリティ システムの詳細を確認しようとして CMTS に繰り返し再登録するユーザを挫折させます。

- 拒否モード：拒否モードでは、CMTS は、CMTS MIC 妥当性チェックに失敗した CM がオンラインになることを拒否します。このようなケーブル モデムは、**show cable modem** コマンドの出力で「reject(m)」（無効な MIC 値）という MAC 状態で示されます。短いタイムアウト期間が経過すると、CM は CMTS に再登録を試みます。CM がオンラインになることを許可されるには、有効な DOCSIS コンフィギュレーション ファイルに登録する必要があります。CM がオンラインになると、CMTS はコンソールに警告メッセージを出力し、**show cable modem** コマンドでこのケーブル モデムに感嘆符（!）マークが付くので、この状況を調査できます。

（注） パケット損失や輻輳など、考えられるネットワークの問題を解明するため、Cisco CMTS はケーブルモデムに対して、動的共有秘密の認証チェックに失敗とマークする前に、2回の登録試行を許可します。

動的共有秘密の動作

動的共有秘密機能は、モデムごとに一意の DOCSIS 共有秘密を自動作成して、現在のセッションでのみ有効なワンタイム使用の DOCSIS コンフィギュレーション ファイルを作成します。これにより、1 つのケーブル モデムにダウンロードされた DOCSIS コンフィギュレーション ファイルを

他のモデムで使用することはできなくなり、同じモデムが後でこのコンフィギュレーション ファイルを再利用することもできなくなります。

特許出願中のこの機能は、登録されたすべてのモデムが、モデムの登録時にその特定のモデム用に DOCSIS プロビジョニング システムが指定した QoS パラメータのみを使用することを保証するために設計されています。

DOCSIS 準拠のケーブル モデムは CMTS への登録時に DHCP 要求を送信します。DHCP サーバは、そのケーブル モデムが指定の TFTP サーバからダウンロードするべき DOCSIS コンフィギュレーション ファイルの名前を含む DHCP 応答を送信します。ケーブル モデムは、DOCSIS コンフィギュレーション ファイルをダウンロードし、そのパラメータを使用して CMTS に登録します。

動的共有秘密機能が有効化されている場合、CMTS は DHCP メッセージを受信したときに次の動作を実行します。

- CMTS は動的に生成された共有秘密を作成します。
- デフォルト設定で、CMTS は DOCSIS コンフィギュレーション ファイルの名前を利用して、ランダム化された新しいファイル名を生成します。ランダム化されたこのファイル名はケーブル モデムが登録されるたびに変更され、DOCSIS 仕様に半分しか準拠しないケーブル モデムによる DOCSIS コンフィギュレーション ファイルのキャッシュを防ぎます。
  cabledynamic-secret コマンドで **nocrypt** オプションを使用することで、このファイル名のランダム化を無効にできます。
- CMTS は、ケーブル モデムが使用すべき TFTP サーバの IP アドレスを CMTS の IP アドレスに変更します。これにより、ケーブル モデムは、CMTS からコンフィギュレーション ファイルをダウンロードする必要があることを認識します。
- CMTS は、新しく生成された動的な秘密を使用するファイルを修正できるよう、当初指定されていた TFTP サーバからのオリジナルの DOCSIS コンフィギュレーション ファイルをダウンロードします。

ケーブル モデムが 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際、CMTS により修正されたファイルを受け取ります。このファイルは動的に生成されたワンタイム使用の共有秘密を使用しているため、CMTS は、ケーブル モデムが CMTS の登録を試みる際にこのコンフィギュレーション ファイルを使用していることを確認できます。

（注） 動的共有秘密機能は、**cable shared-secondary-secret** および **cable shared-secret** コマンドを使って設定されるオリジナルの共有秘密やセカンダリ共有秘密の使用をサポートせず、互換性もありません。

ヒント ユーザが、ローカルの TFTP サーバから 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ことによってこのようなチェックを迂回することは可能ですが、その場合も、ケーブル モデムは CMTS MIC の検証に失敗します。

他のコマンドとのインタラクション

動的共有秘密機能は、ネットワーク セキュリティと整合性を確保するために、他のいくつかのコマンドとともに動作します。

- **cableshared-secret**：DOCSIS 仕様では、サービス プロバイダーが共有秘密を使用して、許可された DOCSIS コンフィギュレーション ファイルのみをケーブル モデムが使用するようにすることができます。

  動的共有秘密機能は **cable shared-secret** と互換性がありません。動的共有秘密機能を使用する場合は、**cable shared-secret** コマンドを設定しないでください。

- **cableshared-secondary-secret**：動的共有秘密機能は **cable shared-secret** と互換性がありません。動的共有秘密機能を使用する場合は、**cable secondary-shared-secret** コマンドを設定しないでください。

パフォーマンス情報

動的共有秘密機能により、ケーブル モデムの登録プロセスに新たな手順が加えられたり、現在のプロビジョニング システムにさらなる要件が必要になることはありません。次の要因によっては、この機能がネットワーク プロビジョニング システムのパフォーマンスにわずかにマイナスまたはプラスの影響を及ぼす場合があります。

- 使用されているプロビジョニング システム（DHCP および TFTP サーバ）
- オンラインになるケーブル モデムの数
- ケーブル モデムのベンダーおよびソフトウェア バージョン
- DOCSIS コンフィギュレーション ファイルの数とサイズ

動的共有秘密機能により、ケーブル モデムがオンラインになるまでの時間が 5% の遅延から 10% 短縮することが大規模な試験により明らかになっています。プロビジョニング プロセスのパフォーマンスに最も大きく影響する要因は、プロビジョニング システム自体です。そのためシスコでは、汎用 DHCP および TFTP サーバで大幅なパフォーマンス向上をもたらす Cisco Network Registrar（CNR）リリース 3.5 以降の使用を推奨します。

ケーブル モデムのプロビジョニング パフォーマンスに 2 番目に影響する要因は、DOCSIS コンフィギュレーションファイルの数とサイズです。コンフィギュレーションファイルのサイズは、ファイルをケーブル モデムに送信するまでにかかる時間を決定します。一方、コンフィギュレーションファイルの数は、同じコンフィギュレーションファイルを複数モデムで再利用できるようにしながら、システムが内部キャッシュにいかに効率的にファイルを保存するかに影響を与える場合があります。

SNMP サポート

Cisco IOS-XE 3.15.0S 以降のリリースでは、動的共有秘密機能に次の SNMP サポートが追加されています。

- 次の MIB オブジェクトが CISCO-DOCS-EXT-MIB に追加されています。
  - cdxCmtsCmDMICMode：特定のケーブル モデムの動的共有秘密機能を設定し、その設定を表示します（[not configured]、[mark]、[lock]、または [reject]）。
  - cdxCmtsCmDMICLockQoS：インターフェイスが [lock] モードに設定されていたときに動的共有秘密セキュリティ チェックに失敗したケーブル モデムに割り当てる制限付き QoS プロファイルを指定します。
  - cdxCmtsCmStatusDMICTable：動的共有秘密セキュリティ チェックに失敗したすべてのケーブル モデムを表示します。
- 動的共有秘密セキュリティ チェックに失敗したためにケーブル モデムがロックされた場合、SNMP トラップ（cdxCmtsCmDMICLockNotification）を送信するよう設定できます。トラップを有効にするには、**snmp-serverenabletrapscabledmic-lock** コマンドを使用します。

（注） DMIC の [lock] モードは、HCCP N+1 冗長性のスイッチオーバー イベントの間、ディセーブルになります。

システム エラー メッセージ

次のシステム エラー メッセージは、動的共有秘密機能がイネーブルのときに CMTS のメッセージ整合性チェック（MIC）に失敗したケーブル モデムに関する情報を提供します。

メッセージ

%CBR-4-CMLOCKED

ケーブル モデムの DOCSIS コンフィギュレーション ファイルに、メッセージ整合性チェック（MIC）の値を符号化するために使用された適切な動的共有秘密機能に対応する MIC 値が含まれていませんでした。このため、CMTS はこのケーブル モデムにネットワークへのアクセスを制限する制限付き Quality of Service（QoS）設定を割り当てました。さらに、CMTS は、このケーブル モデムが少なくとも 24 時間オフラインになり、24 時間後に通常のサービスの登録および取得が許可される（DOCSIS 準拠であり、有効な DOCSIS コンフィギュレーション ファイルを使用していることが想定される）までは制限付き QoS 設定でロックされたままであるよう、ケーブル モデムをロックしました。

このエラー メッセージは、ケーブル インターフェイスに **cable dynamic-secret lock** コマンドが適用されて、そのケーブル インターフェイス上の DOCSIS コンフィギュレーション ファイルの動的共有秘密機能が有効になっている場合に表示されます。ケーブル モデムは登録を許可されてオンラインになりますが、QoS 設定により、アップストリーム フローとダウンストリーム フローはともに最大レートが 10 kbps に制限されます。このケーブル モデムが以前に使用したコンフィギュレーション ファイルをキャッシュした古いソフトウェアを実行していないことを確認してください。また、ローカル TFTP サーバから変更された DOCSIS コンフィギュレーション ファイルをダウンロードしようとするユーザにより、サービス不正使用が試みられていないこともチェックしてください。別の QoS プロファイルで CM を再登録するには、その前に、登録を試行することな

く CM が 24 時間オフライン状態を保つか、または **clear cable modem lock** コマンドを使って手動でロックを解除する必要があります。

メッセージ

%CBR-4-CMMARKED

ケーブル モデムの DOCSIS コンフィギュレーション ファイルに、メッセージ整合性チェック（MIC）の値を符号化するために使用された適切な動的共有秘密機能に対応する MIC 値が含まれていませんでした。CMTS はこのケーブル モデムの登録とオンライン化を許可しましたが、**show cable modem** 表示でこのモデムに感嘆符（!）が付き、状況を調査する対象となっています。

このエラー メッセージは、ケーブル インターフェイスに **cabledynamic-secretmark** コマンドが適用されて、そのケーブル インターフェイス上の DOCSIS コンフィギュレーション ファイルの動的共有秘密機能が有効になっている場合に表示されます。このケーブル モデムが以前に使用したコンフィギュレーション ファイルをキャッシュした古いソフトウェアを実行していないことを確認してください。また、ローカル TFTP サーバから変更された DOCSIS コンフィギュレーション ファイルをダウンロードしようとするユーザにより、サービス不正使用が試みられていないこともチェックしてください。

メッセージ

%CBR-4-NOCFGFILE

CMTS は TFTP サーバからこのケーブル モデムの DOCSIS コンフィギュレーション ファイルを取得できませんでした。 このメッセージは、**cable dynamic-secret** コマンドにより動的共有秘密機能がケーブル インターフェイスで有効になっている場合に表示されます。

CMTS が TFTP サーバとネットワーク接続されているか、また、指定されている DOCSIS コンフィギュレーション ファイルが TFTP サーバ上で使用可能かどうかを確認してください。ケーブル モデムへの DHCP 応答で適切なコンフィギュレーション ファイル名を送信するよう、DHCP サーバが正しく設定されていることを確認してください。DOCSIS コンフィギュレーション ファイルが正しい形式であることも確認してください。

この問題は、TFTP サーバがオフラインであるか、または新しい要求に迅速に対応できない状況までオーバーロードになると発生する可能性があります。また、CMTS と TFTP サーバ間のインターフェイスが正しく設定されておらず、過度にフラッピングしている場合にも発生する場合があります。

（注） このエラーは、Cisco CMTS の外部のプロビジョニング システムの問題を示します。動的共有秘密機能をディセーブルにしても、エラーは解除されず、ケーブル モデムもオンライン化されません。まず最初にプロビジョニング システムの問題を修正する必要があります。

利点

動的共有秘密機能では、ケーブル サービス プロバイダーとそのパートナーおよびカスタマーに次の利点があります。

ネットワーク セキュリティの改善

サービス プロバイダーは、ユーザが共有秘密値を見つけ出し、それを使用して自分自身に高いサービス レベルを与えるように DOCSIS コンフィギュレーション ファイルを変更してしまうといった心配は無用です。仮にユーザが動的に生成された共有秘密の値を見つけ出したとしても、その共有秘密は登録に再度使用できません。

Cisco CMTS ルータにおける汎用 TFTP サーバのパフォーマンスとエラー処理は大幅に改善され、ケーブル モデムを迅速にプロビジョニングするために必要な高いパフォーマンスをサポートします。

可能性のあるサービス不正使用攻撃の対処における柔軟性

サービス プロバイダーでは、DOCSIS コンフィギュレーション ファイルの CMTS MIC チェックに失敗したときの対応を選択することができます。対応は、そのケーブル モデムをマークしてユーザがオンラインになることを許可する、登録要求を拒否して有効な DOCSIS コンフィギュレーション ファイルが使用されるまでユーザがオンラインになることを許可しない、または、ケーブル モデムを制限された QoS 構成にロックしてモデムを 24 時間オフライン状態にする、の中から選択できます。サービス不正使用攻撃を試みるユーザにとって、悪意のあるモデムをロックする方法は代償が大きい割に得るものが少ないため、ハッカーに対して最も効果の高い抑止力になります。

プロビジョニング システムへの変更は不要

サービス プロバイダーは、認証システムのプロビジョニングを変更せずに動的共有秘密機能を使用できます。既存の DOCSIS コンフィギュレーション ファイルは変更せずに使用でき、既存の共有秘密を変更する必要はありません。

ヒント　CMTS ルータだけが TFTP サーバから DOCSIS コンフィギュレーション ファイルのダウンロードを許可するようなアクセス コントロールを設定していない場合は、そのように設定することも可能です。

ケーブル モデムへの変更は不要

動的共有秘密機能では、エンドユーザ側の変更やケーブル モデム構成への変更は不要です。この機能は、DOCSIS 準拠のあらゆるケーブル モデムをサポートします。

（注）　動的共有秘密機能は、すでにオンラインでプロビジョニングされたケーブル モデムに影響しません。この機能が有効または無効になったときにすでにオンラインであるケーブル モデムは、オンライン状態が維持されます。

ネットワーク管理のシンプル化

サービスプロバイダーは、プレミアムサービスを提供するファイルが広く使用可能になるたびにケーブル インターフェイス上の共有秘密を更新し続ける必要はありません。代わりに、動的共有

秘密機能がケーブル モデムごとに提供する一意で単一用途の共有秘密を信頼することで、長期にわたって同じ共有秘密をケーブル インターフェイス上で使用できます。

また、サービス プロバイダーは、ケーブル モデムごとに一意の DOCSIS コンフィギュレーション ファイルを管理する必要がありません。同じコンフィギュレーション ファイルを同じサービス クラス内のすべてのユーザに対して使用でき、ネットワーク セキュリティに影響を与えません。

関連機能

次の機能を動的共有秘密機能と併用して、ケーブル ネットワークの全体的なセキュリティを強化できます。

- ベースライン プライバシー インターフェイス プラス（BPI+）認証と暗号化：ケーブル モデムと CMTS 間にセキュア リンクを提供し、ケーブル インターフェイス上で送信されるパケットをユーザが傍受したり変更したりするのを防ぎます。BPI+ はさらに、X.509 デジタル証明書の使用によるケーブル モデムの安全な承認、およびソフトウェア アップグレードをスプーフィングや傍受、変更から確実に保護するセキュアなソフトウェア ダウンロード機能を提供します。

動的共有秘密機能の設定方法

ここでは、動的共有秘密機能をイネーブルにして設定する方法、ディセーブルにする方法、ケーブル モデムのロックを手動で解除する方法、ケーブル モデムのファームウェアを動的にアップグレードする方法について説明します。

（注） すべての手順は、特権 EXEC プロンプト（「Router#」）で開始、終了します。

動的共有秘密機能の有効化と設定

ここでは、ケーブル インターフェイスで動的共有秘密機能を有効化および設定する方法について説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Router# configure terminal`	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。

	コマンドまたはアクション	目的
	例： `Router(config)#`	

ステップ 2	**cableqospermissioncreate**
	例：
	`Router(config)# cable qos permission create`
	例：
	`Router(config)#`
		（任意）ステップ 6 で **lock** オプションを使用する場合、および特定の QoS プロファイルを指定しない場合は、ケーブル モデムが独自の QoS プロファイルを作成できるようにする必要があります。

ステップ 3	**cableqospermissionupdate**
	例：
	`Router(config)# cable qos permission update`
	例：
	`Router(config)#`
		（任意）ステップ 6 で **lock** オプションを使用する場合、および特定の QoS プロファイルを指定しない場合は、ケーブル モデムが独自の QoS プロファイルを更新できるようにする必要があります。

ステップ 4	**snmp-serverenabletrapscabledmic-lock**
	例：
	`Router(config)# snmp-server enable traps cable dmic-lock`
	例：
	`Router(config)#`
		（任意）ケーブルモデムが動的共有秘密のセキュリティ チェックに失敗した場合、SNMP トラップを送信できるようにすることができます。

ステップ 5	**interfacecable** *interface*
	例：
	`Router(config)# interface cable 3/0`
	例：
	`Router(config-if)#`
		指定したケーブル インターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 6	**cabledynamic-secret** {**lock**[*lock-qos*] | **mark** | **reject**} [**nocrypt**
	
	例：
	`Router(config-if)# cable dynamic-secret lock`
	
	例：
	`Router(config-if)# cable dynamic-secret lock 90`
	
	例：
	`Router(config-if)# cable dynamic-secret mark`
	
	例：
	`Router(config-if)# cable dynamic-secret reject`
	
	例：
	`Router(config-if)#`
		ケーブル インターフェイスで動的共有秘密機能を有効にして、適切なオプションを設定します。
		• **nocrypt**：（任意）Cisco CMTS は DOCSIS コンフィギュレーション ファイルのファイル名を暗号化しませんが、元のファイル名を使用して CM にファイルを送信します。
		• **lock**：MIC の検証に失敗したケーブル モデムは、制限付き QoS プロファイルを使用してオンラインになることができます。異なる QoS プロファイルを使用してケーブル モデムを再登録できるようにするには、24 時間オフラインにする必要があります。
		• *lock-qos*：（任意）ロックされたケーブル モデムに割り当てる必要のある QoS プロファイルを指定します。有効な範囲は 1 ～ 256 であり、プロファイルをあらかじめ作成しておく必要があります。特に指定しない限り、ロックされたケーブル モデムには、サービス フローを 10 kbps（ステップ 2 と 3 で必要）に制限した QoS プロファイルが割り当てられます。
		• **mark**：MIC 検証に失敗したケーブル モデムはオンライン状態を許可されますが、その状況を調査できるように **showcablemodem** 表示にマークが付きます。
		• **reject**：MIC の検証に失敗したケーブル モデムは登録できません。
		
		（注） 設定する各ケーブル インターフェイスでステップ 5 およびステップ 6 を繰り返します。

ステップ 7	**end**
	
	例：
	`Router(config-if)# end`
	
	例：
	`Router#`
		インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次の作業

（注） ケーブルインターフェイスバンドルのインターフェイスで動的共有秘密機能を設定する場合、それと同じバンドル内のすべてのインターフェイスでこの機能を設定する必要があります。

ケーブル インターフェイスでの動的共有秘密の無効化

ここでは、ケーブル インターフェイスで動的共有秘密機能を無効化する方法について説明します。ケーブルモデムは、ケーブルインターフェイスで定義された共有秘密またはセカンダリ共有秘密と比較して継続的に検証されます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configureterminal**
	例：
	`Router# configure terminal`
	例：
	`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 2	**interfacecable** *interface*
	例：
	`Router(config)# interface cable 3/0`
	例：
	`Router(config-if)#`
		指定したケーブルインターフェイスに対してインターフェイス 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	**nocabledynamic-secret**
	例：
	`Router(config-if)# no cable dynamic-secret`
	例：
	`Router(config-if)#`
		ケーブルインターフェイスで動的共有秘密機能を無効にします。
		（注） 設定する各ケーブル インターフェイスでステップ 2 およびステップ 3 を繰り返します。

	コマンドまたはアクション	目的

ステップ 4	**end**
	
	例：
	`Router(config-if)# end`
	
	例：
	`Router#`
		インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

動的共有秘密機能からのケーブル モデムの除外

ここでは、動的共有秘密機能の処理から 1 つ以上のケーブル モデムを除外する方法について説明します。ケーブルモデムは、ケーブルインターフェイスで定義された共有秘密またはセカンダリ共有秘密と比較して継続的に検証されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Router# configure terminal`	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 2	**cable dynamic-secret exclude** {**oui** *oui-id* | **modem** *mac-address*}
	
	例：
	`Router(config)# cable dynamic-secret exclude oui 00.01.B4`
	`Router(config)# cable dynamic-secret exclude modem 00d0.45ba.b34b`
		MAC アドレスまたは OUI に基づいて、動的共有秘密セキュリティ チェックの処理から 1 つ以上のケーブル モデムを除外します。
		
		• **modem** *mac-address*：動的共有秘密機能から除外する、1 つの具体的な個別のケーブル モデムのハードウェア（MAC）アドレスを指定します（マルチキャスト MAC アドレスは指定できません。）
		
		• **oui** *oui-id*：特定のベンダーのケーブル モデム グループが動的共有秘密機能から除外されるように、そのベンダーの組織固有識別子（OUI）を指定します。OUI は、3 個の 16 進数バイトをピリオドまたはコロンで区切って指定する必要があります。
		
		（注） 除外するケーブル モデム MAC アドレスまたは OUI ベンダーのそれぞれに対してこのコマンドを繰り返します。

	コマンドまたはアクション	目的
ステップ 3	**exit** 例： `Router(config)# exit`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

1 つ以上のケーブル モデムのロック削除

ここでは、1 つ以上のケーブル モデムのロックを手動で解除する方法について説明します。これにより、ケーブルモデムの再初期化が強制的に行われます。ケーブルモデムをオンライン状態にするには、有効な DOCSIS コンフィギュレーション ファイルで再登録する必要があります。（**clearcablemodemlock** コマンドを使用して）手動でロックを解除しない場合、ケーブル モデムは現在の制限付き QoS プロファイルにロックされるため、オフライン状態で 24 時間以上経過するまでは、異なるプロファイルで再登録できません。

手順

	コマンドまたはアクション	目的

ステップ 1	**clearcablemodem** {*mac-addr* | *ip-addr* | **all** | **oui***string* | **reject**} **lock**
	
	例：
	`Router# clear cable modem 0001.0203.0405 lock`
	
	例：
	`Router# clear cable modem all lock`
	
	例：
	`Router# clear cable modem oui 00.00.0C lock`
	
	例：
	`Router#`
		次のオプションを指定して、ケーブルモデムのロックを解除します。
		• *mac-addr*：解除する 1 つの特定のケーブル モデムの MAC アドレスを指定します。
		• *ip-addr*：解除する 1 つの特定のケーブル モデムの IP アドレスを指定します。
		• **all**：ロックされたすべてのケーブルモデムのロックを解除します。
		• **oui** *string*：指定した組織固有識別子（OUI）文字列と一致するベンダー ID を持つすべてのケーブル モデムのロックを解除します。
		• **reject**：現在拒否状態にあるすべてのケーブル モデムのロックを解除します（これは、ロックしたケーブル モデムがオフライン状態に移行し、24 時間が経過する前に再登録しようとすると発生します）。

次の作業

ヒント　また、**clearcablemodemdelete** コマンドを使用してすべての CMTS 内部データベースからケーブル モデムを手動で削除するという方法で、ケーブル モデムのロックを解除することもできます。

ケーブル モデムのファームウェアのアップグレード

ここでは、ケーブルモデムでダウンロードしたDOCSISコンフィギュレーション ファイルに正しいTLV値を動的に挿入して、ケーブルモデムのファームウェアをアップグレードする方法について説明します。DOCSIS コンフィギュレーション ファイルには次の TLV 値が含まれます。

- ソフトウェア アップグレード ファイル名（TLV 9）：ファームウェアのファイル名を指定します。
- アップグレード IPv4 TFTP サーバ（TLV21）：モデムが 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 TFTP サーバの IPv4 アドレスを指定します。
- アップグレード IPv6 TFTP サーバ（TLV58）：モデムが 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 TFTP サーバの IPv6 アドレスを指定します。

（注）　ソフトウェア アップグレード ファイル名（TLV9）が指定された場合、および TFTP サーバ アドレス（TLV21/TLV58）が指定されていないか、0 に設定されていない場合のみ、TFTP サーバ アドレスが挿入されます。

はじめる前に

ケーブル モデムのファームウェアをアップグレードするには、まず動的共有秘密機能を有効にする必要があります。詳細については、動的共有秘密機能の有効化と設定，（1399ページ）を参照してください。

（注）　動的共有秘密機能を有効または無効にするコマンドは、MAC ドメイン レベルで使用できます。ただし、ケーブル モデムのファームウェアをアップグレードするコマンドを使用できるのはグローバル レベルです。

手順

	コマンドまたはアクション	目的

ステップ 1	**configureterminal**
	
	例：
	`Router# configure terminal`
	
	例：
	`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 2	cable dynamic-secret tftp insert-upgrade-server 例： `Router(config)# cable dynamic-secret tftp insert-upgrade-server`	DOCSIS コンフィギュレーション ファイルに特定の IPv4 または IPv6 TLV 値を動的に挿入し、ケーブル モデムでファームウェア アップグレードを完了します。

ステップ 3	**end**
	
	例：
	`Router(config)# end`
	
	例：
	`Router#`
		コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次の作業

（注） ケーブルインターフェイス バンドルのインターフェイスで動的共有秘密機能を設定する場合、そのバンドルのすべてのインターフェイスでこの機能を設定する必要があります。

動的共有秘密機能のモニタリング方法

ここでは、動的共有秘密機能に関する情報をモニタリングおよび表示するのに使用できる次の手順について説明します。

マーク付きケーブル モデムの表示

cabledynamic-secretmark コマンドを使用してケーブル インターフェイスを設定した場合、動的に生成される CMTS MIC の検証に失敗してもケーブル モデムはオンラインになります。ただし、**showcablemodem** コマンドの出力で MAC 状態列に感嘆符（!）マークが表示されます。また、この感嘆符は、**cabledynamic-secretreject** コマンドを使って最初に拒否された後、有効な DOCSIS コンフィギュレーション ファイルを使って再登録されたケーブル モデムを識別するためにも使用されます。

たとえば、次に、4 つのケーブル モデムで CMTS MIC の検証に失敗してマークが付けられても、オンラインが許可された例を示します。

```
Router# show cable modems

MAC Address    IP Address      I/F       MAC         Prim RxPwr  Timing  Num BPI
                                         State       Sid  (db)   Offset  CPE Enb
0010.9507.01db 144.205.151.130 C5/1/0/U5 online(pt)  1     0.25    938   1    N
0080.37b8.e99b 144.205.151.131 C5/1/0/U5 online      2     -0.25   1268  0    N
0002.fdfa.12ef 144.205.151.232 C6/1/0/U0 online(pt)  13    -0.25   1920  1    N
0002.fdfa.137d 144.205.151.160 C6/1/0/U0 !online     16    -0.50   1920  1    N
0003.e38f.e9ab 144.205.151.237 C6/1/0/U0 !online     3     -0.50   1926  1    N
0003.e3a6.8173 144.205.151.179 C6/1/1/U2 offline     4     0.50    1929  0    N
0003.e3a6.8195 144.205.151.219 C6/1/1/U2 !online(pt) 22    -0.50   1929  1    N
0006.28dc.37fd 144.205.151.244 C6/1/1/U2 online(pt)  61    0.00    1925  2    N
0006.28e9.81c9 144.205.151.138 C6/1/1/U2 online(pt)  2     0.75    1925  1    N
0006.28f9.8bbd 144.205.151.134 C6/1/1/U2 online      25    -0.25   1924  1    N
0006.28f9.9d19 144.205.151.144 C6/1/1/U2 online(pt)  28    0.25    1924  1    N
0010.7bed.9b6d 144.205.151.228 C6/1/1/U2 online(pt)  59    0.25    1554  1    N
0002.fdfa.12db 144.205.151.234 C7/0/0/U0 online      15    -0.75   1914  1    N
0002.fdfa.138d 144.205.151.140 C7/0/0/U5 online      4     0.00    1917  1    N
0003.e38f.e85b 144.205.151.214 C7/0/0/U5 !online     17    0.25    1919  1    N
0003.e38f.f4cb 144.205.151.238 C7/0/0/U5 online(pt)  16    0.00   !2750  1    N
0003.e3a6.7fd9 144.205.151.151 C7/0/0/U5 online      1     0.25    1922  0    N
0020.4005.3f06 144.205.151.145 C7/0/0/U0 online(pt)  2     0.00    1901  1    N
0020.4006.b010 144.205.151.164 C7/0/0/U5 online(pt)  3     0.00    1901  1    N
0050.7302.3d83 144.205.151.240 C7/0/0/U0 online(pt)  18    -0.25   1543  1    N
00b0.6478.ae8d 144.205.151.254 C7/0/0/U5 online(pt)  44    0.25    1920  21   N
00d0.bad3.c0cd 144.205.151.149 C7/0/0/U5 online      19    0.25    1543  1    N
00d0.bad3.c0cf 144.205.151.194 C7/0/0/U0 online      13    0.00    1546  1    N
00d0.bad3.c0d5 144.205.151.133 C7/0/0/U0 online      12    0.50    1546  1    N
Router#
```

また、**showcablemodemrogue** コマンドを使用すると、動的な共有秘密の認証チェックに失敗して拒否されたケーブル モデムだけを表示することもできます。

```
Router# show cable modem rogue
                                 Spoof TFTP
MAC Address    Vendor     Interface  Count Dnld Dynamic Secret
AAAA.7b43.aa7f Vendor1    C4/0/U5       2  Yes  45494DC933F8F47A398F69EE6361B017
AAAA.7b43.aa7f Vendor1    C4/0/U5       2  Yes  D47BCBB5494E9936D51CB0EB66EF0B0A
BBBB.7b43.aa7f Vendor2    C4/0/U5       2  No   8EB196423170B26684BF6730C099D271
AAAA.7b43.aa7f Vendor1    C4/0/U5       2  No   DF8FE30203010001A326302430120603
BBBB.7b43.aa7f Vendor2    C4/0/U5       2  No   300E0603551D0F0101FF040403020106
AAAA.7b43.aa7f Vendor1    C4/0/U5       2  Yes  820101002D1A264CE212A1BB6C1728B3
DDDD.7b43.aa7f Vendor4    C4/0/U5       2  Yes  7935B694DCA90BC624AC92A519C214B9
AAAA.7b43.aa7f Vendor1    C4/0/U5       2  No   3AB096D00D56ECD07D9B7AB662451CFF
Router#
```

現在の動的秘密の表示

Cisco IOS XE Everest 16.5.1 では、**verbose** オプションを **showcablemodem** コマンドで使用すると、ケーブル モデルの前回の登録サイクルで使用された、動的に生成された共有秘密（16 バイトの 16 進数）が表示されます。また、ケーブル モデムが動的共有秘密の確認に失敗したか、または TFTP サーバから DOCSIS コンフィギュレーション ファイルをダウンロードしたかどうかも表示します。ケーブル モデムがオフラインの場合、動的秘密はすべてゼロと表示されます。

たとえば、次に、動的供給秘密の確認に失敗した単一ケーブル モデムの一般的な表示例を示します。

```
Router# show cable modem 00c0.73ee.bbaa verbose

MAC Address                          : 00c0.73ee.bbaa
IP Address                           : 3.18.1.6
Prim Sid                             : 2
QoS Profile Index                    : 6
Interface                            : C3/0/U0
Upstream Power                       : 0.00 dBmV (SNR = 26.92 dBmV)
Downstream Power                     : 0.00 dBmV (SNR = ----- dBmV)
Timing Offset                        :  2812
Initial Timing Offset                : 2812
Received Power                       :  0.00
MAC Version                          : DOC1.0
Provisioned Mode                     : DOC1.0
Capabilities                         : {Frag=N, Concat=N, PHS=N, Priv=BPI}
Sid/Said Limit                       : {Max Us Sids=0, Max Ds Saids=0}
Optional Filtering Support           : {802.1P=N, 802.1Q=N}
Transmit Equalizer Support           : {Taps/Symbol= 0, Num of Taps= 0}
Number of CPE IPs                    : 0(Max CPE IPs = 1)
CFG Max-CPE                          : 1
Flaps                                : 26(Feb 14 02:35:39)
Errors                               : 0 CRCs, 0 HCSes
Stn Mtn Failures                     : 6 aborts, 0 exhausted
Total US Flows                       : 1(1 active)
Total DS Flows                       : 1(1 active)
Total US Data                        : 0 packets, 0 bytes
Total US Throughput                  : 0 bits/sec, 0 packets/sec
Total DS Data                        : 0 packets, 0 bytes
Total DS Throughput                  : 0 bits/sec, 0 packets/sec
Active Classifiers                   : 0 (Max = NO LIMIT)
Dynamic Secret                       : A3D1028F36EBD54FDCC2F74719664D3F
Router#
```

次に、現在オフライン（[Dynamic Secret] フィールドはすべてゼロ）の単一ケーブル モデムの一般的な表示を示します。

```
Router# show cable modem 00C0.6914.8601 verbose

MAC Address                          : 00C0.6914.8601
IP Address                           : 10.212.192.119
Prim Sid                             : 6231
QoS Profile Index                    : 2
Interface                            : C5/1/0/U3
Upstream Power                       : 0.00 dBmV (SNR = 30.19 dBmV)
Downstream Power                     : 0.00 dBmV (SNR = ----- dBmV)
Timing Offset                        : 1831
Initial Timing Offset                : 1831
Received Power                       : !-2.25
MAC Version                          : DOC1.0
Provisioned Mode                     : DOC1.0
Capabilities                         : {Frag=N, Concat=Y, PHS=N, Priv=BPI}
Sid/Said Limit                       : {Max Us Sids=0, Max Ds Saids=0}
Optional Filtering Support           : {802.1P=N, 802.1Q=N}
```

```
Transmit Equalizer Support          : {Taps/Symbol= 0, Num of Taps= 0}
Number of CPE IPs                   : 4(Max CPE IPs = 4)
CFG Max-CPE                         : 4
Flaps                               : 20638(Feb 10 16:04:10)
Errors                              : 0 CRCs, 0 HCSes
Stn Mtn Failures                    : 108 aborts, 161 exhausted
Total US Flows                      : 1(1 active)
Total DS Flows                      : 1(1 active)
Total US Data                       : 236222 packets, 146630868 bytes
Total US Throughput                 : 0 bits/sec, 0 packets/sec
Total DS Data                       : 9 packets, 1114 bytes
Total DS Throughput                 : 0 bits/sec, 0 packets/sec
Active Classifiers                  : 0 (Max = NO LIMIT)
Dynamic Secret                      : 00000000000000000000000000000000
Router#
```

（注） 上記の [Dynamic Secret] フィールドはすべてゼロ（“00000000000000000000000000000000”）で、このケーブル モデムがオフラインであることを示します。

また、次のコマンドを使用して、使用中の動的に生成された共有秘密をすべて表示することもできます。

```
Router# show cable modem verbose | include Dynamic Secret

Dynamic Secret                      : 43433036434644344643303841313237
Dynamic Secret                      : 308203E0308202C8A003020102021058
Dynamic Secret                      : 0D06092A864886F70D01010505003081
Dynamic Secret                      : 3037060355040A133044617461204F76
Dynamic Secret                      : 20496E7465726661636520537065636369
Dynamic Secret                      : 00000000000000000000000000000000
Dynamic Secret                      : 040B130C4361626C65204D6F64656D73
Dynamic Secret                      : 53204361626C65204D6F64656D20526F
Dynamic Secret                      : 7574686F72697479301E170D30313032
Dynamic Secret                      : 313233353935395A308197310B300906
Dynamic Secret                      : 0A133044617461204F76657220436162
Dynamic Secret                      : 666163652053706563696696396361746 9
Dynamic Secret                      : 626C65204D6F64656D73313630340603
Dynamic Secret                      : 65204D6F64656D20526F6F7420436572
Dynamic Secret                      : 747930820122300D06092A864886F70D
Dynamic Secret                      : 010100C0EF369D7BDAB0A938E6ED29C3
Dynamic Secret                      : DA398BF619A11B3C0F64912D133CFFB6
Dynamic Secret                      : FFAD6CE01590ABF5A1A0F50AC05221F2
Dynamic Secret                      : 73504BCA8278D41CAD50D9849B56552D
Dynamic Secret                      : 05F4655F2981E031EB76C90F9B3100D1
Dynamic Secret                      : F4CB0BF4A13EA9512FDE4A2A219C27E9
Dynamic Secret                      : D47BCBB5494E9936D51CB0EB66EF0B0A
Dynamic Secret                      : 8EB196423170B26684BF6730C099D271
Dynamic Secret                      : DF8FE30203010001A326302430120603
Dynamic Secret                      : 300E0603551D0F0101FF040403020106
Dynamic Secret                      : 820101002D1A264CE212A1BB6C1728B3
Dynamic Secret                      : 7935B694DCA90BC624AC92A519C214B9
Dynamic Secret                      : 3AB096D00D56ECD07D9B7AB662451CFF
Dynamic Secret                      : 92E68CFD8783D58557E3994F23A8140F
Dynamic Secret                      : 225A3B01DB67AF0C3637A765E1E7C329
Dynamic Secret                      : 2BB1E6221B6D5596F3D6F506804C995E
Dynamic Secret                      : 45494DC933F8F47A398F69EE6361B017
Router#
```

動的共有秘密を持つケーブル モデムのトラブルシューティング

ケーブル モデムが動的共有秘密に違反しているとマーキングされた場合は、次のデバッグを有効にすると、発生中のイベントのシーケンスに関する詳細な情報を取得できます。

- **debug cable mac-address** *cm-mac-addr* **verbose**：特定の MAC アドレスを持つケーブル モデムの詳細なデバッグを有効にします。
- **debug cable tlv**：登録プロセス中に送信されるタイプ/長さ/値メッセージの内容が表示されます。
- **debug cable dynamic-secret**：動的共有秘密の動作に関するデバッグ メッセージを表示します。
- **debug tftp server events**：Cisco CMTS ルータのオンボード TFTP サーバで発生する主要なイベントのデバッグ メッセージを表示します。
- **debug tftp server packets**：TFTP サーバがケーブル モデムにダウンロードする DOCSIS コンフィギュレーション ファイルのパケット ダンプを表示します。

ヒント　これらのデバッグ コマンドの詳細は、下記の URL にある『Cisco Broadband Cable Command Reference Guide』の「*Cisco CMTS Debugging Commands*」の章を参照してください。http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

また、ルータのログ バッファ内のメッセージを確認すると有用な情報が得られます。これらのメッセージを表示するためにルータのロギング バッファの内容を表示するには、**show logging** コマンドを使用します。**begin** 出力修飾子を使用すると、特定の時間/分に出力を制限できます。たとえば、12:10 に記録されたメッセージだけを表示するには、次のコマンドを入力します。

```
Router# show logging | begin 12:10
```

（注）　**begin** 出力修飾子の適切な形式は、ロギング バッファで使用しているタイムスタンプによって異なります。

動的共有秘密の設定例

ここでは、動的共有秘密機能の一般的な設定を示します。

（注）　これらの設定では、ケーブル インターフェイスで設定する共有秘密と二次的秘密も示します。この設定はオプションですが、ケーブル モデムの登録時のセキュリティを一層向上させるので、強く推奨します。

マーク設定：例

次に示すCisco CMTSルータのケーブルインターフェイス設定からの抜粋では、CMTS MICチェックに失敗したケーブル モデムにもオンラインになることを許可するものの、**showcablemodem** の表示で感嘆符（!）マークが付くようにケーブルインターフェイスが設定されており、後でこの状態を調査できます。

```
interface cable c5/1/0
 cable dynamic-secret mark
 ...
```

ロックの設定例

Cisco CMTS ルータのケーブル インターフェイスの設定からの抜粋では、CMTS MIC の確認に失敗したケーブル モデムがオンラインになることはできますが、アップストリームとダウンストリームのサービス フローを最大 10 kbps に制限する限定的な QoS 設定にロックできるようにケーブル インターフェイスを設定しています。ロックされたケーブル モデムは、24 時間を超えてオフラインになるか、**clearcablemodemlock** コマンドを使用して手動でモデムをクリアするまで、限定的な QoS 設定にロックされたままになります。

```
cable qos permission create
cable qos permission update
...
interface cable c3/0
 cable dynamic-secret lock
 ...
```

（注） 特定のQoSプロファイルを指定せずに **lock** オプションを使用する場合、**cableqospermission** コマンドを使用して、ケーブル モデムで QoS プロファイルを作成および更新できるようにする必要があります。これを実行せず、特定の QoS プロファイルを指定しないまま **lock** オプションを使用し続けると、ロックされたケーブル モデムは、ロックがクリアされるか期限が切れるまで登録できなくなります。

次の同様の抜粋例では、ロックされたケーブル モデムに QoS プロファイル 90 を割り当てる必要があることを示しています。ケーブル モデムは、24 時間を超えてオフラインになるか、**clearcablemodemlock** コマンドを使って手動でモデムをクリアするまで、この QoS プロファイルにロックされたままになります。特定の QoS プロファイルが指定されているため、**cableqospermission** コマンドを使用する必要はありません。

```
interface cable c3/0
 cable dynamic-secret lock 90
 ...
```

（注） ロックされたモデムをクリアすると、CMTSに再登録するように自動的にリセットされます。動的共有秘密の確認に合格した有効なDOCSIS設定に登録すると、必要なQoSパラメータが設定された状態でオンラインになります。ただし、モデムがDOCSIS仕様に再び違反すると、再度ロックされます。

拒否の設定例

次の抜粋は、Cisco CMTSでのケーブル インターフェイスの設定例で、CMTS MICチェックに失敗したケーブル モデムを拒否し、登録を許可しないようケーブル インターフェイスを設定します。ケーブル モデムは、共有秘密または二次的な共有秘密のいずれかの値に一致するCMTS MICを含むDOCSISコンフィギュレーション ファイルを使用して登録する必要があります。CMがオンラインになると、CMTSはコンソールに警告メッセージを出力し、**show cable modem**コマンドでこのケーブル モデムに感嘆符（!）マークが付くので、この状況を調査できます。

```
interface cable c3/0
 cable dynamic-secret reject
 ...
```

無効の設定例

次の抜粋は、Cisco uBR7100シリーズ ルータのケーブル インターフェイスの設定例で、動的共有秘密機能を無効にしています。この設定では、各DOCSISコンフィギュレーション ファイルのCMTS MIC値を確認する場合、CMTSは、未変更の共有秘密と二次的な共有秘密の値を使用します。

```
interface cable c1/0
 no cable dynamic-secret
 ...
```

その他の参考資料

動的共有秘密に関連する詳細情報については、次の参考資料を参照してください。

標準

標準[9]	タイトル
SP-RFIv1.1-I09-020830	『Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1』

9 サポートされている標準がすべて記載されているわけではありません。

MIB

MIB [10]	MIB のリンク
動的共有秘密機能によってサポートされる新しい MIB オブジェクトまたは変更された MIB オブジェクトはありません。 • CISCO-DOCS-EXT-MIB には、動的共有秘密機能を設定し、ケーブル モデムが共有秘密セキュリティ チェックに失敗した場合にトラップを生成する属性が含まれます。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

10 サポートされている MIB がすべて記載されているわけではありません。

RFC

RFC[11]	タイトル
RFC 2233	『DOCSIS OSSI Objects Support』
RFC 2665	『DOCSIS Ethernet MIB Objects Support』
RFC 2669	『Cable Device MIB』

11 サポートされている RFC がすべて記載されているわけではありません。

動的共有秘密に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *208*：ダウンストリーム インターフェイスの設定に関する機能情報

機能名	リリース	機能情報
動的共有秘密	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 83 章

合法的傍受アーキテクチャ

合法的傍受（LI）機能を利用すると、サービス プロバイダーは、エッジ ルータを通過する Voice-over-Internet（VoIP）トラフィックまたはデータ トラフィックを傍受できる機能を提供するという、司法当局による要求を満たすことができます。このマニュアルでは、Cisco Service Independent Intercept アーキテクチャと PacketCable Lawful Intercept アーキテクチャを含む、LI アーキテクチャについて説明します。また、LI 機能の構成要素と、システムで LI 機能を設定するための手順についても説明します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *209* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

合法的傍受の前提条件

Cisco LI MIB ビューへのアクセスは、メディエーション デバイスと、ルータ上の合法的傍受について知っておく必要があるシステム管理者に制限されます。MIB にアクセスするには、ルータ上でレベル 15 のアクセス権がユーザに必要です。

メディエーション デバイスとの通信

ルータがメディエーション デバイスと通信して合法的傍受を実行するには、次の構成要件が満たされている必要があります。

- ルータとメディエーションデバイスの両方のドメイン名が、ドメイン ネーム システム（DNS）に登録されている必要があります。

DNS では、ルータの IP アドレスは通常、（スーパーバイザがインストールされているスロットに応じて）ルータの TenGigabitEthernet5/1/0 または TenGigabitEthernet4/1/0 インターフェイスのアドレスです。

- メディエーション デバイスに Access Function（AF）および Access Function Provisioning Interface（AFPI）が必要です。
- メディエーション デバイスを、CISCO-TAP2-MIB ビューにアクセスできるシンプル ネットワーク管理プロトコル（SNMP）ユーザ グループに追加する必要があります。グループに追加するユーザとして、メディエーション デバイスのユーザ名を指定します。

メディエーション デバイスを CISCO-TAP2-MIB ユーザとして追加するときに、必要に応じてメディエーション デバイスの認可パスワードを指定できます。パスワードの長さは、最低 8 文字である必要があります。

合法的傍受の制約事項

一般的な制約事項

ルータで LI を設定するためのコマンドライン インターフェイス（CLI）はありません。すべてのエラー メッセージは、メディエーション デバイスに SNMP 通知として送信されます。すべての傍受は、SNMPv3 だけを使用してプロビジョニングされます。

合法的傍受では SUP HA がサポートされません。SUP スイッチオーバーの後に LI 設定を再適用する必要があります。このイベント用に SNMP トラップが生成されます。

合法的傍受 MIB

合法的傍受について知る必要があるメディエーション デバイスとユーザだけに LI MIB へのアクセスが許可されます。

Cisco LI MIB は、その機密性から、LI 機能をサポートしているソフトウェア イメージだけで使用できます。これらの MIB には、Network Management Software MIBs Support ページ（http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml）からはアクセスできません。

SNMP 通知

LI の SNMP 通知は、メディエーションデバイス上のユーザ データグラム プロトコル（UDP）ポート 161 に送信する必要があります。ポート 162（SNMP のデフォルト）ではありません。詳細については、合法的傍受のための SNMP 通知のイネーブル化, （1424 ページ）を参照してください。

合法的傍受に関する情報

合法的傍受の概要

LI は、司法当局（LEA）が、司法命令または行政命令の許可に従って、電子的監視を行うためのプロセスです。ますます多くの法律が採択され、規制が施行されるのに伴い、サービス プロバイダー（SP）やインターネット サービス プロバイダー（ISP）は、許可された電子監視を明示的にサポートするネットワークを実装する必要性に迫られています。LI の指令に従う必要がある SP または ISP の種類は、国によって大きく異なります。米国での LI への準拠は、Commission on Accreditation for Law Enforcement Agencies（CALEA）で規定されています。

シスコでは、LI に対し、PacketCable と Service Independent Intercept の 2 つのアーキテクチャをサポートしています。LI コンポーネントだけでは、該当する規制に準拠できません。LI コンポーネントは、SP および ISP が、LI 準拠のネットワークを構築するために使用可能なツールを提供します。

Cisco Service Independent Intercept アーキテクチャ

『Cisco Service Independent Intercept Architecture Version 3.0』では、Cisco BTS 10200 Softswitch コール エージェント バージョン 5.0 を非 PacketCable ネットワークで使用した、VoIP ネットワーク向けの LI の実装について説明しています。Packet Cable Event Message 仕様バージョン 1.5-I01 は、コール識別情報と、コールの内容に対する Cisco Tap MIB バージョン 2.0 を提供するために使用されます。

『Cisco Service Independent Intercept Architecture Version 2.0』では、Cisco BTS 10200 Softswitch コール エージェント バージョン 4.4 および 4.5 を非 PacketCable ネットワークで使用した、VoIP ネットワーク向けの LI の実装について説明しています。PacketCable ネットワークではありませんが、PacketCable Event Messages Specification バージョン I08 は、コール識別情報と、コール内容に対する Cisco Tap MIB のバージョン 1.0 またはバージョン 2.0 を提供するために引き続き使用されています。『*Cisco Service Independent Intercept Architecture Version 2.0*』では、IP アドレスとセッション ID の両方でデータを傍受するための追加機能について説明しています。これは、どちらも Cisco Tap MIB（CISCO-TAP2-MIB）のバージョン 2.0 でサポートされています。

『Cisco Service Independent Intercept Architecture Version 1.0』では、Cisco BTS 10200 Softswitch コール エージェント バージョン 3.5 および 4.1 を非 PacketCable ネットワークで使用した、VoIP ネットワーク向けの LI の実装について説明しています。PacketCable ネットワークではありませんが、PacketCable Event Message Specification バージョン I03 は、コール識別情報と、コール内容に対する Cisco Tap MIB（CISCO-TAP-MIB）のバージョン 1.0 を提供するために引き続き使用されています。IP アドレスによる単純なデータの傍受についても説明されています。

PacketCable 合法的傍受アーキテクチャ

『*PacketCable Lawful Intercept Architecture for BTS Version 5.0*』では、Cisco BTS 10200 Softswitch コール エージェント バージョン 5.0 を、PacketCable Event Messages Specification バージョン 1.5-I01

に準拠した PacketCable ネットワークで使用した、VoIP 向けの LI の実装について説明しています。

『*PacketCable Lawful Intercept Architecture for BTS Versions 4.4 and 4.5*』では、Cisco BTS 10200 Softswitch コール エージェント バージョン 4.4 および 4.5 を、PacketCable Event Messages Specification バージョン I08 に準拠した PacketCable ネットワークで使用した、VoIP 向けの LI の実装について説明しています。

『PacketCable Lawful Intercept Architecture for BTS Versions 3.5 and 4.1』では、Cisco Broadband Telephony Softswitch (BTS) 10200 Softswitch コール エージェント バージョン 3.5 および 4.1 を、PacketCable Event Message Specification バージョン I03 に準拠した PacketCable ネットワークで使用した、Voice over IP（VoIP）向けの LI の実装について説明しています。

『*PacketCable Control Point Discovery Interface Specification* 』では、指定された IP アドレスのコントロールポイントを発見するために使用可能な IP ベースのプロトコルが定義されています。コントロール ポイントとは、Quality of Service（QoS）操作、LI コンテンツ タッピング操作、その他の操作を実行可能な場所です。

（注） Cisco cBR ルータは、PacketCable に関する Communications Assistance for Law Enforcement Act（CALEA）をサポートしません。

Cisco cBR シリーズ ルータ

Cisco cBR シリーズ ルータは、通常および広帯域（加入者ごと）の 2 種類の LI をサポートしています。通常の盗聴は、アクセス サブインターフェイスおよび物理インターフェイス上で実行します。内部インターフェイス上では盗聴は不要であり、実行されません。ルータは、ターゲット トラフィックが使用しているインターフェイスに基づいて、実行する盗聴の種類を決定します。

Cisco cBR シリーズ ルータ上の LI は、次の 1 つ以上のフィールドの組み合わせに基づいてトラフィックを傍受できます。

- 宛先 IP アドレスとマスク（IPv4 または IPv6 アドレス）
- 宛先ポートまたは宛先ポートの範囲
- 送信元 IP アドレスとマスク（IPv4 または IPv6 アドレス）
- 送信元ポートまたは送信元ポート範囲
- プロトコル ID
- Type of Service（TOS）
- ルータ内で *vrf-tableid* 値に変換される Virtual Routing and Forwarding（VRF）名
- 加入者（ユーザ）接続 ID
- ケーブル モデム
- MAC アドレス

Cisco cBR シリーズ ルータ上の LI の実装は、SNMP3 を使用してプロビジョニングされ、次の機能がサポートされています。

- 通信内容の傍受。ルータは、傍受した各パケットを複製し、パケットのコピーを UDP ヘッダーでカプセル化されたパケットに（設定されたCCCidとともに）格納します。ルータは、カプセル化したパケットを LI メディエーション デバイスに送信します。複数の合法的傍受が同じデータ フローに対して設定されている場合でも、パケットの 1 つのコピーだけメディエーション デバイスに送信されます。必要に応じて、メディエーション デバイスは各 LEA に対しパケットを複製できます。
- IPv4、IPv4 マルチキャスト、IPv6、および IPv6 マルチキャストフローの傍受。
- 最大傍受時間： **cTap2MediationTimeout** の最大値は現在時刻から 260640 分（181 日）です。**cTap2MediationTimeout** の最小値は現在時刻から 1 分です。

LI には、MAC ベースのタップを設定する 2 つの方法があります。

- CPE で：送信元または宛先が CPE デバイスの MAC アドレスと一致するトラフィックのみを傍受します。
- CM で：CMの背後にあるすべてのトラフィック（CMのトラフィック自体を含む）を傍受します。この形式の傍受は、メディエーションデバイスへのトラフィックを多く生成する可能性があります。

VRF 対応 LI

VRF 対応 LI は、特定のバーチャル プライベート ネットワーク（VPN）での IPv4 データの LI 盗聴をプロビジョニングする機能です。この機能により、LEA は、その VPN 内のターゲット データを合法的に傍受できます。VRF ベースの LI タップを受けるのは、その VPN 内の IPv4 データのみです。

VRF 対応の LI は、次の種類のトラフィックに対して使用できます。

- ip2ip
- ip2tag（IP から MPLS）
- tag2ip（MPLS から IP）

VPN ベースの IPv4 タップをプロビジョニングするために、LI 管理機能（メディエーション デバイスで動作します）は、CISCO-IP-TAP-MIB を使用して、ターゲットの VPN が使用している VRF テーブルの名前を特定します。VRF 名は、タップを実行するために LI をイネーブルにする VPN インターフェイスを選択するのに使用します。

ルータは、傍受するトラフィックと、傍受したパケットを送信するメディエーション デバイスを、VRF 名（および送信元および宛先アドレス、送信元および宛先ポート、およびプロトコル）に基づいて決定します。

（注） Cisco-IP-TAP-MIB を使用する場合、VRF 名がストリーム エントリで指定されていない場合、デフォルトでグローバル IP ルーティング テーブルが使用されます。

合法的傍受（冗長仲介デバイス）

Cisco cBR シリーズ コンバージド ブロードバンド ルータでは、合法的傍受（LI）パケットを複数の仲介デバイス（MD）にレプリケートできます。この機能を使用するには、複数の同一タップを設定します。Cisco cBR シリーズ コンバージド ブロードバンド ルータでは、最大 2 つの同一タップで 2 つの MD へのレプリケーションをサポートします。複数 MD でサポートされるのは、MAC タップと CM タップのみです。

2 つの MD に対する 2 つの同一タップを設定する SNMP コンフィギュレーション コマンド セットの例については、例：合法的傍受の設定（冗長仲介デバイス），（1428 ページ）を参照してください。

合法的傍受 MIB

Cisco LI MIB は、その機密性から、LI 機能をサポートしているソフトウェア イメージだけで使用できます。これらの MIB には、Network Management Software MIBs Support ページ（http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml）からはアクセスできません。

合法的傍受 MIB へのアクセスの制限

合法的傍受について知る必要があるメディエーション デバイスとユーザだけに LI MIB へのアクセスを許可する必要があります。これらの MIB へのアクセスを制限するには、次の作業を実行する必要があります。

1. Cisco LI MIB を含むビューを作成します。
2. このビューへの読み取りおよび書き込みアクセス権を持つ SNMP ユーザ グループを作成します。このユーザ グループに割り当てられたユーザだけが、MIB の情報にアクセスできます。
3. ユーザをシスコ LI ユーザ グループに追加し、合法的傍受に関連する MIB および情報にアクセスできるユーザを定義します。このグループのユーザとして、メディエーションデバイスを追加してください。追加しないと、ルータで合法的傍受を実行できません。

詳細は、「合法的傍受 MIB の制限付き SNMP ビューの作成」を参照してください。

（注） Cisco LI MIB ビューへのアクセスは、メディエーション デバイスと、ルータ上の合法的傍受について知っておく必要があるシステム管理者に制限されます。MIB にアクセスするには、ルータ上でレベル 15 のアクセス権がユーザに必要です。

Service Independent Intercept

シスコでは、サービス プロバイダー カスタマーの合法的傍受のサポート要件に対応するため、Service Independent Intercept（SII）アーキテクチャを開発しました。SII アーキテクチャは、コンテンツの傍受アクセス ポイント（IAP）として機能するシスコ機器とメディエーション デバイス間に、明確に定義されたオープン インターフェイスを提供します。SII アーキテクチャのモジュラ特性により、サービス プロバイダーは、特定のネットワーク要件と警察当局の収集機能へのインターフェイスに対する地域的な標準ベースの要件とを満たす最適なメディエーション デバイスを選択できます。

メディエーション デバイスは SNMPv3 を使用してコール接続（CC）IAP を指示し、CC を複製してメディエーション デバイスにコンテンツを送信します。CC IAP は、エッジ ルータまたは音声のトランキング ゲートウェイのいずれか、およびエッジ ルータまたはデータのアクセス サーバのいずれかにできます。

（注） Cisco cBR ルータは、合法的傍受トラフィックの暗号化をサポートしません。

セキュリティを強化し、SNMPv3 脆弱性を緩和するには、次のタスクが必要です。

信頼できるホストへのアクセス制限（暗号化なし）

SNMPv3 は、セキュリティ モデルとセキュリティ レベルの両方をサポートします。セキュリティ モデルは、ユーザおよびユーザに属するグループに合わせて設定される認証方式です。セキュリティ レベルとは、セキュリティ モデル内で許可されるセキュリティのレベルです。セキュリティ モデルとセキュリティ レベルの組み合わせによって、SNMP パケットを処理するときに適用されるセキュリティ メカニズムが決定されます。

さらに、名前付きアクセス リストの SNMP サポート機能により、いくつかの SNMP コマンドに、標準の名前付きアクセス コントロール リスト（ACL）へのサポートが追加されます。

新しい SNMP グループ、または SNMP ユーザを SNMP ビューにマップするテーブルを設定するには、グローバル コンフィギュレーション モードで **snmp-servergroup** コマンドを使用します。

```
access-list my-list permit ip host 10.10.10.1
snmp-server group my-group v3 auth access my-list
```

この例では、**my-list** という名前のアクセス リストは 10.10.10.1 以降の SNMP トラフィックのみ許可します。次にこのアクセス リストは、**my-group** という名前の SNMP グループに適用されます。

合法的傍受の設定方法

ルータで合法的傍受をプロビジョニングするための直接のユーザ コマンドはありませんが、LI MIB へのアクセスの有効化、SNMP 通知の設定など、いくつかの設定タスクを実行する必要があります。ここでは、必要なタスクの実行方法について説明します。

合法的傍受 MIB の制限付き SNMP ビューの作成

ユーザを作成して、シスコの合法的傍受 MIB を含む SNMP ビューに割り当てるには、ここに示す手順を実行します。

はじめる前に

- コマンドは、レベル 15 のアクセス権で、グローバル コンフィギュレーション モードで実行する必要があります。
- デバイスで SNMPv3 が設定されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**snmp-serverview** *view-name MIB-name* **included** 例： `Device(config)# snmp-server view exampleView ciscoTap2MIB included`	CISCO-TAP2-MIB を含む SNMP ビューを作成します（ここで、*exampleView* は、MIB に対して作成するビューの名前です）。 • この MIB は、通常とブロードバンドの両方の合法的傍受に必要です。
ステップ 4	**snmp-serverview** *view-name MIB-name* **included** 例： `Device(config)# snmp-server view exampleView ciscoIpTapMIB included`	CISCO-IP-TAP-MIB を SNMP ビューに追加します。

	コマンドまたはアクション	目的
ステップ 5	**snmp-serverview** *view-name MIB-name* **included** 例： `Device(config)# snmp-server view exampleView cisco802TapMIB included`	CISCO-802-TAP-MIB を SNMP ビューに追加します。
ステップ 6	**snmp-servergroup** *group-name* **v3 noauthread** *view-name* **write** *view-name* 例： `Device(config)# snmp-server group exampleGroup v3 noauth read exampleView write exampleView`	LI MIB ビューにアクセス可能な SNMP ユーザ グループを作成し、グループのビューに対するアクセス権を定義します。
ステップ 7	**snmp-server user** *user-name group-name* **v3authmd5** *auth-password* 例： `Device(config)# snmp-server user exampleUser exampleGroup v3 auth md5 examplePassword`	指定したユーザ グループにユーザを追加します。
ステップ 8	**end** 例： `Device(config)# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

次の作業

これで仲介デバイスは合法的傍受 MIB にアクセスし、SNMP の **set** および **get** 要求を発行して、ルータ上で合法的傍受を設定および実行できるようになります。ルータがメディエーション デバイスに SNMP 通知を送信するよう設定する方法については、「合法的傍受のための SNMP 通知のイネーブル化」を参照してください。

合法的傍受のための SNMP 通知のイネーブル化

SNMP は、合法的傍受イベントについての通知を自動的に生成します。合法的傍受通知をメディエーション デバイスに送信するようにルータを設定するには、ここに示す手順を実行します。

はじめる前に

- コマンドは、レベル 15 のアクセス権で、グローバル コンフィギュレーション モードで実行する必要があります。
- ルータで SNMPv3 が設定されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**snmp-serverhost** *ip-address* **community-stringudp-port** *port notification-type* 例： `Device(config)# snmp-server 10.2.2.1 community-string udp-port 161 udp`	メディエーション デバイスの IP アドレスと、通知要求とともに送信されるパスワードに似たコミュニティ ストリングを指定します。 • 合法的傍受では、**udp-port** は 162（SNMP のデフォルト）で

	コマンドまたはアクション	目的
		はなく 161 とする必要があります。
ステップ 4	**snmp-serverenabletrapssnmpauthenticationlinkuplinkdowncoldstartwarmstart** 例： `Device(config)# snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart`	RFC 1157 通知をメディエーション デバイスに送信するようにルータを設定します。 • これらの通知は、認証の失敗、リンク ステータス（アップまたはダウン）、およびルータ再起動を示します。
ステップ 5	**end** 例： `Device(config)# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SNMP 通知のディセーブル

ルータ上で SNMP 通知をディセーブルにするには、ここに示す手順を実行します。

（注） 合法的傍受通知をディセーブルにするには、SNMPv3 を使用して CISCO-TAP2-MIB オブジェクト cTap2MediationNotificationEnable を false(2) に設定します。SNMPv3 を通じて合法的傍受の通知を再度イネーブルにするには、オブジェクトに true（1）を再設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**nosnmp-serverenabletraps** 例： `Device(config)# no snmp-server enable traps`	システムで使用可能なすべての SNMP 通知タイプをディセーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	現在のコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SNMPv3 によるケーブル モデムの MAC インターセプトのプロビジョニング

1. c802tapStreamInterface オブジェクトを設定します。
2. c802tapStreamFields オブジェクトに次のビット フラグを設定します。
   - dstMacAddress（ビット 1）
   - srcMacAddress（ビット 2）
   - cmMacAddress（ビット 6）：cmMacAddress ビット フィールドはケーブル モデム サポートのために新しく導入されました。インターセプトが CPE ベース インターセプトまたは CM ベース インターセプトかを決定します。
3. 同じ CM MAC アドレス値により次のオブジェクトを設定します。

- c802tapStreamDestinationAddress
- c802tapStreamSourceAddress

SNMPv3 による CPE デバイスの MAC インターセプトのプロビジョニング

1. c802tapStreamInterface オブジェクトを設定します。
2. c802tapStreamFields オブジェクトに次のビット フラグを設定します。
   - dstMacAddress（ビット 1）
   - srcMacAddress（ビット 2）
3. 同じ CPE MAC アドレス値により次のオブジェクトを設定します。
   - c802tapStreamDestinationAddress
   - c802tapStreamSourceAddress

合法的傍受の設定例

例：メディエーション デバイス アクセスの合法的傍受 MIB の有効化

次に、メディエーションデバイスが合法的傍受MIBにアクセスできるようにする例を示します。この例では、4 つの LI MIB（CISCO-TAP2-MIB、CISCO-IP-TAP-MIB、CISCO-802-TAP-MIB、CISCO-USER-CONNECTION-TAP-MIB）を含む SNMP ビュー（tapV）を作成します。また、tapV ビュー内の MIB に読み込み、書き込み、通知アクセス可能なユーザ グループも作成します。

```
snmp-server view tapV ciscoTap2MIB included
snmp-server view tapV ciscoIpTapMIB included
snmp-server view tapV cisco802TapMIB included
snmp-server view tapV ciscoUserConnectionTapMIB included
snmp-server group tapGrp v3 noauth read tapV write tapV notify tapV
snmp-server user MDuser tapGrp v3 auth md5 MDpasswd
snmp-server engineID local 1234
```

例：合法的傍受の設定（冗長仲介デバイス）

合法的傍受を設定するには、SNMPv3 を使用します。次の例は、2 つの MD を傍受する 2 つの同一タップを設定するための SNMP コンフィギュレーション コマンド セットを示しています。

- MD1 を設定します。

```
setany -v3 -timeout 30 -retries 3 10.12.0.34 user1 \
cTap2MediationStatus.1 -i 4 \
cTap2MediationDestAddressType.1 -i 1 \
cTap2MediationTimeout.1 -o 07:E0:04:01:B:15:1A:0 \
cTap2MediationTransport.1 -i 1 \
cTap2MediationSrcInterface.1 -i 0 \
```

```
cTap2MediationDestAddress.1 -o 0a:0a:00:35 \
cTap2MediationDestPort.1 -g 63
```

- CM タップを設定します。

```
setany -v3 -timeout 30 -retries 3 10.12.0.34 user1 \
c802tapStreamStatus.1.2 -i 4 \
c802tapStreamFields.1.2 -o 62 \
c802tapStreamInterface.1.2 -i -1 \
c802tapStreamDestinationAddress.1.2 -o "c8 fb 26 a5 55 98" \
c802tapStreamSourceAddress.1.2 -o "c8 fb 26 a5 55 98"

setany -v3 -timeout 30 -retries 3 10.12.0.34 user1 \
cTap2StreamStatus.1.2 -i 5 \
cTap2StreamType.1.2 -i 2 \
cTap2StreamInterceptEnable.1.2 -i 1 \
cTap2StreamStatus.1.2 -i 4
```

- MD2 を設定します。

```
setany -v3 -timeout 30 -retries 3 10.12.0.34 user1 \
cTap2MediationStatus.2 -i 4 \
cTap2MediationDestAddressType.2 -i 1 \
cTap2MediationTimeout.2 -o 07:E0:03:03:7:15:1A:0 \
cTap2MediationTransport.2 -i 1 \
cTap2MediationSrcInterface.2 -i 0 \
cTap2MediationDestAddress.2 -o 0a:0a:00:06 \
cTap2MediationDestPort.2 -g 63
```

- CM タップを設定します。

```
setany -v3 -timeout 30 -retries 3 10.12.0.34 user1 \
c802tapStreamStatus.2.2 -i 4 \
c802tapStreamFields.2.2 -o 62 \
c802tapStreamInterface.2.2 -i -1 \
c802tapStreamDestinationAddress.2.2 -o "c8 fb 26 a5 55 98" \
c802tapStreamSourceAddress.2.2 -o "c8 fb 26 a5 55 98"

setany -v3 -timeout 30 -retries 3 10.12.0.34 user1 \
cTap2StreamStatus.2.2 -i 5 \
cTap2StreamType.2.2 -i 2 \
cTap2StreamInterceptEnable.2.2 -i 1 \
cTap2StreamStatus.2.2 -i 4
```

