



**Cisco ONS 15454/15454 SDH/15327  
イーサネットカードソフトウェアフィーチャ  
コンフィギュレーションガイド**

Cisco IOS Release 12.2(28)SV  
CTC and Documentation Release 7.0



このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

FCC クラス A 適合装置に関する記述：この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス A デジタル装置の制限に適合していることが確認済みです。これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。住宅地でこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。

FCC クラス B 適合装置に関する記述：このマニュアルに記載された装置は、無線周波エネルギーを生成および放射する可能性があります。シスコシステムズの指示する設置手順に従わずに装置を設置した場合、ラジオおよびテレビの受信障害が起こることがあります。この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス B デジタル装置の制限に適合していることが確認済みです。これらの仕様は、住宅地で使用したときに、このような干渉を防止する適切な保護を規定したものです。ただし、特定の設置条件において干渉が起きないことを保証するものではありません。

シスコシステムズの書面による許可なしに装置を改造すると、装置がクラス A またはクラス B のデジタル装置に対する FCC 要件に適合しなくなることがあります。その場合、装置を使用するユーザの権利が FCC 規制により制限されることがあり、ラジオまたはテレビの通信に対するいかなる干渉もユーザ側の負担で矯正するように求められることがあります。

装置の電源を切ることによって、この装置が干渉の原因であるかどうかを判断できます。干渉がなくなれば、シスコシステムズの装置またはその周辺機器が干渉の原因になっていると考えられます。装置がラジオまたはテレビ受信に干渉する場合には、次の方法で干渉が起きないようにしてください。

- ・干渉がなくなるまで、テレビまたはラジオのアンテナの向きを変えます。
- ・テレビまたはラジオの左右どちらかの側に装置を移動させます。
- ・テレビまたはラジオから離れたところに装置を移動させます。
- ・テレビまたはラジオとは別の回路にあるコンセントに装置を接続します（装置とテレビまたはラジオがそれぞれ別個のブレーカーまたはヒューズで制御されるようにします）。

米国シスコシステムズ社では、この製品の変更または改造を認めていません。変更または改造した場合には、FCC 認定が無効になり、さらに製品を操作する権限を失うことになります。

シスコシステムズが採用している TCP ヘッダー圧縮機能は、UNIX オペレーティングシステムの UCB (University of California, Berkeley) パブリックドメイン パッケージの一部として、UCB が開発したプログラムを最適化したものです。All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコシステムズおよびこれら各社は、商品性や特定の目的への適合性、権利を侵害しないことに関する、または取り扱い、使用、または取り引きによって発生する、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその代理店は、このマニュアルの使用またはこのマニュアルを使用できないことによって起こる制約、利益の損失、データの損傷など間接的で偶発的に起こる特殊な損害のあらゆる可能性がシスコシステムズまたは代理店に知らされていても、それらに対する責任を一切負いかねます。

CCSP、CCVP、Cisco Square Bridge のロゴ、Follow Me Browsing、StackWise は、Cisco Systems, Inc. の商標です。Changing the Way We Work, Live, Play, and Learn、iQuick Study は、Cisco Systems, Inc. のサービスマークです。Access Registrar、Aironet、BPX、Catalyst、CCDA、CCDP、CCIE、CCIP、CCNA、CCNP、Cisco、Cisco Certified Internetwork Expert のロゴ、Cisco IOS、Cisco Press、Cisco Systems、Cisco Systems Capital、Cisco Systems のロゴ、Cisco Unity、Enterprise/Solver、EtherChannel、EtherFast、EtherSwitch、Fast Step、FormShare、GigaDrive、GigaStack、HomeLink、Internet Quotient、IOS、IP/TV、iQ Expertise、iQ のロゴ、iQ Net Readiness Scorecard、LightStream、Linksys、MeetingPlace、MGX、Networkers のロゴ、Networking Academy、Network Registrar、Packet、PIX、Post-Routing、Pre-Routing、ProConnect、RateMUX、ScriptShare、SlideCast、SMARTnet、The Fastest Way to Increase Your Internet Quotient、TransPath は、米国および一部の国における Cisco Systems, Inc. または関連会社の登録商標です。

このマニュアルまたは Web サイトで言及している他の商標はいずれも、それぞれの所有者のもので、「パートナー」という用語を使用しているも、シスコシステムズと他社とのパートナー関係を意味するものではありません。(0601R)

Cisco ONS 15454/15454 SDH/15327 イーサネット カード ソフトウェア フィーチャ コンフィギュレーション ガイド

Copyright © 2000–2005 Cisco Systems, Inc.

All rights reserved.



<b>このマニュアルについて</b>	<b>xix</b>
マニュアルの目的	xx
対象読者	xx
マニュアルの構成	xxi
関連資料	xxiii
表記法	xxiv
安全性および警告に関する情報の入手先	xxiv
マニュアルの入手方法	xxv
Cisco.com	xxv
Product Documentation DVD	xxv
シスコ光ネットワーク製品の Documentation CD-ROM	xxv
マニュアルの発注方法	xxv
シスコ製品のセキュリティ	xxvi
シスコ製品のセキュリティ問題の報告	xxvi
テクニカル サポート	xxvii
Cisco Technical Support & Documentation Web サイト	xxvii
Japan TAC Web サイト	xxvii
Service Request ツールの使用	xxviii
問題の重大度の定義	xxviii
その他の資料および情報の入手方法	xxix

---

CHAPTER 1

<b>ML シリーズ カードの概要</b>	<b>1-1</b>
ML シリーズ カードの説明	1-2
ML シリーズ カードの機能一覧	1-3
ML シリーズ カードの主な機能	1-6
Cisco IOS	1-6
DRPRI	1-6
EoMPLS	1-6
GFP-F フレーミング	1-6
リンク集約 (FEC、GEC、および POS)	1-7
RPR	1-7

TL1	1-7
VRF Lite	1-7

CHAPTER 2

**CTC の動作** 2-1

ML シリーズの POS およびイーサネット統計情報の CTC への表示	2-2
ML シリーズイーサネットポートのプロビジョニング情報の CTC への表示	2-3
ML シリーズ POS ポートのプロビジョニング情報の CTC への表示	2-4
フレーミングモードのプロビジョニング	2-5
SONET/SDH アラームの管理	2-5
FPGA 情報の表示	2-6
SONET/SDH 回線のプロビジョニング	2-7
J1 パストレース	2-7

CHAPTER 3

**初期設定** 3-1

ハードウェアの設置	3-2
ML シリーズカード上の Cisco IOS	3-3
CTC を使用して Cisco IOS セッションを開く方法	3-3
ノードの IP アドレスとスロット番号に Telnet 接続する方法	3-4
管理ポートへの Telnet 接続	3-5
ML シリーズの IOS CLI コンソールポート	3-6
RJ-11/RJ-45 コンソールケーブルアダプタ	3-6
PC または端末からコンソールポートへの接続	3-6
スタートアップ コンフィギュレーション ファイル	3-8
シリアル コンソールポートを使用して手動でスタートアップ コンフィギュレーション ファイルを作成する方法	3-9
パスワード	3-9
管理ポートの設定	3-9
ホスト名の設定	3-10
CTC とスタートアップ コンフィギュレーション ファイル	3-11
CTC での Cisco IOS スタートアップ コンフィギュレーション ファイルのロード	3-11
スタートアップ コンフィギュレーション ファイルのデータベースの復元	3-13
複数のマイクロコード イメージ	3-14
使用中のマイクロコード イメージの変更	3-15
Cisco IOS のコマンド モード	3-16
コマンド モードの使用	3-18
終了	3-18
ヘルプの利用方法	3-18

## CHAPTER 4

**インターフェイスの設定** 4-1

- インターフェイスの一般的な注意事項 4-2
  - MAC アドレス 4-2
  - インターフェイス ポート ID 4-3
- インターフェイスの基本設定 4-4
  - ファストイーサネット、ギガビットイーサネット、および POS インターフェイスの基本設定 4-6
    - ファストイーサネット インターフェイスの設定 (ML100T-12) 4-6
    - ファストイーサネット インターフェイスの設定 (ML100X-8) 4-7
    - ギガビットイーサネット インターフェイスの設定 (ML1000-2) 4-8
    - POS インターフェイスの設定 (ML100T-12、ML100X-8、および ML1000-2) 4-9
  - ファストイーサネット インターフェイスとギガビットイーサネット インターフェイスのモニタリング操作 4-11

## CHAPTER 5

**POS の設定** 5-1

- ML シリーズ カード上の POS 5-2
  - ML シリーズの SONET および SDH の回線サイズ 5-2
  - VCAT 5-3
  - SW-LCAS 5-4
  - フレーミング モード、カプセル化、および CRC のサポート 5-4
    - POS インターフェイス フレーミング モード の設定 5-5
    - POS インターフェイス カプセル化タイプの設定 5-5
    - HDLC フレーミングの POS インターフェイス CRC サイズの設定 5-6
    - MTU サイズの設定 5-6
    - キープアライブ メッセージの設定 5-7
  - SONET/SDH アラーム 5-7
    - SONET/SDH アラームの設定 5-7
    - SONET/SDH 遅延トリガーの設定 5-8
  - C2 バイトとスクランブリング 5-9
    - サードパーティ製 POS インターフェイスの C2 バイトおよびスクランブリングの値 5-10
    - SPE スクランブリングの設定 5-10
- POS のモニタリングと確認 5-11
- POS の設定例 5-13
  - ML シリーズ カード間の設定 5-13
  - ML シリーズ カードと Cisco 12000 GSR シリーズ ルータ間の設定 5-14
  - ML シリーズ カードと G シリーズ カード間の設定 5-16
  - ML シリーズ カードと ONS 15310 ML-100T-8 カード間の設定 5-16

CHAPTER 6

**ブリッジの設定**

6-1

基本的なブリッジングの概要	6-2
基本的なブリッジングの設定	6-3
基本的なブリッジングのモニタリングと確認	6-5
トランスペアレント ブリッジング モードの動作	6-6
IP routing モード	6-6
no IP routing モード	6-8
bridge CRB モード	6-8
bridge IRB モード	6-10

CHAPTER 7

**STP および RSTP の設定**

7-1

STP の機能	7-2
STP の概要	7-2
サポートされている STP インスタンス	7-3
BPDU	7-3
ルート スイッチの選出	7-4
ブリッジ ID、スイッチ プライオリティ、および拡張システム ID	7-4
スパニングツリー タイマー	7-5
スパニングツリー トポロジーの形成	7-5
スパニングツリー インターフェイスのステート	7-6
ブロッキング ステート	7-7
リスニング ステート	7-7
ラーニング ステート	7-7
フォワーディング ステート	7-8
ディセーブル ステート	7-8
スパニングツリー アドレスの管理	7-8
STP および IEEE 802.1Q トランク	7-8
スパニングツリーおよび冗長接続	7-8
接続を維持するためのエージングの加速	7-9
RSTP	7-10
サポートされている RSTP インスタンス	7-10
ポートの役割およびアクティブ トポロジー	7-10
高速コンバージェンス	7-11
ポートの役割の同期化	7-13
BPDU の形式と処理	7-14
優位な BPDU 情報の処理	7-14
下位 BPDU 情報の処理	7-15
TC	7-15

IEEE802.1D STP との相互運用性	7-15
STP および RSTP 機能の設定	7-16
STP および RSTP のデフォルト設定	7-16
STP および RSTP のディセーブル化	7-17
ルート スイッチの設定	7-17
ポート プライオリティの設定	7-18
パス コストの設定	7-18
ブリッジ グループのスイッチ プライオリティの設定	7-19
Hello タイムの設定	7-20
ブリッジ グループの転送遅延時間の設定	7-21
ブリッジ グループの最大エージング タイムの設定	7-21
STP および RSTP のステータスの確認とモニタリング	7-22

## CHAPTER 8

**VLAN の設定** 8-1

VLAN の概要	8-2
IEEE 802.1Q VLAN のカプセル化の設定	8-3
IEEE 802.1Q VLAN の設定	8-4
VLAN 動作のモニタリングと確認	8-6

## CHAPTER 9

**IEEE 802.1Q および レイヤ 2 プロトコルのトンネリング設定** 9-1

IEEE 802.1Q トンネリングの概要	9-2
IEEE 802.1Q トンネリングの設定	9-5
IEEE 802.1Q トンネリングおよび他の機能との互換性	9-5
IEEE 802.1Q トンネル ポートの設定	9-5
IEEE 802.1Q の例	9-7
VLAN 透過サービスおよび VLAN 固有サービスの概要	9-8
VLAN 透過サービスおよび VLAN 固有サービスの設定例	9-9
レイヤ 2 プロトコル トンネリングの概要	9-13
レイヤ 2 プロトコル トンネリングの設定	9-14
レイヤ 2 プロトコル トンネリングのデフォルト設定	9-14
レイヤ 2 プロトコル トンネリングの設定に関する注意事項	9-14
ポートのレイヤ 2 トンネリングの設定	9-15
VLAN 単位のレイヤ 2 トンネリングの設定	9-16
トンネリング ステータスのモニタリングと確認	9-16

## CHAPTER 10

**リンク集約の設定** 10-1

リンク集約の概要	10-2
EtherChannel の設定	10-3
EtherChannel の設定例	10-4

POS チャネルの設定	10-6
POS チャネルの設定例	10-7
EtherChannel または POS チャネルでのカプセル化の概要	10-9
EtherChannel または POS チャネルでのカプセル化の設定	10-9
EtherChannel でのカプセル化の例	10-9
EtherChannel と POS のモニタリングと確認	10-12

CHAPTER 11

<b>ネットワーク プロトコルの設定</b>	<b>11-1</b>
IP ルーティング プロトコルの基本設定	11-2
RIP	11-2
EIGRPEIGRP	11-3
OSPF	11-3
BGP	11-4
IP ルーティングのイネーブル化	11-4
IP ルーティングの設定	11-5
RIP の設定	11-5
RIP 認証	11-8
サマリー アドレスとスプリット ホライズン	11-9
OSPF の設定	11-10
OSPF インターフェイス パラメータ	11-14
OSPF エリア パラメータ	11-16
OSPF のその他の動作パラメータ	11-18
LSA グループ ペーシングの変更	11-19
ループバック インターフェイス	11-20
OSPF のモニタリング	11-21
EIGRP の設定	11-21
EIGRP ルータ モード コマンド	11-24
EIGRP インターフェイス モード コマンド	11-25
EIGRP ルート認証の設定	11-26
EIGRP のモニタリングとメンテナンス	11-27
BGP と CIDR	11-28
BGP の設定	11-29
BGP 設定の確認	11-29
IS-IS の設定	11-31
IS-IS 設定の確認	11-32
スタティック ルートの設定	11-33
スタティック ルートのモニタリング	11-34
IP ネットワークのモニタリングとメンテナンス	11-35
IP マルチキャスト ルーティングの概要	11-36

IP マルチキャスト ルーティングの設定	11-37
IP マルチキャスト動作のモニタリングと確認	11-37

## CHAPTER 12

<b>IRB の設定</b>	12-1
IRB の概要	12-2
IRB の設定	12-3
IRB の設定例	12-5
IRB のモニタリングと確認	12-7

## CHAPTER 13

<b>VRF Lite の設定</b>	13-1
VRF Lite の概要	13-2
VRF Lite の設定	13-3
VRF Lite の設定例	13-4
VRF Lite のモニタリングと確認	13-9

## CHAPTER 14

<b>QoS の設定</b>	14-1
QoS の概要	14-2
IP およびイーサネットのプライオリティ メカニズム	14-2
IP 優先順位および DSCP	14-2
イーサネット CoS	14-3
ML シリーズの QoS	14-4
分類	14-5
ポリシング	14-5
ポリシング機能によるマーキングおよび廃棄	14-6
キューイング	14-6
スケジューリング	14-7
制御パケットと L2 トンネリング プロトコル	14-8
出力プライオリティ マーキング	14-8
入力プライオリティ マーキング	14-9
QinQ 実装	14-9
フロー制御ポーズと QoS	14-10
RPR の QoS	14-11
QoS の設定	14-13
トラフィック クラスの作成	14-13
トラフィック ポリシーの作成	14-14
インターフェイスへのトラフィック ポリシーの適用	14-18
CoS ベース QoS の設定	14-18
QoS 設定のモニタリングおよび確認	14-19
QoS の設定例	14-20

トラフィック クラスの定義例	14-20
トラフィック ポリシーの作成例	14-20
class-map match-any および class-map match-all コマンドの例	14-21
match spr1 インターフェイスの例	14-22
ML シリーズの VoIP の例	14-22
ML シリーズのポリシングの例	14-23
ML シリーズの CoS ベース QoS の例	14-23
マルチキャスト QoS およびプライオリティ マルチキャスト キューイングの概要	14-25
デフォルトのマルチキャスト QoS	14-26
マルチキャスト プライオリティ キューイング QoS の制限	14-26
マルチキャスト プライオリティ キューイング QoS の設定	14-27
CoS ベース パケットの統計情報の概要	14-28
CoS ベース パケット統計情報の設定	14-29
IP SLA の概要	14-31
ML シリーズ カードの IP SLA	14-31
ML シリーズ カードでの IP SLA の制限事項	14-31

CHAPTER 15

<b>SDM の設定</b>	15-1
SDM の概要	15-2
SDM 領域の概要	15-2
SDM の設定	15-3
SDM 領域の設定	15-3
TCAM の ACL のサイズ設定	15-3
SDM のモニタリングと確認	15-4

CHAPTER 16

<b>ACL の設定</b>	16-1
ACL の概要	16-2
ML シリーズにおける ACL サポート	16-2
IP ACL	16-2
名前付き IP ACL	16-3
ユーザの注意事項	16-3
IP ACL の作成	16-3
番号付き標準および拡張 IP ACL の作成	16-3
名前付き標準 IP ACL の作成	16-4
名前付き拡張 IP ACL の作成 (制御プレーン専用)	16-5
インターフェイスへの ACL の適用	16-5
ACL TCAM サイズの変更	16-6

## CHAPTER 17

**RPR の設定** 17-1

## RPR の概要 17-2

SONET/SDH 回線の役割 17-2

パケット処理動作 17-2

リング ラッピング 17-3

RPR フレーミング プロセス 17-5

MAC アドレスと VLAN サポート 17-6

RPR QoS 17-6

CTM および RPR 17-6

## RPR の設定 17-7

ML シリーズ カードとポイントツーポイント STS/STM 回線の接続 17-7

RPR の CTC 回線の設定 17-7

RPR の CTC 回線の設定例 17-8

ML シリーズ カード上の RPR 特性と SPR インターフェイスの設定 17-12

ML シリーズ カードの POS ポートの SPR インターフェイスへの割り当て  
17-14ブリッジ グループの作成とイーサネットおよび SPR インターフェイスの割  
り当て 17-16

RPR Cisco IOS の設定例 17-17

RPR イーサネット アクセス ポート間のイーサネット接続の確認 17-19

## RPR のモニタリングおよび確認 17-19

ML シリーズ カードの RPR への追加 17-20

ML シリーズ カードの RPR への追加 17-22

RPR からの ML シリーズ カードの削除 17-25

RPR からの ML シリーズ カードの削除 17-27

## RPR LFP の概要 17-30

LFP シーケンス 17-31

伝播遅延 17-31

## LFP の設定 17-32

LFP の設定要件 17-33

LFP のモニタリングおよび確認 17-33

## デュアル RPR 相互接続の概要 17-34

## DRPRI の設定 17-36

DRPRI IOS の設定例 17-37

DRPRI のモニタリングおよび確認 17-42

## CHAPTER 18

**EoMPLS の設定** 18-1

## EoMPLS の概要 18-2

EoMPLS のサポート 18-3

EoMPLS の制限	18-4
EoMPLS の QoS	18-4
EoMPLS の設定	18-6
EoMPLS 設定の注意事項	18-6
PE-CLE ポート上での VC タイプ 4 設定	18-6
PE-CLE ポート上での VC タイプ 5 設定	18-8
PE-CLE SPR インターフェイスでの EoMPLS 設定	18-10
MPLS クラウドに面しているポートでのブリッジグループ設定	18-10
パケットのプライオリティと EXP の設定	18-11
EoMPLS の設定例	18-12
EoMPLS のモニタリングと確認	18-15

CHAPTER 19

<b>ML シリーズカードのセキュリティ設定</b>	<b>19-1</b>
セキュリティの概要	19-2
ML シリーズカードの コンソール ポートのディセーブル化	19-2
ML シリーズカードへのセキュアなログイン	19-2
ML シリーズカードの SSH	19-3
SSH の概要	19-3
SSH の設定	19-3
設定の注意事項	19-4
SSH を実行するための ML シリーズカードの設定	19-4
SSH サーバの設定	19-5
SSH 設定およびステータスの表示	19-6
ML シリーズカード上の RADIUS	19-7
RADIUS リレー モード	19-7
RADIUS リレー モードの設定	19-8
RADIUS スタンドアロン モード	19-9
RADIUS の概要	19-9
RADIUS の設定	19-10
RADIUS のデフォルト設定	19-10
RADIUS サーバホストの特定	19-10
AAA ログイン認証の設定	19-13
AAA サーバグループの定義	19-15
ユーザイネーブルアクセスおよびネットワーク サービス用の RADIUS 許可の設定	19-17
RADIUS アカウンティングの開始	19-18
RADIUS パケット内の nas-ip-address の設定	19-19
すべての RADIUS サーバに対する設定	19-20
ベンダー固有の RADIUS 属性用の ML シリーズカードの設定	19-20

ベンダー固有の RADIUS サーバ通信の ML シリーズ カードの設定  
19-22

RADIUS 設定の表示 19-23

CHAPTER 20

**ONS イーサネット カード上の POS 20-1**

POS の概要 20-2

POS 相互運用性 20-3

POS カプセル化タイプ 20-5

LEX 20-5

PPP/BCP 20-5

Cisco HDLC 20-6

E シリーズ専用 20-6

POS フレーミング モード 20-7

HDLC フレーミング 20-7

GFP-F フレーミング 20-7

特定の ONS イーサネット カードの POS 特性 20-8

ONS 15327 E-10/100-4 フレーム化オプションとカプセル化オプション  
20-8

ONS 15454 および ONS 15454 SDH E シリーズのフレーム化オプションとカ  
プセル化オプション 20-8

G シリーズのカプセル化およびフレーム化 20-9

ONS 15454、ONS 15454 SDH、ONS 15310-CL、および ONS 15310-MA CE  
シリーズ カードのカプセル化とフレーム化 20-10

ONS 15310 ML-100T-8 のカプセル化およびフレーム化 20-10

ONS 15454 および ONS 15454 SDH ML シリーズ プロトコルのカプセル化お  
よびフレーム化 20-10

イーサネットのクロッキングと SONET/SDH のクロッキング 20-12

CHAPTER 21

**RMON の設定 21-1**

RMON の概要 21-2

RMON の設定 21-3

RMON のデフォルト設定 21-3

RMON アラームおよびイベントの設定 21-3

インターフェイスでのグループ履歴統計情報の収集 21-5

インターフェイスでのグループ イーサネット統計情報の収集 21-6

ML シリーズ カードの CRC エラー スレッシュホールドの概要 21-7

以前のアクションおよびトリガされたアクション 21-7

CRC-ALARM の SONET/GFP 抑制 21-8

CRC-ALARM のクリア 21-8

同期化のラップ解除 21-8

単一方向エラー	21-9
双方向エラー	21-11
ML シリーズ カードの CRC エラー スレッシュホールドの設定	21-14
クリア CRC エラー コマンドを使用した CRC-ALARM ラップの解除	21-15
CRC エラーの ML シリーズ カードの RMON の設定	21-16
ML シリーズ カードの CRC スレッシュホールドの設定の注意事項	21-16
SNMP を通じた CRC エラーへのアクセス	21-16
Cisco IOS を使用した CRC エラー スレッシュホールドの SNMP トラップの設定	21-16
ML シリーズ カードの ifIndex 番号の判別	21-18
ML シリーズ カードでの手動による CRC エラー検証	21-20
RMON ステータスの表示	21-21

CHAPTER 22

**SNMP の設定** 22-1

SNMP の概要	22-2
ML シリーズ カード上の SNMP	22-3
SNMP のバージョン	22-3
SNMP マネージャの機能	22-4
SNMP エージェントの機能	22-4
SNMP コミュニティ スtring	22-5
SNMP による MIB 変数へのアクセス	22-5
サポート対象の MIB	22-6
SNMP 通知	22-6
SNMP の設定	22-7
SNMP のデフォルト設定	22-7
SNMP 設定時の注意事項	22-7
SNMP エージェントのディセーブル化	22-8
コミュニティ スtring の設定	22-8
SNMP グループおよびユーザの設定	22-10
SNMP 通知の設定	22-11
エージェント コンタクトおよびロケーション情報の設定	22-14
SNMP 経由で使用する TFTP サーバの制限	22-14
SNMP の例	22-15
SNMP ステータスの表示	22-16

CHAPTER 23

**E シリーズおよび G シリーズ イーサネットの運用** 23-1

G シリーズのアプリケーション	23-2
G1K-4 カードと G1000-4 カードの比較	23-3
G シリーズ カードの例	23-3

IEEE 802.3z のフロー制御とフレームバッファリング	23-4
GEC/IEEE 802.3ad リンク集約	23-5
イーサネット リンク完全性のサポート	23-6
イーサネット ポートおよび SONET/SDH ポートの管理状態とサービス状態およびソーク時間	23-7
G シリーズ カードの回線構成	23-8
G シリーズ カードのポイントツーポイント イーサネット回線	23-8
G シリーズ カードの手動クロスコネク	23-9
G シリーズ ギガビット イーサネット トランスポンダ モード	23-10
2 ポート双方向トランスポンダ モード	23-12
1 ポート双方向トランスポンダ モード	23-12
2 ポート単方向トランスポンダ モード	23-13
G シリーズ トランスポンダ モードの特性	23-13
E シリーズ カードのアプリケーション	23-15
E シリーズ カードのモード	23-15
E シリーズのマルチカード EtherSwitch グループ	23-15
E シリーズ シングルカード EtherSwitch	23-16
ポートマップ (リニア マッパー)	23-17
E シリーズ モードで使用可能な回線サイズ	23-18
E シリーズ モードで使用可能な合計帯域幅	23-18
E シリーズ カードの IEEE 802.3z フロー制御	23-18
E シリーズの VLAN サポート	23-19
E シリーズ カードの Q タギング (IEEE 802.1Q)	23-20
E シリーズ カードの優先キューイング (IEEE 802.1Q)	23-21
E シリーズのスパニングツリー (IEEE 802.1D)	23-23
E シリーズ カードの複数インスタンス スパニングツリーと VLAN	23-24
回線単位のスパニングツリー	23-24
E シリーズ カードのスパニングツリー パラメータ	23-24
E シリーズ カードのスパニングツリー設定	23-25
E シリーズ カードの回線構成	23-26
E シリーズ カードの回線保護	23-26
E シリーズ カードのポイントツーポイント イーサネット回線	23-27
E シリーズ カードの共有パケット リング イーサネット回線	23-28
E シリーズ カードのハブアンドスポーク イーサネット回線のプロビジョニング	23-28
E シリーズ カードのイーサネット手動クロスコネク	23-29
RMON 仕様アラーム スレッシュホールド	23-30

CHAPTER 24

<b>CE-100T-8 イーサネットの運用</b>	<b>24-1</b>
CE-100T-8 の概要	24-2
CE-100T-8 のイーサネットの機能	24-3
自動ネゴシエーション、フロー制御、およびフレーム バッファリング	24-3
イーサネット リンク完全性のサポート	24-4
イーサネット ポートおよび SONET/SDH ポートの管理状態とサービス状態およびソーク時間	24-5
IEEE 802.1Q CoS および IP ToS キューイング	24-5
RMON および SNMP のサポート	24-7
統計情報およびカウンタ	24-7
CE-100T-8 の SONET/SDH 回線および機能	24-8
利用可能な回線サイズと組み合わせ	24-8
CE-100T-8 プール	24-12
STS/VT 割り当てタブまたは VC4/VC LO 割り当てタブでの CE-100T-8 プール情報の表示	24-12
CE-100T-8 プール割り当ての例	24-13
CE-100T-8 プール プロビジョニング規則	24-14
CE-100T-8 の VCAT の特性	24-14
CE-100T-8 の POS カプセル化、フレーム化、および CRC	24-14
CE-100T-8 のループバック、J1 パストレース、および SONET/SDH アラーム	24-15

CHAPTER 25

<b>CE-1000-4 イーサネットの動作</b>	<b>25-1</b>
CE-1000-4 の概要	25-2
CE-1000-4 イーサネットの機能	25-3
自動ネゴシエーションおよびフレーム バッファリング	25-3
フロー制御	25-3
フロー制御のスレッシュホールド プロビジョニング	25-4
イーサネット リンク完全性のサポート	25-5
イーサネット ポートおよび SONET/SDH ポートの管理状態とサービス状態およびソーク時間	25-5
RMON および SNMP のサポート	25-6
統計情報およびカウンタ	25-6
CE-1000-4 の SONET/SDH 回線および機能	25-7
CE-1000-4 VCAT の特性	25-7
CE-1000-4 の POS カプセル化、フレーム化、および CRC	25-9
CE-1000-4 のループバック、J1 パストレース、および SONET/SDH アラーム	25-9

## APPENDIX A

**コマンド リファレンス A-1**

[no] bridge bridge-group-number protocol {drpri-rstp   ieee   rstp}	A-2
[no] clock auto	A-3
interface spr 1	A-4
[no] ip radius nas-ip-address {hostname   ip-address}	A-5
microcode fail system reload	A-6
[no] pos pdi holdoff time	A-7
[no] pos report alarm	A-8
[non] pos trigger defects condition	A-9
[no] pos trigger delay time	A-10
[no] pos scramble-spe	A-11
[no] pos vcat defect {immediate   delayed}	A-12
[no] pos vcat resequence {enable   disable}	A-13
show controller pos interface-number [details]	A-14
show interface pos interface-number	A-17
show ons alarm	A-18
show ons alarm defect eqpt	A-19
show ons alarm defect port	A-20
show ons alarm defect pos interface-number	A-21
show ons alarm failure eqpt	A-22
show ons alarm failure port	A-22
show ons alarm failure pos interface-number	A-23
spr drpri-id { 0   1 }	A-24
spr-intf-id shared-packet-ring-number	A-25
[no] spr load-balance { auto   port-based }	A-26
spr station-id station-id-number	A-27
spr wrap { immediate   delayed }	A-28
xconnect	A-29

## APPENDIX B

**サポートされていない CLI コマンド B-1**

サポートされていないイネーブル EXEC コマンド	B-1
サポートされていないグローバル コンフィギュレーション コマンド	B-2
サポートされていない POS インターフェイス コンフィギュレーション コマンド	B-4
サポートされていないファースト イーサネットまたはギガビット 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 コマンド	B-6
サポートされていない Port-Channel インターフェイス コンフィギュレーション コマンド	B-7
サポートされていない BVI インターフェイス コンフィギュレーション コマンド	B-8

---

APPENDIX C

**テクニカル サポートの利用方法 C-1**

インターネットワーク情報の収集 C-2

ML シリーズ カードからのデータの取得 C-3

テクニカル サポート担当者へのデータの提供 C-3

---

INDEX

**索引**



## このマニュアルについて

---

ここでは、このマニュアルの目的、対象読者、構成について説明するとともに、本書で使用している表記法、およびその他の情報を記載しています。

ここでは、次の内容について説明します。

- [マニュアルの目的](#)
- [対象読者](#)
- [マニュアルの構成](#)
- [関連資料](#)
- [表記法](#)
- [安全性および警告に関する情報の入手先](#)
- [マニュアルの入手方法](#)
- [シスコ製品のセキュリティ](#)
- [テクニカル サポート](#)
- [その他の資料および情報の入手方法](#)

## マニュアルの目的

このマニュアルでは、Cisco ONS 15454、Cisco ONS 15454 SDH、および Cisco ONS 15327 のイーサネットカードのソフトウェア機能と運用について説明します。また、ML シリーズカードの Cisco IOS ソフトウェアの機能および設定について説明します。ML シリーズカードは、Cisco ONS 15454 SONET または Cisco ONS 15454 SDH システムのモジュールです。さらに、E シリーズカード、G シリーズカード、CE シリーズカードの CTC ソフトウェアの機能および設定についても説明します。E シリーズカードおよび G シリーズカードは、Cisco ONS 15454、Cisco ONS 15454 SDH、および Cisco ONS 15327 のモジュールです。CE シリーズカードは、Cisco ONS 15454 のモジュールです。また、CE-100T-8 カードは Cisco ONS 15310-CL のモジュールとしても使用できます。Cisco ONS 15310-CL バージョンのカードについては、ONS 15310-CL の『*Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide*』を参照してください。このマニュアルは、[関連資料](#)に記載されている適切なマニュアルと併せて使用してください。

## 対象読者

このマニュアルの ML シリーズカードに関する章の使用に際しては、Cisco IOS を十分に理解していることが必要となります。また、ネットワーキングの技術的な基礎知識と経験があることが望まれます。このマニュアルの E シリーズカード、G シリーズカード、および CE シリーズカードに関する章の使用に際しては、CTC を十分に理解していることが必要となります。また、ネットワーキングの技術的な基礎知識と経験があることが望まれます。

## マニュアルの構成

この『Cisco ONS 15454/15454 SDH/15327 イーサネットカードソフトウェアフィーチャコンフィギュレーションガイド』は、次の章で構成されています。

- **第1章「MLシリーズカードの概要」**では、MLシリーズカード、機能一覧、主要機能について説明します。
- **第2章「CTCの動作」**では、MLシリーズカードでCisco Transport Controller (CTC)ソフトウェアを使用するための詳細と手順について説明します。
- **第3章「初期設定」**では、MLシリーズカードにアクセスし、起動設定ファイルを作成および管理するための手順について説明します。
- **第4章「インターフェイスの設定」**では、MLシリーズカードのインターフェイスの詳細および基本手順について説明します。
- **第5章「POSの設定」**では、MLシリーズカードのPOSインターフェイスの詳細および高度な手順について説明します。
- **第6章「ブリッジの設定」**では、MLシリーズカードのブリッジングの例および手順について説明します。
- **第7章「STPおよびRSTPの設定」**では、MLシリーズカードのスパニングツリーと高速スパニングツリーの例、および手順について説明します。
- **第8章「VLANの設定」**では、MLシリーズカードのVLAN (仮想LAN) の例および手順について説明します。
- **第9章「IEEE 802.1Qおよびレイヤ2プロトコルのトンネリング設定」**では、MLシリーズカードのトンネリングの例および手順について説明します。
- **第10章「リンク集約の設定」**では、MLシリーズカードのEtherChannelとPacket-over-SONET/SDH (POS) チャンネルの例、および手順について説明します。
- **第11章「ネットワークプロトコルの設定」**では、MLシリーズカードのネットワークプロトコルの例および手順について説明します。
- **第12章「IRBの設定」**では、MLシリーズカードのIntegrated Routing and Bridging (IRB; 統合ルーティングおよびブリッジング) の例および手順について説明します。
- **第13章「VRF Liteの設定」**では、MLシリーズカードのVPN Routing and Forwarding Lite (VRF Lite) の例および手順について説明します。
- **第14章「QoSの設定」**では、MLシリーズカードのQuality of Service (QoS; サービス品質) の例および手順について説明します。
- **第15章「SDMの設定」**では、MLシリーズカードのスウィッチングデータベースマネージャの例および手順について説明します。
- **第16章「ACLの設定」**では、MLシリーズカードのAccess Control List (ACL; アクセス制御リスト) の例および手順について説明します。
- **第17章「RPRの設定」**では、MLシリーズカードのResilient Packet Ring (RPR; 復元パケットリング) の例および手順について説明します。
- **第18章「EoMPLSの設定」**では、MLシリーズカードのEthernet over Multiprotocol Label Switching (EoMPLS) の例および手順について説明します。
- **第19章「MLシリーズカードのセキュリティ設定」**では、MLシリーズカードのセキュリティ機能について説明します。
- **第20章「ONS イーサネットカード上のPOS」**では、イーサネットカード上のPOSについて詳細に説明します。また、イーサネットカードの相互運用性についても詳細に説明します。
- **第21章「RMONの設定」**では、MLシリーズカード上でのRemote Network Monitoring (RMON) の設定方法について説明します。
- **第22章「SNMPの設定」**では、MLシリーズカードとSNMP (簡易ネットワーク管理プロトコル) を連携させるための設定方法について説明します。

- 第 23 章「E シリーズおよび G シリーズイーサネットの運用」では、ONS 15454、ONS 15454 SDH、ONS 15327 プラットフォームでの E シリーズおよび G シリーズイーサネットカードの機能と運用について詳細に説明します。
- 第 24 章「CE-100T-8 イーサネットの運用」では、CE-100T-8 イーサネットカードの機能と運用について詳細に説明します。
- 第 25 章「CE-1000-4 イーサネットの動作」では、CE-1000-4 カードの運用について説明します。
- 付録 A「コマンドリファレンス」では、ML シリーズカード固有の Cisco IOS コマンドをアルファベット順に記載し、各コマンドの定義と例について説明します。
- 付録 B「サポートされていない CLI コマンド」では、ML シリーズカードでサポートされていない Cisco IOS コマンドを分類し、アルファベット順に記載しています。
- 付録 C「テクニカルサポートの利用方法」では、ML シリーズカードで問題が発生した場合に、シスコの Technical Assistance Center (TAC) を利用する方法について説明します。

## 関連資料

この『Cisco ONS 15454/15454 SDH/15327 イーサネットカードソフトウェアフィーチャコンフィギュレーションガイド』は、次の ONS 15454 または ONS 15454 SDH システムの一般的なマニュアルと併せて使用してください。

- 『Cisco ONS 15454 Procedure Guide』  
Cisco ONS 15454 ノードとネットワークの設置、ターンアップ、プロビジョニング、および保守の方法について説明しています。
- 『Cisco ONS 15454 SDH Procedure Guide』  
Cisco ONS 15454 SDH ノードとネットワークの設置、ターンアップ、プロビジョニング、および保守の方法について説明しています。
- 『Cisco ONS 15454 Reference Manual』  
カードの詳細仕様、ハードウェアおよびソフトウェア機能の説明、ネットワークトポロジー情報、およびネットワーク要素のデフォルトについて説明します。
- 『Cisco ONS 15454 SDH Reference Manual』  
カードの詳細仕様、ハードウェアおよびソフトウェア機能の説明、ネットワークトポロジー情報、およびネットワーク要素のデフォルトについて説明します。
- 『Cisco ONS 15454 Troubleshooting Guide』  
アラームの説明、アラームおよび一般的なトラブルシューティング手順、エラーメッセージ、パフォーマンスモニタリングと SNMP パラメータについて説明します。
- 『Cisco ONS 15454 SDH Troubleshooting Guide』  
一般的なトラブルシューティング手順、アラームの説明とトラブルシューティング手順、エラーメッセージ、およびパフォーマンスモニタリングと SNMP パラメータに関する情報を提供します。
- 『Cisco ONS SONET TL1 Command Guide』  
Cisco ONS 15454、ONS 15327、ONS 15600、ONS 15310-CL、および ONS 15310-MA システムのパラメータ、AID、条件、修飾子などの、すべての TL1 コマンドおよび自律メッセージセットについて説明します。
- 『Cisco ONS 15454 SDH TL1 Command Guide』  
Cisco ONS 15454 SDH のパラメータ、AID、条件、修飾子などの、すべての TL1 コマンドおよび自律メッセージセットについて説明します。
- 『Cisco ONS SONET TL1 Reference Guide』  
Cisco ONS 15454、ONS 15327、ONS 15600、ONS 15310-CL、および Cisco ONS 15310-MA システムにおける、TL1 の一般的な情報、手順、エラーについて説明します。
- 『Cisco ONS 15454 SDH TL1 Reference Guide』  
Cisco ONS 15454 SDH における、TL1 の一般的な情報、手順、エラーについて説明します。
- 『Release Notes for the Cisco ONS 15454 Release 7.0』  
注意事項、すでに終了した問題、新機能の情報を提供します。
- 『Release Notes for the Cisco ONS 15454 SDH Release 7.0』  
注意事項、すでに終了した問題、新機能の情報を提供します。
- 『Release Notes for the Cisco ONS 15327 Release 7.0』  
注意事項、すでに終了した問題、新機能の情報を提供します。

ML シリーズカードでは、Cisco IOS の Modular QoS CLI (MQC; モジュラ QoS コマンドラインインターフェイス) を使用します。MQC の一般的な設定の詳細については、次の Cisco IOS のマニュアルを参照してください。

- Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2
- Cisco IOS Quality of Service Solutions Command Reference, Release 12.2

ML シリーズカードでは、Cisco IOS 12.2 を使用します。Cisco IOS 12.2 に関する一般的な情報については、次の URL に掲載されているさまざまな Cisco IOS マニュアルを参照してください。

- <http://www.cisco.com/>

## 表記法

このマニュアルでは、次の表記法を使用しています。

表記	適用
太字	コマンドおよびキーワードは、 <b>太字</b> で示しています。
イタリック体	ユーザの入力する引数はイタリック体で示しています。
[ ]	角カッコ内のキーワードや引数は、省略可能です。
{ x   x   x }	必須キーワード (左の表記法では x) は、波カッコで囲み、縦棒で区切って示しています。必ずどれか 1 つを選択する必要があります。
Ctrl	Ctrl キーを表します。たとえば、Ctrl+D と書いてある場合は、Ctrl キーを押しながら D キーを押すことを意味します。
screen フォント	画面に表示される情報は、screen フォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、 <b>太字の screen</b> フォントで示しています。
< >	モジュール固有のコードで置き換える必要があるコマンド パラメータを示しています。



(注)

「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。



注意

「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。



警告

安全上の重要事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。

これらの注意事項を保存しておいてください。

## 安全性および警告に関する情報の入手先

安全情報と警告情報については、本製品に付属している『Cisco Optical Transport Products Safety and Compliance Information』を参照してください。このマニュアルでは、Cisco ONS 15xxx システムの国際機関に対する準拠性と安全性について説明しています。また、ONS 15xxx システムのマニュアルに記載されている安全性に関する警告の各国語訳も記載されています。

## マニュアルの入手方法

シスコ製品のマニュアルおよびその他の資料は、Cisco.com で入手することができます。また、テクニカル サポートおよびその他のテクニカル リソースは、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

### Cisco.com

シスコの最新のマニュアルは、次の URL からアクセスしてください。

<http://www.cisco.com/techsupport>

シスコの Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com>

<http://www.cisco.com/jp>

シスコの Web サイトの各国語版へは、次の URL からアクセスしてください。

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

### Product Documentation DVD

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Product Documentation DVD パッケージでご利用いただけます。Product Documentation DVD は定期的に更新されるので、印刷資料よりも新しい情報が得られます。

Product Documentation DVD は、ポータブル メディアに収容された、技術的な製品マニュアルの総合的なライブラリです。この DVD を使用すると、シスコ製品の各種バージョンのハードウェアのインストール、ソフトウェアのインストール、設定、およびコマンドに関するガイドにアクセスし、HTML で技術マニュアルを表示できます。DVD を使用することで、インターネットに接続しなくてもシスコの Web サイトと同じマニュアルを参照できます。製品によっては、マニュアルの PDF バージョンも用意されています。

Product Documentation DVD は単一製品として、またはサブスクリプションとして入手できます。Cisco.com (Cisco Direct Customers) に登録されている場合、Cisco Marketplace から Product Documentation DVD (Customer Order Number DOC-DOCDVD=) を発注できます。次の URL にアクセスしてください。

<http://www.cisco.com/go/marketplace/>

### シスコ光ネットワーク製品の Documentation CD-ROM

Cisco ONS 15xxx 製品のマニュアルを含む、光ネットワーク関連のマニュアルは、製品に付属の CD-ROM パッケージでご利用いただけます。光ネットワーク製品の Documentation CD-ROM は、定期的に更新されるので、印刷資料よりも新しい情報が得られます。

### マニュアルの発注方法

Cisco.com に登録されている場合、2005 年 6 月 30 日から、次の URL にある Cisco Marketplace の Product Documentation Store でシスコ製品のマニュアルを発注できます。

<http://www.cisco.com/go/marketplace/>

Cisco.com に登録されていない場合、製品を購入された代理店へお問い合わせください。

## シスコ製品のセキュリティ

シスコでは、無償の Security Vulnerability Policy ポータルを次の URL で提供しています。

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

このサイトから、以下のタスクを実行できます。

- シスコ製品における脆弱性を報告する。
- シスコ製品のセキュリティ問題に対する支援を受ける。
- シスコからのセキュリティ情報を入手するために登録を行う。

シスコ製品に関するセキュリティ勧告および注意のリストが以下の URL で確認できます。

<http://www.cisco.com/go/psirt>

勧告および注意事項が変更された際に、リアルタイムで確認したい場合は、以下の URL から Product Security Incident Response Team Really Simple Syndication ( PSIRT RSS ) にアクセスできます。

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## シスコ製品のセキュリティ問題の報告

シスコでは、安全な製品を提供することを目指しています。製品のリリース前に社内でテストを実施し、すべての脆弱性を迅速に修正するように努めております。お客様がシスコ製品の脆弱性を発見したと思われる場合は、次の PSIRT にご連絡ください。

- 緊急度の高い問題 [security-alert@cisco.com](mailto:security-alert@cisco.com)  
緊急度の高い問題とは、システムが激しい攻撃を受けている状態、または急を要する深刻なセキュリティの脆弱性を報告する必要がある状態を指します。それ以外の状態はすべて、緊急度の低い問題とみなされます。
- 緊急度の低い問題 [psirt@cisco.com](mailto:psirt@cisco.com)

緊急度の高い問題の場合、次の電話番号で PSIRT に問い合わせることができます。

- 1 877 228-7302
- 1 408 525-6532



### ヒント

お客様が第三者に知られたいくない情報をシスコに送信する場合、Pretty Good Privacy ( PGP ) または PGP と互換性のある製品を使用して情報を暗号化することを推奨します。PSIRT は、PGP バージョン 2.x ~ 8.x と互換性のある暗号化情報を取り扱うことができます。

無効な暗号鍵または失効した暗号鍵は使用しないでください。PSIRT と通信する際は、次の URL にある Security Vulnerability Policy ページの Contact Summary にリンクされている有効な公開鍵を使用してください。

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.htm](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.htm)

このページのリンクに、現在使用されている PGP 鍵の ID があります。

## テクニカル サポート

Cisco Technical Support では、評価の高い 24 時間体制のテクニカル サポートを提供しています。Cisco.com の Cisco Technical Support & Documentation Web サイトでは、広範囲にわたるオンラインでのサポート リソースを提供しています。さらに、シスコシステムズとサービス契約を結んでいる場合は、Technical Assistance Center (TAC) のエンジニアによる電話サポートも提供されます。シスコシステムズとサービス契約を結んでいない場合は、リセラーにお問い合わせください。

### Cisco Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation Web サイトでは、オンラインで資料やツールを利用して、トラブルシューティングやシスコ製品およびテクノロジーに関する技術上の問題の解決に役立てることができます。この Web サイトは 24 時間ご利用いただけます。次の URL にアクセスしてください。

<http://www.cisco.com/techsupport>

Cisco Technical Support & Documentation Web サイト上のツールにアクセスする際は、いずれも Cisco.com のログイン ID およびパスワードが必要です。サービス契約が有効で、ログイン ID またはパスワードを取得していない場合は、次の URL で登録手続きを行ってください。

<http://tools.cisco.com/RPF/register/register.do>



(注)

テクニカル サポートにお問い合わせいただく前に、Cisco Product Identification (CPI) ツールを使用して、製品のシリアル番号をご確認ください。CPI ツールへは、Documentation & Tools の下にある **Tools & Resources** リンクをクリックして、Cisco Technical Support & Documentation Web サイトからアクセスできます。Alphabetical Index ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下にある **Cisco Product Identification Tool** リンクをクリックしてください。CPI ツールは、製品 ID またはモデル名、ツリー表示、または特定の製品に対する show コマンド出力のコピー & ペーストによる 3 つの検索オプションを提供します。検索結果には、シリアル番号のラベルの場所がハイライトされた製品の説明図が表示されます。テクニカル サポートにお問い合わせいただく前に、製品のシリアル番号のラベルを確認し、メモなどに控えておいてください。

### Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト (<http://www.cisco.com/tac>) のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com/jp/go/tac>

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。

Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

<http://www.cisco.com/jp/register/>

## Service Request ツールの使用

オンラインの TAC Service Request ツールを使えば、S3 および S4 の問題について最も迅速にテクニカルサポートを受けられます(ネットワークの障害が軽微である場合、あるいは製品情報が必要な場合)。状況をご説明いただくと、TAC Service Request が推奨される解決方法を自動的に提供します。これらの推奨リソースを使用しても問題が解決しない場合は、シスコの技術者が問題を診断します。TAC Service Request ツールは次の URL からアクセスできます。

<http://www.cisco.com/techsupport/servicerequest>

問題が S1 または S2 であるか、インターネットにアクセスできない場合は、電話で TAC にご連絡ください(運用中のネットワークがダウンした場合、あるいは重大な障害が発生した場合)。S1 および S2 の問題にはシスコの技術者がただちに対応し、業務を円滑に運営できるよう支援します。

電話でテクニカルサポートを受ける際は、次の番号のいずれかをご使用ください。

アジア太平洋：+61 2 8446 7411 (オーストラリア：1 800 805 227)

EMEA：+32 2 704 55 55

米国：1 800 553-2447

TAC の連絡先一覧については、次の URL にアクセスしてください。

<http://www.cisco.com/techsupport/contacts>

## 問題の重大度の定義

すべての問題を標準形式で報告するために、問題の重大度を定義しました。

**重大度 1 (S1)** ネットワークがダウンし、業務に致命的な損害が発生する場合。24 時間体制であらゆる手段を使用して問題の解決にあたります。

**重大度 2 (S2)** ネットワークのパフォーマンスが著しく低下、またはシスコ製品のパフォーマンス低下により業務に重大な影響がある場合。通常の業務時間内にフルタイムで問題の解決にあたります。

**重大度 3 (S3)** ネットワークのパフォーマンスが低下しているが、ほとんどの業務運用が機能している場合。通常の業務時間内にサービスの復旧を行います。

**重大度 4 (S4)** シスコ製品の機能、インストレーション、基本的なコンフィギュレーションについて、情報または支援が必要で、業務への影響がほとんどまたはまったくない場合。

## その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手することができます。

- Cisco Marketplace では、さまざまなシスコの書籍、参考資料、マニュアル、およびロゴ入り商品を提供しています。Cisco Marketplace には、次の URL からアクセスしてください。

<http://www.cisco.com/go/marketplace/>

- Cisco Press では、ネットワーク、トレーニング、認定関連の出版物を幅広く発行しています。初心者から上級者まで、さまざまな読者向けの出版物があります。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

<http://www.ciscopress.com>

- 『Packet』は、シスコシステムズが発行するテクニカル ユーザ向けの季刊誌で、インターネットやネットワークへの投資を最大限に活用するのに役立ちます。『Packet』には、ネットワーク分野の最新動向、テクノロジーの進展、およびシスコの製品やソリューションに関する記事をはじめ、ネットワークの配置やトラブルシューティングのヒント、設定例、お客様の事例研究、認定やトレーニングに関する情報、および多数の詳細なオンライン リソースへのリンクが盛り込まれています。『Packet』には、次の URL からアクセスしてください。

<http://www.cisco.com/packet>

- 『iQ Magazine』は、シスコのテクノロジーを使って収益の増加、ビジネス効率の向上、およびサービスの拡大を図る方法について学ぶことを目的とした、シスコシステムズが発行する成長企業向けの季刊誌です。この季刊誌は、実際の事例研究や事業戦略を用いて、これら企業が直面するさまざまな課題や、問題解決の糸口となるテクノロジーを明確化し、テクノロジーの投資に関して読者が正しい決断を行う手助けをします。『iQ Magazine』には、次の URL からアクセスしてください。

<http://www.cisco.com/go/iqmagazine>

または次の URL でデジタル版をご覧ください。

<http://ciscoiq.texterity.com/ciscoiq/sample/>

- 『Internet Protocol Journal』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコシステムズが発行する季刊誌です。『Internet Protocol Journal』には、次の URL からアクセスしてください。

<http://www.cisco.com/ipj>

- シスコシステムズが提供するネットワーク製品およびカスタマー サポート サービスについては、次の URL にアクセスしてください。

<http://www.cisco.com/en/US/products/index.html>

- Networking Professionals Connection は、ネットワーキング専門家がネットワーキング製品やネットワーキング技術に関する質問、提案、情報をシスコの専門家および他のネットワーキング専門家と共有するためのインタラクティブな Web サイトです。ディスカッションに参加するには、次の URL にアクセスしてください。

<http://www.cisco.com/discuss/networking>

- シスコシステムズは最高水準のネットワーク関連のトレーニングを実施しています。トレーニングの最新情報については、次の URL からアクセスしてください。

<http://www.cisco.com/en/US/learning/index.html>





# ML シリーズ カードの概要

---

この章では、ONS 15454 (SONET) および ONS 15454 SDH 向けの ML1000-2 カード、ML100T-12 カード、および ML100X-8 カードの概要を説明します。また、イーサネットと SONET/SDH の機能、および Cisco IOS ソフトウェアと Cisco Transport Controller (CTC) ソフトウェアの機能を紹介し、一部の機能を簡単に説明します。

この章の内容は次のとおりです。

- [ML シリーズ カードの説明 \(p.1-2\)](#)
- [ML シリーズ カードの機能一覧 \(p.1-3\)](#)
- [ML シリーズ カードの主な機能 \(p.1-6\)](#)

## ML シリーズカードの説明

ML シリーズカードは、最大処理速度が 5.7 Mpps の、独立したギガビット イーサネット( ML1000-2 ) またはファスト イーサネット ( ML100T-12 および MT100X-8 ) レイヤ 3 スイッチです。これらのカードは、ONS 15454 SONET または ONS 15454 SDH に統合されています。10 ギガビット クロスコネクタ(XC10G または XC-VXC-10G)カードを使用する ONS 15454 SONET では、どのトラフィックカード スロットにも ML シリーズカードを取り付けることができます。ただし、Cross-Connect (XC; クロスコネクタ) カードまたは Cross-Connect Virtual Tributary (XCVT; クロスコネクタ仮想トリビュタリ) カードを使用する ONS 15454 SONET では、4 つのトラフィックカード スロットにしか ML シリーズカードを取り付けることができません。ONS 15454 SDH では、使用する XC カードに関係なく、どのトラフィックカード スロットにも ML シリーズカードを取り付けることができます。

ML シリーズカードは、Cisco IOS Release 12.2(28)SV を使用し、ML シリーズカードでの主なユーザインターフェイスは Cisco IOS CLI (コマンドライン インターフェイス) です。ほとんどの ML シリーズカードの設定 (イーサネット ポート、ブリッジング、VLAN [ 仮想 LAN ] など) では、Cisco IOS CLI のみが使用可能です。

ただし、ONS 15454 SONET/SDH の GUI (グラフィカル ユーザインターフェイス) である CTC でも ML シリーズカードがサポートされます。SONET/SDH 回線は、Cisco IOS からプロビジョニングできませんが、CTC または TL1 から設定する必要があります。CTC では、ML シリーズカードのステータス情報の表示、SONET/SDH のアラーム管理、Cisco IOS Telnet セッションの初期化、Cisco IOS 設定ファイルの管理、プロビジョニング、インベントリなどの標準機能を使用できます。

ML100T-12 には、12 個の RJ-45 インターフェイスが装備されています。また、ML100X-8 および ML1000-2 には、Short Wavelength (SX; 短波長) 光モジュールと Long Wavelength (LX; 長波長) 光モジュールをサポートする 2 つの Small Form-Factor Pluggable (SFP) スロットが装備されています。3 つのカードでは、ハードウェアとソフトウェアに同じ基盤を使用しており、同じフィーチャセットが提供されます。カードの仕様の詳細については、『Cisco ONS 15454 Reference Manual』または『Cisco ONS 15454 SDH Reference Manual』の「Ethernet Cards」の章を参照してください。

ML シリーズカードには、OC-N カードポートと同様に機能する 2 つの仮想 Packet over SONET/SDH (POS) ポートが装備されています。SONET/SDH 回線は、標準の OC-N カード回線と同様に CTC でプロビジョニングできます。ML シリーズカードの POS ポートでは、SONET/SDH 回線の Virtual Concatenation (VCAT; バーチャル コンカチネーション) と Software Link Capacity Adjustment Scheme (SW-LCAS; ソフトウェア リンク キャパシティ 調整方式) がサポートされます。

## ML シリーズカードの機能一覧

ML シリーズカードには次のような機能があります。

- レイヤ 1 データ機能
  - 10/100BASE-TX 半二重および全二重データ転送 (ML100T-12)
  - Auto-MDIX を使用した 100BASE-FX 全二重データ伝送 (ML 100X-8)
  - 1000BASE-SX、1000BASE-LX 全二重データ転送 (ML1000-2)
  - IEEE 802.3z(ギガビットイーサネット)および 802.3x(ファストイーサネット)フロー制御
- SONET/SDH の機能
  - POS 向けの High-level Data Link Control (HDLC; ハイレベル データリンク制御) または frame-mapped Generic Framing Procedure( GFP-F; ジェネリック フレーミング プロシージャ) フレーミング メカニズム
  - 2つの POS 仮想ポート
  - POS 向けの LEX、Cisco HDLC、または PPP/Bridging Control Protocol (PPP/BCP; ポイントツーポイント プロトコル/ブリッジ制御プロトコル) カプセル化
  - VCAT と SW-LCAS
- レイヤ 2 ブリッジング機能
  - トランスペアレント ブリッジング
  - ハードウェアによる MAC (メディア アクセス制御) アドレス学習、エージング、およびスイッチング
  - プロトコルのトンネリング
  - Multiple Spanning Tree (MST) プロトコルのトンネリング
  - 最大 255 個のアクティブブリッジグループ
  - 1 カード当たり最大 60,000 個の MAC アドレス、および 1 ブリッジグループ当たり最大 8,000 個の MAC アドレス
  - Integrated Routing and Bridging (IRB; 統合ルーティングおよびブリッジング)
  - IEEE 802.1P/Q ベースの VLAN トランッキング
  - IEEE 802.1Q VLAN トランッキング
  - IEEE 802.1D Spanning Tree Protocol (STP; スパニング ツリー プロトコル) と IEEE 802.1W Rapid Spanning Tree Protocol (RSTP; 高速スパニング ツリー プロトコル)
  - 1 つのブリッジグループ当たり 1 つの IEEE 802.1D STP インスタンス
  - Resilient Packet Ring (RPR; 復元パケットリング)
  - Dual RPR Interconnect (DRPRI; 二重復元パケットリング相互接続)
  - Ethernet over Multiprotocol Label Switching (EoMPLS)
  - VLAN 透過サービス、および VLAN 固有のサービス (Ethernet Relay Multipoint Service [ERMS; イーサネットリレー マルチポイントサービス])
- Fast EtherChannel (FEC) の機能 (ML100T-12 および ML100X-8)
  - 最大 4 つのファストイーサネットポートのバンドル
  - 送信元 IP アドレスと宛先 IP アドレスに基づくユニキャストパケットのロードシェアリング
  - MAC アドレスに基づくブリッジトラフィックのロードシェアリング
  - IRB
  - IEEE 802.1Q トランッキング
  - アクティブ FEC ポートチャネル (ML100T-12 で最大 6 つ、ML100X-8 で最大 4 つ)
- Gigabit EtherChannel (GEC) の機能 (ML1000-2)
  - 2つのギガビットイーサネットポートのバンドル

- MAC アドレスに基づくブリッジ トラフィックのロード シェアリング
- IRB
- IEEE 802.1Q トランキング
- POS チャンネル
  - 2つの POS ポートのバンドル
  - LEX カプセル化のみ
  - IRB
  - IEEE 802.1Q トランキング
- レイヤ 3 ルーティング、スイッチング、および転送
  - デフォルト ルート
  - IP のユニキャスト転送とマルチキャスト転送
  - 簡易 IP Access Control List (ACL; アクセス制御リスト)(レイヤ 2 とレイヤ 3 の転送パス)
  - ソフトウェアの拡張 IP ACL (制御プレーンのみ)
  - イーサネット ポート間の IP、および IP マルチキャスト ルーティングとスイッチング
  - Reverse Path Forwarding(RPF; リバース パス転送)マルチキャスト(RPF ユニキャスト以外)
  - 送信元と宛先の IP アドレスに基づく等コスト パス間のロード バランシング
  - 最大 18,000 個の IP ルート
  - 最大 20,000 個の IP ホスト エントリ
  - 最大 40 個の IP マルチキャスト グループ
  - IRB ルーティング モードのサポート
- サポートされるルーティング プロトコル
  - Virtual Private Network (VPN; 仮想私設網) Routing and Forwarding Lite (VRF Lite)
  - Intermediate System-to-Intermediate System (IS-IS) プロトコル
  - Routing Information Protocol (RIP; ルーティング情報プロトコル) と RIP II
  - Enhanced Interior Gateway Routing Protocol (EIGRP)
  - Open Shortest Path First (OSPF) プロトコル
  - Protocol Independent Multicast(PIM; プロトコル独立型マルチキャスト) 疎モード、疎/密モード、密モード
  - セカンダリ アドレッシング
  - スタティック ルート
  - ローカル プロキシ ARP
  - Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル)
  - Classless Interdomain Routing (CIDR; クラスレス ドメイン内ルーティング)
- Quality of Service (QoS; サービス品質) の機能
  - マルチキャスト プライオリティ キューイング クラス
  - 1 Mbps 単位の Service Level Agreement (SLA; サービス レベル契約)
  - 入力ポリシング
  - 保証帯域幅 (Weighted Round-Robin [WDRR; 重み付きラウンド ロビン] と完全優先スケジューリング)
  - ユニキャスト Voice-over-IP (VoIP) 用の低遅延キューイング サポート
  - レイヤ 2 プライオリティに基づく Class of Service (CoS; サービス クラス)、VLAN ID、レイヤ 3 Type of Service (ToS; サービス タイプ)/DiffServ Code Point (DSCP; DiffServ コードポイント) およびポート
  - CoS ベースのパケット統計

- Cisco IP SLA (従来の Cisco Service Assurance Agent) を使用した IP SLA ネットワーク モニタリング
- セキュリティ機能
  - Cisco IOS ログイン機能強化
  - Secure Shell (SSH; セキュア シェル) 接続 (SSH バージョン 2)
  - コンソール ポートの無効化
  - Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントिंग) /Remote Authentication Dial-In User Service (RADIUS) (AAA/RADIUS) スタンドアロン モード
  - AAA/RADIUS リレー モード
- その他のプロトコル
  - イーサネット ポートでの Cisco Discovery Protocol (CDP) サポート
  - Dynamic Host Configuration Protocol (DHCP; ダイナミック ホスト コンフィギュレーション プロトコル) リレー
  - 10/100 イーサネット、ギガビット イーサネット、FEC、GEC、および Bridge Group Virtual Interface (BVI; ブリッジ グループ 仮想 インターフェイス) 上での Hot Standby Router Protocol (HSRP; ホットスタンバイ ルータ プロトコル)
  - Internet Control Message Protocol (ICMP; インターネット制御メッセージ プロトコル)
- 管理機能
  - Cisco IOS
  - CTC
  - Remote Monitoring (RMON)
  - SNMP (簡易ネットワーク管理プロトコル)
  - Transaction Language 1 (TL1; トランザクション言語 1)
- システムの機能
  - 自動 Field Programmable Gate Array (FPGA) アップグレード
  - Network Equipment Building Systems 3 (NEBS3) 準拠
  - 複数のマイクロコード イメージ
- CTC の機能
  - フレーミング モードのプロビジョニング
  - POS 仮想ポート向けの標準 STS/STM 回線と VCAT 回線
  - SONET/SDH アラーム レポート (パス アラームなどの ML シリーズ カードに固有のアラーム)
  - ポートに関する未加工の統計情報
  - 標準のインベントリおよびカード管理機能
  - J1 パストレース
  - CTC から開始される Cisco IOS CLI セッション
  - CTC からの Cisco IOS スタートアップ コンフィギュレーション ファイル管理

## ML シリーズカードの主な機能

ここでは、ML シリーズカードの主な機能とその実装について説明します。

### Cisco IOS

Cisco IOS は、ML シリーズカードのデータ機能を制御するためのソフトウェアであり、ONS 15454 SONET/SDH Advanced Timing, Communications, and Control (TCC2) カードおよび Advanced Timing, Communications, and Control Plus (TCC2P) カードにあらかじめロードされて出荷されます。ML シリーズの Cisco IOS イメージは、Cisco Catalyst シリーズの Cisco IOS システム イメージと同じようにアップグレードすることはできません。ML シリーズの Cisco IOS イメージをアップグレードするには、必ず ONS 15454 SONET/SDH の CTC を使用する必要があります。また、ML シリーズカードの Cisco IOS イメージは、ONS 15454 SONET または SDH のソフトウェアリリースの一部として提供され、その他の方法で入手することはできません。この Cisco IOS イメージは、標準の ONS 15454 SONET/SDH システム ソフトウェア CD 内のパッケージ ファイル名 [M\_I.bin] に収録されており、ファイル名は [ons15454m-i7-mz] です。これらのイメージは、個別にダウンロードしたり、入手したりすることはできません。

### DRPRI

ブリッジグループのプロトコル DRPRI では、ONS ノード障害から保護するためにリングを相互接続する RPR メカニズムを使用しています。このプロトコルにより、RSTP の特殊なインスタンスによってリングを 2 つの平行接続でリンクします。一方の接続はアクティブ ノードであり、もう一方はスタンバイ ノードです。アクティブ ノード、リンク、またはカードで障害が発生すると、独自のアルゴリズムによって障害が検出され、スタンバイ ノードにスイッチ オーバーします。ML シリーズカードで拡張マイクロ イメージを使用している場合は、DRPRI によりレイヤ 2 のブリッジドトラフィックに適用される回復時間は 200 ミリ秒未満です。他のマイクロコード イメージについては、レイヤ 2 の回復時間は最大 12 秒です。レイヤ 3 のユニキャストトラフィックおよびマルチキャストトラフィックの回復時間は、使用するマイクロコード イメージに関係なく、実装したルーティングプロトコルのコンバージェンス時間によって異なります。

### EoMPLS

EoMPLS には、MPLS 対応のレイヤ 3 コアを経由するイーサネットトラフィックをトンネリングするメカニズムがあります。このメカニズムでは、イーサネット Protocol Data Unit (PDU; プロトコルデータユニット) を MPLS パケット内にカプセル化し、ラベルスタッキングを使用して MPLS ネットワーク上で転送します。EoMPLS は、Martini 社のドラフト案に基づく、Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) の標準トラック プロトコルです。サービスプロバイダーは、EoMPLS と自社の既存の MPLS バックボーンを使用して、お客様に仮想イーサネット回線サービスまたは VLAN サービスを提供できます。

### GFP-F フレーミング

GFP は、さまざまなサービス タイプを SONET/SDH へマッピングするための標準ベースの方式を定義しています。ML シリーズおよび CE シリーズは、GFP 向けの PDU 型クライアントシグナルアダプテーション モードである、GFP-F をサポートします。GFP-F では、1 つの可変長データパケットを 1 つの GFP パケットにマッピングします。

GFP は、共通機能とペイロード固有の機能で構成されます。共有機能はすべてのペイロードで共有されます。ペイロード固有の機能は、ペイロードの種類によって異なります。GFP は ITU 勧告 G.7041 で詳しく定義されています。

## リンク集約 (FEC、GEC、および POS)

ML シリーズでは、FEC、GEC、および POS チャンネルのリンク集約を使用できます。リンク集約により、複数のポートをより大きい 1 つの論理ポートにグループ化し、個別のポートで障害が発生した場合に復元できます。ML シリーズでは、FEC の場合は最大 4 つのイーサネットポート、GEC の場合は最大 2 つのイーサネットポート、および POS チャンネルでは 2 つの SONET/SDH 仮想ポートがサポートされます。POS チャンネルは、LEX カプセル化を使用してのみサポートされます。

ブリッジド パケットの場合は MAC Source Address (SA; 送信元アドレス) と Destination Address (DA; 宛先アドレス) に基づいて、また ルーテッド パケットの場合は IP の SA と DA に基づいて、トラフィック フローが各ポートにマッピングされます。リンク集約を設定した場合は、ポリシングとクラスベースのケット プライオリティがサポートされません。

## RPR

RPR は、メトロファイバリングネットワーク向けに設計されたネットワークアーキテクチャであり、現在急速に普及しつつあります。この新しい MAC プロトコルは、パケットベースのネットワークでの STP、RSTP、および SONET の限界を解決するように設計されています。RPR のコンバージェンス時間は、SONET とほぼ同じで、STP や RSTP よりもかなり高速です。RPR は、レイヤ 2 レベルで動作し、イーサネット回線や SONET 回線 (保護または非保護) と互換性があります。

## TL1

ML シリーズカードの TL1 を使用して、カードのインベントリ、障害またはアラームの管理、カードのプロビジョニング、およびデータと SONET ポートに関するステータス情報の取得を行うことができます。また、SONET STS 回線のプロビジョニングや TCC2/TCC2P カードメモリへの Cisco IOS スタートアップ コンフィギュレーション ファイルの転送にも TL1 を使用できます。特定の TL1 コマンドや TL1 全般については、『Cisco ONS SONET TL1 Command Guide』を参照してください。

## VRF Lite

VRF Lite は、ML シリーズカード専用実装した VPN Routing/Forwarding instance (VRF; VPN ルーティング/転送インスタンス) です。標準の VRF と異なり、VRF Lite には、Multi-Protocol internal BGP (MP-iBGP; マルチプロトコル内部 BGP) が含まれません。

標準の VRF は、IP ルーティングの拡張機能であり、各 VPN に複数のルーティングインスタンスと独立した IP ルーティング テーブルおよび IP 転送テーブルを提供します。VRF は、内部 MP-iBGP と合わせて使用します。MP-iBGP は、ルータ間で VRF 情報を配布して、レイヤ 3 の MPLS-VPN を実現します。

VRF Lite では、VRF 情報をローカルに保存します。VRF 情報は、接続した機器に配布されません。VRF の情報により、カスタマー ルータやサービス プロバイダーのルータから受信したトラフィックが、正しいインターフェイスとサブインターフェイスに転送されます。

VRF Lite では、カスタマー機器として機能する ML シリーズカードに、サービス プロバイダーの機器とのインターフェイスとサブインターフェイスを複数設定できます。これにより、カスタマーの ML シリーズカードが複数のカスタマーを処理できます。通常のカスタマー機器は、単一のカスタマーしか処理できません。





## CTC の動作

---

この章では、ML シリーズ カードの Cisco Transport Controller (CTC) の動作について説明します。この章で説明するすべての動作は、CTC のカードレベル ビューで行われます。CTC には、ML シリーズ カードのイーサネット ポートと Packet-over-SONET/SDH (POS) ポートの両方に関するプロビジョニング情報と統計情報が表示されます。ML シリーズ カードの場合、CTC は、他の ONS 15454 SONET/SDH トラフィック カードと同じ方法で SONET/SDH アラームを管理し、STS/STM 回線をプロビジョニングします。

CTC を使用して、Cisco IOS コンフィギュレーション ファイルをロードするか、または Cisco IOS CLI (コマンドライン インターフェイス) セッションを開きます。第 3 章「初期設定」を参照してください。

この章の内容は次のとおりです。

- ML シリーズの POS およびイーサネット統計情報の CTC への表示 (p.2-2)
- ML シリーズイーサネットポートのプロビジョニング情報の CTC への表示 (p.2-3)
- ML シリーズ POS ポートのプロビジョニング情報の CTC への表示 (p.2-4)
- フレーミングモードのプロビジョニング (p.2-5)
- SONET/SDH アラームの管理 (p.2-5)
- FPGA 情報の表示 (p.2-6)
- SONET/SDH 回線のプロビジョニング (p.2-7)
- J1 パストレース (p.2-7)

## ML シリーズの POS およびイーサネット統計情報の CTC への表示

POS 統計情報のウィンドウには、POS ポートレベルの統計情報が表示されます。POS 統計情報ウィンドウを表示するには、ML シリーズ カードの CTC カード ビューを表示し、**Performance > POS Ports** タブをクリックします。

イーサネット統計情報のウィンドウには、イーサネット ポートレベルの統計情報が表示されます。イーサネット統計情報のウィンドウの表示は、POS 統計情報のウィンドウの表示に似ています。ML シリーズのイーサネット ポートはゼロ ベースです。イーサネット統計情報ウィンドウを表示するには、ML シリーズ カードの CTC カード ビューを表示し、**Performance > Ether Ports** タブをクリックします。表 2-1 に、POS Ports ウィンドウと Ether Ports ウィンドウのボタンを示します。

ML シリーズ カードで HDLC フレーミングまたは Frame-mapped Generic Framing Procedure (GFP-F) フレーミングのどちらを使用するかによって、表示される統計情報が異なります。ML シリーズ カードの統計情報の定義については、『Cisco ONS 15454 SONET and DWDM Troubleshooting Guide』または『Cisco ONS 15454 SDH Troubleshooting Guide』の「Performance Monitoring」の章を参照してください。

表 2-1 ML シリーズの POS およびイーサネット統計情報のフィールドとボタン

ボタン	説明
Refresh	統計情報を手動でリフレッシュします。
Baseline	カード上の実際の統計情報には影響を与えずにソフトウェアのカウンタ（特定の CTC クライアントのみ）を一時的にゼロにリセットします。その時点以降、一時的なベースラインからの変化を示すカウンタのみがこの CTC クライアントによって表示されます。新しいベースライン カウンタは、ユーザが Performance ウィンドウを表示している間だけ表示されます。ユーザが別の CTC ウィンドウに移動して Performance ウィンドウに戻ってきた場合、カードに保持されている実際の統計情報が表示されます。
Auto-Refresh	統計情報の自動リフレッシュの間隔を設定します。

## ML シリーズイーサネット ポートのプロビジョニング情報の CTC への表示

イーサネット ポート プロビジョニングのウィンドウには、イーサネット ポートのプロビジョニング ステータスが表示されます。このウィンドウを表示するには、**Provisioning > Ether Ports** タブをクリックします。ML シリーズ カードの場合、CTC からプロビジョニングできるのは Port Name フィールドのみです。ML シリーズのポートは、Cisco IOS の CLI を使用して設定する必要があります。

カラム内の Auto は、ポートが、接続されたリンク パートナーと機能を自動ネゴシエーションするように設定されていることを示しています。

すべての ML シリーズ カードで、すべてのカラムが表示されるわけではありません。表 2-2 に、Provisioning > Ether Ports タブで表示される情報の詳細を示します。

表 2-2 イーサネット ポートのプロビジョニング ステータスの CTC 表示

カラム	説明	ML1000-2	ML100T-12	ML100X-8
Port	特定のポートの固定番号 ID	0 または 1	0 ~ 11	0 ~ 7
Port Name	設定可能な英数字 12 文字のポート ID	ユーザ固有	ユーザ固有	ユーザ固有
Admin State	設定されたポートの状態。管理上アクティブまたは非アクティブ	UP および DOWN	UP および DOWN	UP および DOWN
Link State	ポートのシグナリング ポイントと接続装置の間のステータス	UP および DOWN	UP および DOWN	UP および DOWN
MTU	Maximum Transmission Unit ( MTU; 最大伝送ユニット)。ポートに設定されている最大パケット サイズ	デフォルト値は 1500	デフォルト値は 1500	デフォルト値は 1500
Speed	イーサネット ポートの伝送速度	—	Auto、10 Mbps、または 100 Mbps	100 Mbps
Duplex	ポートのデュプレックス モード設定	—	Auto、Full、または Half	Full
Flow Control	ピア装置でネゴシエーションされたフロー制御モード。これらの値は表示されますが、CTC で設定することはできません。	Asymmetrical、Symmetrical、または None	Symmetrical または None	Symmetrical または None
Optics	Small Form-Factor Pluggable ( SFP ) の物理的なメディア タイプ。	Unplugged、1000 SX、または 1000 LX	—	Unplugged、100 FX、または 100 LX



(注) ML100X-8 の Optics カラムに 100 FX 値がある場合、Short Wavelength( SX; 短波長 )SFP を表します。



(注) CTC に設定されたポート名フィールドと Cisco IOS に設定されたポート名は、相互に依存しません。Cisco IOS と CTC に存在する同じポートの名前は、CTC と Cisco IOS の両方で同じ名前を使用してポート名を設定しない限り一致しません。

## ML シリーズ POS ポートのプロビジョニング情報の CTC への表示

POS ポート プロビジョニングのウィンドウには、カードの POS ポートのプロビジョニングステータスが表示されます。このウィンドウを表示するには、**Provisioning > POS Ports** タブをクリックします。ML シリーズカードの場合、CTC から設定できるのは POS Port Name フィールドのみです。ML シリーズのポートは、Cisco IOS の CLI を使用して設定する必要があります。

表 2-3 に、Provisioning > POS Ports タブで表示される情報の詳細を示します。

**表 2-3 POS ポートのプロビジョニングステータスの CTC 表示**

カラム	説明
Port	特定のポートの固定番号 ID
Port Name	設定可能な英数字 12 文字のポート ID
Admin State	設定されたポートの状態。管理上アクティブまたは非アクティブです。表示される値は UP と DOWN です。UP 値にするには、POS ポートは管理上アクティブで、SONET/SDH 回線がプロビジョニングされている必要があります。
Link State	ポートのシグナリングポイントと接続装置間のステータス。表示される値は UP と DOWN です。
MTU	最大伝送ユニット。ポートに設定されている最大パケットサイズです。最大値は 9000 です。デフォルトサイズは、G シリーズカード対応のカプセル化 (LEX) の場合は 1500、Cisco HDLC と PPP/Bridging Control Protocol (ポイントツーポイント プロトコル /BCP) カプセル化の場合は 4470 です。
Framing Type	HDLC フレーミングタイプ、または GFP-F フレーミングタイプは、ポートで使用されている POS フレーミングメカニズムを示します。



**(注)** CTC に設定されたポート名フィールドと Cisco IOS に設定されたポート名は、相互に依存しません。Cisco IOS と CTC に存在するポートの名前は、CTC と Cisco IOS の両方で同じ名前を使用してポート名を設定しないかぎり一致しません。

## フレーミングモードのプロビジョニング

カードモードのプロビジョニング ウィンドウでは ML シリーズ カードで使用するフレーミングモードが表示されるため、ユーザがフレーミング メカニズムを HDLC または GFP-F に変更できます。このウィンドウを表示するには、**Provisioning > Card** タブをクリックします。HDLC は、ONS 15454 または ONS 15454 SDH ML シリーズ カードのデフォルトのフレーミングモードです。フレーミング メカニズムの詳細については、「[ONS イーサネット カード上の POS](#)」を参照してください。

また、ユーザはカードを物理的に取り付ける前に ML シリーズ カードのフレーミングモードを事前にプロビジョニングできます。その後 ML シリーズ カードは、事前にプロビジョニングされたフレーミングモードで起動します。

接続した POS ポートはそのピア ポートのフレーミング メカニズムと一致する必要があります。フレーミングモードを変更するには、まず ML シリーズ カード上の既存の STS/STM 回線をすべて削除する必要があります。



注意

ML シリーズ カードはフレーミングモードが変更されたあとにリポートします。

このウィンドウを表示するには、**Provisioning > Card** タブをクリックします。**Mode** ドロップダウン リストで **Apply** をクリックしてフレーミングモードのタイプをプロビジョニングします。表示された **Reset Card** ダイアログボックスで **Yes** をクリックします。

## SONET/SDH アラームの管理

CTC は、ML シリーズの SONET/SDH アラームの動作管理を、他の ONS 15454 SONET/SDH カードでのアラームの動作管理と同じ方法で行います。詳細については、『*Cisco ONS 15454 Procedure Guide*』または『*Cisco ONS 15454 SDH Procedure Guide*』の「[Manage Alarms](#)」の章を参照してください。特定のアラームの詳細については、『*Cisco ONS 15454 Troubleshooting Guide*』または『*Cisco ONS 15454 SDH Troubleshooting Guide*』の「[Alarm Troubleshooting](#)」の章を参照してください。

このウィンドウを表示するには、イーサネットおよび POS ポート アラーム プロファイル情報で **Provisioning > Alarm Profiles** タブをクリックします。

## FPGA 情報の表示

CTC は、ML シリーズ カードの Field Programmable Gate Array (FPGA) の 2 つのバージョンに関する情報を表示します。1 つは実行 FPGA で、ML シリーズ カードによって TCC2/TCC2P カードからダウンロードされた最新の FPGA バージョンです。もう 1 つはフラッシュ メモリに焼き付けられた FPGA バージョンです。実行 FPGA および焼き込み FPGA のバージョン情報はそれぞれ異なる場合があります。

実行 FPGA は、ML シリーズ カード上で動作する FPGA バージョンで、FPGA がアップグレードすると変更されます。CTC インベントリ ウィンドウには、この実行 FPGA 情報が表示されます。このウィンドウを表示するには、**Inventory > Firmware Rev.** タブをクリックします。

CTC メンテナンス情報ウィンドウには、フラッシュ メモリに焼き付けられた FPGA 情報が表示されます。また、カードが SONET または SDH シェルフのどちらに取り付けられているかも表示されます。このウィンドウを表示するには、**Maintenance > Info** タブをクリックします。

ML100T-12、ML100X-8、および ML1000-2 の FPGA は、カードのネットワーク プロセッサと SONET/SDH クロスコネクタ間のインターフェイスとバッファリングを提供します。FPGA Image Version 3.x は HDLC フレーミングをサポートし、FPGA Image Version 4.x は GFP-F フレーミングをサポートします。両方のイメージは Virtual Concatenation (VCAT; バーチャル コンカチネーション) をサポートします。Release 5.0 以降では、ユーザがフレーミング モードを変更すると、適切な FPGA が自動的にロードされます。



(注)

Software Release 4.6 以前に製造された ML シリーズ カードで VCAT をサポートするには、FPGA の更新バージョンが必要です。



注意

旧 CTC ソフトウェア リリースで現在の FPGA イメージを使用しないでください。

## SONET/SDH 回線のプロビジョニング

CTC は、ML シリーズ カードの 2 つの仮想 SONET/SDH ポートの STS/STM レベル回線を、他の ONS 15454 SONET/SDH OC-N カードのプロビジョニングと同じ方法でプロビジョニングおよび編集します。ONS 15454 ML シリーズ カードは、Contiguous Concatenation (CCAT; 連続コンカチネーション) および VCAT 回線の両方をサポートします。

ML シリーズ カード SONET CCAT または VCAT 回線の詳細な設定手順については、『Cisco ONS 15454 Procedure Guide』の「Create Circuits and VT Tunnels」の章を参照してください。ML シリーズ カード SDH CCAT または VCAT 回線の詳細な設定手順については、『Cisco ONS 15454 SDH Procedure Guide』の「Create Circuits and Tunnels」の章を参照してください。VCAT 回線全般については、『Cisco ONS 15454 Reference Manual』または『Cisco ONS 15454 SDH Reference Manual』の「Circuits and Tunnels」の章を参照してください。

## J1 パストレース

J1 パストレースは、64 の連続する J1 バイトで構成される、反復固定長文字列です。この文字列を使用すると、SONET/SDH 回線トラフィックの中断や変更をモニタリングできます。J1 パストレースの詳細については、『Cisco ONS 15454 Reference Manual』または『Cisco ONS 15454 SDH Reference Manual』を参照してください。





## 初期設定

---

この章では、ML シリーズ カードの初期設定について説明します。主な内容は、次のとおりです。

- [ハードウェアの設置 \( p.3-2 \)](#)
- [ML シリーズ カード上の Cisco IOS \( p.3-3 \)](#)
- [スタートアップ コンフィギュレーション ファイル \( p.3-8 \)](#)
- [複数のマイクロコード イメージ \( p.3-14 \)](#)
- [使用中のマイクロコード イメージの変更 \( p.3-15 \)](#)
- [Cisco IOS のコマンド モード \( p.3-16 \)](#)
- [コマンド モードの使用 \( p.3-18 \)](#)

## ハードウェアの設置

ここでは、ML シリーズ カードの起動など、ハードウェアの設置作業について説明します。ONS 15454 SONET/SDH のカード スロットはあらかじめ ML シリーズ ラインカード用にプロビジョニングされているので、次の物理的な手順は、これらのスロットをプロビジョニングする前でも後でも実行できます。

1. ONS 15454 SONET/SDH に ML シリーズ カードを取り付けます。詳細については、『*Cisco ONS 15454 Procedure Guide*』または『*Cisco ONS 15454 SDH Procedure Guide*』の第2章「Install Cards and Fiber-Optic Cable」を参照してください。
2. ML シリーズ カードの前面ポートにケーブルを接続します。
3. (任意) ML シリーズ カードにコンソール端末を接続します。



---

ML シリーズ カードが挿入済みの場合、Cisco IOS の有効なスタートアップ コンフィギュレーション ファイルが存在しないと、CTC の Alarms ペインの下に NO-CONFIG 状態がレポートされます。この状態をクリアするには、このファイルをロードまたは作成します。このファイルのロードまたは作成については、「[スタートアップ コンフィギュレーション ファイル](#)」(p.3-8)を参照してください。

---

## ML シリーズ カード上の Cisco IOS

ML シリーズ カードで使用する Cisco IOS のソフトウェア イメージは、ML シリーズ カードに永続的に保存されず、TCC2/TCC2P カードのフラッシュ メモリに保存されます。カードを物理的に取り外して再度挿入する、またはカードの電源が切断されるなどのハード リセットが行われると、Cisco IOS のソフトウェア イメージが TCC2/TCC2P のフラッシュ メモリから ML シリーズ カードのメモリ キャッシュにダウンロードされます。キャッシュされたイメージは、ML シリーズ カードによって解凍され、使用できるように初期化されます。

CTC または Cisco IOS CLI ( コマンドライン インターフェイス ) コマンドの `reload` を使用して ML シリーズ カードをリセットするなどのソフトリセットが行われると、ML シリーズ カードはキャッシュ内で Cisco IOS のソフトウェア イメージを確認します。Cisco IOS イメージが有効で最新な場合、ML シリーズ カードはそのイメージを解凍し、初期化します。適切なイメージが検出されない場合は、ML シリーズ カードは TCC2/TCC2P に Cisco IOS イメージの新しいコピーを要求します。Cisco IOS イメージをキャッシュすることにより、ウォーム リセットの実行時間が大幅に短縮されます。

ML シリーズ カードの Cisco IOS コンフィギュレーションにアクセスするには、4 種類の方法が使用できます。2 つの帯域外オプションは、CTC で Cisco IOS セッションを開く方法と、ノードの IP アドレスとスロット番号に 2000 を加えた値に Telnet 接続する方法です。2 つの帯域内シグナリングオプションは、設定済み管理インターフェイスに Telnet 接続する方法と、コンソールポートに直接接続する方法です。

### CTC を使用して Cisco IOS セッションを開く方法

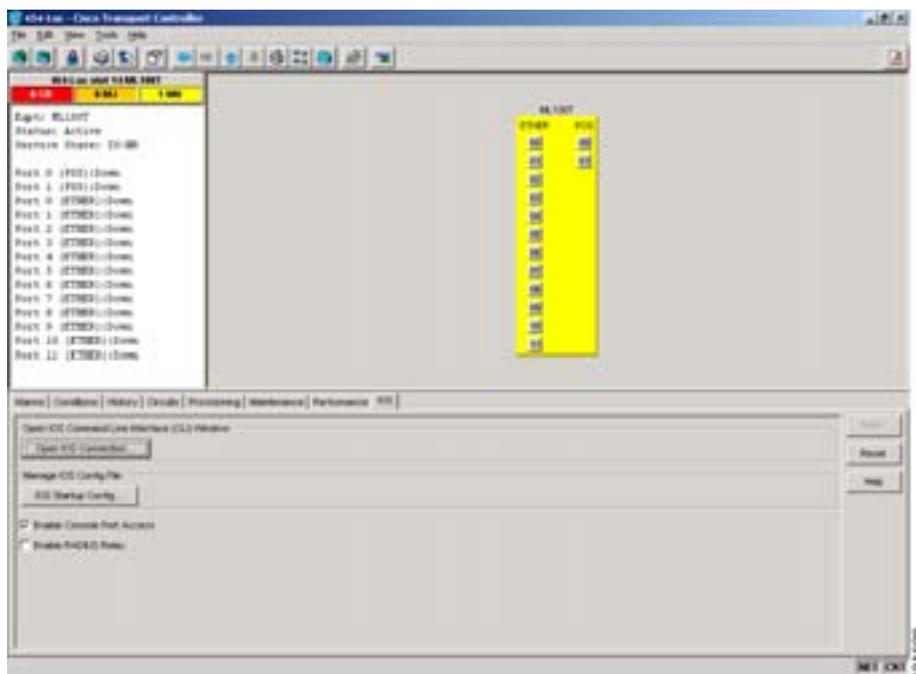
CTC を使用して ML シリーズ カードに対する Cisco IOS の CLI セッションを開始できます。カードレベルの CTC ビューで **IOS** タブをクリックし、**Open IOS Command Line Interface ( CLI )** ボタンをクリックします ( 図 3-1 参照 )。ウィンドウが開き、標準の Cisco IOS CLI User EXEC コマンドモードのプロンプトが表示されます。



(注)

CTC で Cisco IOS の CLI セッションを開始する前に、あらかじめ Cisco IOS のスタートアップ コンフィギュレーション ファイルをロードし、ML シリーズ カードを取り付けて初期化しておいてください。詳細は、「[スタートアップ コンフィギュレーション ファイル](#)」(p.3-8)を参照してください。

図 3-1 CTC IOS ウィンドウ



## ノードの IP アドレスとスロット番号に Telnet 接続する方法

ONS 15454 SONET/SDH の IP アドレスとスロット番号に 2000 を加えた値を使用して Cisco IOS CLI に Telnet 接続できます。



(注) IP アドレスとスロット番号に 2000 を加えた値を使用して Telnet 接続する前に、あらかじめ Cisco IOS のスタートアップ コンフィギュレーション ファイルをロードし、ML シリーズカードを取り付けて初期化しておいてください。詳細については、「[スタートアップ コンフィギュレーション ファイル](#)」(p.3-8)を参照してください。



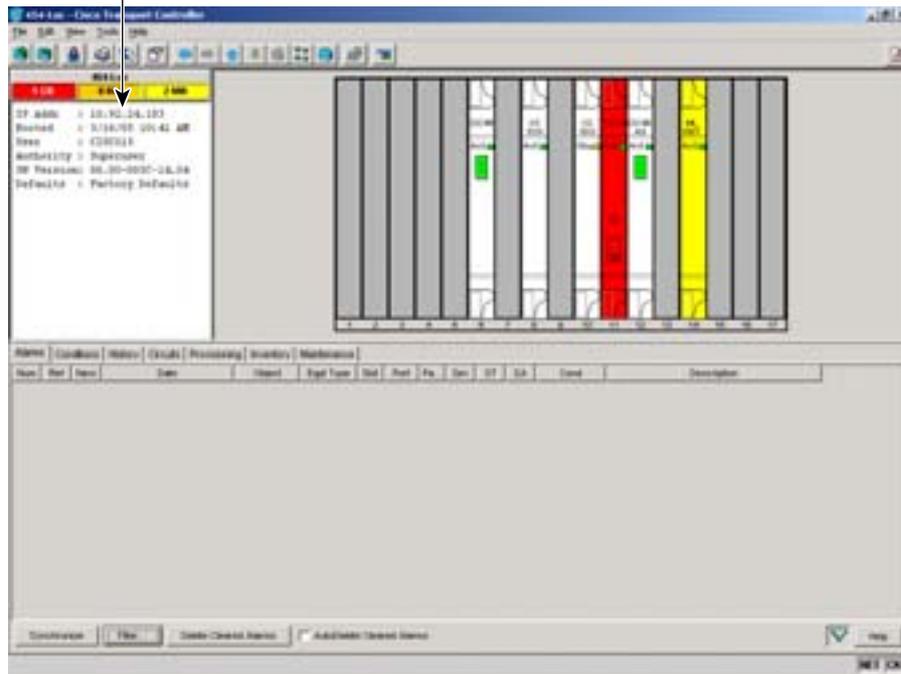
(注) ONS 15454 SONET/SDH ノードがプロキシ サーバとして設定されている場合、つまり、リング内の 1 台の ONS 15454 SONET/SDH ノードが同じリング内の他のノードの Gateway Network Element (GNE; ゲートウェイ ネットワーク エlement)として機能している場合に、GNE のファイアウォールを超えて GNE 以外または End Network Element (ENE; 終端ネットワーク要素)の IP アドレスとスロット番号に Telnet 接続するには、ユーザの Telnet クライアントが SOCKS v5 (RFC 1928) を認識する必要があります。この場合は、Telnet セッションで GNE を Socks v5 プロキシとして認識し、ENE をホストとして認識できるように、この Telnet クライアントを設定します。

**ステップ 1** ONS 15454 SONET/SDH 本体の前面にある LCD でノードの IP アドレスを物理的に確認するか、または、CTC ノードビューの IP Addr フィールドで IP アドレスを確認します (図 3-2 参照)。

**ステップ2** ONS 15454 SONET/SDH の本体または CTC で、対象となる ML シリーズカードを取り付けたスロットの番号を確認します（図 3-2 参照）。スロット番号の例は、「スロット 13」などです。

図 3-2 IP アドレスとスロット番号が表示された CTC ノードビュー

ノードの IP アドレス



**ステップ3** 使用する通信プログラムで、この IP アドレスと、スロット番号に 2000 を加えた値を Telnet アドレスとして使用します。たとえば、IP アドレスが 10.92.18.124 でスロット番号が 13 の場合は、10.92.18.124 2013 を入力して Telnet 接続します。

## 管理ポートへの Telnet 接続

他の Cisco IOS プラットフォームと同様に標準の Cisco IOS 管理ポート経由で ML シリーズカードに接続できます。管理アクセス用のポートと回線の設定については、『Cisco IOS Configuration Fundamentals Configuration Guide』を参照してください。

セキュリティの観点から、Telnet 接続に使用する vty 回線の設定は完全な状態ではありません。ML シリーズカードに Telnet 接続するには、シリアルコンソール接続によって vty 回線を設定するか、または vty 回線を設定するスタートアップコンフィギュレーションファイルをあらかじめロードしておく必要があります。まず、ML シリーズのポートを管理ポートとして設定する必要があります。詳細については、「管理ポートの設定」(p.3-9)を参照してください。

## ML シリーズの IOS CLI コンソール ポート

ML シリーズカードの前面プレートには、CONSOLE というラベルが貼られた RJ-11 シリアル コンソールポートが用意されています。このコンソールポートは、Data Circuit-terminating Equipment (DCE; データ回線終端装置) として配線されています。このポートにより、端末エミュレーションソフトウェアを実行中の PC またはワークステーションのシリアルポートから特定の ML シリーズカードの Cisco IOS CLI に通信できます。

### RJ-11/RJ-45 コンソール ケーブル アダプタ

ML シリーズカードの前面プレートのスペースに制約があるため、コンソールポートには一般的な RJ-45 モジュラ ジャックではなく、RJ-11 モジュラ ジャックを使用しています。シスコでは、各 ML シリーズカード向けに RJ-11/RJ-45 コンソール ケーブル アダプタ (P/N 15454-CONSOLE-02) を用意しています。このアダプタを接続すると、コンソールポートが標準の Cisco RJ-45 コンソールポートと同様に機能します。図 3-3 に RJ-11/RJ-45 コンソール ケーブル アダプタを示します。

図 3-3 コンソール ケーブル アダプタ

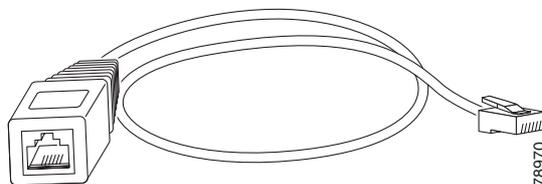


表 3-1 に RJ-11 と RJ-45 のピンの対応関係を示します。

表 3-1 RJ-11 と RJ-45 のピンの対応関係

RJ-11 ピン	RJ-45 ピン
1	1
2	2
3	3
4	4
なし	5
5	6
なし	7
6	8

### PC または端末からコンソールポートへの接続

同梱の RJ-11/RJ-45 コンソール ケーブル アダプタと DB-9 アダプタを使用して、PC を ML シリーズのコンソールポートに接続します。

PC では VT100 端末エミュレーションがサポートされている必要があります。端末エミュレーションソフトウェア (通常は HyperTerminal や Procomm Plus などの PC アプリケーション) によって、セットアッププログラムの実行中に ML シリーズカードと PC または端末の間の通信が可能になります。

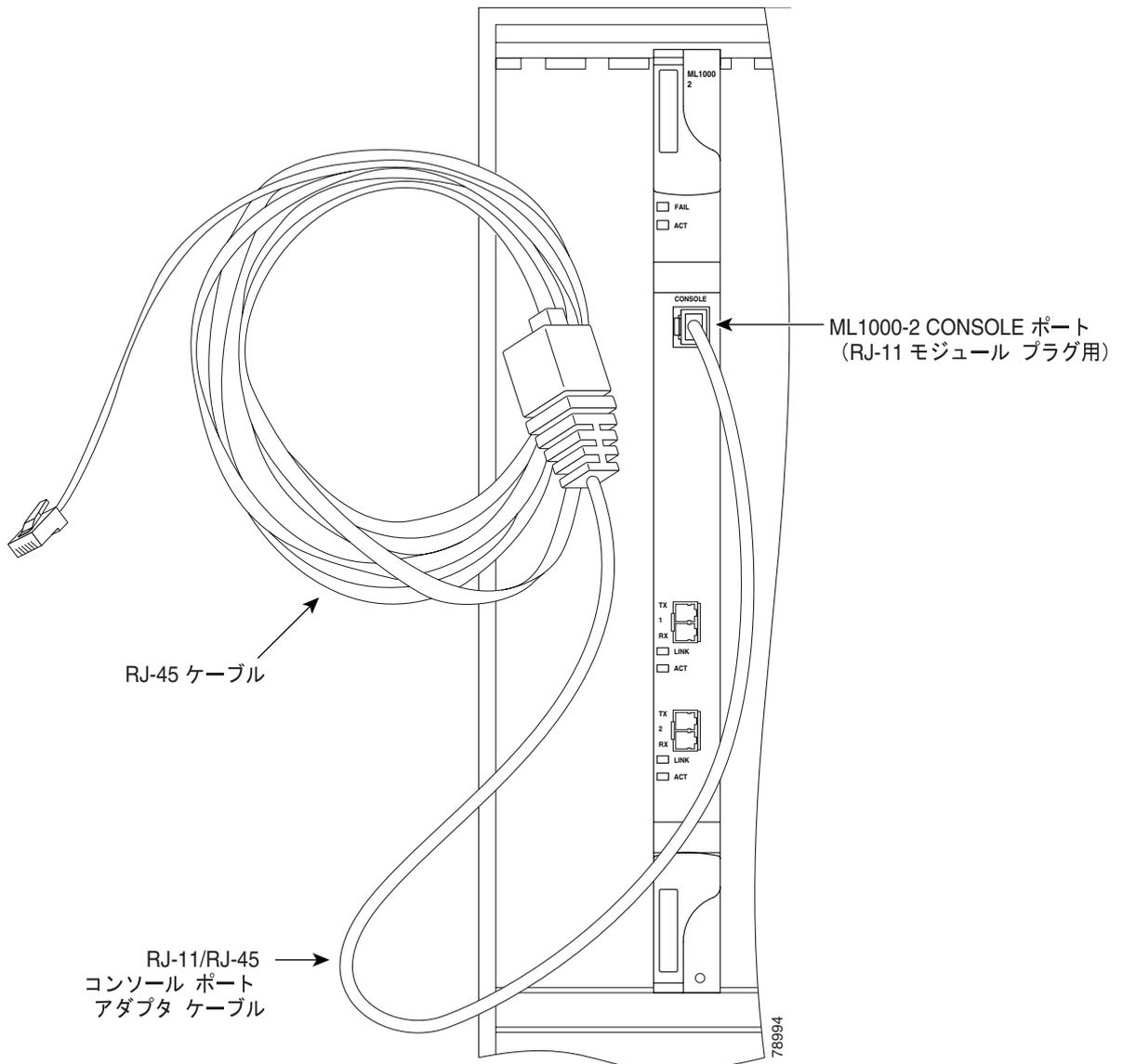
**ステップ 1** PC または 端末のデータレートと文字形式をコンソールポートのデフォルト設定に合わせて設定します。

- 9600 ボー
- 8 データビット
- 1 ストップビット
- パリティなし

**ステップ 2** 同梱ケーブルの RJ-45 コネクタを同梱のコンソールケーブルアダプタのメス側に接続します。

**ステップ 3** 同梱のコンソールケーブルアダプタの RJ-11 モジュラプラグ側を、ML シリーズカードの前面プレートにある CONSOLE というラベルが付いた RJ-11 シリアルコンソールポートに接続します。図 3-4 に ML1000-2 前面プレートとコンソールポートを示します。ML100T-12 および ML100X-8 の場合、コンソールポートはカードの全面プレートが一番下にあります。

図 3-4 コンソールポートへの接続



## ■ スタートアップ コンフィギュレーション ファイル

**ステップ 4** 同梱の RJ-45/DB-9 メス側 DTE アダプタを PC にある 9 ピンの DB-9 シリアルポートに接続します。

**ステップ 5** 接続したアダプタに、この同梱ケーブルの反対側を挿入します。

## スタートアップ コンフィギュレーション ファイル

ML シリーズ カードのリセット時にデフォルト設定以外の値を設定するには、スタートアップ コンフィギュレーション ファイルが必要です。TCC2/TCC2P のフラッシュ メモリにスタートアップ コンフィギュレーション ファイルがない場合は、デフォルト設定でカードが起動します。スタートアップ コンフィギュレーション ファイルを手動でセットアップするには、シリアル コンソールポートおよび Cisco IOS CLI コンフィギュレーション モードから操作するか、または、Cisco IOS が提供するスタートアップ コンフィギュレーション ファイルを CTC からロードします。copy running-config startup-config コマンドで実行コンフィギュレーション ファイルを保存すると、そのファイルがスタートアップ コンフィギュレーション ファイルになります。

ML シリーズ カードへの Telnet 接続を確立するには、あらかじめスタートアップ コンフィギュレーション ファイルを ML シリーズ カードにロードしておく必要があります。コンソールポートを介してアクセスできます。

**注意**

copy running-config startup-config コマンドは、スタートアップ コンフィギュレーション ファイルを ML シリーズ カードのフラッシュ メモリに保存します。この操作は、Cisco IOS の CLI セッションで [OK] が表示されることで確認します。また、スタートアップ コンフィギュレーション ファイルは約 30 秒が経過したあとに ONS ノードのデータベース復元ファイルにも保存されます。

**注意**

シスコ社の保守担当者の支援なしに、ML シリーズ カードの Read-Only Memory Monitor mode (ROMMON; 読み取り専用モニター モード) に絶対にアクセスしないでください。このモードでは、ML シリーズ カードを動作不能にする作業が可能になります。ML シリーズ カードの ROMMON は、ML シリーズ カードに Cisco IOS ソフトウェア イメージを正しくブートできるように、あらかじめ設定されています。

**注意**

スタートアップ コンフィギュレーション ファイルの最大サイズは 98356 バイト (文字) です。

**(注)**

実行 コンフィギュレーション ファイルを変更すると、CTC に RUNCFG-SAVENEED 状態が表示されます。この状態が表示された場合は、Cisco IOS の CLI に copy running-config startup-config コマンドを入力する必要があります。このコマンドを入力しないと、ML シリーズ カードがリブートしたときに変更内容が失われます。

## シリアル コンソール ポートを使用して手動でスタートアップ コンフィギュレーション ファイルを作成する方法

Cisco IOS を使用して他の製品を操作したことがあるユーザにとって、シリアル コンソール ポート経由で設定する方法は、操作し慣れた方法です。設定手順の最後に、`copy running-config startup-config` コマンドを使用してスタートアップ コンフィギュレーション ファイルを保存します。

シリアル コンソール ポートを使用すると、ML シリーズ カードのブート プロセス全体を表示できます。ML シリーズ カードの初期化中には、まず、ローカルでキャッシュされた Cisco IOS の有効なコピーが検索されます。次に、TCC2/TCC2P から Cisco IOS のソフトウェア イメージがダウンロードされるか、または、有効なイメージの解凍と初期化が直接実行されます。Cisco IOS の初期化が完了すると、CLI プロンプトが表示されます。このプロンプトで、Cisco IOS の CLI コンフィギュレーション モードを開始し、ML シリーズ カードの基本設定をセットアップできます。

### パスワード

ML シリーズ カードに設定可能なパスワードには、イネーブルパスワードとイネーブルシークレットパスワードの2種類があります。セキュリティを強化するために、イネーブルパスワードとイネーブルシークレットパスワードは異なるパスワードにしてください。

- **イネーブルパスワード** 暗号化されないパスワードです。このパスワードには、任意の長さの英数字（大文字および小文字）を指定できます。イネーブルパスワードは、ML シリーズカードに対する設定変更を許可するユーザだけに通知してください。
- **イネーブルシークレットパスワード** 暗号化された安全なパスワードです。暗号化されたパスワードを設定することで、設定が不正に変更されるのを防ぐことができます。Cisco IOS ソフトウェアを実行中のシステムでグローバル コンフィギュレーション モードを開始するには、イネーブルシークレットパスワードを入力する必要があります。

イネーブルシークレットパスワードには、1 ~ 25 文字の英数字（大文字および小文字）を使用できます。最初の文字として数字を指定することはできません。このパスワードにはスペースを含めることができます。先頭のスペースは無視されますが、末尾のスペースは認識されません。

パスワードの設定方法については、「[管理ポートの設定](#)」(p.3-9)を参照してください。

### 管理ポートの設定

ML シリーズ カードには独立した管理ポートがないため、ファストイーサネット インターフェイス (ML100T-12 カードの 0 ~ 11 および ML100X-8 の 0 ~ 7)、ギガビットイーサネット インターフェイス (ML1000-2 カードの 0 ~ 1) または Packet-over-SONET (POS) インターフェイス (ML シリーズ カードの 0 ~ 1) を管理ポートとして設定できます。POS インターフェイスを作成するには、まず、CTC または TL1 から STS または STM 回線を作成する必要があります。

ML シリーズ カードは、リモートから管理ポート経由で設定できますが、その前に、ML シリーズカードに到達するための IP アドレスを設定しておくか、または、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ておく必要があります。Cisco IOS の CLI からシリアル コンソール接続経由で管理ポート インターフェイスを手動で設定できます。

リモート管理アクセス用に Telnet を設定するには、ユーザ EXEC モードで次の手順を実行します。

## ■ スタートアップ コンフィギュレーション ファイル

	コマンドの説明	目的
ステップ 1	Router> <b>enable</b> Router#	ユーザ EXEC (イネーブル) モードを開始します。  # プロンプトは、イネーブルモードが開始されていることを表します。
ステップ 2	Router# <b>configure terminal</b> 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。このコマンドを <b>config t</b> と短縮することもできます。Router(config)# プロンプトは、グローバル コンフィギュレーション モードが開始されていることを表します。
ステップ 3	Router(config)# <b>enable password password</b>	イネーブル パスワードを設定します。「パスワード」(p.3-9)を参照してください。
ステップ 4	Router(config)# <b>enable secret password</b>	イネーブル シークレット パスワードを入力できます。「パスワード」(p.3-9)を参照してください。グローバル コンフィギュレーション モードを開始するには、イネーブル シークレット パスワードを入力する必要があります。
ステップ 5	Router(config)# <b>interface type number</b> Router(config-if)#	指定した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 6	Router(config-if)# <b>ip address ip-address subnetmask</b>	ステップ 5 で指定したインターフェイスの IP アドレスと IP サブネット マスクを入力できます。
ステップ 7	Router(config-if)# <b>no shutdown</b>	インターフェイスをイネーブルにします。
ステップ 8	Router(config-if)# <b>exit</b> Router(config)#	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 9	Router(config)# <b>line vty line-number</b> Router(config-line)#	仮想端末接続用のライン コンフィギュレーション モードをアクティブにします。このモードで入力したコマンドによって、ML シリーズ カードに対する Telnet セッションの動作が制御されます。
ステップ 10	Router(config-line)# <b>password password</b>	Telnet セッションのパスワードを入力できます。
ステップ 11	Router(config-line)# <b>end</b> Router#	イネーブル EXEC モードに戻ります。
ステップ 12	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM (不揮発性 RAM) に保存します。

管理ポートでのリモート管理設定が完了すると、Telnet を使用して、設定をリモートで割り当てたり確認したりできます。

## ホスト名の設定

初期設定では、システム パスワードとイネーブルパスワードの他にホスト名を指定し、ML シリーズ カードを簡単に識別できるようにする必要があります。ホスト名を設定するには、イネーブルモードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b> 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	Router(config)# <b>hostname name-string</b>	システム名を入力できます。この例では、ホスト名を [Router] に設定します。

	コマンドの説明	目的
ステップ 3	Router(config)# <b>end</b> Router#	イネーブル EXEC モードに戻ります。
ステップ 4	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM にコピーします。

## CTC とスタートアップ コンフィギュレーション ファイル

CTC を使用すると、ML シリーズ カードに必要なスタートアップ コンフィギュレーション ファイルをロードできます。Cisco ONS 15454 SONET/SDH のソフトウェア CD には、Cisco IOS スタートアップ コンフィギュレーション ファイルのサンプル **Basic-IOS-startup-config.txt** が収録されています。Cisco IOS CLI のデフォルトの回線パスワードと、この設定のイネーブル パスワードは、CISCO15 です。独自のスタートアップ コンフィギュレーション ファイルを作成することもできます。詳細については、「[シリアル コンソール ポートを使用して手動でスタートアップ コンフィギュレーション ファイルを作成する方法](#)」(p.3-9)を参照してください。

CTC では、ML シリーズ カードをスロットに物理的に取り付ける前に、TCC2/TCC2P カードのフラッシュ メモリに Cisco IOS のスタートアップ コンフィギュレーション ファイルをロードできます。この場合、ML シリーズ カードを取り付けると、Cisco IOS ソフトウェア イメージとロード済みの Cisco IOS スタートアップ コンフィギュレーション ファイルがダウンロードされ、適用されます。スタートアップ コンフィギュレーション ファイルをあらかじめロードしておく、ML シリーズ カードは ONS 15454 SONET/SDH に取り付けられた直後から完全に設定済みのカードとして動作できます。

Cisco IOS スタートアップ コンフィギュレーション ファイルを TCC2/TCC2P カードのフラッシュ メモリにロードする前に ML シリーズ カードのブートが完了している場合は、ML シリーズ カードをリセットして Cisco IOS スタートアップ コンフィギュレーション ファイルが使用されるようにするか、または、Cisco IOS の CLI で **copy start run** コマンドを実行して、Cisco IOS スタートアップ コンフィギュレーション ファイルが使用されるように ML シリーズ カードを設定する必要があります。

## CTC での Cisco IOS スタートアップ コンフィギュレーション ファイルのロード

CTC を使用して Cisco IOS スタートアップ コンフィギュレーション ファイルを初めてロードするには、次の手順を実行します。

**ステップ 1** ML シリーズ カードのカードレベルのビューで **IOS** タブをクリックします。

CTC の IOS ウィンドウが開きます (図 3-1)。

**ステップ 2** **IOS startup config** ボタンをクリックします。

config file ダイアログボックスが表示されます。

**ステップ 3** **Local -> TCC** ボタンをクリックします。

**ステップ 4** Cisco IOS スタートアップ コンフィギュレーション ファイルのサンプルは、ONS 15454 SONET/SDH ソフトウェア CD、PC フォルダ、またはネットワーク フォルダからインストールできます。

## ■ スタートアップ コンフィギュレーション ファイル

- シスコが提供するスタートアップ コンフィギュレーション ファイルを ONS 15454 SONET/SDH ソフトウェア CD からインストールするには、PC またはワークステーションの CD ドライブにこの CD を挿入します。CTC の config file ダイアログを使用して、PC またはワークステーションの CD ドライブに移動して、**Basic-IOS-startup-config.txt** ファイルをダブルクリックします。
- シスコが提供するスタートアップ コンフィギュレーション ファイルを PC フォルダまたはネットワーク フォルダからインストールするには、必要な Cisco IOS スタートアップ コンフィギュレーション ファイルが格納されたフォルダに移動して、その Cisco IOS スタートアップ コンフィギュレーション ファイルをダブルクリックします。

**ステップ 5** Are you sure? ダイアログ ボックスで、**Yes** ボタンをクリックします。

configuration file ダイアログの Directory フィールドと Filename フィールドが更新され、TCC2/TCC2P にロードされた Cisco IOS スタートアップ コンフィギュレーション ファイルが反映されます。

**ステップ 6** TCC2/TCC2P から ML シリーズ カードに IOS 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。

- a. ML シリーズ カードを取り付け済みの場合は、CTC のノード レベル ビューまたはカード レベル ビューで ML シリーズ カードを右クリックし、**Reset Card** を選択します。

リセットが完了すると、新しくロードされた Cisco IOS スタートアップ コンフィギュレーション ファイルに基づいて ML シリーズ カードが動作します。

- b. ML シリーズ カードを取り付けていない場合は、スロットに ML シリーズ カードを取り付けると、新しくロードされた Cisco IOS スタートアップ コンフィギュレーション ファイルが ML シリーズ カードにロードされ、実行されます。



**(注)** Cisco IOS スタートアップ コンフィギュレーション ファイルがダウンロードされ、初期化中の解析でこのファイルにエラーが検出されると、ERROR-CONFIG アラームがレポートされ、CTC の Alarms ペインの下、または TL1 で表示されます。テキストの解析に関する他の Cisco IOS エラー メッセージは、CTC または TL1 でレポートされません。Cisco IOS に精通している場合は、Cisco IOS の CLI を開き、**copy start run** コマンドを実行して、解析エラーの原因となっている行をスタートアップ コンフィギュレーション ファイル内で探して問題を解決できます。



**(注)** ONS 15454 SONET/SDH データベースを標準的な方法で復元すると、TCC2/TCC2P にある Cisco IOS スタートアップ コンフィギュレーション ファイルが再インストールされます。ただし、ML シリーズ カードには、この Cisco IOS スタートアップ コンフィギュレーション ファイルが実装されません。詳細については、「[スタートアップ コンフィギュレーション ファイルのデータベースの復元](#)」(p.3-13)を参照してください。

## スタートアップ コンフィギュレーション ファイルのデータベースの復元

ONS 15454 SONET/SDH には、データベースの復元機能があります。データベースを復元すると、ノードと、ML シリーズ カード以外の取り付け済みのライン カードが、保存されているプロビジョニングに再設定されます。ML シリーズ カードは、TCC2/TCC2P データベースに保存されているスタートアップ コンフィギュレーション ファイルを自動的に復元しません。

保存されているスタートアップ コンフィギュレーション ファイルは、2 種類の方法で ML シリーズ カードにロードできます。1 つは、保存されていない実行設定で行った追加設定を失いますが、保存されている起動設定に完全に戻すことができます。この方法は、他の ONS カードの復元方式に似ています。もう 1 つは、保存したスタートアップ コンフィギュレーション ファイルを現在の実行コンフィギュレーションに追加インストールできます。この方法は、多くの Cisco Catalyst 装置で使用されているマージ型復元方式です。

復元されたデータベースに保存されているスタートアップ コンフィギュレーション ファイルに完全に戻すには、ML シリーズ カードをリセットする必要があります。CTC で ML シリーズ カードを右クリックし、**Reset** を選択するか、Cisco IOS の CLI で **reload** コマンドを使用して ML シリーズ カードをリセットします。



**注意** ONS 15454 ML シリーズ カードをリセットすると、トラフィックが損失します。また、カードへの Telnet セッションがすべて閉じられます。

保存されたスタートアップ コンフィギュレーションファイルを実行コンフィギュレーションとマージするには、Cisco IOS CLI の **copy startup-config running-config** コマンドを使用します。この復元方式は、現在の実行コンフィギュレーション、および Cisco IOS の **copy** コマンドを理解している経験のあるユーザだけが行うようにしてください。**copy startup-config running-config** コマンドは ML シリーズ カードをリセットしません。また、Cisco IOS CLI の **copy running-config startup-config** コマンドを使用して、新たにマージされた実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに保存する必要があります。

## 複数のマイクロコードイメージ

ML シリーズ カードでのパケットの一時処理と転送は、ネットワーク プロセッサによって実行されます。ネットワーク プロセッサは、マイクロコードで制御されます。このマイクロコードは、命令セット (ソフトウェア) であり、ネットワーク プロセッサにロードされて、高速実行されます。ネットワーク プロセッサでは、マイクロコードの保存容量が限られています。

ML シリーズ カードに組み込まれた機能によっては、マイクロコードを大量に必要とし、これらの追加マイクロコードがネットワーク プロセッサの保存許容量を超えることがあります。このような機能は、新しいマイクロコードイメージ (別のマイクロコード プログラム) として追加されます。ネットワーク プロセッサに一度に保持できるマイクロコードイメージは、1 つだけです。ロードしたマイクロコードイメージを変更するには、ネットワーク プロセッサをリセットする必要があります。

ML シリーズ カード用のマイクロコードイメージは、3 つの中から選択できます。デフォルトの基本イメージには、Software Release 4.1 IOS のイメージと同じ ML シリーズ カードの基本機能があり、Cisco IOS Release 12.1(19)EO および、ML シリーズ カードの Virtual Concatenation (VCAT; バーチャル コンカチネーション) 回線のようなマイクロコードに依存しない追加機能が含まれています。基本イメージを使用すると、ML シリーズ カードの既存設定を変更せずに、ソフトウェア リリース 4.0 または 4.1 からアップグレードできます。

他の 2 つのマイクロコードイメージ (拡張イメージと Multiprotocol Label Switching [MPLS; マルチプロトコル ラベル スイッチング] イメージ) では、特定の機能が追加されますが、基本イメージの機能の一部が使用できません。拡張マイクロコードイメージを選択すると、IP 分割機能と IP マルチキャスト機能が削除され、Ethernet Relay Multipoint Service (ERMS; イーサネット リレー マルチポイント サービス) および Dual Resilient Packet Ring Interconnect (DRPRI; 二重復元パケット リング相互接続) とパフォーマンス モニタリングの拡張機能が追加されます。MPLS マイクロコードイメージを選択すると、IP マルチキャスト、IP 分割、および ERMS のサポートが削除されますが、EoMPLS (MPLS ネットワーク経路のイーサネット フレームの転送機能) が追加されます。表 3-2 は、各マイクロコードイメージで使用可能な機能の比較表です。

表 3-2 マイクロコードイメージの機能比較

機能	基本(デフォルト)イメージ	拡張イメージ	MPLS イメージ
IP マルチキャスト		×	×
IP 分割		×	×
IP 転送			×
拡張パフォーマンス モニタリング	×		×
拡張 DRPRI	×		×
ERMS	×		×
MPLS	×	×	

## 使用中のマイクロコード イメージの変更

マイクロコード イメージを変更するには、Cisco IOS の CLI コマンドを実行し、CTC 経由で ML シリーズ カードをリセットします。使用中のマイクロコード イメージを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <code>microcode</code> { <code>base</code>   <code>enhanced</code>   <code>fail system-reload</code>   <code>mpls</code> }	<p>次の 3 つのマイクロコード イメージのいずれかを使用して、ML シリーズ カードを設定します。</p> <p><code>base</code> (デフォルト) 基本機能だけをイネーブルにします。基本機能には、マルチキャスト ルーティングと IP 分割が含まれます。</p> <p><code>enhanced</code> ERMS、拡張パケット統計、および拡張 DRPRI をイネーブルにします。マルチキャスト ルーティングと IP 分割がディセーブルになります。</p> <p><code>fail system reload</code> このコマンドと機能は、ML シリーズ カード固有のもので、マイクロコード障害の際に、フラッシュ メモリに情報を保存してリポートするように ML シリーズ カードを設定します。保存される情報は、Cisco TAC で使用されます。TAC へお問い合わせされる場合は、「<a href="#">テクニカル サポート</a>」(p.xxvii)を参照してください。</p> <p><code>mpls</code> MPLS をイネーブルにします。IP マルチキャスト、IP 分割、および ERMS サポートをディセーブルにします。</p>
ステップ 2	Router(config)# <code>exit</code>	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 3	Router# <code>copy running-config startup-config</code>	設定の変更をフラッシュ メモリに保存します。新しいマイクロコード イメージを使用して設定した実行コンフィギュレーション ファイルを ML シリーズ カードのスタートアップ コンフィギュレーション ファイルとして保存し、新しいマイクロコード イメージでリポートします。
ステップ 4	Router# <code>reload</code>	<p>ML シリーズ カードをリセットし、新しいマイクロコード イメージをロードします。</p> <p> <b>注意</b> ML シリーズ カードをリセットすると、トラフィックが損失します。また、カードへの Telnet セッションがすべて閉じられます。</p>
ステップ 5	Router# <code>show microcode</code>	現在ロードされているマイクロコード イメージと、ML シリーズ カードをリセットした場合にロードされるマイクロコード イメージを表示します。

## Cisco IOS のコマンド モード

Cisco IOS ユーザ インターフェイスには複数のモードがあります。使用できるコマンドは、使用中のモードによって異なります。モード別の使用可能コマンド リストを表示するには、システム プロンプトに疑問符 (?) を入力します。

使用頻度が高いモード、そのモードを開始する方法、および表示されるシステム プロンプトを表 3-3 に示します。システム プロンプトによって、どのモードを使用中であることを簡単に識別できるため、使用可能なコマンドも容易に識別できます。



(注)

プロセスが ML シリーズ カードの CPU を大量に消費すると、CPU の応答時間が長くなり、CPUHOG エラー メッセージがコンソールに表示されることがあります。このメッセージでは、イベントによりルーティング テーブル内のルートが大量に更新された場合など、CPU サイクルを大量に使用したプロセスが表示されます。カードのリセットまたは頻繁に発生しないイベントを実行した結果としてこのメッセージが表示された場合は、問題ありません。

表 3-3 Cisco IOS のコマンド モード

モード	用途	アクセス方法	プロンプト
ユーザ EXEC	リモート装置への接続、一時的な端末設定値の変更、基本的なテストの実行、およびシステム情報の表示を行うことができます。	ログインします。	Router>
イネーブル EXEC (イネーブル モードとも呼ぶ)	操作パラメータを設定します。イネーブル コマンド セットには、ユーザ EXEC モードのコマンドと <b>configure</b> コマンドが含まれます。他のコマンド モードにアクセスするには、このコマンド モードを使用します。	ユーザ EXEC モードで、 <b>enable</b> コマンドとイネーブル パスワードを入力します。	Router#
グローバル コンフィギュレーション	システム全体に影響する機能を設定します。	イネーブル EXEC モードで <b>configure terminal</b> コマンドを入力します。	Router(config)#
インターフェイス コンフィギュレーション	特定のインターフェイスの機能をイネーブルにします。インターフェイス コマンドでは、ファストイーサネット ポート、ギガビットイーサネット ポート、または POS ポートの操作をイネーブルにしたり、変更したりできます。	グローバル コンフィギュレーション モードで <b>interface type number</b> コマンドを入力します。  たとえば、ファストイーサネット インターフェイスに対して <b>interface fastethernet 0</b> 、ギガビットイーサネット インターフェイスに対して <b>interface gigabitethernet 0</b> 、Packet over SONET インターフェイスに対して <b>interface pos 0</b> を入力します。	Router(config-if)#

表 3-3 Cisco IOS のコマンドモード (続き)

モード	用途	アクセス方法	プロンプト
ライン コンフィギュレーション	直接接続したコンソールまたは Telnet 接続した仮想端末からコンソールポートまたは vty 回線を設定します。	コンソールポートを設定するには、グローバル コンフィギュレーションモードで <code>line console 0</code> コマンドを入力します。vty 回線を設定するには、グローバル コンフィギュレーションモードで <code>line vty line-number</code> コマンドを入力します。	Router (config-line) #

ML シリーズカードでセッションを開始すると、ユーザ EXEC モードで始まります。ユーザ EXEC モードで使用できるコマンドのサブセットは限られています。すべてのコマンドを実行するには、イネーブル EXEC モード (イネーブルモード) を使用する必要があります。イネーブル EXEC モードでは、すべての EXEC コマンドの入力またはグローバル コンフィギュレーションモードへのアクセスが可能です。ほとんどの EXEC コマンドは、現在の設定ステータスを表示する `show` コマンド、カウンタやインターフェイスをクリアする `clear` コマンドなどのように、一度しか使用しないコマンドです。ML シリーズカードをリブートすると、ブート前に実行した EXEC コマンドは、保存されません。

コンフィギュレーションモードでは、実行コンフィギュレーションを変更できます。コンフィギュレーションを保存すると、ML シリーズカードをリブートしたあともコマンドが保存されます。最初は、グローバル コンフィギュレーションモードから始める必要があります。グローバル コンフィギュレーションモードでは、インターフェイス コンフィギュレーションモード、サブインターフェイス コンフィギュレーションモード、およびプロトコル固有のさまざまなモードに切り替えることができます。

ROMMON モードは、ML シリーズカードを正しくブートできない場合に使用する独立したモードです。たとえば、ML シリーズカードのブート時に有効なシステムイメージが検出されない場合、または起動時にコンフィギュレーションファイルが破損している場合、このカードは ROM モニタモードに入ります。

## コマンドモードの使用

入力したコマンドは、EXEC と呼ばれる Cisco IOS コマンド インタプリタにより解釈および実行されます。コマンドやキーワードは、他のコマンドと区別するのに十分な文字だけを入力して短縮することができます。たとえば、show コマンドは sh に短縮できます。また、configure terminal コマンドは config t に短縮できます。

### 終了

exit と入力すると、ML シリーズカードのレベルが1つ上に戻ります。通常は、exit と入力すると、グローバル コンフィギュレーション モードに戻ります。コンフィギュレーション モードを完全に終了し、イネーブル EXEC モードに戻るには、end コマンドを入力します。

### ヘルプの利用方法

どのコマンドモードでも、疑問符(?)を入力すると、使用可能なコマンドのリストを表示できます。

```
Router> ?
```

特定の文字列で始まるコマンドのリストを表示するには、その文字列の直後に疑問符(?)を続けて入力します。スペースは挿入しないでください。この形式のヘルプは、コマンドワードの完全な形を表示するので、ワードヘルプと呼ばれます。

```
Router# co?
configure
```

キーワードまたは引数のリストを表示するには、キーワードまたは引数の代わりに疑問符(?)を入力します。疑問符の前に1つスペースを挿入します。入力したコマンド、キーワード、および引数に適用できるキーワードまたは引数が表示されるので、この形式のヘルプはコマンドシンタックスヘルプと呼ばれます。

```
Router#configure ?
memory          Configure from NV memory
network         Configure from a TFTP network host
overwrite-network Overwrite NV memory from TFTP network host
terminal       Configure from the terminal
<cr>
```

1つ前に入力したコマンドを再表示するには、上矢印キーを押します。上矢印キーを押し続けると、過去に実行したコマンドがさらに表示されます。



#### ヒント

コマンドの入力ができない場合は、システムプロンプトをチェックし、次に疑問符(?)を入力して利用可能なコマンドのリストを表示します。誤ったコマンドモードやシンタックスを使用している可能性があります。

どのモードからでも Ctrl-Z を押すか、または end と入力すると、イネーブル EXEC (イネーブル) モードに直接戻ることができます。代わりに exit と入力すると、直前のモードに戻ります。



## インターフェイスの設定

---

この章では、ML シリーズカードを起動して実行するための、ML シリーズカードのインターフェイスの基本設定について説明します。Packet-over-SONET/SDH (POS) インターフェイスの高度な設定については、[第 5 章「POS の設定」](#)を参照してください。この章で使用する Cisco IOS コマンドの詳細については、『*Cisco IOS Command Reference*』を参照してください。

この章の内容は次のとおりです。

- [インターフェイスの一般的な注意事項 \(p.4-2\)](#)
- [インターフェイスの基本設定 \(p.4-4\)](#)
- [ファストイーサネット、ギガビットイーサネット、および POS インターフェイスの基本設定 \(p.4-6\)](#)
- [ファストイーサネットインターフェイスとギガビットイーサネットインターフェイスのモニタリング操作 \(p.4-11\)](#)



**(注)** ML シリーズカードの初期設定が完了してからインターフェイスを設定してください。

---

## インターフェイスの一般的な注意事項

ML シリーズ カードの主な機能はデータリンク間でパケットを中継することです。したがって、パケットを送受信するインターフェイスの特性を設定する必要があります。インターフェイスの特性には IP アドレス、ポートのアドレス、データ カプセル化方式、およびメディア タイプなどがあります。

多数の機能がインターフェイスごとにイネーブルにできます。インターフェイス コンフィギュレーション モードには、イーサネット ポートなどのインターフェイスの動作を修正するコマンドがあります。interface コマンドを入力する場合は、インターフェイスのタイプと番号を指定する必要があります。

次の一般的な注意事項は、すべての物理インターフェイスと仮想インターフェイスの設定に当てはまります。

- すべてのインターフェイスに名前があります。名前はインターフェイス タイプ (ワード) とポート ID (番号) から成ります。例としては、FastEthernet 2 があります。
- それぞれのインターフェイスは、ブリッジグループ、または IP アドレスと IP サブネットマスクを使用して設定します。
- VLAN (仮想 LAN) はサブインターフェイスを使用することによりサポートされます。サブインターフェイスとは、関連付けられた物理インターフェイスとは別に設定された論理インターフェイスです。
- 内部 POS インターフェイスを含め、それぞれの物理インターフェイスには、MAC (メディアアクセス制御) アドレスが割り当てられています。

## MAC アドレス

イーサネット ネットワークに接続するポートまたは装置には、MAC アドレスが必要です。ネットワークの他の装置が、特定のポートをネットワーク内で検索したり、ルーティングテーブルとデータ構造を作成および更新したりするために MAC アドレスを使用します。

装置の MAC アドレスを検索するには、**show interfaces** コマンドを次のように使用します。

```
Router# sh interfaces fastEthernet 0
FastEthernet0 is up, line protocol is up
  Hardware is epif_port, address is 0005.9a39.6634 (bia 0005.9a39.6634)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, Auto Speed, 100BaseTX
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:18, 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 :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    11 packets input, 704 bytes
      Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 11 multicast
    0 input packets with dribble condition detected
    3 packets output, 1056 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 output buffer failures, 0 output buffers swapped out
```

## インターフェイス ポート ID

インターフェイス ポート ID によって、ML シリーズ カードのインターフェイスの物理的な位置が指定されます。この ID は、設定するインターフェイスを特定する名前です。システム ソフトウェアは、インターフェイス ポート ID を使用して ML シリーズ カード活動状況を制御し、ステータス情報を表示します。インターフェイス ポート ID は、ネットワークの他の装置が使用することではなく、個々の ML シリーズ カードおよびその内部のコンポーネントとソフトウェアに固有です。

ML100T-12 では、12 個のファストイーサネット インターフェイスのポート ID は Fast Ethernet 0 ~ 11 です。ML100X-8 では、8 個のファストイーサネット インターフェイスのポート ID は Fast Ethernet 0 ~ 7 です。ML1000-2 では、2 個のギガビットイーサネット インターフェイスのポート ID は Gigabit Ethernet 0 ~ 1 です。どちらの ML シリーズ カードにも 2 個の POS ポートがあり、これらの 2 個の POS インターフェイスの ML シリーズ ポート ID は POS 0 と POS 1 です。ポート ID には、ユーザ定義の省略形を使用できます。たとえば、ファストイーサネット インターフェイスの設定には f0、2 個のギガビットイーサネット インターフェイスの設定には gi0 または gi1、2 個の POS ポートの設定には POS0 と POS1 にすることができます。

Cisco IOS の show コマンドを使用すると、ML シリーズ カードの任意またはすべてのインターフェイスに関する情報を表示できます。



### 注意

ギガビットイーサネットのユーザ定義の省略形として、g0 または g1 を使用しないでください。使用すると、サポートされないグループ非同期インターフェイスが作成されます。

## インターフェイスの基本設定

次の一般的な設定方法は、すべてのインターフェイスに当てはまります。インターフェイスを設定する前に、ブリッジまたはルーティングされるネットワークの計画を作成しておいてください。

インターフェイスを設定するには、次の手順を実行します。

- ステップ 1** イネーブル EXEC プロンプトで **configure EXEC** コマンドを入力してグローバル コンフィギュレーション モードを開始します。

```
Router> enable
Password:
Router# configure terminal
Router(config)#
```

- ステップ 2** **interface** コマンド、インターフェイス タイプ (fastethernet、gigabitethernet、pos など)、インターフェイス ポート ID (「[インターフェイス ポート ID](#)」 [p.4-3] を参照) の順に入力します。

たとえば、ギガビット イーサネット ポートを 1 つ設定するには、次のコマンドを入力します。

```
Router(config)# interface gigabitethernet number
```

- ステップ 3** **interface** コマンドの入力後に、設定するインターフェイスに必要なインターフェイス設定コマンドを入力します。

入力するコマンドによって、インターフェイス上で実行するプロトコルとアプリケーションが定義されます。ML シリーズ カードは、**interface** コマンドがもう一度入力されるか、またはインターフェイス コンフィギュレーション コマンド以外のコマンドが入力されるまで、コマンドを集め、**interface** コマンドに適用します。**end** を入力してイネーブル EXEC モードに戻ることもできます。

**ステップ 4** EXEC の `show interface` コマンドを入力して、設定したインターフェイスのステータスを確認します。

```
Router# sh interface fastEthernet 0
FastEthernet0 is up, line protocol is up
Hardware is epif_port, address is 0005.9a39.6634 (bia 0005.9a39.6634)
MTU 1500 bytes, BW 100000 Bit, DLY 100 use,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, Auto Speed, 100BaseTX
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:01, output 00:00:18, 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 :0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  11 packets input, 704 bytes
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 watchdog, 11 multicast
  0 input packets with dribble condition detected
  3 packets output, 1056 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 output buffer failures, 0 output buffers swapped out
```

---

## ファストイーサネット、ギガビットイーサネット、および POS インターフェイスの基本設定

ML シリーズ カードは、ファストイーサネット、ギガビットイーサネット、および POS の各インターフェイスをサポートしています。ここでは、すべてのインターフェイスタイプの設定例をいくつか説明します。

ファストイーサネット、ギガビットイーサネット、または POS のインターフェイスに IP アドレスまたはブリッジ グループ番号を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>interface</b> <i>type number</i>	インターフェイス コンフィギュレーション モードを起動して、ギガビットイーサネットインターフェイス、ファストイーサネットインターフェイス、または POS インターフェイスのいずれかを設定します。
ステップ 2	Router(config-if)# { <b>ip address</b> <i>ip-address subnet-mask</i>   <b>bridge-group</b> <i>bridge-group-number</i> }	インターフェイスに割り当てる IP アドレスと IP サブネットマスクを設定します。  または ネットワークインターフェイスをブリッジグループに割り当てます。
ステップ 3	Router(config-if)# <b>no shutdown</b>	インターフェイスがシャットダウンしないようにすることにより、インターフェイスをイネーブルにします。
ステップ 4	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更をタイミング制御用カード (TCC2/TCC2P) のフラッシュ データベースに保存します。

### ファストイーサネット インターフェイスの設定 (ML100T-12)

ML100T-2 ファストイーサネットインターフェイス上で IP アドレスまたはブリッジグループ番号、速度、デュプレックス、およびフロー制御を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>interface fastethernet</b> <i>number</i>	インターフェイス コンフィギュレーション モードを起動してファストイーサネットインターフェイスを設定します。
ステップ 2	Router(config-if)# { <b>ip address</b> <i>ip-address subnet-mask</i>   <b>bridge-group</b> <i>bridge-group-number</i> }	インターフェイスに割り当てる IP アドレスと IP サブネットマスクを設定します。  または ネットワークインターフェイスをブリッジグループに割り当てます。

	コマンドの説明	目的
ステップ 3	Router(config-if)# [no] speed {10   100   auto}	伝送速度を 10 または 100 Mbps に設定します。speed または duplex を auto に設定した場合、システムで自動ネゴシエーションがイネーブルになります。この場合、ML シリーズ カードはパートナー ノードの speed および duplex モードと一致します。
ステップ 4	Router(config-if)# [no] duplex {full   half   auto}	全二重モード、半二重モード、または自動ネゴシエーション モードを設定します。
ステップ 5	Router(config-if)# flowcontrol send {on   off   desired}	(任意) インターフェイスのフロー制御送信値を設定します。フロー制御は、ポートレベルのポリシングを使用した場合にのみ機能します。ML シリーズ カードのファストイーサネット ポートのフロー制御は IEEE 802.3x 準拠です。  (注) ファストイーサネット ポートは対称フロー制御のみをサポートしているので、flowcontrol send コマンドは送受信両方のフロー制御動作を制御します。
ステップ 6	Router(config-if)# no shutdown	インターフェイスがシャットダウンしないようにすることにより、インターフェイスをイネーブルにします。
ステップ 7	Router(config)# end	イネーブル EXEC モードに戻ります。
ステップ 8	Router# copy running-config startup-config	(任意) 設定の変更を TCC2/TCC2P フラッシュ データベースに保存します。

例 4-1 に、IP アドレスと自動ネゴシエーションを使用した ML100T-12 ファストイーサネット インターフェイスの初期設定方法を示します。

#### 例 4-1 ML100T-12 ファストイーサネット インターフェイスの初期設定

```
Router(config)# interface fastethernet 1
Router(config-if)# ip address 10.1.2.4 255.0.0.0
Router(config-if)# negotiation auto
Router(config-if)# no shutdown
Router(config-if)# end
Router# copy running-config startup-config
```

## ファストイーサネット インターフェイスの設定 (ML100X-8)

ML 100X-8 は、100BASE-FX 全二重データ伝送をサポートしています。ファストイーサネット インターフェイスでは、自動ネゴシエーションや速度を設定できません。またカードには、デフォルトで Automatic Media-Dependent Interface crossover( Auto-MDIX; 自動メディア依存型インターフェイス クロスオーバー) 機能がイネーブルに設定されています。Auto-MDIX は、必要なケーブル接続タイプ(ストレートまたはクロス)を検出し、接続設定を適切に行います。ファストイーサネット インターフェイス上で IP アドレス、ブリッジ グループ番号、またはフロー制御を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

## ■ ファストイーサネット、ギガビットイーサネット、およびPOSインターフェイスの基本設定

	コマンドの説明	目的
ステップ 1	Router(config)# <b>interface fastethernet</b> <i>number</i>	インターフェイス コンフィギュレーション モードを起動してファストイーサネットインターフェイスを設定します。
ステップ 2	Router(config-if)# { <b>ip address</b> <i>ip-address</i> <i>subnet-mask</i>   <b>bridge-group</b> <i>bridge-group-number</i> }	インターフェイスに割り当てる IP アドレスと IP サブネットマスクを設定します。  または  ネットワーク インターフェイスをブリッジグループに割り当てます。
ステップ 3	Router(config-if)# <b>flowcontrol send</b> { <i>on</i>   <i>off</i>   <i>desired</i> }	(任意)インターフェイスのフロー制御送信値を設定します。フロー制御は、ポートレベルのポリシングを使用した場合にのみ機能します。ML シリーズカードのファストイーサネットポートのフロー制御は IEEE 802.3x 準拠です。   (注) ファストイーサネットポートは対称フロー制御のみをサポートしているため、 <b>flowcontrol send</b> コマンドは送受信両方のフロー制御動作を制御します。
ステップ 4	Router(config-if)# <b>no shutdown</b>	インターフェイスがシャットダウンしないようにすることにより、インターフェイスをイネーブルにします。
ステップ 5	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 6	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を TCC2/TCC2P フラッシュデータベースに保存します。

## ギガビットイーサネットインターフェイスの設定 (ML1000-2)

ML1000-2 ギガビットイーサネットインターフェイス上で IP アドレスまたはブリッジグループ番号、自動ネゴシエーション、およびフロー制御を設定するには、グローバルコンフィギュレーションモードで次の手順を実行します。



(注) ネゴシエーションモードのデフォルト設定は、ギガビットイーサネットおよびファストイーサネットのインターフェイスの場合は **auto** です。ギガビットイーサネットポートは、常に全二重モードの 1000 Mbps で動作します。

	コマンドの説明	目的
ステップ 1	Router# <b>interface gigabitethernet</b> <i>number</i>	インターフェイス コンフィギュレーション モードを起動してギガビットイーサネット インターフェイスを設定します。
ステップ 2	Router(config-if)# { <b>ip address</b> <i>ip-address</i> <i>subnet-mask</i>   <b>bridge-group</b> <i>bridge-group-number</i> }	IP アドレスおよびサブネット マスクを設定します。  または  ネットワーク インターフェイスをブリッジ グループに割り当てます。
ステップ 3	Router(config-if)# [ <b>no</b> ] <b>negotiation auto</b>	ネゴシエーション モードを <b>auto</b> に設定します。ギガビットイーサネット ポートはパートナー ポートとリンクのネゴシエーションを試行します。  パートナー ポートの設定に関係なく、このポートでリンクを強制的に起動する場合は、ギガビットイーサネット インターフェイスを <b>no negotiation auto</b> に設定します。
ステップ 4	Router(config-if)# <b>flowcontrol</b> { <b>send</b>   <b>receive</b> } { <b>on</b>   <b>off</b>   <b>desired</b> }	(任意) インターフェイスに送信または受信のフロー制御値を設定します。フロー制御は、ポートレベルのポリシングを使用した場合にのみ機能します。ML シリーズカードのギガビットイーサネット ポートのフロー制御は IEEE 802.3z 準拠です。
ステップ 5	Router(config-if)# <b>no shutdown</b>	インターフェイスがシャット ダウンしないようにすることにより、インターフェイスをイネーブルにします。
ステップ 6	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 7	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を TCC2/TCC2P フラッシュ データベースに保存します。

例 4-2 に、自動ネゴシエーションと IP アドレスを使用したギガビットイーサネット インターフェイスの初期設定方法を示します。

#### 例 4-2 ギガビットイーサネット インターフェイスの初期設定

```
Router(config)# interface gigabitethernet 0
Router(config-if)# ip address 10.1.2.3 255.0.0.0
Router(config-if)# negotiation auto
Router(config-if)# no shutdown
Router(config-if)# end
Router# copy running-config startup-config
```

## POS インターフェイスの設定 (ML100T-12、ML100X-8、および ML1000-2)

POS ポートでカプセル化を変更できるのは、インターフェイスが手動でシャットダウン (ADMIN\_DOWN) されているときだけです。POS インターフェイスの高度な設定については、第 5 章「POS の設定」を参照してください。

POS インターフェイスの IP アドレス、ブリッジ グループ、カプセル化を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

## ■ ファストイーサネット、ギガビットイーサネット、および POS インターフェイスの基本設定

	コマンドの説明	目的
ステップ 1	Router(config)# <b>interface pos number</b>	インターフェイス コンフィギュレーション モードを起動して POS インターフェイスを設定します。
ステップ 2	Router(config-if)# { <b>ip address ip-address subnet-mask</b>   <b>bridge-group bridge-group-number</b> }	IP アドレスおよびサブネット マスクを設定します。  または  ネットワーク インターフェイスをブリッジ グループに割り当てます。
ステップ 3	Router(config-if)# <b>shutdown</b>	インターフェイスを手動でシャット ダウンします。POS ポートでカプセル化を変更できるのは、インターフェイスがシャットダウン (ADMIN_DOWN) されているときだけです。
ステップ 4	Router(config-if)# <b>encapsulation type</b>	カプセル化のタイプを設定します。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• <b>hdlc</b> Cisco HDLC</li> <li>• <b>lex</b> (デフォルト) LAN 拡張。Cisco ONS イーサネット ライン カードと併用するための特殊なカプセル化</li> <li>• <b>ppp</b> ポイントツーポイント プロトコル</li> </ul>
ステップ 5	Router(config-if)# <b>no shutdown</b>	シャットダウンされているインターフェイスを再起動します。
ステップ 6	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 7	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM (不揮発性 RAM) に保存します。

## ファストイーサネット インターフェイスとギガビットイーサネット インターフェイスのモニタリング操作

インターフェイスを設定したあとに設定を確認するには、`show interface` コマンドを入力します。POS インターフェイス上の動作に対するモニタリングの詳細については、「[POS の設定](#)」の章を参照してください。

例 4-3 に `show interface` コマンドの出力を示します。ポート速度とデュプレックス動作を含むインターフェイスのステータスが表示されます。

### 例 4-3 show interface コマンドの出力

```
Router# show interface fastEthernet 0
FastEthernet1 is administratively down, line protocol is down
Hardware is epif_port, address is 000d.bd5c.4c85 (bia 000d.bd5c.4c85)
MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Auto-duplex, Auto Speed, 100BaseTX
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: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
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
Received 0 broadcasts (0 IP multicast)
0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast
0 input packets with dribble condition detected
0 packets output, 0 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 output buffer failures, 0 output buffers swapped out
```

ファストイーサネット コントローラ チップに関する情報を表示するには、`show controller` コマンドを入力します。

例 4-4 に、`show controller` コマンドの出力を示します。初期化ブロック情報を含む統計情報が表示されます。

**例 4-4 show controller コマンドの出力**

```

Router# show controller fastEthernet 0
IF Name: FastEthernet0
Port Status DOWN
Send Flow Control      : Disabled
Receive Flow Control   : Enabled
MAC registers
CMCR : 0x0000042D (Tx Enabled, Rx Disabled)
CMPR : 0x150B0A80 (Long Frame Disabled)
FCR  : 0x0000A00B (Rx Pause detection Enabled)
MII registers:
Control Register          (0x0): 0x4000 (Auto negotiation disabled)
Status Register          (0x1): 0x7809 (Link status Down)
PHY Identification Register 1 (0x2): 0x40
PHY Identification Register 2 (0x3): 0x61D4
Auto Neg. Advertisement Reg (0x4): 0x1E1 (Speed 100, Duplex Full)
Auto Neg. Partner Ability Reg (0x5): 0x0 (Speed 10, Duplex Half)
Auto Neg. Expansion Register (0x6): 0x4
100Base-X Aux Control Reg   (0x10): 0x2000
100Base-X Aux Status Register(0x11): 0x0
100Base-X Rcv Error Counter (0x12): 0x0
100Base-X False Carr. Counter(0x13): 0x0

```

ファストイーサネットインターフェイスの設定に関する情報を表示するには、**show run interface [type number]** コマンドを入力します。複数のインターフェイスがあり、特定のインターフェイスの設定を表示する場合にこのコマンドは便利です。

**例 4-5** に、**show run interface [type number]** コマンドの出力を示します。IP アドレスまたは IP アドレスの未指定、およびインターフェイスの状態に関する情報が含まれます。

**例 4-5 show run interface コマンドの出力**

```

daytona# show run interface FastEthernet 1
Building configuration...

Current configuration : 56 bytes
!
interface FastEthernet1
no ip address
shutdown

end

```



## POS の設定

---

この章では、ML シリーズ カードの Packet-over-SONET/SDH ( POS ) インターフェイスの高度な設定について説明します。POS インターフェイスの基本設定については、[第 4 章「インターフェイスの設定」](#)を参照してください。この章で使用する Cisco IOS コマンドの詳細については、『*Cisco IOS Command Reference*』を参照してください。ML シリーズ カードを含め、ONS イーサネットカードでの POS 操作については [第 20 章「ONS イーサネットカード上の POS」](#)を参照してください。

この章の内容は次のとおりです。

- [ML シリーズ カード上の POS \( p.5-2 \)](#)
- [POS のモニタリングと確認 \( p.5-11 \)](#)
- [POS の設定例 \( p.5-13 \)](#)

## ML シリーズカード上の POS

イーサネット パケットおよび IP データ パケットは、SONET/SDH ネットワーク上で転送するために、SONET/SDH フレームにフレーム化およびカプセル化する必要があります。このフレーミングおよびカプセル化処理は POS として知られ、ML シリーズカードで行われます。POS の詳細については、第 20 章「ONS イーサネットカード上の POS」を参照してください。

ML シリーズカードには、カード前面にある標準のイーサネットポート、および仮想 POS ポートがあり、これらすべてのポートがスイッチポートとして装備されています。Cisco IOS では、POS ポートは ML シリーズカード上の他のイーサネットインターフェイスに類似したインターフェイスです。通常は、トランクポートとして使用されます。IEEE 802.1 Q VLAN (仮想 LAN) 設定など、多くの Cisco IOS の標準機能は、標準イーサネットインターフェイスと同じように POS インターフェイスに設定されています。一部の機能と設定は、厳密に POS インターフェイスだけで行われます。POS ポートに限定された機能の設定については、この章内で説明しています。

## ML シリーズの SONET および SDH の回線サイズ

SONET は、51.840 Mbps (STS-1) ~ 2.488 Gbps (STS-48) 以上の階層レートを持つ光デジタル伝送用 American National Standards Institute (ANSI; 米国規格協会) 標準 (T1.1051988) です。SDH は、155.520 Mbps (STM-1) ~ 2.488 Gbps (STM-16) 以上の階層レートを持つ光デジタル伝送用国際標準です。

SONET および SDH の両方とも、基本フレームと速度を備えた構造に基づいています。SONET で使用するフレーム形式は Synchronous Transport Signal (STS; 同期転送信号) であり、STS-1 が 51.84 Mbps の基本レベル信号です。STS-1 フレームは OC-1 信号で伝送できます。SDH で使用するフレーム形式は Synchronous Transport Module (STM; 同期転送モジュール) であり、STM-1 が 155.52 Mbps の基本レベル信号です。STM-1 フレームは OC-3 信号で伝送できます。

SONET および SDH はともに、信号速度が階層化されています。複数の低レベルの信号を多重化して、高レベルの信号を形成できます。たとえば、3 つの STS-1 信号を多重化して 1 つの STS-3 信号を構成したり、4 つの STM-1 信号を多重化して 1 つの STM-4 信号を構成したりすることができます。

SONET の回線サイズは STS-n として定義されます。ここで、n は 51.84 Mbps の倍数で、1 以上です。SDH の回線サイズは STM-n として定義されます。ここで、n は 155.52 Mbps の倍数で、0 以上です。表 5-1 に、STS および STM の回線レート相当値を示します。

表 5-1 回線レート Mbps での SONET STS 回線容量

SONET 回線サイズ	SDH 回線サイズ	回線レート (Mbps)
STS-1 (OC-1)	VC-3 <sup>1</sup>	52 Mbps
STS-3c (OC-3)	STM-1 (VC4)	156 Mbps
STS-6c (OC-6)	STM-2 (VC4-2c)	311 Mbps
STS-9c (OC-9)	STM-3 (VC4-3c)	466 Mbps
STS-12c (OC-12)	STM-4 (VC4-4c)	622 Mbps
STS-24c (OC-24)	STM-8 (VC4-8c)	1244 Mbps (1.24 Gbps)

1. VC-3 回線サポートでは、XCVL カードを取り付ける必要があります。

ML シリーズカードの SONET STS 回線の詳細な設定手順については、『Cisco ONS 15454 Procedure Guide』の「Create Circuits and VT Tunnels」の章を参照してください。ML シリーズカードの SDH STM 回線の詳細な設定手順については、『Cisco ONS 15454 SDH Procedure Guide』の「Create Circuits and Tunnels」の章を参照してください。

## VCAT

Virtual Concatenation (VCAT; バーチャル コンカチネーション) を使用すると、連続していない SONET/SDH フレームの Synchronous Payload Envelope (SPE; 同期ペイロード エンベロープ) を VCAT グループにグループ化できるので、SONET/SDH 上のデータ転送効率が大きく向上します。VCAT グループの回線帯域幅は、VCAT メンバーという、より小さい回線に分割されます。各メンバーは、独立した回線として機能します。

VCAT メンバーは、中継ノードでは、SONET/SDH ネットワークによって独立的にルーティングおよび保護される通常の回線として処理されます。終端ノードでは、これらのメンバー回線が、連続的なデータストリームに多重化されます。VCAT では、SONET/SDH 帯域幅のフラグメンテーションの問題が防止され、帯域幅サービスをより細かい単位で設定できます。

また、ONS 15454 SONET および ONS 15454 SDH ML シリーズカードの VCAT 回線は、通常のファイバ経由でルーティングし、双方向かつ対称である必要があります。High Order (HO; 高次) VCAT 回線だけがサポートされています。ML シリーズカードでは、最大 2 つの VCAT グループがサポートされ、各グループが POS ポートの 1 つに対応します。各 VCAT グループには、2 つの回線メンバーを含むことができます。ML シリーズカードを起点とする VCAT 回線は、別の ML シリーズカードまたは CE シリーズカードで終端させる必要があります。表 5-2 に、ML シリーズカードがサポートする VCAT の回線サイズを示します。

表 5-2 ML100T-12、ML100X-8、ML1000-2 カードでサポートされる VCAT 回線サイズ

SONET VCAT 回線サイズ	SDH VCAT 回線サイズ
STS-1-2v	VC-3-2v
STS-3c-2v	VC-4-2v
STS-12c-2v	VC-4-4c-2v

ML シリーズカードの SONET VCAT 回線の詳細な設定手順については、『Cisco ONS 15454 Procedure Guide』の「Create Circuits and VT Tunnels」の章を参照してください。ML シリーズカードの SDH VCAT 回線の詳細な設定手順については、『Cisco ONS 15454 SDH Procedure Guide』の「Create Circuits and Tunnels」の章を参照してください。VCAT 回線全般については、『Cisco ONS 15454 Reference Manual』または『Cisco ONS 15454 SDH Reference Manual』の「Circuits and Tunnels」の章を参照してください。



(注)

ML シリーズカードの POS インターフェイスは通常、POS リンクがダウンまたは RPR がラップしたときに、ONS 15454 STS パス オーバーヘッド (PDI-P) の信号ラベル ミスマッチ障害に関するアラームを遠端に送信します。PDI-P が検出されたとき、Remote Defection Indication - Path (RDI-P; リモート障害表示 パス) アラームが遠端に送信されているとき、または検出された障害が Generic Framing Procedure (GFP) -Loss of Frame Delineation (LFD)、GFP Client Signal Fail (CSF)、Virtual Concatenation (VCAT) -Loss of Multiframe (LOM) または VCAT-Loss of Sequence (SQM) の場合は、ML シリーズカードの POS インターフェイスは PDI-P を遠端に送信しません。



(注)

DCC (オープンエンド ノード) によって接続されていないノードの場合は、VCAT を TL-1 経由で設定する必要があります。

## SW-LCAS

Link Capacity Adjustment Scheme (LCAS; リンク キャパシティ調整方式)を使用すると、関係しないメンバーの動作を中断せずに VCAT グループを動的に再設定できるので VCAT の柔軟性が向上します。Software Link Capacity Adjustment Scheme (SW-LCAS; ソフトウェア リンク キャパシティ調整方式)は、LCAS タイプの機能をソフトウェアで実装したものです。SW-LCAS は、LCAS と異なり、エラーが発生することがあるだけでなく、異なるハンドシェイク メカニズムを使用します。

ONS-15454 SONET/SDH ML シリーズカードの SW-LCAS では、2 ファイバ Bidirectional Line Switched Ring (BLSR; 双方向ライン スイッチ型リング)で障害または回復が発生した場合に、VCAT グループのメンバーを自動的に追加または削除できます。保護メカニズム ソフトウェアは、ML シリーズカードのリンク イベントに基づいて動作します。サービス プロバイダーは、SW-LCAS を使用すると、ML シリーズカード上の VCAT メンバーの回線を Protection Channel Access (PCA; 保護チャネル アクセス) 回線として設定できます。この PCA トラフィックは、保護切り替え時にドロップされますが、過剰なトラフィックやコミットされていないトラフィックには適しており、その回線で使用可能な帯域幅を倍増させることができます。

SW-LCAS の詳細な設定手順については、『Cisco ONS 15454 Procedure Guide』の「Create Circuits and VT Tunnels」の章または『Cisco ONS 15454 SDH Procedure Guide』の「Create Circuits and Tunnels」の章を参照してください。SW-LCAS 全般については、『Cisco ONS 15454 Reference Manual』または『Cisco ONS 15454 SDH Reference Manual』の「Circuits and Tunnels」の章を参照してください。

## フレーミングモード、カプセル化、および CRC のサポート

ONS 15454 および ONS 15454 SDH 上の ML シリーズカードは、POS フレーミング メカニズムの2つのモードである、GFP-F フレーミングと High-Level Data Link Control (HDLC; ハイレベル データリンク制御) フレーミング (デフォルト) をサポートします。送信元 POS ポートと宛先 POS ポートのフレーミングモード、カプセル化、および CRC サイズは、POS 回線が正常に動作するために一致する必要があります。フレーミング メカニズム、カプセル化、および Cyclic Redundancy Check (CRC; 巡回冗長検査) ビット サイズの詳細については、第 20 章「ONS イーサネットカード上の POS」を参照してください。

表 5-3 に、フレーミング タイプでサポートされているカプセル化および CRC サイズの詳細を示します。

表 5-3 ONS 15454 および ONS 15454 SDH 上の ML シリーズカードでサポートされているカプセル化、フレーミング、および CRC サイズ

	HDLC フレーミングの カプセル化	HDLC フレーミングの CRC サイズ	GFP-F フレーミングの カプセル化	GFP-F フレーミングの CRC サイズ
ML シリーズ	LEX (デフォルト)  Cisco HDLC  PPP/BCP	16 ビット  32 ビット (デフォルト)	LEX (デフォルト)  Cisco HDLC  PPP/BCP	32 ビット (デフォルト)



(注)

ML シリーズカードの POS インターフェイスは通常、POS リンクがダウンまたは RPR がラップしたときに、PDI-P を遠端に送信します。PDI-P が検出されたとき、RDI-P が遠端に送信されているとき、検出された障害が GFP LFD、GFP CSF、VCAT LOM または VCAT SQM の場合には、ML シリーズカードの POS インターフェイスは PDI-P を遠端に送信しません。

## POS インターフェイス フレーミング モード の設定

ML シリーズカードのフレーミングモードは、CTC から設定します。CTC でのフレーミングモードの設定の詳細については、第2章「CTC の動作」を参照してください。

## POS インターフェイス カプセル化タイプの設定

デフォルトの Cisco EoS LEX は ONS イーサネットカードの主要なカプセル化方式です。このカプセル化は、HDLC フレーミングのもと、Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) の Request For Comments (RFC; コメント要求) 1841 で指定された値にプロトコルフィールドを設定した状態で使用されます。GFP-F フレーミング下では、Cisco IOS CLI もキーワード `lex` を使用します。GFP-F フレーミングでは、`lex` キーワードは ITU-T G.7041 に基づいた GFP-F 上の標準マップイーサネットを表すために使用されます。

ML シリーズカードのカプセル化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次の手順を実行します。

	コマンドの説明	目的
ステップ 1	<code>Router(config)# interface pos number</code>	インターフェイス コンフィギュレーション モードを起動して POS インターフェイスを設定します。
ステップ 2	<code>Router(config-if)# shutdown</code>	インターフェイスを手動でシャットダウンします。POS ポートでカプセル化を変更できるのは、インターフェイスがシャットダウン (ADMIN_DOWN) されているときだけです。
ステップ 3	<code>Router(config-if)# encapsulation type</code>	カプセル化のタイプを設定します。有効な値は次のとおりです。 <ul style="list-style-type: none"> <li>• <code>hdlc</code> Cisco HDLC</li> <li>• <code>lex</code> (デフォルト) LAN 拡張。Cisco ONS イーサネット ライン カードと併用するための特殊なカプセル化。GFP-F フレーミングで <code>lex</code> キーワードが使用される場合、ITU-T G.7041 に基づいた GFP-F 上の標準マップイーサネットになります。</li> <li>• <code>ppp</code> ポイントツーポイントプロトコル</li> </ul>
ステップ 4	<code>Router(config-if)# no shutdown</code>	シャットダウンされているインターフェイスを再起動します。
ステップ 5	<code>Router(config)# end</code>	イネーブル EXEC モードに戻ります。
ステップ 6	<code>Router# copy running-config startup-config</code>	(任意) 設定の変更を NVRAM (不揮発性 RAM) に保存します。

## HDLC フレーミングの POS インターフェイス CRC サイズの設定

遠端のインターフェイスのプロパティと一致させるために追加のプロパティを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>interface pos number</b>	インターフェイス コンフィギュレーション モードを起動して POS インターフェイスを設定します。
ステップ 2	Router(config-if)# <b>crc {16   32}</b>	HDLC フレーミングの CRC 値を設定します。POS モジュールに接続している装置がデフォルト CRC 値の 32 をサポートしない場合は、16 の値を使用するように両方の装置を設定します。   (注) CRC 値は、GFP-F フレーミングでは 32 に固定されます。
ステップ 3	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM (不揮発性 RAM) に保存します。

## MTU サイズの設定

Maximum Transmission Unit (MTU; 最大伝送ユニット) サイズを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>interface pos number</b>	インターフェイス コンフィギュレーション モードを起動して POS インターフェイスを設定します。
ステップ 2	Router(config-if)# <b>mtu bytes</b>	最大 9000 バイトまでの MTU サイズを設定します。デフォルトの MTU サイズについては表 5-4 を参照してください。
ステップ 3	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM (不揮発性 RAM) に保存します。

表 5-4 に、デフォルトの MTU サイズを示します。

表 5-4 デフォルトの MTU サイズ

カプセル化タイプ	デフォルト サイズ
LEX (デフォルト)	1500
HDLC	4470
PPP	4470

## キープアライブメッセージの設定

ML シリーズカードのキープアライブメッセージを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>interface pos number</b>	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、設定する POS インターフェイスを指定します。
ステップ 2	Router(config-if)# <b>[no] keepalive</b>	キープアライブメッセージを設定します。  キープアライブメッセージはデフォルトでオンになっています。必須ではありませんが、オンにするなら推奨します。  このコマンドの no 形式はキープアライブメッセージをオフにします。
ステップ 3	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM (不揮発性 RAM) に保存します。

## SONET/SDH アラーム

ML シリーズカードは、Cisco IOS および CTC/TL1 で SONET/SDH アラームをレポートします。多数のパスアラームが Cisco IOS コンソールにレポートされます。Cisco IOS コンソールのアラームレポートを設定しても、CTC のアラームレポートには影響しません。「[SONET/SDH アラームの設定](#)」の手順では、Cisco IOS コンソールにレポートするアラームを指定します。

CTC/TL1 には、高度な SONET/SDH アラームのレポート機能があります。ONS ノードのカードとして、ML シリーズカードは他の ONS カードと同様に、CTC/TL-1 にアラームをレポートします。ONS 15454 SONET で ML シリーズカードを使用する場合は、このカードの CTC の Alarms パネルに Telcordia GR-253 SONET アラームがレポートされます。アラームとアラームの定義の詳細については、『[Cisco ONS 15454 Troubleshooting Guide](#)』または『[Cisco ONS 15454 SDH Troubleshooting Guide](#)』の「Alarm Troubleshooting」の章を参照してください。

## SONET/SDH アラームの設定

デフォルトではすべての SONET/SDH アラームが表示されますが、Cisco IOS の CLI での SONET/SDH アラームのレポートをプロビジョニングするには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>interface pos number</b>	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、設定する POS インターフェイスを指定します
ステップ 2	Router(config-if)# <b>pos report {all   encap   pais   plop   ppdi   pplm   prdi   ptim   puneq   sd-ber-b3   sf-ber-b3}</b>	<p>選択した SONET/SDH アラームのコンソール ロギングを許可します。特定のアラームのレポートを無効にするには、このコマンドの <b>no</b> 形式を使用します。</p> <p>アラームの種類は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>all</b> すべてのアラーム / 信号</li> <li>• <b>encap</b> パスのカプセル化ミスマッチ</li> <li>• <b>pais</b> パス アラーム表示信号</li> <li>• <b>plop</b> パス ポインタ喪失</li> <li>• <b>ppdi</b> パス ペイロード障害表示</li> <li>• <b>pplm</b> ペイロードラベル、C2 ミスマッチ</li> <li>• <b>prdi</b> パス リモート障害表示</li> <li>• <b>ptim</b> パス トレース ID ミスマッチ</li> <li>• <b>puneq</b> ゼロと同等のパス ラベル</li> <li>• <b>sd-ber-b3</b> PBIP BER SD スレッシュホールド超過</li> <li>• <b>sf-ber-b3</b> PBIP BER SF スレッシュホールド超過</li> </ul>
ステップ 3	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります
ステップ 4	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM (不揮発性 RAM) に保存します

POS インターフェイスでレポートするアラームを決定して BER スレッシュホールドを表示するには、**show controllers pos** コマンドを使用します。「[POS のモニタリングと確認](#)」(p.5-11)を参照してください。



(注)

Cisco IOS アラーム レポート コマンドは、Cisco IOS の CLI のみに適用されます。TCC2/TCC2P にレポートされる SONET/SDH アラームは影響を受けません。

## SONET/SDH 遅延トリガーの設定

リストされているパス アラームをトリガーとして設定して、POS インターフェイスのライン プロトコルをダウンさせることができます。パス アラームをトリガーとして設定する場合は、**pos trigger delay** コマンドを使用してトリガーの遅延を指定することもできます。遅延は 200 ~ 2000 ミリ秒に設定できます。間隔を指定しないと、遅延はデフォルトの 200 ミリ秒に設定されます。

パス アラームをトリガーとして設定して遅延を指定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>interface pos number</b>	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、設定する POS インターフェイスを指定します。
ステップ 2	Router(config-if)# <b>pos trigger defect</b> {all   <b>ber_sf_b3</b>   <b>encap</b>   <b>pais</b>   <b>plop</b>   <b>ppdi</b>   <b>pplm</b>   <b>prdi</b>   <b>ptim</b>   <b>puneq</b> }	<p>特定のバス障害をトリガーとして設定して、POS インターフェイスをダウンさせます。設定可能なトリガーは次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>all</b> すべてのリンク ダウン アラーム障害</li> <li>• <b>ber_sd_b3</b> PBIP BER SD スレッシュホールド超過障害</li> <li>• <b>ber_sf_b3</b> PBIP BER SD スレッシュホールド超過障害 (デフォルト)</li> <li>• <b>encap</b> パス信号ラベル カプセル化ミスマッチ障害 (デフォルト)</li> <li>• <b>pais</b> パス アラーム表示信号障害 (デフォルト)</li> <li>• <b>plop</b> パス ポインタ損失障害 (デフォルト)</li> <li>• <b>ppdi</b> パス ペイロード障害表示障害(デフォルト)</li> <li>• <b>pplm</b> ペイロード ラベル ミスマッチ パス (デフォルト)</li> <li>• <b>prdi</b> パス リモート障害表示障害 (デフォルト)</li> <li>• <b>ptim</b> パス トレース インジケータ ミスマッチ障害 (デフォルト)</li> <li>• <b>puneq</b> ゼロと同等のパス ラベル障害 (デフォルト)</li> </ul>
ステップ 3	Router(config-if)# <b>pos trigger delay</b> <i>millisecond</i>	インターフェイスの回線プロトコルがダウンするまでに待機する時間を設定します。遅延は 200 ~ 2000 ミリ秒に設定できます。間隔を指定しないと、遅延はデフォルトの 200 ミリ秒に設定されます。
ステップ 4	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	Router# <b>copy running-config startup-config</b>	(任意)設定の変更を NVRAM (不揮発性 RAM) に保存します。

## C2 バイトとスクランプリング

SONET/SDH フレーム内のオーバーヘッド バイトの 1 つに C2 バイトがあります。SONET/SDH 規格では、C2 バイトをバス信号ラベルとして定義しています。このバイトの目的は、SONET Framing Overhead (FOH; フレーミング オーバーヘッド) でカプセル化されているペイロード タイプと通信することです。C2 バイトの機能は、イーサネット ネットワークの EtherType および Logical Link Control (LLC; 論理リンク制御) /Subnetwork Access Protocol (SNAP; サブネットワーク アクセス プロトコル) のヘッダー フィールドと似ています。C2 バイトによって 1 つのインターフェイスで複数のペイロード タイプを同時に送信できるようになります。C2 バイトは設定できません。表 5-5 に、C2 バイトの 16 進数値を示します。

表 5-5 C2 バイトおよびスクランプリングのデフォルト値

信号ラベル	SONET/SDH ペイロードの内容
0x01	スクランプリングを使用した、または使用しない、32 ビット CRC の LEX カプセル化
0x05	スクランプリングを使用した、または使用しない、16 ビット CRC の LEX カプセル化
0xCF	スクランプリングを使用した Cisco HDLC または PPP/BCP
0x16	スクランプリングを使用しない Cisco HDLC または PPP/BCP
0x1B	GFP-F

### サードパーティ製 POS インターフェイスの C2 バイトおよびスクランプリングの値

サードパーティ製の装置と接続したときにシスコ製の POS インターフェイスが起動しない場合は、スクランプリング設定、CRC 設定、および C2 バイトでアダプタイズされる値を確認します。Juniper Networks 製ルータでは、RFC 2615 モードを設定すると、次の 3 つのパラメータが設定されます。

- スクランプリングのイネーブル
- C2 値 0x16
- CRC-32

従来は、スクランプリングをイネーブルにしても、これらのサードパーティ製の装置は 0xCF の C2 値を使用し続けたため、スクランブルされたペイロードが適切に反映されませんでした。

### SPE スクランプリングの設定

SPE スクランプリングはデフォルトではオンに設定されています。POS SONET/SDH ペイロード (SPE) スクランプリングを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
<b>ステップ 1</b>	Router(config)# <b>interface pos number</b>	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、設定する POS インターフェイスを指定します。
<b>ステップ 2</b>	Router(config-if)# <b>no pos scramble-spe</b>	ペイロード スクランプリングをインターフェイス上でディセーブルにします。ペイロード スクランプリングはデフォルトではオンに設定されています。
<b>ステップ 3</b>	Router(config-if)# <b>no shutdown</b>	以前の設定を使用してインターフェイスをイネーブルにします。
<b>ステップ 4</b>	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
<b>ステップ 5</b>	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM (不揮発性 RAM) に保存します。

## POS のモニタリングと確認

`show controller pos [0 | 1]` コマンド (例 5-1) は受信値と送信値および C2 値を出力します。したがって、ローカル エンドで値を変更しても `show controller` コマンドの出力値は変わりません。

### 例 5-1 show controller pos [0 | 1] コマンド

```

ML_Series# sh controllers pos 0
Interface POS0
Hardware is Packet/Ethernet over Sonet
Framing Mode: HDLC
Concatenation: CCAT
Alarms reportable to CLI: PAIS PLOP PUNEQ PTIM PPLM ENCAP PRDI PPDI BER_SF_B3
BER_SD_B3 VCAT_OOU_TPT LOM SQM
Link state change defects: PAIS PLOP PUNEQ PTIM PPLM ENCAP PRDI PPDI BER_SF_B3
Link state change time : 200 (msec)
***** Path *****
Circuit state: IS
    PAIS      = 0          PLOP      = 0          PRDI      = 0          PTIM      = 0
    PPLM      = 0          PUNEQ     = 0          PPDI      = 0          PTIU      = 0
    BER_SF_B3 = 0          BER_SD_B3 = 0          BIP(B3)   = 0          REI       = 0
    NEWPTR    = 0          PSE       = 0          NSE       = 0          ENCAP     = 0
Active Alarms : PAIS
Demoted Alarms: None
Active Defects: PAIS
DOS FPGA channel number : 0
Starting STS (0 based) : 0
VT ID (if any) (0 based) : 255
Circuit size : STS-3c
RDI Mode : 1 bit
C2 (tx / rx) : 0x01 / 0x01
Framing : SONET
Path Trace
    Mode : off
    Transmit String :
    Expected String :
    Received String :
    Buffer : Stable
    Remote hostname :
    Remote interface:
    Remote IP addr :
B3 BER thresholds:
SFBER = 1e-4, SDBER = 1e-7
0 total input packets, 0 post-HDLC bytes
0 input short packets, 0 pre-HDLC bytes
0 input long packets , 0 input runt packets
0 input CRCError packets , 0 input drop packets
0 input abort packets
0 input packets dropped by ucode
0 total output packets, 0 output pre-HDLC bytes
0 output post-HDLC bytes
Carrier delay is 200 msec

```

`show interface pos {0|1}` コマンド (例 5-2) はスクランプリングを表示します。

### 例 5-2 show interface pos [0 | 1] コマンド

```
ML_Series# show interface pos 0
POS0 is administratively down, line protocol is down
  Hardware is Packet/Ethernet over Sonet, address is 0011.2130.b340 (bia
0011.2130.b340)
  MTU 1500 bytes, BW 145152 Kbit, DLY 100 usec,
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation: Cisco-EoS-LEX, crc 32, loopback not set
  Keepalive set (10 sec)
  Scramble enabled
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 01:21:02, output never, output hang never
  Last clearing of "show interface" counters 00:12:01
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  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
    Received 0 broadcasts (0 IP multicast)
  0 runts, 0 giants, 0 throttles
    0 parity
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
  0 input packets with dribble condition detected
  0 packets output, 0 bytes, 0 underruns
  0 output errors, 0 applique, 0 interface resets
  0 babbles, 0 late collision, 0 deferred
  0 lost carrier, 0 no carrier
  0 output buffer failures, 0 output buffers swapped out
  0 carrier transitions
```

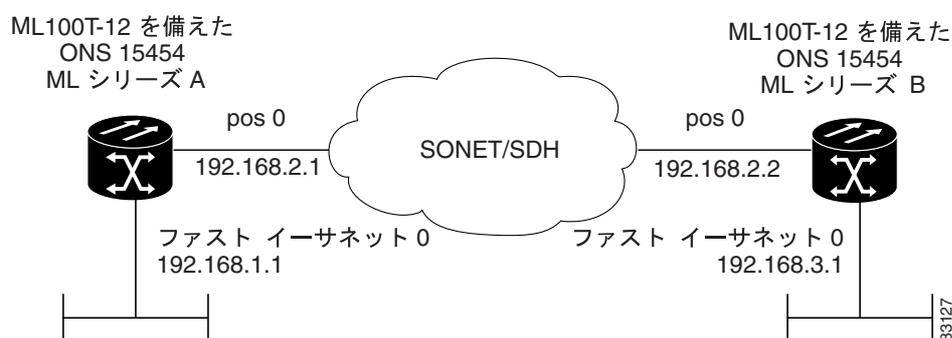
## POS の設定例

ここでは、他の ONS イーサネット カードおよび POS 対応ルータに接続するための ML シリーズ カードの POS 設定例を説明します。ここに示す例は、他の ONS イーサネット カードおよび POS 対応ルータとの接続に使用可能な ML シリーズ カード設定の一例です。ONS イーサネット カードの POS 特性の詳細については、第 20 章「ONS イーサネット カード上の POS」を参照してください。

### ML シリーズ カード間の設定

図 5-1 に、2 つの ONS 15454 または ONS 15454 SDH ML シリーズ カード間の POS 設定を示します。

図 5-1 ML シリーズ カード間の POS 設定



例 5-3 に、ML シリーズ カード A の設定に関連するコードを示します。

例 5-3 ML シリーズ カード A の設定

```
hostname ML_Series_A
!
interface FastEthernet0
 ip address 192.168.1.1 255.255.255.0
!
interface POS0
 ip address 192.168.2.1 255.255.255.0
 crc 32
 pos flag c2 1
!
router ospf 1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
```

例 5-4 に、ML シリーズ カード B の設定に関連するコードを示します。

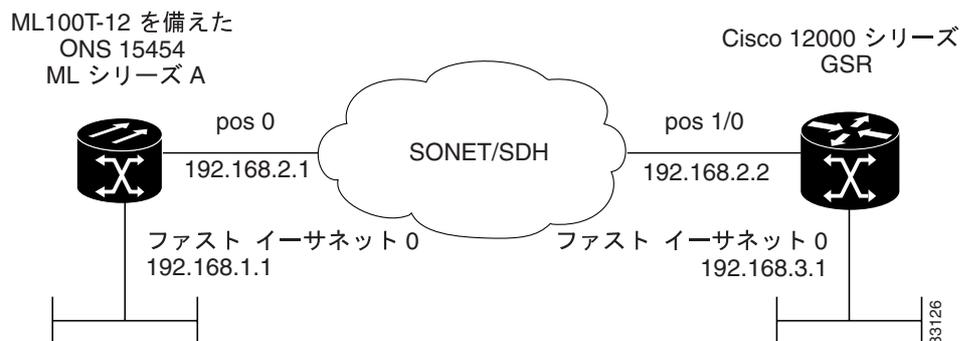
#### 例 5-4 ML シリーズ カード B の設定

```
hostname ML_Series_B
!
interface FastEthernet0
 ip address 192.168.3.1 255.255.255.0
!
interface POS0
 ip address 192.168.2.2 255.255.255.0
 crc 32
 pos flag c2 1
!
router ospf 1
 log-adjacency-changes
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.3.0 0.0.0.255 area 0
!
```

## ML シリーズ カードと Cisco 12000 GSR シリーズ ルータ間の設定

図 5-2 に、ML シリーズ カードと Cisco 12000 Gigabit Switch Router( GSR; ギガビット スイッチ ルータ ) シリーズ ルータ間の POS 設定を示します。相互運用するには、PPP/BCP カプセル化または Cisco HDLC カプセル化が使用できます。

図 5-2 ML シリーズ カードと Cisco 12000 シリーズ GSR 間の POS 設定



例 5-5 に、ML シリーズ カード A の設定に関連するコードを示します。

#### 例 5-5 ML シリーズ カード A の設定

```
hostname ML_Series_A
!
interface FastEthernet0
 ip address 192.168.1.1 255.255.255.0
!
!
interface POS0
 ip address 192.168.2.1 255.255.255.0
 encapsulation ppp
 crc 32
!
router ospf 1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
```

例 5-6 に、GSR-12000 の設定に関連するコードを示します。

#### 例 5-6 GSR-12000 の設定

```
hostname GSR
!
interface FastEthernet1/0
 ip address 192.168.3.1 255.255.255.0
!
interface POS2/0
 ip address 192.168.2.2 255.255.255.0
 crc 32
 encapsulation PPP
 pos scramble-atm
!
router ospf 1
 log-adjacency-changes
 network 192.168.2.0 0.0.0.255 area 0
 network 192.168.3.0 0.0.0.255 area 0
!
```

ML シリーズ カードの場合、デフォルトのカプセル化は LEX で、対応するデフォルト MTU は 1500 バイトです。外部 POS 装置と接続している場合は、表 5-6 に示すパラメータが ML シリーズ スイッチと外部装置の両方で同じ設定になっていることを確認してください。

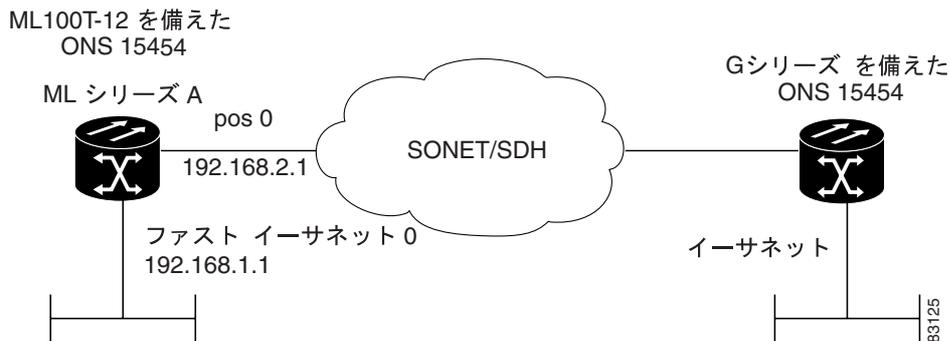
表 5-6 Cisco 12000 GSR シリーズ ルータに接続する場合の ML シリーズのパラメータ設定

コマンドの説明	パラメータ
Router(config-if)# <b>encapsulation ppp</b>  または Router(config-if)# <b>encapsulation hdlc</b>	カプセル化 Cisco 12000 GSR シリーズでのデフォルトのカプセル化は、ML シリーズでサポートされている HDLC です。また、PPP は ML シリーズ カードおよび Cisco 12000 GSR シリーズの両方でサポートされています。  Cisco 12000 GSR シリーズは LEX カプセル化をサポートしません。LEX は、ML シリーズ カードでデフォルトのカプセル化としてサポートされています。
Router(config-if)# <b>show controller pos</b>	C2 バイト <b>show controller pos</b> コマンドを使用して送信と受信の C2 値が同じであることを確認します。
Router(config-if)# <b>pos flag c2 value</b>	C2 バイト値を設定します。有効な値は、0 ~ 255 (10 進数) です。LEX のデフォルト値は 0x01 (16 進数) です。

## ML シリーズカードと G シリーズカード間の設定

図 5-3 に、ML シリーズカードと G シリーズカード間の POS 設定を示します。

図 5-3 ML シリーズカードと G シリーズカード間の POS 設定



例 5-7 に、ML シリーズカード A の設定に関連するコードを示します。

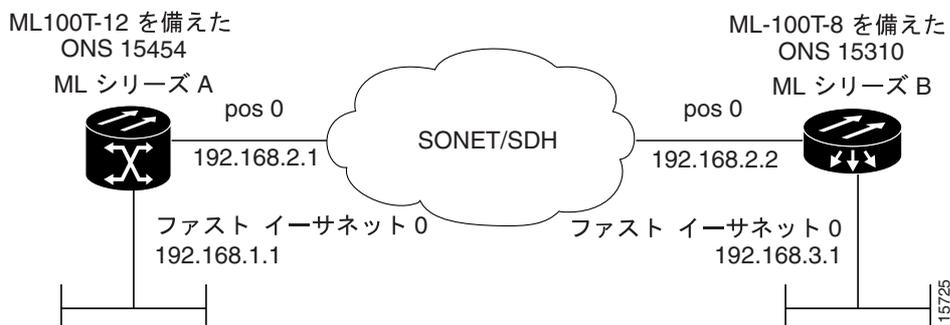
例 5-7 ML シリーズカード A の設定

```
hostname ML_Series_A
!
interface FastEthernet0
 ip address 192.168.1.1 255.255.255.0
!
interface POS0
 ip address 192.168.2.1 255.255.255.0
 crc 32
!
router ospf 1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
```

## ML シリーズカードと ONS 15310 ML-100T-8 カード間の設定

図 5-4 に、ML シリーズカードと ONS 15310 ML-100T-8 カード間の POS 設定を示します。接続された ML-100T-8 カードの回線の詳細な設定手順については、『Cisco ONS 15310-CL and Cisco ONS 15310-MA Ethernet Card Software Feature and Configuration Guide』を参照してください。

図 5-4 ML シリーズカードと ONS 15310 ML-100T-8 カード間の設定



例 5-8 に、ML シリーズ カード A の設定に関連するコードを示します。

#### 例 5-8 ML シリーズ カード A の設定

```
hostname ML_Series_A
!
interface FastEthernet0
 ip address 192.168.1.1 255.255.255.0
!
interface POS0
 ip address 192.168.2.1 255.255.255.0
 crc 32
!
router ospf 1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.255 area 0
 network 192.168.2.0 0.0.0.255 area 0
```





## ブリッジの設定

---

この章では、ML シリーズ カードに対してブリッジングを設定する方法について説明します。この章で使用する Cisco IOS コマンドの詳細については、『*Cisco IOS Command Reference*』を参照してください。

この章の主な内容は次のとおりです。

- [基本的なブリッジングの概要 \(p.6-2\)](#)
- [基本的なブリッジングの設定 \(p.6-3\)](#)
- [基本的なブリッジングのモニタリングと確認 \(p.6-5\)](#)
- [トランスペアレント ブリッジング モードの動作 \(p.6-6\)](#)



### 注意

Cisco ISL (スイッチ間リンク) と Cisco Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル) は、ML シリーズ カードではサポートされませんが、ML シリーズ ブロードキャストではこれらの形式が転送されます。装置間の接続に ISL または DTP を使用しないことを推奨します。シスコの装置によっては、デフォルトで ISL または DTP を使用するものがあります。

## 基本的なブリッジングの概要

ML シリーズ カードは、ファストイーサネットポート、ギガビットイーサネットポート、および POS ポートでのランスペアレントブリッジングをサポートします。最大 255 個のアクティブなブリッジグループをサポートします。ランスペアレントブリッジングのモードの詳細については、「[トランスペアレントブリッジングモードの動作](#)」(p.6-6)を参照してください。

ブリッジングを設定するには、次に示すモードで作業を実行する必要があります。

- グローバル コンフィギュレーション モード：
  - IP パケットのブリッジングをイネーブルにします。
  - Spanning Tree Protocol( STP; スパニングツリー プロトコル )のタイプを選択します( 任意 )。
- インターフェイス コンフィギュレーション モード：
  - 同じブリッジグループに属するインターフェイスを特定します。

ML シリーズ カードは、ブリッジグループを構成するネットワーク インターフェイス間ですべてのルーテッドトラフィックをブリッジできます。スパニングツリーがイネーブルになっている場合は、インターフェイスが同じスパニングツリーの一部になります。ブリッジグループに参加していないインターフェイスは、ブリッジドトラフィックを転送できません。

パケットの宛先アドレスがブリッジテーブルに存在する場合、そのパケットはブリッジグループの単一のインターフェイスに転送されます。パケットの宛先アドレスがブリッジテーブルに存在しない場合、パケットはブリッジグループのすべての転送インターフェイスでフラッディングされます。ブリッジはブリッジングのプロセスにおいて送信元アドレスを学習すると、そのアドレスをブリッジテーブルに記録します。

スパニングツリーは、ML シリーズ カードのブリッジグループに必須ではありません。ただし設定した場合、設定されたブリッジグループごとに個別のスパニングツリー プロセスが実行されます。ブリッジグループは受信した Bridge Protocol Data Unit ( BPDU; ブリッジ プロトコル データ ユニット ) に基づいて、所属するメンバー インターフェイス上のみスパニングツリーを確立します。

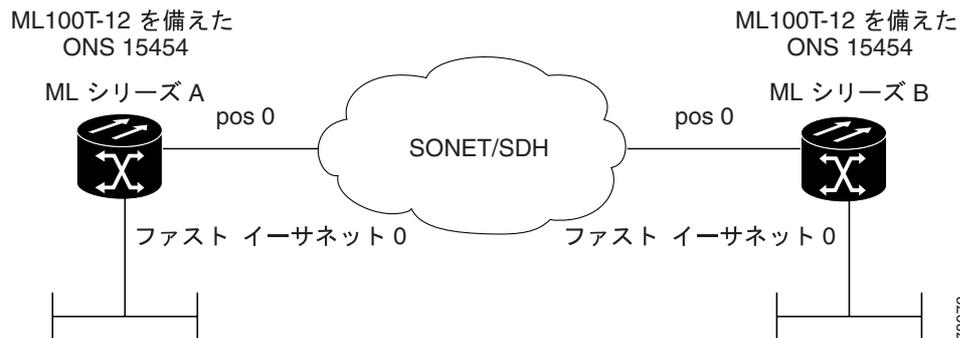
## 基本的なブリッジの設定

ブリッジを設定するには、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>no ip routing</b>	IP パケットのブリッジングをイネーブルにします。このコマンドは、ブリッジ グループごとではなく、カードごとに 1 回実行します。この手順は、Integrated Routing and Bridging (IRB; 統合ルーティングおよびブリッジング) に対しては実行しません。
ステップ 2	Router(config)# <b>bridge</b> <i>bridge-group-number</i> [ <b>protocol</b> { <b>drpri-rstp</b>   <b>rstp</b>   <b>ieee</b> }]	ブリッジ グループ番号を割り当て、適切なスパンニングツリーのタイプを定義します。  bridge-group-number の範囲は 1 ~ 4096 です。  <ul style="list-style-type: none"> <li>• <b>drpri-rstp</b> は、デュアル RPR を相互接続してノード障害から保護するために使用するプロトコルです。</li> <li>• <b>rstp</b> は IEEE 802.1W 高速スパンニングツリーです。</li> <li>• <b>ieee</b> は IEEE 802.1D STP です。</li> </ul>  <b>(注)</b> スパンニングツリーは、ML シリーズカードのブリッジ グループに必須ではありません。ただし、スパンニングツリーを設定するとネットワークループが防止されます。
ステップ 3	Router(config)# <b>bridge</b> <i>bridge-group-number</i> <b>priority</b> <i>number</i>	(任意) スパンニングツリーのルート定義で利用するために、特定のプライオリティをブリッジに割り当てます。プライオリティが低いブリッジほど、ルートとして選択される可能性が高くなります。
ステップ 4	Router(config)# <b>interface</b> <i>type number</i>	インターフェイス コンフィギュレーション モードを開始して、ML シリーズカードのインターフェイスを設定します。
ステップ 5	Router(config-if)# <b>bridge-group</b> <i>bridge-group-number</i>	ネットワーク インターフェイスをブリッジ グループに割り当てます。
ステップ 6	Router(config-if)# <b>no shutdown</b>	シャットダウン ステートをアップにし、インターフェイスをイネーブルにします。
ステップ 7	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 8	Router# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

図 6-1 に、ブリッジングの例を示します。例 6-1 に、ML シリーズ カード A の設定を示します。例 6-2 に、ML シリーズ カード B の設定を示します。

図 6-1 ブリッジングの例



例 6-1 ルータ A の設定

```
bridge 1 protocol ieee
!
!
interface FastEthernet0
no ip address
bridge-group 1
!
interface POS0
no ip address
crc 32
bridge-group 1
pos flag c2 1
```

例 6-2 ルータ B の設定

```
bridge 1 protocol ieee
!
!
interface FastEthernet0
no ip address
bridge-group 1
!
interface POS0
no ip address
crc 32
bridge-group 1
pos flag c2 1
```

## 基本的なブリッジングのモニタリングと確認

ML シリーズ カードに対してブリッジングを設定したら、イネーブル EXEC モードで次の手順を実行すると、ML シリーズ カードの動作をモニタリングおよび確認できます。

	コマンドの説明	目的
ステップ 1	Router# <b>clear bridge</b> <i>bridge-group-number</i>	学習したエントリを特定のブリッジ グループの転送データベースから削除し、送信をクリアして、静的に設定された転送エントリのカウントを受信します。
ステップ 2	Router# <b>show bridge</b> [ <i>bridge-group-number</i>   <i>interface-address</i> ]	ブリッジ転送データベースのエントリのクラスを表示します。
ステップ 3	Router# <b>show bridge verbose</b>	設定したブリッジ グループの詳細情報を表示します。
ステップ 4	ML_Series# <b>show spanning-tree</b> [ <i>bridge-group-number</i> ] [ <b>brief</b> ]	<p>スパニングツリーの詳細情報を表示します。</p> <p><b>bridge-group-number</b> を指定すると、スパニングツリー情報が特定のブリッジ グループに制限されます。</p> <p><b>brief</b> を指定すると、スパニングツリーに関する要約情報が表示されます。</p>

例 6-3 に、ブリッジングのモニタリングと確認の例を示します。

### 例 6-3 ブリッジングのモニタリングと確認

```

ML-Series# show bridge

Total of 300 station blocks, 298 free
Codes: P - permanent, S - self

Bridge Group 1:

Maximum dynamic entries allowed: 1000
Current dynamic entry count: 2

      Address      Action  Interface
0000.0001.6000  forward FastEthernet0
0000.0001.6100  forward POS0

ML-Series# show bridge verbose

Total of 300 station blocks, 298 free
Codes: P - permanent, S - self

Maximum dynamic entries allowed: 1000
Current dynamic entry count: 2

BG Hash      Address      Action  Interface      VC   Age   RX count  TX co
unt
  1 60/0  0000.0001.6000 forward FastEthernet0   -
  1 61/0  0000.0001.6100 forward POS0      -

Flood ports
FastEthernet0
POS0

ML-Series# show spanning-tree brief

Bridge group 1
Spanning tree enabled protocol ieee
Root ID      Priority    32769

```

## ■ トランスペアレントブリッジングモードの動作

```

Address      0005.9a39.6634
This bridge is the root
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Bridge ID Priority 32769 (priority 32768 sys-id-ext 1)
Address      0005.9a39.6634
Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
Aging Time   300

Interface      Role Sts Cost      Prio.Nbr Type
-----
Fa0            Desg FWD 19        128.3    P2p
PO0           Desg FWD 9         128.20   P2p

```

## トランスペアレントブリッジングモードの動作

Cisco IOS ソフトウェアのランスペアレントブリッジング機能は、ブリッジグループとIPルーティングを組み合わせたものです。この組み合わせは、適応スパンニングツリーブリッジの高速性を提供し、ルータの機能性、信頼性、安全性を実現します。MLシリーズカードは、他のCisco IOSプラットフォームと同じ方法でランスペアレントブリッジングをサポートします。

ランスペアレントブリッジングは、4つの異なるモードでIPフレームを処理します。モードには、IP routing、no IP routing、bridge crb、bridge irbの4つがあり、それぞれ異なるルールと設定オプションが適用されます。ここでは、MLシリーズカードのこの4つのモードの設定および動作について説明します。

ランスペアレントブリッジングの設定に関する一般的なCisco IOS ユーザマニュアルについては、『Cisco IOS Bridging and IBM Networking Configuration Guide』Release 12.2 の「Configuring Transparent Bridging」の章を参照してください。次のURLからアクセスしてください。

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products\\_configuration\\_guide\\_chapter09186a00800ca767.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca767.html)

## IP routing モード

IP routing モードはデフォルトのモードです。このモードは他のモード（no IP routing、bridge crb、bridge irb）をディセーブルにします。グローバルコマンド **ip routing** を使用すると、IP routing モードがイネーブルになります。

IP routing モードのブリッジグループはIPパケットを処理しません。IPパケットはルーティングされるか、または廃棄されます。

次の規則は、このモードでのパケット処理について説明します。

- ブリッジグループのみを設定した入力インターフェイスまたはサブインターフェイスは、非IPパケットをブリッジングし、IPパケットを廃棄します（例 6-4）。
- IPアドレスのみを設定した入力インターフェイスまたはサブインターフェイスは、IPパケットをルーティングし、非IPパケットを廃棄します（例 6-5）。
- IPアドレスとブリッジグループ両方を設定した入力インターフェイスまたはサブインターフェイスは、IPパケットをルーティングし、非IPパケットをブリッジングします（例 6-6）。この設定は、フォールバックブリッジングともいいます。プロトコルをルーティングできない場合、インターフェイスはブリッジングにフォールバックします。
- 特定のブリッジグループに属するすべてのインターフェイスまたはサブインターフェイスで、IPアドレスの設定の有無を統一させる必要があります。同じブリッジグループ内でIPアドレスを設定したインターフェイスと、IPアドレスを設定していないインターフェイスを混在させると、ネットワークレベルでルーティングが矛盾したり予測不可能な事態を招いたりします。

- 同じブリッジグループに属するすべてのインターフェイスおよびサブインターフェイスで、IPアドレスの設定を統一させる必要があります。ブリッジグループのすべてのインターフェイスにIPアドレスを設定するか、またはブリッジグループのインターフェイスのいずれにもIPアドレスを設定しないでください。

例 6-4 に、ブリッジグループ内で、IPアドレスが設定されていないMLシリーズカードインターフェイスを示します。

#### 例 6-4 IPアドレスが設定されていないブリッジグループ

```
ip routing
bridge 1 proto rstp

int f0
bridge-group 1

int pos 0
bridge-group 1
```

例 6-5 に、ブリッジグループが存在しない状態でIPアドレスが設定されているMLシリーズカードインターフェイスを示します。

#### 例 6-5 ブリッジグループに存在しないIPアドレス

```
ip routing

int f0
ip address 10.10.10.2 255.255.255.0

int pos 0
ip address 20.20.20.2 255.255.255.0
```

例 6-6 に、ブリッジグループ内で、IPアドレスが設定されているMLシリーズカードインターフェイスを示します。

#### 例 6-6 ブリッジグループに属するIPアドレス

```
ip routing
bridge 1 proto rstp

int f0
ip address 10.10.10.2 255.255.255.0
bridge-group 1

int pos 0
ip address 20.20.20.2 255.255.255.0
bridge-group 1
```

## no IP routing モード

no IP routing モードでは、IP パケットと非 IP パケットの両方をブリッジングし、ルーティングを回避します。Cisco IOS では、管理ポートとして設定されたインターフェイスの IP アドレスを使用できますが、IP アドレス間でのルーティングは行われません。

グローバル コマンド `no ip routing` を使用するとこの機能がイネーブルになり、`no ip routing` を使用すると他のモードがディセーブルになります。

次の規則は、このモードでのパケット処理について説明します。

- 1つのブリッジ グループのみで、IP アドレスなしで設定された入力インターフェイスまたはサブインターフェイスは、すべてのパケットをブリッジングします (例 6-7)。
- 1つの IP アドレスのみで設定された入力インターフェイスまたはサブインターフェイスは、すべてのパケットを廃棄します。ただし、宛先 MAC (メディア アクセス制御) および入力インターフェイスの IP アドレスがあるパケットは Cisco IOS によって処理されます。これは有効な設定ではありません。
- IP アドレスとブリッジ グループの両方が設定された入力インターフェイスまたはサブインターフェイスは、入力インターフェイスの MAC アドレスに送信されるパケット以外のすべてのパケットをブリッジングします。入力インターフェイスの MAC アドレスとインターフェイス IP アドレスに送信されたパケットは、Cisco IOS によって処理されます。入力インターフェイスの MAC アドレスに送信されたその他のパケットは廃棄されます。これは IP アドレスの有効な設定ではありません。
- 特定のブリッジ グループに属するすべてのインターフェイスまたはサブインターフェイスで、IP アドレスの設定の有無を統一させる必要があります。同じブリッジ グループ内で IP アドレスを設定したインターフェイスと、IP アドレスを設定していないインターフェイスを混在させると、ネットワーク レベルでルーティングが矛盾したり予測不可能な事態を招いたりします。

例 6-7 に、ブリッジ グループ内で、IP アドレスが設定されていない ML シリーズ カード インターフェイスを示します。

### 例 6-7 IP アドレスが設定されていないブリッジ グループ

```
no ip routing
bridge 1 proto rstp

int f0
bridge-group 1

int pos 0
bridge-group 1
```

## bridge CRB モード

bridge crb モードでは、各ブリッジ グループのデフォルトのサブモードは、IP パケットをブリッジングしますがルーティングしません。これは、no ip routing モードの動作と似ています。ただし、bridge crb では、パケット処理はグローバルに設定されず、特定のブリッジ グループに対して設定されます。ブリッジ グループをディセーブルにして IP パケットをブロックするか、またはルーテッド インターフェイスのグループにフォールバック ブリッジングを設定するかを選択できます。

グローバル コマンド `bridge crb` を使用すると、同時ルーティングとブリッジングがイネーブルになります。bridge crb をイネーブルにすると、他のモードがディセーブルになります。

次の規則は、このモードでのパケット処理について説明します。

- **bridge x bridge ip** コマンド ( $x$  はブリッジグループ番号) は、IP パケットをブリッジングするブリッジグループを設定します。ブリッジグループに属するインターフェイスおよびサブインターフェイスは、no IP routing モードの規則に従います。
- **bridge x route IP** コマンド ( $x$  はブリッジグループ番号) は、IP パケットを無視するブリッジグループを設定します。このブリッジグループに属するインターフェイスおよびサブインターフェイスは、IP routing モードの規則に従います (例 6-8)。
- 既存のブリッジグループで bridge crb をイネーブルにすると、ルーティング用に設定 (IP アドレスが設定) されたインターフェイスのある既存のブリッジグループに対して、**bridge x route IP** コンフィギュレーション コマンドを生成します。このことは、crb が最初にイネーブルになった場合に注意してください。
- 特定のブリッジグループに属するすべてのインターフェイスまたはサブインターフェイスで、IP アドレスの設定の有無を統一させる必要があります。同じブリッジグループ内で IP アドレスを設定したインターフェイスと、IP アドレスを設定していないインターフェイスを混在させると、ネットワークレベルでルーティングが矛盾したり予測不可能な事態を招いたりします。
- 同じブリッジグループに属さないインターフェイスまたはサブインターフェイス間のルーティングは、ネットワーク動作が矛盾する原因となります。このモードは、ブリッジグループのメンバー間のルーティング用であり、ブリッジグループ内外のルーティング用ではありません。

例 6-8 に、IP アドレスと複数のブリッジグループが設定された ML シリーズ カード インターフェイスを示します。

#### 例 6-8 IP アドレスおよび複数のブリッジグループ

```
bridge crb
bridge 1 proto rstp
bridge 1 route ip
bridge 2 proto rstp

int f0
ip address 10.10.10.2 255.255.255.0
bridge-group 1

int pos 0
ip address 20.20.20.2 255.255.255.0
bridge-group 1

int f1
bridge-group 2

int pos 1
bridge-group 2
```



#### ヒント

bridge crb コンフィギュレーションをトラブルシューティングする場合、同じサブネットに属する IP アドレスがインターフェイスに割り当てられていないことを確認してください。ルーティングする場合、IP アドレスは異なるサブネットに属する必要があります。

## bridge IRB モード

グローバル コマンド `bridge irb` を使用すると、統合ルーティングとブリッジング モードがイネーブルになります。bridge irb をイネーブルにすると、他のモードがディセーブルになります。

bridge irb モードは、bridge crb モードのスーパーセットです。IRB モードのみが Bridged Virtual Interface (BVI) をサポートします。これは、特定のブリッジ グループに属する仮想レイヤ 3 インターフェイスです。BVI が機能するためには IP アドレスが必要です。BVI はそのブリッジ グループのすべてのメンバー インターフェイスから見るできます。ブリッジ グループ内外のルーティングを正しく実行する唯一の方法は、BVI を使用することです。

bridge irb の動作は、bridge crb の動作に次を追加したものです。

- BVI インターフェイスが 1 つのブリッジ グループに設定されている場合、BVI IP アドレスは、そのブリッジ グループのメンバー上で設定する唯一のアドレスである必要があります (例 6-9)。
- 1 つの IP アドレスと 1 つのブリッジ グループの両方が 1 つのインターフェイス上に設定されている場合、IP ブリッジングまたは IP ルーティングのいずれかをイネーブルにします。両方イネーブルにすることはできません (例 6-10)。
- IP ルーティングがブリッジ グループでディセーブルの場合、すべてのパケットがブリッジングされ、BVI インターフェイスは IP をルーティングしません。これは各ブリッジ グループのデフォルトです。
- BVI のあるブリッジ グループで IP ブリッジングと IP ルーティングの両方がイネーブルの場合、IP パケットをブリッジ グループ メンバーの間でブリッジングし (同じサブネット内でブリッジ)、BVI を介してブリッジ グループ内外でルーティングできます。
- IP ブリッジングがディセーブルで、IP ルーティングがブリッジングでイネーブルの場合、BVI を介してブリッジ グループ内外で IP パケットをルーティングできますが、レイヤ 2 インターフェイス間ではブリッジングできません。グローバル コマンド `bridge x route ip` とグローバル コマンド `no bridge x bridge ip` を組み合わせると、IP ルーティングがイネーブルになり、IP ブリッジングがディセーブルになります。

例 6-9 に、ブリッジ グループに設定された ML シリーズ カード インターフェイスと、IP アドレスが設定された BVI を示します。ブリッジングとルーティングは両方ともイネーブルです。

### 例 6-9 ブリッジングとルーティングがイネーブルである bridge irb

```
bridge irb
bridge 1 proto rstp
bridge 1 route ip

int f0
bridge-group 1

int pos 0
bridge-group 1

int bvi 1
ip address 10.10.10.1 255.255.255.0
```

例 6-10 に、IP アドレスとブリッジ グループの両方が設定された ML シリーズ カード インターフェイスを示します。IP ルーティングはイネーブルで、IP ブリッジングはディセーブルです。

**例 6-10 IP アドレスおよび複数のブリッジ グループ**

```
bridge irb
bridge 1 proto rstp
bridge 1 route ip
no bridge 1 bridge ip

int f0
ip address 10.10.10.1 255.255.255.0
bridge-group 1

int pos 0
ip address 20.20.20.2 255.255.255.0
bridge-group 2
```

**ヒント**

---

bridge irb をトラブルシューティングする場合、BVI に IP アドレスが設定され、BVI ブリッジ メンバーには IP アドレスが設定されていないことを確認してください。

---





## STP および RSTP の設定

---

この章では、IEEE 802.1D Spanning Tree Protocol (STP; スパニングツリー プロトコル) および IEEE 802.1W Rapid Spanning Tree Protocol (RSTP; 高速スパニングツリー プロトコル) の ML シリーズ実装について説明します。また、ML シリーズ カードで STP および RSTP を設定する方法についても説明します。

この章の内容は次のとおりです。

- [STP の機能 \( p.7-2 \)](#)
- [RSTP \( p.7-10 \)](#)
- [IEEE802.1D STP との相互運用性 \( p.7-15 \)](#)
- [STP および RSTP 機能の設定 \( p.7-16 \)](#)
- [STP および RSTP のステータスの確認とモニタリング \( p.7-22 \)](#)

## STP の機能

次の項では、スパニングツリー機能概要について説明します。

- [STP の概要 \(p.7-2\)](#)
- [サポートされている STP インスタンス \(p.7-3\)](#)
- [BPDU \(p.7-3\)](#)
- [ルート スイッチの選出 \(p.7-4\)](#)
- [ブリッジ ID、スイッチ プライオリティ、および拡張システム ID \(p.7-4\)](#)
- [スパニングツリー タイマー \(p.7-5\)](#)
- [スパニングツリー トポロジーの形成 \(p.7-5\)](#)
- [スパニングツリー インターフェイスのステート \(p.7-6\)](#)
- [スパニングツリー アドレスの管理 \(p.7-8\)](#)
- [STP および IEEE 802.1Q トランク \(p.7-8\)](#)
- [スパニングツリーおよび冗長接続 \(p.7-8\)](#)
- [接続を維持するためのエージングの加速 \(p.7-9\)](#)

## STP の概要

STP は、ネットワーク内のループを防ぎながら、パスの冗長性を実現するレイヤ 2 リンク管理プロトコルです。レイヤ 2 イーサネット ネットワークが正常に機能するのは、任意の 2 つのステーション間にアクティブなパスが 1 つだけ存在する場合です。スパニングツリーの動作はエンドステーションに対して透過的であるため、1 つの LAN セグメントに接続されているのか、複数のセグメントで構成されたスイッチド LAN に接続されているのかエンドステーションで検出することはできません。

フォールトトレランスなインターネットワークを構築するときには、ネットワーク内のすべてのノード間にループのないパスが必要となります。スパニングツリー アルゴリズムでは、スイッチ型レイヤ 2 ネットワーク全体にわたる最適なループフリーパスを計算します。スイッチは、Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) と呼ばれるスパニングツリー フレームを定間隔で送受信します。スイッチはこれらのフレームを転送せず、フレームを使用してループフリーパスを構築します。

エンドステーション間に複数のアクティブなパスがあると、ネットワーク内にループが発生する原因となります。ネットワークにループが存在すると、エンドステーションが重複したメッセージを受信する可能性があります。また、スイッチが複数のレイヤ 2 インターフェイスでエンドステーションの MAC (メディア アクセス制御) アドレスを学習する可能性もあります。このような状況は、ネットワークを不安定にします。

スパニングツリーでは、ルート スイッチおよびルートからレイヤ 2 ネットワーク内のすべてのスイッチからのループフリーパスによってツリーを定義します。スパニングツリーは、冗長データパスを強制的にスタンバイ (ブロック) 状態にします。スパニングツリー内のネットワーク セグメントで障害が発生したときに冗長パスが存在する場合、スパニングツリー アルゴリズムは、スパニングツリー トポロジーを再計算し、スタンバイパスをアクティブにします。

スイッチの 2 つのインターフェイスがループに含まれているときには、スパニングツリーのポートプライオリティとパスコストの設定によって、フォワーディングステートになるインターフェイスとブロッキングステートになるインターフェイスが決まります。ポートプライオリティ値は、ネットワーク トポロジー内のインターフェイスの位置を表すとともに、そのインターフェイスがトラフィックを渡すためにどの程度適しているかを表します。パスコスト値は、メディア速度を表します。

## サポートされている STP インスタンス

ML シリーズ カードでは、Per-VLAN (仮想 LAN) Spanning Tree (PVST+) と最大 255 のスパニングツリー インスタンスをサポートしています。

## BPDU

スイッチド ネットワークのスパニングツリー トポロジーマトリクスが、安定でアクティブになるかどうかは、次の要素によって決まります。

- 各スイッチの各 VLAN に関連付けられた一意のブリッジ ID (スイッチ プライオリティおよび MAC アドレス)
- ルート スイッチへのスパニングツリー パス コスト
- 各レイヤ 2 インターフェイスに関連付けられたポート識別子 (ポート プライオリティおよび MAC アドレス)

ネットワーク内のスイッチの電源がオンになっているときには、各スイッチはルート スイッチとして機能します。各スイッチは、そのすべてのポートからコンフィギュレーション BPDU を送信します。BPDU によって、スパニングツリー トポロジーマトリクスの通信と計算が行われます。各コンフィギュレーション BPDU には、次の情報が格納されます。

- 送信スイッチがルート スイッチとして識別するスイッチの一意のブリッジ ID
- ルートへのスパニングツリー パス コスト
- 送信スイッチのブリッジ ID
- メッセージの有効期間
- 送信インターフェイスの識別子
- Hello タイマー、転送遅延タイマー、および最大エージング プロトコル タイマーの値

スイッチは、小さいブリッジ ID、低いパス コストなど、より優れた情報が格納されたコンフィギュレーション BPDU を受信すると、そのポートの情報を保存します。この BPDU がスイッチのルートポートで受信された場合、この指定スイッチに接続されているすべての LAN に最新のメッセージとともにこの BPDU を転送します。

スイッチは、そのポート用に現在保存されている情報より下位の情報が格納されたコンフィギュレーション BPDU を受信した場合には、その BPDU を廃棄します。スイッチがその LAN の指定スイッチであり、その LAN から下位 BPDU を受信した場合、スイッチはそのポート用に保存している最新情報が含まれている BPDU を、その LAN に送信します。このようにして、下位情報は廃棄されるので、優位情報がネットワークで伝播されます。

BPDU を交換することによって、次の処理が実行されます。

- ネットワーク内の 1 台のスイッチがルート スイッチとして選出されます。
- 各スイッチに対して 1 つのルート ポートが選択されます (ルート スイッチを除く)。このポートは、スイッチがルート スイッチにパケットを転送する際に最適パス (最もコストの低いパス) を提供します。
- パス コストに基づいて、各スイッチからルート スイッチまでの最短距離が計算されます。
- 各 LAN セグメントの指定スイッチが選択されます。指定スイッチは、その LAN からルート スイッチにパケットを転送する際に最もコストの低いパスを選択します。指定スイッチと LAN との接続に使用されるポートを指定ポートと呼びます。
- スパニングツリー インスタンスに含まれているインターフェイスが選択されます。ルート ポートと指定ポートがフォワーディング ステートになります。
- スパニングツリーに含まれていないすべてのインターフェイスはブロックされます。

## ルート スイッチの選出

スパニングツリーに關与するレイヤ 2 ネットワーク内のすべてのスイッチは、BPDU データ メッセージの交換を通じてネットワーク内の他のスイッチの情報を収集します。このメッセージの交換によって、次の処理が実行されます。

- 各スパニングツリー インスタンスに対して一意のルート スイッチが選出されます。
- すべてのスイッチド LAN セグメントの指定スイッチが選出されます。
- 冗長リンクに接続されているレイヤ 2 インターフェイスをブロッキングすることにより、スイッチド ネットワーク内のループを除去します。

各 VLAN では、スイッチ プライオリティが最も高い (プライオリティ値が最も小さい) スイッチが、ルート スイッチとして選出されます。すべてのスイッチがデフォルトのプライオリティ (32768) に設定されている場合は、VLAN 内で MAC アドレスが最も小さいスイッチがルート スイッチになります。スイッチ プライオリティ値は、ブリッジ ID の最上位ビット部分に割り当てられます。

スイッチ プライオリティ値を変更すると、スイッチがルート スイッチとして選出される可能性が変わります。設定する値が大きくなるほどルート スイッチとして選出される可能性が低くなり、値が小さくなるほど可能性が高くなります。

ルート スイッチは、スイッチド ネットワークのスパニングツリー トポロジーの論理的な中心部分です。スイッチド ネットワーク内の任意の場所からルート スイッチに到達する必要のないパスはすべて、スパニングツリー ブロッキング モードになります。

BPDU には、スイッチ アドレスと MAC アドレス、スイッチ プライオリティ、ポート プライオリティ、パス コストなど、送信スイッチとそのポートに関する情報が格納されています。スパニングツリーはこの情報を使用して、スイッチド ネットワークのルート スイッチとルート ポート、および各スイッチド セグメントのルート ポートと指定ポートを選出します。

## ブリッジ ID、スイッチ プライオリティ、および拡張システム ID

IEEE 802.1D 規格では、各スイッチには一意のブリッジ識別子 (ブリッジ ID) が割り当てられている必要があります。このブリッジ ID によって、ルート スイッチが選択されます。各 VLAN は PVST+ を備えた別の論理ブリッジとみなされるため、各スイッチには設定されている VLAN と同数の異なるブリッジ ID が必要となります。スイッチの各 VLAN には、8 バイトの一意のブリッジ ID が割り当てられています。最上位の 2 バイトはスイッチ プライオリティに使用され、残りの 6 バイトはスイッチの MAC アドレスから取得されます。

ML シリーズ カードでは、IEEE 802.1T のスパニングツリー拡張機能をサポートしています。以前にスイッチ プライオリティに使用されていたビットの一部は、現在ブリッジ ID として使用されています。その結果、スイッチ用に予約される MAC アドレスが減り、ブリッジ ID の一意性を維持しながら、広範囲の VLAN ID をサポートできるようになりました。表 7-1 に示すように、これまでスイッチ プライオリティに使用されていた 2 バイトは、4 ビットのプライオリティ値、およびブリッジ ID と等しい 12 ビットの拡張システム ID 値に再割り当てされています。以前のリリースでは、スイッチ プライオリティは 16 ビット値です。

表 7-1 スイッチ プライオリティ値と拡張システム ID

スイッチ プライオリティ値				拡張システム ID (ブリッジ ID と同じ値に設定)											
ビット 16	ビット 15	ビット 14	ビット 13	ビット 12	ビット 11	ビット 10	ビット 9	ビット 8	ビット 7	ビット 6	ビット 5	ビット 4	ビット 3	ビット 2	ビット 1
32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

スパンニングツリーは、拡張システム ID、スイッチ プライオリティ、および割り当てられたスパンニングツリー MAC アドレスを使用して、各 VLAN のブリッジ ID を一意にします。以前のリリースでは、スパンニングツリーは VLAN ごとに 1 つの MAC アドレスを使用して、各 VLAN のブリッジ ID を一意にしていました。

## スパンニングツリー タイマー

表 7-2 に、スパンニングツリー全体のパフォーマンスに影響を及ぼすタイマーを示します。

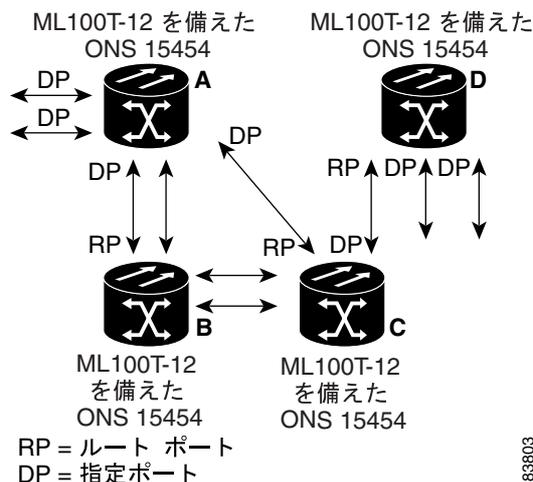
表 7-2 スパンニングツリー タイマー

変数	説明
Hello タイマー	このタイマーが満了すると、インターフェイスは近接ノードに Hello メッセージを送信します。
転送遅延タイマー	インターフェイスが転送を開始するまでの、リスニング ステートおよびラーニング ステートの継続時間を決定します。
最大エージング タイマー	インターフェイスで受信したプロトコル情報をスイッチが保管する時間を決定します。

## スパンニングツリー トポロジーの形成

図 7-1 では、すべてのスイッチのスイッチ プライオリティがデフォルト (32768) に設定されており、スイッチ A の MAC アドレスが最も小さいため、スイッチ A がルート スイッチとして選出されます。ただし、トラフィック パターン、転送インターフェイスの数、またはリンク タイプによっては、スイッチ A が最適なルート スイッチではない場合があります。最適なスイッチがルート スイッチになるように、そのスイッチのプライオリティを上げる (数値を下げる) ことによって、最適なスイッチをルートにした新しいトポロジーを形成するよう強制的にスパンニングツリーで再計算させます。

図 7-1 スパンニングツリー トポロジー



スパンニングツリー トポロジーをデフォルトのパラメータに基づいて計算すると、スイッチド ネットワークの送信元エンド ステーションから宛先エンド ステーションまでのパスが最適にならない可能性があります。たとえば、より高速のリンクをルート ポートよりも値の大きいインターフェイスに接続すると、ルート ポートが変更される可能性があります。目標は、最も高速のリンクをルート ポートにすることです。

## スパンニングツリー インターフェイスのステート

プロトコル情報がスイッチド LAN を通過するときに、伝播遅延が発生する場合があります。その結果、さまざまな時点およびスイッチドネットワークのさまざまな場所でトポロジーの変更が発生します。インターフェイスが、スパンニングツリー トポロジーに含まれていない状態からフォワーディング ステートに直接移行すると、一時的なデータ ループが形成される可能性があります。インターフェイスは、新しいトポロジー情報がスイッチド LAN 経由で伝播されるまで待機してから、フレームの転送を開始する必要があります。また、以前のトポロジーを使用して転送されたフレームの存続時間が満了できるようにする必要もあります。

スパンニングツリーを使用するスイッチの各レイヤ 2 インターフェイスは、次のいずれかの状態になります。

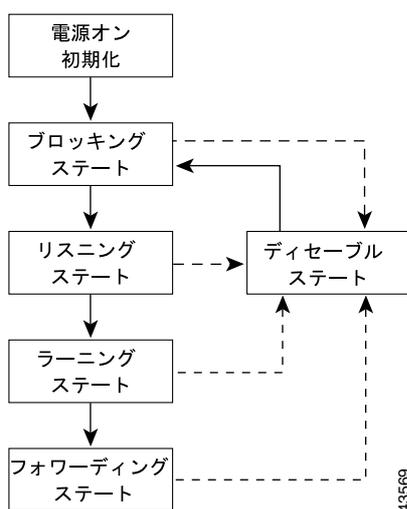
- **ブロッキング** インターフェイスはフレーム転送に関与しません。
- **リスニング** インターフェイスがフレーム転送に関与する必要があるとスパンニングツリーが判断したときに、ブロッキング ステートから最初に移行するステートです。
- **ラーニング** インターフェイスがフレーム転送に関与する準備をしているステートです。
- **フォワーディング** インターフェイスはフレームを転送します。
- **ディセーブル** ポートのシャットダウン、ポート上のリンクの欠落、またはポートで稼働するスパンニングツリー インスタンスがないことなどが原因で、インターフェイスはスパンニングツリーに関与していません。

インターフェイスは、次のようにステートを移行します。

1. 初期化からブロッキング
2. ブロッキングからリスニングまたはディセーブル
3. リスニングからラーニングまたはディセーブル
4. ラーニングからフォワーディングまたはディセーブル
5. フォワーディングからディセーブル

図 7-2 に、インターフェイスのステートがどのように移行するかを示します。

図 7-2 スパンニングツリー インターフェイスのステート



スイッチの電源をオンにすると、STP はデフォルトでイネーブルになり、スイッチ、VLAN、またはネットワーク内のすべてのインターフェイスは、ブロッキング ステートを経てリスニングおよびラーニングという移行ステートになります。スパンニングツリーは、各インターフェイスをフォワーディング ステートまたはブロッキング ステートで安定させます。

スパニングツリー アルゴリズムによって、レイヤ 2 インターフェイスがフォワーディング ステートになると、次のプロセスが発生します。

1. インターフェイスをブロッキング ステートに移行するためのプロトコル情報をスパニングツリーが待っている間、インターフェイスはリスニング ステートになります。
2. スパニングツリーは転送遅延タイマーの満了を待っている間、インターフェイスをラーニング ステートに移行して転送遅延タイマーをリセットします。
3. ラーニング ステートでは、スイッチが転送データベースのエンド ステーション位置情報を学習する間、インターフェイスは継続的にフレーム転送をブロックします。
4. 転送遅延タイマーが満了すると、スパニングツリーはインターフェイスをフォワーディング ステートに移行します。この時点で、ラーニングとフレーム転送の両方がイネーブルになります。

## ブロッキング ステート

ブロッキング ステートのレイヤ 2 インターフェイスは、フレーム転送に関与しません。初期化後、スイッチの各インターフェイスに BPDU が送信されます。スイッチは他のスイッチと BPDU を交換するまで、最初はルートとして機能します。この交換により、ネットワーク内のどのスイッチがルートまたはルート スイッチであるかが確定します。ネットワークにスイッチが 1 台しかない場合、交換は行われずに転送遅延タイマーが満了し、インターフェイスはリスニング ステートに移行します。スイッチの初期化後、インターフェイスは常にブロッキング ステートになります。

ブロッキング ステートのインターフェイスは、次の処理を実行します。

- ポートで受信したフレームを廃棄します。
- 転送のために別のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

## リスニング ステート

リスニング ステートは、レイヤ 2 インターフェイスがブロッキング ステート後に最初に移行するステートです。インターフェイスがフレーム転送に関与する必要があるとスパニングツリーが判断したときに、インターフェイスはこのステートになります。

リスニング ステートのインターフェイスは、次の処理を実行します。

- ポートで受信したフレームを廃棄します。
- 転送のために別のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習しません。
- BPDU を受信します。

## ラーニング ステート

ラーニング ステートのレイヤ 2 インターフェイスは、フレーム転送に関与するように準備しています。インターフェイスは、リスニング ステートからラーニング ステートになります。

ラーニング ステートのインターフェイスは、次の処理を実行します。

- ポートで受信したフレームを廃棄します。
- 転送のために別のインターフェイスからスイッチングされたフレームを廃棄します。
- アドレスを学習します。
- BPDU を受信します。

## フォワーディング ステート

フォワーディング ステートのレイヤ 2 インターフェイスはフレームを転送します。インターフェイスは、ラーニング ステートからフォワーディング ステートになります。

フォワーディング ステートのインターフェイスは、次の処理を実行します。

- ポートで受信したフレームを受け入れて転送します。
- 別のポートからスイッチングされたフレームを転送します。
- アドレスを学習します。
- BPDU を受信します。

## ディセーブル ステート

ディセーブル ステートのレイヤ 2 インターフェイスは、フレーム転送またはスパニングツリーに関与しません。ディセーブル ステートのインターフェイスは動作していません。