- 傍受されたパケット数を取得します。

```
getmany -v3 -timeout 30 -retries 3 10.12.0.34 user1 \
cTap2StreamInterceptedPackets
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
SNMP サポートの設定	『*Configuring SNMP Support*』
セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

標準および RFC

標準/RFC	タイトル
PacketCable™ コントロール ポイント検出インターフェイス仕様	『*PacketCable™ Control Point Discovery Interface Specification*』（PKT-SP-CPD-I02-061013）
RFC-3924	『*Cisco Architecture for Lawful Intercept in IP Networks*』

MIB

MIB	MIB のリンク
• CISCO-TAP2-MIB • CISCO-IP-TAP-MIB • CISCO-802-TAP-MIB • CISCO-USER-CONNECTION-TAP-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

合法的傍受に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *210*：合法的傍受に関する機能情報

機能名	リリース	機能情報
合法的傍受（冗長仲介デバイス）	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 84 章

Cisco cBR シリーズ ルータのケーブル モニタリング機能

ケーブルモニタリングを設定すると、ケーブルインターフェイス上の選択したパケットのコピーが、Cisco CMTS ルータ上の別のインターフェイスに接続された外部 LAN アナライザに転送されます。このコマンドは、ネットワークとアプリケーションで発生した問題のトラブルシューティングに役立ちます。

（注） この機能は、サービス妨害攻撃や他のタイプのネットワーク攻撃を防ぐ目的でトラフィックをモニタリングするのではありません。ケーブル モニタリング機能を設定しても、トラフィックが送信される宛先は変わらず、選択したパケットのコピーだけがCALEA サーバまたはLAN アナライザに転送されます。

（注） この機能は、ライン カード高可用性（LCHA）をサポートしていません。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

cBR のケーブル モニタ コマンドの概要

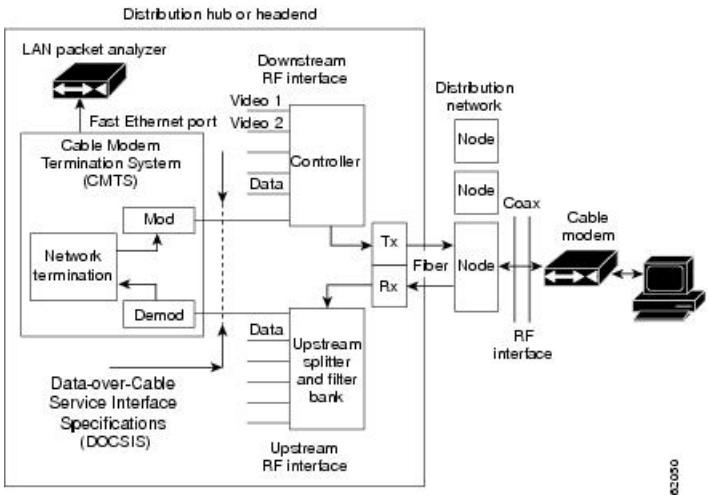
cable monitor コマンドは、特定のケーブル インターフェイス経由で送られる特定の種類のトラフィックのパケットのコピーをLANアナライザに送信します。これにより、ネットワークの問題のトラブルシューティングでそれを使用できます。このコマンドでは、次の 1 つ以上のパラメータを使用して、転送するパケットを選択できます。

- 着信パケットまたは発信パケットのいずれか
- 特定の MAC アドレス（送信元および宛先）に一致するパケット
- 特定のサービス ID（SID）が設定されたパケット

トラブルシューティングに役立つよう、パケットにタイムスタンプを追加することもできます。その後、指定した 10 ギガビット イーサネット ポートからパケットが LAN アナライザに転送され、さらに分析されます。

次の図に、DOCSIS 双方向構成のファスト イーサネット ポートに接続された LAN パケット アナライザを示します。

図 *34*：*DOCSIS* 双方向構成での *LAN* パケット アナライザ



（注） ケーブル モニタリングに使用する WAN ポートは、LAN パケット アナライザ専用にしてください。

cBR ルータのケーブル モニタリングの設定

特定のケーブルインターフェイスでケーブル トラフィック モニタリング機能を有効にするには、特権 EXEC モードから開始して、次の手順に従います。

手順

	コマンドまたはアクション	目的

ステップ 1	**enable**
	
	例：
	`Router> enable`
	
	例：
	`Router#`
		特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

ステップ 2	**configureterminal**
	
	例：
	`Router# configure terminal`
	
	例：
	`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 monitor**
	
	例：
	`Router(config)# cable monitor`
	
	例：
	`Router(config-cable-monitor)#`
		ケーブルモニタ コンフィギュレーション モードを開始します。

ステップ 4	**sniff card <slot num> <ds/us> <sniff point> <filter> dest cmon-tunnel <cmon-tunnel num>**
	
	例：
	ダウンストリーム トラフィック：各チャネル用
	`Router(config-cable-monitor)sniff card 3 outbound`
	`docsis integrated-Cable 3/0/0:0 dest cmon-tunnel 3`
	
	例：
		スニッフィングされたパケットを転送するようにカードを設定します。
		• **slot number**：ライン カードのスロット番号
		• **ds/us**：ダウンストリームまたはアップストリーム
		• **sniff point**：ダウンストリームまたはアップストリーム FPGA（フィールドプログラマブルゲー

	コマンドまたはアクション	目的

	ダウンストリーム トラフィック：各ワイドバンド チャネル用
	`Router(config-cable-monitor)sniff card 3 outbound`
	`pre-docsis wideband-Cable 3/0/0:0 dest cmon-tunnel 3`
	
	例：
	ダウンストリーム トラフィック：各 MAC アドレス用
	`Router(config-cable-monitor)sniff card 3 outbound`
	`docsis mac-address 0100.5e01.0101 dest cmon-tunnel 3`
	
	例：
	アップストリーム トラフィック：各チャネル用
	`Router(config-cable-monitor)# sniff card 3 incoming`
	`post-docsis upstream-cable 3/0/0 us-channel 0 dest cmon-tunnel 3`
	
	例：
	アップストリーム トラフィック：各 MAC アドレス用（ケーブル モデムまたは CPE）
	`Router(config-cable-monitor)#sniff card 3 incoming`
	`docsis mac-address e448.c70c.9c27 dest cmon-tunnel 3`
	
	例：
	アップストリーム トラフィック：MD/SID 用
	`Router(config-cable-monitor)#sniff card 3 incoming`
	`docsis cable 3/0/0 sid 12 upstream 0 dest cmon-tunnel 3`
		トアレイ）のスニッフィング ポイント
		• **filter**：パケット タイプ フィルタ
		• **dest cmon-tunnel**：キャプチャされたパケットのケーブル モニタ トンネル
		• **cmon-tunnel num**：キャプチャされたパケットのケーブル モニタ トンネル番号

ステップ 5	**end**
	
	例：
	`Router(config)# end`
	
	例：
	`Router#`
		グローバル コンフィギュレーション モードを終了します。

次の作業

スニッフィングされたパケットをキャプチャして、それを外部サーバまたはローカル ハードディスクに転送できます。詳細については、スニッフィングされたパケットのキャプチャ，（1437 ページ）を参照してください。

スニッフィングされたパケットのキャプチャ

キャプチャされたトラフィックを外部サーバに転送するには、トンネルを設定する必要があります。外部サーバは直接接続されない場合もあり、CMTS から離れていることもあります。

スニッフィングされたパケットをキャプチャするには、次のいずれかの手順に従います。

- 外部ホストを使用して出力パケットをキャプチャする
- ハードディスクを検出することによってパケットをキャプチャする

外部ホストでスニッフィングされたパケットのキャプチャ

キャプチャされたトラフィックを外部サーバに転送するには、トンネルを設定する必要があります。外部サーバは直接接続されない場合もあり、CMTS から離れていることもあります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configureterminal**
	
	例：
	`Router# configure terminal`
	
	例：
	`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 2	**interface cmon-tunnel number**
	
	例：
	`Router(config)# interface CMON-Tunnel 3`
	`Router(config-if)#`
		スニッフィングされたパケットをキャプチャするには、インターフェイス cmon-tunnel モードを開始します。

ステップ 3	**tunnel destination IP address**, **tunnel source IP address**
	
	例：
	`Router(config-if)#tunnel destination 10.10.21.11`
	`Router(config-if)#tunnel source 10.10.21.1`
		外部ホストが出力パケットをキャプチャするための宛先 IP アドレスと送信先 IP アドレスを設定します。

ステップ 4	**end**
	
	例：
	`Router(config)# end`
	
	例：
	`Router#`
		グローバル コンフィギュレーション モードを終了します。

次の作業

Wireshark プラグインを使用して、キャプチャされたパケットをデコードします。

ローカル ハード ドライブでのスニッフィングされたパケットのキャプチャ

キャプチャされたパケットをローカル ハード ドライブに転送するには、次の手順に従います。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`Router#configure CMON-Tunnel 3`
	
	例：
	`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 2	**interface cmon-tunnel number**
	
	例：
	`Router(config)#interface CMON-Tunnel 3`
	`Router(config-if)#`
		インターフェイス cmon-tunnel モードを開始します。

ステップ 3	**mode buffer** 例： `Router(config-if)#mode buffer`	ハード ディスクを指定することによってパケットをキャプチャするために cmon-tunnel 内のモード バッファを有効にします。

ステップ 4	**end**
	
	例：
	`Router(config-if)#end`
	`Router#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 5	**show platform software interface r0 name-string CMON-Tunnel number**
	
	例：
	`Router# show platform software interface r0 name-string CMON-Tunnel3`
	`Name: CMON-Tunnel3, ID: 14585, QFP ID: 0, Schedules: 0`
	`Monitor Type: 0, Instance ID: 0, Mode: 3`
	`Monitor Tunnel Source: 0.0.0.0, Destination: 0.0.0.0`
	`Router# test platform hardware qfp active feature docsis cmon-copy 3 14585`
	`Router# dir harddisk: | in CMON`
	`105 -rw- 11161490 Aug 27 2016 15:32:30 +08:00`	

	コマンドまたはアクション	目的
	CMON_7_20151207-153225.pcap 106 -rw- 10874548 Aug 27 2015 15:47:56 +08:00 CMON_7_20151207-154751.pcap	

次の作業

Wireshark プラグインを使用して、キャプチャされたパケットをデコードします。

ケーブル モニタリングに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *211*：ケーブル モニタリングに関する機能情報

機能名	リリース	機能情報
ケーブル モニタリング	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 85 章

送信元ベースのレート制限

送信元ベースのレート制限（SBRL）機能は、Cisco CMTS に向けられたサービス妨害（DoS）攻撃やハードウェア障害によって発生する可能性がある、フォワーディング プロセッサ（FP）上のパケットのルート プロセッサ（RP）インターフェイスへの輻輳を防止します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

• 送信元ベースのレート制限に関する機能情報，1460 ページ

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *212*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

送信元ベースのレート制限の前提条件

• WAN 側 SBRL のコントロール プレーン ポリシング（CoPP）を設定する必要があります。

送信元ベースのレート制限の制限事項

- WAN-IP および加入者の MAC アドレスのエンティティはハッシュを使用して識別され、2 つ（またはそれ以上の）エンティティ間でハッシュ衝突が発生する可能性があります。
- Cisco cBR ルータはハッシュ衝突に対し特別な処理を実行しません。ハッシュ衝突が発生する送信元は、それらが同じ送信元であるかのように、レート制限されています。
- QOS グループ 99 は SBRL 用に予約されており、他のクラス マップには使用できません。

送信元ベースのレート制限に関する情報

送信元ベースのレート制限（SBRL）機能は、CPP のパント パスで動作します。SBRL は、パント パスまたは RP でオーバーロードになる可能性のあるパケット ストリームを識別してレート制限を実施します。

パントされたパケットは、FP - RP キュー経由で FP から RP に送信されます。サービス妨害（DoS）は次の状況で発生する可能性があります。

- FP - RP キューが輻輳している
- RP がパントされたパケットを十分高速に処理できない

いずれの状況でも、有効なパントされたパケットが適切に処理されません。このような状況は、DoS 攻撃または外部ハードウェア障害によって意図的に発生する可能性があります。

SBRL で特定されたパケット ストリームは、設定されたパラメータに従ってレート制限されます。FP - RP キューにパケットが到達する前に、CPP でレート制限が発生します。これによって RP が保護され、他の有効なパントされたパケットが RP に到達できます。

デフォルトでは、SBRL は Cisco cBR ルータで無効です。SBRL には、WAN 側と加入者側で別々の設定があります。

WAN 側送信元ベースのレート制限

WAN 側 SBRL は、コントロール プレーン ポリシング（CoPP）を使用します。CoPP は、SBRL 宛の WAN 側パケット ストリームを指定します。信頼済みサイトと非信頼サイトの両方を CoPP を使用して指定できます。CoPP を使用すると、信頼済みサイトを無制限に指定できます。信頼済みサイトを指定するには、アクセス コントロール リスト（ACL）を使用します。

WAN 側 SBRL は、隔離機能もサポートします。パケット ストリームが隔離に入ると、パケット ストリームのすべてのパントが設定した期間にわたってドロップされます。

加入者側送信元ベースのレート制限

加入者側 SBRL 設定はグローバルであり、各ケーブル インターフェイスで設定する必要はありません。Cisco cBR ルータは、レイヤ 3 モビリティの原因単位の加入者側設定もサポートします。

（注） レイヤ 3 モビリティのデフォルトの加入者側原因単位レートは 4 パケット/秒です。加入者側原因単位レートは変更できますが、無効にできません。

送信元ベースのレート制限の設定方法

この項の構成は、次のとおりです。

WAN 側送信元ベースのレート制限の設定

次の 2 つの設定で、WAN 側 SBRL をイネーブルにする必要があります。

1. どのパケットを SBRL の対象にするかを指定するために、コントロール プレーン ポリシング（CoPP）を設定します。
2. 指定したパント要因に対するレート制限パラメータを設定するために、WAN 側 SBRL を設定します。

CoPP ポリシー マップでの特殊なアクション **set qos-group 99** は、特定のクラスに一致するパケットが WAN 側 SBRL の対象であることを表します。これは、QoS グループ 99 が SBRL 用にグローバルに確保されており、他のポリシー マップには使用できないことを意味します。

set qos-group 99 を含まないクラスにマッチするパケットは、WAN 側 SBRL をバイパスします。これは、CoPP は、WAN 側 SBRL の対象とならない信頼済みトラフィック ストリームを指定するためにも使用できることを意味します。

すべてのパントされたパケットは CoPP の対象となります。したがって、加入者側のトラフィックが信頼済みクラスに一致しないことを確認する必要があります。

WAN 側 SBRL は、パント要因、VRF インデックス、および送信元 IP アドレスをハッシュすることにより、トラフィック ストリームを特定します。この値は、レート制限のインデックスとして使用されます。ルータはハッシュ衝突に対して特別な処理を実行しないため、ハッシュ衝突をしているストリームは同じストリームからのものとして処理されます。

デフォルトでは、WAN 側 SBRL はディセーブルになっています。

制限事項

- パントされたすべてのパケットは、CoPP とパント ポリシングの対象です。

この項の構成は、次のとおりです。

コントロール プレーン ポリシングの設定

信頼済みクラスと一致するパントされたパケットは、WAN 側の SBRL を回避します。WAN 側の残りのパントは、WAN 側の SBRL に送信されます。

（注） 次に、信頼済みクラスの簡単な例を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**access-list** *access-list-number***permit** *protocol* {**any**	**host** {*address*	*name*}} {**any**	**host** {*address*	*name*}} **tos** *tos* 例： `Router(config)# access-list 130 permit ip 192.168.1.10 0.0.0.0 192.168.1.11 0.0.0.0 tos 4`	プロトコル タイプを基準にフレームをフィルタリングするためのアクセス リストを設定します。 （注） すべてのパントされたパケットは CoPP の対象となるため、加入者側のトラフィックが信頼済みクラスと同じでないことを確認する必要があります。
ステップ 4	**class-map** *class-map-name* 例： `Router(config)# class-map match-all sbrl_v4_trusted`	クラスマップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 5	**match access-group** *access-list-index* 例： `Router(config-cmap)# match access-group 130`	アイデンティティ ポリシーを適用するアクセス グループを指定します。その範囲は 1 ～ 2799 です。
ステップ 6	**exit** 例： `Router(config-cmap)# exit`	QoS クラス マップ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**policy-map** *policy-map-name* 例： `Router(config)# policy-map copp_policy`	サービス ポリシーを指定し、QoS ポリシーマップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 8	**class** *class-map-name* 例： `Router(config)# class sbrl_v4_trusted`	QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 9	**police rate** *units***pps conform-action** *action* **exceed-action** *action* 例： `Router(config-pmap-c)# police rate 1000 pps conform-action transmit exceed-action transmit`	コントロール プレーン宛てのトラフィックを指定のレートでポリシングします。 （注） 設定したアクションを両方とも**送信**する場合は、レートは関係ありません。
ステップ 10	**exit** 例： `Router(config-pmap-c)# exit`	ポリシー マップ クラス ポリシング コンフィギュレーション モードを終了します。
ステップ 11	**class class-default** 例： `Router(config-pmap)# class class-default`	ポリシー マップ内の他のどのクラスとも一致しないパケットに実行するアクションを指定します。
ステップ 12	**set qos-group 99** 例： `Router(config-pmap-c)# set qos-group 99`	このクラスに一致するパケットの WAN 側の SBRL を有効にします。
ステップ 13	**exit** 例： `Router(config-pmap-c)# exit`	ポリシーマップ クラス コンフィギュレーション モードを終了します。
ステップ 14	**exit** 例： `Router(config-pmap)# exit`	ポリシーマップ コンフィギュレーション モードを終了します。
ステップ 15	**control-plane** [**host** | **transit** | **cef-exception**] 例： `Router(config)# control-plane`	ルータのコントロール プレーンに属性（サービス ポリシーなど）を関連付けるか、関連付けられている属性を変更し、コントロール プレーン コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 16	**service-policy** {**input** |**output**出力ポリシー マップ名前 例： `Router(config-cp)#` **`service-policy input copp_policy`**	ポリシー マップをコントロール プレーンに関連付けます。
ステップ 17	**end** 例： `Router(config-cp)#` **`end`**	コントロール プレーン コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

WAN 側の送信元ベースのレート制限の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router>` **`enable`**	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router#` **`configure terminal`**	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	**platform punt-sbrl wan punt-cause** *punt-cause* **rate** *rate* 例： `Router(config)#` **`platform punt-sbrl wan punt-cause 10 rate 4`**	WAN 側のレート制限を設定します。 • **punt-cause** *punt-cause*：パント要因を指定します。範囲は 1 ～ 107 です。 • **rate** *rate*：1 秒間のパケット数でレートを指定します。範囲は 2 の累乗で指定される 1 ～ 256 です。

WAN 側の隔離の設定

WAN 側の隔離により、WAN 側の SBRL 設定が拡張されます。トラフィック ストリームが隔離に入ると、ストリーム内のパントされたすべてのパケットが設定した期間にわたってドロップされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**platform punt-sbrl wan punt-cause** *punt-cause* **rate** *rate* **quarantine-time** *time* **burst-factor** *burst-factor* 例： `Router(config)# platform punt-sbrl wan punt-cause 10 rate 4 quarantine-time 10 burst-factor 500`	WAN 側のパケット ストリームの隔離を設定します。 • **punt-cause** *punt-cause*：パント要因を指定します。範囲は 1 ～ 107 です。 • **rate** *rate*：レート制限を毎秒のパケット数単位で指定します。範囲は 2 の累乗で指定される 1 ～ 256 です。 • **quarantine-time** *time*：隔離時間（分単位）を指定します。指定できる範囲は 1 ～ 60 です。 • **burst-factor** *burst-factor*：バースト係数をパケット数単位で指定します。範囲は 50 ～ 1000 です。

パケット（*burst-factor* x *rate*）が *rate* よりも高速なレートで届く場合は、そのパケット ストリームは隔離されます。

たとえば、DoS 攻撃では次のようになります。

- WAN 側の送信元からパントされたパケットは、毎秒 100 パケットで到着します。
- WAN 側の SBRL は、毎秒 4 パケットのレート、隔離時間 10 分、バースト係数 500 パケットで設定されています。

パケット レートは、設定したレートよりもかなり高く設定されています。そのため、2000（4 x 500）パケットが到着したら、パケット ストリームが隔離されます。隔離は 20 秒間（毎秒 100 パケットごとに 2000 パケット）で有効になり、ストリームからパントされたパケットは 10 分間ドロップされます。10 分後、隔離は無効になります。

隔離の計算はすぐに再開します。したがって、スキャン攻撃が継続すると、次の20秒後には隔離が再び有効になります。

加入者側送信元ベースのレート制限の設定

この項の構成は、次のとおりです。

加入者ケーブル モデムの送信元ベースのレート制限の設定

加入者ケーブル モデムの SBRL では、パケットに関連するスロット、MAC ドメイン、サービス ID（つまり、*slot/MD/SID*）を使用して、トラフィック ストリームを特定します。この *slot/MD/SID* のすべてのパントは集約され、設定のとおりにレート制限されています。

はじめる前に

制限事項

- パントされたすべてのパケットは、CoPP とパント ポリシングの対象です。
- レイヤ 3 モビリティのパントは、加入者ケーブル モデムの SBRL の対象ではありません。レイヤ 3 モビリティのパントは、加入者 MAC アドレスの SBRL の対象です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**platform punt-sbrl subscriber rate** *rate* 例： `Router(config)# platform punt-sbrl subscriber rate 4`	毎秒のパケット数で加入者ケーブル モデム レートを設定します。範囲は 1 ～ 256 で、2 のべき乗で示します。

加入者 MAC アドレスの送信元ベースのレート制限の設定

加入者 MAC アドレス SBRL では、パント要因と送信元 MAC アドレスのハッシュ値でトラフィック ストリームを識別します。この値は、レート制限のインデックスとして使用されます。Cisco cBR ルータはハッシュ衝突に対し特別な処理を実行しません。そのため、ハッシュ衝突パケット ストリームは同じパケット ストリームからのようにレート制限されます。

レイヤ 3 モビリティ パントのデフォルトのレートは 4 パケット/秒です。

はじめる前に

制限事項

- パントされたすべてのパケットは、CoPP とパント ポリシングの対象です。
- 加入者 MAC アドレス SBRL は、加入者側のレイヤ 3 モビリティ パントにのみ適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**platform punt-sbrl subscriber punt-cause** *punt-cause* **rate** *rate* 例： `Router(config)# platform punt-sbrl subscriber punt-cause 99 rate 2`	加入者 MAC アドレス SBRL を設定します。 • **punt-cause** *punt-cause*：パント要因を指定します。レイヤ 3 モビリティのパント要因は 99 です。 • **rate** *rate*：レート制限を毎秒のパケット数単位で指定します。範囲は 2 の累乗で指定される 1 ～ 256 です。

送信元ベースのレート制限 ping バイパスの設定

送信元ベースのレート制限 ping バイパスを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**platform punt-sbrl ping-bypass** 例： `Router(config)# platform punt-sbrl ping-bypass`	送信元ベースのレート制限 ping バイパスを設定します。

パント ポリシングの設定

パント ポリサーが、指定したパント要因ですべてのパケット（加入者側と WAN 側の両方）を収集し、設定したパラメータに従ってパケットをレート制限します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**platform punt-policer** *punt-cause punt-rate* [**high**] 例： `Router(config)# platform punt-policer 1 10`	パント ポリシングを設定します。 • *punt-cause*：パント要因。範囲は 1 ～ 107 です。 • *punt-rate*：レート制限を毎秒のパケット数で設定します。範囲は 10 ～ 146484 です。

	コマンドまたはアクション	目的
		• **high**：（任意）パントのポリシングが優先順位の高いトラフィックに対してのみ実行されるように指定します。

送信元ベースのレート制限設定の確認

- **show running-config | include punt-sbrl**：SBRL 設定を表示します。

  次に、コマンドの出力例を示します。

```
Router# show running-config | include punt-sbrl

platform punt-sbrl wan punt-cause 11 rate 8
platform punt-sbrl wan punt-cause 24 rate 4
platform punt-sbrl subscriber rate 8
```

- **show access-lists** ：CoPP 設定を確認するためのアクセス リスト情報を表示します。

  次に、コマンドの出力例を示します。

```
Router# show access-lists

Extended IP access list 120
    10 permit ip any any dscp af31
    20 permit ip any any dscp cs2
    30 permit ip any any dscp af21
    40 permit ip 68.86.0.0 0.1.255.255 any
IPv6 access list TRUSTEDV6
    permit ipv6 2001:558::/32 any sequence 10
```

- **show policy-map** *policy-map-name*：ポリシー マップの情報を表示します。

  次に、コマンドの出力例を示します。

```
Router# show policy-map copp_policy

  Policy Map copp_policy
    Class sbrl_trusted
     police rate 1000 pps
       conform-action transmit
       exceed-action transmit
    Class class-default
      set qos-group 99
```

- **show policy-map control-plane**：コントロールプレーン ポリシーマップの情報を表示します。

  次に、コマンドの出力例を示します。

```
Router# show policy-map control-plane

 Control Plane

  Service-policy input: copp_policy

    Class-map: sbrl_trusted (match-any)
      0 packets, 0 bytes
```

```
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: access-group 120
    Match: access-group name TRUSTEDV6
    police:
        rate 1000 pps, burst 244 packets
      conformed 0 packets, 0 bytes; actions:
        transmit
      exceeded 0 packets, 0 bytes; actions:
        transmit
      conformed 0 pps, exceeded 0 pps

  Class-map: class-default (match-any)
    28 packets, 4364 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: any
    QoS Set
      qos-group 99
        Marker statistics: Disabled
```

- **show platform hardware qfp active infrastructure punt sbrl**：SBRL 統計情報を表示します。

次に、コマンドの出力例を示します。

```
Router# show platform hardware qfp active infrastructure punt sbrl

SBRL statistics

Subscriber CM
  drop-cnt  evict-cnt    SID  Interface
-----------------------------------------------
         1          1      5  Cable3/0/0
       982        982      5  Cable3/0/0

Subscriber MAC-addr
  nothing to report

WAN-IPv4
  drop-cnt  evict-cnt  quar  VRF  cause  IP-address
-------------------------------------------------------
    456788     456788     0    0    050  1.2.0.66

WAN-IPv6
  drop-cnt  evict-cnt  quar  VRF  cause  IP-address
-------------------------------------------------------------------------
    129334     129334     1    0    011  3046:1829:fefb::ddd1
       965        965     0    0    011  2001:420:2c7f:fc01::3
```

（注） *quar* の値は 0 または 1 です。値が 1 の場合は、隔離が有効であることを示します。値 *quar* は、送信元からのパケットがドロップされた場合のみ更新されます。送信元が隔離され、パケットの送信が停止した場合、値 *quar* は 1 のままです。ただし、*drop-cnt* の値は増えません。

（注） SBRL統計アルゴリズムに最悪の攻撃者のデータが保存されます。いくつかのパケットのみがドロップされた送信元がまずテーブルに表示されますが、*drop-cnt* が増え続けないと上書きされる場合があります。*evict-cnt* は *drop-cnt* と連動して増えますが、送信元がアクティブにレート制限されなくなると減り始めます。*evict-cnt* が 10 未満になると、レコードが上書きされる場合があります。

- **show platform hardware qfp active infrastructure punt statistics type global-drop**：グローバル パント ポリサーの統計情報を表示します。

  次に、コマンドの出力例を示します。

```
Router# show platform hardware qfp active infrastructure punt statistics type global-drop

Global Drop Statistics

  Number of global drop counters = 22

  Counter ID  Drop Counter Name                              Packets
  ------------------------------------------------------------------
  000         INVALID_COUNTER_SELECTED                      0
  001         INIT_PUNT_INVALID_PUNT_MODE                   0
  002         INIT_PUNT_INVALID_PUNT_CAUSE                  0
  003         INIT_PUNT_INVALID_INJECT_CAUSE                0
  004         INIT_PUNT_MISSING_FEATURE_HDR_CALLBACK        0
  005         INIT_PUNT_EXT_PATH_VECTOR_REQUIRED            0
  006         INIT_PUNT_EXT_PATH_VECTOR_NOT_SUPPORTED       0
  007         INIT_INJ_INVALID_INJECT_CAUSE                 0
  008         INIT_INJ_MISSING_FEATURE_HDR_CALLBACK         0
  009         PUNT_INVALID_PUNT_CAUSE                       0
  010         PUNT_INVALID_COMMON_HDR_VERSION               0
  011         PUNT_INVALID_PLATFORM_HDR_VERSION             0
  012         PUNT_PATH_NOT_INITIALIZED                     0
  013         PUNT_GPM_ALLOC_FAILURE                        0
  014         PUNT_TRANSITION_FAILURE                       0
  015         PUNT_DELAYED_PUNT_PKT_SB_NOT_IN_USE           0
  016         PUNT_CAUSE_GLOBAL_POLICER                     0
  017         INJ_INVALID_INJECT_CAUSE                      0
  018         INJ_INVALID_COMMON_HDR_VERSION                0
  019         INJ_INVALID_PLATFORM_HDR_VERSION              0
  020         INJ_INVALID_PAL_HDR_FORMAT                    0
  021         PUNT_GPM_TX_LEN_EXCEED                        0
```

- **show platform hardware qfp active infrastructure punt summary** [**threshold** *threshold-value*]：パント パス レート制限の概要を表示します。

  次に、コマンドの出力例を示します。

```
Router# show platform hardware qfp active infrastructure punt summary

Punt Path Rate-Limiting summary statistics

Subscriber-side
ID   punt cause           CPP punt        CoPP  ARPfilt/SBRL   per-cause      global
-------------------------------------------------------------------------------------
017  IPv6 Bad hop limit         22           0             0           0           0
050  IPv6 packet                13           0             0           0           0
080  CM not online             335           0             0           0           0

WAN-side
ID   punt cause           CPP punt        CoPP        SBRL   per-cause      global
-------------------------------------------------------------------------------------
017 IPv6 Bad hop limit         471           0           0           0           0
018 IPV6 Hop-by-hop Options  29901           0           0        1430           0
024 Glean adjacency            111           0           0           0           0
025 Mcast PIM signaling         19           0           0           0           0
050 IPv6 packet                 11           0           0           0           0
```

- **show platform software punt-policer**：パント ポリサーの設定と統計情報を表示します。

  次に、コマンドの出力例を示します。

```
Router# show platform software punt-policer

Per Punt-Cause Policer Configuration and Packet Counters
```

```
Punt                                  Configured (pps) Conform Packets   Dropped Packets
Cause Description                     Normal   High    Normal     High   Normal     High
------------------------------------------------------------------------------------------
  2   IPv4 Options                    4000     3000    0          0      0          0
  3   Layer2 control and legacy       40000    10000   16038      0      0          0
  4   PPP Control                     2000     1000    0          0      0          0
  5   CLNS IS-IS Control              2000     1000    0          0      0          0
  6   HDLC keepalives                 2000     1000    0          0      0          0
  7   ARP request or response         2000     1000    0          49165  0          0
  8   Reverse ARP request or re...    2000     1000    0          0      0          0
  9   Frame-relay LMI Control         2000     1000    0          0      0          0
 10   Incomplete adjacency            2000     1000    0          0      0          0
 11   For-us data                     40000    5000    279977     0      0          0
 12   Mcast Directly Connected ...    2000     1000    0          0      0          0
 . . .
```

- **show platform hardware qfp active infrastructure punt policer summary**：パント ポリサーの概要を表示します。

  次に、コマンドの出力例を示します。

```
Router# show platform hardware qfp active infrastructure punt policer summary

QFP Punt Policer Config Summary


Policer  Rate     PeakRate   ConformBurst  ExceedBurst   Scaling
Handle   (pps)    (pps)      (pps)         (pps)         Factor
-------------------------------------------------------------------
001      300000   0          2288          2288          0
002      4000     0          4000          0             0
003      3000     0          3000          0             0
004      40000    0          40000         0             0
005      10000    0          10000         0             0
006      2000     0          2000          0             0
007      1000     0          1000          0             0
008      2000     0          2000          0             0
009      1000     0          1000          0             0
010      2000     0          2000          0             0
011      1000     0          1000          0             0
012      2000     0          2000          0             0
013      1000     0          1000          0             0
014      2000     0          2000          0             0
 . . .
```

送信元ベースのレート制限の設定例

例：WAN 側 SBRL の設定

```
access-list 120 permit ip any any dscp af31
access-list 120 permit ip any any dscp cs2
access-list 120 permit ip any any dscp af21
access-list 120 permit ip 192.168.1.10 0.1.255.255 any

ipv6 access-list TRUSTEDV6
  permit ipv6 any any dscp af31
  permit ipv6 any any dscp cs2
  permit ipv6 any any dscp af21
  permit ipv6 2001:558::/32 any


class-map match-all sbrl_trusted_v4
  match access-group 120

class-map match-all sbrl_trusted_v6
```

```
  match access-group name TRUSTEDV6


policy-map copp_policy
  ! IPv4 trusted:
  !   Specified rate is irrelevant.
  !   No special action; these packets bypass WAN-side SBRL.
  class sbrl_trusted_v4
    police rate 1000 pps conform transmit exceed transmit
  ! IPv6 trusted:
  !   Specified rate is irrelevant.
  !   No special action; these packets bypass WAN-side SBRL.
  class sbrl_trusted_v6
    police rate 1000 pps conform transmit exceed transmit

  ! add other classes here, if necessary

  ! Special action to activate WAN-side SBRL for this class.
  class class-default
    set qos-group 99


control-plane
  service-policy input copp_policy


! punt-cause 11 is FOR_US, punt-cause 24 is GLEAN_ADJ
platform punt-sbrl wan punt-cause 11 rate 4
platform punt-sbrl wan punt-cause 24 rate 4
```

例：加入者側の SBRL の設定

```
platform punt-sbrl subscriber rate 4
```

例：SBRL の設定

```
…
platform punt-sbrl wan punt-cause 11 rate 4
platform punt-sbrl wan punt-cause 18 rate 16 quarantine-time 10 burst-factor 500
platform punt-sbrl wan punt-cause 24 rate 4
platform punt-sbrl subscriber rate 4
…
access-list 120 permit ip any any dscp af31
access-list 120 permit ip any any dscp cs2
access-list 120 permit ip any any dscp af21
access-list 120 permit ip 192.168.1.10 0.1.255.255 any
…
ipv6 access-list TRUSTEDV6
permit ipv6 any any dscp af31
permit ipv6 any any dscp cs2
permit ipv6 any any dscp af21
permit ipv6 2001:558::/32 any
…
policy-map copp_policy
class sbrl_trusted_v4
  police rate 1000 pps conform-action transmit  exceed-action transmit
 class sbrl_trusted_v6
  police rate 1000 pps conform-action transmit  exceed-action transmit
 class class-default
  set qos-group 99
…
control-plane
service-policy input copp_policy
…
```

Cisco uBR10012 ルータにおける転送レート制限の設定から Cisco cBR シリーズ ルータにおける SBRL 設定への変換

Cisco uBR10012 ルータにおける転送レート制限の設定

次に、Cisco uBR10012 ルータにおける転送レート制限（DRL）の設定例を示します。

```
service divert-rate-limit ip fib_rp_glean rate 4 limit 4
service divert-rate-limit ip fib_rp_dest rate 4 limit 4
service divert-rate-limit ip fib_rp_punt rate 4 limit 4
service divert-rate-limit ipv6 ipv6_rp_dest rate 4 limit 4
service divert-rate-limit ipv6 ipv6_rp_punt rate 4 limit 4
service divert-rate-limit ipv6 ipv6_rp_glean rate 4 limit 4
service divert-rate-limit ipv6 icmpv6 rate 4 limit 4

service divert-rate-limit trusted-site 0.0.0.0 0.0.0.0 tos 0x68 mask 0xFF
service divert-rate-limit trusted-site 0.0.0.0 0.0.0.0 tos 0x40 mask 0xFF
service divert-rate-limit trusted-site 68.86.0.0 255.254.0.0 tos 0x0 mask 0x0
service divert-rate-limit trusted-site 0.0.0.0 0.0.0.0 tos 0x48 mask 0xFF
service divert-rate-limit trusted-site-ipv6 ::/0 traffic-class 0x40 mask 0xFF
service divert-rate-limit trusted-site-ipv6 ::/0 traffic-class 0x48 mask 0xFF
service divert-rate-limit trusted-site-ipv6 ::/0 traffic-class 0x68 mask 0xFF
service divert-rate-limit trusted-site-ipv6 2001:558::/32 traffic-class 0x0 mask 0x0

interface Cablex/y/z
   cable divert-rate-limit rate 4 limit 30
```

Cisco IOS リリース 12.2(33)SCH2 では、**divert-rate-limit max-rate wan** コマンドが Cisco uBR10012 ルータに追加されました。この設定により、WAN 側の転送パケットの集約レートが転送コード単位で制限されます。次に、**divert-rate-limit max-rate wan** コマンドで推奨されるベストプラクティスの設定を示します。

```
service divert-rate-limit max-rate wan fib_rp_glean rate 5000
service divert-rate-limit max-rate wan fib_rp_punt rate 5000
service divert-rate-limit max-rate wan fib_rp_dest rate 40000

service divert-rate-limit max-rate wan ipv6_fib_glean rate 5000
service divert-rate-limit max-rate wan ipv6_fib_punt rate 5000
service divert-rate-limit max-rate wan ipv6_fib_dest rate 40000
```

Cisco cBR シリーズ ルータにおける SBRL 設定

DRL 機能は、Cisco cBR シリーズルータでは送信元ベースのレート制限（SBRL）と呼ばれています。パント パスには 3 つの保護レイヤがあります。

- CoPP, （1457 ページ）
- SBRL, （1458 ページ）
- パント ポリサー, （1459 ページ）

CoPP

CoPP は、信頼済みサイトの指定と WAN 側 SBRL の有効化に使用されます。ただし、CoPP はパントパケットすべてに適用されるため、ケーブル側のパントが信頼済みサイトと一致しないことを確認する必要があります。

次に、CoPP 設定の例を示します。これは、Cisco uBR10012 ルータでの設定と同じです。

```
access-list 120 permit ip any any dscp af31
access-list 120 permit ip any any dscp cs2
access-list 120 permit ip any any dscp af21
access-list 120 permit ip 68.86.0.0 0.1.255.255 any

ipv6 access-list TRUSTEDV6
   permit ipv6 any any dscp af31
   permit ipv6 any any dscp cs2
   permit ipv6 any any dscp af21
   permit ipv6 2001:558::/32 any

class-map match-all sbrl_trusted_v4
   match access-group 120

class-map match-all sbrl_trusted_v6
   match access-group name TRUSTEDV6

policy-map copp_policy
   class sbrl_trusted_v4
     police rate 1000 pps conform transmit exceed transmit
   class sbrl_trusted_v6
     police rate 1000 pps conform transmit exceed transmit
   class class-default
     set qos-group 99

control-plane
   service-policy input copp_policy
```

（注）

- **set qos-group 99** コマンドを使用すると、指定したクラスの SBRL が有効化されます。
- 両方のアクションが **transmit** に設定されているため、**sbrl_trusted_v***x* のポリシー レートは無関係です。
- 必要に応じて、他の信頼済みサイトも追加できます。

SBRL

加入者側の SBRL 設定には、グローバル コンフィギュレーション モードの単一コマンドを使用します。ハードウェアのポリサーが使用されているため、制限は設定できません。そのため、最初に高いレートを設定することを推奨します。

Cisco cBR シリーズ ルータにおける WAN 側の SBRL では、パント要因が IPv4 と IPv6 の間で共有されるため、IPv4 と IPv6 の設定を分けられません。ハードウェアのポリサーが使用されているため、制限は設定できません。そのため、最初に高いレートを設定することを推奨します。次の設定例では、パント要因 24 は *Glean adjacency* を、パント要因 11 は *For-us data* を示しています。これらは、Cisco uBR10012 ルータの *x*_rp_glean と *x*_rp_dest にそれぞれ相当します。

```
platform punt-sbrl subscriber rate 16

platform punt-sbrl wan punt-cause 11 rate 8
platform punt-sbrl wan punt-cause 24 rate 8
```

（注）

- *fib-punt* パント要因は、管理イーサネット宛てのパケット用として Cisco uBR10012 ルータで使用されます。このパント要因は、Cisco cBR シリーズ ルータでは使用されません。
- Cisco cBR シリーズ ルータには、ICMPV6 のパント要因に相当するものがありません。Cisco uBR10012 ルータでは、ICMPv6 パケットをルート プロセッサで処理し、チェックサムを生成する必要があります。Cisco cBR シリーズ ルータでは、ICMPv6 をコントロール プレーンで処理します。ただし、CoPP を使用して、ICMPv6 パントを識別し、レート制限（アグリゲーション）することができます。

パント ポリサー

パント ポリサーは、すべてのパント要因に対して動作できるだけでなく、完全に設定可能です。また、WAN 側と加入者側で分けられてはいません。特定のパント要因を持つすべてのパケットが、設定通りに集約され、レート制限されます。

次に、Cisco cBR シリーズ ルータでのパント ポリサーのデフォルト設定（ベスト プラクティス設定）を示します。

```
punt-cause                      LO     HI

CPP_PUNT_CAUSE_GLEAN_ADJ        2000   5000
CPP_PUNT_CAUSE_FOR_US           40000  5000
```

（注）

- *fib-glean*（Cisco uBR10012 ルータ上）に相当するパント要因は、Cisco cBR シリーズ ルータでは *GLEAN_ADJ/HI* です。
- （Cisco uBR10012 ルータ上の）*fib-dest* に相当するパント要因は、Cisco cBR シリーズ ルータでは *FOR_US/LO* です。

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

送信元ベースのレート制限に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *213*：送信元ベースのレート制限に関する機能情報

機能名	リリース	機能情報
送信元ベースのレート制限	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 86 章

ケーブル重複 MAC アドレス拒否

ケーブル重複 MAC アドレス拒否機能は、複製されたケーブル モデムによって生じるサービス妨害（DOS）攻撃を排除するのに役立つ DOCSIS 1.1 対応セキュリティ拡張です。複製とは、同じ HFC インターフェイスの MAC アドレスを持つ、同じ Cisco CMTS ルータ上の 2 つの物理ケーブル モデムの 1 つと仮定されます。複製されたケーブル モデムは、DOCSIS 1.0 以降のものである場合もあれば、DOCSIS 仕様に半分しか準拠しないか、またはその一部に準拠していない場合があります。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *214*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

ケーブル重複 MAC アドレス拒否の前提条件

ケーブル重複MACアドレス拒否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 ルータで、正規のケーブル モデムが ベースライン プライバシー インターフェイス プラス（BPI+）に準拠している必要があります。つまり、少なくとも 1 つの BPI+ 関連のタイプ、長さ、値（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。簡潔にするために、ここでは、これらの状態を online(p_) で示します。
- Cisco CMTS ルータは、次の 4 つのいずれかの状態の Cisco CMTS ルータ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 ルータは、これら 4 つの状態のいずれかですでに動作中のモデムと同じ MAC アドレスの使用を意図する他のデバイスによる登録要求をドロップします。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス, （36 ページ） に、この機能のハードウェア互換性に関する前提条件を示します。

（注） Cisco IOS の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、それ以降のすべてのリリースでもサポートされます。

ケーブル重複 MAC アドレス拒否の制約事項

- 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_) の初期状態ではオンラインにならないため、Cisco CMTS ルータ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 システムにより BPI+ がイネーブル化された DOCSIS コンフィギュレーション ファイルが提供されないと、Cisco CMTS ルータは 2 つのケーブル モデムを区別しようとしません。
- この機能が有効な場合、Cisco CMTS ルータは、layer2events ログを記録するケーブルのログ メッセージでセキュリティ違反通知を発行します。または、Cisco CMTS ルータに **cable logging layer2events** コマンドが設定されていない場合は、汎用ログでこの通知を発行します。

ケーブル重複 MAC アドレス拒否に関する情報

Cisco CMTS ルータでは、ケーブル重複 MAC アドレス拒否機能はデフォルトでイネーブルになっており、関連の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、それはデフォルトでシステム ログに表示されます。

このマニュアルでは、ケーブル重複MACアドレス拒否機能に関連付けられた、次のセキュリティ機能についても説明します。

初期認証と暗号化

初期認証と暗号化（EAE）機能により、Cisco CMTS ルータは、レンジング プロセスの完了直後に DOCSIS 3.0 ケーブル モデムを認証し、DHCP および TFTP トラフィックなどの登録パケット パッケージをすべて暗号化できます。DOCSIS 3.0 ケーブル モデムにのみ対応したこのセキュリティ機能は、マルチプル サービス オペレータ（MSO）が不正に使用されないようにするために導入されました。

この機能は、Cisco CMTS ルータが MAC ドメイン記述子（MDD）メッセージを送信しているダウンストリーム チャネルで初期化するケーブル モデムに対してのみイネーブルになります。Cisco CMTS ルータは、EAE をケーブル モデムに伝えるために MDD MAC メッセージで TLV タイプ 6 を使用します。この機能をイネーブルにすると、認証されたケーブル モデムのみが初期化プロセスを続行できるため、ネットワークへのアクセスも許可されます。初期認証と暗号化には以下のプロセスがあります。

- レンジング プロセス後のケーブル モデムの認証（BPI+ 承認交換）。
- ケーブル モデムのプライマリ セキュリティ アソシエーション ID（SAID）のトラフィック暗号キー（TEK）交換。
- ケーブル モデム初期化中の IP プロビジョニング トラフィックとマルチパート登録要求（REG-REQ-MP）メッセージの暗号化。

EAE 適用ポリシー

Cisco CMTS ルータでは、次の EAE 適用ポリシーをサポートします。

- EAE 適用なし（ポリシー 1）：EAE は無効で、Cisco CMTS ルータは EAE をケーブル モデムに適用できません。
- レンジングベースの EAE 適用（ポリシー 2）：EAE は、B-INIT-RNG-REQ MAC メッセージを使用するすべての DOCSIS 3.0 ケーブル モデムに適用されます。
- 機能ベースの EAE 適用（ポリシー 3）：EAE は、EAE 機能フラグを設定した B-INIT-RNG-REQ MAC メッセージを使用するすべての DOCSIS 3.0 ケーブル モデムに適用されます。
- トータル EAE 適用（ポリシー 4）：EAE は、EAE 機能フラグのステータスに関係なく、すべてのケーブル モデムに適用されます。

選択する EAE 適用ポリシーは 1 つです。デフォルトでは、EAE は Cisco CMTS ルータで無効です。

EAE の除外

グローバル コンフィギュレーション モードで **cable privacy eae-exclude** コマンドを使用すると、EAE 適用からケーブル モデムを除外できます。EAE 除外リストに含まれるケーブル モデムは常に EAE 適用から除外されます。**cable privacy eae-exclude** コマンドの no 形式を使用すると、除外リストからケーブル モデムを削除できます。

BPI+ セキュリティおよび複製ケーブル モデム

BPI+セキュリティおよび複製ケーブル モデム機能では、同じケーブル モデムの MAC アドレスを使用する新しいケーブルモデム登録要求で、BPI+セキュリティが有効な状態でオンラインであるケーブル モデムを優先します。その結果、HFC MAC アドレスが同じ非準拠のケーブル モデムが登録を試みた場合であっても、BPI+ セキュリティ証明書を持ち、HFC MAC アドレスが一致する正規のケーブル モデムではサービス中断は発生しません。

複製ケーブル モデムの検出機能では、ケーブル モデムが DOCSIS 1.1 以降のバージョンを使用する必要があり、BPI+ が有効な状態でプロビジョニングされる必要があります。つまり、1 つの BPI+ TLV（タイプ、長さ、値）が DOCSIS コンフィギュレーション ファイルに含まれる必要があります。DOCSIS BPI+ が有効ではない状態でプロビジョニングされたすべての DOCSIS 1.0、DOCSIS 1.1、およびそれ以降のケーブル モデムでは、レガシーの DOCSIS の動作を使用し続けることになり、複製ケーブル モデムが Cisco CMTS ルータ上にある場合は DoS 攻撃が発生します。

この複製ケーブル モデムの検出機能では、BPI+ と DOCSIS 1.1 QoS が有効な状態でプロビジョニングされたケーブル モデムは、BPI+ に登録する必要があり、BPI を使用できません。広く使用可能な DOCSIS 非準拠のケーブル モデムでは、DOCSIS 1.1 QoS および BPI+ が DOCSIS コンフィギュレーション ファイルで指定されている場合でも BPI+ モードではなく BPI で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。クローン ケーブル モデムのロギング機能はデフォルトでイネーブルに設定されています。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。デフォルトでは、クローン ケーブル モデムのメッセージは、ケーブル ロガー cable layer2events logging に配置されます。グローバル コンフィギュレーション モードで **cable logging layer2events** コマンドの no 形式 を使用してこの機能を無効にすると、クローン ケーブル モデムのメッセージがシステム ログ（syslog）に保管されます。

クローン ケーブル モデムは、短期間に数十回の登録試行を試みる場合があります。生成されるログ メッセージの数を抑制するために、Cisco CMTS ルータは、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 ルータ上のどこかですでに 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。

DOCSIS 3.0 BPI+ ポリシーの適用

DOCSIS 3.0 BPI+ ポリシーの適用機能は、ケーブル モデムの MAC アドレス複製やサービスの不正使用を防ぐために導入されました。この機能により、Cisco CMTS ルータは各ケーブル モデムの MAC アドレスを検証できます。ケーブル モデムで BPI+ を適用するには、ルータの MAC ドメインごとに次の適用ポリシーの 1 つを設定する必要があります。

- 1.1 形式のコンフィギュレーション ファイル パラメータと機能（ポリシー 1）：Cisco CMTS ルータは、BPI+ が TLV 29 あり/なしで有効であることを示すパラメータを使用して DOCSIS 1.1 コンフィギュレーション ファイルに登録されたケーブル モデム上で BPI+ を適用します。このポリシーを設定するには、DOCSIS コンフィギュレーション ファイルのプライバシー サポート モデム機能 TLV（タイプ 5.6）が BPI+ をサポートするように設定されている必要があります。このポリシーは、BPI+ に対応していて DOCSIS1.1 コンフィギュレーション ファイルでプロビジョニングされているケーブル モデム上で BPI+ を適用します。登録中にこれらの機能をシグナリングするケーブル モデムは、モデムが BPI+ ネゴシエーションを完了するまで、ネットワーク アクセスがブロックされます。
- 1.1 形式のコンフィギュレーション ファイル パラメータ（ポリシー 2）：Cisco CMTS ルータは、BPI+ が TLV 29 あり/なしで有効であることを示すパラメータを使用して DOCSIS 1.1 コンフィギュレーション ファイルに登録されたケーブル モデム上で BPI+ を適用します。このタイプのコンフィギュレーション ファイルに登録されるケーブル モデムは、モデムが BPI+ ネゴシエーションを完了するまで、ネットワーク アクセスがブロックされます。
- 1.1 形式のコンフィギュレーション ファイル（ポリシー 3）：Cisco CMTS ルータは、DOCSIS 1.1 コンフィギュレーション ファイルに登録されたケーブル モデム上で BPI+ を適用します。つまり、セキュリティが無効な（プライバシー フラグがコンフィギュレーション ファイルに存在しない）状態で DOCSIS 1.1 コンフィギュレーション ファイルをプロビジョニングする場合、すべての DOCSIS 1.1 および 2.0 ケーブル モデムはネットワーク アクセスがブロックされます。プライバシー フラグがコンフィギュレーション ファイルに存在しない場合、セキュリティが暗黙的に有効な DOCSIS 3.0 ケーブル モデムのみがこのチェックに合格します。
- 全適用（ポリシー 4）：Cisco CMTS ルータは、すべてのケーブル モデム上で BPI+ を適用します。つまり、BPI+ を実行していないすべてのケーブル モデムはネットワーク アクセスがブロックされます。

（注） 設定できる適用ポリシーは、MAC ドメインあたり一度に 1 つのみです。ポリシーを 1 つずつ設定する場合、最新のポリシーが既存のポリシーを置き換えます。たとえば、ポリシー 2 がポリシー 1 を引き継ぐ場合は、ポリシー 1 を無効にせずにポリシー 2 を直接設定できます。

これらの適用ポリシーは、CableLabs Security Specification の CM-SP-SECv3.0-I13-100611 に基づいて実装されます。これらの適用ポリシーを設定するには、ケーブル インターフェイス コンフィ

ギュレーション モードで **cableprivacybpi-plus-policy** コマンドを使用します。設定されたポリシーに準拠していないケーブル モデムも引き続きオンラインになることができますが、DOCSIS ネットワークにはアクセスできず、一部のデュアル スタック ケーブル モデムは IPv4 アドレスと IPv6 アドレスの両方を取得しない可能性があります。

ポリシー 1、2、および 3 は、DOCSIS 1.0（DOCSIS セットトップ ゲートウェイを含む）、DOCSIS 1.1、およびそれ以降のケーブル モデムが混在するネットワークをサポートします。ケーブル モデムの MAC アドレス複製を防ぐための最も効果的な設定がポリシー 4 です。このポリシーは、すべてのケーブル モデム上で BPI+ を適用します。ポリシー 4 では、すべての DOCSIS 1.0 ケーブル モデムが BPI+ モードで登録されないため、そのようなモデムをすべてブロックします。したがって、ポリシー 4 を使用する場合、すべての承認済み DOCSIS 1.0 ケーブル モデムをアップグレードするか、またはネットワークから削除する必要があります。

BPI+ ポリシーの適用の除外

グローバル コンフィギュレーション モードで **cable privacy bpi-plus-exclude** コマンドを使用することで、MAC アドレスに基づいて、BPI+ ポリシーの適用対象からケーブル モデム（DOCSIS 1.0 以降のバージョン）を除外できます。MAC ドメインごとに最大 30 個のケーブル モデムを除外できます。

EAE および BPI+ 適用機能の設定方法

ここでは、次の BPI+ 適用機能の設定方法について説明します。

EAE 適用ポリシーの設定

デフォルトでは、EAE は Cisco CMTS ルータで無効です。ケーブル インターフェイス コンフィギュレーション モードで **cableprivacyeae-policy** コマンドを使用すると、EAE 適用ポリシーを設定できます。

（注） EAE 適用ポリシーは、ダウンストリーム チャネルで初期化する DOCSIS 3.0 ケーブル モデムに対してのみ有効になります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interface cable** {*slot*/*cable-interface-index* | *slot*/*subslot*/*cable-interface-index*} 例： `Router(config)# interface cable 6/0/1`	インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**cableprivacyeae-policy** {**capability-enforcement** | **disable-enforcement** | **ranging-enforcement** | **total-enforcement**} 例： `Router(config-if)# cable privacy eae-policy total-enforcement`	DOCSIS 3.0 ケーブル モデムで EAE 適用ポリシーを指定します。
ステップ 5	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。

BPI+ 適用ポリシーの設定

BPI+ 適用ポリシーは、ケーブル モデムの MAC アドレスのクローン作成およびサービスの窃盗を防止するために MAC ドメインごとに設定されます。

はじめる前に

顧客宅内機器（CPE）がネットワーク アクセス用の IP アドレスを取得するために DHCP を使用したり、静的に割り当てられた IP アドレスが適切に管理されるようにする必要があります。

（注） 1 つの MAC ドメインに対して適用できる適用ポリシーは 1 つのみです。

手順

	コマンドまたはアクション
ステップ 1	**enable** 例： `Router> enable`
ステップ 2	**configure terminal** 例： `Router# configure terminal`

	コマンドまたはアクション
ステップ 3	**interfacecable** *{slot/subslot/port |slot/port}* 例： `Router(config)# interface cable 5/1/0`
ステップ 4	**cableprivacybpi-plus-policy{capable-enforcement|d11-enabled-enforcement|d11-enforcement|total-enforcem** 例： `Router (config-if)# cable privacy bpi-plus-policy total-enforcement`
ステップ 5	**end** 例： `Router(config-if)# end`

非 MTC DOCSIS3.0 ケーブル モデムの AES-128 の設定

この機能は、デフォルトで有効になっています。この機能を無効にするには、次の手順に従います。

enable
configure terminal
no cable privacy non-mtc-aes128
end

非 MTC DOCSIS3.0 ケーブル モデムの AES-128 の確認

非 MTC DOCSIS3.0 ケーブル モデムで AES-128 がサポートされるかどうかを確認するには、次の例に示すように **show running-config** コマンドを使用します。

```
Router# show running-config | include cable privacy non-mtc-aes128
no cable privacy non-mtc-aes128
```

トラブルシューティングのヒント

BPI+ポリシー適用の設定をトラブルシューティングするには、次のデバッグ コマンドを使用します。

- **debug cable mac-address**：特定のケーブル モデムに関するデバッグ情報を提供します。
- **debug cable bpiatp**：BPI ハンドラのデバッグをイネーブルにします。

EAE および BPI+ 適用ポリシーの設定例

次に、Cisco cBR-8 ルータで EAE 適用ポリシーを構成する例を示します。

```
Router# configure terminal
Router(config)# interface cable 8/1/0
Router (config-if)# cable privacy eae-policy capability-enforcement
Router (config-if)# cable privacy eae-policy ranging-enforcement
Router (config-if)# cable privacy eae-policy total-enforcement
```

次に、Cisco cBR-8 ルータのスロット/サブスロット/ポート 5/1/0 で BPI+ 適用ポリシーを構成する例を示します。

```
Router# configure terminal
Router(config)# interface cable 5/1/0
Router (config-if)# cable privacy bpi-plus-policy total-enforcement
```

EAE および BPI+ 適用ポリシーの確認

EAE および BPI+ 適用設定を確認するには、次の show コマンドを使用します。

- **showinterfacecableprivacy**
- **showcableprivacy**
- **showcablemodemaccess-group**

Cisco CMTS ルータに設定された EAE ポリシーを確認するには、**showinterfacecableprivacy** コマンドを使用します。

Cisco CMTS ルータの EAE 適用から除外されたケーブル モデムを確認するには、**showcableprivacy** コマンドを使用します。

BPI+ 適用ポリシーを確認するには、**showinterfacecableprivacy** コマンドを使用します。

（注） bpi-plus-policy を満たしていないモデムを特定するには、オンライン状態の前に文字「*」を入力します。

次の作業

複製ケーブル モデムの検出機能は、BPI+ 証明書と DOCSIS 1.1 による要因に関連しています。

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、Cisco cBR-8 ルータでの複製ケーブル モデムの検出機能に関しロギングされたイベントの例を示します。

次のシナリオでは、複製された MAC アドレスを持つ 2 つのケーブル モデムが存在します。

- 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、複製されたケーブル 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、複製されたケーブル モデムも同じインターフェイス上にあります。
- 次の例では、MAC アドレス 000f.66f9.48b1 の複製されたケーブル 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、複製された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: %CBR-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: %CBR-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: %CBR-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: %CBR-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: %CBR-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: %CBR-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、ケーブル モデムの詳細情報を表示する **showcable modem** コマンドの例を示します。

```
Router# show cable modem 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
```

その他の参考資料

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ケーブル重複 MAC アドレス拒否に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *215*：ケーブル重複 *MAC* アドレス拒否に関する機能情報

機能名	リリース	機能情報
ケーブル重複 MAC アドレス拒否	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。
非 MTC DOCSIS 3.0 ケーブル モデル用 AES-128	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 87 章

ケーブル ARP フィルタリング

このマニュアルでは、Cisco ケーブル モデム終端システム（CMTS）のケーブル ARP フィルタリング機能を説明します。サービス プロバイダーはこの機能を使用して Address Resolution Protocol（ARP）要求パケットおよび応答パケットをフィルタリングし、大容量のパケットがケーブル ネットワーク上の他のトラフィックに干渉するのを防ぐことができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *216* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

ケーブル ARP フィルタリングの前提条件

ケーブルARPフィルタリング機能を使用するために、特別な装置やソフトウェアは必要ありません。

ケーブル ARP フィルタリングの制約事項

Cisco cBR-8 ルータに関する制約事項

- Cisco cBR-8 ルータはスーパーバイザ（SUP）モジュールに ARP フィルタリングの統計情報を維持します。指定したインターフェイスについての統計情報を **showcablearp-filter** コマンドで確認できます。SUP 冗長性などでスイッチオーバー イベントが発生すると、これらの ARP フィルタリング統計がゼロにリセットされます。

- ケーブルの ARP フィルタ機能はサブインターフェイスごとには設定できません。

FP での ARP フィルタの制限事項

- FP での ARP フィルタリングにレート制限機能を提供するために FP マイクロコードが強化される必要があります。

- FP での ARP フィルタ機能は、サブインターフェイスごとには設定できません。

ケーブル ARP フィルタリングに関する情報

概要

サービス不正使用攻撃およびサービス妨害（DNS）攻撃は、ケーブルブロードバンドネットワークでますます一般化してきました。さらに、ウイルスの攻撃も一般的になりつつあり、自分のコンピュータが感染していてネットワーク攻撃を維持するために使用されていることにユーザは気付かないことも珍しくありません。

このような攻撃中によく現れる兆候の 1 つとして、Address Resolution Protocol（ARP）パケットの量が異常に高くなります。ユーザまたはウイルスは、ARP 要求を繰り返し発行して、攻撃を受けやすい可能性のあるその他のコンピュータの IP アドレスを探そうとします。

ARP 要求はブロードキャストパケットであるため、そのネットワーク セグメント上にあるすべてのデバイスにブロードキャストされます。状況によっては、さらに処理するためにルータが ARP ブロードキャストを ARP プロキシに転送することもあります。

ホーム ネットワークの加入者で一般的に使用されるローエンド ルータではすべての ARP 要求に適切に対応しない可能性もあるため、生成されるトラフィックがさらに増大することになり、この問題は悪化します。このような顧客宅内機器（CPE）デバイスが適切な Request for Comments（RFC）仕様に準拠しているファームウェアでアップグレードできるようにならない限り、サービス プロバイダーは不適切に生成または転送されるトラフィックを取り扱える必要があります。

また、Cisco CMTS ルータは自動的に ARP トラフィックをモニタし、ARP 要求で見つかった IP アドレスを専用の ARP テーブルに入力します。これは、デバイスが最終的にはその IP アドレスで検出されることを想定しているためです。確認応答されない IP アドレスは、ルータの ARP テー

ブルに 60 秒間とどまります。つまり、大量の ARP トラフィックがルータの ARP テーブルを埋め尽くすことがあります。

このプロセスによって、ネットワーク全体で大量の ARP トラフィックが作成される可能性があります。状況によっては、ARP 要求と応答のボリュームが大きいために、その他のトラフィックを絞り、Cisco CMTS ルータの処理時間の大半を占有した結果、技術者のネットワーク回復作業を妨げてしまう可能性があります。

ルータは ARP パケットを処理するためにファスト スイッチングを使用できず、代わりに ARP パケットをルートプロセッサ（RP）に転送する必要があります。このため、大量の ARP トラフィックを処理するために、ルータが通常のトラフィックを処理できない可能性もあります。

ARP トラフィックのフィルタリング

ケーブル インターフェイス上の ARP トラフィックの量を制御するには、**cable arp filter** コマンドを設定して、ユーザ指定の期間にわたるサービス ID（SID）あたりの許容 ARP パケット数を指定します。ARP 要求パケット用と ARP 応答パケット用に別々のしきい値を設定できます。

ARP パケットをフィルタリングするようにケーブル インターフェイスが設定されると、SID ごとに受信した ARP 要求または応答パケットの数のテーブルがケーブル インターフェイスで維持されます。ウィンドウ期間中に SID がパケットの最大数を超えると、新しい期間が開始するまで Cisco CMTS でパケットがドロップされます。

（注） バンドル ケーブル インターフェイスを使用する場合、ケーブル ARP フィルタリング機能がマスターおよびスレーブ インターフェイスで個別に設定されます。これにより、この機能を必要とする特定のインターフェイスでのみ機能を設定することができます。また、さまざまなしきい値を使用して機能を設定すると、各インターフェイスのトラフィック パターンに対応するように機能をカスタマイズすることができます。

フィルタリングされた ARP トラフィックのモニタリング

ケーブル インターフェイスの ARP フィルタリングを有効にした後は、**divert-rate-limit** コマンドを使用することで、過剰な量の ARP トラフィックを生成している装置を表示できます。これらの装置がそのようなトラフィックを生成する理由として、次の理由が考えられます。

- DOCSIS に準拠していないか、サービス不正使用攻撃目的でハッキングされているソフトウェア イメージを実行しているケーブル モデム。
- サービス不正使用攻撃またはサービス妨害攻撃を実行しているか、またはウイルス感染し、感染可能な他のコンピュータを探している CPE デバイス。
- 誤ってすべての ARP 要求に応答するか、それらを転送しているルータまたは他の装置。

このようなトラフィックを生成している装置を特定した後は、サービス レベル契約（SLA）で許可された方法を使用して問題を修正できます。

Linksys 無線ブロードバンド ルータ（BEFW11S4）

Linksys 無線 B ブロードバンド ルータ（モデル番号 BEFW11S4 バージョン 4、1.44.2 ファームウェア付き）は、このルータ用に向けられた ARP 要求のみに応答する代わりに、受信したすべての ARP 要求パケットに対して ARP 応答パケットを送信する誤作動をします。このバグを修正するため、顧客は最新のリビジョンにファームウェアをアップグレードする必要があります。ファームウェアをアップグレードするには、Linksys Web サイトのダウンロード セクションにアクセスします。

（注） コンプライアンス違反の CPE デバイスを、ARP や他のブロードキャスト トラフィックを適切に処理するファームウェアに更新することはきわめて重要です。セグメントに 1 個か 2 個のコンプライアンス違反のデバイスがあるだけで、セグメント上の他の顧客すべてに影響するパケットのドロップの問題が生じる可能性があります。

FP での ARP フィルタリング

ARP フィルタ機能は、SUP FP コンプレックスで実行されます。有効にすると、この FP コンプレックスは識別された ARP 違反者の ARP パケットをフィルタリングして、ARP パント レートと RP CPU 使用量を減らします。また、SID の代わりに送信元 MAC アドレスを使用して、ARP フィルタリングで提供する分離を一層明確にします。

フィルタのロジックでは、SID ではなく送信元 MAC アドレスによってフィルタリングするようになりました。現在、モデムの MAC アドレスは ARP のフィルタリングから除外されています。ただし、すべての ARP が同じ SID から発信されたように見えるため、マルチメディア ターミナル アダプタ（MTA）やその他の違反していない CPE は引き続き（静的に）ARP がフィルタリングされます。このため、送信元 MAC アドレスによるフィルタリングでは、違反しているデバイスのレベルまで分離します。これにより、MTA と汚染された CPE 経由で Voice-over-IP（VoIP）サービスを利用するカスタマーは、汚染された CPE に関してサービス プロバイダーに連絡している間は MTA の問題はありません。

ARP 違反者は、構成済みまたはプロビジョニング済みのゲートウェイ アドレスを通じてインターネット接続が完全に失われることを避けるため、引き続き ARP を使用することが許可されます。このような理由から、「ARP Input」プロセスは CPU 使用率が低い割合を示し続けますが、正味の割り込み CPU 使用率は下がることが予想されます。

（注） Cisco cBR-8 ルータでは、FP における ARP フィルタリングがデフォルトで有効です。

FP の ARP トラフィックのフィルタリング

FP の ARP トラフィックを有効にすると、ARP 違反者を送信元 MAC アドレスまたは SID で特定するために、RP 上で実行される軽量アルゴリズムが使用されます。違反しているすべての送信元 MAC アドレスまたは SID は、ARP フィルタ コントロール モジュールによって FP ucode 転送レー

ト制限モジュールにプログラミングされます（ARP違反者は引き続きARPトランザクションを実行できますが、設定されたフィルタリング レートでのみとなります）。

違反している送信元 MAC アドレスまたは SID は少なくとも 50 分間（違反発生なしの場合で 5 分間を 10 回）、FP でフィルタリングされます。ケーブル オペレータは既存の ARP フィルタ CLI ツールを利用し、エンドユーザに連絡してCPEに必要なウイルス対策ソフトウェアのインストールまたはファームウェアのアップグレードを要求するために十分なモデムおよびCPEの情報を入手できます。

（注） 違反しているデバイスが「修復」されないか停止している場合、FP ARP フィルタに無期限で残ります。

FP ARP レート リミッタは、最大 16,000 人の ARP 違反者をフィルタリングするように設計されています。この 16,000 のフィルタリング可能なエンティティのプールが枯渇すると、エンティティは RP でフィルタリングされます。CLI 統計は、RP と FP でフィルタリングされた MAC アドレスを区別します。

MAC アドレスのハッシュ衝突が発生する可能性があるため、FP ARP レート リミッタにプログラミングできない ARP 違反者は、SID によって FP でフィルタリングされます。送信元 MAC アドレスおよび SID でハッシュが実行されるため、関連付けられたモデムを削除して新しい SID でオンラインに戻すことにより、実際にはこのようなデバイスを MAC アドレス フィルタリングに戻すことができます（このような状況はほとんど可能性がないため、一般的なプラクティスであるとは言えません）。

モデムまたはCPEとしてのCMTSで送信元MACアドレスが「既知」ではないARPパケットは、その SID によって FP でフィルタリングされます。したがって、FP でフィルタリングされない異常な ARP パケット送信元は存在しません。動作コードが無効な偽の ARP パケットは、ARP 応答であるかのようにフィルタリングされます。

ケーブル ARP フィルタリングの設定方法

ARP フィルタリングが必要かどうかを判別し、1 つまたは複数のケーブル インターフェイスで ARP フィルタリングを設定するには、次の手順を使用します。

ARP 処理のモニタリング

ルータがARPトラフィックをどのように処理するかと、ARPパケットのボリュームに潜在的な問題があるかどうかをモニタするには、次の手順を使用します。

手順

ステップ 1 最も頻繁に実行される CPU 処理を見つけるには、**showprocesscpusorted** コマンドを使用して ARP Input プロセスを探します。

例：

```
Router# show process cpu sorted

CPU utilization for five seconds: 99%/28%; one minute: 93%; five minutes: 90%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
  19   139857888  44879804       3116 31.44% 28.84% 28.47%   0 ARP Input
 154    74300964  49856254       1490 20.29% 19.46% 15.78%   0 SNMP ENGINE
  91    70251936   1070352      65635  8.92%  9.62%  9.59%   0 CEF process
  56    17413012  97415887        178  3.01%  3.67%  3.28%   0 C10K BPE IP Enqu
  78    24985008  44343708        563  3.68%  3.47%  3.24%   0 IP Input
  54     6075792   6577800        923  0.90%  0.67%  0.65%   0 CMTS SID mgmt ta
...
```

この例では、ARP Input プロセスが 5 秒前に CPU の 31.44 パーセントを使用しています。CPU 使用率合計は 99 パーセントで、ルータに大きな問題があることを示しています。

（注） 一般的な規則として、ARP Input プロセスが使用するのは、通常動作時の CPU 処理時間の 1 パーセント未満である必要があります。ARP Input プロセスは、数千個のケーブルモデムを同時に登録する場合など、特定の状況下で処理時間が長くなる可能性がありますが、通常動作時に処理時間の 1 パーセント以上を使用する場合は、問題がある可能性があります。

ステップ 2 ARP プロセスのみをモニタリングするには、**showprocesscpu|includeARP** コマンドを使用します。

例：