ディセーブルになったインターフェイスは、次の処理を実行します。

- 転送のために別のインターフェイスからスイッチングされたフレームを転送します。
- アドレスを学習します。
- BPDU を受信しません。

## スパニングツリー アドレスの管理

IEEE 802.1D には、さまざまなブリッジ プロトコルが使用するマルチキャスト アドレスとして、0x00180C2000000 ~ 0x0180C2000010 の範囲の 17 個のアドレスが指定されています。これらのアドレスは、削除できないスタティック アドレスです。

ML シリーズ カードは、プロトコル トンネリング機能によってトンネリングされているときには、サポートされている BPDU (0x0180C2000000 および 01000CCCCCD) をスイッチングします。

## STP および IEEE 802.1Q トランク

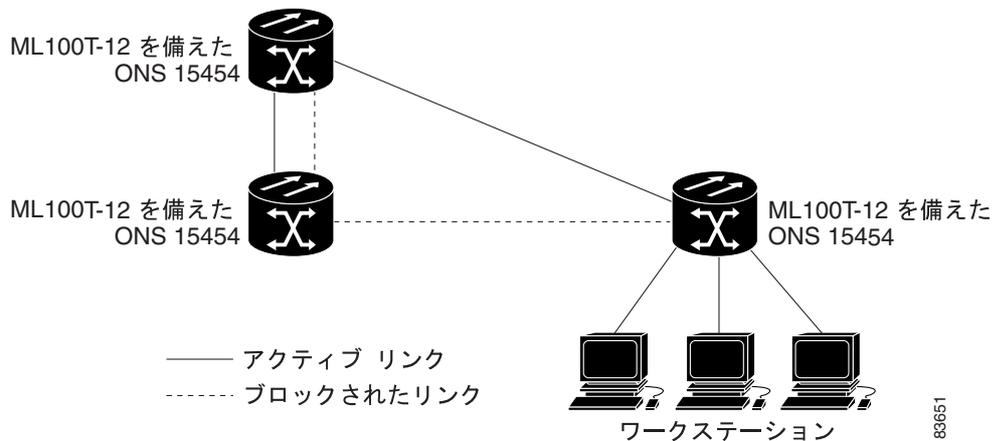
IEEE 802.1Q トランクを介してシスコ スイッチを他社製の装置に接続する場合、シスコ スイッチでは PVST+ を使用してスパニングツリーの相互運用性を実現します。ユーザがブリッジ グループにプロトコルを割り当てると、PVST+ は IEEE 802.1Q トランクで自動的にイネーブルになります。アクセス ポートおよび ISL (スイッチ間リンク) トランク ポートの外部スパニングツリーの動作は、PVST+ の影響を受けません。

IEEE 802.1Q トランクの詳細については、[第 8 章「VLAN の設定」](#)を参照してください。

## スパニングツリーおよび冗長接続

2つのスイッチ インターフェイスをもう 1 台の装置、または 2 台の異なる装置に接続することにより、スパニングツリーで冗長バックボーンを作成できます。[図 7-3](#) に示すように、スパニングツリーは、一方のインターフェイスを自動的にディセーブルにしますが、もう一方のインターフェイスに障害が発生すると、ディセーブルになっているインターフェイスをイネーブルにします。一方のリンクが高速で、もう一方が低速の場合、低速のリンクが常にディセーブルになります。両方の速度が同じである場合は、ポート プライオリティとポート ID が加算され、スパニングツリーは値の小さいリンクをディセーブルにします。

図 7-3 スパニングツリーおよび冗長接続



EtherChannel グループを使用して、スイッチ間に冗長リンクを作成することもできます。詳細については、[第 10 章「リンク集約の設定」](#)を参照してください。

## 接続を維持するためのエイジングの加速

ダイナミック アドレスのデフォルトのエイジング タイムは 5 分です。この値は、`bridge bridge-group-number aging-time` グローバル コンフィギュレーション コマンドのデフォルト設定です。ただし、スパニングツリーの再構成により、多数のステーションの位置が変更される可能性があります。再構成時には、5 分以上の間、これらのステーションに到達できない場合があるため、ステーション アドレスがアドレス テーブルから削除されて再度学習されるように、アドレス エイジング タイムが加速されます。

各 VLAN は個別のスパニングツリー インスタンスであるため、スイッチは VLAN 単位でエイジングを加速します。ある VLAN でスパニングツリーの再構成が行われると、その VLAN で学習されたダイナミック アドレスがエイジング短縮の対象になる場合があります。他の VLAN のダイナミック アドレスは影響を受けず、スイッチに設定されたエイジング間隔がそのまま適用されます。

## RSTP

RSTP は、スパンニングツリーの高速コンバージェンスを実現します。RSTP を使用すると、1 つのインスタンス（転送パス）で障害が発生しても、他のインスタンス（転送パス）に影響を及ぼすことがないため、ネットワークのフォールトトレランスが向上します。RSTP の最も一般的な初期配備は、レイヤ2 スイッチドネットワークのバックボーンレイヤおよびディストリビューションレイヤへの配備です。このように配備することによって、サービスプロバイダー環境で必要とされる高可用ネットワークが実現できます。

RSTP は、（元の）IEEE 802.1D スパンニングツリーに基づく機器との下位互換性を維持しながら、スパンニングツリーの動作を向上させます。

RSTP はポイントツーポイントの配線を利用して、スパンニングツリーの高速コンバージェンスを実現します。スパンニングツリーの再構成は、2 秒未満で行われます（IEEE 802.1D スパンニングツリーのデフォルト設定では 50 秒）。これは、音声やビデオなど、遅延に影響されやすいトラフィックを伝送するネットワークには不可欠です。

次の項では、RSTP の機能概要について説明します。

- [サポートされている RSTP インスタンス \(p.7-10\)](#)
- [ポートの役割およびアクティブトポロジー \(p.7-10\)](#)
- [高速コンバージェンス \(p.7-11\)](#)
- [ポートの役割の同期化 \(p.7-13\)](#)
- [BPDU の形式と処理 \(p.7-14\)](#)
- [TC \(p.7-15\)](#)

## サポートされている RSTP インスタンス

ML シリーズでは、Per-VLAN Rapid Spanning Tree (PVRST) と最大 255 の高速スパンニングツリーインスタンスをサポートしています。

## ポートの役割およびアクティブトポロジー

RSTP は、ポートの役割を割り当ててアクティブトポロジーを決定することにより、スパンニングツリーの高速コンバージェンスを実現します。「[ルートスイッチの選出](#)」(p.7-4) で説明したように、RSTP は IEEE 802.1D STP を構築し、最高のスイッチプライオリティを持つ（プライオリティ値が最も小さい）スイッチをルートスイッチとして選択します。さらに、RSTP は次のポート役割のいずれかを各ポートに割り当てます。

- **ルートポート** スイッチがルートスイッチにパケットを転送する際に最適パス（最もコストの低いパス）を提供します。
- **指定ポート** 指定スイッチに接続します。これにより、その LAN からルートスイッチにパケットを転送するときのパスコストが最も低くなります。指定スイッチと LAN との接続に使用されるポートを指定ポートと呼びます。
- **代替ポート** 現在のルートポートによって提供されたパスに替わるルートスイッチへの代替パスを提供します。
- **バックアップポート** 指定ポートによって提供されたスパンニングツリーのリーフに向かうパスのバックアップとして機能します。バックアップポートが存在できるのは、2 つのポートがポイントツーポイントリンクによってループバックで接続されている場合、または 1 台のスイッチに共有 LAN セグメントへの接続が 2 つ以上ある場合のみです。
- **ディセーブルポート** スパンニングツリーの動作における役割はありません。

ルートポートまたは指定ポートの役割を持つポートは、アクティブトポロジーに含まれます。代替ポートまたはバックアップポートの役割を持つポートは、アクティブトポロジーから除外されます。

ネットワーク全体にわたってポートの役割が一貫している安定したトポロジーでは、すべてのルートポートと指定ポートはすぐにフォワーディングステートに移行し、すべての代替ポートとバックアップポートは常に廃棄ステート（IEEE 802.1D のブロッキングに相当）になることが RSTP によって保証されます。フォワーディングプロセスおよびラーニングプロセスの動作は、ポートステートによって制御されます。表 7-3 は、IEEE 802.1D と RSTP のポートステートを比較したものです。

表 7-3 ポートステートの比較

動作ステータス	STP ポートステート	RSTP ポートステート	ポートがアクティブトポロジーに含まれているか
イネーブル	ブロッキング	廃棄	含まれていない
イネーブル	リスニング	廃棄	含まれていない
イネーブル	ラーニング	ラーニング	含まれている
イネーブル	フォワーディング	フォワーディング	含まれている
ディセーブル	ディセーブル	廃棄	含まれていない



## 注意

STP エッジポートは、そのポートの外部でループ保護を必要としない場合、またはそのポートの外部に STP ネイバが存在しない場合に、STP をイネーブルにする必要のないブリッジポートです。RSTP の場合、適切なインターフェイスで `bridge bridge-group-number spanning-disabled` コマンドを使用して、エッジポート（通常は正面側のイーサネットポート）で STP をディセーブルにすることが重要です。RSTP がエッジポートでディセーブルになっていない場合、エッジポートを通過するパケットのコンバージェンスタイムが過大になります。



## (注)

シスコの STP 実装で一貫性を保つために、表 7-3 では、ポートステートを廃棄ではなくブロッキングと表現しています。指定ポートはリスニングステートから開始します。

## 高速コンバージェンス

RSTP を使用すると、スイッチ、スイッチポート、または LAN に障害が発生しても、接続を迅速に回復できます。RSTP は、新しいルートポート、およびポイントツーポイントリンクによって接続されているポートに次のように高速コンバージェンスを提供します。

- ルートポート RSTP は新しいルートポートを選択すると、以前のルートポートをブロックし、新しいルートポートをただちにフォワーディングステートにします。
- ポイントツーポイントリンク ポート間をポイントツーポイントリンクによって接続し、ローカルポートが指定ポートになると、その指定ポートは提案合意ハンドシェイクを使用して相手側のポートと高速移行をネゴシエーションし、ループフリーのトポロジーを保証します。

図 7-4 に示すように、スイッチ A はポイントツーポイントリンクによってスイッチ B に接続され、すべてのポートがブロッキングステートになっています。スイッチ A のプライオリティは、スイッチ B のプライオリティよりも小さい数値であるとします。スイッチ A は提案メッセージ（提案フラグが設定されたコンフィギュレーション BPDUs）をスイッチ B に送信し、スイッチ A 自身が指定スイッチになることを提案します。

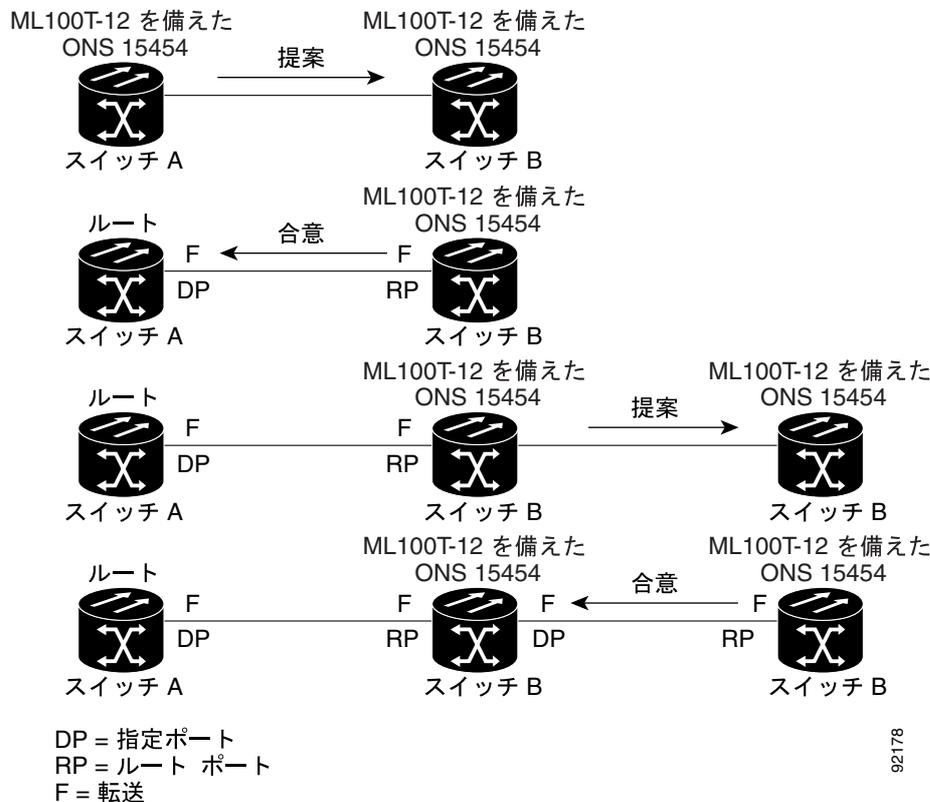
スイッチ B は提案メッセージを受信すると、提案メッセージの受信ポートを新しいルートポートとして選択し、すべての非エッジポートを強制的にブロッキングステートにします。さらに、その新しいルートポート経由で合意メッセージ（合意フラグが設定された BPDU）を送信します。

スイッチ A はスイッチ B から合意メッセージを受信すると、ただちに自分の指定ポートをフォワーディングステートにします。スイッチ B はそのすべての非エッジポートをブロックしており、さらにスイッチ A と B はポイントツーポイントリンクで接続されているため、ネットワークにループは形成されません。

スイッチ C がスイッチ B に接続された場合も、同様の一連のハンドシェイクメッセージが交換されます。スイッチ C はスイッチ B に接続されたポートをルートポートとして選択し、両端のポートはすぐにフォワーディングステートに移行します。このハンドシェイクプロセスの繰り返しによってアクティブトポロジーにスイッチがもう 1 つ追加されます。ネットワークが収束するにつれて、この提案合意ハンドシェイクがルートからスパンニングツリーのリーフに進みます。

スイッチは、ポートのデュプレックスモードからリンクタイプを判断します。つまり、全二重ポートはポイントツーポイント接続とみなされ、半二重ポートは共有接続とみなされます。

図 7-4 高速コンバージェンスの提案合意ハンドシェイク



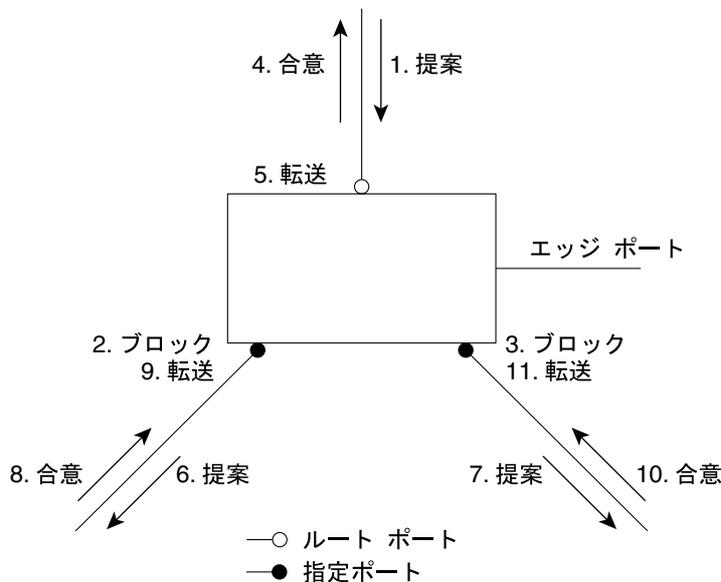
## ポートの役割の同期化

スイッチのポートの1つで提案メッセージを受信し、そのポートが新しいルートポートと選出されると、RSTP は他のすべてのポートを新しいルート情報と強制的に同期化させます。他のポートがすべて同期化されると、スイッチはルートポートで受信した優位なルート情報と同期化されません。

指定ポートがフォワーディング ステートの場合、RSTP によって新しいルート情報と強制的に同期化されると、その指定ポートはブロッキング ステートになります。一般的に、RSTP がポートをルート情報と強制的に同期化させ、ポートが上記のどの条件も満たしていない場合、そのポートステートはブロッキングに設定されます。

スイッチはすべてのポートが同期化されたことを確認すると、そのルートポートに対応する指定スイッチに合意メッセージを送信します。ポイントツーポイントリンクによって接続されたスイッチがそれぞれのポートの役割について合意すると、RSTP はポートステートをただちにフォワーディングステートに移行させます。図 7-5 に、このイベントシーケンスを示します。

図 7-5 高速コンバージェンス時のイベントシーケンス



## BPDU の形式と処理

RSTP の BPDU の形式は、プロトコルバージョンが 2 に設定されている点を除き、IEEE 802.1D の BPDU の形式と同じです。新しい Length フィールドは 0 に設定されます。これは、バージョン 1 のプロトコル情報が存在しないことを意味します。表 7-4 に、RSTP のフラグ フィールドを示します。

表 7-4 RSTP の BPDU のフラグ

ビット	説明
0	Topology Change ( TC; トポロジーの変更)
1	提案
2 ~ 3:	ポートの役割
00	不明
01	代替ポート
10	ルートポート
11	指定ポート
4	ラーニング
5	フォワーディング
6	合意
7	TC 確認

送信スイッチは、自分をその LAN の指定スイッチとして提案するために提案フラグを RSTP の BPDU に設定します。提案メッセージでは、ポートの役割は常に指定ポートに設定されます。

送信スイッチは、前の提案を受け入れる合意フラグを RSTP の BPDU に設定します。合意メッセージでは、ポートの役割は常にルートポートに設定されます。

RSTP には、独立した Topology Change Notification ( TCN; トポロジー変更通知) BPDU はありません。TC は、TC フラグによって示されます。ただし、IEEE 802.1D スイッチとの相互運用性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。

ラーニングフラグとフォワーディングフラグは、送信ポートのステートに応じて設定されます。

## 優位な BPDU 情報の処理

ポート用に現在保存されているルート情報よりも優位なルート情報(小さいブリッジ ID、低いパスコストなど)をポートが受信すると、RSTP は再構成を開始します。そのポートが新しいルートポートとして提案され選択されると、RSTP は他のすべてのポートを強制的に同期化します。

受信した BPDU が提案フラグの設定された RSTP BPDU である場合、スイッチは他のすべてのポートを同期化してから合意メッセージを送信します。BPDU が IEEE 802.1D BPDU の場合は、スイッチは提案フラグを設定せずに、ポートの転送遅延タイマーを開始します。新しいルートポートは、フォワーディングステートに移行するために 2 倍の転送遅延時間を必要とします。

ポートで優位な情報が受信されたために、そのポートがバックアップポートまたは代替ポートになる場合、RSTP はポートをブロッキングステートに設定しますが、合意メッセージは送信しません。指定ポートは、転送遅延タイマーが満了するまで、提案フラグの設定された BPDU の送信を続けます。タイマーが満了すると、ポートはフォワーディングステートに移行します。

## 下位 BPDU 情報の処理

指定ポートが、指定ポートの役割を持つポート用に現在保存されている情報より下位の BPDU（大きいブリッジ ID、高いパス コストなど）を受信すると、その指定ポートは自分の情報でただちに応答します。

## TC

ここでは、スパンニングツリー TC を処理する際の RSTP と IEEE 802.1D の違いについて説明します。

- **検出** IEEE 802.1D では、ブロッキング ステートとフォワーディング ステート間の移行で TC が発生しますが、RSTP で TC が生じるのは、ブロッキング ステートからフォワーディング ステートに移行する場合だけです（TC とみなされるのは、接続で増加する場合だけです）。エッジポートでステートが変更されても、TC は発生しません。RSTP スイッチは TC を検出すると、すべての非エッジポートで学習済みの情報を一斉に流します。
- **通知** IEEE 802.1D は TCN BPDU を使用しますが、RSTP は使用しません。ただし、IEEE 802.1D との相互運用性を保つために、RSTP スイッチは TCN BPDU の処理と生成を行います。
- **確認** RSTP スイッチは指定ポートで IEEE 802.1D スイッチから TCN メッセージを受信すると、TC 確認ビットを設定した IEEE 802.1D コンフィギュレーション BPDU で応答します。ただし、IEEE 802.1D スイッチに接続されたルートポートで TC 時間タイマー（IEEE 802.1D の TC タイマーと同じ）がアクティブであり、TC 確認ビットが設定されたコンフィギュレーション BPDU を受信した場合、TC 時間タイマーがリセットされます。

この動作は、IEEE 802.1D スイッチをサポートする場合にのみ必要です。RSTP の BPDU では、TC 確認ビットは設定されません。

- **伝播** RSTP スイッチは、指定ポートまたはルートポート経由で別のスイッチから TC メッセージを受信すると、そのすべての非エッジポート、エッジポート、指定ポート、およびルートポート（TC メッセージの受信ポートを除く）に TC を伝播します。スイッチは、これらのすべてのポートの TC 時間タイマーを開始し、これらのポート上で学習した情報を一斉に流します。
- **プロトコルの移行** IEEE 802.1D スイッチとの下位互換性を保つために、RSTP は IEEE 802.1D コンフィギュレーション BPDU と TCN BPDU をポート単位で選択的に送信します。

ポートが初期化されると、タイマーが開始され（RSTP BPDU を送信する最短時間を指定）、RSTP BPDU が送信されます。このタイマーがアクティブな間、スイッチはそのポートで受信したすべての BPDU を処理し、プロトコルタイプは無視します。

ポートの移行遅延タイマーの満了後に、スイッチが IEEE 802.1D BPDU を受信した場合、IEEE 802.1D スイッチに接続されているとみなし、IEEE 802.1D BPDU のみの使用を開始します。ただし、RSTP スイッチがポートで IEEE 802.1D BPDU を使用している場合に、タイマー満了後に RSTP BPDU を受信すると、スイッチはタイマーを再起動し、そのポートで RSTP BPDU の使用を開始します。

## IEEE802.1D STP との相互運用性

RSTP を実行しているスイッチは、IEEE 802.1D レガシー スイッチとの相互運用を可能にする内蔵プロトコル移行メカニズムをサポートしています。このスイッチが IEEE 802.1D レガシー コンフィギュレーション BPDU（プロトコルバージョンが 0 に設定されている BPDU）を受信すると、そのポートで IEEE 802.1D BPDU だけを送信します。

ただし、スイッチが IEEE 802.1D の BPDU を受信しなくなっても、自動的に RSTP モードに戻るわけではありません。これは、レガシー スイッチが指定スイッチでない限り、リンクからレガシー スイッチが削除されているかどうかを判断できないためです。また、このスイッチの接続先スイッチがその領域に加入した場合に、引き続きポートに境界の役割を割り当てる可能性があります。

## STP および RSTP 機能の設定

この項では、スパンニングツリー機能の設定方法について説明します。

- STP および RSTP のデフォルト設定 (p.7-16)
- STP および RSTP のディセーブル化 (p.7-17)
- ルート スイッチの設定 (p.7-17)
- ポート プライオリティの設定 (p.7-18)
- パス コストの設定 (p.7-18)
- ブリッジグループのスイッチ プライオリティの設定 (p.7-19)
- Hello タイムの設定 (p.7-20)
- ブリッジグループの転送遅延時間の設定 (p.7-21)
- ブリッジグループの最大エージング タイムの設定 (p.7-21)

## STP および RSTP のデフォルト設定

表 7-5 に、STP および RSTP のデフォルト設定を示します。

表 7-5 STP および RSTP のデフォルト設定

機能	デフォルト設定
イネーブル状態	最大 255 のスパンニングツリー インスタンスをイネーブルにできます。
スイッチ プライオリティ	32768 + ブリッジ ID
スパンニングツリー ポート プライオリティ(インターフェイス単位で設定可能 レイヤ 2 アクセスポートとして設定されたインターフェイスで使用)	128
スパンニングツリー ポート コスト(インターフェイス単位で設定可能)	1000 Mbps : 4 100 Mbps : 19 10 Mbps : 100 STS-1 : 37 STS-3c : 14 STS-6c : 9 STS-9c : 7 STS-12c : 6 STS-24c : 3
Hello タイム	2 秒
転送遅延時間	15 秒
最大エージング タイム	20 秒

## STP および RSTP のディセーブル化

ネイティブ VLAN 1 および新規作成されたすべての VLAN 上で、スパンニングツリーに指定された 255 の制限を上限として、STP はデフォルトでイネーブルになっています。ネットワーク トポロジーにループが存在しないことが確実にある場合のみ、STP をディセーブルにします。



### 注意

STP エッジ ポートは、そのポートの外部でループ保護を必要としない場合、またはそのポートの外部に STP ネイバが存在しない場合に、STP をイネーブルにする必要のないブリッジ ポートです。RSTP の場合、適切なインターフェイスで `bridge bridge-group-number spanning-disabled` コマンドを使用して、エッジ ポート（通常は正面側のイーサネット ポート）で STP をディセーブルにすることが重要です。RSTP がエッジ ポートでディセーブルになっていない場合、エッジ ポートを通するパケットのコンバージェンス タイムが過大になります。



### 注意

STP がディセーブルで、トポロジーにループが存在していると、過度のトラフィックが発生し、パケットの重複が無限に繰り返されるため、ネットワークのパフォーマンスが大幅に低下します。

VLAN 単位で STP または RSTP をディセーブルにするには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <code>configure terminal</code>	グローバル 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	Router(config)# <code>interface interface-id</code>	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	Router(config-if)# <code>bridge-group bridge-group-number spanning disabled</code>	インターフェイス単位で STP または RSTP をディセーブルにします。
ステップ 4	Router(config-if)# <code>end</code>	イネーブル EXEC モードに戻ります。

STP を再度イネーブルにするには、`no bridge-group bridge-group-number spanning disabled` インターフェイスレベル コンフィギュレーション コマンドを使用します。

## ルート スイッチの設定

スイッチは、スイッチに設定されたアクティブな各 VLAN について個別のスパンニングツリー インスタンスを保持します。スイッチ プライオリティとスイッチ MAC アドレスで構成されるブリッジ ID は、各インスタンスに関連付けられています。各 VLAN では、最小のブリッジ ID を持つスイッチがその VLAN のルート スイッチになります。



### (注)

ネットワークが拡張システム ID をサポートするスイッチとサポートしていないスイッチの両方で構成されている場合、拡張システム ID をサポートするスイッチがルート スイッチになる可能性はほとんどありません。ブリッジ ID が旧ソフトウェアを実行している接続スイッチのプライオリティよりも大きくなるたびに、拡張システム ID のスイッチ プライオリティ値が増加します。

## ポート プライオリティの設定

ループが発生した場合、スパニングツリーはポート プライオリティを使用して、フォワーディング状態にするインターフェイスを選択します。最初に選択させたいインターフェイスには、高いプライオリティ値（小さい数値）を割り当て、最後に選択させたいインターフェイスには、低いプライオリティ値（大きい数値）を割り当てることができます。すべてのインターフェイスに同じプライオリティ値が割り当てられている場合、スパニングツリーはインターフェイス番号が最も小さいインターフェイスをフォワーディング状態にし、他のインターフェイスをブロックします。

インターフェイスのポート プライオリティを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b>	グローバル 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	Router(config)# <b>interface interface-id</b>	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、設定するインターフェイスを指定します。  有効なインターフェイスとして、物理インターフェイスとポートチャネル論理インターフェイス ( <b>port-channel port-channel-number</b> ) があります。
ステップ 3	Router(config-if)# <b>bridge-group bridge-group-number priority-value</b>	アクセスポートであるインターフェイスのポート プライオリティを設定します。  <i>priority-value</i> に指定できる範囲は、0 ~ 255 です。デフォルトは 128 で 16 ずつ増加します。数字が小さいほど、プライオリティは高くなります。
ステップ 4	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。

インターフェイスをデフォルト設定に戻すには、**no bridge-group id bridge-group-number priority-value** コマンドを使用します。

## パス コストの設定

スパニングツリーのパス コストのデフォルト値は、インターフェイスのメディア速度から取得されます。ループが発生した場合、スパニングツリーはコストを使用して、フォワーディング状態にするインターフェイスを選択します。最初に選択させたいインターフェイスには、低いコスト値を割り当て、最後に選択させたいインターフェイスには高いコスト値を割り当てることができます。すべてのインターフェイスに同じコスト値が割り当てられている場合、スパニングツリーはインターフェイス番号が最も小さいインターフェイスをフォワーディング状態にし、他のインターフェイスをブロックします。

インターフェイスのコストを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b>	グローバル 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	Router(config)# <b>interface interface-id</b>	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、設定するインターフェイスを指定します。  有効なインターフェイスとして、物理インターフェイスとポートチャネル論理インターフェイス ( <b>port-channel port-channel-number</b> ) があります。
ステップ 3	Router(config-if)# <b>bridge-group bridge-group-number path-cost cost</b>	アクセス ポートであるインターフェイスのコストを設定します。  ループが発生した場合、スパニングツリーはパス コストを使用して、フォワーディング ステートにするインターフェイスを選択します。パス コストが小さいほど、高速な伝送になります。  <i>cost</i> に指定できる範囲は、0 ~ 65535 です。デフォルト値は、インターフェイスのメディア速度から取得されます。
ステップ 4	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。



(注) **show spanning-tree interface interface-id** イネーブル EXEC コマンドは、リンクアップ動作状態になっているポートの情報だけを表示します。それ以外の場合は、**show running-config** イネーブル EXEC コマンドを使用して設定を確認できます。

インターフェイスをデフォルト設定に戻すには、**no bridge-group bridge-group-number path-cost cost** コマンドを使用します。

## ブリッジグループのスイッチ プライオリティの設定

スイッチ プライオリティを設定し、スイッチがルート スイッチとして選択される可能性を高くできます。

ブリッジグループのスイッチ プライオリティを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b>	グローバル 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	Router(config)# <b>bridge</b> <i>bridge-group-number priority priority</i>	ブリッジ グループのスイッチ プライオリティを設定します。  <i>priority</i> に指定できる範囲は、0 ~ 61440 で 4096 ずつ増加します。デフォルトは 32768 です。数値が小さいほど、ルートスイッチとして選択される可能性が高まります。  指定した値は、4096 の倍数のうち、小さい方の数値になります。実際の数値は、ブリッジ グループ番号にこの数値を加算して算出されます。
ステップ 3	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。

スイッチをデフォルト設定に戻すには、**no bridge bridge-group-number priority priority** コマンドを使用します。

## Hello タイムの設定

Hello タイムを変更することによって、ルートスイッチで設定メッセージが生成される間隔を設定できます。

ブリッジグループの Hello タイムを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b>	グローバル 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	Router(config)# <b>bridge</b> <i>bridge-group-number hello-time seconds</i>	ブリッジ グループの Hello タイムを設定します。 Hello タイムは、ルートスイッチによって設定メッセージが生成される間隔です。このメッセージは、スイッチが動作中であることを意味します。  <i>seconds</i> に指定できる範囲は、1 ~ 10 です。デフォルトは 2 です。
ステップ 3	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。

スイッチをデフォルト設定に戻すには、**no bridge bridge-group-number hello-time seconds** コマンドを使用します。

## ブリッジグループの転送遅延時間の設定

ブリッジグループの転送遅延時間を設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b>	グローバル 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	Router(config)# <b>bridge bridge-group-number forward-time seconds</b>	VLAN の転送時間を設定します。転送遅延は、ポートが、スパンニングツリーのラーニングおよびリスニング ステートからフォワーディング ステートに移行するまでに待機する秒数です。  <i>seconds</i> に指定できる範囲は、4 ~ 200 です。デフォルトは 15 です。
ステップ 3	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。

スイッチをデフォルト設定に戻すには、**no bridge bridge-group-number forward-time seconds** コマンドを使用します。

## ブリッジグループの最大エイジング タイムの設定

ブリッジグループの最大エイジング タイムを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b>	グローバル 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	Router(config)# <b>bridge bridge-group-number max-age seconds</b>	ブリッジグループの最大エイジング タイムを設定します。最大エイジング タイムは、スイッチがスパンニングツリー設定メッセージを受信しない状態で、再構成を試みるまでに待機する秒数です。  <i>seconds</i> に指定できる範囲は、6 ~ 200 です。デフォルトは 20 です。
ステップ 3	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。

スイッチをデフォルト設定に戻すには、**no bridge bridge-group-number max-age seconds** コマンドを使用します。

## STP および RSTP のステータスの確認とモニタリング

STP または RSTP のステータスを表示するには、表 7-6 に示す 1 つまたは複数のイネーブル EXEC コマンドを使用します。

表 7-6 スパニングツリー ステータスを表示するコマンド

コマンドの説明	目的
ML_Series# <b>show spanning-tree</b>	STP または RSTP の詳細情報を表示します。
ML_Series# <b>show spanning-tree brief</b>	STP または RSTP の要約情報を表示します。
ML_Series# <b>show spanning-tree interface interface-id</b>	指定したインターフェイスの STP または RSTP 情報を表示します。
ML_Series# <b>show spanning-tree summary [totals]</b>	ポート ステートの要約、あるいは STP または RSTP の状態セクションの全ての行を表示します。



(注)

**show spanning-tree interface interface-id** イネーブル EXEC コマンドは、ポートがリンクアップ動作状態になっている場合にのみ情報を表示します。それ以外の場合は、**show running-config interface** イネーブル EXEC コマンドを使用して設定を確認できます。

**show spanning-tree** イネーブル EXEC コマンドの例を次に示します。

### 例 7-1 show spanning-tree コマンド

```
Router# show spanning-tree brief

Bridge group 1
  Spanning tree enabled protocol ieee
  Root ID    Priority    32769
             Address     0005.9a39.6634
             This bridge is the root
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    32769 (priority 32768 sys-id-ext 1)
             Address     0005.9a39.6634
             Hello Time  2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300

Interface          Role Sts Cost          Prio.Nbr Type
-----
Fa0                 Desg FWD 19          128.3   P2p
PO0                 Desg FWD 3           128.20  P2p

Router# show spanning-tree detail

Bridge group 1 is executing the ieee compatible Spanning Tree protocol
Bridge Identifier has priority 32768, sysid 1, address 0005.9a39.6634
Configured hello time 2, max age 20, forward delay 15
We are the root of the spanning tree
Topology change flag not set, detected flag not set
Number of topology changes 2 last change occurred 00:16:45 ago
from POS0
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15
Timers: hello 0, topology change 0, notification 0, aging 300

Port 3 (FastEthernet0) of Bridge group 1 is forwarding
Port path cost 19, Port priority 128, Port Identifier 128.3.
Designated root has priority 32769, address 0005.9a39.6634
```

```

Designated bridge has priority 32769, address 0005.9a39.6634
Designated port id is 128.3, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 1
Link type is point-to-point by default
BPDU: sent 641, received 0

```

```

Port 20 (POS0) of Bridge group 1 is forwarding
Port path cost 3, Port priority 128, Port Identifier 128.20.
Designated root has priority 32769, address 0005.9a39.6634
Designated bridge has priority 32769, address 0005.9a39.6634
Designated port id is 128.20, designated path cost 0
Timers: message age 0, forward delay 0, hold 0
Number of transitions to forwarding state: 6
Link type is point-to-point by default
BPDU: sent 582, received 15

```

Router# **show spanning-tree interface fast 0**

Bridge Group	Role	Sts	Cost	Prio.Nbr	Type
Bridge group 1	Desg	FWD	19	128.3	P2p

Router# **show spanning-tree interface pos 0**

Bridge Group	Role	Sts	Cost	Prio.Nbr	Type
Bridge group 1	Desg	FWD	3	128.20	P2p

Router# **show spanning-tree summary totals**

```

Switch is in pvst mode
Root bridge for: Bridge group 1

```

Name	Blocking	Listening	Learning	Forwarding	STP Active
1 bridge	0	0	0	2	2

■ STP および RSTP のステータスの確認とモニタリング



## VLAN の設定

---

この章では、ML シリーズ カードの VLAN (仮想 LAN) 設定について説明します。ここでは、IEEE 802.1Q VLAN カプセル化の設定方法について説明します。この章で使用する Cisco IOS コマンドの詳細については、『Cisco IOS Command Reference』を参照してください。

この章の内容は次のとおりです。

- [VLAN の概要 \(p.8-2\)](#)
- [IEEE 802.1Q VLAN のカプセル化の設定 \(p.8-3\)](#)
- [IEEE 802.1Q VLAN の設定 \(p.8-4\)](#)
- [VLAN 動作のモニタリングと確認 \(p.8-6\)](#)



(注)

---

VLAN の設定は任意です。任意の手順として VLAN の設定に進む前に、一般的なインターフェイスの設定を完了してください。

---

## VLAN の概要

VLAN を使用することで、ネットワーク管理者は物理的な位置に基づいてではなく、論理的にユーザをグループ化できます。VLAN は、ネットワークに付随する従来の制約を受けることなく、イントラグループの安全なデータ転送および通信を可能にする標準 LAN のエミュレーションです。また、VLAN をスイッチ内部で設定されたブロードキャスト ドメインとみなすこともできます。VLAN を設定すると、各スイッチで複数のサブネット（または VLAN）をサポートできるため、ルータおよびスイッチは 1 つの物理リンク上で複数のサブネットをサポートすることが可能になります。同じ VLAN に属する装置グループは、異なる LAN セグメントに配置されていても、同じ LAN セグメントに配置されている場合と同様に通信するよう設定されます。

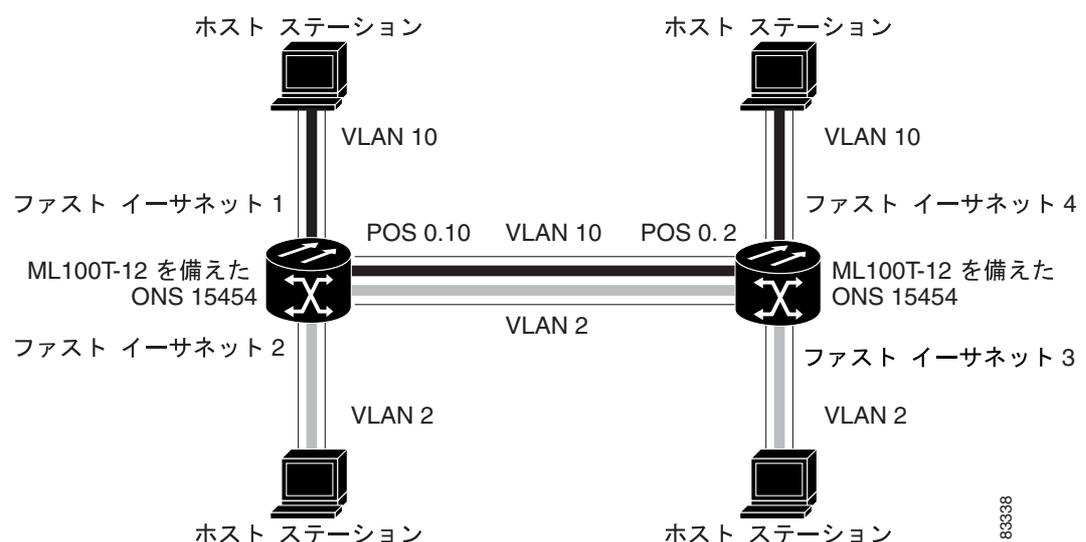
VLAN によって、トラフィックを効率的に分離し、優れた帯域幅利用率を実現できます。VLAN は、パケットが同じ VLAN 内のポート間だけでスイッチングされるように、物理的な LAN 構造を異なるサブネットワークに論理的に分割するため、スケーリングの問題も軽減されます。これは、セキュリティ、ブロードキャストの抑制、およびアカウントिंगにおいて非常に役立ちます。

ML シリーズ ソフトウェアは、ポートベースの VLAN および VLAN トランク ポートをサポートします。VLAN トランク ポートは、複数の VLAN のトラフィックを伝送するポートです。トランクリンク上で送信される各フレームには、1 つの VLAN にだけ属していることを示すタグが付けられます。

ML シリーズ カード ソフトウェアは、IEEE 802.1Q 規格による VLAN フレームのカプセル化をサポートします。Cisco ISL（スイッチ間リンク）の VLAN フレームのカプセル化はサポートされていません。ISL フレームは、レイヤ 2 でブロードキャストされるか、レイヤ 3 でドロップされます。

ML シリーズのスイッチングは、カードごとに最大 900 の VLAN サブインターフェイスをサポートします（たとえば、4 つのインターフェイスの 200 の VLAN では、800 の VLAN サブインターフェイスを使用します）。最大 255 の論理 VLAN をカードごとにブリッジできます（ブリッジグループの数により制限される）。各 VLAN サブインターフェイスは、1 ~ 4095 の範囲の任意の VLAN ID に対して設定できます。図 8-1 に、ML シリーズ カードを備えた 2 つの ONS 15454 にまたがる 2 つの VLAN が設定されたネットワーク トポロジを示します。

図 8-1 ネットワーク内の装置にまたがる VLAN



## IEEE 802.1Q VLAN のカプセル化の設定

ML シリーズ カードのどちらかのタイプのインターフェイス (イーサネットまたは Packet-over-SONET/SDH [POS]) で、IEEE 802.1Q の VLAN カプセル化を設定できます。VLAN カプセル化は、HDLC カプセル化が設定された POS インターフェイスではサポートされません。

ネイティブ VLAN は、ML シリーズ カードでは必ず VLAN ID 1 になります。ネイティブ VLAN 上のフレームは通常、タグなしで送受信されます。トランク ポートでは、ネイティブ VLAN 以外の VLAN からのすべてのフレームは、タグ付きで送受信されます。

IEEE 802.1Q の VLAN カプセル化を使用する VLAN を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>bridge</b> <i>bridge-group-number</i> <b>protocol</b> <i>type</i>	ブリッジ グループ (VLAN) 番号を割り当て、適切な spanning-tree タイプを定義します。
ステップ 2	Router(config)# <b>interface</b> <i>type number</i>	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、インターフェイスを設定します。
ステップ 3	Router(config-if)# <b>no ip</b> <b>address</b>	IP 処理をディセーブルにします。
ステップ 4	Router(config)# <b>interface</b> <i>type</i> <i>number.subinterface-number</i>	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、サブインターフェイスを設定します。
ステップ 5	Router(config-subif)# <b>encap dot1q</b> <i>vlan-number</i>	VLAN のカプセル化を IEEE 802.1Q に設定します。
ステップ 6	Router(config-subif)# <b>bridge-group</b> <i>bridge-group-number</i>	ネットワーク インターフェイスをブリッジ グループに割り当てます。
ステップ 7	Router(config-subif)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 8	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM (不揮発性 RAM) に保存します。



(注) ML シリーズ カードのブリッジ グループでは、そのブリッジ グループに属するインターフェイス間で VLAN ID が同一である必要はありません。たとえば、ブリッジ グループは、ある VLAN ID のサブインターフェイスから異なる VLAN ID を持つサブインターフェイスに接続できます。さらに、ある VLAN ID で受信したフレームを別の VLAN ID で送信するよう変更できます。これは、VLAN 変換と呼ばれます。



(注) IP ルーティングは、デフォルトでイネーブルになっています。ブリッジングをイネーブルにするには、**no ip routing** または **bridge IRB** コマンドを使用します。



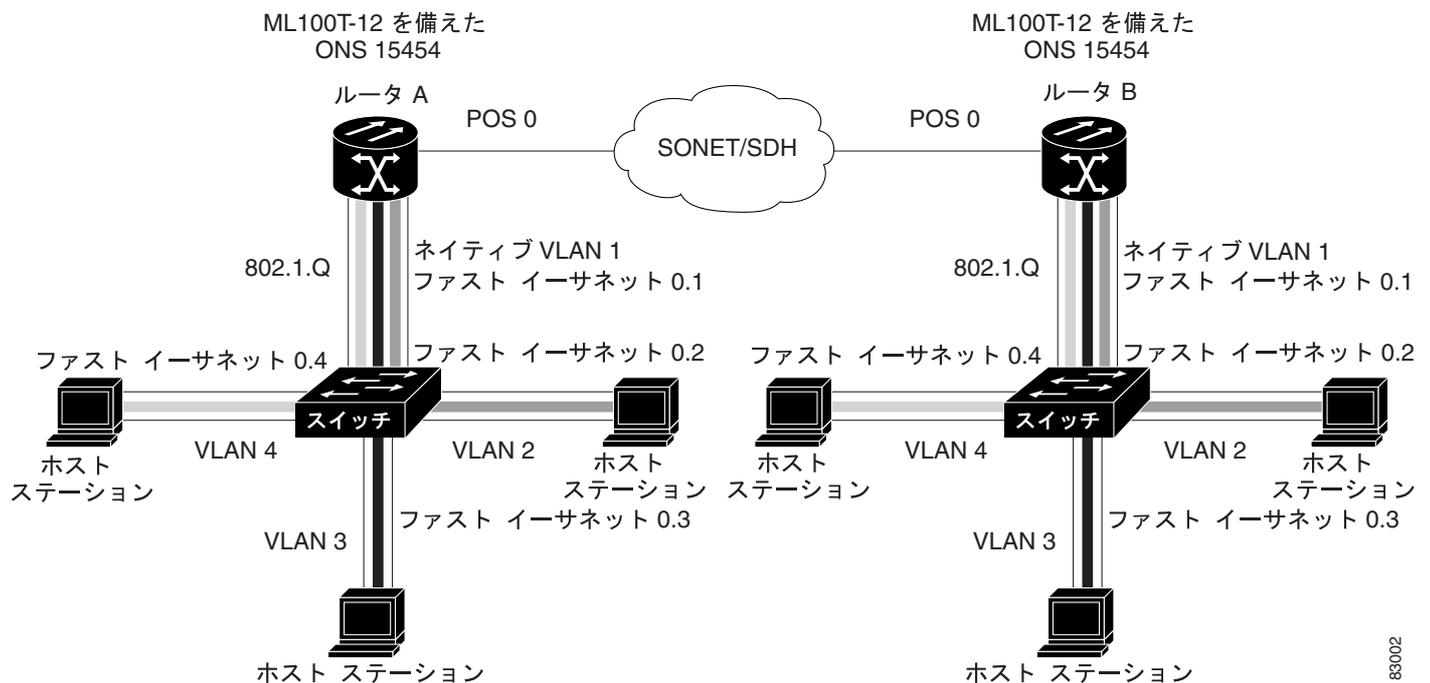
(注) インターフェイス上で送信されるネイティブ VLAN フレームは、通常タグなしです。インターフェイス上で受信されるすべてのタグなしフレームは、ネイティブ VLAN に関連付けられます。ネイティブ VLAN は、常に VLAN 1 です。 **encapsulation dot1q 1 native** コマンドを使用します。

## IEEE 802.1Q VLAN の設定

図 8-2 に示す ML100T-12 の VLAN 設定例は、次の VLAN を表しています。

- ファストイーサネットサブインターフェイス 0.1 は、IEEE 802.1Q ネイティブ VLAN 1 に含まれます。
- ファストイーサネットサブインターフェイス 0.2 は、IEEE 802.1Q VLAN 2 に含まれます。
- ファストイーサネットサブインターフェイス 0.3 は、IEEE 802.1Q VLAN 3 に含まれます。
- ファストイーサネットサブインターフェイス 0.4 は、IEEE 802.1Q VLAN 4 に含まれます。

図 8-2 IEEE 802.1Q VLAN のブリッジング



例 8-1 に、IEEE 802.1Q VLAN をカプセル化するための VLAN の設定方法を示します。この設定は、ルータ A とルータ B の両方に使用します。図 8-2 に例を示します。

## 例 8-1 IEEE 802.1Q VLAN カプセル化の VLAN 設定

```
bridge 1 protocol ieee
bridge 2 protocol ieee
bridge 3 protocol ieee
bridge 4 protocol ieee
!
!
interface FastEthernet0
  no ip address
!
interface FastEthernet0.1
  encapsulation dot1Q 1 native
  bridge-group 1
!
interface FastEthernet0.2
  encapsulation dot1Q 2
  bridge-group 2
!
interface FastEthernet0.3
  encapsulation dot1Q 3
  bridge-group 3
!
interface FastEthernet0.4
  encapsulation dot1Q 4
  bridge-group 4
!
interface POS0
  no ip address
  crc 32
  pos flag c2 1
!
interface POS0.1
  encapsulation dot1Q 1 native
  bridge-group 1
!
interface POS0.2
  encapsulation dot1Q 2
  bridge-group 2
!
interface POS0.3
  encapsulation dot1Q 3
  bridge-group 3
!
interface POS0.4
  encapsulation dot1Q 4
  bridge-group 4
```

## VLAN 動作のモニタリングと確認

ML シリーズ カードで VLAN を設定したあと、イネーブル EXEC コマンド `show vlans vlan-id` を使用して動作をモニタリングできます。このコマンドは、設定されているすべての VLAN または特定の VLAN (VLAN ID 番号を指定) の情報を表示します。

`show vlans` イネーブル EXEC コマンドの例は次の通りです。

### 例 8-2 show vlan コマンド

```
ML1000-121#show vlans
Virtual LAN ID: 1 (IEEE 802.1Q Encapsulation)
  vLAN Trunk Interfaces: POS1
GigabitEthernet0
  This is configured as native Vlan for the following interface(s) :
POS1
GigabitEthernet0
  Protocols Configured:  Address:          Received:      Transmitted:
Virtual LAN ID: 5 (IEEE 802.1Q Encapsulation)
  vLAN Trunk Interfaces: POS1.1
GigabitEthernet0.1
  Protocols Configured:  Address:          Received:      Transmitted:
  Bridging               Bridge Group 2   157           0
  Bridging               Bridge Group 2   157           0
```



# IEEE 802.1Q および レイヤ 2 プロトコルのトンネリング設定

Virtual Private Network (VPN; 仮想私設網) は、共有インフラストラクチャ (多くの場合、イーサネットベース) 上で、プライベート ネットワークと同じセキュリティ、優先順位付け、信頼性および管理性の要件で企業規模の接続を行います。トンネリングは、ネットワークで複数のカスタマーのトラフィックを伝送するサービス プロバイダーを対象に設計された機能です。サービス プロバイダーは、他のカスタマーのトラフィックを低下させることなく、各カスタマーの VLAN (仮想 LAN) およびレイヤ 2 プロトコル設定を維持する必要があります。ML シリーズ カードは、IEEE 802.1Q トンネリングおよびレイヤ 2 プロトコル トンネリングをサポートしています。

この章の内容は次のとおりです。

- [IEEE 802.1Q トンネリングの概要 \(p.9-2\)](#)
- [IEEE 802.1Q トンネリングの設定 \(p.9-5\)](#)
- [VLAN 透過サービスおよび VLAN 固有サービスの概要 \(p.9-8\)](#)
- [レイヤ 2 プロトコル トンネリングの概要 \(p.9-13\)](#)
- [レイヤ 2 プロトコル トンネリングの設定 \(p.9-14\)](#)

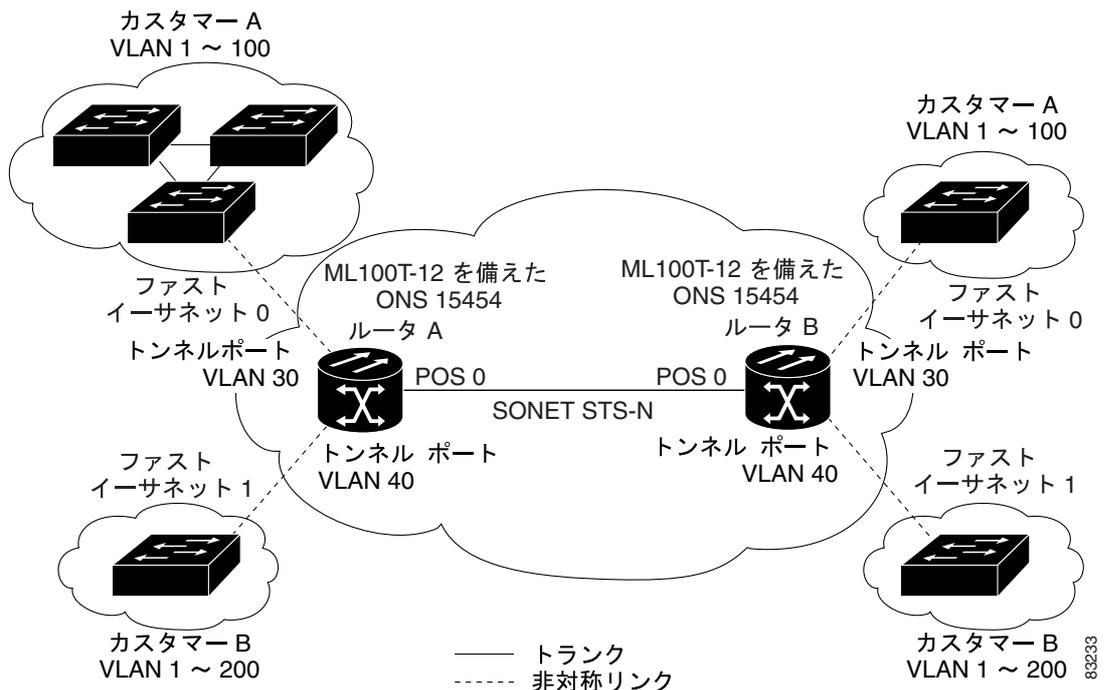
## IEEE 802.1Q トンネリングの概要

多くの場合、サービスプロバイダーのビジネスカスタマーには、VLAN ID (VID) と、サポートされる VLAN の数について特定の要件があります。同じサービスプロバイダー ネットワーク内のさまざまなカスタマーが必要とする VLAN の範囲は重複する場合があります、インフラストラクチャを介したカスタマーのトラフィックが混在する場合があります。各カスタマーに、固有の範囲の VLAN ID を割り当てると、カスタマーの設定を制限することになり、IEEE 802.1Q 仕様の 4096 という VLAN の制限を容易に超える可能性があります。

IEEE 802.1Q トンネリング (QinQ) 機能を使用することにより、サービスプロバイダーは複数の VLAN を設定しているカスタマーを、1 つの VLAN を使用してサポートできます。カスタマーの VID は保持されるため、さまざまなカスタマーからのトラフィックは、同じ VLAN 上に存在するように見える場合でも、サービスプロバイダーのインフラストラクチャ内では分離されています。IEEE 802.1Q トンネリングでは、VLAN 内 VLAN 階層を使用して、タグ付きパケットに再度タグ付けを行うことによって、VLAN スペースを拡張します。IEEE 802.1Q トンネリングをサポートするように設定されたポートは、トンネルポートと呼ばれます。トンネリングを設定するときには、トンネリング専用の VLAN にトンネルポートを割り当てます。各カスタマーは個別の VLAN を必要としますが、その VLAN はカスタマーのすべての VLAN をサポートします。

通常の方法で適切な VID をタグ付けされたカスタマー トラフィックは、カスタマー装置の IEEE 802.1Q トランクポートから ML シリーズカードのトンネルポートに着信します。カスタマー装置と ML シリーズカード間のリンクは非対称リンクです。これは、両端の片方が IEEE 802.1Q トランクポートとして設定されており、もう片方がトンネルポートとして設定されているためです。各カスタマーの一意のアクセス VID に、トンネルポートインターフェイスを割り当てます (図9-1)。

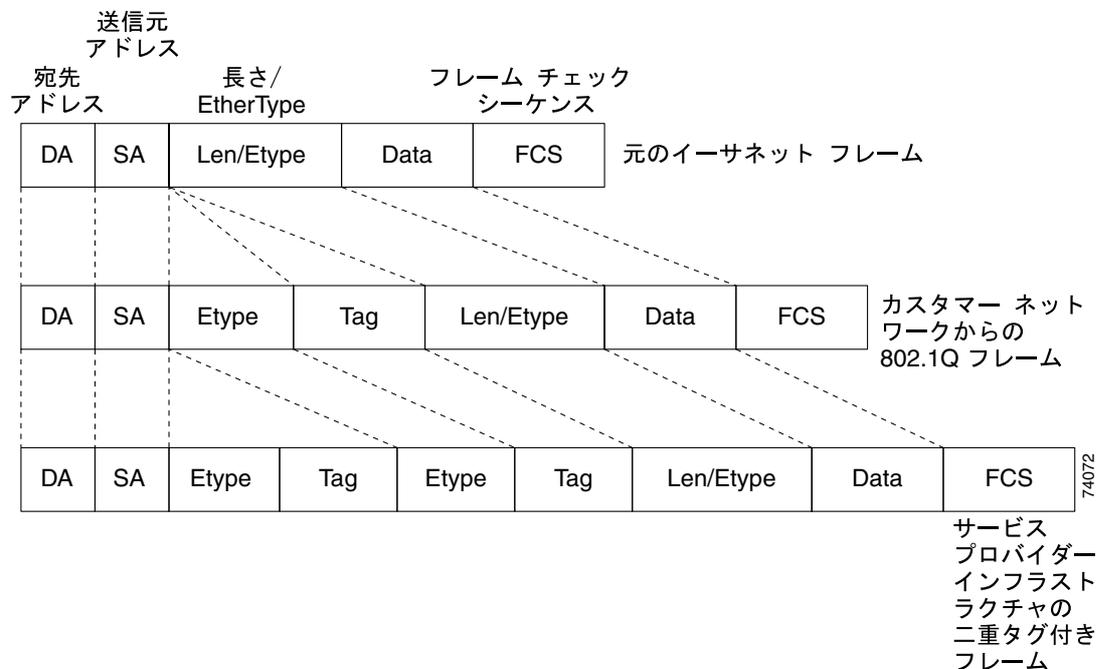
図 9-1 サービスプロバイダー ネットワークの IEEE 802.1Q トンネルポート



カスタマーのトランク ポートから、ML シリーズ カードのトンネル ポートに着信するパケットには、通常、適切な VID を持つ IEEE 802.1Q がタグ付けされています。このタグ付きパケットは、ML シリーズ カード内に元の状態のまま保たれ、パケットがトランク ポートからサービス プロバイダー ネットワークに発信されるときに、カスタマーの一意の VID が含まれた別のレイヤの IEEE 802.1Q タグ (メトロ タグ) 付きでカプセル化されます。カスタマーの元の IEEE 802.1Q タグは、カプセル化されたパケット内に保存されます。したがって、サービスプロバイダー インフラストラクチャに入るパケットには、二重のタグが付けられていることとなります。外側のタグにはカスタマーのアクセス VID が格納されており、着信トラフィックの VLAN となる内部 VID が格納されています。

二重タグ付きパケットがサービス プロバイダーの ML シリーズ カードにある別のトランク ポートに入ると、スイッチ内でパケットが処理されるときに、外側のタグが外されます。同じコア スイッチの別のトランク ポートからパケットが送出されるときには、同じメトロ タグがパケットに再度追加されます。図 9-2 に、二重タグ付きパケットの構造を示します。

図 9-2 イーサネット パケットの形式 (標準、IEEE 802.1Q、および IEEE 802.1Q トンネリング)



パケットがサービスプロバイダー出力スイッチのトランク ポートに入ると、スイッチでパケットが内部処理されるときに、外側のタグが再度除去されます。ただし、パケットがエッジスイッチのトンネル ポートからカスタマー ネットワークに送信されるときには、メトロ タグは追加されません。カスタマー ネットワーク内の元の VLAN 番号を保持するために、パケットは通常の IEEE 802.1Q タグ付きフレームとして送信されます。

図 9-1 では、カスタマー A には VLAN 30 が、カスタマー B には VLAN 40 がそれぞれ割り当てられています。IEEE 802.1Q タグ付きで ML シリーズ カードのトンネル ポートに入るパケットは、サービスプロバイダー ネットワークに入る時点で二重タグ付きになります。外側のタグには VLAN ID 30 または 40 が適宜格納され、内側のタグには元の VLAN 番号 (VLAN 100 など) が格納されます。カスタマー A と B の両方がネットワークで VLAN 100 を使用している場合でも、外側のタグが異なるため、トラフィックはサービスプロバイダー ネットワーク内で分離された状態で保たれます。

IEEE 802.1Q トンネリングでは、各カスタマーは固有の VLAN 番号スペースを制御します。これは、他のカスタマーやサービスプロバイダー ネットワークが使用する VLAN 番号スペースとは別のものです。

発信トンネルポートでは、カスタマー ネットワークの元の VLAN 番号が復元されます。カスタマー ネットワークから着信するトラフィックがタグ付けされていない場合（ネイティブ VLAN フレーム）、これらのパケットは通常のパケットと同様にブリッジングまたはルーティングされ、サービスプロバイダーのネットワークに送出されるときに、メトロ タグが（単一レベルのタグとして）追加されます。

ネイティブ VLAN（VLAN 1）が、サービスプロバイダー ネットワークでメトロ タグとして使用されている場合は、ネイティブ VID が通常は送信フレームに追加されていない場合でも、このタグはカスタマー トラフィックに必ず追加される必要があります。VLAN 1 メトロ タグがサービスプロバイダー ネットワークに入ったフレームに追加されないと、カスタマー VLAN タグがメトロ タグとみなされるという、あってはならない結果を招きます。vlan dot1q tag native 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 VLAN 1 に強制的にタグを追加し、このような状況を防ぐ必要があります。誤った設定のリスクを軽減するために、カスタマー トラフィックを搬送するメトロ タグとして VLAN 1 を使用しないようにすることを推奨します。最も望ましい設定は、VLAN 1 を、サービスプロバイダーのネットワークでプライベートに管理された VLAN として使用することです。

追加されたメトロ タグの IEEE 802.1Q Class of Service（CoS; サービス クラス）のプライオリティ フィールドは、デフォルトでは0（ゼロ）に設定されていますが、入力または出力ポリシー マップで変更できます。

## IEEE 802.1Q トンネリングの設定

ここでは、IEEE 802.1Q トンネリングの設定について説明します。内容は次のとおりです。

- [IEEE 802.1Q トンネリングおよび他の機能との互換性 \(p.9-5\)](#)
- [IEEE 802.1Q トンネル ポートの設定 \(p.9-5\)](#)
- [IEEE 802.1Q の例 \(p.9-7\)](#)



(注) ML シリーズでは、デフォルトで IEEE 802.1Q トンネリングは設定されていません。

### IEEE 802.1Q トンネリングおよび他の機能との互換性

IEEE 802.1Q トンネリングは、レイヤ 2 パケット スイッチングについては適切に機能しますが、レイヤ 2 機能の一部およびレイヤ 3 スイッチングとの互換性はありません。

- トンネル ポートはルーテッド ポートにできません。
- トンネル ポートは IP Access Control List (ACL; アクセス制御リスト) をサポートしていません。
- レイヤ 3 の Quality of Service (QoS; サービス品質) ACL とレイヤ 3 情報に関連する他の QoS 機能は、トンネル ポートではサポートされていません。MAC (メディア アクセス制御) ベースの QoS は、トンネル ポートでサポートされています。
- EtherChannel ポート グループは、IEEE 802.1Q 設定が EtherChannel ポート グループ内で矛盾がない限り、トンネル ポートと互換性があります。
- Port Aggregation Protocol (PAgP; ポート集約プロトコル) および Unidirectional Link Detection (UDLD; 単一方向リンク検出) プロトコルは、IEEE 802.1Q トンネル ポートではサポートされていません。
- Dynamic Trunking Protocol (DTP; ダイナミック トランキング プロトコル) は、IEEE 802.1Q トンネリングと互換性はありません。これは、トンネル ポートとトランク ポートの非対称リンクを手動で設定する必要があるためです。
- ループバック検出は、IEEE 802.1Q トンネル ポートでサポートされています。
- ポートが IEEE 802.1Q トンネル ポートとして設定されている場合、スパンニングツリーの Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) フィルタリングは、インターフェイスで自動的にディセーブルになります。

### IEEE 802.1Q トンネル ポートの設定

ポートを IEEE 802.1Q トンネル ポートとして設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <code>configure terminal</code>	グローバル 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	Router(config)# <code>bridge bridge-number protocol bridge-protocol</code>	ブリッジ番号を作成し、プロトコルを指定します。

## ■ IEEE 802.1Q トンネリングの設定

	コマンドの説明	目的
ステップ 3	Router(config)# <b>interface fastethernet</b> <i>number</i>	インターフェイス コンフィギュレーション モードを開始して、トンネルポートとして設定するインターフェイスを指定します。これは、カスタマー スイッチに接続するサービスプロバイダー ネットワークのエッジポートである必要があります。有効なインターフェイスには、物理インターフェイスとポートチャンネル論理インターフェイス（ポートチャンネル 1 ~ 64）があります。
ステップ 4	Router(config-if)# <b>bridge-group</b> <i>number</i>	ブリッジ グループにトンネルポートを割り当てます。ポートからのすべてのトラフィック（タグ付きおよびタグなし）は、このブリッジグループに基づいてスイッチングされます。ブリッジグループの他のメンバーは、プロバイダー トランク インターフェイスの VLAN サブインターフェイスである必要があります。
ステップ 5	Router(config-if)# <b>mode dot1q-tunnel</b>	インターフェイスを IEEE 802.1Q トンネルポートとして設定します。
ステップ 6	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 7	Router# <b>show dot1q-tunnel</b>	スイッチのトンネルポートを表示します。
ステップ 8	Router# <b>copy running-config startup-config</b>	（任意）コンフィギュレーション ファイルにエントリを保存します。



(注) ML シリーズ カードの IEEE 802.1Q トンネリング用に推奨される VID の範囲は 2 ~ 4095 です。



(注) VID 1 をメトロ タグとして使用する必要がある場合は、次のコマンドを使用します。

```
Router (config)# VLAN dot1Q tag native
```

インターフェイスから IEEE 802.1Q トンネルを削除するには、**no mode dot1q-tunnel** 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。

## IEEE 802.1Q の例

次の例は、[図 9-1](#) の例の設定方法を示しています。[例 9-1](#) をルータ A に適用し、[例 9-2](#) をルータ B に適用します。

### 例 9-1 ルータ A の設定

```
bridge 30 protocol ieee
bridge 40 protocol ieee
!
!
interface FastEthernet0
no ip routing
no ip address
mode dot1q-tunnel
bridge-group 30
!
interface FastEthernet1
no ip address
mode dot1q-tunnel
bridge-group 40
!
interface POS0
no ip address
crc 32
pos flag c2 1
!
interface POS0.1
encapsulation dot1Q 30
bridge-group 30
!
interface POS0.2
encapsulation dot1Q 40
bridge-group 40
```

### 例 9-2 ルータ B の設定

```
bridge 30 protocol ieee
bridge 40 protocol ieee
!
!
interface FastEthernet0
no ip routing
no ip address
mode dot1q-tunnel
bridge-group 30
!
interface FastEthernet1
no ip address
mode dot1q-tunnel
bridge-group 40
!
interface POS0
no ip address
crc 32
pos flag c2 1
!
interface POS0.1
encapsulation dot1Q 30
bridge-group 30
!
interface POS0.2
encapsulation dot1Q 40
bridge-group 40
```

## VLAN 透過サービスおよび VLAN 固有サービスの概要

ML シリーズ カードでは、VLAN 透過サービスと 1 つまたは複数の VLAN 固有サービスを同じポートで組み合わせることができます。この VLAN 透過サービスおよび VLAN 固有サービスはすべて、ポイントツーポイントまたはマルチポイントツーマルチポイントにできます。

これにより、サービス プロバイダーは、同じカスタマー ポートで、IEEE 802.1Q トンネリング (QinQ) などの VLAN 透過サービスと、特定の VLAN のブリッジングなどの VLAN 固有サービスを組み合わせることができます。たとえば、各サイトの 1 つのポート全体で、あるカスタマー VLAN はインターネット アクセスに接続し、他のカスタマー VLAN は単一のプロバイダー VLAN 上で別のカスタマー サイトにトンネリングできます。表 9-1 に、VLAN 透過サービスと VLAN 固有サービスの違いをまとめます。

表 9-1 VLAN 透過サービスと VLAN 固有サービス

VLAN 透過サービス	VLAN 固有サービス
ブリッジングのみ	ブリッジングまたはルーティング
ポート 1 つにつき 1 つのサービス	ポート 1 つにつき最大 254 の VLAN 固有サービス
物理インターフェイスのすべての VLAN に無差別に適用	指定した VLAN だけに適用



(注)

VLAN 透過サービスは、Ethernet Wire Service (EWS) とも呼びます。VLAN 固有サービスは、メトロイーサネット用語で QinQ トンネリング トランク UNI とも呼ばれます。

サブインターフェイスの VLAN 固有サービスは、物理インターフェイスの VLAN 透過サービス(多くの場合、IEEE 802.1Q トンネリング)と共存しています。VLAN 透過サービスと VLAN 固有サービス用に VLAN を設定する場合、VLAN 固有サービス設定に従います。802.1Q トンネリングを設定する必要がある場合は、通常の方法でこの VLAN 透過サービスを設定します(「[IEEE 802.1Q トンネリングの設定](#)」[p.9-5] を参照)。

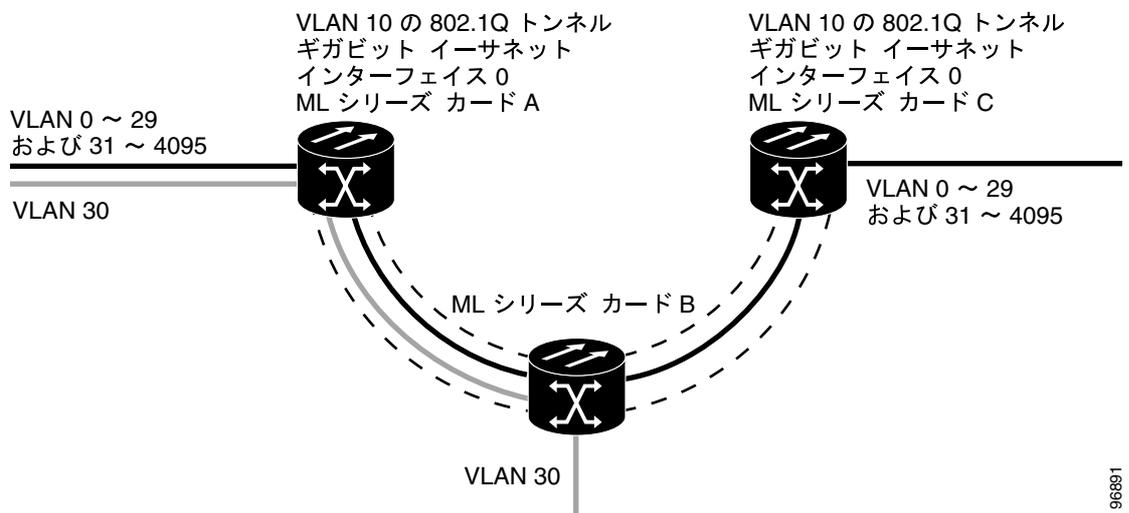
VLAN 固有サービスには、VLAN に通常適用できるサービスであれば、どのサービスでも指定できます。ERMS VLAN 固有サービスを設定する場合は、通常の方法でサービスを設定します。

## VLAN 透過サービスおよび VLAN 固有サービスの設定例

この例では、ML シリーズカード A と ML シリーズカード C のギガビット イーサネット インターフェイス 0 は、VLAN 透過サービスである IEEE 802.1Q トンネルのトランク ポートです。VLAN 10 は VLAN 透過サービスに使用されます。VLAN 透過サービスは、ML シリーズカード A のギガビット イーサネット インターフェイス 0 のすべてのカスタマー VLAN を通常どおり伝送します。また、指定されていないすべての VLAN と VLAN 1 も VLAN 10 でトンネリングされます。

VLAN 30 は、VLAN 透過サービスに入らない代わりに、特定の VLAN サービスに転送され、ML シリーズカード A のギガビット イーサネット インターフェイス 0 と、ML シリーズカード B のギガビット イーサネット インターフェイス 0 をブリッジングします。図 9-3 は、設定例 9-3、9-4、および 9-5 を実行する際の例として使用します。

図 9-3 ERMS の例



16896

例 9-3 は、ML シリーズ カード A に適用します。

### 例 9-3 ML シリーズ カード A の設定

```
hostname ML-A
bridge 10 protocol rstp
bridge 30 protocol ieee
!
!
interface GigabitEthernet0
  no ip address
  no ip route-cache
  mode dot1q-tunnel
  bridge-group 10
  bridge-group 10 spanning-disabled
!
interface GigabitEthernet0.3
  encapsulation dot1Q 30
  no ip route-cache
  bridge-group 30
!
interface POS0
  no ip address
  no ip route-cache
  crc 32
!
interface POS0.1
  encapsulation dot1Q 10
  no ip route-cache
  bridge-group 10
!
interface POS0.3
  encapsulation dot1Q 30
  no ip route-cache
  bridge-group 30
```

例 9-4 は、ML シリーズ カード B に適用します。

#### 例 9-4 ML シリーズ カード B の設定

```
hostname ML-B
!
bridge 10 protocol rstp
bridge 30 protocol ieee
!
!
interface GigabitEthernet0
  no ip address
!
interface GigabitEthernet0.3
  encapsulation dot1Q 30
  bridge-group 30
!
interface GigabitEthernet1
  no ip address
  shutdown
!
interface POS0
  no ip address
  crc 32
!
interface POS0.1
  encapsulation dot1Q 10
  bridge-group 10
!
interface POS0.3
  encapsulation dot1Q 30
  bridge-group 30
!
interface POS1
  no ip address
  crc 32
!
interface POS1.1
  encapsulation dot1Q 10
  bridge-group 10
!
interface POS1.3
  encapsulation dot1Q 30
  bridge-group 30
```

例 9-5 は、ML シリーズ カード C に適用します。

#### 例 9-5 ML シリーズ カード C の設定

```
hostname ML-C
bridge 10 protocol rstp
!
!
interface GigabitEthernet0
  no ip address
  no ip route-cache
  mode dot1q-tunnel
  bridge-group 10
  bridge-group 10 spanning-disabled
!
interface POS0
  no ip address
  no ip route-cache
  crc 32
!
interface POS0.1
  encapsulation dot1Q 10
  no ip route-cache
  bridge-group 10
```

## レイヤ 2 プロトコル トンネリングの概要

サービスプロバイダー ネットワークで接続されたさまざまなサイトのカスタマーは、各種のレイヤ 2 プロトコルを実行してトポロジをスケーリングし、ローカル サイトだけでなく、すべてのリモート サイトも含める必要があります。Spanning Tree Protocol (STP; スパニングツリー プロトコル) が正常に実行されていることが必要となります。また、すべての VLAN で、サービスプロバイダー インフラストラクチャ内にあるローカル サイトとすべてのリモート サイトが含まれた適切なスパニングツリーを構築することが必要です。Cisco Discovery Protocol (CDP) により、ローカルおよびリモート サイトから隣接するシスコ装置を検出する必要があります。VLAN Trunking Protocol (VTP; VLAN トランキング プロトコル) により、カスタマー ネットワークのすべてのサイトで VLAN 設定に一貫性を持たせるようにする必要があります。

プロトコル トンネリングがイネーブルの場合、サービスプロバイダー インフラストラクチャの着信側のエッジスイッチは、特殊 MAC アドレスを使用してレイヤ 2 プロトコル パケットをカプセル化し、サービスプロバイダー ネットワークに送信します。ネットワークのコア スイッチはこれらのパケットを処理せずに、通常のパケットとして転送します。CDP、STP、または VTP のレイヤ 2 Protocol Data Unit (PDU; プロトコル データ ユニット) は、サービスプロバイダー インフラストラクチャを横断し、サービスプロバイダー ネットワークの出力側のカスタマー スイッチに配信されます。同じ VLAN 上のすべてのカスタマー ポートで同じパケットが受信され、次のような結果になります。

- 各カスタマー サイトのユーザは、STP を正常に実行できます。また、すべての VLAN はローカル サイトだけでなく、すべてのサイトからのパラメータに基づいて、適切なスパニングツリーを構築できます。
- CDP は、サービスプロバイダー ネットワーク経由で接続している他のシスコ装置の情報を検出し、表示します。
- VTP は、サービス プロバイダーを介してすべてのスイッチに伝播し、カスタマー ネットワーク全体で VLAN 設定に一貫性を持たせます。

レイヤ 2 プロトコル トンネリングは、単独で使用することも IEEE 802.1Q トンネリングを強化するために使用することもできます。プロトコル トンネリングが IEEE 802.1Q トンネリング ポートまたは特定の VLAN で無効になっていない場合、サービスプロバイダー ネットワークの受信側の終端にあるリモート スイッチは PDU を受信しないため、STP、CDP、および VTP を正常に実行することはできません。プロトコル トンネリングがイネーブルの場合は、各カスタマー ネットワーク内のレイヤ 2 プロトコルは、サービスプロバイダー ネットワーク内で実行するプロトコルから完全に分離されます。IEEE 802.1Q トンネリングが設定された サービスプロバイダー ネットワーク経由でトラフィックを送信するさまざまなサイト上のカスタマー スイッチは、カスタマー VLAN を完全に認識するようになります。IEEE 802.1Q トンネリングを使用していない場合には、アクセス ポートを介してカスタマー スイッチに接続し、サービスプロバイダーのアクセス ポートでトンネリングをイネーブルにすることにより、レイヤ 2 プロトコル トンネリングをイネーブルにできます。

## レイヤ 2 プロトコル トンネリングの設定

レイヤ 2 プロトコル トンネリング (プロトコル単位) は、トンネル ポート、またはサービスプロバイダー ネットワークのエッジ スイッチによってカスタマーに接続しているトンネル VLAN でイネーブルにします。ML シリーズ カードのトンネル ポートは、カスタマー IEEE 802.1Q トランク ポートに接続します。ML シリーズ カードは、インターフェイスおよびサブインターフェイス レベルで、CDP、STP、VTP のレイヤ 2 プロトコル トンネリングをサポートしています。Multiple STP (MSTP) トンネリングは、サブインターフェイス プロトコル トンネリングを通じてサポートされます。カスタマー スイッチに接続された ML シリーズ カードは、トンネリング処理を実行します。

トンネル ポートを介して着信 ML シリーズ スイッチに入ったレイヤ 2 PDU が、トランク ポートを介してサービスプロバイダー ネットワークに入ると、スイッチはカスタマー PDU の宛先 MAC アドレスをシスコ独自の既知のマルチキャスト アドレス (01-00-0c-cd-cd-d0) で上書きします。IEEE 802.1Q トンネリングがイネーブルになっている場合、パケットは二重タグ付きになります。外側のタグは、カスタマー メトロ タグであり、内側のタグはカスタマー VLAN タグです。コア スイッチは内側のタグを無視し、同じメトロ VLAN のすべてのトランク ポートにパケットを転送します。出力側の ML シリーズ スイッチは、レイヤ 2 プロトコルと MAC アドレスの適切な情報を復元してパケットを転送します。したがって、レイヤ 2 PDU は元の状態のまま保たれ、サービスプロバイダー インフラストラクチャを介してカスタマー ネットワークのもう一方の側に配信されます。

ここでは、レイヤ 2 プロトコル トンネリングの設定について説明します。内容は次のとおりです。

- [レイヤ 2 プロトコル トンネリングのデフォルト設定 \(p.9-14\)](#)
- [レイヤ 2 プロトコル トンネリングの設定に関する注意事項 \(p.9-14\)](#)
- [ポートのレイヤ 2 トンネリングの設定 \(p.9-15\)](#)
- [VLAN 単位のレイヤ 2 トンネリングの設定 \(p.9-16\)](#)
- [トンネリング ステータスのモニタリングと確認 \(p.9-16\)](#)

## レイヤ 2 プロトコル トンネリングのデフォルト設定

表 9-2 に、レイヤ 2 プロトコル トンネリングのデフォルト設定を示します。

表 9-2 レイヤ 2 プロトコル トンネリングのデフォルト設定

機能	デフォルト設定
レイヤ 2 プロトコル トンネリング	CDP、STP、および VTP に対して無効
CoS 値	データ パケット用のインターフェイスで CoS 値が設定されている場合、その値がレイヤ 2 PDU のデフォルトとして使用されます。CoS 値が設定されていない場合、デフォルトはありません。これにより、ユーザが他の方法で設定しない限り、既存の CoS 値が保持されるようになります。

## レイヤ 2 プロトコル トンネリングの設定に関する注意事項

レイヤ 2 プロトコル トンネリングの設定に関する注意事項と動作特性は次のとおりです。

- ML シリーズ カードは、Per-VLAN Protocol Tunneling (PVPT) をサポートしています。これにより、特定のサブインターフェイス (VLAN) でプロトコル トンネリングを設定し、実行できます。PVPT 設定は、サブインターフェイス レベルで行われます。
- PVPT は、接続された装置上で Multi-Session Transport (MST) BPDU を伝送する VLAN で設定する必要があります。

- ML シリーズ カードは、CDP、STP (MSTP プロトコルおよび VTP プロトコルを含む) のトンネリングをサポートしています。プロトコル トンネリングは、デフォルトでディセーブルになっていますが、IEEE 802.1Q トンネル ポートまたは特定の VLAN 上で個々のプロトコルに対してイネーブルにできます。
- トンネリングは、トランク ポートではサポートされていません。トランク ポートで `l2protocol-tunnel` インターフェイス コンフィギュレーション コマンドを入力した場合、コマンドは受け入れられますが、ポートをトンネル ポートに変更しない限り、レイヤ 2 トンネリングはイネーブルになりません。
- EtherChannel ポート グループは、IEEE 802.1Q 設定が EtherChannel ポート グループ内で設定されている限り、トンネル ポートと互換性があります。
- レイヤ 2 トンネリングがイネーブルになっているトンネル ポートまたはアクセス ポートから、カプセル化された PDU (独自の宛先 MAC アドレスを持つ) を受信すると、ループを防ぐためにそのトンネル ポートはシャットダウンされます。
- カプセル化を解除された PDU だけがカスタマー ネットワークに転送されます。サービスプロバイダー ネットワーク上で動作しているスパニングツリー インスタンスは、トンネル ポートに BPDU を転送しません。トンネル ポートから転送される CDP パケットはありません。
- トンネリングされた PDU (特に STP BPDU) は、カスタマーの仮想ネットワークが正常に動作するように、すべてのリモート サイトに配信する必要があるため、サービスプロバイダー ネットワーク内の PDU には、同じトンネル ポートから受信されるデータ パケットよりも高いプライオリティを付与できます。デフォルトでは、PDU はデータ パケットと同じ CoS 値を使用します。
- プロトコル トンネリングは、入力側ポイントと出力側ポイントの両方で対称的に設定する必要があります。たとえば、STP、CDP、VTP をトンネリングする入力側ポイントを設定した場合、同じ方法で出力側ポイントを設定する必要があります。

## ポートのレイヤ 2 トンネリングの設定

ポートをレイヤ 2 トンネル ポートとして設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <code>configuration terminal</code>	グローバル 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	Router(config)# <code>bridge bridge-group-number protocol type</code>	ブリッジ グループ番号を作成し、プロトコルを指定します。
ステップ 3	Router(config)# <code>l2protocol-tunnel cos cos-value</code>	CoS 値をレイヤ 2 トンネリング ポートに関連付けます。 <i>cos-value</i> に指定できる有効な数値の範囲は 0 ~ 7 です。
ステップ 4	Router(config)# <code>interface type number</code>	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、トンネル ポートとして設定するインターフェイスを指定します。
ステップ 5	Router(config-if)# <code>bridge-group bridge-group-number</code>	ブリッジ グループをインターフェイスに割り当てます。
ステップ 6	Router(config-if)# <code>mode dot1q tunnel</code>	インターフェイスを IEEE 802.1Q トンネル VLAN として設定します。
ステップ 7	Router(config-if)# <code>l2protocol-tunnel {all   cdp   stp   vtp}</code>	インターフェイスをレイヤ 2 プロトコル トンネル ポートとして設定し、3 つのプロトコルすべてをイネーブルにするか、CDP、STP、または VTP のいずれかを指定してイネーブルにします。これらのプロトコルは、デフォルトではオフになっています。
ステップ 8	Router(config-if)# <code>end</code>	イネーブル EXEC モードに戻ります。

## ■ レイヤ2 プロトコル トンネリングの設定

	コマンドの説明	目的
ステップ 9	Router# <code>show dot1q-tunnel</code>	スイッチのトンネルポートを表示します。
ステップ 10	Router# <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエントリを保存します。

## VLAN 単位のレイヤ2 トンネリングの設定

VLAN をレイヤ2 トンネル VLAN として設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <code>configuration terminal</code>	グローバル 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	Router(config)# <code>bridge bridge-group-number protocol type</code>	ブリッジ グループ番号を作成し、プロトコルを指定します。
ステップ 3	Router(config)# <code>l2protocol-tunnel cos cos-value</code>	CoS 値をレイヤ2 トンネリング VLAN に関連付けます。 <i>cos-value</i> に指定できる有効な数値の範囲は 0 ~ 7 です。
ステップ 4	Router(config)# <code>interface type number.subinterface-number</code>	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、トンネル VLAN として設定するサブインターフェイスを指定します。
ステップ 5	Router(config-subif)# <code>encapsulation dot1q bridge-group-number</code>	サブインターフェイスを IEEE 802.1Q のトンネル VLAN として設定します。
ステップ 6	Router(config-subif)# <code>bridge-group bridge-group-number</code>	ブリッジ グループをインターフェイスに割り当てます。
ステップ 7	Router(config-subif)# <code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 8	Router# <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエントリを保存します。

## トンネリング ステータスのモニタリングと確認

表 9-3 に、IEEE 802.1Q およびレイヤ2 プロトコル トンネリングのモニタリングおよび保守に使用するイネーブル EXEC コマンドを示します。

表 9-3 トンネリングのモニタリングおよび保守に使用するコマンド

コマンドの説明	目的
<code>show dot1q-tunnel</code>	スイッチの IEEE 802.1Q トンネルポートを表示します。
<code>show dot1q-tunnel interface interface-id</code>	特定のインターフェイスがトンネルポートかどうかを確認します。
<code>show l2protocol-tunnel</code>	レイヤ2 プロトコル トンネリング のポート情報を表示します。
<code>show vlan dot1q tag native</code>	IEEE 802.1Q トンネルの情報を表示します。



## リンク集約の設定

---

この章では、EtherChannel と Packet-over-SONET/SDH (POS) チャンネルの両方の ML シリーズ カードに対するリンク集約設定方法について説明します。この章で使用する Cisco IOS コマンドの詳細については、『*Cisco IOS Command Reference*』を参照してください。

この章の内容は次のとおりです。

- [リンク集約の概要 \(p.10-2\)](#)
- [EtherChannel または POS チャンネルでのカプセル化の概要 \(p.10-9\)](#)
- [EtherChannel と POS のモニタリングと確認 \(p.10-12\)](#)

## リンク集約の概要

ML シリーズ カードでは、EtherChannel と POS チャンネルの両方を使用できます。EtherChannel は、複数の全二重 IEEE 802.3 イーサネット インターフェイスをグループ化してスイッチ、ルータ、およびサーバの間にフォールトトレラントな高速リンクを実現するトランキングテクノロジーです。EtherChannel は単一の高帯域幅のルーティングまたはブリッジングエンドポイントを形成します。主にホストとスイッチ間の接続用に設計されたものです。ML シリーズカードは、ブリッジされた POS インターフェイスまでこのリンク集約テクノロジーを拡張します。POS チャンネルは、LEX カプセル化だけでサポートされます。

リンク集約には、次のような利点があります。

- 帯域幅の論理集約
- ロード バランシング
- フォールトトレランス

ポート チャンネルは、POS チャンネルおよび EtherChannel の両方で使用される用語です。ポート チャンネル インターフェイスは、複数のインターフェイスで構成されている場合でも単一の論理インターフェイスとして扱われます。各ポート チャンネル インターフェイスは、ファスト イーサネット、ギガビット イーサネット、または POS のいずれかのタイプのインターフェイスで構成されています。すべてのポート チャンネル設定は、イーサネットまたは POS インターフェイスの個々のメンバー上ではなく、ポート チャンネル (EtherChannel または POS チャンネル) インターフェイスで実行する必要があります。ポート チャンネル インターフェイスを作成するには、`interface port-channel` インターフェイス コンフィギュレーション コマンドを入力します。

ポート チャンネル の接続は IEEE 802.1Q トランキングおよびルーティングテクノロジーと完全に互換性があります。IEEE 802.1Q トランキングでは、ポート チャンネル内で複数の VLAN を伝送できます。

各 ML100T-12、ML100X-8、または ML1000-2 カードでは、1 つの POS チャンネル、2 つの POS ポートで構成されている 1 つのポート チャンネルをサポートしています。1 つの POS チャンネルは、2 つの POS ポート容量を STS-48c または VC4-16c の最大集約容量にまとめたものです。

各 ML100T-12 は、最大 6 つの Fast Ethernet Channel (FEC; ファスト イーサネット チャンネル) および 1 つの POS チャンネルをサポートします。各 ML100T-8 は、最大 4 つの FEC および 1 つの POS チャンネルをサポートします。最大で 4 つのファスト イーサネット ポートを 1 つの FEC に束ねて、最大で 400 Mbps の全二重ファスト イーサネットまでの帯域幅スケーラビリティを提供できます。

各 ML1000-2 は、POS チャンネルを含む最大で 2 つのポート チャンネルをサポートします。最大で 2 つのギガビット イーサネット ポートを 1 つの Gigabit Ethernet Channel (GEC; ギガビット イーサネット チャンネル) に束ねて、ML1000-2 上で 2 Gbps の全二重集約容量を提供できます。



### 注意

EtherChannel インターフェイスは、レイヤ 2 またはレイヤ 3 のインターフェイスです。レイヤ 3 アドレスを物理インターフェイス上でイネーブルにしないでください。ループが発生するため、物理インターフェイス上でブリッジ グループを割り当てないでください。



### 注意

物理インターフェイスを EtherChannel (ポート チャンネル) インターフェイスから削除する前に、物理インターフェイスをディセーブルにする必要があります。物理インターフェイスをディセーブルにするには、インターフェイス コンフィギュレーション モードで `shutdown` コマンドを使用します。



(注) 複数の ML シリーズ カードにわたるリンク集約はサポートされません。



(注) ポリシングは、ポートチャネル インターフェイスではサポートされません。



(注) ML シリーズ では、Subnetwork Access Protocol (SNAP; サブネットワーク アクセス プロトコル) や ISL (スイッチ間リンク) のカプセル化されたフレームのルーティングはサポートされません。

## EtherChannel の設定

FEC または GEC を設定するには、EtherChannel インターフェイス (ポートチャネル) を作成してネットワーク IP アドレスを割り当てます。FEC または GEC のメンバーであるインターフェイスはすべて、デュプレックスや速度などのリンクパラメータが同じである必要があります。

EtherChannel インターフェイスを作成するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>interface port-channel channel-number</b>	EtherChannel インターフェイスを作成します。最大 6 つの FEC を ML100T-12 上に、4 つの FEC を ML100X-8 上に、1 つの GEC を ML1000-2 上に設定できます。
ステップ 2	Router(config-if)# <b>ip address ip-address subnet-mask</b>	IP アドレスとサブネットマスクを EtherChannel インターフェイスに割り当てます (レイヤ 3 EtherChannel の場合のみ必須)。
ステップ 3	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM (不揮発性 RAM) に保存します。

EtherChannel の他の設定作業については、<sup>『</sup>[Cisco IOS Configuration Fundamentals Configuration Guide](#)』を参照してください。

イーサネット インターフェイスを EtherChannel に割り当てるには、グローバル コンフィギュレーション モードで次の手順を実行します。

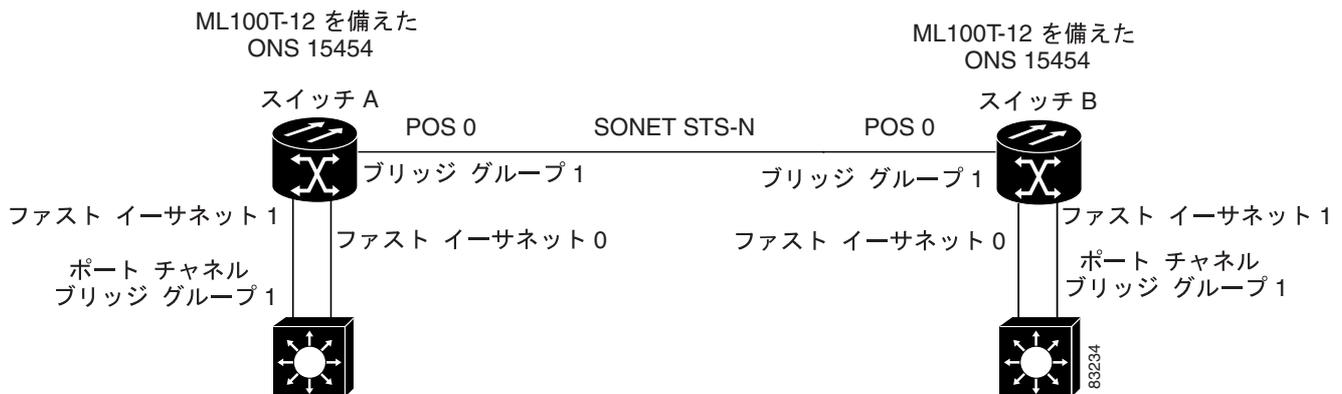
## ■ リンク集約の概要

	コマンドの説明	目的
ステップ 1	Router(config)# <b>interface fastethernet</b> <i>number</i>  または  Router(config)# <b>interface gigabitethernet</b> <i>number</i>	EtherChannel に割り当てるインターフェイス コンフィギュレーション モードとしてファスト イーサネットまたはギガビットイーサネットのうち1つを入力します。どのイーサネット インターフェイスでも EtherChannel に割り当てることができますが、インターフェイスは両方とも FEC または GEC のどちらか一方にする必要があります。
ステップ 2	Router(config-if)# <b>channel-group</b> <i>channel-number</i>	ファスト イーサネットまたはギガビット イーサネットのインターフェイスを EtherChannel に割り当てます。チャンネル番号は、EtherChannel インターフェイスに割り当てたチャンネル番号と同じである必要があります。
ステップ 3	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM (不揮発性 RAM) に保存します。

## EtherChannel の設定例

図 10-1 に、EtherChannel の設定例を示します。関連するコマンドを例 10-1 (スイッチ A) と例 10-2 (スイッチ B) に示します。

図 10-1 EtherChannel の設定例



**例 10-1 スイッチ A の設定**

```
hostname Switch A
!
bridge 1 protocol ieee
!
interface Port-channel 1
  no ip address
  bridge-group 1
  hold-queue 150 in
!
interface FastEthernet 0
  no ip address
  channel-group 1
!
interface FastEthernet 1
  no ip address
  channel-group 1
!
interface POS 0
  no ip routing
  no ip address
  crc 32
  bridge-group 1
  pos flag c2 1
```

**例 10-2 スイッチ B の設定**

```
hostname Switch B
!
bridge 1 protocol ieee
!
interface Port-channel 1
  no ip routing
  no ip address
  bridge-group 1
  hold-queue 150 in
!
interface FastEthernet 0
  no ip address
  channel-group 1
!
interface FastEthernet 1
  no ip address
  channel-group 1
!
interface POS 0
  no ip address
  crc 32
  bridge-group 1
  pos flag c2 1
!
```

## POS チャンネルの設定

POS チャンネルを設定するには、POS チャンネル インターフェイス (ポート チャンネル) を作成して、任意で IP アドレスを割り当てます。POS チャンネルのメンバーである POS インターフェイスはすべて、同じポート プロパティを持ち、同じ ML シリーズ カード上にある必要があります。



(注) POS チャンネルは、LEX カプセル化だけでサポートされます。

POS チャンネル インターフェイスを作成するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>interface port-channel</b> <i>channel-number</i>	POS チャンネル インターフェイスを作成します。ML シリーズ カード上に 1 つの POS チャンネルを設定できません。
ステップ 2	Router(config-if)# <b>ip address</b> <i>ip-address</i> <i>subnet-mask</i>	IP アドレスとサブネット マスクを POS チャンネル インターフェイスに割り当てます(レイヤ 3 POS チャンネルの場合のみ必須)。
ステップ 3	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM に保存します。



### 注意

POS チャンネル インターフェイスはルーテッド インターフェイスです。レイヤ 3 アドレスを物理 インターフェイス上でイネーブルにしないでください。ループが発生するため、物理 インターフェイス上でブリッジ グループを割り当てないでください。

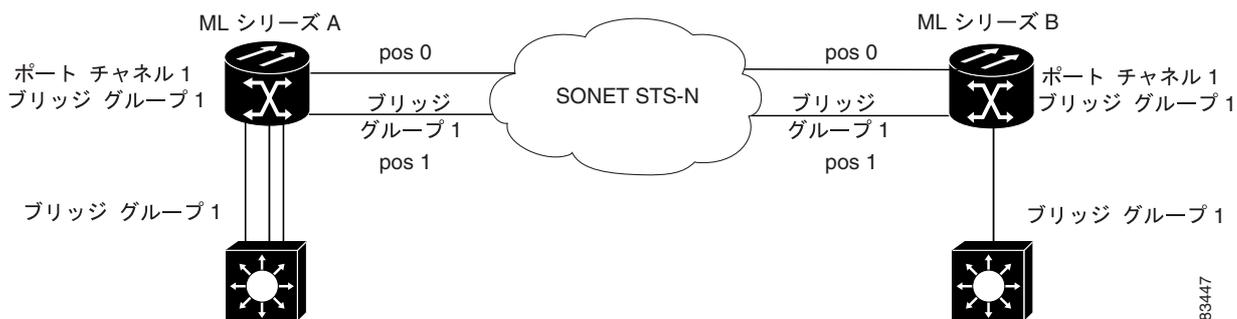
POS インターフェイスを POS チャンネルに割り当てるには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>interface pos</b> <i>number</i>	インターフェイス コンフィギュレーション モードを開始して、POS チャンネルに割り当てる POS インターフェイスを設定します。
ステップ 2	Router(config-if)# <b>channel-group</b> <i>channel-number</i>	POS インターフェイスを POS チャンネルに割り当てます。チャンネル番号は、POS チャンネル インターフェイスに割り当てたチャンネル番号と同じにする必要があります。
ステップ 3	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM に保存します。

## POS チャンネルの設定例

図 10-2 に、POS チャンネルの設定例を示します。関連するコードを 例 10-3 (スイッチ A) と 例 10-4 (スイッチ B) に示します。

図 10-2 POS チャンネルの例



例 10-3 スイッチ A の設定

```
bridge irb
bridge 1 protocol ieee
!
!
interface Port-channel1
no ip address
no keepalive
bridge-group 1
!
interface FastEthernet0
no ip address
bridge-group 1
!
interface POS0
no ip address
channel-group 1
crc 32
pos flag c2 1
!
interface POS1
no ip address
channel-group 1
crc 32
pos flag c2 1
```

**例 10-4 スイッチ B の設定**

```
bridge irb
bridge 1 protocol ieee
!
!
interface Port-channel1
 no ip address
 no keepalive
 bridge-group 1
!
interface FastEthernet0
 no ip address
 bridge-group 1
!
interface POS0
 no ip address
 channel-group 1
 crc 32
 pos flag c2 1
!
interface POS1
 no ip address
 channel-group 1
 crc 32
 pos flag c2 1
```

## EtherChannel または POS チャンネルでのカプセル化の概要

FEC、GEC、または POS 上でカプセル化を設定する場合は、必ずメンバー ポートではなく、ポート チャンネル インターフェイス上で IEEE802.1Q を設定します。ただし、デュプレックス モードなど、ポート チャンネルの特定の属性は、メンバー ポート レベルで設定する必要があります。また、メンバー インターフェイスには、プロトコル レベルの設定（IP アドレスやブリッジ グループの割り当てなど）を適用しないでください。すべてのプロトコル レベル設定は、ポート チャンネルまたはそのサブインターフェイス上で行う必要があります。IEEE 802.1Q カプセル化は、EtherChannel のパートナー システムでも設定する必要があります。

## EtherChannel または POS チャンネルでのカプセル化の設定

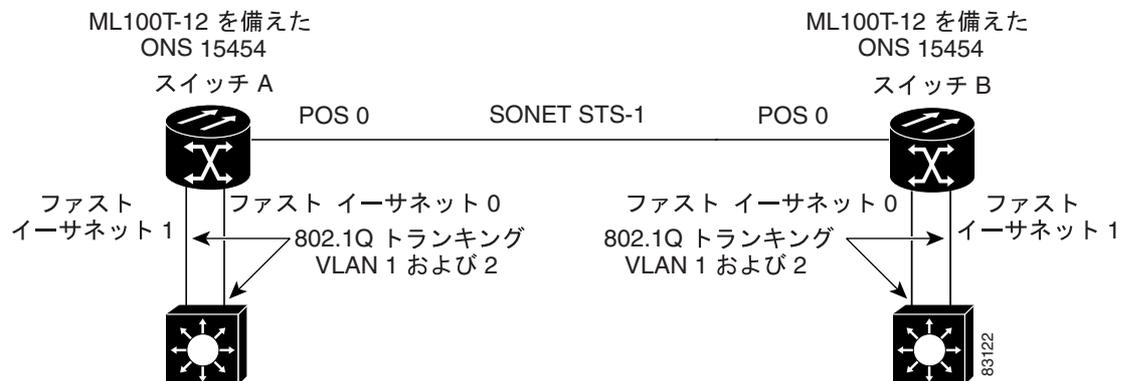
EtherChannel または POS チャンネルでカプセル化を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>interface port-channel</b> <i>channel-number.subinterface-number</i>	作成したポート チャンネル上でサブインターフェイスを設定します。
ステップ 2	Router(config-subif)# <b>encapsulation dot1q</b> <i>vlan-id</i>	IEEE 802.1Q カプセル化をサブインターフェイスに割り当てます。
ステップ 3	Router(config-subif)# <b>bridge-group</b> <i>bridge-group-number</i>	サブインターフェイスをブリッジ グループに割り当てます。
ステップ 4	Router(config-subif)# <b>end</b>	イネーブル EXEC モードに戻ります。
		 (注) 任意で、インターフェイス コンフィギュレーション モードで、要件を満たすためサポートされている他のインターフェイス コマンドをイネーブルにできます。
ステップ 5	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM に保存します。

## EtherChannel でのカプセル化の例

図 10-3 に、EtherChannel でのカプセル化の例を示します。関連するコードを例 10-5（スイッチ A）と例 10-6（スイッチ B）に示します。

図 10-3 EtherChannel でのカプセル化の例



この EtherChannel でのカプセル化の例では、EtherChannel での IEEE 802.1Q カプセル化もサポートしている 2 台のスイッチと相互運用するために、ML100T-12 カードを備えた 2 台の ONS 15454 (スイッチ A とスイッチ B) を設定する方法を示しています。この例を設定するには、次に示すスイッチ A およびスイッチ B 両方の設定を使用します。

#### 例 10-5 スイッチ A の設定

```
hostname Switch A
!
bridge irb
bridge 1 protocol ieee
bridge 2 protocol ieee
!
interface Port-channel1
 no ip address
 hold-queue 150 in
!
interface Port-channel1.1
 encapsulation dot1Q 1 native
 bridge-group 1
!
interface Port-channel1.2
 encapsulation dot1Q 2
 bridge-group 2

!
interface FastEthernet0
 no ip address
 channel-group 1
!
interface FastEthernet1
 no ip address
 channel-group 1
!
interface POS0
 no ip address
 crc 32
 pos flag c2 1
!
interface POS0.1
 encapsulation dot1Q 1 native
 bridge-group 1
!
interface POS0.2
 encapsulation dot1Q 2
 bridge-group 2
```

**例 10-6 スイッチ B の設定**

```
hostname Switch B
!
bridge irb
bridge 1 protocol ieee
bridge 2 protocol ieee
!
interface Port-channel1
  no ip address
  hold-queue 150 in
!
interface Port-channel1.1
  encapsulation dot1Q 1 native
  bridge-group 1
!
interface Port-channel1.2
  encapsulation dot1Q 2
  bridge-group 2
!
interface FastEthernet0
  no ip address
  channel-group 1
!
interface FastEthernet1
  no ip address
  channel-group 1
!
interface POS0
  no ip address
  crc 32
  pos flag c2 1
!
interface POS0.1
  encapsulation dot1Q 1 native
  bridge-group 1
!
interface POS0.2
  encapsulation dot1Q 2
  bridge-group 2
!
```

## EtherChannel と POS のモニタリングと確認

FEC、GEC、または POS を設定すると、`show interfaces port-channel` コマンドを使用してステータスをモニタリングできます。

### 例 10-7 show interfaces port-channel コマンド

```
Router# show int port-channel 1
Port-channell is up, line protocol is up
Hardware is FEChannel, address is 0005.9a39.6634 (bia 0000.0000.0000)
MTU 1500 bytes, BW 200000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Unknown duplex, Unknown Speed
ARP type: ARPA, ARP Timeout 04:00:00
    No. of active members in this channel: 2
        Member 0 : FastEthernet0 , Full-duplex, Auto Speed
        Member 1 : FastEthernet1 , Full-duplex, Auto Speed
Last input 00:00:01, output 00:00:23, output hang never
Last clearing of "show interface" counters never
Input queue: 0/150/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue :0/80 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
 820 packets input, 59968 bytes
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
 0 watchdog, 0 multicast
 0 input packets with dribble condition detected
32 packets output, 11264 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 output buffer failures, 0 output buffers swapped out.
```



# ネットワーク プロトコルの設定

この章では、ML シリーズ カードでサポートされている IP ルーティング プロトコルを設定する方法について説明します。ここでは、ネットワーク管理者がプロトコルを起動して実行するために必要な情報を提供します。ただし、各プロトコルの詳細な設定情報については説明しません。詳細については、『Cisco IOS IP and IP Routing Configuration Guide』および『Cisco IOS IP and IP Routing Command Reference』を参照してください。

この章の内容は次のとおりです。

- [IP ルーティング プロトコルの基本設定 \(p.11-2\)](#)
- [IP ルーティングの設定 \(p.11-5\)](#)
- [スタティック ルートのモニタリング \(p.11-34\)](#)
- [IP ネットワークのモニタリングとメンテナンス \(p.11-35\)](#)
- [IP マルチキャストルーティングの概要 \(p.11-36\)](#)
- [IP マルチキャストルーティングの設定 \(p.11-37\)](#)
- [IP マルチキャスト動作のモニタリングと確認 \(p.11-37\)](#)

## IP ルーティング プロトコルの基本設定

ML シリーズ カードでは、IP ルーティングがデフォルトでイネーブルになっています。

IP ルーティングの場合は、インターフェイスの設定に次の情報が必要です。

- IP アドレス
- IP サブネット マスク

また、次の操作が必要です。

- ルーティング プロトコルの選択
- アドバタイズする IP ネットワーク番号の割り当て

ML シリーズでは、以降で紹介するルーティング プロトコルがサポートされます。

IP ルーティング プロトコルをファスト イーサネット インターフェイス、ギガビット イーサネット インターフェイス、または Packet-over-SONET/SDH (POS) インターフェイスで実行できるように設定するには、設定中のプロトコルに応じて、次のいずれかの手順を実行します。

### RIP

Routing Information Protocol (RIP; ルーティング情報プロトコル) を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>router rip</b>	ルータ コンフィギュレーション モードを開始し、RIP をルーティング プロトコルとして定義して、RIP ルーティング プロセスを開始します。
ステップ 2	Router(config-router)# <b>network net-number</b>	サブネット番号や個別のアドレスではなく、Internet Network Information Center(InterNIC; インターネット ネットワーク情報センター)のネットワーク番号に基づいて、直接接続するネットワークを指定します。ルーティング プロセスによってインターフェイスと適切なアドレスが関連付けられ、指定したネットワークでパケットの処理が開始されます。
ステップ 3	Router(config-router)# <b>exit</b>	グローバル コンフィギュレーション モードに戻ります。

## EIGRPEIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP) を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>router eigrp</b> <i>autonomous-system-number</i>	EIGRP を IP ルーティング プロトコルとして定義します。  この Autonomous System (AS; 自律システム) 番号は、ML シリーズ カードが属する AS を表します。
ステップ 2	Router(config-router)# <b>network</b> <i>net-number</i>	EIGRP を実行する直接接続されたネットワークを定義します。  このネットワーク番号は、ML シリーズ カードでアダプタイズされるネットワークの番号です。
ステップ 3	Router(config-router)# <b>exit</b>	グローバル コンフィギュレーション モードに戻ります。

## OSPF

Open Shortest Path First (OSPF) プロトコルを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>router ospf</b> <i>process-ID</i>	OSPF を IP ルーティング プロトコルとして定義します。  プロセス ID は、一意の OSPF ルータ プロセスを識別します。この番号は、ML シリーズ カードの内部のみで使用されます。このプロセス ID と他のルータのプロセス ID を一致させる必要はありません。
ステップ 2	Router(config-router)# <b>network</b> <i>net-address wildcard-mask area area-ID</i>	特定のエリアにインターフェイスを割り当てます。 <ul style="list-style-type: none"> <li>net-address: 直接接続されたネットワークまたはサブネットのアドレス</li> <li>wildcard-mask: 指定されたアドレスとインターフェイスのアドレッシングを比較して、OSPF でこのインターフェイスを使用するかどうかを判断するための逆マスク</li> <li>area: インターフェイスが属するエリアを特定するパラメータ</li> <li>area-ID: ネットワーク アドレスに関連付けられたエリアを指定</li> </ul>
ステップ 3	Router(config-router)# <b>end</b>	イネーブル EXEC モードに戻ります。

## BGP

Border Gateway Protocol (BGP; ボーダー ゲートウェイ プロトコル) を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>router bgp</b> <i>autonomous-system-number</i>	BGP を IP ルーティング プロトコルとして定義します。  この AS 番号は、ML シリーズ カードが属する AS を表します。
ステップ 2	Router(config-router) # <b>network</b> <i>net-number</i>	BGP を実行する直接接続されたネットワークを定義します。  このネットワーク番号は、ML シリーズ カードでアダプタイズされるネットワークの番号です。
ステップ 3	Router(config-router)# <b>exit</b>	グローバル コンフィギュレーション モードに戻ります。

## IP ルーティングのイネーブル化

IP ルーティングをイネーブルにするには、イネーブル EXEC モードで次の手順を実行します。



(注) デフォルトでは、IP ルーティングがすでにイネーブルに設定されています。

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b>	グローバル 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	Router(config)# <b>ip routing</b>	IP ルーティングをイネーブルにします (デフォルト)。
ステップ 3	Router(config)# <b>router</b> <i>ip-routing-protocol</i>	IP ルーティング プロトコルを指定します。このステップでは、他のコマンドも実行する場合があります (network [RIP] ルータ設定コマンドを使用して、ルーティングするネットワークを指定する場合など)。特定のプロトコルの詳細については、この章で後述する情報と『Cisco IOS IP and IP Routing Configuration Guide』を参照してください。
ステップ 4	Router(config-router)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	Router(config)# <b>show running-config</b>	エントリを確認します。
ステップ 6	Router(config)# <b>copy running-config</b> <b>startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

ルーティングをディセーブルにするには、no ip routing グローバル コンフィギュレーション コマンド (例 11-1) を使用します。

**例 11-1 ルーティング プロトコルとして RIP を使用した IP ルーティングのイネーブル化**

```
Router# configure terminal
Router(config)# ip routing
Router(config)# router rip
Router(config-router)# network 10.0.0.0
Router(config-router)# end
```

## IP ルーティングの設定

この説明に従って、選択したルーティング プロトコルのパラメータを設定できます。

- [RIP の設定 \(p.11-5\)](#)
- [OSPF の設定 \(p.11-10\)](#)
- [EIGRP の設定 \(p.11-21\)](#)
- [BGP の設定 \(p.11-29\)](#)
- [IS-IS の設定 \(p.11-31\)](#)
- [スタティック ルートの設定 \(p.11-33\)](#)

## RIP の設定

RIP は、小規模な同種ネットワーク向けに作成された Interior Gateway Protocol (IGP; 内部ゲートウェイ プロトコル) です。また、RIP は、ブロードキャスト UDP データ パケットを使用し、ルーティング情報を交換するディスタンス ベクタ ルーティング プロトコルです。このプロトコルは RFC 1058 で規定されています。RIP の詳細については、Cisco Press 発行の『*IP Routing Fundamentals*』を参照してください。

スイッチは、RIP を使用して、ルーティングの更新情報を 30 秒ごとに送信 (アドバタイズ) します。ルータが他のルータから 180 秒以上更新情報を受信しないと、その発信側ルータから配信されるルートを使用不可とマーキングします。さらに 240 秒経過しても、ルータが他のルータから更新情報を受信できない場合は、受信側ルータがその発信側ルータに関連するルーティング テーブルのエントリすべてを削除します。

RIP では、ホップ カウントを使用して、各ルートの値を評価します。ホップ カウントは、1 つのルートで経由するルータの数を表します。直接接続したネットワークのホップ カウントは、0 (ゼロ) です。ホップ カウントが 16 のネットワークは、到達不能であることを表します。RIP のホップ カウントの範囲は 0 ~ 15 と狭いので、RIP は大規模ネットワークに適していません。

ルータにデフォルトのネットワーク パスが設定されている場合は、ルータを擬似ネットワーク 0.0.0.0 にリンクするルートが RIP でアドバタイズされます。0.0.0.0 ネットワークは存在しませんが、RIP では、デフォルトのルーティング機能を実装するためにネットワークとして処理されます。RIP がデフォルト ネットワークを学習している場合、またはルータが最終手段としてゲートウェイを用意しており、RIP がデフォルトのメトリックで設定されている場合は、スイッチは、デフォルトのネットワークをアドバタイズします。RIP は、指定されたネットワークのインターフェイスに更新情報を送信します。インターフェイスのネットワークを指定していない場合は、RIP の更新情報がアドバタイズされません。

表 11-1 に、RIP のデフォルト設定を示します。

表 11-1 RIP のデフォルト設定

機能	デフォルト設定
自動サマリー	イネーブル
デフォルト情報発信	ディセーブル
デフォルトのメトリック	組み込み：自動メトリック変換
IP RIP 認証キー チェーン	認証なし 認証モード：クリア テキスト
IP RIP 受信バージョン	version ルータ コンフィギュレーション コマンドで指定
IP RIP 送信バージョン	version ルータ コンフィギュレーション コマンドで指定
IP RIP トリガー	version ルータ コンフィギュレーション コマンドで指定
IP スプリット ホライズン	メディアによって異なる
ネイバ	未定義
ネットワーク	未指定
オフセット リスト	ディセーブル
出力遅延	0 ミリ秒
タイマーの基本値	更新：30 秒 無効：180 秒 ホールドダウン：180 秒 フラッシュ：240 秒
更新情報発信元の確認	イネーブル
バージョン	RIP バージョン 1 とバージョン 2 のパケットを受信 バージョン 1 のパケットを送信

RIP を設定するには、ネットワークで RIP ルーティングをイネーブルにし、他のパラメータを任意に設定します。

RIP をイネーブルにして設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b>	グローバル 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	Router(config)# <b>ip routing</b>	IP ルーティングをイネーブルにします (IP ルーティングがディセーブルになっている場合にのみ必須)。
ステップ 3	Router(config)# <b>router rip</b>	RIP ルーティング プロセスをイネーブルにし、ルータ 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	Router(config-router)# <b>network network-number</b>	ネットワークを RIP ルーティング プロセスに関連付けます。複数の <b>network</b> コマンドを指定できます。RIP ルーティング更新は、指定したネットワークだけでインターフェイス経由で送受信されます。
ステップ 5	Router(config-router)# <b>neighbor ip-address</b>	(任意) ルーティング情報を交換する近接ルータを定義します。このステップでは、ブロードキャスト対象外のネットワークに RIP (通常はブロードキャスト プロトコル) からのルーティング更新を送信できます。

	コマンドの説明	目的
ステップ 6	Router(config-router)# <b>offset list</b> {[access-list-number   name]} {in out} offset [type-number]	(任意)オフセットリストをルーティングメトリックに適用し、RIP 経由で学習したルートに着信と発信のメトリックを増やします。オフセット リストをアクセス リストやインターフェイスで制限できます。
ステップ 7	Router(config-router)# <b>timers basic update</b> invalid holddown flush	(任意)ルーティング プロトコル タイマーを調整します。すべてのタイマーの有効値の範囲は、0 ~ 4294967295 秒です。 <ul style="list-style-type: none"> <li>• update ルーティング更新を送信する間隔 (秒単位)。デフォルトは 30 秒です。</li> <li>• invalid ルートが無効だと宣言されるまでの時間 (秒単位)。デフォルトは 180 秒です。</li> <li>• holddown ルーティングテーブルからルートを削除するまでに経過する時間 (秒単位)。デフォルトは 180 秒です。</li> <li>• flush ルーティングの更新が延期される時間 (秒単位)。デフォルトは 240 秒です。</li> </ul>
ステップ 8	Router(config-router)# <b>version</b> {1   2}	(任意)スイッチを設定し、RIP バージョン 1 または RIP バージョン 2 のパケットだけを送受信するようにします。デフォルトでは、スイッチは、バージョン 1 とバージョン 2 を受信しますが、送信するのはバージョン 1 のみです。 インターフェイス コマンド <b>ip rip {send   receive} version {1   2   1 2}</b> を使用して、インターフェイスでの送受信に使用するバージョンを制御することもできます。
ステップ 9	Router(config-router)# <b>no auto summary</b>	(任意)自動サマリーをディセーブルにします。デフォルトでは、スイッチは、全クラスのネットワーク境界を通過するときにサブプレフィックスをサマリーします。このサマリーをディセーブルにして (RIP バージョン 2 のみ)、サブネットとホストのルーティング情報を全クラスのネットワーク境界にアダバタイズします。
ステップ 10	Router(config-router)# <b>no validate-update-source</b>	(任意)着信する RIP ルーティング更新の送信元 IP アドレスの検証をディセーブルにします。デフォルトでは、スイッチは、着信 RIP ルーティング更新の送信元 IP アドレスを検証し、送信元アドレスが無効な場合にその更新情報を廃棄します。通常は、この機能をイネーブルにすることを推奨します。ただし、ネットワーク外のルータがあり、その更新情報を受信する場合は、このコマンドを使用できます。
ステップ 11	Router(config-router)# <b>output-delay</b> delay	(任意)送信する RIP 更新パケット間に遅延を追加します。デフォルトでは、複数のパケットを使用する RIP 更新内のパケット間には遅延が追加されていません。パケットをより低速な装置に送信する場合、8 ~ 50 ミリ秒の範囲でパケット間に遅延を追加できます。
ステップ 12	Router(config-router)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 13	Router# <b>show ip protocols</b>	エントリを確認します。
ステップ 14	Router# <b>copy running-config startup-config</b>	(任意)コンフィギュレーション ファイルにエントリを保存します。

RIP ルーティング プロセスをディセーブルにするには、`no router rip` グローバル コンフィギュレーション コマンドを使用します。

アクティブなルーティング プロトコル プロセスのパラメータと最新状態を表示するには、`show ip protocols` イネーブル EXEC コマンド (例 11-2) を使用します。

#### 例 11-2 show ip protocols コマンドの出力 (RIP プロセスの表示)

```
Router# show ip protocols
Routing Protocol is "rip"
  Sending updates every 30 seconds, next due in 15 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: rip
  Default version control: send version 1, receive any version
  Interface          Send Recv  Triggered RIP  Key-chain
  FastEthernet0      1      1 2
  POS0                1      1 2
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    192.168.2.0
    192.168.3.0
  Routing Information Sources:
    Gateway          Distance    Last Update
    192.168.2.1      120        00:00:23
  Distance: (default is 120)
```

RIP データベース内のサマリー アドレス エントリを表示するには、`show ip rip database` イネーブル EXEC コマンドを使用します (例 11-3)。

#### 例 11-3 show ip rip database コマンドの出力

```
Router# show ip rip database
192.168.1.0/24    auto-summary
192.168.1.0/24
  [1] via 192.168.2.1, 00:00:24, POS0
192.168.2.0/24    auto-summary
192.168.2.0/24    directly connected, POS0
192.168.3.0/24    auto-summary
192.168.3.0/24    directly connected, FastEthernet0
```

## RIP 認証

RIP バージョン 1 では、認証がサポートされません。RIP バージョン 2 のパケットを送受信するには、インターフェイスで RIP 認証をイネーブルにできます。キー チェーンは、インターフェイスで使用できるキー セットを表します。キーチェーンを設定していない場合は、認証が実行されません。デフォルトでも同様です。

このスイッチでは、RIP 認証がイネーブルのインターフェイスで 2 つの認証モード (平文とメッセージダイジェスト キー [MD5]) がサポートされています。デフォルトは、平文です。

インターフェイスに RIP 認証を設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b>	グローバル 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	Router(config)# <b>interface interface-id</b>	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、設定するインターフェイスを指定します。
ステップ 3	Router(config-if)# <b>ip rip authentication key-chain name-of-chain</b>	RIP 認証をイネーブルにします。
ステップ 4	Router(config-if)# <b>ip rip authentication mode {text   md5}</b>	平文による認証 (デフォルト) または MD5 ダイジェスト認証を使用するようにインターフェイスを設定します。
ステップ 5	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 6	Router# <b>show running-config interface [interface-id]</b>	エントリを確認します。
ステップ 7	Router# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

平文認証に戻すには、**no ip rip authentication mode** 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。認証を実行しない場合は、**no ip rip authentication key-chain** 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。

## サマリー アドレスとスプリット ホライズン

ブロードキャスト型 IP ネットワークに接続され、ディスタンス ベクタ ルーティング プロトコルを使用するルータは、通常、スプリット ホライズン メカニズムを使用してルーティンググループの発生を抑えます。スプリット ホライズンでは、ルータがルート情報をアドバタイズするのを、情報発信側のインターフェイスで防ぎます。この機能によって、通常 (特にリンクに障害がある場合) 複数のルータ間で通信が最適化されます。



(注) スプリット ホライズンをディセーブルにしないとアプリケーションが正しくルートをアドバタイズできない場合を除き、通常は、スプリット ホライズンをイネーブルにすることを推奨します。

RIP を実行するインターフェイスを設定し、ダイヤルアップクライアント用ネットワーク アクセスサーバ上のサマリー ローカル IP アドレス プールをアドバタイズするには、**ip summary-address rip** 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。

インターフェイスを設定し、サマリー ローカル IP アドレス プールをアドバタイズして、このインターフェイスでスプリット ホライズンをディセーブルにするには、イネーブル EXEC モードで次のステップを実行します。

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b>	グローバル 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	Router(config)# <b>interface interface-id</b>	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、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	Router(config-if)# <b>ip address ip-address subnet-mask</b>	IP アドレスと IP サブネットを設定します。

	コマンドの説明	目的
ステップ 4	Router(config-if)# <b>ip summary-address rip</b> ip-address ip-network-mask	IP アドレスのサマリーと IP ネットワーク マスクを設定します。
ステップ 5	Router(config-if)# <b>no ip split horizon</b>	インターフェイスでのスプリット ホライズンをディセーブルにします。
ステップ 6	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 7	Router# <b>show ip interface interface-id</b>	エントリを確認します。
ステップ 8	Router# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

IP サマリーをディセーブルにするには、**no ip summary-address rip** ルータ設定コマンドを使用します。



(注)

スプリット ホライズンをイネーブルにすると、自動サマリーもインターフェイスでのサマリー アドレス (**ip summary-address rip** ルータ コンフィギュレーション コマンドで設定したサマリー アドレス) もアドバタイズされません。

## OSPF の設定

ここでは、OSPF プロトコルの設定方法を簡単に説明します。OSPF のコマンドの詳細については、『Cisco IOS IP and IP Routing Command Reference』の「OSPF Commands」の章を参照してください。

OSPF は、IP ネットワーク用に特別に設計された IGP であり、外部で派生したルーティング情報の IP サブネット化とタギングをサポートします。OSPF では、パケット認証が可能で、パケットの送受信時に IP マルチキャストを使用します。シスコ製品では、RFC 1253 の OSPF MIB がサポートされています。

シスコ製品は、次の機能を持つ OSPF バージョン 2 の規格に準拠しています。

- スタブ エリア   スタブ エリアの定義がサポートされます。
- ルート再配布   IP ルーティング プロトコルが学習したルートを他の IP ルーティング プロトコルに再配布できます。これは、ドメイン内では、EIGRP や RIP などのプロトコルで学習したルートを OSPF がインポートしたり、エクスポートしたりできることを表します。
- 認証   エリア内の近接ルータで平文と MD5 による認証がサポートされます。
- ルーティング インターフェイス パラメータ   サポートされている設定可能なパラメータには、インターフェイス出力コスト、再送間隔、インターフェイス送信遅延、ルータのプライオリティ、ルータのデッドおよび Hello インターバル、認証キーなどがあります。
- 仮想リンク   仮想リンクがサポートされます。
- Not-So-Stubby-Area (NSSA; 準スタブ エリア)   RFC 1587

OSPF では、通常、多数の内部ルータ、複数のエリアに接続された Area Border Router (ABR; エリア境界ルータ)、および Autonomous System Boundary Router (ASBR; 自律システム境界ルータ) の間で調整を行う必要があります。最小設定では、すべてのデフォルトパラメータ値、認証設定 (認証なし)、およびエリアに割り当てられたインターフェイスを使用します。使用中の環境をカスタマイズする場合は、すべてのルータで設定を調整する必要があります。

表 11-2 にデフォルトの OSPF 設定を示します。

表 11-2 OSPF のデフォルト設定

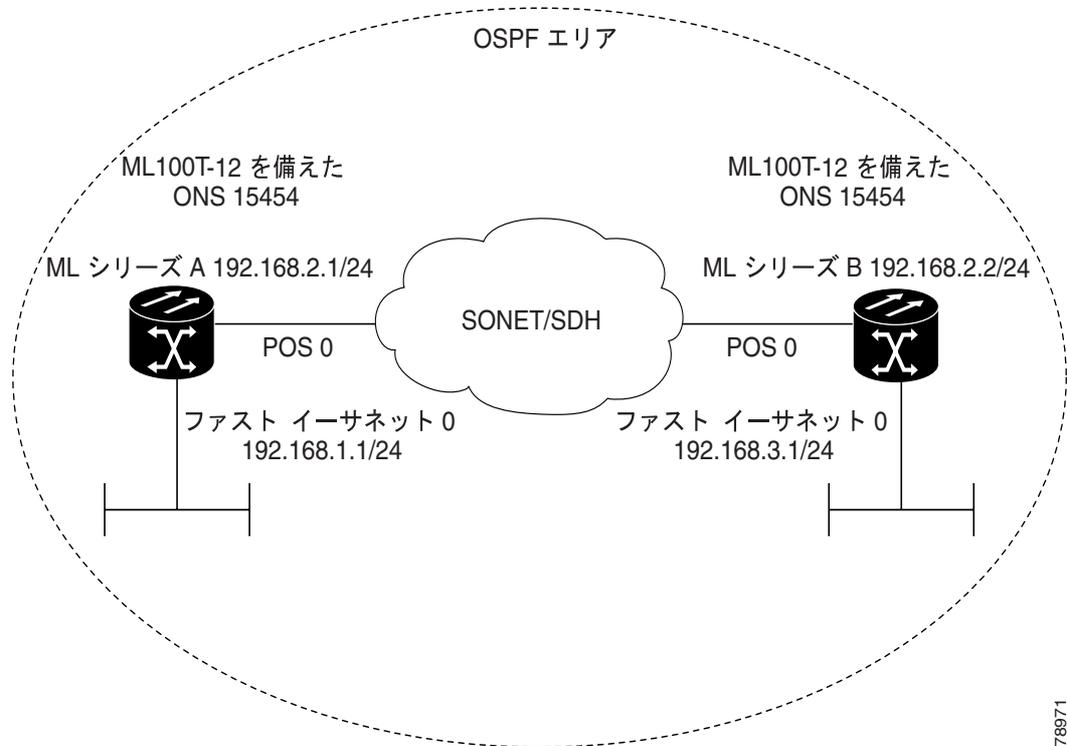
機能	デフォルト設定
インターフェイスのパラメータ	コスト：デフォルト値は未設定 再送間隔：5 秒 送信遅延：1 秒 プライオリティ：1 Hello インターバル：10 秒 デッド インターバル：Hello インターバルの 4 倍 認証なし パスワード未指定 MD5 認証ディセーブル
エリア	認証タイプ：0 ( 認証なし ) デフォルトのコスト：1 範囲：ディセーブル スタブ：スタブ エリア未定義 NSSA：NSSA エリア未定義
自動コスト	100 Mbps
デフォルト情報発信元	ディセーブル。イネーブルにした場合、デフォルトのメトリック設定は 10 で、外部ルート タイプのデフォルト値は Type 2 です。
デフォルトのメトリック	組み込み、自動メトリック変換、各ルーティング プロトコルに適切なメトリック
長距離 OSPF	dist1 ( すべてのルートが 1 エリア内に存在 )：110 dist2 ( 2 つのエリア間のすべてのルート )：110 dist3 ( 他のルーティング ドメインからのルート )：110
OSPF データベース フィルタ	ディセーブル。すべての発信 Link-State Advertisements ( LSA; リンクステート アドバタイズメント ) がインターフェイスにフラッディングされます。
IP OSPF 名前検索	ディセーブル
隣接関係変更ログ	イネーブル
ネイバ	未指定
ネイバ データベース フィルタ	ディセーブル。すべての発信 LSA がネイバにフラッディングされます。
ネットワーク エリア	ディセーブル
ルータ ID	OSPF ルーティング プロセス未定義
サマリー アドレス	ディセーブル
タイマー LSA グループ ペーシング	240 秒
タイマー Shortest Path First ( SPF; 最短パス優先 )	SPF 遅延：5 秒 SPF 待機時間：10 秒

表 11-2 OSPF のデフォルト設定 (続き)

機能	デフォルト設定
仮想リンク	エリア ID または ルータ ID は未定義 Hello インターバル : 10 秒 再送間隔 : 5 秒 送信遅延 : 1 秒 デッド インターバル : 40 秒 認証キー : キー未定義 MD5 : キー未定義

図 11-1 に OSPF を使用した IP ルーティング プロトコルの例を示します。

図 11-1 OSPF を使用した IP ルーティング プロトコルの例



78971

OSPF をイネーブルにするには、OSPF ルーティング プロセスを作成し、このルーティング プロセスに関連付ける IP アドレスの範囲を指定して、その範囲に関連付けるエリア ID を割り当てる必要があります。

OSPF をイネーブルにするには、イネーブル EXEC モードを開始し、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b>	グローバル 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	Router(config)# <b>router ospf process-id</b>	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。プロセス ID は、ローカルに割り当てられ、内部的に使用される識別パラメータです。この ID には、どの正の整数でも指定できます。各 OSPF ルーティング プロセスには、一意の値を指定します。
ステップ 3	Router(config)# <b>network address wildcard-mask area area-id</b>	OSPF を実行するインターフェイスと、そのインターフェイスのエリア ID を定義します。1 つのコマンドで 1 つ以上のインターフェイスを特定の OSPF エリアに関連付けるには、ワイルドカード マスクを使用します。エリア ID は、10 進値または IP アドレスです。
ステップ 4	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	Router# <b>show ip protocols</b>	エントリを確認します。
ステップ 6	Router# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

OSPF ルーティング プロセスを終了するには、**no router ospf process-id** グローバル コンフィギュレーション コマンドを使用します。

例 11-4 に OSPF ルーティング プロセスの設定例を示します。この例では、プロセス番号 1 を割り当てます。例 11-5 に、OSPF プロセス ID の確認に使用する、コマンド出力を示します。

#### 例 11-4 OSPF ルーティング プロセスの設定

```
Router(config)# router ospf 1
Router(config-router)# network 192.168.1.0 0.0.0.255 area 0
```

#### 例 11-5 show ip protocols イネーブル EXEC コマンドの出力

```
Router# show ip protocols
Routing Protocol is "ospf 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Router ID 192.168.3.1
  Number of areas in this router is 1. 1 normal 0 stub 0 nssa
  Maximum path: 4
  Routing for Networks:
    192.168.2.0 0.0.0.255 area 0
    192.168.3.0 0.0.0.255 area 0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.3.1          110          00:03:34
    192.168.2.1          110          00:03:34
  Distance: (default is 110)
```

## OSPF インターフェイス パラメータ

インターフェイスに固有の OSPF パラメータを変更するには、`ip ospf` 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。これらのパラメータを変更する必要はありませんが、一部のインターフェイス パラメータ (Hello インターバル、デッド インターバル、および認証キー) は、接続されたネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを変更する場合は、ネットワーク内のすべてのルータの値に互換性があることを確認してください。



(注) `ip ospf` インターフェイス コンフィギュレーション コマンドは、すべて任意です。

OSPF インターフェイス パラメータを変更するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <code>configure terminal</code>	グローバル 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	Router(config)# <code>interface interface-id</code>	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、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	Router(config-if)# <code>ip ospf cost</code>	(任意) インターフェイスでのパケット送信コストを明示的に指定します。
ステップ 4	Router(config-if)# <code>ip ospf retransmit-interval seconds</code>	(任意) リンクステート アドパタイズメントの送信間隔を秒単位で指定します。範囲は、1 ~ 65535 秒です。デフォルト値は、5 秒です。
ステップ 5	Router(config-if)# <code>ip ospf transmit-delay seconds</code>	(任意) リンク ステート 更新パケットを送信するまでの待機時間を設定します。範囲は、1 ~ 65535 秒です。デフォルトは 1 秒です。
ステップ 6	Router(config-if)# <code>ip ospf priority number</code>	(任意) ネットワークの OSPF 指定ルータを決定するためのプライオリティを設定します。範囲は 0 ~ 255 です。デフォルトは 1 です。
ステップ 7	Router(config-if)# <code>ip ospf hello-interval seconds</code>	(任意) OSPF インターフェイスで Hello パケットを送信する間隔を秒単位で設定します。この値は、1 つのネットワーク上にあるすべてのノードで統一する必要があります。範囲は、1 ~ 65535 秒です。デフォルトは 10 秒です。
ステップ 8	Router(config-if)# <code>ip ospf dead-interval seconds</code>	(任意) 装置の最後の Hello パケットが検出されてから OSPF ルータが停止していることをネイバが宣言するまでの時間を秒単位で設定します。この値は、1 つのネットワーク上にあるすべてのノードで統一する必要があります。範囲は、1 ~ 65535 秒です。デフォルトは、Hello インターバルの 4 倍です。
ステップ 9	Router(config-if)# <code>ip ospf authentication-key key</code>	(任意) 近接 OSPF ルータが使用するパスワードを割り当てます。このパスワードには、キーボードで入力できる文字列を 8 バイトの長さまで指定できます。OSPF 情報を交換するために、同一ネットワーク上のすべての近接ルータに同じパスワードを指定する必要があります。

	コマンドの説明	目的
ステップ 10	Router(config-if)# <b>ip ospf message-digest-key keyid md5 key</b>	(任意) 認証をイネーブルにします。 <ul style="list-style-type: none"> <li>keyid 1 ~ 255 の識別子</li> <li>key 16 バイトまでの英数字パスワード</li> </ul>
ステップ 11	Router(config-if)# <b>ip ospf database-filter all out</b>	(任意) OSPF LSA パケットがインターフェイスにフラッディングされるのを防ぎます。デフォルトでは、OSPF が同じエリア内のすべてのインターフェイス (LSA が到達済みのインターフェイスを除く) に新しい LSA をフラッディングします。
ステップ 12	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 13	Router# <b>show ip ospf interface [interface-name]</b>	OSPF 関連のインターフェイス情報を表示します。
ステップ 14	Router# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

設定したパラメータ値を削除する場合、またはデフォルト値に戻す場合は、これらのコマンドの **no** 形式を使用します。例 11-6 に **show ip ospf interface** イネーブル EXEC コマンドの出力を示します。

#### 例 11-6 show ip ospf interface イネーブル EXEC コマンドの出力

```
Router# show ip ospf interface
FastEthernet0 is up, line protocol is up
  Internet Address 192.168.3.1/24, Area 0
  Process ID 1, Router ID 192.168.3.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.3.1, Interface address 192.168.3.1
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 0, maximum is 0
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
POS0 is up, line protocol is up
  Internet Address 192.168.2.2/24, Area 0
  Process ID 1, Router ID 192.168.3.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.3.1, Interface address 192.168.2.2
  Backup Designated router (ID) 192.168.2.1, Interface address 192.168.2.1
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 2, maximum is 2
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.2.1 (Backup Designated Router)
  Suppress hello for 0 neighbor(s)
```

## OSPF エリア パラメータ

任意で複数の OSPF エリア パラメータを設定できます。これらのパラメータには、エリア、スタブ エリア、および NSSA への不正アクセスを防ぐためにパスワードベースで保護する認証があります。スタブ エリアは、外部ルート情報が送信されないエリアです。代わりに、ABR によって AS 外の宛先について、スタブ エリアへのデフォルトの外部ルートが作成されます。NSSA では、すべての LSA がコアからエリアにフラディングされるわけではありませんが、再配布により AS の外部ルートをエリア内にインポートできます。

経路集約は、アドバタイズされたアドレスを 1 つのサマリー ルートに統合し、他のエリアでアドバタイズする機能です。ネットワーク番号が連続している場合は、`area range` ルータ コンフィギュレーション コマンドを使用して、ABR を設定し、その範囲内のすべてのネットワークをカバーするサマリー ルートをアドバタイズできます。



(注) OSPF の `area` ルータ設定コマンドは、すべてオプションです。

エリア パラメータを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <code>configure terminal</code>	グローバル 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	Router(config)# <code>router ospf process-id</code>	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	Router(config)# <code>area area-id authentication</code>	(任意) 指定したエリアへの不正アクセスに対してパスワードベースの保護を可能にします。この ID は、10 進値または IP アドレスです。
ステップ 4	Router(config)# <code>area area-id authentication message-digest</code>	(任意) このエリアで MD5 認証をイネーブルにします。
ステップ 5	Router(config)# <code>area area-id stub [no-summary]</code>	(任意) エリアをスタブ エリアとして定義します。 <code>no-summary</code> キーワードを指定すると、ABR がスタブ エリア内にサマリー リンク アドバタイズメントを送信するのを防ぐことができます。
ステップ 6	Router(config)# <code>area area-id nssa {no-redistribution   default-information-originate   no-summary}</code>	(任意) エリアを NSSA として定義します。同一エリア内のすべてのルータは、このエリアが NSSA であることを認識している必要があります。次のいずれかのキーワードを指定します。 <ul style="list-style-type: none"> <li>• <code>no-redistribution</code> ルータが NSSA ABR であり、<code>redistribute</code> コマンドを使用して NSSA 以外の通常のエリア内にルートをインポートする場合に選択します。</li> <li>• <code>default-information-originate</code> ABR で NSSA 内にタイプ 7 の LSA をインポートする場合に選択します。</li> <li>• <code>no-summary</code> NSSA 内にサマリー LSA を送信しない場合に選択します。</li> </ul>
ステップ 7	Router(config)# <code>area area-id range address-mask</code>	(任意) アドレスの範囲を指定し、その範囲に 1 つのルートをアドバタイズします。このコマンドは、ABR だけで使用します。

	コマンドの説明	目的
ステップ 8	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 9	Router# <b>show ip ospf</b> [process-id]	OSPF ルーティング プロセスの全般情報を表示するか、または、指定したプロセス ID について情報を表示して確認します。
ステップ 10	Router# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

設定したパラメータ値を削除する場合、またはデフォルト値に戻す場合は、これらのコマンドの **no** 形式を使用します。例 11-7 に、**show ip ospf database** および **show ip ospf** イネーブル EXEC コマンドの出力を示します。

#### 例 11-7 show ip ospf database および show ip ospf イネーブル EXEC コマンドの出力

```
Router# show ip ospf database

      OSPF Router with ID (192.168.3.1) (Process ID 1)

          Router Link States (Area 0)

Link ID        ADV Router    Age           Seq#           Checksum Link count
192.168.2.1    192.168.2.1  428          0x80000003    0x004AB8  2
192.168.3.1    192.168.3.1  428          0x80000003    0x006499  2

          Net Link States (Area 0)

Link ID        ADV Router    Age           Seq#           Checksum
192.168.2.2    192.168.3.1  428          0x80000001    0x00A4E0

Router# show ip ospf
Routing Process "ospf 1" with ID 192.168.3.1
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 2
    Area has no authentication
    SPF algorithm executed 4 times
    Area ranges are
    Number of LSA 3. Checksum Sum 0x015431
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0
```

## OSPF のその他の動作パラメータ

ルータ コンフィギュレーション モードでは、他の OSPF パラメータも任意で設定できます。

- **経路集約** 他のプロトコルからのルートを再配布する場合は、各ルートが外部 LSA 内で個別にアドバタイズされます。OSPF リンク状態データベースのサイズを減らすには、`summary-address` ルータ コンフィギュレーション コマンドを使用して、指定したネットワークアドレスとマスクに含まれるすべての再配布ルートについて 1 つのルータをアドバタイズします。
- **仮想リンク** OSPF では、すべてのエリアをバックボーン エリアに接続する必要があります。1 つの仮想リンクのエンドポイントとして 2 つの ABR を設定することにより、バックボーンの導通性が損なわれた場合に仮想リンクを確立できます。設定情報には、他の仮想エンドポイント (他の ABR) の ID、2 つのルータが共通して把握するバックボーン以外のリンク (中継エリア) などが含まれます。スタブ エリア経由で仮想リンクを設定することはできません。
- **デフォルトルート** OSPF ルーティング ドメイン内にルートの再配布を個別に設定すると、そのルートが自動的に ASBR になります。ASBR によって OSPF ルーティング ドメイン内にデフォルト ルートを強制的に作成できます。
- **OSPF のすべての show イネーブル EXEC コマンド表示** Domain Name Server (DNS; ドメインネーム サーバ) 名を使用すると、ルータ ID またはネイバ ID でルータを表示する場合よりも、ルータを識別しやすくなります。
- **デフォルトのメトリック** OSPF は、インターフェイスの帯域幅に基づいてそのインターフェイスの OSPF メトリックを計算します。このメトリックは、帯域幅で除算された *ref-bw* として計算されます。*ref* のデフォルト値は 10 で、帯域幅 (*bw*) は、`bandwidth` インターフェイス コンフィギュレーション コマンドで判別する値です。高帯域幅を持つ複数のリンクについては、より大きい数値を指定して、これらのリンクのコストを区別できます。
- **管理距離** ルーティング情報の送信元の信頼性について 0 ~ 255 の整数で評価します。値が大きいほど、信頼性が低いことを表します。管理距離が 255 の場合は、ルーティング情報の送信元がまったく信頼できず、無視する必要があります。OSPF では、3 種類の管理距離 (エリア内のルート [intra-area]、他のエリアへのルート [interarea]、および再配布によって学習された他のルーティング ドメインからのルート [external]) を使用します。管理距離の値は、どれにでも変更できます。
- **受動インターフェイス** イーサネット上の 2 つの装置の間にあるインターフェイスは、1 つのネットワーク セグメントだけを表すので、OSPF が送信側インターフェイスに対して Hello パケットを送信するのを防ぐには、送信側の装置を受動インターフェイスとして設定する必要があります。両方の装置は、受信インターフェイス用の Hello パケットで互いを識別できます。
- **ルート計算タイマー** OSPF がトポロジ変更を受信してから SPF 計算を開始するまでの遅延時間を設定できます。2 つの SPF 計算の間の待機時間も設定できます。
- **ネイバ変更のログ** OSPF ネイバの状態が変化した場合に Syslog メッセージを送信するようにルータを設定できます。この場合、ルータの変化を高度なビューで表示できます。

これらの OSPF パラメータを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <code>configure terminal</code>	グローバル 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	Router(config)# <code>router ospf process-id</code>	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	Router(config)# <code>summary-address address-mask</code>	(任意) 1 つのサマリー ルートだけをアドバタイズするように、再配布ルートのアドレスと IP サブネット マスクを指定します。

	コマンドの説明	目的
ステップ 4	Router(config)# <b>area area-id virtual-link</b> router-id [hello-interval seconds] [retransmit-interval seconds] [trans] [[authentication-key key]   [message-digest-key key-id md5 key]]	(任意) 仮想リンクを確立し、そのパラメータを設定します。パラメータの定義については、「 <a href="#">OSPF インターフェイス パラメータ</a> 」(p.11-14)を参照してください。仮想リンクのデフォルトについては、 <a href="#">表 11-2</a> を参照してください。
ステップ 5	Router(config)# <b>default-information originate</b> [always] [metric metric-value] [metric-type type-value] [route-map map-name]	(任意) ASBR が強制的に OSPF ルーティング ドメイン内にデフォルト ルートを作成します。パラメータは、すべて任意です。
ステップ 6	Router(config)# <b>ip ospf name-lookup</b>	(任意) DNS 名検索を設定します。デフォルトではディセーブルに設定されています。
ステップ 7	Router(config)# <b>ip auto-cost</b> reference-bandwidth ref-bw	(任意) アドレスの範囲を指定し、その範囲に 1 つのルートをアドバタイズします。このコマンドは、ABR だけで使用します。
ステップ 8	Router(config)# <b>distance ospf</b> {[inter-area dist1]   [inter-area dist2]   [external dist3]}	(任意) OSPF の距離の値を変更します。各ルート タイプのデフォルトの距離は 110 です。指定できる範囲は 1 ~ 255 です。
ステップ 9	Router(config)# <b>passive-interface type</b> number	(任意) 指定したインターフェイス経由での Hello パケットの送信を停止します。
ステップ 10	Router(config)# <b>timers spf</b> spf-delay spf-holdtime	(任意) ルート計算タイマーを設定します。 <ul style="list-style-type: none"> <li>spf-holdtime 0 ~ 65535 の整数を入力します。デフォルトは 5 秒です。値 0 は、遅延させないことを表します。</li> <li>spf-delay 0 ~ 65535 の整数を入力します。デフォルトは 10 秒です。値 0 は、遅延させないことを表します。</li> </ul>
ステップ 11	Router(config)# <b>ospf log-adj-changes</b>	(任意) ネイバの状態が変化した場合に、Syslog メッセージを送信します。
ステップ 12	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 13	Router# <b>show ip ospf</b> [process-id [area-id]] <b>database</b>	指定したルータの OSPF データベースに関連する情報のリストを表示します。一部のキーワード オプションについては、「 <a href="#">OSPF のモニタリング</a> 」(p.11-21)を参照してください。
ステップ 14	Router# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

## LSA グループ ペーシングの変更

OSPF の LSA グループ ペーシング機能では、ルータをより効率的に使用できるように、ルータによって OSPF LSA がグループ化され、更新機能、チェックサム機能、およびエージング機能の発生頻度が設定されます。この機能は、デフォルトでイネーブルになっています。デフォルトのペーシング間隔は 4 分ですが、通常は、このパラメータを変更する必要はありません。最適なグループ ペーシング間隔は、ルータが更新、チェックサム、およびエージングを行う LSA の数に反比例します。たとえば、データベースに約 10,000 個の LSA があるような場合は、ペーシング間隔の値を減らすと、より効率化できます。データベースのサイズが非常に小さい場合 (LSA 数が 40 ~ 100 の場合) は、ペーシング間隔の値を 10 ~ 20 分に増やすと、やや効率化されます。

OSPF LSA ペーシングを設定するには、イネーブル EXEC モードで次の手順を実行します。

## ■ IP ルーティングの設定

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b>	グローバル 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	Router(config)# <b>router ospf process-id</b>	OSPF ルーティングをイネーブルにし、ルータ コンフィギュレーション モードを開始します。
ステップ 3	Router(config)# <b>timers lsa-group-pacing seconds</b>	LSA のグループ ページングを変更します。
ステップ 4	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	Router# <b>show running-config</b>	エントリを確認します。
ステップ 6	Router# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

デフォルト値に戻すには、**no timers lsa-group-pacing** ルータ コンフィギュレーション コマンドを使用します。

## ループバック インターフェイス

OSPF では、インターフェイスに設定されている最も数値の高い IP アドレスをルータ ID として使用します。このインターフェイスが故障したり、取り外されたりした場合は、OSPF のプロセスで新しいルータ ID を再計算し、インターフェイスからすべてのルーティング情報を再送する必要があります。IP アドレスを使用してループバック インターフェイスを設定した場合、OSPF はこの IP アドレスをルータ ID として使用します。他のインターフェイスがより数値の高い IP アドレスを持っている場合でも同様です。ループバック インターフェイスで障害が発生することはないので、この方法により安定性が向上します。OSPF では、他のインターフェイスよりループバック インターフェイスが自動的に優先され、すべてのループバック インターフェイスの中で最も数値の高い IP アドレスを持つループバック インターフェイスが選択されます。

ループバック インターフェイスを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b>	グローバル 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	Router(config)# <b>interface loopback 0</b>	ループバック インターフェイスを作成し、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 3	Router(config)# <b>ip address address mask</b>	このインターフェイスに IP アドレスを割り当てます。
ステップ 4	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	Router# <b>show ip interface</b>	エントリを確認します。
ステップ 6	Router# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

ループバック インターフェイスをディセーブルにするには、**no interface loopback 0** グローバル コンフィギュレーション コマンドを使用します。

## OSPF のモニタリング

IP ルーティング テーブル、キャッシュ、およびデータベースの内容など、特定の統計を表示できます。

表 11-3 に統計を表示するためのイネーブル EXEC コマンドの一部をリストします。show ip ospf database イネーブル EXEC コマンド オプションとコマンド出力内のフィールドの詳細については、『Cisco IOS IP and IP Routing Command Reference』を参照してください。

表 11-3 Show IP OSPF 統計コマンド

コマンドの説明	目的
Router(config)# <b>show ip ospf</b> [process-id]	OSPF ルーティング プロセスの全般情報を表示します。
Router(config)# <b>show ip ospf</b> [process-id] <b>database</b> [router] [link-state-id]	OSPF データベース関連情報のリストを表示します。
Router(config)# <b>show ip ospf</b> border-routes	内部 OSPF ルーティング ABR テーブルおよび ASBR テーブルのエントリを表示します。
Router(config)# <b>show ip ospf interface</b> [interface-name]	OSPF 関連のインターフェイス情報を表示します。
Router(config)# <b>show ip ospf neighbor</b> [interface-name] [neighbor-id] <b>detail</b>	OSPF インターフェイスのネイバ情報を表示します。
Router(config)# <b>show ip ospf</b> virtual-links	OSPF 関連の仮想リンク情報を表示します。

## EIGRP の設定

EIGRP は、Interior Gateway Routing Protocol (IGRP) をシスコが独自に拡張したバージョンです。EIGRP では、IGRP と同じディスタンス ベクタ アルゴリズムと距離情報を使用していますが、EIGRP のコンバージェンスのプロパティと運用効率は、大きく向上しました。

コンバージェンス テクノロジーでは、Diffusing Update Algorithm (DUAL; 拡散更新アルゴリズム) というアルゴリズムを採用しています。このアルゴリズムでは、ルート計算中は常にループしないことが保証されており、トポロジー変更に関係するすべての装置を同時に同期させることができます。トポロジー変更の影響を受けないルータは、再計算に関係しません。

IP EIGRP によりネットワークの規模が拡大します。RIP では、ネットワークの最大幅は、15 ホップでした。IGRP をイネーブルにすると、最大 224 ホップが可能で、EIGRP メトリックでは数千ホップがサポートされるので、ネットワークを拡大する場合の唯一の障害は、トランスポート層のホップカウントになります。EIGRP では、IP パケットが 15 個のルータを経由したあと、EIGRP が宛先までのネクスト ホップを学習している場合だけに、転送制御フィールドの値が増加します。宛先までのネクスト ホップとして RIP ルートが使用された場合は、転送制御フィールドの値が通常どおりに増加します。

EIGRP には、次の機能があります。

- 高速コンバージェンス
- 宛先の状態が変化した場合の差分更新。ルーティング テーブルの内容全体を送信する代わりに、EIGRP パケットに必要な帯域幅を最小限に抑えます。
- IGRP より低い CPU 使用率 (完全に更新されたパケットは、受信するたびに処理する必要がないため)
- プロトコルに関係なく、近接ルータ情報を学習するネイバ検出メカニズム
- Variable-Length Subnet Mask (VLSM; 可変長サブネット マスク)

- 任意の経路集約
- EIGRP による大規模ネットワークへの拡大

EIGRP には、次の 4 つの基本的なコンポーネントがあります。

- ネイバ検出および回復は、ルータが、直接接続されたネットワーク上の他のルータについて動的に学習するために使用するプロセスです。ルータは、ネイバが到達不能または動作不能になった場合も検出できる必要があります。ネイバ検出および回復機能では、定期的に少量の Hello パケットを送信するだけなので、オーバーヘッドが少なくてすみます。Cisco IOS ソフトウェアでは、Hello パケットを受信している限り、ネイバが機能しているものと判断されます。この状態にあると判断された場合、近接ルータはルーティング情報を交換できます。
- 高信頼性転送プロトコルにより、すべてのネイバに EIGRP パケットを確実に順序どおりに転送できます。マルチキャスト パケットとユニキャスト パケットが混在している場合でも転送が可能です。EIGRP パケットには、確実に送信する必要があるパケットとその必要がないパケットがあります。効率化するために、必要な場合に限って信頼性を確保します。たとえば、マルチアクセス ネットワークにはマルチキャスト機能（イーサネットなど）がありますが、すべてのネイバに Hello パケットを確実に送信する必要はありません。そのため、EIGRP では、マルチキャスト Hello パケットを 1 つ送信し、そのパケット内でそのパケットの確認応答が不要であることを受信側に通知します。その他のタイプのパケット（更新など）では、確認応答が必要なので、パケット内でそのことを通知します。転送の信頼性を確保するには、確認応答を受信していないパケットがある場合に、すぐにマルチキャスト パケットを送信するように設定します。この方法により、速度が異なるリンクがある場合にも、コンバージェンス時間を短く抑えることができます。
- DUAL 有限状態マシンは、すべてのルート計算を決定するプロセスです。このプロセスは、すべてのネイバからアドバタイズされたすべてのルートをトラッキングします。DUAL は、距離情報（メトリック）を使用して、効率がいいループフリー パスを選択します。また、DUAL は、サクセサ候補に基づいて、ルーティング テーブルに挿入するルートを選択します。サクセサとは、パケット転送に使用する近接ルータを指します。サクセサとなる近接ルータは、宛先までの最短コスト パスが設定されていて、ルーティング ループに関与しないことが保証されています。サクセサ候補がないにもかかわらず、ネイバが宛先をアドバタイズしている場合は、再計算が必要です。新しいサクセサは、このような方法で決定されます。ルートの再計算時間は、コンバージェンス時間に影響します。再計算には、大量のプロセッサ リソースが集中的に必要なので、できるだけ再計算しない方が便利です。トポロジー変更が発生すると、DUAL によってサクセサ候補がテストされます。サクセサ候補が検出されると、不必要な再計算を避けるために、その候補が使用されます。
- プロトコル依存型モジュールは、ネットワーク層プロトコル固有のタスクを実行します。このタイプのモジュールの例として、IP にカプセル化された EIGRP パケットを送受信する IP EIGRP モジュールがあげられます。このモジュールは、EIGRP パケットの解析、および新着情報の DUAL への通知も処理します。EIGRP は、DUAL にルーティングを決定するように要求しますが結果は IP ルーティング テーブルに保存されます。EIGRP は、他の IP ルーティング プロトコルが学習したルートも再配布します。

表 11-4 にデフォルトの EIGRP 設定を示します。

表 11-4 EIGRP のデフォルト設定

機能	デフォルト設定
自動サマリー	イネーブル。サブプレフィックスは、全クラスを使用したネットワーク境界を通過するときに、そのネットワーク境界に集約されます。
デフォルト情報	外部ルートが許可され、再配布時に IGRP プロセスまたは EIGRP プロセスの間でデフォルトの情報が渡されます。

表 11-4 EIGRP のデフォルト設定 (続き)

機能	デフォルト設定
デフォルトのメトリック	デフォルトのメトリックを使用せずに、接続されたルートとインターフェイスのスタティックルートだけを再配布できます。このメトリックには、次の情報が含まれています。 <ul style="list-style-type: none"> <li>帯域幅：0 Kbps 以上</li> <li>遅延 (10 マイクロ秒単位)：0、または 39.1 ナノ秒の倍数である正数</li> <li>信頼性：0 ~ 255 の任意の数値 (255 は信頼性 100%)</li> <li>ロード：有効帯域幅。0 ~ 255 の任意の数値 (255 はロード 100%)</li> <li>MTU：ルートの最大伝送ユニット サイズ (バイト単位)。0 または正の整数</li> </ul>
距離	内部距離：90 外部距離：170
EIGRP 近隣ルータの変更ログ	ディセーブル。隣接関係の変更はログに記録されません。
IP 認証キーチェーン	認証なし
IP 認証モード	認証なし
IP 帯域幅 (%)	50 %
IP Hello 間隔	低速 Nonbroadcast Multiaccess (NBMA) ネットワークの場合は 60 秒、その他のネットワークの場合は 5 秒
IP 待機時間	低速 NBMA ネットワークの場合は 180 秒、他のすべてのネットワークの場合は 15 秒
IP スプリット ホライズン	イネーブル
IP サマリー アドレス	サマリー集約アドレスは未定義
メトリックの重み	tos : 0 k1 および k3 : 1 k2、k4、および k5 : 0
ネットワーク	未指定
オフセットリスト	ディセーブル
ルータ EIGRP	ディセーブル
メトリック設定	ルート マップでのメトリックは未設定
トラフィック共有	メトリックの割合に比例して分散
分散	1 (等コスト ロード バランシング)

EIGRP ルーティング プロセスを作成するには、EIGRP をイネーブルにして、ネットワークを関連付けます。EIGRP は、指定されたネットワークのインターフェイスに更新情報を送信します。インターフェイスのネットワークを指定しない場合は、EIGRP の更新情報でアドバタイズされません。

## EIGRP ルータ モード コマンド

EIGRP を設定するには、イネーブル EXEC モードで次の手順を実行します。ルーティング プロセスの設定は必須ですが、それ以外は任意です。

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b>	グローバル 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	Router(config)# <b>router eigrp</b> <i>autonomous-system-number</i>	EIGRP ルーティング プロセスをイネーブルにし、ルータ コンフィギュレーション モードを開始します。AS 番号により他の EIGRP ルータへのルートが指定されます。この番号は、ルーティング情報のタグ付けに使用されます。
ステップ 3	Router(config)# <b>network</b> <i>network-number</i>	ネットワークを EIGRP ルーティング プロセスに関連付けます。EIGRP は、指定されたネットワークのインターフェイスに更新情報を送信します。インターフェイスのネットワークを指定していない場合は、IGRP または EIGRP の更新情報でアドバタイズされません。
ステップ 4	Router(config)# <b>eigrp log-neighbor-changes</b>	(任意) EIGRP ネイバ変更のログをイネーブルにし、ルーティングシステムの安定性をモニタリングします。
ステップ 5	Router(config)# <b>metric weights</b> <i>tos k1 k2</i> <i>k3 k4 k5</i>	(任意) EIGRP メトリックを調整します。デフォルト値は、ほとんどのネットワークで効率的に運用できるように慎重に決定されていますが、カスタマイズすることもできます。   <b>注意</b> メトリックの決定は複雑なので、カスタマイズする場合は、必ず経験豊富なネットワーク設計者の指示を受けてください。
ステップ 6	Router(config)# <b>offset list</b> [ <i>{access-list-number   name}</i> ]{ <b>in</b>   <b>out</b> } <i>offset [type-number]</i>	(任意) オフセット リストをルーティング メトリックに適用し、EIGRP 経由で学習したルートに着信と発信のメトリックを増やします。オフセット リストをアクセス リストやインターフェイスで制限できます。
ステップ 7	Router(config)# <b>no auto-summary</b>	(任意) ネットワークレベルのルートへのサブネット ルートの自動サマリーをディセーブルにします。
ステップ 8	Router(config)# <b>ip summary-address eigrp</b> <i>autonomous-system-number address-mask</i>	(任意) サマリー集約を設定します。
ステップ 9	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 10	Router# <b>show ip protocols</b>	エントリを確認します。
ステップ 11	Router# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

この機能をディセーブルにする場合、またはデフォルト値に戻す場合は、これらのコマンドの **no** 形式を使用します。例 11-8 に **show ip protocols** イネーブル EXEC コマンドの出力を示します。

**例 11-8 show ip protocols イネーブル EXEC コマンドの出力 (EIGRP の場合)**

```
Router# show ip protocols
Routing Protocol is "eigrp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Default networks flagged in outgoing updates
  Default networks accepted from incoming updates
  EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0
  EIGRP maximum hopcount 100
  EIGRP maximum metric variance 1
  Redistributing: eigrp 1
  Automatic network summarization is in effect
  Automatic address summarization:
    192.168.3.0/24 for POS0
    192.168.2.0/24 for FastEthernet0
  Maximum path: 4
  Routing for Networks:
    192.168.2.0
    192.168.3.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.1          90          00:03:16
  Distance: internal 90 external 170
```

**EIGRP インターフェイス モード コマンド**

他の任意の EIGRP パラメータは、インターフェイス ベースで設定できます。

イネーブル EXEC モードを開始し、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b>	グローバル 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	Router(config)# <b>interface interface-id</b>	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、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	Router(config)# <b>ip bandwidth-percent eigrp autonomous-system-number percent</b>	(任意) インターフェイスで EIGRP に使用できる帯域幅の最大パーセンテージを設定します。デフォルトは 50 % です。
ステップ 4	Router(config)# <b>ip summary-address eigrp autonomous-system-number address mask</b>	(任意) 指定したインターフェイスについて、サマリー集約アドレスを設定します(自動サマリーをイネーブルにしている場合は、通常不要)。
ステップ 5	Router(config)# <b>ip hello-interval eigrp autonomous-system-number seconds</b>	(任意) EIGRP ルーティング プロセスの Hello 時間間隔を変更します。範囲は、1 ~ 65535 秒です。低速 NBMA ネットワークのデフォルトは 60 秒、他のすべてのネットワークのデフォルトは 5 秒です。
ステップ 6	Router(config)# <b>ip hold-time eigrp autonomous-system-number seconds</b>	(任意) EIGRP ルーティング プロセスの待機時間間隔を変更します。範囲は、1 ~ 65535 秒です。低速 NBMA ネットワークのデフォルトは 180 秒、他のすべてのネットワークのデフォルトは 15 秒です。
		 <p><b>注意</b> 待機時間を調整する場合は、シスコのテクニカル サポートに相談してください。</p>

## ■ IP ルーティングの設定

	コマンドの説明	目的
ステップ 7	Router(config)# <b>no ip split-horizon eigrp autonomous-system-number</b>	(任意) スプリット ホライズンをディセーブルにし、ルート情報を発信したインターフェイス上にあるルータがそのルート情報をアドバタイズできるようにします。
ステップ 8	Router# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 9	Router# <b>show ip eigrp interface</b>	EIGRP がアクティブなインターフェイスとこれらのインターフェイスに関する EIGRP 情報を表示します。
ステップ 10	Router# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

この機能をディセーブルにする場合、またはデフォルト値に戻す場合は、これらのコマンドの **no** 形式を使用します。例 11-9 に **show ip eigrp interface** イネーブル EXEC コマンドの出力を示します。

## 例 11-9 show ip eigrp interface イネーブル EXEC コマンドの出力

```
Router# show ip eigrp interface
IP-EIGRP interfaces for process 1
```

Interface	Peers	Xmit Queue Un/Reliable	Mean SRTT	Pacing Time Un/Reliable	Multicast Flow Timer	Pending Routes
PO0	1	0/0	20	0/10	50	0
Fa0	0	0/0	0	0/10	0	0

## EIGRP ルート認証の設定

EIGRP のルート認証では、EIGRP ルーティング プロトコルからのルーティング更新を MD5 認証し、承認されていない送信元から権限がないルーティング メッセージや不正ルーティング メッセージを受信するのを防ぐことができます。

認証をイネーブルにするには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b>	グローバル 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	Router(config)# <b>interface interface-id</b>	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、設定するレイヤ 3 インターフェイスを指定します。
ステップ 3	Router(config-if)# <b>ip authentication mode eigrp autonomous-system-number md5</b>	IP EIGRP パケットで MD5 認証をイネーブルにします。
ステップ 4	Router(config-if)# <b>ip authentication key-chain eigrp autonomous-system-number key-chain</b>	IP EIGRP パケットの認証をイネーブルにします。
ステップ 5	Router(config-if)# <b>exit</b>	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	Router(config)# <b>key chain name-of-chain</b>	キーチェーンを指定し、キーチェーン 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 で設定した名前を指定します。
ステップ 7	Router(config-keychain)# <b>key number</b>	キーチェーン コンフィギュレーション モードで、キー番号を指定します。

	コマンドの説明	目的
ステップ 8	Router(config-keychain)# <b>key-string</b> text	キーチェーンのキー コンフィギュレーション モードで、キー文字列を指定します。
ステップ 9	Router(config-keychain-key)# <b>accept-lifetime</b> start-time {infinite   end-time   duration seconds}	(任意) キーを受信できる期間を指定します。  start-time と end-time の構文には、hh:mm:ss Month date year または hh:mm:ss date Month year のいずれかを使用します。デフォルトの start-time (および指定可能な最も古い日付) は、1993 年 1 月 1 日です。デフォルトの end-time と duration に制限はありません。
ステップ 10	Router(config-keychain-key)# <b>send-lifetime</b> start-time {infinite   end-time   duration seconds}	(任意) キーを送信できる期間を指定します。  start-time と end-time の構文には、hh:mm:ss Month day year または hh:mm:ss day Month year のいずれかを指定します。デフォルトの start-time (および指定可能な最も古い日付) は、1993 年 1 月 1 日です。デフォルトの end-time と duration に制限はありません。
ステップ 11	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 12	Router# <b>show key chain</b>	認証キー情報を表示します。
ステップ 13	Router# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

機能をディセーブルにするか、または設定値をデフォルトに戻す場合は、これらのコマンドの **no** 形式を指定します。

## EIGRP のモニタリングとメンテナンス

ネイバ テーブルからネイバを削除できます。各種の EIGRP ルーティング統計情報も表示できます。表 11-5 に、ネイバを削除して統計情報を表示するイネーブル EXEC コマンドを示します。コマンド出力のフィールドの詳細については、『Cisco IOS IP and IP Routing Command Reference』を参照してください。

表 11-5 IP EIGRP の Clear コマンドと Show コマンド

コマンドの説明	目的
Router# <b>clear ip eigrp neighbors</b> {ip-address   interface}	ネイバ テーブルからネイバを削除します。
Router# <b>show ip eigrp interface</b> [interface] [as-number]	EIGRP に設定したインターフェイスの情報を表示します。
Router# <b>show ip eigrp neighbors</b> [type-number]	EIGRP で検出されたネイバを表示します。
Router# <b>show ip eigrp topology</b> {autonomous-system-number   [ip-address] mask}	特定のプロセスについて EIGRP トポロジー テーブルを表示します。
Router# <b>show ip eigrp traffic</b> [autonomous-system-number]	すべての EIGRP プロセス、または指定した EIGRP プロセスについて送受信されたパケットの数を表示します。

例 11-10 に show ip eigrp interface イネーブル EXEC コマンドの出力を示します。

例 11-11 に show ip eigrp neighbors イネーブル EXEC コマンドの出力を示します。

例 11-12 に show ip eigrp topology イネーブル EXEC コマンドの出力を示します。

例 11-13 に show ip eigrp traffic イネーブル EXEC コマンドの出力を示します。

**例 11-10 show ip eigrp interface イネーブル EXEC コマンドの出力**

```
Router# show ip eigrp interface
IP-EIGRP interfaces for process 1

Interface          Xmit Queue  Mean   Pacing Time  Multicast    Pending
                   Un/Reliable SRTT   Un/Reliable  Flow Timer   Routes
PO0                 1           0/0    20           0/10         50          0
Fa0                 0           0/0    0            0/10         0           0
```

**例 11-11 show ip eigrp neighbors イネーブル EXEC コマンドの出力**

```
Router# show ip eigrp neighbors
IP-EIGRP neighbors for process 1
H   Address                Interface    Hold Uptime   SRTT   RTO  Q  Seq Type
                   (sec)      (ms)      Cnt Num
0   192.168.2.1              PO0         13 00:08:15    20    200  0  2
```

**例 11-12 show ip eigrp topology イネーブル EXEC コマンドの出力**

```
Router# show ip eigrp topology
IP-EIGRP Topology Table for AS(1)/ID(192.168.3.1)

Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
       r - reply Status, s - sia Status

P 192.168.1.0/24, 1 successors, FD is 30720
   via 192.168.2.1 (30720/28160), POS0
P 192.168.2.0/24, 1 successors, FD is 10752
   via Connected, POS0
P 192.168.3.0/24, 1 successors, FD is 28160
   via Connected, FastEthernet0
```

**例 11-13 show ip eigrp traffic イネーブル EXEC コマンドの出力**

```
Router# show ip eigrp traffic
IP-EIGRP Traffic Statistics for process 1
Hellos sent/received: 273/136
Updates sent/received: 5/2
Queries sent/received: 0/0
Replies sent/received: 0/0
Acks sent/received: 1/2
Input queue high water mark 1, 0 drops
SIA-Queries sent/received: 0/0
SIA-Replies sent/received: 0/0
```

## BGP と CIDR

Border Gateway Protocol (BGP) は、AS 間でループフリーなルーティング情報交換を自動的に保証するようにドメイン間のルーティングシステムをセットアップするための Exterior Gateway Protocol (EGP; 外部ゲートウェイ プロトコル) です。BGP では、各ルートが、ネットワーク番号、情報が通過した AS (AS パス) のリスト、および他のパス属性のリストで構成されます。

レイヤ 3 のスイッチングでは、Classless Interdomain Routing (CIDR) を含む BGP バージョン 4 がサポートされます。CIDR では、集約ルートを作成してスーパーネットにすることで、ルーティングテーブルのサイズを減らすことができます。CIDR により、BGP 内のネットワーク クラスの概念が取り除かれ、IP プレフィックスのアドバタイズがサポートされます。CIDR のルートは、OSPF、EIGRP、および RIP で伝送されます。

## BGP の設定

BGP ルーティングを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>ip routing</b>	IP ルーティングをイネーブルにします (デフォルト)。
ステップ 2	Router(config)# <b>router bgp autonomous-system</b>	BGP をルーティング プロトコルとして定義して、BGP ルーティング プロセスを開始します。
ステップ 3	Router(config-router)# <b>network network-number</b> [ <b>mask network-mask</b> ] [ <b>route-map route-map-name</b> ]	ネットワークがこの AS に対してローカルであることを表すフラグを設定し、BGP テーブルにそのフラグを追加します。
ステップ 4	Router(config-router)# <b>end</b>	イネーブル EXEC モードに戻ります。

例 11-14 に BGP ルーティングの設定例を示します。

### 例 11-14 BGP ルーティングの設定

```
Router(config)# ip routing
Router(config)# router bgp 30
Router(config-router)# network 192.168.1.1
Router(config-router)# neighbor 192.168.2.1
Router(config-router)# end
```

BGP ルーティング設定の詳細については、『Cisco IOS IP and IP Routing Configuration Guide』の「Configuring BGP」の章を参照してください。

## BGP 設定の確認

表 11-6 に BGP 設定を表示するための共通 EXEC コマンドの一部を示します。また、例 11-15 に表 11-6 でリストされたコマンドの出力を示します。

表 11-6 BGP の Show コマンド

コマンドの説明	目的
Router# <b>show ip protocols</b> [summary]	プロトコル設定を表示します。
Router# <b>show ip bgp neighbor</b>	各ネイバへの BGP 接続と TCP 接続の詳細情報を表示します。
Router# <b>show ip bgp summary</b>	すべての BGP 接続のステータスを表示します。
Router# <b>show ip bgp</b>	BGP ルーティング テーブルの内容を表示します。

## 例 11-15 BGP 設定情報

```

Router# show ip protocols
Routing Protocol is "bgp 1"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  IGP synchronization is enabled
  Automatic route summarization is enabled
  Redistributing: connected
  Neighbor(s):
    Address          FiltIn FiltOut DistIn DistOut Weight RouteMap
    192.168.2.1
  Maximum path: 1
  Routing for Networks:
  Routing Information Sources:
    Gateway          Distance      Last Update
  Distance: external 20 internal 200 local 200

Router# show ip bgp neighbor
BGP neighbor is 192.168.2.1, remote AS 1, internal link
  BGP version 4, remote router ID 192.168.2.1
  BGP state = Established, up for 00:08:46
  Last read 00:00:45, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received(new)
    Address family IPv4 Unicast: advertised and received
  Received 13 messages, 0 notifications, 0 in queue
  Sent 13 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Default minimum time between advertisement runs is 5 seconds

For address family: IPv4 Unicast
  BGP table version 3, neighbor version 3
  Index 1, Offset 0, Mask 0x2
  2 accepted prefixes consume 72 bytes
  Prefix advertised 2, suppressed 0, withdrawn 0
  Number of NLRIs in the update sent: max 2, min 0

  Connections established 1; dropped 0
  Last reset never
  Connection state is ESTAB, I/O status: 1, unread input bytes: 0
  Local host: 192.168.2.2, Local port: 179
  Foreign host: 192.168.2.1, Foreign port: 11001

  Enqueued packets for retransmit: 0, input: 0  mis-ordered: 0 (0 bytes)

Event Timers (current time is 0x45B7B4):
Timer          Starts      Wakeups      Next
Retrans        13          0            0x0
TimeWait       0           0            0x0
AckHold        13          9            0x0
SendWnd        0           0            0x0
KeepAlive      0           0            0x0
GiveUp         0           0            0x0
PmtuAger       0           0            0x0
DeadWait       0           0            0x0

iss: 3654396253  snduna: 3654396567  sndnxt: 3654396567  sndwnd: 16071
irs: 3037331955  rcvnxt: 3037332269  rcvwnd: 16071  delrcvwnd: 313

SRTT: 247 ms, RTTO: 663 ms, RTV: 416 ms, KRTT: 0 ms
minRTT: 4 ms, maxRTT: 300 ms, ACK hold: 200 ms
Flags: passive open, nagle, gen tcbs

Datagrams (max data segment is 1460 bytes):
Rcvd: 15 (out of order: 0), with data: 13, total data bytes: 313
Sent: 22 (retransmit: 0), with data: 12, total data bytes: 313

Router# show ip bgp summary

```

```
BGP router identifier 192.168.3.1, local AS number 1
BGP table version is 3, main routing table version 3
3 network entries and 4 paths using 435 bytes of memory
2 BGP path attribute entries using 120 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP activity 3/6 prefixes, 4/0 paths, scan interval 60 secs
```

```
Neighbor      V    AS MsgRcvd MsgSent  TblVer  InQ  OutQ Up/Down  State/PfxRcd
192.168.2.1    4    1     14     14       3     0    0 00:09:45      2
```

```
Router# show ip bgp
```

```
BGP table version is 3, local router ID is 192.168.3.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
Network          Next Hop           Metric LocPrf Weight Path
* i192.168.1.0    192.168.2.1        0      100      0 ?
* i192.168.2.0    192.168.2.1        0      100      0 ?
*>                0.0.0.0            0                   32768 ?
*> 192.168.3.0    0.0.0.0            0                   32768 ?
```

## IS-IS の設定

Intermediate System-to-Intermediate System (IS-IS) ルーティングを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>router isis</b> [tag]	IS-IS を IP ルーティング プロトコルとして定義します。
ステップ 2	Router(config-router)# <b>net</b> network-entity-title	ルーティング プロセスについて Network Entity Title (NET) を設定します。NET には、名前とアドレスを指定できます。
ステップ 3	Router(config-router)# <b>interface</b> interface-type interface-id	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)# <b>ip address</b> ip-address mask	このインターフェイスに IP アドレスを割り当てます。
ステップ 5	Router(config-if)# <b>ip router isis</b> [tag]	このインターフェイスで IS-IS を実行することを指定します。
ステップ 6	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。

例 11-16 に IS-IS ルーティングの設定例を示します。

### 例 11-16 IS-IS ルーティングの設定

```
Router(config)# router isis
Router(config-router)# net 49.0001.0000.0000.000a.00
Router(config-router)# interface gigabitethernet 0
Router(config-if)# ip router isis
Router(config-if)# end
```

IS-IS ルーティング設定の詳細については、『Cisco IOS IP and IP Routing Configuration Guide』の「Configuring Integrated IS-IS」の章を参照してください。

## IS-IS 設定の確認

IS-IS 設定を確認するには、表 11-7 に示した EXEC コマンドを使用します。例 11-17 に表 11-7 のコマンドとその出力の例を示します。

表 11-7 IS-IS の Show コマンド

コマンドの説明	目的
Router# <code>show ip protocols [summary]</code>	プロトコル設定を表示します。
Router# <code>show isis database</code>	IS-IS リンク状態データベースを表示します。
Router# <code>show clns neighbor</code>	ES と IS のネイバを表示します。



(注)

ML シリーズでは、Connectionless Network Service (CLNS; コネクションレス型ネットワーク サービス) プロトコルのルーティングがサポートされません。

### 例 11-17 IS-IS の設定

```
Router# show ip protocols
Routing Protocol is "isis"
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Redistributing: isis
  Address Summarization:
    None
  Maximum path: 4
  Routing for Networks:
    FastEthernet0
    POS0
  Routing Information Sources:
    Gateway         Distance      Last Update
    192.168.2.1      115          00:06:48
  Distance: (default is 115)

Router# show isis database

IS-IS Level-1 Link State Database:
LSPID                LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
Router_A.00-00       0x00000003   0xA72F        581            0/0/0
Router_A.02-00       0x00000001   0xA293        581            0/0/0
Router.00-00         * 0x00000004   0x79F9        582            0/0/0
IS-IS Level-2 Link State Database:
LSPID                LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
Router_A.00-00       0x00000004   0xF0D6        589            0/0/0
Router_A.02-00       0x00000001   0x328C        581            0/0/0
Router.00-00         * 0x00000004   0x6A09        586            0/0/0

Router# show clns neighbors

System Id      Interface  SNPA                State  Holdtime  Type Protocol
Router_A       PO0       0005.9a39.6790     Up     7          L1L2 IS-IS
```

## スタティック ルートの設定

スタティック ルートは、ユーザが定義するルートです。パケットは、ユーザが指定したパスを通して、送信元と宛先の間で移動します。スタティック ルートは、ルータが特定の宛先までのルートを作成できない場合に重要になります。また、最終手段としてゲートウェイを指定し、ルーティングできないパケットをすべてそのゲートウェイに送信する場合にも便利です。

スタティック ルートを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b>	グローバル 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	Router(config)# <b>ip route prefix mask</b> { address   interface } [distance]	スタティック ルートを設定します。例 11-18 に例を示します。
ステップ 3	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 4	Router# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

### 例 11-18 スタティック ルート

```
Router(config)# ip route 0.0.0.0 0.0.0.0 192.168.2.1
```

スタティック ルートを削除するには、**no ip route prefix mask {address | interface}** グローバル コンフィギュレーション コマンドを使用します。スタティック IP ルートの情報を表示するには、**show ip routes** イネーブル EXEC コマンドを使用します (例 11-19)。

### 例 11-19 show ip route イネーブル EXEC コマンドの出力 (スタティック ルートを設定した場合)

```
Router# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route
Gateway of last resort is 192.168.2.1 to network 0.0.0.0

C    192.168.2.0/24 is directly connected, POS0
C    192.168.3.0/24 is directly connected, FastEthernet0
S*   0.0.0.0/0 [1/0] via 192.168.2.1
```

**show ip route** イネーブル EXEC コマンドの出力では、ルーティング プロトコルのコードが表示されます。表 11-8 に、これらのルーティング プロトコルに関するデフォルトの管理距離を示します。

表 11-8 ルーティング プロトコルのデフォルトの管理距離

ルートソース	デフォルトの距離
接続されたインターフェイス	0
スタティック ルート	1
EIRGP サマリー ルート	5
外部 BGP	20
内部 EIGRP	90
OSPF	110

表 11-8 ルーティング プロトコルのデフォルトの管理距離 (続き)

ルートソース	デフォルトの距離
RIP	120
外部 EIGRP	170
内部 BGP	200
不明	225

## スタティック ルートのモニタリング

スタティック ルートの統計情報を表示するには、`show ip route` コマンドを使用します (例 11-20)。`show ip` イネーブル EXEC コマンドのオプションとコマンド出力内のフィールドの詳細については、『Cisco IOS IP and IP Routing Command Reference』を参照してください。

### 例 11-20 show ip route コマンドの出力 (スタティック ルートを設定した場合)

```
Router# show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.2.1 to network 0.0.0.0

C    192.168.2.0/24 is directly connected, POS0
C    192.168.3.0/24 is directly connected, FastEthernet0
S*   0.0.0.0/0 [1/0] via 192.168.2.1
```

## IP ネットワークのモニタリングとメンテナンス

特定のキャッシュ、テーブル、またはデータベースの内容をすべて削除できます。また、特定の統計情報も表示できます。ルートのクリアやステータスの表示には、表 11-9 のイネーブル EXEC コマンドを使用します。

表 11-9 IP ルートのクリアまたはルート ステータスの表示を行うコマンド

コマンドの説明	目的
Router# <b>clear ip route</b> {network [mask   *]}	IP ルーティング テーブルから 1 つまたは複数のルートをクリアします。
Router# <b>show ip protocols</b>	パラメータとアクティブなルーティング プロトコル プロセスの状態を表示します。
Router# <b>show ip route</b> [{address [mask] [longer-prefixes]   [protocol [process-id]]}]	ルーティング テーブルの現在の状態を表示します。
Router# <b>show ip interface interface</b>	インターフェイスの詳細情報を表示します。
Router# <b>show ip interface brief</b>	すべてのインターフェイスの状態に関する要約情報を表示します。
Router# <b>show ip route summary</b>	ルーティング テーブルの現在の状態を要約して表示します。
Router# <b>show ip route supernets-only</b>	スーパーネットを表示します。
Router# <b>show ip cache</b>	IP トラフィックのスイッチングに使用するルーティング テーブルを表示します。
Router# <b>show route-map [map-name]</b>	設定済みのすべてのルート マップまたは指定したルート マップだけを表示します。

## IP マルチキャスト ルーティングの概要

ネットワークの規模が拡大するにつれて、マルチキャスト トラフィックを必要としているセグメントとそれ以外のセグメントを判断する上で、マルチキャスト ルーティングの重要性が非常に高まります。IP マルチキャストでは、IP トラフィックを 1 つまたは多数の送信元から多数の宛先に伝播させることができます。1 つのパケットを各宛先に送信するのではなく、1 つのパケットを 1 つの IP 宛先グループアドレスによって識別されるマルチキャスト グループに送信します。

IP マルチキャストの最も重要なコンポーネントは、Internet Group Management Protocol (IGMP) です。ホストは、IGMP メッセージを ML シリーズ カードに送信して、マルチキャスト グループのメンバーシップを識別します。トラフィックは、マルチキャスト グループのすべてのメンバーに送信されます。1 つのホストを同時に複数のグループのメンバーに指定することも可能です。また、ホストがデータ送信先グループのメンバーである必要はありません。インターフェイスで Protocol Independent Multicast (PIM; プロトコル独立型マルチキャスト) をイネーブルにすると、同じインターフェイスで IGMP の操作もイネーブルになります。

ML シリーズ カードでは、PIM ルーティング プロトコルと Auto-RP 設定がサポートされます。

PIM には、トラフィック密度環境 (密および疎) に関する 3 種類の動作モードがあります。これらのモードは、dense (密) モード、sparse (疎) モード、および疎 / 密モードと呼ばれます。

PIM の密モードでは、ダウンストリーム ネットワークがそこに転送されるデータグラムの受信を要求していると見なします。ML シリーズ カードは、ブルーニングや切り捨てが発生するまで、すべての発信インターフェイスですべてのパケットを転送します。PIM の密モードをイネーブルにしているインターフェイスは、タイムアウトするまでマルチキャスト データ ストリームを受信できます。次の条件下では、PIM の密モードが最も便利です。

- 送信側と受信側が近接して存在している。
- ネットワーク間で受信側より送信側が少ない。
- マルチキャスト トラフィックのストリームが一定である。

PIM の疎モードでは、トラフィックで明示的に要求されていない限り、ダウンストリーム ネットワークがグループに対するマルチキャスト パケットの転送を要求していないとみなします。PIM の疎モードでは、パケットを正しくルーティングするための登録ポイントとして使用する Rendezvous Point (RP; ランデブー ポイント) を定義します。

送信側がデータを送信する場合は、そのデータを RP に送信します。ML シリーズ カードでデータを受信する準備が整っている場合は、このカードが RP に登録されます。データ ストリームが送信側から RP 経由で受信側に送信され始めると、データ パス内にある ML シリーズ カードが不要なホップ (RP を含む) を自動的に削除してパスを最適化します。

PIM の疎モードは、マルチポイント データ ストリームが多く、各マルチキャスト ストリームがネットワーク内の比較的少数の LAN に送信される環境に適しています。次の条件下では、PIM の疎モードが最も便利です。

- グループ内に受信側がほとんどない。
- 送信側と受信側の間が WAN リンク で区切られている。
- マルチキャスト トラフィックのストリームが途切れがちである。



(注)

ML シリーズ カードでは、Reverse Path Forwarding (RPF; リバース パス転送) マルチキャストがサポートされますが、RPF ユニキャストはサポートされません。

## IP マルチキャスト ルーティングの設定

IP マルチキャスト ルーティングを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>ip multicast-routing</b>	ML シリーズ カードで IP マルチキャストをイネーブルにします。
ステップ 2	Router(config)# <b>interface type number</b>	インターフェイスを設定するために、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	Router(config-if)# <b>ip pim {dense-mode   sparse mode   sparse-dense-mode}</b>	このコマンドを入力する各インターフェイスで IP マルチキャスト ルーティングを実行します。dense(密)モード、sparse(疎)モード、または疎/密モードを指定する必要があります。
ステップ 4	Router(config)# <b>ip pim rp-address rendezvous-point ip-address</b>	マルチキャストグループの RP を設定します。
ステップ 5	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 6	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM に保存します。

## IP マルチキャスト動作のモニタリングと確認

IP マルチキャスト ルーティングの設定後に、イネーブル EXEC モードで表 11-10 のコマンドを実行すると、設定した IP マルチキャスト ルーティングの動作をモニタリングして確認できます。

表 11-10 IP マルチキャスト ルーティングの Show コマンド

コマンドの説明	目的
Router# <b>show ip mroute</b>	完全なマルチキャスト ルーティング テーブルと処理済みパケットの複合統計を表示します。
Router# <b>show ip pim neighbor</b>	このコマンドを EXEC モードで使用すると、Cisco IOS ソフトウェアで検出された PIM のネイバが表示されます。
Router# <b>show ip pim interface</b>	PIM に設定したインターフェイスの情報を表示します。
Router# <b>show ip pim rp</b>	このコマンドを EXEC モードで使用すると、関連するマルチキャスト ルーティング エントリとともにキャッシュされたアクティブな RP が表示されます。





## IRB の設定

---

この章では、ML シリーズのカードに Integrated Routing and Bridging (IRB; 統合ルーティングおよびブリッジング) を設定する方法を説明します。この章で使用する Cisco IOS のコマンドについては、『Cisco IOS Command Reference』を参照してください。

この章の主な内容は次のとおりです。

- [IRB の概要 \(p.12-2\)](#)
- [IRB の設定 \(p.12-3\)](#)
- [IRB の設定例 \(p.12-5\)](#)
- [IRB のモニタリングと確認 \(p.12-7\)](#)



### 注意

ML シリーズでは、Cisco ISL (スイッチ間リンク) と Cisco Dynamic Trunking Protocol (DTP) はサポートされませんが ML シリーズのブロードキャストでこれらの形式は転送されます。装置間の接続に ISL または DTP を使用しないことを推奨します。シスコの装置によっては、デフォルトで ISL または DTP を使用するものがあります。

---

## IRB の概要

ネットワークによっては、複数のセグメント内でローカルトラフィックをブリッジングし、これらのセグメント上のホストをルーティング対象ネットワーク上のホストまたは ML シリーズ カードに接続する必要がある場合があります。たとえば、ブリッジトポロジをルーティングトポロジに移行するために、ブリッジド セグメントの一部をルーテッド ネットワークに接続するような場合です。

IRB 機能を使用すると、指定したプロトコルを 1 つの ML シリーズ カード内のルーテッド インターフェイスやブリッジ グループの間でルーティングできます。具体的には、ローカルまたはルーティング不能のトラフィックは同じブリッジ グループ内のブリッジド インターフェイス間でブリッジされ、ルーティング可能なトラフィックは他のルーテッド インターフェイスまたはブリッジ グループにルーティングされます。

ブリッジングはデータリンク層で実行され、ルーティングはネットワーク層で実行されるため、それぞれのプロトコル設定モデルが異なります。たとえば IP の場合、ブリッジ グループ インターフェイスは同じ 1 つのネットワークに属し、1 つの共同の IP ネットワーク アドレスがあります。一方、各ルーテッド インターフェイスは、個別のネットワークを表し、独自の IP ネットワーク アドレスを取得しています。IRB では、Bridge Group Virtual Interface ( BVI; ブリッジ グループ仮想インターフェイス ) の概念を使用して、これらのインターフェイスで特定のプロトコルのパケット交換を可能にします。

BVI は、ML シリーズ カード内の仮想インターフェイスとして、通常のルーテッドインターフェイスと同様に機能します。BVI は、ブリッジングをサポートしませんが、ML シリーズ カード内のルーテッド インターフェイスに対して、対応するブリッジ グループを表します。インターフェイス番号は、BVI とブリッジ グループの間のリンクとなります。

IRB を設定する前に、次の点に注意してください。

- ブリッジ グループでのデフォルトのルーティングまたはブリッジング ( IRB がイネーブルな場合 ) の動作は、すべてのパケットがブリッジされます。BVI で IP トラフィックのルーティングを明示的に設定してください。
- Local-Area Transport ( LAT ) などのルーティングできないプロトコルは、必ずブリッジされます。ルーティングできないトラフィックのブリッジングをディセーブルにすることはできません。
- IRB を使用して特定のプロトコルをブリッジおよびルーティングする場合、ブリッジド インターフェイスでプロトコル属性を設定しないでください。BVI でプロトコル属性を設定することはできますが、ブリッジング属性を設定することはできません。
- 1 つのブリッジにより複数のネットワーク セグメントが 1 つの大きいフラット ネットワークにリンクされます。1 つのルーテッド インターフェイスから着信したパケットを複数のブリッジド インターフェイス間でブリッジングするには、そのブリッジ グループを 1 つのインターフェイスで表す必要があります。
- 1 つの BVI グループ内のすべてのポートで Maximum Transmission Unit ( MTU; 最大伝送ユニット ) の設定を同一にする必要があります。

## IRB の設定

IRB を設定するには、次の手順を実行します。

1. ブリッジグループとルーテッド インターフェイスを設定します。
  - a. ブリッジングをイネーブルにします。
  - b. インターフェイスをブリッジグループに割り当てます。
  - c. ルーティングを設定します。
2. IRB をイネーブルにします。
3. BVI を設定します。
  - a. BVI をイネーブルにして、ルーティングされたパケットを受け付けます。
  - b. BVI でルーティングをイネーブルにします。
4. ルーテッド インターフェイスで IP アドレスを設定します。
5. IRB 設定を確認します。

BVI を設定してルーティングをイネーブルにした場合、ブリッジグループ内のセグメントにあるホスト宛てのパケットがルーテッド インターフェイスに着信すると、BVI にルーティングされ、ブリッジング エンジンに転送されます。このパケットは、ブリッジング エンジンからブリッジド インターフェイス経由で送出されます。同様に、ルーテッド インターフェイスにあるホスト宛てのパケットがブリッジド インターフェイスに着信すると、このパケットは、まず BVI に送信されます。さらに、このパケットは、BVI からルーティング エンジンに転送され、このルーティング エンジンからルーテッド インターフェイスに送信されます。

ブリッジグループとそのブリッジグループ内のインターフェイスを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>bridge</b> <i>bridge-group</i> <b>protocol</b> { <i>ieee</i>   <i>rstp</i> }	1 つまたは複数のブリッジグループを定義します。
ステップ 2	Router(config)# <b>interface</b> <i>type number</i>	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	Router(config-if)# <b>bridge-group</b> <i>bridge-group</i>	インターフェイスを特定のブリッジグループに割り当てます。
ステップ 4	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。

IRB と BVI をイネーブルにして設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>bridge</b> <i>irb</i>	IRB をイネーブルにします。トラフィックのブリッジングを有効にします。
ステップ 2	Router(config)# <b>interface</b> <i>bvi</i> <i>bridge-group</i>	BVI に対応するブリッジグループの番号を割り当て、BVI を設定します。各ブリッジグループに対応させることができる BVI は、1 つだけです。
ステップ 3	Router(config-if)# <b>ip address</b> <i>ip-address</i> <i>ip-address-subnet-mask</i>	ルーテッド インターフェイスに IP アドレスを設定します。
ステップ 4	Router(config-if)# <b>exit</b>	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。

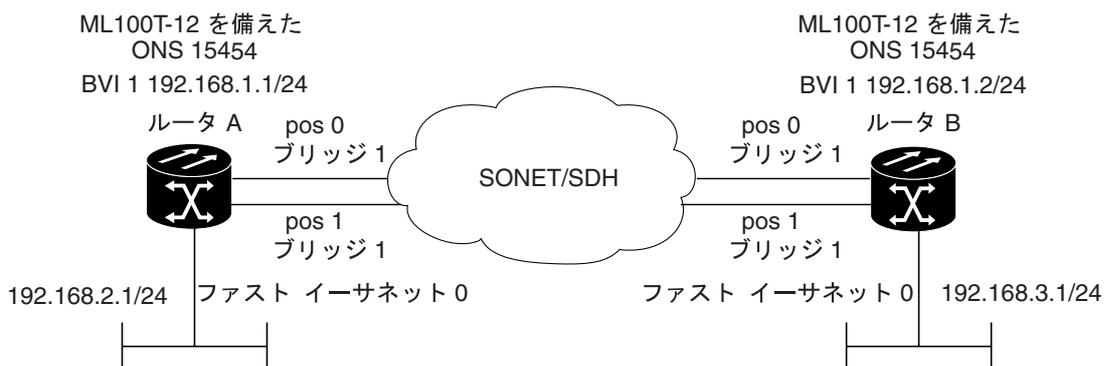
## ■ IRB の設定

	コマンドの説明	目的
ステップ 5	Router(config)# <b>bridge bridge-group route protocol</b>	BVI をイネーブルにして、対応するブリッジ グループから受信したルーティング可能パケットをルーティングします。  BVI を使用して対応するブリッジ グループから他のルーテッド インターフェイスにルーティングするプロトコルごとに、このコマンドを実行してください。
ステップ 6	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 7	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM (不揮発性 RAM) に保存します。

## IRB の設定例

図 12-1 は、IRB の設定例です。例 12-1 はルータ A の設定コードを、例 12-2 はルータ B の設定コードを表しています。

図 12-1 IRB の設定



83446

例 12-1 ルータ A の設定

```
bridge irb
bridge 1 protocol ieee
  bridge 1 route ip
!
!
interface FastEthernet0
  ip address 192.168.2.1 255.255.255.0
!
interface POS0
  no ip address
  crc 32
  bridge-group 1
  pos flag c2 1
!
interface POS1
  no ip address
  crc 32
  bridge-group 1
  pos flag c2 1
!
interface BVI1
  ip address 192.168.1.1 255.255.255.0
!
router ospf 1
  log-adjacency-changes
  network 192.168.1.0 0.0.0.255 area 0
  network 192.168.2.0 0.0.0.255 area 0
```

**例 12-2 ルータ B の設定**

```
bridge irb
bridge 1 protocol ieee
  bridge 1 route ip
!
!
interface FastEthernet0
  ip address 192.168.3.1 255.255.255.0
!
interface POS0
  no ip address
  crc 32
bridge-group 1
  pos flag c2 1
!
interface POS1
  no ip address
  crc 32
bridge-group 1
  pos flag c2 1
!
interface BVI1
  ip address 192.168.1.2 255.255.255.0
!
router ospf 1
  log-adjacency-changes
  network 192.168.1.0 0.0.0.255 area 0
  network 192.168.3.0 0.0.0.255 area 0
```

## IRB のモニタリングと確認

表 12-1 に、IRB をモニタリングおよび確認するためのイネーブル EXEC コマンドを示します。

表 12-1 IRB をモニタリングおよび確認するためのコマンド

コマンドの説明	目的
Router# <code>show interfaces bvi</code> <code>bvi-interface-number</code>	BVI MAC (メディア アクセス制御) アドレスや処理統計情報などの BVI 情報を表します。 <code>bvi-interface-number</code> は BVI インターフェイスに割り当てられたブリッジグループの番号です。
Router# <code>show interfaces [type-number] irb</code>	次のプロトコルについて BVI 情報を表示します。 <ul style="list-style-type: none"> <li>このブリッジド インターフェイスから他のルーテッド インターフェイスにルーティングできるプロトコル (ただし、ルーティング可能なパケットに限る)</li> <li>このブリッジド インターフェイスがブリッジングするプロトコル</li> </ul>

`show interfaces bvi` コマンドおよび `show interfaces irb` コマンドの出力例を次に示します。

## 例 12-3 IRBのモニタリングと確認

```

Router# show interfaces bvi1
BVI1 is up, line protocol is up
  Hardware is BVI, address is 0011.2130.b340 (bia 0000.0000.0000)
  Internet address is 100.100.100.1/24
  MTU 1500 bytes, BW 145152 Kbit, DLY 5000 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 03:35:28, output never, 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
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicast)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    1353 packets output, 127539 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out

Router# show interfaces irb
BVI1
Software MAC address filter on BVI1
  Hash Len  Address  Matches  Act  Type
  0x00:  0 ffff.ffff.ffff  0 RCV Physical broadcast
GigabitEthernet0
Bridged protocols on GigabitEthernet0:
  clns  ip
Software MAC address filter on GigabitEthernet0
  Hash Len  Address  Matches  Act  Type
  0x00:  0 ffff.ffff.ffff  0 RCV Physical broadcast
  0x58:  0 0100.5e00.0006  0 RCV IP multicast
  0x5B:  0 0100.5e00.0005  0 RCV IP multicast
  0x65:  0 0011.2130.b344  0 RCV Interface MAC address
  0xC0:  0 0100.0ccc.cccc  0 RCV CDP
  0xC2:  0 0180.c200.0000  0 RCV IEEE spanning tree
POS0
Routed protocols on POS0:
  ip
Bridged protocols on POS0:
  clns  ip
Software MAC address filter on POS0
  Hash Len  Address  Matches  Act  Type
  0x00:  0 ffff.ffff.ffff  9 RCV Physical broadcast
  0x58:  0 0100.5e00.0006  0 RCV IP multicast
  0x5B:  0 0100.5e00.0005  1313 RCV IP multicast
  0x61:  0 0011.2130.b340  38 RCV Interface MAC address
  0x61:  1 0011.2130.b340  0 RCV Bridge-group Virtual Interface
  0x65:  0 0011.2130.b344  0 RCV Interface MAC address
  0xC0:  0 0100.0ccc.cccc  224 RCV CDP
  0xC2:  0 0180.c200.0000  0 RCV IEEE spanning tree
POS1
SPR1
Bridged protocols on SPR1:
  clns  ip
Software MAC address filter on SPR1
  Hash Len  Address  Matches  Act  Type
  0x00:  0 ffff.ffff.ffff  0 RCV Physical broadcast
  0x60:  0 0011.2130.b341  0 RCV Interface MAC address
  0x65:  0 0011.2130.b344  0 RCV Interface MAC address
  0xC0:  0 0100.0ccc.cccc  0 RCV CDP
  0xC2:  0 0180.c200.0000  0 RCV IEEE spanning tree

```

表 12-1 に、表示される重要なフィールドを説明します。

表 12-2 show interfaces irb コマンドで出力されるフィールドの説明

フィールド	説明
Routed protocols on...	指定したインターフェイスに対して設定されたルーテッドプロトコルの一覧
Bridged protocols on...	指定したインターフェイスに対して設定されたブリッジドプロトコルの一覧
Software MAC address filter on...	指定したインターフェイスに対するソフトウェア MAC アドレスフィルタ情報の表
Hash	この MAC アドレス エントリの鍵付きリストのハッシュキー / 相対位置
Len	このハッシュチェーンの開始要素へのこのエントリの長さ
Address	正準（イーサネット順の）MAC アドレス
Matches	この MAC アドレスに一致した受信パケットの数
Routed protocols on...	指定したインターフェイスに対して設定されたルーテッドプロトコルの一覧
Bridged protocols on...	指定したインターフェイスに対して設定されたブリッジドプロトコルの一覧





## VRF Lite の設定

---

この章では、ML シリーズ カードの VPN ( 仮想私設網 ) Routing and Forwarding Lite ( VRF Lite ) の設定方法について説明します。この章で使用する Cisco IOS コマンドの詳細については、『*Cisco IOS Command Reference*』を参照してください。この章の内容は次のとおりです。

- [VRF Lite の概要 \( p.13-2 \)](#)
- [VRF Lite の設定 \( p.13-3 \)](#)
- [VRF Lite の設定例 \( p.13-4 \)](#)
- [VRF Lite のモニタリングと確認 \( p.13-9 \)](#)



**(注)** ブリッジングをすでに設定している場合は、任意の手順である VRF Lite の設定に進むことができます。

---

## VRF Lite の概要

VRF は、複数のルーティング インスタンスを提供する IP ルーティングの拡張機能です。VRF は、各 VPN に個別の IP ルーティング テーブルと転送テーブルを提供します。また、Provider Equipment (PE) のルータ間で Multi-Protocol internal BGP (MP-iBGP) とともに使用し、レイヤ 3 MPLS-VPN を提供します。ただし、ML シリーズの VRF 実装では、MP-iBGP は含まれていません。VRF Lite を使用した場合、ML シリーズは PE 拡張機能または Customer Equipment (CE) 拡張機能とみなされます。VRF Lite が PE 拡張機能とみなされるのは、VRF を持つためです (MP-iBGP は備えていません)。また、CE 拡張機能ともみなされるのは、この CE は複数の VRF を持ち、1 台の CE ボックスで多数のカスタマーに対応できるためです。

VRF Lite を使用すると、ML シリーズの CE は、さまざまなカスタマーを対象に、PE とのインターフェイスおよびサブインターフェイスを複数持つことができます (通常の CE が対象にするのは 1 カスタマーのみ)。CE は VRF (ルーティング情報) をローカルで保持し、接続されている PE に VRF を配信することはありません。CE はカスタマーのルータまたは Internet Service Provider (ISP; インターネット サービス プロバイダー) PE のルータからトラフィックを受信すると、VRF 情報を使用して、適切なインターフェイスやサブインターフェイスにトラフィックを直接送信します。

## VRF Lite の設定

VRF Lite を設定するには、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>ip vrf vrf-name</b>	VRF コンフィギュレーション モードを開始し、VRF 名を指定します。
ステップ 2	Router(config-vrf)# <b>rd route-distinguisher</b>	VPN Route Distinguisher (RD) を作成します。RD では、ルーティング テーブルおよび転送テーブルを作成し、VPN のデフォルトの RD を指定します。カスタマーの IPv4 プレフィックスの先頭に RD が追加されることで、VPN-IPv4 プレフィックスをグローバルに一意にします。  RD は、Autonomous System (AS; 自律システム) 番号と任意の数値で構成される ASN 関連 RD か、または IP アドレスと任意の数値で構成される IP アドレス相対 RD のどちらかです。  次のいずれかの形式で <i>route-distinguisher</i> を入力できます。  16 ビット AS 番号 : 32 ビット数値 たとえば、101:3  32 ビット IP アドレス : 16 ビット数値 たとえば、192.168.122.15:1
ステップ 3	Router(config-vrf)# <b>route-target {import   export   both} route-distinguisher</b>	指定した VRF に対する、インポートまたはエクスポート (またはその両方) ルートの対象コミュニティ一覧を作成します。
ステップ 4	Router(config-vrf)# <b>import map route-map</b>	(任意) 指定したルート マップを VRF に関連付けます。
ステップ 5	Router(config-vrf)# <b>exit</b>	現在の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	Router(config)# <b>interface type number</b>	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 7	Router(config-vrf)# <b>ip vrf forwarding vrf-name</b>	インターフェイスまたはサブインターフェイスに VRF を関連付けます。
ステップ 8	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 9	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM (不揮発性 RAM) に保存します。

例 13-1 は、VRF の設定例を示しています。この例では、VRF 名は `customer_a`、RD は `1:1`、インターフェイス タイプはファストイーサネット `0.1` 番です。

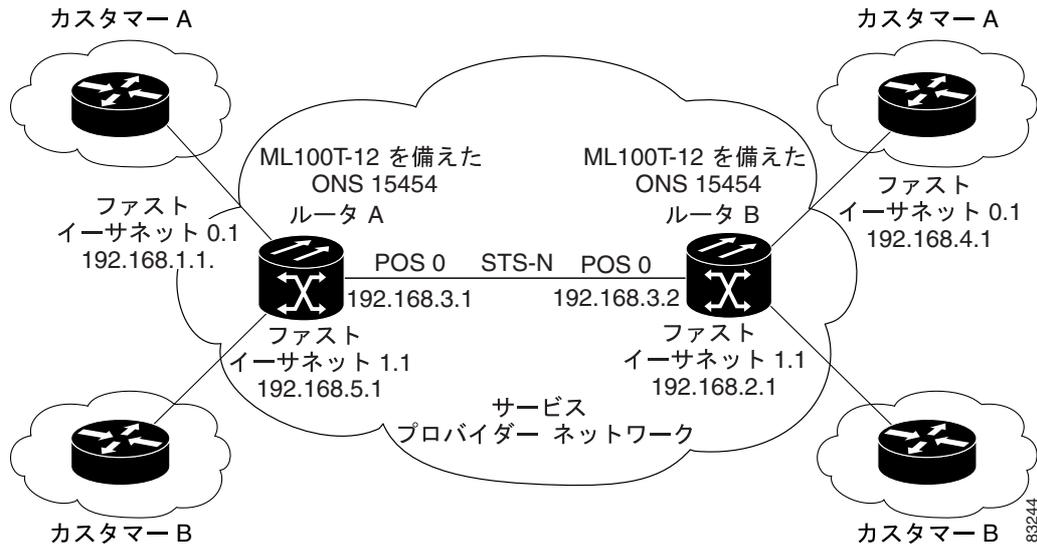
### 例 13-1 VRF の設定

```
Router(config)# ip vrf customer_a
Router(config-vrf)# rd 1:1
Router(config-vrf)# route-target both 1:1
Router(config)# interface fastEthernet 0.1
Router(config-subif)# ip vrf forwarding customer_a
```

## VRF Lite の設定例

図 13-1 に、VRF Lite の設定例を示します。ルータ A とルータ B の設定は、例 13-2 および例 13-3 でそれぞれ説明しています。関連付けられているルーティング テーブルは、例 13-4 ~ 例 13-9 に示しています。

図 13-1 VRF Lite ネットワーク シナリオ例



例 13-2 ルータ\_A の設定

```
hostname Router_A
!
ip vrf customer_a
 rd 1:1
  route-target export 1:1
  route-target import 1:1
!
ip vrf customer_b
 rd 2:2
  route-target export 2:2
  route-target import 2:2
!
bridge 1 protocol ieee
bridge 2 protocol ieee
bridge 3 protocol ieee
!
!
interface FastEthernet0
 no ip address
!
interface FastEthernet0.1
 encapsulation dot1q 2
 ip vrf forwarding customer_a
 ip address 192.168.1.1 255.255.255.0
 bridge-group 2
!
interface FastEthernet1
 no ip address
!
interface FastEthernet1.1
```

```
encapsulation dot1Q 3
ip vrf forwarding customer_b
ip address 192.168.2.1 255.255.255.0
bridge-group 3
!
interface POS0
no ip address
crc 32
no cdp enable
pos flag c2 1
!
interface POS0.1
encapsulation dot1Q 1 native
ip address 192.168.50.1 255.255.255.0
bridge-group 1
!
interface POS0.2
encapsulation dot1Q 2
ip vrf forwarding customer_a
ip address 192.168.100.1 255.255.255.0
bridge-group 2
!
interface POS0.3
encapsulation dot1Q 3
ip vrf forwarding customer_b
ip address 192.168.200.1 255.255.255.0
bridge-group 3
!
router ospf 1
log-adjacency-changes
network 192.168.50.0 0.0.0.255 area 0
!
router ospf 2 vrf customer_a
log-adjacency-changes
network 192.168.1.0 0.0.0.255 area 0
network 192.168.100.0 0.0.0.255 area 0
!
router ospf 3 vrf customer_b
log-adjacency-changes
network 192.168.2.0 0.0.0.255 area 0
network 192.168.200.0 0.0.0.255 area 0
!
```

## 例 13-3 ルータ\_B の設定

```

hostname Router_B
!
ip vrf customer_a
rd 1:1
  route-target export 1:1
  route-target import 1:1
!
ip vrf customer_b
rd 2:2
  route-target export 2:2
  route-target import 2:2
!
bridge 1 protocol ieee
bridge 2 protocol ieee
bridge 3 protocol ieee
!
!
interface FastEthernet0
  no ip address
!
interface FastEthernet0.1
  encapsulation dot1Q 2
  ip vrf forwarding customer_a
  ip address 192.168.4.1 255.255.255.0
  bridge-group 2
!
interface FastEthernet1
  no ip address
!
interface FastEthernet1.1
  encapsulation dot1Q 3
  ip vrf forwarding customer_b
  ip address 192.168.5.1 255.255.255.0
  bridge-group 3
!
interface POS0
  no ip address
  crc 32
  no cdp enable
  pos flag c2 1
!
interface POS0.1
  encapsulation dot1Q 1 native
  ip address 192.168.50.2 255.255.255.0
  bridge-group 1
!
interface POS0.2
  encapsulation dot1Q 2
  ip vrf forwarding customer_a
  ip address 192.168.100.2 255.255.255.0
  bridge-group 2
!
interface POS0.3
  encapsulation dot1Q 3
  ip vrf forwarding customer_b
  ip address 192.168.200.2 255.255.255.0
  bridge-group 3
!
router ospf 1
  log-adjacency-changes
  network 192.168.50.0 0.0.0.255 area 0
!
router ospf 2 vrf customer_a
  log-adjacency-changes
  network 192.168.4.0 0.0.0.255 area 0
  network 192.168.100.0 0.0.0.255 area 0
!