```
Router# show process cpu | include ARP

  19   139857888  44879804       3116 31.44% 28.84% 28.47%   0 ARP Input
 110           0         1          0  0.00%  0.00%  0.00%   0 RARP Input
```

ステップ 3 処理される ARP パケットの数をモニタリングするには、**showiptraffic** コマンドを使用します。

例：

```
Router# show ip traffic | begin ARP

ARP statistics:
  Rcvd: 11241074 requests, 390880354 replies, 0 reverse, 0 other
  Sent: 22075062 requests, 10047583 replies (2127731 proxy), 0 reverse
```

ARP トラフィックの増加速度を確認するには、このコマンドを繰り返します。

ステップ 4 ARP トラフィックが過剰に見える場合は、**showcablearp-filter** コマンドを使用して各ケーブル インターフェイスの ARP トラフィックを表示し、大量のトラフィックを生成しているインターフェイスを特定します。

例：

```
Router# show cable arp-filter Cable5/0/0

ARP Filter statistics for Cable5/0/0:
  Rcvd Replies: 177387 total, 0 unfiltered, 0 filtered
  Sent Requests For IP: 68625 total, 0 unfiltered, 0 filtered
  Sent Requests Proxied: 7969175 total, 0 unfiltered, 0 filtered
```

上記の例では、フィルタリングされていないカウンタとフィルタリングされたカウンタにゼロと表示されており、ARP フィルタリングがケーブルインターフェイスでイネーブルになっていないことを示しています。ARP フィルタリングを **cablearpfilter** コマンドで有効にした後、**servicedivert-rate-limit** コマンド（主な ARP トラフィックの送信元の特定, （1483 ページ）を参照）を使用して、過剰な ARP トラフィックを生成している特定のデバイスを識別できます。

ARP フィルタリングの有効化

特定のケーブルインターフェイスで ARP フィルタリングをイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**interfacecable** *x/y* 例： `Router(config)# interface cable 5/1`	指定したケーブル インターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**cablearpfilter reply-accept** *number window-size* 例： `Router(config-if)# cable arp filter reply-accept 2 2`	ケーブル インターフェイス上のアクティブな各サービス ID（SID）で *window-size* 秒ごとに指定した数の ARP 応答パケットのみを受け入れるようにケーブルインターフェイスを設定します。ケーブルインターフェイスは、SID ごとにこの数を超える ARP 応答パケットをドロップします。（デフォルトの動作は、すべての ARP 応答パケットを受け入れます。）

	コマンドまたはアクション	目的
ステップ 5	**cablearpfilter request-send** *number window-size* 例： `Router(config-if)# cable arp filter request-send 3 1`	ケーブル インターフェイス上のアクティブな各 SID で *window-size* 秒ごとに指定した数の ARP 要求パケットのみを送信するようにケーブル インターフェイスを設定します。ケーブル インターフェイスは、SID ごとにこの数を超える ARP 要求をドロップします。（デフォルトの動作は、すべての ARP 要求パケットを送信します。） （注） 他のケーブル インターフェイスで ARP フィルタリングをイネーブルにするには、ステップ 3 ～ 5 を繰り返します。ケーブル バンドル内のマスターとスレーブのインターフェイスは個別に設定する必要があります。
ステップ 6	**end** 例： `Router(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

主な ARP トラフィックの送信元の特定

ケーブル インターフェイスで ARP トラフィックのフィルタリングを開始したら、多量の ARP トラフィックを生成または転送するケーブルモデムまたはCPEデバイスを特定するために、次の手順を使用します。

ヒント Linksys 無線 B ブロードバンド ルータ（モデル番号 BEFW11S4 バージョン 4、1.44.2 ファームウェア付き）には、受信したすべての ARP 要求パケットに対して ARP 応答を誤って生成する既知の問題があります。この問題の解決方法については、「Linksys 無線ブロードバンド ルータ（BEFW11S4）」のガイドを参照してください。

手順

ステップ 1 特定のケーブルインターフェイスで、指定した最小数のパケットよりも多くの ARP 要求を生成または転送するデバイスを検出するには、**showcablearp-filterrequests-filtered** コマンドを使用します。ここで、*number* は生成されるパケット数のしきい値です。

例：

show cable arp-filter cable *interface* **requests-filtered** *number*

たとえば、100 以上の ARP 要求パケットを生成したデバイスを表示するには、次のコマンドを入力します。

例：

```
Router# show cable arp-filter cable 5/1/0 requests-filtered 100

Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
1    0006.2854.72d7 10.3.81.4       12407          0                    0
81   00C0.c726.6b14 10.3.81.31      743            0                    0
```

ステップ 2 デバイスが ARP パケットをどれだけ素早く生成するかを表示するには、 **show cable arp-filter** コマンドを繰り返し実行します。

ステップ 3 特定のケーブルインターフェイスで、指定した最小数のパケットよりも多くの ARP 応答を生成または転送するデバイスを検出するには、**showcablearp-filterreplies-filtered** コマンドを使用します。ここで、*number* は生成されるパケット数のしきい値です。

例：

show cable arp-filter cable *interface* **requests-filtered** *number*

たとえば、200 以上の ARP 応答パケットを生成したデバイスを表示するには、次のコマンドを入力します。

例：

```
Router# show cable arp-filter cable 5/0/0 replies-filtered 200


Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
2    0006.53b6.562f 10.11.81.16      0             0                    2358
191  0100.f31c.990a 10.11.81.6       0             0                    11290
```

ステップ 4 （任意）特定のケーブル モデムが過剰な ARP 応答を生成または転送する場合は、Linksys 無線 B ブロードバンド ルータ（モデル番号 BEFW11S4）を使用しているかを確認します。使用している場合は、このルータが誤って過剰な ARP パケットを生成する古いファームウェアを実行している可能性があり、このファームウェアをアップグレードする必要があります。詳細については、「Linksys 無線ブロードバンド ルータ（BEFW11S4）」のガイドを参照してください。

ステップ 5 デバイスが ARP パケットをどれだけ素早く生成するかを表示するには、各フィルタ期間（**cablearpfilter** コマンドで入力した時間）でこのコマンドを繰り返し実行します。

ステップ 6 （任意）ARP 応答と要求パケットのカウンタは 16 ビット カウンタであるため、非常に大量のパケットがインターフェイスで生成されると、このカウンタは数時間または数分でゼロにラップ アラウンドする場合があります。ARP のカウンタをクリアすると、表示から古い情報を削除し、ARP トラフィックでネットワークの問題が現在発生していると考えられる場合に最悪の攻撃者を簡単に確認できます。

ARP フィルタを現在トリガーしていないモデムを除外し、最悪の攻撃者を分離するには、**clearcounterscable** インターフェイス コマンドを使用してすべてのインターフェイス カウンタをゼロにリセットします。その後、**showcablearp-filter** コマンドを実行すると、ほとんどの ARP トラフィックを現在転送しているモデムの SID を明確に識別できます。

たとえば次の例では、多くのモデムが、ARPパケットフィルタを起動するのに十分な大量のARPトラフィックを転送していることを示しています。

例：

```
Router# show cable arp-filter cable 5/1/0 requests-filtered 10

Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
1    0006.2854.72d7 10.3.81.4       8              0                    0
23   0007.0e02.b747 10.3.81.31      32             0                    0
57   0007.0e03.2c51 10.3.81.31      12407          0                    0
...
81   00C0.c726.6b14 10.3.81.31      23             0                    0
```

SID 57 のパケット数は最大ですが、このモデムが現在問題を引き起こしているのかはすぐには分かりません。カウンタをクリアすると、最悪の攻撃者は簡単に判明します。

例：

```
Router# clear counter cable 5/1/0

Clear show interface counters on this interface [confirm] y

08:17:53.968: %CLEAR-5-COUNTERS: Clear counter on interface Cable5/1/0 by console
Router# show cable arp cable 5/1/0

ARP Filter statistics for Cable3/0:
  Replies Rcvd: 0 total. 0 unfiltered, 0 filtered
  Requests Sent For IP: 0 total. 0 unfiltered, 0 filtered
  Requests Forwarded: 0 total. 0 unfiltered, 0 filtered

Router# show cable arp-filter cable 5/1/0 requests-filtered 10

Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
Router# show cable arp-filter cable 5/1/0 requests-filtered 10

Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
57   0007.0e03.2c51 10.3.81.31      20             0                    0
81   00C0.c726.6b14 10.3.81.31      12             0                    0
Router# show cable arp-filter cable 5/1/0 requests-filtered 10

Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
57   0007.0e03.2c51 10.3.81.31      31             0                    0
81   00C0.c726.6b14 10.3.81.31      18             0                    0
```

ステップ 7 （任意）Req-For-IP-Filtered 列に大部分の ARP パケットがある場合は、**showcablearp-filterip-requests-filtered** コマンドを使用して、このトラフィックを生成している CPE デバイスの詳細を表示します。その後、**debugcablemac-address** and **debugcablearpfilter** コマンドを使用して、この特定のトラフィックに関する詳細情報を表示します。たとえば、

例：

```
Router# show cable arp-filter c5/0/0 ip-requests-filtered 100

Sid  MAC Address    IP Address      Req-Filtered Req-For-IP-Filtered Rep-Filtered
1    0007.0e03.1f59 50.3.81.3       0            37282               0
Router# debug cable mac-address 0007.0e03.1f59

Router# debug cable arp filter
```

```
Router#
Apr 23 23:03:23.565: ARP for IP Filter=F sid 1 s 0000.0000.0049 d 0005.00e5.3610 sip
50.3.81.13 dip 50.3.82.173 prot 6 len 46 SrcP 445 DstP 445
Apr 23 23:03:23.565: ARP for IP Filter=F sid 1 s 0000.0000.0049 d 0005.00e5.3610 sip
50.3.81.13 dip 50.3.82.174 prot 6 len 46 SrcP 445 DstP 445
Apr 23 23:03:23.565: ARP for IP Filter=F sid 1 s 0000.0000.0049 d 0005.00e5.3610 sip
50.3.81.13 dip 50.3.82.175 prot 6 len 46 SrcP 445 DstP 445
[additional output omitted]...
```

この例では、IP アドレス 50.3.81.13 の CPE デバイスが、TCP ポート 445 のサブネット 50.3.82.0 のすべての IP アドレスにパケットを送信し、Microsoft Windows ファイル共有に対応したコンピュータを検索しようとしている可能性があります。

ステップ 8 過剰な ARP を生成する特定のデバイスが判別したら、問題を修正するために、会社のサービス レベル契約（SLA）で許可されたあらゆる対策を実行することができます。

例

この例では、C5/0/0 と C7/0/0 の 2 つのインターフェイスが同じバンドルに結合されています。これは、このインターフェイスが同じブロードキャスト トラフィックを共有することを意味しています。各インターフェイスのそれぞれのデバイスが、過度な ARP トラフィックを生成します。

- インターフェイス C7/0/0 の MAC アドレス 000C.2854.72D7 のデバイスは、大量の ARP 要求を生成または転送します。通常、このデバイスは、モデム内の CPE デバイスによって生成された ARP 要求を転送するケーブル モデムです。CPE デバイスは、サービスの窃盗またはサービス妨害攻撃を試したり、自身がウイルスに感染して、ウィルス感染できる他のコンピュータを探したりできます。
- ケーブル 5/0/0 の MAC アドレス 000C.53B6.562F にあるデバイスは、大量の ARP 要求に応答しています。これは、不具合のあるソフトウェアを実行しているルータであることを示している可能性があります。

次のコマンドにより、過度な ARP 要求を生成するインターフェイス C7/0/0 のデバイスが特定されます。

```
Router# show cable arp-filter c7/0/0

ARP Filter statistics for Cable7/0/0:
  Replies Rcvd: 3 total. 3 unfiltered, 0 filtered
  Requests Sent For IP: 0 total. 0 unfiltered, 0 filtered
  Requests Forwarded: 27906 total. 562 unfiltered, 27344 filtered
Router# show cable arp-filter c7/0/0 requests-filtered 100

Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
1    000C.2854.72d7 50.3.81.4       62974          0                    0
```

次のコマンドにより、過度な ARP 応答を生成するインターフェイス C5/0/0 のデバイスが特定されます。

```
Router# show cable arp-filter c5/0/0

ARP Filter statistics for Cable5/0/0:
```

```
  Replies Rcvd: 2400 total. 456 unfiltered, 1944 filtered
  Requests Sent For IP: 0 total. 0 unfiltered, 0 filtered
  Requests Forwarded: 26 total. 26 unfiltered, 0 filtered
Router# show cable arp-filter c5/0/0 replies-filtered 100

Sid  MAC Address    IP Address      Req-Filtered   Req-For-IP-Filtered  Rep-Filtered
2    000C.53b6.562f 50.3.81.6       0              0                    2097
```

パケット カウンタのクリア

インターフェイスのパケット カウンタ（ARP パケット カウンタを含む）をクリアするには、**clearcounterscable** インターフェイス コマンドを使用します。また、オプションを指定せずに **clearcounters** コマンドを使用することで、すべてのインターフェイスのパケット カウンタをクリアできます。これにより、**showcablearp** コマンドを使用して、非常に多くのトラフィックを現在生成している CPE デバイスのみを表示できます。

（注） **clearcounters** コマンドは、ARP パケット カウンタだけでなく、インターフェイスのすべてのパケット カウンタをクリアします。

FP での ARP 違反者の特定

FP ARP フィルタ機能が有効な状態で、**showcablearp-filter** *interface* コマンドを使用して、ARP 違反者のリストを生成します。

FP における cBR-8 の出力

FP ARP フィルタ機能を有効にすると、cBR-8 出力形式にはモデムと CPE アドレス、および次の列が 1 行で表示されます。

- M/S：この列には、パケットが MAC アドレスと SID のどちらでフィルタ処理されているのかが示されます。これらの列の大部分には MAC アドレスが表示されます。
- Rate：この列には、最後の 5 分間のモニタリング タイム ウィンドウで、FP フィルタ処理されたパケットのパケット レートが示されます。Rate は RP フィルタ処理されたパケットに対して計算されません。
- Pro：この列では、フィルタ処理を実行したプロセッサを「RP」または「FP」で識別します。cBR-8 では、[Pro] フィールドの 99.9% で「FP」と示されることが予想されます。

次は FP における cBR-8 での ARP 要求の出力例です。

```
Router# show cable arp-filter Bundle1 requests-filtered 40
Interface Cable5/0/0 - none
Interface Cable6/0/2
Sid  CPE Mac        CPE IP          Modem MAC      Modem IP        M/S Rate Pro REQS
4    00d0.b75a.822a 50.3.81.56      0007.0e03.9cad 50.3.81.15      MAC -    RP  46
4    00d0.b75a.822a 50.3.81.56      0007.0e03.9cad 50.3.81.15      MAC 25   FP  5012
5    00b0.d07c.e51d 50.3.81.57      0007.0e03.1f59 50.3.81.13      MAC -    RP  64000
6    -              -               0006.2854.7347 50.3.81.4       MAC 101  FP  5122
```

```
7    -              -              0006.2854.72d7 50.3.81.11      SID -    FP  961205
Interface Cable7/0/0 - none
```

この出力例では、次の内容について説明します。

- SID 4 は、FP でフィルタ処理された CPE を示します。指定されたしきい値は、違反者が特定されたときに RP でフィルタ処理されていたパケットを示すのに十分低い値です。しきい値が十分高くなると、RP でフィルタ処理されたパケットを示さなくなります。FP でフィルタ処理されたパケットの場合は、ARP パケット レート 25 が示されます。
- SID 5 は、RP でフィルタ処理された CPE を示します。これは非常にまれであり、FP フィルタ処理可能なエンティティの最大数に達した場合のみ発生します。
- SID 6 は、FP においてフィルタ処理されたモデムを示します（CPE MAC または CPE IP は示されていません）。
- SID 7 は、FP の SID でフィルタ処理された、「不明」な送信元 MAC アドレスからの ARP パケットを示します。

行が簡潔で 90 文字未満になるように、要求数、応答数、IP 要求数は 1 行で表示されなくなりました。

ARP 応答時には [REQs] 列が表示されます。この列は、IP の ARP 要求が含まれる場合は [REQ-IP] と表示されます。

侵害する IP パケットのせいで CMTS によって送信される要求「ip-requests-filtered」は、IP ベースのスキャン トラフィックを阻止するためのアクセス コントロール リスト（ACL）とこのようなトラフィックのプント レートを減少させるために使用される cBR-8 のプント レート制限機能とを併用して、引き続き FP ではなく RP でフィルタ処理されます。ARP フィルタは、引き続きこれらの IP トラフィック ストリーム分析を実行するために使用できます。

ケーブル ARP フィルタリングの設定例

ここでは、ケーブル ARP フィルタリング機能を設定する方法について説明します。

個別のケーブル インターフェイスの ARP フィルタ設定例

次に、ケーブル ARP フィルタリング機能用に設定されたケーブル インターフェイスの一般的な設定例を示します。

```
!
interface Cable5/0/0
 ip address 192.168.100.1 255.255.255.0 secondary
 ip address 192.168.110.13 255.255.255.0
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream channel-id 0
 cable upstream 0 frequency 6000000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 3200000 200000
 cable upstream 0 minislot-size 16
 cable upstream 0 modulation-profile 6 7
 no cable upstream 0 shutdown
 cable upstream 1 frequency 26000000
```

```
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000 200000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 6 7
 no cable upstream 1 shutdown
 cable upstream 2 frequency 15008000
 cable upstream 2 power-level 0
 cable upstream 2 channel-width 3200000 200000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 6 7
 cable upstream 2 shutdown
 cable upstream 3 spectrum-group 25
 cable upstream 3 channel-width 3200000 200000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 1
 cable upstream 3 shutdown
 cable upstream 4 frequency 21008000
 cable upstream 4 power-level 0
 cable upstream 4 channel-width 3200000 200000
 cable upstream 4 minislot-size 16
 cable upstream 4 modulation-profile 1
 no cable upstream 4 shutdown
 cable upstream 5 spectrum-group 25
 cable upstream 5 channel-width 3200000 200000
 cable upstream 5 minislot-size 4
 cable upstream 5 modulation-profile 1
 cable upstream 5 shutdown
 cable arp filter request-send 4 2
 cable arp filter reply-accept 4 2
end
```

バンドル ケーブル インターフェイスの ARP フィルタ設定例

次に、ケーブル ARP フィルタリング機能も使用するケーブル インターフェイス バンドルの一般的な設定例を示します。マスターとスレーブの両方のインターフェイスを個別に設定すると、機能を必要とする特定のインターフェイスに対してのみ設定できます。また、さまざまなしきい値を使用して機能を設定すると、各インターフェイスのトラフィック パターンに対応するように機能をカスタマイズすることができます。

```
!
interface Cable5/0/0
 description Master cable interface
 ip address 10.3.130.1 255.255.255.0 secondary
 ip address 10.3.131.1 255.255.255.0 secondary
 ip address 10.3.132.1 255.255.255.0 secondary
 ip address 10.3.133.1 255.255.255.0 secondary
 ip address 10.3.81.1 255.255.255.0
 ip helper-address 10.14.0.4
 load-interval 30
 cable bundle 1 master
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 441000000
 cable downstream channel-id 0
 cable upstream 0 frequency 5008000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 modulation-profile 1
 no cable upstream 0 shutdown
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 1
 cable upstream 1 shutdown
 cable upstream 2 channel-width 1600000
 cable upstream 2 minislot-size 4
```

```
 cable upstream 2 modulation-profile 1
 cable upstream 2 shutdown
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 1
 cable upstream 3 shutdown
 cable arp filter request-send 4 2
 cable arp filter reply-accept 4 2
!
interface Cable7/0/0
 description Slave cable interface--Master is C5/0/0
 no ip address
 cable bundle 1
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 562000000
 cable downstream channel-id 0
 no cable downstream rf-shutdown
 cable upstream 0 connector 0
 cable upstream 0 frequency 5008000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 modulation-profile 21
 no cable upstream 0 shutdown
 cable upstream 1 connector 1
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 21
 cable upstream 1 shutdown
 cable upstream 2 connector 2
 cable upstream 2 channel-width 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 21
 cable upstream 2 shutdown
 cable upstream 3 connector 3
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 21
 cable upstream 3 shutdown
 cable arp filter request-send 20 5
 cable arp filter reply-accept 20 5
end
```

FP のデフォルト設定での ARP フィルタリング例

次に、FP 機能で ARP フィルタリングに対応する ケーブル インターフェイスのデフォルト設定の例を示します。

```
interface Bundle1
 cable arp filter request-send 3 2
 cable arp filter reply-accept 3 2
end
```

その他の参考資料

ここでは、ケーブル ARP フィルタリング機能に関する参考資料について説明します。

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html
送信元ベースのレート制限	http://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b_cmts_sec_and_cable_mon_features_cbr/source-based_rate_limit.html
show platform hardware qfp active infrastructure punt summary コマンド	http://www.cisco.com/c/en/us/td/docs/cable/cmts/cmd_ref/b_cmts_cable_cmd_ref/b_cmts_cable_cmd_ref_chapter_010100.html

ケーブル ARP フィルタリングに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *217*：ケーブル *ARP* フィルタリング機能に関する機能情報

機能名	リリース	機能情報
ケーブル ARP フィルタリング	Cisco IOS XE Everest 16.6.1	この機能は、 Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 88 章

DOCSIS 2.0 用サブスクライバ管理パケット フィルタリング拡張

Cisco コンバージド ブロードバンド ルータは、加入者の優先度や基準に基づくデータ パケット フィルタリングの管理をサポートします。パケット フィルタリングは、特定のパケットのみを顧客宅内機器（CPE）に流しながら、ケーブル ネットワークの不要なデータ パケットをドロップすることで、ケーブル ネットワークに対するセキュリティを強化します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

• サブスクライバ管理パケット フィルタリングに関する機能情報，1500 ページ

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *218*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

サブスクライバ管理パケット フィルタリングの設定の前提条件

サブスクライバ管理パケット フィルタリング機能のソフトウェア要件は次のとおりです。

- 最新のソフトウェアイメージがロードされ、ケーブルモデム終端システム（CMTS）とケーブル モデム（CM）で動作している。
- メインスーパーバイザ（SUP）とスタンバイSUPの設定情報が、スイッチオーバー前には同じである。

サブスクライバ管理パケットフィルタリングの設定に関する制限事項

- この機能は最大254のフィルタリング グループを定義できます。各グループ内のフィルタの数は 255 です。

サブスクライバ管理パケット フィルタリングの設定に関する情報

フィルタ グループは、特定の CM または CPE デバイスごとに発着信するパケットに適用されるフィルタを指定します。これは、パケットをフィルタ処理またはドロップするルールや基準を定義します。フィルタ処理する必要がある各パケットは、送信が許可されるか、ドロップ対象としてフィルタ処理されます。パケットをフィルタ処理する基準は、加入者の設定によって異なります。フィルタ グループは、さまざまなサブスクライバ管理グループに適用できます。

ケーブル サブスクライバ管理は、次の設定方法を使用して確立することができます。

- CMTS ルータ設定（CLI 経由）
- SNMP コンフィギュレーション

サブスクライバ管理パケット フィルタリングを設定するプロセスは次のとおりです。

1. パケット フィルタ グループは、パケットに対するアクションを定義します。パケットは、加入者のパケット基準に基づいて、CPE に送信できるか、またはケーブル ネットワークからドロップされます。
2. CM は、CMTS に登録要求を送信します。登録要求にはプロビジョニング情報が含まれます。プロビジョニング情報は、パケット フィルタリング グループ（PFG）と CM および CM の加入者との関連付けを定義します。
3. CM、CPE、組み込み型マルチメディア ターミナル アダプタ（eMTA）、組み込み型セットトップ ボックス（eSTB）、および組み込み型ポータル サーバ（ePS）を特定の PFG に接続するために、特定のダウンストリームまたはアップストリーム PFG が使用されます。
4. CMTS は、CPE の DHCP 情報に基づいて CPE デバイスを特定します。

（注） CM で動作するフィルタ グループについては、CMTS ルータを設定してから、CM を再登録する必要があります。

サブスクライバ管理パケット フィルタリングの設定方法

ここでは、Cisco CMTS プラットフォームでのサブスクライバ パケット フィルタリングを管理するために実行する設定タスクについて説明します。コマンドライン インターフェイス（CLI）コマンドを使用して設定を完了できます。

フィルタ グループの設定

ここでは、パケット フィルタ グループの設定手順について説明します。設定を完了するには、次の手順の概要に従ってください。

TCP/IP および UDP/IP ヘッダーに基づいてパケットをフィルタリングする DOCSIS フィルタ グループを作成、設定、有効化にするには、グローバル コンフィギュレーション モードでケーブル フィルタ グループ コマンドを使用します。

手順

	コマンドまたはアクション	目的

ステップ 1	**enable**
	例：
	`Router> enable`
	例：
	`Router#`
		特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

ステップ 2	**configure terminal**
	例：
	`Router# configure terminal`
	例：
	`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	**cablefiltergroupgroup-idindexindex-num[optionoption-value]** 例： `Router(config)# cable filter group 10 index 10 src-ip 10.7.7.7`	パケットをフィルタリングする DOCSIS フィルタ グループを作成、設定、および有効化します。

アップストリームとダウンストリーム MTA フィルタ グループの定義

ここでは、組み込み型マルチメディア ターミナル アダプタ（eMTA）のアップストリームとダウンストリームのサブスクライバ管理フィルタ グループを定義する設定タスクについて説明します。設定を完了するには、次の手順の概要に従ってください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 submgmt default filter-group mta {downstream | upstream} group-id 例： `Router(config)# cable submgmt default filter-group mta downstream 130`	MTA のアップストリームとダウンストリームのサブスクライバ管理フィルタ グループを定義します。

アップストリームとダウンストリーム STB フィルタ グループの定義

ここでは、セットトップ ボックス（STB）のアップストリームとダウンストリームのサブスクライバ管理フィルタ グループを定義する設定タスクについて説明します。設定を完了するには、次の手順の概要に従ってください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 submgmt default filter-group stb {downstream | upstream} group-id 例： `Router(config)# cable submgmt default filter-group stb downstream 20`	STB のアップストリームとダウンストリームのサブスクライバ管理フィルタ グループを定義します。

アップストリームとダウンストリーム PS フィルタ グループの定義

ここでは、ポータル サーバ（PS）のアップストリームとダウンストリームのサブスクライバ管理フィルタ グループを定義する設定タスクについて説明します。設定を完了するには、次の手順の概要に従ってください。

手順

	コマンドまたはアクション	目的

ステップ 1	**enable**
	
	例：
	`Router> enable`
	
	例：
	`Router#`
		特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

ステップ 2	**configure terminal**
	
	例：
	`Router# configure terminal`
	
	例：
	`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。

	コマンドまたはアクション	目的
ステップ 3	cable submgmt default filter-group ps {downstream | upstream} group-id 例： `Router(config)# cable submgmt default filter-group ps downstream 10`	ポータル サーバ のアップストリームとダウンストリームのサブスクライバ管理フィルタ グループを定義します。

サブスクライバ管理パケット フィルタリングの設定例

このセクションでは、サブスクライバ管理パケット フィルタリングを構成するための設定例を説明します。

フィルタ グループの設定例

次に、送信元 IP アドレス（10.7.7.7）と宛先 IP アドレス（10.8.8.8）のパケットと、送信元ポート番号（2000）と宛先ポート番号（3000）のパケットをドロップするフィルタ グループの設定例を示します。すべてのプロトコル タイプおよび ToS と TCP フラグの値が一致します。

```
Router(config)# cable filter group 10 index 10 src-ip 10.7.7.7
Router(config)# cable filter group 10 index 10 src-mask 255.255.0.0
Router(config)# cable filter group 10 index 10 dest-ip 10.8.8.8
Router(config)# cable filter group 10 index 10 dest-mask 255.255.0.0
Router(config)# cable filter group 10 index 10 ip-proto 256
Router(config)# cable filter group 10 index 10 src-port 2000
Router(config)# cable filter group 10 index 10 dest-port 3000
Router(config)# cable filter group 10 index 10 tcp-flags 0 0
Router(config)# cable filter group 10 index 10 match-action drop
```

アップストリームとダウンストリーム MTA フィルタ グループの定義例

次に、アップストリームとダウンストリームの MTA フィルタ グループの設定例を示します。

```
Router# configure terminal
Router(config)# cable submgmt default filter-group mta downstream 10
```

アップストリームとダウンストリーム STB フィルタ グループの定義例

次に、アップストリームとダウンストリームの STB フィルタ グループの設定例を示します。

```
Router#configure terminal
Router(config)#cable submgmt default filter-group stb downstream 20
```

アップストリームとダウンストリーム PS フィルタ グループの定義例

次に、アップストリームとダウンストリームのポータル サーバ フィルタ グループの設定例を示します。

```
Router#configure terminal
Router(config)#cable submgmt default filter-group ps downstream 10
```

その他の参考資料

ここでは、サブスクライバ管理パケット フィルタリング機能の設定に関する関連資料を示します。

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

サブスクライバ管理パケット フィルタリングに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *219*：サブスクライバ管理パケット フィルタリングに関する機能情報

機能名	リリース	機能情報
サブスクライバ管理パケット フィルタリング	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました

第 89 章

MAC フィルタリング

この機能により、バックホール インターフェイスでの MAC アドレス フィルタを有効/無効にすることができます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *220* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

MAC フィルタリングについて

この機能を使用すると、ルータ インターフェイスの MAC アドレスが宛先 MAC アドレスとして設定されているパケットだけを転送できます。インターフェイスごとに32個のユニキャスト フィルタ エントリがサポートされます。この機能はデフォルトではディセーブルになっています。

（注） port-channel が有効になっている場合、バックホール インターフェイスで MAC フィルタリングを有効にする必要があります。

（注） バックホール インターフェイスで dot1q l2vpn と MAC フィルタリングの両方が有効になっている場合は、バックホール インターフェイスごとに 1 つのユニキャスト フィルタ エントリだけがサポートされます。MAC フィルタリングは、非 l2vpn ユニキャスト パケットに関してのみサポートされます。

MAC フィルタリングの設定方法

ここでは、MACフィルタリングを管理するために行う設定タスクについて説明します。コマンドライン インターフェイス（CLI）コマンドを使用して設定を完了できます。

MAC フィルタリングの設定

MAC フィルタリングを設定するには、以下の手順に従います。

enable
configure terminal
interface tenGigabitEthernet *slot/subslot/port*
mac-addr-filter
end

MAC フィルタリングの確認

バックホール インターフェイス上の MAC フィルタリング設定を確認するには、次に示すように **show running-config interface** コマンドを使用します。

```
Router# show running-config interface tenGigabitEthernet 4/1/0
Building configuration...

Current configuration : 73 bytes
!
interface TenGigabitEthernet4/1/0
 no ip address
 mac-addr-filter
end
```

特定の SUP スロットと SUP-PIC ベイでの MAC フィルタリングのステータスを確認するには、次に示すように **show platform software iomd** コマンドを使用します。

```
Router# show platform software iomd 4/4 mac-filter
IOMD (Input Output Module Driver) Mac Filter Status


port: 0     promiscuous mode:     unicast:  enable   multicast:  enable      broadcast:
enable
            Input Drop cnt:                       0      Total Drop cnt:
```

```
    0
            Entry Number:   1
    Index      Mode    Action            Entry MAC           Entry MASK             Match
Count
       00    enable      pass    c4:14:3c:16:7c:04    ff:ff:ff:ff:ff:ff
    0


port: 1     promiscuous mode:     unicast:  enable   multicast:  enable      broadcast:
enable
            Input Drop cnt:                     0      Total Drop cnt:
    0
            Entry Number:   1
    Index      Mode    Action            Entry MAC           Entry MASK             Match
Count
       00    enable      pass    c4:14:3c:16:7c:05    ff:ff:ff:ff:ff:ff
 1729


port: 2     promiscuous mode:     unicast:  enable   multicast:  enable      broadcast:
enable
            Input Drop cnt:                     0      Total Drop cnt:
    0
            Entry Number:   1
    Index      Mode    Action            Entry MAC           Entry MASK             Match
Count
       00    enable      pass    c4:14:3c:16:7c:06    ff:ff:ff:ff:ff:ff
    0


port: 3     promiscuous mode:     unicast:  enable   multicast:  enable      broadcast:
enable
            Input Drop cnt:                     0      Total Drop cnt:
    0
            Entry Number:   1
    Index      Mode    Action            Entry MAC           Entry MASK             Match
Count
       00    enable      pass    c4:14:3c:16:7c:07    ff:ff:ff:ff:ff:ff
    0


port: 4     promiscuous mode:     unicast:  enable   multicast:  enable      broadcast:
enable
            Input Drop cnt:                     0      Total Drop cnt:
    0
            Entry Number:   1
    Index      Mode    Action            Entry MAC           Entry MASK             Match
Count
       00    enable      pass    c4:14:3c:16:7c:08    ff:ff:ff:ff:ff:ff
    0


port: 5     promiscuous mode:     unicast:  enable   multicast:  enable      broadcast:
enable
            Input Drop cnt:                     0      Total Drop cnt:
    0
            Entry Number:   1
    Index      Mode    Action            Entry MAC           Entry MASK             Match
Count
       00    enable      pass    c4:14:3c:16:7c:09    ff:ff:ff:ff:ff:ff
   15


port: 6     promiscuous mode:     unicast:  enable   multicast:  enable      broadcast:
enable
            Input Drop cnt:                     0      Total Drop cnt:
    0
            Entry Number:   1
    Index      Mode    Action            Entry MAC           Entry MASK             Match
Count
       00    enable      pass    c4:14:3c:16:7c:0a    ff:ff:ff:ff:ff:ff
    0
```

```
port: 7     promiscuous mode:     unicast:  enable   multicast:  enable      broadcast:
enable
            Input Drop cnt:                      0      Total Drop cnt:
    0
            Entry Number:   1
    Index      Mode    Action            Entry MAC           Entry MASK             Match
Count
       00    enable      pass    c4:14:3c:16:7c:0b    ff:ff:ff:ff:ff:ff
    0
```

MAC フィルタリングが無効になっている場合、**show platform software iomd** コマンドの出力は次のようになります。

```
Router# show platform software iomd 4/5 mac-filter
IOMD (Input Output Module Driver) MAC filter Status


port: 0     promiscuous mode:     unicast:  enable   multicast:  enable      broadcast:
enable
            Input Drop cnt:                      0      Total Drop cnt:
    0
            Entry Number:   0

port: 1     promiscuous mode:     unicast:  enable   multicast:  enable      broadcast:
enable
            Input Drop cnt:                      0      Total Drop cnt:
    0
            Entry Number:   0

port: 2     promiscuous mode:     unicast:  enable   multicast:  enable      broadcast:
enable
            Input Drop cnt:                      0      Total Drop cnt:
    0
            Entry Number:   0

port: 3     promiscuous mode:     unicast:  enable   multicast:  enable      broadcast:
enable
            Input Drop cnt:                      0      Total Drop cnt:
    0
            Entry Number:   0

port: 4     promiscuous mode:     unicast:  enable   multicast:  enable      broadcast:
enable
            Input Drop cnt:                      0      Total Drop cnt:
    0
            Entry Number:   0

port: 5     promiscuous mode:     unicast:  enable   multicast:  enable      broadcast:
enable
            Input Drop cnt:                      0      Total Drop cnt:
    0
            Entry Number:   0

port: 6     promiscuous mode:     unicast:  enable   multicast:  enable      broadcast:
enable
            Input Drop cnt:                      0      Total Drop cnt:
    0
            Entry Number:   0

port: 7     promiscuous mode:     unicast:  enable   multicast:  enable      broadcast:
enable
            Input Drop cnt:                      0      Total Drop cnt:
    0
```

```
                    Entry Number:   0
```

MAC フィルタリングの設定例

ここでは、MAC フィルタリングを構成するための設定例を説明します。

```
router> enable
router# configure terminal
router(config)# interface tenGigabitEthernet 4/1/0
router(config-if)# mac-addr-filter
router(config-if)# end
```

MAC フィルタリングに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *221*：*MAC* フィルタリングに関する機能情報

機能名	リリース	機能情報
MAC フィルタリング	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 XII 部

トラブルシューティングおよびネットワーク管理構成

第 90 章

Call Home

Call Home は、選択したシスコ デバイスに関する予防的診断およびリアルタイム アラートを提供し、ネットワークの可用性および運用効率を向上させます。Smart Call Home は、Cisco cBR ルータ用 Cisco SMARTnet のセキュアな接続サービスです。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *222*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

Call Home の前提条件

- 受信者が受け取ったメッセージの送信元を判別できるように、連絡先の電子メールアドレス（Smart Call Home のフル登録では必須、Call Mode が匿名モードでイネーブルになっている場合は任意）、電話番号（任意）、住所情報（任意）を設定する必要があります。

（注） スマート ライセンスを有効にすることにより Smart Call Home をイネーブルにすると、連絡先の電子メール アドレスが不要になります。

- 少なくとも 1 つの宛先プロファイル（定義済みまたはユーザ定義）を設定する必要があります。設定された宛先プロファイルは、受信エンティティがポケットベル、E メール、または Cisco Smart Call Home などの自動サービスかどうかにより異なります。
  - 宛先プロファイルが E メール メッセージ送信を使用している場合、シンプル メール転送プロトコル（SMTP）サーバを指定する必要があります。
  - トラストプール機能はデフォルトでイネーブルに設定されているため、HTTPS サーバ接続でトラストプール認証局（CA）を設定する必要はありません。
- ルータは E メール サーバまたは宛先 HTTP（S）サーバに IP 接続されている必要があります。
- Cisco Smart Call Home サービスを使用する場合は、完全な Smart Call Home サービスを提供するために、デバイスを対象としたアクティブなサービス契約が必要です。

（注） アクティブなサービス契約は、シスコの Technical Assistance Center（TAC）を自動呼出しする場合など、完全な Smart Call Home サービスにのみ必要です。

Call Home の制約事項

- IP 接続機能がない場合、または宛先プロファイルに対する VRF のインターフェイスが停止している場合は、Smart Call Home メッセージを送信できません。
- Smart Call Home はあらゆる SMTP サーバで動作します。
- Smart Call Home に対して最大 5 つの SMTP サーバを設定できます。

Call Home の概要

Call Home 機能は、クリティカルなシステム イベントを E メールおよび Web 上で通知します。ポケットベル サービス、通常の電子メール、または XML ベースの自動解析アプリケーションとの

適切な互換性のために、さまざまなメッセージの形式が使用できます。この機能の一般的な使用方法としては、ネットワーク サポート技術者の直接ページング、ネットワーク オペレーション センターへの E メール通知、サポート Web サイトへの XML 送信、シスコの Technical Assistance Center（TAC）で事例を直接生成するための Cisco Smart Call Home サービスの使用などがあります。

Call Home 機能を使用すると、設定、環境条件、インベントリ、syslog、スナップショット、およびクラッシュ イベントについての情報を含むアラート メッセージを送信できます。

Call Home 機能では、*Call Home* 宛先プロファイルに従って複数の受信者にアラートを送信できます。宛先プロファイルには、メッセージ形式とコンテンツのカテゴリを設定できます。定義済みの宛先プロファイル（CiscoTAC-1）が提供されており、独自の宛先プロファイルを定義することもできます。CiscoTAC-1 プロファイルを使用して、Cisco TAC へのサービス要求の作成に使用できる Smart Call Home サービスのバック エンド サーバにアラートを送信します。Cisco TAC は、デバイスに提供される Smart Call Home サービス サポートおよびアラートの重大度に依存します。

柔軟なメッセージの配信オプションとフォーマット オプションにより、個別のサポート要件を簡単に統合できます。

Call Home の利点

- 関連する CLI コマンド出力の実行および添付が自動化されます。
- 次のような、複数のメッセージ フォーマット オプションがあります。
  - ショート テキスト：ポケットベルまたは印刷形式のレポートに最適。
  - フルテキスト：人間が判読しやすいように完全にフォーマットされたメッセージ情報です。
  - XML：Extensible Markup Language（XML）を使用した、照合型の読み取り可能な形式です。XML 形式では、シスコ TAC と通信できます。
- 複数のメッセージ宛先への同時配信が可能。
- 構成、クラッシュ、診断、環境、インベントリ、スナップショットおよび syslog を含む複数のメッセージ カテゴリ。
- 重大度およびパターン マッチングによるメッセージのフィルタリング
- 定期的なメッセージ送信のスケジューリング

Smart Call Home サービスの取得

シスコと直接サービス契約を結んでいる場合は、Smart Call Home サービスに登録できます。Smart Call Home は、Smart Call Home メッセージを分析し、背景説明と推奨措置を提供します。クリティカルな問題については、Cisco TAC に Automatic Service Request が作成されます。

Smart Call Home には、次の機能があります。

- 継続的なデバイス ヘルス モニタリングとリアルタイム アラート。

- Smart Call Home メッセージの分析。必要に応じて、自動サービス要求（詳細な診断情報が含まれる）が作成され、該当する TAC チームにルーティングされるため、問題解決を高速化できます。
- セキュアなメッセージ転送が、ご使用のデバイスから直接、または HTTP プロキシ サーバやダウンロード可能な転送ゲートウェイ（TG）を経由して行われます。TG 集約ポイントは、複数のデバイスをサポートする場合またはセキュリティ要件によって、デバイスをインターネットに直接接続できない場合に使用できます。
- すべての Smart Call Home デバイスの Smart Call Home メッセージと推奨事項、インベントリ情報、および設定情報に Web アクセスすることにより、関連するフィールド通知、セキュリティ勧告、およびサポート終了日情報にアクセスできます。

Smart Call Home で次の項目を登録する必要があります。

- ルータの SMARTnet 契約番号
- 電子メール アドレス
- Cisco.com のユーザ名

Call Home を Smart Call Home サービスと連動するように設定する方法については、Smart Call Home を参照してください。

Anonymous Reporting

Smart Call Home は、多くのシスコ サービス契約に含まれるサービス機能で、顧客が問題をより迅速に解決できるように支援することを目的としています。また、クラッシュ メッセージから取得した情報は、シスコが現場の機器や発生している問題を理解しやすくします。Smart Call Home を使用しない場合でも、Anonymous Reporting をイネーブルにすると、シスコはデバイスから最小限のエラーおよびヘルス情報をセキュアに受信できます。Anonymous Reporting をイネーブルにした場合、顧客が誰であるかは匿名のままで、識別情報は送信されません。

（注） Anonymous Reporting をイネーブルにすると、シスコまたはシスコに代わって業務を行うベンダーに指定データを転送することに同意することになります（米国以外の国を含む）。シスコでは、すべてのお客様のプライバシーを保護しています。シスコでの個人情報の取り扱いについては、Cisco Online Privacy Statement にあるシスコのプライバシー ステートメントを参照してください。

Call Home が匿名で設定されていると、クラッシュ、インベントリ、およびテスト メッセージだけがシスコに送信されます。識別情報は送信されません。

これらのメッセージで送信される情報の詳細については、「アラート グループの起動イベントとコマンド」セクションを参照してください。

スマート ライセンス

スマート ライセンスでは、Smart Call Home サービスが使用されます。

スマート ライセンス サービスは、Cisco Software Licensing（CSL）の代替となるライセンス アーキテクチャです。スマートライセンスでは、ライセンスを管理するためのバックエンドツールとして Smart Software Manager が使用されます。スマート ライセンスを使用するには、事前に Smart Call Home を設定する必要があります。デフォルトで、スマート ライセンスおよび Smart Call Home は Cisco cBR ルータでイネーブルになっています。

スマート ライセンスについての詳細は、『Cisco Smart Licensing on the Cisco cBR Router』を参照してください。

Call Home の設定方法

Smart Call Home の設定（単一コマンド）

ルータでは、Smart Call Home がデフォルトでイネーブルに設定されています。シスコにデータを送信する CiscoTAC-1 プロファイルも、デフォルトではイネーブルに設定されています。

匿名モードに変更したり、1 つのコマンドを使用して HTTP プロキシを追加したりする必要がない限り、1 つのコマンドを使用してルータで Smart Call Home をイネーブルにする必要はありません。

1 つのコマンドですべての Call Home の基本設定をイネーブルにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device#` **configure terminal**	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 2	**call-home reporting** {**anonymous** | **contact-email-addr** *email-address*} [**http-proxy** {*ipv4-address* | *ipv6-address* | **name**} **port** *port number*] 例： `Device(config)#` **call-home reporting contact-email-addr email@company.com**	1 つのコマンドを使用してすべての Call Home の基本設定をイネーブルにします。 • **anonymous**：Call Home TAC プロファイルがクラッシュ、インベントリ、およびテスト メッセージだけを送信し、匿名でメッセージを送信できるようにします。 • **contact-email-addr**：Smart Call Home サービスのフル レポート機能をイネーブルにし、フル インベントリ メッセージを Call Home TAC プロファイルから Smart Call Home サーバに送信してフル登録プロセスを開始します。 • **http-proxy** {*ipv4-address* | *ipv6-address* | **name**：ipv4 または ipv6 アドレス、またはサーバ名。最大長は 64 文字です。

	コマンドまたはアクション	目的
		• **port** *port number*：ポート番号。有効値の範囲は 1 ～ 65535 です。 （注） HTTP プロキシオプションでは、バッファリングするための独自のプロキシサーバおよびデバイスからのセキュア接続を利用できます。 （注） **call-home reporting** コマンドを使用して匿名またはフル登録モードで Call Home を正常にイネーブルにした後、インベントリ メッセージが送信されます。Call Home が匿名モードでイネーブルになっている場合、匿名のインベントリ メッセージが送信されます。Call Home がフル登録モードでイネーブルになっている場合、フル登録モードのフル インベントリ メッセージが送信されます。これらのメッセージの送信内容の詳細については、アラート グループの起動イベントとコマンド, （1560 ページ）を参照してください。

Call Home の設定

HTTPS には追加的なペイロード暗号化が含まれているため、セキュリティ上の理由から、HTTPS 転送オプションを使用することをお勧めします。インターネットへの接続に集約ポイントまたはプロキシが必要な場合は、Cisco.com からダウンロード可能な転送ゲートウェイ ソフトウェアを使用できます。

ルータ上の実装には、トラストプール機能（IOS イメージに組み込まれた CA 証明書）がサポートされます。トラストプール機能により、Smart Call Home サービスが設定されたデバイスでは容易にイネーブルに設定できるようになります。これにより、トラストプールを手動で設定する必要がなくなり、将来変更があった場合に CA 証明書が自動的に更新されます。

Call Home のイネーブル化とディセーブル化

Call Home 機能をイネーブルまたはディセーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Router#` **configure terminal**	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 2	**service call-home** 例： `Router(config)#` **service call-home**	Call Home 機能をイネーブルにします。
ステップ 3	**no service call-home** 例： `Router(config)#` **no service call-home**	Call Home 機能をディセーブルにします。

連絡先情報の設定

各ルータには必ず連絡用の電子メール アドレスが含まれている必要があります。任意で、電話番号、住所、契約 ID、カスタマー ID、サイト ID を割り当てることができます。

連絡先情報を割り当てるには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Router>` **configure terminal**	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 2	**call-home** 例： `Router(config)#` **call-home**	Call Home 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	**contact-email-addr** *email-address* 例： `Router(cfg-call-home)#`	顧客の E メール アドレスを割り当てます。E メール アドレス フォーマットにはスペースなしで最大 200 文字まで入力できます。

	コマンドまたはアクション	目的
	contact-email-addr username@example.com	
ステップ 4	**phone-number** +*phone-number* 例： `Router(cfg-call-home)#` **phone-number +1-222-333-4444**	（任意）顧客の電話番号を割り当てます。 （注） 番号は必ずプラス（+)記号で始まり、ダッシュ（-）と数字だけが含まれるようにしてください。最大16文字まで入力できます。スペースを含める場合、入力内容を二重引用符（“ ”）で囲む必要があります。
ステップ 5	**street-address** *street-address* 例： `Router(cfg-call-home)#` **street-address “1234 Any Street, Any city, Any state, 12345”**	（任意）RMA 機器の配送先である顧客の住所を割り当てます。最大200文字まで入力できます。スペースを含める場合、入力内容を二重引用符（“ ”）で囲む必要があります。
ステップ 6	**customer-id** *text* 例： `Router(cfg-call-home)#` **customer-id Customer1234**	（任意）カスタマーIDを指定します。最大64文字まで入力できます。スペースを含める場合、入力内容を二重引用符（“ ”）で囲む必要があります。
ステップ 7	**site-id** *text* 例： `Router(cfg-call-home)#` **site-id Site1ManhattanNY**	（任意）カスタマーのサイト ID を指定します。最大200文字まで入力できます。スペースを含める場合、入力内容を二重引用符（“”）で囲む必要があります。
ステップ 8	**contract-id** *text* 例： `Router(cfg-call-home)#` **contract-id Company1234**	（任意）ルータに顧客の契約 ID を指定します。最大 64 文字まで入力できます。スペースを含める場合、入力内容を二重引用符（“”）で囲む必要があります。

宛先プロファイルの設定

宛先プロファイルには、アラート通知に必要な配信情報が入っています。少なくとも 1 つの宛先プロファイルが必要です。1 つまたは複数のタイプの複数の宛先プロファイルを設定できます。

新しい宛先プロファイルを作成して定義することも、定義済みの宛先プロファイルをコピーして使用することもできます。新しい宛先プロファイルを定義する場合は、プロファイル名を割り当てる必要があります。プロファイルのスマートライセンシングデータを有効または無効にするこ

とにより、どのプロファイルをスマート ライセンシングに使用するかを制御できます。スマート ライセンシング データは、1 つのアクティブなプロファイルでのみイネーブルにできます。

（注） Cisco Smart Call Home サービスを使用する場合、宛先プロファイルは XML メッセージ フォーマットでなければなりません。

宛先プロファイルには、次の情報が含まれます。

- プロファイル名：ユーザ定義の宛先プロファイルを一意に識別する文字列。プロファイル名は 31 文字までで大文字と小文字は区別されません。プロファイル名として **all** は使用できません。
- 転送方法：アラートを送信するための転送メカニズム（電子メールまたは HTTP（HTTPS を含む））。
  - ユーザ定義の宛先プロファイルの場合、電子メールがデフォルトで、どちらかまたは両方の転送メカニズムをイネーブルにできます。両方の方法をディセーブルにすると、電子メールがイネーブルになります。
  - あらかじめ定義された Cisco TAC-1 プロファイルの場合、いずれかの転送メカニズムをイネーブルにできますが、同時にはイネーブルにできません。
- 宛先アドレス：アラートを送信する転送方法に関連した実際のアドレス。Cisco TAC-1 プロファイルの宛先は変更することができます。
- メッセージ形式：アラートの送信に使用するメッセージ形式。ユーザ定義宛先プロファイルの形式オプションは、ロング テキスト、ショート テキスト、または XML です。デフォルトは XML です。定義済みの Cisco TAC-1 プロファイルの場合、XML しか使用できません。
- メッセージ サイズ：宛先メッセージの最大サイズ。有効範囲は 50 ～ 3,145,728 バイトです。デフォルト値は 3,145,728 バイトです。
- レポート方法：プロファイルのどのデータをレポートするかを選択できます。Smart Call Home データ、スマート ライセンシング データ、またはその両方のレポートをイネーブルにできます。スマート ライセンシング データのレポートは、1 度に 1 つのアクティブなプロファイルについてのみ許可されます。
- Anonymous Reporting：顧客 ID を匿名のままにするよう選択できます。これにより、識別情報が送信されません。
- 関心のあるアラート グループへの登録：各自の関心事項を示すアラート グループに登録することができます。
- メッセージの重大度：宛先プロファイルに指定されたすべての電子メール アドレスに対して Call Home メッセージが生成される前に、アラートが満たしていなければならない Call Home の重大度。アラートの Call Home 重大度が宛先プロファイルに設定されたメッセージの重大度に満たない場合、アラートを生成しません。

inventory アラート グループを使用して、宛先プロファイルが定期的なインベントリの更新メッセージを許可するよう設定できます。

事前定義された宛先プロファイルである、Cisco TAC-1 がサポートされます。これは XML メッセージ形式をサポートします。このプロファイルは、Cisco Smart Call Home サーバの HTTPS URL、サーバに接続するための電子メールアドレス、最大メッセージサイズ、および各アラートグループのメッセージの重大度について事前設定されています。

重要 メッセージの重大度 0 の使用は推奨しません。メッセージの重大度 0 を使用すると、すべての syslog が Call Home メッセージをトリガーするため、CPU とメモリの問題が起きる可能性があります。

この項の構成は、次のとおりです。

新しい宛先プロファイルの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**call-home** 例： `Router(config)# call-home`	Call Home コンフィギュレーション モードを開始します。
ステップ 4	**profile** *name* 例： `Router(cfg-call-home)# profile profile1`	指定された宛先プロファイルに対する Call Home 宛先プロファイル設定モードを開始します。指定された宛先プロファイルが存在しない場合、作成されます。
ステップ 5	**destination transport-method {email | http}** 例： `Router(cfg-call-home-profile)# destination transport-method email`	（任意）メッセージ転送方法をイネーブルにします。 • **email**：電子メール メッセージの転送方式を設定します。 • **http**：HTTP メッセージの転送方式を設定します。

	コマンドまたはアクション	目的
		（注） **no** オプションを選択すると、その方法が無効になります。
ステップ 6	**destination address** {**email** *email-address* | **http** *url*} 例： `Router(cfg-call-home-profile)# destination address email myaddress@example.com`	Call Home メッセージを送信する宛先 E メール アドレスまたは URL を設定します。 （注） 宛先 URL を入力する場合は、サーバがセキュア サーバであるかどうかに応じて **http://** または **https://** を指定します。宛先がセキュア サーバである場合、トラストポイント CA も設定する必要があります。
ステップ 7	**destination preferred-msg-format** {**long-text** | **short-text** | **xml**} 例： `Router(cfg-call-home-profile)# destination preferred-msg-format xml`	（任意）使用するメッセージ形式を設定します。デフォルトは XML です。 • **long-text**：ロング テキスト メッセージ フォーマットを設定します。 • **short-text**：ショート テキスト メッセージ フォーマットを設定します。 • **xml**：XML メッセージ フォーマットを設定します。
ステップ 8	**destination message-size** *bytes* 例： `Router(cfg-call-home-profile)# destination message-size 3,145,728`	（任意）宛先プロファイルの宛先メッセージの最大サイズを設定します。
ステップ 9	**active** 例： `Router(cfg-call-home-profile)# active`	宛先プロファイルをイネーブルにします。デフォルトでは、プロファイルは作成時にイネーブルになります。 スマート ライセンシング データがすでに別のアクティブ プロファイルで報告されている場合に、スマート ライセンシング データをイネーブルにするプロファイルを有効化すると、エラー メッセージが表示されます。
ステップ 10	**reporting** {**all** | **smart-call-home-data** | **smart-licensing-data**} 例： `Router(cfg-call-home-profile)# reporting smart-call-home-data`	プロファイルで報告するデータの種類を設定します。 Smart Call Home データまたはスマート ライセンシング データのいずれかの報告を選択できます。**all** オプションを選択すると、両方の種類のデータが報告されます。

	コマンドまたはアクション	目的
ステップ 11	**end** 例： `Router(cfg-call-home-profile)# end`	特権 EXEC モードに戻ります。
ステップ 12	**show call-home profile** {*name* | **all**} 例： `Router# show call-home profile profile1`	指定されたプロファイルまたはすべての設定されたプロファイルに対する宛先プロファイル設定を表示します。
ステップ 13	**show call-home smart-licensing** 例： `Router# show call-home smart-licensing`	設定した宛先プロファイルの現在の Call Home スマート ライセンシング設定を表示します。
ステップ 14	**show call-home smart-licensing statistics** 例： `Router# show call-home smart-licensing statistics`	Call Home スマート ライセンシング統計情報を表示します。

宛先プロファイルのコピー

既存のプロファイルをコピーして新しい接続先プロファイルを作成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**call-home** 例： `Router(config)# call-home`	Call Home コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**copy profile** *source-profile target-profile* 例： `Router(cfg-call-home)# copy profile profile1 profile2`	既存の宛先プロファイルと同じ設定で新しい宛先プロファイルを作成します。 • *source-profile*：送信元接続先プロファイルの名前。 • *target-profile*：ターゲットまたは新しい接続先プロファイルの名前。

宛先プロファイルの名前変更

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**call-home** 例： `Router(config)# call-home`	Call Home コンフィギュレーション モードを開始します。
ステップ 4	**rename profile** *source-profile target-profile* 例： `Router(cfg-call-home)# rename profile profile1 profile2`	既存の宛先プロファイルの名前を変更します。 • *source-profile*：送信元接続先プロファイルの名前。 • *target-profile*：ターゲット接続先プロファイルの名前。

プロファイルの匿名モードの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**call-home** 例： `Router(config)# call-home`	Call Home コンフィギュレーション モードを開始します。
ステップ 4	**profile** *name* 例： `Router(cfg-call-home)# profile profile1`	指定された宛先プロファイルに対する Call Home 宛先プロファイル設定モードを開始します。指定された宛先プロファイルが存在しない場合、作成されます。
ステップ 5	**anonymous-reporting-only** 例： `Router(cfg-call-home-profile)# anonymous-reporting-only`	プロファイルを匿名モードに設定します。 （注） デフォルトでは、プロファイルはプロファイルに登録されているすべてのイベントタイプが記載された完全なレポートを送信します。**anonymous-reporting-only** が設定されている場合は、クラッシュ、インベントリ、およびテスト メッセージだけが送信されます。

アラート グループへの登録

アラート グループは、サポートされる Call Home アラートの定義済みサブセットです。宛先プロファイルごとに受信するアラート グループを 1 つまたは複数選択できます。

- Configuration
- Crash
- Diagnostic
- Environment
- Inventory

- Snapshot
- Syslog

各アラート グループの起動イベントは「アラート グループの起動イベントとコマンド」に示しています。アラート グループ メッセージの内容は「メッセージの内容」に示しています。

宛先プロファイルごとに受信するアラート グループを 1 つまたは複数選択できます。

（注） Call Home アラートは、その Call Home アラートが含まれているアラート グループに登録されている宛先プロファイルにしか送信されません。アラート グループをイネーブルにする必要があります。Call Home イベントの重大度は、宛先プロファイルに設定されたメッセージの重大度以上である必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**call-home** 例： `Router(config)# call-home`	Call Home コンフィギュレーション モードを開始します。
ステップ 4	**alert-group** {**all** | **configuration** | **crash** | **diagnostic** | **environment** | **inventory** | **snapshot** | **syslog**} 例： `Router(cfg-call-home)# alert-group all`	指定されたアラート グループをイネーブルにします。すべてのアラート グループをイネーブル（有効）にするには、**all** キーワードを使用します。デフォルトでは、すべてのアラート グループがイネーブルになります。
ステップ 5	**profile** *name* 例： `Router(cfg-call-home)# profile profile1`	指定された宛先プロファイルに対する Call Home 宛先プロファイル設定モードを開始します。指定された宛先プロファイルが存在しない場合、作成されます。
ステップ 6	**subscribe-to-alert-group configuration** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}]	この宛先プロファイルを Configuration アラート グループに登録します。定期的に通知を受信するようにコンフィギュレーション アラート グループを設定できます。

	コマンドまたはアクション	目的
	例： `Router(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic daily 12:00`	
ステップ 7	**subscribe-to-alert-group crash** 例： `Router(cfg-call-home-profile)# subscribe-to-alert-group crash`	ユーザ プロファイルの Crash アラート グループに登録します。デフォルトで Cisco TAC プロファイルは Crash アラート グループに登録され、登録を解除できません。
ステップ 8	**subscribe-to-alert-group diagnostic** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**}] 例： `Router(cfg-call-home-profile)# subscribe-to-alert-group syslog severity major`	この宛先プロファイルを Diagnostic アラート グループに登録します。Diagnostic アラート グループは、重大度に基づいてメッセージをフィルタリングするように設定できます。
ステップ 9	**subscribe-to-alert-group environment** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**}] 例： `Router(cfg-call-home-profile)# subscribe-to-alert-group environment severity major`	この宛先プロファイルを Environment アラート グループに登録します。環境アラート グループは、重大度に基づいてメッセージをフィルタリングするように設定できます。
ステップ 10	**subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}] 例： `Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 12:00`	この宛先プロファイルを Inventory アラート グループに登録します。定期的な通知を受信するように Inventory アラート グループを設定できます

ステップ 11	**subscribe-to-alert-group snapshot** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm* | **hourly** *mm* | **interval** *mm*}]
	
	例：
	`Router(cfg-call-home-profile)# subscribe-to-alert-group snapshot`
	
	`periodic daily 12:00`
		この宛先プロファイルを Snapshot アラート グループに登録します。定期的な通知を受信するように Snapshot アラート グループを設定できます。
		
		デフォルトでは、Snapshot アラート グループに実行するコマンドはありません。コマンドをアラート グループ内に追加できます。こうすることで、Snapshot アラート グループに追加された

	コマンドまたはアクション	目的
		コマンドの出力がスナップショット メッセージに組み込まれます。
ステップ 12	**subscribe-to-alert-group syslog** [**severity** {**catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging**}] [**pattern** *string*] 例： `Router(cfg-call-home-profile)# subscribe-to-alert-group syslog severity major`	この宛先プロファイルを Syslog アラート グループに登録します。Syslog アラート グループは、重大度に基づいてメッセージをフィルタリングするように設定できます。syslog メッセージで一致するパターンを指定できます。パターンにスペースが含まれている場合は、引用符（""）で囲む必要があります。 各 syslog メッセージ内で照合するテキスト パターンを指定できます。パターンを設定すると、指定されたパターンが含まれ、重大度しきい値に一致する場合にだけ Syslog アラート グループ メッセージが送信されます。パターンにスペースが含まれる場合は、引用符（“”）でスペースを囲む必要があります。宛先プロファイルごとにパターンを 5 つまで指定できます。
ステップ 13	**subscribe-to-alert-group all** 例： `Router(cfg-call-home-profile)# subscribe-to-alert-group all`	（任意）使用可能なすべてのアラート グループに登録します。 **重要** このコマンドを入力すると、多数の syslog メッセージが生成されます。可能な場合は、適切な重大度およびパターンを使用してアラート グループに個別に登録することを推奨します。

定期通知

Configuration、Inventory、または Snapshot アラート グループのいずれかに宛先プロファイルを登録するとき、アラート グループ メッセージを非同期的に受信するか、または指定の時間に定期的に受信するかを選択できます。次の時間間隔を使用できます。

- 毎日：24時間の時間:分形式 *hh:mm*（例：14:30）で送信する時刻を指定します。
- 毎週：day *hh:mm* という形式で曜日と時刻を指定します。ここで、day は曜日をスペルアウトします（例：monday）。
- 毎月：date *hh:mm* という形式で 1 ～ 31 の日と時刻を指定します。
- 間隔：定期的なメッセージが送信される間隔を 1 ～ 60 分で指定します。
- 毎時：定期的なメッセージが送信される時刻（分）を 0 ～ 59 分で指定します。

（注） 毎時および間隔による定期通知は、Snapshot アラート グループでのみ使用可能です。

メッセージ重大度しきい値

Call Home を使用すると、重大度に基づいてメッセージをフィルタリングできます。各定義済みまたはユーザ定義宛先プロファイルを、0（最小緊急度）～ 9（最大緊急度）までの Call Home しきい値と関連付けることができます。デフォルトは 0（全メッセージを送信）です。

宛先プロファイルを Environment または Syslog アラート グループに加入させる場合、メッセージの重大度に基づいてアラート グループ メッセージのリレーのしきい値を設定できます。宛先プロファイルのしきい値より低い値のメッセージは、宛先に送信されません。

特定の重大度が指定された宛先プロファイルを持つアラート グループに加入する場合、そのアラート グループで指定された以上の重大度のイベントによってトリガーされるメッセージの取得に加入することになります。

（注） 重大度レベルが低い syslog メッセージに加入させるのはお勧めしません。Syslog メッセージをトリガーする数が多すぎてシステム パフォーマンスが低下するおそれがあるためです。

（注） Call Home の重大度は、システム メッセージ ロギングの重大度とは異なります。

表 *223*：重大度と *syslog* レベルのマッピング

Smart Call Home レベル	キーワード	Syslog レベル	説明
9	**catastrophic**	—	ネットワーク全体に壊滅的な障害が発生しています。
8	**disaster**	—	ネットワークに重大な影響が及びます。
7	**fatal**	緊急（0）	システムが使用不可能な状態。
6	**critical**	アラート（1）	クリティカルな状況で、すぐに対応する必要があります。
5	**major**	重要（2）	重大な状態。
4	**minor**	エラー（3）	軽微な状態。
3	**warning**	警告（4）	警告状態。

Smart Call Home レベル	キーワード	Syslog レベル	説明
2	**notification**	通知（5）	基本的な通知および情報メッセージです。他と関係しない、重要性の低い障害です。
1	**normal**	情報（6）	標準状態に戻ることを示す標準イベントです。
0	**debugging**	デバッグ（7）	デバッグ メッセージ。

Syslog パターン マッチング

宛先プロファイルを Syslog アラート グループに登録すると、各 syslog メッセージ内で一致するテキスト パターンを任意で指定できます。パターンを設定すると、指定されたパターンが含まれ、重大度しきい値に一致する場合にだけ Syslog アラート グループ メッセージが送信されます。パターンにスペースが入っている場合、設定時にそのパターンを引用符（" "）で囲みます。宛先プロファイルごとにパターンを 5 つまで指定できます。

スナップショット コマンド リストの設定

スナップショット コマンド リストを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device#` **configure terminal**	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 2	**call-home** 例： `Device(config)#` **call-home**	Call Home 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	[**no** | **default**] **alert-group-config snapshot** 例： `Device(cfg-call-home)#` **alert-group-config snapshot**	スナップショット コンフィギュレーション モードを開始します。 **no** または **default** コマンドは、すべてのスナップショット コマンドを削除します。

	コマンドまたはアクション	目的
ステップ 4	[**no** | **default**] **add-command** *command string* 例： `Device(cfg-call-home-snapshot)#` **add-command** *"show version"*	Snapshot アラート グループにコマンドを追加します。**no** または **default** コマンドは、対応するコマンドを削除します。 • *command string*：IOS コマンド。最大長は 128 文字です。
ステップ 5	**end** 例： `Device(cfg-call-home-snapshot)#` **exit**	終了し、設定を保存します。

一般的な電子メール オプションの設定

メール サーバの設定

E メール メッセージ転送を使用するには、少なくとも 1 つの Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）E メール サーバ アドレスを設定する必要があります。最大で合計 5 つのメール サーバ定義に対し、最大 4 つのバックアップ電子メール サーバを指定できます。

メール サーバを設定する場合は、次のガイドラインを考慮してください。

- バックアップ E メール サーバは、異なるプライオリティ番号を使用して、**mail-server** コマンドを繰り返すと定義できます。
- **mail-serverpriority** *number* パラメータには 1 ～ 100 の値を設定できます。プライオリティが最も高い（プライオリティ番号が最も低い）サーバを最初に試します。

一般的な電子メール オプションを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device#` **configure terminal**	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 2	**call-home** 例： `Device(config)#` **call-home**	Call Home コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**mail-server**{*ipv4-address* | *name*} **priority** *number* 例： `Device(cfg-call-home)#` **mail-server stmp.example.com priority 1**	電子メールサーバアドレスを割り当て、設定済みの電子メールサーバ内の相対的なプライオリティを割り当てます。 次のいずれかの方法で指定します。 • 電子メール サーバの IP アドレスまたは • 電子メール サーバの完全修飾ドメイン名（FQDN）（64 文字まで） 1（最高のプライオリティ）から 100（最低のプライオリティ）のプライオリティ番号を割り当てます。
ステップ 4	**senderfrom** *email-address* 例： `Device(cfg-call-home)#` **sender from username@example.com**	（任意）Call Home E メール メッセージの [from] フィールドに表示される E メール アドレスを割り当てます。アドレスが指定されていない場合は、連絡用の E メール アドレスが使用されます。
ステップ 5	**senderreply-to** *email-address* 例： `Device(cfg-call-home)#` **sender reply-to username@example.com**	（任意）Call Home E メール メッセージの [reply-to] フィールドに表示される E メール アドレスを割り当てます。
ステップ 6	**source-interface** *interface-name* 例： `Device(cfg-call-home)#` **source-interface loopback1**	Call-Home メッセージを送信するための発信元インターフェイス名を割り当てます。 *interface-name*：発信元インターフェイス名。最大長は 64 文字です。 （注） HTTP メッセージの場合、発信元インターフェイス名を設定するには、グローバル コンフィギュレーション モードで **ip http client source-interface** *interface-name* コマンドを使用します。これにより、デバイスのすべての HTTP クライアントが同じ発信元インターフェイスを使用できるようになります。
ステップ 7	**source-ip-address** *ipv4/ipv6 address* 例： `Device(cfg-call-home)#` **ip-address 209.165.200.226**	Call-Home メッセージを送信するための発信元 IP アドレスを割り当てます。 • *ipv4/ipv6 address*：発信元 IP（ipv4 または ipv6）アドレス。最大長は 64 文字です。

	コマンドまたはアクション	目的
ステップ 8	**vrf***vrf-name* 例： `Device(cfg-call-home)#` **vrf** *vpn1*	（任意）Call Home E メール メッセージを送信する VRF インスタンスを指定します。VRF を指定しないと、グローバル ルーティング テーブルが使用されます。 （注） HTTP メッセージでは、発信元インターフェイスが VRF に関連付けられている場合、グローバル コンフィギュレーション モードで **ip http client source-interface** *interface-name* コマンドを使用して、デバイスのすべての HTTP クライアントで使われる VRF インスタンスを指定します。

Call Home メッセージ送信のレート制限の指定

Call Home メッセージ送信のレート制限を指定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device#` **configure terminal**	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 2	**call-home** 例： `Device(config)#` **call-home**	Call Home 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	**rate-limit** *number* 例： `Device(cfg-call-home)#` **rate-limit 40**	1 分間に送信するメッセージ数の制限を指定します。 • *number*：範囲は 1 ～ 60 です。デフォルトは 20 です。

HTTP プロキシ サーバの指定

宛先に Call Home HTTP（S）メッセージを送信するために HTTP プロキシ サーバを指定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device#` **configure terminal**	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 2	**call-home** 例： `Device(config)#` **call-home**	Call Home 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	**http-proxy** {*ipv4-address* | *ipv6-address name*} *name* 例： `Device(config)#` **http-proxy 1.1.1.1 port 1**	HTTP 要求のプロキシ サーバを指定します。

Call Home メッセージの *IOS* コマンドを実行するための *AAA* 認証の有効化

AAA 認証をイネーブルにして Call Home メッセージの出力の収集をイネーブルにする IOS コマンドを実行するには、次の作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device#` **configure terminal**	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 2	**call-home** 例： `Device(config)#` **call-home**	Call Home 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	**aaa-authorization** 例： `Device(cfg-call-home)#` **aaa-authorization**	AAA 認証をイネーブルにします。 （注） デフォルトでは、AAA 認証は Call Home でディセーブルです。

	コマンドまたはアクション	目的
ステップ 4	**aaa-authorization** [**username** *username*] 例： `Device(cfg-call-home)#` **aaa-authorization username** *username*	許可のためのユーザ名を指定します。 • **username** *user*：デフォルトのユーザ名は callhome です。最大長は 64 文字です。

syslog スロットリングの設定

Call Home syslog メッセージのスロットリングをイネーブルまたはディセーブルにし、Call Home syslog メッセージが繰り返し送信されないようにするには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device#` **configure terminal**	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 2	**call-home** 例： `Device(config)#` **call-home**	Call Home 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	[**no**] **syslog-throttling** 例： `Device(cfg-call-home)#` **syslog-throttling**	Call Home syslog メッセージのスロットリングをイネーブルまたはディセーブルにし、Call Home syslog メッセージが繰り返し送信されないようにします。デフォルトでは、syslog メッセージ スロットリングはイネーブルです。

Call Home データ プライバシーの設定

data-privacy コマンドは、顧客のプライバシーを保護するために、実行コンフィギュレーション ファイルのパスワードや IP アドレスなどのデータをスクラビング処理します。**data-privacy** コマンドをイネーブルにすると、大量のデータのスクラビング処理を行ったときにCPU使用率に影響を及ぼすことがあります。現在、**show** と **show running-config** の設定メッセージを除いて、コマンドの出力結果はスクラビング処理されていません。

手順

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Device#` **configure terminal**	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 2	**call-home** 例： `Device(config)#` **call-home**	Call Home 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	**data-privacy** {**level** {**normal** | **high**} | **hostname**} 例： `Device(cfg-call-home)#` **data-privacy level high**	ユーザのプライバシーを保護するために、実行コンフィギュレーション ファイルのデータをスクラビング処理します。デフォルトの data-privacy レベルは normal です。 （注） data-privacy コマンドをイネーブルにすると、大量のデータのスクラビング処理を行ったときに CPU 使用率に影響を及ぼすことがあります。 • **normal**：パスワードなどの機密データをスクラビング処理します。 • **high**：標準レベル コマンドに加えて、IP ドメイン名と IP アドレスのコマンドのスクラビング処理を行います。 • **hostname**：高レベル コマンドに加えてホスト名のコマンドのスクラビング処理を行います。 （注） 一部のプラットフォームでは、設定メッセージのホスト名をスクラビング処理すると、Smart Call Home 処理が失敗することがあります。

Call Home メッセージの手動送信

Call Home テスト メッセージの手動送信

call-hometest コマンドを使用して、ユーザ定義の Call Home テスト メッセージを送信できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**call-hometest** [**"***test-message***"**] **profile** *name* 例： `Router# call-home test profile profile1`	指定された宛先プロファイルにテストメッセージを送信します。ユーザ定義のテストメッセージのテキストは任意指定ですが、スペースが含まれる場合には、引用符（""）で囲む必要があります。ユーザ定義のメッセージが設定されていない場合、デフォルトメッセージが送信されます。

Call Home アラート グループ メッセージの手動送信

はじめる前に

- 手動で送信できるのは、Snapshot、Crash、Configuration、および Inventory アラート グループだけです。Syslog アラート グループは手動で送信できません。
- Snapshot、Configuration、または Inventory アラート グループ メッセージを手動でトリガーする場合、宛先プロファイル名を指定すると、プロファイルのアクティブ ステータス、加入ステータス、または重大度設定に関係なく、宛先プロファイルにメッセージが送信されます。
- Snapshot、Configuration、または Inventory アラート グループ メッセージを手動でトリガーするとき、宛先プロファイル名を指定しないと、normal または指定されたアラート グループへの定期的な登録に指定されたアクティブなプロファイルすべてにメッセージが送信されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**call-home send alert-group snapshot** [**profile** *name*] 例： `Router# call-home send alert-group snapshot profile profile1`	1 つの宛先プロファイル（指定されている場合）または登録されているすべての宛先プロファイルに Snapshot アラート グループ メッセージを送信します。

	コマンドまたはアクション	目的
ステップ 3	**call-home send alert-group crash** [**profile** *name*] 例： `Router# call-home send alert-group configuration profile profile1`	1つの宛先プロファイル（指定されている場合）または登録されているすべての宛先プロファイルに Crash アラート グループ メッセージを送信します。
ステップ 4	**call-home send alert-group configuration** [**profile** *name*] 例： `Router# call-home send alert-group configuration profile profile1`	宛先プロファイルの 1 つ（指定されている場合）または登録されているすべての宛先プロファイルに Configuration アラート グループ メッセージを送信します。
ステップ 5	**call-home send alert-group inventory** [**profile** *name*] 例： `Router# call-home send alert-group inventory`	宛先プロファイルの 1 つ（指定されている場合）または登録されているすべての宛先プロファイルに Inventory アラート グループ メッセージを送信します。

Call Home 分析およびレポート要求の送信

call-homerequest コマンドを使用して、システム固有の便利な分析およびレポート情報を送信するため、システムに関する情報を Cisco Systems に送信できます。セキュリティの警告、既知のバグ、ベスト プラクティス、コマンド リファレンスなど、さまざまなレポートを要求できます。

Call Home 分析およびレポート要求を手動で送信する場合、次の注意事項に従ってください。

- **profile** *name* を指定すると、要求はプロファイルに送信されます。プロファイルが指定されていない場合、要求は Cisco TAC プロファイルに送信されます。Call Home 要求の受信者プロファイルをイネーブルにする必要はありません。要求メッセージを Cisco TAC に転送し、Smart Call Home サービスから返信を受信できるように、Transport Gateway が設定された電子メール アドレスをプロファイルに指定します。
- **ccoid** *user-id* は、Smart Call Home ユーザの登録済み ID です。*user-id* を指定すると、応答は登録ユーザの E メール アドレスに送信されます。*user-id* を指定しなければ、応答はデバイスの連絡先電子メール アドレスに送信されます。
- 要求するレポートのタイプを指定するキーワードに基づいて、次の情報が返されます。
  - **config-sanity**：現在の実行コンフィギュレーションに関連するベスト プラクティスの情報。
  - **bugs-list**：実行中のバージョンおよび現在適用されている機能の既知のバグ。
  - **command-reference**：実行コンフィギュレーションに含まれるすべてのコマンドへの参照リンク。

- **product-advisory**：ネットワーク内の装置に影響を与える可能性がある Product Security Incident Response Team（PSIRT）警告、廃止（EOL）または販売終了（EOS）警告、Field Notice（FN）のいずれか

Cisco Output Interpreter ツールから分析およびレポート情報の要求を送信するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**call-homerequestoutput-analysis** “*show-command*” 例： [**profile** *name*] [**ccoid** *user-id*] 例： `Device#` **call-home request output-analysis “show diag” profile TG**	分析用として指定した **show** コマンドの出力を送信します。**show** コマンドは、引用符（""）で囲む必要があります。
ステップ 2	**call-homerequest** {**config-sanity**| **bugs-list** | **command-reference** | **product-advisory**} 例： [**profile** *name*] [**ccoid** *user-id*] 例： `Device#` **call-home request config-sanity profile TG**	分析のため、**showrunning-configall** および **showversion** コマンドなど所定のコマンドセットの出力を送信します。また、**callhomerequestproduct-advisory** サブコマンドには、すべてのインベントリ アラート グループ コマンドが含まれます。**call-home request** コマンドの後に指定するキーワードは、必要なレポートのタイプを示します。

1 つのコマンドまたはコマンド リスト用のコマンド出力メッセージの手動送信

call-homesend コマンドを使用すると、CLI を実行し、コマンド出力をシスコまたは指定の電子メール アドレスに送信できます。

コマンド出力を送信する場合は、次の注意事項に従ってください。

- IOS コマンドまたは IOS コマンド リストとして、すべてのモジュール用のコマンドを含めて、任意の実行コマンドを指定できます。コマンドは、引用符（“”）で囲む必要があります。
- 「email」キーワードを使って電子メール オプションを選択し、電子メール アドレスを指定すると、コマンド出力はそのアドレスに送信されます。電子メール オプションも HTTP オプションも指定しない場合、出力は指定のサービス要求番号と共にロング テキスト形式で Cisco TAC（attach@cisco.com）に送信されます。

- 「email」キーワードも「http」キーワードも指定しない場合、ロング テキスト形式と XML メッセージ形式の両方でサービス要求番号が必要とされ、電子メールの件名行にサービス要求番号が示されます。
- プロファイル名または宛先 URL を使用せずに HTTP オプションを指定している場合、Cisco TAC-1 プロファイルの宛先 HTTP または HTTPS URL が宛先として使用されます。Smart Call Home から電子メール アドレスにメッセージを転送するよう、宛先の電子メール アドレスを指定できます。ユーザは、宛先の電子メール アドレスまたは SR 番号のいずれかを指定する必要があります（両方を指定することもできます）。
- プロファイルを指定し、そのプロファイルの電子メール宛先の 1 つに callhome@cisco.com が設定されている場合は、XML をメッセージ形式で使用する必要があります。ロング テキスト形式を使用すると、エラー メッセージが表示されます。

コマンドを実行し、コマンド出力を送信するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	次のいずれかのコマンドを使用します。 • **call-home send** {*cli command* | *cli list*} [**email** [**profile** *profile-name* | *email*] [**msg-format** {**long-text** | **xml**}]] [**tac-sevice-request** *SR#*] • **call-home send** {*cli command* | *cli list*} [**http** [**profile** *profile-name* | *URL-dest*] [**destination-email-address** *email*]] [**tac-sevice-request** *SR#*] 例： `Router# call-home send "show version;show running-config show inventory" email support@example.com msg-format xml`	CLI または CLI リストを実行し、電子メールまたは HTTP 経由で出力を送信します。 • {*cli command* | *cli list*}：1 つの IOS コマンドまたは（「,」で区切った）IOS コマンド リストを指定します。すべてのモジュールに対するコマンドを含む、あらゆる run コマンドを指定できます。これらのコマンドは引用符（“”）で囲む必要があります。 • **email** [**profile** *profile-name* | *email*] [**msg-format** {**long-text** | **xml**}]：電子メール オプションを選択し、プロファイル名を指定した場合は、プロファイルで設定されている電子メール アドレスにコマンド出力が送信されます。電子メール アドレスを指定した場合は、指定したアドレスにコマンド出力が送信されます。メッセージはロング テキスト形式または XML 形式で、件名にサービス要求番号が記載されます。プロファイル名や電子メール アドレス、サービス要求番号、またはその両方を指定する必要があります。プロファイル名または電子メール アドレスが指定されない場合は、サービス リクエスト番号が必要です（デフォルトでは、ロング テキスト形式の場合は attach@cisco.com、XML 形式の場合は callhome@cisco.com）。 • **http** [**profile** *profile-name* | *URL-dest*] [**destination-email-address** *email*]：プロファイル名や宛先 URL を指定せずに HTTP オプションが選択された場合、Smart Call Home バックエンド サーバ（TAC プロファイル

	コマンドまたはアクション	目的
		で指定されているURL）にXML形式でコマンド出力が送信されます。プロファイル名または宛先 URL を指定した場合、コマンド出力は、プロファイル（profile-name case）で設定した宛先URL またはコマンドで指定した宛先URL に送信されます。 **destination-email-address** バックエンドサーバから電子メールアドレスにメッセージを転送できるように、*email* を指定できます。電子メール アドレス、サービス要求番号、またはその両方を指定する必要があります。 • **tac-service-request** *SR#*：サービス要求番号を指定します。電子メール アドレスが指定されない場合は、サービス リクエスト番号が必要です。

診断シグニチャの設定

診断シグニチャ機能は、デジタル署名されたシグニチャをデバイスにダウンロードします。診断シグニチャ（DS）ファイルは、診断イベントの情報を含んでいるフォーマット済みファイルです。これにより、シスコ ソフトウェアをアップグレードすることなくトラブルシューティングを実行できます。DSの目的は、お客様のネットワークで発生している既知の問題を解決するために使用可能なトラブルシューティング情報を検出/収集できる、柔軟性の高いインテリジェンスを提供することです。

診断シグニチャの前提条件

デバイスに診断シグニチャ（DS）をダウンロードして設定する前に、次の条件を満たしていることを確認します。

- デバイスに DS を割り当てる必要があります。デバイスに DS を割り当てる方法の詳細については、「診断シグニチャのダウンロード」セクションを参照してください。
- DS ファイルをダウンロードするためには HTTP/Secure HTTP（HTTPS）トランスポートが必要です。宛先 HTTPS サーバの認証をイネーブルにするには、認証局（CA）証明書をインストールする必要があります。

（注） トラストプール機能を設定する場合は、CA 証明書は不要です。

診断シグニチャについて

診断シグニチャの概要

Call Home システムの診断シグニチャ（DS）に備わっている柔軟なフレームワークにより、新しいイベントおよび対応する CLI を定義できます。これらの CLI を使用すると、シスコ ソフトウェアをアップグレードせずにこれらのイベントを分析できます。

DS により、標準の Call Home 機能でサポートされていないイベント タイプとトリガー タイプを追加的に定義できます。DS サブシステムは、ファイルをデバイスにダウンロードして処理し、診断シグニチャ イベントのコールバックを処理します。

診断シグニチャ機能は、ファイルの形式のデジタル署名シグニチャをデバイスにダウンロードします。DS ファイルは、診断イベントの情報を照合し、これらのイベントのトラブルシューティング手段を提供する、フォーマット済みファイルです。

DS ファイルには、イベントの説明を指定する XML データと、必要なアクションを実行する CLI コマンドまたはスクリプトが含まれています。これらのファイルは、整合性、信頼性、セキュリティを証明するために、シスコまたはサード パーティによりデジタル署名されています。

DS ファイルの構造は、次のいずれかです。

- イベント タイプを指定する、メタデータに基づく単純な署名。また、イベントの照合やアクションの実行（たとえば CLI を使用した情報の収集）に使用できるその他の情報もこれに含まれます。さらに、この署名は、特定のバグに対する回避策としてデバイスの設定を変更することもできます。
- 組み込みイベント マネージャ（EEM）Tool Command Language（Tcl）スクリプトに基づく署名。これはイベント レジスタ行で新しいイベントを指定し、Tcl スクリプトで追加のアクションを指定します。
- 上記の両方の形式の組み合わせ。

DS ファイルには次の基本情報が含まれています。

- ID（一意の番号）：DS の検索に使用できる DS ファイルを表す一意のキー。
- 名前（ShortDescription）：選択用リストで使用できる、DS ファイルに関する一意の記述。
- 説明：シグニチャに関する長い説明。
- リビジョン：バージョン番号。DS の内容が更新されると増加します。
- イベントおよび処理：検出対象のイベントと、イベントの発生後に実行すべき処理を定義します。

診断シグニチャのダウンロード

診断シグニチャ（DS）ファイルをダウンロードするには、セキュア HTTP（HTTPS）プロトコルが必要です。デバイスにファイルをダウンロードする方式として電子メール転送方式をすでに設

定している場合、DS をダウンロードして使用するには、割り当て済みプロファイル転送方式を HTTPS に変更する必要があります。

Cisco ソフトウェアは既知の証明機関（CA）からの証明書プールをプロビジョニング、保存、および管理する方式を作成するために PKI トラストプール管理機能を使用します。デバイスではこの機能がデフォルトでイネーブルに設定されています。トラストプール機能により、CA 証明書が自動的にインストールされます。CA 証明書は、宛先 HTTPS サーバの認証に必要です。

DS ファイルをダウンロードするための DS 更新要求には、標準ダウンロードと強制ダウンロードの 2 種類があります。

標準ダウンロードは、最近更新された DS ファイルを要求します。標準ダウンロード要求をトリガーするには、定期的な設定を使用するか、またはオンデマンドで CLI を開始します。標準ダウンロード更新は、要求された DS バージョンがデバイス上の DS バージョンと異なる場合にのみ実行されます。定期的なダウンロードは、DS Web ポータルからデバイスにすでに割り当てられた DS が存在する場合にのみ開始されます。割り当てが行われた後、同じデバイスからの定期インベントリ メッセージへの応答の中に、定期的な DS のダウンロードおよび更新を開始するようデバイスに通知するフィールドが含まれます。DS 更新要求メッセージには、DS のステータスとリビジョン番号が含まれます。これにより、最新リビジョン番号の DS だけがダウンロードされます。

強制ダウンロードでは、特定の 1 つの DS または一連の DS がダウンロードされます。強制ダウンロード更新要求をトリガーする唯一の方法は、オンデマンドで CLI を開始することです。強制ダウンロード更新要求では、デバイス上の現在の DS ファイルのバージョンに関係なく、最新バージョンの DS ファイルがダウンロードされます。

DS ファイルにはデジタル署名が付いています。ダウンロードされるすべての DS ファイルに対して署名の検証が実行され、ファイルが信頼できるソースからのものであることが確認されます。

診断シグニチャの署名

診断シグニチャ（DS）ファイルは、ダウンロードできるようになる前にデジタル署名されます。DS ファイルのデジタル署名では次の方法が使用されます。

- 署名アルゴリズム（Rivest Shamir and Adleman（RSA）2048 ビット）
- デジタル署名クライアントである Abraxas システムへの要求キー ペア
- コード署名クライアントを介してセキュア ソケット レイヤ（SSL）経由で署名された DS（署名は XML タグを使用して埋め込まれる）
- 公開キーはシスコ ソフトウェアの DS サブシステム（シスコ署名、パートナー署名、サードパーティ署名）に組み込まれます。デジタル署名された DS ファイルは、Diagnostic_Signatures（シスコ署名）、Diagnostic_Signatures_Partner、Diagnostic_Signatures_3rd_Party のように製品名が含まれます。製品名は、DS ファイルへの署名にのみ使用されます。

デジタル署名クライアントは、https://abraxas.cisco.com/SignEngine/submit.jsp にあります。

DS ファイルのデジタル署名を検証するには、以下の条件を満たす必要があります。

- コード署名コンポーネント サポートがシスコ ソフトウェアで利用できる必要があります。

- 各種の診断シグニチャを確認するさまざまな公開キーが、DS がサポートされているプラットフォームに含まれる必要があります。
- DS の解析および取得後に、DS は、検証アプリケーション プログラム インターフェイス（API）を実行して、DS が有効であることを確認する必要があります。

診断シグニチャのワークフロー

Cisco ソフトウェアでは診断シグニチャ（DS）機能がデフォルトでイネーブルに設定されています。診断シグニチャを作成する際のワークフローを次に示します。

1. ダウンロードする DS を見つけて、それらをデバイスに割り当てます。このステップは、標準の定期ダウンロードでは必須ですが、強制ダウンロードでは必要ではありません。
2. デバイスは、標準の定期ダウンロードまたはオンデマンドの強制ダウンロードで、割り当てられているすべての DS または特定の 1 つの DS をダウンロードします。
3. デバイスはすべての DS のデジタル署名を検証します。検証に合格すると、デバイスはブートフラッシュやハード ディスクなどの固定型ディスクに DS ファイルを保存します。これにより、デバイスのリロード後に DS ファルを読み取ることができます。ルータでは、DS ファイルが bootflash:/call home ディレクトリに保存されます。
4. デバイスはDSの最新リビジョンを取得してデバイス内の古いリビジョンを置き換えるために、標準の定期 DS ダウンロード要求を送信し続けます。
5. デバイスはイベントを監視し、イベントが発生すると、DSファイルに定義されているアクションを実行します。

診断シグニチャのイベントとアクション

イベントセクションとアクションセクションは、診断シグニチャで使用される主な領域です。イベント セクションでは、イベント検出に使用されるすべてのイベントの属性を定義します。アクション セクションでは、イベント発生後に実行する必要があるすべてのアクション（たとえば **show** コマンド出力を収集して解析のために Smart Call Home に送信）がリストされます。

診断シグニチャのイベント検出

診断シグニチャ（DS）のイベント検出の方法として、単一イベント検出と複数イベント検出の 2 つが定義されています。

単一イベント検出

単一イベント検出では、DS 内で 1 つのイベント ディテクタだけが定義されます。イベントの指定形式は、次の 2 種類のいずれかです。

- DS イベント指定タイプ：サポートされているイベント タイプは、syslog、定期、設定、即時活性挿抜（OIR）、および Call Home です。「即時」とは、このタイプの DS はイベントを検出せず、ダウンロードされるとただちにそのアクションが実行されることを示しています。Call-Home タイプは、既存のアラート グループに関して定義されている現在の CLI コマンドを変更します。

- 組み込みイベントマネージャ（EEM）指定タイプ：Ciscoソフトウェアを変更することなく、すべての新しいEEMイベントディテクタをサポートします。

  EEMを使用したイベント検出以外では、Tool Command Language（Tcl）スクリプトを使ってイベント検出タイプが指定されると、DSがトリガーされます。

複数イベント検出

複数イベント検出では、複数のイベントディテクタ、対応する複数の追跡対象オブジェクト状態、およびイベント発生期間を定義します。複数イベント検出の指定形式には、追跡対象イベントディテクタに関する複合イベント相関を含めることができます。たとえば、3つのイベントディテクタ（syslog、OIR、IPSLA）が、DSファイルの作成時に定義されます。これらのイベントディテクタに関して指定される相関は、syslogイベントおよびOIRイベントが同時にトリガーされるか、またはIPSLAが単独でトリガーされる場合に、DSがアクションを実行することを示します。

診断シグニチャのアクション

診断シグニチャ（DS）ファイルは、イベントの発生時に開始すべきさまざまなアクションで構成されます。アクションタイプは、特定のイベントに対応して開始されるアクションの種類を示します。

変数は、ファイルをカスタマイズするために使用されるDSファイル内の要素です。

DSアクションは、次の5つのタイプに分類されます。

- call-home
- command
- emailto
- script
- message

DSアクションタイプcall-homeおよびemailtoはイベントデータを収集し、Call-Homeサーバまたは定義済み電子メールアドレスにメッセージを送信します。このメッセージでは、メッセージタイプとして「diagnostic-signature」、メッセージサブタイプとしてDS IDが使用されます。

DSアクションタイプに関して定義されているコマンドは、デバイスの設定の変更、showコマンド出力の収集、またはデバイスでの任意のEXECコマンドの実行を行うCLIコマンドを開始します。DSアクションタイプscriptは、Tclスクリプトを実行します。

DSアクションタイプメッセージは、重要な情報をユーザに通知または催促するメッセージを生成するためのアクションを定義します。メッセージはすべてのTTY回線にブロードキャストしたり、syslogエントリとして生成したりできます。

アクションタイプ

DSアクションは、次の4つのタイプに分類されます。

- call-home
- command

- emailto
- script

DS アクション タイプ call-home および emailto はイベント データを収集し、Call-Home サーバまたは定義済み電子メール アドレスにメッセージを送信します。メッセージに含まれる要素は、次のとおりです。

- メッセージのタイプ：diagnostic-signature
- メッセージのサブタイプ：ds-id
- メッセージの説明：event-id：ds name

DS アクション タイプに対して定義されたコマンドは、デバイスの設定を変更できる CLI コマンドを開始します。DS アクション タイプ script は、Tcl スクリプトを実行します。

診断シグニチャの変数

変数は診断シグニチャ（DS）内で参照され、DS ファイルをカスタマイズするために使用されます。DS 変数を他の変数と区別するために、すべての DS 変数名にはプレフィックス ds_ が付いています。サポートされる DS 変数のタイプを以下に示します。

- システム変数：設定を変更することなく、デバイスにより自動的に割り当てられる変数。診断シグニチャ機能では、ds_hostname および ds_signature_id の 2 つのシステム変数がサポートされています。
- 環境変数：Call-Home 診断シグニチャ コンフィギュレーション モードで **environment***variable-namevariable-value* コマンドを使って手動で割り当てられる値。すべての DS 環境変数の名前と値を表示するには、**show call-home diagnostic-signature** コマンドを使用します。未解決の環境変数が DS ファイルに含まれている場合、変数が解決されるまで、この DS は保留状態のままになります。
- プロンプト変数：特権 EXEC モードで **call-home diagnostic-signature install** *ds-id* コマンドを使って手動で割り当てられる値。この値を設定しない場合、DS のステータスは保留中になります。
- 正規表現変数：事前定義された CLI コマンド出力との、正規表現を使用したパターンマッチによって割り当てられる値。この値は DS の実行中に割り当てられます。
- syslog イベント変数：DS ファイルでの syslog イベント検出中に割り当てられる値。この変数は、syslog イベント検出に関してのみ有効です。

診断シグニチャの設定方法

診断シグニチャの Service Call Home の設定

診断シグニチャ（DS）に関連する通知の送信先である連絡先の電子メール アドレスや、DS ファイルのダウンロード元である HTTP/secure HTTP（HTTPS）URL などの属性を設定するために、Service Call Home 機能を設定します。

また、新しいユーザ プロファイルを作成し、正しい属性を設定し、そのプロファイルを DS プロファイルとして割り当てることもできます。定期的なダウンロードの場合、フル インベントリ メッセージの直後に要求が送信されます。インベントリの定期設定を変更すると、DSの定期ダウンロードも再スケジュールされます。

（注） デフォルトでは、事前定義された Cisco TAC-1 プロファイルが DS プロファイルとしてイネーブルに設定されます。これを使用することをお勧めします。これを使用する場合、必要となる設定は、宛先転送方式の設定を **http** に変更することだけです。

はじめる前に

デバイスに診断シグニチャ（DS）をダウンロードして設定する前に、次の条件を満たしていることを確認します。

- デバイスに 1 つ以上の DS を割り当てる必要があります。
- DS ファイルをダウンロードするためには HTTP/Secure HTTP（HTTPS）トランスポートが必要です。宛先 HTTPS サーバの認証をイネーブルにするには、認証局（CA）証明書をインストールする必要があります。

（注） トラストプール機能を設定する場合は、CA 証明書は不要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**service call-home** 例： `Router(config)# service call-home`	デバイスで Call Home サービスをイネーブルにします。
ステップ 4	**call-home** 例： `Router(config)# call-home`	Call Home コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**contact-email-addr** *email-address* 例： `Router(cfg-call-home)# contact-email-addr username@example.com`	お客様の電子メールアドレスを割り当てます。スペースを入れず E メール アドレス形式で、200 文字まで入力できます。 （注） 任意の有効な E メール アドレスを使用できます。スペースは使用できません。
ステップ 6	**mail-server** {*ipv4-address* | *name*} **priority** *number* 例： `Router(cfg-call-home)# mail-server 10.1.1.1 priority 4`	（任意）Call Home の Simple Mail Transfer Protocol（SMTP）の電子メール サーバ アドレスを設定します。このコマンドは、いずれかの DS で定義されているアクションに電子メール送信が含まれる場合にのみ使用されます。
ステップ 7	**profile** *name* 例： `Router(cfg-call-home)# profile profile1`	指定された宛先プロファイルに対する Call Home 宛先プロファイル設定モードを開始します。指定された宛先プロファイルが存在しない場合、作成されます。
ステップ 8	**destination transport-method** {**email** | **http**} 例： `Router(cfg-call-home-profile)# destination transport-method email`	（任意）メッセージ転送方法をイネーブルにします。 • **email**：電子メール メッセージの転送方式を設定します。 • **http**：HTTP メッセージの転送方式を設定します。 （注） 診断シグニチャを設定するには、**http** オプションを使用する必要があります。
ステップ 9	**destination address** {**email** *email-address* | **http** *url*} 例： `Router(cfg-call-home-profile)# destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService`	Call Home メッセージを送信する宛先 E メール アドレスまたは URL を設定します。 （注） 診断シグニチャを設定するには、**http** オプションを使用する必要があります。
ステップ 10	**subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}] 例： `Router(cfg-call-home-profile)# subscribe-to-alert-group inventory`	この宛先プロファイルを Inventory アラート グループに登録します。定期的な通知を受信するように目録アラート グループを設定できます （注） このコマンドは、DS ファイルの定期的ダウンロード用にのみ使用されます。

	コマンドまたはアクション	目的
	periodic daily 12:00	

次の作業

前述の手順で設定したプロファイルをDSプロファイルとして設定し、その他のDSパラメータを設定します。

診断シグニチャの設定

はじめる前に

Service Call Home 機能を設定して、Call Home プロファイルの属性を設定します。デフォルトの Cisco TAC-1 プロファイルを使用するか、新しく作成したユーザ プロファイルを使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**call-home** 例： `Router(config)# call-home`	Call Home コンフィギュレーション モードを開始します。
ステップ 4	**diagnostic-signature** 例： `Router(cfg-call-home)# diagnostic-signature`	Call Home 診断シグニチャ モードを開始します。
ステップ 5	**profile** *ds-profile-name* 例： `Router(cfg-call-home-diag-sign)# profile user1`	デバイス上で診断シグニチャ（DS）が使用する宛先プロファイルを指定します。

	コマンドまたはアクション	目的
ステップ 6	**environment** *ds_env-var-name ds-env-var-value* 例： `Router(cfg-call-home-diag-sign)# environment ds_env1 envarval`	デバイスの DS の環境変数値を設定します。
ステップ 7	**end** 例： `Router(cfg-call-home-diag-sign)# end`	Call-Home 診断シグニチャ モードを終了して、特権 EXEC モードに戻ります。
ステップ 8	**call-home diagnostic-signature** {{**deinstall** | **download**} {*ds-id* | **all**} | **install** *ds-id*} 例： `Router# call-home diagnostic-signature download 6030`	デバイスで診断シグニチャ ファイルをダウンロード、インストール、またはアンインストールします。
ステップ 9	**show call-home diagnostic-signature** [*ds-id* [**actions** | **events** | **prerequisite** | **prompt** | **variables**] | **failure** | **statistics** [download]] 例： `Router# show call-home diagnostic-signature actions`	Call-Home 診断シグニチャ情報を表示します。

Call Home 設定の確認

- **show call-home** ：Call Home 設定の概要を表示します。

  次に、コマンドの出力例を示します。

```
Router# show call-home

Current call home settings:
    call home feature : enable
    call home message's from address: Not yet set up
    call home message's reply-to address: Not yet set up

    vrf for call-home messages: Not yet set up

    contact person's email address: sch-smart-licensing@cisco.com (default)

    contact person's phone number: Not yet set up
    street address: Not yet set up
    customer ID: Not yet set up
    contract ID: Not yet set up
    site ID: Not yet set up

    source ip address: Not yet set up
    source interface: TenGigabitEthernet4/1/1
    Mail-server[1]: Address: 173.36.13.143 Priority: 60
    http proxy: Not yet set up
```

```
    Diagnostic signature: enabled
    Profile: CiscoTAC-1 (status: ACTIVE)

    Smart licensing messages: enabled
    Profile: CiscoTAC-1 (status: ACTIVE)

    aaa-authorization: disable
    aaa-authorization username: callhome (default)
    data-privacy: normal
    syslog throttling: enable

    Rate-limit: 20 message(s) per minute

    Snapshot command[0]: show cable modem summary totalb
    Snapshot command[1]: show cable modem summary total

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- --------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    diagnostic               Enable  diagnostic info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info

Profiles:
    Profile Name: CiscoTAC-1
    Profile Name: test
```

- **show call-home detail**：Call Home 設定の詳細を表示します。

  次に、コマンドの出力例を示します。

```
Router# show call-home detail

Current call home settings:
    call home feature : enable
    call home message's from address: Not yet set up
    call home message's reply-to address: Not yet set up

    vrf for call-home messages: Not yet set up

    contact person's email address: sch-smart-licensing@cisco.com (default)

    contact person's phone number: Not yet set up
    street address: Not yet set up
    customer ID: Not yet set up
    contract ID: Not yet set up
    site ID: Not yet set up

    source ip address: Not yet set up
    source interface: TenGigabitEthernet4/1/1
    Mail-server[1]: Address: 173.36.13.143 Priority: 60
    http proxy: Not yet set up

    Diagnostic signature: enabled
    Profile: CiscoTAC-1 (status: ACTIVE)

    Smart licensing messages: enabled
    Profile: CiscoTAC-1 (status: ACTIVE)

    aaa-authorization: disable
    aaa-authorization username: callhome (default)
    data-privacy: normal
    syslog throttling: enable

    Rate-limit: 20 message(s) per minute

    Snapshot command[0]: show cable modem summary totalb
    Snapshot command[1]: show cable modem summary total
```

```
Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- --------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    diagnostic               Enable  diagnostic info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info

Profiles:

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Profile mode: Anonymous Reporting Only
    Reporting Data: Smart Call Home, Smart Licensing
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: http
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

   Periodic configuration info message is scheduled every 17 day of the month at 09:39


    Periodic inventory info message is scheduled every 17 day of the month at 09:24

    Alert-group               Severity
    ------------------------  ------------
    crash                     debug
    diagnostic                minor
    environment               minor
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major
```

- **show call-home alert-group** ：使用可能なアラート グループとそれらのステータスを表示します。

  次に、コマンドの出力例を示します。

```
Router# show call-home alert-group

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- --------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    diagnostic               Enable  diagnostic info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info
```

- **show call-home mail-server status**：設定済みの電子メール サーバのアベイラビリティをチェックし、表示します。

  次に、コマンドの出力例を示します。

```
Router# show call-home mail-server status

    Mail-server[1]: Address: 173.36.13.143 Priority: 60
```

- **show call-home profile** {**all** | *name*}：指定された宛先プロファイルの設定を表示します。すべての宛先プロファイルの設定を表示するには、**all** キーワードを使用します。

  次に、コマンドの出力例を示します。

```
Router# show call-home profile CiscoTac-1

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Profile mode: Full Reporting
    Reporting Data: Smart Call Home, Smart Licensing
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): http://10.22.183.117:8080/ddce/services/DDCEService

   Periodic configuration info message is scheduled every 17 day of the month at 09:39


    Periodic inventory info message is scheduled every 17 day of the month at 09:24

    Alert-group               Severity
    ------------------------  ------------
    crash                     debug
    diagnostic                minor
    environment               minor
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major
```

- **show call-home statistics** [**detail** | **profile** *profile-name*]：Call Home イベントの統計情報を表示します。

  次に、コマンドの出力例を示します。

```
Router# show call-home statistics

Message Types    Total                Email                HTTP
-------------   -------------------- -------------------- --------------------
Total Success   4                    3                    1
    Config      1                    1                    0
    Crash       0                    0                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   1                    0                    1
    Snapshot    0                    0                    0
    SysLog      2                    2                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0
    SCH         0                    0                    0

Total In-Queue  0                    0                    0
    Config      0                    0                    0
    Crash       0                    0                    0
    Diagnostic  0                    0                    0
    Environment 0                    0                    0
    Inventory   0                    0                    0
    Snapshot    0                    0                    0
    SysLog      0                    0                    0
    Test        0                    0                    0
    Request     0                    0                    0
    Send-CLI    0                    0                    0
    SCH         0                    0                    0

Total Failed    0                    0                    0
    Config      0                    0                    0
```

```
    Crash       0                   0                   0
    Diagnostic  0                   0                   0
    Environment 0                   0                   0
    Inventory   0                   0                   0
    Snapshot    0                   0                   0
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0
    SCH         0                   0                   0

Total Ratelimit
      -dropped  0                   0                   0
    Config      0                   0                   0
    Crash       0                   0                   0
    Diagnostic  0                   0                   0
    Environment 0                   0                   0
    Inventory   0                   0                   0
    Snapshot    0                   0                   0
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0
    SCH         0                   0                   0

Last call-home message sent time: 2015-03-06 18:21:49 GMT+00:00
```

- **show call-home diagnostic-signature**：診断シグニチャ情報の設定を表示します。

  次に、コマンドの出力例を示します。

```
Router# show call-home diagnostic-signature

Current diagnostic-signature settings:
 Diagnostic-signature: enabled
 Profile: CiscoTAC-1 (status: ACTIVE)
 Environment variable:
           Not yet set up

Downloaded DSes:
                                                                  Last Update
DS ID    DS Name                          Revision Status     (GMT-05:00)
-------- -------------------------------- -------- ---------- -------------------
```

- **show call-home version**：Call Home バージョン情報を表示します。

  次に、コマンドの出力例を示します。

```
Router# show call-home version

Call-Home Version 3.0
Component Version:
 call-home: (rel4)1.0.15
 eem-call-home: (rel2)1.0.5
```

Call Home の コンフィギュレーション例

例：Call Home の設定

次に、HTTPS 転送を設定するための設定例を示します。

```
ip host tools.cisco.com 72.163.4.38
vrf definition smart-vrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
interface TenGigabitEthernet4/1/1
 vrf forwarding smart-vrf
 ip address 172.22.11.25 255.255.255.128
 no ip proxy-arp
!
ip route vrf smart-vrf 72.163.4.38 255.255.255.255 172.22.11.1
!
ip http client source-interface TenGigabitEthernet4/1/1
!
```

次に、電子メール オプションを設定するための設定例を示します。

```
call-home
 mail-server 173.36.13.143 priority 60
 source-interface TenGigabitEthernet4/1/1
 vrf smart-vrf
 alert-group-config snapshot
  add-command "show cable modem summary total"
 profile "test"
  active
  destination transport-method email
  destination address email call-home@cisco.com
  subscribe-to-alert-group configuration
  subscribe-to-alert-group crash
  subscribe-to-alert-group diagnostic severity debug
  subscribe-to-alert-group environment severity debug
  subscribe-to-alert-group inventory
  subscribe-to-alert-group syslog severity major pattern .*
  subscribe-to-alert-group syslog severity notification pattern "^.+UPDOWN.+changed state
to (down|up)$"
  subscribe-to-alert-group snapshot periodic daily 12:00
!
ip route vrf smart-vrf 173.36.13.143 255.255.255.255 172.22.11.1
!
```

例：Cisco cBR シリーズ ルータでの Call Home に対する HTTP 転送の設定

手順

ステップ 1 現在の実行コンフィギュレーション ファイルをバックアップします。

ステップ 2 組み込まれたルータ証明書を確認します。

例：

```
Router# show crypto pki trustpool | include Class 3 Public

    ou=Class 3 Public Primary Certification Authority
    ou=Class 3 Public Primary Certification Authority
```

ステップ 3 （任意）VRF を設定します。

例：
```
Router(config)# vrf def smart-vrf
Router(config-vrf)# address-family ipv4
Router(config-vrf-af)# exit-address-family
Router(config-vrf)# address-family ipv6
Router(config-vrf-af)# exit-address-family
```

ステップ 4 ネットワーク インターフェイスをセットアップします。

例：
```
Router(config)# interface TenGigabitEthernet4/1/1
Router(config)# vrf forward smart-vrf
Router(config-if)# ip address 172.22.11.25 255.255.255.128
Router(config-if)# no ip proxy-arp
Router(config-if)# no shut
```

（注） IPv6 が有効な場合、IPv6 アドレスを設定する必要があります。

ステップ 5 シスコのポータルをセットアップします。

例：
```
Router(config)# ip host tools.cisco.com 72.163.4.38
Router(config)# ip route vrf smart-vrf 72.163.4.38 255.255.255.255 172.22.11.1
```

ステップ 6 データ パスを確認します。

例：
```
!Verify the connectivity to TenGigabitEthernet4/1/1 interface
Router# ping vrf smart-vrf 172.22.11.25

!Verify the connectivity to TenGigabitEthernet4//1/1 gateway
Router# ping vrf smart-vrf 172.22.11.1

!Verify the connectivity to tools.cisco.com
Router# ping vrf smart-vrf 72.163.4.38
```

ステップ 7 HTTP クライアント インターフェイスを設定します。

例：
```
Router(config)# ip http client source-interface TenGigabitEthernet4/1/1
```

ステップ 8 Call Home アラート グループ メッセージを手動で送信し、設定を確認します。

例：
```
Router# call-home send alert inventory profile CiscoTAC-1

Sending inventory info call-home message ...
Please wait. This may take some time ...

Router# show call-home statistics | include Total
Message Types    Total               Email               HTTP
Total Success   0                   0                   0
Total In-Queue  1                   0                   1
Total Failed    0                   0                   0
Total Ratelimit

Router# show call-home statistics | include Total
Message Types    Total               Email               HTTP
```

```
Total Success   1                   0                   1
Total In-Queue  0                   0                   0
Total Failed    0                   0                   0
Total Ratelimit
```

ステップ 9 Call Home の設定を表示します。

例：

```
Router# show call-home profile CiscoTAC-1

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Profile mode: Full Reporting
    Reporting Data: Smart Call Home, Smart Licensing
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: http
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 15 day of the month at 15:37

    Periodic inventory info message is scheduled every 15 day of the month at 15:22
Alert-group               Severity
    ------------------------  ------------
    crash                     debug
    diagnostic                minor
    environment               minor
    inventory                 normal

    Syslog-Pattern            Severity
    ------------------------  ------------
    .*                        major
```

例：Cisco cBR シリーズ ルータでの Call Home に対する電子メール転送の設定

手順

ステップ 1 現在の実行コンフィギュレーション ファイルをバックアップします。

ステップ 2 （任意）VRF を設定します。

例：

```
Router(config)# vrf def smart-vrf
Router(config-vrf)# address-family ipv4
Router(config-vrf-af)# exit-address-family
Router(config-vrf)# address-family ipv6
Router(config-vrf-af)# exit-address-family
```

ステップ 3 ネットワーク インターフェイスをセットアップします。

例：

```
Router(config)# interface TenGigabitEthernet4/1/1
Router(config)# vrf forward smart-vrf
Router(config-if)# ip address 172.22.11.25 255.255.255.128
Router(config-if)# no ip proxy-arp
```

```
Router(config-if)# no shut
```

（注） IPv6 が有効な場合、IPv6 アドレスを設定する必要があります。

ステップ 4 データ パスを確認します。

例：

```
!Verify the connectivity to TenGigabitEthernet4/1/1 interface
Router# ping vrf smart-vrf 172.22.11.25

!Verify the connectivity to TenGigabitEthernet4//1/1 gateway
Router# ping vrf smart-vrf 172.22.11.1

!Verify the connectivity to tools.cisco.com
Router# ping vrf smart-vrf 72.163.4.38
```

ステップ 5 （任意）Call Home を設定します。

例：

```
Router(config)# call-home

!Configure the TenGigabitEthernet 4/1/1
Router(cfg-call-home)# source-ip-address 172.22.11.25
```

ステップ 6 電子メール サーバを設定し、設定を確認します。

例：

```
Router(config)# call-home
Router(cfg-call-home)# mail-server 173.36.13.143 priority 60
Router(cfg-call-home)# vrf smart-vrf
Router(cfg-call-home)# exit
Router(config)# ip route vrf smart-vrf 173.36.13.143 255.255.255.255 172.22.11.1
Router(config)# end

Router# ping vrf smart-vrf 173.36.13.143
…

Router# show call-home mail status

Please wait. Checking for mail server status ...

Mail-server[1]: Address: 173.36.13.143 Priority: 60 [Available]
```

（注） VRF 設定はオプションです。

ステップ 7 新しい宛先プロファイルを作成し、アラート グループに登録します。

例：

```
Router(config)# call-home
Router(cfg-call-home)# alert-group-config snapshot
Router(cfg-call-home-snapshot)# add-command "show cable modem summary total”
Router(cfg-call-home-snapshot)# exit
Router(cfg-call-home)# profile test
Router(cfg-call-home-profile)# active
Router(cfg-call-home-profile)# destination transport-method email
Router(cfg-call-home-profile)# destination address email xyz@company.com
Router(cfg-call-home-profile)# subscribe syslog severity notification pattern
"^.+UPDOWN.+changed state to (down|up)$”
Router(cfg-call-home-profile)# subscribe-to-alert-group snapshot periodic daily 12:00
```

```
Router(cfg-call-home-profile)# end
```

ステップ 8 Call Home アラート グループ メッセージを手動で送信し、設定を確認します。

例：

```
Router# call-home send alert-group inventory profile test
Sending inventory info call-home message ...
Please wait. This may take some time ...

Router# show call-home statistics | include Total
Message Types    Total               Email               HTTP
Total Success   1                   0                   1
Total In-Queue  2                   2                   0
Total Failed    0                   0                   0
Total Ratelimit

Router# show call-home statistics | include Total
Message Types    Total               Email               HTTP
Total Success   3                   2                   1
Total In-Queue  0                   0                   0
Total Failed    0                   0                   0
Total Ratelimit
```

ステップ 9 Call Home の設定を表示します。

例：

```
Router# show call-home profile test

Profile Name: test
    Profile status: ACTIVE
    Profile mode: Full Reporting
    Reporting Data: Smart Call Home
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): abcd@company.com
    HTTP  address(es): Not yet set up

    Periodic snapshot info message is scheduled daily at 12:00

    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    crash                     debug
    diagnostic                debug
    environment               debug
    inventory                 normal
Syslog-Pattern            Severity
    ------------------------  ------------
    ^.+UPDOWN.+changed state
     to (down|up)$            notification
```

デフォルト設定

表 *224*：デフォルトの *Call Home* パラメータ

パラメータ	デフォルト
Call Home 機能のステータス	イネーブル
ユーザ定義プロファイルのステータス	Active
定義済みの Cisco TAC-1 プロファイルのステータス	Active
転送方法	HTTP
メッセージのフォーマット タイプ	XML
アラート グループのステータス	イネーブル
Call Home メッセージの重大度しきい値	Debug
1 分間に送信するメッセージのレート制限	20
AAA 許可	ディセーブル
Call Home の syslog メッセージ スロットリング	イネーブル
データ プライバシー レベル	標準

アラート グループの起動イベントとコマンド

以下の表に、サポートされるアラート グループと、アラート グループ用に生成された Call Home メッセージに含まれるデフォルトのコマンド出力を示します。

表 *225*：*Call Home* アラート グループ、イベント、および動作

アラート グループ	**Call Home** 起動イベント	**Syslog** イベント	重大度	説明と実行されるコマンド
Configuration	—	—	**normal periodic**	毎月送信される構成に関連した定期的なイベント。 実行するコマンド： • **show platform** • **show version** • **show inventory** • **show running-config all** • **show startup-config**

アラート グループ	Call Home 起動イベント	Syslog イベント	重大度	説明と実行されるコマンド
Crash	—	—	**debug**	スーパーバイザまたはライン カードのクラッシュなど、ルータでのクラッシュによって生成されたイベント。 実行するコマンド： クラッシュのトレースバック • **show version** • **show logging** • **show region** • **show stack** クラッシュ システム • **show version** • **show inventory** • **show logging** • **show region** • **show stack** • **more crashinfo-file** クラッシュ モジュール • **show version** • **show inventory** • **show platform** • **show logging** • **show region** • **show stack** • **more crashinfo-file**

アラート グループ	Call Home 起動イベント	Syslog イベント	重大度	説明と実行されるコマンド
Diagnostic	—	—	**minor**	診断によって生成されたイベント。 実行するコマンド： • **show platform** • **show version** • **show diagnostic event slot detail** • **show inventory** • **show buffers** • **show logging** • **show diagnostic events slot all**
Environmental	FAN_FAILURE	CBR_PEM-6-FANOK CBR_PEM-3-FANFAIL	**minor**	電源、ファン、温度アラームのような環境感知要素に関連するイベント 実行するコマンド： • **show platform** • **show environment** • **show inventory** • **show logging**
	TEMPERATURE_ALARM	ENVIRONMENTAL-1-ALERT		
	POWER_SUPPLY_FAILURE	CBR_PEM-6-PEMOK CBR_PEM-3-PEMFAIL		

アラート グループ	Call Home 起動イベント	Syslog イベント	重大度	説明と実行されるコマンド
Inventory	OIR_REMOVE OIR_INSERTION	—	**normal**	装置がコールドブートした場合、または FRU の取り付けまたは取り外しを行った場合に示されるコンポーネント ステータス。このアラートは、重大ではないイベントと見なされ、情報はステータスと権限付与に使用される。 実行するコマンド： • **show platform** • **show version** • **show inventory oid** • **show diag all eeprom detail** • **show interfaces** • **show file systems** • **show bootflash: all** • **show data-corruption** • **show memory statistics** • **show process memory** • **show process cpu** • **show process cpu history** • **show license udi** • **show license detail** • **show buffers** • **show platform software proc slot monitor cycle**
Snapshot	—	—	**normal**	ユーザ生成の CLI コマンド。

アラート グループ	Call Home 起動イベント	Syslog イベント	重大度	説明と実行されるコマンド
Syslog	—	—	**major**	Syslog メッセージによって生成されたイベント。 実行するコマンド： • **show inventory** • **show logging**
Test	—	—	**normal**	宛先プロファイルに送信される、ユーザ生成のテストメッセージ。 実行するコマンド： • **show inventory** • **show platform** • **show version**

メッセージの内容

Smart Call Home では、次のメッセージ フォーマットがサポートされます。

- ショート テキスト メッセージ フォーマット
- フル テキストと XML メッセージに共通のフィールド
- フル テキストおよび XML メッセージのアラート グループ メッセージに固有のフィールド
- リアクティブおよびプロアクティブ イベント メッセージに挿入されるフィールド
- コンポーネント イベント メッセージの挿入フィールド
- ユーザが作成したテスト メッセージの挿入フィールド

次の表に、すべてのメッセージ タイプのショート テキスト書式設定オプションを示します。

表 *226*：ショート テキスト メッセージ フォーマット

データ項目	説明
デバイス ID	設定されたデバイス名
日時スタンプ	起動イベントのタイム スタンプ
エラー判別メッセージ	起動イベントの簡単な説明（英語）

データ項目	説明
アラームの緊急度	エラー レベル（システム メッセージに適用されるエラー レベルなど）

次の表では、フル テキストまたは XML メッセージに共通するイベント メッセージ フィールドの最初のセットについて説明します。

表 *227*：フル テキストと *XML* メッセージに共通のフィールド

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
Time stamp	ISO 時刻通知でのイベントの日付/タイム スタンプ *YYYY-MM-DD HH:MM:SS GMT+HH:MM.*	CallHome/EventTime
メッセージ名	メッセージの名前。	ショート テキスト メッセージの場合のみ
メッセージ タイプ	メッセージ タイプの名前、特に「Call Home」。	CallHome/Event/Type
Message subtype	特定のメッセージ タイプ：full、delta、test	CallHome/Event/SubType
メッセージ グループ	アラート グループの名前、特に「リアクティブ」。デフォルトは「リアクティブ」であるため、任意。	Long-text メッセージ専用
重大度	メッセージの重大度	Body/Block/Severity
送信元 ID	ワークフロー エンジンから経路指定する製品タイプ。一般に製品ファミリ名です。	Long-text メッセージ専用

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
デバイス ID	メッセージを生成したエンド デバイスの固有デバイス識別情報（UDI）。メッセージがデバイスに対して固有でない場合は、このフィールドを空にする必要があります。形式は、*type@Sid@serial*。 • *type* はバックプレーン IDPROM から取得した製品モデル番号です。 • @ は区切り文字です。 • *Sid* は C で、シリアル ID をシャーシ シリアル番号として特定します。 • *serial* は、Sid フィールドによって識別される番号です。 例：WS-C6509@C@12345678	CallHome/CustomerData/ContractData/DeviceId
Customer ID	サポート サービスによって契約情報やその他の ID に使用されるオプションのユーザ設定可能なフィールド。	CallHome/CustomerData/ContractData/CustomerId
契約 ID	サポート サービスによって契約情報やその他の ID に使用されるオプションのユーザ設定可能なフィールド。	CallHome/CustomerData/ContractData/ContractId
サイト ID	シスコが提供したサイト ID または別のサポート サービスにとって意味のあるその他のデータに使用されるオプションのユーザ設定可能なフィールド。	CallHome/CustomerData/ContractData/SiteId

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
Server ID	デバイスからメッセージが生成された場合、これはデバイスの Unique Device Identifier（UDI）フォーマットです。形式は、*type@Sid@serial*。 • *type* はバックプレーン IDPROM から取得した製品モデル番号です。 • @ は区切り文字です。 • *Sid* は C で、シリアル ID をシャーシ シリアル番号として特定します。 • *serial* は、Sid フィールドによって識別される番号です。 例：WS-C6509@C@12345678	ロング テキスト メッセージの場合のみ
メッセージの説明	エラーを説明するショート テキスト	CallHome/MessageDescription
デバイス名	イベントが発生したノード（デバイスのホスト名）	CallHome/CustomerData/ SystemInfo/NameName
担当者名	イベントが発生したノード関連の問題について問い合わせる担当者名	CallHome/CustomerData/SystemInfo/Contact
連絡先 E メール	この装置の担当者の E メール アドレス	CallHome/CustomerData/SystemInfo/ContactEmail
Contact phone number	このユニットの連絡先である人物の電話番号。	CallHome/CustomerData/SystemInfo/ContactPhoneNumber
住所	この装置関連の返品許可（RMA）部品の送付先住所を保存するオプション フィールド	CallHome/CustomerData/SystemInfo/StreetAddress
Model name	デバイスのモデル名（製品ファミリ名に含まれる具体的なモデル）	CallHome/Device/Cisco_Chassis/Model
Serial number	ユニットのシャーシのシリアル番号。	CallHome/Device/Cisco_Chassis/SerialNumber

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	Call-Home メッセージ タグ（XML のみ）
シャーシの部品番号	シャーシの最上アセンブリ番号。	/aml/body/chassis/partNo
System object ID	システムを一意に識別するシステム オブジェクト ID。	CallHome/Device/Cisco_Chassis/ AdditionalInformation/AD@name=“sysObjectID”
システム記述	管理対象デバイスのシステム説明。	CallHome/Device/Cisco_Chassis/ AdditionalInformation/AD@name=“sysDescr”

次の表に、フル テキストおよび XML のアラート グループ メッセージに固有のフィールドについて説明します。1 つのアラート グループに対して複数のコマンドが実行される場合は、これらのフィールドが繰り返されることがあります。

表 *228*：フル テキストおよび *XML* メッセージのアラート グループ メッセージに固有のフィールド

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
コマンド出力名	実行されたコマンドの正確な名前。	/aml/attachments/attachment/name
添付タイプ	特定のコマンド出力	/aml/attachments/attachment/type
MIME タイプ	プレーン テキストまたは符号化タイプ	/aml/attachments/attachment/mime
コマンド出力テキスト	自動的に実行されるコマンドの出力	/mml/attachments/attachment/atdata

次の表では、フル テキストまたは XML メッセージのリアクティブおよびプロアクティブ イベント メッセージ形式について説明します。

表 *229*：リアクティブおよびプロアクティブ イベント メッセージに挿入されるフィールド

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
シャーシのハードウェア バージョン	シャーシのハードウェア バージョン。	/aml/body/chassis/hwVersion
スーパーバイザ モジュール ソフトウェア バージョン	最上レベルのソフトウェア バージョン。	/aml/body/chassis/swVersion

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
影響のある FRU の名前	イベント メッセージを生成する関連 FRU の名前	/aml/body/fru/name
影響のある FRU のシリアル番号	関連 FRU のシリアル番号	/aml/body/fru/serialNo
影響のある FRU の製品番号	関連 FRU の部品番号	/aml/body/fru/partNo
FRU スロット	イベント メッセージを生成する FRU のスロット番号	/aml/body/fru/slot
FRU ハードウェア バージョン	関連 FRU のハードウェア バージョン	/aml/body/fru/hwVersion
FRU ソフトウェア バージョン	関連 FRU で稼働しているソフトウェア バージョン	/aml/body/fru/swVersion

次の表では、フル テキストまたは XML メッセージのインベントリ イベント メッセージ形式について説明します。

表 *230*：コンポーネント イベント メッセージの挿入フィールド

データ項目（プレーン テキストおよび XML）	説明（プレーン テキストおよび XML）	XML タグ（XML のみ）
シャーシのハードウェア バージョン	シャーシのハードウェア バージョン	/aml/body/chassis/hwVersion
スーパーバイザ モジュール ソフトウェア バージョン	最上レベルのソフトウェア バージョン。	/aml/body/chassis/swVersion
FRU name	イベント メッセージを生成する関連 FRU の名前	/aml/body/fru/name
FRU s/n	FRU のシリアル番号	/aml/body/fru/serialNo
FRU 製品番号	FRU の部品番号	/aml/body/fru/partNo
FRU スロット	FRU のスロット番号	/aml/body/fru/slot
FRU ハードウェア バージョン	FRU のハードウェア バージョン	/aml/body/fru/hwVersion
FRU ソフトウェア バージョン	FRUで稼働しているソフトウェア バージョン	/aml/body/fru/swVersion

次の表に、フル テキストまたは XML のユーザが作成したテスト メッセージ形式について説明します。

表 *231*：ユーザが作成したテスト メッセージの挿入フィールド

データ項目（プレーン テキストおよび **XML**）	説明（プレーン テキストおよび **XML**）	**XML** タグ（**XML** のみ）
プロセス ID	固有のプロセス ID。	/aml/body/process/id
Process state	プロセスの状態（実行中、中止など）。	/aml/body/process/processState
Process exception	原因コードの例外。	/aml/body/process/exception

XML 形式での syslog アラート通知の例

```
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope
xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session
xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml
-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>MA:FXS1739Q0NR:548F4417</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block
xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/syslog</aml-block
:Type>
<aml-block:CreationDate>2014-12-16 04:27:03
GMT+08:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>CBR8</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>GB:FXS1739Q0NR:548F4417</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>6</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome"
version="1.0">
<ch:EventTime>2014-12-16 04:26:59 GMT+08:00</ch:EventTime>
<ch:MessageDescription>Dec 16 04:26:59.885 CST: %ENVIRONMENTAL-1-ALERT:
Temp: INLET, Location: 6, State: Critical, Reading: 53
Celsius</ch:MessageDescription> <ch:Event> <ch:Type>syslog</ch:Type>
<ch:SubType></ch:SubType> <ch:Brand>Cisco Systems</ch:Brand>
```

```
<ch:Series>CBR8 Series Routers</ch:Series> </ch:Event>
<ch:CustomerData> <ch:UserData> <ch:Email>xxxx@company.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId></ch:CustomerId>
<ch:SiteId></ch:SiteId>
<ch:ContractId></ch:ContractId>
<ch:DeviceId>CBR-8-CCAP-CHASS@C@FXS1739Q0NR</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>sig-cbr</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>xxxx@company.com</ch:ContactEmail>
<ch:ContactPhoneNumber></ch:ContactPhoneNumber>
<ch:StreetAddress></ch:StreetAddress>
</ch:SystemInfo>
<ch:CCOID></ch:CCOID>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>CBR-8-CCAP-CHASS</rme:Model>
<rme:HardwareVersion>0.1</rme:HardwareVersion>
<rme:SerialNumber>FXS1739Q0NR</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="000-00000-00" /> <rme:AD
name="SoftwareVersion" value="15.5(20141214:005145) " /> <rme:AD
name="SystemObjectId" value="1.3.6.1.4.1.9.1.2141" /> <rme:AD
name="SystemDescription" value="Cisco IOS Software, IOS-XE Software
(X86_64_LINUX_IOSD-ADVENTERPRISEK9-M), Experimental Version
15.5(20141214:005145) [ece5_throttle_ios-ram-ece5-bk 105] Copyright (c)
1986-2014 by Cisco Systems, Inc.
Compiled Sun 14-Dec-14 00:20 by ram" /> <rme:AD name="ServiceNumber"
value="" /> <rme:AD name="ForwardAddress" value="" />
</rme:AdditionalInformation> </rme:Chassis> </ch:Device> </ch:CallHome>
</aml-block:Content> <aml-block:Attachments> <aml-block:Attachment
type="inline"> <aml-block:Name>show inventory</aml-block:Name>
<aml-block:Data encoding="plain"> show inventory Load for five
secs: 2%/0%; one minute: 2%; five minutes: 2% Time source is NTP,
04:27:02.278 CST Tue Dec 16 2014
NAME: "Chassis", DESCR: "Cisco cBR-8 CCAP Chassis"
PID: CBR-8-CCAP-CHASS  , VID: V01, SN: FXS1739Q0NR

NAME: "sup 0", DESCR: "Cisco cBR CCAP Supervisor Card"
PID: CBR-CCAP-SUP-160G , VID: V01, SN: CAT1736E05L

NAME: "harddisk 4/1", DESCR: "Hard Disk"
PID: UGB88RTB100HE3-BCU-DID, VID:    , SN: 11000072780

NAME: "sup-pic 4/1", DESCR: "Cisco cBR CCAP Supervisor Card PIC"
PID: CBR-SUPPIC-8X10G  , VID: V01, SN: CAT1735E004

NAME: "SFP+ module 4/1/0", DESCR: "iNSI xcvr"
PID: SFP+ 10GBASE-SR   , VID: A   , SN: FNS1727294V

NAME: "SFP+ module 4/1/1", DESCR: "iNSI xcvr"
PID: SFP+ 10GBASE-SR   , VID: A   , SN: FNS172727WZ

NAME: "SFP+ module 4/1/4", DESCR: "iNSI xcvr"
PID: 10GE ZR           , VID:     , SN: AGM120525EW

NAME: "sup 1", DESCR: "Cisco cBR CCAP Supervisor Card"
PID: CBR-CCAP-SUP-160G , VID: V01, SN: CAT1736E05L

NAME: "clc 6", DESCR: "Cisco cBR CCAP Line Card"
PID: CBR-CCAP-LC-40G   , VID: V01, SN: CAT1736E0EN

NAME: "Cable PHY Module", DESCR: "CLC Downstream PHY Module 6/0"
PID: cBR-8-GEMINI      , VID: V01 , SN: CSJ13152101

NAME: "Cable PHY Module", DESCR: "CLC Upstream PHY Module 6/2"
PID: cBR-8-LEOBEN      , VID: V01 , SN: TST98765432

NAME: "Power Supply Module 0", DESCR: "Cisco cBR CCAP AC Power Supply"
```

```
PID: PWR-3KW-AC-V2     , VID: V02, SN: DTM173702KQ

NAME: "Power Supply Module 2", DESCR: "Cisco cBR CCAP AC Power Supply"
PID: PWR-3KW-AC-V2     , VID: V02, SN: DTM173702GD


sig-cbr#</aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging</aml-block:Name> <aml-block:Data
encoding="plain"> show logging Load for five secs: 2%/0%; one
minute: 2%; five minutes: 2% Time source is NTP, 04:27:02.886 CST Tue
Dec 16 2014

Syslog logging: enabled (0 messages dropped, 51 messages rate-limited,
0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.