```

```

router ospf 3 vrf customer_b
  log-adjacency-changes
  network 192.168.5.0 0.0.0.255 area 0
  network 192.168.200.0 0.0.0.255 area 0
!
```

### 例 13-4 ルータ\_A のグローバルルーティングテーブル

```

Router_A# sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.50.0/24 is directly connected, POS0.1
```

### 例 13-5 ルータ\_A の customer\_a VRF ルーティングテーブル

```

Router_A# show ip route vrf customer_a
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

O    192.168.4.0/24 [110/2] via 192.168.100.2, 00:15:35, POS0.2
C    192.168.1.0/24 is directly connected, FastEthernet0.1
C    192.168.100.0/24 is directly connected, POS0.2
```

### 例 13-6 ルータ\_A の customer\_b VRF ルーティングテーブル

```

Router_A# show ip route vrf customer_b
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.200.0/24 is directly connected, POS0.3
O    192.168.5.0/24 [110/2] via 192.168.200.2, 00:10:32, POS0.3
C    192.168.2.0/24 is directly connected, FastEthernet1.1
```

**例 13-7 ルータ\_B のグローバルルーティングテーブル**

```
Router_B# sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.50.0/24 is directly connected, POS0.1
```

**例 13-8 ルータ\_B の customer\_a VRF ルーティングテーブル**

```
Router_B# sh ip route vrf customer_a
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.4.0/24 is directly connected, FastEthernet0.1
O    192.168.1.0/24 [110/2] via 192.168.100.1, 00:56:24, POS0.2
C    192.168.100.0/24 is directly connected, POS0.2
```

**例 13-9 ルータ\_B の customer\_b VRF ルーティングテーブル**

```
Router_B# show ip route vrf customer_b
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.200.0/24 is directly connected, POS0.3
C    192.168.5.0/24 is directly connected, FastEthernet1.1
O    192.168.2.0/24 [110/2] via 192.168.200.1, 00:10:51, POS0.3
```

## VRF Lite のモニタリングと確認

表 13-1 に、VRF Lite のモニタリングおよび確認に使用するイネーブル EXEC コマンドを示します。

表 13-1 VRF Lite のモニタリングと確認に使用するコマンド

コマンドの説明	目的
Router# <code>show ip vrf</code>	VRF とインターフェイスのセットを表示します。
Router# <code>show ip route vrf vrf-name</code>	VRF の IP ルーティングテーブルを表示します。
Router# <code>show ip protocols vrf vrf-name</code>	VRF のルーティング プロトコル情報を表示します。
Router# <code>ping vrf vrf-name ip ip-address</code>	特定の VRF を持つ IP アドレスの ping を実行します。





## QoS の設定

この章では、ML シリーズ カードに組み込まれている Quality of Service (QoS; サービス品質) 機能、およびシステム レベルとインターフェイス レベルの両方で QoS スケジューリングをマップする方法について説明します。

この章の内容は次のとおりです。

- [QoS の概要 \( p.14-2 \)](#)
- [ML シリーズの QoS \( p.14-4 \)](#)
- [RPR の QoS \( p.14-11 \)](#)
- [QoS の設定 \( p.14-13 \)](#)
- [QoS 設定のモニタリングおよび確認 \( p.14-19 \)](#)
- [QoS の設定例 \( p.14-20 \)](#)
- [マルチキャスト QoS およびプライオリティ マルチキャスト キューイングの概要 \( p.14-25 \)](#)
- [マルチキャスト プライオリティ キューイング QoS の設定 \( p.14-27 \)](#)
- [CoS ベース パケットの統計情報の概要 \( p.14-28 \)](#)
- [CoS ベース パケット統計情報の設定 \( p.14-29 \)](#)
- [IP SLA の概要 \( p.14-31 \)](#)

ML シリーズ カードでは、Cisco IOS の Modular QoS CLI (MQC; モジュラ QoS コマンドライン インターフェイス) を使用します。MQC の一般的な設定の詳細については、次の Cisco IOS のマニュアルを参照してください。

- 『Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.2』には、次の URL からアクセスできます。  
<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122mindx/122index.htm>
- 『Cisco IOS Quality of Service Solutions Command Reference, Release 12.2』には、次の URL からアクセスできます。  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos\\_r/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fqos_r/index.htm)

## QoS の概要

QoS は、サービス セットに対して重要度の低いサービスによる損害を受けないように、優先または特別な処理を行うネットワークの機能です。ML シリーズ カードでは、QoS を使用して、SONET/SDH 回線に多重化されている各サービスに対して動的に伝送帯域幅を割り当てています。QoS によって、ML シリーズ カードを設定して各サービスに個別の処理レベルを提供できます。各レベルは、損失や遅延を含めて、帯域幅のサービス要素によって定義されます。Service-Level Agreement (SLA; サービス レベル契約) は、これらのサービス要素の保証されたレベルのことで、

QoS メカニズムには、3 つの基本的なステップがあります。トラフィックのタイプを分類し、それぞれのタイプに対応して実行するアクションを指定し、さらに、アクションを実行する場所を指定します。以降では、ML シリーズ カードがユニキャストトラフィックに対してこれらの手順をどのように実行するかを説明します。プライオリティ マルチキャストトラフィックと宛先アドレスが不明なトラフィックに対する QoS は、「[マルチキャスト QoS およびプライオリティ マルチキャスト キューイングの概要](#)」(p.14-25)で詳しく説明している別のメカニズムで処理します。

## IP およびイーサネットのプライオリティ メカニズム

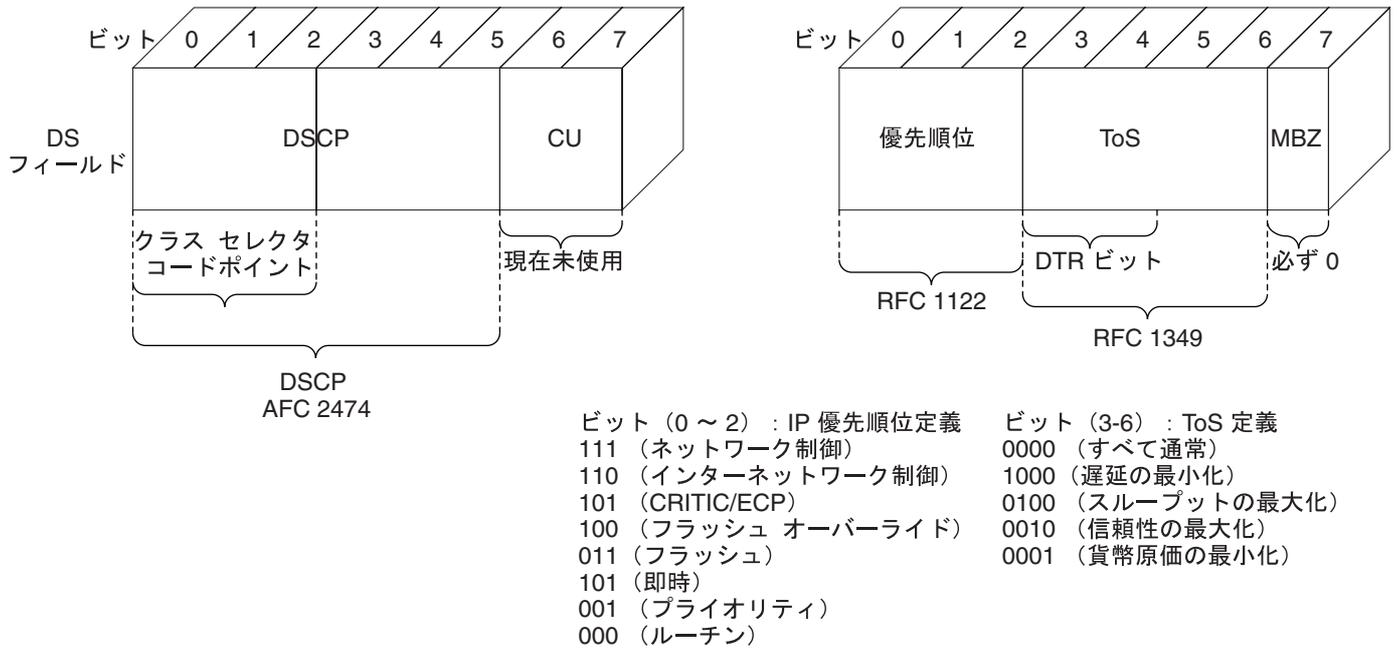
データに QoS を適用する場合、IP パケットまたはイーサネット フレームをマーキングまたは識別する方法が必要となります。識別ができると、特定のプライオリティを個々の IP パケットまたはイーサネット フレームに割り当てることができます。IP 優先順位または IP Differentiated Service Code Point (DSCP) フィールドは、IP パケットに優先順位を付けます。また、イーサネット フレームには、イーサネット Class of Service (CoS; サービス クラス) (IEEE 802.1p で定義された CoS) が使用されます。以降で、IP 優先順位とイーサネット CoS の詳細について説明します。

## IP 優先順位および DSCP

IP 優先順位は、IPv4 ヘッダーの Type of Service (ToS; サービス タイプ) フィールドの 3 ビットの優先順位ビットを使用して、各 IP パケットの CoS を指定します (RFC 1122)。IPv4 ToS フィールドの最上位 3 ビットは、最大 8 つの別個のクラスを提供します。8 つのクラスのうち 6 つはサービスの分類に使用され、残りの 2 つは予約されています。ネットワーク エッジでは、クライアント装置またはルータによって IP 優先順位が割り当てられるため、後続の各ネットワーク要素は、順次、決定済みのポリシーまたは SLA に基づいてサービスを提供できます。

IP DSCP は IPv4 ヘッダーの 6 ビットを使用して、各 IP パケットの CoS を指定します (RFC 2474)。図 14-1 に、IP 優先順位と DSCP を示します。DSCP フィールドは、使用可能な 64 個のクラスのいずれかにパケットを分類します。ネットワーク エッジで、IP DSCP はクライアント装置またはルータによって割り当てられるため、後続の各ネットワーク要素は、決定済みのポリシーまたは SLA に基づいてサービスを提供できます。

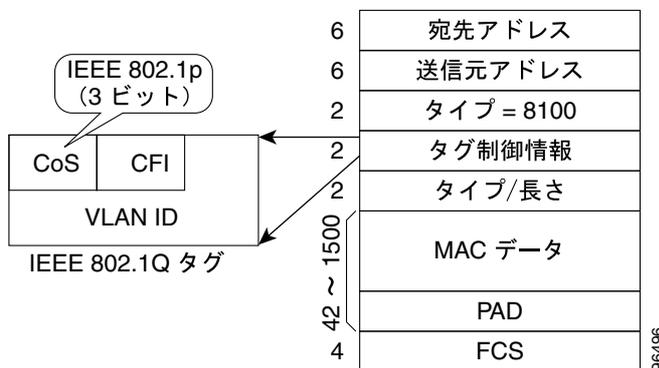
図 14-1 IP 優先順位と DSCP



## イーサネット CoS

イーサネット CoS は、4 バイトの IEEE 802.1Q (VLAN [仮想 LAN]) ヘッダー内の 3 ビットを参照して、イーサネット フレームがスイッチド ネットワークを通過する際にフレームのプライオリティを指示します。IEEE 802.1Q ヘッダーの CoS ビットは、一般に IEEE 802.1p ビットと呼ばれます。3 ビットの CoS ビットは、8 つのクラスを提供します。これは IP 優先順位によって提供される数と一致しています。実際に多くのネットワークでは、パケットはレイヤ 2 とレイヤ 3 の両方のドメインを経由する場合があります。ネットワークでの QoS を維持するために、IP ToS をイーサネット CoS にマップすることも、逆にイーサネット CoS を IP ToS にマップすることもできます (リニア マッピングや 1 対 1 マッピングなど)。これは、それぞれのメカニズムで 8 つのクラスをサポートしているためです。同様に、一連の DSCP 値 (64 クラス) は、8 つの各イーサネット CoS 値にマップできます。図 14-2 に、イーサネット プロトコル ヘッダーで 2 バイトの Ethertype と 2 バイトのタグ (IEEE 802.1Q タグ) で構成された IEEE 802.1Q イーサネット フレームを示します。

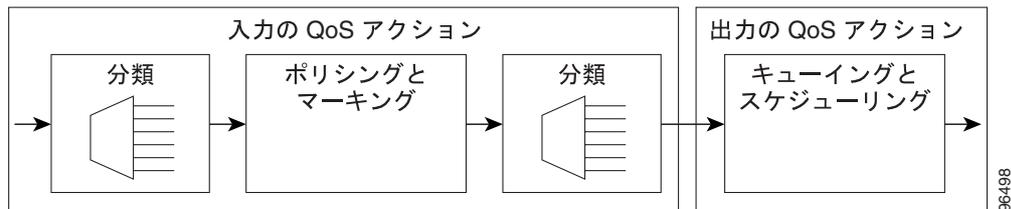
図 14-2 イーサネットフレームと CoS ビット (IEEE 802.1p)



## ML シリーズの QoS

ML シリーズの QoS は、入力インターフェイス、ブリッジグループ (VLAN)、イーサネット CoS、IP 優先順位、IP DSCP、または Resilient Packet Ring (RPR; 復元パケット リング)-CoS に基づいて、ネットワーク内の各パケットを分類します。パケットがクラスフローに分類されたあと、パケットがカードを経由する際に各パケットに詳細な QoS 機能を適用できます。図 14-3 に、ML シリーズの QoS フローを示します。

図 14-3 ML シリーズの QoS フロー



ML シリーズカードが提供するポリシングによって、接続装置は事前定義された帯域幅量 (レート制限) を超えてネットワークに送信しないことが保証されます。ポリシング機能を使用すると、インターフェイスでカスタマーに使用可能な Committed Information Rate (CIR; 認定情報速度) と Peak Information Rate (PIR; 最大情報速度) を実行できます。また、ポリシングは、ネットワークに許容されている情報の統計的特性を把握するのに役立ちます。これに基づきトラフィック エンジニアリングの観点から、コミットされる帯域幅の量がネットワークで使用可能なこと、ネットワークに適切な比率で最大帯域幅をオーバーサブスクライブすることが、より効果的に保証できるようになります。ポリシングアクションは分類別に適用されます。

プライオリティ マーキングは、イーサネット IEEE 802.1p CoS ビットまたは RPR-CoS ビットを ML シリーズカードから送出するときに設定できます。マーキング機能は、外側の IEEE 802.1p タグで動作し、QinQ パケットの着信時にパケットにタグ付けするメカニズムを提供します。この Service Provider (SP; サービス プロバイダー) で作成された QoS インジケータだけに基いて、後続のネットワーク要素は QoS を提供できます。

クラス別フロー キューイングによって、超過ネットワーク帯域幅へのアクセスを適正化し、帯域幅を割り当てて SLA をサポートできるほか、ネットワーク リソースを多く必要とするアプリケーションにも十分に対応できます。バッファは、共有リソース プールからキューに動的に割り当てられます。割り当てプロセスには、迅速なシステム ロードと各キューへの帯域幅の割り当てが含まれています。このプロセスによって、バッファ割り当てが最適化されます。ML シリーズの輻輳管理は、出力スケジューラの廃棄適性に加え、テールドロップ メカニズムを通じて行われます。

ML シリーズでは、Weighted Deficit Round Robin (WDRR) スケジューリング プロセスを使用して、超過帯域幅へのアクセスを適正化するとともに、各クラスフローのスルーットを保証します。

アドミッション制御は、ML シリーズカードでサービスが設定されるたびに起動するプロセスで、QoS リソースが過度にコミットされていないかどうかを確認します。特に、アドミッション制御は、インターフェイス上でコミットされる帯域幅の合計がインターフェイスの総帯域幅を上回る場合、設定を受け入れないようにします。

## 分類

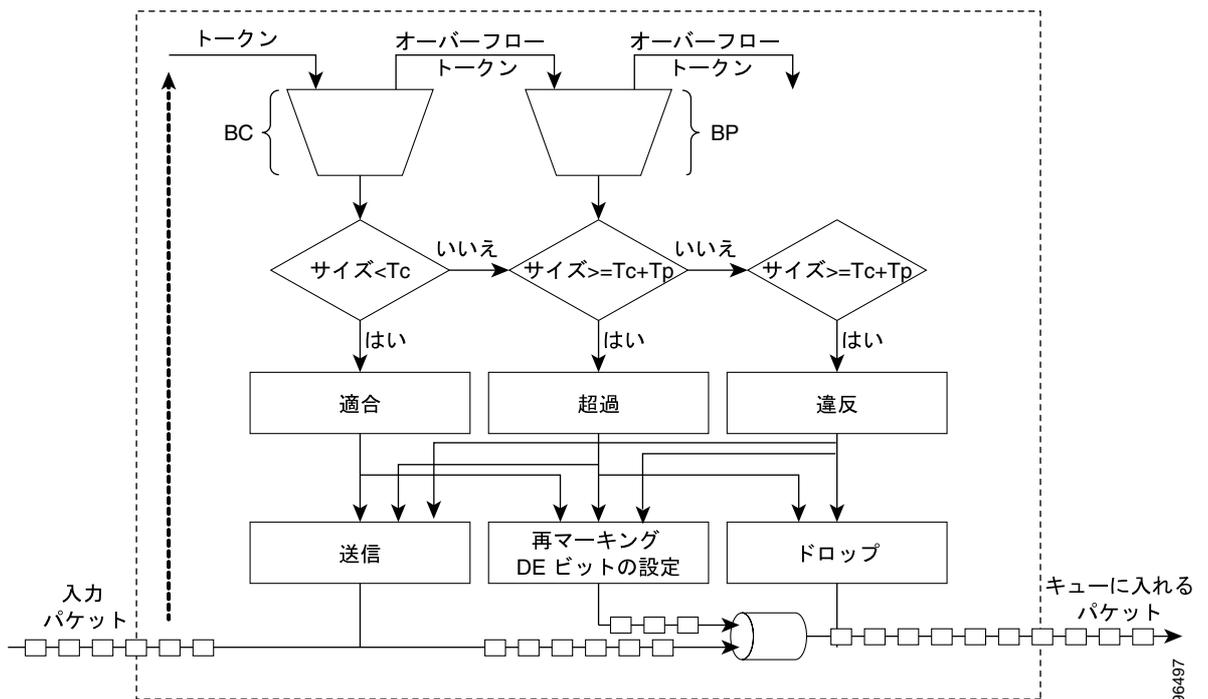
分類は、単一の packets 分類基準または分類基準の組み合わせ (論理 AND と OR) に基づいて行うことができます。カードに定義できるクラスの総数は 254 個です (デフォルト クラスは含まれません)。Packets の分類は、モジュラ CLI の `class-map` コマンドを使用して設定します。RPR を経由するトラフィックに対して、入力インターフェイスと RPR-CoS のいずれかまたは両方を分類基準として使用できます。

## ポリシング

デュアル漏出パケット ポリシング機能は、既知のレート (CIR) で 1 つめのパケット (CIR パケット) がトークンで満杯になった場合のプロセスです。CIR はオペレータが設定できるパラメータです。図 14-4 に、デュアル漏出パケット ポリシング機能モデルを示します。トークンは最大レベル (ポリシング機能での Burstable Committed [BC; パースト可能認定] トラフィック量) までパケットを満たします。1 つめのパケットの非適合パケットは、オーバーフローパケットです。これらのパケットは、2 つめの漏出パケット (PIR パケット) に渡されます。既知のレート (PIR) で 2 つめの漏出パケットがこれらのトークンで満杯になります。PIR は、オペレータが設定できるパラメータです。トークンは最大レベル (BP) まで PIR パケットを満たします。BP は、ポリシング機能での最大パースト可能トラフィック量です。2 つめのパケットの非適合パケットは、オーバーフローパケットです。これらのパケットはポリシング機能の定義によって廃棄またはマーキングできます。

デュアル漏出パケット ポリシング機能では、CIR に適合するパケットは適合パケットであり、CIR に適合せず PIR に適合するパケットは超過パケットです。また、PIR と CIR のどちらにも適合しないパケットは違反パケットです。

図 14-4 デュアル漏出パケット ポリシング機能モデル



## ポリシング機能によるマーキングおよび廃棄

ML シリーズ カードのポリシング機能では、適合パケットを送信することも、マーキングして送信することもできます。超過パケットは、送信、マーキングして送信、または廃棄できます。違反パケットは、送信、マーキングして送信、または廃棄できます。デュアルレート ポリシング機能または 3 種ポリシング機能の主な用途は、適合パケットを CoS ビット 21 でマーキング、および超過パケットを CoS ビット 1 でマーキング、違反パケットの廃棄です。そのため、後続のネットワーク装置は、各 SLA を認識せずに、これらのプライオリティ マーキングに基づいてフレームまたはパケット単位で適切な QoS 処理を適用できます。

場合によっては、特定の入力クラスのトラフィックをすべて廃棄することが望ましい場合があります。トラフィックの廃棄は、`police 96000 conform-action drop exceed-action drop` という形式で、クラスを指定した `police` コマンドを使用することで行えます。

送信前に、マーキングされたパケットにプロバイダー提供の Q タグが挿入されている場合、マーキングはプロバイダー Q タグだけに影響します。Q タグを受信すると、その Q タグは再度マーキングされます。マーキングされたパケットが RPR リング上で転送されると、マーキングは RPR-CoS ビットにも影響を与えます。

Q タグが挿入されると (QinQ)、マーキングは追加された Q タグに影響を与えます。Q タグが含まれる入力パケットが透過的にスイッチングされると、既存の Q タグがマーキングされます。パケットに Q タグが含まれていない場合は、マーキングは特に意味を持ちません。

ローカル スケジューラは、CoS 設定やグローバル CoS コミット定義には関係なく、すべての非適合パケットを廃棄可能として処理します。RPR 実装の場合、Discard Eligible (DE; 廃棄適性) パケットは、RPR ヘッダーの DE ビットを使用してマーキングされます。CoS コミットまたはポリシングアクションに基づく廃棄適性は、ML シリーズ カード スケジューラに対してローカルですが、RPR リングに対してはグローバルです。

## キューイング

ML シリーズ カードのキューイングでは、共有バッファ プールを使用してさまざまなトラフィック キューにメモリを動的に割り当てます。ML シリーズ カードが使用するバッファ プールの総量は 12 MB メモリです。イーサネット ポートが 6 MB のメモリを共有し、Packet-over-SONET/SDH (POS) ポートが残りの 6 MB を共有します。メモリ スペースの割り当ては、1500 バイトずつ増加します。

各キューには、キューのクラス帯域幅割り当ておよび設定されているキューの数に基づいて、割り当てられるバッファ数に上限があります。通常、この上限は共有バッファ容量の 30 ~ 50 % です。各キューへの動的バッファ割り当ては、追加のバッファリングを必要とするキューの数に基づいて減らすことができます。動的割り当てメカニズムは、サービス コミットメントに応じて適正化を図るとともに、システムトラフィック負荷の範囲全体でシステム スループットを最適化します。

Low Latency Queue (LLQ; 低遅延キュー) は、重みを無限大に設定するか、または 100 % 帯域幅をコミットして定義されます。LLQ を定義するときには、その特定クラスの入口でポリシング機能を定義し、LLQ が使用する最大帯域幅を制限する必要があります。そうしないと、LLQ が帯域幅全体を占有し、他のユニキャスト キューが帯域幅を使用できなくなる恐れがあります。

ML シリーズでは、ユーザ定義可能な 400 個のキューをサポートしています。これらのキューは、分類および帯域幅割り当て定義に従って割り当てられます。スケジューリングに使用する分類では、ポリシングアクションのあとにフレームおよびパケットを分類するので、ポリシング機能を入力フレームおよびパケットの CoS ビットのマーキングや変更を使用する場合、新しい値をキューイングおよびスケジューリング用のトラフィックの分類に適用できます。ML シリーズでは、4000 個のパケットのバッファリングが可能です。

## スケジューリング

スケジューリングは、WDRR を実行する一連のスケジューラと、各出力ポートに関連付けられているキューに入れられたトラフィックのプライオリティ スケジューリング メカニズムによって行われます。

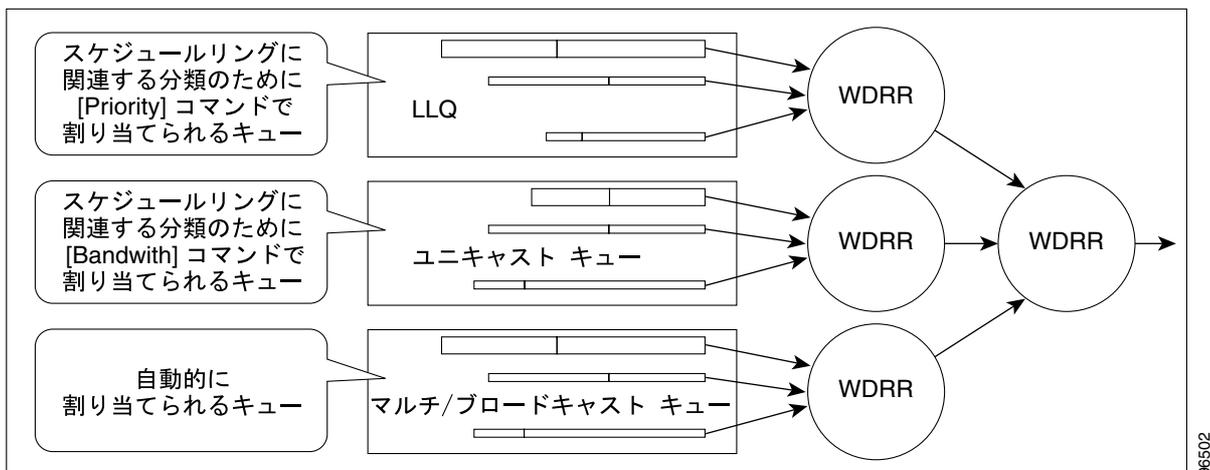
キューの通常のラウンド ロビン サービスは定期的に行われますが、異なるキューでさまざまなパケット サイズを使用すると不均等が生じます。この問題は、Deficit Round Robin ( DRR ) スケジューリングによって解決されます。パケット サイズが大きすぎたために、前回のラウンドでキューがパケットを送信できなかった場合、各ラウンドでキューに入る前回のクレジット量の剰余 ( 量子 ) は、次のラウンドの量子に追加されます。

WDRR は、DRR の量子の概念を拡張し、各キューのスループットに重み付けします。キューごとに異なる重みが設定されており、ラウンドの各キューに割り当てられた量子は、そのスケジューラが処理するすべてのキューにおけるキューの相対重みに比例します。

サービス プロビジョニング プロセスの結果として、重みが各キューに割り当てられます。ポリシーとポリシー マッピング プロビジョニングを組み合わせると、このような重みと WDRR スケジューリング プロセスによって、QoS コミットメントが各サービス フローに確実に提供されるようになります。

図 14-5 に、ML シリーズ カードのキューイングとスケジューリングを示します。

図 14-5 キューイングおよびスケジューリング モデル



重み付け構造によって、トラフィックを 1/2048 のポート レートでスケジューリングできます。これは、ギガビット イーサネット ポートを出るトラフィックでは約 488 Kbps、OC-12c ポートから出るトラフィックでは約 293 Kbps、ファスト イーサネット ポートを出るトラフィックでは約 49 Kbps に相当します。

ユニキャスト キューは、出力ポートの出力サービス ポリシー実装として作成されます。各ユニキャスト キューには、コミット済み帯域幅が割り当てられ、キューの重みはそのポート用に定義されているすべてのユニキャスト キューのコミット済み帯域幅の正規化によって決定されます。どのキューでもコミット済み帯域幅を超えるトラフィックは、キューの相対重みに従ってスケジューラで処理されます。

LLQ は、出力ポートの出力サービス ポリシー実装として作成されます。各 LLQ キューは、100 % のコミット済み帯域幅が割り当てられ、低遅延で処理されます。LLQ による帯域幅の使用を制限するには、LLQ トラフィック クラスの入口で厳格なポリシング機能を実装する必要があります。

DE を使用すると、あるパケットはコミット済みとして処理し、別のパケットはスケジューラで DE として処理できます。イーサネット フレームでは、RPR-CoS および DE ビットが RPR トラフィックに使用される場合に、CoS (IEEE 802.1p) ビットがコミット済みパケットと DE パケットの識別に使用されます。輻輳が発生し、キューが満杯になり始めると、DE パケットはコミット済みパケットよりも低いテールドロップ スレッショールドに達します。コミット済みパケットは、コミット済み負荷総量がインターフェイス出力を超えるまでは廃棄されません。あらゆる状況で均等性を保証しながら共有バッファ プールを最大限に使用できるように、カードのテールドロップ スレッショールドは動的に調整されます。

## 制御パケットと L2 トンネリング プロトコル

ML シリーズ カードで生成される制御パケットは、データ パケットよりも高いプライオリティが割り当てられます。外部レイヤ 2 およびレイヤ 3 制御パケットはデータ パケットとして処理され、ブロードキャストキューに割り当てられます。ML シリーズ カードの Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット) の優先順位付けでは、マルチキャストおよびブロードキャストキューに送信するトンネリングされたレイヤ 2 BPDU に、より高い廃棄値が与えられます。したがって、マルチキャストおよびブロードキャストキューの他のパケットよりもプライオリティは高くなります。レイヤ 2 トンネリング プロトコルのイーサネット CoS (IEEE 802.1p) は、ML シリーズ カードによって割り当てることができます。

## 出力プライオリティ マーキング

出力プライオリティ マーキングを使用すると、オペレータはカードを出るパケットの IEEE 802.1p CoS ビットを割り当てることができます。このマーキングにより、オペレータは、パケットに対して行う必要のある QoS 処理をダウンストリーム ノードにシグナリングするメカニズムとして、CoS ビットを使用することが可能になります。この機能は、最も外側の IEEE 802.1p CoS フィールドで動作します。プライオリティ マーキングを QinQ 機能と共に使用すると、ユーザトラフィック (内側の Q タグ) はネットワークを透過的に経由できるようになります。さらに、ネットワークがレイヤ 2 で QoS 処理を内部的にシグナリングする方法も提供できます。

プライオリティ マーキングは、分類プロセスのあとに行われます。したがって、以前に識別された分類条件のいずれかを基準として使用して、発信 IEEE 802.1p CoS フィールドを設定できます。たとえば、特定の CoS 値を特定のブリッジグループにマップできます。

プライオリティ マーキングは、MQC `set-cos` コマンドを使用して設定します。IEEE 802.1Q タグのないパケットが何らかの方法でカードを出たとすると、`set-cos` コマンドはそのパケットでは有効でなくなります。IEEE 802.1Q タグ (通常タグまたは QinQ タグ) がパケットに挿入されると、その挿入されたタグには `set-cos` プライオリティが設定されます。入力パケットに IEEE 802.1Q タグが存在し、出力パケットで保持されている場合、そのタグのプライオリティは変更されます。入力インターフェイスが QinQ アクセスポートであり、`set-cos` ポリシーマップが入力タグのプライオリティに基づいて分類を行う場合、これはユーザプライオリティに基づく分類となります。これは、ユーザタグのプライオリティによって、SP タグのプライオリティを決める 1 つの方法です。パケットが `set-cos` ポリシーマップに一致しないときには、保持されているタグのプライオリティは変更されず、挿入された IEEE 802.1Q タグのプライオリティはいずれも 0 に設定されます。

出力サービス ポリシーの `set-cos` コマンドは、ユニキャストトラフィックにだけ適用されます。マルチキャストおよびブロードキャストトラフィックのプライオリティ マーキングは、入力サービスポリシーに対するポリシングプロセスの `set-cos` アクション以外ではできません。

## 入カプライオリティ マーキング

入カプライオリティ マーキングは、ある 1 つのポートのすべての入カパケットに対して、または分類に一致するすべての入カパケットに対して、または測定されたレートに基づいて実行できます。ある 1 つの入カクラスのパケットすべてに対するマーキングは、`police 96000 conform-action set-cos-transmit exceed-action set-cos-transmit` ポリシング コマンドでも行うことができます。[class-default] だけを含むポリシー マップとともにこのコマンドを使用すると、すべての入カパケットがその値にマーキングされます。レートに基づくプライオリティ マーキングについては、「[ポリシング機能によるマーキングおよび廃棄](#)」(p.14-6)を参照してください。

## QinQ 実装

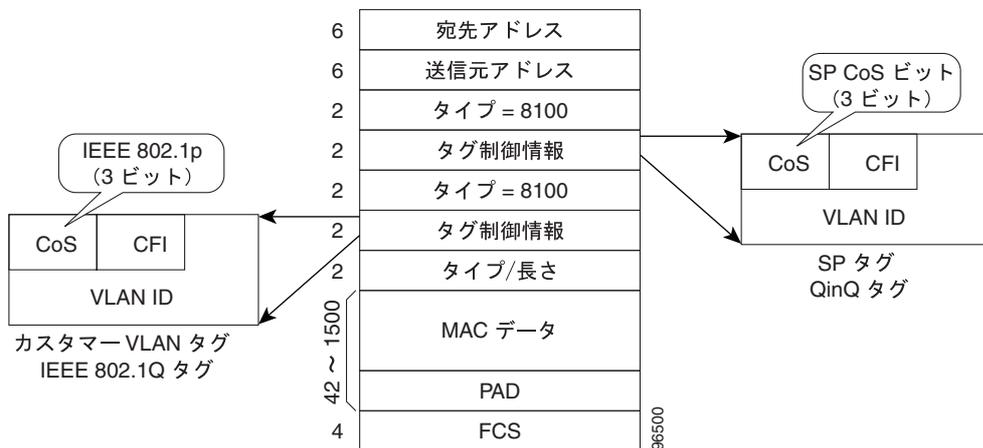
階層型 VLAN または IEEE 802.1Q トンネリング機能により、SP は特定のポート (UNI) から受信するカスタマー VLAN を透過的に伝送し、SP ネットワーク上で転送できます。この機能は QinQ とも呼ばれ、すべてのカスタマー フレームに IEEE 802.1Q タグを追加することによって実行されます。

QinQ 機能を使用すると、SP は複数の VLAN を設定しているカスタマーを 1 つの VLAN でサポートできます。QinQ はカスタマーの VLAN ID を保存するため、別のカスタマーからのトラフィックが元は同じ VLAN ID を共有していた場合でも、SP のインフラストラクチャ内でさまざまなカスタマーからのトラフィックを分離します。また、QinQ は、VLAN 内 VLAN 階層を使用してタグ付きパケットに再度タグ付けすることによって、VLAN スペースを拡張します。SP タグが追加されると、QinQ ネットワークでは通常、QinQ カプセル化フレームの IP ヘッダーまたはカスタマー イーサネット IEEE 802.1Q タグが認識できなくなります。

ML シリーズ カードでは、QinQ アクセス ポート (IEEE 802.1Q トンネル ポートまたは QinQ UNI ポート) は、カスタマーの CoS および IP precedence または IP DSCP 値を認識できます。したがって、SP タグにカスタマーの IP precedence、IP DSCP または CoS ビットを反映する適切な CoS ビットを割り当てることができます。QinQ ネットワークでは、QoS は SP タグの IEEE 802.1p ビットに基づいて実装されます。ML シリーズ カードは、パケットが二重にタグ付けされると、カスタマーの CoS、IP precedence、または DSCP 値を認識できません (パケットが QinQ サービスの送信ポイントを離れているため)。

図 14-6 に、ML シリーズ カードの QinQ 実装を示します。

図 14-6 QinQ



ML シリーズ カードは、QinQ ネットワークの IEEE 802.1Q トンネリング装置として使用できます。また、追加された QinQ タグの CoS ビットにカスタマー フレームの CoS ビットをコピーするオプションも用意されています。このようにして、SP の QinQ ネットワークは、個々のカスタマー フレームに必要な QoS 処理を完全に認識できます。

## フロー制御ポーズと QoS

インターフェイスでフロー制御とポートベース ポリシングが両方ともイネーブルな場合、フロー制御は帯域幅を処理します。ポリシング機能は、不適合フローを検出すると、インターフェイスのポリシング機能定義を使用して、パケットを廃棄またはマーク解除します。



(注) リンク集約を使用している場合は、ML シリーズ カード インターフェイスで QoS およびポリシングはサポートされません。



(注) 出力シェーピングは ML シリーズ カードではサポートされていません。

## RPR の QoS

RPR で VLAN ブリッジングを設定する場合、RPR および RPR QoS の基本設定でリング上のすべての ML シリーズ カードを設定する必要があります。SLA とブリッジングの設定は、IEEE 802.1Q の VLAN CoS が RPR CoS にコピーされるカスタマー RPR アクセス ポイントでのみ必要です。この IEEE 802.1Q の VLAN CoS のコピーは、`set-cos action` コマンドで上書きできます。CoS コミットルールは、RPR リングの入口で適用されます。

パケットに VLAN ヘッダーが含まれていない場合、次のルールを使用して、非 VLAN トラフィックの RPR CoS が設定されます。

1. デフォルトの CoS は 0 です。
2. CoS が割り当てられているパケットが着信すると、割り当てられている CoS はデフォルトに置き換えられます。IP パケットがローカルで生成されると、IP 優先順位設定は CoS 設定を置き換えます。
3. 入力ポリシー マップには、`set-cos` アクションが含まれます。
4. 出力ポリシー マップには、`set-cos` アクションが含まれます (ブロードキャストまたはマルチキャスト パケットを除く)。

RPR ヘッダーには、CoS 値と DE インジケータが格納されます。RPR DE は、コミットされていないトラフィックに対して設定されます。

ML シリーズ カード RPR 中継トラフィックは、POS ポートから RPR 周辺の POS ポートに発信するトラフィックとして定義され、レイヤ 2 CoS によってのみ分類できます。他の一致ルールは無視されます。これは、Cisco Metro Ethernet Solution の CoS ベース QoS モデル用に設計され、ML シリーズ カード専用実装した RPR の QoS です。

このレイヤ 2 の CoS 依存は、DSCP ベースの出力ポリシー マップが ML シリーズ カード上で RPR と正常に動作するのを妨げます。DSCP ベースのポリシーマップを使用すると、すべての中継トラフィックがクラス デフォルトとして不正に処理されます。これにより、中継ステーションで輻輳が発生したときに、DSCP プライオリティに関係なく、中継トラフィックが廃棄されます。

DSCP ベースの出力ポリシー マップの限界には対処法があります。各 RPR フレームには、独自の 3 ビットの CoS マーキングがあり、通常 VLAN COS からコピーされます。これは、中継 RPR トラフィック用に「match cos」分類が行われるフィールドです。入力ステーションの DSCP 一致に基づいて RPR COS をマーキングしてから、中継ステーションの RPR COS に基づいて分類できます。この方法は最大 8 つのクラスをサポートできます。9 つのクラス (class-default を含め) を使用する場合は、この対処法を使用するために 2 つのクラスを組み合わせる必要があります。

例 14-1 に、DSCP 限界を解決するクラスおよびポリシー マップ定義コンフィギュレーションを示します。Voice クラスと Call-Sig クラスを組み合わせることで、9 つのクラスを 8 つのクラスに変更する例も示します。



### 注意

「match cos 0」は、いずれのクラス マップの定義にも含めないでください。VLAN タグなしイーサネット パケットは、イーサネットからの入力ですべて COS 0 として処理されるからです。「match cos 0」を使用すると、イーサネットから着信するすべてのトラフィックとの一致が誤って行われます。

**例 14-1 DSCP 限界を解決するクラスおよびポリシー マップ定義コンフィギュレーション**

```
class-map match-any Bulk-Data
  match ip dscp af11
  match cos 3
class-map match-any Crit-Data
  match ip dscp af21 af31
  match cos 7
class-map match-any Net-Management
  match ip dscp cs2
  match cos 2
class-map match-any Video
  match ip dscp cs4 af41
  match cos 4
class-map match-any Voice
  description Includes Voice and Call Signalling
  match ip dscp ef
  match ip dscp cs3
  match cos 5
class-map match-any Routing
  match ip dscp cs6
  match cos 6
class-map match-any Scavenger
  match ip dscp cs1
  match cos 1
policy-map MAN-QoS-DSCP
  class Voice
    priority percent 4
    set cos 5
  class Bulk-Data
    bandwidth percent 20
    set cos 3
  class Crit-Data
    bandwidth percent 20
    set cos 7
  class Net-Management
    bandwidth percent 2
    set cos 2
  class Video
    bandwidth percent 5
    set cos 4
  class Routing
    bandwidth percent 2
    set cos 6
  class Scavenger
    bandwidth percent 1
    set cos 1
  class class-default
    bandwidth percent 45
    set cos 0
```

## QoS の設定

このセクションでは、MQC を使用して ML シリーズ カードの QoS 機能を設定するタスクについて説明します。ML シリーズ カードは、MQC の全機能をサポートするわけではありません。

クラスベースの QoS 機能を設定してイネーブルにするには、以降で説明する手順を実行します。

- [トラフィック クラスの作成 \(p.14-13\)](#)
- [トラフィック ポリシーの作成 \(p.14-14\)](#)
- [インターフェイスへのトラフィック ポリシーの適用 \(p.14-18\)](#)
- [CoS ベース QoS の設定 \(p.14-18\)](#)

QoS の設定例については、「[QoS の設定例](#)」(p.14-20)を参照してください。

### 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` グローバル コンフィギュレーション コマンドを使用します。`class-map` コマンドの構文は次のとおりです。

```
class-map [match-any | match-all] class-map-name
no class-map [match-any | match-all] class-map-name
```

`match-all` および `match-any` オプションは、トラフィック クラスに複数の一致条件が設定されている場合にのみ指定する必要があります。`class-map match-all` コマンドは、パケットが指定のトラフィック クラスに適合するために、トラフィック クラスのすべての一致条件が満たされる必要がある場合に使用します。`class-map match-any` コマンドは、パケットが指定のトラフィック クラスに適合するためには、トラフィック クラスの一致条件のうち 1 つだけが満たされる必要がある場合に使用します。`match-all` も `match-any` キーワードも指定されていない場合、トラフィック クラスは `class-map match-all` コマンドと同様に動作します。

一致条件を含むトラフィック クラスを作成するには、`class-map` 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トラフィック クラス名を指定し、必要に応じて表 14-1 の `match` コマンドを使用します。

表 14-1 トラフィック クラス コマンド

コマンドの説明	目的
Router(config)# <code>class-map class-map-name</code>	<p>トラフィック クラスのユーザ定義名を指定します。名前には、最大 40 文字の英数字を指定できます。<code>match-all</code> も <code>match-any</code> も指定しない場合、トラフィック クラスのメンバーとして分類するには、トラフィックがすべての一致条件を満たす必要があります。</p> <p>デフォルトの一致条件はありません。</p> <p>複数の一致条件がサポートされます。<code>class-map</code> コマンドの <code>match-all</code> および <code>match-any</code> サブコマンドによって制御されるとおり、コマンドは条件のすべてまたはいずれかを照合します。</p>
Router(config)# <code>class-map match-all class-map-name</code>	<p>トラフィック クラスに入るトラフィックを、トラフィック クラスのメンバーとして分類するには、すべての一致条件を満たす必要があることを指定します。</p>
Router(config)# <code>class-map match-any class-map-name</code>	<p>トラフィック クラスに入るトラフィックを、トラフィック クラスのメンバーとして分類するには、一致条件のいずれか 1 つを満たす必要があることを指定します。</p>
Router(config-cmap)# <code>match any</code>	<p>すべてのパケットを照合することを指定します。</p>

表 14-1 トラフィック クラス コマンド (続き)

コマンドの説明	目的
Router (config-cmap) # <b>match bridge-group</b> <i>bridge-group-number</i>	ブリッジグループ番号を指定します。パケットの内容はこのブリッジグループ番号に対して照合され、そのクラスに属するかどうかを判別されます。
Router (config-cmap) # <b>match cos</b> <i>cos-number</i>	CoS 値を指定します。パケットの内容はこの CoS 値に対して照合され、そのクラスに属するかどうかを判別されます。
Router (config-cmap) # <b>match input-interface</b> <i>interface-name</i>	一致条件として使用する入力インターフェイスの名前を指定します。パケットはこの一致条件に対して照合され、そのクラスに属するかどうかを判別されます。  RPR で使用する Shared Packet Ring ( SPR; 共有パケットリング) インターフェイスである SPR1 は、ML シリーズカードの有効なインターフェイス名です。SPR インターフェイスの詳細については、 <a href="#">第 17 章「RPR の設定」</a> を参照してください。  インターフェイスの INPUT (冗長) に適用する場合、 <b>input-interface</b> の選択は有効ではありません。
Router (config-cmap) # <b>match ip dscp</b> <i>ip-dscp-value</i>	一致条件として使用する最大 8 つの DSCP 値を指定します。各サービスコードポイントに指定できる値は、0 ~ 63 です。
Router (config-cmap) # <b>match ip precedence</b> <i>ip-precedence-value</i>	一致条件として使用する最大 8 つの IP 優先順位値を指定します。

## トラフィック ポリシーの作成

トラフィック ポリシーを設定するには、**policy-map** 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、トラフィック ポリシー名を指定し、以降に示すコンフィギュレーション コマンドを使用してトラフィック クラスを関連付けます。このトラフィック クラスは、**class-map** コマンドと 1 つ以上の QoS 機能で設定したものです。**class** コマンドを使用すると、トラフィック クラスはトラフィック ポリシーに関連付けられます。**class** コマンドは、ポリシーマップ コンフィギュレーション モードを開始してから発行する必要があります。トラフィック ポリシーの QoS ポリシーが定義されている場合、**class** コマンドを入力すると、自動的にポリシーマップ クラス コンフィギュレーション モードになります。

ポリシー マップの任意のクラスで、帯域幅またはプライオリティ アクションを使用するときには、**match-any** コマンドで定義され、そのポリシー マップに帯域幅またはプライオリティ アクションが設定されているクラスが存在している必要があります。これは、ある帯域幅が割り当てられたデフォルトクラスに、すべてのトラフィックを確実に分類できるようにするためです。そのクラスを使用することを予定していない場合や、デフォルトトラフィックに対して帯域幅を予約する必要がない場合には、最小帯域幅を割り当てることができます。

次の例は、ポリシーマップ クラス コンフィギュレーション モードのトラフィック ポリシーで適用できる QoS ポリシーの詳細です。

**policy-map** コマンドの構文は次のとおりです。

```
policy-map policy-name
no policy-map policy-name
```

**class** コマンドの構文は次のとおりです。

```
class class-map-name
no class class-map-name
```

一致条件を満たさないすべてのトラフィックは、デフォルトトラフィッククラスに属します。ユーザはデフォルトトラフィッククラスを設定できますが、削除することはできません。

トラフィックポリシーを作成するには、必要に応じて表 14-2 のコマンドを使用します。

表 14-2 トラフィックポリシー コマンド

コマンドの説明	目的
Router (config)# <b>policy-map</b> <i>policy-name</i>	設定するトラフィックポリシーの名前を指定します。名前には、最大 40 文字の英数字を指定できます。
Router (config-pmap)# <b>class</b> <i>class-map-name</i>	事前定義されたトラフィッククラスの名前を指定します。このクラスは、 <b>class-map</b> コマンドで設定したクラスであり、トラフィックをトラフィックポリシーに分類するために使用します。
Router (config-pmap)# <b>class</b> <b>class-default</b>	トラフィックポリシーの一部として作成するデフォルトクラスを指定します。
Router (config-pmap-c)# <b>bandwidth</b> { <i>bandwidth-kbps</i>   <b>percent</b> <i>percent</i> }	<p>輻輳時におけるトラフィッククラスへの最小帯域幅保証を指定します。最小帯域幅保証は、Kbps (キロビット / 秒) または使用可能帯域幅全体のパーセンテージで指定できます。</p> <p>ML シリーズカードでの有効な選択肢は次のとおりです。</p> <ul style="list-style-type: none"> <li>• Kbps で指定したレート</li> <li>• 使用可能帯域幅全体のパーセンテージ (1 ~ 100)</li> </ul> <p>1 つのポリシーマップに複数のクラスおよび帯域幅アクションが指定されている場合、帯域幅指定時に同じ選択肢を使用する必要があります (キロビットまたは %)。</p> <p> (注) <b>bandwidth</b> コマンドを使用すると、超過トラフィック (設定したコミットを超えるトラフィック) には、他のトラフィッククラスと比較してそのトラフィッククラスの相対的な帯域幅コミットメントに応じて、使用可能帯域幅が割り当てられます。同じコミットが設定された 2 つのクラスの超過トラフィックは、使用可能帯域幅に同等にアクセスできます。最小コミットが設定されたクラスの超過トラフィックには、高いコミットが設定されたクラスの超過帯域幅と比較して最小限の使用可能帯域幅だけが割り当てられます。</p> <p> (注) 実際に設定できる帯域幅 (Kbps または Mbps) はポートごとで、ML シリーズカードの設定によって異なります。show interface コマンドは、ポートの最大帯域幅を表示します (たとえば、BW 100000 キロビット)。インターフェイスに適用されたすべての帯域幅とプライオリティアクション、および cos priority-mcast 帯域幅の合計は、ポートの合計帯域幅を超えることはできません。</p>

表 14-2 トラフィック ポリシー コマンド (続き)

コマンドの説明	目的
<pre>Router (config-pmap-c)# police   cir-rate-bps normal-burst-byte   [max-burst-byte] [pir pir-rate-bps]   [conform-action {set-cos-transmit     transmit   drop}] [exceed-action   {set-cos-transmit   drop}] [violate-action   {set-cos-transmit   drop}]</pre>	<p>ポリシー マップが入力に適用されているときに、現在選択されているクラスのポリシング機能を定義します。ポリシングは、出口ではなく入口でのみサポートされています。</p> <ul style="list-style-type: none"> <li>• <i>cir-rate-bps</i> には、bps (ビット / 秒) で平均 CIR を指定します。指定できる範囲は 96000 ~ 800000000 です。</li> <li>• <i>normal-burst-byte</i> には、CIR のバースト サイズをバイトで指定します。指定できる範囲は 8000 ~ 64000 です。</li> <li>• (任意) <i>maximum-burst-byte</i> には、PIR のバーストをバイトで指定します。指定できる範囲は 8000 ~ 64000 です。</li> <li>• (任意) <i>pir-rate-bps</i> には、平均 PIR トラフィック レートを bps で指定します。指定できる範囲は 96000 ~ 800000000 です。</li> <li>• (任意) 適合アクション オプションは次のとおりです。       <ul style="list-style-type: none"> <li>- CoS プライオリティ値を設定して送信</li> <li>- パケットの送信 (デフォルト)</li> <li>- パケットの廃棄</li> </ul> </li> <li>• (任意) 超過アクション オプションは次のとおりです。       <ul style="list-style-type: none"> <li>- CoS 値を設定して送信</li> <li>- パケットの廃棄 (デフォルト)</li> </ul> </li> <li>• (任意) 違反アクションは、<i>pir</i> が設定された場合にのみ有効です。違反アクション オプションは次のとおりです。       <ul style="list-style-type: none"> <li>- CoS 値を設定して送信</li> <li>- パケットの廃棄 (デフォルト)</li> </ul> </li> </ul>

表 14-2 トラフィック ポリシー コマンド (続き)

コマンドの説明	目的
<pre>Router (config-pmap-c)# priority kbps</pre>	<p>現在選択しているクラスの低遅延キューイングを指定します。このコマンドは、出力にのみ適用できます。ポリシーマップを出力に適用している場合は、このクラスに対して完全プライオリティが設定された出力キューを作成します。有効なレート選択肢は、Kbps だけです。</p> <p> (注) priority コマンドは、デフォルトのクラスには適用されません。</p> <p> (注) プライオリティ アクションを使用すると、プライオリティ レートとして指定されたレートに関係なく、そのクラスのトラフィックには 100% の CIR が与えられます。他の帯域幅コミットメントをインターフェイスに確実に適合させるには、この出力クラスにトラフィックを配信する可能性があるすべてのインターフェイスの入力でポリシング機能を設定し、最大レートを指定したプライオリティ レートに制限する必要があります。</p> <p> (注) 実際に設定できる帯域幅 (Kbps または Mbps) はポートごとで、ML シリーズ カードの設定によって異なります。show interface コマンドは、ポートの最大帯域幅を表示します (たとえば、BW 100000 キロビット)。インターフェイスに適用されたすべての帯域幅とプライオリティ アクション、および cos priority-mcast 帯域幅の合計は、ポートの合計帯域幅を超えることはできません。</p>
<pre>Router (config-pmap-c)# set cos cos-value</pre>	<p>CoS 値またはパケットに関連付ける値を指定します。指定できる範囲は 0 ~ 7 です。</p> <p>このコマンドは、出力に適用したポリシーマップでのみ使用できます。このコマンドは、現在選択しているクラスの発信パケットに設定する VLAN CoS プライオリティを指定します。QinQ を使用する場合、最上位の VLAN タグがマーキングされます。発信パケットに VLAN タグがない場合、アクションは無効になります。このアクションは、ポリシング機能によって set-cos アクションが実行されたあとに、パケットに適用されます。したがって、ポリシング機能のアクションによって設定された CoS は上書きされます。</p> <p>パケットがポリシング機能によりマーキングされてインターフェイスから転送され、しかもインターフェイスにトラフィック クラスの set-cos アクションが割り当てられている場合、ポリシングアクションで指定された値は、IEEE 802.1p CoS フィールドの設定に優先します。</p> <p>このコマンドも、RPR インターフェイスで ML シリーズを出て行くパケットの RPR ヘッダーに CoS 値を設定します。</p>

## インターフェイスへのトラフィック ポリシーの適用

トラフィック ポリシーをインターフェイスに適用し、ポリシーを適用する必要がある方向（インターフェイスへの着信パケット、またはインターフェイスからの送信パケット）を指定するには、`service-policy` 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。指定した方向でインターフェイスに適用できるトラフィック ポリシーは1つだけです。

インターフェイスからトラフィック ポリシーを削除する場合は、このコマンドの `no` 形式を使用します。`service-policy` コマンドの構文は次のとおりです。

```
service-policy {input | output} policy-map-name
no service-policy {input | output} policy-map-name
```

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、グローバル コンフィギュレーション モードで、必要に応じて次のコマンドを使用します。

ステップ 1	Router(config)# <b>interface</b> interface-id	<p>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、ポリシー マップを適用するインターフェイスを指定します。</p> <p>有効なインターフェイスは、物理イーサネットと POS インターフェイスに制限されています。</p> <p> (注) ポリシー マップは、SPR インターフェイス、サブインターフェイス、ポート チャネル インターフェイス、または Bridge Group Virtual Interface (BVI; ブリッジ グループ仮想インターフェイス) には適用できません。</p>
ステップ 2	Router(config-if)# <b>service-policy output</b> policy-map-name	<p>インターフェイスの出力方向に適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 ポリシーは、そのインターフェイスを出るすべてのトラフィックを評価します。</p>
ステップ 3	Router(config-if)# <b>service-policy input</b> policy-map-name	<p>インターフェイスの入力方向に適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 ポリシーは、そのインターフェイスに入るすべてのトラフィックを評価します。</p>

## CoS ベース QoS の設定

`cos commit cos-value` グローバル コマンドを使用すると、ML シリーズ カードでネットワーク インターフェイスに着信するパケットの QoS 処理を、per-customer-queue ポリシング機能ではなく、添付されてくる CoS 値に従って行わせることができます。

CoS ベース QoS は、表 14-3 に示す 1 つの `cos commit cos-value` グローバル コマンドで実行できます。

表 14-3 CoS Commit コマンド

コマンドの説明	目的
Router(config)# <b>cos-commit</b> cos-value	CIR として <i>cos-value</i> 以上の CoS が設定された着信パケットと、DE としてこの値より小さい CoS が設定されたパケットにラベルを付けます。

## QoS 設定のモニタリングおよび確認

ML シリーズ カードの QoS を設定したあと、さまざまな `show` コマンドを使用して、クラス マップ およびポリシー マップの設定を表示できます。トラフィック クラスまたはトラフィック ポリシーに関する情報を表示するには、EXEC モードで、必要に応じて次のコマンドのいずれかを使用します。表 14-4 に、QoS ステータスに関連するコマンドを示します。

表 14-4 QoS ステータスに関するコマンド

コマンドの説明	目的
Router# <code>show class-map name</code>	ユーザ固有のトラフィック クラスの情報を表示します。
Router# <code>show policy-map</code>	設定されているすべてのトラフィック ポリシーを表示します。
Router# <code>show policy-map name</code>	ユーザ固有のポリシー マップを表示します。
Router# <code>show policy-map interface interface</code>	インターフェイスに適用されたすべての入力および出力ポリシーの設定を表示します。このコマンドによって表示される統計情報はサポートされていないため、0 が表示されます。

例 14-2 に、QoS コマンドの例を示します。

### 例 14-2 QoS ステータス コマンドの例

```
Router# show class-map
Class Map match-any class-default (id 0)
  Match any
Class Map match-all policer (id 2)
  Match ip precedence 0

Router# show policy-map
Policy Map police_f0
  class policer
    police 1000000 10000 conform-action transmit exceed-action drop

Router# show policy-map interface

FastEthernet0

  service-policy input: police_f0

    class-map: policer (match-all)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      match: ip precedence 0

    class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      match: any
        0 packets, 0 bytes
        5 minute rate 0 bps
```

## QoS の設定例

このセクションでは、特定のコマンドとネットワーク設定の例について説明します。

- [トラフィック クラスの定義例](#)
- [トラフィック ポリシーの作成例](#)
- [class-map match-any および class-map match-all コマンドの例](#)
- [match spr1 インターフェイスの例](#)
- [ML シリーズの VoIP の例](#)
- [ML シリーズのポリシングの例](#)
- [ML シリーズの CoS ベース QoS の例](#)

### トラフィック クラスの定義例

例 14-3 に、インターフェイス fastethernet0 への着信トラフィックと一致する class1 というクラスマップの作成方法を示します。

#### 例 14-3 クラス インターフェイス コマンドの例

```
Router(config)# class-map class1
Router(config-cmap)# match input-interface fastethernet0
```

例 14-4 に、IP precedence 値 5、6、7 が設定された着信トラフィックと一致する class2 というクラスマップの作成方法を示します。

#### 例 14-4 クラス IP precedence コマンドの例

```
Router(config)# class-map match-any class2
Router(config-cmap)# match ip precedence 5 6 7
```



(注)

この例の 5 6 7 のように、複数の値を指定する一致ルールが class-map に含まれている場合、class-map をデフォルトの match-all ではなく、match-any にする必要があります。match-any class-map を指定しないと、エラーメッセージが表示され、そのクラスは無視されます。サポートされている複数の値を使用できるコマンドは、`match cos`、`match ip precedence`、および `match ip dscp` です。

例 14-5 に、ブリッジグループ 1 に基づいた着信トラフィックと一致する class3 というクラスマップの作成方法を示します。

#### 例 14-5 クラス マップブリッジグループ コマンドの例

```
Router(config)# class-map class3
Router(config-cmap)# match bridge-group 1
```

### トラフィック ポリシーの作成例

例 14-6 では、policy1 というトラフィック ポリシーは、ポリシー仕様 (デフォルト クラスの帯域幅割り当て要求など) と、2 つの追加クラス (class1 および class2) を含むように定義されています。これらのクラスの一致条件は、トラフィック クラスで定義済みです。「[トラフィック クラスの作成](#)」(p.14-13)を参照してください。

### 例 14-6 トラフィック ポリシーの作成例

```
Router(config)# policy-map policy1
Router(config-pmap)# class class-default
Router(config-pmap-c)# bandwidth 1000
Router(config-pmap)# exit

Router(config-pmap)# class class1
Router(config-pmap-c)# bandwidth 3000
Router(config-pmap)# exit

Router(config-pmap)# class class2
Router(config-pmap-c)# bandwidth 2000
Router(config-pmap)# exit
```

## class-map match-any および class-map match-all コマンドの例

ここでは、class-map match-any コマンドと class-map match-all コマンドの違いについて説明します。match-any および match-all オプションは、複数の一致条件が存在するときに、パケットをどのように評価するかを決定します。パケットがトラフィック クラスのメンバーとみなされるためには、すべての一致条件 (match-all) または一致条件のいずれか 1 つ (match-any) を満たす必要があります。

例 14-7 に、class-map match-all コマンドを使用して設定したトラフィック クラスを示します。

### 例 14-7 class-map match-all コマンドの例

```
Router(config)# class-map match-all cisco1
Router(config-cmap)# match cos 1
Router(config-cmap)# match bridge-group 10
```

インターフェイスで設定された cisco1 というトラフィック クラスにパケットが到着すると、そのパケットが評価され、cos 1 および bridge-group 10 と一致するかどうかが判別されます。この両方の一致条件を満たしている場合、パケットはトラフィック クラス cisco1 に一致します。

cisco2 というトラフィック クラスでは、使用できる一致条件が見つかるまで、一致条件の評価が続けられます。パケットが評価され、まず cos 1 を一致条件として使用できるかどうか判別され、cos 1 が一致条件として使用できる場合、パケットはトラフィック クラス cisco2 と照合され、cos 1 が一致条件として使用できない場合、次に bridge-group 10 が一致条件として評価されます。各一致条件が評価され、パケットがその条件と一致するかどうか確認されます。一致に成功すると、パケットはトラフィック クラス cisco2 のメンバーとして分類されます。パケットが指定されたどの条件にも一致しない場合は、パケットはトラフィック クラスのメンバーとして分類されず。

class-map match-all コマンドでは、パケットが指定されたトラフィック クラスのメンバーとみなされるには、すべての一致条件を満たす必要があります (論理 AND 演算子)。この例では、cos 1 AND bridge-group 10 という条件に一致する必要があります。ただし、class-map match-any コマンドでパケットをトラフィック クラスのメンバーとして分類する場合は、1 つの一致条件だけが満たされる必要があります (論理 OR 演算子)。この例では、cos 1 OR bridge-group 10 OR ip dscp 5 という条件に一致する必要があります。

例 14-8 に、class-map match-any コマンドで設定されたトラフィック クラスを示します。

### 例 14-8 class-map match-any コマンドの例

```
Router(config)# class-map match-any cisco2
Router(config-cmap)# match cos 1
Router(config-cmap)# match bridge-group 10
Router(config-cmap)# match ip dscp 5
```

## match spr1 インターフェイスの例

例 14-9 では、class-map を定義するとき、SPR インターフェイスは `match input-interface CLI` に対するパラメータとして指定します。

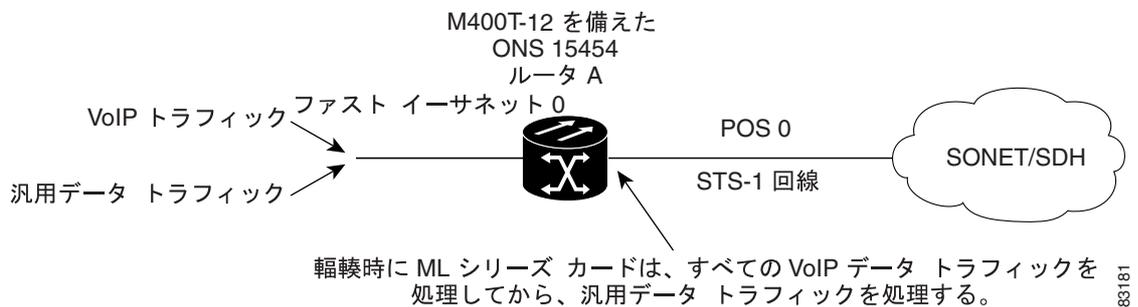
### 例 14-9 class-map SPR インターフェイス コマンドの例

```
Router(config)# class-map spr1-cos1
Router(config-cmap)# match input-interface spr1
Router(config-cmap)# match cos 1
Router(config-cmap)# end
Router# sh class-map spr1-cos1
Class Map match-all spr1-cos1 (id 3)
  Match input-interface SPR1
  Match cos 1
```

## ML シリーズの VoIP の例

図 14-7 に、ML シリーズ QoS の例を示します。関連するコマンドは、例 14-10 に示しています。

図 14-7 ML シリーズの VoIP の例



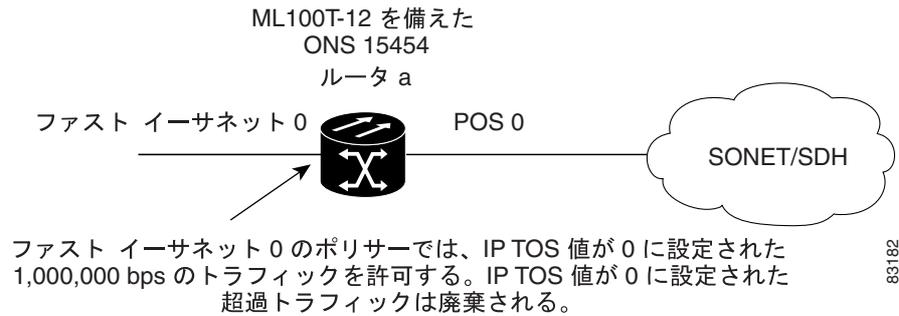
### 例 14-10 ML シリーズの VoIP コマンド

```
Router(config)# class-map match-all voip
Router(config-cmap)# match ip precedence 5
Router(config-cmap)# exit
Router(config)# class-map match-any default
Router(config-cmap)# match any
Router(config-cmap)# exit
Router(config)# policy-map pos0
Router(config-pmap)# class default
Router(config-pmap-c)# bandwidth 1000
Router(config-pmap-c)# class voip
Router(config-pmap-c)# priority 1000
Router(config-pmap-c)# interface FastEthernet0
Router(config-if)# ip address 1.1.1.1 255.255.255.0
Router(config-if)# interface POS0
Router(config-if)# ip address 2.1.1.1 255.255.255.0
Router(config-if)# service-policy output pos0
Router(config-if)# crc 32
Router(config-if)# no cdp enable
Router(config-if)# pos flag c2 1
```

## ML シリーズのポリシングの例

図 14-8 に、ML シリーズのポリシングの例を示します。この例では、0 ~ 1,000,000 bps の IP precedence でトラフィックを制限するポリシング機能の設定方法を示しています。関連するコードは、例 14-11 に示しています。

図 14-8 ML シリーズのポリシングの例



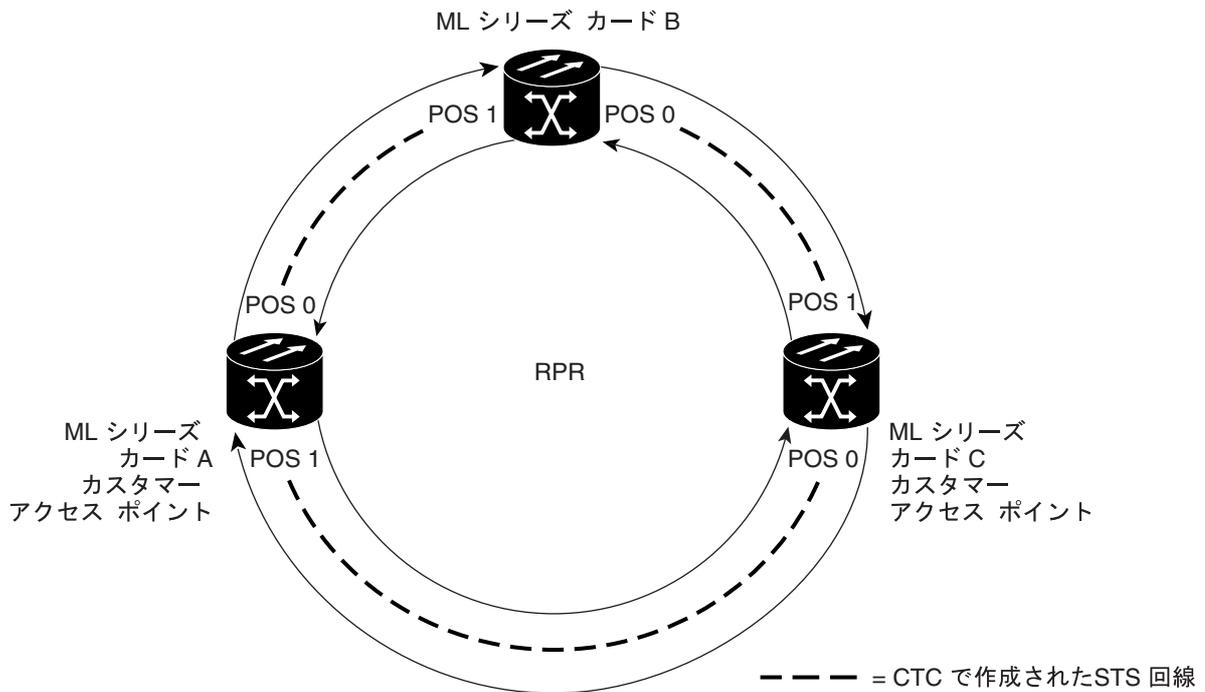
例 14-11 ML シリーズのポリシング コマンド

```
Router(config)# class-map match-all policer
Router(config-cmap)# match ip precedence 0
Router(config-cmap)# exit
Router(config)# policy-map police_f0
Router(config-pmap)# class policer
Router(config-pmap-c)# police 1000000 10000 conform-action transmit exceed-action drop
Router(config-pmap-c)# interface FastEthernet0
Router(config-if)# service-policy input police_f0
```

## ML シリーズの CoS ベース QoS の例

図 14-9 に、ML シリーズの CoS ベース QoS の例を示します。関連するコードは、図の次の例に示しています。CoS の例は、ML シリーズ カードが RPR に設定され、ML シリーズ カードの POS ポートがポイントツーポイント SONET 回線によってリンクされていることを前提としています。ML シリーズ カード A および ML シリーズ カード C は、カスタマー アクセス ポイントです。ML シリーズ カード B は、カスタマー アクセス ポイントではありません。RPR の設定方法の詳細については、第 17 章「RPR の設定」を参照してください。

図 14-9 ML シリーズの CoS の例



10596

例 14-12 に、図 14-9 の ML シリーズ カード A の設定に使用したコマンドを示します。

#### 例 14-12 ML シリーズ カード A の設定 (カスタマー アクセス ポイント)

```
ML_Series_A(config)# cos commit 2
ML_Series_A(config)# policy-map Fast5_in
ML_Series_A(config-pmap)# class class-default
ML_Series_A(config-pmap-c)# police 5000 8000 8000 pir 10000 conform-action
set-cos-transmit 2 exceed-action set-cos-transmit 1 violate-action drop
```

例 14-13 に、図 14-9 の ML シリーズ カード B の設定に使用したコマンドを示します。

#### 例 14-13 ML シリーズ カード B の設定 (非カスタマー アクセス ポイント)

```
ML_Series_B(config)# cos commit 2
```

例 14-14 に、図 14-9 の ML シリーズ カード C の設定に使用したコマンドを示します。

#### 例 14-14 ML シリーズ カード C の設定 (カスタマー アクセス ポイント)

```
ML_Series_B(config)# cos commit 2
ML_Series_B(config)# policy-map Fast5_in
ML_Series_B(config-pmap)# class class-default
ML_Series_B(config-pmap-c)# police 5000 8000 8000 pir 10000 conform-action
set-cos-transmit 2 exceed-action set-cos-transmit 1 violate-action drop
```

## マルチキャスト QoS およびプライオリティ マルチキャスト キューイングの概要

ML シリーズ カードの QoS は、デフォルトのマルチキャスト トラフィック クラスの他に、マルチキャスト トラフィック に対する 2 つのプライオリティ クラスの作成をサポートします。トラフィックのマルチキャスト プライオリティ キューイング クラスを作成することで、ML シリーズ カードがプライオリティ処理を行うために入力マルチキャスト トラフィック内の既存の CoS 値を認識するように設定します。

マルチキャスト プライオリティ キューイングの CoS 照合は、各パケットの「内部」CoS 値に基づいています。通常ではこの値は、出力 CoS 値 (ポリシング機能でマーキングがイネーブルの場合はマーキング後) と同じですが、2 つの状況においては異なります。dot1q トンネリングが使用された場合には、「内部」CoS 値は、出力値と異なります。dot1q トンネルでは、dot1q トンネルに入るときおよびトンネルから出るときに、内部 CoS 値は必ず外部タグ CoS の値となります。また、パケットが VLAN 上で転送され、VLAN タグが出口で削除されてパケットがタグなしで送信された場合にも、「内部」CoS 値は出力値と異なります。この場合、内部 CoS はタグが削除された CoS です (入力ポリシングとマーキングがイネーブルな場合には入力ポリシングとマーキングを含む)。

`cos priority-mcast` コマンドは、マルチキャスト パケットの CoS は変更せず、マルチキャスト プライオリティ キューイング クラスの帯域幅の割り当てだけ変更します。このコマンドにより帯域幅は最小となり、デフォルトのマルチキャストまたはブロードキャスト キューとは別にキューイングされます。

マルチキャスト プライオリティ キューイング クラスを作成することで、特定のタイプのマルチキャスト トラフィックで特別な処理を行うことができます。この処理は、マルチキャスト ビデオ配信および SP のマルチキャスト トラフィックの場合に特に有益です。たとえば、SP は SP 自身のマルチキャスト管理トラフィックを確実に保護する必要がある場合があります。保護するには、マルチキャスト管理トラフィックの CoS 値に対して、ML シリーズ カードでマルチキャスト プライオリティ キューイング クラスを作成して、最小帯域幅を保証できます。マルチキャスト ビデオ配信の場合、マルチキャスト ビデオ トラフィックの CoS 値に対する、ML シリーズ カード上のマルチキャスト プライオリティ キューイング クラスにより、VoIP や他のイーサネット サービスと共有するネットワークでマルチキャスト ビデオに使用する帯域幅の需要を効率的に管理できます。



(注)

マルチキャスト プライオリティ キューイング トラフィックは、RPR およびイーサチャネル上でポートベースのロード バランシングを使用します。デフォルトのマルチキャスト トラフィックは、イーサチャネル上ではなく、RPR 上でロード バランシングされます。マルチキャスト ロード バランシングは、ギガビット イーサネット ポート 0 を POS ポート 0 にマップし、ギガビット イーサネット ポート 1 を POS ポート 1 にマップします。マルチキャスト ロード バランシングは、ファストイーサネット ポート 0 およびすべての偶数番号のファストイーサネット ポートを POS 0 に、すべての奇数番号のファストイーサネット ポートを POS 1 にマップします。



(注)

マルチキャスト プライオリティ キューイングの帯域幅は、複数の送信元からのトラフィックで長期間にわたって使用超過にならないようにします。使用超過が続くと、マルチキャスト プライオリティ キューイングのスループットが減少します。

## デフォルトのマルチキャスト QoS

デフォルトのマルチキャスト トラフィックは、マルチキャスト プライオリティ キューイングとして分類されないマルチキャスト トラフィック (フラッディングしたトラフィックを含む) です。また、デフォルトのマルチキャスト クラスには、ブロードキャスト データ トラフィック、制御 トラフィック、レイヤ 2 プロトコル トンネリング、および MAC (メディア アクセス制御) 学習時の未知の MAC のフラッディング トラフィックが含まれます。

ML シリーズ カードで QoS が設定されていない (マルチキャスト プライオリティ キューイングなし、出力ポリシー マップなし) 場合、デフォルトのマルチキャスト 帯域幅は最小で合計帯域幅の 10% です。

マルチキャスト プライオリティ キューイングに帯域幅が割り当てられ、出力ポリシー マップが適用されていない場合、デフォルトのマルチキャスト 輻輳帯域幅は、最小で、マルチキャスト プライオリティ キューイングに割り当てられていない帯域幅の 10% です。

出力ポリシー マップがインターフェイスに適用されている場合、デフォルトのマルチキャストおよびデフォルトのユニキャストではデフォルトのクラスに割り当てられた最小帯域幅を共有します。また、このデフォルト クラスは match-any クラスとしても知られています。デフォルト マルチキャストの最小帯域幅は、デフォルト クラス帯域幅の合計の 10% です。

## マルチキャスト プライオリティ キューイング QoS の制限

マルチキャスト プライオリティ キューイング QoS に適用される制限は次のとおりです。

- マルチキャスト プライオリティ キューイング トラフィックに設定された帯域割り当てと利用率はグローバルで、ML シリーズ カード上のすべてのポート (POS とファスト イーサネットの両方またはギガビット イーサネット) に適用されます。これらのポートでマルチキャスト プライオリティ キューイング トラフィックを伝送するかどうかは関係ありません。この機能を設定した場合、ML シリーズ カード上のすべてのポートでトラフィックのレートを低減できます。デフォルトのマルチキャスト トラフィックは、マルチキャスト プライオリティ キューイングのようにグローバルではなく、出力ポートでのみ帯域幅を使用します。
- マルチキャスト プライオリティ キューイング QoS は、レイヤ 2 ブリッジングに対してのみサポートされています。
- ML シリーズ カードは、最大で 2 つのマルチキャスト プライオリティ キューイング クラスをサポートします。
- ML シリーズ カードの他の QoS とは異なり、マルチキャスト プライオリティ キューイング QoS は Cisco IOS MQC の一部ではありません。
- priority-mcast 帯域幅の割り当てはポートごとに行われ、cos priority-mcast を使用して ML1000-2 で設定可能な最大帯域幅は 1000 Mbps です。ただし、マルチキャスト プライオリティ キューイングのロード バランシングにより、有効な帯域幅が増えます。たとえば、GEC 回線と STS-24c RPR 回線を備えた ML1000-2 では、ポートごとに 1000 Mbps を割り当てることができ、ロード バランシングにより合計で 2000 Mbps の有効な帯域幅を得ることができます。

## マルチキャスト プライオリティ キューイング QoS の設定

マルチキャスト トラフィックのプライオリティ クラスを設定するには、表 14-5 に示す `cos priority-mcast` グローバル コンフィギュレーション コマンドを使用します。

表 14-5 CoS マルチキャスト プライオリティ キューイング コマンド

コマンドの説明	目的
<pre>Router (config)# [no] cos priority-mcast cos-value {bandwidth-kbps   mbps bandwidth-mbps   percent percent}</pre>	<p>マルチキャスト CoS 値に基づいてマルチキャスト トラフィックのプライオリティ クラスを作成し、輻輳が発生したときのトラフィック クラスの最小帯域幅保証を指定します。</p> <p><i>cos-value</i> では、帯域割り当てに使用されるマルチキャスト パケットの CoS 値を指定します。トラフィックの単一 CoS にのみ一致します (範囲ではありません)。サポートされている CoS の範囲は 0 ~ 7 です。</p> <p>最小帯域幅保証は、Kbps、Mbps、または使用可能帯域幅全体のパーセンテージで指定できます。</p> <p>ML シリーズ カードの有効な選択肢は次のとおりです。</p> <ul style="list-style-type: none"> <li>• Kbps で指定したレート</li> <li>• Mbps で指定したレート</li> <li>• 使用可能ポート帯域幅全体のパーセンテージ (1 ~ 100)</li> </ul> <p>コマンドを再入力するときに、<i>cos-value</i> が同じでも帯域幅レートが異なる場合は、既存のクラスの帯域幅が変更されます。</p> <p>異なる <i>cos-value</i> を指定してコマンドを再入力すると、別のマルチキャスト プライオリティ キューイングが作成されます。最大 2 つのマルチキャスト プライオリティ キューイング クラスが作成可能です。</p> <p>このコマンドの <code>no</code> 形式を使用すると、マルチキャスト プライオリティ キューイング クラスが削除されます。</p> <hr/> <p> (注) 実際に設定できる帯域幅 (Kbps または Mbps) はポートごとで、ML シリーズ カードの設定によって異なります。 <code>show interface</code> コマンドは、ポートの最大帯域幅を表示します (たとえば、BW 100000 キロビット)。インターフェイスに適用されたすべての帯域幅とプライオリティ アクション、および <code>cos priority-mcast</code> 帯域幅の合計は、ポートの合計帯域幅を超えることはできません。</p> <hr/> <p> (注) ポートで、実際に設定できる帯域幅を超える <code>priority-mcast</code> 帯域幅を設定しようとすると、<code>priority-mcast</code> 設定変更が失敗し、マルチキャスト プライオリティ キューイングの帯域幅保証は変更されません。</p>

## CoS ベースパケットの統計情報の概要

CoS アカウンティングがイネーブルの場合、拡張パフォーマンス モニタリングでは、ML シリーズカード インターフェイスの CoS 単位のパケット統計情報が表示されます。CoS 単位のパケット統計情報は、ブリッジド サービスに対してのみサポートされており、IP ルーティングや Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング) に対してはサポートされていません。CoS ベースのトラフィック利用率は、ファスト イーサネットまたはギガビット イーサネット インターフェイスあるいはサブインターフェイス (VLAN) レベル、POS インターフェイス レベルで表示されます。ただし、POS サブインターフェイス レベルでは表示されません。RPR 統計情報は SPR インターフェイス レベルでは使用できませんが、SPR インターフェイスで構成された各 POS ポートには使用できます。EtherChannel (ポートチャネル) および BVI の統計情報は、メンバー ポート レベルでのみ使用できます。表 14-6 に、特定のインターフェイスで使用できる統計情報のタイプを示します。

表 14-6 ML シリーズカード インターフェイスのパケット統計情報

収集される統計情報	ギガビット/ファスト イーサネット インターフェイス	ギガビット/ファストイーサネット サブインターフェイス (VLAN)	POS インターフェイス	POS サブインターフェイス
入力 パケットおよびバイト	含まれている	含まれている	含まれていない	含まれていない
出力 パケットおよびバイト	含まれている	含まれている	含まれていない	含まれていない
廃棄カウント パケットおよびバイト <sup>1</sup>	含まれている	含まれていない	含まれている	含まれていない

1. 廃棄カウントに含まれるのは出力輻輳が原因の廃棄だけであり、出力インターフェイスでカウントされます。

CoS ベースパケット統計情報は、CISCO-PORT-QOS MIB (管理情報ベース) の拡張機能を使用して、Cisco IOS の CLI および SNMP (簡易ネットワーク管理プロトコル) を通じて使用できます。CTC を通じて利用できません。

## CoS ベース パケット統計情報の設定



(注) CoS ベース パケット統計情報を使用するには、拡張マイクロコード イメージを ML シリーズ カードにロードする必要があります。



(注) IEEE 802.1Q (QinQ) 対応インターフェイスの場合、CoS アカウンティングはサービス プロバイダーが付けた外側のメトロ タグの CoS 値にのみ基づきます。カスタマー ネットワークによって送信されたパケット内部の CoS 値は、CoS アカウンティング用とはみなされません。

拡張マイクロコード イメージの詳細については、「複数のマイクロコード イメージ」(p.3-14)を参照してください。

インターフェイスで CoS ベース パケット統計情報をイネーブルにするには、インターフェイス コンフィギュレーション レベルで表 14-7 に示すコマンドを使用します。

表 14-7 CoS ベース パケット統計情報のコマンド

コマンドの説明	目的
Router(config-if)# <b>cos accounting</b>	CoS ベース パケット統計情報をイネーブルにし、特定のインターフェイスとそのインターフェイスのすべてのサブインターフェイスで記録されるようにします。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 モードでのみサポートされています。サブインターフェイス コンフィギュレーション モードではサポートされていません。  統計情報をディセーブルにするには、このコマンドの <b>no</b> 形式を使用します。

ML シリーズ カードで CoS ベース パケット統計情報を設定したあと、さまざまな **show** コマンドを使用して統計情報を表示できます。この情報を表示するには、EXEC モードで表 14-8 のコマンドのいずれかを使用します。

表 14-8 CoS ベース パケット統計情報のコマンド

コマンドの説明	目的
Router# <b>show interface type number cos</b>	インターフェイスで使用できる CoS ベース パケット統計情報を表示します。
Router# <b>show interface type number.subinterface-number cos</b>	ファスト イーサネットまたはギガビット イーサネット サブインターフェイスで使用できる CoS ベース パケット統計情報を表示します。POS サブインターフェイスでは使用できません。

例 14-15 に、これらのコマンドの例を示します。

## 例 14-15 CoS ベース パケットの統計情報のコマンド例

```
Router# show interface gigabitethernet 0.5 cos
GigabitEthernet0.5
```

```
Stats by Internal-Cos
Input: Packets      Bytes
  Cos 0: 31         2000
  Cos 1:
  Cos 2: 5           400
  Cos 3:
  Cos 4:
  Cos 5:
  Cos 6:
  Cos 7:
Output: Packets      Bytes
  Cos 0: 1234567890 1234567890
  Cos 1: 31           2000
  Cos 2:
  Cos 3:
  Cos 4:
  Cos 5:
  Cos 6: 10           640
  Cos 7:
```

```
Router# show interface gigabitethernet 0 cos
GigabitEthernet0
```

```
Stats by Internal-Cos
Input: Packets      Bytes
  Cos 0: 123         3564
  Cos 1:
  Cos 2: 3           211
  Cos 3:
  Cos 4:
  Cos 5:
  Cos 6:
  Cos 7:
Output: Packets      Bytes
  Cos 0: 1234567890 1234567890
  Cos 1: 3            200
  Cos 2:
  Cos 3:
  Cos 4:
  Cos 5:
  Cos 6: 1            64
  Cos 7:
Output: Drop-pkts    Drop-bytes
  Cos 0: 1234567890 1234567890
  Cos 1:
  Cos 2:
  Cos 3:
  Cos 4:
  Cos 5: 1            64
  Cos 6: 10           640
  Cos 7:
```

```
Router# show interface pos0 cos
```

```
POS0
Stats by Internal-Cos
Output: Drop-pkts    Drop-bytes
  Cos 0: 12           1234
  Cos 1: 31           2000
  Cos 2:
  Cos 3:
  Cos 4:
  Cos 5:
  Cos 6: 10           640
  Cos 7:
```

## IP SLA の概要

Cisco IP SLA は、今まで Cisco Service Assurance Agent と呼ばれていたもので、IP サービス レベルを保証するための Cisco IOS の機能です。IP SLA を使用すると、SP のカスタマーは SLA の測定や提供が可能になり、またエンタープライズ カスタマーは、サービス レベルの確認、アウトソーシングした SLA の確認、および新規または既存の IP サービスとアプリケーションのネットワーク パフォーマンスの把握が可能になります。IP SLA では、固有のサービス レベル保証メトリックと手法が使用されていて、非常に正確で高精度のサービス レベル保証測定値を提供します。

特定の SLA 運用に応じて、遅延の統計値、パケット損失、ジッタ、パケット シーケンス、接続、パス、サーバ応答時間、およびダウンロード時間がシスコの装置内でモニタリングされて CLI および SNMP MIB で保存されます。パケットには、送信元および宛先 IP アドレス、UDP および TCP ポート番号、ToS バイト (DSCP および IP プレフィクス ビットを含む)、Virtual Private Network (VPN; 仮想私設網) Routing/Forwarding instance (VRF; VPN ルーティング/転送インスタンス)、URL Web アドレスなどの、設定可能な IP およびアプリケーション層オプションがあります。

IP SLA では、生成されたトラフィックを使用して 2 つのネットワーキング装置 (ルータなど) 間のネットワーク パフォーマンスを測定します。IP SLA 装置が生成されたパケットを宛先装置に送信する際に IP SLA が開始します。宛先装置がパケットを受信したあと、IP SLA 動作のタイプに応じて、装置はパフォーマンス メトリックの計算を行うために送信元のタイム スタンプ情報で応答します。IP SLA 動作は、UDP などの特定のプロトコルを使用して動作する送信元装置からネットワーク内の宛先装置へのネットワーク測定です。

IP SLA は SNMP を使用して操作可能なので、CiscoWorks2000 (CiscoWorks Blue) や Internetwork Performance Monitor (IPM) などの、Network Management System (NMS; ネットワーク管理システム) 用パフォーマンス モニタリング アプリケーションでも使用できます。IP SLA 通知は、NetView などのアプリケーション用にある System Network Architecture (SNA) の Network Management Vector Transport (NMVT) を通じてイネーブルにすることもできます。

一般的な IP SLA 情報については、<http://www.cisco.com/warp/public/732/Tech/nmp/ipsla> にある「Cisco IOS IP Service Level Agreements」の技術ページを参照してください。Cisco IP SLA 機能の設定に関する詳細については、次の URL の『Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2』にある「Network Monitoring Using Cisco Service Assurance Agent」の章を参照してください。  
[http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products\\_configuration\\_guide\\_chapter09186a008030c773.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a008030c773.html)

## ML シリーズカードの IP SLA

ML シリーズカードには、完全な IP SLA Cisco IOS サブシステムがあり、Cisco IOS Release 12.2S で使用可能なすべての通常機能を装備しています。ここでは、標準 IP SLA Cisco IOS CLI コマンドを使用します。SNMP のサポートは、rttMon MIB である IP SLA サブシステム 12.2(S) で提供されるサポートと同等です。

## ML シリーズカードでの IP SLA の制限事項

ML シリーズカードは、Cisco IOS 12.2S ブランチの機能のみをサポートしています。IP SLA 精度機能や更新された IP SLA ラベルによる拡張 Cisco IOS CLI サポートなど、今後の Cisco IOS バージョンで利用可能な機能はサポートしていません。

このほかの制限は、以下の通りです。

- CoS ビットの設定はサポートしていますが、設定された CoS ビットは、送信側または応答側が ONS 15454、ONS 15454 SDH、または ONS 15310-CL プラットフォームの場合に、CPU に入出力される際に優先されません。設定された CoS ビットは、中間 ONS ノードで優先されます。

- RPR では、IP SLA パケットのデータフローの方向は、カスタマー トラフィックの方向とは異なります。
- ML シリーズ カードのシステム クロックは、TCC2/TCC2P カードのクロックと同期します。NTP サーバとの同期は、ML シリーズ カードのクロックではなく、TCC2/TCC2P カードのクロックとの間で実行されます。



## SDM の設定

---

この章では、ML シリーズ カードに組み込まれている Switching Database Manager (SDM; スイッチング データベース マネージャ) について説明します。内容は次のとおりです。

- [SDM の概要 \(p.15-2\)](#)
- [SDM 領域の概要 \(p.15-2\)](#)
- [SDM の設定 \(p.15-3\)](#)
- [SDM のモニタリングと確認 \(p.15-4\)](#)

## SDM の概要

ML シリーズ カードでは、転送エンジンおよび Ternary CAM (TCAM) を使用して、高速転送を実現しています。高速転送情報は、TCAM に保持されます。SDM は、TCAM に保持されているスイッチング情報を管理するソフトウェア サブシステムです。

SDM は、TCAM 内のスイッチング情報をアプリケーション固有の領域に編成し、これらのアプリケーション領域のサイズを設定します。SDM によって完全一致および最長一致のアドレス検索が可能となるため、高速転送が実現します。SDM は、アプリケーション固有のスイッチング情報を複数の領域に分割することにより、TCAM のスペースを管理します。

TCAM は、転送される各パケットに関連付けられたロケーション インデックスを識別して転送エンジンに伝えます。転送エンジンでは、このロケーション インデックスを使用して、各転送パケットに関連付けられた情報を取得します。

## SDM 領域の概要

SDM は、複数のアプリケーション固有の領域を分割し、個々のアプリケーション制御層と連動してスイッチング情報を保存します。この領域は、使用可能なスペース全体を共有します。SDM は、次の種類の領域で構成されています。

- **完全一致領域** 完全一致領域は、IP 隣接など、複数のアプリケーション領域のエントリで構成されます。
- **最長一致領域** 各最長一致領域は、マスク長に基づいて降順に編成されたレイヤ 3 アドレス エントリの複数のパケットまたはグループで構成されます。パケット内のすべてのエントリは、同じマスク値とキー サイズを共有します。パケットは、近接パケットからアドレス エントリを借用することにより、サイズを動的に変更できます。アプリケーション領域全体のサイズは決まっていますが、この設定は変更できます。
- **重み付け完全一致領域** 重み付け完全一致領域は、重み付けまたはプライオリティが割り当てられた完全一致エントリで構成されます。たとえば、Quality of Service (QoS; サービス品質) では、複数の完全一致エントリが存在する場合がありますが、他のエントリよりもプライオリティの高いエントリがあります。重み付けは、複数のエントリが一致するときに 1 つのエントリを選択するために使用します。

表 15-1 に、各アプリケーション領域のデフォルト パーティションを示します。

表 15-1 アプリケーション領域のデフォルト パーティション

アプリケーション領域	検索タイプ	キー サイズ	デフォルト サイズ
IP Adjacency	完全一致	64 ビット	300 (共有)
IP Prefix	最長一致	64 ビット	300 (共有)
QoS Classifiers	重み付け完全一致	64 ビット	300 (共有)
IP VRF Prefix	最長プレフィックス一致	64 ビット	300 (共有)
IP Multicast	最長プレフィックス一致	64 ビット	300 (共有)
MAC Addr	最長プレフィックス一致	64 ビット	8192
Access List	重み付け完全一致	64 ビット	300 (共有)

## SDM の設定

ここでは、SDM 領域のサイズと Access Control List (ACL; アクセス制御リスト) のサイズの設定について説明します。ここで説明するコマンドは、スイッチング ソフトウェア固有のコマンドです。設定の変更は、ML-100T-8 カード上でただちに反映されます。

### SDM 領域の設定

各アプリケーション領域の SDM の最大サイズを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	<code>ML_Series(config)# sdm size region-name number-of-entries</code>	SDM 領域のエントリの最大数を設定します。
ステップ 2	<code>ML_Series(config)# end</code>	イネーブル EXEC モードに戻ります。

例 15-1 に、この設定の一例を示します。

#### 例 15-1 IP-Prefix 領域を 2 K エントリに制限する場合

```
ML_Series # configure terminal
ML_Series(config)# sdm size ip-prefix 200
ML_Series(config)# end
```

### TCAM の ACL のサイズ設定

ACL のデフォルトの最大サイズは、300 の 64 ビット エントリです。表 15-2 に示すように、`sdm access-list` コマンドを使用して、ACL データベースの最大サイズを変更することができます。

表 15-2 ACL に使用する TCAM サイズの割り当て

機能	コマンドの説明
<code>sdm access-list number-entries</code>	サイズを設定するアプリケーション領域の名前を指定します。サイズは、エントリの絶対数で指定できます。

例 15-2 に、この設定の一例を示します。

#### 例 15-2 TCAM の ACL 領域へのエントリの設定

```
ML_Series# configure terminal
ML_Series(config)# sdm access-list 100
ML_Series(config)# end
```

## SDM のモニタリングと確認

使用できる TCAM エントリの数を表示するには、グローバル コンフィギュレーション モードから `show sdm size` コマンドを入力します。

```
ML_Series # show sdm size
Active Switching Database Region Maximum Sizes :
  IP Adjacency           : 300      64-bit entries
  IP Prefix              : 300      64-bit entries
  QoS Classifiers        : 300      64-bit entries
  IP VRF Prefix          : 300      64-bit entries
  IP Multicast           : 300      64-bit entries
  MAC Addr               : 8192     64-bit entries
  Access List            : 300      64-bit entries
```



## ACL の設定

---

この章では、ML シリーズ カードに組み込まれている Access Control List (ACL; アクセス制御リスト) について説明します。

この章の内容は次のとおりです。

- [ACL の概要 \(p.16-2\)](#)
- [ML シリーズにおける ACL サポート \(p.16-2\)](#)
- [ACL TCAM サイズの変更 \(p.16-6\)](#)

## ACL の概要

ACL は、ネットワークの制御とセキュリティを実現する機能で、ML シリーズのインターフェイスに出入りするパケットのフローをフィルタリングできます。フィルタとも呼ばれる ACL により、特定のユーザや装置によるネットワークの使用を制限できます。ACL はプロトコルごとに作成し、着信トラフィックまたは発信トラフィックのどちらか一方のインターフェイスに適用します。ACL はコントロールプレーンの発信トラフィックには適用されません。1 つの方向、1 つのサブインターフェイスごとに適用できる ACL フィルタは 1 つだけです。

ACL を作成する場合は、ML シリーズカードが処理する各パケットに適用する基準を定義します。これによって ML シリーズカードでは、パケットがリストの基準に一致するかどうかに基づいて、パケットを転送するか、ブロックするかを決定します。リストのどの基準にも一致しないパケットは、各 ACL の末尾にある暗黙的な「deny all traffic」基準ステートメントによって、自動的にブロックされます。

## ML シリーズにおける ACL サポート

制御プレーン ACL とデータプレーン ACL は、どちらも ML シリーズカードでサポートされます。

- 制御プレーン ACL : ML シリーズカードの CPU によって処理される制御データをフィルタするための ACL (たとえば、ルーティング情報、Internet Group Membership Protocol [IGMP] 加入の配布など)
- データプレーン ACL : ML シリーズのハードウェアを使用してルーティングまたはブリッジされているユーザデータをフィルタするための ACL (たとえば、ホストへのアクセスの拒否など)。データプレーン ACL は、`ip access-group` コマンドを使用して入力方向または出力方向のインターフェイスに適用されます。

データプレーン ACL を ML シリーズカード上で使用する際には、次の制限があります。

- ACL は、ブリッジド インターフェイスを含む、あらゆる種類のインターフェイスでサポートされます。
- 再帰的 ACL とダイナミック ACL は、ML シリーズカードではサポートされません。
- アクセス違反のアカウントリングは、ML シリーズカードではサポートされません。
- ACL のロギングは、交換されたパケットではなく、CPU に送信するパケットに対してのみサポートされます。
- 出力ブリッジド インターフェイスに適用された IP 標準 ACL は、データプレーンではサポートされません。ブリッジングの場合は、ACL は入力側でのみサポートされます。

## IP ACL

IP に対しては、次のような ACL 形式がサポートされています。

- 標準 IP ACL : 送信元アドレスを使用してマッチングを行います。
- 拡張 IP ACL (制御プレーン専用) : 送信元アドレスおよび宛先アドレスを使用してマッチングを行います。さらに細かく制御するためには、任意でプロトコルタイプとポート番号を使用します。
- 名前付き ACL : 送信元アドレスを使用してマッチングを行います。



(注)

デフォルトでは、ACL の末尾には、末尾に到達する前に一致するステートメントが見つからなかった場合のための暗黙的な拒否ステートメントがあります。標準 ACL では、関連付けられた IP ホストアドレスの ACL 指定からマスクを省略すると、マスクが 0.0.0.0 であるとみなされます。

ACL を作成したら、その ACL をインターフェイスに適用する必要があります。「[インターフェイスへの ACL の適用](#)」(p.16-5)を参照してください。

## 名前付き IP ACL

IP ACL は名前で特定できます。ただし、名前は英数字の文字列である必要があります。名前付き IP ACL を使用すると、番号付き ACL の場合よりも多くの IP ACL を 1 つのルータに設定できます。数値の文字列ではなく英字の文字列で ACL を特定する場合は、モードとコマンドの構文が多少異なります。

次の事項を検討してから名前付き ACL を設定してください。

- 標準 ACL と拡張 ACL に同じ名前を付けることはできません。
- 番号付き ACL も利用できます。「[番号付き標準および拡張 IP ACL の作成](#)」(p.16-3)を参照してください。

## ユーザの注意事項

IP ネットワークのアクセス制御を設定するときは、次のことに留意してください。

- Ternary CAM (TCAM) 内に ACL エントリをプログラムできます。
- ACL の末尾には、すべてを拒否するステートメントが暗黙的に指定されているため、入力する必要がありません。
- ACL エントリはどのような順序で入力しても、パフォーマンスに影響しません。
- 8 個の TCAM エントリごとに、ML シリーズ カードは TCAM の管理用のエントリを 1 個使用します。
- パケット損失を引き起こす条件を設定しないでください。パケット損失は、特定のサービスのパケットを拒否する ACL が設定されたネットワークで、そのサービスをアダプタイズするように装置またはインターフェイスが設定されている場合に発生します。
- IP ACL は、ダブルタグ (QinQ) パケットに対してサポートされていません。ただし、IP ACL は QinQ アクセス ポートに着信する IP パケットに対して適用されます。

## IP ACL の作成

ここでは、番号付き標準 IP ACL、拡張 IP ACL、および名前付き標準 IP ACL の作成方法について説明します。

- [番号付き標準および拡張 IP ACL の作成](#) (p.16-3)
- [名前付き標準 IP ACL の作成](#) (p.16-4)
- [名前付き拡張 IP ACL の作成 \(制御プレーン専用\)](#)(p.16-5)
- [インターフェイスへの ACL の適用](#) (p.16-5)

## 番号付き標準および拡張 IP ACL の作成

表 16-1 に、番号付き標準 IP ACL と拡張 IP ACL の作成に使用するグローバル コンフィギュレーション コマンドを示します。

表 16-1 番号付き標準および拡張 IP ACL のコマンド

コマンドの説明	目的
Router(config)# <b>access-list</b> access-list-number {deny   permit} source [source-wildcard]	送信元アドレスとワイルドカードを使用して標準 IP ACL を定義します。
Router(config)# <b>access-list</b> access-list-number {deny   permit} any	0.0.0.0 255.255.255.255 という送信元と送信元マスクの省略形を使用して標準 IP ACL を定義します。
Router(config)# <b>access-list</b> extended-access-list-number {deny   permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos]	拡張 IP ACL 番号とアクセス条件を定義します。
Router(config)# <b>access-list</b> extended-access-list-number {deny   permit} protocol any any	0.0.0.0 255.255.255.255 という送信元と送信元ワイルドカードの省略形と、0.0.0.0 255.255.255.255 という宛先と宛先ワイルドカードの省略形を使用して、拡張 IP ACL を定義します。
Router(config)# <b>access-list</b> extended-access-list-number {deny   permit} protocol host source host destination	source 0.0.0.0 という送信元と送信元ワイルドカードの省略形と、destination 0.0.0.0 という宛先と宛先ワイルドカードの省略形を使用して、拡張 IP ACL を定義します。

## 名前付き標準 IP ACL の作成

名前付き標準 IP ACL を作成するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>ip access-list standard</b> name	英字の名前を使用して標準 IP ACL を定義します。
ステップ 2	Router(config-std-nacl) # <b>deny</b> {source [source-wildcard]   any}  または <b>permit</b> {source [source-wildcard]   any}	アクセス リスト設定モードで、許可または拒否する条件を1つ以上指定します。これによって、パケットを通過させるか、廃棄するかが決定します。
ステップ 3	Router(config)# <b>exit</b>	アクセス リスト コンフィギュレーション モードを終了します。

## 名前付き拡張 IP ACL の作成 (制御プレーン専用)

名前付き拡張 IP ACL を作成するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>ip access-list extended</b> <i>name</i>	英字の名前を使用して拡張 IP ACL を定義します。
ステップ 2	Router(config-ext-nacl)# { <b>deny</b>   <b>permit</b> } <i>protocol source source-wildcard</i> <i>destination destination-wildcard</i> [ <b>precedence precedence</b> ] [ <b>tos tos</b> ]	アクセス リスト コンフィギュレーション モードで、許可または拒否する条件を指定します。
	または	または 0.0.0.0 255.255.255.255 という送信元と送信元ワイルドカードの省略形と、0.0.0.0 255.255.255.255 という宛先と宛先ワイルドカードの省略形を使用して、拡張 IP ACL を定義します。
	{ <b>deny</b>   <b>permit</b> } <i>protocol any any</i>	
	または	または
	{ <b>deny</b>   <b>permit</b> } <i>protocol host source host destination</i>	<i>source</i> 0.0.0.0 という送信元と送信元ワイルドカードの省略形と、 <i>destination</i> 0.0.0.0 という宛先と宛先ワイルドカードの省略形を使用して、拡張 IP ACL を定義します。

## インターフェイスへの ACL の適用

ACL を作成したら、その ACL を 1 つまたは複数のインターフェイスに適用できます。ACL を適用できるのは、インターフェイスの着信方向または発信方向のどちらか一方です。インターフェイスへのアクセスを制御するには、名前または番号を使用します。標準 ACL を適用した場合、ML シリーズ カードは送信元 IP アドレスを ACL と比較します。ACL を 1 つまたは複数のインターフェイスに適用するには、表 16-2 に示すコマンドを使用します。



(注)

Bridge Group Virtual Interface (BVI; ブリッジ グループ仮想インターフェイス) の入力側に適用された IP 標準 ACL は、BVI 入力トラフィックだけでなく、関連付けられたブリッジ グループ内のブリッジされたすべての IP トラフィックに適用されます。

表 16-2 インターフェイスへの ACL の適用

コマンドの説明	目的
<b>ip access-group</b> { <i>access-list-number</i>   <i>name</i> } { <b>in</b>   <b>out</b> }	インターフェイスへのアクセスを制御します。

## ACL TCAM サイズの変更

TCAM サイズを変更するには、`sdm access-list` コマンドを入力します。ACL TCAM サイズの詳細については、「[TCAM の ACL のサイズ設定](#)」(p.15-3)を参照してください。例 16-1 には、ACL の変更と確認の例を示します。



(注)

ACL TCAM サイズを増やすには、IP、IP マルチキャスト、L2 スイッチングなどの別の領域の TCAM サイズを縮小する必要があります。



注意

次のエラーメッセージが表示された場合は、TCAM サイズを増やす必要があります。

```
Warning:Programming TCAM entries failed
Please remove last ACL command to re-activate ACL operation.
!<ACL number or name> <IP or IPX> <INPUT_ACL or OUTPUT_ACL> from TCAM group for
!<interface>
Please see the documentation to see if TCAM space can be
increased on this platform to alleviate the problem.
```

### 例 16-1 ACL のモニタリングと確認

```
Router# show ip access-lists 1
Standard IP access list 1
  permit 192.168.1.1
  permit 192.168.1.2
```



## RPR の設定

---

この章では、ML シリーズ カードの Resilient Packet Ring (RPR; 復元パケット リング)、RPR Link Fault Propagation (LFP; リンク障害伝播)、および Dual RPR Interconnect (DRPRI; 二重 RPR 相互接続) の設定方法について説明します。

この章の内容は次のとおりです。

- [RPR の概要 \(p.17-2\)](#)
- [RPR の設定 \(p.17-7\)](#)
- [RPR のモニタリングおよび確認 \(p.17-19\)](#)
- [ML シリーズ カードの RPR への追加 \(p.17-20\)](#)
- [RPR からの ML シリーズ カードの削除 \(p.17-25\)](#)
- [RPR LFP の概要 \(p.17-30\)](#)
- [LFP の設定 \(p.17-32\)](#)
- [デュアル RPR 相互接続の概要 \(p.17-34\)](#)
- [DRPRI の設定 \(p.17-36\)](#)

## RPR の概要

RPR は、レイヤ 2 レベルで動作する新しい MAC (メディア アクセス制御) プロトコルです。RPR は、SONET/SDH リング トポロジ ー上でのイーサネットの転送に非常に適しており、複数の ML シリーズ カードをイネーブルにして、1 つの機能ネットワーク セグメントまたは Shared Packet Ring (SPR; 共有パケットリング) にすることが可能です。RPR は、このような役割における IEEE 802.1D Spanning Tree Protocol (STP; スパニング ツリー プロトコル)、IEEE 802.1W Rapid Spanning Tree Protocol (RSTP; 高速スパニング ツリー プロトコル) SONET/SDH などの初期のスキームの限界を克服します。IEEE 802.17 ドラフトは Cisco ML シリーズ RPR 実装の参照用として使用されていましたが、現在の ML シリーズ カード RPR プロトコルは、IEEE 802.17 の条項とはまったく適合しません。

## SONET/SDH 回線の役割

SPR 内の ML シリーズ カードは、ポイントツーポイント STS/STM 回線を介して、直接または間接的に接続する必要があります。ポイントツーポイント STS/STM 回線は ONS ノード上で設定され、保護回線または非保護回線のいずれかで ONS ノードの SONET/SDH トポロジ ー上で転送されます。

SONET/SDH メカニズムによって保護されていない回線上の場合、RPR は SONET/SDH 保護回線が必要とする冗長保護パスを使用せずに、復元機能を提供します。そのため、トラフィック量を増やすことができます。また、RPR はリングの帯域幅全体を使用するため、STP や RSTP のようにセグメントをブロックしません。

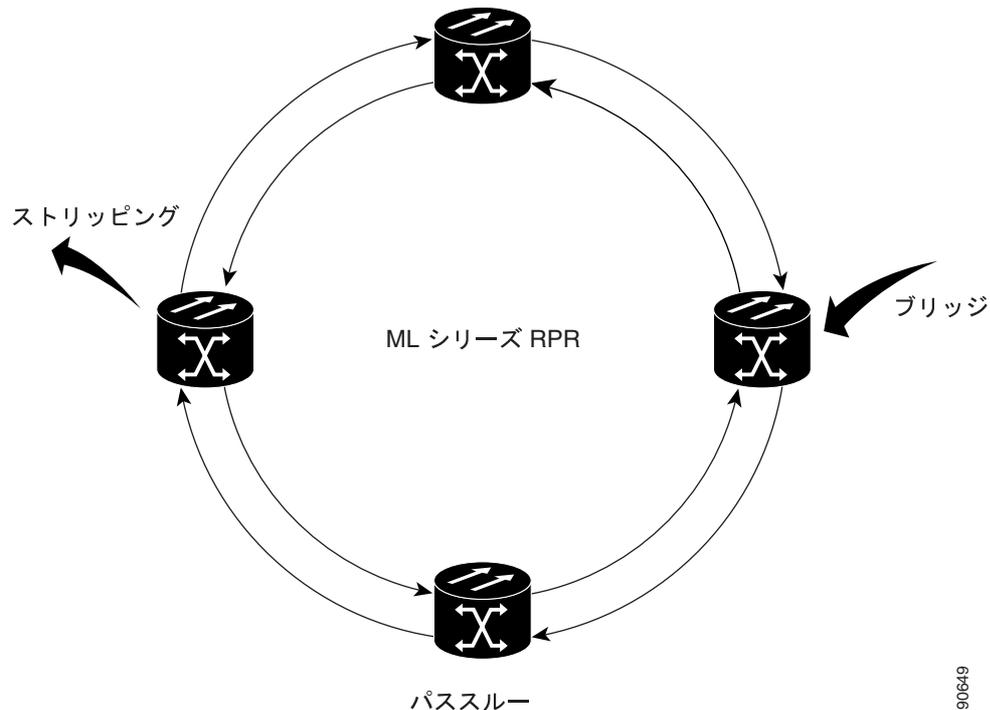
## パケット処理動作

ML シリーズ カードに RPR が設定されていて、SPR の一部にした場合、ML シリーズ カードはリング トポロジ ーとみなされます。パケットが、特定の ML シリーズ カードのイーサネット ポート経由でブリッジングされたネットワーク装置宛てでない場合、ML シリーズ カードは、リングアーキテクチャの巡回パスを信頼して、SONET/SDH 回線に沿ってこの中継トラフィックの転送を続け、パケットが最終的に宛先に到達することを保証します。これにより、宛先ではない ML シリーズ カード経由で通過するパケットをキューに入れて処理する必要がなくなります。レイヤ 2 またはレイヤ 3 から見ると、RPR 全体が 1 つの共有ネットワーク セグメントのように見えます。

RPR が設定された ML シリーズ カードは、ブリッジ、パススルー、ストリッピングという 3 つの基本的なパケット処理動作を行います。図 17-1 に、これらの動作を示します。ブリッジングは、ML シリーズのイーサネット ポートと、リングを巡回する SONET/SDH 回線に使用される Packet-over-SONET/SDH (POS) ポート間を接続し、パケットを渡します。パススルーにより、パケットは ML シリーズ カード経由でリング内を巡回します。また、ストリッピングはリングからパケットを除去し廃棄します。

RPR プロトコルが送信パケットのヘッダー情報を使用することで、インターフェイスはパケットに適用する必要のある動作を迅速に決定できます。また、RPR プロトコルはパケットの送信元および宛先アドレスを使用して、リング方向を選択します。フローベースのロードシェアリングにより、同じ送信元および宛先のアドレス ペアが組み込まれたすべてのパケットを同じ方向に送信し、正しい順で宛先に着信できます。リング方向も、スペース再利用をイネーブルにして、全体的なリング集約帯域幅を増やしています。ユニキャスト パケットは宛先がストリッピングされています。宛先ストリッピングにより、RPR の異なる部分間で同時にトラフィック フローを転送する機能が提供されます。隣接するノード間で双方向に同時にトラフィックを送信できます。また、複数のノードをスパンすることもでき、同じリング帯域幅を効率的に再利用できます。マルチキャストパケットは送信元がストリッピングされています。

図 17-1 RPR のパケット処理動作



69406

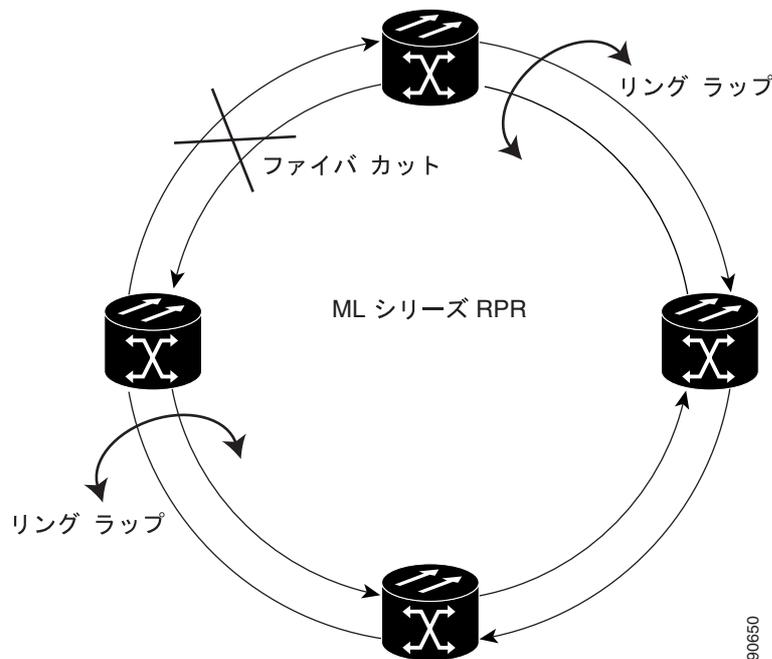
## リングラッピング

ファイバカット、ノードの障害、ノードの復元、新しいノードの挿入、またはその他のトラフィック上の問題が発生すると、RPR はリングラップを開始します。この保護メカニズムによって、リンク状態の変更後、または SONET/SDH パスレベルのアラーム受信後に、トラフィックはリング内で反対方向に送信され、元の宛先にリダイレクトされます。ML シリーズカードのリングラッピングでは、ユニキャストおよびパススルートラフィックの 50 ミリ秒未満のコンバージェンス時間が許容されます。RPR のコンバージェンス時間は、SONET/SDH とほぼ同じで、STP や RSTP よりもきわめて高速です。

ML シリーズカードの RPR は、リング内で発生する単一方向送信と双方向送信の両方の障害に対応します。STP や RSTP とは異なり、RPR の復元はスケーラブルです。リング内で ML シリーズカードの数が増えても、コンバージェンス時間は延びません。

リングラップは、デフォルトでは `spr wrap immediate` で設定され、障害状態に陥ってから 50 ミリ秒内に発生します。`spr wrap delay` が設定されている場合、POS インターフェイスがリンクダウンするまでラップが遅れます。CLI `pos trigger delay <msec>` で指定された時間が経過すると、リンクがダウンします。回線が VCAT の場合、Cisco IOS CLI コマンド `pos vcat defect delayed` も設定する必要があります。この遅延により、RPR に SONET/SDH 帯域幅保護が設定されている場合、レイヤ 2 RPR 保護が有効になる前に、このレイヤ 1 保護を有効にできます。SONET エラーなしでインターフェイスがダウンする場合、キャリア遅延も発生します。図 17-2 に、リングラッピングを示します。

図 17-2 RPR リングラッピング



リングに障害が発生した場合、RPR の障害が発生した部分に接続された ML シリーズ カードは SONET/SDH パス アラームを通じて障害を検出します。いずれかの ML シリーズ カードがこのパス AIS 信号を受信すると、カードは信号を受信した POS インターフェイスをラップします。



(注)

ML シリーズ カードの RPR コンバージェンス時間は、同じリングで複数の障害が発生したときに、ML シリーズ カードのリロード中に DRPRI が設定された ML シリーズ カード (アクティブ モード) をトラフィックが通過する場合、または ML シリーズ カード間のマイクロコード イメージに mismatches が発生した場合に、50 ミリ秒を超える可能性があります。



(注)

キャリア遅延時間をデフォルトから変更する場合、新しいキャリア遅延時間は、SPR、POS、およびギガビットイーサネットまたはファストイーサネット インターフェイスなど、ML シリーズ カードのすべてのインターフェイスで設定する必要があります。



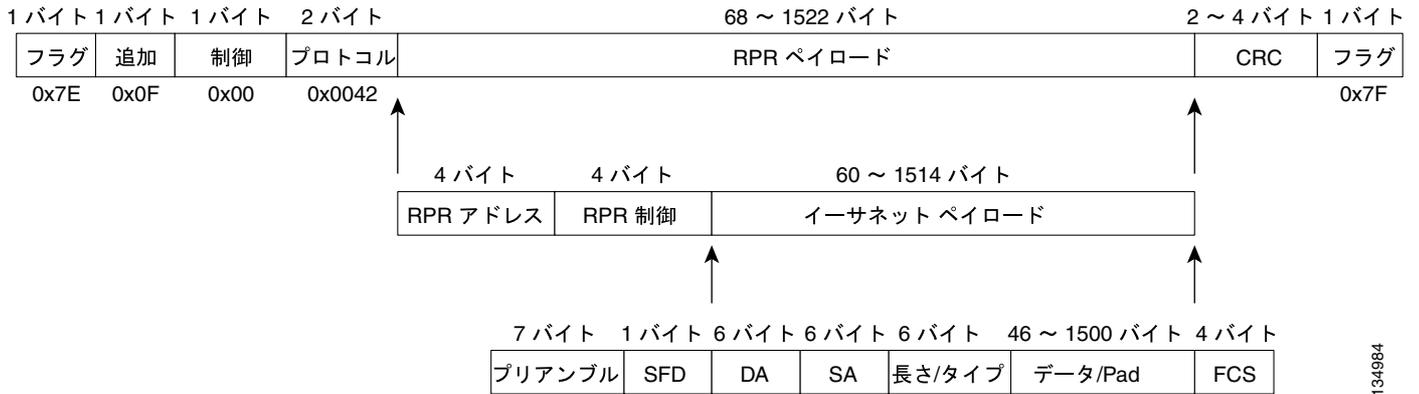
(注)

ML シリーズ カードの POS インターフェイスは通常、POS リンクがダウンまたは RPR がラップしたときに、ONS 15454 STS パス オーバーヘッド (PDI-P) の信号ラベル mismatches に関するアラームを遠端に送信します。PDI-P が検出されたとき、Remote Defection Indication - Path (RDI-P; リモート障害表示 - パス) アラームが遠端に送信されているとき、または検出された障害が Generic Framing Procedure (GFP) -Loss of Frame Delineation (LFD)、GFP Client Signal Fail (CSF)、Virtual Concatenation (VCAT) -Loss of Multiframe (LOM) または VCAT-Loss of Sequence (SQM) の場合のみ、ML シリーズ カードの POS インターフェイスは PDI-P を遠端に送信しません。

## RPR フレーミング プロセス

ML シリーズ カードは、固有の RPR フレームと、HDLC または GFP-F フレーミングを使用します。カードは RPR フレーム ヘッダーを各イーサネット フレームに組み込み、RPR フレームを SONET/SDH ペイロードにカプセル化し、SONET/SDH トポロジー上で転送できるようにします。RPR ヘッダーは出力側 ML シリーズ カードで削除されます。図 17-3 に、RPR フレームを示します。

図 17-3 ML シリーズ カードの RPR フレーム



134984

RPR フレーミングとヘッダーには、送信元および宛先ステーション情報の 4 バイト、RPR 制御および Quality of Service (QoS; サービス品質) の 4 バイトなどのフィールド数が含まれます。図 17-4 に、RPR フレーム形式を示します。表 17-1 に最重要フィールドを示します。

図 17-4 RPR フレームのフィールド



134982

表 17-1 RPR フレーム フィールドの定義

宛先ステーション	8 ビットのフィールド。RPR 内の特定の ML シリーズ カードの MAC アドレスを宛先として指定します。このフィールドには、Multicast DA-MAC の 0xff と Unknown DA-MAC の 0x00 という既知のアドレスが 2 つのあります。
送信元ステーション	8 ビットのフィールド。RPR 内の特定の ML シリーズ カードの MAC アドレスを送信元として指定します。
PRI	3 ビットの Class of Service ( CoS; サービス クラス ) フィールド。RPR プライオリティを確立します。
DE	Discard Eligible ( DE; 廃棄適性 ) フラグ用の 1 ビットのフィールド
TTL	フレームの time-to-live 用 9 ビット フィールド
タイプ	データ パケットか制御パケットを示すフィールド

## MAC アドレスと VLAN サポート

RPR では、ML シリーズ カードを通過するパケットの MAC ID が ML シリーズ カードによって記録されないため、サポートされる MAC アドレスの総数が増加します。ML シリーズ カードは、そのカードによってブリッジングまたはストリッピングされたパケットの MAC ID だけを記録します。これにより、RPR の集合アドレス テーブルに、より多くの MAC アドレスを保持することが可能になります。

また、STP および RSTP 上の VLAN がリングの全 POS インターフェイスで設定する必要があるのに比べ、RPR 上の VLAN ( 仮想 LAN ) はより少ないインターフェイス設定ですみます。RPR の VLAN は、その VLAN でパケットをブリッジングまたはストリップする SPR インターフェイス上の設定だけが必要です。

ML シリーズ カードには、カードごとに設定できる VLAN またはブリッジ グループの最大数が 255 というアーキテクチャ上の制限がまだ残されています。ただし、ML シリーズ カードが MAC アドレスを管理する必要があるのは、直接接続されている装置であるため、RPR ネットワークではより多くの接続装置を使用できます。

## RPR QoS

ML シリーズ カードの RPR は、Service Level Agreement ( SLA; サービス レベル契約 ) をサポートする効果的な帯域幅利用率を実現するために、ML シリーズ カードの QoS 機能を信頼しています。ML シリーズ カードの QoS メカニズムは、トラフィックがパススルー、ブリッジ、またはストリッピングされているかどうかに関係なく、ML シリーズ カードのすべての SONET/SDH トラフィックに適用されます。RPR QoS の詳細については、第 14 章「QoS の設定」の「RPR の QoS」を参照してください。

## CTM および RPR

Cisco Transport Manager ( CTM ) は、Network Management System ( NMS; ネットワーク管理システム ) 全体と、他の高レベルの管理ツールを持ったインターフェイスを統合するよう設計された Element Management System ( EMS; 要素管理システム ) です。CTM は、ML シリーズ カード上で RPR プロビジョニングをサポートします。詳細については、『Cisco Transport Manager User Guide』を参照してください。次の URL からアクセスしてください。

[http://www.cisco.com/en/US/products/sw/opticsw/ps2204/products\\_user\\_guide\\_list.html](http://www.cisco.com/en/US/products/sw/opticsw/ps2204/products_user_guide_list.html)

## RPR の設定

ML シリーズ カード用に RPR を設定するには、Cisco Transport Controller (CTC) と Cisco IOS の両方を使用する必要があります。CTC は、Graphical User Interface (GUI; グラフィカル ユーザ インターフェイス) で、RPR に必要なポイントツーポイント SONET/SDH 回線のプロビジョニングなど、特定の ONS ノード動作の拡張クラフト ツールとして機能します。Cisco IOS は、ML シリーズ カードとそのインターフェイス上で RPR を設定するために使用されます。

RPR を作成するには、次の手順を順番に実行します。

1. ML シリーズ カードとポイントツーポイント STS/STM 回線の接続 (p.17-7) (CTC または TL1)
2. RPR の CTC 回線の設定 (p.17-7) (CTC または TL1)
3. ML シリーズ カード上の RPR 特性と SPR インターフェイスの設定 (p.17-12) (Cisco IOS)
4. ML シリーズ カードの POS ポートの SPR インターフェイスへの割り当て (p.17-14) (Cisco IOS)
- 5.ブリッジ グループの作成とイーサネットおよび SPR インターフェイスの割り当て (p.17-16) (Cisco IOS)
6. RPR イーサネット アクセス ポート間のイーサネット接続の確認 (p.17-19) (Cisco IOS)



(注)

Transaction Language One (TL1) を使用して、CTC の代わりに、必要な SONET/SDH ポイントツーポイント回線をプロビジョニングできます。

## ML シリーズ カードとポイントツーポイント STS/STM 回線の接続

RPR 内の ML シリーズ カードをポイントツーポイント STS/STM 回線を介して接続します。この回線は、ONS 15454 SONET/SDH ネットワークを使用し、光回線をプロビジョニングする通常の方法で、CTC を使用してプロビジョニングされます。