    Console logging: level debugging, 213 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 262 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 209 message lines logged
        Logging Source-Interface:       VRF Name:

Log Buffer (1000000 bytes):

*Dec 15 20:20:16.188: Rommon debug: debugFlagsStr[7], flags[0x7] *Dec
15 20:20:16.188: TRACE - Debug flag set 0x7 *Dec 15 20:20:16.188: TRACE
- Register NV N:systemInitByEvent V:True with no CallBack *Dec 15
20:20:16.188: TRACE - Register NV N:routingReadyByEvent V:True with no
CallBack *Dec 15 20:20:16.188: TRACE - Smart agent init started.
Version=1.2.0_dev/22
*Dec 15 20:20:16.188: ERROR - PD init failed: The requested operation
is not supported *Dec 15 20:20:16.188: ERROR - Pre Role Init Failed:
The requested operation is not supported *Dec 15 20:20:16.188: TRACE -
Smart agent init Done. status 10, state 4294967295, init 0 enable 0
Current Role Invalid *Dec 15 20:20:16.188: TRACE - Shutdown Started
*Dec 15 20:20:16.188: DEBUG - Scheduler shutdown start *Dec 15
20:20:16.188: ERROR - Failed to set shutdown watched boolean (code
Invalid argument (22)). Going the hard way!!!
*Dec 15 20:20:16.188: DEBUG - Destroying XOS stuff to exit dispatch
loop *Dec 15 20:20:16.188: DEBUG - XDM dispatch loop about to exit *Dec
15 20:20:16.188: DEBUG - Scheduler shutdown end *Dec 15 20:20:16.188:
ERROR - SmartAgent not initialized.
*Dec 15 20:20:16.188: ERROR - Smart Agent not a RF client *Dec 15
20:20:16.188: ERROR - Smart Agent not a CF client *Dec 15 20:20:16.188:
TRACE - Setting Ha Mgmt Init FALSE *Dec 15 20:20:16.188: TRACE -
Shutting down Any Role *Dec 15 20:20:17.432: (DBMS RPHA) Client
initialization; status=success *Dec 15 20:20:17.432: CABLE Parser
Trace:  cable_parser_init:82 *Dec 15 20:20:17.774: ****
mcprp_ubr_punt_init: Initialized*****
-->RF_STATUS_SEND_RF_STATE received-->RF_PROG_INITIALIZATION received
*Dec 15 20:20:20.790: CWAN OIR debugging enabled (ROMMON variable
DEBUG_CWAN_OIR set)-->RF_PROG_ACTIVE_FAST
received-->RF_PROG_ACTIVE_DRAIN
received-->RF_PROG_ACTIVE_PRECONFIG
received-->received-->RF_PROG_ACTIVE_POSTCONFIG
received-->RF_PROG_ACTIVE received
```

```
*Dec 15 20:20:20.841: **** IPC port 0x1000E created!
*Dec 15 20:20:20.841:  **** CIPC RP Server created UBRCCE_CIPC_14/0 !
*Dec 15 20:20:28.294: %SPANTREE-5-EXTENDED_SYSID: Extended SysId
enabled for type vlan *Dec 15 20:20:31.944: %VOICE_HA-7-STATUS: CUBE
HA-supported platform detected.
*Dec 15 20:20:33.391:  instant_msg_handle_proc_sup started!!
*Dec 15 20:20:33.391:  queue_msg_handle_proc_sup started!!
*Dec 15 20:20:35.603: %IOSXE_MGMTVRF-6-CREATE_SUCCESS_INFO: Management
vrf Mgmt-intf created with ID 1, ipv4 table-id 0x1, ipv6 table-id
0x1E000001
*Dec 15 20:20:34.513: %IOSXE-6-PLATFORM: CLC4: cpp_cp: Process
CPP_PFILTER_EA_EVENT__API_CALL__REGISTER
*Dec 15 20:20:03.806: %HW_PFU-3-PFU_IDPROM_CORRUPT: R0/0: cmand:  The
PEM/FM idprom could be read, but is corrupt in slot P11 The system will
run without environmental monitoring for this component *Dec 15
20:20:09.012: %SYSTEM-3-SYSTEM_SHELL_LOG: R0/0:  2014/12/15
20:20:08 : <anon>
*Dec 15 20:20:13.919: %IOSXE-4-PLATFORM: R0/0: kernel: astro: FD open
*Dec 15 20:20:13.919: %IOSXE-4-PLATFORM: R0/0: kernel: astro: astro:
mmio_start=d0000000 mmio_len=2000000
*Dec 15 20:20:13.919: %IOSXE-4-PLATFORM: R0/0: kernel: astro: Done
astro Memory map base_ptr ffffc90016600000, astro_reg_ptr ffffc90016600000...
*Dec 15 20:20:16.259: %IOSXE-4-PLATFORM: R0/0: kernel: astro: FD open
*Dec 15 20:20:16.553: %CPPHA-7-START: F0: cpp_ha:  CPP 0 preparing
ucode *Dec 15 20:20:17.220: %CPPHA-7-START: F0: cpp_ha:  CPP 0 startup
init *Dec 15 20:20:18.549: %PMAN-3-PROC_EMPTY_EXEC_FILE: F0: pvp.sh:
Empty executable used for process iosdb *Dec 15 20:20:20.003:
%PMAN-3-PROC_EMPTY_EXEC_FILE: CLC4: pvp.sh:  Empty executable used for
process iosdb *Dec 15 20:20:20.783: %PMAN-3-PROC_EMPTY_EXEC_FILE: CLC4:
pvp.sh:  Empty executable used for process iosdb *Dec 15 20:20:24.061:
%HW_PFU-3-PFU_IDPROM_CORRUPT: R0/0: cmand:  The PEM/FM idprom could be
read, but is corrupt in slot P11 The system will run without
environmental monitoring for this component *Dec 15 20:20:31.722:
%CPPHA-7-START: F0: cpp_ha:  CPP 0 running init *Dec 15 20:20:32.070:
%CPPHA-7-READY: F0: cpp_ha:  CPP 0 loading and initialization complete
*Dec 15 20:20:36.528 UTC: TRACE - Platform EventCB invoked. EventType:
8 *Dec 15 20:20:36.528 UTC: DEBUG - Hostname changed. Old:sig-cbr
New:sig-cbr *Dec 15 20:20:36.528 UTC: %CNS IQ:0.1 ID:0
Changed:[sig-cbr] *Dec 15 20:20:36.528 UTC: %CNS IQ:0.2 ID:1
Changed:[sig-cbr] *Dec 15 20:20:36.528 UTC: %CNS IQ:0.3 ID:2
Changed:[sig-cbr] *Dec 15 20:20:36.594 UTC: %SYS-5-LOG_CONFIG_CHANGE:
Buffer logging: level debugging, xml disabled, filtering disabled, size
(1000000) *Dec 16 04:20:36.597 CST: %SYS-6-CLOCKUPDATE: System clock
has been updated from 20:20:36 UTC Mon Dec 15 2014 to 04:20:36 CST Tue
Dec 16 2014, configured from console by console.
*Dec 16 04:20:36.607 CST: spa_type 2946 ports 8 *Dec 16 04:20:36.622
CST: spa_type 2946 ports 8 *Dec 16 04:20:37.350 CST:
cmts_set_int_us_qos_flags: move US-QOS flags 0 to CDMAN *Dec 16
04:20:37.350 CST: cmts_set_int_us_default_weights: move US-QOS weights
to CDMAN *Dec 16 04:20:36.625 CST: %IOSXE-4-PLATFORM: R0/0: kernel:
astro: FD open *Dec 16 04:20:43.221 CST: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Video6/0/0, changed state to up *Dec 16
04:20:43.223 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Video6/0/1, changed state to up *Dec 16 04:20:43.502 CST: % Redundancy
mode change to SSO

*Dec 16 04:20:43.502 CST: %VOICE_HA-7-STATUS: NONE->SSO; SSO mode will
not take effect until after a platform
reload.-->RF_STATUS_REDUNDANCY_MODE_CHANGE received *Dec 16
04:20:44.220 CST: %SYS-5-CONFIG_I: Configured from memory by console
*Dec 16 04:20:44.228 CST: %IOSXE_OIR-6-INSCARD: Card (rp) inserted in
slot R1 *Dec 16 04:20:44.229 CST: %IOSXE_OIR-6-INSCARD: Card (fp)
inserted in slot F0 *Dec 16 04:20:44.229 CST: %IOSXE_OIR-6-ONLINECARD:
Card (fp) online in slot F0 *Dec 16 04:20:44.263 CST:
%IOSXE_OIR-6-INSCARD: Card (fp) inserted in slot F1 *Dec 16
04:20:44.263 CST: %IOSXE_OIR-6-INSCARD: Card (cc) inserted in slot 4
*Dec 16 04:20:44.263 CST: %IOSXE_OIR-6-ONLINECARD: Card (cc) online in
slot 4 *Dec 16 04:20:44.264 CST: %IOSXE_OIR-6-INSCARD: Card (cc)
inserted in slot 5 *Dec 16 04:20:44.264 CST: %IOSXE_OIR-6-INSCARD: Card
(cc) inserted in slot 6 *Dec 16 04:20:44.330 CST: %IOSXE_OIR-6-INSSPA:
SPA inserted in subslot 4/1 *Dec 16 04:20:44.751 CST: %SYS-5-RESTART:
System restarted -- Cisco IOS Software, IOS-XE Software
(X86_64_LINUX_IOSD-ADVENTERPRISEK9-M), Experimental Version
```

```
15.5(20141214:005145) [ece5_throttle_ios-ram-ece5-bk 105] Copyright (c)
1986-2014 by Cisco Systems, Inc.
Compiled Sun 14-Dec-14 00:20 by ram
*Dec 16 04:20:44.775 CST: %XML-SRVC: Security Enforcement XML
Service(111) OK. PID=574
*Dec 16 04:20:44.775 CST: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Dec 16 04:20:45.453 CST: %LINK-3-UPDOWN: Interface GigabitEthernet0,
changed state to up *Dec 16 04:20:45.543 CST: %LINK-5-CHANGED:
Interface TenGigabitEthernet4/1/2, changed state to administratively
down *Dec 16 04:20:45.546 CST: %LINK-5-CHANGED: Interface
TenGigabitEthernet4/1/3, changed state to administratively down *Dec 16
04:20:45.548 CST: %LINK-5-CHANGED: Interface TenGigabitEthernet4/1/4,
changed state to administratively down *Dec 16 04:20:45.551 CST:
%LINK-5-CHANGED: Interface TenGigabitEthernet4/1/5, changed state to
administratively down *Dec 16 04:20:45.571 CST: %LINK-5-CHANGED:
Interface TenGigabitEthernet4/1/6, changed state to administratively
down *Dec 16 04:20:45.574 CST: %LINK-5-CHANGED: Interface
TenGigabitEthernet4/1/7, changed state to administratively down *Dec 16
04:20:45.576 CST: %LINK-5-CHANGED: Interface TenGigabitEthernet5/1/0,
changed state to administratively down *Dec 16 04:20:45.578 CST:
%LINK-5-CHANGED: Interface TenGigabitEthernet5/1/1, changed state to
administratively down *Dec 16 04:20:45.580 CST: %LINK-5-CHANGED:
Interface TenGigabitEthernet5/1/2, changed state to administratively
down *Dec 16 04:20:45.582 CST: %LINK-5-CHANGED: Interface
TenGigabitEthernet5/1/3, changed state to administratively down *Dec 16
04:20:45.584 CST: %LINK-5-CHANGED: Interface TenGigabitEthernet5/1/4,
changed state to administratively down *Dec 16 04:20:45.586 CST:
%LINK-5-CHANGED: Interface TenGigabitEthernet5/1/5, changed state to
administratively down *Dec 16 04:20:45.588 CST: %LINK-5-CHANGED:
Interface TenGigabitEthernet5/1/6, changed state to administratively
down *Dec 16 04:20:45.590 CST: %LINK-5-CHANGED: Interface
TenGigabitEthernet5/1/7, changed state to administratively down *Dec 16
04:20:45.596 CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/0:0,
changed state to down *Dec 16 04:20:45.602 CST: %LINK-3-UPDOWN:
Interface Integrated-Cable6/0/0:1, changed state to down *Dec 16
04:20:45.603 CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/0:2,
changed state to down *Dec 16 04:20:45.604 CST: %LINK-3-UPDOWN:
Interface Integrated-Cable6/0/0:3, changed state to down *Dec 16
04:20:45.606 CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/0:4,
changed state to down *Dec 16 04:20:45.607 CST: %LINK-3-UPDOWN:
Interface Integrated-Cable6/0/0:5, changed state to down *Dec 16
04:20:45.608 CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/0:6,
changed state to down *Dec 16 04:20:45.610 CST: %LINK-3-UPDOWN:
Interface Integrated-Cable6/0/0:7, changed state to down *Dec 16
04:20:45.648 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Bundle1, changed state to up *Dec 16 04:20:45.649 CST: %LINK-3-UPDOWN:
Interface Bundle1, changed state to up *Dec 16 04:20:45.649 CST:
%LINK-3-UPDOWN: Interface Cable6/0/0, changed state to down *Dec 16
04:20:45.649 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Cable6/0/0 changed state to down
*Dec 16 04:20:45.666 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:0, changed state to down *Dec 16 04:20:45.666 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:1, changed state to down
*Dec 16 04:20:45.681 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:2, changed state to down *Dec 16 04:20:45.681 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:3, changed state to down
*Dec 16 04:20:45.681 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:4, changed state to down *Dec 16 04:20:45.681 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:5, changed state to down
*Dec 16 04:20:45.682 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:6, changed state to down *Dec 16 04:20:45.682 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:7, changed state to down
*Dec 16 04:20:45.685 CST: %LINK-3-UPDOWN: Interface
Integrated-Cable6/0/1:0, changed state to down *Dec 16 04:20:45.694
CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/1:1, changed state
to down *Dec 16 04:20:45.694 CST: %LINK-3-UPDOWN: Interface Cable6/0/1,
changed state to down *Dec 16 04:20:45.694 CST: %SNMP-5-LINK_DOWN:
LinkDown:Interface
Cable6/0/1 changed state to down
*Dec 16 04:20:45.699 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/1:0, changed state to down *Dec 16 04:20:45.703 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/1:1, changed state to down
*Dec 16 04:20:45.706 CST: %LINK-3-UPDOWN: Interface
```

```
Integrated-Cable6/0/1:2, changed state to down *Dec 16 04:20:45.707
CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/1:3, changed state
to down *Dec 16 04:20:45.709 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/2:0, changed state to down *Dec 16 04:20:46.469 CST:
%SNMP-5-COLDSTART: SNMP agent on host sig-cbr is undergoing a cold
start *Dec 16 04:20:46.472 CST: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0, changed state to up *Dec 16 04:20:46.543
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/2, changed state to down *Dec 16 04:20:46.546
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/3, changed state to down *Dec 16 04:20:46.548
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/4, changed state to down *Dec 16 04:20:46.551
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/5, changed state to down *Dec 16 04:20:46.571
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/6, changed state to down *Dec 16 04:20:46.574
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/7, changed state to down *Dec 16 04:20:46.576
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/0, changed state to down *Dec 16 04:20:46.578
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/1, changed state to down *Dec 16 04:20:46.580
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/2, changed state to down *Dec 16 04:20:46.582
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/3, changed state to down *Dec 16 04:20:46.584
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/4, changed state to down *Dec 16 04:20:46.586
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/5, changed state to down *Dec 16 04:20:46.588
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/6, changed state to down *Dec 16 04:20:46.590
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/7, changed state to down *Dec 16 04:20:46.641
CST: %SYS-6-BOOTTIME: Time taken to reboot after reload =  374 seconds
*Dec 16 04:20:53.697 CST: %IOSXE-1-PLATFORM: R0/0: kernel: Raptor MAC
image download wrote 55917152 bytes *Dec 16 04:21:23.432 CST:
%TRANSCEIVER-6-INSERTED: CLC4: iomd:
transceiver module inserted in TenGigabitEthernet4/1/0 *Dec 16
04:21:23.435 CST: %TRANSCEIVER-6-INSERTED: CLC4: iomd:
transceiver module inserted in TenGigabitEthernet4/1/1 *Dec 16
04:21:23.440 CST: %TRANSCEIVER-6-INSERTED: CLC4: iomd:
transceiver module inserted in TenGigabitEthernet4/1/4 *Dec 16
04:21:29.430 CST: %CBRDTI-5-DTISLOT: DTI slot 4/1: card role changed to
Active

*Dec 16 04:21:29.454 CST: %SPA_OIR-6-ONLINECARD: SPA (CBR-SUPPIC-8X10G)
online in subslot 4/1 *Dec 16 04:21:31.403 CST: %LINK-3-UPDOWN:
Interface TenGigabitEthernet4/1/0, changed state to up *Dec 16
04:21:31.405 CST: %CBR_SPA-7-RAPTOR_ESI_EGRESS_HDR_LO_INTERRUPT:
CLC4: iomd:  LOCAL RAPTOR, DP 0, channel_not_found_err *Dec 16
04:21:31.412 CST: %LINK-3-UPDOWN: Interface TenGigabitEthernet4/1/1,
changed state to up *Dec 16 04:21:32.403 CST: %LINEPROTO-5-UPDOWN: Line
protocol on Interface TenGigabitEthernet4/1/0, changed state to up *Dec
16 04:21:32.412 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/1, changed state to up *Dec 16 04:21:41.171 CST:
%IOSXE-3-PLATFORM: R0/0: kernel: i801_smbus
0000:00:1f.3: Transaction timeout
*Dec 16 04:21:41.174 CST: %IOSXE-3-PLATFORM: R0/0: kernel:
/nobackup/ram/ece5-bk/binos/os/linux/drivers/binos/i2c/max3674/max3674_
mai n.c:show_reg_pll (line 88): show_reg_pll failed *Dec 16
04:21:58.237 CST: %IOSXE-5-PLATFORM: CLC6: cdman: Basestar FPGA rev_id
0x00000002, fpga_rev_id 0x00000032 *Dec 16 04:21:59.074 CST:
%CMRP-3-BAD_ID_HW: R0/0: cmand:  Failed Identification Test in CBR
linecard. The module linecard slot 6 in this router may not be a
genuine Cisco product. Cisco warranties and support programs only apply
to genuine Cisco products. If Cisco determines that your insertion of
non-Cisco memory, WIC cards, AIM cards,  Network Modules, SPA cards,
GBICs or other modules into a  Cisco product is the cause of a support
issue, Cisco may  deny support under your warranty or under a Cisco
support  pro *Dec 16 04:21:59.075 CST: %IOSXE_OIR-6-ONLINECARD: Card
(cc) online in slot 6 *Dec 16 04:22:08.825 CST:
```

```
%ASR1000_INFRA-3-EOBC_SOCK: CLC6:
ubrclc-k9lc-ms:  Socket event for  EO6/0/1, fd 11, failed to bind;
Address already in use success *Dec 16 04:22:09.605 CST:  SNMP IPC
session up(RP <-> slot 6)!
*Dec 16 04:22:09.605 CST:  CMTS IPC session up!
*Dec 16 04:22:14.564 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Cable6/0/0-upstream0 changed state to up *Dec 16 04:22:14.565 CST:
%SNMP-5-LINK_UP: LinkUp:Interface
Cable6/0/0-upstream1 changed state to up *Dec 16 04:22:14.566 CST:
%SNMP-5-LINK_UP: LinkUp:Interface
Cable6/0/2-upstream0 changed state to up *Dec 16 04:22:14.566 CST:
%SNMP-5-LINK_UP: LinkUp:Interface
Cable6/0/2-upstream1 changed state to up *Dec 16 04:22:15.051 CST:
%SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/0 changed state to up *Dec
16 04:22:15.258 CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/1
changed state to up *Dec 16 04:22:15.258 CST: %SNMP-5-LINK_UP:
LinkUp:Interface Cable6/0/2 changed state to up *Dec 16 04:22:15.259
CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/3 changed state to up
*Dec 16 04:22:15.259 CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/4
changed state to up *Dec 16 04:22:15.411 CST: %SNMP-5-LINK_UP:
LinkUp:Interface Cable6/0/5 changed state to up *Dec 16 04:22:15.411
CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/6 changed state to up
*Dec 16 04:22:15.411 CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/7
changed state to up *Dec 16 04:22:15.411 CST: %SNMP-5-LINK_UP:
LinkUp:Interface Cable6/0/8 changed state to up *Dec 16 04:22:15.432
CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/9 changed state to up
*Dec 16 04:22:15.432 CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/10
changed state to up *Dec 16 04:22:15.433 CST: %SNMP-5-LINK_UP:
LinkUp:Interface Cable6/0/11 changed state to up *Dec 16 04:22:15.433
CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/12 changed state to up
*Dec 16 04:22:15.433 CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/13
changed state to up *Dec 16 04:22:15.433 CST: %SNMP-5-LINK_UP:
LinkUp:Interface Cable6/0/14 changed state to up *Dec 16 04:22:15.433
CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/15 changed state to up
*Dec 16 04:22:15.677 CST: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Cable6/0/8, changed state to up *Dec 16 04:22:15.678 CST:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Cable6/0/9, changed
state to up *Dec 16 04:22:15.901 CST: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Cable6/0/10, changed state to up *Dec 16
04:22:15.902 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/11, changed state to up *Dec 16 04:22:15.902 CST:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Cable6/0/12, changed
state to up *Dec 16 04:22:15.903 CST: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Cable6/0/13, changed state to up *Dec 16
04:22:15.903 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/14, changed state to up *Dec 16 04:22:15.904 CST:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Cable6/0/15, changed
state to up *Dec 16 04:22:17.046 CST: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Cable6/0/0, changed state to up *Dec 16
04:22:17.047 CST: %LINK-3-UPDOWN: Interface Cable6/0/0, changed state
to up *Dec 16 04:22:17.256 CST: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Cable6/0/1, changed state to up *Dec 16 04:22:17.257 CST:
%LINK-3-UPDOWN: Interface Cable6/0/1, changed state to up *Dec 16
04:22:17.259 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/2, changed state to up *Dec 16 04:22:17.260 CST:
%LINK-3-UPDOWN: Interface Cable6/0/2, changed state to up *Dec 16
04:22:17.260 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/3, changed state to up *Dec 16 04:22:17.260 CST:
%LINK-3-UPDOWN: Interface Cable6/0/3, changed state to up *Dec 16
04:22:17.260 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/4, changed state to up *Dec 16 04:22:17.260 CST:
%LINK-3-UPDOWN: Interface Cable6/0/4, changed state to up *Dec 16
04:22:17.411 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/5, changed state to up *Dec 16 04:22:17.411 CST:
%LINK-3-UPDOWN: Interface Cable6/0/5, changed state to up *Dec 16
04:22:17.411 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/6, changed state to up *Dec 16 04:22:17.411 CST:
%LINK-3-UPDOWN: Interface Cable6/0/6, changed state to up *Dec 16
04:22:17.411 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/7, changed state to up *Dec 16 04:22:17.412 CST:
%LINK-3-UPDOWN: Interface Cable6/0/7, changed state to up *Dec 16
04:22:16.714 CST: %IOSXE-5-PLATFORM: CLC6: cdman: DS-JIB:ILK Interrupts
Enabled. (Init:20539, Check:9566 1stPKO:8942) *Dec 16 04:22:17.809 CST:
```

```
%CMRP-3-IDPROM_SENSOR: R0/0: cmand:  One or more sensor fields from the
idprom failed to parse properly because Invalid argument.
Dec 16 04:22:57.161 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream0 changed state to down Dec 16
04:22:57.161 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream1 changed state to down Dec 16
04:22:57.161 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream2 changed state to down Dec 16
04:22:57.162 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream3 changed state to down Dec 16
04:22:57.162 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream4 changed state to down Dec 16
04:22:57.162 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream5 changed state to down Dec 16
04:22:57.162 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream6 changed state to down Dec 16
04:22:57.162 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream7 changed state to down Dec 16
04:22:57.163 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream8 changed state to down Dec 16
04:22:57.163 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream9 changed state to down Dec 16
04:22:57.163 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream10 changed state to down Dec 16
04:22:57.163 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/1-downstream0 changed state to down Dec 16
04:22:57.164 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/1-downstream1 changed state to down Dec 16
04:22:57.164 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/1-downstream2 changed state to down Dec 16
04:22:57.164 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/1-downstream3 changed state to down Dec 16
04:22:57.164 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/1-downstream4 changed state to down Dec 16
04:22:57.164 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/1-downstream5 changed state to down Dec 16
04:22:57.183 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream0 changed state to up Dec 16
04:22:57.184 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream1 changed state to up Dec 16
04:22:57.189 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream2 changed state to up Dec 16
04:22:57.211 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream3 changed state to up Dec 16
04:22:57.212 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream4 changed state to up Dec 16
04:22:57.212 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream6 changed state to up Dec 16
04:22:57.213 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream7 changed state to up Dec 16
04:22:57.213 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream8 changed state to up Dec 16
04:22:57.213 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream9 changed state to up Dec 16
04:22:57.213 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream10 changed state to up Dec 16
04:22:57.214 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/1-downstream0 changed state to up Dec 16
04:22:57.424 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/1-downstream1 changed state to up Dec 16
04:22:57.426 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/1-downstream2 changed state to up Dec 16
04:22:57.435 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/1-downstream3 changed state to up Dec 16
04:22:57.437 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/1-downstream4 changed state to up Dec 16
04:22:57.449 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/1-downstream5 changed state to up Dec 16
04:22:59.219 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Integrated-Cable6/0/1:0, changed state to up Dec 16 04:22:59.219 CST:
%LINK-3-UPDOWN: Interface Integrated-Cable6/0/1:0, changed state to up
Dec 16 04:22:59.427 CST: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Integrated-Cable6/0/1:1, changed state to up Dec 16
```

```
04:22:59.427 CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/1:1,
changed state to up Dec 16 04:22:59.449 CST: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Wideband-Cable6/0/0:0, changed state to up Dec 16
04:22:59.450 CST: %LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:0,
changed state to up Dec 16 04:22:59.450 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:1, changed state to up Dec 16 04:22:59.450 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:2, changed state to up
Dec 16 04:22:59.450 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:3, changed state to up Dec 16 04:22:59.450 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:4, changed state to up
Dec 16 04:22:59.450 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:5, changed state to up Dec 16 04:22:59.451 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:6, changed state to up
Dec 16 04:22:59.451 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:7, changed state to up Dec 16 04:22:59.451 CST:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Wideband-Cable6/0/1:0,
changed state to up Dec 16 04:22:59.451 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/1:0, changed state to up Dec 16 04:22:59.451 CST:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Wideband-Cable6/0/1:1,
changed state to up Dec 16 04:22:59.452 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/1:1, changed state to up Dec 16 04:22:59.452 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/2:0, changed state to up
Dec 16 04:23:27.352 CST: %IOSXE-5-PLATFORM: CLC6: cdman: DSPHY Gemini
module  1 was not present Dec 16 04:26:59.885 CST:
%ENVIRONMENTAL-1-ALERT: Temp: INLET, Location:
6, State: Critical, Reading: 53 Celsius sig-cbr#</aml-block:Data>
</aml-block:Attachment> </aml-block:Attachments> </aml-block:Block>
</soap-env:Body> </soap-env:Envelope>
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS XE コマンド	『Cisco IOS Master Commands List, All Releases』
すべての関連製品の情報にアクセスするための Cisco.com の Smart Call Home のサイト ページ。	『Cisco Smart Call Home site』
Smart Call Home サービスが選択したシスコ デバイスに Web アクセスする方法、また予防的診断を行い、リアルタイム アラートを提供することでネットワーク可用性を向上して業務の効率化を図る方法を説明します。	『Smart Call Home User Guide』
Call Home クイック スタート ガイド	『Smart Call Home Quick Start Configuration Guide for Cisco cBR Series Routers』

MIB

MIB	MIB のリンク
CISCO-CALLHOME-MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

Call Home に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *232* : *Call Home* に関する機能情報

機能名	リリース	機能情報
Smart Call Home	Cisco IOS XE Everest 16.6.1	この機能は、 Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 91 章

SNMP Support over VPNs：コンテキストベース アクセス コントロール

SNMP Support over VPNs：コンテキストベース アクセス コントロール機能は、SNMP コンテキスト サポートのインフラストラクチャを使用して、シスコ ソフトウェアでの複数のシンプル ネットワーク管理プロトコル（SNMP）のコンテキストのサポートに対応するインフラストラクチャ、および VPN 対応の MIB インフラストラクチャを提供します。

機能情報の確認

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソ

フトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *233* : ***Cisco cBR*** シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

SNMP Support over VPNs の制限事項：コンテキストベース アクセス コントロール

- **nosnmp-servercontext** コマンドを使用して SNMP コンテキストを削除すると、そのコンテキストのすべての SNMP インスタンスが削除されます。
- すべての MIB が VPN に対応しているわけではありません。

SNMP Support over VPNs に関する情報：コンテキストベース アクセス コントロール

SNMP のバージョンとセキュリティ

Cisco ソフトウェアでは、次のバージョンの SNMP がサポートされています。

- SNMPv1：RFC 1157 で規定された、完全なインターネット標準のシンプル ネットワーク管理プロトコル（RFC 1157 は、RFC 1067 および RFC 1098 として公開されたそれより古いバージョンを置き換えるものです）。コミュニティ ストリングに基づいてセキュリティを実現します。
- SNMPv2c：SNMPv2 のためのコミュニティ ストリング ベースの管理フレームワーク。SNMPv2c（「c」は「community」を示す）は RFC 1901、RFC 1905、および RFC 1906 で規定されている実験的なインターネット プロトコルです。SNMPv2c は、SNMPv2p（SNMPv2 Classic）のプロトコル操作とデータ タイプが更新されたもので、SNMPv1 のコミュニティベースのセキュリティ モデルを使用します。

SNMP のバージョンに関する情報については、『*Cisco Network Management Configuration Guide*』の「Configuring SNMP Support」モジュールを参照してください。

SNMPv1 または SNMPv2 セキュリティ

Cisco IOS ソフトウェアでは、次のバージョンの SNMP がサポートされています。

- SNMPv1：RFC 1157 で規定された、完全なインターネット標準のシンプル ネットワーク管理プロトコル（RFC 1157 は、RFC 1067 および RFC 1098 として公開されたそれより古いバージョンを置き換えるものです）。コミュニティ ストリングに基づいてセキュリティを実現します。
- SNMPv2c：SNMPv2 のためのコミュニティ ストリング ベースの管理フレームワーク。SNMPv2c（「c」は「community」を示す）は RFC 1901、RFC 1905、および RFC 1906 で規定されている実験的なインターネット プロトコルです。SNMPv2c は、SNMPv2p（SNMPv2 Classic）のプロトコル操作とデータ タイプが更新されたもので、SNMPv1 のコミュニティベースのセキュリティ モデルを使用します。

SNMPv1 と SNMPv2 は、SNMPv3 ほど安全ではありません。SNMP バージョン 1 と 2 では、プレーン テキスト コミュニティを使用し、SNMP バージョン 3 で実行される認証やセキュリティ チェックを実行しません。SNMP バージョン 1 または SNMP バージョン 2 を使用するときに SNMP Support over VPNs：コンテキストベース アクセス コントロール機能を設定するには、コミュニティ名を VPN に関連付ける必要があります。関連付けると、SNMP は、特定のコミュニティ ストリングの着信要求を、設定されている VRF から受信した場合だけ処理します。着信パケットに含まれているコミュニティ ストリングに VRF が関連付けられていない場合は、VRF 以外のインターフェイス経由で着信した場合だけパケットを処理します。このプロセスによって、VPN 外のユーザがクリア テキスト コミュニティ ストリングをスヌーピングして VPN データを照会するのを防ぐことができます。送信元アドレス確認のこれらの方法は、SNMPv3 を使用するほど安全ではありません。

SNMPv3 セキュリティ

SNMPv3 を使用する場合は、常にセキュリティ名を認証や特権パスワードに関連付ける必要があります。SNMPv3 ユーザには送信元アドレス検証が実行されません。VPN のユーザがその VPN に関連付けられたコンテキストにしかアクセスできず、他の VPN の MIB データを表示できない場合、AuthNoPriv の最小セキュリティ レベルを設定する必要があります。

送信元アドレス検証を可能にするには、プロバイダーエッジ（PE）ルータでコミュニティを VRF に関連付けます。ただし、カスタマーエッジ（CE）ルータで送信元アドレス検証を可能にするには、アクセス コントロール リストを使用して送信元アドレスをコミュニティ リストに関連付ける必要があります。

SNMPv3 を使用すると、VPN のユーザのセキュリティ名やセキュリティ パスワードが他の VPN のユーザに知られることがありません。管理情報のセキュリティが必要な場合は、SNMPv3 非承認ユーザを使用しないことをお勧めします。

SNMP Notification Support over VPNs

SNMP Notification Support over VPNs 機能では、VPN ルーティングおよび転送（VRF）インスタンス テーブルを使用して SNMP 通知（トラップおよびインフォーム）の送信および受信を行えます。特に、この機能では、個々の VPN に固有の SNMP 通知（トラップおよびインフォーム）の送受信のために、Cisco ソフトウェアでのサポートが追加されます。

SNMP は、アプリケーション層プロトコルであり、SNMP マネージャと SNMP エージェントとの通信に使用されるメッセージ フォーマットを提供します。

VPN は、プライベート ネットワークと同じ使用ガイドラインを持つ共有システム上での接続性の高い転送を提供するネットワークです。VPN は IP でのインターネット、フレーム リレー、または ATM ネットワーク上で構築できます。

VRF では VPN ごとにルーティング データを保存します。これはネットワーク アクセス サーバ（NAS）に接続された顧客のサイトの VPN メンバーシップを定義します。VRF は、IP ルーティング テーブル、派生する Cisco Express Forwarding（以前の CEF）テーブル、ガイドラインおよびルーティング テーブルに含まれる情報を制御するルーティング プロトコル パラメータで構成されます。

VPN のための SNMP サポート：コンテキストベース アクセス コントロール機能は、ユーザが SNMP エージェントとマネージャを特定の VRF と関連付けることを可能にするコンフィギュレーション コマンドを提供します。関連付けられた VRF は、エージェントとマネージャの間の SNMP 通知（トラップおよびインフォーム）と応答の送信に使用されます。VRF が指定されなかった場合は、その VPN のデフォルトのルーティング テーブルが使用されます。

VPN 対応 SNMP

VPN の SNMP サポート：コンテキストベース アクセス コントロール機能により、SNMP Notification Support for VPNs 機能が拡張され、異なる VPN からの着信パケットを SNMP で区別できるようになります。

VPN の SNMP サポート時：コンテキストベース アクセス コントロール機能が設定され、SNMP は、設定された VRF 要求を受け付け、同じ VRF に応答を返します。トラップ ホストは、特定の VRF に関連付けることもできます。これにより、設定された VRF を使用してトラップが送信されます。関連付けしない場合は、デフォルトのルーティング テーブルが使用されます。特定の VRF にリモート ユーザを関連付けることもできます。また、SNMP が要求を受け入れる必要がある VRF を設定できます。指定されていない VRF から送信される要求はドロップされます。

IP アクセス リストを設定し、SNMP コミュニティ ストリングに関連付けることができます。この機能を使用すると、VRF インスタンスと SNMP コミュニティ ストリング間のアソシエーションを設定できます。VRF インスタンスが SNMP コミュニティ ストリングに関連付けられている場合、SNMP はその要求が設定されている VRF から受信した場合だけ、特定のコミュニティ ストリングの着信要求を処理します。着信パケットに含まれているコミュニティ ストリングに関連付けられている VRF がない場合、コミュニティ ストリングは VRF 以外のインターフェイス経由で着信した場合だけ処理されます。

VRF のミスマッチによりドロップされた SNMP パケットの認証トラップをイネーブルまたはディセーブルにすることもできます。デフォルトでは、SNMP 認証トラップをイネーブルすると、VRF 認証トラップもイネーブルになります。

VPN ルート識別子

ルート識別子（RD）はルーティング テーブルとフォワーディング テーブルを作成し、VPN のデフォルトのルート識別子を指定します。RD は顧客の IPv4 プレフィックスの先頭に追加され、その IPv4 プレフィックスはグローバルに一意の VPN-IPv4 プレフィックスになります。

RD は、自律システム番号と任意の番号で構成される自律システム番号（ASN）相対 RD、または IP アドレスと任意の番号で構成される IP アドレス相対 RD のいずれかです。

RD は、次のいずれかの形式で入力できます。

- 16 ビット ASN：101:3 などの 16 ビット数値
- 32 ビット IP アドレス：192.168.122.15:1 などの 32 ビット数値

SNMP コンテキスト

SNMP コンテキストによって、MIB データにアクセスする安全な方法が VPN ユーザに提供されます。VPN がコンテキストに関連付けられると、VPN 固有の MIB データがそのコンテキストに存在します。VPN をコンテキストに関連付けると、サービス プロバイダーが、複数 VPN でネットワークを管理できます。コンテキストを作成して VPN に関連付けることにより、プロバイダーは、ある VPN のユーザが同じネットワーキング デバイス上で他の VPN のユーザに関する情報にアクセスするのを防ぐことができます。

VPN 対応 SNMP で、SNMP セキュリティ名と VPN ID のマッピングの VPN 環境で実行する SNMP マネージャとエージェント エンティティ間の契約が必要です。このマッピングは、SNMP-VACM-MIB の設定を通じて、異なる VPN の SNMP データ用に複数のコンテキストを使用して作成されます。セキュリティ名を持つ VPN 上のユーザがその VPN のユーザに関連付けられたコンテキストのユーザのアクセス タイプに関連づけられた制限付きオブジェクト領域にアクセスできるように、SNMP-VACM-MIB がビューとともに設定されます。

応答メッセージが、VPN コンテキスト内のオブジェクト値を使用して返信される前に、SNMP 要求メッセージは、セキュリティとアクセス コントロールの次のような 3 つのフェーズを経ます。

- 最初のフェーズでは、ユーザ名が認証されます。このフェーズでは、ユーザが SNMP アクセスに対して認証および許可されるようにします。
- 第 2 フェーズでは、ユーザは、設定されている SNMP コンテキストの考慮時にグループ オブジェクトに対して要求された SNMP アクセス用に承認されます。このフェーズは、アクセス制御フェーズと呼ばれます。
- 第 3 フェーズでは、テーブル エントリの特定のインスタンスへのアクセスが行われます。この 3 つ目のフェーズでは、完全な取得は、SNMP コンテキスト名を使用して行えます。

SNMP Support over VPNs の設定方法：コンテキストベース アクセス コントロール

SNMP コンテキストの設定および SNMP コンテキストと VPN の関連付け

SNMP コンテキストを設定し、VPN と SNMP コンテキストを関連付けるには、この作業を実行します。

（注）
- 次の MIB コンテキストだけを認識します。これらの MIB のすべてのテーブルをポーリングできます。
  - CISCO-IPSEC-FLOW-MONITOR-MIB
  - CISCO-IPSEC-MIB
  - CISCO-PING-MIB
  - IP-FORWARD-MIB
  - MPLS-LDP-MIB
- IP-FORWARD-MIB の 2 個の SNMP 変数 1.3.6.1.2.1.4.24.3（ipCidrRouteNumber：スカラ）と 1.3.6.1.2.1.4.24.4.1（ipCidrRouteEntry：テーブル）だけをポーリングできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**snmp-servercontext** *context-name* 例： `Device(config)# snmp-server context context1`	SNMP コンテキストを作成し、その名前を指定します。
ステップ 4	**vrf definition** *vrf-name* 例： `Device(config)# vrf definition vrf1`	VRF ルーティング テーブルを設定し、VRF コンフィギュレーション モードを開始します。
ステップ 5	**rd** *route-distinguisher* 例： `Device(config-vrf)# rd 100:120`	VPN ルート識別子を作成します。

	コマンドまたはアクション	目的
ステップ 6	**context** *context-name* 例： `Device(config-vrf)# context context1`	SNMP コンテキストを特定の VRF に関連付けます。 （注） リリースに応じて、**context** コマンドは **snmpcontext** コマンドに置き換えられます。詳細については、『*Cisco IOS Network Management Command Reference*』を参照してください。
ステップ 7	**route-target** {**import** | **export** | **both**} *route-target-ext-community* 例： `Device(config-vrf)# route-target export 100:1000`	（任意）VRF 用の route-target 拡張コミュニティを作成します。
ステップ 8	**end** 例： `Device(config-vrf)# end`	インターフェイス モードを終了し、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 9	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了します。

SNMP サポートの設定および SNMP コンテキストの関連付け

SNMP サポートの設定と SNMP コンテキストへの関連付けを行うには、この作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	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	**snmp-serveruser** *username group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] {**v1** | **v2c** | **v3** [**encrypted**] [**auth** {**md5** | **sha**} *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** {**des** | **3des** | **aes** {**128** | **192** | **256**}} *privpassword*] {*acl-number* | *acl-name*}] 例： `Device(config)# snmp-server user customer1 group1 v1`	SNMP グループに新しいユーザを設定します。
ステップ 4	**snmp-servergroup** *group-name* {**v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**}} [**context** *context-name*] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*] [*acl-number*| *acl-name*]] 例： `Device(config)# snmp-server group group1 v1 context context1 read view1 write view1 notify view1`	新規 SNMP グループ、または SNMP ユーザを SNMP ビューにマッピングするテーブルを設定します。 • **context** *context-name* キーワードと引数のペアを使用して、指定した SNMP グループを設定済み SNMP コンテキストに関連付けます。
ステップ 5	**snmp-serverview** *view-name oid-tree* {**included** | **excluded**} 例： `Device(config)# snmp-server view view1 ipForward included`	ビュー エントリを作成または更新します。
ステップ 6	**snmp-serverenabletraps** [*notification-type*] [**vrrp**] 例： `Device(config)# snmp-server enable traps`	システムで使用できるすべての SNMP 通知（トラップまたは応答要求）をイネーブルにします。
ステップ 7	**snmp-servercommunity** *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number* | *extended-access-list-number* | *access-list-name*]	SNMP へのアクセスを許可するコミュニティ アクセス ストリングを設定します。

	コマンドまたはアクション	目的
	例： `Device(config)# snmp-server community public view view1 rw`	
ステップ 8	**snmp-serverhost** {*hostname* | *ip-address*} [**vrf** *vrf-name*] [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] 例： `Device(config)# snmp-server host 10.0.0.1 vrf vrf1 public udp-port 7002`	SNMP 通知動作の指定
ステップ 9	**snmpmibcommunity-map** *community-name* [**context** *context-name*] [**engineid** *engine-id*] [**security-name** *security-name*][**target-list** *upn-list-name*] 例： `Device(config)# snmp mib community-map community1 context context1 target-list commAVpn`	SNMP コミュニティを SNMP コンテキスト、エンジン ID、またはセキュリティ名にマッピングします。
ステップ 10	**snmpmibtargetlist** *vpn-list-name* {**vrf** *vrf-name* | **host** *ip-address*} 例： `Device(config)# snmp mib target list commAVpn vrf vrf1`	SNMP コミュニティに関連付けるターゲット VRF とホストのリストを作成します。
ステップ 11	**nosnmp-servertrapauthenticationvrf** 例： `Device(config)# no snmp-server trap authentication vrf`	（任意）VRF インターフェイスで受信したパケットについて生成されるすべての SNMP 認証通知（トラップまたは応答要求）をディセーブルにします。 • このコマンドを使用して、関連付けられているコミュニティが正しくない VRF インターフェイス上のパケットに対する認証トラップだけをディセーブルにします。

SNMP Support over VPNs の設定例：コンテキスト ベース アクセス コントロール

例：コンテキストベース アクセス コントロールの設定

次の設定例では、SNMP Support over VPNs（SNMPv1 または SNMPv2 のコンテキストベース アクセス コントロール機能）の設定方法を示します。

（注） リリースに応じて、**context** コマンドは **snmpcontext** コマンドに置き換えられます。詳細については、『*Cisco IOS Network Management Command Reference*』を参照してください。

```
snmp-server context A
snmp-server context B
ip vrf Customer_A
 rd 100:110
 context A
 route-target export 100:1000
 route-target import 100:1000
!
ip vrf Customer_B
 rd 100:120
 context B
 route-target export 100:2000
 route-target import 100:2000
!
interface TenGigabitEthernet4/1/0
 description Belongs to VPN A
 ip vrf forwarding CustomerA
 ip address 192.168.2.1 255.255.255.0

interface TenGigabitEthernet4/1/1
 description Belongs to VPN B
 ip vrf forwarding CustomerB
 ip address 192.168.2.2 255.255.255.0
snmp-server user commA grp1A v1
snmp-server user commA grp2A v2c
snmp-server user commB grp1B v1
snmp-server user commB grp2B v2c
snmp-server group grp1A v1 context A read viewA write viewA notify viewA
snmp-server group grp1B v1 context B read viewB write viewB notify viewB
snmp-server view viewA ipForward included
snmp-server view viewA ciscoPingMIB included
snmp-server view viewB ipForward included
snmp-server view viewB ciscoPingMIB included
snmp-server enable traps
snmp-server host 192.168.2.3 vrf CustomerA commA udp-port 7002
snmp-server host 192.168.2.4 vrf CustomerB commB udp-port 7002
snmp mib community-map commA context A target-list commAvpn
! Configures source address validation
snmp mib community-map commB context B target-list commBvpn
! Configures source address validation
snmp mib target list commAvpn vrf CustomerA
! Configures a list of VRFs or from which community commA is valid
snmp mib target list commBvpn vrf CustomerB
! Configures a list of VRFs or from which community commB is valid
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
シスコ ソフトウェア コマンド	『Cisco IOS Master Command List, All Releases』
シスコ ネットワーク管理コマンド	『*Cisco IOS Network Management Command Reference*』
SNMP コンフィギュレーション	『*Cisco Network Management Configuration Guide*』「Configuring SNMP Support」章
VPN のための SNMP サポート	『SNMP Notification Support for VPNs』

標準

規格	タイトル
なし	--

MIB

MIB	MIB のリンク
• CISCO-PING-MIB • IP-FORWARD-MIB • SNMP-VACM-MIB、*SNMP* 用 *View-based Access Control Model*（*ACM*）*MIB*	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 1441	『*Introduction to version 2 of the Internet-standard Network Management Framework*』

RFC	タイトル
RFC 1442	『*Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)*』
RFC 1443	『*Textual Conventions for version 2 of the Simple Network Management Protocol (SNMPv2)*』
RFC 1444	『*Conformance Statements for version 2 of the Simple Network Management Protocol (SNMPv2)*』
RFC 1445	『*Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2)*』
RFC 1446	『*Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)*』
RFC 1447	『*Party MIB for version 2 of the Simple Network Management Protocol (SNMPv2)*』
RFC 1448	『*Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)*』
RFC 1449	『*Transport Mappings for version 2 of the Simple Network Management Protocol (SNMPv2)*』
RFC 1450	『*Management Information Base for version 2 of the Simple Network Management Protocol (SNMPv2)*』
RFC 2571	『*An Architecture for Describing SNMP Management Frameworks*』
RFC 2576	『*Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

SNMP Support over VPNs に関する機能情報：コンテキストベース アクセス コントロール

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *234*：***SNMP Support over VPNs*** に関する機能情報：コンテキストベース アクセス コントロール

機能名	リリース	機能情報
SNMP Support over VPNs：コンテキストベース アクセス コントロール	Cisco IOS XE Everest 16.6.1	この機能は、 Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 92 章

SNMP エンジンの機能拡張

SNMP キャッシュ エンジンの機能拡張により、スーパーバイザ上の SNMP 情報がキャッシュされます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *235* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

SNMP キャッシュ エンジンの機能拡張に関する制限事項

キャッシュされた情報をスーパーバイザで使用できる時間間隔は 5 秒間です。

SNMP キャッシュ エンジンの機能拡張に関する情報

SNMP キャッシュ エンジンの機能拡張は、MIB テーブルについて スーパーバイザ に情報をキャッシュします。MIB テーブルはインターフェイス カードからデータを取得する必要があります。MIB テーブル項目がインターフェイス カードから照会されると、次の *N* 個の項目が取得され、スーパーバイザ にキャッシュされます。

たとえば、SNMP クライアントが docsIf3CmtsCmRegStatusMacAddr.1 を照会すると、インターフェイス カードは docsIf3CmtsCmRegStatusMacAddr.1、docsIf3CmtsCmRegStatusMacAddr.2、docsIf3CmtsCmRegStatusMacAddr.3、.... docsIf3CmtsCmRegStatusMacAddr.N を 1 つの IPC 応答にバンドルして、スーパーバイザに送信します。スーパーバイザは、すべての項目をローカルにキャッシュします。SNMP クライアントが後で docsIf3CmtsCmRegStatusMacAddr.2 を照会すると、別の IPC メッセージをインターフェイス カードに送信しなくても、その情報を スーパーバイザ キャッシュで直接使用できます。数 *N* は、単一 MIB 項目サイズと最大 IPC メッセージ バッファ サイズによって異なります。

次の MIB について、MIB テーブル情報が取得され、スーパーバイザ にキャッシュされます。

- DOCS-IF-MIB
- DOCS-IFEXT2-MIB
- DOCS-QOS-MIB
- DOCS-IF3-MIB
- DOCS-IF31-MIB
- DOCS-QOS3-MIB
- DOCS-IETF-QOS-MIB
- DOCS-BPI-PLUS-MIB
- DOCS-LOADBALANCING-MIB
- DOCS-LOADBAL3-MIB
- DOCS-DSG-IF-MIB
- CISCO-DOCS-EXT-MIB
- CISCO-CABLE-WIDEBAND-MIB
- CISCO-CABLE-SPECTRUM-MIB

この機能は、Cisco cBR ルータでデフォルトで有効です。SNMP キャッシュ情報が スーパーバイザ に保存される時間間隔は、期間経過と呼ばれ、5 秒に設定されます。

SNMP キャッシュ エンジンの機能拡張の設定方法

はじめる前に

SNMP キャッシュ エンジンの機能拡張を有効または無効にするには、グローバル コンフィギュレーション モードで **service internal** コマンドを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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 snmp cache active** 例： `Router(config)# cable snmp cache active`	SNMP キャッシュ ステータスをアクティブに設定します。 （注） SNMP キャッシュ ステータスを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 4	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

SNMP キャッシュ エンジン ステータスの確認

現在の SNMP キャッシュ エンジンのステータスを表示するには、**show cable snmp cache-status** コマンドを使用します。

重要 SNMP キャッシュ エンジンのステータスを確認するには、グローバル コンフィギュレーション モードで **service internal** コマンドを設定する必要があります。

次に、コマンドの出力例を示します。

```
Router# show cable snmp cache-status
```

```
    Cache engine is ON, age: 5 seconds
```

キャッシュ カウンタの情報を表示するには、**test cable snmp counter-show** コマンドを使用します。

```
Router# test cable snmp counter-show
========== cache counters ==========
ubrcce_snmp_cache_hit_counter:0.
ubrcce_snmp_cache_get_from_lc_counter:1.
ubrcce_snmp_cache_miss_counter:0.
ubrcce_snmp_cache_ipc_fail_counter:0.
ubrcce_snmp_cache_buffer_full_counter:0.
```

hit および *mis* は、システム起動後の SNMP キャッシュの履歴情報です。*hit* は SNMP クエリがキャッシュ内でヒットした回数を示し、*mis* は SNMP クエリが SNMP キャッシュ内でヒットしなかった回数を示します。

その他の参考資料

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

SNMP キャッシュ エンジンの機能拡張に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *236* : *SNMP* キャッシュ エンジンの機能拡張に関する機能情報

機能名	リリース	機能情報
SNMP キャッシュ エンジンの機能拡張	Cisco IOS XE Everest 16.6.1	この機能は、 Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 93 章

オンボード障害ロギング

オンボード障害ロギング（OBFL）は、ハードウェア障害および環境情報を取得して不揮発性メモリに保存します。OBFLにより、ハードウェアのトラブルシューティングと根本原因の分離解析をより正確に行うことができます。保存されたOBFLデータは、ルータのクラッシュや障害時に取得できます。

機能情報の確認

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *237* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

OBFL の概要

OBFL は、ルータ上のフラッシュ EPROM、EEPROM などの不揮発性メモリに、ハードウェア、ソフトウェア、および環境関連のクリティカル データを保存するメカニズムを提供します。ハー

ドウェア問題をトラブルシューティングし、解決するために、TAC チームによってロギング情報が使用されます。

OBFL は、温度や電圧などのデータを収集します。データは、ルータのフラッシュ メモリの専用エリアに保存されます。このデータを TAC の担当者は取得して、ルータをトラブルシューティングします。また、このデータをバックエンド ソフトウェアで分析することで、障害パターンを検出し、場合によっては具体的な品質向上を提案することができます。

OBFL メッセージの取得

ハードウェアに欠陥があり、システムが起動できない場合、フラッシュ内のデータにはアクセスできません。この場合、OBFL データを回復するために、次のいずれかの方法を実行してください。

- JTAG によるフラッシュの読み込み：これには、ハードウェア設計でのプロビジョニング、バックエンドのハードウェアおよびソフトウェアのサポート ツールが必要です。
- システムを修復し、システムを起動して、OBFL CLI コマンドを使用します。

OBFL の設定

指定したハードウェア モジュールで OBFL を有効（イネーブル）または無効にするには、**hw-module** {**all**|**slot**|**module**} {*slotnumber*/*subslotnumber*|*modulenumber*} **logging onboard** {**disable** | **enable**} コマンドを使用します。

（注） OBFL はデフォルトでイネーブルになっています。

```
Router# hw-module slot R0 logging onboard enable
```

OBFL ロギング情報の表示

OBFL のログ情報を表示するには、**show logging onboard** {**slot**|**module**|**bay**} {*slotnumber*/*subslotnumber*|*modulenumber*} {**dram** | **message** | **serdes** | **status** | **temperature** | **uptime** | **voltage**] コマンドを使用します。

（注） OBFL は、Cisco cBR シリーズ ルータでデフォルトでイネーブルになっています。

カード PIC の OBFL 情報を表示するには、**show logging onboardbay** *slotnumber*/*subslotnumber* {**dram** | **message** | **serdes** | **status** | **temperature** | **uptime** | **voltage**] コマンドを使用します。

OBFL ロギングのクリア

OBFL ロギングをクリアするには、**clear logging onboard** {**slot**|**module**} {*slotnumber*|*subslotnumber*|*modulenumber*} {**dram** | **message** | **serdes** | **temperature** | **voltage**} コマンドを使用します。

次の例に、DRAM ECC エラー ログをクリアする方法を示します。

```
Router# clear logging onboard slot R0 dram
```

次の例に、OBFL エラー メッセージをクリアする方法を示します。

```
Router# clear logging onboard slot R0 message
```

次の例に、オンボードの SerDes ログをクリアする方法を示します。

```
Router# clear logging onboard slot R0 serdes
```

次の例に、オンボードの温度ログをクリアする方法を示します。

```
Router# clear logging onboard slot R0 temperature
```

次の例に、オンボードの電圧ログをクリアする方法を示します。

```
Router# clear logging onboard slot R0 voltage
```

設定および確認の例

例：OBFL 設定ステータスの確認

```
Router#show logging onboard slot R1 status
Status: Enabled

Router#show logging onboard slot 5 status
Status: Disabled
```

例：OBFL ログの表示

```
Router#show logging onboard slot R1 message
timestamp            module    sev  message

------------------------------------------------------------------------------------------------------------------------
01/01/12 12:00:23    SUP_PSOC  3    SUP MB PSOC alert interrupt

01/01/12 12:00:23    SUP_PSOC  3    SUP MB PSOC alert interrupt

01/01/12 12:00:23    SUP_PSOC  3    SUP MB PSOC alert interrupt

01/01/12 12:00:23    SUP_PSOC  3    SUP MB PSOC alert interrupt

01/01/12 12:01:15    SUP_PSOC  3    SUP MB PSOC alert interrupt
```

```
Router#show logging onboard slot R1 voltage
Name              Id    Data (mV)  Poll      Last Update
-------------------------------------------------------------------
PSOC-MB2_20: VO   40         1791  1         01/01/12 17:03:03
PSOC-MB2_21: VO   41         3290  1         01/01/12 17:03:03
PSOC-MB2_22: VO   42         3293  1         01/01/12 17:03:03
PSOC-MB2_23: VO   43         3299  1         01/01/12 17:03:03
PSOC-MB2_24: VO   44         4958  1         01/01/12 17:03:03
PSOC-MB2_25: VO   45         4508  1         01/01/12 17:03:03
```

```
PSOC-MB3_0: VOU   46         4999  1         01/01/12 17:03:03
PSOC-MB3_1: VOU   47         4982  1         01/01/12 17:03:03
PSOC-MB3_2: VOU   48         1499  1         01/01/12 17:03:03
PSOC-MB3_3: VOU   49         1193  1         01/01/12 17:03:03
PSOC-MB3_4: VOU   50          708  1         01/01/12 17:03:03
PSOC-MB3_5: VOU   51          757  1         01/01/12 17:03:03
PSOC-MB3_6: VOU   52          585  1         01/01/12 17:03:03
PSOC-MB3_7: VOU   53         1501  1         01/01/12 17:03:03
```

```
Router#show logging onboard slot R1 temperature
Name              Id     Data (C)  Poll      Last Update
-------------------------------------------------------------------------
Temp: BB_DIE      159          25  1         01/02/12 23:04:19
Temp: VP_DIE      160          21  1         01/02/12 23:04:19
Temp: RT-E_DIE    161          29  1         01/02/12 23:04:19
Temp: INLET_1     162          20  1         01/02/12 23:04:19
Temp: INLET_2     163          18  1         01/02/12 23:04:19
Temp: OUTLET_1    164          22  1         01/02/12 23:04:19
Temp: 3882_1      165          44  1         01/02/12 23:04:19
Temp: 3882_1A     166          38  1         01/02/12 23:04:19
Temp: 3882_1B     167          36  1         01/02/12 23:04:19
Temp: 3882_2      168          38  1         01/02/12 23:04:19
Temp: 3882_2A     169          37  1         01/02/12 23:04:19
Temp: 3882_2B     170          35  1         01/02/12 23:04:19
Temp: 3882_3      171          38  1         01/02/12 23:04:19
```

```
Router#show logging onboard slot R1 uptime latest
 Slot              Reset reason  Power On
-----------------------------------------------------------
    1      reset local software  01/02/12 23:02:46
```

```
Router#show logging onboard slot R1 uptime
 Slot              Reset reason  Power On
-----------------------------------------------------------
    0      reset local software  01/06/12 01:52:26
    4      reset local software  01/06/12 01:52:42
    0      reset local software  01/06/12 01:52:45
    0      reset local software  01/06/12 02:20:27
    4      reset local software  01/06/12 02:20:43
    0      reset local software  01/06/12 02:20:46
    0      reset local software  01/06/12 05:12:02
    4      reset local software  01/06/12 05:12:19
    0      reset local software  01/06/12 05:12:22
    0      reset local software  01/06/12 05:17:31
    4      reset local software  01/06/12 05:17:48
    0      reset local software  01/06/12 05:17:51
    0            reset power on  01/01/12 08:56:44
    4            reset power on  01/01/12 08:57:00
```

```
Router#show logging onboard bay 4/3 message
timestamp            module    sev  message
```

```
01/02/12 08:14:22    RFSW-PIC  6    CAT1836E07Q:7.13:Initialize:3/1

01/02/12 08:20:42    RFSW-PIC  6    CAT1836E07Q:7.13:Initialize:3/1

01/02/12 09:13:23    RFSW-PIC  6    CAT1836E07Q:7.13:Initialize:3/1

01/02/12 09:42:33    RFSW-PIC  6    CAT1836E07Q:7.13:Initialize:3/1

01/02/12 11:56:09    RFSW-PIC  6    CAT1836E07Q:7.13:Initialize:3/1

01/02/12 12:27:23    RFSW-PIC  6    CAT1836E07Q:7.13:Initialize:3/1
```

```
Router#show logging onboard bay 5/3 message
timestamp            module    sev  message
```

```
------------------------------------------------------------------------------------------------------------------
01/22/15 01:06:05    RFSW-PIC  6    JAB092709EL:7.35:Init--stby:3/1

01/22/15 01:19:01    RFSW-PIC  6    JAB092709EL:7.35:Init--stby:3/1

01/22/15 01:31:47    RFSW-PIC  6    JAB092709EL:7.35:Init--stby:3/1

01/22/15 01:44:38    RFSW-PIC  6    JAB092709EL:7.35:Init--stby:3/1

01/22/15 01:59:04    RFSW-PIC  6    JAB092709EL:7.35:Init--stby:3/1

01/22/15 02:12:07    RFSW-PIC  6    JAB092709EL:7.35:Init--stby:3/1


Router#show logging onboard bay 4/4 message
timestamp            module    sev  message
------------------------------------------------------------------------------------------------------------------
01/01/12 10:01:44    SUP-PIC   0    TEST1122334:0.130:PLL-LOS:1[04]

01/01/12 10:01:45    SUP-PIC   0    TEST1122334:0.130:PLL-LOS:2[04]

01/01/12 10:01:46    SUP-PIC   0    TEST1122334:0.130:PLL-LOS:3[04]

01/01/12 10:01:49    SUP-PIC   0    TEST1122334:0.130:PLL-LOS:4[04]

01/01/12 10:01:50    SUP-PIC   0    TEST1122334:0.130:PLL-LOS:5[04]

01/01/12 10:01:51    SUP-PIC   0    TEST1122334:0.130:PLL-LOS:6[04]

Router#show logging onboard bay 5/5 message
timestamp            module    sev  message
------------------------------------------------------------------------------------------------------------------
01/03/12 13:52:55    SUP-PIC   0    TEST8877665:0.130:PLL-LOS:1[04]

01/03/12 13:52:56    SUP-PIC   0    TEST8877665:0.130:PLL-LOS:2[04]

01/03/12 13:52:57    SUP-PIC   0    TEST8877665:0.130:PLL-LOS:3[04]

01/03/12 13:53:00    SUP-PIC   0    TEST8877665:0.130:PLL-LOS:4[04]

01/03/12 13:53:01    SUP-PIC   0    TEST8877665:0.130:PLL-LOS:5[04]
```

オンボード障害ロギングに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *238*：オンボード障害ロギングに関する機能情報

機能名	リリース	機能情報
オンボード障害ロギング	Cisco IOS XE Everest 16.6.1	この機能は、 Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 94 章

コントロール ポイント検出

このマニュアルでは、コントロール ポイント検出（CPD）機能について説明します。この機能は、ネットワーク レイヤ シグナリング（NLS）とともに、エンド ポイントに関連付けられているコントロール ポイントの自動検出を可能にします。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *239* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

コントロール ポイント検出の前提条件

コントロール ポイント検出機能を使用するために、特別な装置やソフトウェアは必要ありません。

コントロール ポイント検出の制約事項

- CPD 機能は、ルート プロセッサ（RP）間の動的 CPD/NLS 関連データのいずれをも同期しません。コントローラに NLS チャレンジを送信した後、新しいアクティブ PRE は RP スイッチオーバーの結果として NLS 応答を無視します。
- ラインカードのスイッチオーバーでは短時間の間、CPE がアクセス不可になります。この間に CMTS で受信された CPD 要求は、エンドポイントが接続されていないかまたは制御リレーションシップがサポートされていないかのように応答されます。
- CPD 機能はデフォルトの VPN テーブル ID（0）に制限されます。
- CPD/NLS セキュリティについては、NLS 認証パス フレーズの手動設定のみサポートされます。
- NLS 認証には、MAC 長が 96 ビットに切り捨てられた HMAC SHA1（設定オプションなし）が使用されます。

コントロール ポイント検出に関する情報

コントロール ポイント検出機能を設定するには、次の概念を理解しておく必要があります。

コントロール ポイント

コントロールポイントとは、メディアストリーミングの特定の機能や制御を適用できる、ネットワーク内のポイントです。ケーブル環境では、コントロールポイントはケーブルモデム終端システム（CMTS）であり、これらのコントロール ポイントを使用するデバイスは CPD 要求元（またはコントローラ）と呼ばれます。

ケーブル CPD 要求元には以下があります。

- コール管理サーバ（CMS）
- ポリシー サーバ（PS）
- 合法的傍受のメディエーション デバイス（MD）

ネットワーク レイヤ シグナリング（NLS）

ネットワーク レイヤ シグナリング（NLS）は、さまざまなアプリケーションのサポートにおいて、トポロジの検出や他の要求を送信するために使用される、On-Path の要求プロトコルです。CPD 機能では、CPD メッセージの転送に NLS が使用されます。

CPD 用 NLS

NLS は、CPD メッセージの転送に使用されます。CPD データは、NLS のアプリケーション ペイロードに従って伝送され、フロー ID を含む NLS ヘッダーを含みます。NLS 認証時には、NLS のフロー ID が、対象のエンド ポイントの CPD 要求および応答を一意に識別するのに使用されます。

NLS フラグ

すべての NLS ヘッダーはビットごとのフラグを含みます。CMTS には、CPD アプリケーション用の次の NLS フラグ設定が用意されています。

- HOP-BY-HOP = 0
- BUILD-ROUTE = 0
- TEARDOWN = 0
- BIDIRECTOINAL = 0
- AX_CHALLENGE = 0/1
- AX_RESPONSE = 0/1

（注） AX フラグ以外のフラグによる要求は、1 に設定されると、不正な形式のメッセージであることを示すエラーにより拒否されます。

NLS TLV

次の NLS TLV はすべての CPD アプリケーションでサポートされます。

- APPLICATION_PAYLOAD
- IPV4_ERROR_CODE
- IPV6_ERROR_CODE
- AGID
- A_CHALLENGE
- A_RESPONSE
- B_CHALLENGE
- B_RESPONSE
- AUTHENTICATION
- echo

次の NLS TLV は CPD アプリケーションでサポートされません。

- NAT_ADDRESS
- TIMEOUT
- IPV4_HOP

• IPV6_HOP

コントロール ポイント検出

コントロール ポイント検出機能では、CPD 要求元が CPD 要求元とメディア エンドポイントの間にあるコントロール ポイントの IP アドレスを判別できます。

コントロール ポイント検出機能は Networking Layer Signaling（NLS）を使用して、エンド ポイント（MTA）へ CPD メッセージを送信します。要求元とエンドポイントの間にあるエッジ/集約デバイス（CMTS）は、その IP アドレスでメッセージに応答します。

（注） 合法的傍受のために、エンドポイントは CPD メッセージを受信しないことが重要です。この例では、CMTS は宛先に転送せずにメッセージを応答します。

CPD プロトコル階層

CPD メッセージは、NLS 上で送信されます。

CPD プロトコル階層は次のようになっています。

1. CPD
2. NLS
3. UDP
4. IP

（注） NLS は UDP プロトコル上に実装されるため、メッセージ損失の可能性があります。メッセージが失われると、コントローラはそのようなイベントで CPD 要求を再送信します。

制御関係

コントロール ポイントとコントローラの間の制御関係は、コントロール ポイントをパス スルーするメディア フロー上の機能として識別されます。制御関係は、制御関係タイプ（CR TYPE）と制御関係 ID（CR ID）によって一意に定義されます。CR ID は CMTS とコントローラでプロビジョニングされます。

サポートされる CR TYPE と対応する定義済み CR ID を表に示します

表 *240*：サポートされる制御関係タイプと対応する制御関係 *ID*

制御関係タイプ	対応する定義済み制御関係 ID
CR TYPE = 1（合法的傍受）	CR ID = 1：CMTS
	CR ID = 2：CMTS の前にある集約ルータまたはスイッチ
	CR ID = 3：メディア サービスの前にある集約ルータまたはスイッチ
	CR ID = 4：メディア ゲートウェイ
	CR ID = 5：電話会議サーバ
	CR ID = 6：その他
CR TYPE = 2（DQoS）	CR ID = 1：CMTS
CR TYPE = 3（PCMM）	CR ID = 1：CMTS

CPD の設定方法

CPD 機能の有効化

CPD機能をイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。CPD メッセージ認証は NLS 設定によって決定されます。

はじめる前に

CPD メッセージ認証は NLS 設定によって決定されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cpd** 例： `Router (config)# cpd`	CPD 機能をイネーブルにします。 • CPD 機能をディセーブルにするには、このコマンドの「no」形式を使用します。
ステップ 4	**end** 例： `Router# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

CPD 有効化の例

次に、ルータ上で有効化した CPD の例を示します。

```
Router (config)# cpd
```

CPD 機能のデバッグ

CPD 機能をデバッグするには、特権 EXEC モードで **debugcpd** コマンドを使用します。デバッグを無効にするには、このコマンドの **no** 形式を使用します。

制御関係 ID の設定

CMTS の制御関係 ID（CR ID）を設定するには、cpd cr-id コマンドを使用します。CPD 要求にワイルドカードの CR ID が設定されていると、CMTS はこの設定値を返します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**cpdcr-id** 例： `Router (config)# cpd cr-id 100`	CMTS の制御関係 ID（CR ID）を設定します。
ステップ 4	**end** 例： `Router# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

例

次の例では、ルータの cr-id 番号が 100 で設定された cpd cr-id コマンドを示します。

```
Router (config)# cpd cr-id 100
```

NLS 機能の有効化

NLS 機能をイネーブルにするには、グローバル コンフィギュレーション モードで nls コマンドを使用します。NLS メッセージの承認が常にイネーブルであることを推奨します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**nls** 例： `Router (config)# nls`	NLS 機能をイネーブルにします。 • NLS 認証は、任意です。 • NLS メッセージの承認が常にイネーブルであることを推奨します。
ステップ 4	**end** 例： `Router# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

例

次に、ルータ上で有効化された nls コマンドの例を示します。

```
Router (config)# nls
```

NLS 機能のデバッグ

NLS 機能をデバッグするには、特権 EXEC モードで **debugnls** コマンドを使用します。デバッグを無効にするには、このコマンドの **no** 形式を使用します。

権限付与グループ ID と認証キーの設定

権限付与グループ ID（AG ID）と対応する認証キーは、CMTS およびコントローラ/CPD のリクエスタでプロビジョニングされます。

権限付与グループ ID と認証キーを設定するには、グローバル コンフィギュレーション モードで nls ag-id コマンドを使用します。NLS メッセージの承認が常にイネーブルであることを推奨します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**nlsag-id** 例： `Router (config)# nls ag-id 100 auth-key 20`	権限付与グループ ID と認証キーを設定します。
ステップ 4	**end** 例： `Router# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

例

次の例では、権限付与グループ ID が 100 で認証キーが 20 の nls ag-id コマンドを示します。

```
Router (config)# nls ag-id 100 auth-key 20
```

NLS 応答タイムアウトの設定

NLS 応答タイムアウトは、CMTS が NLS 認証要求の応答を受け取るまでの待機時間を制御します。

NLS 応答タイムアウトを制御するには、グローバル コンフィギュレーション モードで nls ag-id コマンドを使用します。NLS メッセージの承認が常にイネーブルであることを推奨します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**nlsresp-timeout** 例： `Router (config)# nls resp-timeout 60`	NLS 応答時間を設定します。
ステップ 4	**end** 例： `Router# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

例

次の例では、応答タイムアウトを 60 秒に設定した nls resp-timeout コマンドを示します。

```
Router (config)# nls resp-timeout 60
```

その他の参考資料

ここでは、CPD 機能に関する参考資料について説明します。

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

コントロール ポイント検出に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *241*：コントロール ポイント検出に関する機能情報

機能名	リリース	機能情報
コントロール ポイント検出	Cisco IOS XE Everest 16.6.1	この機能は、 Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 95 章

IPDR Streaming Protocol

Cisco cBR シリーズ コンバージド ブロードバンド ルータは、ネットワーク機器からメディエーション システム（運用サポート システム（OSS）やビジネス サポート システム（BSS）など）にエクスポートされる大量のデータを提供する Internet Protocol Detail Record（IPDR）のストリーミング プロトコル機能をサポートします。IPDR は、OSS および BSS で使用される IP ベース サービス使用や他のアクティビティに関する情報を提供します。従来のシンプル ネットワーク管理プロトコル（SNMP）のポーリング メカニズムと異なり、このプロトコルではプッシュ モデルを使用してさまざまなネットワーク要素または機器からデータを収集するメカニズムが提供されます。

DOCSIS 3.0 仕様に基づき、IPDR 機能は、管理システムへの大量のパフォーマンス メトリックの転送において、時間とリソースの効率を最適化します。DOCSIS 3.0 には 5 つの管理機能、つまり FCAPS モデルが導入されています。FCAPS は、障害、コンフィギュレーション、アカウンティング、パフォーマンス、セキュリティを表します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

IPDR Streaming Protocol の設定の制限事項

- IPDR エクスポータは、多くのコレクタに接続可能ですが、指定の時間に最も高いプライオリティで動作するコレクタにのみデータを送信します。
- 各 IPDR セッションを、優先する 1 つのアクティブ（ゼロ）コレクタまたは複数のスタンバイ コレクタに関連付けることができます。

IPDR Streaming Protocol に関する情報

IPDR Streaming Protocol は、請求、パフォーマンス、診断データのような大量のデータ レコードのエクスポート プロセスを信頼性があり、高速かつ効率的で柔軟な方法で実施するというニーズに対処するように設計されています。

IPDR/SP プロセスは、IPDR コレクタと通信します。IPDR Streaming Protocol は、複数の IPDR セッションをサポートします。このアーキテクチャは、フェールオーバーのためにプライマリおよびセカンダリ コレクタをサポートします。いずれの時点でも、データはコレクタ 1 つのみに送信されます。なんらかの理由でエクスポータからプライマリ コレクタへの接続が失敗すると、データはセカンダリ コレクタに送信されます。ネットワーク構成に応じて、セッションごとにプライマリ コレクタを 1 つのみ設定できます。セッションが異なれば、異なるプライマリ コレクタを設定できます。たとえば、課金コレクタや診断コレクタなどを設定できます。

（注） IPDR エクスポータはケーブル モデム終端システム（CMTS）を参照し、IPDR コレクタはネットワーク機器を参照します。

データ収集の方法論

IPDR は、各種のパフォーマンス関連測定指標（請求情報、診断、ネットワーク トポロジ、信号品質のモニタリングなどの管理データ）のために生成または収集されたデータです。これらのデータは FCAPS モデル（障害、構成、アカウンティング、パフォーマンス、およびセキュリティ）に基づいています。

IPDR クライアント アプリケーションは、IPDR エクスポータが提供するストリームを特定するために、IPDR_GET_SESSIONS メッセージを使用してエクスポータと通信します。エクスポータは、IPDR_GET_SESSIONS_RESPONSE メッセージを使用してクライアントに応答を送信します。この

データ収集方法は、『*Operations Support System Interface Specification*』（CM-SP-OSSIv3.0-I13-101008）に基づいています。

IPDR_GET_SESSIONS_RESPONSE メッセージには、IPDR セッション ID を特定するための SessionBlock.reserved 属性が含まれます。この属性により、Cisco CMTS ルータが各 IPDR サービス定義でサポートされるデータ収集メカニズムごとに IPDR セッション ID を定義します。この属性は、Cisco IOS リリース 12.2(33)SCE より前の Cisco IOS リリースで使用されていませんでした。

IPDR 機能は、コレクタまたはネットワーク要素が CMTS からデータを取得するための方法を定義します。以下に収集方法論のリストを示します。

時間間隔セッション：この方法では、スケジュール ベースのセッションに従って、CMTS が定期的な時間間隔でデータをストリーミングします。この時間間隔は、隣接する 2 つのセッションの開始メッセージの時間ギャップです。この方法では、セッションの開始および停止動作の制御が CMTS で管理されます。時間間隔セッションは、CMTS がレコードをエクスポートした後に終了されます。

（注） CMTS がレコードがストリーミングしているワンタイム間隔時に、別の時間間隔が期待された場合、CMTS は新しい時間間隔を無視し、前の時間間隔が終了するまでデータのエクスポートを続行します。

イベント ベースのセッション：この方法では、CMTS はセッションが開いているときはいつでもレコードをエクスポートできます。つまり、この方法は無期限のセッションで機能します。

アドホック セッション：この方法では、CMTS はセッションを作成し、データ ストリーミングを許可し、データのエクスポートが完了するか終了コマンドが生成されるとセッションを閉じます。

ipdrsession コマンドを発行することで、新しいセッションが作成されます。すると、CMTS はコレクタから FLOW_START メッセージを受信し、CMTS エクスポータは SESSION_START メッセージを送信して、コレクタからの IPDR データのエクスポートを開始します。すべてのデータが転送されると、エクスポータはコレクタから ACK メッセージを受信し、そのコレクタに SESSION_STOP メッセージを送信します。この方法はアドホック セッションと呼ばれます。

IPDR Streaming Protocol の設定方法

このセクションでは、Cisco CMTS プラットフォームで IPDR Streaming Protocol 機能を使用するときに実行される設定タスクについて説明します。

（注） IPDR コンフィギュレーションを削除するには、no ipdr コマンドを使用します。

IPDR セッションの設定

CMTS アプリケーションが IPDR エクスポータにセッションを追加できるようにするには、グローバル コンフィギュレーション モードで ipdr session コマンドを使用します。

IPDR セッションを削除するには、このコマンドの no 形式を使用します。

（注）
- セッション ID は一意である必要があります。
- アクティブ セッションを削除するには、このコマンドを削除する前に非アクティブ化する必要があります。

>

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	ipdr session session_id session_name session_descr 例： `Router(config)# ipdr session 1 samis_sxn test`	CMTS アプリケーションが IPDR エクスポータにセッションを追加できるようにします。

IPDR タイプの設定

IPDR セッション タイプを設定するには、グローバル コンフィギュレーション モードで ipdr タイプ コマンドを使用します。このコマンドを使用して定義できる IPDR セッション タイプには、event タイプ、time-interval タイプ、および ad hoc タイプがあります。

セッション タイプをデフォルトの「event」タイプにリセットするには、コマンドの no 形式を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	ipdr type session_id [ad-hoc | event | time-interval value] 例： `Router(config)# ipdr type 1 time-interval 15`	CMTS アプリケーションで IPDR セッション タイプを設定できるようにします。

次の作業

（注） IPDR セッション タイプを設定したら、このタイプと関連付けられるのは、IPDR タイプでサポートされるテンプレートのみです。また、コンソールには、タイプの変更時にこの IPDR セッション タイプではサポートされていないテンプレートに関する情報が表示されます。

IPDR コレクタの設定

IPDR コレクタの詳細を設定するには、グローバル コンフィギュレーション モードで ipdr collector コマンドを使用します。ポート番号は、エクスポータがアクティブな接続を作成する場合に使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**ipdr collector** 例： `Router(config)# ipdr collector federal 192.168.6.5`	CMTS アプリケーションが IPDR コレクタを設定し、IPDRプロトコルを認証できるようにします。 （注） NAT 対応ネットワークで実行している IPDR コレクタには NAT アドレスを設定します。

IPDR の関連付けの設定

コレクタとセッションを関連付けるには、グローバル コンフィギュレーション モードで ipdr associate コマンドを使用します。

はじめる前に

- 関連付けを設定する前に、セッションを非アクティブ化する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**ipdr associate session_id collector_name priority** 例： `Router(config)# ipdr associate 1`	コレクタとセッションを関連付けます。

	コマンドまたはアクション	目的
	`federal 1`	

IPDR テンプレートの設定

IPDR セッションに IPDR テンプレートを追加するには、グローバル コンフィギュレーション モードで ipdr テンプレート コマンドを使用します。コマンド プロンプトで「?」を入力すると、テンプレートのリストが表示されます。

（注）
- システムでサポートされたテンプレートのみを追加できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**ipdr template session_id template_name** 例： `Router(config)# ipdr template 1 SAMIS`	IPDR セッションに IPDR テンプレートを追加します。

IPDR エクスポータの設定

次のコマンドを使用して、キープアライブ タイマー数、未確認のレコードの最大数、未確認のタイムアウト間隔値など、IPDR エクスポータ パラメータを設定できます。

- **ipdrexporterkeepalive**：IPDR エクスポータのキープアライブ タイマーのカウント値を設定します。

- **ipdrexportermax-unacked**：IPDR エクスポータの未確認のレコードの最大数を設定します。
- **ipdrexporterack-timeout**：IPDR エクスポータの確認済みレコードの時間間隔を設定します。

（注） DataAckTimeInterval のデフォルト値は 60 秒で、DataAckSequenceInterval のデフォルト値は 200 秒です。

設備で使用するコレクタのエクスポータをカスタマイズする IPDR パラメータの値を設定できます。ただし、これらのコマンドはオプションです。設定しない場合は、**ipdrexporterstart** コマンドを実行するときに、これらのコマンドのデフォルト値が使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**ipdrexporterkeepalive** *time_interval* 例： `Router(config)# ipdr exporter keepalive 300`	（任意）IPDR エクスポータのキープアライブタイマーカウントを設定します。有効な範囲は 5 ～ 300 秒です。デフォルト値は 300 です。
ステップ 4	**ipdrexportermax-unacked** *records* 例： `Router(config)# ipdr exporter max-unacked 200`	（任意）IPDR エクスポータの未確認のレコードの最大数を設定します。有効範囲は 5 ～ 200 レコードです。デフォルト値は 200 です。
ステップ 5	**ipdrexporterack-timeout** *time_interval* 例： `Router(config)# ipdr exporter ack-timeout 60`	（任意）IPDR エクスポータの確認済みレコードのタイムアウト間隔を設定します。有効な範囲は 5 ～ 60 秒です。デフォルト値は 60 です。

	コマンドまたはアクション	目的
ステップ 6	ipdr exporter start 例： `Router(config)# ipdr exporter start`	CMTS アプリケーションが IPDR エクスポータ プロセスを開始してエクスポータとコレクタに接続できるようにします。

IPDR Streaming Protocol の設定例

例：IPDR セッションの設定

次に、IPDR セッションの設定方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# ipdr session 1 test no_descr
```

例：IPDR タイプの設定

次に、IPDR の「期間」セッション タイプを 15 分間隔に設定する方法について説明します。

```
Router> enable
Router# configure terminal
Router(config)# ipdr type 1 time-interval 15
```

例：IPDR コレクタの設定

次に、IPDR コレクタの設定方法を示します。

```
Router> enable
Router# configure terminal
Router(config)# ipdr collector federal 209.165.200.225
```

NAT アドレスを使用した IPDR コレクタの設定例

この例に示されている **nat-address** キーワードを使用して、IPDR コレクタの NAT アドレスを設定します。

```
Router(config)#ipdr collector federal 192.0.2.225 nat-address 192.0.2.51
```

例：IPDR の関連付けの設定

次に、コントローラとセッションを関連付ける方法について説明します。

```
Router> enable
Router# configure terminal
Router(config)# ipdr associate 1 federal 1
```

例：IPDR テンプレートの設定

次に、IPDR テンプレートを IPDR セッションに追加する方法について説明します。

```
Router> enable
Router# configure terminal
Router(config)# ipdr template 1 SAMIS-TYPE1
```

例：IPDR エクスポータの設定

次に、エクスポータとコレクタの接続のために IPDR エクスポータ プロセスを設定する方法について説明します。

```
Router> enable
Router# configure terminal
Router(config)# ipdr exporter keepalive 300
Router(config)# ipdr exporter max-unacked 200
Router(config)# ipdr exporter ack_timeout 60
Router(config)# ipdr exporter start
```

IPDR Streaming Protocol の確認

このセクションでは、Cisco CMTS プラットフォーム上の IPDR Streaming Protocol の確認に使用するコマンドについて説明します。

IPDR コレクタの確認

showipdrcollector コマンドは、コレクタ情報、メッセージの統計情報、およびコレクタに関連付けられたすべてのセッションに関するイベントを表示します。

次に、**showipdrcollector** コマンドの出力例を示します。

```
Router# show ipdr collector federal
Collector Name: federal, IP: 192.0.2.0, Port: 0
2001-07-05T19:28:22 Collector in session 1 Statistics:
 Transmitted 12658 Acknowledged 12658 Enqueued 12658 Lost 0
 Last Event: Event Id 1 IPDR_EVENT_SERVER_CONNECTED - INCOMING
Router(config)#
```

IPDR エクスポータの確認

showipdrexporter コマンドは、下記の IPDR エクスポータの情報を表示します。

- started（開始）
- not started（未開始）
- not initialized（未初期化）

次に、**showipdrexporter** コマンドの出力例を示します。

```
Router# show ipdr exporter
IPDR exporter is started.
Current parameters:
        KeepAliveInterval   :300
        AckTimeInterval     :60
        AckSequenceInterval :200
Router#
```

IPDR セッションの確認

showipdrsession コマンドは、すべてのセッションまたは特定のセッションの詳細（セッション ID、説明、セッション状態など）を表示します。

次に、**all** キーワードを指定した **showipdrsession** コマンドの出力例を示します。

```
Router# show ipdr session all
Session ID: 1, Name: utilsta, Descr: test, Started: False
```

次に、**session_id** キーワードを指定した **showipdrsession** コマンドの出力例を示します。

```
Router# show ipdr session 1
Session ID: 1, Name: utilsta, Descr: test, Started: False
2001-07-05T19:36:28 Statistics:
Transmitted 0 Acknowledged 0 Enqueued 0 Lost 0
queuedOutstanding 0 queuedUnacknowledged 0
1 Collectors in the session:
Name: federal, IPAddr: 192.0.2.0, Port: 0, Priority: 1
```

IPDR セッション コレクタの確認

showipdrsessioncollector コマンドは、特定のセッションに関連付けられたコレクタの詳細を表示します。1つのセッションに複数のコレクタを関連付けられるため、このコマンドを使用すると、特定のセッションとコレクタのペアを表示できます。

次に、**showipdrsessioncollector** コマンドの出力例を示します。

```
Router# show ipdr session 1 collector federal
Session ID: 1, Name: utilsta, Descr: test, Started: False
Collecotr Name: federal, IP: 192.0.2.0, Port: 0
2001-07-05T19:38:02 Collector in session 1 Statistics:
 Transmitted 0 Acknowledged 0 Enqueued 0 Lost 0
 Last Event: Event Id 0 WRONG_EVENT_ID
```

IPDR セッション テンプレートの確認

showipdrsessiontemplate コマンドは、特定のセッションでサポートされるすべてのアクティブ テンプレートのリストを表示します。

次に、**showipdrsessiontemplate** コマンドの出力例を示します。

```
Router# show ipdr session 1 template
Template ID: 2, Name:
http://www.cablelabs.com/namespaces/DOCSIS/3.0/xsd/ipdr/DOCSIS-CMTS-CMSERVICE-FLOW-TYPE,
Type: DOCSIS-Type, KeyNumber: 22
Session 1 has totally 1 templates.
```

その他の参考資料

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPDR Streaming Protocol に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *242*：ダウンストリーム インターフェイスの設定に関する機能情報

機能名	リリース	機能情報
IPDR Streaming Protocol	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 96 章

従量制課金（SAMIS）

このマニュアルでは、Cisco ケーブル モデム終端システム（CMTS）ルータの従量制課金機能について説明します。この機能を使用すると、加入者のアカウントおよび課金情報が、サブスクライバ アカウント管理インターフェイス仕様（SAMIS）形式で提示されます。SAMIS 形式は、Data-over-Cable Service Interface Specifications（DOCSIS）Operations Support System Interface（OSSI）仕様によって指定されています。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *243* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

従量制課金（SAMIS）の前提条件

従量制課金機能の前提条件は、次のとおりです。

- ケーブル モデムは、DOCSIS 1.0 または DOCSIS 2.0、OSSI バージョン 3.0 および DOCSIS 3.0 に準拠している必要があります。
- モニタされるケーブル モデムで、サービス クラス ネーミング（SCN [TLV 24/25, subTLV 4]）によりアップストリームおよびダウンストリームのプライマリ サービス フローを定義する DOCSIS コンフィギュレーション ファイルを使用する必要があります。動的に作成されたサービス フローをモニタする場合は、それらのサービス フローも SCN の名前で作成される必要があります。
- この機能がファイル モードで動作している場合、外部サーバに課金レコードをコピーするには、セキュア コピー（SCP）または Trivial File Transfer Protocol（TFTP）を使用して、外部課金サーバから Cisco CMTS にログインする必要があります。Cisco CMTS は FTP やセキュア FTP（SFTP）サーバとして動作することはできません。
- この機能が非セキュア モードのストリーミング モードで動作している場合、設定可能な TCP ポートで課金レコードを受信するよう外部課金サーバを設定する必要があります。
- この機能がセキュア モードのストリーミング モードで動作している場合は、次の条件が必要です。
  - 外部課金サーバを Secure Sockets Layer（SSL）接続を使用して設定可能な TCP ポートで課金レコードを受信するように設定する必要があります。

ヒント　課金アプリケーション サーバでの SSL サポートについては、入手可能なサードパーティ ソリューションが複数あります（http://www.openssl.org/index.html を参照）。

-
  - 課金アプリケーションと Cisco CMTS ルータに必要なデジタル証明書を提供する認証局（CA）が設定され、利用できる必要があります。CA は Verisign などのパブリック CA、または Cisco Provisioning Center（CPC）などのソフトウェアが実行されているプライベート管理ネットワーク上のサーバにすることができます。
- **full-records** キーワードを使用するには、Cisco CMTS ルータが Cisco IOS-XE リリースで稼働している必要があります。
- ipdr/ipdr-d3 に **flow-aggregate** キーワードを使用するには、Cisco CMTS ルータが Cisco IOS-XE リリースで稼働している必要があります。

flow-aggregate が有効な場合、ケーブル モデムごとにサービス フローが結合されて 1 つのレコードになります。

-
  - ServiceClassName 要素は常に、IPDR レコードで NULL 値を返します。これは、ケーブル モデムのサービス フローに有効なサービス クラス名がある場合でも同様です。
  - ServiceIdentifier の要素は常にゼロの値を返します。

従量制課金の制限事項

従量制課金機能には、次の制約事項と制限があります。

- SNMP コマンドを使用して従量制課金の設定を表示、変更することができます。SNMP トラップを使用すると、課金レコードが使用可能になったときに課金アプリケーション システムに通知されるようにすることができます。ただし、SNMP コマンドを使用して課金レコードを取得することはできません。
- SNMP による IPDR モードのイネーブル化はサポートされていません。

ラインカードがスイッチオーバーすると、ラインカード内のアイテムは失われます。同様に、PRE がスイッチオーバーすると、sflog ファイルの RP 内のアイテムが失われます。

ユーザが SAMIS ファイルの宛先を使用している場合、さらに PRE のスイッチオーバーにより出力ファイルが再初期化されます。

- 課金レコードには、マルチキャスト サービス フローとトラフィック カウンタに関する情報は含まれません。
- Cisco CMTS ルータが再起動するたびに、CLI コマンドにより表示されるパケット カウンタはゼロにリセットされます。SNMP コマンドにより表示されるパケット カウンタは、ルータがリロードされると保持されず、SNMP MIB カウンタはリロード時に維持されません。これらのカウンタは 64 ビット値で、高使用率の状況ではゼロにロール オーバーされる場合があります。
- 従量制課金のファイル モードでケーブル計測を設定する場合、cable metering filesystem コマンドを使用した直後に送信元インターフェイスを指定することはできません。cable metering filesystem コマンドを使用すると、ケーブル計測ファイルがブートフラッシュに書き込まれます。この操作が完了するまで、ケーブル計測の設定はできません。ファイル書き込み操作が完了したら、source-interface コマンド（cable metering source-interface）を設定することができます。課金パケットの IP アドレスが送信元インターフェイスの IP アドレスとなるよう、ブートフラッシュ中の計測ファイルは削除する必要があります。

（注） このケーブル計測の制限はリロード中には問題になりません。

- 従量制課金のストリーミング モードでケーブル計測を設定する場合、ループバック インターフェイスがコレクタ サーバからアクセス可能であることを確認します。コレクタ サーバからループバック インターフェイスの IP アドレスへの Telnet 接続は、コレクタ サーバからループバック インターフェイスにアクセス可能かどうかをテストするのに適した方法です。

従量制課金の情報

機能の概要

従量制課金機能は、DOCSISネットワークのトラフィック課金情報を記録したり取得したりする、各種の標準規格に準拠したオープンアプリケーションアプローチを提供します。この機能を有効にすると、ケーブル ネットワークを使用しているケーブル モデムおよび顧客宅内機器（CPE）デバイスについて、次の請求情報を提供します。

- ケーブル モデムの IP アドレスと MAC アドレス。
- 使用されるサービス フロー（アップストリームおよびダウンストリームの両方のサービス フローが追跡されます）。
- ケーブル モデムを使用している CPE デバイスの IP アドレス。
- 収集期間中に、ケーブル モデムが受信した（ダウンストリーム）、またはケーブル モデムが送信した（アップストリーム）オクテットとパケットの総数。
- 加入者のサービス レベル契約（SLA）によって許容される帯域幅レベルを超過するおそれがあったために、CMTSがドロップまたは遅延したケーブルモデムのダウンストリーム パケットの総数。

課金レコードは、標準化されたテキスト形式で保持されるため、サービス プロバイダーは既存の課金アプリケーションに簡単に統合できます。サービス プロバイダーはこの情報を使用して、サービス アップグレードの潜在顧客と考えられるユーザや、SLA の制限を定期的に超過しそうになる顧客を判断できます。

Cisco CMTS ルータの従量制課金と DOCSIS サポート

従量制課金機能は Cisco CMTS ルータで次の DOCSIS 機能をサポートします。

- DOCSIS 1.0、DOCSIS 2.0 および DOCSIS 3.0 準拠ケーブル モデムがサポートされます。
- ベストエフォート サービス フローが、DOCSIS 準拠のケーブル モデムでサポートされます。
- セカンダリ サービス フローが、DOCSIS 準拠のケーブル モデムでサポートされます。
- 動的サービス フローが、DOCSIS 準拠のケーブル モデムでサポートされます。
- 削除されたサービス フローに関する情報は、DOCSIS 1.1 サービス フローでのみ取得でき、DOCSIS 1.0 サービス フロー用では取得できません。
- 終了したサービス フローのサポートを有効にするには、グローバル モードで **cablesflog** コマンドを使用する必要があります。

標準

従量制課金機能は、さまざまなオープン スタンダードに基づいており、商用アプリケーションやカスタム開発された課金アプリケーションによりサポートされます。CMTS によって生成される課金レコードの書き込みと使用のため主なガイドラインは、次の標準により提供されています。

- Extensible Markup Language（XML）：課金レコードなどのあらゆる種類の構造化された情報を含めるよう、容易に他のマークアップ言語を定義できすることができるメタ言語。XML ベースのアプローチにより、収集された課金情報を他のベンダーによるさまざまな課金アプリケーションで使用したり、それらのアプリケーションに配布することができます。さらに、他のプロバイダーの必要に応じて容易に形式を更新したりカスタマイズすることができます。
- IP Detail Record（IPDR）：*Network Data Management—Usage (NDM-U) For IP-Based Services* 仕様で定義された、ベンダーに依存しないオープンな標準。IP ベースのネットワーク経由で提供可能なあらゆる種類のサービス向けに、課金レコードおよび利用状況レコードの維持を簡素化します。サービス プロバイダーは IPDR を使用して、DOCSIS、Voice-over-IP などの使用中のすべてのサービス（それらが異なるプロトコルやアプリケーション サーバを使用している場合も）を統合した課金アプリケーションを作成できます。
- DOCSIS Operations Support System Interface（OSSI）：課金レコード インターフェイス用のサブスクライバ アカウント管理インターフェイス仕様（SAMIS）など、DOCSIS ネットワークのネットワーク管理要件を定義する DOCSIS 仕様。DOCSIS 2.0 バージョンの本仕様には、CMTS では課金インターフェイスを提供する必要がないこと、ただし CMTS が課金インターフェイスを提供する場合は、IPDR/XML 標準に準拠する必要があることが示されています。

ヒント　これらの標準の詳細については、38 ページの「標準」に記載されているドキュメントを参照してください。

IPDR サービス定義スキーマ

オブジェクト管理を標準化するため、MIB が SNMP に関連付けられているように、サービス定義スキーマは IPDR に関連付けられています。

詳細については、OSSI 仕様の資料（http://www.cablelabs.com/wp-content/uploads/specdocs/CM-SP-OSSIv3.0-I02-070223.pdf）を参照してください。

このスキーマは、Cisco IOS-XE リリースでサポートされます。

表 *244* : *DOCSIS 3.0* の *IPDR* スキーマ リスト

カテゴリ	サービス定義	スキーマ定義	収集方法
SAMIS	SAMIS-TYPE-1	DOCSIS-SAMIS-TYPE-1_3.5.1-A.1.xsd	時間間隔、アドホック
	SAMIS-TYPE-2	DOCSIS-SAMIS-TYPE-2_3.5.1-A.1.xsd	時間間隔、アドホック
診断ログ サービス定義スキーマ	DIAG-LOG-TYPE	DOCSIS-DIAG-LOG-TYPE_3.5.1-A.1.xsd	アドホック
	DIAG-LOG-EVENT-TYPE	DOCSIS-DIAG-LOG-EVENT-TYPE_3.5.1-A.1.xsd	イベント
	DIAG-LOG-DETAIL-TYPE	DOCSIS-DIAG-LOG-DETAIL-TYPE_3.5.1-A.1.xsd	時間間隔、アドホック、イベント
スペクトル管理	SPECTRUM-MEASUREMENT-TYPE	DOCSIS-SPECTRUM-MEASUREMENT-TYPE_3.5.1-A.1.xsd	時間間隔、アドホック
CMTS CM 登録ステータス情報	CMTS-CM-REG-STATUS-TYPE	DOCSIS-CMTS-CM-REG-STATUS-TYPE_3.5.1-A.1.xsd	時間間隔、アドホック、イベント
CMTS CM アップストリーム ステータス情報	CMTS-CM-US-STATS-TYPE	DOCSIS-CMTS-CM-US-STATS-TYPE_3.5.1-A.1.xsd	時間間隔、アドホック
CMTS トポロジ	CMTS-TOPOLOGY-TYPE	DOCSIS-CMTS-TOPOLOGY-TYPE_3.5.1-A.1.xsd	アドホック、イベント
CPE 情報	CPE-TYPE	DOCSIS-CPE-TYPE_3.5.1-A.1.xsd	アドホック、イベント
CMTS 使用率統計	CMTS-US-UTIL-STATS-TYPE	DOCSIS-CMTS-US-UTIL-STATS-TYPE_3.5.1-A.1.xsd	イベント
	CMTS-DS-UTIL-STATS-TYPE	DOCSIS-CMTS-DS-UTIL-STATS-TYPE_3.5.1-A.1.xsd	イベント

表に示すスキーマは、システムの管理情報に従ってこれらの IPDR レコードを生成する SNMP エージェントとして機能する各コレクタを実装することによりサポートされます。

IPDR CM-STATUS-2008

Cisco IOS-XE リリース 16.5.1 では、古い IPDR コレクタの上位互換性をサポートするために IPDR CM-STATUS 2008 バージョンをサポートしています。IPDR CM-STATUS 2008 バージョンで CmtsRcsId および CmtsTcsId オブジェクトは 16 ビット長ですが、CM-STATUS バージョンでこれらはどちらも 32 ビット長です。

CmtsRcsId オブジェクトは、CM-STATUS バージョンからの値を CM-STATUS-2008 バージョンに下位 16 ビットで返します。ただし、CmtsTcsId オブジェクトについてはどちらのスキーマでも値が 16 ビットを超えることはないため、CM-STATUS-2008、CM-STATUS の両バージョンで同じ値を返します。

DOCSIS SAMIS サービス定義

DOCSIS 3.0 の SAMIS サービス定義は構造化されています。SAMIS-TYPE-1 と SAMIS-TYPE-2 という 2 つのバージョンがあり、SAMIS とは異なる詳細レベルの情報を提供します。

DOCSIS 2.0 SAMIS は、イベント セッション（デフォルト タイプ）のみをサポートします。DOCSIS 3.0 SAMIS タイプ 1 と DOCSIS 3.0 SAMIS タイプ 2 は、時間間隔セッションとアドホック セッションのみをサポートします。

SAMIS は設定可能な時間間隔に基づいて収集されます。間隔ごとに異なるドキュメントになり、エクスポータは新しい間隔の新しいセッションを停止および開始します。この間隔は、固定の開始点と間隔を持つ時間間隔とは異なり、成功または失敗した最後の計測から開始します。

（注） SAMIS スキーマを設定するには、**cable metering ipdr session** コマンドを使用できます。SAMIS-TYPE-1 および SAMIS-TYPE-2 スキーマは、**cable metering ipdr-d3** コマンドを使用して設定できます。これらのスキーマはいずれか 1 つを選択しなければなりません。

Limitation To DOCSIS SAMIS

- **cable metering ipdr| ipdr-d3** コマンドとの一貫性があるスキーマのみが実行されます。いずれのスキーマも、一貫性がなければ実行されません。
- SAMIS IPDR タイプを変更すると、IPDR データのエクスポートが中断されます。

DOCSIS 診断ログ サービス定義

このサービス定義は、2 つのステップからなるプロセスを使用して IPDR ストリーミングを定義します。

- SNMP や他の構成管理インターフェイス（CLI など）は、診断ログを設定するために使用されます。
- IPDR/SP は、診断ログのインスタンスをストリーミングするために使用されます。

これらの診断ログ サービス定義スキーマは、次の収集方法をサポートします。

- Cisco CMTS は、DIAG-LOG-TYPE レコード収集のストリーミングをアドホック セッションとしてサポートします。
- Cisco CMTS は、DIAG-LOG-EVENT-TYPE レコード収集のストリーミングをイベント セッションとしてサポートします。イベント ベースの診断ログ レコードの場合、イベントが診断ログに記録され、IPDR メッセージがコレクタに送信されると、Cisco CMTS はレコードをストリーミングします。
- DOCSIS-DIAG-LOG-DETAIL-TYPE は、次の収集方法をサポートします。
  - 時間間隔：セッション設定に基づくスケジュールに従って、定期的な間隔でデータをエクスポートします。時間間隔の終了に到達すると、エクスポータは診断ログを収集し、このセッションに関連付けられているコレクタにレコードをストリーミングします。時

間間隔に基づく診断ログ レコードの場合、スケジュールされた収集時に、Cisco CMTS は診断ログのスナップショットをストリーミングします。

- アドホック：エクスポータは、「FlowStart」メッセージを受信すると、診断レコードを収集してそのデータをコレクタに送信するために、アプリケーションをトリガーします。
- イベント：診断ログ レコードが作成されると、ipdr メッセージがコレクタに送信されます。詳細については、『Operations Support System Interface (OSSI) Specification』を参照してください。

DOCSIS スペクトル測定サービス定義

このサービス定義スキーマは、信号品質のモニタリング機能の IPDR スキーマを定義します。

DOCSIS-SPECTRUM-MEASUREMENT-TYPE スキーマは、次の収集方法をサポートします。

- 時間間隔：セッション設定に基づくスケジュールに従って、定期的な間隔でデータをエクスポートします。時間期間の終了に到達すると、エクスポータはスペクトル情報を収集し、コレクタにレコードをストリーミングします。
- アドホック：エクスポータは、「FlowStart」メッセージを受信すると、スペクトル情報を収集してそのデータをコレクタに送信するために、アプリケーションをトリガーします。

DOCSIS CMTS CM 登録ステータス サービス定義

このサービス定義スキーマは、CMTS CM 登録ステータス情報の IPDR サービス定義スキーマを定義します。

DOCSIS-CMTS-CM-REG-STATUS-TYPE スキーマは、次の収集方法をサポートします。

- 時間間隔：セッション設定に基づくスケジュールに従って、定期的な間隔でデータをエクスポートします。時間期間の終了に到達すると、エクスポータは CM ステータス情報を収集し、コレクタにレコードをストリーミングします。
- アドホック：エクスポータは、「FlowStart」メッセージを受信すると、ケーブル モデムのすべてのステータス情報を収集してそのデータをコレクタに送信するために、アプリケーションをトリガーします。
- イベント：ケーブルモデムが「offline」状態から「online」に、または「online」から「offline」になると（中間状態の変化は含まない）、エクスポータはケーブル モデムのステータス情報を収集するアプリケーションを呼び出し、コレクタにデータを送信します。詳細については、『Operations Support System Interface (OSSI) Specification』を参照してください。

DOCSIS CMTS CM アップストリーム ステータス サービス定義

このサービス定義スキーマは、ケーブル モデムと Cisco CMTS の観点から、ケーブル モデムの登録ステータス オブジェクトとアップストリーム ステータス オブジェクトを定義します。

CmtsCmUsEqData IPDR スキーマ フィールドで、対応する MAC ドメインの **cable upstream equalization-coefficient** コマンドを設定して、この機能がデータを使用できるようにします。このコマンドの詳細については、『Cisco IOS CMTS Cable Command Reference Guide』を参照してください。

DOCSIS-CMTS-CM-US-STATS-TYPE スキーマは、次の収集方法をサポートします。

- 時間間隔：セッション設定に基づくスケジュールに従って、定期的な間隔でデータをエクスポートします。時間期間の終了に到達すると、エクスポータはケーブル モデムのアップストリーム ステータス情報を収集し、コレクタにレコードをストリーミングします。
- アドホック：エクスポータは、「FlowStart」メッセージを受信すると、ケーブル モデムのすべてのアップストリーム ステータス情報を収集してそのデータをコレクタに送信するために、アプリケーションをトリガーします。

DOCSIS CMTS トポロジ サービス定義

イベント セッションでは、イベントによってトポロジが変更されます。

このサービス定義スキーマは、CMTS トポロジ情報の IPDR サービス定義スキーマを定義します。

DOCSIS-CMTS-TOPOLOGY-TYPE スキーマは、次の収集方法をサポートします。

- アドホック：すべてのファイバ ノードの全体図を送信します。
- イベント：更新されたファイバ ノード チャネル ステータスのみを送信します。

DOCSIS CPE サービス定義

DOCSIS-CPE-TYPE スキーマは、次の収集方法をサポートします。

- アドホック：セッション設定に基づくスケジュールに従って、定期的な間隔でデータをエクスポートします。時間期間の終了に到達すると、エクスポータは CPE ステータス情報を収集し、コレクタにレコードを転送します。
- イベント：新しい CPE が追加されると、CPE のステータスが変更されるか（IP アドレスの変更を含む）、または新しい CPE が古い CPE を置き換えます（この例では、2 つのメッセージが置き換わります。古い CPE の削除と新しい CPE の追加です）。詳細については、『Operations Support System Interface (OSSI) Specification』を参照してください。

DOCSIS CMTS 使用率統計サービス定義

CMTS 使用率統計は、主にチャネルの使用率に焦点を当てます。CMTS MAC ドメイン、チャネル識別子、およびアップストリームまたはダウンストリーム使用率の属性とカウンタが対象です。

DOCSIS-CMTS-US-UTIL-STATS-TYPE スキーマは、指定された Cisco CMTS の指定されたアップストリーム論理チャネル インターフェイスに関するアップストリーム使用率統計を定義します。間隔は、[Channel Utilization Interval] で設定できます。

DOCSIS-CMTS-DS-UTIL-STATS-TYPE スキーマは、指定された Cisco CMTS の指定されたダウンストリームインターフェイスに関するダウンストリーム使用率統計を定義します。間隔は、[Channel Utilization Interval] で設定できます。

詳細は、次の URL にある『Cisco CMTS Routers』ガイドの「IPDR Streaming Protocol」を参照してください。

IPDR Streaming Protocol

これらのスキーマは、ダウンストリームおよびアップストリーム全体の間隔駆動型イベント セッションのみをサポートします。間隔は、docsIfCmtsChannelUtilizationInterval MIB で定義され、エクスポートごとにドキュメントを作成します。

（注） UsUtilTotalCntnReqDataMslots、UsUtilUsedCntnReqDataMslots、および UsUtilCollCntnReqDataMslots MIB は、Cisco CMTS 実装ではサポートされていません。

RF ゲートウェイ RF チャネル用の DsUtilTotalBytes MIB は、この RF チャネルが間隔中に渡すことができる最大バイト カウンタです。

動作モード

使用量ベースの課金機能は、次の 3 つのモードで動作します。

- ファイルモード：ファイルモードでは、CMTS が課金情報を収集し、その課金情報をローカル ファイル システム上のファイルに書き込みます。その際のファイル名には、ルータのホスト名が前半に、ファイル書き込み時のタイムスタンプが後半に使用されます。次に、リモート アプリケーションが CMTS にログインし、課金アプリケーションがアクセスできる外部サーバに課金情報ファイルを転送します。

リモート アプリケーションは、Secure Copy Protocol（SCP）または Trivial File Transfer Protocol（TFTP）を使用することでファイルを転送できます。転送が成功すると、リモート アプリケーションは課金情報ファイルを削除します。この際に、新しいファイルが作成可能であることが CMTS に伝えられます。リモート アプリケーションは、定期的に CMTS にログインして課金情報ファイルを転送することも、課金情報ファイルが使用可能であることをアプリケーションに通知するために CMTS が SNMPv2 トラップを送信するまで待機することもできます。

- ストリーミング モード：ストリーミング モードでは、CMTS が課金情報を収集し、その後定期的に課金情報ファイルを外部サーバのアプリケーションに転送します。この際は、非セキュア TCP 接続または Secure Sockets Layer（SSL）接続のいずれかが使用されます。収集された課金データはリアルタイムでストリーミングされます。ストリーミングに失敗した場合は、次回の間隔でのみ SAMIS データが送信されます。

CMTS が外部サーバとの接続に失敗した場合は、1 ～ 3 回の間（設定に応じて決まる）で接続を再試行します。CMTS が引き続き外部サーバと接続できない場合、Cisco CMTS は SNMPv2 トラップを送信し、障害が発生したことを SNMP マネージャに通知します。

ストリーミング モードでは、CMTS から定期間隔で課金情報ファイルを転送するように設定できます。ここでの間隔は通常、ケーブル モデム数と、CMTS が作成する課金情報ファイルのサイズによって決まります。

- IPDR モード：IPDR モードでは、IPDR エクスポート プロセスが IPDR コレクタと通信します。このアーキテクチャは複数のコレクタをサポートします。各コレクタは、フェールオーバーのためのプライオリティ値によって識別されます。コレクタが少ないほど、プライオリティ値が高くなります。同じプライオリティ値を持つ 2 つ以上のコレクタへ単一セッションを関連付けることは、ランダム プライオリティと見なされます。いずれの時点でも、データは、最もプライオリティが高い有効なコレクタにのみ送信されます。なんらかの理由で最もプライオリティが高いコレクタへの接続に失敗した場合、データは、次にプライオリティが高い有効なコレクタへ送信されます。最も高いプライオリティのコレクタがオンラインに戻ると、フェールオーバーが再び実行されます。ネットワークの設定によっては、さまざまな IPDR セッションに対して異なるプライマリ コレクタを設定できます。たとえば、課金コレクタや診断コレクタを設定できます。

課金レコード フォーマット

各課金レコードは、DOCSIS 仕様で要求される課金レコード オブジェクトを符号化するために XML フォーマットを使用する ASCII テキスト ファイルです。このファイルは、XML データ ファイルを解析するために構成できる課金アプリケーションで読み取ることができます。

CMTS が生成する各課金レコードに含まれるオブジェクトを以下の表に示します。この表には、オブジェクトの名前（課金レコードに出現するとおり）、およびそのオブジェクトの説明を示しています。

表 *245*：課金レコード オブジェクト

オブジェクト名	説明
IPDRcreationTime	（課金レコードのヘッダーに現れる）CMTS が作成した課金情報の作成日時。
serviceClassName	サービス フロー（たとえば BronzeDS）を識別するサービス クラス名（SCN）。
CMmacAddress	ケーブル モデムの MAC アドレス。ダッシュで区切られた 6 個の 16 進数バイトとして表されます（たとえば 00-00-0C-01-02-03）。
CMipAddress	ケーブル モデムの IP アドレス。ドット付き 10 進表記で表されます（たとえば 192.168.100.101）。

オブジェクト名	説明
CMdocsisMode	ケーブル モデムが現在使用している DOCSIS QoS プロビジョニングのバージョン（DOCSIS 1.0 または 1.1）。
CPEipAddress	このケーブル モデムを使用している各 CPE デバイスの IP アドレス。ドット付き 10 進表記で表されます。このオブジェクトはオプションであり、課金レコードファイルのサイズを削減することでパフォーマンスを向上するために省略できます。
CMTSipAddress	CMTS の IP アドレス。ドット付き 10 進表記で表されます。
CMTShostName	CMTS の完全修飾ホスト名（たとえば cmts01.cisco.com）。
CMTSsysUpTime	CMTS 管理インターフェイスの最後の初期化からの経過時間（100 秒単位）。32 ビットの 10 進数（0 ～ 4,294,967,296）で表されます。
RecType（SFType は Cisco IOS リリース 12.3(17a)BC で RecType に名称変更されました）	記述しているサービス フローのタイプ： • **Interim**：サービス フローは、収集期間を通じてアクティブであったため、1 として報告されます。 • **Stop**：サービス フローは、収集期間のある時点で削除されたため、2 として報告されます。
serviceIdentifier	CMTS によってこのサービス フローに割り当てられたサービス フロー ID。10 進数で表されます。 （注） DOCSIS 1.0 ケーブル モデムの場合、SFID フィールドは常にアップストリームまたはダウンストリームのプライマリ サービス フローを示します。
serviceDirection	サービス フローの方向（**Downstream** または **Upstream**）。

オブジェクト名	説明
serviceOctetsPassed	収集期間に、ケーブルモデム（ダウンストリーム サービス フロー）で受信した、またはケーブル モデム（アップストリーム サービス フロー）で送信した、オクテットの総数。64 ビットの 10 進数で表されます。
servicePktsPassed	収集期間に、ケーブルモデム（ダウンストリーム サービス フロー）で受信した、またはケーブル モデム（アップストリーム サービス フロー）で送信した、パケットの総数。64 ビットの 10 進数で表されます。
SLAdropPkts	（ダウンストリーム サービス フローのみ）加入者のサービス レベル契約（SLA）によって許容される帯域幅レベルを超過するおそれがあったために、CMTS がドロップしたケーブルモデムのダウンストリームパケットの総数。64 ビットの 10 進数で表されます。
SLAdelayPkts	（ダウンストリーム サービス フローのみ）加入者のサービス レベル契約（SLA）によって許容される帯域幅レベルを超過するおそれがあったために、ダウンストリームでケーブルモデムへの送信を CMTS が遅延させたパケットの総数。64 ビットの 10 進数で表されます。
CMTScatvIfIndex	MAC インターフェイスの ifIndex。
CMTScatvIfName	このケーブル モデムに関連付けられている CMTS CATV（MAC）インターフェイスの ifName。
CMTSupIfName	このケーブル モデムに関連付けられている CMTS アップストリーム インターフェイスの ifName。
CMTSdownIfName	このケーブル モデムに関連付けられている CMTS ダウンストリーム インターフェイスの ifName。
CMcpeFqdn	ケーブル モデム関連 CPE の FQDN。
serviceTimeCreated	SF 作成のタイムスタンプ（QoS MIB モデルと一貫性がある）。

オブジェクト名	説明
serviceTimeActive	SF のアクティブ時間（秒）。

（注） バイト カウンタおよびパケット カウンタは 64 ビット値であるため、課金期間中にゼロにラップ アラウンドすることができます。最後の課金期間以降にカウンタがラップされたかどうかを判断するために、課金アプリケーションではカウンタとともに sysUpTime 値を使用する必要があります。カウンタが復帰したように見える場合、この請求サイクルはこのケーブル モデムの次のスケジュールされたサイクルであることを現在の sysUpTime が示していれば、課金サイクル中にカウンタがラップされたと考えられます。

（注） これらの課金レコード オブジェクトは、『*DOCSIS 2.0 OSSI Specification*』（SP-OSSIv2.0-IO3-021218）の付録 B「*IPDR Standards Submission for Cable Data Systems Subscriber Usage Billing Records*」で定義されています。

次の例は、ダウンストリーム サービス フローのサンプル IPDR 課金レコードを示しています。

```
<?xml version="1.0" encoding="UTF-8"?>
<IPDRDoc xmlns="http://www.ipdr.org/namespaces/ipdr"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="DOCSIS-3.1-B.0.xsd"
docId="C341A679-0000-0000-0000-000BBF54D000"
creationTime="2002-05-25T14:41:29Z"
IPDRRecorderInfo="CMTS01"
version="3.1">
</IPDR>
<IPDR xsi:type="DOCSIS-Type">
<IPDRcreationTime>2003-09-18T16:52:34Z</IPDRcreationTime>
<CMTShostname>R7519-UBR7246.cisco.com</CMTShostname>
<CMTSipAddress>1.8.8.21</CMTSipAddress>
<CMTSsysUpTime>287315    </CMTSsysUpTime>
<CMTScatvIfName>Cable8/0/0</CMTScatvIfName>
<CMTScatvIfIndex>13</CMTScatvIfIndex>
<CMTSupIfName>Ca8/0/0-upstream0</CMTSupIfName>
<CMTSupIfType>129</CMTSupIfType>
<CMTSdownIfName>Ca8/0/0-downstream</CMTSdownIfName>
<CMmacAddress>00-00-39-AB-D4-53</CMmacAddress>
<CMdocsisMode>1.0</CMdocsisMode>
<CMipAddress>3.8.21.3</CMipAddress>
<CPEipAddress></CPEipAddress>
<RecType>1</SFtype>
<serviceIdentifier>3</serviceIdentifier>
<serviceClassName></serviceClassName>
<serviceDirection>2</serviceDirection>
<serviceOctetsPassed>23457</ServiceOctetsPassed>
<servicePktsPassed>223</ServicePktsPassed>
<serviceSlaDropPkts>2</serviceSlaDropPkts>
<serviceSlaDelayPkts>0</serviceSlaDelayPkts>
<serviceTimeCreated>11000</serviceTimeCreated>
<serviceTimeActive>15890</serviceTimeActive>
</IPDR>
</IPDRDoc>
```

次の例は、アップストリーム サービス フローのサンプル IPDR 課金レコードを示しています。

<?xml version="1.0" encoding="UTF-8"?>

```
<IPDRDoc xmlns="http://www.ipdr.org/namespaces/ipdr"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="DOCSIS-3.1-B.0.xsd"
docId="docId="C3146152-0000-0000-0000-000BBF7D5800"
creationTime="2003-09-18T16:52:34Z"
IPDRRecorderInfo="CMTS01-UBR7246.cisco.com"
version="3.1">
<IPDR xsi:type=" DOCSIS-Type">
<IPDRcreationTime>2003-09-18T16:52:34Z</IPDRcreationTime>
<CMTShostname>R7519-UBR7246.cisco.com</CMTShostname>
<CMTSipAddress>1.8.8.21</CMTSipAddress>
<CMTSsysUpTime>287315    </CMTSsysUpTime>
<CMTScatvIfName>Cable8/0/0</CMTScatvIfName>
<CMTScatvIfIndex>13</CMTScatvIfIndex>
<CMTSupIfName>Ca8/0/0-upstream0</CMTSupIfName>
<CMTSupIfType>129</CMTSupIfType>
<CMTSdownIfName>Ca8/0/0-downstream</CMTSdownIfName>
<CMmacAddress>00-00-39-18-8A-4D</CMmacAddress>
<CMdocsisMode>1.0</CMdocsisMode>
<CMipAddress>3.8.21.14</CMipAddress>
<CPEipAddress></CPEipAddress>
<RecType>1</SFtype>
<serviceIdentifier>3</serviceIdentifier>
<serviceClassName></serviceClassName>
<serviceDirection>1</serviceDirection>
<serviceOctetsPassed>1404</ServiceOctetsPassed>
<servicePktsPassed>6</ServicePktsPassed>
<serviceSlaDropPkts>0</serviceSlaDropPkts>
<serviceSlaDelayPkts>0</serviceSlaDelayPkts>
<serviceTimeCreated>11000</serviceTimeCreated>
<serviceTimeActive>15890</serviceTimeActive>
</IPDR>
</IPDRDoc>
```

SNMP サポート

Cisco cBR シリーズ コンバージド ブロードバンド ルータs は、従量制課金機能の SNMPv2 サポートを提供する次の MIB をサポートします。

CISCO-CABLE-METERING-MIB

- SNMPv2 コマンドを使用して従量制課金機能の設定をサポートします。
- SNMPv2 コマンドを使用して現在の従量制課金設定を表示します。
- 次の従量制課金イベントに基づき SNMPv2 トラップを送信します。
  - Cisco CMTS により、新しい課金レコードが使用可能であることがレポートされる。
  - Cisco CMTS により、最新の課金レコードの書き込みが失敗したこと（たとえばディスクが満杯）がレポートされる。
  - Cisco CMTS により、課金サーバに課金レコードをストリーミングするためのセキュアな SSL 接続を開くことができなかったことがレポートされる。

CISCO-CABLE-WIDEBAND-MIB

ccwbRFChanUtilInterval オブジェクトを使用して RF チャネルの使用率を計算するためのポーリング間隔を設定します。

DOCS-QOS-MIB

- **docsIfCmtsChannelUtilizationInterval** オブジェクトによりアップストリームおよびダウンストリームの物理チャネルの負荷と使用率を設定します。この情報はキャパシティプランニングおよびインシデント分析に使用でき、特に高値のQoSをプロビジョニングする場合に役立ちます。
- すべてのサービス フロー（DOCSIS 1.1 サービス フローのみ）に関する情報を表示します。たとえば、マルチキャスト サービス フローは、DOCS-QOS-MIB の **docsQosServiceFlowLogTable**、DOCS-IETF-QOS-MIB の **docsIetfQosServiceFlowLogTable**、DOCS-QOS3-MIB の **docsQos3ServiceFlowLogTable** で維持されます。

削除されたサービス フローに関する情報を表示するには、**cablesflog** グローバル コンフィギュレーション コマンドを使用して、削除されたサービスのロギングを有効にします。

利点

従量制課金機能では、ケーブル サービス プロバイダーとそのパートナーおよびカスタマーに次の利点があります。

- サービス プロバイダーは、自社の DOCSIS サービス用課金アプリケーションと他の XML 対応課金アプリケーションとを統合できます。
- 既存のネットワークとサービス（DOCSIS、PacketCable など）をサポートする各種の標準規格に準拠したアプローチであり、Cisco CMTS でのサポートに合わせて将来のサービスをサポートするような拡張が容易です。

従量制課金機能の設定方法

ここでは、従量制課金機能を導入するために必要な次のタスクについて説明します。

CLI コマンドを使用した従量制課金機能ファイル モードの有効化

ここでは、ローカル ファイル システムに課金レコード ファイルを書き込むときに、従量制課金機能がファイル モードで動作するように、従量制課金機能を有効化および設定する方法について説明します。課金アプリケーションは Cisco CMTS にログインし、課金レコード ファイルを定期的に検索する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	例： `Router#`	

ステップ 2	**configureterminal**
	例：
	`Router# configure terminal`
	例：
	`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	**cablemeteringfilesystem** *filesys* [**flow-aggregate**] [**cpe-list-suppress**] [**full-records**]
	例：
	`Router(config)# cable metering filesystem harddisk:`
	例：
	`Router(config)#`
		ファイル モードに対して従量制課金機能をイネーブルにして設定します。
		システムは、ルータのホスト名の後にレコードが書き込まれたときのタイムスタンプが続くファイル名を使用して、このファイル システムに課金レコードを書き込みます。

ステップ 4	**snmp-serverenabletrapscablemetering**
	例：
	`Router(config)# snmp-server enable traps cable metering`
	例：
	`Router(config)#`
		（任意）従量制課金イベントの SNMP トラップをイネーブルにします。新しい課金レコードが使用可能な場合、またはシステムで新しい課金レコードの書き込みの際に障害（ディスク領域の不足など）が発生した場合、トラップは送信されます。

ステップ 5	**cablesflogmax-entry** *number* **entry-duration** *time*
	例：
	`Router(config)# cable sflog max-entry 2000 entry-duration 7200`
	例：
	`Router(config)#`
		（任意）削除した SNMP サービス フローのロギングをイネーブルにすると、課金機能に削除したサービス フローの情報を含められます。

	コマンドまたはアクション	目的

ステップ 6	**cablemeteringsource-interface** *interface*
	
	例：
	`Router(config)# cable metering source-interface loopback100`
	
	例：
	`Router(config)#`
		（任意）課金パケットの送信元インターフェイス（通常はループバック インターフェイス）を指定できるようにします。

ステップ 7	**end**
	
	例：
	`Router(config)# end`
	
	例：
	`Router#`
		グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SNMP コマンドを使用した従量制課金機能ファイル モードの有効化

ここでは、従量制課金機能がファイル モードで動作し、ローカル ファイル システムに課金レコード ファイルを書き込むように、従量制課金機能を有効化および設定する方法について説明します。課金アプリケーションは Cisco CMTS にログインし、課金レコード ファイルを定期的に検索する必要があります。

Cisco CMTS でファイル モードの従量制課金機能を設定するには、CISCO-CABLE-METERING-MIB で多くのオブジェクトを設定する必要があります。

また、課金レコードで削除したサービス フロー（DOCSIS 1.1 サービス フローのサポート）の情報を含めるには、**cablesflog** グローバル コンフィギュレーション コマンドを使用して、削除したサービス フローのロギングを有効にする必要があります。

表 *246*：ファイル モード用に設定する *SNMP* オブジェクト

オブジェクト	タイプ	説明
ccmtrCollectionType	整数	従量制課金機能機能を有効または無効にします。有効な値は次のとおりです。 • 1：なし。従量制課金機能は無効です（デフォルト）。 • 2：ローカル。従量制課金機能は有効で、ファイル モード用に設定されています。 • 3：ストリーム従量制課金機能は有効で、ストリーミング モード用に設定されています。 ccmtrCollectionType を 2（ローカル）に設定し、ファイルモードに対して機能を有効にします。
ccmtrCollectionFilesystem	DisplayString	課金レコードファイルを書き込む必要があるファイル システムを指定します。このオブジェクトの最大長は 25 文字で、ルータ上（slot0、disk1、または flash）の有効なファイル システムを指定する必要があります。 （注） Cisco CMTS は、ルータのホスト名の後にレコードが書き込まれたときのタイムスタンプが続くファイル名を使用して、このファイル システムに課金レコードを書き込みます。

オブジェクト	タイプ	説明
ccmtrCollectionCpeList	TruthValue	（任意）課金レコードのサイズを減らし、パフォーマンスを向上させるために顧客宅内機器（CPE）デバイスのIPアドレスが省略されているかどうかを示します。有効な値は、次のとおりです。 • true：CPE情報が表示されています（デフォルト）。 • false：CPE情報は省略されています。 （注） trueに設定されているとき、ケーブル モデムごとに最大5つのCPEのIPアドレスが表示されます。
ccmtrCollectionAggregate	TruthValue	（任意）個々のケーブルモデムのすべての情報が結合されて、1つのレコードになっているかどうかを示します。アップストリーム トラフィックおよびダウンストリーム トラフィックに対して個別のカウンタが維持されますが、これらのカウンタには、その方向のサービス フローが含まれています。有効な値は次のとおりです。 • true：各ケーブルモデムのすべてのサービス フロー情報が、単一の課金レコードに集約されます。この設定では、課金レコードのサービス フローID（SFID）が0に設定され、サービス クラス名（SCN）は空白になります。 • false：各ケーブル モデムの情報が1つの課金レコードに集約されることはありませんが、代わりに各サービスフローが自身のレコードに記録されます（デフォルト）。
ccmtrCollectionSrcIfIndex	TruthValue	（任意）課金パケットの送信元インターフェイスを示します。

（注） 次の手順では、多くの Unix および Linux システムで利用できる標準的な SNMP コマンドを使用します。各手順では、*ip-address* を Cisco CMTS の IP アドレスと置き換え、読み込みと書き込みのアクセス権をルータに提供する SNMP コミュニティ ストリングと *rw-community-string* を置き換えます。

手順

ステップ 1 ccmtrCollectionType オブジェクトを 2 に設定して、従量制課金機能をイネーブルにし、ファイル モードに対してこの機能を設定します。

例：

```
workstation# setany -v2c

ip-address rw-community-string

ccmtrCollectionType.0 -i 2

workstation#
```

ステップ 2 ccmtrCollectionFilesystem オブジェクトを Cisco CMTS が課金レコードを書き込むローカル ファイル システムに設定します。

例：

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionFilesystem.0 -D disk0:

workstation#
```

ステップ 3 （任意）課金レコードから CPE デバイスの IP アドレスを省略するには、ccmtrCollectionCpeList オブジェクトを 2（false）に設定します。デフォルトでは、CPE 情報が含まれます。

例：

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionCpeList.0 -i 2
workstation#
```

ステップ 4 （任意）単一レコードに各ケーブル モデムのすべてのサービス フロー情報を集約するには、ccmtrCollectionAggregate オブジェクトを 1（true）に設定します。デフォルトは、別のレコードに書き込まれる各サービス フロー用です。

例：

```
workstation# setany -v2c

ip-address rw-community-string
```

```
 ccmtrCollectionAggregate.0 -i 1
workstation#
```

ステップ 5 （任意）課金パケットの送信元インターフェイスを指定するには、ccmtrtrCollectionSrcIfIndex オブジェクトを 1（true）に設定します。デフォルトは、送信元インターフェイスを自動的に選択する課金パケット用です。

例：

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrtrCollectionSrcIfIndex.0 -i 1
workstation#
```

SNMP モードを使用した従量制課金有効化の例

次に、SNMP コマンドを使用して設定された従量制課金機能の例を示します。次に、IP アドレス 10.8.8.21 の Cisco CMTS ルータがデフォルト設定（従量制課金機能は無効）に設定されていることを示します。

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB

ccmtrCollectionType.0 = none(1)
ccmtrCollectionFilesystem.0 =
ccmtrCollectionCpeList.0 = true(1)
ccmtrCollectionAggregate.0 = false(2)
ccmtrCollectionStatus.0 = 0
ccmtrCollectionDestination.0 =
ccmtrCollectionTimestamp.0 = 00 00  00 00   00 00  00 00
ccmtrCollectionNotifEnable.0 = true(1)
workstation#
```

次の SNMP コマンドにより、従量制課金機能を有効にし、ファイル モード用に設定します。

```
workstation# setany -v2c 10.8.8.21 rw-string ccmtrCollectionType.0 -i 2
workstation# setany -v2c 10.8.8.21 rw-string
ccmtrCollectionFilesystem
.0 -D disk1:
workstation#
```

これらのコマンドにより、ルータの実行コンフィギュレーション ファイルに次の行が追加されます。

```
Router# show running-config | include metering

cable metering filesystem disk1:
Router#
```

次の SNMP の表示では、Cisco CMTS が課金レコードの上書きに成功すると、新しい設定を表示します。

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB

ccmtrCollectionType.0 = local(2)
ccmtrCollectionFilesystem.0 = disk1:
ccmtrCollectionCpeList.0 = true(1)
ccmtrCollectionAggregate.0 = false(2)
```

```
ccmtrCollectionStatus.0 = success(1)
ccmtrCollectionDestination.0 = disk1:UBR7246.cisco.com-20030925-185827
ccmtrCollectionTimestamp.0 = 07 d3  09 19   12 3a  1c 00
ccmtrCollectionNotifEnable.0 = true(1)
workstation#
```

CLI コマンドを使用した従量制課金機能ストリーミング モードの有効化

ここでは、従量制課金機能が課金アプリケーションで使用する外部サーバに課金レコードを定期的に送信する場合、従量制課金機能がストリーミング モードで動作するように有効化および設定する方法について説明します。

手順

	コマンドまたはアクション	目的

ステップ 1	**enable**
	
	例：
	`Router> enable`
	
	例：
	`Router#`
		特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

ステップ 2	**configureterminal**
	
	例：
	`Router# configure terminal`
	
	例：
	`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	**cablemeteringdestination** *ip-address port* [*ip-address2 port2*] *retries minutes* {**non-secure** | **secure**} [**flow-aggregate**] [**cpe-list-suppress**] [**full-records**]
	
	例：
	`Router(config)# cable metering destination 10.10.21.3 5300 10.10.21.4 5300 2 30 secure`
	
	例：
	`Router(config)#`
		ストリーミング モードに対して従量制課金機能をイネーブルにして、次のパラメータを設定します。

	コマンドまたはアクション	目的

ステップ 4	**snmp-serverenabletrapscablemetering**
	
	例：
	`Router(config)# snmp-server enable traps cable metering`
	
	例：
	`Router(config)#`
		（任意）従量制課金イベントのSNMPトラップをイネーブルにします。新しい課金レコードが使用可能な場合、またはシステムで新しい課金レコードの書き込みの際に障害（ディスク領域の不足など）が発生した場合、トラップは送信されます。

ステップ 5	**cablesflogmax-entry** *number* **entry-duration** *time*
	
	例：
	`Router(config)# cable sflog max-entry 2000 entry-duration 7200`
	
	例：
	`Router(config)#`
		（任意）削除したSNMPサービス フローのロギングをイネーブルにすると、課金機能に削除したサービス フローの情報を含められます。

ステップ 6	**cablemeteringsource-interface** *interface*
	
	例：
	`Router(config)# cable metering source-interface loopback100`
	
	例：
	`Router(config)#`
		（任意）課金パケットの送信元インターフェイス（通常はループバック インターフェイス）を指定できるようにします。

ステップ 7	**end**
	
	例：
	`Router(config)# end`
	
	例：
	`Router#`
		グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SNMP コマンドを使用した従量制課金機能ストリーミング モードの有効化

ここでは、従量制課金機能がストリーミング モードで動作するように従量制課金機能を有効化および設定する SNMP コマンドの使用方法について説明します。この機能は、課金アプリケーションで使用する外部サーバに課金レコードを定期的に送信します。

Cisco CMTS でストリーミング モードの従量制課金機能を設定するには、CISCO-CABLE-METERING-MIB で多くのオブジェクトを設定する必要があります。

（注） また、課金レコードで削除したサービス フロー（DOCSIS 1.1 サービス フローのみ）の情報を含めるには、**cablesflog** グローバル コンフィギュレーション コマンドを使用して、削除したサービス フローのロギングを有効にする必要があります。Cisco.com にある『*Cisco IOS CMTS Cable Command Reference Guide*』を参照してください。

『Cisco CMTS Cable Command Reference』

表 *247*：ストリーミング モード用に設定する *SNMP* オブジェクト

オブジェクト	タイプ	説明
[illegible]	整数	

オブジェクト	タイプ	説明
		従量制課金機能機能を有効または無効にします。有効な値は次のとおりです。 • :1 なし。従量

オブジェクト	タイプ	説明
		制課金機能は無効です(デフォルト)。

オブジェクト	タイプ	説明
		• 2 ヒカル従量制課金機能は有効で、アイルモード用に設定されています。

オブジェクト	タイプ	説明
		• 3 ストサム従量制課金機能は有効で、ストサミングモード用に設定されています。

オブジェクト	タイプ	説明
		[redacted] を 3（ストリーム）に設定し、ストリーミングモードに対して機能を有効にします。

オブジェクト	タイプ	説明
[illegible]	[illegible]	外部収集サーバのIPアドレス。この値は指定する必要があります。

オブジェクト	タイプ	説明
[illegible]	[illegible]	

オブジェクト	タイプ	説明
		課金レコードの送信先である外部収集サーバのTCPポート番号。有効範囲は0～65535ですが、ポートを既知

オブジェクト	タイプ	説明
		の範囲 0 ～ 1024 に指定しないでください。この値は指定する必要があります。

（注） ccmCollectionIpAddress オブジェクトおよび ccmCollectionPort オブジェクトを 2 度設定し、プライマリ収集サーバとセカンダリ収集サーバを指定できます。

オブジェクト	タイプ	説明
[illegible]	[illegible]	

オブジェクト	タイプ	説明
		（任意）収集サーバで使用されるIPアドレスのタイプ。有効な値はipv4のみで、これがデフォルト値で

オブジェクト	タイプ	説明
		す。

オブジェクト	タイプ	説明
[illegible]	[illegible]	

オブジェクト	タイプ	説明
		（任意）課金レコードが外部サーバにストリーミングされる頻度を分単位で指定します。有効範囲は 2

オブジェクト	タイプ	説明
		～1440分（24時間、デフォルトは30分です。（最小の間隔は30分にすることをお勧めします。）

オブジェクト	タイプ	説明
[illegible]	[illegible]	

オブジェクト	タイプ	説明
		（任意）セカンダリサーバ（設定されている場合）を使用して障害に関するSNMPトラップを送信する前

オブジェクト	タイプ	説明
		に、CMTSが外部サーバとのセキュアな接続を確立するための再試行回数を指定します。*n* の有効な範

オブジェクト	タイプ	説明
		囲は 0 ～ 5、デフォルトは 0 です。

（注） SNMP コマンドでストリーミング モードに従量制課金を設定するとき、ccmCollectionInterval パラメータと ccmCollectionRetries パラメータは任意ですが、これらのパラメータは、CLI コマンドで機能を設定するときには必須です。

オブジェクト	タイプ	説明
[illegible]	[illegible]	

オブジェクト	タイプ	説明
		（任意）Cisco CMTSが、外部サーバの課金アプリケーションと接続するとき、セキュアソケットレイヤ（SSL）接続を使

オブジェクト	タイプ	説明
		用するかどうかを指定します有効な値は次のとおりです。

オブジェクト	タイプ	説明
		Int cs C STC LSS は S 接続を使用します。 このオプション は、 ベースラインプライバシインタフェイス （ BP 暗号

オブジェクト	タイプ	説明
		SMC化をサポートするソフトウェアイメージでのみ使用できます。

オブジェクト	タイプ	説明
		は非暗号化 PCT 接続を使用します。これはデフォルト値です。

オブジェクト	タイプ	説明
[illegible]	[illegible]	

オブジェクト	タイプ	説明
		（任意）課金レコードのサイズを減らし、パフォーマンスを向上させるために顧客宅内機器（CPE）デバイ

オブジェクト	タイプ	説明
		スのIPアドレスが省略されているかどうかを示します。有効な値は、次のとおりです。

オブジェクト	タイプ	説明
		• true EPC 情報が表示されています(デフォルト)。 • false EPC 情報は省略されています。

オブジェクト	タイプ	説明
		（注）

に設定されているときケーブルモデムごとに最大5つのIPのPアドレスが表示されます

オブジェクト	タイプ	説明
[illegible]	[illegible]	

オブジェクト	タイプ	説明
		（任意）個々のケーブルモデムのすべての情報が結合されて、1つのレコードになっているかどうかを示

オブジェクト	タイプ	説明
		します。アップストリームトラフィックおよびダウンストリームトラフィックに対して個別のカウンタが

オブジェクト	タイプ	説明
		維持されますが、これらのカウンタには、その方向のサービスフローが含まれています。有効な値

オブジェクト	タイプ	説明
		は次のとおりです。

オブジェクト	タイプ	説明
		crt 各ケーブルモデムのすべてのサービスフロー情報が単一の課金レコードに集約されます。この設

オブジェクト	タイプ	説明
		定では課金レコードのサービスフロー DIS が 0 に設定され、サービスクラス名 (SN) は空白になります。

オブジェクト	タイプ	説明
		各ケーブルモデムの情報が1つの課金レコードに集約されることはありませんが代わりに

オブジェクト	タイプ	説明
		各サービスフローが自身のレコードに記録されますデフォルト。

オブジェクト	タイプ	説明
[illegible]	[illegible]	（任意）課金パケットの送信元インターフェイスを示します。

（注） 次の手順では、多くの Unix および Linux システムで利用できる標準的な SNMP コマンドを使用します。各手順では、*ip-address* を Cisco CMTS の IP アドレスと置き換え、読み込みと書き込みのアクセス権をルータに提供する SNMP コミュニティ ストリングと *rw-community-string* を置き換えます。

手順

ステップ 1 ccmCollectionType オブジェクトを 3 に設定して、従量制課金機能をイネーブルにし、ストリーミング モードに対してこの機能を設定します。

例：

```
workstation# setany -v2c
ip-address rw-community-string
```

```
 ccmCollectionType.0 -i 3
workstation#
```

ステップ 2 ccmCollectionIpAddress オブジェクトと ccmCollectionPort オブジェクトを、外部収集サーバの IP アドレスと課金レコードの送信先である TCP ポート番号に設定します。

例：

```
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionIpAddress.1 -o '0a 08 06 0b'

workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionPort.1 -g 6789

workstation#
```

ステップ 3 （任意）Cisco CMTS がプライマリ収集サーバに接続できない場合は、ccmCollectionIpAddress オブジェクトと ccmCollectionPort オブジェクトを 2 度設定し、課金レコードの送信先である 2 番目の外部収集サーバの IP アドレスと TCP ポート番号を指定します。

例：

```
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionIpAddress.1 -o '0a 08 06 0c'

workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionPort.1 -g 7000

workstation#
```

ステップ 4 （任意）他のデフォルト パラメータのいずれかを変更するには、適切なオブジェクトを目的の値に設定します。たとえば、次の行では、収集間隔は 45 分、最大試行回数は 3 回で、非セキュアな接続に従量制課金機能を設定しています。

例：

```
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionSecure.1 -i 2
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionInterval.1 -i 45
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionRetries.1 -i 3
workstation#
```

ステップ 5 （任意）課金レコードから CPE デバイスの IP アドレスを省略するには、ccmCollectionCpeList オブジェクトを 2（false）に設定します。デフォルトでは、CPE 情報が含まれます。

例：

```
workstation# setany -v2c

ip-address rw-community-string
```

```
 ccmCollectionCpeList.0 -i 2
workstation#
```

ステップ 6 （任意）単一レコードに各ケーブル モデムのすべてのサービス フロー情報を集約するには、ccmCollectionAggregate オブジェクトを 1（true）に設定します。デフォルトは、別のレコードに書き込まれる各サービス フロー用です。

例：

```
workstation# setany -v2c

ip-address rw-community-string
 ccmCollectionAggregate.0 -i 1
workstation#
```

ステップ 7 （任意）課金パケットの送信元インターフェイスを指定するには、ccmtrCollectionSrcIfIndex オブジェクトを 1（true）に設定します。デフォルトは、送信元インターフェイスを自動的に選択する課金パケット用です。

例：

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionSrcIfIndex.0 -i 1
workstation#
```

SNMP コマンドの例

次に、SNMP コマンドを使用して設定された従量制課金機能の例を示します。次に、IP アドレス 10.8.8.21 の Cisco CMTS ルータがデフォルト設定（従量制課金機能は無効）に設定されていることを示します。

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB

ccmCollectionType.0 = none(1)
ccmCollectionFilesystem.0 =
ccmCollectionCpeList.0 = true(1)
ccmCollectionAggregate.0 = false(2)
ccmCollectionStatus.0 = 0
ccmCollectionDestination.0 =
ccmCollectionTimestamp.0 = 00 00  00 00   00 00  00 00
ccmCollectionNotifEnable.0 = true(1)
workstation#
```

次の SNMP コマンドにより、従量制課金機能を有効にし、ストリーミング モード用に設定します。

```
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionType.0 -i 3
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionIpAddress.1 -o '0a 08 06 0b'

workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionPort.1 -g 6789

workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionSecure.1 -i 2
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionRetries.1 -i 3
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionInterval.1 -i 45
```