## RPR の CTC 回線の設定

RPR が必要とする CTC 回線を設定する場合の注意事項は次のとおりです。

- Circuit Routing Preferences ダイアログボックスの **Fully Protected Path** 以外の CTC Circuit Creation Wizard のすべてのオプションをデフォルト設定のままにします。**Fully Protected Path** には SONET/SDH 保護が指定されているため、オフにする必要があります。RPR は通常、SPR 回線のレイヤ 2 保護を提供します。
- Circuit Routing Preferences ダイアログボックスで、**Using Required Nodes and Spans** をオンにし、自動的にルーティングするようにします。送信元ノードと宛先ノードがリング上で隣接している場合、Circuit Routing Preferences ダイアログボックスで、送信元と宛先を除くすべてのノードを除外します。これにより、回線で送信元ノードと宛先ノード間が直接ルーティングされるようになり、STS/STM 回線を使用しなくて済みます。この STS/STM 回線は、リング内の他のノード経由で回線がルーティングされると消費されます。ML シリーズ カードが設定された 2 つのノード間に、ML シリーズ カードが設定されていない 1 つまたは複数のノードが存在する場合は、Circuit Routing Preference ダイアログボックスの含まれているノード領域に、送信元および宛先ノードとともにこれらのノードを含めます。
- ML シリーズ カードの STS/STM 回線は、次の CTC のチェック ボックス タイトル、双方向トラフィック、クロス コネクトのみの作成 (TL1 と同様)、ドメイン間 (Unified Control Plane [UCP]) 保護ドロップ、Subnetwork connection protection (SNCP; サブネットワーク接続保護)、Unidirectional Path Switched Ring (UPSR; 単方向パス スイッチ型リング) パス セレクタなど、関係のない回線作成オプションはサポートしていません。

- 最適な方法は、イーストからウェスト、またはウェストからイーストに SONET/SDH 回線を設定することです。つまり、SONET/SDH リングで、ポート 0 (イースト) からポート 1 (ウェスト)、またはポート 1 (ウェスト) からポート 0 (イースト) のように設定します。ポート 0 からポート 0 またはポート 1 からポート 1 は設定しないでください。イーストからウェストまたはウェストからイーストのセットアップは、CTM ネットワーク管理ソフトウェアが ML シリーズの設定を SPR として認識するためにも必要です。

CTC 回線手順の詳細については『Cisco ONS 15454 Procedure Guide』の、「Create Circuits and VT Tunnels」の章および『Cisco ONS 15454 SDH Procedure Guide』の「Create Circuits and Tunnels」の章を参照してください。

## RPR の CTC 回線の設定例

図 17-5 に、3 つのノードの RPR の例を示します。

図 17-5 3 つのノードの例

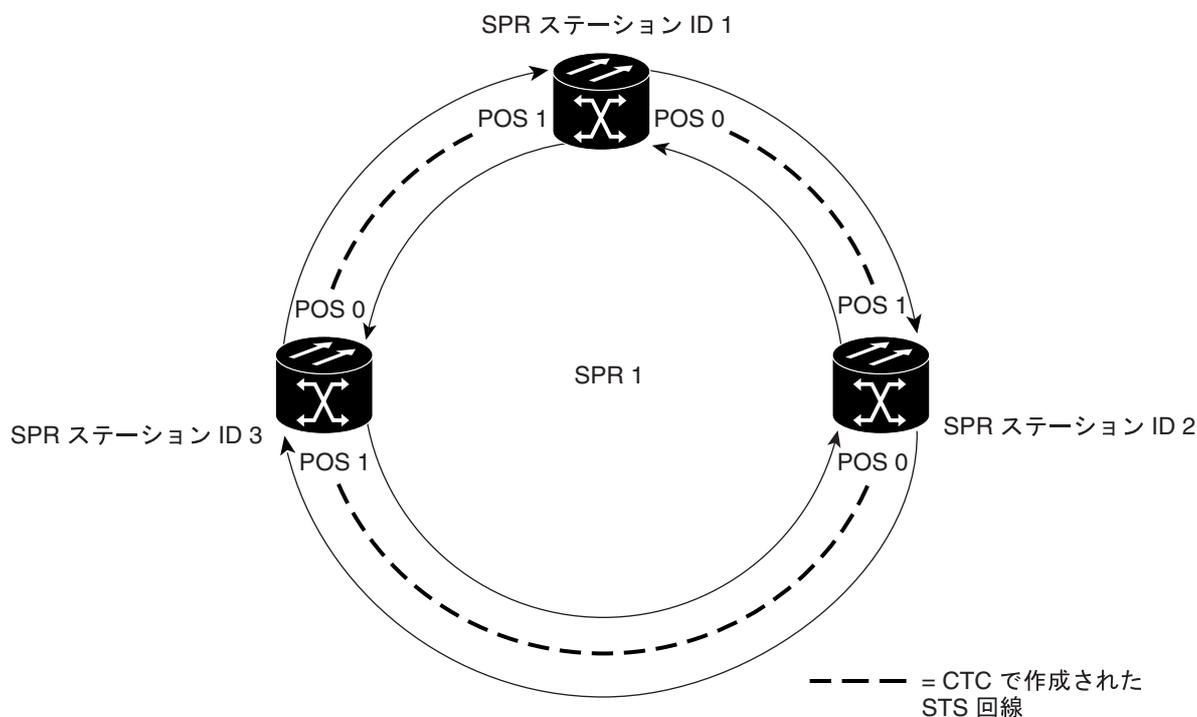


図 17-5 の 3 つのノードの RPR は、RPR の連続した手順のすべての例に使用します。これらの例を組み合わせると、RPR 作成のエンドツーエンドの例となります。SONET/SDH ノードとそのネットワークはすでにアクティブであると想定します。



### 注意

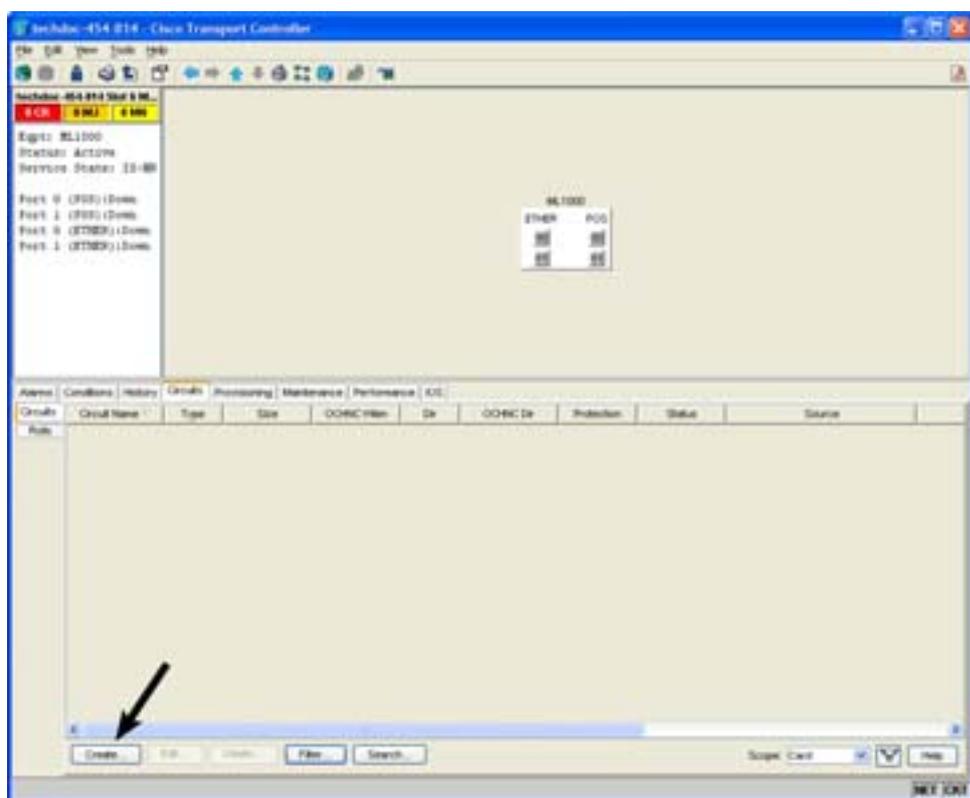
次の手順におけるステップは、例で示すトポロジー用の手順です。使用する手順は、ネットワークによって異なります。専門のネットワーク設計者による詳細な計画または方法を得ずに、この手順を実行しないでください。

回線を設定するには、CTC に次の 3 つの回線を作成します。

- ノード 1 の POS ポート 0 からノード 2 の POS ポート 1 へ回線を作成します。
- ノード 2 の POS ポート 0 からノード 3 の POS ポート 1 へ回線を作成します。
- ノード 3 の POS ポート 0 からノード 1 の POS ポート 1 へ回線を作成します。

**ステップ 1** CTC では、ノード 1 にログインして、RPR 内に存在する ML シリーズカードの CTC カードビューに移動します。

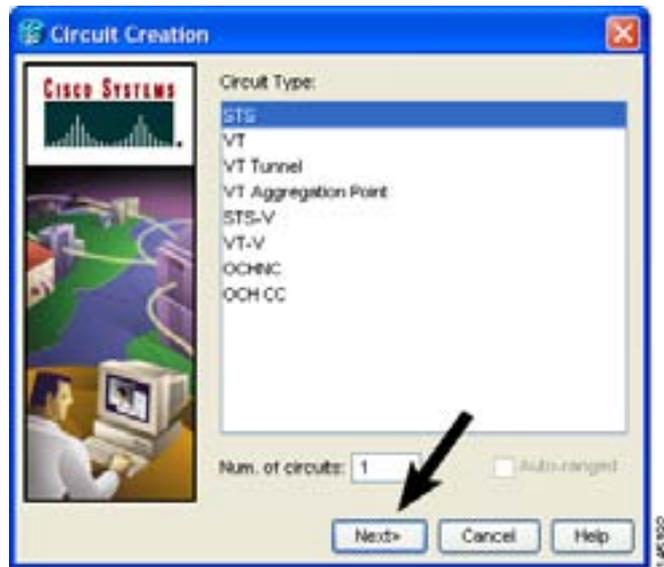
図 17-6 ML シリーズカードの CTC カードビュー



**ステップ 2** Circuits > Create タブをクリックします。

Circuit Creation ウィザードの最初のページが表示されます。

図 17-7 CTC Circuit Creation ウィザード



**ステップ 3** Circuit Type リストで、STS を選択します。

**ステップ 4** Next をクリックします。

Circuit Attributes ページが表示されます。

**ステップ 5** Name フィールドに回線名を入力します。

**ステップ 6** Size ドロップダウンリストから該当する回線のサイズを選択し、State リストから適切なステートを選択します。

**ステップ 7** SD スレッシュホールドが SD スレッシュホールド フィールドの  $1E-6$  (デフォルト) または  $1E-6$  ~  $1E-9$  の範囲に設定されていることを確認します。

- a. SD スレッシュホールドがデフォルトの  $1E-6$  または適切な範囲内である場合は、[ステップ 8](#) へ進みます。
- b. SD スレッシュホールドがデフォルトの  $1E-6$  でない場合、または適切な範囲内でない場合は、メニューから  $1E-6$  または適切な範囲内のスレッシュホールドを選択します。



**(注)** SD スレッシュホールド値を小さくすると CTC コンバージェンスの速度が速くなりますが、特定の状況ではインターフェイスのフラッピング (イネーブルとディセーブルの繰り返し) の可能性が高くなります。

**ステップ 8** Next をクリックします。

Source ページが表示されます。

**ステップ 9** Node ドロップダウン リストから ノード 1 を送信元ノードとして選択します。

**ステップ 10** Slot ドロップダウン リストから ML シリーズ カードを選択し、Port ドロップダウン リストから 0 (POS) を選択します。

**ステップ 11** Next をクリックします。

Destination ページが表示されます。

**ステップ 12** Node ドロップダウン リストから ノード 2 を宛先ノードとして選択します。

**ステップ 13** Slot ドロップダウン リストから ML シリーズ カードを選択し、Port ドロップダウン リストから 1 (POS) を選択します。

**ステップ 14** Next をクリックします。

Circuit Routing Preferences ページが表示されます。

**ステップ 15** Fully Protected Path チェック ボックスをオフにします。

**ステップ 16** Next をクリックします。

Circuit Constraints for Automatic Routing ページが表示されます。

**ステップ 17** ノード 1 アイコンをクリックして選択し、Next をクリックします。

Route Review/Edit ページが表示されます。

**ステップ 18** Finish をクリックします。

これで、RPR 用の最初の回線の設定が完了しました。



**(注)** 回線を作成すると、TPTFAIL アラームが CTC に表示される場合があります。POS ポートを「ML シリーズ カードの POS ポートの SPR インターフェイスへの割り当て (p.17-14)」の手順でイネーブルにすると、このアラームは消えます。

**ステップ 19** 2 番めの回線をノード 2 の POS 0 とノード 3 の POS 1 の間に作成します。ステップ 1 ~ 18 と同じ手順を使用します。ただし、ノード 1 をノード 2 に、ノード 2 をノード 3 に置き換えます。

**ステップ 20** 3 番めの回線をノード 3 の POS 0 とノード 1 の POS 1 の間に作成します。ステップ 1 ~ 18 と同じ手順を使用します。ただし、ノード 1 をノード 3 に、ノード 2 をノード 1 に置き換えます。

これにより、3 つのノードの POS ポートすべてが STS ポイントツーポイント回線によってイーストからウェストのパターンで接続されました (図 17-5 を参照)。

**ステップ 21** CTC 回線プロセスはこれで完了です。

## ML シリーズ カード上の RPR 特性と SPR インターフェイスの設定

ML シリーズ カードで RPR を設定するには、Cisco IOS の CLI (コマンドライン インターフェイス) から SPR インターフェイスを作成します。SPR インターフェイスは SPR の仮想インターフェイスです。1 枚の ML シリーズ カードは単一の MAC アドレスを持つ 1 つの SPR インターフェイスをサポートします。SPR インターフェイスは、デフォルト ルートのサポートなど、Cisco IOS インターフェイスの通常のすべての属性を提供します。

SPR インターフェイスは、EtherChannel (ポートチャネル) インターフェイスと同様に設定されます。channel-group コマンドを使用してメンバーを定義するのではなく、spr-intf-ID コマンドを使用します。ポートチャネルと同様に、物理 POS インターフェイスの代わりに仮想 SPR インターフェイスを設定します。SPR インターフェイスはトランク ポートとみなされるため、すべてのトランク ポートと同様に、SPR インターフェイスがブリッジグループに加入するようにサブインターフェイスを設定する必要があります。

ML シリーズ カードの物理 POS インターフェイスは、SPR インターフェイスに適した唯一のメンバーです。一方の POS ポートはノードから東方向にリングを回る SONET/SDH 回線と関連付けられ、もう一方の POS ポートは西方向の回線に関連付けられています。SPR インターフェイスを使用し、POS ポートが関連付けられている場合、RPR カプセル化を SONET/SDH ペイロードで使用します。



### 注意

SPR の設定時に、1 枚の ML シリーズ カードで SPR インターフェイスを設定せずに、有効な STS/STM 回線でこの ML シリーズ カードを SPR 内の他の ML シリーズ カードに接続すると、SPR 内で適切に設定された ML シリーズ カード間でトラフィックが流れなくなり、この状況を示すアラームも出ません。シスコでは、トラフィックを送信する前に、SPR 内のすべての ML シリーズ カードを設定することを推奨しています。



### 注意

ネイティブ VLAN を使用して RPR でトラフィックを伝送しないでください。



### (注)

ML シリーズ カードの RPR はデフォルトの LEX カプセル化でのみサポートされています。これは、Cisco ONS イーサネット ライン カードで使用される特別な CISCO-EOS-LEX カプセル化方式です。

RPR は、RPR 内に存在する各 ML シリーズ カード上でプロビジョニングする必要があります。RPR を設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>bridge irb</b>	Cisco IOS ソフトウェアで、1 枚の ML シリーズ カード内の個々のインターフェイスで特定のプロトコルをルーティングおよびブリッジングできるようにします。
ステップ 2	Router(config)# <b>interface spr 1</b>	ML シリーズ カードの SPR インターフェイスを作成するか、SPR 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。有効な SPR 番号は 1 だけです。

	コマンドの説明	目的
ステップ 3	Router(config-if)# <b>spr station-id</b> <i>station-ID-number</i>	ステーション ID を設定します。ユーザは、RPR に接続する各 SPR インターフェイスごとに異なる番号を設定する必要があります。有効なステーション ID 番号の範囲は、1 ~ 254 です。
ステップ 4	Router(config-if)# <b>spr wrap</b> { <b>immediate</b>   <b>delayed</b> }	(任意) RPR リングラップモードを、SONET/SDH パスアラーム検出したらただちにトラフィックをラップするか、200 ミリ秒の遅延後にトラフィックをラップするように設定します。これにより、不具合を記録してリンクダウンしていることを宣言する SONET/SDH 保護時間を指定します。RPR が SONET/SDH 非保護回線上で稼働している場合は、 <b>immediate</b> を使用します。Bidirectional Line Switched Ring (BLSR; 双方向ラインスイッチ型リング)、UPSR、Multiplex Section-Shared Protection Ring (MS-SPRing) または SNCP 保護回線には、 <b>delayed</b> を使用します。  デフォルトの設定は <b>immediate</b> です。
ステップ 5	Router(config-if)# <b>carrier-delay msec</b> <i>milliseconds</i>	(任意) キャリア遅延時間を設定します。デフォルトの設定は、200 ミリ秒です。これは、SONET/SDH 保護回線に最適な時間です。   (注) キャリア遅延時間をデフォルトから変更する場合、新しいキャリア遅延時間は、SPR、POS、およびギガビットイーサネットまたはファストイーサネットインターフェイスなど、ML シリーズカードのすべてのインターフェイスで設定する必要があります。
ステップ 6	Router(config-if)# <b>[no] spr load-balance</b> { <b>auto</b>   <b>port-based</b> }	(任意) ユニキャストパケットの RPR ロードバランシング方式を指定します。 <b>port-based</b> ロードバランシングオプションは、偶数のポートを POS 0 インターフェイスに、奇数のポートを POS 1 インターフェイスにマップします。デフォルトの <b>auto</b> オプションは、IP パケットの MAC (メディアアクセス制御) アドレスまたは送信元アドレスと宛先アドレスに基づいて負荷を分散します。
ステップ 7	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 8	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM (不揮発性 RAM) に保存します。

## ML シリーズ カードの POS ポートの SPR インターフェイスへの割り当て

**注意**

SPR インターフェイスは、ルーテッド インターフェイスです。レイヤ 3 アドレスをイネーブルにしたり、SPR インターフェイスに割り当てられた POS インターフェイスにブリッジ グループを割り当てたりしないでください。

**注意**

SPR インターフェイスの着信トラフィックでポリシングが必要な場合は、SPR インターフェイスの一部である両方の POS ポートに同じ入力サービス ポリシーを適用する必要があります。

RPR で使用するために、POS ポートは LEX カプセル化を必要とします。RPR 設定の最初のステップは、POS 0 ポートと POS 1 ポートのカプセル化を LEX に設定することです。

また、ML シリーズ カードの 2 つの POS ポートをそれぞれ SPR インターフェイスに割り当てる必要があります。LEX カプセル化を設定し、ML シリーズ カードの POS インターフェイスを SPR に割り当てるには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
<b>ステップ 1</b>	Router(config)# <b>interface pos 0</b>	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、SPR に割り当てる 1 つめの POS インターフェイスを設定します。
<b>ステップ 2</b>	Router(config-if)# <b>encapsulation lex</b>	POS インターフェイスのカプセル化を LEX として設定します (デフォルト)。ML シリーズ カードの RPR では、LEX カプセル化が必要です。
<b>ステップ 3</b>	Router(config-if)# <b>spr-intf-id</b> <i>shared-packet-ring-number</i>	POS インターフェイスを SPR インターフェイスに割り当てます。共有パケット リング番号は 1 である必要があります。この番号は、SPR インターフェイスに割り当てられる唯一の共有パケット リング番号です。
<b>ステップ 4</b>	Router(config-if)# <b>carrier-delay msec</b> <i>milliseconds</i>	(任意) キャリア遅延時間を設定します。デフォルトの設定は、200 ミリ秒です。これは、SONET/SDH 保護回線に最適な時間です。   <b>(注)</b> キャリア遅延時間の設定に使用するデフォルトの時間単位は秒です。msec コマンドは、時間単位をミリ秒にリセットします。

	コマンドの説明	目的
ステップ 5	Router(config-if)# <b>pos trigger defect ber_sd-b3</b>	<p>(任意) SONET/SDH ビットエラー レートが信号劣化アラームに設定されているスレッシュホールドを超えたときに、POS インターフェイスがダウンするようにトリガーを設定します。POS インターフェイスがダウンすると、RPR ラップを開始します。</p> <p>過度の SONET/SDH ビットエラーにより RPR トラフィックでパケット損失が発生する可能性があるため、すべての RPR POS インターフェイスに対してこのコマンドを使用することを推奨します。</p> <p> (注) Cisco ONS 15310 がリングの一部である場合、このコマンドを使用しないでください。RPR ラッピングが矛盾する可能性があります。</p>
ステップ 6	Router(config-if)# <b>no shutdown</b>	POS ポートをイネーブルにします。
ステップ 7	Router(config-if)# <b>interface pos 1</b>	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、SPR に割り当てる 2 つめの POS インターフェイスを設定します。
ステップ 8	Router(config-if)# <b>encapsulation lex</b>	POS インターフェイスのカプセル化を LEX として設定します (デフォルト)。ML シリーズカードの RPR では、LEX カプセル化が必要です。
ステップ 9	Router(config-if)# <b>spr-intf-id shared-packet-ring-number</b>	POS インターフェイスを SPR インターフェイスに割り当てます。共有パケット リング番号は 1 である必要があります (ステップ 3 で割り当てた共有パケット リング番号と同じ番号)。この番号は、SPR インターフェイスに割り当てられる唯一の共有パケット リング番号です。
ステップ 10	Router(config-if)# <b>carrier-delay msec milliseconds</b>	(任意) キャリア遅延時間を設定します。デフォルトの設定は、200 ミリ秒です。これは、SONET/SDH 保護回線に最適な時間です。
ステップ 11	Router(config-if)# <b>pos trigger defect ber_sd-b3</b>	<p>(任意) SONET/SDH ビットエラー レートが信号劣化アラームに設定されているスレッシュホールドを超えたときに、POS インターフェイスがダウンするようにトリガーを設定します。POS インターフェイスがダウンすると、RPR ラップを開始します。</p> <p>過度の SONET/SDH ビットエラーにより RPR トラフィックでパケット損失が発生する可能性があるため、すべての RPR POS インターフェイスに対してこのコマンドを使用することを推奨します。</p>
ステップ 12	Router(config-if)# <b>no shutdown</b>	POS ポートをイネーブルにします。
ステップ 13	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 14	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM に保存します。

## ブリッジグループの作成とイーサネットおよび SPR インターフェイスの割り当て

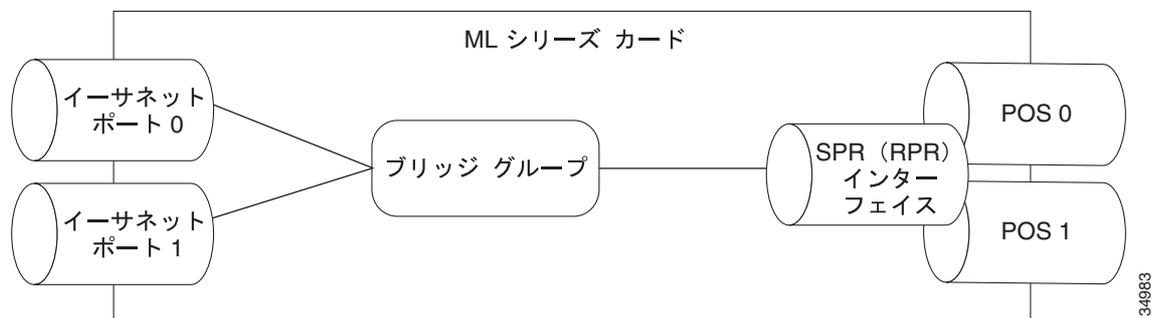
ML シリーズ カードのデフォルト動作では、インターフェイスがイネーブルであってもトラフィックは RPR 上でブリッジされません。これは、Cisco Catalyst 6500 や Cisco Catalyst 7600 を含めた多くのレイヤ 2 スイッチとは対照的です。これらのスイッチはデフォルトでは VLAN 1 を転送します。ML シリーズ カードは、タグなしパケットまたは VLAN 1 タグ付きパケットを含め、デフォルトではトラフィックを転送しません。

ML シリーズ カードでブリッジされる RPR トラフィックの場合、そのトラフィック用にブリッジグループを作成する必要があります。ブリッジグループは ML シリーズ カードのインターフェイス間でブリッジングおよび転送を維持するので、ローカルでは重要です。ブリッジグループに参加していないインターフェイスは、ブリッジドトラフィックを転送できません。

RPR 用のブリッジグループを作成するには、同じブリッジグループ内に含める必要のあるイーサネット インターフェイスを決定し、ブリッジグループを作成し、これらのインターフェイスとブリッジグループを関連付けます。次に、RPR インフラストラクチャ上での転送を行うため、SPR インターフェイスおよび同じブリッジグループを関連付けます。

図 17-8 に、RPR の SPR 仮想インターフェイスを含めた ML シリーズ カード インターフェイスをスパニングするブリッジグループを示します。

図 17-8 RPR ブリッジグループ



### 注意

適切な RPR 運用のため、RPR トポロジー以外の、接続ネットワーク内のレイヤ 2 ネットワーク冗長リンク（ループ）をすべて削除する必要があります。ループが存在する場合、STP/RSTP を設定する必要があります。

必要なインターフェイスを設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>interface</b> type number	イーサネット インターフェイスをブリッジグループに参加させるため、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 2	Router(config-if)# <b>no shutdown</b>	インターフェイスをイネーブルにします。

	コマンドの説明	目的
ステップ 3	Router(config-if)# <b>bridge-group</b> <i>bridge-group-number</i>	特定のブリッジグループを作成し、そのブリッジグループをインターフェイスに割り当てます。インターフェイス コンフィギュレーションからブリッジを作成すると、STP または RSTP がディセーブルになります (spanning-disabled)。これは RPR に推奨されません。
ステップ 4	Router(config)# <b>interface spr1</b>	SPR 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 5	Router(config-subif)# <b>bridge-group</b> <i>bridge-group-number</i>	SPR インターフェイスを特定のブリッジグループに関連付けます。

## RPR Cisco IOS の設定例

図 17-5 に、RPR Cisco IOS の完全な設定例を示します。関連する Cisco IOS コードは、17-1、17-2、17-3 に示します。この設定は、ML シリーズカードの POS ポートが、CTC から設定されたポイントツーポイント SONET/SDH 回線によって、すでにリンクされていることを前提としています。

### 例 17-1 SPR ステーション ID 1 の設定

```
bridge irb

interface SPR1
no ip address
no keepalive
spr station-id 1
bridge-group 10
bridge-group 10 spanning-disabled
hold-queue 150 in

interface GigabitEthernet0
no ip address
bridge-group 10
bridge-group 10 spanning-disabled

interface GigabitEthernet1
no ip address
shutdown

interface POS0
no ip address
carrier-delay msec 0
spr-intf-id 1
crc 32

interface POS1
no ip address
carrier-delay msec 0
spr-intf-id 1
crc 32
!
```

**例 17-2 SPR ステーション ID 2 の設定**

```
bridge irb

interface SPR1
no ip address
no keepalive
spr station-id 2
bridge-group 10
bridge-group 10 spanning-disabled

interface GigabitEthernet0
no ip address
bridge-group 10
bridge-group 10 spanning-disabled

interface GigabitEthernet1
no ip address
shutdown

interface POS0
no ip address
shutdown
spr-intf-id 1
crc 32

interface POS1
no ip address
spr-intf-id 1
crc 32
```

**例 17-3 SPR ステーション ID 3 の設定**

```
bridge irb

interface SPR1
no ip address
no keepalive
spr station-id 3
bridge-group 10
bridge-group 10 spanning-disabled
hold-queue 150 in

interface GigabitEthernet0
no ip address
bridge-group 10
bridge-group 10 spanning-disabled

interface GigabitEthernet1
no ip address
shutdown

interface POS0
no ip address
spr-intf-id 1
crc 32

interface POS1
no ip address
spr-intf-id 1
crc 32
!
```

## RPR イーサネット アクセス ポート間のイーサネット接続の確認

RPR のプロビジョニング手順が終了したあと、標準イーサネット接続テストを使用して、個別の ML シリーズ カード上のイーサネット アクセス ポート間のイーサネット接続をテストします。

## RPR のモニタリングおよび確認

RPR を設定したあと、`show interface spr 1` コマンド (例 17-4) または `show run interface spr 1` コマンド (例 17-5) を使用して、RPR のステータスをモニタリングできます。

### 例 17-4 show interface spr 1 の出力例

```
ML-Series# show interfaces spr 1

SPR1 is up, line protocol is up
  Hardware is POS-SPR, address is 0005.9a39.77f8 (bia 0000.0000.0000)
  MTU 1500 bytes, BW 290304 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation: Cisco-EoS-LEX, loopback not set
  Keepalive not set
  DTR is pulsed for 27482 seconds on reset, Restart-Delay is 65 secs
  ARP type: ARPA, ARP Timeout 04:00:00
    No. of active members in this SPR interface: 2
      Member 0 : POS1
      Member 1 : POS0
  Last input 00:00:38, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/150/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/80 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    37385 packets input, 20993313 bytes
    Received 0 broadcasts (0 IP multicast)
    0 runts, 0 giants, 0 throttles
      0 parity
    2 input errors, 2 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
  37454 packets output, 13183808 bytes, 0 underruns
    0 output errors, 0 applique, 4 interface resets
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
```

### 例 17-5 show run interface spr 1 の出力例

```
ML-Series# show run interface spr 1

Building configuration...
Current configuration : 141 bytes
interface SPR1
 no ip address
 no keepalive
 spr station-id 2
 bridge-group 10
 bridge-group 10 spanning-disabled
 hold-queue 150 in
end
```

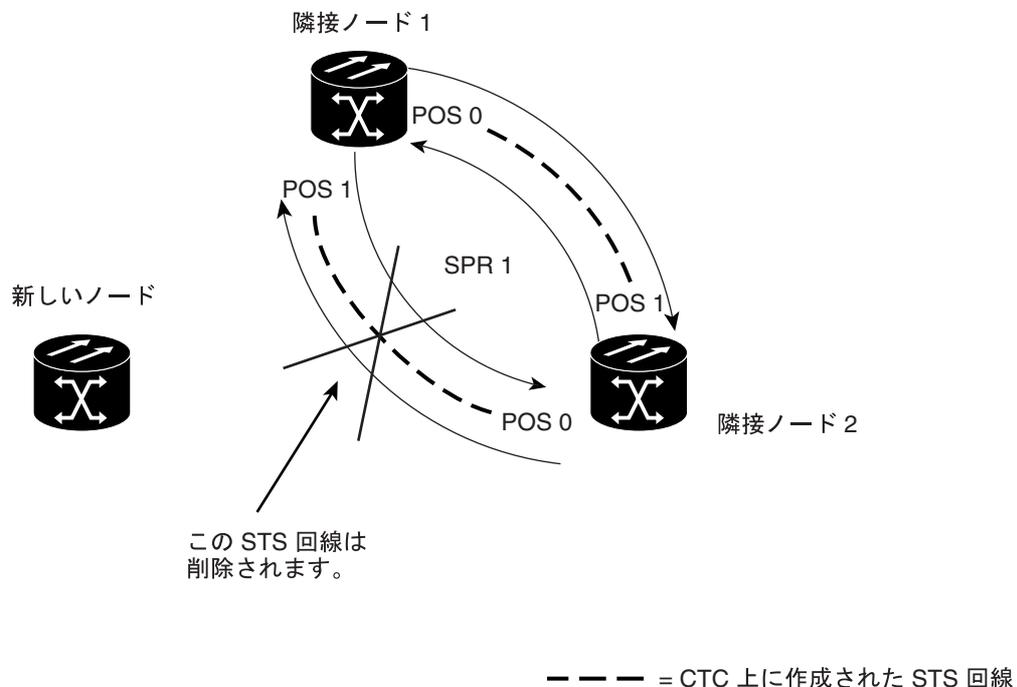
## ML シリーズカードの RPR への追加

既存の RPR は、ML シリーズカードを追加する必要があります。RPR ラッピング機能とリングアーキテクチャにより、データトラフィックをダウンさせることなく、追加できます。ML シリーズカードは、カードを含んだノードを含んだリードとともに、基盤となる SONET/SDH アーキテクチャに追加できます。すでに SONET/SDH トポロジーの一部であるノードに、ML シリーズカードを追加することもできます。

次の例では、ML シリーズカードを接続する 2 つの STS 回線を持った 2 ノードの RPR の例を示します。回線の 1 つは削除されます。RPR は、ping 損失を最小限にして、残りの回線上でトラフィックをラップします。そのあと 3 番めのノードと ML シリーズカードが追加され、このカード用にスパンと回線が作成されます。

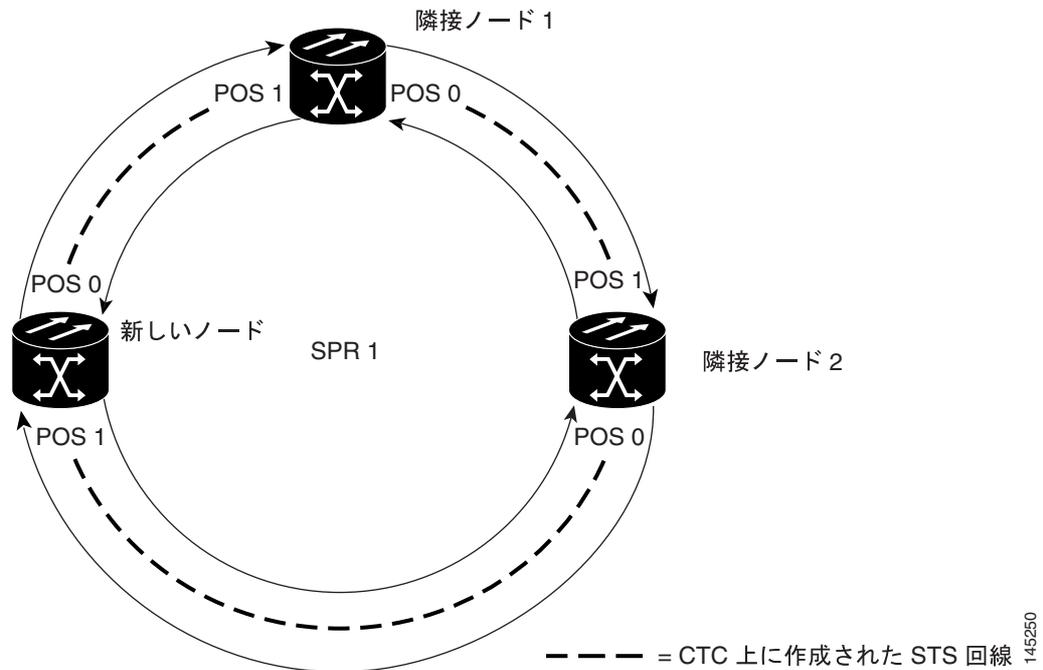
図 17-9 に、削除される単一 STS 回線とスパンを持った既存の 2 ノードの RPR を示します。図 17-10 に、追加される新しい 2 つの STS 回線、およびスパンが 3 番めのノードに追加されたあとの RPR を示します。

図 17-9 追加前の 2 つのノードの RPR



145252

図 17-10 追加後の 3 ノードの RPR



ML シリーズ カードを RPR に追加するには、次の一般的な手順を実行する必要があります。

- 削除するスパンを使用する既存の非 ML シリーズ カード回線 (DS-1 など) を遠ざけます。
- RPR ラップを開始するため、削除する STS 回線の隣接する ML シリーズ カードの POS ポートをシャットダウンします。
- RPR ラップが正常に行われたことを確認するため、テスト セットを使用して、既存の隣接 ML シリーズ カードのアクセス ポート間のイーサネット接続をテストします。
- 新しい回線で置き換えられる STS 回線を削除します (図 17-9 では、POS 0 の隣接ノード 2 と POS 1 の隣接ノード 1 間の回線です)。
- ノードがトポロジーの一部ではない場合、新しいノードをリング トポロジーに接続します。
- ML シリーズ カードを接続し、初期コンフィギュレーション ファイルをロードするか、または ML シリーズ カードを初期設定します。
- POS ポートを手動でイネーブルにするか、またはコンフィギュレーション ファイルを介してイネーブルにする前に、新しいノードに RPR が設定されていることを確認してください。
- 既存の隣接 ML シリーズ カードの POS ポートの 1 つから、新しい ML シリーズ カードの POS ポートへの STS 回線を作成します (図 17-10 では、POS ポート 0 の隣接ノード 2 と POS ポート 1 の新しいノード間の回線です)。
- 別の既存の隣接 ML シリーズ カードの POS ポートの 1 つから、新しい ML シリーズ カードの残りの POS ポートへの 2 番目の STS 回線を作成します (図 17-10 では、POS ポート 0 の新しいノードと POS ポート 1 の隣接ノード 1 間の回線です)。
- 初期コンフィギュレーション ファイルが RPR に参加し、POS ポートをイネーブルにしなかった場合、新しい ML シリーズ カードがこれを実行するよう設定します。
- 新しい ML シリーズ カードに接続された既存の隣接 ML シリーズ カード上で POS ポートをイネーブルにします (図 17-10 では、POS ポート 1 の隣接ノード 1 と POS ポート 0 の隣接ノード 2 です)。
- 新しく作成された 3 ノードの RPR を検証するため、テスト セットを使用して、新しい ML シリーズ カードのアクセス ポート間のイーサネット接続をテストします。

## ■ ML シリーズカードの RPR への追加

- ノードの挿入後、最低 1 時間以上は、イーサネット トラフィックと既存のルーティング プロトコルをモニタリングします。



## 注意

次の手順におけるステップは、例で示すトポロジー用の手順です。使用する手順は、ネットワーク設計によって異なります。専門のネットワーク設計者による詳細な計画または方法を得ずに、この手順を実行しないでください。

## ML シリーズカードの RPR への追加

ML シリーズカードを例に示す RPR に追加するには、次の手順を実行します。

**ステップ 1** 最初の隣接ノードの ML シリーズカードの Cisco IOS CLI セッションを開始します。これは、[図 17-9](#) の隣接ノード 1 です。

**ステップ 2** グローバル コンフィギュレーション モードを開始して、最初の隣接ノードの ML シリーズカード上で次の Cisco IOS コンフィギュレーションを完了します。

a. Router(config)# <b>interface pos</b> <i>interface-number</i>	削除する回線の 1 つのエンドポイントで、POS ポート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。
b. Router(config-if)# <b>shutdown</b>	インターフェイスを閉じて、RPR ラップを開始します。

**ステップ 3** [図 17-9](#) で示す隣接ノード 2 の ML シリーズカードの Cisco IOS CLI セッションを開始します。

**ステップ 4** グローバル コンフィギュレーション モードを開始して、隣接ノード 2 の ML シリーズカード上で次の Cisco IOS コンフィギュレーションを完了します。

a. Router(config)# <b>interface pos</b> <i>interface-number</i>	削除する回線の 1 つのエンドポイントで、POS ポート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。
b. Router(config-if)# <b>shutdown</b>	インターフェイスを閉じます。

**ステップ 5** CTC で、隣接ノード 1 にログインします。

**ステップ 6** 隣接ノード 1 の ML シリーズカードをダブルクリックします。

カード ビューが表示されます。

**ステップ 7** **Circuits** タブをクリックします。

**ステップ 8** **Circuits** サブタブをクリックします。

**ステップ 9** 削除する回線のエンドポイントで POS ポートと一致する回線エントリの送信元カラムと宛先カラムを参照して、適切な STS 回線を特定します。

回線エントリは、Node-1/s12(ML100T)/pPOS-0 などのように *node-name/card-slot/port-number* 形式になっています。

**ステップ 10** ハイライトする回線エントリをクリックします。

**ステップ 11** Delete をクリックします。

confirmation ダイアログ ボックスが表示されます。

**ステップ 12** Yes をクリックします。

**ステップ 13** テスト セットを使用して、隣接ノード 1 のイーサネット アクセス ポートと隣接ノード 2 のイーサネット アクセス ポート間にイーサネット接続がまだ存在するかどうかを確認します。



**(注)** ML シリーズ カードの SPR インターフェイスおよびイーサネット インターフェイスは、RPR トラフィックが RPR をブリッジングするため、ブリッジ グループに存在する必要があります。

**ステップ 14** 新しいノードが SONET/SDH リング トポロジーでまだアクティブ ノードではない場合、ノードをリングに追加します。ONS ノードの設置手順については、『Cisco ONS 15454 Procedure Guide』の「Add and Remove Nodes」の章、または『Cisco ONS 15454 SDH Procedure Guide』の「Add and Remove Nodes」の章を参照してください。

**ステップ 15** 新しいノードの ML シリーズ カードがまだ取り付けられていない場合、新しいカードをそのノードに取り付けます。カードの ONS ノードへの取り付け手順については、『Cisco ONS 15454 Procedure Guide』の「Install Cards and Fiber-Optic Cable」の章、または『Cisco ONS 15454 SDH Procedure Guide』の「Install Cards and Fiber-Optic Cable」の章を参照してください。

**ステップ 16** 新しい ML シリーズ カードの初期スタートアップ コンフィギュレーション ファイルをアップロードします(「CTC での Cisco IOS スタートアップ コンフィギュレーション ファイルのロード」[p.3-11]を参照)。スタートアップ コンフィギュレーション ファイルの準備ができていない場合、「シリアル コンソール ポートを使用して手動でスタートアップ コンフィギュレーション ファイルを作成する方法」(p.3-9)を参照してください。



**注意**

POS ポートを手動でイネーブルにするか、またはコンフィギュレーション ファイルを介してイネーブルにする前に、新しいノードに RPR が設定されていることを確認してください。

**ステップ 17** 回線ステートが In-Service (IS) である STS 回線を、隣接ノード 1 の利用可能な POS ポートから新しいノードに作成します(図 17-10 を参照)。新しいノードでは、隣接ノード 1 の利用可能な POS ポートのインターフェイス番号と一致しないインターフェイス番号の付いた POS ポートを使用します。たとえば、隣接ノード 1 の POS ポート 0 は新しいノードの POS ポート 1 に接続します。

回線接続手順の詳細については、「RPR の CTC 回線の設定」(p.17-7)を参照してください。



**(注)** 最良の方法は、イーストからウェスト、またはウェストからイーストに SONET/SDH 回線を設定することです。つまり、SONET/SDH リングで、ポート 0 (イースト) からポート 1 (ウェスト)、またはポート 1 (ウェスト) からポート 0 (イースト) のように設定します。

## ■ ML シリーズカードの RPR への追加

**ステップ 18** 回線ステートが IS である STS 回線を、隣接ノード 2 の利用可能な POS ポートから新しいノードの残りの POS ポートに作成します (図 17-10 を参照)。

**ステップ 19** 図 17-9 で示す隣接ノード 1 の ML シリーズカードの Cisco IOS CLI セッションを開始または再開します。

**ステップ 20** グローバル コンフィギュレーション モードを開始して、次の Cisco IOS コンフィギュレーションを完了します。

a. Router(config)# <b>interface pos</b> <i>interface-number</i>	新しく最初に作成した回線の 1 つのエンドポイントで、POS ポート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。
b. Router(config-if)# <b>no shutdown</b>	ポートをイネーブルにします。

**ステップ 21** 図 17-9 で示す隣接ノード 2 の ML シリーズカードの Cisco IOS CLI セッションを開始します。

**ステップ 22** グローバル コンフィギュレーション モードを開始して、隣接ノード 2 の ML シリーズカード上で次の Cisco IOS コンフィギュレーションを完了します。

a. Router(config)# <b>interface pos</b> <i>interface-number</i>	新しく 2 番めに作成した回線の 1 つのエンドポイントで、POS ポート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。
b. Router(config-if)# <b>no shutdown</b>	ポートをイネーブルにします。

**ステップ 23** イーサネット接続が RPR に存在するかどうか確認するため、テスト セットを使用します。

**ステップ 24** ノードの挿入後、最低 1 時間以上は、イーサネット トラフィックとルーティング テーブルをモニタリングします。

**終了。手順はこれで完了です。**

## RPR からの ML シリーズカードの削除

既存の RPR は、ML シリーズカードを削除する必要があります。RPR ラッピング機能とリングアーキテクチャにより、データトラフィックをダウンさせることなく、削除できます。

次の例では、ML シリーズカードを接続する 3 つの STS 回線を持った 3 ノードの RPR の例を示します。回線の 2 つは削除されます。RPR は、ping 損失を最小限にして、残りの回線でトラフィックをラップします。そのあと、3 番めのノードと ML シリーズカードは削除され、新しい STS 回線が残りのカード間に作成されます。

図 17-11 に、3 つの STS 回線とスパンを持った既存の 3 ノードの RPR を示します。図 17-12 に、3 番めのノード、回線、スパンが削除され、新しい STS 回線が追加されたあとの RPR を示します。

図 17-11 削除前の 3 つのノードの RPR

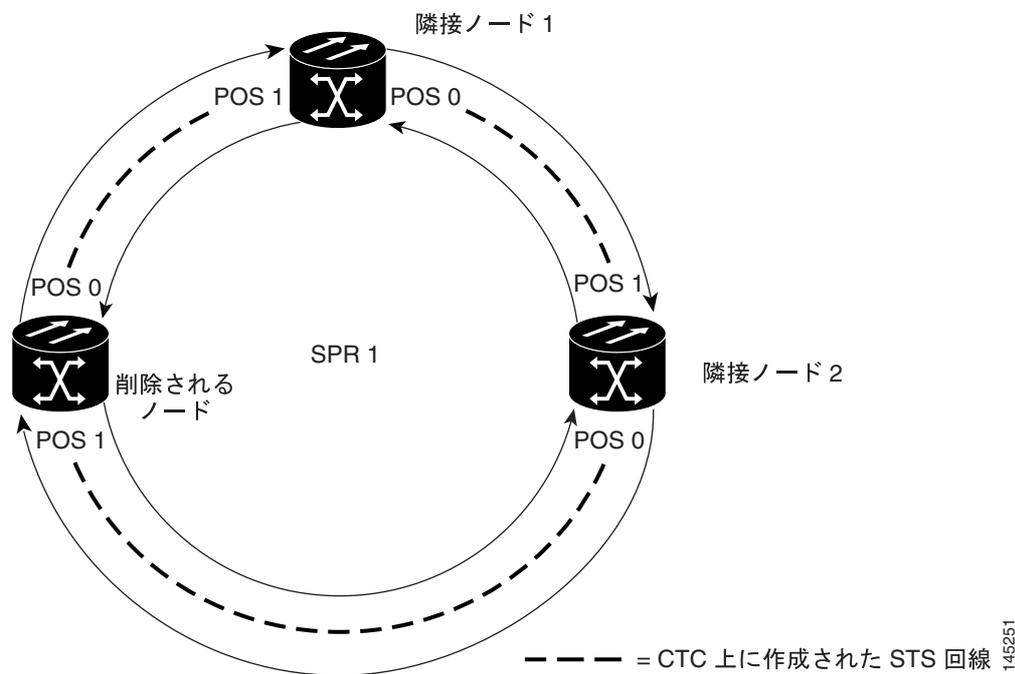
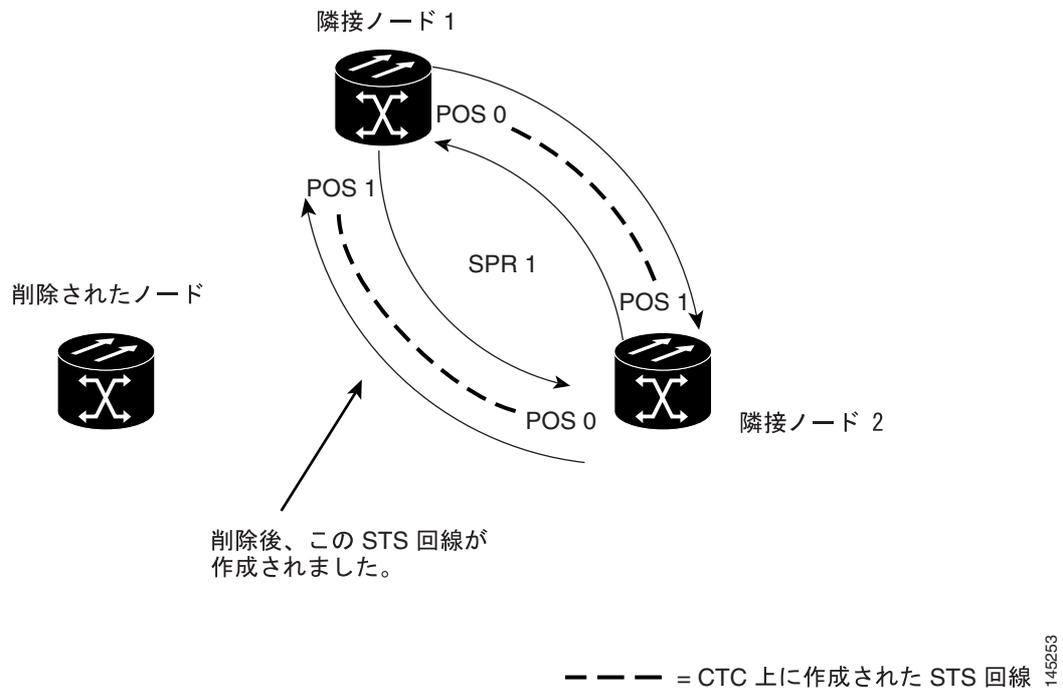


図 17-12 削除後の 2 つのノードの RPR



ML シリーズカードを RPR から削除するには、次の一般的な手順を実行する必要があります。

- 削除するスパンを使用する既存の非 ML シリーズカード回線（DS-1 など）を遠ざけます。
- RPR ラップを開始するため、削除する STS 回線の隣接する ML シリーズカードの POS ポートをシャットダウンします。
- RPR ラップが正常に行われたことを確認するため、テストセットを使用して、既存の隣接 ML シリーズカードのアクセスポート間のイーサネット接続をテストします。
- 新しい回線で置き換えられる 2 つの STS 回線を削除します（図 17-11 では、削除ノードと隣接ノード間の回線および削除ノードと別の隣接ノード間の回線です）。
- 必要に応じて、リングトポロジーから削除ノードを削除します。
- 必要に応じて、ノードから削除 ML シリーズカードを物理的に取り外します。
- 残りの隣接 ML シリーズカードのうちの 1 枚の利用可能な POS ポートから、別の残りの隣接 ML シリーズカードの利用可能な POS ポートへ STS 回線を作成します（図 17-12 では、POS ポート 0 の隣接ノード 2 と POS ポート 1 の隣接ノード 1 間の回線です）。
- 既存の隣接 ML シリーズカードの POS ポートをイネーブルにします（図 17-12 では、POS ポート 0 の隣接ノード 2 と POS ポート 1 の隣接ノード 1 です）。
- 2 ノードの RPR を検証するため、テストセットを使用して、隣接 ML シリーズカードのアクセスポート間のイーサネット接続をテストします。
- ノードの削除後、最低 1 時間以上は、イーサネットトラフィックと既存のルーティングプロトコルをモニタリングします。



#### 注意

次の手順におけるステップは、例で示すトポロジー用の手順です。使用する手順は、ネットワーク設計によって異なります。専門のネットワーク設計者による詳細な計画または方法を得ずに、この手順を実行しないでください。

## RPR からの ML シリーズカードの削除

RPR から ML シリーズカードを削除するには、次の手順を実行します。

**ステップ 1** 最初の隣接ノードの ML シリーズカードの Cisco IOS CLI セッションを開始します。これは、[図 17-11](#) の隣接ノード 1 です。

**ステップ 2** グローバル コンフィギュレーション モードを開始して、最初の隣接ノードの ML シリーズカード上で次の Cisco IOS コンフィギュレーションを完了します。

a. Router(config)# <b>interface pos</b> <i>interface-number</i>	回線の最後で削除ノードに直接接続されている POS ポート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。
b. Router(config-if)# <b>shutdown</b>	インターフェイスを閉じて、RPR ラップを開始します。

**ステップ 3** [図 17-11](#) で示す隣接ノード 2 の ML シリーズカードの Cisco IOS CLI セッションを開始します。

**ステップ 4** グローバル コンフィギュレーション モードで、隣接ノード 2 の ML シリーズカード上で次の Cisco IOS コンフィギュレーションを完了します。

a. Router(config)# <b>interface pos</b> <i>interface-number</i>	回線の最後で削除ノードに直接接続されている POS ポート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。
b. Router(config-if)# <b>shutdown</b>	インターフェイスを閉じます。

**ステップ 5** CTC を使用して隣接ノード 1 にログインします。

**ステップ 6** 隣接ノード 1 の ML シリーズカードをダブルクリックします。

カード ビューが表示されます。

**ステップ 7** **Circuits** タブをクリックします。

**ステップ 8** **Circuits** サブタブをクリックします。

**ステップ 9** 最初に削除する回線のエンドポイントで POS ポートと一致する回線エントリの送信元カラムと宛先カラムを参照して、適切な STS 回線を特定します。

回線エントリは、Node-1/s12(ML100T)/pPOS-0 などのように *node-name/card-slot/port-number* 形式になっています。

**ステップ 10** ハイライトする回線エントリをクリックします。

**ステップ 11** **Delete** をクリックします。

confirmation ダイアログ ボックスが表示されます。

**ステップ 12** **Yes** をクリックします。

**ステップ 13** テストセットを使用して、隣接ノード 1 のイーサネットアクセスポートと隣接ノード 2 のイーサネットアクセスポートの間にイーサネット接続がまだ存在するかどうかを確認します。



**(注)** ML シリーズカードの SPR インターフェイスおよびイーサネットインターフェイスは、RPR トラフィックが RPR をブリッジングするため、ブリッジグループに存在する必要があります。

**ステップ 14** CTC を使用して隣接ノード 2 にログインします。

**ステップ 15** 隣接ノード 2 の ML シリーズカードをダブルクリックします。

カードビューが表示されます。

**ステップ 16** Circuits タブをクリックします。

**ステップ 17** Circuits サブタブをクリックします。

**ステップ 18** 2 番めに削除する回線のエンドポイントで POS ポートと一致する回線エントリの送信元カラムと宛先カラムを参照して、適切な STS 回線を特定します。

回線エントリは、Node-1/s12(ML100T)/pPOS-0 などのように *node-name/card-slot/port-number* 形式になっています。

**ステップ 19** ハイライトする回線エントリをクリックします。

**ステップ 20** Delete をクリックします。

confirmation ダイアログボックスが表示されます。

**ステップ 21** Yes をクリックします。

**ステップ 22** 新しいノードが SONET/SDH リングトポロジでアクティブノードにならない場合、ノードをリングから削除します。ONS ノードの削除手順については、『Cisco ONS 15454 Procedure Guide』の「Add and Remove Nodes」の章、または『Cisco ONS 15454 SDH Procedure Guide』の「Add and Remove Nodes」の章を参照してください。

**ステップ 23** 新しいノードの ML シリーズカードを CTC で削除し、物理的に取り外す必要がある場合は、そのようにしてください。カードの ONS ノードへの取り付け手順については、『Cisco ONS 15454 Procedure Guide』の「Install Cards and Fiber-Optic Cable」の章、または『Cisco ONS 15454 SDH Procedure Guide』の「Install Cards and Fiber-Optic Cable」の章を参照してください。

**ステップ 24** 回線状態が IS である STS 回線を、隣接ノード 1 の利用可能な POS ポートから隣接ノード 2 の利用可能な POS ポートに作成します (図 17-12 を参照)。回線接続手順の詳細については、「RPR の CTC 回線の設定」(p.17-7)を参照してください。



**(注)** 最良の方法は、イーストからウェスト、またはウェストからイーストに SONET/SDH 回線を設定することです。つまり、SONET/SDH リングで、ポート 0 (イースト) からポート 1 (ウェスト)、またはポート 1 (ウェスト) からポート 0 (イースト) のように設定します。

**ステップ 25** 隣接ノード 1 の ML シリーズカードの Cisco IOS CLI セッションを開始または再開します。

**ステップ 26** グローバル コンフィギュレーション モードを開始して、隣接ノード 1 の ML シリーズカードの次の Cisco IOS コンフィギュレーションを完了します。

a. Router(config)# <b>interface pos</b> <i>interface-number</i>	新しく最初に作成した回線の 1 つのエンドポイントで、POS ポート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。
b. Router(config-if)# <b>no shutdown</b>	ポートをイネーブルにします。

**ステップ 27** 隣接ノード 2 の ML シリーズカードの Cisco IOS CLI セッションを開始します。

**ステップ 28** グローバル コンフィギュレーション モードを開始して、隣接ノード 2 の ML シリーズカード上で次の Cisco IOS コンフィギュレーションを完了します。

a. Router(config)# <b>interface pos</b> <i>interface-number</i>	新しく 2 番めに作成した回線の 1 つのエンドポイントで、POS ポート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。
b. Router(config-if)# <b>no shutdown</b>	ポートをイネーブルにします。

**ステップ 29** イーサネット接続が RPR に存在するかどうか確認するため、テスト セットを使用します。

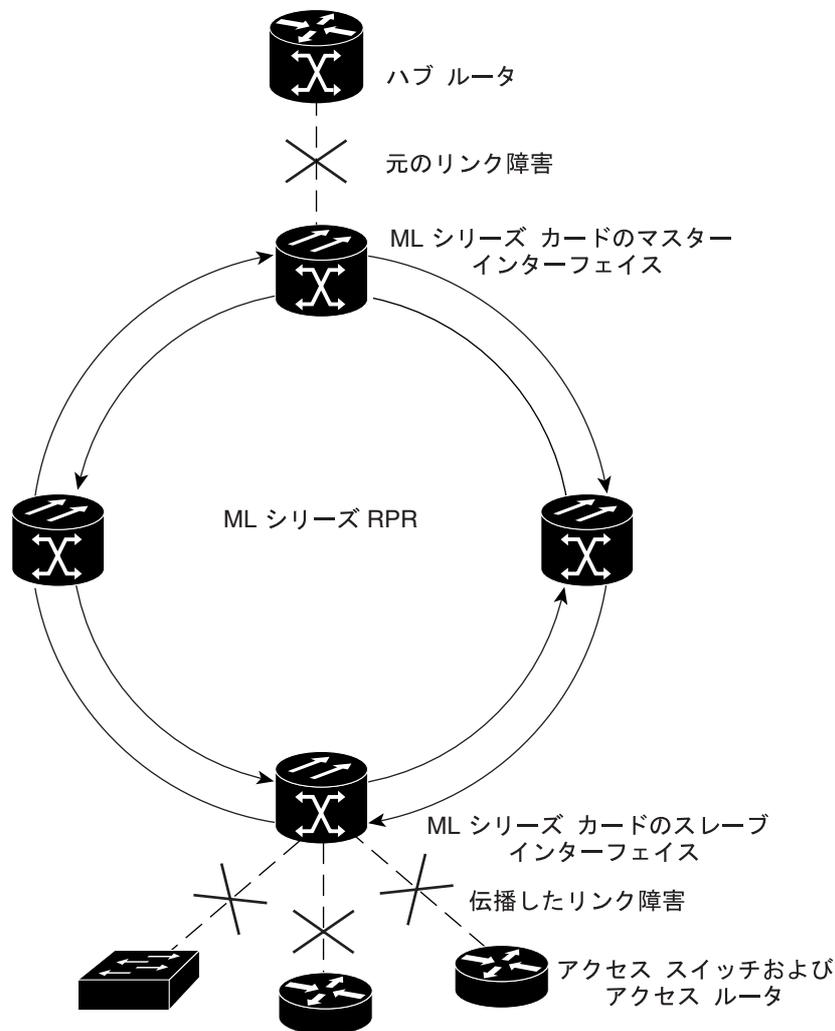
**ステップ 30** ノードの削除後、最低 1 時間以上は、イーサネット トラフィックとルーティング テーブルをモニタリングします。

**終了。手順はこれで完了です。**

## RPR LFP の概要

Link Fault Propagation (LFP) は、リンク パススルーとしても知られ、ルータが ML シリーズ カードの RPR で相互接続されているネットワーク内でコンバージェンス時間を短縮します。LFP は、マスター ギガビット イーサネット リンクからギガビット イーサネットやファストイーサネットのリモート スレーブ リンクへリンク障害をすばやく中継します。LFP により、スレーブ リンクに接続されたルータから代替パスへのフェールオーバーの時間が大幅に改善されます。通常の保護方式では、コンバージェンス時間は 40 秒くらいとなります。LFP を使用すると、スレーブ インターフェイスはマスター インターフェイスの状態を 1 秒未満で反映します。この機能は多くの場合、遠端ハブ サイトのリンク障害をトリガーとして、近端アクセス サイトをリンク ダウン状態にするために使用します。図 17-13 に LFP を示します。

図 17-13 RPR リンク障害の伝播例



131696

## LFP シーケンス

LFP の更新は CDP パケット拡張で行われます。更新は定期的には送信されますが、マスター インターフェイスでリンクダウン状態になった場合は、ただちに送信されます。LFP の更新は通常の Cisco Discovery Protocol (CDP) パケットとは別に送信され、これらは互いに影響し合うことはありません。インターフェイス上で CDP を設定したり、ディセーブルにしても LFP の更新には影響しません。

管理上の理由でシャットダウンする場合も含め、マスター インターフェイスがダウンすると、スレーブ インターフェイスが強制的にダウンします。マスター インターフェイスがアップ状態になると、スレーブ インターフェイスもアップ状態に戻ります。スレーブ インターフェイスを管理上の理由でシャットダウンすると、スレーブ インターフェイスで LFP 機能が一時停止します。スレーブ インターフェイスを再度起動すると、LFP 機能が再開します。

マスターからスレーブへの接続で障害があると、スレーブ リンクでもまたリンクのダウン障害が強制的に起こります。接断の原因を次に示します。

- マスター ML シリーズカードの取り外しまたは再設置
- マスターとスレーブ間の両方の RPR パスでのシャットダウンまたは障害
- マスター インターフェイス上での LFP のディセーブル

リンク障害はマスターからスレーブへのみ伝播されます。通常のスレーブのリンク障害は伝播されません。RPR のラッピングとラッピングの解除は LFP には影響しません。

## 伝播遅延

伝播遅延には、スレーブ インターフェイスでのキャリア遅延時間も含まれます。キャリア遅延時間は設定可能で、そのデフォルト値は 200 ミリ秒です。キャリア遅延時間の設定の詳細については、「[RPR の設定](#)」(p.17-7)を参照してください。

伝播遅延にはそれぞれ、異なる LFP のシナリオがあります。

- マスターのリンクダウンとスレーブのリンクダウンの間の伝播遅延は、50 ミリ秒にスレーブ インターフェイスでのキャリア遅延時間を加えたものです。
- マスターのリンクアップとスレーブのリンクアップの間の伝播遅延には、インターフェイスのフラッピングを防止するために、マスター インターフェイスでの組み込み遅延がさらに加わります。リンクアップの伝播には、約 50 ~ 200 ミリ秒とスレーブ インターフェイスでのキャリア遅延時間がかかります。
- マスターからスレーブへのリンク障害からスレーブ リンクがダウンするまでの伝播遅延は、約 600 ミリ秒にスレーブ インターフェイスでのキャリア遅延時間を加えたものです。

## LFP の設定

図 17-13 に LFP を設定した RPR の例を示します。LFP 設定のプロセスは、次のタスクで構成されます。

1. ある ML シリーズ カードのギガビット イーサネット インターフェイスをマスター リンクとして設定します。
2. 別の ML シリーズ カードのギガビット イーサネットまたはファスト イーサネット インターフェイスをスレーブ リンクとして設定します。

LFP マスター リンクをイネーブルにして設定するには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <b>interface gigabit ethernet number</b>	インターフェイス コンフィギュレーション モードを起動してギガビット イーサネット インターフェイスを設定します。
ステップ 2	Router(config-if)# <b>link-fault rpr-master</b>	インターフェイスのリンク障害マスター ステータスをイネーブルにします。  このコマンドの <b>no</b> 形式はリンク障害マスター ステータスをディセーブルにします。
ステップ 3	Router(config-if)# <b>no shutdown</b>	インターフェイスがシャット ダウンしないようにすることにより、インターフェイスをイネーブルにします。
ステップ 4	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を TCC2/TCC2P フラッシュ データベースに保存します。

LFP スレーブ リンクをイネーブルに設定するには、マスター リンク用に設定された ML シリーズ カード以外の、RPR 内の ML シリーズ カードに対して次の手順を実行します。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。

	コマンドの説明	目的
ステップ 1	Router# <b>interface [gigabit ethernet   fastethernet] number</b>	インターフェイス コンフィギュレーション モードを起動してギガビット イーサネットまたはファスト イーサネット インターフェイスを設定します。
ステップ 2	Router(config-if)# <b>link-fault rpr-slave</b>	インターフェイスのリンク障害スレーブ ステータスをイネーブルにします。  このコマンドの <b>no</b> 形式はリンク障害スレーブ ステータスをディセーブルにします。
ステップ 3	Router(config-if)# <b>no shutdown</b>	インターフェイスがシャット ダウンしないようにすることにより、インターフェイスをイネーブルにします。
ステップ 4	Router(config)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を TCC2/TCC2P フラッシュ データベースに保存します。

## LFP の設定要件

LFP の設定要件には次のものがあります。

- リンク障害マスターとリンク障害スレーブを同じカード上で設定しない。
- ML シリーズ カードで拡張マイクロコード イメージを実行する必要がある。
- RPR 内のすべての ML シリーズ カードでリリース 5.0 以降のソフトウェアを実行する必要がある。
- DRPRI 用に設定された ML シリーズ カードは LFP 用に設定しない。DRPRI での LFP はサポートされていない。
- ML シリーズ カードのギガビット イーサネット インターフェイスだけがリンク障害マスターになれる。
- RPR ごとに許可されているリンク障害マスターは 1 つのみ。
- ギガビット イーサネット インターフェイスとファストイーサネット インターフェイスの両方がリンク障害スレーブになれる。
- RPR のリンク障害スレーブには設定に関する制限はありません。

## LFP のモニタリングおよび確認

リンク ダウン状態のスレーブ インターフェイスがあると、CTC で CARLOSS アラームが発生します。CTC は、スレーブ リンクでのローカルの損失と LFP による損失とを区別しません。CARLOSS の詳細については、『Cisco ONS 15454 Troubleshooting Guide』の「Alarm Troubleshooting」の章または『Cisco ONS 15454 SDH Troubleshooting Guide』の「Alarm Troubleshooting」の章を参照してください。

リンク ダウンしているインターフェイスの Cisco IOS ステータスは、プロトコル ダウンまたはリンク ダウンとして表示されます。`show controller` コマンドでも `show interface` コマンドでも、リンク上のローカル損失と LFP 損失との違いは表示されません。

LFP を設定したあと、`show link-fault` コマンドを使用して各マスター リンクまたはスレーブ リンクの LFP ステータスをモニタリングできます。このコマンドを使用して、LFP が原因でスレーブ インターフェイスでリンク ダウンが発生したかを判別します。例 17-6 に、スレーブ インターフェイスでこのコマンドを実行した場合の出力を示します。

### 例 17-6 LFP のモニタリングおよび確認

```
Router# show link-fault
Link Fault Propagation Configuration:
-----
LFP Config Mode   : LFP_SLAVE
LFP Master State  : LFP_STATUS_DOWN
Interfaces configured for LFP:
FastEthernet0 (down)
```

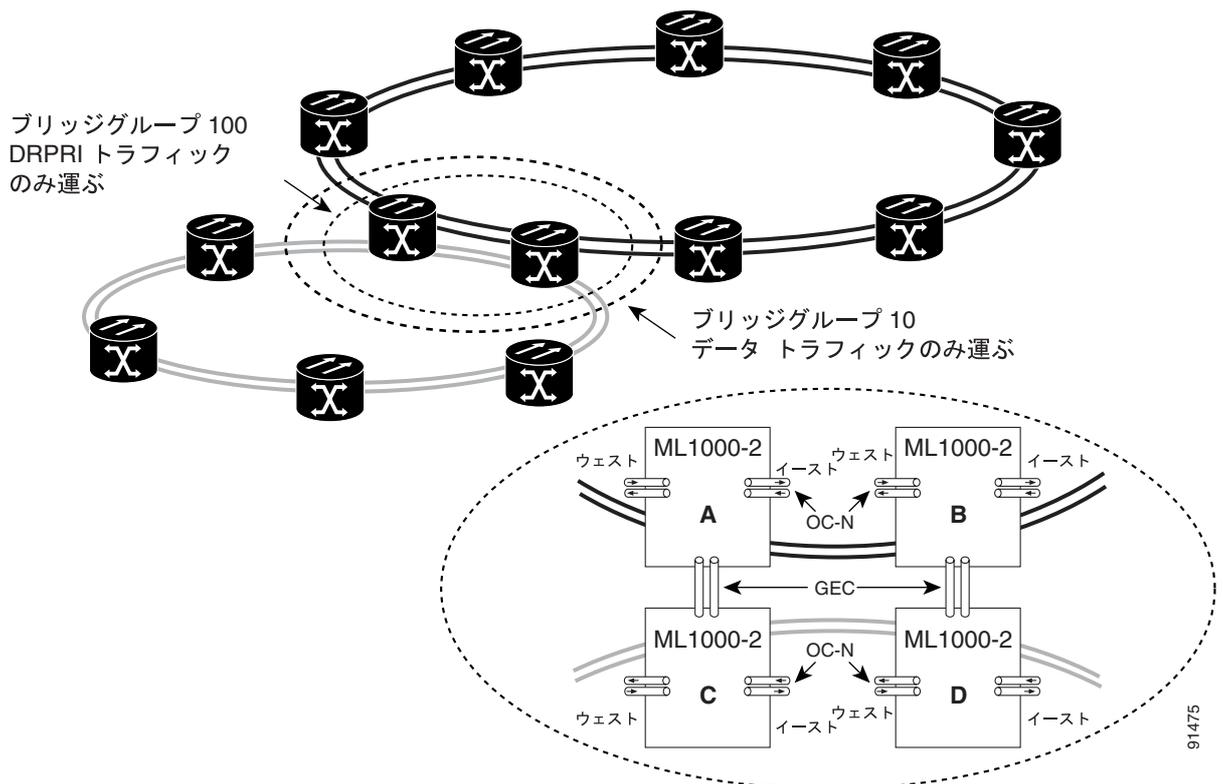
## デュアル RPR 相互接続の概要

Cisco ML シリーズの RPR には、ブリッジグループ プロトコル DRPRI が含まれます。これは、ノード障害から保護するためにリング間を相互接続するメカニズムです。DRPRI は、異なる RPR ネットワーク間のバックツーバック イーサネット接続の冗長ペアをサポートします。一方の接続はアクティブ ノードであり、もう一方はスタンバイ ノードです。アクティブ ノード、リンク、またはカードで障害が発生すると、独自のアルゴリズムによって障害が検出され、スタンバイ ノードへのスイッチ オーバーが発生します。

ML シリーズ カードで拡張マイクロ コード イメージを使用している場合は、DRPRI でレイヤ 2 のブリッジドトラフィックに適用される回復時間は 200 ミリ秒未満です。ML シリーズ カードが基本マイクロコード イメージ、または Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング) マイクロコード イメージを使用している場合、レイヤ 2 ブリッジドトラフィックの回復時間は最長 12 秒になります。どのマイクロコード イメージを使用している場合でも、レイヤ 3 のユニキャストおよびマルチキャストトラフィックの回復時間は、実装しているルーティング プロトコルのコンバージェンス時間にも依存します。DRPRI ホップに関係なく、カスタマー ルーティング プロトコルとスパニングツリー インスタンスは接続されません。

ML1000-2 カードのペアは同じステーション ID を共有し、RPR の他のメンバーには 1 枚のカードとして認識されます。図 17-14 では、ペア カード A と B が、同じ SPR ステーション ID を持ち、ペア カード C と D が、同じステーション ID を持ちます。相互接続するノードは、RPR で隣接している必要はありません。ブリッジング、IP ルーティング、ポリシング、および帯域幅割り当ては、DRPRI ML1000-2 カードにもプロビジョニングできます。次の例のブリッジグループ 100 は DRPRI トラフィックを伝送します。次の例のブリッジグループ 10 はデータトラフィックを伝送します。

図 17-14 デュアル RPR 相互接続ネットワークとペア カード



DRPRI には、次の特性があります。

- DRPRI ブリッジグループをデータトラフィックの伝送に使用することもできません。
- DRPRI ブリッジグループは 1 つの protocol に制限されるため、DRPRI を実装しているブリッジグループは、RSTP や STP を実装することはできません。
- 4 枚の ML1000-2 カードが必要です。
- 4 枚の ML1000-2 カードはすべて、同じブリッジグループ (VLAN) に属している必要があります。
- ML1000-2 カードの各ペアは、同じ SPR ステーション ID が割り当てられている必要があります。
- ブリッジグループを SPR サブインターフェイスで設定する必要があります。
- 4 枚の各 ML1000-2 カードで、両方のギガビットイーサネットポートは、Gigabit EtherChannel (GEC) に加入し、GEC インターフェイスは DRPRI ブリッジグループに含まれている必要があります。または、一方のギガビットイーサネットポートをシャットダウンし、もう一方のポートを DRPRI ブリッジグループに含める必要があります。GEC 方式を推奨します。
- DRPRI ブリッジグループに含まれるサブインターフェイスまたは GEC インターフェイス上で手動シャットダウンを行う場合、リング間の GEC またはイーサネット接続の両端のインターフェイスで行う必要があります。
- DRPRI ノードを使用できるのは、2 つの RPR を相互接続する場合だけです。カードのフロントポートを他のトラフィックの伝送に使用しないでください。
- リング間でトラフィックを伝送する DRPRI 以外のブリッジグループでは、STP または RSTP を設定できません。
- リング間でトラフィックを伝送する DRPRI 以外のブリッジグループは、4 枚の各 ML シリーズカードで設定する必要があります。
- 802.1 Q トンネル (QinQ) およびプロトコルトンネルを DRPRI ノードで開始することはできませんが、DRPRI ノードは接続されたリング間で QinQ とプロトコルトンネルをブリッジできます。
- ユーザが DRPRI ブリッジグループのメンバーのパスコストを変更してはなりません。パスコストは ML シリーズカードによって割り当てられ、DRPRI が正常に動作することが保証されます。ユーザが設定したパスコストは、割り当てられた DRPRI のデフォルトのパスコストで上書きされます。

## DRPRI の設定

DRPRI には、2 組の ML シリーズ カードが必要です。1 組は RPR として設定し、隣接する 2 つの RPR の 1 つめに属します。もう 1 組は RPR として設定し、2 つめの RPR に属します (図 17-14)。2 つの隣接する RPR を接続する 4 枚の各 ML1000-2 カードで DRPRI を設定します。DRPRI の設定プロセスのおおまかな手順は次のとおりです。この手順の詳細は、Cisco IOS 手順で説明されています。

**ステップ 1** DRPRI プロトコルでブリッジ グループを設定します。

**ステップ 2** SPR インターフェイスを設定します。

- a. ステーション ID 番号を割り当てます。
- b. DRPRI ID として 0 または 1 を割り当てます。

**ステップ 3** SPR サブインターフェイスを作成し、ブリッジ グループをサブインターフェイスに割り当てます。

**ステップ 4** GEC インターフェイスを作成します。

**ステップ 5** GEC サブインターフェイスを作成し、ブリッジ グループをサブインターフェイスに割り当てます。

DRPRI をイネーブルにして設定するには、グローバル コンフィギュレーション モードで、次の手順を実行します。

	コマンドの説明	目的
<b>ステップ 1</b>	<code>Router(config)# bridge crb</code>	同時ルーティングとブリッジングをイネーブルにします。同時ルーティングとブリッジングがイネーブルになっている場合、デフォルトの動作では、ブリッジ グループで明示的にルーティングされていないすべてのプロトコルがブリッジされます。
<b>ステップ 2</b>	<code>Router(config)# bridge bridge-group-number protocol drpri-rstp</code>	4 枚の ML1000-2 カードで共有するブリッジ グループ番号を作成し、DRPRI のプロトコルをブリッジ グループに割り当てます。同じブリッジ グループ番号を使用した同じコマンドを、4 枚の各カードで指定する必要があります。   <b>注意</b> データトラフィックを伝送するのに、DRPRI ブリッジ グループを使用しないでください。DRPRI ブリッジ グループのデータトラフィックは不安定さや、トラフィック ヒットの原因となります。
<b>ステップ 3</b>	<code>Router(config)# interface spr 1</code>	RPR の SPR インターフェイスを作成するか、すでに作成済みの SPR インターフェイスで SPR 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。有効な SPR 番号は 1 だけです。
<b>ステップ 4</b>	<code>Router(config-if)# spr station-ID station-ID-number</code>	ステーション識別番号を設定します。ユーザは、2 組のカードで同じステーション ID を設定する必要があります。有効なステーション ID 番号の範囲は、1 ~ 254 です。

	コマンドの説明	目的
ステップ 5	Router(config-if)# <b>spr drpri-ID</b> {0   1}	DRPRI ID 番号 (0 または 1) を作成し、DRPRI の ML1000-2 カードのペアを区別します。DRPRI 識別番号 0 がデフォルトです。
ステップ 6	Router(config-if)# <b>interface spr</b> <i>shared-packet-ring-subinterface-number</i>	SPR サブインターフェイスを作成します。
ステップ 7	Router(config-subif)# <b>encapsulation dot1q</b> <i>vlan-ID</i>	SPR サブインターフェイスのカプセル化を IEEE 802.1Q に設定します。
ステップ 8	Router(config-subif)# <b>bridge-group</b> <i>bridge-group-number</i>	SPR サブインターフェイスを DRPRI ブリッジグループに割り当てます。
ステップ 9	Router(config)# <b>interface port-channel</b> <i>channel-number</i>	GEC インターフェイスまたはチャンネルグループを作成します。
ステップ 10	Router(config-if)# <b>interface Gigabit Ethernet</b> <i>number</i>	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、GEC サブインターフェイスに割り当てる 1 つめのギガビット イーサネット インターフェイスを指定します。
ステップ 11	Router(config-if)# <b>channel-group</b> <i>channel-number</i>	ギガビット イーサネット インターフェイスを GEC に割り当てます。チャンネル番号は、EtherChannel インターフェイスに割り当てたチャンネル番号と同じ番号であることが必要です。
ステップ 12	Router(config-if)# <b>interface Gigabit Ethernet</b> <i>number</i>	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、GEC サブインターフェイスに割り当てる 2 つめのギガビット イーサネット インターフェイスを指定します。
ステップ 13	Router(config-if)# <b>channel-group</b> <i>channel-number</i>	ギガビット イーサネット インターフェイスを GEC に割り当てます。チャンネル番号は、EtherChannel インターフェイスに割り当てたチャンネル番号と同じ番号であることが必要です。
ステップ 14	Router(config-subif)# <b>interface port-channel</b> <i>channel-sub-interface-number</i>	GEC サブインターフェイスを作成します。
ステップ 15	Router(config-subif)# <b>encapsulation dot1q</b> <i>vlan-ID</i>	サブインターフェイスのカプセル化を IEEE 802.1Q に設定します。使用する VLAN ID は、7 で使用した VLAN ID と同じ ID であることが必要です。
ステップ 16	Router(config-subif)# <b>bridge-group</b> <i>bridge-group-number</i>	GEC サブインターフェイスを DRPRI ブリッジグループに割り当てます。
ステップ 17	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 18	Router# <b>copy running-config startup-config</b>	(任意) 設定の変更を NVRAM に保存します。

## DRPRI IOS の設定例

図 17-14 に、RPR の設定例を示します。show run コマンドの出力は、例 17-7、17-8、17-9、17-10 に示します。



### 注意

データトラフィックを伝送するのに、DRPRI ブリッジグループを使用しないでください。DRPRI ブリッジグループのデータトラフィックは不安定さや、トラフィック ヒットの原因となります。



(注)

DRPRI の ML1000-2 カードのペアを区別するため、カードには DRPRI 識別番号 0 または 1 が付けられています。DRPRI ID 1 が付いたカード上の `show run` コマンドは、Cisco IOS CLI 出力で `spr drpr-id 1` を表示します。ただし、DRPRI ID 0 が付いたカード上の `show run` コマンドは、Cisco IOS CLI 出力で DRPRI ID を表示しません。

### 例 17-7 ML シリーズカード A の設定

```
hostname ML-Series A
bridge crb
bridge 100 protocol drpri-rstp
bridge 100 forward-time 4
!
!
interface SPR1
no ip address
no keepalive
spr station-id 1
spr drpri-id 0
hold-queue 150 in
!
interface SPR1.1
encapsulation dot1Q 100
bridge-group 100
!
interface SPR1.10
encapsulation dot1Q 10
bridge-group 10
bridge-group 10 spanning-disabled
!
interface Port-channel1
no ip address
hold-queue 150 in
!
interface Port-channel1.1
encapsulation dot1Q 100
bridge-group 100
bridge-group 100 path-cost 32000
!
interface Port-channel1.10
encapsulation dot1Q 10
bridge-group 10
bridge-group 10 spanning-disabled
!
interface GigabitEthernet0
no ip address
channel-group 1
!
interface GigabitEthernet1
no ip address
channel-group 1
!
interface POS0
no ip address
spr interface-id 1
crc 32
!
interface POS1
no ip address
spr interface-id 1
crc 32
!
ip classless
no ip http server
```

## 例 17-8 ML シリーズカード B の設定

```
hostname ML-Series B
nodeB_ML1000#
bridge crb
bridge 100 protocol drpri-rstp
bridge 100 forward-time 4
!
!
interface SPR1
no ip address
no keepalive
spr station-id 1
spr drpri-id 1
hold-queue 150 in
!
interface SPR1.1
encapsulation dot1Q 100
bridge-group 100
!
interface SPR1.10
encapsulation dot1Q 10
bridge-group 10
bridge-group 10 spanning-disabled
!
interface Port-channel1
no ip address
hold-queue 150 in
!
interface Port-channel1.1
encapsulation dot1Q 100
bridge-group 100
bridge-group 100 path-cost 32000
!
interface Port-channel1.10
encapsulation dot1Q 10
bridge-group 10
bridge-group 10 spanning-disabled
!
interface GigabitEthernet0
no ip address
channel-group 1
!
interface GigabitEthernet1
no ip address
channel-group 1
!
interface POS0
no ip address
spr interface-id 1
crc 32
!
interface POS1
no ip address
spr interface-id 1
crc 32
!
ip classless
no ip http server
```

**例 17-9 ML シリーズカード C の設定**

```
hostname ML-Series C
bridge crb
bridge 100 protocol drpri-rstp
bridge 100 forward-time 4
bridge 100 priority 0
!
!
interface SPR1
no ip address
no keepalive
spr station-id 2
spr drpri-id 0
hold-queue 150 in
!
interface SPR1.1
encapsulation dot1Q 100
bridge-group 100
!
interface SPR1.10
encapsulation dot1Q 10
bridge-group 10
bridge-group 10 spanning-disabled
!
interface Port-channel1
no ip address
hold-queue 150 in
!
interface Port-channel1.1
encapsulation dot1Q 100
bridge-group 100
bridge-group 100 path-cost 32000
!
interface Port-channel1.10
encapsulation dot1Q 10
bridge-group 10
bridge-group 10 spanning-disabled
!
interface GigabitEthernet0
no ip address
channel-group 1
!
interface GigabitEthernet1
no ip address
channel-group 1
!
interface POS0
no ip address
spr interface-id 1
crc 32
!
interface POS1
no ip address
spr interface-id 1
crc 32
!
ip classless
no ip http server
```

## 例 17-10 ML シリーズカード D の設定

```
hostname ML-Series D
bridge crb
bridge 100 protocol drpri-rstp
bridge 100 forward-time 4
!
!
interface SPR1
no ip address
no keepalive
spr station-id 2
spr drpri-id 1
hold-queue 150 in
!
interface SPR1.1
encapsulation dot1Q 100
bridge-group 100
!
interface SPR1.10
encapsulation dot1Q 10
bridge-group 10
bridge-group 10 spanning-disabled
!
interface Port-channel1
no ip address
hold-queue 150 in
!
interface Port-channel1.1
encapsulation dot1Q 100
bridge-group 100
bridge-group 100 path-cost 65535
!
interface Port-channel1.10
encapsulation dot1Q 10
bridge-group 10
bridge-group 10 spanning-disabled
!
interface GigabitEthernet0
no ip address
channel-group 1
!
interface GigabitEthernet1
no ip address
channel-group 1
!
interface POS0
no ip address
spr interface-id 1
crc 32
!
interface POS1
no ip address
spr interface-id 1
crc 32
!
ip classless
no ip http server
```

## DRPRI のモニタリングおよび確認

DRPRI を設定したあと、`show bridge verbose` コマンドを使用して DRPRI のステータスをモニタリングできます (例 17-11)。

### 例 17-11 show bridge verbose コマンド

```
Router# show bridge bridge-group-number verbose
```



## EoMPLS の設定

---

この章では、ML シリーズ カードで Ethernet over Multiprotocol Label Switching ( EoMPLS ) を設定する方法について説明します。

この章の主な内容は次のとおりです。

- [EoMPLS の概要 \( p.18-2 \)](#)
- [EoMPLS の設定 \( p.18-6 \)](#)
- [EoMPLS の設定例 \( p.18-12 \)](#)
- [EoMPLS のモニタリングと確認 \( p.18-15 \)](#)

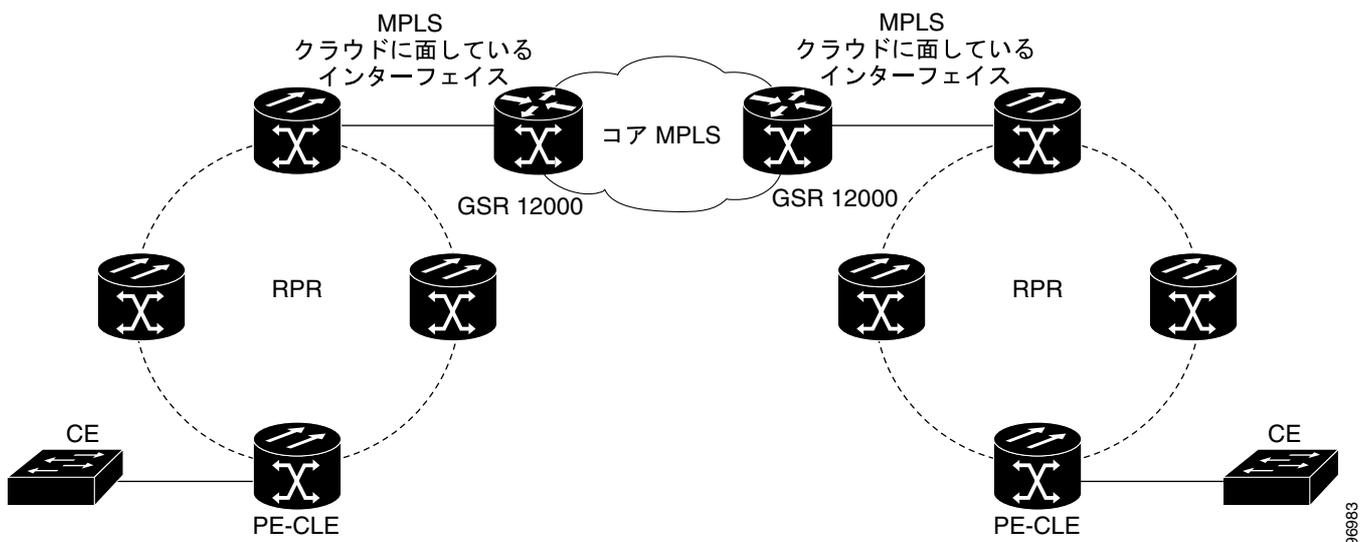
## EoMPLS の概要

EoMPLS には、MPLS 対応のレイヤ 3 コアを経由するイーサネットトラフィックをトンネリングするメカニズムがあります。このメカニズムでは、イーサネット Protocol Data Unit (PDU; プロトコルデータユニット) を MPLS パケット内にカプセル化し、ラベルスタッキングを使用して MPLS ネットワーク上で転送します。EoMPLS は、Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) 標準トラック プロトコルであり、Martini ドラフト、特に draft-martini-l2circuit-encap-mpls-01 セクションと draft-martini-l2circuit-transport-mpls-05 セクションに基づいています。

EoMPLS を使用することによって、サービス プロバイダーは自社の既存の MPLS バックボーンを使用して顧客に仮想イーサネット回線サービスや VLAN (仮想 LAN) サービスを提供できます。サービス プロバイダーのプロビジョニングも簡便化します。これは、Provider Edge Customer-Leading Edge (PE-CLE) 装置が、接続されている Customer Edge (CE; カスタマー エッジ) 装置にレイヤ 2 接続するだけだからです。

図 18-1 に、サービス プロバイダーのネットワークに実装されている EoMPLS の例を示します。この例では、ML シリーズ カードは、RPR アクセス リングを介して Cisco GSR 12000 シリーズに接続した PE-CLE 装置として動作します。ポイントツーポイント サービスは、ML シリーズ カードを介して ML シリーズ カード RPR アクセス リングに接続されている様々なサイトの CE 装置に提供されます。

図 18-1 サービス プロバイダーのネットワークでの EoMPLS



EoMPLS をサービス プロバイダーのネットワークに実装する場合、ML シリーズ カード インターフェイスで 3 つの重要な機能を実行する必要があります。これらの ML シリーズ カード インターフェイスの機能は、MPLS コアを通過する EoMPLS ポイントツーポイント サービスの両側で設定する必要があります。

- ML シリーズ カード インターフェイスは、プロバイダーのネットワークと CE 装置を直接接続し、PE-CLE インターフェイスと呼ばれています。この ML シリーズ カードの PE-CLE インターフェイスはファストイーサネットまたはギガビットイーサネットであり、EoMPLS ポイントツーポイントセッションのエンドポイントとなるように設定されます。
- ML シリーズ カード インターフェイスは、ML シリーズ カードの PE-CLE インターフェイスと RPR ネットワークをブリッジングします。この RPR/SPR インターフェイスは POS ポートを含み、MPLS IP 用に設定されています。

- ML シリーズ カード インターフェイスは、コア MPLS インターフェイスに接続します。コア MPLS インターフェイスはファスト イーサネットまたはギガビット イーサネットであり、MPLS ネットワーク上で Cisco GSR 12000 シリーズのポートまたは同様の装置に接続します。この MPLS のクラウドに面しているインターフェイスは、SPR インターフェイスと MPLS クラウドをブリッジングします。

サービス プロバイダーのネットワークに EoMPLS を実装するには、入力側および出力側の PE-CLE ルータの間にディレクテッド Label Distribution Protocol (LDP; ラベル配布プロトコル) セッション (LSP) を設定して、Virtual Circuit (VC; 仮想回線) の情報を交換する必要があります。それぞれの VC は各方向に 1 つ、合計 2 つの LSP から構成されます。これは、LSP がレイヤ 2 フレームを一方方向にだけ転送するディレクテッド パスであるためです。

EoMPLS は 2 段階のラベル スタックを使用してレイヤ 2 フレームを転送します。下側または内側のラベルが VC ラベル、上側または外側のラベルがトンネル ラベルです。VC ラベルが特定の LSP の出力側 PE-CLE によって入力側 PE-CLE に提供され、出力側 PE-CLE の特定の出力インターフェイスにトラフィックを転送します。VC ラベルは、VC のセットアップ中に出力側 PE-CLE によって割り当てられ、出力側インターフェイスと一意の設定用 VC ID 間のバインディングを表現します。VC のセットアップ中に入力側および出力側 PE-CLE は、指定した VC ID の VC ラベル バインディングを交換します。

ML シリーズ カードの EoMPLS VC は、MPLS 上でイーサネット ポートまたは IEEE 802.1Q VLAN を転送できます。VC タイプ 5 はイーサネット ポートをトンネリングし、VC タイプ 4 は、MPLS 上で VLAN を転送します。VC タイプ 5 セッションでは、`mpls l2transport route` コマンドを使用して、ML シリーズ カードの PE-CLE ポートで受信したトラフィックはすべて、遠端の ML シリーズ カードの PE-CLE ポートでリモート出力インターフェイスにトンネリングされることが予想できます。VC タイプ 4 では、トンネルはその VLAN への物理的な拡張として動作することが予想されます。EoMPLS セッション コマンドは、PE-CLE の VLAN サブインターフェイスに入ります。そのポート上で受信した VLAN タグ付きトラフィックのみがリモート PE-CLE にトンネリングされます。

## EoMPLS のサポート

ML シリーズ カードの EoMPLS には次のような特性があります。

- EoMPLS は、ファスト イーサネットとギガビット イーサネットのインターフェイスまたはサブインターフェイス上でのみサポートされます。
- MPLS タグ スイッチングは、SPR インターフェイスでのみサポートされます。
- Class of Service (CoS; サービス クラス) 値は MPLS ラベル内の experimental (EXP) ビットに、静的にまたは IEEE 802.1p ビット (デフォルト) を使用してマップされます。
- 入力側 PE-CLE ML シリーズ カードによって、time-to-live フィールドが 2 に、トンネル ラベルが 255 の値に設定されます。
- 入力側 PE-CLE ML シリーズ カードによって、VC ラベルの S ビットが 1 に設定され、VC ラベルがスタックの下側にあることを示しています。
- EoMPLS トラフィックが RPR 上で伝送されるため、RPR に入ってくるトラフィックに適用できるロード バランシングはすべて、EoMPLS トラフィックにも適用できます。
- EoMPLS は、GFP-F フレーミングおよび HDLC フレーミングにおいて RPR でサポートされません。
- Ethernet over MPLS の機能は、Cisco Any Transport over MPLS (AToM) 製品の一部です。
- EoMPLS のエンドポイント ポートをホスティングする ML シリーズ カードは、MPLS マイクロコード イメージを実行して EoMPLS をサポートする必要があります。複数のマイクロコード イメージの詳細については、「[複数のマイクロコード イメージ](#)」(p.3-14)を参照してください。RPR 内の他の ML シリーズ カードは、MPLS マイクロコード イメージの制限を受けません。

## EoMPLS の制限

ML シリーズ カードの EoMPLS には次のような制限があります。

- パケットベースのロード バランシングはサポートされません。代わりに回線 ID ベースのロード バランシングが使用されます。
- ゼロ ホップやヘアピン VC はサポートされません。1 つの ML シリーズ カードを VC の送信元と宛先の両方にすることはできません。
- データ伝送を順序化するための MPLS 制御ワードはサポートされません。制御ワードを使用せずにパケットを送受信する必要があります。
- EoMPLS トラフィックのシーケンス チェックや再順序化はサポートされません。どちらも制御ワードに依存して機能します。
- Maximum Transmission Unit (MTU; 最大伝送ユニット) のフラグメント化はサポートされません。
- バックツーバック LDP セッションの明示ヌル ラベルはサポートされません。



### 注意

MTU のフラグメント化は MPLS バックボーン全体にわたってサポートされないため、ネットワーク オペレータは、エンドポイント間のすべての中間リンクの MTU がレイヤ 2 の最大 PDU を伝送するのに十分であることを確認する必要があります。

## EoMPLS の QoS

EXP は 3 ビットのフィールドであり、MPLS ヘッダーの一部です。IETF が実験的に作成しましたが、後に標準 MPLS ヘッダーの一部になりました。MPLS ヘッダー内の EXP ビットはパケット プライオリティを伝送します。パス上の各ラベル スイッチ ルータは、パケットを適切なキューにキューイングし、それに基づいてパケットを処理することによって、パケット プライオリティに従います。

デフォルトでは、ML シリーズ カードは VLAN タグ ヘッダーの IEEE 802.1p ビットを MPLS EXP ビットにマップしません。MPLS EXP ビットはゼロ (0) の値に設定されます。

レイヤ 2 CoS と MPLS EXP の間は直接コピーできませんが、`set mpls experimental` アクションを使用すると、802.1p ビットとの照合に基づいて MPLS EXP ビット値を設定できます。このようなマッピングは、エントリ ポイントであるネットワークの入力側で行われます。

ML シリーズ カードでの EoMPLS トラフィックの Quality of Service (QoS; サービス品質) は、インポジション ルータとディスポジション ルータの出力側インターフェイスで完全プライオリティまたは重み付きラウンド ロビン スケジューリング、あるいはその両方を使用します。このためには、スケジューリングのタイプを決定するサービス クラス キューを選択する必要があります。インポジション ルータでは、ポリシングに基づいてマーキングされたプライオリティ ビット EXP または RPR CoS がサービス クラス キューの選択に使用されます。ディスポジション ルータでは、dot1p CoS ビット (ラベルの EXP ビットからコピーされたもの) がサービス クラス キューの選択に使用されます。出力側インターフェイスのスケジューリングの他に、ポリシー出力アクションにも EXP ビットと RPR CoS ビットのリマーキングを含めることができます。

ML シリーズ カードの EoMPLS では、Cisco Modular QoS CLI (MQC; モジュラ QoS コマンドライン インターフェイス) を使用します。これは ML シリーズ カードの標準 QoS と同じようなものです。ただし、一部の MQC コマンドは利用できません。表 18-1 に、ML シリーズ カード インターフェイスに適用できる MQC ステートメントとアクションを示します。

表 18-1 適用できる EoMPLS QoS の文とアクション

インターフェイス	適用できる MQC match ステートメント	適用できる MQC アクション
インポジション入力側	match cos match ip precedence match ip dscp match vlan	<b>police cir</b> <i>cir-burst</i> [ <i>pir-burst</i> <b>pir</b> <i>pir</i> <b>conform</b> [ <i>set-mpls-exp</i>   <b>exceed</b> [ <i>set-mpls-exp</i> ] [ <b>violate</b> <i>set-mpls-exp</i> ]
インポジション出力側	match mpls exp	<b>bandwidth</b> { <i>bandwidth-kbps</i>   <b>percent</b> <i>percent</i> } および <b>priority</b> <i>kpbs</i> および [ <i>set-mpls-exp</i> ]
ディスポジション入力側	適用されない	適用されない
ディスポジション出力側	match mpls exp	<b>bandwidth</b> { <i>bandwidth-kbps</i>   <b>percent</b> <i>percent</i> } および <b>priority</b> <i>kpbs</i> および <b>set-cos</b> <i>cos-value</i>

## EoMPLS の設定

EoMPLS ポイントツーポイント サービスの両エンドポイントの ML シリーズ ピア カードを設定する必要があります。EoMPLS をイネーブルにするには、次の設定手順を実行します。

- PE-CLE ポート上での VC タイプ 4 設定 (p.18-6) (VC タイプ 4 または VC タイプ 5 が必須)
- PE-CLE ポート上での VC タイプ 5 設定 (p.18-8) (VC タイプ 4 または VC タイプ 5 が必須)
- PE-CLE SPR インターフェイスでの EoMPLS 設定 (p.18-10) (必須)
- MPLS クラウドに面しているポートでのブリッジ グループ設定 (p.18-10) (必須)
- パケットのプライオリティと EXP の設定 (p.18-11)

### EoMPLS 設定の注意事項

EoMPLS を設定する場合の注意事項は次のとおりです。

- ループバック アドレスを使用してピア ML シリーズ カードの IP アドレスを指定します。
- LDP 設定は必須です。デフォルトの Tag Distribution Protocol (TDP; タグ配布プロトコル) は機能しません。
- EoMPLS は、ML シリーズ カード間で LDP をターゲットとするセッションを使用して EoMPLS VC を作成します。
- MPLS バックボーンが、Intermediate System-to-Intermediate System (IS-IS) プロトコルや Open Shortest Path First (OSPF) などの Interior Gateway Protocol (IGP; 内部ゲートウェイ プロトコル) ルーティング プロトコルを使用する必要があります。
- IP パケットのタグ スイッチングが PE-CLE ML シリーズ カードの SPR インターフェイス上でイネーブルになっている必要があります。

### PE-CLE ポート上での VC タイプ 4 設定

カスタマーに面しているファスト イーサネット ポートまたはギガビット イーサネット ポートは EoMPLS、および VC タイプ 4 またはタイプ 5 にプロビジョニングされている必要があります。カード A とカード C 上のインターフェイス GigE 0.1 は、[図 18-2](#) の VC タイプ 4 の機能を実行します。VC タイプ 4 の機能の詳細については、「[EoMPLS の概要](#)」(p.18-2) を参照してください。

VC タイプ 4 は、2 枚の PE-CLE ML シリーズ カード間で IEEE 802.1Q VLAN パケットを転送します。VC タイプ 4 をプロビジョニングするには、カスタマーに面しているポート上で、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。

	コマンドの説明	目的
ステップ 1	<code>Router(config)# mpls label protocol ldp</code>	LDP を LDP として指定します。  LDP を指定する必要があります。ML シリーズ カードは、LDP としてデフォルトの TDP を使用した場合、EoMPLS は動作しません。
ステップ 2	<code>Router(config)# interface loopback0</code>	ループバック 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	<code>Router(config-if)# ip address ip-address 255.255.255.255</code>	IP アドレスを ループバック インターフェイスに割り当てます。このループバック IP アドレスは、EoMPLS ポイントツーポイント セッションでピアを特定するために使用されます。  サブネット マスクは必要ありません。

	コマンドの説明	目的
ステップ 4	Router(config)# <b>interface</b> {GigabitEthernet   FastEthernet} <i>interface-number.sub-interface- number</i>	インポジション インターフェイスに対してイーサネット サブインターフェイスを指定します。隣接する CE 装置のサブインターフェイスがこのサブインターフェイスと同じ VLAN 上にあることを確認します。
ステップ 5	Router(config-subif)# <b>no ip address</b>	IP アドレスが割り当てられている場合は IP アドレスをディセーブルにします。
ステップ 6	Router(config-subif)# <b>encapsulation dot1q</b> <i>vlan-id</i>	サブインターフェイスによる 802.1q VLAN パケット受信をイネーブルにします。VLAN ID が隣接する CE 装置の VLAN ID と同じであることを確認します。
ステップ 7	Router(config-subif)# <b>mpls l2transport</b> <b>route destination vc-id</b>  または  <b>xconnect destination vc-id encapsulation</b> <b>mpls</b>	VLAN ベース EoMPLS の dot1q VLAN サブインターフェイスに <b>mpls l2transport route</b> または <b>xconnect</b> インターフェイス コンフィギュレーション コマンドを入力することで、カスタマー VLAN に基づいてトラフィックを転送するように EoMPLS トンネルを設定できます。  <b>mpls l2transport route</b> は、使用する VC が VLAN パケットを転送するように指定します。ピアのポイントツーポイント エンドポイント インターフェイスを使用してリモート LDP セッションを開始します。  <ul style="list-style-type: none"> <li>• <i>destination</i> によって、VC (PE-CLE) のもう一方の端にあるリモート ML シリーズのループバック IP アドレスを指定します。</li> <li>• <i>vc-id</i> はユーザ指定値です。この値は各 VC に対して一意である必要があります。VC ID は、VC のエンドポイントの接続に使用されます。VC の両端に同じ VC ID を指定します。</li> </ul> <b>xconnect</b> は、クロスコネク ト サービス用に 802.1q VLAN 回線を擬似配線にバインドします。 <b>encapsulation mpls</b> 擬似配線クラス パラメータは、トンネリング方式用に MPLS を指定します。   <b>(注)</b> <b>xconnect</b> コマンドは、 <b>mpls l2transport route</b> インターフェイス コンフィギュレーション コマンドの新しいバージョンです。   <b>(注)</b> EoMPLS トンネルを削除するには、 <b>no mpls l2transport route destination vc-id</b> または <b>no xconnect destination vc-id encapsulation mpls</b> インターフェイス コマンドを使用します。
ステップ 8	Router(config-subif)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 9	Router# <b>show mpls l2transport vc</b>	設定を確認します。
ステップ 10	Router# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

## PE-CLE ポート上での VC タイプ 5 設定

カスタマーに面しているファストイーサネットポートまたはギガビットイーサネットポートは EoMPLS、および VC タイプ 4 またはタイプ 5 を使用してプロビジョニングする必要があります。カード A とカード C 上のインターフェイス GigE 1 は、図 18-2 の VC タイプ 5 の機能を実行します。VC タイプ 5 の機能の詳細については、「EoMPLS の概要」(p.18-2) を参照してください。

VC タイプ 5 では、設定されたポートのパケットを 2 枚の PE-CLE ML シリーズカード間で転送します。VC タイプ 5 をプロビジョニングするには、カスタマーに面しているポート上で、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。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>mpls label protocol ldp</b>	LDP を LDP として指定します。  LDP を指定する必要があります。ML シリーズカードは、LDP としてデフォルトの TDP を使用した場合、EoMPLS は動作しません。
ステップ 2	Router(config)# <b>interface loopback0</b>	ループバック 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	Router(config-if)# <b>ip address ip-address 255.255.255.255</b>	IP アドレスを ループバック インターフェイスに割り当てます。このループバック IP アドレスは、EoMPLS ポイントツーポイント セッションでピアを特定するために使用されます。  サブネット マスクは必要ありません。
ステップ 4	Router(config)# <b>interface {GigabitEthernet   FastEthernet} interface-number</b>	インポジション インターフェイスに対してイーサネット インターフェイスを指定します。
ステップ 5	Router(config-if)# <b>no ip address</b>	IP アドレスが割り当てられている場合は IP アドレスをディセーブルにします。

	コマンドの説明	目的
ステップ 6	<pre>Router(config-subif)# mpls l2transport route destination vc-id</pre> <p>または</p> <pre>xconnect destination vc-id encapsulation mpls</pre>	<p>VLAN ベース EoMPLS の VLAN に <b>mpls l2transport route</b> または <b>xconnect</b> インターフェイス コンフィギュレーション コマンドを入力することで、カスタマー VLAN に基づいてトラフィックを転送するように EoMPLS トンネルを設定できます。</p> <p><b>mpls l2transport route</b> は、使用する VC が VLAN パケットを転送するように指定します。ピアのポイントツーポイント エンドポイント インターフェイスを使用してリモート LDP セッションを開始します。</p> <ul style="list-style-type: none"> <li>• <i>destination</i> によって、VC (PE-CLE) のもう一方の端にあるリモート ML シリーズのループバック IP アドレスを指定します。</li> <li>• <i>vc-id</i> はユーザ指定値です。この値は各 VC に対して一意である必要があります。VC ID は、VC のエンドポイントの接続に使用されます。VC の両端に同じ VC ID を指定します。</li> </ul> <p><b>xconnect</b> は、クロスコネク ト サービス用に 802.1q VLAN 回線を擬似配線にバインドします。<b>encapsulation mpls</b> 擬似配線クラス パラメータは、トンネリング方式用に MPLS を指定します。</p> <p> (注) <b>xconnect</b> コマンドは、<b>mpls l2transport route</b> インターフェイス コンフィギュレーション コマンドの新しいバージョンです。</p> <p> (注) EoMPLS トンネルを削除するには、<b>no mpls l2transport route destination vc-id</b> または <b>no xconnect destination vc-id encapsulation mpls</b> インターフェイス コマンドを使用します。</p>
ステップ 7	<pre>Router(config-subif)# end</pre>	イネーブル EXEC モードに戻ります。
ステップ 8	<pre>Router# show mpls l2transport vc</pre>	設定を確認します。
ステップ 9	<pre>Router# copy running-config startup-config</pre>	(任意) コンフィギュレーション ファイルにエントリを保存します。

## PE-CLE SPR インターフェイスでの EoMPLS 設定

RPR を MPLS クラウドのアクセス リングとして機能させるには、EoMPLS PE-CLE ファスト イーサネットまたはギガビット イーサネットをホスティングする同一 ML シリーズ カード上で SPR インターフェイスをプロビジョニングする必要があります。カード A とカード C 上のインターフェイス SPR 1 が、[図 18-2](#) に示すように、この機能を実行します。

MPLS に対して SPR インターフェイスをプロビジョニングするには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>mpls label protocol ldp</b>	LDP を LDP として指定します。  LDP を指定する必要があります。ML シリーズ カードは、LDP としてデフォルトの TDP を使用した場合、EoMPLS は動作しません。
ステップ 2	Router(config)# <b>interface spr 1</b>	RPR 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	Router(config-if)# <b>ip address ip-address mask</b>	IP アドレスを MPLS の RPR インターフェイスに割り当てます。
ステップ 4	Router(config-if)# <b>mpls ip</b>	SPR インターフェイスにタグ スwitチングを実装します。
ステップ 5	Router(config-if)# <b>end</b>	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	Router# <b>copy running-config startup-config</b>	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 ファイルに保存します。

## MPLS クラウドに面しているポートでのブリッジ グループ設定

RPR の ML シリーズ カードのファスト イーサネット ポートまたはギガビット イーサネット ポートは、MPLS クラウドの一部であるルータのインターフェイスに接続する必要があります。このファスト イーサネット ポートまたはギガビット イーサネット ポートと SPR サブインターフェイスを含むブリッジ グループを作成する必要があります。カード B とカード D 上のインターフェイス GigE 0 が、[図 18-2](#) に示すように、この機能を実行します。

MPLS クラウドに面しているポートで EoMPLS をプロビジョニングするには、グローバル コンフィギュレーション モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>bridge bridge-group-number protocol {rstp   ieee}</b>	(任意)ブリッジ グループ番号を割り当て、IEEE 802.1D スパニングツリー プロトコルまたは IEEE 802.1W 高速スパニングツリーのいずれか適切なスパニングツリーのタイプを定義します。
ステップ 2	Router(config)# <b>interface {GigabitEthernet   FastEthernet} interface-number</b>	インターフェイス コンフィギュレーション モードを開始して ML シリーズ カードの MPLS クラウドに面するファスト イーサネット インターフェイスまたはギガビット イーサネット インターフェイスを設定します。
ステップ 3	Router(config-if)# <b>bridge-group bridge-group-number</b>	ネットワーク インターフェイスをブリッジ グループに割り当てます。
ステップ 4	Router(config-if)# <b>no shutdown</b>	シャットダウン ステートをアップにし、インターフェイスをイネーブルにします。

	コマンドの説明	目的
ステップ 5	Router(config)# <b>interface</b> <b>spr 1.subinterface-number</b>	ML シリーズ カードの SPR 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 6	Router(config-if)# <b>bridge-group</b> <b>bridge-group-number</b>	ネットワーク インターフェイスをブリッジ グループに割り当てます。
ステップ 7	Router(config-if)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 8	Router# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

## パケットのプライオリティと EXP の設定

EoMPLS では、ラベル内の 3 つの EXP ビットを使用して QoS を提供し、パケットのプライオリティを決定します。ML シリーズカードのポイントツーポイントのエンドポイント間で QoS をサポートするには、VC ラベルとトンネル ラベルの両方に EXP ビットを設定します。

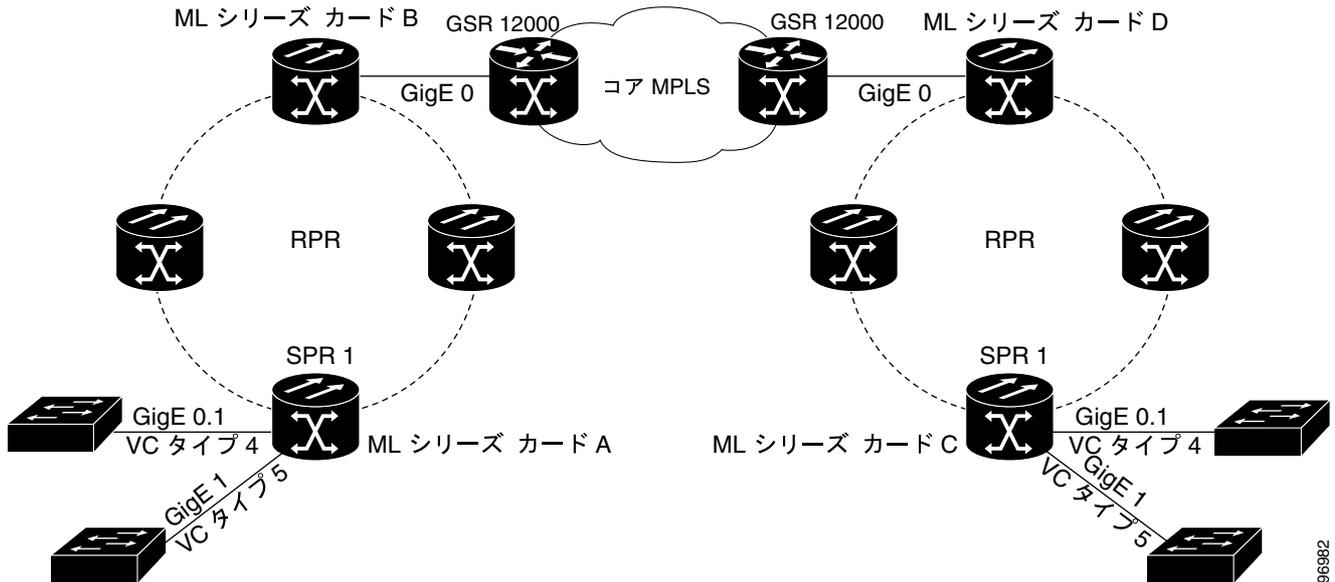
EXP ビットを設定するには、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router(config)# <b>class-map</b> <i>class-name</i>	トラフィック クラスのユーザ定義名を指定します。
ステップ 2	Router(config-cmap)# <b>match any</b>	すべてのパケットを照合することを指定します。
ステップ 3	Router(config-cmap)# <b>end</b>	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 4	Router(config)# <b>policy-map</b> <i>policy-name</i>	設定するトラフィック ポリシーの名前を指定します。
ステップ 5	Router(config-pmap)# <b>class</b> <i>class-name</i>	定義しておいたトラフィック クラス名を指定します。この名前は class-map コマンドを使用して設定されたもので、トラフィックをトラフィック ポリシーに分類するために使用します。
ステップ 6	Router (config-pmap-c)# <b>set mpls</b> <b>experimental imposition</b> <i>value</i>	パケットが指定したポリシー マップと一致する場合に MPLS ビットに設定する値を指定します。
ステップ 7	Router(config)# <b>interface GigabitEthernet</b> <i>interface-number</i>  または <b>interface FastEthernet</b> <i>interface-number</i>	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	Router(config-if)# <b>service-policy input</b> <i>policy-name</i>	トラフィック ポリシーをインターフェイスに付加します。

## EoMPLS の設定例

図 18-2 に、コンフィギュレーション コマンドで参照しているネットワーク例を示します。例 18-1、18-2、18-3、および 18-4 に、コンフィギュレーション ファイルの中で、ネットワーク例の ML シリーズカード上で EoMPLS をイネーブルにしている部分を示します。

図 18-2 EoMPLS の設定例



**例 18-1 ML シリーズカード A の設定**

```
microcode mpls
ip subnet-zero
no ip domain-lookup
!
mpls label protocol ldp
!
interface Loopback0

    ip address 10.10.10.10 255.255.255.255
    !
interface SPR1
    ip address 100.100.100.100 255.255.255.0
    no keepalive
    spr station-id 1
    mpls ip
    hold-queue 150 in
    !
interface GigabitEthernet0
    no ip address
    !
interface GigabitEthernet0.1
    encapsulation dot1q 10
    mpls l2transport route 3.3.3.3 1
    !
interface GigabitEthernet1
    no ip address
    mpls l2transport route 4.4.4.4 2
    !
interface POS0
    no ip address
    spr-intf-id 1
    crc 32
    !
interface POS1
    no ip address
    spr-intf-id 1
    crc 32
router ospf 1
    log-adjacency-changes
    network 1.1.1.0 0.0.0.255 area 0
    network 10.10.10.0 0.0.0.255 area 0
    !
ip classless
no ip http server
```

**例 18-2 ML シリーズカード B の設定**

```
bridge 10 protocol ieee
!
!
interface SPR1
no ip address
no keepalive
    bridge-group 10
    hold-queue 150 in
!
interface GigabitEthernet0
no ip address
bridge-group 10
```

**例 18-3 ML シリーズカード C の設定**

```

microcode mpls
ip subnet-zero
no ip domain-lookup
!
mpls label protocol ldp
!
interface Loopback0

    ip address 20.20.20.20 255.255.255.255
    !
interface SPR1
    ip address 100.100.100.100 255.255.255.0
    no keepalive
    spr station-id 4
    mpls ip
    hold-queue 150 in
    !
interface GigabitEthernet0
    no ip address
    !
interface GigabitEthernet0.1
    encapsulation dot1q 10
    mpls l2transport route 1.1.1.1 1
    !
interface GigabitEthernet1
    no ip address
    mpls l2transport route 2.2.2.2 2
    !
interface POS0
    no ip address
    spr-intf-id 1
    crc 32
    !
interface POS1
    no ip address
    spr-intf-id 1
    crc 32
    !
router ospf 1
    log-adjacency-changes
    network 1.1.1.0 0.0.0.255 area 0
    network 10.10.10.0 0.0.0.255 area 0
    !
ip classless
no ip http server

```

**例 18-4 ML シリーズカード D の設定**

```

bridge 20 protocol ieee
!
!
interface SPR1
no ip address
no keepalive
    bridge-group 20
    hold-queue 150 in
    !
interface GigabitEthernet0
no ip address
bridge-group 20

```

## EoMPLS のモニタリングと確認

表 18-2 に、EoMPLS をモニタリングおよび確認するためのイネーブル EXEC コマンドを示します。

表 18-2 トンネリングのモニタリングおよび保守に使用するコマンド

コマンドの説明	目的
<code>show mpls l2transport vc</code>	すべての EoMPLS トンネルに関する情報を示します。
<code>show mpls l2transport vc detail</code>	EoMPLS トンネルに関する詳細情報を示します。
<code>show mpls l2transport vc vc-id</code>	特定の EoMPLS トンネルに関する情報を示します。





# ML シリーズ カードのセキュリティ設定

---

この章では、ML シリーズ カードのセキュリティ機能について説明します。

この章の主な内容は次のとおりです。

- [セキュリティの概要 \(p.19-2\)](#)
- [ML シリーズ カードの コンソール ポートのディセーブル化 \(p.19-2\)](#)
- [ML シリーズ カードへのセキュアなログイン \(p.19-2\)](#)
- [ML シリーズ カードの SSH \(p.19-3\)](#)
- [ML シリーズ カード上の RADIUS \(p.19-7\)](#)
- [RADIUS リレー モード \(p.19-7\)](#)
- [RADIUS スタンドアロン モード \(p.19-9\)](#)

## セキュリティの概要

ML シリーズカードには、いくつかのセキュリティ機能が含まれています。これらの機能の中には、ML シリーズカードが取り付けられている ONS ノードから独立して動作するものがあります。それ以外の機能は、Cisco Transport Controller (CTC) または Transaction Language One (TL1) を使用して設定されます。

Cisco IOS で設定されるセキュリティ機能は、以下の通りです。

- Cisco IOS ログイン強化
- Secure Shell (SSH; セキュア シェル) 接続
- Authentication, Authorization, Accounting (AAA; 認証、許可、アカウントिंग) /Remote Authentication Dial-In User Service (RADIUS) (AAA/RADIUS) スタンドアロンモード
- Cisco IOS 基本パスワード (Cisco IOS 基本パスワード設定の詳細については、「パスワード」(p.3-9)を参照してください)

CTC または TL1 で設定されるセキュリティ機能は、以下の通りです。

- ディセーブルのコンソールポート
- AAA/RADIUS リレーモード

## ML シリーズカードのコンソールポートのディセーブル化

コンソールポート(カードの前面にある RJ-11 シリアルポート)へ直接接続するなど、ML カード上で動作している Cisco IOS にアクセスする方法には数種類あります。ユーザは、このようなデフォルトでイネーブルになっている直接接続をディセーブルにすることでセキュリティを強化できます。これにより、Cisco IOS エラーメッセージなどのコンソールポート出力を妨げずにコンソールポート入力を防ぐことができます。

CTC または TL1 を使用してコンソールポートへのアクセスをディセーブルにできます。CTC を使用してこれをディセーブルにするには、ML シリーズカードのカードレベルビューで、IOS タブの下をクリックして、**Enable Console Port Access** ボックスをオフにして、**Apply** をクリックします。ユーザは、Superuser レベルでログインしてこのタスクを完了する必要があります。

TL1 を使用してこれをディセーブルにするには、『Cisco ONS SONET TL1 Command Guide』を参照してください。

## ML シリーズカードへのセキュアなログイン

ML シリーズカードは、Cisco IOS Release 12.2(25)S に統合され、Cisco IOS Release 12.3(4)T に導入された Cisco IOS ログイン強化をサポートしています。この強化により、ユーザは Telnet、SSH、HTTP などの仮想接続を確立するときに ML シリーズカードのセキュリティを強化できます。セキュアなログイン機能では、ML シリーズカードの vty セッション(監査証跡)に対するログイン試行の成功および失敗を記録します。これらの機能は、Cisco IOS CLI (コマンドライン インターフェイス) を使用して設定されます。

詳細な設定例などの詳細な情報については、

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products\\_feature\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guides_list.html) にある Cisco IOS Release 12.2(25)S 機能ガイド モジュール「Cisco IOS Login Enhancements」を参照してください。

## ML シリーズカードの SSH

このセクションでは、SSH 機能の設定方法について説明します。

以下のセクションがあります。

- SSH の概要 ( p.19-3 )
- SSH の設定 ( p.19-3 )
- SSH 設定およびステータスの表示 ( p.19-6 )

SSH の設定例については、『Cisco IOS Security Configuration Guide, Cisco IOS Release 12.2』の「Configuring Secure Shell」の章にある「SSH Configuration Examples」を参照してください。次の URL にあります。

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur\\_c/fothersf.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fothersf.htm)



(注)

このセクションで使用されている全構文と使用方法の情報については、次の URL にある Cisco IOS Release 12.2 のコマンド リファレンスを参照してください。

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm>

## SSH の概要

ML シリーズカードは、SSH のバージョン 1 ( SSH v1 ) およびバージョン 2 ( SSHv2 ) の両方をサポートしています。SSHv2 は、SSHv1 のセキュリティ面を改善したもので、ML シリーズカードではデフォルトで選択されています。

SSH には、SSH サーバおよび SSH クライアントの 2 種類のアプリケーションがあります。ML シリーズカードは、SSH サーバのみをサポートし、SSH クライアントはサポートしていません。Cisco IOS ソフトウェアの SSH サーバは、公的および商用で利用可能な SSH クライアントと連動します。

SSH サーバにより、着信 Telnet 接続と同様ですがよりセキュリティが強化された ML シリーズカードへの接続が可能になります。SSH が登場するまで、セキュリティは Telnet 固有のセキュリティに限定されていました。SSH により、Cisco IOS ソフトウェア認証が使用できるようになり、セキュリティ面が改善されました。

ONS ノードも SSH をサポートしています。SSH が ONS ノードでイネーブルの場合、Cisco IOS CLI セッションで、SSH を使用して ML シリーズカードに接続します。



(注)

SSH がイネーブルの場合には、ML シリーズカードへの Telnet アクセスが自動的にディセーブルになりません。ユーザは、`transport input ssh vty` ライン コンフィギュレーション コマンドを使用して Telnet アクセスをディセーブルにできます。

## SSH の設定

ここでは、次の設定情報について説明します。

- 設定の注意事項 ( p.19-4 )
- SSH を実行するための ML シリーズカードの設定 ( p.19-4 ) ( 必須 )
- SSH サーバの設定 ( p.19-5 ) ( 必須 )

## 設定の注意事項

ML シリーズカードを SSH サーバとして設定する場合には、以下の注意事項に従ってください。

- AAA の新規モデルおよび AAA ログイン方式をイネーブルにする必要があります。まだイネーブルでない場合は、「[AAA ログイン認証の設定](#)」(p.19-13)の手順を完了してください。
- SSHv1 サーバで生成された Rivest, Shamir, and Adelman (RSA) キーペアを SSH v2 サーバで使用することも、またその逆も可能です。
- `crypto key generate rsa` グローバル コンフィギュレーション コマンドを入力したあとに CLI エラーメッセージを取得した場合、RSA キーペアが生成されていません。ホスト名とドメインを再設定して、`crypto key generate rsa` コマンドを入力します。詳細については、「[SSH を実行するための ML シリーズカードの設定](#)」(p.19-4)を参照してください。
- RSA キーペアを生成する際に、`No host name specified` メッセージが表示される場合があります。表示される場合は、`hostname` 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設定する必要があります。
- RSA キーペアを生成する際に、`No domain specified` メッセージが表示される場合があります。表示される場合は、`ip domain-name` 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 ドメイン名を設定する必要があります。

## SSH を実行するための ML シリーズカードの設定

SSH サーバとして動作するように ML シリーズカードを設定するには、以下の手順を実行します。

1. ML シリーズカードのホスト名と IP ドメイン名を設定します。
2. ML シリーズカードの RSA キーペアを生成します。これで、SSH が自動的にイネーブルになります。
3. ローカルまたはリモート アクセス用のユーザ認証を設定します。この手順は必須です。

ホスト名と IP ドメイン名を設定して RSA キーペアを生成するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	<code>Router #configure terminal</code>	グローバル 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	<code>Router (config)# hostname <i>hostname</i></code>	ML シリーズカードのホスト名を設定します。
ステップ 3	<code>Router (config)# ip domain-name <i>domain_name</i></code>	ML シリーズカードのホストドメインを設定します。
ステップ 4	<code>Router (config)# crypto key generate rsa</code>	ML シリーズカードでローカルおよびリモート認証用の SSH サーバをイネーブルにして、RSA キーペアを生成します。  RSA キーを生成する際に、モジュラス長を入力するように要求されます。デフォルトのモジュラス長は 512 ビットです。モジュラス長が長いほど安全ですが、生成や使用の際により時間がかかります。

	コマンドの説明	目的
ステップ 5	<code>Router (config)# ip ssh timeout seconds</code>	タイムアウト時間を秒単位で指定します。デフォルトは 120 秒です。範囲は、0 ~ 120 秒です。このパラメータは、SSH ネゴシエーション フェーズに適用されます。接続の確立後、ML シリーズ カードはデフォルトの CLI ベース セッションのタイムアウト値を使用します。  デフォルトで、ネットワーク上で複数の CLI ベース セッションに対して 5 つまでの同時暗号化 SSH 接続が可能です (セッション 0 ~ 4)。実行シェルの開始後、CLI ベース セッションのタイムアウト値がデフォルトの 10 分に戻ります。
ステップ 6	<code>Router (config)# ip ssh authentication-retries number</code>	クライアントがサーバの再認証を受けられる回数を指定します。デフォルトは 3 です。範囲は 0 ~ 5 です。
ステップ 7	<code>Router (config)# end</code>	イネーブル EXEC モードに戻ります。
ステップ 8	<code>Router # show ip ssh</code> または <code>Router # show ssh</code>	使用している SSH サーバのバージョンおよび設定情報を表示します。  ML シリーズ カードの SSH サーバのステータスを表示します。
ステップ 9	<code>Router # show crypto key mypubkey rsa</code>	この ML シリーズ カードに関連付けられた生成済み RSA 鍵ペアを表示します。
ステップ 10	<code>Router # copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエントリを保存します。

RSA 鍵ペアを削除するには、`crypto key zeroize rsa` グローバル コンフィギュレーション コマンドを使用します。RSA 鍵ペアが削除されると、SSH サーバも自動的に削除されます。

## SSH サーバの設定

SSH サーバを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	<code>Router # configure terminal</code>	グローバル 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	<code>Router (config)# ip ssh version [1   2]</code>	(任意) SSH バージョン 1 または SSH バージョン 2 を実行するように ML シリーズ カードを設定します。  <ul style="list-style-type: none"> <li>1 SSH バージョン 1 を実行するように ML シリーズ カードを設定します。</li> <li>2 SSH バージョン 2 を実行するように ML シリーズ カードを設定します。</li> </ul> このコマンドを入力しなかったりキーワードを指定しなかったりした場合、SSH サーバは SSH クライアントでサポートされている最新の SSH バージョンを選択します。例えば、SSH クライアントが SSHv1 および SSHv2 をサポートしている場合、SSH サーバは SSHv2 を選択します。

## ■ ML シリーズカードの SSH

	コマンドの説明	目的
ステップ 3	<code>Router (config)# ip ssh timeout seconds</code>	タイムアウト時間を秒単位で指定します。デフォルトは 120 秒です。範囲は、0 ~ 120 秒です。このパラメータは、SSH ネゴシエーション フェーズに適用されます。接続の確立後、ML シリーズ カードはデフォルトの CLI ベース セッションのタイムアウト値を使用します。  デフォルトで、ネットワーク上で複数の CLI ベース セッションに対して 5 つまでの同時暗号化 SSH 接続が可能です (セッション 0 ~ 4)。実行シェルの開始後、CLI ベース セッションのタイムアウト値がデフォルトの 10 分に戻ります。
ステップ 4	<code>Router (config)# ip ssh authentication-retries number</code>	クライアントがサーバの再認証を受けられる回数を指定します。デフォルトは 3 です。範囲は 0 ~ 5 です。
ステップ 5	<code>Router (config)# end</code>	イネーブル EXEC モードに戻ります。
ステップ 6	<code>Router # show ip ssh</code> または <code>Router # show ssh</code>	使用している SSH サーバのバージョンおよび設定情報を表示します。  ML シリーズ カードの SSH サーバの接続ステータスを表示します。
ステップ 7	<code>Router # copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエントリを保存します。

デフォルトの SSH 制御パラメータに戻すには、`no ip ssh {timeout | authentication-retries}` グローバル コンフィギュレーション コマンドを使用します。

## SSH 設定およびステータスの表示

SSH サーバの設定とステータスを表示するには、表 19-1 に示す 1 つまたは複数のイネーブル EXEC コマンドを使用します。

表 19-1 SSH 設定およびステータスを表示するコマンド

コマンドの説明	目的
<code>show ip ssh</code>	SSH サーバのバージョンおよび設定情報を表示します。
<code>show ssh</code>	SSH サーバのステータスを表示します。

これらのコマンドの詳細については、『Cisco IOS Security Command Reference, Cisco IOS Release 12.2』の「Other Security Features」の章にある「Secure Shell Commands」を参照してください。次の URL にあります。

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur\\_r/fothercr.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_r/fothercr.htm)

## ML シリーズカード上の RADIUS

RADIUS は、無許可アクセスに対してネットワークをセキュリティ保護する分散型クライアント / サーバシステムです。クライアントは、中央 RADIUS サーバに認証要求を送信します。これには、すべてのユーザ認証およびネットワーク サービス アクセス情報が含まれています。RADIUS ホストは、通常 Cisco や他のソフトウェア プロバイダーから RADIUS サーバソフトウェアを実行するマルチユーザシステムです。

ONS 15454、ONS 15454 SDH、ONS 15327、ONS 15310-CL、ONS 15600 など、多くの Cisco 製品で RADIUS がサポートされています。ML シリーズカードでも、RADIUS をサポートしています。

ML シリーズカードは、RADIUS リレー モードまたは RADIUS スタンドアロン モード（デフォルト）のいずれかで動作できます。いずれのモードでも、ML シリーズカードからの RADIUS メッセージは、ONS ノードの管理に使用される Data Communication Network (DCN; データ通信ネットワーク) 上にある RADIUS サーバに渡されます。

## RADIUS リレー モード

RADIUS リレー モードでは、ML シリーズカードの RADIUS は CTC または TL1 によって設定され、ML シリーズカードを含む ONS 15454 または ONS 15454 SDH ノードの AAA/RADIUS 機能を使用します。RADIUS リレー モードと RADIUS スタンドアロン モードとの間の相互作用はありません。ONS ノード セキュリティの詳細については、ONS ノードのリファレンス マニュアルにある「Security」の章を参照してください。

RADIUS リレー モードで動作している ML シリーズカードは、クライアントとして RADIUS エントリに指定する必要がありません。RADIUS サーバは、ML シリーズカードのプロキシとして ONS ノードのクライアント エントリを使用します。

リレー モードをイネーブルにすると、AAA/RADIUS を設定するのに使用される Cisco IOS CLI コマンドがディセーブルになります。ユーザは、AAA/RADIUS に関連しない Cisco IOS CLI コマンドはそのまま使用できます。

リレー モードでは、ML シリーズカードは、実際にはアクティブな Timing, Communications, and Control カード (TCC2/TCC2P) の内部 IP アドレスである IP アドレスに RADIUS サーバ ホストが表示されます。ML シリーズカードが実際に RADIUS パケットをこの内部アドレスに送信すると、TCC2/TCC2P が RADIUS パケット宛先を RADIUS サーバの実際の IP アドレスに変換します。スタンドアロン モードでは、ML シリーズカードが RADIUS サーバの実際の IP アドレスを表示します。

複数の RADIUS サーバ ホストを使用した ML シリーズカードがリレー モードの場合、ML シリーズカード IOS CLI の `show run` 出力もアクティブな TCC2/TCC2P カードの内部 IP アドレスを表示します。単一の IP アドレスで複数のホストを表しているため、個々のホストを識別するために異なるポート番号と IP アドレスがペアになっています。1860 ~ 1869 のポートには各認証サーバ ホストが設定されていて、1870 ~ 1879 のポートには各アカウントリングサーバ ホストが設定されています。

IP アドレスの 1 つは、CTC で示されるホスト IP アドレスとは一致しません。CTC では RADIUS サーバ ホストの実際のアドレスを使用しているためです。これらの実際の同一 IP アドレスは、ML シリーズカードがスタンドアロン モードのときに、ML シリーズカード IOS CLI `show run` 出力で表示されます。



(注) ユーザは、認証またはアカウントングアプリケーションのいずれかに対して最大で 10 のサーバを設定でき、1 つのサーバ ホストで認証アプリケーションとアカウントングアプリケーションの両方を実行できます。

## RADIUS リレー モードの設定

この機能は、CTC または TL1 でオンにします。CTC を使用して RADIUS リレー モードをイネーブルにするには、ML シリーズカードのカードレベルビューで、**Enable RADIUS Relay** チェックボックスをオンにして、**Apply** をクリックします。ユーザは、Superuser レベルでログインしてこのタスクを完了する必要があります。

TL1 を使用してこれをイネーブルにするには、『*Cisco ONS SONET TL1 Command Guide*』を参照してください。



### 注意

ML シリーズカードを RADIUS リレー モードに切り替えると、Cisco IOS コンフィギュレーションファイルの AAA/RADIUS に関連した設定が消去されます。クリアされた AAA/RADIUS 設定は、ML シリーズカードがスタンドアロン モードに戻った場合でも Cisco IOS コンフィギュレーションファイルに復元されません。



### 注意

ML シリーズカードがリレー モードのときに Cisco IOS コマンド `copy running-config startup-config` を使用しないでください。このコマンドは、RADIUS リレーがイネーブルの Cisco IOS コンフィギュレーションファイルを保存します。リポート時に、CTC の **Enable RADIUS Relay** チェックボックスがオンになっていなくても、ML シリーズカードが RADIUS リレー モードで起動します。このような状態が発生した場合、ユーザは **Enable RADIUS Relay** チェックボックスをオンにして **Apply** をクリックしてから、**Enable RADIUS Relay** チェックボックスをオフにして **Apply** をクリックします。これを行うと、ML シリーズカードがスタンドアロン モードに設定されて、ML シリーズカードの設定から RADIUS リレーがクリアされます。

## RADIUS スタンドアロン モード

スタンドアロン モードでは、ML シリーズ カードの RADIUS は、Cisco Catalyst スイッチの RADIUS と同じ一般的な方法で Cisco IOS CLI を使用して設定されます。

ここでは、ML シリーズ カードで RADIUS スタンドアロン モードのイネーブルおよび設定方法について説明します。スタンドアロン モードの RADIUS は、AAA 経由で機能し、AAA コマンドでイネーブルになります。



(注)

この章ではこれ以降、RADIUS とは、ML シリーズ カードがスタンドアロン モードのときに利用可能な Cisco IOS RADIUS のことを指します。RADIUS リレー モードのことは指しません。



(注)

ここで使用されている全構文と使用方法の情報については、『Cisco IOS Security Command Reference, Release 12.2』を参照してください。

ここでは、次の設定情報について説明します。

- [RADIUS の概要 \(p.19-9\)](#)
- [RADIUS スタンドアロン モード \(p.19-9\)](#)
- [RADIUS の設定 \(p.19-10\)](#)
- [RADIUS 設定の表示 \(p.19-23\)](#)

### RADIUS の概要

RADIUS サーバによってアクセス制御されるユーザが ML シリーズ カードにログインして認証を受けようとする場合に、次のイベントが発生します。

1. ユーザはユーザ名やパスワードを入力するように求められます。
2. ユーザ名と暗号化されたパスワードがネットワークを通じて RADIUS サーバへ送信されます。
3. ユーザは RADIUS サーバから以下のいずれかの応答を受信します。
  - a. ACCEPT ユーザが認証されました。
  - b. REJECT ユーザが認証されずにユーザ名とパスワードの再入力を求められるか、アクセスが拒否されました。

ACCEPT および REJECT 応答には、イネーブル EXEC またはネットワーク許可で使用される追加データが付いています。RADIUS がイネーブルの場合に、ユーザは RADIUS 許可の前にまず RADIUS 認証を正常に完了させる必要があります。ACCEPT および REJECT パケットに含まれる追加データには、以下の項目があります。

- Telnet、SSH、rlogin、およびイネーブル EXEC サービス
- ホストまたはクライアント IP アドレスなどの接続パラメータ、アクセス リスト、およびユーザ タイムアウト

## RADIUS の設定

ここでは、RADIUS をサポートするように ML シリーズカードを設定する方法について説明します。少なくとも、RADIUS サーバソフトウェアが稼働するホスト（複数可）を特定し、RADIUS 認証の方式リストを定義する必要があります。また認証を行うインターフェイスに方式リストを定義する必要があります。ML シリーズカードの場合、これは vty ポートです。任意で RADIUS 許可およびアカウントングの方式リストを定義することもできます。

ML シリーズカードに RADIUS 機能を設定する前に、RADIUS サーバにアクセスして設定を行う必要があります。

ここでは、以下の設定情報について説明します。

- [RADIUS のデフォルト設定 \(p.19-10\)](#)
- [RADIUS サーバホストの特定 \(p.19-10\)](#) (必須)
- [AAA ログイン認証の設定 \(p.19-13\)](#) (必須)
- [AAA サーバグループの定義 \(p.19-15\)](#) (任意)
- [ユーザイネーブルアクセスおよびネットワークサービス用の RADIUS 許可の設定 \(p.19-17\)](#) (任意)
- [RADIUS アカウントングの開始 \(p.19-18\)](#) (任意)
- [RADIUS パケット内の nas-ip-address の設定 \(p.19-19\)](#) (任意)
- [すべての RADIUS サーバに対する設定 \(p.19-20\)](#) (任意)
- [ベンダー固有の RADIUS 属性用の ML シリーズカードの設定 \(p.19-20\)](#) (任意)
- [ベンダー固有の RADIUS サーバ通信用の ML シリーズカードの設定 \(p.19-22\)](#) (任意)

## RADIUS のデフォルト設定

RADIUS と AAA は、デフォルトでディセーブルに設定されています。セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。RADIUS は、イネーブルに設定されている場合 Cisco IOS CLI を使用して、ML シリーズカードにアクセスするユーザを認証できます。

## RADIUS サーバホストの特定

ML シリーズカードと RADIUS サーバ間の通信には、次の要素が含まれています。

- ホスト名または IP アドレス
- 認証宛先ポート
- アカウントング宛先ポート
- キー文字列
- タイムアウト時間
- 再送信値

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号で識別されます。IP アドレスと UDP ポート番号の組み合わせによって一意の識別子が作成され、特定の AAA サービスを提供する RADIUS ホストとしてさまざまなポートを個別に定義できます。この一意の識別子によって、サーバ上の複数の UDP ポートに同じ IP アドレスで RADIUS 要求を送信できるようになります。

同一の RADIUS サーバ上の 2 つの異なるホスト エントリが同じサービス(たとえば、アカウントティング)を設定している場合、設定された 2 番目のホスト エントリは、最初のエントリの代行バックアップとして機能します。この例では、最初のホスト エントリがアカウントティング サービスを提供できない場合は、ML シリーズカードは、同じ装置上に設定された 2 番目のホスト エントリでアカウントティング サービスを試行します。

AAA セキュリティ コマンドを使用するように RADIUS を設定するには、RADIUS サーバデーモンが稼働するホストと、その ML シリーズカードと共有するシークレット(鍵)文字列を指定する必要があります。RADIUS サーバ、ONS ノード、および ML シリーズカードは、共有するシークレット文字列を使用してパスワードを暗号化し、応答を交換します。システムでは、ML シリーズカードの共有シークレット鍵が NE の共有シークレット鍵と一致することを保証しています。



(注)

スイッチにグローバルおよびサーバ単位の両方の機能(タイムアウト、再送信回数、およびキー コマンド)を設定すると、サーバ単位のタイマー、再送信回数、およびキー値コマンドは、グローバルのタイマー、再送信回数、およびキー値コマンドを上書きします。すべての RADIUS サーバに対してこれらの値を設定するには、「すべての RADIUS サーバに対する設定」(p.19-20)を参照してください。



(注)

再送信回数およびタイムアウト時間値は、スタンドアロン モードの ML シリーズカードに設定されます。これらの値は、リレー モードの ML シリーズカードには設定できません。

認証用に既存のサーバ ホストをグループ化するために、AAA サーバグループを使用するように ML シリーズカードを設定できます。詳細については、「AAA サーバグループの定義」(p.19-15)を参照してください。

サーバ単位での RADIUS サーバ通信を設定するには、イネーブル EXEC モードで次の手順を実行します。この手順は必須です。

	コマンドの説明	目的
ステップ 1	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	Router (config)# aaa new-model	AAA をイネーブルにします。

## ■ RADIUS スタンドアロン モード

	コマンドの説明	目的
ステップ 3	<pre>Router (config)# radius-server host {hostname   ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]</pre>	<p>リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。</p> <ul style="list-style-type: none"> <li>• (任意) <code>auth-port port-number</code> には、認証要求の UDP 宛先ポートを指定します。</li> <li>• (任意) <code>acct-port port-number</code> には、アカウントिंग要求の UDP 宛先ポートを指定します。</li> <li>• (任意) <code>timeout seconds</code> には、RADIUS サーバが応答するのを待ってスイッチが再送信するまでの時間を指定します。この範囲は 1 ~ 1000 です。この設定は、<code>radius-server timeout</code> グローバル コンフィギュレーション コマンドを上書きします。<code>radius-server host</code> コマンドでタイムアウトが設定されていない場合は、<code>radius-server timeout</code> コマンドの設定が使用されません。</li> <li>• (任意) <code>retransmit retries</code> には、サーバが応答しないか、応答が遅い場合に、RADIUS 要求をそのサーバに再送信する回数を指定します。この範囲は 1 ~ 1000 です。<code>radius-server host</code> コマンドで再送信値が設定されていない場合は、<code>radius-server retransmit</code> グローバル コンフィギュレーション コマンドの設定が使用されます。</li> <li>• (任意) <code>key string</code> には、スイッチと RADIUS サーバ上で稼働する RADIUS デーモンとの間で使用する認証および暗号化鍵を指定します。</li> </ul> <p> (注) 鍵は、RADIUS サーバ上で使用する暗号化鍵と一致する必要のある文字列です。鍵は、必ず <code>radius-server host</code> コマンドの最後の項目として設定します。先行スペースは無視されますが、鍵の途中および末尾のスペースは使用されます。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。</p> <p>1 つの IP アドレスに関連付けられた複数のホスト エントリをスイッチが認識するように設定するには、必要な回数だけこのコマンドを入力し、それぞれの UDP ポート番号が必ず異なるようにしてください。スイッチ ソフトウェアは、指定された順序でホストを検索します。特定の RADIUS ホストで使用するタイムアウト、再送信回数、および暗号化鍵の値を設定します。</p>
ステップ 4	<pre>Router (config)# end</pre>	イネーブル EXEC モードに戻ります。
ステップ 5	<pre>Router# show running-config</pre>	エントリを確認します。
ステップ 6	<pre>Router# copy running-config startup-config</pre>	(任意) コンフィギュレーション ファイルにエントリを保存します。

特定の RADIUS サーバを削除するには、`no radius-server host hostname | ip-address` グローバル コンフィギュレーション コマンドを使用します。

次の例では、ある RADIUS サーバを認証用に、別の RADIUS サーバをアカウントリング用に設定する方法を示します。

```
Switch(config)# radius-server host 172.29.36.49 auth-port 1612 key rad1
Switch(config)# radius-server host 172.20.36.50 acct-port 1618 key rad2
```

次の例では、RADIUS サーバとして *host1* を設定し、認証およびアカウントリングの両方にデフォルトポートを使用する方法を示します。

```
Switch(config)# radius-server host host1
```



(注)

さらに、RADIUS サーバでいくつかの設定を行う必要があります。この設定とは、スイッチの IP アドレス、およびサーバとスイッチで共有するキー文字列です。詳細については、RADIUS サーバのマニュアルを参照してください。

## AAA ログイン認証の設定

AAA 認証を設定するには、認証方式の名前付きリストを定義してから、さまざまなポートにそのリストを適用します。方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外は、*default* という名前のデフォルトの方式リストです。デフォルトの方式リストは、名前付き方式リストが明示的に定義されたポートを除いて、自動的にすべてのポートに適用されます。

方式リストは、ユーザ認証のためクエリ送信を行う順序と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティ プロトコルを指定できるので、最初の方式が失敗した場合のバックアップシステムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはその方式リストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試すまで続きます。この処理のある時点で認証が失敗した場合（つまり、セキュリティ サーバまたはローカルのユーザ名データベースがユーザ アクセスを拒否すると応答した場合）認証プロセスは停止し、それ以上認証方式が試行されることはありません。

AAA ログインの詳細については、『Cisco IOS Security Configuration Guide, Release 12.2』の「Authentication, Authorization, and Accounting (AAA)」の章を参照してください。次の URL にあります。

[http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html)

ログイン認証を設定するには、イネーブル EXEC モードで次の手順を実行します。この手順は必須です。

	コマンドの説明	目的
ステップ 1	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	Router (config)# aaa new-model	AAA をイネーブルにします。

	コマンドの説明	目的
ステップ 3	<pre>Router (config)# aaa authentication login {default   list-name} method1 [method2...]</pre>	<p>ログイン認証方式リストを作成します。</p> <ul style="list-style-type: none"> <li>• <b>login authentication</b> コマンドに名前付きリストが指定されていない場合に使用されるデフォルトのリストを作成するには、<b>default</b> キーワードの後ろにデフォルト状況で使用する方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。</li> <li>• <i>list-name</i> には、作成するリストの名前として使用する文字列を指定します。</li> <li>• <i>method1...</i> には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。</li> </ul> <p>次のいずれかの方式を選択します。</p> <ul style="list-style-type: none"> <li>- <b>enable</b> イネーブル パスワードを認証に使用します。この認証方式を使用するには、<b>enable password</b> 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、イネーブル パスワードをあらかじめ定義しておく必要があります。</li> <li>- <b>group radius</b> RADIUS 認証を使用します。この認証方式を使用するには、RADIUS サーバをあらかじめ設定しておく必要があります。詳細については、「<a href="#">RADIUS サーバ ホストの特定</a>」(p.19-10)を参照してください。</li> <li>- <b>line</b> 回線パスワードを認証に使用します。この認証方式を使用するには、回線パスワードをあらかじめ設定しておく必要があります。<b>password password</b> ライン コンフィギュレーション コマンドを使用します。</li> <li>- <b>local</b> ローカル ユーザ名データベースを認証に使用します。データベースにユーザ名情報を入力しておく必要があります。<b>username name password</b> グローバル コンフィギュレーション コマンドを使用します。</li> <li>- <b>local-case</b> 大文字と小文字が区別されるローカル ユーザ名データベースを認証に使用します。<b>username password</b> 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、データベースにユーザ名情報を入力する必要があります。</li> <li>- <b>none</b> ログインに認証を使用しません。</li> </ul>
ステップ 4	<pre>Router (config)# line [console   tty   vty] line-number [ending-line-number]</pre>	<p>ライン コンフィギュレーション モードを開始し、認証リストの適用対象とする回線を設定します。</p>
ステップ 5	<pre>Router (config-line)# login authentication {default   list-name}</pre>	<p>回線または回線セットに対して、認証リストを適用します。</p> <ul style="list-style-type: none"> <li>• <b>default</b> を指定する場合は、<b>aaa authentication login</b> コマンドで作成したデフォルトのリストを使用します。</li> <li>• <i>list-name</i> には、<b>aaa authentication login</b> コマンドで作成したリストを使用します。</li> </ul>
ステップ 6	<pre>Router (config)# end</pre>	<p>イネーブル EXEC モードに戻ります。</p>

	コマンドの説明	目的
ステップ 7	Router# show running-config	エントリを確認します。
ステップ 8	Router# copy running-config startup-config	(任意) コンフィギュレーション ファイルにエントリを保存します。

AAA をディセーブルにするには、`no aaa new-model` グローバル コンフィギュレーション コマンドを使用します。AAA 認証をディセーブルにするには、`no aaa authentication login {default | list-name} method1 [method2...]` グローバル コンフィギュレーション コマンドを使用します。ログイン用の RADIUS 認証をディセーブルにするかデフォルト値に戻す場合は、`no login authentication {default | list-name}` ライン コンフィギュレーション コマンドを使用します。

## AAA サーバ グループの定義

認証用に既存のサーバ ホストをグループ化するために、AAA サーバ グループを使用するように ML シリーズ カードを設定できます。設定済みサーバ ホストのサブセットを選択し、特定のサービスに使用できます。サーバ グループには、グローバル サーバ ホスト リストを使用します。このリストは、選択したサーバ ホストの IP アドレスのリストです。

サーバ グループには、各エントリが一意の識別子 (IP アドレスと UDP ポート番号の組み合わせ) を持っていれば、同じサーバに対して複数のホスト エントリを組み込むことができます。また、アカウントिंगなどの特定の AAA サービスを提供する RADIUS ホストとして、さまざまなポートを個別に定義できます。同じサービスに対して、同一 RADIUS サーバ上に 2 つの異なるホスト エントリを設定すると、設定された 2 番めのホスト エントリは、最初のエントリのフェールオーバー バックアップとして機能します。

定義済みのグループ サーバに特定のサーバを対応付けるには、`server` グループ サーバ コンフィギュレーション コマンドを使用します。IP アドレスでサーバを特定したり、任意の `auth-port` および `acct-port` キーワードを使用して複数のホスト インスタンスまたはエントリを識別することもできます。

AAA サーバ グループを定義してそれを特定の RADIUS サーバに対応付けるには、イネーブル EXEC モードで次の手順を実行します。

## ■ RADIUS スタンドアロン モード

	コマンドの説明	目的
ステップ 1	<code>Router# configure terminal</code>	グローバル 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	<code>Router (config)# aaa new-model</code>	AAA をイネーブルにします。
ステップ 3	<code>Router (config)# radius-server host {hostname   ip-address} [auth-port port-number] [acct-port port-number] [timeout seconds] [retransmit retries] [key string]</code>	<p>リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定します。</p> <ul style="list-style-type: none"> <li>• (任意) <code>auth-port port-number</code> には、認証要求の UDP 宛先ポートを指定します。</li> <li>• (任意) <code>acct-port port-number</code> には、アカウントینگ要求の UDP 宛先ポートを指定します。</li> <li>• (任意) <code>timeout seconds</code> には、RADIUS サーバが応答するのを待ってスイッチが再送信するまでの時間を指定します。この範囲は 1 ~ 1000 です。この設定は、<code>radius-server timeout</code> グローバル コンフィギュレーション コマンド設定を上書きします。<code>radius-server host</code> コマンドでタイムアウトが設定されていない場合は、<code>radius-server timeout</code> コマンドの設定が使用されます。</li> <li>• (任意) <code>retransmit retries</code> には、サーバが応答しないか、応答が遅い場合に、RADIUS 要求をそのサーバに再送信する回数を指定します。この範囲は 1 ~ 1000 です。<code>radius-server host</code> コマンドで再送信値が設定されていない場合は、<code>radius-server retransmit</code> グローバル コンフィギュレーション コマンドの設定が使用されます。</li> <li>• (任意) <code>key string</code> には、スイッチと RADIUS サーバ上で稼働する RADIUS デーモンとの間で使用する認証および暗号化鍵を指定します。</li> </ul> <p> (注) 鍵は、RADIUS サーバ上で使用する暗号化鍵と一致する必要のある文字列です。鍵は、必ず <code>radius-server host</code> コマンドの最後の項目として設定します。先行スペースは無視されますが、鍵の途中および末尾のスペースは使用されます。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。</p> <p>1 つの IP アドレスに関連付けられた複数のホスト エントリをスイッチが認識するように設定するには、必要な回数だけこのコマンドを入力し、それぞれの UDP ポート番号が必ず異なるようにしてください。スイッチ ソフトウェアは、指定された順序でホストを検索します。特定の RADIUS ホストで使用するタイムアウト、再送信回数、および暗号化鍵の値を設定します。</p>
ステップ 4	<code>Router (config)# aaa group server radius group-name</code>	<p>グループ名で AAA サーバグループを定義します。</p> <p>このコマンドによって、ML シリーズカードはサーバグループ コンフィギュレーション モードになります。</p>

	コマンドの説明	目的
ステップ 5	Router (config-sg-radius)# server ip-address	特定の RADIUS サーバを定義済みサーバ グループに対応付けます。AAA サーバグループの RADIUS サーバごとに、このステップを繰り返します。  グループの各サーバは、ステップ 2 で定義済みのものでなければなりません。
ステップ 6	Router (config-sg-radius)# end	イネーブル EXEC モードに戻ります。
ステップ 7	Router # show running-config	エントリを確認します。
ステップ 8	Router # copy running-config startup-config	(任意) コンフィギュレーション ファイルにエントリを保存します。
ステップ 9		RADIUS ログイン認証をイネーブルにします。「AAA ログイン認証の設定」(p.19-13)を参照してください。

特定の RADIUS サーバを削除するには、`no radius-server host hostname | ip-address` グローバル コンフィギュレーション コマンドを使用します。コンフィギュレーション リストからサーバグループを削除するには、`no aaa group server radius group-name` グローバル コンフィギュレーション コマンドを使用します。RADIUS サーバの IP アドレスを削除するには、`no server ip-address` サーバグループ コンフィギュレーション コマンドを使用します。

この例では、ML シリーズカードが、2つの異なる RADIUS グループサーバ (`group1` と `group2`) を認識するように設定されます。`group1` では、同一の RADIUS サーバ上の 2 つの異なるホスト エントリに同じサービスを設定しています。2 番目のホスト エントリは、最初のエントリのフェールオーバー バックアップとして機能します。

```
Switch(config)# radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config)# radius-server host 172.10.0.1 auth-port 1645 acct-port 1646
Switch(config)# aaa new-model
Switch(config)# aaa group server radius group1
Switch(config-sg-radius)# server 172.20.0.1 auth-port 1000 acct-port 1001
Switch(config-sg-radius)# exit
Switch(config)# aaa group server radius group2
Switch(config-sg-radius)# server 172.20.0.1 auth-port 2000 acct-port 2001
Switch(config-sg-radius)# exit
```

## ユーザイネーブルアクセスおよびネットワーク サービス用の RADIUS 許可の設定

AAA 許可は、ユーザが利用できるサービスを制限します。AAA 許可がイネーブルに設定されていると、ML シリーズカードはユーザのプロファイルから取得した情報を使用します。このプロファイルは、ローカルのユーザ データベースまたはセキュリティ サーバ上にあり、ユーザのセッションを設定します。ユーザは、プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが許可されます。

ML シリーズカードでのイネーブル レベルの設定または `priv-lvl` コマンドの使用は、サポートされていません。RADIUS サーバで認証されたユーザは、デフォルトのログイン権限レベルであるイネーブル モード 1 でのみ ML シリーズカードにアクセスできます。このため、RADIUS サーバに設定されている `priv-lvl` は、`priv-lvl 0` または `1` になります。ユーザが認証されて ML シリーズカードへのアクセスが許可されると、イネーブル パスワードを使用してイネーブル EXEC 認証を得ることができ、権限レベル 15 のスーパーユーザになることができます。これは、イネーブル モードのデフォルトの権限レベルです。

## ■ RADIUS スタンドアロン モード

この ML シリーズカード ユーザ レコードの例は、RADIUS サーバからの出力で、権限レベルを示しています。

```
CISCO15 Auth-Type := Local, User-Password == "otbu+1"
Service-Type = Login,
Session-Timeout = 100000,
Cisco-AVPair = "shell:priv-lvl=1"
```

**aaa authorization** グローバル コンフィギュレーション コマンドに **radius** キーワードを付けて使用すると、イネーブル EXEC モードへのユーザのネットワーク アクセスを制限するパラメータを設定できます。

**aaa authorization exec radius local** コマンドは、以下の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、イネーブル EXEC アクセス許可に RADIUS を使用します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。



(注) 許可が設定されていても、CLI 経由でログインして認証されたユーザに対して、許可が省略されます。

イネーブル EXEC アクセスおよびネットワーク サービスに関する RADIUS 許可を指定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <b>configure terminal</b>	グローバル 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	Router (config)# <b>aaa authorization network radius</b>	ネットワーク関連のすべてのサービス要求に対するユーザ RADIUS 許可を ML シリーズカードに設定します。
ステップ 3	Router (config)# <b>aaa authorization exec radius</b>	イネーブル EXEC アクセスの有無を、ユーザ RADIUS 許可によって判別するように ML シリーズカードを設定します。  exec キーワードを指定すると、ユーザ プロファイル情報 (autocommand 情報など) を返すことができます。
ステップ 4	Router (config)# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 5	Router# <b>show running-config</b>	エントリを確認します。
ステップ 6	Router# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

許可をディセーブルにするには、**no aaa authorization {network | exec} method1** グローバル コンフィギュレーション コマンドを使用します。

## RADIUS アカウンティングの開始

AAA アカウンティング機能は、ユーザがアクセスしているサービスと、ユーザが消費しているネットワーク リソースを追跡します。AAA アカウンティングがイネーブルに設定されていると、ML シリーズカードは、アカウンティング レコードの形式でユーザの活動状況を RADIUS セキュリティサーバにレポートします。各アカウンティング レコードには、アカウンティングの Attribute-Value (AV) のペアが含まれ、セキュリティ サーバ上に保存されます。このデータを分析し、ネットワーク管理、クライアントへの課金、または監査に利用できます。

各 Cisco IOS 権限レベルおよびネットワーク サービスに関する RADIUS アカウンティングをイネーブルにするには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <code>configure terminal</code>	グローバル 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	Router (config)# <code>aaa accounting network start-stop radius</code>	ネットワーク関連のすべてのサービス要求に関する RADIUS アカウンティングをイネーブルにします。
ステップ 3	Router (config)# <code>aaa accounting exec start-stop radius</code>	RADIUS アカウンティングをイネーブルにして、イネーブル EXEC プロセスの開始時に記録開始アカウンティング通知を送信し、終了時に記録停止通知を送信します。
ステップ 4	Router (config)# <code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	Router# <code>show running-config</code>	エントリを確認します。
ステップ 6	Router# <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエントリを保存します。

アカウンティングをディセーブルにするには、`no aaa accounting {network | exec} start-stop method1...` グローバル コンフィギュレーション コマンドを使用します。

## RADIUS パケット内の nas-ip-address の設定

RADIUS リレー モードの ML シリーズカードを使用すると、ユーザは各 ML シリーズカードに対して個別の `nas-ip-address` を設定できます。RADIUS スタンドアロン モードでは、このコマンドは Cisco IOS CLI に隠されています。これにより、RADIUS サーバが同一 ONS ノード内の ML シリーズカードを個別に識別できます。サーバに要求を送信した特定の ML シリーズカードを識別できると、サーバのデバッグ時に便利です。`nas-ip-address` は、主に RADIUS 認証およびアカウンティング要求の検証に使用されます。

この値が設定されていない場合、`nas-ip-address` は、`ip radius-source` コマンドで設定された値を使用して通常の Cisco IOS メカニズムによって設定されます。値が設定されていない場合は、サーバヘルディング可能な最良の IP アドレスが使用されます。ルーティング可能なアドレスを使用できない場合は、サーバの IP アドレスが使用されます。

`nas-ip-address` を設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	Router# <code>configure terminal</code>	グローバル 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	Router (config)# <code>[no] ip radius nas-ip-address {hostname   ip-address}</code>	RADIUS パケット内にある属性 4 ( <code>nas-ip-address</code> ) の IP アドレスまたはホスト名を指定します。  ONS ノードに ML シリーズカードが 1 つしかない場合は、このコマンドを使用するメリットはありません。ONS ノードのパブリック IP アドレスは、サーバに送信される RADIUS パケット内の <code>nas-ip-address</code> として機能します。
ステップ 3	Router (config)# <code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 4	Router# <code>show running-config</code>	エントリを確認します。
ステップ 5	Router# <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエントリを保存します。

## ■ RADIUS スタンドアロン モード

## すべての RADIUS サーバに対する設定

ML シリーズカードとすべての RADIUS サーバ間のグローバル通信設定を設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	<code>Router# configure terminal</code>	グローバル 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	<code>Router (config)# radius-server key string</code>	ML シリーズカードとすべての RADIUS サーバとの間で使用する、共有シークレット文字列を指定します。   (注) 鍵は、RADIUS サーバ上で使用する暗号化鍵と一致する必要のある文字列です。先行スペースは無視されますが、鍵の途中および末尾のスペースは使用されません。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。
ステップ 3	<code>Router (config)# radius-server retransmit retries</code>	ML シリーズカードが、サーバに各 RADIUS 要求を送信する回数を指定します。デフォルトは 3 で、指定できる範囲は 1 ~ 1000 です。
ステップ 4	<code>Router (config)# radius-server timeout seconds</code>	ML シリーズカードが、RADIUS 要求に対する応答を待つ要求を再送信するまでの秒数を指定します。デフォルトは 5 秒で、指定できる範囲は 1 ~ 1000 です。
ステップ 5	<code>Router (config)# radius-server deadtime minutes</code>	認証要求への応答に失敗した RADIUS サーバに [dead] とマーキングするまでの分数を指定します。[dead] としてマーキングされている RADIUS サーバは、指定した分数の間追加の認証要求をスキップされます。これにより、要求がタイムアウトするまで待たずに、次の設定サーバを試行できます。すべての RADIUS サーバが [dead] としてマーキングされている場合、スキップは行われません。  デフォルトは 0 で、指定できる範囲は 0 ~ 1440 分です。
ステップ 6	<code>Router (config)# end</code>	イネーブル EXEC モードに戻ります。
ステップ 7	<code>Router# show running-config</code>	エントリを確認します。
ステップ 8	<code>Router# copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエントリを保存します。

再送信、タイムアウト、デッドタイムの設定をデフォルトに戻すには、これらのコマンドの `no` 形式を使用します。

## ベンダー固有の RADIUS 属性用の ML シリーズカードの設定

Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) ドラフト規格では、Vendor-Specific Attribute (VSA) (属性 26) を使用して、ML シリーズカードと RADIUS サーバとの間のベンダー固有情報の通信方式を定めています。VSA を使用すると、ベンダーは、汎用に適さない独自の拡張属性をサポートできます。シスコの RADIUS 実装では、仕様で推奨された形式を使用して 1 つのベンダー固有オプションをサポートします。シスコのベンダー ID は 9 で、サポート対象のオプションにはベンダータイプ 1 が設定されており、`cisco-avpair` と名前が付けられています。この値は次の形式の文字列です。

`protocol : attribute sep value *`

*protocol* は、特定のタイプの許可に対応する シスコ プロトコル属性です。 *attribute* と *value* は、シスコ Terminal Access Controller Access Control System Plus (TACACS+) 仕様で定義されている適切な AV のペアです。 *sep* は、必須属性の場合は =、任意属性の場合は \* です。 TACACS+ 許可で利用できるすべての機能は、RADIUS にも使用できます。

たとえば、次の AV ペアは、IP 許可時 (PPP [ポイントツーポイント プロトコル] の Internet Protocol Control Protocol [IPCP] アドレス割り当て時) に、シスコの複数の名前付き IP アドレス プール機能をアクティブにします。

```
cisco-avpair= "ip:addr-pool=first"
```

次の例では、RADIUS サーバ データベース内の許可 VLAN を指定する方法を示します。

```
cisco-avpair= "tunnel-type(#64)=VLAN(13)"
cisco-avpair= "tunnel-medium-type(#65)=802 media(6)"
cisco-avpair= "tunnel-private-group-ID(#81)=vlanid"
```

次の例では、この接続中に ASCII 形式の入力 Access Control List (ACL; アクセス制御リスト) をインターフェイスに適用する方法を示します。

```
cisco-avpair= "ip:inacl#1=deny ip 10.10.10.10 0.0.255.255 20.20.20.20 255.255.0.0"
cisco-avpair= "ip:inacl#2=deny ip 10.10.10.10 0.0.255.255 any"
cisco-avpair= "mac:inacl#3=deny any any decnet-iv"
```

次の例では、この接続中に ASCII 形式の出力 ACL をインターフェイスに適用する方法を示します。

```
cisco-avpair= "ip:outacl#2=deny ip 10.10.10.10 0.0.255.255 any"
```

その他のベンダーにも、独自に一意のベンダー ID、オプション、および対応する VSA が割り当てられます。ベンダー ID と VSA の詳細については、RFC 2138 『Remote Authentication Dial-In User Service (RADIUS)』を参照してください。

VSA を認識して使用するように ML シリーズカードを設定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	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	Router (config)# radius-server vsa send [accounting   authentication]	ML シリーズカードが、RADIUS IETF 属性 26 に定義されている VSA を認識して使用できるようにします。 <ul style="list-style-type: none"> <li>(任意) <b>accounting</b> キーワードを使用して、認識される VSA の集合をアカウント属性のみに限定します。</li> <li>(任意) <b>authentication</b> キーワードを使用して、認識されるベンダー固有の属性の集合を認証属性に限定します。</li> </ul> キーワードなしでこのコマンドを入力すると、アカウントおよび認証の両方の VSA が使用されます。 AAA サーバは、ML シリーズカードの VSA 応答メッセージに認証レベルを含めます。
ステップ 3	Router (config)# end	イネーブル EXEC モードに戻ります。
ステップ 4	Router# show running-config	エントリを確認します。
ステップ 5	Router# copy running-config startup-config	(任意) コンフィギュレーション ファイルにエントリを保存します。

## ■ RADIUS スタンドアロン モード

RADIUS 属性の完全リスト、またはベンダー固有の属性 26 の詳細については、『Cisco IOS Security Configuration Guide, Release 12.2』の付録「RADIUS Attributes」を参照してください。

## ベンダー固有の RADIUS サーバ通信の ML シリーズカードの設定

RADIUS に関する IETF ドラフト規格では、ML シリーズカードと RADIUS サーバとの間のベンダー固有情報の通信方法を規定していますが、一部のベンダーは、固有の方法で RADIUS 属性の集合を機能拡張しています。Cisco IOS ソフトウェアは、ベンダー固有仕様の RADIUS 属性のサブセットをサポートします。

前述したように、RADIUS (ベンダー固有または IETF のドラフト準拠) を設定するには、RADIUS サーバ デモンが稼働しているホスト、および ML シリーズカードと共有するシークレット文字列を指定する必要があります。RADIUS ホストおよびシークレット文字列を指定するには、`radius-server` グローバル コンフィギュレーション コマンドを使用します。

ベンダー固有の RADIUS サーバ ホスト、および共有シークレット文字列を指定するには、イネーブル EXEC モードで次の手順を実行します。

	コマンドの説明	目的
ステップ 1	<code>Router# configure terminal</code>	グローバル 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	<code>Router (config)# radius-server host {hostname   ip-address} non-standard</code>	リモート RADIUS サーバ ホストの IP アドレスまたはホスト名を指定し、ベンダー固有の RADIUS 実装を使用していることを明確にします。
ステップ 3	<code>Router (config)# radius-server key string</code>	ML シリーズカードとベンダー固有の RADIUS サーバとの間で使用する、共有シークレット文字列を指定します。ML シリーズカードおよび RADIUS サーバは、この文字列を使用してパスワードを暗号化し、応答を交換します。   (注) 鍵は、RADIUS サーバ上で使用する暗号化鍵と一致する必要のある文字列です。先行スペースは無視されますが、鍵の途中および末尾のスペースは使用されません。鍵にスペースを使用する場合は、鍵の一部として引用符を使用する場合を除いて、鍵を引用符で囲まないでください。
ステップ 4	<code>Router (config)# end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>Router# show running-config</code>	エントリを確認します。
ステップ 6	<code>Router# copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエントリを保存します。

ベンダー固有の RADIUS ホストを削除するには、`no radius-server host {hostname | ip-address} non-standard` グローバル コンフィギュレーション コマンドを使用します。鍵をディセーブルにするには、`no radius-server key` グローバル コンフィギュレーション コマンドを使用します。

次の例では、ベンダー固有の RADIUS ホストを指定して、ML シリーズカードとサーバの間で `rad124` という秘密鍵を使用する方法を示します。

```
Switch(config)# radius-server host 172.20.30.15 nonstandard
Switch(config)# radius-server key rad124
```

## RADIUS 設定の表示

RADIUS 設定を表示するには、`show running-config` イネーブル EXEC コマンドを使用します。

■ RADIUS スタンドアロン モード



## ONS イーサネット カード上の POS

---

この章では、Packet-over-SONET/SDH (POS) および ONS イーサネット カードでの POS の実装について説明します。

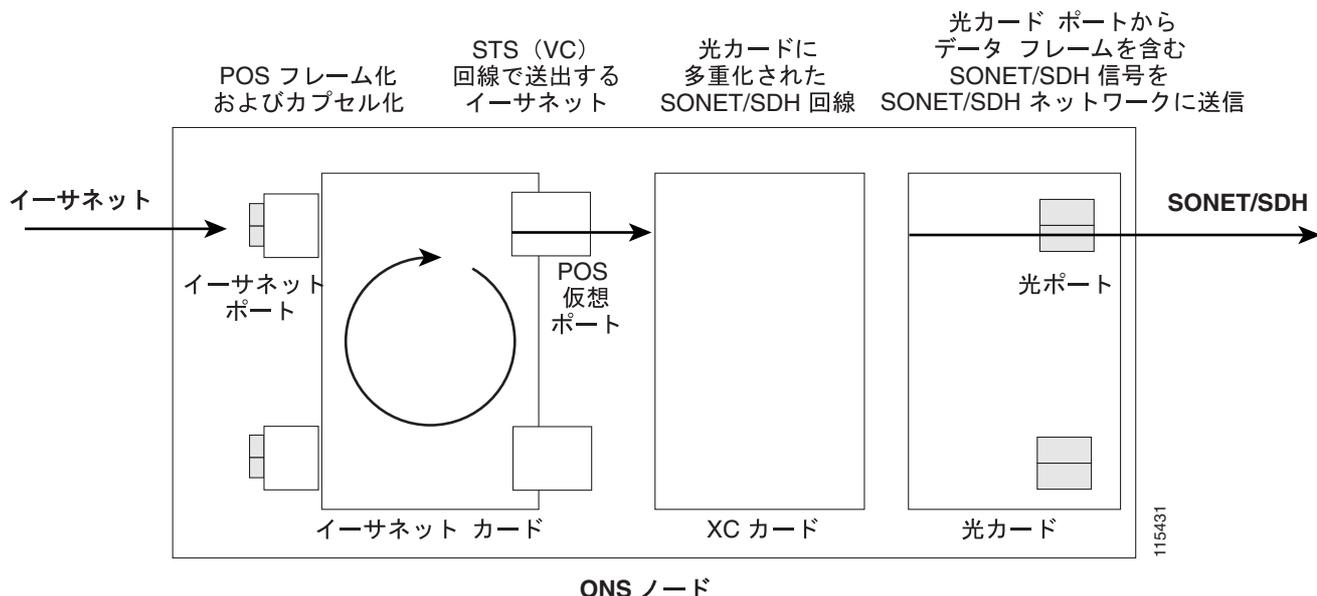
この章の内容は次のとおりです。

- [POS の概要 \(p.20-2\)](#)
- [POS 相互運用性 \(p.20-3\)](#)
- [POS カプセル化タイプ \(p.20-5\)](#)
- [POS フレーミング モード \(p.20-7\)](#)
- [特定の ONS イーサネット カードの POS 特性 \(p.20-8\)](#)
- [イーサネットのクロッキングと SONET/SDH のクロッキング \(p.20-12\)](#)

## POS の概要

Asynchronous Transfer Mode( ATM; 非同期転送モード )およびフレームリレーと異なり、イーサネットは本来、SONET/SDH とインターフェイスするように設計されていませんでした。イーサネットのデータ パッケージは、SONET/SDH ネットワーク上で転送するために、SONET/SDH フレームにフレーム化およびカプセル化する必要があります。このフレーム化およびカプセル化処理は POS として知られています。

図 20-1 ONS ノードでのイーサネットから POS へのプロセス



すべての ONS イーサネット カードは POS を使用します。イーサネット フレームは、標準ファストイーサネットまたはギガビットイーサネットポートのカードに到着し、ONS イーサネットカードのフレーム化メカニズムによって処理されて、POS フレームにカプセル化されます。POS フレームが ONS イーサネットカードから POS 回線に出ると、この回線は ONS ノードの他の SONET 回線 (STS) または SDH 回線 (VC) と同じように処理されます。この回線は相互接続され、光カードのポートから SONET/SDH ネットワークへ SONET/SDH 信号を送出します。

POS 回線の宛先は、ONS イーサネットカードまたは POS インターフェイスをサポートする他の装置です。宛先カードで受信した POS フレームは、データ パッケージが取り外されてイーサネットフレームに処理されます。次に、イーサネットフレームは、ONS イーサネットカードの標準イーサネットポートに送信されて、イーサネットネットワークに送信されます。

G シリーズ、CE シリーズ、および E シリーズ ( port-mapper モードに設定 ) ONS イーサネットカードは、SONET/SDH または POS 回線をカードのいずれかのイーサネットポートに直接マップします。ML シリーズおよび E シリーズ ( EtherSwitch モードに設定 ) ONS イーサネットカードには、カードの標準イーサネットポートを備えたスイッチング ファブリックのスイッチポートとして POS ポートが含まれます。ONS 15454 および ONS 15454 SDH ML シリーズカードもレイヤ 3 機能をサポートします。

## POS 相互運用性

同じファミリーのイーサネットカード間の POS 回線に加えて、異なるファミリーの一部のイーサネットカード間の POS 回線の作成も可能です。Cisco Transport Controller (CTC) の回線作成ウィザードでは、特定のイーサネットカードタイプを回線作成の送信元カードとして選択したときに、宛先カードオプションの下に使用可能な相互運用できるイーサネットカードが表示されます。SDH ノードからの回線と SONET ノードからの回線を混在することはできません。

POS 回線は、マッパータイプのカードとスイッチタイプの ONS イーサネットカード間で作成できます。ただし、回線からポートへの転送だけが可能であり、スイッチング機能はサポートされません。たとえば、POS 回線の送信元カードとして ONS 15454 ML シリーズカードを使用する場合、G シリーズまたは CE シリーズが宛先カードとして使用できます。ただし、ML シリーズスイッチ機能をすべて設定できるわけではありません。たとえば、ML シリーズと ML シリーズとの間の回線では、接続された POS ポートを VLAN のメンバーとして設定できますが、接続された G シリーズの POS ポートは、G シリーズカードが VLAN をサポートしないために、VLAN メンバーとして設定できません。

イーサネットカード POS で相互運用を行うためには、次の主要な 3 つの POS ポートの特性が一致する必要があります。

- POS カプセル化
- CRC サイズ
- フレーミングモード

Frame-mapped Generic Framing Procedure (GFP-F) フレーミングモードを使用する場合には、CRC サイズオプションが両方のエンドポイントで一致する必要はありません。

すべてのイーサネットカードが相互運用できるわけではなく、また、すべての POS ポート特性オプションをサポートするわけではありません。次に示す 2 つの表に、相互運用可能なイーサネットカードとその特性を示します。表 20-1 に、High-Level Data Link Control (HDLC; ハイレベルデータリンク制御) フレーミングモードがサポートされて設定されているカードに対する情報を示します。

表 20-2 に、GFP-F フレーミングモードがサポートされ設定されているカードに対する情報を示します。表 20-2 と GFP-F フレーミングでは、LEX という用語は ITU-T G.7041 に基づいた GFP-F 上の標準マップイーサネットを表します。GFP-F フレーミングでは、Cisco IOS CLI も lex キーワードを使用して ITU-T G.7041 に基づいた GFP-F 上の標準マップイーサネットを表します。

表 20-1 HDLC フレーミングでの ONS SONET/SDH イーサネットカードの相互運用性 (カプセル化タイプと CRC も含む)

	ポートマップ E シリーズ (ONS 15327) <sup>1</sup>	ポートマップ E シリーズ (ONS 15454 SONET/SDH) <sup>1</sup>	G シリーズ (すべてのプラットフォーム)	ML シリーズ (ONS 15454 SONET/SDH)	ML シリーズ (ONS 15310-CL/ONS 15310-MA)	CE シリーズ (すべてのプラットフォーム)
ポートマップ E シリーズ (ONS15327)	独自仕様 LEX (CRC 16)	独自仕様	互換性なし	LEX (CRC 16)	互換性なし	互換性なし
ポートマップ E シリーズ (ONS 15454 SONET/SDH)	独自仕様	独自仕様	互換性なし	互換性なし	互換性なし	互換性なし
G シリーズ (すべてのプラットフォーム)	互換性なし	互換性なし	LEX (CRC 16) LEX (CRC 32)	LEX (CRC 16) LEX (CRC 32)	LEX (CRC 32)	LEX (CRC 32)

## ■ POS 相互運用性

表 20-1 HDLC フレーミングでの ONS SONET/SDH イーサネット カードの相互運用性 (カプセル化タイプと CRC も含む)(続き)

	ポートマップ E シリーズ (ONS 15327) <sup>1</sup>	ポートマップ E シリーズ (ONS 15454 SONET/SDH) <sup>1</sup>	G シリーズ (すべてのプラッ トフォーム)	ML シリーズ (ONS 15454 SONET/SDH)	ML シリーズ (ONS 15310-CL/ ONS 15310-MA)	CE シリーズ (すべてのプラッ トフォーム)
ML シリーズ (ONS 15454 SONET/SDH)	LEX (CRC 16)	互換性なし	LEX (CRC 16) LEX (CRC 32)	LEX (CRC 16) LEX (CRC 32) Cisco HDLC PPP/BCP	LEX (CRC 32)	LEX (CRC 32)
ML シリーズ (ONS 15310-CL/ ONS 15310-MA)	互換性なし	互換性なし	LEX (CRC 32)	LEX (CRC 32)	LEX (CRC 32)	LEX (CRC 32)
CE シリーズ (すべてのプラッ トフォーム)	互換性なし	互換性なし	LEX (CRC 32)	LEX (CRC 32)	LEX (CRC 32)	LEX (CRC 32)

1. EtherSwitch モードの E シリーズ カードは、他の ONS イーサネット カード タイプとは相互運用できません。

表 20-2 GFP-F フレーミングでの ONS SONET/SDH イーサネット カードの相互運用性 (カプセル化タイプを含む)

	ML シリーズ (ONS 15454)	ML シリーズ (ONS 15310)	CE シリーズ (すべてのプラットフォーム)
ML シリーズ (ONS 15454 SONET/SDH)	LEX (CRC 32) Cisco HDLC (CRC 32) PPP/BCP (CRC 32)	LEX (CRC 32) Cisco HDLC (CRC 32) PPP/BCP (CRC 32)	LEX (CRC 32)
ML シリーズ (ONS 15310-CL/ ONS 5310-MA)	LEX (CRC 32) Cisco HDLC (CRC 32) PPP/BCP (CRC 32)	LEX (CRC 32 またはなし) Cisco HDLC (CRC 32 または なし) PPP/BCP (CRC 32 またはな し)	LEX (CRC 32 またはなし)
CE シリーズ (すべてのプラットフォーム)	LEX (CRC 32)	LEX (CRC 32 またはなし)	LEX (CRC 32 またはなし)



(注) RPR では、すべての ML シリーズ カードで LEX カプセル化が必要です。



(注) GFP-F 上では、LEX は ITU-T G.7041 に基づいた GFP-F 上の標準マップ イーサネットです。

GFP-F フレーミングは、Release 5.0 以降のソフトウェアを実行しているノードのみでサポートされています。また、ML100T-12 カードおよび ML1000-2 カードでは、GFP-F フレーミングを行うために Field Programmable Gate Array (FPGA) バージョン 4.0 以降が必要です。

# POS カプセル化タイプ

ONS イーサネットカードは、Cisco Ethernet-over-SONET LEX (LEX)、Cisco HDLC、Point-to-Point Protocol (PPP) /Bridging Control Protocol (ポイントツーポイント プロトコル /BCP)、および E シリーズ専用の 4 つの POS カプセル化方式をサポートします。ONS イーサネット送信元カードおよび宛先カードは、相互運用を行うために同じ POS カプセル化方式で設定する必要があります。すべての ONS イーサネットカードが相互運用できるわけではなく、すべてのカプセル化タイプをサポートするわけではありません。

## LEX

Cisco EoS LEX は ONS イーサネットカードの主要なカプセル化方式です。このカプセル化は HDLC フレーミングで行われ、そのプロトコルフィールドは、Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) の Request For Comments (RFC; コメント要求) 1841 で指定された値に設定されます。GFP-F フレーミングでの Cisco IOS CLI も lex キーワードを使用します。GFP-F フレーミングでは、lex キーワードを使用して ITU-T G.7041 に基づいた GFP-F 上の標準マップイーサネットを表します。

図 20-2 に、HDLC フレーミングでの EoS LEX を示します。

LEX は、ONS 15454 および ONS 15454 SDH E シリーズカードを除く、すべての ONS イーサネットカードでサポートされます。

図 20-2 HDLC フレーミングでの LEX

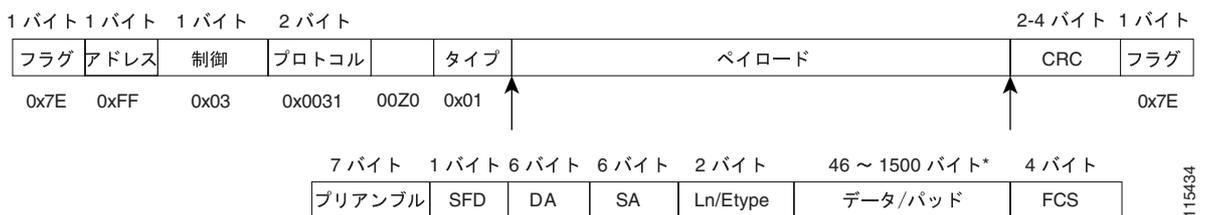


115433

## PPP/BCP

PPP カプセル化方式は、RFC 2615 (PPP-over-SONET/SDH) の標準実装で、SONET 上で 802.1Q タグ付きおよびタグなしイーサネット フレームを送信するために RFC 3518 (BCP) が標準実装されています。図 20-3 に、BCP を示します。

図 20-3 HDLC フレーミングでの BCP

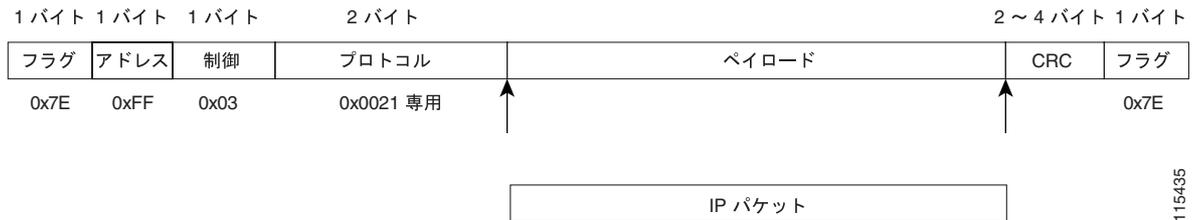


115434

## ■ POS カプセル化タイプ

ONS 15454/ONS 15454 SDH の ML シリーズでは、ルーティング機能をサポートします。このカードの POS ポートが PPP カプセル化によってルーティングをサポートするように設定された場合、IP パケットは、標準 0x0021 プロトコル コード ポイントを使用する HDLC フレームにマップされません。図 20-4 に PPP を示します。

図 20-4 HDLC フレーミングでの PPP フレーム

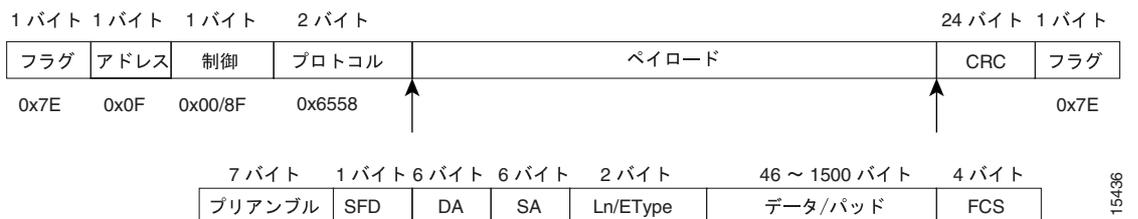


## Cisco HDLC

Cisco HDLC は、シリアル インターフェイスへパケットをマッピングするシスコ標準方式です。このカプセル化は、ML シリーズ カードを、Cisco HDLC 準拠のルータおよびスイッチの POS インターフェイスへインターフェイスする場合に使用できます。

IP パケットの搬送に使用する場合、同じ HDLC フレーム構造が使用されますが、プロトコル フィールドは 0x0800 に設定され、ペイロードに IP パケットが含まれます。図 20-5 に、Cisco HDLC を示します。

図 20-5 HDLC フレーミングでの Cisco HDLC



## E シリーズ専用

E シリーズでは、HDLC に似た専用のカプセル化方式を使用します。この方式は、LEX、Cisco HDLC、または PPP/BCP との互換性がありません。この専用のカプセル化方式は、E シリーズが他の ONS イーサネット カードと相互運用するのを防ぎます。

リリース 5.0 以降では、ONS 15327 E シリーズ カード、E10/100-4 は、本来の専用 E シリーズ カプセル化だけでなく、16 ビット CRC の LEX カプセル化もサポートします。



(注) E シリーズ カード (ONS 15327 または ONS 15454) のどちらも G シリーズ カードと相互運用できません。

## POS フレーミングモード

この POS フレーミングモードは、データパケットをフレーム化して POS 信号にカプセル化するための、ONS イーサネットカードで使用するフレーミングメカニズムのタイプです。これらのデータパケットは当初、ONS イーサネットカードの標準ファストイーサネットまたはギガビットイーサネットインターフェイスに入力されるイーサネットフレームにカプセル化されていました。すべての ONS イーサネットカードは HDLC フレーミングをサポートします。また、ML シリーズおよび CE シリーズカードは、GFP-F フレーミングモードもサポートします。

### HDLC フレーミング

HDLC は、最も使用されているレイヤ 2 プロトコルのうちの 1 つです。HDLC プロトコルで 사용되는フレーミングメカニズムである、HDLC フレーミングは、ONS イーサネットカード上の POS を含め、さまざまな他のプロトコルで使用されています。HDLC フレーミングメカニズムの詳細については、IETF の RFC 1662「PPP in HDLC-like Framing」を参照してください。

HDLC フレームでは、ゼロ挿入 / 削除処理（ビットスタッフィングとして一般に知られている）を使用して、区切りフラグのビットパターンがフラグ間のフィールドで発生しないようにします。HDLC フレームは同期を取ります。このため、クロッキング方式の提供と、フレームの送受信の同期を取るために物理層に依存します。

### GFP-F フレーミング

GFP は、さまざまなサービスタイプを SONET/SDH の標準ベースのマッピング方式を定義しています。ML シリーズおよび CE シリーズは、GFP 向けの PDU 型クライアントシグナルアダプテーションモードである、GFP-F をサポートします。GFP-F では、1 つの可変長データパケットを 1 つの GFP パケットにマッピングします。

GFP は、共通機能とペイロード固有の機能で構成されます。共有機能はすべてのペイロードで共有されます。ペイロード固有の機能は、ペイロードの種類によって異なります。GFP は ITU 勧告 G.7041 で詳しく定義されています。

## 特定の ONS イーサネット カードの POS 特性

ここでは、特定の ONS イーサネット カードでサポートされるさまざまなフレーム化オプションとカプセル化オプションを説明します。

### ONS 15327 E-10/100-4 フレーム化オプションとカプセル化オプション

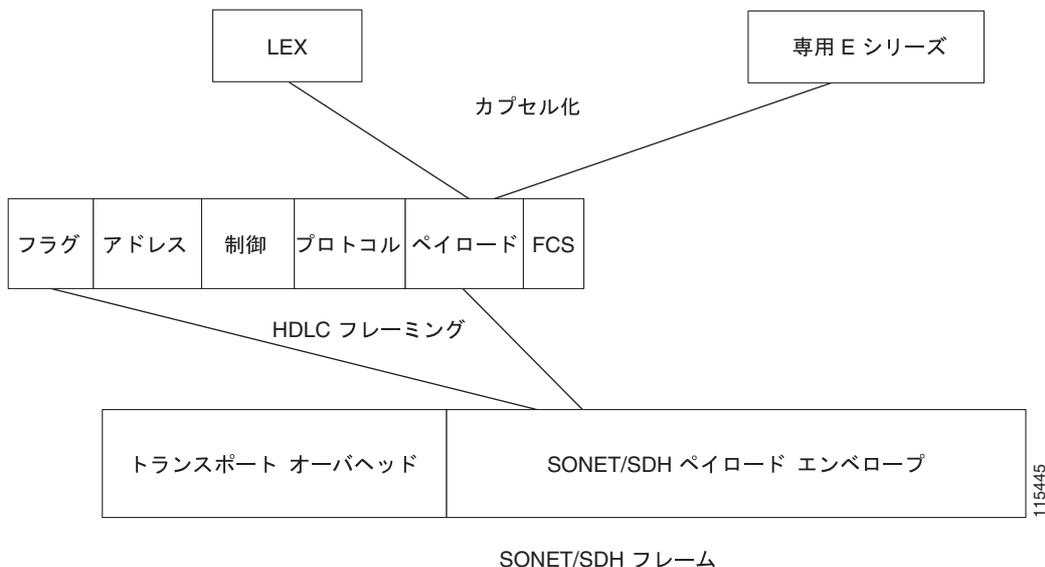
Release 5.0 以降のソフトウェアでは、ONS 15327 の、ポートマップ モードに設定された E-10/100-4 カードで、LEX カプセル化の設定または本来の専用 E シリーズ カプセル化の設定を選択できます。LEX カプセル化を設定した場合、ONS 15327 E シリーズ カードは ML シリーズ カードと相互運用できます。E-10/100-4 を EtherSwitch モードに設定した場合、本来の専用 E シリーズ カプセル化に限定されます。ONS 15327 の E シリーズ カードは、16 ビット CRC に限定されます。図 20-6 に、ONS 15327 E シリーズのフレーム化とカプセル化を示します。



(注) E シリーズ カード (ONS 15327 または ONS 15454) のどちらも G シリーズ カードと相互運用できません。

ポートのプロジジョニング手順については、『ONS 15327 Procedure Guide』を参照してください。

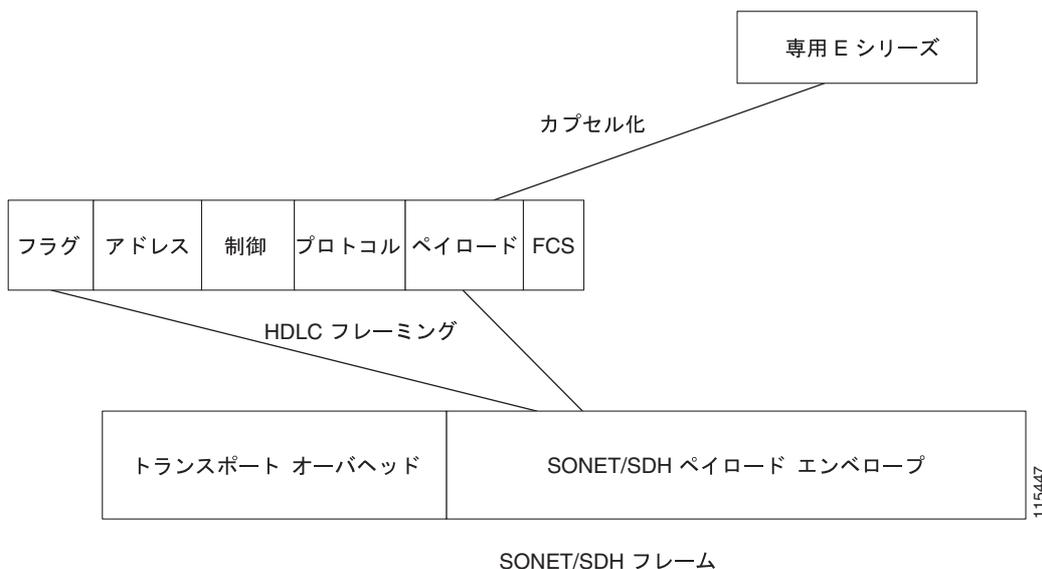
図 20-6 ONS 15327 E シリーズのカプセル化オプションおよびフレーム化オプション



### ONS 15454 および ONS 15454 SDH E シリーズのフレーム化オプションとカプセル化オプション

ONS 15454 や ONS 15454 SDH の E シリーズ カードでは LEX を利用できません。これらのカードは、E シリーズ カード以外のカードとの POS の相互運用を許可しない、本来の専用 E シリーズ カプセル化に限定されます。図 20-7 に、ONS 15454 および ONS 15454 SDH の E シリーズのフレーム化とカプセル化を示します。

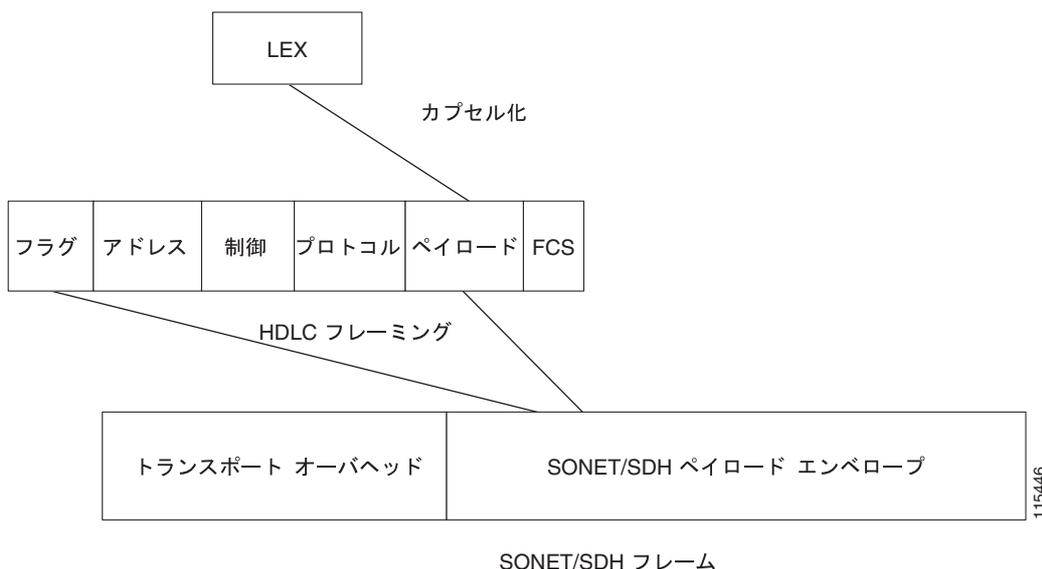
図 20-7 ONS 15454 および ONS 15454 SDH E シリーズのカプセル化オプションおよびフレーム化オプション



## G シリーズのカプセル化およびフレーム化

G シリーズカードは、ONS 15454、ONS 15454 SDH、および ONS 15327 プラットフォームでサポートされています。G シリーズカードは、LEX カプセル化と HDLC フレーム化をサポートします。このカードでは、他の POS フレーミングモードやカプセル化オプションはありません。図 20-8 に、G シリーズのカプセル化とフレーム化を示します。

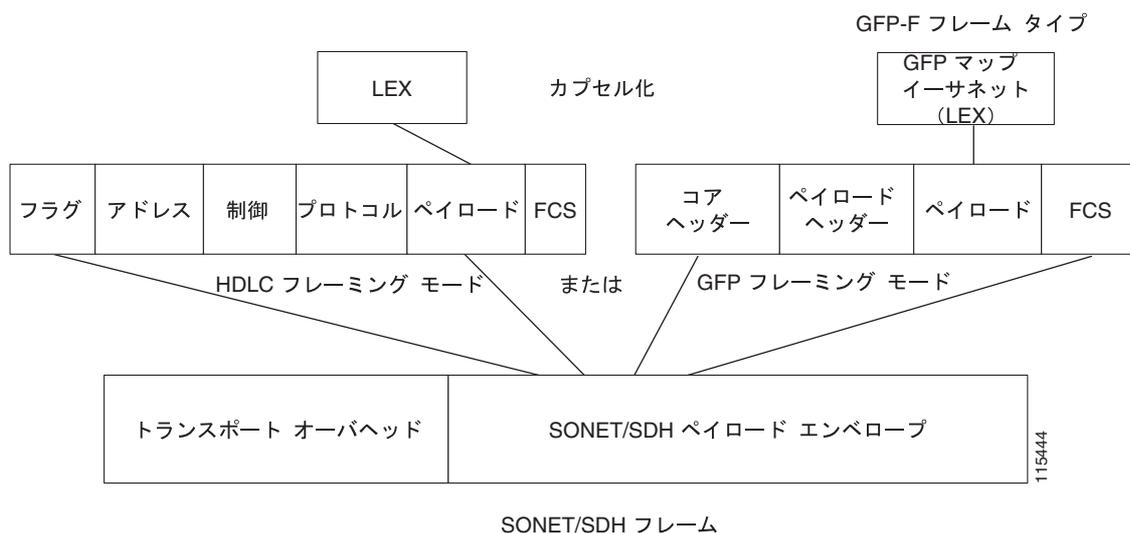
図 20-8 ONS G シリーズのカプセル化オプションおよびフレーム化オプション



## ONS 15454、ONS 15454 SDH、ONS 15310-CL、および ONS 15310-MA CE シリーズ カードのカプセル化とフレーム化

CE-100T-8 カードは、ONS 15454、ONS 15454 SDH、ONS 15310-CL、および ONS 15310-MA プラットフォームで使用できます。CE-1000-4 カードは、ONS 15454 および ONS 15454 SDH プラットフォームで使用できます。このカードは、HDLC フレーミングおよび GFP-F フレーミングをサポートします。GFP-F または HDLC フレーミング モードでは、LEX カプセル化のみがサポートされます。図 20-9 に、CE シリーズのフレーム化とカプセル化を示します。

図 20-9 ONS CE-100T-8 および ONS CE-1000-4 のカプセル化オプションとフレーム化オプション



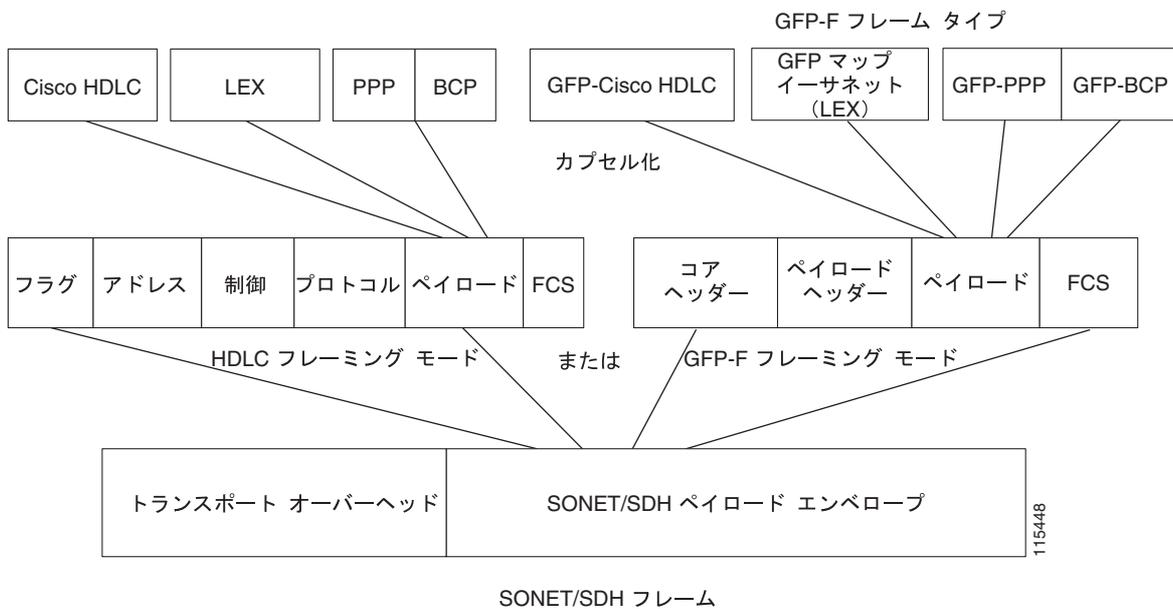
## ONS 15310 ML-100T-8 のカプセル化およびフレーム化

ONS 15310 の ML-100T-8 カードは、HDLC フレーミングおよび GFP-F フレーミングをサポートします。HDLC フレーミング モードでは、LEX がサポートされます。GFP-F フレーミング モードでは、LEX、Cisco HDLC、および PPP/BCP カプセル化がサポートされます。また、LEX カプセル化は、ML シリーズ カードの RPR 用のカプセル化です。RPR では、どちらのフレーミング モードでも LEX カプセル化が必要です。

## ONS 15454 および ONS 15454 SDH ML シリーズ プロトコルのカプセル化およびフレーム化

ONS 15454 および ONS 15454 SDH の ML シリーズ カードは、HDLC フレーミングおよび GFP-F フレーミングをサポートします。HDLC フレーミング モードおよび GFP-F フレーミング モードの両方で、LEX、Cisco HDLC、および PPP/BCP カプセル化がサポートされます。また、LEX カプセル化は、ML シリーズ カードの RPR 用のカプセル化です。RPR では、どちらのフレーミング モードでも LEX カプセル化が必要です。図 20-10 に、ONS 15454 および ONS 15454 SDH のフレーム化オプションおよびカプセル化オプションを示します。

図 20-10 ML シリーズのフレーム化オプションおよびカプセル化オプション



## イーサネットのクロッキングと SONET/SDH のクロッキング

イーサネットのクロッキングは非同期です。IEEE 802.3 のクロック許容値により、ネットワークの一部のリンクでは他のリンクより 200 ppm ( パーツまたはビット /100 万 ) まで遅くなっても構いません ( 0.02% )。あるリンクの回線レートで発生したトラフィック ストリームは、0.02% 遅い他のリンクを経由できます。速いソース クロックまたは遅い中間のクロックにより、エンドツーエンドのスループットがソース リンク レートの 99.98% にしかならない場合があります。

従来、イーサネットは共有メディアで、複数の装置からの結合により集約ポイントで回線レートを上回るような短いバーストを除き、十分に利用されていません。この使用モデルのため、イーサネットの非同期クロッキングが容認されてきました。損失のない TDM 転送に慣れている一部のサービス プロバイダーは、イーサネットが 99.98% のスループットしか保証しないことに驚くかもしれません。

E シリーズ カードを除く、ONS イーサネット カードのクロッキング拡張により、最速対応ソース クロックより最悪でも 50 ppm しか遅くないイーサネット送信レートが保証されます。つまり、最悪の場合でも 50 ppm のクロッキング損失であり、99.995% のスループットが保証されます。多くの場合、カードのクロックは送信元トラフィックのクロックより速いので、回線レートトラフィック転送の損失はゼロになります。実際の結果は、トラフィック ソース トランスミッタのクロック変動によって異なります。



## RMON の設定

この章では、ONS 15454 SONET/SDH の ML シリーズカード上で Remote Network Monitoring (RMON) を設定する方法について説明します。

RMON は、RMON 準拠のコンソールシステムとネットワーク プローブ間で交換可能な一連の統計情報と機能を定義した標準モニタリング仕様です。RMON は総合的なネットワーク障害診断、プランニング、パフォーマンス調整に関する情報を提供します。ML シリーズカードは RMON を特徴としており、Network Management System (NMS; ネットワーク管理システム) と連動するよう設計されています。



(注) この章で使用されるコマンドの構文および使用方法の詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』 Release 12.2 の「System Management Commands」を参照してください。



(注) Cisco IOS を使用して RMON を管理する場合の詳細については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』の「Configuring RMON Support」の章を参照してください。

この章の内容は次のとおりです。

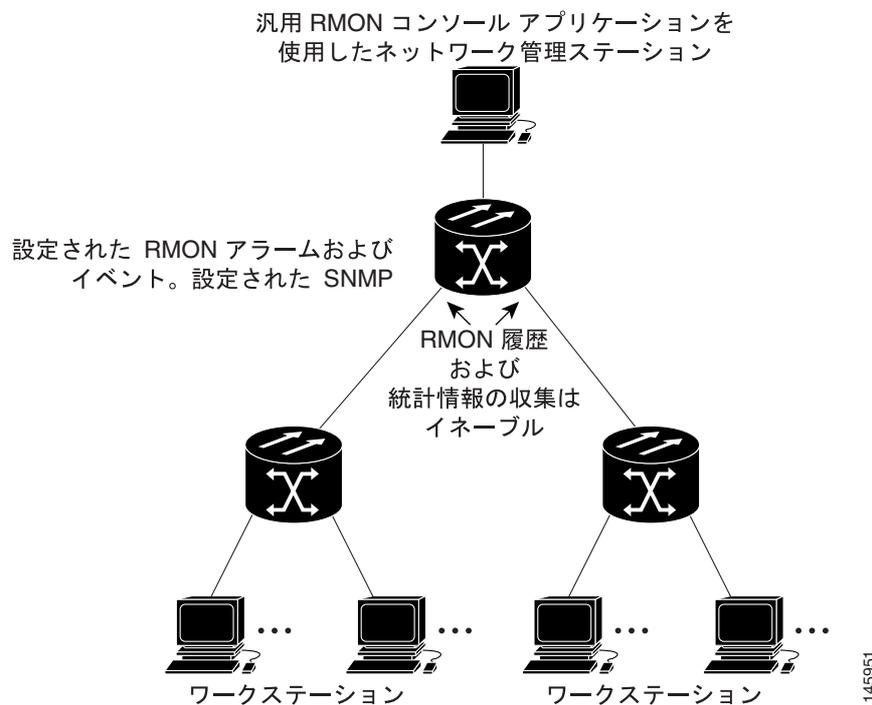
- [RMON の概要 \(p.21-2\)](#)
- [RMON の設定 \(p.21-3\)](#)
- [CRC エラーの ML シリーズカードの RMON の設定 \(p.21-16\)](#)
- [RMON ステータスの表示 \(p.21-21\)](#)

## RMON の概要

RMON は、Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) 標準モニタ仕様で、各種ネットワーク エージェントおよびコンソール システムがネットワーク モニタリング データを交換できるようにします。RMON 機能を SNMP (簡易ネットワーク管理プロトコル) エージェントとともに使用すると、接続されたすべての LAN セグメント上の ML シリーズ カードと他のスイッチ間を流れるトラフィックをモニタリングできます。

ML シリーズ カードによってサポートされる MIB (管理情報ベース) の詳細については、「[サポート対象の MIB](#)」(p.22-6)を参照してください。

図 21-1 RMON の例



## RMON の設定

ここでは、ML シリーズ カードで RMON を設定する方法について説明します。

- [RMON のデフォルト設定 \(p.21-3\)](#)
- [RMON アラームおよびイベントの設定 \(p.21-3\)](#) (必須)
- [インターフェイスでのグループ履歴統計情報の収集 \(p.21-5\)](#) (任意)
- [インターフェイスでのグループイーサネット統計情報の収集 \(p.21-6\)](#) (任意)

### RMON のデフォルト設定

RMON はデフォルトでディセーブルに設定されています。アラームやイベントは設定されていません。

### RMON アラームおよびイベントの設定

CLI (コマンドライン インターフェイス) または SNMP 互換 Network Management Station (NMS; ネットワーク管理ステーション) を使用することにより、ML シリーズ カードを RMON 用に設定できます。NMS 上で汎用 RMON コンソール アプリケーションを使用し、RMON のネットワーク管理機能を利用することを推奨します。また、RMON MIB オブジェクトにアクセスするため、ML シリーズの SNMP を設定する必要があります。SNMP の設定方法の詳細については、[第 22 章「SNMP の設定」](#)を参照してください。

RMON アラームおよびイベントをイネーブルにするには、イネーブル EXEC モードを開始して、次の手順を実行します。この手順は必須です。

	コマンドの説明	目的
ステップ 1	<code>configure terminal</code>	グローバル 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	<code>rmon event number [description string] [log] [owner string] [trap community]</code>	<p>RMON イベント テーブルに RMON イベント番号に対応付けられたイベントを追加します。</p> <ul style="list-style-type: none"> <li>• <i>number</i> には、イベント番号を指定します。指定できる範囲は 1 ~ 65,535 です。</li> <li>• (任意) <i>description string</i> には、イベントの説明を指定します。</li> <li>• (任意) イベントがトリガされたときに RMON ログ エントリを生成するには、<code>log</code> キーワードを使用します。</li> <li>• (任意) <i>owner string</i> には、このイベントの所有者を指定します。</li> <li>• (任意) <i>trap community</i> には、このトラップに使用される SNMP コミュニティ スtring を入力します。</li> </ul>

	コマンドの説明	目的
ステップ 3	<code>rmon alarm number variable interval {absolute   delta} rising-threshold value [event-number] falling-threshold value [event-number] [owner string]</code>	MIB オブジェクトに対してアラームを設定します。 <ul style="list-style-type: none"> <li><code>number</code> には、アラーム番号を指定します。指定できる範囲は 1 ~ 65,535 です。</li> <li><code>variable</code> には、モニタリングする MIB オブジェクトを指定します。</li> <li><code>interval</code> には、アラームが MIB 変数をモニタする時間を秒単位で指定します。範囲は、1 ~ 2,147,483,647 秒です。</li> <li>各 MIB 変数を直接テストするには、<code>absolute</code> キーワードを指定します。MIB 変数のサンプル間の変動をテストする場合は、<code>delta</code> キーワードを指定します。</li> <li><code>value</code> には、アラームをトリガする数値とアラームをリセットする数値を指定します。上限スレッショールドおよび下限スレッショールド値の範囲は、-2,147,483,648 ~ 2,147,483,647 です。</li> <li>(任意) <code>event-number</code> には、上限または下限スレッショールドの限度を超過したときにトリガされるイベント数を指定します。</li> <li>(任意) <code>owner string</code> には、このアラームの所有者を指定します。</li> </ul>
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	エンTRIESを確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエンTRIESを保存します。

アラームをディセーブルにするには、設定したアラームごとに `no rmon alarm number` グローバル コンフィギュレーション コマンドを実行します。特定の番号を指定しないで、設定したアラームをすべてディセーブルにすることはできません。アラームは個別にディセーブルにする必要があります。イベントをディセーブルにするには、`no rmon event number` グローバル コンフィギュレーション コマンドを使用します。アラームおよびイベントとその相互作用の詳細については、Request For Comments (RFC; コメント要求) 1757 を参照してください。

アラームはいずれの MIB オブジェクトに対しても設定できます。次の例では、`rmon alarm` コマンドを使用して RMON アラーム番号 10 を設定します。このアラームは、MIB 変数 `ifEntry.20.1` を 20 秒ごとに 1 回モニタし、アラームがディセーブルになるまで、変数の上昇または下降の変化をチェックします。`ifEntry.20.1` 値が 15 以上の MIB カウンタの増加を示した場合(たとえば 100000 から 100015)、アラームがトリガされます。次にアラームは、イベント番号 1 をトリガします。これは、`rmon event` コマンドで設定されます。設定可能なイベントにはログ エンTRIESまたは SNMP トラップを含めることができます。`ifEntry.20.1` 値が 0 に変化した場合、アラームはリセットされ、再度トリガできます。

```
ML_Series(config)# rmon alarm 10 ifInErrors.65539 20 delta rising 15 1 fall 0
```



(注) この例では、下限スレッショールドが 0 の場合、任意のイベントをトリガしません。

65539 がインターフェイス POS 0 の SNMP ifIndex である場合、SNMP get の付いた特定のポート用に SNMP ifIndex を取得できます。この出力例では、POS0 の SNMP ifIndex は 65539 です。

```
tuvoks-view:128> getmany -v2c 10.92.56.97 tcc@1 ifDescr
ifDescr.65536 = GigabitEthernet0
ifDescr.65537 = GigabitEthernet1
ifDescr.65538 = Null0
ifDescr.65539 = POS0
ifDescr.65540 = POS1
ifDescr.65541 = SPR1
tuvoks-view:129>
```

次の例では、`rmon event` コマンドを使用して RMON イベント番号 1 を作成します。イベントは *High ifOutErrors* として定義され、アラームによってイベントがトリガされるときにログ エントリが生成されます。ユーザ *jjones* は、このコマンドによってイベント テーブルに作成された行を所有します。この例では、イベントがトリガされたときに SNMP トラップも生成されます。

```
ML_Series(config)# rmon event 1 log trap eventtrap description "High ifOutErrors"
owner jjones
```

## インターフェイスでのグループ履歴統計情報の収集

収集情報を表示するには、最初に RMON アラームおよびイベントを設定する必要があります。

インターフェイス上でグループ履歴統計情報を収集するには、イネーブル EXEC モードを開始して、次の手順を実行します。この手順は任意です。

	コマンドの説明	目的
ステップ 1	<code>configure terminal</code>	グローバル 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	<code>interface interface-id</code>	履歴を収集する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。
		 <p>(注) グループ履歴統計情報は、Packet-over-SONET/SDH (POS)(POS_interface) では動作せず、イーサネット インターフェイスでのみ動作します。</p>
ステップ 3	<code>rmon collection history index</code> [buckets bucket-number] [interval seconds] [owner ownername]	<p>指定されたパケット数および時間に関する履歴収集をイネーブルにします。</p> <ul style="list-style-type: none"> <li><i>index</i> には、統計情報の RMON グループを指定します。指定できる範囲は 1 ~ 65,535 です。</li> <li>(任意) <i>buckets bucket-number</i> には、統計情報の RMON 収集履歴グループに対する、最大パケット数を指定します。指定できる範囲は 1 ~ 65,535 です。デフォルトは 50 パケットです。</li> <li>(任意) <i>interval seconds</i> には、各ポーリング サイクルの秒数を指定します。指定できる範囲は 1 ~ 3600 です。デフォルトは 1800 秒です。</li> <li>(任意) <i>owner ownername</i> には、統計情報の RMON グループの所有者名を入力します。</li> </ul>
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	エントリを確認します。

	コマンドの説明	目的
ステップ 6	<code>show rmon history</code>	ML シリーズ カード履歴テーブルの内容を表示します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエントリを保存します。

履歴収集をディセーブルにするには、`no rmon collection history index` 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。

次に、所有者 `root` の RMON 履歴を収集および表示する例を示します。

```
ML_Series(config)# interface gigabitethernet1
ML_Series(config-if)# rmon collection history 2 owner root
ML_Series(config-if)# end
ML_Series# show rmon history
Entry 2 is active, and owned by root
Monitors ifIndex.393217 every 1800 second(s)
Requested # of time intervals, ie buckets, is 50,
```

## インターフェイスでのグループイーサネット統計情報の収集

インターフェイス上でグループイーサネット統計情報を収集するには、イネーブル EXEC モードを開始して、次の手順を実行します。この手順は任意です。

	コマンドの説明	目的
ステップ 1	<code>configure terminal</code>	グローバル 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	<code>interface interface-id</code>	統計情報を収集する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 3	<code>rmon collection stats index [owner ownername]</code>	インターフェイスでの RMON 統計情報収集をイネーブルにします。 <ul style="list-style-type: none"> <li><code>index</code> には、統計情報の RMON グループを指定します。指定できる範囲は 1 ~ 65,535 です。</li> <li>(任意) <code>owner ownername</code> には、統計情報の RMON グループの所有者名を入力します。</li> </ul>
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	エントリを確認します。
ステップ 6	<code>show rmon statistics</code>	ML シリーズ カード統計情報テーブルの内容を表示します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエントリを保存します。

グループイーサネット統計情報の収集をディセーブルにするには、`no rmon collection stats index` 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。

次に、所有者 `root` の RMON 統計情報を収集する例を示します。

```
ML_Series(config)# interface gigabitethernet1
ML_Series(config-if)# rmon collection stats 2 owner root
```

## ML シリーズカードの CRC エラー スレッシュホールドの概要

ML シリーズカードの POS ポートは、signal fail (SF; 信号障害) アラームおよび signal degrade (SD; 信号劣化) アラームを含めた、SONET/SDH 障害および GFP 障害のアラームを報告します。多くの場合、これらのアラームはユーザに対し、POS ポート上で超過 Cyclic Redundancy Check (CRC; 巡回冗長チェック) エラーを発生させる原因ともなる問題を警告します。ただし、超過 CRC エラーが POS ポートで発生しても、リンクには報告されるべき SONET 障害または GFP 障害が存在しないことがあります。このような状況には、リンクの他端の ML シリーズカードから送信されるパケットの CRC エラーまたはビット エラー レートが SF または SD 障害をトリガするには低すぎるが、重大な CRC パケット エラー レートを引き起こすには十分に高いといった例が含まれます。

デフォルトの ML シリーズカードの RPR が実装され、SONET/SDH 障害または GFP 障害が報告されていない状況では、POS インターフェイスは Shared Packet Ring (SPR; 共有パケット リング) インターフェイスのメンバーとしてアップステートのままになります。トラフィックはゆっくり失われ、アラームまたはアクションをトリガしません。

FCS スレッシュホールド設定および検出機能はこの問題を解決します。CRC エラーによるパケット損失のパーセンテージが、設定可能なスレッシュホールドを超過する場合、アラームを発生するよう ML シリーズカードを設定できます。発生したアラームは、CRC Threshold Crossing Alarm (CRC-ALARM; CRC スレッシュホールド超過アラーム) で、アラーム重大度が Major (MA) で、サービスに影響する (SA) SONET/SDH アラームです。報告された SONET/SDH アラームは、CTC の Alarms タブの下に表示されます。

また、ポートのリンク ダウン状態をトリガし、RPR をラップするよう CRC-ALARM を設定することもできます。デフォルトでは、CRC-ALARM はディセーブルです。アラームが設定されているとき、デフォルトではリンク ダウン アクションおよびラップ アクションはディセーブルのままです。この機能も ML シリーズカードのイーサネット ポートでサポートされます。

### 以前のアクションおよびトリガされたアクション

設定可能なスレッシュホールドは、可変フレーム長およびさまざまな帯域幅のパーセンテージによってその有用性が損なわれるので、BER は設定されていません。代わりに、CRC エラー レートをトラフィックのパーセンテージとして使用して、より適切な測度を設定します。トリガするスレッシュホールドは次のとおりです。

- 10e-2 または 1% トラフィック (100 パケットで 1 個の CRC エラー)
- 10e-3 または 0.1% トラフィック (1000 パケットで 1 個の CRC エラー) (デフォルト)
- 10e-4 または 0.01% トラフィック (10000 パケットで 1 個の CRC エラー)

デフォルトのスレッシュホールドは、トラフィックの CRC エラー レート 0.1% です。音声およびビデオトラフィックの場合、エラー レート 1% は通常、Critical な問題で、0.1% は Major な問題です。エラー レートが 0.1% (1000 パケットごとに 1 エラー) を超えると、音声およびビデオはラップをトリガする必要があります。通常のデータトラフィックの場合、エラー レート 10% のトラフィックは Critical な問題で、ただちに解決する必要があります。1% のトラフィックは Minor な問題です。

超過 CRC エラーが検出されたあと、次のアクションが発生します。

1. このオプションが設定されている場合、RPR がラップします。
2. このオプションが設定されている場合、リンクがシャットダウンします。
3. リンクがシャットダウンすると、Path Defect Indication (PDI; パス障害表示) が遠端の ML シリーズカード ポートに送信されます。これにより、リモートエンドがラップします。
4. ローカルエンドの ML シリーズカードに対して、CRC-ALARM が発生します (リモートエンドも超過 CRC エラーを受信している場合、CRC-ALARM が遠端の ML シリーズカード ポートに対して発生します)。

## CRC-ALARM の SONET/GFP 抑制

この超過 CRC エラー検出は、SONET/GFP 障害とは別のものです。1 つの問題により、SONET/GFP 障害と CRC-ALARM の両方が引き起こされる可能性があります。この事例では、CRC エラー スレッシュホールド検出は遅いプロセスなので、CRC-WRAP アラームの前に SONET/GFP 障害が発生します。SONET/GFP 障害によりリンクがダウンする場合、このリンクダウンは CRC-ALARM が検出される前に発生して CRC-ALARM を抑制します。CRC-ALARM を発生させる SONET/GFP 障害がリンクダウン トリガではなく、CRC-ALARM によってリンクダウンするよう設定されている場合、CRC-ALARM はリンクダウンを報告してトリガします。

## CRC-ALARM のクリア

トリガアクションがディセーブルの場合（デフォルト）、一定の時間、エラー レートがスレッシュホールドを下回ると CRC-ALARM は自動的にクリアされます。

トリガアクションがイネーブルの場合、ユーザが手動で CRC-ALARM をクリアする必要があります。アラームによるラップまたはリンクダウンは、トラフィックとポートからのトラフィック内の CRC エラー両方をブロックするので、これが必要になります。CRC エラーがない場合、ファイバの汚れや障害の発生した ML シリーズ カードなどの根本的な問題が存続しても、自動的にクリアされます。この状況では、インターフェイスのフラッピングが発生します。

手動でクリアする前に、CRC-ALARM の根本原因を判別し、解決する必要があります。解決したら、アラームを手動でクリアする方法がいくつかあります。

- Cisco IOS CLI を通じて、EXEC レベルで `clear crc alarm interface interface-type interface-number` コマンドを入力します。
- Cisco IOS CLI を通じて、リンクされたポートで管理上の `shutdown` を行ってから、`no shutdown` を行ってポートをイネーブルにします。
- CTC または TL-1 を通じて、回線をディセーブルにしてから再度イネーブルにします。
- CTC または TL-1 を通じて、SONET/SDH 回線を削除し、同じ送信元と宛先を持った回線を作成します。

## 同期化のラップ解除

ML シリーズ カードのソフトウェアは、エラー フレームを監視する POS インターフェイスで CRC-ALARM アラームを発生させます。単一方向の FCS エラーの場合、ユーザは、CRC-ALARM アラームが発生したスパンの一方の端の POS ポートで `unwrap` コマンドを実行するだけです。双方向の障害の場合、スパンの両端で CRC-ALARM アラームが発生するので、スパンの各端で一度にコマンドを実行する必要があります。

リンクの各端の POS ポートはラップされるので、CRC-ALARM がクリアされたときにラップを削除する（ラップ解除）には、調整が必要です。また、ソフトウェアはラッピングを発生させる他のエラーがないことを確認する必要があります。次の例では、単一方向と双方向両方の障害のこの処理の方法を示します。簡単にするために、この例では、超過 CRC エラーはラッピングを引き起こす唯一の条件であることを前提とします。