```
workstation#
```

これらのコマンドにより、ルータの実行コンフィギュレーション ファイルに次の行が追加されます。

```
Router# show running-config | include metering

cable metering destination 10.8.6.11 6789 3 45 non-secure
Router#
```

次の SNMP の表示は新しい設定を示します。

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB

ccmCollectionType.0 = stream(3)
ccmCollectionFilesystem.0 =
ccmCollectionIpAddrType.1 = ipv4(1)
ccmCollectionIpAddress.1 = 0a 08  06 0b
ccmCollectionPort.1 = 6789
ccmCollectionInterval.1 = 45
ccmCollectionRetries.1 = 3
ccmCollectionSecure.1 = false(2)
ccmCollectionRowStatus.1 = active(1)
ccmCollectionCpeList.0 = true(1)
ccmCollectionAggregate.0 = false(2)
ccmCollectionStatus.0 = 0
ccmCollectionDestination.0 =
ccmCollectionTimestamp.0 = 00 00  00 00   00 00  00 00
ccmCollectionNotifEnable.0 = true(1)
workstation#
```

Secure Copy Protocol の有効化と設定（任意）

ここでは、Cisco CMTS に Secure Copy Protocol（SCP）を設定する方法について説明します。これにより、外部サーバは Cisco CMTS にログインし、Cisco CMTS から外部サーバに課金レコードをコピーできます。

手順

	コマンドまたはアクション	目的

ステップ 1	**enable**
	
	例：
	`Router> enable`
	
	例：
	`Router#`
		特権EXECモードをイネーブルにします。パスワードを入力します（要求された場合）。

ステップ 2	**configureterminal** 例： `Router# configure terminal`	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。

	コマンドまたはアクション	目的
	例： `Router(config)#`	

ステップ 3	**aaanew-model**
	例：
	`Router(config)# aaa new-model`
	例：
	`Router(config)#`
		認証、許可、アカウンティング（AAA）アクセス コントロール モデルをイネーブルにします。

ステップ 4	**aaaauthenticationlogin** {**default** | *list-name* } *method1* [*method2* ...]
	例：
	`Router(config)# aaa authentication login default enable`
	例：
	`Router(config)#`
		次のパラメータを使用して、ログインでのAAA アクセス コントロール認証をイネーブルにします。
		有効な方法には **enable**、**line**、および **local** があります。

ステップ 5	**aaaauthorization exec**{**default** | *list-name* } *method1* [*method2* ...]
	例：
	`Router(config)# aaa authorization exec default local`
	例：
	`Router(config)#`
		ユーザが EXEC シェルを実行し、Secure Copy コマンド実行のためにCLIにアクセスできるように CMTS を設定します。
		有効な方法には **local** があります。

ステップ 6	**username** *name* **privilege** *level* **password** *encryption-type password*
	例：
	`Router(config)# username billingapp privilege 15 password 7 billing-password`
	例：
	`Router(config)#`
		（任意）ログイン アクセスのユーザ アカウントを作成し、そのアカウントの特権レベルおよびパスワードを指定します。
		（注） この手順はオプションですが、セキュリティと管理のために、CMTS へのログインに使用する課金アプリケーション用の独自のアカウントを作成することを推奨します。

	コマンドまたはアクション	目的

ステップ 7	**ipsshtime-out** *seconds*
	
	例：
	`Router(config)# ip ssh time-out 120`
	
	例：
	`Router(config)#`
		SCP の使用に必要なセキュア シェル（SSH）アクセスを Cisco CMTS でイネーブルにします。*seconds* パラメータは、SSH 認証に許可する最長時間を秒単位で指定します。有効範囲は 0 ～ 120 秒、デフォルトは 120 秒です。

ステップ 8	**ipsshauthentication-retries** *n*
	
	例：
	`Router(config)# ip ssh authentication-retries 3`
	
	例：
	`Router(config)#`
		ルータが SSH セッションを切断するまでに、ユーザに許可するログイン試行最大回数を指定します。有効範囲は 1 ～ 5、デフォルトは 3 回です。

ステップ 9	**ipscpserverenable**
	
	例：
	`Router(config)# ip scp server enable`
	
	例：
	`Router(config)#`
		Cisco CMTS で SCP アクセスをイネーブルにします。

ステップ 10	**end**
	
	例：
	`Router(config)# end`
	`Router#`
		グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

SSL 運用に対応する Cisco CMTS の設定

このセクションでは、従量制課金機能が SSL 接続を使用してストリーミング モードで課金レコード ファイルを転送できるようにするため、Secure Sockets Layer（SSL）運用に対応するように Cisco CMTS を設定する手順について説明します。

（注） この手順が必要になるのは、**secure** オプションを指定した **cable metering destination** コマンドを使用する場合のみです。

CA の前提条件

- 課金アプリケーション サーバを SSL 動作用に設定する必要があります。
- 課金アプリケーションと Cisco CMTS ルータに必要なデジタル証明書を提供する認証局（CA）が設定される必要があります。CA は Verisign などのパブリック CA、または Cisco Provisioning Center（CPC）などのソフトウェアが実行されているプライベート管理ネットワーク上のサーバにすることができます。

手順の概要

Cisco CMTS ルータを SSL 動作用に準備するには、次の手順を実行します。

- ルータのホスト名と IP ドメイン名を設定します（設定されていない場合）。
- RSA キー ペアを生成します。
- 認証局を宣言します。
- ルート CA（Trusted Root）を設定します。
- CA を認証します。
- 証明書を要求します。

これらの手順の詳細については、「Configuring Certification Authority Interoperability」を参照してください。

ファイル モードでの Cisco CMTS からのレコードの取得

従量制課金機能がイネーブル化され、ファイル モード用に設定されている場合、課金アプリケーション サーバは、Cisco CMTS から定期的に課金レコードを取得する必要があります。これは通常、Cisco CMTS にログインし、CLI コマンドを使用してファイルを転送するか、または SNMP コマンドを使用するスクリプトによってファイルを転送するかにより実行されます。

CLI コマンドを使用する場合は、次のようにな手順になります。

1. 課金レコードが書き込まれると、課金アプリケーション サーバは Cisco CMTS から SNMP トラップを受信します。この通知には、取得する必要がある課金レコードのファイル名が含まれます。
2. 課金アプリケーション サーバは、課金レコードを取得するためのカスタム スクリプトの書き込みを開始します。このスクリプトにより、次のいずれかが実行されます。
   a. CLI コマンドを使用している場合、スクリプトは Telnet 接続を使用して Cisco CMTS にログインし、続いて **copy** CLI コマンドを使用して課金アプリケーション サーバに課金レコードを転送します。転送は Secure Copy Protocol（SCP）または Trivial File Transfer Protocol（TFTP）を使用して実行できます。

（注） File Transfer Protocol（FTP）を使用して Cisco CMTS から外部 FTP サーバにファイルを転送することもできますが、FTP プロトコルはログイン ユーザ名とパスワードをクリアテキストで送信するため、これは推奨されません。

1. SNMP コマンドを使用している場合、スクリプトは CISCO-FLASH-MIB に ciscoFlashCopyEntry オブジェクトを設定し、TFTP を使用してアプリケーション サーバに課金レコードを転送します。
2. 課金レコードの転送後は、Cisco CMTS が新しい課金レコードの作成を開始できるよう、スクリプトは Cisco CMTS ファイル システム上の課金レコードを削除します。

次のセクションに、それぞれ方法を使用した場合にこれがどのように実行されるかを例により示します。

ヒント 次の例は、単なる説明用です。通常、これらのコマンドは、課金レコードを取得するための自動化されたスクリプトに組み込まれています。

SCP の使用

SCP を使用して課金レコードを転送するには、21 ページの「Secure Copy Protocol の有効化と設定（任意）」セクションにある手順に従って、まず SCP の動作に合わせてルータを有効化および設定する必要があります。次に、アプリケーション サーバで Cisco CMTS にログインし、特権 EXEC プロンプトで **copy** コマンドを使用します。**copy** コマンドでは、ローカル ファイルシステム上の課金レコードの場所と、SCP 転送の宛先サーバの場所を指定する必要があります。

次に、slot0 の課金レコードが billserver.mso-example.com というホスト名の FTP サーバに転送される場合の一般的なセッション例を示します。

```
CMTS01# copy slot0:CMTS01_20030211-155025 scp://billingapp-server.mso-example.com/

Address or name of remote host [billingapp-server.mso-example.com]?
Destination username [billing-app]?
Destination filename [CMTS01_20030211-155025]?
Writing CMTS01_20030211-155025
Password: billing-password

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1403352/1024 bytes]
1403352 bytes copied in 17.204 secs (85631 bytes/sec)
CMTS01# delete slot0:CMTS01_20030211-155025

CMTS01# squeeze slot0:

CMTS01#
```

（注） 課金アプリケーションは、Cisco CMTS が次のレコードを書き込むことができるように、課金レコードの転送が正常に完了したら、その課金レコードを削除する必要があります。**squeeze** コマンドは、フラッシュ メモリ上および旧式の PCMCIA カード（ブートフラッシュ、フラッシュ、slot0、slot1）上で削除されたディスク領域を解放します。新しい ATA 形式の PCMCIA カード（disk0、disk1、disk2）では不要です。ただし、**squeeze** コマンドが完了するまでに数秒かかるため、新しい課金レコードに十分なディスク領域がない場合にのみこのコマンドを実行する必要があります。この問題を回避するために、削除したファイルのディスク領域を自動的に解放する 64 MB（またはそれ以上）の ATA 形式の PCMCIA メモリ カードを使用することを推奨します。

TFTP の使用

TFTP を使用して課金レコードを転送するには、まず外部ワークステーションを TFTP サーバになるように設定する必要があります。セキュリティ上の理由から、Cisco CMTS ルータなどの許可された TFTP クライアントのみが TFTP サーバにアクセスできるように、TFTP サーバをインターネットまたは外部ネットワークから隔離する必要があります。

課金レコードを転送するには、アプリケーション サーバで Cisco CMTS にログインし、特権 EXEC プロンプトで **copy** コマンドを使用します。**copy** コマンドでは、ローカル ファイルシステム上の課金レコードの場所と TFTP を転送する宛先サーバの場所を指定する必要があります。

次に、slot0 の課金レコードが billserver.mso-example.com というホスト名の TFTP サーバに転送される場合の一般的なセッション例を示します。

```
Router# copy slot0:CMTS01_20030211-155025 tftp://billingapp-server.mso-example.com/incoming

Address or name of remote host [billingapp-server.mso-example.com]?
Destination username [billing-app]?
Destination filename [CMTS01_20030211-155025]?
Writing CMTS01_20030211-155025
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1102348/1024 bytes]
1102348 bytes copied in 14.716 secs (63631 bytes/sec)
Router# delete slot0:CMTS01_20030211-155025

Router# squeeze slot0:

Router#
```

（注） 課金アプリケーションは、Cisco CMTS が次のレコードを書き込むことができるように、課金レコードの転送が正常に完了したら、その課金レコードを削除する必要があります。**squeeze** コマンドは、フラッシュ メモリ上および旧式の PCMCIA カード（ブートフラッシュ、フラッシュ、slot0、slot1）上で削除されたディスク領域を解放します。新しい ATA 形式の PCMCIA カード（disk0、disk1、disk2）では不要です。ただし、**squeeze** コマンドが完了するまでに数秒かかるため、新しい課金レコードに十分なディスク領域がない場合にのみこのコマンドを実行する必要があります。この問題を回避するために、削除したファイルのディスク領域を自動的に解放する 64 MB（またはそれ以上）の ATA 形式の PCMCIA メモリ カードを使用することを推奨します。

SNMP の使用

SNMP コマンドを使用して課金レコード ファイルを転送するには、CISCO-FLASH-MIB で大量のオブジェクトを設定し、ファイルを TFTP サーバに転送する必要があります。ファイルの転送に成功すると、SNMp コマンドを使用して課金レコード ファイルを削除できます。

（注） 次の手順に進む前に、TFTP サーバが課金レコードを受信できるように正しく設定されていることを確認します。少なくとも、すべてのユーザが読み取りおよび書き込み可能なディレクトリを作成しておく必要があります。また、一部のサーバの TFTP サーバ ソフトウェアでは、受信するファイルと同じ名前のファイルも作成する必要があります。このファイルは、すべてのユーザが読み取りと書き込みを行える必要があります。

TFTP サーバに課金レコード ファイルを転送するには、SNMP コマンドを使用して、CISCO-FLASH-MIB で大量のオブジェクトを設定します。

表 *248*：*SNMP* コマンドを使用した *TFTP* サーバへのファイルの転送

オブジェクト	タイプ	説明
ciscoFlashCopyEntryStatus	RowStatus	このテーブル エントリのステータス。通常、このオブジェクトの最初の設定は 5（create-and-wait）です。他のすべてのパラメータを指定すると、Active（1）に設定され、コマンドが実行されます。
ciscoFlashCopyCommand	INTEGER	実行する copy コマンドのタイプ。TFTP サーバに課金レコード ファイルをコピーするには、このオブジェクトを 3（copyFromFlash）に設定します。

オブジェクト	タイプ	説明
ciscoFlashCopyServerAddress	IpAddress	TFTP サーバの IP アドレスです。 （注） このパラメータはブロードキャスト アドレス 255.255.255.255 にデフォルトで設定されます。つまり、課金レコード ファイルが応答する最初の TFTP サーバに転送されます。セキュリティ上の理由から、このオブジェクトは許可された TFTP サーバの IP アドレスに必ず送信されます。
ciscoFlashCopySourceName	DisplayString	保存されているフラッシュ デバイスなど、転送する課金レコードファイルの名前。
ciscoFlashCopyDestinationName	DisplayString	（任意）パスを含む、TFTP サーバの課金レコードの名前。指定しない場合は、コピー操作により、課金レコードが元のファイル名で TFTP サーバの最上位ディレクトリにデフォルトで保存されます。 （注） 接続先のファイル名を持つファイルが、TFTP サーバにすでに存在している必要があります。このファイルは、課金レコード ファイルで置き換えられるように、すべてのユーザが読み取りおよび書き込みを行える必要があります。
ciscoFlashCopyProtocol	INTEGER	（任意）ファイルをコピーするときに使用するプロトコルを指定します。TFTP 転送の場合、このオブジェクトをデフォルトの 1（tftp）に設定します。
ciscoFlashCopyNotifyOnCompletion	TruthValue	（任意）Cisco CMTS がコピー操作を完了するときにトラップを生成するかどうかを指定します。デフォルトは false です（トラップは生成されません）。

課金レコード ファイルの転送後、Cisco CMTS が新しいファイルの作成を開始できるように、CISCO-FLASH-MIB で大量のオブジェクトを設定する必要があります。フラッシュ メモリが ATA 互換でない場合は、大量のオブジェクトを設定し、フラッシュ メモリをスクイーズして、新しいファイルのために削除されたスペースを使用できるようにする必要があります。表 249：SNMP コマンドを使用したファイルの削除，（1714 ページ） では、次のオブジェクトを説明し、必須またはオプションかどうかを示します。

表 *249*：*SNMP* コマンドを使用したファイルの削除

オブジェクト	タイプ	説明
ciscoFlashMiscOpCommand	INTEGER	実行する操作を指定します。 • 3：ファイルを削除します。 • 5：フラッシュ メモリをスクイーズし、削除されたスペースを回復して、新しいファイルが使用できるようにします。
ciscoFlashMiscOpDestinationName	DisplayString	ファイルを削除する場合、ファイル システム名など、削除するファイルの名前（最大 255 文字）。 ファイル システムをスクイーズする場合、スクイーズするファイル システムの名前（slot0:、slot1:、flash:、または bootflash:）。
ciscoFlashMiscOpEntryStatus	RowStatus	このテーブル エントリのステータス。通常、このオブジェクトの最初の設定は 5（create-and-wait）です。他のすべてのパラメータを指定すると、Active（1）に設定され、コマンドが実行されます。
ciscoFlashMiscOpNotifyOnCompletion	TruthValue	（任意）Cisco CMTS がこの操作を完了するときにトラップを生成するかどうかを指定します。デフォルトは false です（トラップは生成されません）。

手順の詳細

（注） 次の手順では、多くの Unix および Linux システムで利用できる標準的な SNMP コマンドを使用します。各手順では、*ip-address* を Cisco CMTS の IP アドレスと置き換え、読み込みと書き込みのアクセス権をルータに提供する SNMP コミュニティ ストリングと *rw-community-string* を置き換えます。

TFTP サーバへの課金レコード ファイルのコピー

手順

ステップ 1 コピーを実行するスクリプトでは、この copy コマンドのインデックス エントリとして使用する 32 ビットの数値を生成する必要があります。このスクリプトは、インデックス数値が他の操作で現在使用されていない限り、この数値を便利な方法で生成できます。

ステップ 2 ステップ 1 で生成された数値を使用し、ciscoFlashCopyEntryStatus オブジェクトを create-and-wait 状態（5）に設定して、copy コマンドのテーブル エントリを作成します。

例：

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyEntryStatus.582 -i 5

workstation#
```

ステップ 3 ciscoFlashCopyCommand を 3（copyFromFlash）に設定し、課金レコード ファイルがルータのフラッシュ ファイル システムからコピーされるように指定します。

例：

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyCommand
.582

-i 3
workstatioN#
```

ステップ 4 ciscoFlashCopyServerAddress オブジェクトを TFTP サーバの IP アドレスに設定します。

例：

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyServerAddress
.582

-a "172.20.12.193"

workstatioN#
```

ステップ 5 ciscoFlashCopySourceName オブジェクトを、転送する課金レコードのデバイス名などのファイル名に設定します。

例：

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopySourceName
.582
-D
"slot0:CMTS01_20030211-155025
```

```
"
workstation#
```

ステップ 6 （任意）TFTP サーバで特定の接続先を指定するには、ciscoFlashCopyDestinationName オブジェクトを、TFTP サーバの課金レコード ファイルのパス名とファイル名に設定します。（通常、パス名およびファイル名が TFTP サーバ上にすでに存在している必要があります。）

例：

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyDestinationName
.582
-D
"/cmts01-billing/billing-file
"
workstation#
```

ステップ 7 コマンドを実行するには、ciscoFlashCopyEntryStatus オブジェクトを active 状態（1）に設定します。

例：

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyEntryStatus.582 -i 1

workstation#
```

ステップ 8 ファイル転送が完了するまで ciscoFlashCopyStatus オブジェクトを定期的にポーリングします。

例：

```
workstation# getmany -v2c ip-address rw-community-string ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyInProgress(1)
workstation# getmany -v2c ip-address rw-community-string ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyInProgress(1)
workstation# getmany -v2c ip-address rw-community-string ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyOperationSuccess(2)
workstation#
```

ファイル転送に失敗した場合、ciscoFlashCopyStatus オブジェクトで報告される共通のステータス値は次のとおりです。

- 3：copyInvalidOperation。通常、接続先ファイル名およびパス名が TFTP サーバに存在しないか、または存在するけれどもすべてのユーザが書き込みできないため、操作が TFTP サーバで失敗したことを示します。
- 5：copyInvalidSourceName。ciscoFlashCopySourceName で指定された課金レコードのファイル名が存在しません。正しいデバイス名を指定していること、ファイル名にスペースがないことを確認します。
- 6：copyInvalidDestName。ciscoFlashCopyDestinationName で指定した接続先パス名およびファイル名に、TFTP サーバからアクセスすることができません。これは、パス名が存在しないか、または書き込みアクセスを許可するように設定されていない可能性があります。また、同じパス名とファイル名を持つファイルが TFTP サーバ上にすでに存在すると、このエラーが発生する場合があります。

- 7：copyInvalidServerAddress。ciscoFlashCopyServerAddress で指定された TFTP サーバの IP アドレスが無効であるか、または TFTP サーバが応答していません。
- 14：copyFileTransferError。ネットワーク エラーが発生し、ファイル転送が完了できませんでした。

ステップ 9 ファイルの転送に成功したら、ciscoFlashCopyEntryStatus オブジェクトを 6（delete）に設定してこの copy コマンドの行エントリを削除します。

例：

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyEntryStatus.582 -i 6
workstation#
```

次の作業

課金レコード ファイルの削除

SNMP の使用

課金レコード ファイルの転送に成功したら、Cisco CMTS が新しい課金レコードを書き込むことができるように、次の手順を実行して Cisco CMTS フラッシュ ファイル システムの課金レコードを削除します。

手順

ステップ 1 インデックス エントリとして使用する別の乱数を生成し、ciscoFlashMiscOpTable の次のオブジェクトを設定します。

例：

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus
.31 -i 5

workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpCommand
.31 -i 3
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpDestinationName
.31 -D
"/cmts01-billing/CMTS01_20030211-155025
"
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus
.31 -i 1

workstation#
```

ステップ 2 ファイル転送が完了するまで ciscoFlashMiscOpStatus オブジェクトを定期的にポーリングします。

例：

```
workstation# getmany -v2c ip-address rw-community-string ciscoFlashMiscOpStatus
```

```
.31
  ciscoFlashCopyStatus.31 = miscOpInProgress(1)
workstation# getmany -v2c ip-address rw-community-string ciscoFlashMiscOpStatus
.31
  ciscoFlashCopyStatus.582 = miscOpOperationSuccess(2)
workstation#
```

ステップ 3 フラッシュ メモリ システムが ATA 互換でない場合（slot0:、slot1:、flash:、または bootflash:）、ciscoFlashMiscOpTable の次のオブジェクトを設定し、フラッシュ ファイル システムをスクイーズして、削除したファイル スペースを回復します。

例：

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus
.32
-i 5

workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpCommand
.32 -i 5
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpDestinationName
.32 -D slot0:
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus
.32
-i 1

workstation#
```

SNMP を使用した転送の例

次の SNMP コマンドにより、IP アドレス 10.10.31.3 にある TFTP サーバに CMTS01_20030211-155025 という名前のファイルが転送されます。ファイルが正常に転送されると、このコピー コマンドの行エントリが削除されます。

```
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyEntryStatus.582 -i 5

workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyCommand
.582
 -i 3
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyServerAddress
.582
 -a "10.10.31.3"

workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopySourceName
.582 -D
"slot0:CMTS01_20030211-155025
"
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyDestinationName
.582 -D
"/cmts01-billing/CMTS01_20030211-155025
"
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyEntryStatus.582 -i 1

workstation# getmany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyStatus
```

```
.582
  ciscoFlashCopyStatus.582 = copyInProgress(1)
workstation# getmany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyOperationSuccess(2)
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyEntryStatus.582 -i 6

workstation#
```

次のコマンドでは、Cisco CMTS ファイル システムで削除された課金レコード ファイル、およびスクイーズ操作によって回復された削除済みファイルのスペースを示します。

```
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpEntryStatus
.31 -i 5

workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpCommand
.31 -i 3
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpDestinationName
.31 -D
"/cmts01-billing/CMTS01_20030211-155025
"
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpEntryStatus
.31 -i 1

workstation# getmany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpStatus
.31
  ciscoFlashCopyStatus.31 = miscOpInProgress(1)
workstation# getmany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpStatus
.31
  ciscoFlashCopyStatus.582 = miscOpOperationSuccess(2)
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpEntryStatus
.32 -i 5

workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpCommand
.32 -i 5
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpDestinationName
.32 -D slot0:
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpEntryStatus
.32 -i 1

workstation#
```

従量制課金機能の無効化

ここでは、従量制課金をディセーブルにする方法について説明します。このコマンドを実行すると、課金情報の収集がすぐに停止されます。課金レコードの上書きや外部サーバへの送信が行われている場合は、CMTS はその操作を完了してから、従量制課金機能をディセーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**enable**
	例：
	`Router> enable`
	例：
	`Router#`
		特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。

ステップ 2	**configureterminal**
	例：
	`Router# configure terminal`
	例：
	`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	**nocablemetering**
	例：
	`Router(config)# no cable metering`
	例：
	`Router(config)#`
		従量制課金機能をすぐにディセーブルにし、課金情報の収集を停止します。

ステップ 4	**nosnmp-serverenabletrapscablemetering**
	例：
	`Router(config)# no snmp-server enable traps cable metering`
	例：
	`Router(config)#`
		（任意）従量制課金イベントの SNMP トラップをディセーブルにします。

ステップ 5	**nocablesflog**
	例：
	`Router(config)# no cable sflog`
	例：
	`Router(config)#`
		（任意）削除したサービス フローのロギングをディセーブルにします。

	コマンドまたはアクション	目的

ステップ 6	**nocablemeteringsource-interface**
	
	例：
	`Router(config)# no cable metering source-interface`
	
	例：
	`Router(config)#`
		（任意）課金パケットで指定した送信元インターフェイスをディセーブルにします。

ステップ 7	**exit**
	
	例：
	`Router(config)# exit`
	
	例：
	`Router#`
		グローバル コンフィギュレーション モードを終了します。

従量制課金用に認定された SSL サーバの設定

Cisco IOS リリースでは、Cisco CMTS の従量制課金機能で使用されるセキュア ソケット レイヤ（SSL）サーバのサポートを導入しています。従量制課金では、DOCSIS サブスクライバ アカウント管理インターフェイス仕様（SAMIS）形式を実装します。

この新機能により、Cisco CMTS と収集サーバ間の SSL サーバを設定できます。SSL サーバおよび証明書をサポートするために、証明書の作成手順と **debug** コマンドが追加または強化されました。このセクションでは、一般的な手順について説明します。

「SSL 運用に対応する Cisco CMTS の設定」セクションも参照してください。

SSL サーバ証明書の生成

ここでは、セキュア ソケット レイヤ（SSL）サーバの証明書の作成と実装に関する一般的な手順について説明します。

1. CA キーを生成します。
2. ディレクトリとサブディレクトリを含めるように OpenSSL 環境をセットアップします。
3. ファイルを適切なディレクトリにコピーします。
4. SSL サーバ証明書の要求を生成します。
5. SSL サーバ証明書の要求を許可します。
6. SSL サーバ証明書を DER 形式に変換します。
7. SSL 証明書をブートフラッシュ メモリにコピーします（メモリへの書き込み）。

8 SSL サーバを起動します。

認定 SSL サーバ サポート用の Cisco CMTS の設定とテスト

Cisco ルータで SSL サーバおよび認定をサポートするように設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Router# configure terminal`	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	**ipdomainname** *domain* 例： `Router(config)# ip domain name Cisco.com`	Cisco IOS ソフトウェアが未修飾ホスト名（ドット付き 10 進ドメイン名を含まない名前）を作成するときに使用するデフォルトのドメイン名を定義します。ドメイン名を未修飾の名前から区切るために使用される最初のピリオドは入れないでください。 （注） DNS の詳細情報については、Cisco.com にある『Domain Name System (DNS)』のマニュアルを参照してください。
ステップ 4	**cryptokeygeneratersa** 例： `Router(config)# crypto key generate rsa`	RSA キー ペアを生成します。

ステップ 5	Ctrl-Z
	
	例：
	`Router(config)# Ctrl-Z`
	
	例：
	`Router#`
		特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**testcablereadcertificate** 例： `Router# test cable read certificate`	証明書が Cisco CMTS 上で有効で、運用されていることを確認します。
ステップ 7	**showcryptocacertificate** 例： `Router# show crypto ca certificate`	Cisco CMTS で利用可能な証明書を表示します。

ステップ 8	**configure terminal**
	
	例：
	
	`Router# configure terminal`
	
	例：
	
	`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 9	**cablemeteringdestination** *ip-addr num-1 num-2 num-3***secure** 例： `Router(config)# cable metering destination 1.7.7.7 6789 0 15 secure`	証明書で使用するケーブル計測用の宛先 IP アドレスを定義します。
ステップ 10	test cable metering 例： `Router# test cable metering`	サポート対象の SSL サーバおよび計測設定を考慮して、ケーブル計測をテストします。

従量制課金機能のモニタリング

最新の課金レコードを表示するには、**showcablemetering-status** コマンドを使用します。次の例では、課金レコードがローカルファイルシステムに書き込まれるように従量制課金を設定した場合の一般的な出力結果を示します。

```
CMTS01# show cable metering-status

destination                          complete-time   flow   cpe     status
                                                    aggr suppress
disk0:R7519-UBR7246-20000308-004428 Jun 12 09:33:05  No     No     success
CMTS01#
```

次の例では、課金レコードが外部サーバにストリーミングされるように従量制課金を設定した場合の **showcablemetering-status** コマンドの一般的な出力結果を示します。

```
Router# show cable metering-status

destination                       complete-time   flow cpe  full status
                                                  aggr supp rec
10.11.37.2 :1234                  Jun 12 09:33:05  No   No  No success
Router#
```

次の例では、冗長オプションを使用した **showcablemetering-status** コマンドの一般的な出力を示します。

```
Router# show cable metering-status verbose
Last export status
Destination : disk0:sunethra10k-20070129-190423
Complete Time : Jan29 19:04:38
Flow Aggregate : No
Full records : No
Cpe list suppression : No
Source interface : FastEthernet0/0/0
Status of last export : success
Current export status : In progress
```

次の例では、IPDRエクスポータを使用して課金レコードが外部サーバにストリーミングされるように従量制課金を設定した場合の **show cable metering-status** コマンドの一般的な出力結果を示します。

```
Router# show cable metering-status
destination                 complete-time   flow  cpe   full    status
              aggr  supp  rec
IPDR_Session2               Apr12 16:51:15  No    No    No    success
```

次の例では、IPDRエクスポータを使用して課金レコードが外部サーバにストリーミングされるように従量制課金を設定した場合の、冗長形式での **showcablemetering-status** コマンドの一般的な出力結果を示します。

```
Router# show cable metering-status
 verbose

Last export status
Destination                : IPDR_Session2
Complete Time          : Apr12 16:51:15
Flow Aggregate         : No
Full records               :No
Cpe list suppression   : No
Source interface       : Not defined
Status of last export  : success
```

（注） **showcablemetering-status** コマンドでストリーミング動作のステータスが「success」と表示されるのに、レコードが課金アプリケーション サーバに届いていない場合は、Cisco CMTS およびサーバが同一タイプの通信方式（非セキュア TCP またはセキュア SSL）に設定されていることを確認してください。Cisco CMTS で非セキュア TCP が設定されており、サーバでセキュア SSL が設定されている場合、Cisco CMTS による課金レコードの送信は正常に完了しますが、データがセキュア SSL ストリームで到着しないため、サーバはすべてのデータを破棄します。

ヒント **showcablemetering-status** コマンドにより、最新の課金レコードが削除されるまで、最新の課金レコード作業のステータスが表示され続けます。レコードを削除しないと、レコードは新しく作成されません。

IPDR エクスポータのステータスに関する情報を表示するには、show ipdr exporter コマンドを使用します。次に、一般的な出力例を示します。

```
Router#configure terminal
Router#show ipdr exporter
```

IPDR エクスポータが開始されます。

従量制課金の設定例

ここには、従量制課金機能の設定例を示します。

ファイル モード設定（Secure Copy 付き）

コンフィギュレーションファイルからの次の抜粋では、ファイルモードで動作し、ファイル転送で Secure Copy（SCP）を有効にした場合の、従量制課金機能の一般的な設定を示します。

```
!
cable metering filesystem disk1:
snmp-server enable traps cable metering
...
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
username billingapp level 15 password 7 billing-password
ip ssh time-out 120
ip ssh authentication-retries 3
ip scp server enable
```

非セキュアなストリーミング モード設定

コンフィギュレーションファイルからの次の抜粋では、ストリーミングモードで動作し、プライマリとセカンダリの両方の外部サーバを指定した場合の、従量制課金機能の一般的な設定を示します。データは、暗号化されずに標準 TCP パケットを使用して送信されます。

```
cable metering destination 10.10.10.171 5321 10.10.10.173 5321 2 30 non-secure
snmp-server enable traps cable metering
```

コンフィギュレーションファイルからの次の抜粋では、ストリーミングモードで動作し、プライマリ外部サーバのみを指定した場合の、従量制課金機能の一般的な設定を示します。

```
cable metering destination 10.10.11.181 6789 2 30 non-secure
snmp-server enable traps cable metering
```

（注） 課金アプリケーション サーバに標準 TCP 通信が設定されていることを確認する必要があります。Cisco CMTS に標準 TCP が設定されている場合に課金アプリケーション サーバに SSL 通信を設定すると、Cisco CMTS はサーバに課金レコードを送信できますが、レコードがセキュアなストリーミングで届かないため、サーバはその情報すべてを廃棄します。

セキュアなストリーミング モード設定

コンフィギュレーションファイルからの次の抜粋では、ストリーミングモードで動作し、プライマリ外部サーバのみを指定した場合の、従量制課金機能の一般的な設定を示します。セキュア ソケット レイヤ（SSL）TCP 接続は、デジタル証明書を設定する必要のあるデータを送信するために使用されます。

```
cable metering destination 10.10.11.181 6789 2 30 secure cpe-list-suppress
snmp-server enable traps cable metering
...
crypto ca trustpoint SSL-CERT
!
crypto ca certificate chain SSL-CERT
 certificate ca 00
  308204A6 3082038E A0030201 02020100 300D0609 2A864886 F70D0101 04050030
  8198310B 30090603 55040613 02555331 13301106 03550408 130A4361 6C69666F
  726E6961 3111300F 06035504 07130853 616E204A 6F736531 1C301A06 0355040A
  13134369 73636F20 53797374 656D732C 20496E63 2E311130 0F060355 040B1308
  4361626C 65204255 310E300C 06035504 03130553 65656D61 3120301E 06092A86
...
  3E65DBBA 337627E8 589980D6 C8836C7E 3D3C3BC1 F21973BF 7B287D7A 13B16DA2
  02B2B180 C2A125C7 368BDA4C 0B8C81B7 7D5BEFF9 A6618140 1E95D19E BD0A84F5
  B43702AB 39B5E632 87BA36AC A3A8A827 C5BAC0F1 B24B8F4D 55615C49 5B6E4B61
  B15CC48A 8EF566C8 6E449B49 BF8E9165 317C1734 9A48A240 78A356B5 403E9E9B
  88A51F5B 0FE38CC2 F431
  quit
!
```

（注） 課金アプリケーション サーバにもSSL通信が設定されていることを確認する必要があります。

第 97 章

Cisco CMTS ルータの周波数割り当て情報

Cisco CMTS ルータの周波数割り当て

次の表に、NTSC 6 MHz チャネル帯域に関する情報を示します。

表 *250*：*NTSC CATV* のチャネルおよび関連周波数（*MHz*）

チャネル番号	帯域幅	ビデオ キャリア	カラー キャリア	音声キャリア
T 7	5.75 ～ 11.75	7	10.58	11.5
T 8	11.75 ～ 17.75	13	16.58	17.5
T9	17.75 ～ 23.75	19	22.58	23.5
T10	23.75 ～ 29.75	25	28.58	29.5
T11	29.75 ～ 35.75	31	34.58	35.5
T12	35.75 ～ 41.75	37	40.58	41.5
T13	41.75 ～ 47.75	43	46.58	47.5
TV-IF	40.0 ～ 46.0	45.75	42.17	41.25
2-2	54.0 ～ 60.0	55.25	58.83	59.75
3-3	60.0 ～ 66.0	61.25	64.83	65.75
4-4	66.0 ～ 72.0	67.25	70.83	71.75

チャネル番号	帯域幅	ビデオ キャリア	カラー キャリア	音声キャリア
5-5	76.0 ～ 82.0	77.25	80.83	81.75
6-6	82.0 ～ 88.0	83.25	86.83	87.75
FM	88.0 ～ 108.0			
A-5-95	90.0 ～ 96.0	91.25	94.83	95.75
A-4-96	96.0 ～ 102.0	97.25	100.83	101.75
A-3-97	102.0 ～ 108.0	103.25	106.83	107.75
A-2-98	108.0 ～ 114.0	109.25	112.83	113.75
A-1-99	114.0 ～ 120.0	115.25	118.83	119.75
A-14	120.0 ～ 126.0	121.25	124.83	125.75
B-15	126.0 ～ 132.0	127.25	130.83	131.75
C-16	132.0 ～ 138.0	133.25	136.83	137.75
D-17	138.0 ～ 144.0	139.25	142.83	143.75
E-18	144.0 ～ 150.0	145.25	148.83	149.75
F-19	150.0 ～ 156.0	151.25	154.83	155.75
G-20	156.0 ～ 162.0	157.25	160.83	161.75
H-21	162.0 ～ 168.0	163.25	166.83	167.75
I-22	168.0 ～ 174.0	169.25	172.83	173.75
7-7	174.0 ～ 180.0	175.25	178.83	179.75
8-8	180.0 ～ 186.0	181.25	184.83	185.75
9-9	186.0 ～ 192.0	187.25	190.83	191.75
10-10	192.0 ～ 198.0	193.25	196.83	197.75
11-11	198.0 ～ 204.0	199.25	202.83	203.75
12-12	204.0 ～ 210.0	205.25	208.83	209.75

チャネル番号	帯域幅	ビデオ キャリア	カラー キャリア	音声キャリア
13-13	210.0 ～ 216.0	211.25	214.83	215.75
J-23	216.0 ～ 222.0	217.25	220.83	221.75
K-24	222.0 ～ 228.0	223.25	226.83	227.75
L-25	228.0 ～ 234.0	229.25	232.83	233.75
M-26	234.0 ～ 240.0	235.25	238.83	239.75
N-27	240.0 ～ 246.0	241.25	244.83	245.75
O-28	246.0 ～ 252.0	247.25	250.83	251.75
P-29	252.0 ～ 258.0	253.25	256.83	257.75
Q-30	258.0 ～ 264.0	259.25	262.83	263.75
R-31	264.0 ～ 270.0	265.25	268.83	269.75
S-32	270.0 ～ 276.0	271.25	274.83	275.75
T-33	276.0 ～ 282.0	277.25	280.83	281.75
U-34	282.0 ～ 288.0	283.25	286.83	287.75
V-35	288.0 ～ 294.0	289.25	292.83	293.75
W-36	294.0 ～ 300.0	295.25	298.83	299.75
AA-37	300.0 ～ 306.0	301.25	304.83	305.75
BB-38	306.0 ～ 312.0	307.25	310.83	311.75
CC-39	312.0 ～ 318.0	313.25	316.83	317.75
DD-40	318.0 ～ 324.0	319.25	322.83	323.75
EE-41	324.0 ～ 330.0	325.25	328.83	329.75
FF-42	330.0 ～ 336.0	331.25	334.83	335.75
GG-43	336.0 ～ 342.0	337.25	340.83	341.75
HH-44	342.0 ～ 348.0	343.25	346.83	347.75

チャネル番号	帯域幅	ビデオ キャリア	カラー キャリア	音声キャリア
II-45	348.0 ～ 354.0	349.25	352.83	353.75
JJ-46	354.0 ～ 360.0	355.25	358.83	359.75
KK-47	360.0 ～ 366.0	361.25	364.83	365.75
LL-48	366.0 ～ 372.0	367.25	370.83	371.75
MM-49	372.0 ～ 378.0	373.25	376.83	377.75
NN-50	378.0 ～ 384.0	379.25	382.83	383.75
OO-51	384.0 ～ 390.0	385.25	388.83	389.75
PP-52	390.0 ～ 396.0	391.25	394.83	395.75
QQ-53	396.0 ～ 402.0	397.25	400.83	401.75
RR-54	402.0 ～ 408.0	403.25	406.83	407.75
SS-55	408.0 ～ 414.0	409.25	412.83	413.75
TT-56	414.0 ～ 420.0	415.25	418.83	419.75
UU-57	420.0 ～ 426.0	421.25	424.83	425.75
VV-58	426.0 ～ 432.0	427.25	430.83	431.75
WW-59	432.0 ～ 438.0	433.25	436.83	437.75
XX-60	438.0 ～ 444.0	439.25	442.83	443.75
YY-61	444.0 ～ 450.0	445.25	448.83	449.75
ZZ-62	450.0 ～ 456.0	451.25	454.83	455.75
AAA-63	456.0 ～ 462.0	457.25	460.83	461.75
BBB-64	462.0 ～ 468.0	463.25	466.83	467.75
CCC-65	468.0 ～ 474.0	469.25	472.83	473.75
DDD-66	474.0 ～ 480.0	475.25	478.83	479.75
EEE-67	480.0 ～ 486.0	481.25	484.83	485.75

チャネル番号	帯域幅	ビデオ キャリア	カラー キャリア	音声キャリア
FFF-68	486.0 ～ 492.0	487.25	490.83	491.75
GGG-69	492.0 ～ 498.0	493.25	496.83	497.75
HHH-70	498.0 ～ 504.0	499.25	502.83	503.75
III-71	504.0 ～ 510.0	505.25	508.83	509.75
JJJ-72	510.0 ～ 516.0	511.25	514.83	515.75
KKK-73	516.0 ～ 522.0	517.25	520.83	521.75
LLL-74	522.0 ～ 528.0	523.25	526.83	527.75
MMM-75	528.0 ～ 534.0	529.25	532.83	533.75
NNN-76	534.0 ～ 540.0	535.25	538.83	539.75
OOO-77	540.0 ～ 546.0	541.25	544.83	545.75
PPP-78	546.0 ～ 552.0	547.25	550.83	551.75
QQQ-79	552.0 ～ 558.0	553.25	556.83	557.75
RRR-80	558.0 ～ 564.0	559.25	562.83	563.75
SSS-81	564.0 ～ 570.0	565.25	568.83	569.75
TTT-82	570.0 ～ 576.0	571.25	574.83	575.75
UUU-83	576.0 ～ 582.0	577.25	580.83	581.75
VVV-84	582.0 ～ 588.0	583.25	586.83	587.75
WWW-85	588.0 ～ 594.0	589.25	592.83	593.75
XXX86	594.0 ～ 600.0	595.25	598.83	599.75
YYY-87	600.0 ～ 606.0	601.25	604.83	605.75
ZZZ-88	606.0 ～ 612.0	607.25	610.83	611.75
89-89	612.0 ～ 618.0	613.25	616.83	617.75
90-90	618.0 ～ 624.0	619.25	622.83	623.75

チャネル番号	帯域幅	ビデオ キャリア	カラー キャリア	音声キャリア
91-91	624.0 ～ 630.0	625.25	628.83	629.75
92-92	630.0 ～ 636.0	631.25	634.83	635.75
93-93	636.0 ～ 642.0	637.25	640.83	641.75
94-94	642.0 ～ 648.0	643.25	646.83	647.75
100-100	648.0 ～ 654.0	649.25	652.83	653.75
101-101	654.0 ～ 660.0	655.25	658.83	659.75
102-102	660.0 ～ 666.0	661.25	664.83	665.75
103-103	666.0 ～ 672.0	667.25	670.83	671.75
104-104	672.0 ～ 678.0	673.25	676.83	677.75
105-105	678.0 ～ 684.0	679.25	682.83	683.75
106-106	684.0 ～ 690.0	685.25	688.83	689.75
107-107	690.0 ～ 696.0	691.25	694.83	695.75
108-108	696.0 ～ 702.0	697.25	700.83	701.75
109-109	702.0 ～ 708.0	703.25	706.83	707.75
110-110	708.0 ～ 714.0	709.25	712.83	713.75
111-111	714.0 ～ 720.0	715.25	718.83	719.75
112-112	720.0 ～ 726.0	721.25	724.83	725.75
113-113	726.0 ～ 732.0	727.25	730.83	731.75
114-114	732.0 ～ 738.0	733.25	736.83	737.75
115-115	738.0 ～ 744.0	739.25	742.83	743.75
116-116	744.0 ～ 750.0	745.25	748.83	749.75
117-117	750.0 ～ 756.0	751.25	754.83	755.75
118-118	756.0 ～ 762.0	757.25	760.83	761.75

チャネル番号	帯域幅	ビデオ キャリア	カラー キャリア	音声キャリア
119-119	762.0 ～ 768.0	763.25	766.83	767.75
120-120	768.0 ～ 674.0	769.25	772.83	773.75
121-121	774.0 ～ 780.0	775.25	778.83	779.75
122-122	780.0 ～ 786.0	781.25	784.83	785.75
123-123	786.0 ～ 792.0	787.25	790.83	791.75
124-124	792.0 ～ 798.0	793.25	796.83	797.75
125-125	798.0 ～ 804.0	799.25	802.83	803.75
126-126	804.0 ～ 810.0	805.25	808.83	809.75
127-127	810.0 ～ 816.0	811.25	814.83	815.75
128-128	816.0 ～ 822.0	817.25	820.83	821.75
129-129	822.0 ～ 828.0	823.25	826.83	827.75
130-130	828.0 ～ 834.0	829.25	832.83	833.75
131-131	834.0 ～ 840.0	835.25	838.83	839.75
132-132	840.0 ～ 846.0	841.25	844.83	845.75
133-133	846.0 ～ 852.0	847.25	850.83	851.75
134-134	852.0 ～ 858.0	853.25	856.83	857.75
135-135	858.0 ～ 864.0	859.25	862.83	863.75
136-136	864.0 ～ 870.0	865.25	868.83	869.75
137-137	870.0 ～ 876.0	871.25	874.83	875.75
138-138	876.0 ～ 882.0	877.25	880.83	881.75
139-139	882.0 ～ 888.0	883.25	886.83	887.75
140-140	888.0 ～ 894.0	889.25	892.83	893.75
141-141	894.0 ～ 900.0	895.25	898.83	899.75

チャネル番号	帯域幅	ビデオ キャリア	カラー キャリア	音声キャリア
142-142	900.0 ～ 906.0	901.25	904.83	905.75
143-143	906.0 ～ 912.0	907.25	910.83	911.75
144-144	912.0 ～ 918.0	913.25	916.83	917.75
145-145	918.0 ～ 924.0	919.25	922.83	923.75
146-146	924.0 ～ 930.0	925.25	928.83	929.75
147-147	930.0 ～ 936.0	931.25	934.83	935.75
148-148	936.0 ～ 942.0	937.25	940.83	941.75
149-149	942.0 ～ 948.0	943.25	946.83	947.75
150-150	948.0 ～ 954.0	949.25	952.83	953.75
151-151	954.0 ～ 960.0	955.25	958.83	959.75
152-152	960.0 ～ 966.0	961.25	964.83	965.75
153-153	966.0 ～ 972.0	967.25	970.83	971.75
154-154	972.0 ～ 978.0	973.25	976.83	977.75
155-155	978.0 ～ 984.0	979.25	982.83	983.75
156-156	984.0 ～ 990.0	985.25	988.83	989.75
157-157	990.0 ～ 996.0	991.25	994.83	995.75
158-158	996.0 ～ 1002.0	997.25	1000.83	1001.75

次の表に、位相反転線（PAL）および Systeme Electronique Couleur Avec Memoire（SECAM）の 8 MHz チャネル帯域について示します。

表 *251*：欧州 *CATV* のチャネルおよび関連周波数（*MHz*）

チャネル番号	帯域幅	ビデオ キャリア	音声キャリア
2	47 ～ 54	48.25	48.25
3	54 ～ 61	55.25	55.25

チャネル番号	帯域幅	ビデオ キャリア	音声キャリア
4	61 ～ 68	62.25	62.25
S2	111 ～ 118	112.25	112.25
S3	118 ～ 125	119.25	119.25
S4	125 ～ 132	126.25	126.25
S5	132 ～ 139	133.25	133.25
S6	139 ～ 146	140.25	140.25
S7	146 ～ 153	147.25	147.25
S8	153 ～ 160	154.25	154.25
S9	160 ～ 167	161.25	161.25
S10	167 ～ 174	168.25	168.25
5	174 ～ 181	175.25	175.25
6	181 ～ 188	182.25	182.25
7	188 ～ 195	189.25	189.25
8	195 ～ 202	196.25	196.25
9	202 ～ 209	203.25	203.25
10	209 ～ 216	210.25	210.25
11	216 ～ 223	217.25	217.25
12	223 ～ 230	224.25	224.25
S11	230 ～ 237	231.25	231.25
S12	237 ～ 244	238.25	238.25
S13	244-251	245.25	245.25
S14	251 ～ 258	252.25	252.25
S15	258 ～ 265	259.25	259.25

チャネル番号	帯域幅	ビデオ キャリア	音声キャリア
S16	265 ～ 272	266.25	266.25
S17	272 ～ 279	273.25	273.25
S18	279 ～ 286	280.25	280.25
S19	286 ～ 293	287.25	287.25
S20	293 ～ 300	294.25	294.25
S21	302 ～ 310	303.25	303.25
S22	310 ～ 318	311.25	311.25
S23	318 ～ 326	319.25	319.25
S24	326 ～ 334	327.25	327.25
S25	334 ～ 342	335.25	335.25
S26	342 ～ 350	343.25	343.25
S27	350 ～ 358	351.25	351.25
S28	358 ～ 366	359.25	359.25
S29	366 ～ 374	367.25	367.25
S30	374 ～ 382	375.25	375.25
S31	382 ～ 390	383.25	383.25
S32	390 ～ 398	391.25	391.25
S33	398 ～ 406	399.25	399.25
S34	406 ～ 414	407.25	407.25
S35	414 ～ 422	415.25	415.25
S36	422 ～ 430	423.25	423.25
S37	430 ～ 438	431.25	431.25
S38	438 ～ 446	439.25	439.25

チャネル番号	帯域幅	ビデオ キャリア	音声キャリア
21	470 ～ 478	471.25	471.25
22	478 ～ 486	479.25	479.25
23	486 ～ 494	487.25	487.25
24	494 ～ 502	495.25	495.25
25	502 ～ 510	503.25	503.25
26	510 ～ 518	511.25	511.25
27	518 ～ 526	519.25	519.25
28	526 ～ 534	527.25	527.25
29	534 ～ 542	535.25	535.25
30	542 ～ 550	543.25	543.25
31	550 ～ 558	551.25	551.25
32	558 ～ 566	559.25	559.25
33	566 ～ 574	567.25	567.25
34	574 ～ 582	575.25	575.25
35	582 ～ 590	583.25	583.25
36	590 ～ 598	591.25	591.25
37	598 ～ 606	599.25	599.25
38	606 ～ 614	607.25	607.25
39	614 ～ 622	615.25	615.25
40	622 ～ 630	623.25	623.25
41	630 ～ 638	631.25	631.25
42	638 ～ 646	639.25	639.25
43	646 ～ 654	647.25	647.25

チャネル番号	帯域幅	ビデオ キャリア	音声キャリア
44	654 ～ 662	655.25	655.25
45	662 ～ 670	663.25	663.25
46	670 ～ 678	671.25	671.25
47	678 ～ 686	679.25	679.25
48	686 ～ 694	687.25	687.25
49	694 ～ 702	695.25	695.25
50	702 ～ 710	703.25	703.25
51	710 ～ 718	711.25	711.25
52	718 ～ 726	719.25	719.25
53	726 ～ 734	727.25	727.25
54	734 ～ 742	735.25	735.25
55	742 ～ 750	743.25	743.25
56	750 ～ 758	751.25	751.25
57	758 ～ 766	759.25	759.25
58	766 ～ 774	767.25	767.25
59	774 ～ 782	775.25	775.25
60	782 ～ 790	783.25	783.25
61	790 ～ 798	791.25	791.25
62	798 ～ 806	799.25	799.25
63	806 ～ 814	807.25	807.25
64	814 ～ 822	815.25	815.25
65	822 ～ 830	823.25	823.25
66	830 ～ 838	831.25	831.25

チャネル番号	帯域幅	ビデオ キャリア	音声キャリア
67	838 ～ 846	839.25	839.25
68	846 ～ 854	847.25	847.25
69	854 ～ 862	855.25	855.25

第 98 章

フラップ リストのトラブルシューティング

このマニュアルでは、Cisco ケーブル モデム終端システム（CMTS）ルータのフラップ リストのトラブルシューティング機能を設定および使用する方法について説明します。フラップ リストは、Cisco CMTS ルータで特定のケーブル モデムや特定のケーブル インターフェイスの潜在的な問題を診断するための特許取得済みツールです。フラップ リストは、「フラップする」ケーブル モデム（断続的な接続問題を抱えたケーブル モデム）を追跡します。過剰にフラップする場合、特定のケーブル モデムまたはケーブル設備のアップストリームまたはダウンストリーム部分に問題がある可能性があります。

機能情報の確認

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載され

ている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *252*：*Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

フラップ リスト トラブルシューティングの前提条件

- SNMP コマンドを使用してフラップ リストを設定してアクセスするには、SNMPv3 マネージャを使用し、SNMP 動作用に Cisco CMTS ルータが設定されていることが必要です。

フラップ リスト トラブルシューティングの制約事項

- フラップ リスト トラブルシューティング機能は、双方向ケーブル モデムでのみ使用できます。フラップ リストは Telco リターン ケーブル モデムまたはセットトップ ボックスをサポートしません。

（注） ケーブル フラップ リストが最初に開発されて以来、ポーリング メカニズムが拡張され、ポーリング失敗時にレートが 1/秒に引き上げられるようになりました。ケーブル モデムは周波数ホップ期間より早くオフラインになるので、ケーブル モデムがオフラインになっても周波数は固定されたままになる可能性があります。これを補正するには、ホップ間隔を 10 秒まで引き下げます。

フラップ リストのトラブルシューティングに関する情報

ここでは、フラップ リストのトラブルシューティング機能に関する次の情報について説明します。

機能の概要

フラップ リストのトラブルシューティングは、Cisco ケーブル モデム終端システム（CMTS）ルータの Cisco IOS ソフトウェアに組み込まれている特許取得済みツールです。フラップ リストは、「フラッピング」ケーブル モデムを追跡します。これは、断続的に接続の問題があるケーブル モデムです。フラッピング ケーブル モデムは、そのケーブル モデムに問題があるか、またはケーブル設備のアップストリームまたはダウンストリーム部分に RF ノイズの問題があることを示している可能性があります。

フラップ リスト機能は、ケーブル モデムをポーリングしたりケーブル モデムから特別な情報を要求したりするための特別なメッセージングを使用するため、Data-over-Cable Service Interface Specifications（DOCSIS）に準拠したケーブル モデムをサポートします。代わりに、この機能は DOCSIS ケーブル ネットワーク上ですでに実行された通常の登録およびステーション メンテナンス アクティビティをモニタします。

これにより、Cisco CMTS はパケット オーバーヘッドをさらに発生させたりネットワーク スループットやパフォーマンスに影響を与えたりすることなくフラップリストデータを収集できます。これはつまり、フラップ リストのトラブルシューティング機能は Cisco CMTS ルータの独自の機能であっても、すべての DOCSIS 準拠ケーブル モデムと互換性があることも意味します。また、

シンプル ネットワーク管理プロトコル（SNMP）を使用するその他のモニタリング方法とは異なり、フラップ リストが使用する帯域幅はゼロです。

フラップ リストに関する情報

フラップ リスト トラブルシューティング機能は次の状況を追跡します。

- 再挿入：ユーザが指定した挿入時間よりも頻繁にケーブル モデムの再登録が行われると、再挿入が発生します。再挿入のパターンは、ダウンストリームに潜在的な問題があること、またはケーブル モデムのプロビジョニングが不適切であることを示す場合があります。
- ヒットおよびミス：Cisco CMTS が DOCSIS 規格に準拠して送信するステーション メンテナンス メッセージ（MAC レイヤ「キープアライブ」メッセージ）に対して、ケーブル モデムが正しく応答すると、「ヒット」が発生します。ユーザが指定したタイムアウト期間内にケーブル モデムが要求に応答しない場合、「ミス」が発生します。ミスのパターンは、ダウンストリームまたはアップストリームの経路に潜在的な問題があること、または登録プロセスで問題が起きている可能性があることを示す場合があります。
- 出力調整：DOCSIS ケーブル モデムは、最大許容出力レベルの範囲内で、アップストリームの送信出力レベルを調整することによって、ケーブル設備の不安定な信号レベルを調整することができます。出力調整が繰り返される場合は通常、アップストリームの復路の増幅器に問題があります。

フラップ リスト機能は自動的にイネーブルになりますが、フラップ リストを効果的に利用するには通常、ケーブル システム管理者側で次の作業が必要です。

- フラップ リストを定期的（15 分間隔など）にポーリングするためのスクリプトを設定します。
- 生成されたデータを検査してトレンド分析を実施し、フラップ リストに継続して存在するケーブル モデムを特定します。
- ケーブル モデムの MAC アドレスを住所に変換するために課金および管理データベースに照会し、レポートを作成します。このレポートは、カスタマー サービス部門またはケーブル設備の運用保守部門に提出されます。保守担当者は、これらのレポートを使用して、フラッピング ケーブル モデムの特性パターン、住所、フラップ統計情報を把握し、障害のある増幅器またはフィーダ回線を迅速に特定できます。また、これらのレポートから、問題がダウンストリームの経路またはアップストリームの経路のどちらにあるのか、イングレス ノイズまたは機器のどちらに関係する問題なのかを素早く判別することができます。

フラップ リストにより、可能性のある一連の問題を短時間で診断する手軽な手段が得られます。たとえば、加入者から問題が伝えられても、サービスを提供しているケーブル インターフェイスのフラップ リストに、フラップ リスト アクティビティがまったく、またはほとんど示されていない場合、ケーブル技術者はCisco CMTS とケーブル設備間の通信に問題はないと推測できます。したがって、問題は加入者側のコンピュータ機器またはケーブル モデムとのローカル接続にあると考えられます。

ケーブル技術者はさらに、再挿入、ヒット/ミス、および出力調整のパターンから、次のタイプの問題を手早く突き止めることもできます。

- 加入者のケーブル モデムが多数のフラップ リスト アクティビティを示している場合は、通信にある種の問題があります。ケーブルモデムのハードウェアに障害が発生しているか、インストレーションに問題があるか、使用している同軸ケーブルに問題があるか、あるいはこのケーブル モデムを処理するケーブル設備のある部分に問題があるかのいずれかです。
- フラップ リストで最もアクティブな上位 10 パーセントのケーブル モデムに焦点を当てます。これは、ヘッドエンドとの通信を中断させ続ける、広範囲にわたる一貫したプラントまたは装置の問題を示す場合が多いためです。
- 1 日に 50 回以上の出力調整を行っているケーブル モデムは、アップストリームの経路に問題があると考えられます。
- ヒットとミスがほぼ同数で、多数の挿入が行われているケーブルモデムは、ダウンストリームの経路に問題があると考えられます（ケーブル モデムへの送信レベル不足など）。
- すべてのケーブル モデムで同時に挿入が増えている場合、プロビジョニング サーバの障害が考えられます。
- 巡回冗長検査（CRC）エラーが多いケーブルモデムは、アップストリームに不良経路があるか、または屋内の配線に問題があります。
- アップストリームの同じ物理ポート上にある、類似のフラップリスト統計情報を持つケーブルモデムを比較することによって、プラント外部の問題を特定のノードまたは地域にただちに限定することができます。

さらに、ケーブルネットワークの管理者は、フラップリストを使用することによって、品質管理とアップストリームのパフォーマンスに関するデータを収集できます。ネットワーク オペレーション センター（NOC）は通常、フラップ リストをローカル コンピュータのデータベースに毎日保存し、アップストリームのパフォーマンスと導入先の品質管理を追跡したレポート、およびケーブル設備の問題の傾向を分析したレポートを作成できるようにしています。

ヒント システムは、自動出力調整をサポートしています。show cable flap-list コマンドおよび show cable modem コマンドにより、ヘッドエンドのケーブル ルータがいつ、特定のモデムの不安定なリターン パスを検出し、出力調整によって補正したかが表示されます。出力調整が行われた場合は、モデムに対応する出力調整フィールドにアスタリスク（*）が表示されます。モデムの送信出力レベルが最大値に達して、それ以上は出力レベルを上げることができない場合は、感嘆符（!）が表示されます。

Cisco Cable Manager および Cisco Broadband Troubleshooter

フラップ リストのトラブルシューティング機能は、Cisco Cable Manager（CCM）リリース 2.0 以降でサポートされます。CCM は、ルータと DOCSIS 準拠ケーブル モデムの管理、パフォーマンス レポートの生成、接続の問題のトラブルシューティング、ネットワークのグラフィカル表示、DOCSIS コンフィギュレーション ファイルの編集を実行する、UNIX ベースのソフトウェア スイートです。CCM には CCM サーバ コンソールからローカルで、または UNIX ワークステーションや PC からリモートでアクセスできます。

フラップ リストのトラブルシューティング機能は、Cisco Broadband Troubleshooter（CBT）とも連携します。CBT は、光同軸ハイブリッド（HFC）ネットワークの問題を管理および診断する、グラフィカル ベースのアプリケーションです。無線周波数（RF）の技術者は、設備とプロビジョニングの問題を切り分け、フラッピング モデムの分析を含むアップストリームおよびダウンストリームの問題パターンの特徴を把握することが迅速にできます。

利点

フラップ リストのトラブルシューティング機能は、HFC ネットワークにおける問題を管理およびトラブルシューティングする予防的な方法です。パッシブ モニタリングを使用すると、特殊なメッセージをケーブル モデムに送信する手法や、シンプル ネットワーク管理プロトコル（SNMP）コマンドを使用してケーブル モデムを定期的にポーリングする手法よりスケーラブルで効率的です。DOCSIS ネットワークにすでに存在するメカニズムを使用するため、任意の DOCSIS 認定ケーブル モデムまたはセットトップ ボックスで使用できます。

ケーブル技術者はフラップ リストを使用して、ケーブル ヘルス統計情報をリアルタイムと履歴の両方で得られるため、問題の切り分けやネットワークの診断を迅速かつ正確に実施できます。フラップ リストを使用して、ケーブル技術者は次の作業を実行できます。

- 光同軸ハイブリッド（HFC）ネットワークにおけるトラブル パターンの特徴を把握する方法をすばやく理解します。
- 不良な増幅器または分配線を調べます。
- アップストリーム パスの問題とダウンストリーム パスの問題を区別します。
- イングレス ノイズの問題を設備機器の問題から分離します。

フラップ リストのトラブルシューティングの設定方法

ここでは、Cisco CMTS でフラップ リスト動作を設定する方法について説明します。コマンドライン インターフェイス（CLI）コマンドまたはシンプル ネットワーク管理プロトコル（SNMP）コマンドを使用して、フラップ リストを設定するか、ケーブル モデムをリストから削除するか、フラップ リスト カウンタをクリアすることができます。

CLI を使用したフラップ リストの動作設定（任意）

フラップ リストの動作を設定するには、まず EXEC モードで次の手順を実行します。フラップ リストのデフォルト値の変更が必要な場合を除き、これらの手順は任意です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cableflap-listinsertion-time** *seconds* 例： `Router(config)# cable flap-list insertion-time 3600`	（任意）インサート（登録）の最小時間間隔を秒で指定します。この間隔よりも頻繁に登録要求を行うケーブル モデムはフラップ リストに追加されます。
ステップ 4	**cableflap-listpower-adjustthreshold** *db* 例： `Router(config)# cable flap-list power-adjust threshold 5`	（任意）フラップ リスト イベントを形成する最小出力調整を dB で指定します。 （注） しきい値が 2 dB 未満の場合は、多数のフラップ リスト イベントが記録される可能性があります。デフォルト値からこのパラメータを変更する必要がある場合は、3 dB 以上に設定することを推奨します。
ステップ 5	**cableflap-listmiss-threshold** *misses* 例： `Router(config)# cable flap-list miss-threshold 10`	（任意）CMTS がケーブル モデムをフラップ リストに追加する前に連続してミスできる MAC レイヤ ステーション メンテナンス（キープアライブ）メッセージ数を指定します。 （注） ミスの回数が多い場合は、アップストリームの間欠的な問題、光ファイバ レーザー クリッピング、または共通パスのひずみなどの設備の問題が起きている可能性があります。
ステップ 6	**cableflap-listaging** *minutes* 例： `Router(config)# cable flap-list aging 20160`	（任意）Cisco CMTS がケーブル モデムの情報をフラップ リストに保持する期間を分数で指定します。

	コマンドまたはアクション	目的
ステップ 7	**cableflap-listsize** *number* 例： `Router(config)# cable flap-list size 4000`	フラップ リスト内に保持可能なケーブル モデムの最大数を指定します。 ヒント　プロセッサ メモリを浪費しないようにするために、Cisco CMTS が処理する実際のケーブル モデム数を超える値を設定しないでください。
ステップ 8	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

CLI を使用したフラップ リストとカウンタのクリア（任意）

フラップ リストから 1 つ以上のケーブル モデムを削除するには、または（フラップ リスト内にモデムを維持した状態で）1 つ以上のケーブル モデムのフラップ リスト カウンタをクリアするには、次の手順に従って EXEC モードで実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

ステップ 2	**clearcableflap-list** *mac-addr* | **all**} [**save-counters**]
	
	例：
	`Router# clear cable flap-list 0102.0304.0506 save-counters`
	
	例：
	`Router# clear cable flap-list 000C.0102.0304`
		フラップ リストから 1 つまたはすべてのケーブル モデムを削除します。

	コマンドまたはアクション	目的

ステップ 3	**clearcablemodem** {*mac-addr* | *ip-addr* | [**cable** *interface*]**all** | **oui***string* | **reject**} } **counters**
	
	例：
	`Router# clear cable modem 172.12.23.45 counters`
	
	例：
	`Router# clear cable modem oui Cisco counters`
	
	例：
	`Router# clear cable modem reject counters`
	
	例：
	`Router# clear cable modem c4/0 counters`
	
	例：
		1 つ以上の CM のフラップ リスト カウンタをゼロに設定します。

CLI を使用した電力調整の有効化または無効化（任意）

Cisco CMTS は、ケーブル モデムの電力調整を自動的にモニタし、特定のケーブル モデムに電力調整法が必要かどうかを決定します。ケーブル インターフェイスで自動電力調整を実行し、その調整に対して周波数しきい値を設定するには、まず EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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。

	コマンドまたはアクション	目的
ステップ 3	**interfacecable** *x/y* 例： `Router(config)# interface cable 4/0`	指定したケーブルインターフェイスに対してケーブルインターフェイス コンフィギュレーション モードを開始します。

ステップ 4	**cableupstream** *n* **power-adjust** {**continue** *pwr-level* | **noise** *perc-pwr-adj* | **threshold value**}
	
	例：
	
	`Router(config-if)# cable upstream 0 power-adjust threshold 2`
	
	例：
	
	`Router(config-if)# cable upstream 0 power-adjust noise 50`
		このケーブルインターフェイスのアップストリーム ポートで自動電力調整をイネーブルにします。
		
		（注） ケーブル インターフェイスの各アップストリーム ポートで 4 を繰り返します。

ステップ 5	**cableupstream** *n* **freq-adjaveraging** *percent* 例： `Router(config-if)# cable upstream 0 freq-adj averaging 50`	通常の電力調整法から自動電力調整法に調整法を変更するには、周波数調整パケットの割合を指定します。
ステップ 6	**exit** 例： `Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 7	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

次の作業

注意 システム運用に適切なのはデフォルト設定です。振幅の平均化は自動的に行われます。通常、値の調整は推奨していません。ただし、フラッピング ケーブル モデムがある場合は、ケーブル設備のクリーンアップを推奨します。

（注） 状況によっては、**cableupstreampower-adjust** コマンドの特定の値を調整できる場合があります。CM が最大電力レベルに到達したためレンジングを完了できない場合は、デフォルトの 2 dB よりも大きな値に **continue** *pwr-level* パラメータを増やします。ケーブル インターフェイス ライン カードの「C」バージョンでは 10 dB を超える値、または FPGA バージョンでは 5 dB を超える値を推奨していません。多くの電力調整が行われた CM がフラップ リストに表示されているのに、CM が「noisy」と検出されない場合は、**noise** *perc-pwr-adj* 値を減らします。あまりにも多くの CM が不必要に「noisy」と検出される場合は、割合を上げます。

SNMP を使用したフラップ リストの動作設定（任意）

SNMP を使用して Cisco CMTS でフラップ リスト トラブルシューティング機能を設定するには、CISCO-CABLE-SPECTRUM-MIB で適切な cssFlapObjects 属性を設定します。次の表では、設定可能な各属性を説明します。

表 *253*：フラップ リスト設定の属性

属性	タイプ	範囲	説明
ccsFlapListMaxSize	Integer32	1 ～ 65536[12]	フラップ リストが 1 つのライン カードでサポートできるモデムの最大数。デフォルト値は 100 です。[13]
ccsFlapListCurrentSize	Integer32	1 ～ 65536	フラップ リスト内の現在のモデム数。[14]
ccsFlapAging	Integer32	1 ～ 86400	フラップ エントリのエージングしきい値（分）。デフォルトは 10080 分（180 時間すなわち 7 日）です。

属性	タイプ	範囲	説明
ccsFlapInsertionTime	Integer32	60 ～ 86400	最悪の場合のインサート時間（秒）。ケーブル モデムがこの時間内に登録ステージを完了しなかった場合、そのケーブル モデムはフラップ リストに追加されます。デフォルト値は 90 秒です。
ccsFlapPowerAdjustThreshold	Integer32	1 ～ 10	モデムの出力が出力調整しきい値を超えて調整されると、そのモデムはフラップ リストに追加されます。
ccsFlapMissThreshold	Unsigned32	1 ～ 12	ケーブル モデムが連続してこの回数だけ MAC レイヤ ステーション メンテナンス（キープアライブ）メッセージを確認しなかった場合、そのケーブル モデムはフラップ リストに追加されます。

12 このパラメータで SNMP を使用する場合の許容範囲は 1 ～ 65536（32 ビット値）ですが、有効な動作範囲は 1 ～ 8191 です。

13 この値は、**cable flap-list size** コマンドで設定する場合と同じで、コマンドの出力にのみ適用されます。これは SNMP で表示されるフラップ リスト エントリには影響しません。

14 SNMP エントリ数はこの値と同じです。CLI エントリ数は、**ccsFlapListMaxSize** で設定される値によって異なります。

（注） **ccsFlapListMaxSize** は、ダウンストリーム ケーブル インターフェイスごとのフラップ リストの表示を制御します。ライン カードごとのフラップ リスト エントリ数が 8191 を超えない限り、これらのエントリはシステムに保存され、CLI では表示されません。

ccsFlapListCurrentSize は、CLI の表示に関係なく、システム内のすべてのライン カードのフラップ リスト エントリ数を反映します。

SNMP を使用したフラップ リストとカウンタのクリア（任意）

フラップ リストからケーブル モデムを削除したり、フラップ リスト カウンタの 1 つまたはすべてを消去したりするには、CISCO-CABLE-SPECTRUM-MIB に適切な cssFlapObjects 属性を設定します。このテーブルには、SNMP カウンタを消去した属性が表示されます。

表 *254*：フラップ リストを消去する属性

属性	タイプ	説明
ccsFlapResetAll	Boolean	このオブジェクトを [True (1)] に設定すると、すべてのフラップ リストがゼロにリセットされます。
ccsFlapClearAll	Boolean	このオブジェクトを [True (1)] に設定すると、フラップリストからすべてのケーブル モデムが削除され、ccsFlapTable 内のエントリがすべて破棄されます。モデムのフラッピングが継続する場合は、このモデムがフラップリストに新しいエントリとして追加されます。

（注） ccsFlapLastClearTime 属性には、ccsFlapTable テーブル内のエントリが最後に消去された日時が含まれます。

フラップリストを使用したモニタリングおよびトラブルシューティング方法

show cable flap-list コマンドを使用したフラップ リストの表示

フラップ リストの現在の内容を表示するには、特権 EXEC モードで show cable flap-list コマンドを使用します。このコマンドの構文は次のとおりです。

- **showcableflap-list**：完全なフラップ リストを表示します。
- **showcableflap-listsort-interface**：ケーブル インターフェイスでソートされた完全なフラップ リストを表示します。
- **showcableflap-list cable** *interface* **upstream** *port*：特定のケーブル インターフェイス、またはそのケーブル インターフェイスの特定のアップストリーム ポートのフラップ リストを表示します。

出力のソート方法を変更するには、次のオプション キーワードのいずれかを追加します。

- **sort-flap**：ケーブル モデムのフラップ回数で出力をソートします。
- **sort-time**：ケーブル モデムの最新のフラップ回数で出力をソートします。

次に、**show cable flap-list** コマンドの一般的な出力例を示します。

```
Router# show cable flap-list
Mac Addr       CableIF Ins    Hit   Miss    CRC  P-Adj   Flap    Time
0010.9500.461f C1/0 U1 56  18857    887      0      1    116 Jun 1  14:09:12
0010.9500.446e C1/0 U1 38  18686   2935      0      1     80 Jun 2  19:03:57
0010.9500.38ec C1/0 U2 63  18932   1040      0      8    138 Jun 2  23:50:53
0010.9500.4474 C1/0 U2 65  18913   1053      0      3    137 Jun 2  09:30:09
0010.9500.4672 C1/0 U2 56  18990   2327      0      6    124 Jun 2  10:44:14
0010.9500.38f0 C1/0 U2 50  18964   2083      0      5    111 Jun 2  20:46:56
0010.9500.e8cb C1/0 U2  0   6537    183      0      1      5 Jun 2  22:35:48
0010.9500.38f6 C1/0 U3 50  19016   2511      0      2    104 Jun 2  07:46:31
0010.9500.4671 C1/0 U3 43  18755   3212      1      1     89 Jun 1  19:36:20
0010.9500.38eb C1/0 U0 57  36133   1608      0      6    126 Jun 2  20:04:58
0010.9500.3ce2 C1/0 U0 44  35315   1907      0      4     99 Jun 2  16:42:47
0010.9500.e8d0 C1/0 U2  0  13213    246      0      1      5 Jun 3  04:15:30
0010.9500.4674 C1/0 U2 56  36037   2379      0      4    121 Jun 3  00:34:12
0010.9500.4677 C1/0 U2 40  35781   2381      0      4     91 Jun 2  12:14:38
0010.9500.4614 C1/0 U2 40  21810   2362      0    502    586 Jun 2  21:43:02
0010.9500.3be9 C1/0 U2 63  22862    969      0      0    128 Jun 1  14:09:03
0010.9500.4609 C1/0 U2 55  22723   2127      0      0    112 Jun 1  14:08:02
0010.9500.3cb8 C1/0 U2 49  22607   1378      0      0    102 Jun 1  14:08:58
0010.9500.460d C1/0 U3 46  22477   2967      0      2     96 Jun 2  17:03:48
0010.9500.3cba C1/0 U3 39  22343   3058      0      0     81 Jun 1  14:13:16
0010.9500.3cb4 C1/0 U3 38  22238   2936      0      0     79 Jun 1  14:09:26
0010.9500.4612 C1/0 U3 38  22306   2928      0      0     79 Jun 1  14:09:29
Router#
```

show cable modem flap コマンドを使用したフラップ リストの表示

特定のケーブル モデムのフラップ リストの内容を表示するには、特権 EXEC モードで **show cable modem flap** コマンドを使用します。このコマンドの構文は次のとおりです。

- **showcablemodem** [*ip-address*| *mac-address*] **flap**：IP アドレスまたは MAC アドレスで識別される特定のケーブル モデムのフラップ リストを表示します。
- **showcablemodem cable***interface*[**upstream***port*] **flap**：特定のケーブル インターフェイス上のすべてのケーブル モデムのフラップ リストを表示します。

（注） **show cable modem flap** コマンドによって表示される情報は、モデム単位で表示されるという点を除き、**showcableflap-list** コマンドで表示される情報と同様です。

次に、特定のケーブル モデムに対する **showcablemodemflap** コマンドの出力例を示します。

```
Router# show cable modem 0010.7bb3.fcd1 flap
MAC Address    I/F       Ins   Hit   Miss  CRC   P-Adj   Flap  Time
0010.7bb3.fcd1 C5/0/U5   0     36278 92    0     369     372   Jun 1  13:05:23 (18000msec)
```

次に、特定のケーブルインターフェイス上のすべてのケーブルモデムに対する **showcablemodemflap** コマンドの出力例を示します。

```
Router# show cable modem cable 6/0/0 flap
MAC Address    I/F           Ins   Hit   Miss  CRC   P-Adj   Flap  Time
0025.2e34.4386 C6/0/0/U0     0     46778 3980  0      0      0     (14212 msec)
0025.2e2f.d4b6 C6/0/0/U0     0     48002 1899  0      0      0     (18000 msec)
0025.2e2f.d4de C6/0/0/U0     0     48098 1889  0      0      0     (19552 msec)
0023.bee1.e96b C6/0/0/U0     0     46658 4351  0      0      0     (22432 msec)
0025.2e2f.d4d8 C6/0/0/U0     0     21979 781   0      0      0     ( -- )
```

```
0025.2e2f.d48c C6/0/0/U0     0     48048 1835  0      0      0     ( -- )
0025.2e2f.d490 C6/0/0/U0     0     48029 1819  0      0      0     ( -- )
```

SNMP を使用したフラップ リストの表示

SNMP を使用してフラップ リストの内容を表示するには、CISCO-CABLE-SPECTRUM-MIB の ccsFlapTable テーブルに照会します。このテーブルには、各ケーブル モデムのエントリが含まれています。次に、このテーブルの各属性を簡単に説明します。

表 *255* : ***cssFlapTable*** 属性

属性	タイプ	説明
cssFlapMacAddr	MacAddress	ケーブル モデムのケーブル インターフェイスの MAC アドレス。フラッピング ケーブル モデムのフラップ リスト エントリを示します。
ccsFlapUpstreamIfIndex	InterfaceIndex	フラッピング ケーブル モデムによって使用されるアップストリーム。
ccsFlapDownstreamIfIndex	InterfaceIndex	フラッピング ケーブル モデムによって使用されるダウンストリーム。
ccsFlapLastFlapTime	DateAndTime	ケーブルモデムが最後にフラップしたときのタイムスタンプ。
ccsFlapCreateTime	DateAndTime	このエントリがテーブルに追加されたときのタイムスタンプ。
ccsFlapRowStatus	RowStatus	このエントリのステータスの制御属性。

属性	タイプ	説明
ccsFlapInsertionFailNum	Unsigned32	CM が起動し、自身をネットワークに挿入する回数。初期のリンク確立から再確立までの時間が、**cableflap-listinsertion-time** コマンドまたはccsFlapInsertionTime 属性で設定したしきい値パラメータよりも少ない場合に、このカウンタが増えます。 ケーブル モデムが挿入回数（ccsFlapInsertionTime）内に登録を完了できない場合は、初期メンテナンス パケットを再送信します。CMTS が予想よりも前にパケットを受信すると、CMTS はこのカウンタの値を増やします。
ccsFlapHitNum	Unsigned32	CM が MAC レイヤ ステーション メンテナンス（キープアライブ）メッセージに応答する回数。（最小ヒット率は 30 秒ごとに 1 回です。）
ccsFlapMissNum	Unsigned32	CM が MAC レイヤ ステーション メンテナンス（キープアライブ）メッセージを見逃して応答しない回数。シスコのケーブル インターフェイス ライン カードでは、8%のミス率は普通です。CMTS が 25 マイクロ秒以内のレンジング要求を見逃すと、ミス回数が増えます。
ccsFlapCrcErrorNum	Unsigned32	CMTS アップストリーム レシーバが CRC エラーのパケットにフラグを付けた回数。値が大きい場合は、ケーブルのアップストリームのノイズ レベルが高いことを示します。モデムはまだフラッピングしていないかもしれませんが、問題になる可能異性があります。
ccsFlapPowerAdjustmentNum	Unsigned32	ケーブルモデムのアップストリームが電力を送信する回数は、ステーション メンテナンス中に調整されます。調整が電力調整のしきい値を超えると、回数が増加します。

属性	タイプ	説明
ccsFlapTotalNum	Unsigned32	モデムがフラップした回数です。次の項目の合計値です。 • ccsFlapInsertionFailNum が増加したとき • CMTSがヒットの次にミスを受信したとき • ccsFlapPowerAdjustmentNum が増加したとき
ccsFlapResetNow	Boolean	このオブジェクトを [True (1)] に設定すると、すべてのフラップ リストがゼロにリセットされます。
ccsFlapLastResetTime	DateAndTime	この特定のエントリのすべてのカウンタがゼロにリセットされたときのタイムスタンプ。

特定のケーブル モデムのフラップ リスト情報の表示

特定のケーブル モデムのフラップ リスト情報を表示するSNMP要求を使用するには、ccsFlapTableからエントリを検索するインデックスとしてケーブル モデムのMACアドレスを使用します。特定のケーブル モデムのフラップ リスト エントリを検索するには、次の手順を実行します。

手順

ステップ 1 ケーブル モデムのMACアドレスをドット付き10進数文字列に変換します。たとえば、MACアドレス000C.64ff.eb95は0.12.100.255.235.149になります。

ステップ 2 ccsFlapTableの情報を要求するインスタンスとしてMACアドレスのドット付き10進数を使用します。たとえば、このケーブル モデムのccsFlapHits、ccsFlapMisses、ccsFlapPowerAdjustmentsの値を検索するには、次のオブジェクトにSNMP要求を行います。

- ccsFlapHits.0.12.100.255.235.149
- ccsFlapMisses.0.12.100.255.235.149
- ccsFlapPowerAdjustments.0.12.100.255.235.149

例

MAC アドレス 000C.64ff.eb95 のケーブル モデムに関して、**showcableflap-list** コマンドを使用した場合と同じフラップ リスト情報を取得する必要があるとします。

```
Router# show cable flap-list
MAC Address     Upstream     Ins   Hit   Miss  CRC   P-Adj Flap  Time
000C.64ff.eb95  Cable3/0/U4  3314  55605 50460 0    *42175 47533 Jan 27 02:49:10
Router#
```

SNMP ツールを使用して、ccsFlapTable を取得し、10 進数の MAC アドレスでフィルタリングします。たとえば、標準的な Unix の **getone** コマンドを使用する場合は、次のコマンドを入力します。

```
csh% getmany -v2c 192.168.100.121 public ccsFlapTable | grep 0.12.100.255.235.149

ccsFlapUpstreamIfIndex.0.12.100.255.235.149 = 15
ccsFlapDownstreamIfIndex.0.12.100.255.235.149 = 17
ccsFlapInsertionFails.0.12.100.255.235.149 = 3315
ccsFlapHits.0.12.100.255.235.149 = 55608
ccsFlapMisses.0.12.100.255.235.149 = 50460
ccsFlapCrcErrors.0.12.100.255.235.149 = 0
ccsFlapPowerAdjustments.0.12.100.255.235.149 = 42175
ccsFlapTotal.0.12.100.255.235.149 = 47534
ccsFlapLastFlapTime.0.12.100.255.235.149 = 07 d4  01 1b   02 33  1a 00
ccsFlapCreateTime.0.12.100.255.235.149 = 07 d4  01 16   03 23  22 00
ccsFlapRowStatus.0.12.100.255.235.149 = active(1)
ccsFlapInsertionFailNum.0.12.100.255.235.149 = 3315
ccsFlapHitNum.0.12.100.255.235.149 = 55608
ccsFlapMissNum.0.12.100.255.235.149 = 50460
ccsFlapCrcErrorNum.0.12.100.255.235.149 = 0
ccsFlapPowerAdjustmentNum.0.12.100.255.235.149 = 42175
ccsFlapTotalNum.0.12.100.255.235.149 = 47534
ccsFlapResetNow.0.12.100.255.235.149 = false(2)
ccsFlapLastResetTime.0.12.100.255.235.149 = 07 d4  01 16   03 20  18 00
csh%
```

1 つの特定の値のみを要求するには、そのオブジェクトのインスタンスとして 10 進数の MAC アドレスを使用します。

```
csh% getone -v2c 172.22.85.7 public ccsFlapMisses.0.12.100.255.235.149

ccsFlapMisses.0.12.100.255.235.149 = 50736
csh %
```

トラブルシューティング情報

ここでは、フラップ リスト カウンタを理解するためのヒント、およびフラッピング ケーブル モデムに最適な電力レベルを決定するためのヒントを提供します。

トラブルシューティングのヒント

ここでは、フラップ リストの統計情報に基づいてさまざまなネットワーク状況を理解するためのヒントを示します。

- 状況 1：ミスまたはヒット比が低く、挿入が少なく、P-Adj が小さく、フラップ カウンタ値が小さく、タイムスタンプが古い。分析：最適なネットワーク状況であることを示しています。
- 状況 2：ヒットに比べてミスの比率が高い（10% を超える）。分析：ヒットおよびミスの分析は、挿入カウントの増加が止まってから行う必要があります。一般に、ヒット数とミス数が同程度の場合、アップストリームに雑音が生じている可能性があります。ミスのほうが多い場合は、モデムの接続が頻繁に切断されて、登録が完了していない可能性があります。アップストリームまたはダウンストリームが十分に安定していないために、信頼性のあるリンクが確立されていません。ヒットとミスが非常に少なく、挿入カウンタ値が高い場合、プロビジョニングに問題があります。
- 状況 3：出力調整カウンタ値が相対的に高い。分析：出力調整しきい値がデフォルト値の 2 dB に設定されていると考えられます。モデムのトランスミッタ ステップ サイズは 1.5 dB ですが、ヘッドエンドは 0.25 dB のステップ サイズを要求することができます。フラップ リストの不適切なエントリ数を少なくするために、出力しきい値を 6 dB に調整することを推奨します。出力調整しきい値は、Cisco IOS のグローバル コンフィギュレーション モードで、cable flap power threshold <0-10 dB> を使用して設定できます。短い増幅器のカスケードで正常に運用されている HFC ネットワークでは、2 ～ 3 dB のしきい値を使用できます。
- 状況 4：出力調整カウンタ値および CRC エラーが多い。分析：ファイバ ノードがアップストリームのリターン レーザーをクリッピングしている状況を示しています。CRC カウントが最も高いモデムを最初に調べてください。モデムがオフラインにならない場合（Ins=0）、加入者が気づくことはありません。ただし、アップストリームで IP パケットがドロップされるので、加入者に対するサービス提供が遅くなることがあります。この状況では、Cisco CMTS ルータのケーブル インターフェイス上で入力エラーが発生します。
- 状況 5：挿入レートが高い。分析：リンクの再確立が過度に頻繁な場合、通常は、モデムの登録に問題があります。これは、フラップ カウンタを追跡する挿入カウンタ値が高くなることで示されます。

振幅の平均化の実行

CMTS では、平均化アルゴリズムを使用して、搬送波対ノイズ比が小さいために過度の電力調整（いわゆるフラッピング）が行われているケーブル モデムについて、最適な電力レベルを決定します。フラッピング中のケーブル モデムがドロップされるのを防ぐため、CMTS は、設定可能な RNG-REQ メッセージ数を平均化してから、電力調整を行います。潜在的に不安定なリターン パスを補正することによって、CMTS は、影響のあるケーブル モデムとの接続を維持します。ただし、このような電力調整は、不安定なリターン パス接続を示していると解釈できます。

showcableflap-list および **showcablemodem** コマンドが機能強化されて、CMTS が電力を調整しているパスと、最大送信電力設定値に達したモデムを示すようになりました。これらの状況は、補正する必要がある不安定なパスであることを示します。

次に、**showcableflap-list** コマンドの出力例を示します。

```
Router# show cable flap-list
MAC Address     Upstream     Ins   Hit   Miss  CRC   P-Adj Flap  Time
 0010.7bb3.fd19  Cable1/0/U1  0     2792  281   0     *45    58    Jul 27 16:54:50
 0010.7bb3.fcfc  Cable1/0/U1  0     19    4     0     !43    43    Jul 27 16:55:01
```

```
 0010.7bb3.fcdd  Cable1/0/U1  0     19    4     0    *3     3     Jul 27 16:55:01
```

アスタリスク（*）は、CMTSがこのモデムに電力調整法を使用していることを示しています。感嘆符（!）は、モデムが最大送信電力に達していることを示しています。

showcablemodem コマンドの出力は次のとおりです。

```
Router# show cable modem
 Interface   Prim Online     Timing Rec    QoS CPE IP address      MAC address
             Sid  State      Offset Power
 Cable1/0/U0 1    online     2257    0.00  3   0   10.30.128.142   0090.8330.0217
 Cable1/0/U0 2    online     2262  *-0.50  3   0   10.30.128.145   0090.8330.020f
 Cable1/0/U0 3    online     2260    0.25  3   0   10.30.128.146   0090.8330.0211
 Cable1/0/U0 4    online     2256   *0.75  3   0   10.30.128.143   0090.8330.0216
 Cable1/0/U0 5    online     2265   *0.50  3   0   10.30.128.140   0090.8330.0214
 Cable1/0/U0 6    online     2256    0.00  3   0   10.30.128.141   0090.8330.0215
 Cable1/0/U0 7    online     4138  !-1.00  3   1   10.30.128.182   0050.7366.124d
 Cable1/0/U0 8    online     4142  !-3.25  3   1   10.30.128.164   0050.7366.1245
 Cable1/0/U0 9    online     4141  !-3.00  3   1   10.30.128.185   0050.7366.17e3
 Cable1/0/U0 10   online     4142  !-2.75  3   0   10.30.128.181   0050.7366.17ab
 Cable1/0/U0 11   online     4142  !-3.25  3   1   10.30.128.169   0050.7366.17ef
```

showcableflap-list コマンド表示の場合と同様に、**showcablemodem** コマンド出力に示されている * 記号は、このCMでCMTSが電力調整法を使用していることを意味します。記号!は、CMが最大送信電力に達していることを示しています。

その他の関連するコマンドの使用

次の関連するCisco IOSコマンドを使用すると、ケーブル モデムのメンテナンスおよび情報を表示できます。

- 次のコマンドは、ステーション メンテナンス リストの1つのケーブル モデム（またはすべてのケーブル モデム）のカウンタをクリアします。

```
clear cable modem {mac-addr | ip-addr | all} counters
```

- 次のコマンドは、SIDに基づいて、QoS、モデム ステータス、In/Outオクテット、IPアドレス、およびMACアドレスを表示します。

```
show int cable slot/port sid
```

- 次のコマンドは、キープアライブ ポーリング リストからモデムを削除することにより、モデムのRFリンクを切断します。これにより、モデムは強制的にリセットされます。次の警告に注意してください。

```
clear cable-modem {mac-addr | ip-addr | all} reset
```

ヒント **clearcable-modem** *all* **reset** コマンドを実行すると、すべてのモデムがオフラインになり、ユーザに対するサービスが停止します。テスト環境または非実働環境で使用するのが最良です。

- 次のコマンドは、MAC レイヤの ping を使用してケーブル モデムがオンラインかどうかを調べます。この場合、オーバーヘッドを軽減するために、標準IP pingより小さいデータ ユニットをワイヤ上で使用します。このコマンドは、モデムのIP レイヤが停止している場合、または登録が未完了の場合でも有効です。

```
ping DOCSIS cable-modem mac-addr | IP address
```

- 次のコマンドは、ケーブル インターフェイス、SID、またはMAC アドレスに基づいて、タイミング オフセット、受信電力、およびQoS 値を表示します。

```
show cable modem [ip-address | MAC-address]
```

- 次のコマンドは、現在のアロケーション テーブルおよび周波数割り当てを表示します。

```
show cable spectrum-group [spectrum group number]
```

- 次のコマンドは、特定のケーブル ルータ インターフェイス上の特定の SID について、オンライン時間とオフライン時間の最大、平均、最小パーセンテージを表示します。

```
show int slot/port sid connectivity
```

- 次のコマンドは、入力レート、出力レート、入力エラー、CRC、フレーム、オーバーラン、アンダーラン、コリジョン、インターフェイスのリセットを表示します。このクエリでCMTS が検索した入力エラー数が多い場合は、アップストリームで雑音が生じている可能性があります。旧バージョンのシャーシの場合、ミッドプレーンやライン カードのネジが緩んでいると、同様の問題が起きます。

```
show interface slot/downstream-port
```

- 次のコマンドは、アップストリーム パケットの廃棄数、エラー数、正常なパケット数、修正可能なエラー数、修正不能なエラー数、ノイズ、およびマイクロ リフレクションに関する統計情報を表示します。

```
show interface slot/downstream-port upstream
```

フラップ リスト トラブルシューティングの設定例

次のコンフィギュレーション ファイルの抜粋では、一般的なフラップ リスト設定を示します。

```
!
cable flap-list insertion-time 120
cable flap-list power-adjust threshold 3
cable flap-list miss-threshold 4
```

```
cable flap-list aging 8
cable flap-list size 8191
...
```

その他の参考資料

フラップリストトラブルシューティング機能の詳細については、次の参考資料を参照してください。

関連資料

関連項目	マニュアル タイトル
CMTS コマンド リファレンス	『Cisco CMTS Cable Command Reference』
Cisco Broadband Troubleshooter	http://www.cisco.com/c/en/us/support/cloud-systems-management/broadband-troubleshooter/tsd-products-support-series-home.html

標準

標準[15]	タイトル
ANSI/SCTE 22-1 2012（以前の SP-RFI-C01-011119）	『Data-Over-Cable Service Interface Specification DOCSIS 1.0 Radio Frequency Interface (RFI)』
SP-RFIv1.1-I08-020301	『Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification』
SP-BPI+-I08-020301	『DOCSIS Baseline Privacy Interface Plus Specification』

15 サポートされている標準がすべて記載されているわけではありません。

MIB

MIB [16]	MIB のリンク
CISCO-CABLE-SPECTRUM-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://tools.cisco.com/ITDIT/MIBS/servlet/index

16 サポートされている MIB がすべて記載されているわけではありません。

RFC

説明	リンク
この機能でサポートが追加または変更された RFC はありません。	Request for Comment（RFC）とインターネット ドラフトを検索してダウンロードするには、次の URL から Internet Engineering Task Force（IETF）の Web サイトを参照してください。 http://www.ietf.org/index.html

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

フラップ リストのトラブルシューティングに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *256*：フラップ リストのトラブルシューティングに関する機能情報

機能名	リリース	機能情報
フラップ リストのトラブルシューティング	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 99 章

MAX CPE と Host パラメータ

このマニュアルでは、ケーブル ネットワークで使用する、Data-over-Cable Service Interface Specifications（DOCSIS）により許可される加入者アクセスを制御するためのさまざまな方法について説明します。

機能情報の確認

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

Cisco cBR シリーズ ルータに関するハードウェア互換性マトリクス

（注） Cisco IOS-XE の特定のリリースで追加されたハードウェア コンポーネントは、特に明記しない限り、以降のすべてのリリースでもサポートされます。

表 *257* : *Cisco cBR* シリーズ ルータに関するハードウェア互換性マトリクス

Cisco CMTS プラットフォーム	プロセッサ エンジン	インターフェイス カード
Cisco cBR-8 コンバージド ブロードバンド ルータ	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8スーパーバイザ： • PID：CBR-CCAP-SUP-160G • PID：CBR-CCAP-SUP-60G • PID：CBR-SUP-8X10G-PIC	**Cisco IOS-XE リリース 16.5.1 以降のリリース** Cisco cBR-8 CCAP ライン カード： • PID：CBR-LC-8D30-16U30 • PID：CBR-LC-8D31-16U30 • PID：CBR-RF-PIC • PID：CBR-RF-PROT-PIC • PID：CBR-CCAP-LC-40G-R Cisco cBR-8 ダウンストリーム PHY モジュール： • PID：CBR-D30-DS-MOD • PID：CBR-D31-DS-MOD Cisco cBR-8 アップストリーム PHY モジュール： • PID：CBR-D30-US-MOD • PID：CBR-D31-US-MOD

MAX CPE と Host パラメータの情報

DOCSIS 仕様には、サービス プロバイダーが特定のケーブル モデムを介してネットワークにアクセスできる加入者数を制御できるようにする多数のプロビジョンが含まれます。

ネットワークにアクセスできる CPE の数を制御するパラメータは次のとおりです。

（注） また、DOCSIS コンフィギュレーション ファイルには、ケーブル モデムの背後にある CPE デバイスがケーブル ネットワークにアクセスできるかどうかを指定する Network Access パラメータが含まれています。Network Access パラメータが Disabled に設定されている場合、ケーブル モデムの背後にある CPE デバイスはネットワークにアクセスできません。

ヒント また、Cisco CMTS は、オフラインのケーブル モデムを内部データベースに 24 時間リストします。CMTS は、24 時間の期間が終了してケーブル モデムがオンラインに戻るまで、これらのオフライン ケーブル モデムの CPE カウントをリセットしません。24 時間の期間が終了する前にケーブル モデムがオンラインに戻った場合は、CMTS は既存の CPE カウントを継続して使用します。

これらの方法はすべて目的が似ていますが、設定は異なり、ケーブルモデムやCPEデバイスに与える影響が異なります。

ケーブル モデムは MAX CPE 値を適用し、CMTS は MAX Host、Max CPE IP、および MAX CPE IPv6 値を適用します。

（注） MAX CPE パラメータは、CPE デバイスのレイヤ 2 制御を提供します。MAX CPE IP および MAX CPE IPv6 パラメータは、CPE デバイスのレイヤ 3 制御を提供します。2 つの方法は補完し合う関係にありますが、それ以外の関係性はありません。

MAX CPE

MAX CPE は必須パラメータであり、現在のセッション中にネットワークにアクセスできる CPE デバイスの数を制御するために使用されます。DOCSIS 1.0 ケーブル ネットワークでは、MAX CPE パラメータは、任意の特定のケーブルモデムを使用してケーブル ネットワークに接続できる CPE デバイスの数を制御するための主な手段です。このパラメータは、DOCSIS コンフィギュレーション ファイル（TLV 18）内に設定されます。DOCSIS コンフィギュレーション ファイルに設定されていない場合、このパラメータの値はデフォルトで 1 になります。

（注） DOCSIS 1.1 ケーブル ネットワークでは、CMTS は DOCSIS コンフィギュレーション ファイル内で指定されている MAX CPE パラメータを無視し、代わりに MAX Host パラメータを使用します。

新しい CPE デバイスがケーブル ネットワークに接続しようとするたびに、ケーブル モデムは装置のアドレス（MAC アドレス）をログします。ケーブル モデムが MAC アドレスの MAX CPE 数に到達していい場合、新しい CPE デバイスはネットワークへのアクセスが許可されます。ケーブル モデムが MAX CPE 制限に達すると、他の CPE デバイスからのトラフィックをドロップします。

ケーブル モデムはデフォルトで、新しい MAC アドレスを先着順に学習します。また、DOCSIS コンフィギュレーション ファイル（TLV 14）に MAC アドレスを入力することで、許可する CPE デバイス の MAC アドレスを予め設定できます。これらのケーブル モデムは、事前に設定された MAC アドレスに対して優先的にネットワークへの接続を許可します。

DOCSIS 仕様では、ケーブル モデムによる MAC アドレスのエージアウトが許可されていないため、ケーブル モデムがリセットされるまで MAC アドレスはケーブル モデムのログに残ります。したがって、このパラメータについては、「ケーブル ネットワークに同時接続可能な CPE デバイスの最大数」としてではなく、「特定のセッション中に接続可能な CPE デバイスの最大数」として考える必要があります。

たとえば、MAX CPE を 2 に設定すると、顧客は 1 台のケーブル モデムを使用して、最大で 2 台の CPE デバイス（2 個の MAC アドレス）をケーブル ネットワークに接続します。顧客は、2 台の PC を同時にケーブル モデムに接続し、両方からネットワークにアクセスすることが可能です。

しかし、顧客がこれらの PC を切断して新たに別の 2 台を接続した場合、これらの PC はケーブル モデム上では 3 番目および 4 番目の MAC アドレスとなるので、ケーブル モデムは新しい PC をオンラインにすることはできません。顧客がそれらの PC を使用するには、ケーブル モデムをリセットする必要があります。

（注） MAX CPE 値（指定した場合）は、DOCSIS 1.0 コンフィギュレーション ファイルで正の整数を指定する必要があります。このパラメータは DOCSIS 1.1 コンフィギュレーション ファイルではゼロにすることもできますが、その場合、ケーブル モデムの MAX CPE 値には 1 を使用します。MAX CPE パラメータをいずれのタイプの DOCSIS コンフィギュレーション ファイルにも指定しない場合、デフォルトの 1 に設定されます。

MAX Host

MAX Host パラメータはオプションのパラメータであり、Cisco CMTS に設定され、CMTS がネットワーク アクセスを許可する CPE デバイス（MAC アドレス）の最大数を指定します。使用する CLI コマンドに応じて、個々のケーブル モデム、特定のケーブル インターフェイス上のすべてのケーブル モデム、または Cisco CMTS 上のすべてのケーブル モデムに対してこのパラメータを制御できます。

- **cablemodemmax-cpe**：Cisco CMTS 上のすべてのケーブル モデムの MAX Host を設定します。**unlimited** キーワードを使用して、Cisco CMTS がケーブル モデムに対して MAX Host 制限を実行しないように指定できます。

これをイネーブルにすると、Cisco CMTS は、CPE デバイスがケーブル ネットワークに初めてアクセスした際に MAC アドレスを学習します。Cisco CMTS が MAX Host パラメータで指定された最大 MAC アドレス数をログすると、その後は他の MAC アドレスを持つ CPE デバイスのすべてのトラフィックがドロップされます。

ヒント DOCSIS 1.1 ケーブル ネットワークでは、MAX CPE IP および MAX Host パラメータの両方が設定された場合、各ケーブル モデムの背後で許可される CPE デバイスの最大数を決めるために、Cisco CMTS は小さい方の値を使用します。デフォルトでは、MAX Host は 16 に設定されています。

（注） Cisco CMTS がリセットされるたびに、MAX Host アドレス テーブル全体がクリアされます。また、**clearcablehost** コマンドを使用して特定の CPE デバイスのエントリをクリアすることもできます。

MAX Host への任意の値の指定

CMTS 上のすべてのケーブル モデムに適用される **cable modem max-cpe** コマンドは、CMTS が CPE デバイスに対していかなる制限も実施しないことを指定する **unlimited** キーワードをサポートします。unlimited **keyword**を使って CMTS を設定すると、あらゆる数の CPE デバイスがケーブル モデムでサポートされます。

unlimited オプションを使用する場合は、各ケーブル モデムがサポートする CPE デバイスの最大数を制御できるよう、DOCSIS コンフィギュレーション ファイルで適切な MAX CPE 値を必ず指定してください。また、ユーザが無制限の数の IP アドレスを要求するのを防ぐため、DHCP サーバを設定して、各ケーブル モデムの背後にある CPE デバイスに割り当てられる IP アドレスの数を制御します。

MAX CPE IP

MAX CPE IP パラメータは DOCSIS 1.1 ケーブル ネットワークでのみ適用可能であり、オプションのパラメータです。このパラメータは、ケーブル モデムが CPE デバイスで IP アドレス フィルタリングを実行するか否かを設定します。フィルタリングを実行する場合、この属性は、同時にモデムの背後で許可される同時 IP アドレスの最大数も指定します。

MAX CPE IP パラメータは、DOCSIS コンフィギュレーション ファイル（TLV 35）に設定されるか、ケーブル モデム用に（DOCS-CABLE-DEVICE-MIB 内の）docsDevCpeIpMax 属性を設定する SNMP コマンドを使用して設定します。デフォルトでは、このパラメータは有効ではありません。**cablesubmgmtdefaultactive** コマンドを使って MAX CPE IP パラメータの使用を有効にしない限り、Cisco CMTS はアクティブに CPE デバイスを管理しません。**cable submgmt default max-cpe** コマンドを使用して、ケーブル モデムの背後にある IP アドレスの数を制限することができます。

この機能をイネーブルにすると、CPE デバイスが最初に IP パケットをネットワークに送信するときに、ケーブル モデムが許容 IP アドレスを学習します。IP アドレスが docsDevFilterCpeTable テーブルに追加されます。このアドレステーブルは、ケーブルモデムがリセットされるか、または電源がオフになると自動的にクリアされます。また、このケーブルモデムの該当するテーブルエントリ内で docsSubMgtCpeControlReset 属性を設定することにより、IP アドレス テーブルを手動でクリアできます。

ヒント　CMTS は、フィルタリング処理の一部として MAX CPE IP 値を使用しますが、この 2 つのフィルタはケーブル モデムと CMTS で独立して動作します。

MAX CPE IPv6

MAX CPE IPv6 パラメータはオプションのパラメータであり、任意の時点にケーブル モデムに許可される同時 IPv6 アドレスの最大数を指定します。

MAX CPE IPv6 パラメータは、DOCSIS 3.0 コンフィギュレーション ファイル（TLV 63）に設定されるか、ケーブル モデム用に（DOCS-SUBMGT3-MIB 内の）docsSubmgt3BaseCpeMaxIpv6PrefixDef 属性を設定する SNMP コマンドを使用して設定します。デフォルトでは、このパラメータは有効ではありません。**cablesubmgmtdefaultactive** コマンドを使用して MAX CPE IPv6 パラメータの使用を有効にしない限り、Cisco CMTS はアクティブに CPE デバイスを管理しません。**cable submgmt default max-ipv6-cpe** コマンドを使用して、ケーブル モデムの背後で許可される IPv6 アドレスの数を制限することができます。

MAX CPE IPv6 機能をイネーブルにすると、CPE デバイスが最初に IPv6 パケットをネットワークに送信するときにケーブル モデムが許容 IPv6 アドレスを学習します。IPv6 アドレスが IPv6 アドレス テーブルに追加されます。アドレス テーブルは、ケーブル モデムがリセットされるか電源がオフになると自動的にクリアされます。

MAX CPE パラメータの相互運用

異なる CPE 制御方式をすべて同時にアクティブにすることができます。この場合、相互関係はあっても衝突することはありません。表にそれぞれの方法と特長を示します。

表 *258*：各 *MAX CPE* および *MAX Host* 制御メカニズムの比較

CM 設定パラメータ	機能	CMTS の対応する機能	CMTS 適用のプライオリティ
Network Access Control	CPE デバイスのすべてのネットワーク アクセスを防止	Cable submgmt default learnable	CMTS は CM コンフィギュレーション ファイルをオーバーライドします
MAX CPE	CM ごとに MAC アドレスを制限	Cable modem max-hosts	最小制限が適用されます
MAX CPE IP	CM ごとに IP アドレスを制限	Cable submgmt default max-cpe	最大制限が適用されます
MAX CPE IPv6	CM ごとに IPv6 アドレスを制限	Cable submgmt default max-ipv6-cpe	最大制限が適用されます

表は、MAX CPE パラメータをプライオリティ順に示しています。たとえば、Network Access Control パラメータと MAX CPE パラメータの相互関係は次のとおりです。

- ケーブル モデムの [Network Access Control] フィールドが [Disabled] に設定されている場合、他のパラメータがどのように設定されているかに関わらず、そのモデムの CPE デバイスのどれにもアクセスできません。
- ケーブル モデムの [Network Access Control] が [Enabled]、[MAX CPE] が 1 に設定されている場合、残りのパラメータがどのように設定されているかに関わらず、最大 1 つの CPE デバイスがネットワークにアクセスできます。

利点

- CMTS の柔軟性により、マルチプル サービス オペレータのプロビジョニング担当者、サービス プロバイダー、その他のユーザは、ケーブル モデムの背後で接続可能な CPE デバイスの最大数、IPv4 アドレスの最大数、および IPv6 アドレスの最大数を CMTS とケーブル モデムの間で同期できます。
- 変更は、CLI コマンドを使用するか SNMP コマンドを使用して行うことができます。

MAX CPE と Host パラメータの設定方法

CMTS で認識される許可された CPE デバイスの最大数をリセットするには、次のコンフィギュレーション コマンドのいずれかを使用します。すべての手順は必要に応じてオプションとなります。

（注） ケーブル モデムが CMTS に登録する際に、CMTS はケーブル モデムに MAX Host 値を割り当てます。MAX Host コマンドに変更を加えた場合、変更後に登録されたケーブル モデムのみに影響します。

Cisco CMTS での CPE デバイスの最大数の設定

ケーブル モデムごとに CPE デバイスの最大数を設定するには、次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configureterminal** 例： `Router# configure terminal`	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	**cablemodemmax-cpe** [*number* | **unlimited**] 例： `Router(config)# cable modem max-cpe 8`	すべてのケーブル インターフェイスに対して Cisco CMTS で MAX CPE パラメータの値を設定します。 **show cable modem subscriber** は、cable modem max-cpe の MAXIMUM 値と、ケーブル モデムの DOCSIS コンフィギュレーション ファイル内の MAX CPE 値を表示します。 オンラインにできる CPR の数は、次のいずれかの要因に基づいて決定されます。 • CPE の数が、ケーブル モデムの DOCSIS コンフィギュレーション ファイル内の MAX CPE 値よりも小さい場合、**cable modem max-cpe** コマンドはコンフィギュレーション ファイルの値をオーバーライドします。 • CPE の数が、ケーブル モデムの DOCSIS コンフィギュレーション ファイル内の MAX CPE 値より大きい場合、または無制限と設定されている場合は、コンフィギュレーション ファイルの設定値が優先されます。 （注） コンフィギュレーション ファイル内の値がゼロで、**nocablemodemmax-cpe** が設定されている場合、IP アドレスを取得できる CPE デバイスはありません。
ステップ 4	**cablesubmgmtdefaultactive** 例： `Router(config)# cable submgmt default active`	CMTS が CPE デバイスをアクティブに管理するように指定します。デフォルト値はこのコマンドの **no** バージョンです。つまり、CMTS は CPE デバイスをアクティブに管理しません。

	コマンドまたはアクション	目的
ステップ 5	**cablesubmgmtdefaultmax-cpe** *cpe-ip* 例： `Router(config)# cable submgmt default max-cpe 4`	（任意）MAX CPE IP のデフォルト値を指定します。
ステップ 6	**cablesubmgmtdefaultmax-ipv6-cpe** *ipv6-num* 例： `Router(config)# cable submgmt default max-ipv6-cpe 4`	（任意）MAX IPv6 CPE のデフォルト値を指定します。
ステップ 7	**exit** 例： `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。

次の作業

（注） **cablemodemmax-cpeunlimited** コマンドを使用すると、サービス妨害攻撃が可能になり、システムにセキュリティ ホールが発生します。これにより、単一ユーザが大量の IP アドレスを取得できるため、利用可能なすべての IP アドレスを予約すると、ネットワーク全体がダウンします。

設定例

ケーブル インターフェイスの現在の設定とステータスを表示するには、特権 EXEC モードで **showrunning-config** コマンドを使用します。次の出力例では、最大 5 つの CPE デバイスがトラフィックを送るために指定されたケーブル インターフェイスを使用できるように、CMTS が許可しています。

```
interface Cable3/0
 ip address 192.168.1.1 255.255.255.0 secondary
 ip address 10.1.1.1 255.255.255.0
 load-interval 30
 no keepalive
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream frequency 507000000
```

```
 cable upstream 0 frequency 27008000
 cable upstream 0 power-level 0
 cable upstream 0 minislot-size 32
 cable upstream 0 modulation-profile 2
 no cable upstream 0 shutdown
 cable upstream 1 frequency 29008000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
 cable upstream 1 minislot-size 4
 no cable upstream 1 shutdown
 cable dhcp-giaddr policy
 cable helper-address 172.17.110.131
end
```

また、**more system:running-config** コマンドを使用すると、ケーブルインターフェイスで許可される最大 CPE デバイス数を確認することもできます。

```
CMTS01# more system:running-config
Building configuration...
Current configuration:
!
interface Cable6/0
 ip address 1.1.1.1 255.255.255.0
 no keepalive
 cable insertion-interval 2000
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream symbol-rate 5056941
 cable upstream 0 frequency 15008000
 cable upstream 0 fec
 cable upstream 0 scrambler
 no cable upstream 0 shutdown
```

その他の参考資料

Cisco CMTS での MAX CPE と Host パラメータの設定に関連する詳細については、次の参考資料を参照してください。

関連資料

関連項目	マニュアル タイトル
Cisco CMTS コマンド	『Cisco CMTS Cable Command Reference』
MAX CPE パラメータの相互運用	『Using the max-cpe Command in the DOCSIS and CMTS』

標準

標準[17]	タイトル
SP-RFIv1.1-I08-020301	『*Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification , version 1.1*』（http://www.cablelabs.com/cablemodem/）

17 サポートされている標準がすべて記載されているわけではありません。

MIB

MIB [18]	MIB のリンク
DOCS-CABLE-DEVICE-MIB DOCS-SUBMGT-MIB DOCS-SUBMGT3-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

18 サポートされている MIB がすべて記載されているわけではありません。

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

MAX CPE と Host パラメータに関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *259* : ***MAX CPE*** と ***Host*** パラメータに関する機能情報

機能名	リリース	機能情報
MAX CPE と Host パラメータ	Cisco IOS XE Everest 16.6.1	この機能は、 Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 100 章

SNMP バックグラウンド同期

SNMP バックグラウンド同期機能は、DOCSIS MIB テーブルの SNMP ポーリングのパフォーマンスを改善するために、バックグラウンドで定期的にライン カードからスーパーバイザに DOCSIS MIB データを同期します。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このマニュアルの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/ からアクセスできます。http://www.cisco.com/ のアカウントは必要ありません。

目次

SNMP バックグラウンド同期について

SNMP のパフォーマンスを向上させるために、ライン カードとスーパーバイザの間で SNMP MIB 情報を同期する SNMP バックグラウンド同期機能が導入されています。この機能は raw ソケットに基づいており、TCP プロトコルを使用します。SNMP バックグラウンド同期には、次の利点があります。

- 複数の小さなパケットを一緒にバンドルして送信し、IPC チャネル使用率を向上させます。
- 事前に割り当てられた静的バッファを使用してメッセージを送受信することで、実行時のバッファ割り当てを回避します。
- システムに高い負荷がかかっているときに CPU に負担をかけないように、CPU 使用率に基づいてSNMPバックグラウンド同期の受信プロセスをスリープ状態にすることで、他の優先されるプロセスと競合しません。
- サポート対象の MIB テーブルに関する SNMP ポーリングのパフォーマンスを大幅に向上させて、スーパーバイザとライン カードの両方で CPU 使用率を低減させます。

SNMP バックグラウンド同期では、次の MIB テーブルがサポートされます。

- docsQosParamSetEntry
- docsIetfQosParamSetEntry
- docsQos3ParamSetEntry
- docsIf3CmtsCmUsStatusEntry
- docsIfCmtsCmStatusEntry
- docsSubMgtCpeControlEntry
- docsSubMgtCmFilterEntry
- cdxCmtsCmStatusExtEntry
- docsLoadBalCmtsCmStatusEntry
- docsIf3CmtsCmRegStatusTable
- docsIfSignalQualityTable
- docsifCmtsServiceTable
- cdxCmtsServiceExtEntry

SNMP バックグラウンド同期の設定方法

SNMP バックグラウンド同期の有効化

はじめる前に

cable bgsync コマンドを使用するには、グローバル コンフィギュレーション モードで **service internal** コマンドを設定する必要があります。

SNMP バックグラウンド同期はデフォルトで有効にされています。この機能を無効にするには **no cable bgsync active** を使用し、再び有効にするには **cable bgsync active** を使用します。次の手順で、SNMP バックグラウンド同期を有効にする具体的なステップを記載します。

enable
configure terminal

cable bgsync active
exit

データ間隔の設定

はじめる前に

cable bgsync コマンドを使用するには、グローバル コンフィギュレーション モードで **service internal** コマンドを設定する必要があります。**cable bgsync** コマンドは CPU 使用率に影響を与える可能性があるため、慎重に使用してください。

Cisco cBR ルータ上の SNMP MIB データのバックグラウンド同期のデータ間隔を設定するには、グローバル コンフィギュレーション モードで **cable bgsync** {**itime** *i-interval*|**ptime** *p-interval*} コマンドを使用します。バックグラウンド同期を無効にするには、このコマンドの **no** 形式を使用します。次の手順で、データ間隔を設定する具体的なステップを記載します。

enable
configure terminal
service internal
cable bgsync itime *i-interval*
cable bgsync ptime *p-interval*
exit
itime 関連するすべての MIB テーブルをライン カードから スーパーバイザ に同期する間隔です。有効な範囲は 5 ～ 31536000 です。デフォルト値は 86400 です。**ptime** 変更された MIB の内容をライン カードから スーパーバイザ に同期する間隔です。

SNMP バックグラウンド同期の確認

- SNMP バックグラウンド同期の現在のステータスを表示するには、次の例に示すように **show cable bgsync** コマンドを使用します。

```
Router#show cable bgsync
Background Sync is active, uptime is 5 minutes, 14 seconds.
Background Sync last active time is 5 minutes, 14 seconds. ago.
I-packet interval time is 1 day,  P-packet interval time is 5 senconds.
Line Card with bg-sync: 3/0
Line Card working on I syncing:
Last clear cable bg sync counters Time:
Total bytes: 85864
Total background sync packets: 2109
  Ack packets: 0
  Run Ctrl Msg packets: 2
  Data packets: 0
Interval packets: 2002
  I Type packets: 230
  P Type packets: 1772
Bg sync data IPC lost packets: 0

Background Sync statistics for the last 00:07:34
================================================================
 ipc packets 0-30k:      105
 ipc packets 30-60k:     0
 ipc packets 60-100k:    0
 msg per packet average: 20
 msg per packet max:     113
 msg per packet min:     1
 msg per packet under 3: 60
================================================================
```

```
type       packets        cpu-total(ms)    avg(us)   max(us)
serv flow  904            3                3         1000
sflog      0              0                0         0
cm         17             0                0         0
cmtx       296            0                0         0
paramset   112            0                0         0
DXIF       298            0                0         0
sid        208            0                0         0
uschan     167            1                5         1000
------------------------------------------------------------
IPC PKTs   105            4                0      ms 1      ms
============================================================================================
slot type       packets        bytes            pps        Bps        wrong_len_pkts
0    serv flow  0              0                0.0        0.0        0

0    sflog      0              0                0.0        0.0        0

0    cm         0              0                0.0        0.0        0

0    cmtx       0              0                0.0        0.0        0

0    paramset   0              0                0.0        0.0        0

0    DXIF       0              0                0.0        0.0        0

0    sid        0              0                0.0        0.0        0

0    uschan     0              0                0.0        0.0        0

1    serv flow  0              0                0.0        0.0        0

1    sflog      0              0                0.0        0.0        0

1    cm         0              0                0.0        0.0        0

1    cmtx       0              0                0.0        0.0        0

1    paramset   0              0                0.0        0.0        0

1    DXIF       0              0                0.0        0.0        0

1    sid        0              0                0.0        0.0        0

1    uschan     0              0                0.0        0.0        0

2    serv flow  0              0                0.0        0.0        0

2    sflog      0              0                0.0        0.0        0

2    cm         0              0                0.0        0.0        0

2    cmtx       0              0                0.0        0.0        0

2    paramset   48             7680             0.0        0.0        0

2    DXIF       0              0                0.0        0.0        0

2    sid        16             512              0.0        0.0        0

2    uschan     0              0                0.0        0.0        0

3    serv flow  904            25104            4.4        115.4      0

3    sflog      0              0                0.0        0.0        0

3    cm         17             981              0.0        2.0        0

3    cmtx       296            8607             0.7        20.6       0

3    paramset   64             8368             0.0        0.0        0

3    DXIF       298            21876            0.9        74.3       0
```

3	sid	192	4756	0.1	6.8	0
3	uschan	167	5832	0.3	10.7	0
6	serv flow	0	0	0.0	0.0	0
6	sflog	0	0	0.0	0.0	0
6	cm	0	0	0.0	0.0	0
6	cmtx	0	0	0.0	0.0	0
6	paramset	0	0	0.0	0.0	0
6	DXIF	0	0	0.0	0.0	0
6	sid	0	0	0.0	0.0	0
6	uschan	0	0	0.0	0.0	0
7	serv flow	0	0	0.0	0.0	0
7	sflog	0	0	0.0	0.0	0
7	cm	0	0	0.0	0.0	0
7	cmtx	0	0	0.0	0.0	0
7	paramset	0	0	0.0	0.0	0
7	DXIF	0	0	0.0	0.0	0
7	sid	0	0	0.0	0.0	0
7	uschan	0	0	0.0	0.0	0
8	serv flow	0	0	0.0	0.0	0
8	sflog	0	0	0.0	0.0	0
8	cm	0	0	0.0	0.0	0
8	cmtx	0	0	0.0	0.0	0
8	paramset	0	0	0.0	0.0	0
8	DXIF	0	0	0.0	0.0	0
8	sid	0	0	0.0	0.0	0
8	uschan	0	0	0.0	0.0	0
9	serv flow	0	0	0.0	0.0	0
9	sflog	0	0	0.0	0.0	0
9	cm	0	0	0.0	0.0	0
9	cmtx	0	0	0.0	0.0	0
9	paramset	0	0	0.0	0.0	0
9	DXIF	0	0	0.0	0.0	0
9	sid	0	0	0.0	0.0	0
9	uschan	0	0	0.0	0.0	0

- スーパーバイザ 側またはライン カード側のすべての SNMP バックグラウンド同期データを表示するには、次の例に示すように **show cable bgsync sync-info cable** コマンドを使用します。

```
Router#show cable bgsync sync-info cable 9/0/1
 part1 for srv template:
srv_tmp_id   min_rate    max_rate    max_burst
0            0           0           0
1            0           64000       0
2            0           1000000     0
3            0           1000000     3044
4            0           0           3044
5            0           110000000   30000
6            0           0           3044
7            0           2000000000  5000000
8            0           0           3044
 part2 for srv flow:
sfid     prov_qos   adm_qos    act_qos    wb_mode    octets    pkts    delay_pkts
drop_pkts    gate_id    create_time    total_active_time
1        0          0          0          0          0         0          0
 0          0             0              0
2        0          0          0          0          0         0          0
 0          0             0              0
3        0          0          0          0          0         0          0
 0          0             0              0
4        0          0          0          0          0         0          0
 0          0             0              0
5        0          0          0          0          0         0          0
 0          0             0              0
6        0          0          0          0          0         0          0
 0          0             0              0
7        0          0          0          0          0         0          0
 0          0             0              0
8        0          0          0          0          0         0          0
 0          0             0              0
9        0          0          0          0          0         0          0
 0          0             0              0
10       0          0          0          0          0         0          0
 0          0             0              0
11       0          0          0          0          0         0          0
 0          0             0              0
12       0          0          0          0          0         0          0
 0          0             0              0
13       0          0          0          0          0         0          0
 0          0             0              0
14       0          0          0          0          0         0          0
 0          0             0              0
15       3          3          3          0          0         0          0
 0          0             3600           179
16       3          3          3          0          0         0          0
 0          0             3600           179
17       3          3          3          0          0         0          0
 0          0             3600           179
18       3          3          3          0          0         0          0
 0          0             3600           179
19       3          3          3          0          0         0          0
 0          0             3600           179
20       3          3          3          0          0         0          0
 0          0             3600           179
21       3          3          3          0          0         0          0
 0          0             3600           179
22       3          3          3          0          0         0          0
 0          0             3600           179
23       3          3          3          0          0         0          0
 0          0             3600           179
24       3          3          3          0          0         0          0
 0          0             3600           179
25       3          3          3          0          0         0          0
 0          0             3600           179
26       3          3          3          0          0         0          0
 0          0             3600           179
27       4          5          5          0          8925      42         0
```

```
 0          0              12700          88
28       6          7           7          3          0          0          0
 0          0              12700          88
29       4          5           5          3          3855       21         0
 0          0              11500          100
30       6          7           7          3          0          0          0
 0          0              11500          100
31       8          8           8          3          222        3          0
 0          0              11500          100
32       4          5           5          3          1277       11         0
 0          0              12100          94
33       6          7           7          0          0          0          0
 0          0              12100          94
34       4          5           5          0          3851       21         0
 0          0              12300          92
35       6          7           7          3          0          0          0
 0          0              12300          92
36       8          8           8          0          148        2          0
 0          0              12100          94
37       4          5           5          0          3855       21         0
 0          0              12700          88
38       6          7           7          3          0          0          0
 0          0              12700          88
39       8          8           8          3          222        3          0
 0          0              12300          92
40       4          5           5          3          3281       20         0
 0          0              13100          84
41       6          7           7          3          0          0          0
 0          0              13100          84
42       8          8           8          3          222        3          0
 0          0              12700          88
43       8          8           8          3          222        3          0
 0          0              12700          88
44       4          5           5          3          3308       21         0
 0          0              13100          84
45       6          7           7          3          0          0          0
 0          0              13100          84
46       8          8           8          3          296        4          0
 0          0              13100          84
47       8          8           8          3          296        4          0
 0          0              13100          84
48       4          5           5          3          73         2          0
 0          0              14500          70
49       6          7           7          3          0          0          0
 0          0              14500          70
50       8          8           8          3          74         1          0
 0          0              14500          70
part3 for sid
sid_entry[1] sid 1 service_class 2 create_time 127 total_octets 8925
sid_entry[2] sid 2 service_class 2 create_time 115 total_octets 3855
sid_entry[3] sid 3 service_class 2 create_time 121 total_octets 1277
sid_entry[4] sid 4 service_class 2 create_time 123 total_octets 3851
sid_entry[5] sid 5 service_class 2 create_time 127 total_octets 3855
sid_entry[6] sid 6 service_class 2 create_time 131 total_octets 3281
sid_entry[7] sid 7 service_class 2 create_time 131 total_octets 3308
sid_entry[8] sid 8 service_class 2 create_time 145 total_octets 73
part4 for cm and cmtx
cm_mac: 68ee.9633.0699, tcsbmp: 0x1, admin_status 1, md_sg_id 0x1510505, rcc_status_id
0x4, rcs_id 0x1520005, tcs_id 0x1 last_reg_time 1444372688, RCP ID:00 10 00 00 10
usch 1, modulation_type 2, rx_power -5, signal_noise 390, time_offset 2085
cm_mac: e448.c70c.96e7, tcsbmp: 0x4, admin_status 1, md_sg_id 0x1510505, rcc_status_id
0x4, rcs_id 0x1520005, tcs_id 0x3 last_reg_time 1444372678, RCP ID:00 10 00 00 08
usch 3, modulation_type 2, rx_power -15, signal_noise 381, time_offset 1785
cm_mac: 0019.474a.c126, tcsbmp: 0x1, admin_status 1, md_sg_id 0x1510505, rcc_status_id
0x0, rcs_id 0x22, tcs_id 0x1 last_reg_time 1444372682, RCP ID:00 00 00 00 00
usch 1, modulation_type 2, rx_power -15, signal_noise 390, time_offset 1792
cm_mac: e448.c70c.982b, tcsbmp: 0x1, admin_status 1, md_sg_id 0x1510505, rcc_status_id
0x4, rcs_id 0x1520005, tcs_id 0x1 last_reg_time 1444372685, RCP ID:00 10 00 00 08
usch 1, modulation_type 2, rx_power -10, signal_noise 390, time_offset 1786
cm_mac: e448.c70c.96d5, tcsbmp: 0x2, admin_status 1, md_sg_id 0x1510505, rcc_status_id
0x4, rcs_id 0x1520005, tcs_id 0x2 last_reg_time 1444372688, RCP ID:00 10 00 00 08
usch 2, modulation_type 2, rx_power -15, signal_noise 381, time_offset 1786
cm_mac: e448.c70c.9819, tcsbmp: 0x1, admin_status 1, md_sg_id 0x1510505, rcc_status_id
```

```
 0x4, rcs_id 0x1520005, tcs_id 0x1 last_reg_time 1444372692, RCP ID:00 10 00 00 08
 usch 1, modulation_type 2, rx_power -10, signal_noise 390, time_offset 1789
 cm_mac: e448.c70c.980d, tcsbmp: 0x4, admin_status 1, md_sg_id 0x1510505, rcc_status_id
 0x4, rcs_id 0x1520005, tcs_id 0x3 last_reg_time 1444372695, RCP ID:00 10 00 00 08
 usch 3, modulation_type 2, rx_power -10, signal_noise 390, time_offset 1783
 cm_mac: e448.c70c.96f3, tcsbmp: 0x1, admin_status 1, md_sg_id 0x1510505, rcc_status_id
 0x4, rcs_id 0x1520005, tcs_id 0x1 last_reg_time 1444372723, RCP ID:00 10 00 00 04
 usch 1, modulation_type 2, rx_power 0, signal_noise 420, time_offset 1798
 part5 for dxif info ifnum 1
 basedata[1][1]: cmstatusindex 2375681, cm_mac 68ee.9633.0699, cm_ip 0x5011961F, cm_ds_if
 59881, cm_us_if 204952
 cmregmode 2, cmmodultype 2, cmdocmode 2
 basedata[1][2]: cmstatusindex 2375682, cm_mac e448.c70c.96e7, cm_ip 0x5011961D, cm_ds_if
 59882, cm_us_if 204954
 cmregmode 2, cmmodultype 2, cmdocmode 2
 basedata[1][3]: cmstatusindex 2375683, cm_mac 0019.474a.c126, cm_ip 0x50119602, cm_ds_if
 59914, cm_us_if 204952
 cmregmode 2, cmmodultype 2, cmdocmode 2
 basedata[1][4]: cmstatusindex 2375684, cm_mac e448.c70c.982b, cm_ip 0x50119612, cm_ds_if
 59881, cm_us_if 204952
 cmregmode 2, cmmodultype 2, cmdocmode 2
 basedata[1][5]: cmstatusindex 2375685, cm_mac e448.c70c.96d5, cm_ip 0x5011960D, cm_ds_if
 59881, cm_us_if 204953
 cmregmode 2, cmmodultype 2, cmdocmode 2
 basedata[1][6]: cmstatusindex 2375686, cm_mac e448.c70c.9819, cm_ip 0x5011961E, cm_ds_if
 59881, cm_us_if 204952
 cmregmode 2, cmmodultype 2, cmdocmode 2
 basedata[1][7]: cmstatusindex 2375687, cm_mac e448.c70c.980d, cm_ip 0x5011961A, cm_ds_if
 59882, cm_us_if 204954
 cmregmode 2, cmmodultype 2, cmdocmode 2
 basedata[1][8]: cmstatusindex 2375688, cm_mac e448.c70c.96f3, cm_ip 0x5011960E, cm_ds_if
 59882, cm_us_if 204952
 cmregmode 2, cmmodultype 2, cmdocmode 2
 part6 uschan for ifnum 1
usport 1 micro_reflections 0 us_snr 390 snmp_sigq_unerroreds 0 snmp_sigq_correcteds 0
  snmp_sigq_uncorrectables 0
usport 2 micro_reflections 0 us_snr 381 snmp_sigq_unerroreds 0 snmp_sigq_correcteds 0
  snmp_sigq_uncorrectables 0
usport 3 micro_reflections 0 us_snr 390 snmp_sigq_unerroreds 0 snmp_sigq_correcteds 0
  snmp_sigq_uncorrectables 0
usport 4 micro_reflections 0 us_snr 0 snmp_sigq_unerroreds 0 snmp_sigq_correcteds 0
snmp_sigq_uncorrectables 0
```

- 指定した Field Replaceable Unit（FRU）の raw ソケット プロセス間通信（IPC）インフラストラクチャ統計情報を表示するには、次の例に示すように **show platform software ios** *slot-id* **socket statistics** コマンドを使用します。

```
Router#show platform software ios R0 socket statistics 0
-------------------------------------------

Session Slot             : 2
Socket FD                : 93
Client ID                : 0
Message Receive Count    : 0
Message Receive Bytes    : 0

-------------------------------------------

Session Slot             : 2
Socket FD                : 93
Client ID                : 1
Message Receive Count    : 30155
Message Receive Bytes    : 1326820

-------------------------------------------

Session Slot             : 3
Socket FD                : 86
Client ID                : 0
Message Receive Count    : 0
Message Receive Bytes    : 0
```

```
-------------------------------------------

Session Slot              : 3
Socket FD                 : 86
Client ID                 : 1
Message Receive Count     : 29611
Message Receive Bytes     : 69782901
```

SNMP バックグラウンド同期の設定例

次に、SNMP バックグラウンド同期を設定する例を示します。

```
enable
configure terminal
cable bgsync active
service internal
cable bgsync itime 200
cable bgsync ptime 500
exit
```

SNMP バックグラウンド同期に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *260*：*SNMP* バックグラウンド同期に関する機能情報

機能名	リリース	機能情報
SNMP バックグラウンド同期	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

第 101 章

オンライン オフライン診断

お客様はオンライン オフライン診断（OOD）フィールド診断機能を使用して、現場に導入されているライン カードのハードウェア関連の問題をテストおよび検証できます。テスト結果に基づき、ライン カードで障害が発生しているかどうかを確認し、ネットワークの問題をトラブルシューティングすることができます。

オンライン オフライン診断の概要

フィールド診断メカニズムであるオンライン オフライン診断を使用すると、お客様はライン カード ハードウェアの問題をテストして検証することができます。

Cisco cBR ユニバーサル ブロードバンド ルータ内のライン カードに関するハードウェア診断テストを実行するには、Cisco.com から無料の OOD フィールド診断イメージをダウンロードし、それを使用して、ライン カードの問題の原因がハードウェア障害にあるかどうかを検証します。お客様はスタンバイ ライン カードに対して随時、サービスを中断することなく、フィールド診断テストを実行できます。スタンバイ ライン カードがスイッチオーバー可能であることを確認することで、システムの高可用性を向上させることができます。

フィールド診断イメージについて

ラインカードに関する診断テストを実行するために使用するフィールド診断イメージは、Cisco.com から入手できます。

まず、Cisco.com から、このイメージをルータ上のいずれかのフラッシュ ファイル システムにダウンロードします。ダウンロードしたイメージをラインカードに移動すると、ラインカードは自動的にオフラインになります。フィールド診断テストを完了してテスト結果を収集した後は、フィールド診断イメージをライン カードからアンロードする必要があります。フィールド診断イ

メージをライン カードからアンロードすると、ライン カードは自動的に通常の動作を再開します。

オンライン オフライン診断の利点

- トラブルシューティングの改善フィールド診断では、ライン カードの問題がハードウェアに関連しているかどうかを検証します。問題がソフトウェアに関連している場合、フィールド診断イメージによってハードウェアが原因でないことがすぐに解明するため、問題の原因となっているソフトウェアの問題を解決することに集中できます。
- **装着前のライン カード ハードウェアの検証**フィールド診断では、Cisco cBR ルータに装着される前のライン カードにハードウェア上の問題があるかどうかを検証します。
- **オンサイトでの障害検出**フィールド診断を利用することで、問題がハードウェアに関連するかどうか、ライン カードを交換する必要があるかどうかを確認できます。
- 稼働時間の増加問題がハードウェアに関連していない場合、フィールド診断によってライン カードを不必要にオフラインにすることを回避できるため、ネットワークの稼働率を向上させることができます。

オンライン オフライン診断機能の前提条件

- N+1 冗長構成内の現用（アクティブ）ライン カードに対して OOD フィールド診断テストを実行するには、サービスの中断を避けるために、フィールド診断イメージをライン カードにロードする前に、保護（スタンバイ）ライン カードへのスイッチオーバーを行うことを推奨します。
- OOD フィールド診断イメージがライン カードにロードされると、ライン カードがオフラインになります。したがって、フィールド診断テストを行う前に、テスト対象のライン カードのダウンタイムをスケジュールしてください。
- フィールド診断テストを行う前に必ず、他のインターフェイスに接続されているすべてのケーブルをデバイスから取り外してください。一部のフィールド診断テストではパケットが接続先デバイスに送信されることがあるため、インターフェイスを接続するケーブルを取り外さないと、受信側インターフェイスのパケット カウンタが増加します。

オンライン オフライン診断機能の制限事項

- OOD フィールド診断テストの実行中に Telnet を使用してルータにアクセスしても、テストの進行状況メッセージが画面に表示されません。
- フィールド診断テストの実行中にスーパバイザ スイッチオーバが発生すると、テストは直ちに停止され、ライン カード上のフィールド診断イメージは自動的にライン カードのランタイム イメージに置き換えられます。
- この機能は、Cisco IOS-XE リリース 3.18.0S 以降の CBR-CCAP-LC-40G ライン カードでサポートされます。

- サービスへの影響を避けるために、一度に 1 つのライン カードに対して OOD を実行することを推奨します。
- 複数のライン カードに対して OOD を実行するには、次のライン カードに OOD イメージをロードする前に 5 分 ～ 10 分の間隔を置いてください。

オンライン オフライン診断の設定方法

フィールド診断テストの設定

フィールド診断イメージをロードしてフィールド診断テストを開始するには、次の手順に従います。

copy *tftp:image-file* **{harddisk: | bootflash: | flash:}**
request platform hardware diagnostic load slot *slot-id image-file* **autostart**

テスト プロセスの検証

フィールド診断テストが実行中であるかどうかを確認するには、次の例に示すように **show platform hardware diagnostic status slot** *slot-id* コマンドを使用します。

```
Router# show platform hardware diagnostic status slot 0
Online Offline Diagnostic Status (P=Passed, F=Failed, U=Untested)
State                 Overall Test Num        Test Done Num          Test Result

--------------------------------------------------------------------------------
Running Auto Test     75                      70                     P:69 F:1 U:5
```

（注） テスト結果に 0 以外のテスト失敗番号が示されている場合は、完全なログをコピーし、Cisco TAC チームに連絡してサポートを求めてください。ログ ファイルの一覧を表示するには、**dir harddisk:ood/** コマンドを使用できます。

ライン カードからのフィールド診断イメージの削除

フィールド診断イメージをアンロードするには、次のように **request platform hardware diagnostic unload slot** *slot-id* コマンドを使用します。

request platform hardware diagnostic unload slot *slot-id*

その後、ライン カードがランタイム イメージにリロードされます。

（注） 診断テストの結果を保持するには、フィールド診断イメージをアンロードする前に、**show platform hardware diagnostic status slot** コマンド出力を別のファイルにコピー アンド ペーストします。ライン カードからフィールド診断イメージをアンロードした後に、**show platform hardware diagnostic status slot** コマンド出力を収集することはできません。

オンライン オフライン診断の設定例

次に、オンライン オフライン診断の実行時の出力例を示します。

```
copy tftp:field_diag harddisk:
request platform hardware diagnostic load slot 0 harddisk:field_diag autostart

Mar 2 16:00:51.933 CST: %IOSXE_OIR-6-REMCARD: Card (cc) removed from slot x
Mar 2 16:00:51.934 CST: %CABLE_CLC-5-LOGGER_LC_REMOVED: Carrier Card x removed
```

オンライン オフライン診断に関する機能情報

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、ソフトウェア イメージがサポートする特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 次の表は、特定のソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースのみを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *261*：オンライン オフライン診断に関する機能情報

機能名	リリース	機能情報
オンライン オフライン診断	Cisco IOS XE Everest 16.6.1	この機能が Cisco cBR シリーズ コンバージド ブロードバンド ルータ上の Cisco IOS XE Everest 16.6.1 に統合されました。

索 引

C

D

E

G

I

M

V

と

ね

ふ

も