## 単一方向エラー

図 21-2 に、ノード E の POS ポート 0 での単一方向の超過 CRC エラーによってラップされた RPR を示します。これは、CRC-ALARM も報告します。これにより、ノード E の POS ポート 1 とノード D の POS ポート 0 がラップします。図のキャプションでは、プロセスをさらに説明します。

図 21-2 単一方向の超過 CRC エラーでラップされた RPR

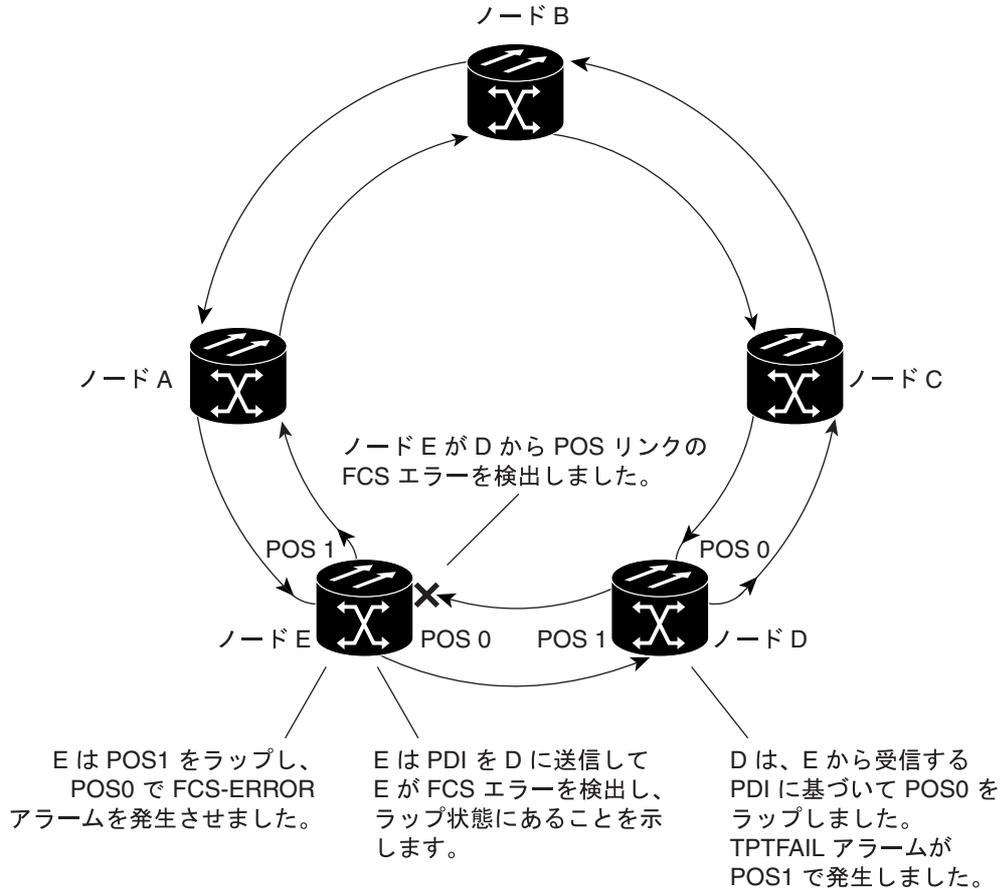
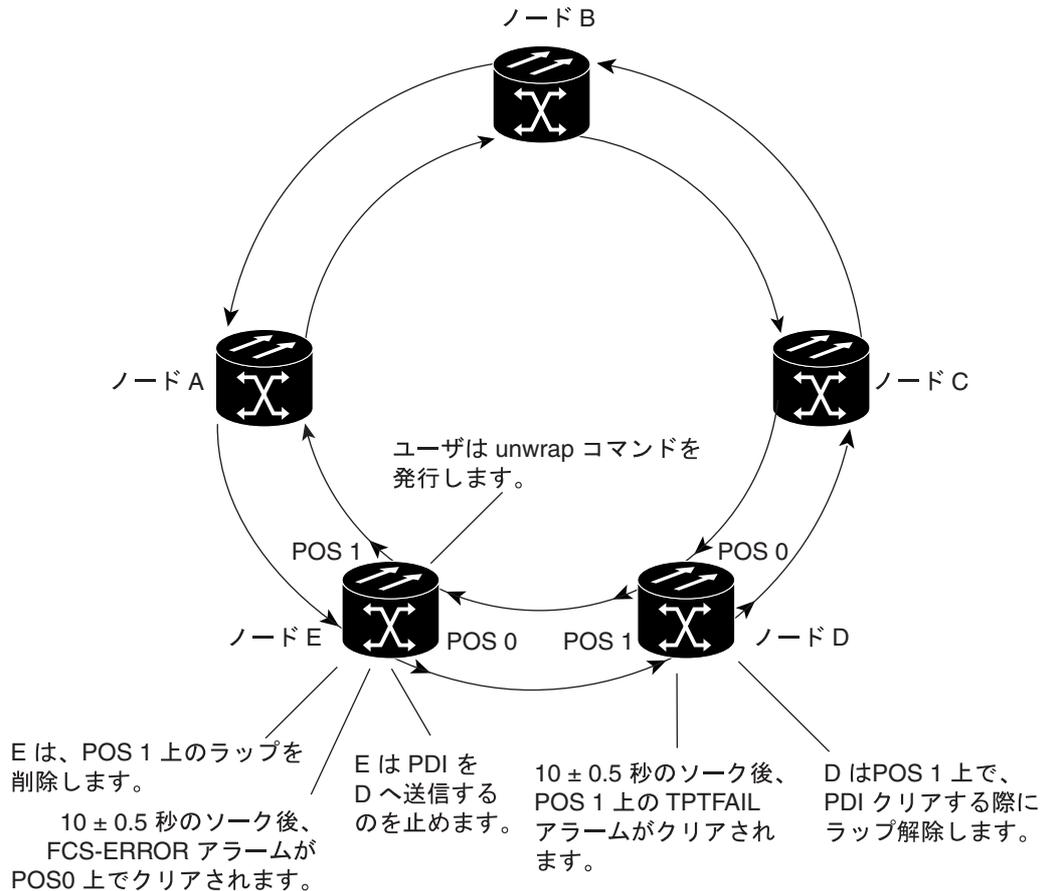


図 21-3 に、図 21-2 のラップ解除シーケンスを示します。ラップ解除のためのトラフィック ヒットは、ノード D でクリアされた PDI を宣言するのに必要なソーク時間に依存します。

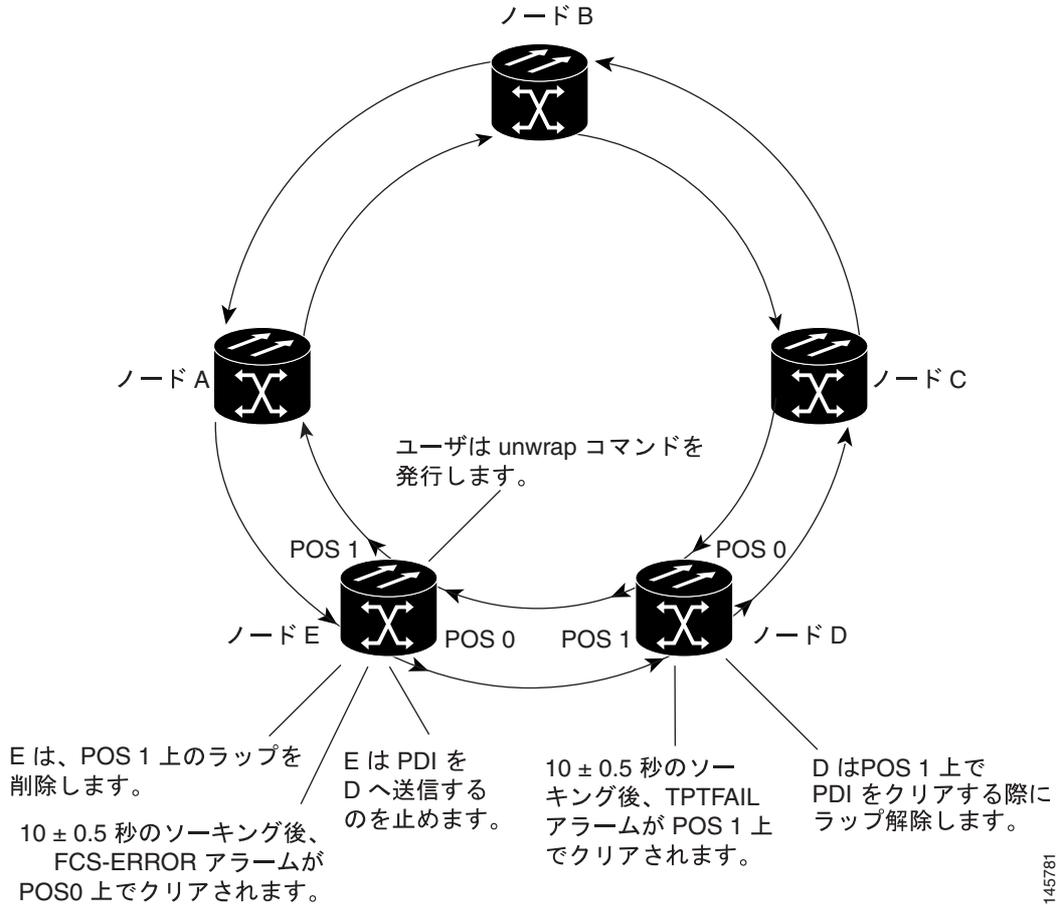
図 21-3 双方向の超過 CRC エラーでラップ解除された RPR



## 双方向エラー

図21-4 に、双方向の超過 CRC エラーでラップされた RPR を示します。両方のポートが CRC-ALARM を報告します。図のキャプションでは、プロセスをさらに説明します。

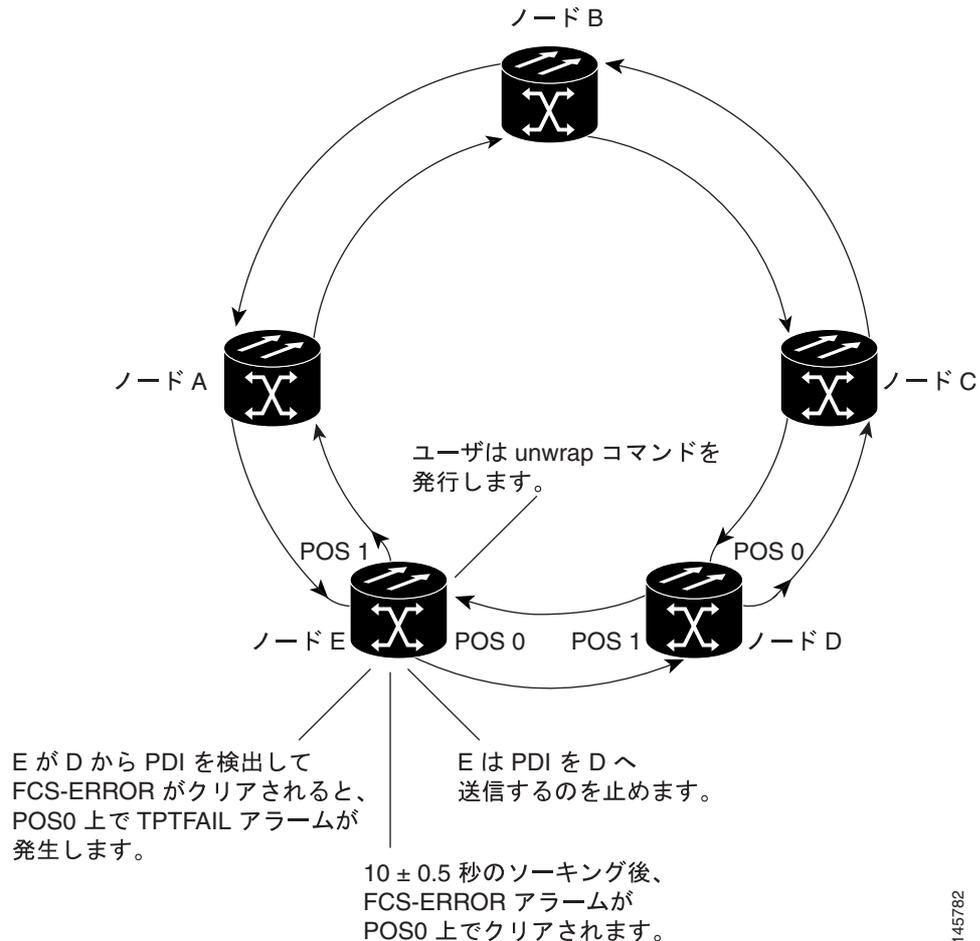
図 21-4 双方向の超過 CRC エラーでラップされた RPR



145781

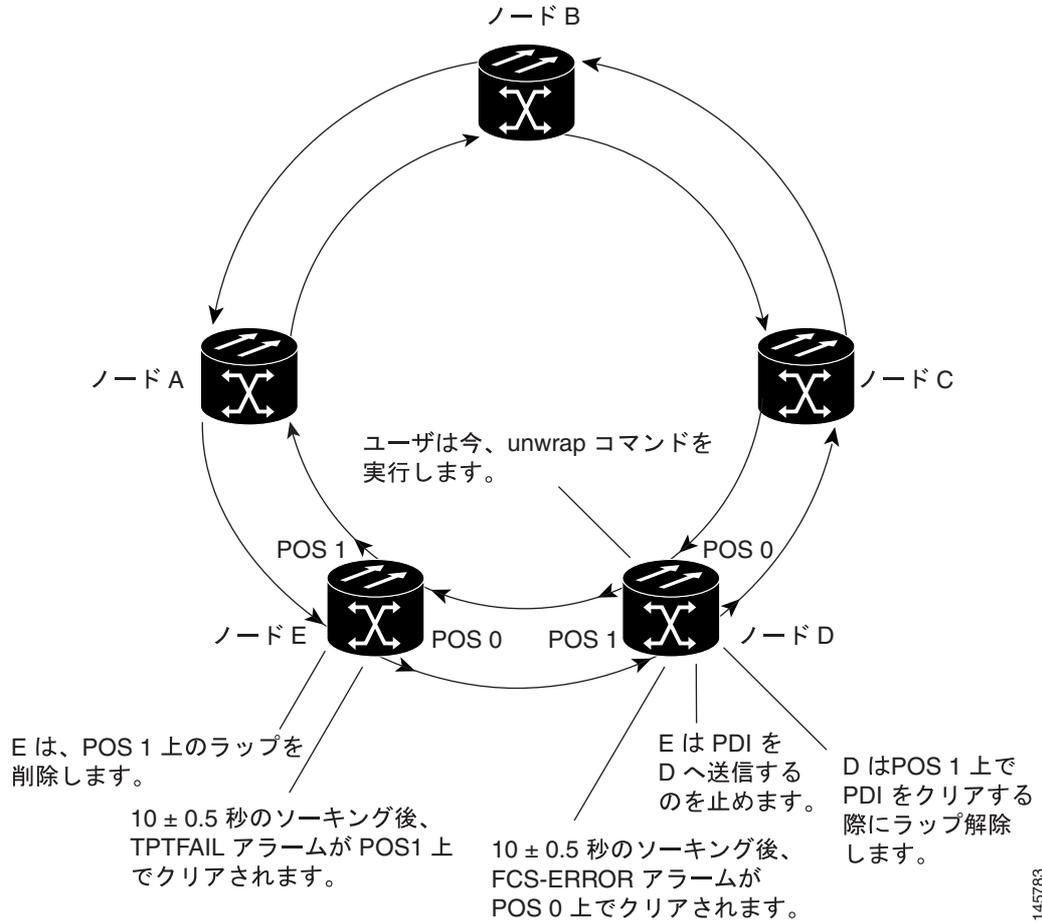
図 21-5 に、図 21-4 のラップ解除シーケンスの最初の部分を示します。ノード E で unwrap コマンドが設定されたあと、ラップ解除が行われます。この双方向事例でのラップ解除の場合、リンクの両端の POS ポートにコマンドを設定する必要があります。

図 21-5 双方向の超過 CRC エラーでラップ解除された RPR の最初の段階



最初の CRC-ALARM クリア コマンドのあと、ノード E は POS ポート 1 をラップ解除しません。ノード D は PDI をノード E に送信し続けるので、CRC-ALARM がクリアされるとノード E は TPTFAIL アラームを発生します。この時点では、RPR は単一方向障害と同様の状態にあります。図 21-5 に示すように、ユーザが 2 回目の unwrap コマンドを実行したらラップ解除は完了です。

図 21-6 双方向の超過 CRC エラーでラップ解除された RPR の第 2 段階



145783

## ML シリーズカードの CRC エラー スレッシュホールドの設定

ML シリーズカードの CRC エラー スレッシュホールドを設定するには、イネーブル EXEC モードを開始して、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	ML_Series# <b>configure terminal</b>	グローバル 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	ML_Series (config)# <b>interface interface-type interface-number</b>	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	ML_Series (config-if)# <b>[no] trigger crc threshold [threshold-value]</b>	<p>fcs エラー レベルを帯域幅のパーセンテージとして設定し、SONET/SDH CRC-ALARM をトリップします。有効な値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 2 10e-2 または 1% トラフィック (100 パケットで 1 CRC エラー)</li> <li>• 3 10e-3 または 0.1% トラフィック (1000 パケットで 1 CRC エラー) (デフォルト)</li> <li>• 4 10e-4 または 0.01% トラフィック (10000 パケットで 1 CRC エラー)</li> </ul> <p>このコマンドの <b>no</b> 形式では、レベルの設定をデフォルトのスレッシュホールド 3 に戻します。</p>
ステップ 4	ML_Series (config-if)# <b>[no] trigger crc action</b>	<p>(任意) 報告するポートに対して、リンクダウンを発生させるよう CRC-ALARM を設定します。RPR POS ポートに対して設定します。これも RPR をラップします。</p> <p>このコマンドの <b>no</b> 形式では、トリガの設定をデフォルトのオフに戻します。</p>
ステップ 5	ML_Series(config-if)# <b>[no] trigger crc delay soak-time</b>	<p>(任意) 超過 CRC エラー検出のソーク時間 (分) を設定します。有効な値は 3 ~ 10 分です。</p> <p>このコマンドの <b>no</b> 形式では、遅延の設定をデフォルトの 1 分に戻します。</p>
ステップ 6	ML_Series# <b>end</b>	イネーブル EXEC モードに戻ります。
ステップ 7	ML_Series# <b>show running-config</b>	エントリを確認します。
ステップ 8	ML_Series# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルにエントリを保存します。

## クリア CRC エラー コマンドを使用した CRC-ALARM ラップの解除

Cisco IOS CLI の `clear crc alarm interface interface-type interface-number` コマンドは、対応する SONET/SDH エラーがなく、FCS エラーによって RPR ラップが発生したときにこれを解除します。SONET/SDH 障害またはキープ アライブ (KA) 障害などの他の原因によるラップの解除は行いません。FCS エラーがなくても SONET/SDH または KA 障害が存在する場合、ソフトウェアはエラーメッセージを出してコマンドを拒否します。FCS エラーが存在し、SONET/SDH または KA 障害が存在する場合、コマンドはソフトウェアによって受け入れられますが、ノードは障害が解決してからのみラップ解除します。この場合、SONET/SDH または KA 障害がクリアされたあと、コマンドを再度実行する必要はありません。



(注) ラップ解除はただちに行われませんが、条件が満たされれば行われます。

ML シリーズカードの CRC-ALARM をクリアするには、イネーブル EXEC モードを開始して、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	ML_Series # <code>clear crc alarm interface interface-type interface-number</code>	SONET/SDH CRC-ALARM をクリアし、条件が満たされれば RPR がラップ解除できるようにします。

## CRC エラーの ML シリーズカードの RMON の設定

ML シリーズカードは、CRC エラーのモニタリングを含め、NMS を使用して SNMP Performance Monitoring (PM) を行うことをサポートします。NMS が、ML シリーズカード インターフェイスすべてのインターフェイス インデックス エラー (ifInErrors) をモニタするために、定期的なポーリングとプログラムされたスレッシュホールド値をサポートする場合、NMS を信頼して CRC エラーを管理およびモニタリングできます。

NMS がポーリングをサポートしない場合、または望ましいポーリング周波数によって使用される帯域幅が多すぎる場合、Cisco IOS CLI を通じて SNMP トラップを ML シリーズカードに設定できます。この方法は、ONS 15454 SONET/SDH の ML シリーズカード専用です。ONS 15310-CL および ONS 15310-MA の ML シリーズカードの RMON 機能は、Cisco Transport Controller (CTC)、Transaction Language One (TL1)、または Cisco Transport Manager (CTM) を介した、ノードを管理する標準的な方法で管理するのが一番です。

### ML シリーズカードの CRC スレッシュホールドの設定の注意事項

NMS PM アラートを生成するインターフェイス CRC エラー (ifInErrors) のスレッシュホールド値を決定するための注意事項です。

- SONET/SDH ビットエラーは POS CRC エラーも作成します。SONET/SDH エラーと POS エラー間にはアラーム抑制階層がないので、各エラー セットは個別のアラートを作成します。
- インターフェイスの実際のパケット レートは、予測不可能です。高帯域幅のインターフェイスでは、低いデータトラフィックが続く特定の時間に、分単位でわずかなパケットのみを転送する可能性があります。これは、比較的少ない CRC エラー数でも 100% の損失であることを意味します。低帯域幅のインターフェイスは、特定の時間に、分単位で高パケット カウント (100 万単位) を転送します。したがって、比較的少ない CRC エラー数の場合には、エラー レート  $10^{-9}$  を意味します。この状況により、非パケットベースの PM にしばしば使用される最大 BER を単純に判別できなくなります。
- モニタリング問題または主要な問題の兆候を示す ML シリーズカードの CRC エラーのモニタリングも設定できます。マイナーな問題のモニタリングの場合、60 秒間に 10 個のエラーなど、比較的速くて影響されやすいエラー レートのトリガを設定します。この方法は、インターフェイスがアップ状態またはダウン状態になるか、ファイバエラーが発生するか、あるいは SONET/SDH 保護イベントが発生する (保護が 50 ms 以内に発生しても) たびに NMS アラートを発生します。主要な問題のみをモニタリングし、アラート数を減らすには、300 秒間に 1000 個のエラーなど比較的高いスレッシュホールドを設定します。

### SNMP を通じた CRC エラーへのアクセス

各インターフェイスの CRC エラーは、IF-MIB オブジェクトの ifInErrors (OID 1.3.6.1.2.1.2.2.1.14) で報告されます。SNMP get 要求により、ifInErrors の現在値を確認できます。各 ML シリーズカードは、SNMP のインスタンスを個別に実行します。SNMP 要求は、コミュニティ スtring に基づいて各 ML シリーズカードにリレーされます。コミュニティ スtring は次の形式を使用します。

```
com_str_configured_from_CTC@ml_slot_number
```

### Cisco IOS を使用した CRC エラー スレッシュホールドの SNMP トラップの設定

ML シリーズカードは、Cisco IOS の RMON トラップ機能をサポートします。Cisco IOS CLI を使用して、ifInErrors をモニタリングし、スレッシュホールドを超過した場合に NMS に対しトラップを生成するよう RMON を設定する必要があります。ONS 15454 SONET/SDH の ML シリーズカードは、SNMP set 要求による RMON トラップの設定をサポートしません。この要求は、一般にネットワーク装置上のアクションを開始します。

ifInErrors をモニタリングし、スレッシュホールドを超過した場合に NMS に対しトラップを生成するよう RMON を設定するには、イネーブル EXEC モードを開始して、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	<code>configure terminal</code>	グローバル 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	<code>rmon event number [log] [trap community] [description string] [owner string]</code>	<p>RMON イベント テーブルに RMON イベント番号に対応付けられたイベントを追加します。</p> <ul style="list-style-type: none"> <li><code>number</code> には、イベント番号を指定します。指定できる範囲は 1 ~ 65535 です。</li> <li>(任意) イベントがトリガされたときに RMON ログ エントリを生成するには、<code>log</code> キーワードを使用します。</li> <li>(任意) <code>trap community</code> には、このトラップに使用される SNMP コミュニティ スtring を入力します。</li> <li>(任意) <code>description string</code> には、イベントの説明を指定します。</li> <li>(任意) <code>owner string</code> には、このイベントの所有者を指定します。</li> </ul>
ステップ 3	<code>rmon alarm number ifInErrors.ifIndex-number interval {absolute   delta} rising-threshold value [event-number] falling-threshold value [event-number] [owner string]</code>	<p>MIB オブジェクトに対してアラームを設定します。</p> <ul style="list-style-type: none"> <li><code>number</code> には、イベント番号を指定します。指定できる範囲は 1 ~ 65535 です。</li> <li><code>ifIndex-number</code> 変数は、10 進表記の ML シリーズカード インターフェイスの <code>ifIndex</code> 番号です(この番号の決定に関する詳細は、「ML シリーズカードの <code>ifIndex</code> 番号の判別」[p.21-18] を参照)。</li> <li><code>interval</code> には、MIB 変数をアラームがモニタする時間を秒単位で指定します。範囲は、1 ~ 4,294,967,295 秒です。</li> <li>各 MIB 変数を直接テストするには、<code>absolute</code> キーワードを指定します。MIB 変数のサンプル間の変動をテストする場合は、<code>delta</code> キーワードを指定します。</li> <li><code>value</code> には、アラームをトリガする数値とアラームをリセットする数値を指定します。上限スレッシュホールドおよび下限スレッシュホールド値の範囲は、-2,147,483,648 ~ 2,147,483,647 です。</li> <li>(任意) <code>event-number</code> には、上限または下限スレッシュホールドの限度を超過したときにトリガされるイベント番号を指定します。</li> <li>(任意) <code>owner string</code> には、このアラームの所有者を指定します。</li> </ul>
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	エントリを確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエントリを保存します。

次に、CRC エラー スレッシュホールドの SNMP トラップを設定する例を示します。

```
ML_Series # configure terminal
ML_Series(config)# rmon event 10 log trap slot15 owner config
ML_Series(config)# rmon alarm 9 ifInErrors.983043 300 delta rising-threshold 1000 10
    falling-threshold 1000 10 owner config
ML_Series(config)# end
ML_Series # show running-config
ML_Series # copy running-config startup-config
```

この例で、`rmon alarm` コマンドに使用される 10 進表記の ML シリーズカード インターフェイスの ifIndex 番号は、`ifInErrors.983043` です。この変数は、ML シリーズカード インターフェイスの ifIndex 番号と組み合わせてモニタリングする MIB オブジェクトです。ML シリーズカード インターフェイスの ifIndex 番号の決定に関する詳細は、「[ML シリーズカードの ifIndex 番号の判別](#)」(p.21-18)を参照してください。

次に、5 分間にスレッシュホールド 1000 を超過する 1002 ifInErrors によって生成された上限スレッシュホールド トラップの例を示します。

```
2005-03-22 16:25:38 ptlm9-454e56-97.cisco.com [10.92.56.97]:
SNMPv2-MIB:sysUpTime.0 = Wrong Type (should be Timeticks): 43026500
SNMPv2-MIB:snmpTrapOID.0 = OID: RMON-MIB:risingAlarm
RFC1271-MIB:alarmIndex.9 = 9
RFC1271-MIB:alarmVariable.9 = OID: IF-MIB:ifInErrors.983043
RFC1271-MIB:alarmSampleType.9 = deltaValue(2)
RFC1271-MIB:alarmValue.9 = 1002
RFC1271-MIB:alarmRisingThreshold.9 = 1000
SNMPv2-SMI:snmpModules.18.1.3.0 = IPAddress: 10.92.56.97
```

## ML シリーズカードの ifIndex 番号の判別

NMS がパフォーマンス データについて ML シリーズカードをポーリングする場合、NMS は内部で ifIndex 番号を使用して、複数の MIB からのインターフェイス データを統合し、このデータとインターフェイス名を関連付けます。インターフェイス名は信頼できるので、実際の ifIndex 番号を知る必要はありません。

Cisco IOS CLI を使用してトラップを直接、生成するよう ML シリーズカードを設定する場合、この関連付けた名前は使用しません。トラップを設定している各インターフェイスの実際の ifIndex 番号を使用する必要があります。実際の ifIndex 番号を決定するには、NMS を使用して各 ML シリーズカード インターフェイスと VLAN (仮想 LAN) サブインターフェイスの ifIndex 番号を取得するか、またはインターフェイスの ifIndex 番号を計算します。

また、MIB ブラウザ (SNMP MIB 定義の検索サービス) を使用して、適切な ifIndex 番号の ifDescr を検証できます。ifDescr からの ifIndex 番号は、希望の ifIndex 番号でなければなりません。

ML シリーズカードでは、イーサネットおよび POS インターフェイスの ifIndex 番号は、次の 2 種類のカードの情報からコンパイルされています。

- カードのシャーシ スロット番号 スロット番号は、ML シリーズカードが常駐するシェルフの物理的なスペースの番号です。ONS 15454 SONET/SDH シェルフの場合、有効な範囲はスロット 1 ~ 6、またはスロット 12 ~ 17 です。この情報は、CTC のシェルフ スロットのグラフ表示、あるいは物理シェルフの前面で見つけることができます。
- カード内のローカル ポート番号 ONS 15454 SONET/SDH の ML シリーズカードのポート番号は、ファストイーサネット インターフェイスおよび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番号と一致します。POS ポート番号はインターフェイス番号と一致せず、イーサネット ポートを連続してナンバリングしません。連続値は、最後のイーサネット ポート番号と最初の POS 番号 (POS ポート 0) の間ではスキップされます。インターフェイスのポート番号を [表 21-1](#) に示します。

表 21-1 ML シリーズカードのインターフェイスのポート番号

ML100T-12 ファストイーサネット インターフェイス	ML100T-12 POS インターフェイス	ML100X-8 ファストイーサネット インターフェイス	ML100X-8 POS インターフェイス	ML1000-2 ギガビットイーサネット インターフェイス	ML1000-2 POS インターフェイス
FE 0 = ポート 0	POS 0 = ポート 13	FE 0 = ポート 0	POS 0 = ポート 9	GE 0 = ポート 0	POS 0 = ポート 3
FE 1 = ポート 1	POS 1 = ポート 14	FE 1 = ポート 1	POS 1 = ポート 10	GE 1 = ポート 1	POS 1 = ポート 4
FE 2 = ポート 2		FE 2 = ポート 2			
FE 3 = ポート 3		FE 3 = ポート 3			
FE 4 = ポート 4		FE 4 = ポート 4			
FE 5 = ポート 5		FE 5 = ポート 5			
FE 6 = ポート 6		FE 6 = ポート 6			
FE 7 = ポート 7		FE 7 = ポート 7			
FE 8 = ポート 8					
FE 9 = ポート 9					
FE 10 = ポート 10					
FE 11 = ポート 11					

次の公式を使用して、スロットおよびポートを組み合わせて ifIndex を出します。

$$\text{ifIndex} = (\text{slot} * 10000\text{h}) + (\text{port})$$

10000h は、16 進数を示し 65536 に相当します。その結果の ifIndex は 16 進数で有意な 2 値数字ですが、10 進数では紛らわしく、明確でない数字です。たとえば、ifIndex E0002h はポート 2 のスロット 14 です。10 進表記での同じ番号は 917506 になります。rmon alarm コマンドは、10 進数表記の ifindex 番号を必要とします。

rmon alarm コマンドを使用して正確な ifindex 値を算出するための参照として、表 21-1 にスロット 1 ~ 17 のベース ifindex 番号を示します。希望のポート番号をスロット ベース番号に足すと正しい ifIndex 番号をすばやく決定できます。

表 21-2 ML シリーズカードのインターフェイスのポート番号

ML シリーズカードの スロット番号	16 進表記のベース ifIndex 番号	10 進表記のベース ifIndex 番号
1	10000h	65536
2	20000h	131072
3	30000h	196608
4	40000h	262144
5	50000h	327680
6	60000h	393216
12	C0000h	786432
13	D0000h	851968
14	E0000h	917504
15	F0000h	983040
16	100000h	1048576
17	110000h	1114112

## ML シリーズカードでの手動による CRC エラー検証

`show interface` コマンドを使用して、インターフェイス上の ML シリーズカードの現在の CRC エラー カウントも検証できます。次に、6 つの総入力エラーの例を示します。これはすべての CRC エラーで、出力の最後の行にあります。

```
ML_Series(config)# show interface pos 0

POS0 is up, line protocol is up
Hardware is Packet/Ethernet over Sonet, address is 0005.9a39.713e (bia 0005.9a39.713e)
MTU 1500 bytes, BW 48384 Kbit, DLY 100 usec,
reliability 255/255, txload 1/255, rxload 182/255
Encapsulation: Cisco-EoS-LEX, crc 32, loopback not set
Keepalive set (10 sec)
Scramble enabled
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: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 34621000 bits/sec, 60083 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
311190527 packets input, 931220183 bytes
Received 0 broadcasts (0 IP multicast)
6 runts, 0 giants, 0 throttles
0 parity
6 input errors, 6 CRC, 0 frame, 0 overrun, 0 ignored
```

## RMON ステータスの表示



(注) RMON ステータス コマンドは、POS インターフェイス用には動作しません。

RMON のステータスを表示するには、表 21-3 に示す 1 つまたは複数のイネーブル EXEC コマンドを使用します。

表 21-3 RMON ステータスの表示用コマンド

コマンドの説明	目的
<code>show rmon</code>	一般的な RMON 統計情報を表示します。
<code>show rmon alarms</code>	RMON アラーム テーブルを表示します。
<code>show rmon events</code>	RMON イベント テーブルを表示します。
<code>show rmon history</code>	RMON 履歴テーブルを表示します。
<code>show rmon statistics</code>	RMON 統計情報テーブルを表示します。

例 21-1 に、表 21-3 のコマンドの例を示します。

### 例 21-1 show rmon コマンドで表示された CRC エラー

```
ML_Series# show rmon alarms

Alarm 9 is active, owned by config
Monitors ifInErrors.983043 every 300 second(s)
Taking delta samples, last value was 0
Rising threshold is 1000, assigned to event 10
Falling threshold is 1000, assigned to event 10
On startup enable rising or falling alarm

ML_Series# show rmon events
Event 10 is active, owned by config
Description is
Event firing causes log and trap to community slot15,
last event fired at 0y3w2d,00:32:39,
Current uptime      0y3w6d,03:03:12
Current log entries:
index  uptime              description
1      0y3w2d,00:32:39
```





## SNMP の設定

---

この章では、ML シリーズ カードと SNMP (簡易ネットワーク管理プロトコル) を連動させるための設定方法について説明します。



(注)

---

この章で使用されている全構文と使用方法の情報については、『*Cisco IOS Configuration Fundamentals Command Reference*』 Release 12.2 を参照してください。

---

この章の内容は次のとおりです。

- [SNMP の概要 \(p.22-2\)](#)
- [SNMP の設定 \(p.22-7\)](#)
- [SNMP ステータスの表示 \(p.22-16\)](#)

## SNMP の概要

SNMP は、マネージャとエージェント間の通信用にメッセージ形式を提供するアプリケーションレイヤ プロトコルです。SNMP システムは、SNMP マネージャ、SNMP エージェント、および MIB で構成されます。SNMP マネージャは、CiscoWorks などの Network Management System (NMS; ネットワーク管理システム) に組み込むことができます。SNMP を設定するには、マネージャとエージェントの間の関係を定義します。

SNMP エージェントには MIB 変数があり、SNMP マネージャはこの変数の値を要求または変更できます。マネージャはエージェントから値を取得したり、エージェントに値を格納したりすることができます。エージェントは、装置のパラメータとネットワーク データの情報リポジトリである MIB からデータを収集します。エージェントは、マネージャのデータ取得またはデータ設定要求に応じることできます。

エージェントはマネージャに、非送信請求トラップを送信できます。トラップは、ネットワークの状態を SNMP マネージャに伝えるメッセージです。トラップは、不正なユーザ認証、再起動、リンク ステータス (アップまたはダウン)、MAC (メディア アクセス制御) アドレス追跡、TCP 接続の終了、ネイバとの接続の切断、または他の重要なイベントを伝えることができます。

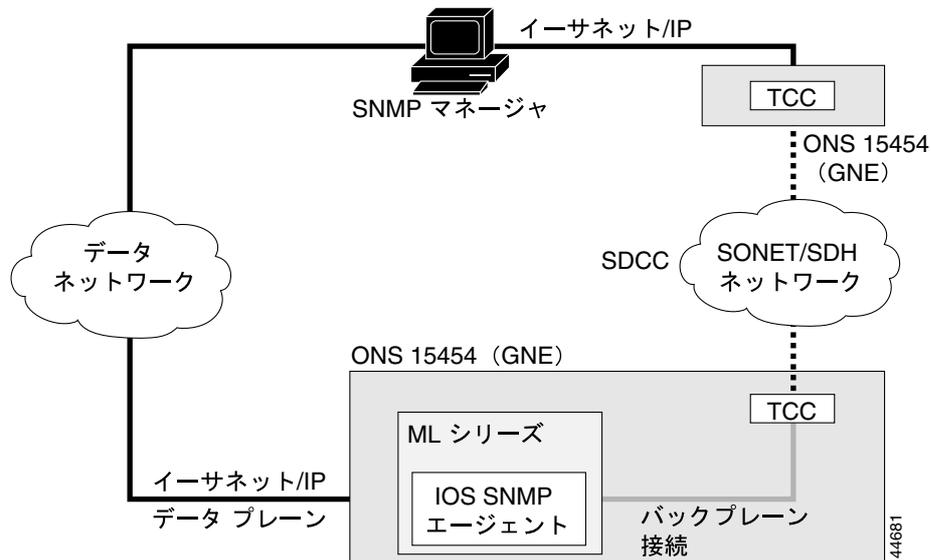
ここでは、次の内容について説明します。

- [ML シリーズ カード上の SNMP \(p.22-3\)](#)
- [SNMP のバージョン \(p.22-3\)](#)
- [SNMP マネージャの機能 \(p.22-4\)](#)
- [SNMP エージェントの機能 \(p.22-4\)](#)
- [SNMP コミュニティ スtring \(p.22-5\)](#)
- [SNMP による MIB 変数へのアクセス \(p.22-5\)](#)
- [サポート対象の MIB \(p.22-6\)](#)
- [SNMP 通知 \(p.22-6\)](#)

## ML シリーズカード上の SNMP

SNMP は、ONS 15454 SONET/SDH ML シリーズ カード上で、2 種類の方法で動作します。1 つは直接通信する方法です。これも、直接通信、Cisco IOS、データ プレーンを使用して、小さな Catalyst スイッチの SNMP が動作する方法です。ML シリーズ カードと連動する SNMP エージェントも ONS 15454 SONET/SDH および SONET ネットワークを経由して通信できます。両方の方法を 図 22-1 に示します。

図 22-1 ML シリーズ カード上の SNMP の例



ONS 15454 SONET/SDH ノードが ML シリーズ カードの SNMP 通信をリレーする場合、ノードはプロキシ エージェントを使用して get 要求、getNext 要求、set 要求を受信および検証し、ML シリーズ カードに転送します。ML シリーズの要求には、ML シリーズ カードの スロット ID が含まれているので、ONS 15454 SONET/SDH ノードへの通常の SNMP 要求と区別できます。ML シリーズ カードからの応答は、ONS 15454 SONET/SDH ノードによって、要求を送信した SNMP エージェントにリレーされます。

SNMP アクセスは、ML シリーズ カードに対し、Cisco IOS データ プレーン イベント、アラーム、統計情報を収集するのに役立ちます。デフォルトでは、ML シリーズ カードで定義された SNMP イベントおよびトラップはすべて TCC2/TCC2P カードの SNMP エージェントに報告されます。TCC2/TCC2P カードの SNMP エージェントがアクティブの場合、このイベントが定義済みの SNMP サーバに送信されます。

## SNMP のバージョン

ML シリーズ カードと ONS 15454 SONET/SDH ノードは両方とも SNMP バージョン 1 (SNMPv1) と SNMP バージョン 2c (SNMPv2c) をサポートします。定義は次のとおりです。

- SNMPv1 Request For Comments (RFC; コメント要求) 1157 で定義されている、SNMP の完全インターネット標準規格
- SNMPv2c では、SNMPv2 classic のパーティベース管理およびセキュリティ フレームワークが SNMPv2C のコミュニティストリングベース管理フレームワークに変わりましたが、SNMPv2classic のバルク検索機能と改良されたエラー処理機能は残されています。バルク検索

メカニズムは、テーブルや大量の情報を検索し、必要な往復回数を削減します。SNMPv2c ではエラー処理機能が改善され、さまざまなエラー状態を区別するための拡張エラーコードが使用されています。これらのエラー状態は、SNMPv1 の単一のエラーコードで報告されます。SNMPv2c のエラーリターンコードはエラータイプを報告します。

SNMPv1 および SNMPv2C は、次の同じセキュリティモデルとレベルを使用します。

- レベル noAuthNoPriv
- 認証 コミュニティストリング
- 暗号化 なし
- 結果 認証用コミュニティストリングの一致を使用

管理ステーションによってサポートされる SNMP バージョンを使用するように、SNMP エージェントを設定する必要があります。エージェントは複数のマネージャと通信できるので、SNMPv1 プロトコルと SNMPv2 プロトコルを使用する通信をサポートするようソフトウェアを設定できます。

## SNMP マネージャの機能

SNMP マネージャは MIB の情報を使用して、表 22-1 に示す動作を実行します。

表 22-1 SNMP の動作

動作	説明
get-request	特定の変数から値を取得します。
get-next-request	テーブル内の変数から値を取得します。 <sup>1</sup>
get-bulk-request <sup>2</sup>	テーブルの複数の行など、通常はサイズの小さい多数のデータブロックに分割して送信する必要のある大きなデータブロックを取得します。
get-response	NMS から送信された get-request、get-next-request、set-request に応答します。
set-request	特定の変数に値を格納します。
trap	あるイベントが発生したときに、SNMP エージェントから SNMP マネージャに送信される非送信請求メッセージ

1. この動作の場合、SNMP マネージャは正確な変数名を知る必要はありません。順番に検索を実行し、テーブルの中から必要な変数を見つけます。
2. get-bulk-request コマンドは、SNMPv2 以降でのみ動作します。

## SNMP エージェントの機能

SNMP エージェントは、次の SNMP マネージャの要求に応答します。

- MIB 変数の取得 SNMP エージェントは NMS からの要求に応答して、この機能を開始します。エージェントは要求された MIB 変数の値を取得し、その値を使用して NMS に応答します。
- MIB 変数の設定 SNMP エージェントは NMS からのメッセージに応答して、この機能を開始します。SNMP エージェントは、MIB 変数の値を NMS から要求された値に変更します。

SNMP エージェントは、エージェントで重要なイベントが発生したことを NMS に通知するために、非送信請求トラップメッセージも送信します。トラップ条件の例には、ポートまたはモジュールがアップまたはダウン状態になった場合、スパンニングツリー トポロジーマネージャが変更された場合、認証エラーが発生した場合などが含まれます。

## SNMP コミュニティ ストリング

SNMP コミュニティ ストリングは、MIB オブジェクトに対するアクセスを認証し、組み込みパスワードとして機能します。NMS が ML シリーズ カードにアクセスするには、NMS 上のコミュニティ ストリング定義が ML シリーズ カード上の 3 つのコミュニティ ストリング定義の少なくとも 1 つと一致しなければなりません。

コミュニティ ストリングの属性は、次の 3 つのうちのいずれかです。

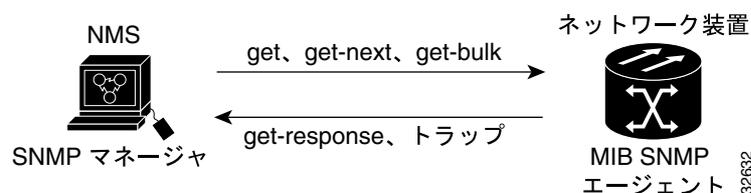
- read-only (RO) 許可した管理ステーションに、コミュニティ ストリングを除く MIB 内のオブジェクトすべてに対する読み取りアクセス権を与えます。ただし、書き込みアクセスは許可しません。
- read-write (RW) 許可した管理ステーションに、MIB 内のオブジェクトすべてに対する読み取りおよび書き込みアクセス権を与えます。ただし、コミュニティ ストリングへのアクセスは許可しません。
- read-write-all 許可した管理ステーションに、コミュニティ ストリングも含めた MIB 内のオブジェクトすべてに対する読み取りおよび書き込みアクセス権を与えます。

## SNMP による MIB 変数へのアクセス

NMS の例として、CiscoWorks ネットワーク管理ソフトウェアがあります。CiscoWorks ソフトウェアは、ML シリーズ カードの MIB 変数を使用して、装置の変数を設定し、ネットワーク上の装置をポーリングして特定の情報を入手します。ポーリング結果はグラフとして表示されます。この結果を分析して、問題のトラブルシューティング、ネットワーク パフォーマンスの改善、装置の設定の確認、トラフィック負荷のモデルなどを行うことができます。

図 22-2 に示すように、SNMP エージェントは MIB からデータを収集します。エージェントは SNMP マネージャに対し、トラップまたは特定イベントの通知を送信します。SNMP マネージャはトラップを受信して処理します。トラップは、ネットワーク上で発生した不正なユーザ認証、再起動、リンク ステータス(アップまたはダウン)、MAC アドレス追跡などに関する状態を SNMP マネージャに通知します。SNMP エージェントはさらに、get-request、get-next-request、set-request 形式で SNMP マネージャから送信される MIB 関連のクエリに応答します。

図 22-2 SNMP ネットワーク



## サポート対象の MIB

サポート対象となる ML シリーズ カードの MIB の完全リストは、使用している ONS ソフトウェア CD の MIBsREADME.txt ファイルにあります。このソフトウェア CD には、必要な MIB モジュールと MIB のロードに関する情報も含まれます。

サポート対象となる重要な MIB には次が含まれます。

- Bridge-MIB (RFC 1493) からの Spanning Tree Protocol (STP) のトラップ
- RFC 1157 の認証トラップ
- IF-MIB (RFC 1573) からのイーサネット ポート用リンクアップ トラップとリンクダウン トラップ
- CISCO-PORT-QOS-MIB 拡張による Quality of Service (QoS; サービス品質) 統計のエクスポート



(注)

ML シリーズ カードの CISCO-PORT-QOS-MIB 拡張では、Class of Service (CoS; サービス クラス) ベースの QoS 指標がサポートされています。設定オブジェクトは、サポートされません。

## SNMP 通知

SNMP を使用すると、ML シリーズ カードは特定のイベントが発生したときに SNMP マネージャに通知を送信できます。SNMP 通知はトラップまたはインフォーム要求として送信できます。コマンド構文内に、トラップ要求またはインフォーム要求を選択するコマンド オプションが指定されていない場合、キーワード *traps* はトラップ要求、インフォーム要求、またはその両方を表します。SNMP 通知をトラップ要求またはインフォーム要求のどちらで送信するかを指定するには、`snmp-server host` コマンドを使用します。



(注)

SNMPv1 はインフォーム要求をサポートしていません。

レシーバはトラップの受信時に確認応答を送信しないため、トラップは信頼性が低く、送信側はトラップが受信されたかどうかを判別できません。SNMP マネージャはインフォーム要求を受信すると、SNMP 応答 Protocol Data Unit (PDU; プロトコル データ ユニット) を使用してメッセージを確認します。送信側が応答を受信しない場合は、インフォーム要求が再送信されます。このため、インフォーム要求の方がトラップよりも目的の宛先に到達する可能性が高くなります。

インフォームはトラップよりも信頼性が高いため、ML シリーズ カードおよびネットワーク内のリソースの消費量も多くなります。送信後すぐに廃棄されるトラップとは異なり、インフォーム要求は応答を受信するか、または要求が時間切れになるまでメモリ内に保持されます。トラップの送信は 1 回限りですが、インフォームは何回も再送信されたり、再試行されることがあります。再試行が繰り返されるとトラフィックが増加し、ネットワークのオーバーヘッドが大きくなります。したがって、トラップおよびインフォームを使用する場合は信頼性とリソースのどちらを重視するかの選択が必要となります。SNMP マネージャですべての通知を受信することが重要な場合はインフォーム要求を使用します。ネットワークのトラフィックまたは ML シリーズ カードのメモリが重要で、通知が必要ない場合は、トラップを使用します。

## SNMP の設定

ここでは、ML シリーズ カードに SNMP を設定する方法について説明します。以下の設定情報について説明します。

- [SNMP のデフォルト設定 \(p.22-7\)](#)
- [SNMP 設定時の注意事項 \(p.22-7\)](#)
- [SNMP エージェントのディセーブル化 \(p.22-8\)](#)
- [コミュニティ スtring の設定 \(p.22-8\)](#)
- [SNMP グループおよびユーザの設定 \(p.22-10\)](#)
- [SNMP 通知の設定 \(p.22-11\)](#)
- [エージェント コンタクトおよびロケーション情報の設定 \(p.22-14\)](#)
- [SNMP 経由で使用する TFTP サーバの制限 \(p.22-14\)](#)
- [SNMP の例 \(p.22-15\)](#)

## SNMP のデフォルト設定

表 22-2 にデフォルトの SNMP 設定を示します。

表 22-2 SNMP のデフォルト設定

機能	デフォルト設定
SNMP エージェント	イネーブル
SNMP コミュニティ スtring	read-only : パブリック read-write : プライベート read-write-all : シークレット
SNMP トラップ レシーバ	設定なし
SNMP トラップ	TCP 接続のトラップ (tty) 以外はディセーブル
SNMP バージョン	version キーワードを指定しない場合、デフォルトはバージョン 1 です。
SNMP 通知タイプ	タイプを指定しない場合、すべての通知が送信されます。

## SNMP 設定時の注意事項

SNMP を設定する場合、以下の注意事項に従ってください。

- SNMP グループを設定する場合は、通知ビューを指定しないでください。snmp-server host グローバル コンフィギュレーション コマンドを使用すると、ユーザ用の通知ビューを自動生成し、そのユーザに関連付けられたグループにビューを追加します。グループの通知ビューを変更すると、そのグループに関連付けられたすべてのユーザに影響を与えます。通知ビューを設定する場合については、『Cisco IOS Configuration Fundamentals Command Reference』Release 12.2 を参照してください。
- SNMP グループは、SNMP ユーザを SNMP ビューにマッピングするテーブルです。
- SNMP ユーザは、SNMP グループのメンバーです。
- SNMP ホストは、SNMP トラップ動作の受信側です。
- SNMP エンジン ID は、ローカルまたはリモート SNMP エンジンの名前です。

## SNMP エージェントのディセーブル化

SNMP エージェントをディセーブルするには、イネーブル EXEC モードを開始して、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	<code>configure terminal</code>	グローバル 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	<code>no snmp-server</code>	SNMP エージェントの動作をディセーブルにします。
ステップ 3	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 4	<code>show running-config</code>	エントリを確認します。
ステップ 5	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエントリを保存します。

`no snmp-server` グローバル コンフィギュレーション コマンドは、装置上で実行されているすべてのバージョンをディセーブルにします。SNMP をイネーブルにする特定の IOS コマンドはありません。最初に入力する `snmp-server` グローバル コンフィギュレーション コマンドによって、SNMP のすべてのバージョンがイネーブルになります。

## コミュニティ スtring の設定

SNMP マネージャとエージェント間の関係を定義するには、SNMP コミュニティ スtring を使用します。コミュニティ スtring はパスワードと同様に機能し、ML シリーズカードのエージェントへのアクセスを許可します。任意で、文字列に関連付けられた次の特性を 1 つまたは複数指定できます。

- コミュニティ スtring を使用してエージェントにアクセスできる SNMP マネージャの IP アドレスを指定したアクセス リスト
- 特定のコミュニティにアクセス可能な、すべての MIB オブジェクトのサブセットを定義した MIB ビュー
- コミュニティがアクセスできる MIB オブジェクトに対応する読み書きアクセス許可または読み取り専用アクセス許可

ML シリーズカード上でコミュニティ スtring を設定するには、イネーブル EXEC モードを開始して、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	<code>configure terminal</code>	グローバル 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	<code>snmp-server community string [view view-name] [ro   rw] [access-list-number]</code>	<p>コミュニティ スtring を設定します。</p> <ul style="list-style-type: none"> <li><code>string</code> には、パスワードのように機能し、SNMP プロトコルへのアクセスを許可する文字列を指定します。任意の長さのコミュニティ スtring を 1 つまたは複数設定できます。</li> <li>(任意) <code>view view-name</code> には、コミュニティ がアクセスできるビュー レコードを指定します。</li> <li>(任意) 許可された管理ステーションで MIB オブジェクトを取得する場合、読み取り専用 (<code>ro</code>) を指定します。または、許可された管理ステーションで MIB オブジェクトを取得および変更する場合、読み書き (<code>rw</code>) を指定します。デフォルトでは、コミュニティ スtring のアクセス権は、すべてのオブジェクトに対して読み取り専用になっています。</li> <li>(任意) <code>access-list-number</code> には、1 ~ 99 および 1300 ~ 1999 の範囲で標準の IP アクセス リスト番号を入力します。</li> </ul>
ステップ 3	<code>access-list access-list-number {deny   permit} source [source-wildcard]</code>	<p>(任意) ステップ 2 で標準の IP アクセス リスト番号を指定した場合は、リストを作成し、必要な回数だけこのコマンドを繰り返します。</p> <ul style="list-style-type: none"> <li><code>access-list-number</code> には、ステップ 2 で指定したアクセス リスト番号を入力します。</li> <li><code>deny</code> キーワードを指定すると、条件が一致した場合にアクセスが拒否されます。<code>permit</code> キーワードを指定すると、条件が一致した場合にアクセスが許可されます。</li> <li><code>source</code> には、コミュニティ スtring を使用してエージェントにアクセスできる SNMP マネージャの IP アドレスを指定します。</li> <li>(任意) <code>source-wildcard</code> には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を配置します。</li> </ul> <p>アクセス リストは必ず、すべてに対し、暗黙的な拒否ステートメントで終了することに注意してください。</p>
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	エントリを確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエントリを保存します。



(注)

SNMP コミュニティのアクセスをディセーブルにするには、そのコミュニティに対するコミュニティ スtring をヌル スtring に設定します (コミュニティ スtring に値を入力しないでください)。

特定のコミュニティ スtring を削除するには、`no snmp-server community string` グローバル コンフィギュレーション コマンドを使用します。

次に、SNMP に `comaccess` という文字列を割り当て、読み取り専用アクセスを許可し、IP アクセスリスト 4 がコミュニティ スtring を使用して ML シリーズ カードの SNMP エージェントにアクセスするよう指定する方法を示します。

```
ML_Series(config)# snmp-server community comaccess ro 4
```

## SNMP グループおよびユーザの設定

ML シリーズ カード上のローカルまたはリモート SNMP サーバ エンジンに、識別名 (エンジン ID) を指定できます。SNMP ユーザを SNMP ビューにマッピングする SNMP サーバグループを設定し、SNMP グループに新規ユーザを追加できます。

ML シリーズ カード上で SNMP を設定するには、イネーブル EXEC モードを開始して、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	<code>configure terminal</code>	グローバル 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	<code>snmp-server engineID {local <i>engineid-string</i>   remote <i>ip-address</i> [<i>udp-port port-number</i>]}</code>	SNMP のローカル コピーまたはリモート コピーのいずれかの名前を設定します。 <ul style="list-style-type: none"> <li><code>engineid-string</code> は、SNMP のコピー名を含む 24 文字の ID スtring です。</li> <li><code>remote</code> を選択した場合、SNMP のリモート コピーが格納された装置の <code>ip-address</code>、およびリモート装置上の任意の UDP ポートを指定します。UDP ポートのデフォルト値は 162 です。</li> </ul>
ステップ 3	<code>snmp-server group <i>groupname</i> {v1   v2c [<i>auth</i>   <i>noauth</i>   <i>priv</i>]} [<i>read readview</i>] [<i>write writeview</i>] [<i>notify notifyview</i>] [<i>access access-list</i>]</code>	リモート装置に新規の SNMP グループを設定します。 <ul style="list-style-type: none"> <li><code>groupname</code> には、グループ名を指定します。</li> <li>セキュリティ モデルを指定します。 <ul style="list-style-type: none"> <li><code>v1</code> は、安全性が低いセキュリティ モデルです。</li> <li><code>v2c</code> は、安全性が高いセキュリティ モデルです。このモデルを使用すると、インフォーム要求および整数を標準の 2 倍の幅で伝送できます。</li> </ul> </li> </ul> <p> (注) <code>priv</code> キーワードは、暗号ソフトウェア イメージがインストールされている場合のみ使用できます。</p> <ul style="list-style-type: none"> <li>(任意) <code>read readview</code> には、エージェント内容のみを表示できるビューの名前を示す文字列 (64 文字以下) を指定して、入力します。</li> <li>(任意) <code>write writeview</code> には、データを入力してエージェント内容を設定できるビューの名前を示す文字列 (64 文字以下) を指定して、入力します。</li> <li>(任意) <code>notify notifyview</code> には、通知、インフォーム要求、またはトラップを指定できるビューの名前を示す文字列 (64 文字以下) を指定して、入力します。</li> <li>(任意) <code>access access-list</code> には、アクセス リストの名前を示す文字列 (64 文字以下) を指定して、入力します。</li> </ul>

	コマンドの説明	目的
ステップ 4	<code>snmp-server user username groupname [remote host [udp-port port]] {v1   v2c [access access-list]}</code>	SNMP グループに新規ユーザを設定します。 <ul style="list-style-type: none"> <li><code>username</code> は、エージェントに接続されたホスト上のユーザ名です。</li> <li><code>groupname</code> は、ユーザが関連付けられているグループの名前です。</li> <li>(任意)ユーザが属するリモート SNMP エンティティを指定するには、<code>remote</code> を入力します。このエンティティのホスト名または IP アドレスを指定し、さらに任意で UDP ポート番号を指定します。UDP ポートのデフォルト値は 162 です。</li> <li>SNMP バージョン番号 (<code>v1</code> または <code>v2c</code>) を入力します。</li> <li>(任意) <code>access access-list</code> には、アクセスリストの名前を示す文字列 (64 文字以下) を指定して、入力します。</li> </ul>
ステップ 5	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 6	<code>show running-config</code>	エントリを確認します。
ステップ 7	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエントリを保存します。

## SNMP 通知の設定

トラップ マネージャは、通知タイプ (トラップ) を受信して処理する管理ステーションです。トラップは、特定のイベントが発生した場合に、ML シリーズ カードが生成するシステム アラートです。デフォルトではトラップ マネージャが定義されていないため、トラップは送信されません。すべてのトラップをイネーブルにするには、通知タイプ キーワードを指定しないで、`snmp-server enable traps` コマンドを設定します。

表 22-3 に、一般的によく使用され、ML シリーズ カードによってサポートされるトラップの一部を示します。これらのトラップの一部またはすべてをイネーブルにし、トラップ マネージャがトラップを受信するように設定できます。

表 22-3 ML シリーズ カードの通知タイプ

通知タイプのキーワード	説明
<code>bridge</code>	STP ブリッジ MIB トラップを生成します。
<code>config</code>	SNMP 設定の変更時にトラップを生成します。
<code>config-copy</code>	SNMP コピー設定の変更時にトラップを生成します。
<code>entity</code>	SNMP エンティティ トラップを生成します。
<code>rsvp</code>	RSVP フロー変更トラップを生成します。
<code>rtr</code>	SNMP Response Time Reporter (RTR) に対してトラップを生成します。

表 22-3 に示す通知タイプを特定のホストに受信させるには、`snmp-server host` グローバル コンフィギュレーション コマンドをそのホストに対して実行します。

ホストにトラップまたはインフォーム要求を送信するように ML シリーズ カードを設定するには、イネーブル EXEC モードを開始して、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	<code>configure terminal</code>	グローバル 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	<code>snmp-server engineID remote ip-address engineid-string</code>	リモート ホストの IP アドレスおよびエンジン ID を指定します。
ステップ 3	<code>snmp-server user username groupname remote host [udp-port port] {v1   v2c}[access access-list]</code>	<p>ステップ 2 で作成したリモート ホストに関連付けるよう SNMP ユーザを設定します。</p> <ul style="list-style-type: none"> <li><code>username</code> は、エージェントに接続されたホスト上のユーザ名です。</li> <li><code>groupname</code> は、ユーザが関連付けられているグループの名前です。</li> <li>(任意)ユーザが属するリモート SNMP エンティティを指定するには、<code>remote</code> を入力します。このエンティティのホスト名または IP アドレスを指定し、さらに任意で UDP ポート番号を指定します。UDP ポートのデフォルト値は 162 です。</li> <li>SNMP バージョン番号 (<code>v1</code> または <code>v2c</code>) を入力します。</li> <li>(任意) <code>access access-list</code> には、アクセス リストの名前を示す文字列 (64 文字以下) を指定して、入力します。</li> </ul> <p> (注) 最初にリモート ホストのエンジン ID を設定しないと、アドレスに対してリモート ユーザを設定できません。リモート エンジン ID を設定する前にユーザを設定しようとすると、エラー メッセージが表示され、コマンドは実行されません。</p>
ステップ 4	<code>snmp-server host host-addr [traps   informs] [version {1   2c}] community-string [udp-port port] [notification-type]</code>	<p>SNMP トラップ動作の受信側を指定します。</p> <ul style="list-style-type: none"> <li><code>host-addr</code> には、ホスト (対象となる受信側) の名前またはインターネット アドレスを指定します。</li> <li>(任意)SNMP トラップをホストに送信するには、<code>traps</code> (デフォルト) を入力します。</li> <li>(任意)SNMP インフォーム要求をホストに送信するには、<code>informs</code> を入力します。</li> <li>(任意) SNMP バージョン (1 または 2c) を指定します。SNMPv1 はインフォーム要求をサポートしていません。</li> <li><code>community-string</code> には、通知動作によって送信されたパスワードと同様のコミュニティ スtring を入力します。</li> <li>(任意) <code>udp-port port</code> には、リモート装置の UDP ポートを入力します。</li> <li>(任意)<code>notification-type</code> には、表 22-3 に示すキーワードを使用します。タイプを指定しない場合、すべての通知が送信されます。</li> </ul>

	コマンドの説明	目的
ステップ 5	<code>snmp-server enable traps notification-types</code>	<p>トラップまたはインフォーム要求を送信するよう ML シリーズカードをイネーブルにし、送信する通知タイプを指定します。通知タイプのリストについては、次を入力します。</p> <p><code>snmp-server enable traps ?</code></p> <p>複数のトラップタイプをイネーブルにするには、トラップタイプごとに <code>snmp-server enable traps</code> コマンドを個別に入力する必要があります。</p>
ステップ 6	<code>snmp-server trap-source interface-id</code>	(任意) 送信元インターフェイスを指定します。これにより、トラップメッセージ用の IP アドレスが設定されます。このコマンドにより、インフォーム要求用の送信元 IP アドレスも設定されます。
ステップ 7	<code>snmp-server queue-length length</code>	(任意) 各トラップホストが保持できるトラップメッセージ数 (メッセージキュー長) を設定します。指定できる範囲は 1 ~ 1000 です。デフォルトは 10 です。
ステップ 8	<code>snmp-server trap-timeout seconds</code>	(任意) トラップメッセージの再送信間隔を定義します。指定できる範囲は 1 ~ 1000 です。デフォルトは 30 秒です。
ステップ 9	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 10	<code>show running-config</code>	エントリを確認します。
ステップ 11	<code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルにエントリを保存します。

`snmp-server host` コマンドは、通知を受信するホストを指定します。`snmp-server enable trap` コマンドは、指定された通知 (トラップまたはインフォーム要求用) のメカニズムをグローバルにイネーブルにします。インフォーム要求を受信するようホストをイネーブルにするには、ホストに対して `snmp-server host informs` コマンドを設定して、`snmp-server enable traps` コマンドを使用してインフォーム要求をグローバルにイネーブルにする必要があります。

受信トラップから特定のホストを削除するには、`no snmp-server host host` グローバル コンフィギュレーション コマンドを使用します。`no snmp-server host` コマンドにキーワードを指定しないで使用すると、ホストに対して、トラップはディセーブルになりますが、インフォームはディセーブルになりません。インフォーム要求をディセーブルにするには、`no snmp-server host informs` グローバル コンフィギュレーション コマンドを使用します。特定のトラップタイプをディセーブルにするには、`no snmp-server enable traps notification-types` グローバル コンフィギュレーション コマンドを使用します。

## エージェント コンタクトおよびロケーション情報の設定

SNMP エージェントのシステム コンタクトおよびロケーションを設定して、コンフィギュレーション ファイルからこれらの記述にアクセスできるようにするには、イネーブル EXEC モードを開始して、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	<code>configure terminal</code>	グローバル 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	<code>snmp-server contact <i>text</i></code>	システム コンタクト スtring を設定します。  次に、例を示します。  <code>snmp-server contact Dial System Operator at beeper 21555.</code>
ステップ 3	<code>snmp-server location <i>text</i></code>	システム ロケーション スtring を設定します。  次に、例を示します。  <code>snmp-server location Building 3/Room 222</code>
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	エントリを確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエントリを保存します。

## SNMP 経由で使用する TFTP サーバの制限

SNMP 経由でコンフィギュレーション ファイルの保存およびロードに使用する Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバを、アクセス リストに指定されたサーバに限定するには、イネーブル EXEC モードを開始して、次の手順を実行します。

	コマンドの説明	目的
ステップ 1	<code>configure terminal</code>	グローバル 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	<code>snmp-server tftp-server-list <i>access-list-number</i></code>	SNMP 経由でコンフィギュレーション ファイルのコピーに使用する TFTP サーバを、アクセス リスト内のサーバに限定します。  <i>access-list-number</i> には、1 ~ 99 および 1300 ~ 1999 の範囲で標準の IP アクセス リスト番号を入力します。

	コマンドの説明	目的
ステップ 3	<code>access-list access-list-number {deny   permit} source [source-wildcard]</code>	<p>標準アクセス リストを作成します。必要な回数だけこのコマンドを繰り返します。</p> <ul style="list-style-type: none"> <li><code>access-list-number</code> には、ステップ 2 で指定したアクセス リスト番号を入力します。</li> <li><code>deny</code> キーワードを指定すると、条件が一致した場合にアクセスが拒否されます。<code>permit</code> キーワードを指定すると、条件が一致した場合にアクセスが許可されます。</li> <li><code>source</code> には、ML シリーズ カードにアクセスできる TFTP サーバの IP アドレスを入力します。</li> <li>(任意) <code>source-wildcard</code> には、送信元に適用するワイルドカード ビットをドット付き 10 進表記で入力します。無視するビット位置に 1 を配置します。</li> </ul> <p>アクセス リストは必ず、すべてに対し、暗黙的な拒否ステートメントで終了することに注意してください。</p>
ステップ 4	<code>end</code>	イネーブル EXEC モードに戻ります。
ステップ 5	<code>show running-config</code>	エントリを確認します。
ステップ 6	<code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルにエントリを保存します。

## SNMP の例

次に、SNMP のすべてのバージョンをイネーブルにする例を示します。この設定では、コミュニティ スtring「public」を使用し、すべてのオブジェクトに読み取り専用権限でアクセスする許可を SNMP マネージャに与えます。この設定では、ML シリーズ カードはトラップを送信しません。

```
ML_Series(config)# snmp-server community public
```

次に、コミュニティ スtring「public」を使用し、すべてのオブジェクトに読み取り専用権限でアクセスする許可を SNMP マネージャに与える例を示します。ML シリーズ カードは、SNMPv1 を使用してホスト 192.180.1.111 および 192.180.1.33 に、SNMPv2C を使用してホスト 192.180.1.27 に、それぞれ VTP トラップを送信します。コミュニティ スtring「public」がトラップとともに送信されます。

```
ML_Series(config)# snmp-server community public
ML_Series(config)# snmp-server host 192.180.1.27 version 2c public
ML_Series(config)# snmp-server host 192.180.1.111 version 1 public
ML_Series(config)# snmp-server host 192.180.1.33 public
```

次に、コミュニティ スtring `comaccess` を使用するアクセス リスト 4 のメンバーに、すべてのオブジェクトへの読み取り専用アクセスを許可する例を示します。その他の SNMP マネージャは、オブジェクトへのアクセス権がありません。コミュニティ スtring「public」を使用し、SNMP 認証失敗トラップが SNMPv2C によってホスト `cisco.com` に送信されます。

```
ML_Series(config)# snmp-server community comaccess ro 4
ML_Series(config)# snmp-server enable traps snmp authentication
ML_Series(config)# snmp-server host cisco.com version 2c public
```

次に、エンティティ MIB トラップをホスト `cisco.com` に送信する例を示します。コミュニティストリングは制限されています。2 行めはこれらのトラップの宛先を指定し、ホスト `cisco.com` に対する以前の `snmp-server host` コマンドを無効にします。

```
ML_Series(config)# snmp-server enable traps
ML_Series(config)# snmp-server host cisco.com restricted
```

次に、ML シリーズカードがコミュニティストリング「`public`」を使用して、すべてのトラップをホスト `myhost.cisco.com` に送信できるように設定する例を示します。

```
ML_Series(config)# snmp-server enable traps
ML_Series(config)# snmp-server host myhost.cisco.com public
```

## SNMP ステータスの表示

不正なコミュニティストリング エントリ数、エラー数、要求された変数の数を含めた SNMP 出力の統計情報を表示するには、`show snmp` イネーブル EXEC コマンドを使用します。また、SNMP 情報を表示するには、表 22-4 のイネーブル EXEC コマンドも使用できます。この出力に表示されるフィールドの詳細については、『*Cisco IOS Configuration Fundamentals Command Reference*』Release 12.2 を参照してください。

表 22-4 SNMP 情報の表示コマンド

機能	デフォルト設定
<code>show snmp</code>	SNMP 統計情報を表示します。
<code>show snmp group</code>	ネットワーク上の各 SNMP グループに関する情報を表示します。
<code>show snmp pending</code>	SNMP 要求のペンディングに関する情報を表示します。
<code>show snmp sessions</code>	現在の SNMP セッションに関する情報を表示します。
<code>show snmp user</code>	SNMP ユーザ テーブル内の各 SNMP ユーザ名に関する情報を表示します。



# E シリーズおよび G シリーズ イーサネットの運用

この章では、E シリーズ カードおよび G シリーズ イーサネット カードの運用について説明します。E シリーズおよび G シリーズ カードは、ONS 15454、ONS 15454 SDH、および ONS 15327 でサポートされています。プロビジョニングは、Cisco Transport Controller (CTC) または Transaction Language One (TL1) を使用して行います。Cisco IOS は、E シリーズまたは G シリーズ カードでサポートされていません。

イーサネット カードの仕様については、『Cisco ONS 15454 Reference Manual』、『Cisco ONS 15454 SDH Reference Manual』、または『Cisco ONS 15327 Reference Manual』を参照してください。イーサネット カードの回線の詳細な設定手順については、『Cisco ONS 15454 Procedure Guide』、『Cisco ONS 15454 SDH Procedure Guide』、または『Cisco ONS 15327 Procedure Guide』を参照してください。TL1 プロビジョニング コマンドについては、『Cisco ONS SONET TL1 Command Guide』または『Cisco ONS SDH TL1 Command Guide』を参照してください。

この章では、次の内容について説明します。

- [G シリーズのアプリケーション \(p.23-2\)](#)
- [G シリーズ カードの回線構成 \(p.23-8\)](#)
- [G シリーズ ギガビット イーサネット トランスポンダ モード \(p.23-10\)](#)
- [E シリーズ カードのアプリケーション \(p.23-15\)](#)
- [E シリーズ カードの回線構成 \(p.23-26\)](#)
- [RMON 仕様アラーム スレッシュホールド \(p.23-30\)](#)

## G シリーズのアプリケーション

G シリーズ カードを使用すると、SONET/SDH バックボーン上でイーサネットおよび IP データを確実に転送できます。ONS 15454 および ONS 15454 SDH の G シリーズ カードは、SONET/SDH 転送ネットワークに最大 4 つのギガビット イーサネット ポートをマッピングし、1 カードあたり STS-48c/VC4-16 までの信号レベルで、スケラブルでプロビジョニング可能な転送帯域幅を提供します。ONS 15327 の G シリーズ カードは 2 つのギガビット イーサネット ポートをマッピングします。G シリーズ カードでは、すべてのイーサネット フレーム (ユニキャスト、マルチキャスト、ブロードキャスト) で回線レートでの転送が可能であり、ジャンボ フレーム (最大 10,000 バイトと定義される) をサポートするように設定できます。G シリーズ カードには、次のように、キャリアクラスのアプリケーション向けに最適化された機能が組み込まれています。

- High Availability (HA; ハイ アベイラビリティ) (ソフトウェア アップグレード時での中断のない [50 ミリ秒未満] パフォーマンス、およびあらゆるタイプの SONET/SDH 機器の保護切り替えを含む)
- 中断のない再プロビジョニング
- 最大回線レートでのギガビット イーサネット トラフィックのサポート
- 完全な TL1 ベースのプロビジョニング機能
- 拡張ポート状態、ターミナル ループバックとファシリティ ループバックおよび J1 パストレースなどの有用なオプション
- SONET/SDH 形式のアラーム サポート
- イーサネット Performance Monitoring (PM) と Remote Monitoring (RMON) 機能

G シリーズ カードを使用して、従来の SONET/SDH 回線のように、イーサネット専用回線サービスをプロビジョニングして管理できます。G シリーズ カードのアプリケーションには、キャリアクラスの Transparent LAN Service (TLS; 透過 LAN サービス)、100 Mbps イーサネット専用回線サービス (ギガビット アップリンクを持つ外部の 100 Mbps イーサネット スイッチと組み合せた場合) および HA 転送があります。

ONS 15454 または ONS 15327 のカードは、1 つのイーサネット ポートを 1 本の STS 回線にマップします。G シリーズ カードの 4 つのポートは、STS-1、STS-3c、STS-6c、STS-9c、STS-12c、STS-24c、および STS-48c のどの回線サイズの組み合わせでもそれぞれ個別にマップできます。ただし、1 枚のカードで終端する回線サイズの合計は STS-48c 以内にする必要があります。

ONS 15454 SDH のカードは、1 つのイーサネット ポートを 1 本の STM 回線にマップします。G シリーズ カードの 4 つのポートは、VC4、VC4-2c、VC4-3c、VC4-4c、VC4-8c と VC4-16c のどの回線サイズの組み合わせでもそれぞれ個別にマップできます。ただし、1 枚のカードで終端する回線サイズの合計は VC4-16c 以内にする必要があります。

ギガビット イーサネット ポートを最大回線レートでサポートするには、1 Gbps (双方向では 2 Gbps) 以上の容量を持つ STS/VC4 回線が必要です。ギガビット イーサネット ポートを最大回線レートでサポートできる最小回線サイズは、STS-24c/VC4-8c です。G シリーズ カードは、最大回線レートのポートを 2 つまでサポートします。

G シリーズ カードは、OC-N/STM-N カードと同様の方法で J1 パストレース バイトを送信およびモニタリングします。詳細については、『ONS 15454 Reference Manual』、『ONS 15454 SDH Reference Manual』、または『ONS 15327 Reference Manual』のうちから、該当するプラットフォームのリファレンス マニュアルを参照してください。



(注) G シリーズ カードは LEX カプセル化を使用します。LEX は、RFC 1622 および RFC 2615 に記述されているように SONET/SDH 上での標準の High-Level Data Link Control (HDLC; ハイレベル データ リンク制御) フレーミングで、PPP (ポイントツーポイント プロトコル) フィールドは RFC 1841 で定義されている値に設定されます。LEX の詳細については、第 20 章「ONS イーサネット カード上の POS」を参照してください。

## G1K-4 カードと G1000-4 カードの比較

ONS 15454 および ONS 15454 SDH の G シリーズには、G1K-4 カードと G1000-4 カードがあります。G1K-4 カードは、以前の G1000-4 カードと同等のハードウェアです。

Release 3.4 以前のソフトウェアを実行している ONS 15454 に装着して運用する場合は、どちらのカードにも XC10G カードが必要です。R4.0 以降のソフトウェアを実行している ONS 15454 に G1K-4 カードを取り付ける場合、XC10G カードを取り付けた ONS 15454 だけではなく、XC カードおよび XCVT カードを取り付けた ONS 15454 にも装着できます。R 4.0 以降のソフトウェアを実行している ONS 15454 で XC カードおよび XCVT カードと併用する場合には、G1K-4 カードをスロット 5、6、12、および 13 に装着する必要があります。

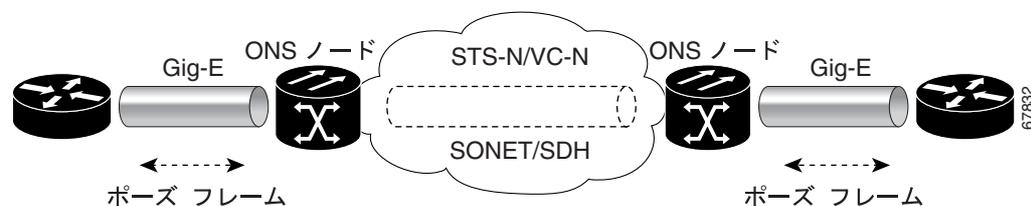
これらの制限は、ギガビット イーサネット トランスポンダ モードに設定された G シリーズ カードには適用されません。詳細については、「G シリーズ ギガビット イーサネット トランスポンダ モード」(p.23-10)を参照してください。

R4.0 以降のソフトウェアでは、G1K-4 カードは物理的に取り付けた際に認識されます。R3.4 以前のソフトウェアでは、G1000-4 カードと G1K-4 カードの両方が、物理的に取り付けた際に G1000-4 として認識されます。

## G シリーズ カードの例

図 23-1 に、G シリーズのアプリケーションを示します。この例では、データ トラフィックがハイ エンド ルータのギガビット イーサネット ポートから、ONS ノードのポイントツーポイント回線を經由して、別のハイエンド ルータのギガビット イーサネット ポートに到達しています。

図 23-1 G シリーズのポイントツーポイント回線上のデータ トラフィック



G シリーズ カードは、ギガビット イーサネット上でカプセル化および転送可能な任意のレイヤ 3 プロトコル (IP や IPX など) を伝送します。データは、ギガビット イーサネット ファイバによって ONS 15454 や ONS 15454 SDH G シリーズ カードの標準 Cisco GBIC (ギガビット インターフェイス コンバータ)、ONS 15327 G シリーズ カードの標準 Small Form-Factor Pluggable (SFP) モジュールに送信されます。G シリーズ カードは、ペイロードを OC-N/STM-N カード上へ多重化して、イーサネット フレームを SONET/SDH ペイロードに透過的にマップします。ペイロードが宛先ノードに到達すると、逆のプロセスが行われ、宛先の G シリーズ カードの標準 Cisco GBIC または SFP からギガビット イーサネット ファイバへデータが送信されます。

G シリーズ カードは、特定の種類のエラーが発生しているイーサネット フレームを、SONET/SDH 上で転送せずに廃棄します。エラーになったイーサネット フレームとは、破損して Cycle Redundancy Check (CRC; 巡回冗長検査) エラーになったフレームや、イーサネット規格の最小のフレーム長である 64 バイトに満たない短いフレームなどです。G シリーズ カードは、正常なフレームには変更を加えないで SONET/SDH ネットワークに転送します。ヘッダー内の情報は、カプセル化や転送によって影響を受けません。たとえば、IEEE 802.1Q 情報を含む形式の packets は、影響を受けずにプロセスを通過します。

## IEEE 802.3z のフロー制御とフレームバッファリング

G シリーズ カードでは、IEEE 802.3z のフロー制御とフレームバッファリングにより、データトラフィックの輻輳を緩和できます。オーバーサブスクライブを避けるために、各ポートの送受信チャネルでは 512 KB のバッファメモリを利用できます。イーサネットポートのバッファメモリが容量に近づくと、G シリーズ カードは IEEE 802.3z のフロー制御を使用して、ギガビットイーサネット接続の反対側で送信元にポーズフレームを送信します。

ポーズフレームは、送信元に一定期間パケットの送信を停止するように指示します。送信側ステーションは、要求された時間が経過してから残りのデータを送信します。図 23-1 は、G シリーズ カードと接続されているスイッチで送受信されているポーズフレームを示しています。

G シリーズ カードには対称フロー制御機能があります。対称フロー制御により、G シリーズ カードは、外部装置から送信されたポーズフレームにตอบสนองし、ポーズフレームを外部装置に送信できます。R4.0 より前のソフトウェアでは、G シリーズ カードのフロー制御は非対称でした。つまり、カードはポーズフレームを送信しますが、受信したポーズフレームは廃棄します。

Release 5.0 以降のソフトウェアでは、自動ネゴシエーションとフロー制御を CTC で個別にプロビジョニングできます。自動ネゴシエーションが失敗すると、リンクがダウンします。

自動ネゴシエーションとフロー制御の両方をイネーブルにすると、G シリーズ カードでは接続されているイーサネット装置に対して対称フロー制御が提案されます。フロー制御を使用するかどうかは、自動ネゴシエーションの結果によって異なります。

自動ネゴシエーションがイネーブルで、フロー制御がディセーブルの場合、G シリーズ カードでは自動ネゴシエーションする際に、フロー制御が提案されません。このネゴシエーションが成功するのは、接続されている装置でフロー制御なしが同意された場合だけです。

自動ネゴシエーションがディセーブルの場合、接続されている装置のプロビジョニングは無視されます。G シリーズ カードのフロー制御のイネーブルまたはディセーブルは、G シリーズ カードのプロビジョニングのみに基づきます。

このフロー制御メカニズムでは、送受信装置のスループットが、STS/VC 回線の帯域幅のスループットと一致します。たとえば、1 台のルータが G シリーズ カード上のギガビットイーサネットポートに送信を行うとします。この特定のデータレートは 622 Mbps を超える場合がありますが、G シリーズポートに割り当てられている SONET 回線は STS-12c (622 Mbps) のみです。この例では、ONS 15454 はポーズフレームを送信し、一定期間ルータからの送信を遅らせるように要求します。フロー制御と十分なポート単位のプロビジョニング機能を使用すると、フレーム損失の大部分を制御できるため、回線レートの最大容量 (STS-24c) 未満でプロビジョニングされる専用回線サービスが効率良く行えます。同じことが ONS 15454 SDH または ONS 15327 に適用されます。

G シリーズ カードでは、フロー制御のスレッシュホールドプロビジョニングが可能であり、ユーザは 3 つの基準 (バッファサイズ) 設定、すなわち、デフォルト、低遅延、カスタム設定から 1 つを選択できます。デフォルトが通常の使用に最適であり、R4.1 より前のソフトウェアでは、デフォルトしか適用できませんでした。低遅延は、STS-1c での Voice-over-IP (VoIP) のようなサブレートアプリケーションに適しています。バッファリングが十分でない、ベストエフォートトラフィック、またはアクセスする回線が長距離である接続装置では、G シリーズ カードを高遅延に設定します。

カスタム設定では、Flow Ctrl Lo と Flow Ctrl Hi に対して正確なパッファ サイズのスレッシュホールドを設定できます。フロー制御高 (Flow Ctrl Hi) の設定は接続されているイーサネット装置に [Pause On] フレームを送るための基準であり、このフレームは装置に一時的に送信を停止させる信号を送信します。フロー制御低 (Flow Ctrl Lo) の設定は接続されているイーサネット装置に [Pause Off] フレームを送るための基準であり、このフレームは装置に送信を再開させる信号を送信します。G シリーズカードでは、ポートに接続されている装置で自動ネゴシエーションがイネーブルになっている場合にだけ、ポート上でフロー制御をイネーブルにできます。



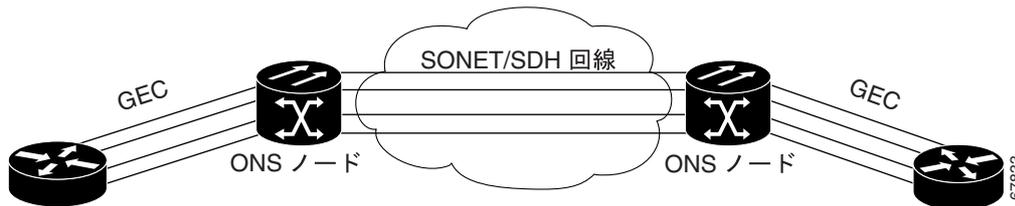
(注)

自動ネゴシエーションを R 4.0 より前のソフトウェア リリースを実行している G シリーズカードと相互運用するように設定している外部のイーサネット装置では、R4.0 以降のソフトウェアを実行している G シリーズカードと相互運用する際に自動ネゴシエーションの設定を変更する必要はありません。

## GEC/IEEE 802.3ad リンク集約

G シリーズは、シスコ独自の規格である Gigabit EtherChannel (GEC) や IEEE 802.3ad 規格などのあらゆる形式のリンク集約技術をサポートします。G シリーズカードのエンドツーエンド リンク完全性機能により、回線でイーサネット リンクをエミュレートできます。これにより、あらゆる種類のレイヤ 2 およびレイヤ 3 再ルーティングを、G シリーズカードで適切に処理できます。図 23-2 に、G シリーズカードの GEC サポートを示します。

図 23-2 G シリーズカードの GEC のサポート



G シリーズカードは、GEC を直接実行しませんが、接続されているイーサネット装置間のエンドツーエンドの GEC 機能をサポートしています。GEC を実行している 2 つのイーサネット装置が G シリーズカードを通じて ONS ネットワークに接続している場合、ONS SONET/SDH 側のネットワークは EtherChannel 装置に対して透過的になります。2 つの EtherChannel 装置は、相互に直接接続されているかのように動作します。G シリーズカードの平行回線サイズを任意に組み合わせ、GEC のスループットをサポートできます。

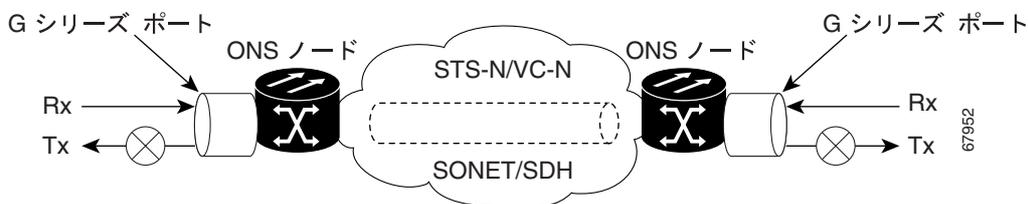
GEC は、接続されているイーサネット装置に回線レベルのアクティブな冗長性と保護 (1:1) を提供します。また、平行の G シリーズ データ リンクを 1 つにバンドルして、より集約された帯域幅を提供することもできます。Spanning Tree Protocol (STP; スパニング ツリー プロトコル) は、バンドルされたリンクが 1 本のリンクであるかのように動作し、GEC に対して、これらの複数の平行パスを利用することを許可します。GEC を使用しない場合、STP は 1 つのノンブロッキングパスのみを許可します。また、GEC は、各種カード (または各種ノード) 上のポートのグループをサポートできるため、G シリーズカードのカードレベルの保護と冗長性を提供します。これにより、1 つのポートまたはカードに障害が発生した場合でもトラフィックはほかのポートまたはカードに再ルーティングされます。

エンドツーエンドのイーサネットリンク完全性機能は、接続されている装置上の GEC 機能と組み合わせて使用できます。この機能を組み合わせることにより、スパニングツリーの再ルーティングなどの代替方法よりも応答時間が短いイーサネットトラフィックの回復スキームが提供されます。また、予備の帯域幅を予約する必要がないため、帯域幅をより効率的に利用できます。

## イーサネットリンク完全性のサポート

G シリーズカードは、エンドツーエンドのイーサネットリンク完全性をサポートします( 図 23-3 )。この機能は、イーサネット専用回線サービスの提供と、接続されているイーサネット装置でのレイヤ 2 およびレイヤ 3 プロトコルの適切な運用に不可欠です。エンドツーエンドのイーサネットリンク完全性では、エンドツーエンドのパスの一部に障害が発生すると、パス全体で障害が発生したことになります。パス全体の障害は、パスの各端にある送信レーザーがオフになることで確認できます。接続されているイーサネット装置は、ディセーブルになった送信レーザーを搬送波損失と認識し、その結果非アクティブリンクとみなします。

図 23-3 エンドツーエンドのイーサネットリンク完全性のサポート



(注)

搬送波損失状態を無視するように設定できるネットワーク装置もあります。搬送波損失状態を無視するように設定された装置が一方の端で G シリーズカードに接続されている場合は、障害を回避してトラフィックをルーティングするために代替の方法(レイヤ 2 またはレイヤ 3 のキーブアライブメッセージの使用など)を用意する必要があります。通常、このような代替方法の応答時間は、エラー状態の識別にリンク状態を使用する方法よりもかなり長くなります。

図 23-3 に示すように、パスの任意のポイントでの障害によって、各端の G シリーズカードでは Tx 送信レーザーがディセーブルになり、その結果、両端の装置はリンクがダウンしたことを検出します。イーサネットポートの 1 つが管理上ディセーブルな場合やループバックモードで設定されている場合、エンドツーエンドのイーサネットパスは使用できなくなるため、そのポートはエンドツーエンドのリンク完全性に関して「障害」とみなされます。ポートの「障害」により、パスの両端もディセーブルになります。

## イーサネット ポートおよび SONET/SDH ポートの管理状態とサービス状態およびソーク時間

G シリーズ カードは、イーサネット ポートおよび SONET/SDH 回線の管理状態とサービス状態をサポートします。カードと回線のサービス状態の詳細については、『Cisco ONS 15454 Reference Manual』または『Cisco ONS 15454 SDH Reference Manual』の付録「Administrative and Service States」を参照してください。

ギガビットイーサネットポートには、IS AINS 管理状態を含む、サービス状態を設定できます。IS AINS はポートを最初に OOS-AU AINS 状態に設定します。このサービス状態では、アラームレポートは抑制されますが、トラフィックは伝送され、ループバックは許可されます。ソーク期間が終了すると、ポートの状態が IS-NR に変わります。アラームがレポートされるかどうかに関係なく、発生した障害状態は、CTC の Conditions タブまたは TL1 の RTRV-COND コマンドを使用して取得できます。

イーサネットポートのアラームおよび状態である、CARLOSS および TPTFAIL の 2 つは、ポートが稼動中になるのを防ぎます。ギガビットイーサネットポートを IS AINS 状態に設定して G シリーズ回線をプロビジョニングし、アラームが抑制されている場合でも、この状態が発生します。これは、G シリーズのリンク完全性機能がアクティブであり、パス内のすべての SONET およびイーサネットエラーが解決されるまで、どちらかの終端の Tx 送信レーザーがイネーブルにならないためです。リンク完全性機能によりエンドツーエンドパスがダウンした状態にある限り、両方のポートの状態は、AINS から IS への状態の変更を抑制するために必要な 2 つの状態のうちの少なくとも 1 つになります。これにより、ポートは AINS 状態のままとなり、アラームレポートが抑制されます。

また、この状態は G シリーズカードの SONET/SDH 回線にも適用されます。SONET/SDH 回線の状態が IS AINS 状態に設定されて、回線状態が IS に変わる前にイーサネットエラーが発生した場合、イーサネットエラーが両端で解決されるまで、リンク完全性は回線の状態が IS に変わるのも防止します。管理状態が IS AINS である限り、サービス状態は OOS-AU AINS となります。イーサネットエラーまたは SONET エラーがなくなると、リンク完全性機能は両端でギガビットイーサネット Tx 送信レーザーをイネーブルにします。同時に、AINS カウントダウンが通常どおりに開始されます。経過時間中に別の状態が発生しない場合は、各ポートの状態が IS NR 状態に変わります。AINS カウントダウン中、ソーク時間の残り時間が CTC および TL1 で使用できます。ソーク期間に状態が再度発生すると、AINS ソーキングロジックが最初から再開します。

IS AINS 状態にプロビジョニングされた SONET/SDH 回線は、回線のどちらかの側のギガビットイーサネットポートの状態が IS NR に変わるまで最初の OOS 状態のままです。AINS から IS への変更が完了するかどうかに関係なく、リンク完全性機能によりギガビットイーサネットポートの Tx 送信レーザーがオンになると、SONET/SDH 回線はイーサネットトラフィックを転送し統計情報をカウントします。

## G シリーズカードの回線構成

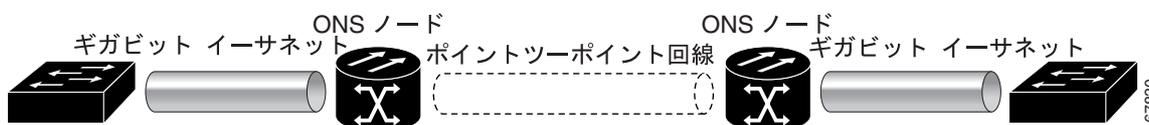
ここでは、G シリーズカードのポイントツーポイント回線および手動クロスコネクトについて説明します。イーサネットの手動クロスコネクトを使用すると、ONS 以外の SONET/SDH ネットワークセグメントをブリッジングできます。

### G シリーズカードのポイントツーポイント イーサネット回線

G シリーズカードは、ポイントツーポイント回線構成をサポートします(図 23-4)。回線は、SONET または SDH ラインカードと同様に CTC で設定できます。G シリーズカードは、回線サービス状態をサポートします。

ONS 15454 および ONS 15327 でプロビジョニング可能な SONET 回線のサイズは、STS 1、STS 3c、STS 6c、STS 9c、STS 12c、STS 24c、および STS 48c です。ONS 15454 SDH でプロビジョニング可能な SDH 回線のサイズは、VC4、VC4-2c、VC4-3c、VC4-4c、VC4-8c、VC4-9c、および VC4-16c です。各イーサネットポートは G シリーズカードの個々の STS/VC 回線にマップされます。

図 23-4 G シリーズカードのポイントツーポイント回線



G シリーズカードでは、有効な回線サイズのリストの中から最大 4 つの回線を組み合わせて使用できます。ただし、回線サイズの合計が 48 本の STS または 16 本の VC4 以内になる必要があります。

ハードウェア上の制限で、G シリーズカードにドロップされる回線の組み合わせには、さらにいくつかの制約があります。この制約はノードで透過的に強制されるもので、回線の組み合わせの制限を気にする必要はありません。

1 本の STS-24c または VC4-8c がカードで終端する場合、そのカードの残りの回線を別の 1 本の STS-24c または VC4-8c に使用することも、合計 12 本以内の STS または合計 4 本以内の VC4 になるように (つまり、カードでの STS の合計が 36 本または VC4 の合計が 12 本) STS-12c または VC4-4c 以内のサイズの回線を組み合わせることもできます。

STS-24c または VC4-8c 回線がカードにドロップされない場合は、全帯域幅が無制限に使用できます (たとえば、1 本の STS-48c または VC4-16c や 4 本の STS-12c または VC4-4c 回線などを使用できます)。

この STS-24c または VC4-8c の制限は 1 本の STS-24c または VC4-8c 回線がドロップされた場合のみ適用されるので、この制限による影響は最小となります。カード上の STS-24c または VC4-8c 回線は、ほかのサイズの回線と分離してグループ化します。グループ化した回線は、ほかの G シリーズカードにドロップできます。



(注) G シリーズカードは STS/VC クロスコネクトのみを使用します。VT レベルのクロスコネクトは使用されません。



注意

G シリーズカードは E シリーズカードと接続できません。相互運用性の詳細については、第 20 章「ONS イーサネットカード上の POS」を参照してください。

## G シリーズカードの手動クロスコネクト

ONS ノードで通常のイーサネット回線のプロビジョニングを行うためには、ノード間でエンドツーエンド CTC を確認できる必要があります。ONS ノード間に他のベンダーの機器が配置されている場合、そのベンダーの SNMP/Target Identifier Address Resolution Protocol (OSI/TARP; 簡易ネットワーク管理プロトコル/ターゲット ID アドレス解決プロトコル) ベースの機器では、ONS ノードの TCP/IP ベースの Data Communication Channel (DCC; データ通信チャンネル) のトンネリングは使用できません。矛盾した DCC を回避するために、イーサネット回線は、ONS 以外のネットワークを使用して、STS/VC チャンネルに手動でクロスコネクトする必要があります。手動によるクロスコネクトを使用すると、ONS 以外のネットワークを活用しながら、イーサネット回線を ONS ノード間で実行できます (図 23-5)。



(注)

ここでは「クロスコネクト」および「回線」を次のような意味で使用します。「クロスコネクト」は、1 つの ONS ノード内で発生する接続を表し、回線が ONS ノードに出入りできることを意味します。「回線」は、トラフィック送信元 (トラフィックが ONS ノードネットワークへ入る場所) からドロップまたは宛先 (トラフィックが ONS ノードネットワークを出る場合) までの一連の接続を表します。

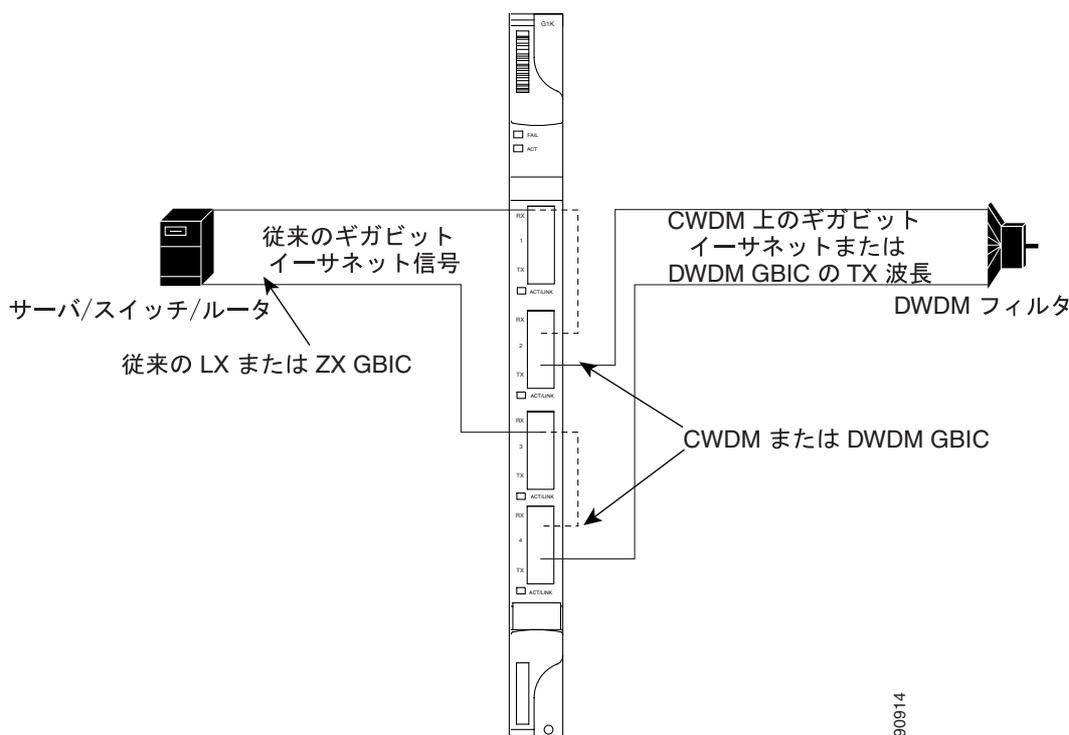
図 23-5 G シリーズカードの手動クロスコネクト



## G シリーズギガビットイーサネットトランスポンダモード

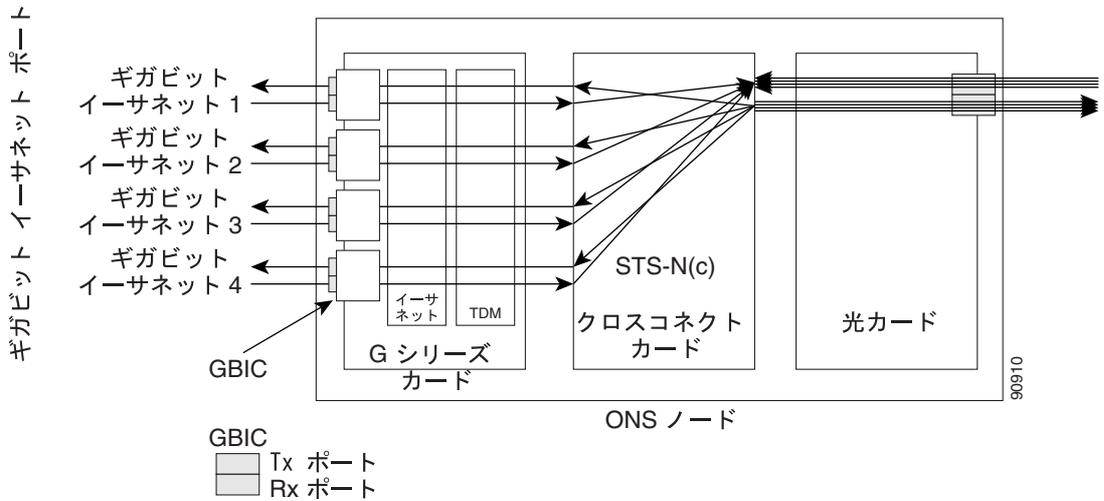
ONS 15454 および ONS 15454 SDH の G シリーズカードはトランスポンダとして設定できます。ONS 15327 の G シリーズカードはトランスポンダとして設定できません。トランスポンダモードは、G シリーズでサポートされている GBIC (SX、LX、ZX、Coarse Wavelength Division Multiplexing [ CWDM; 低密度波長分割多重 ] や Dense Wavelength Division Multiplexing [ DWDM; 高密度波長分割多重 ]) とともに使用できます。図 23-6 は、トランスポンダモードのカードレベルでの概略を示しています。

図 23-6 G シリーズの 1 ポート トランスポンダモードのアプリケーションのカードレベルでの概略



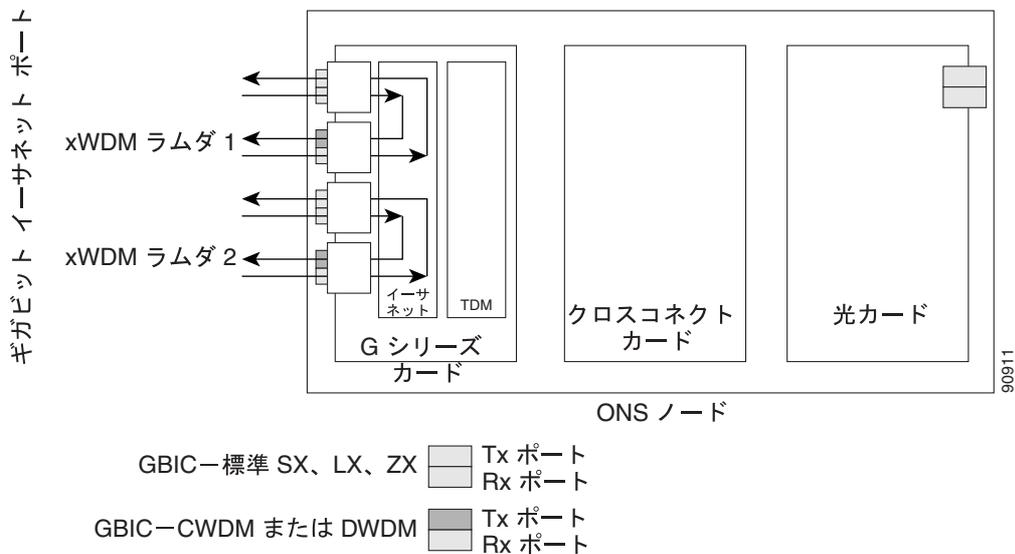
トランスポンダとして設定された G シリーズカードは、SONET/SDH 用に設定された G シリーズカードとは全く異なる動作をします。SONET/SDH 設定では、G シリーズカードはカード正面のイーサネットポートと GBIC からギガビットイーサネットトラフィックを送受信します。このイーサネットトラフィックは、クロスコネクタカードと光カードを介して多重化されて SONET/SDH ネットワークを出入りします (図 23-7 参照)。

図 23-7 デフォルトの SONET/SDH モードでの G シリーズ



トランスポンダモードでは、G シリーズのイーサネットのトラフィックはクロスコネクタカードや SONET/SDH ネットワークと通信することなく G シリーズカードの内部に留まり、カード上で GBIC へ送り返されます (図 23-8)。

図 23-8 トランスポンダモードでの G シリーズカード (2 ポート双方向)



G シリーズカードはトランスポンダモードあるいは SONET/SDH デフォルトに設定できます。1 つでもポートがトランスポンダモードにプロビジョニングされると、カードはトランスポンダモードとなり、カードのすべてのポートが SONET/SDH モードに戻らないと SONET/SDH 回線を設定できません。G シリーズポートをトランスポンダモードにプロビジョニングするには、『Cisco ONS 15454 Procedure Guide』または『Cisco ONS 15454 SDH Procedure Guide』を参照してください。

## ■ G シリーズギガビットイーサネットトランスポンダモード

G シリーズ カードをトランスポンダ モードに設定する前に、すべての SONET/SDH 回線を削除する必要があります。ONS 15454 または ONS 15454 SDH は、12 個のトラフィック スロットの任意のスロットまたはすべてのスロットでトランスポンダ モードに設定された G シリーズ カードをホスティングでき、最大 24 双方向、あるいは 48 単方向のラムダをサポートします。

トランスポンダとして設定された G シリーズ カードは、次の 3 つのいずれかのモードになります。

- 2 ポート双方向トランスポンダ モード
- 1 ポート双方向トランスポンダ モード
- 2 ポート単方向トランスポンダ モード

## 2 ポート双方向トランスポンダ モード

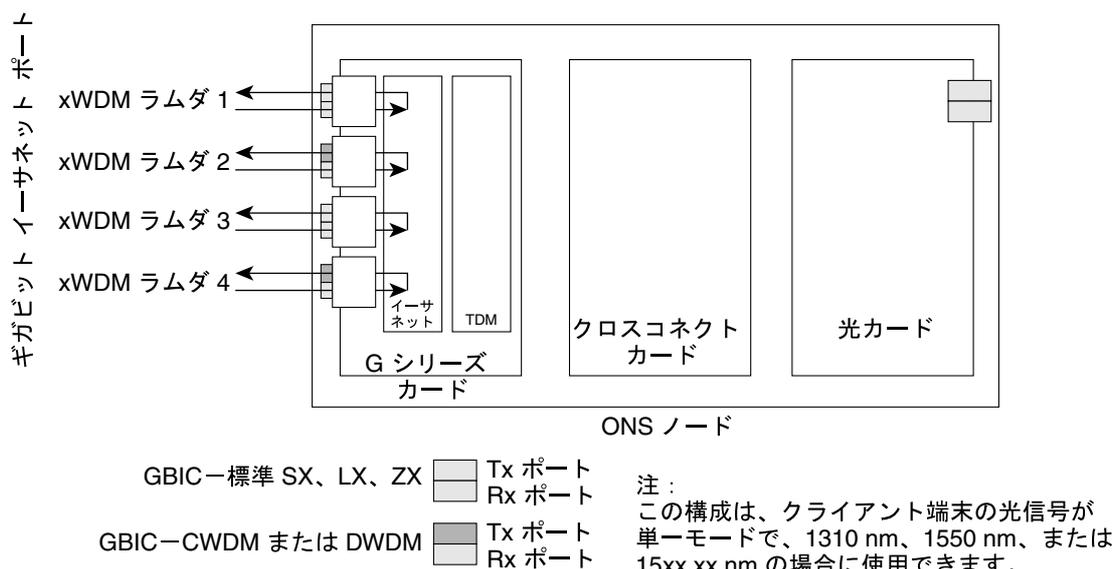
2 ポート双方向トランスポンダ モードは、1 つの G シリーズ カード ポートの送受信イーサネット フレームを他のポートの送受信イーサネット フレームへマッピングします (図 23-8)。トランスポンダの双方向ポート マッピングは同一カードの任意の 2 つのポート間で可能です。

## 1 ポート双方向トランスポンダ モード

1 ポート双方向トランスポンダ モードは、あるポートで受信されたイーサネット フレームを同一ポートの送信側へマッピングします (図 23-9)。このモードは、ポートが他のポートではなく同一ポートにマッピングされる点を除けば、2 ポート双方向トランスポンダと同じです。1 ポート双方向トランスポンダモードのデータパスはファシリティ ループバックと同一ですが、トランスポンダモードは保守モードではなく、搬送波損失 (CARLOSS) のような非 SONET/SDH アラームを抑制することはありません。

このモードは、中間 DWDM 信号再生成で使用し、CWDM および DWDM GBIC の広帯域容量の利点を利用できます。その結果、ノードは複数の波長で受信できますが、送信できるのは固定波長でのみとなります。

図 23-9 1 ポート双方向トランスポンダ モード



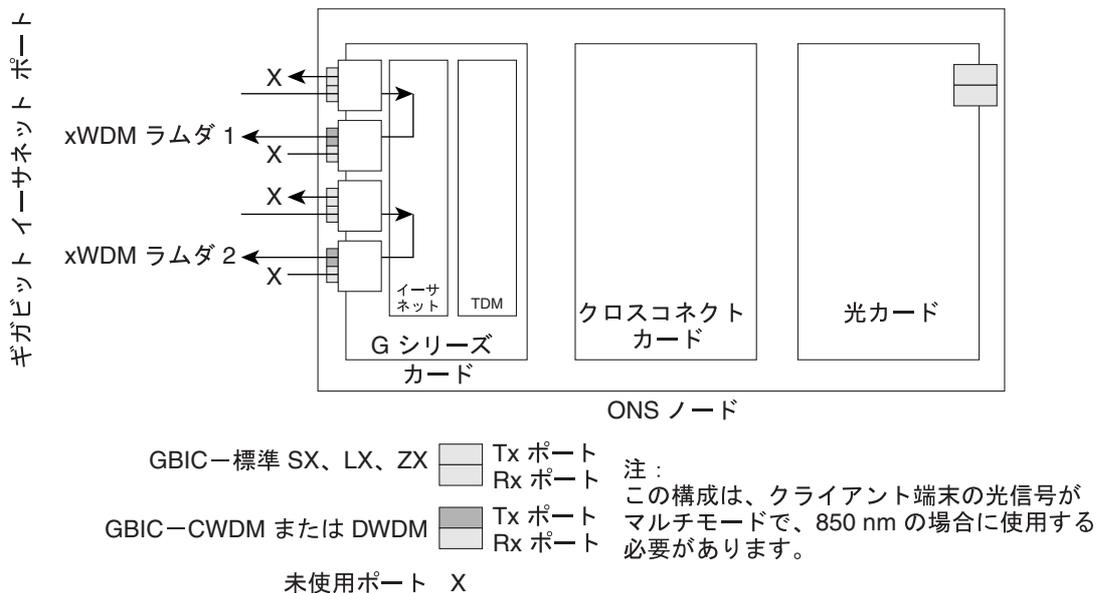
90913

## 2 ポート単方向トランスポンダモード

1 つのレシーバーで受信されたイーサネット フレームは、他のポートの送信側から送信されます。このモードは、1 つの方向だけが使われる点を除けば、2 ポート双方向トランスポンダと同じです (図 23-10)。1 つのポートは単方向送信専用としてプロビジョニングし、もう 1 つのポートは単方向受信専用としてプロビジョニングする必要があります。単方向送信用として設定されたポートは受信ポート上の損失信号を無視するので、受信ポートのファイバを接続する必要はありません。単方向受信用として設定されたポートは送信レーザーをオンにしないので、送信ポートのファイバを接続する必要はありません。

このモードは、たとえば、ある種の Video on Demand (VoD; ビデオ オン デマンド) アプリケーションのように、1 方向のみが CWDM または DWDM 上で送信される必要がある場合に使用されます。

図 23-10 2 ポート単方向トランスポンダ



## G シリーズ トランスポンダ モードの特性

G シリーズカードのトランスポンダモードでの動作は、SDH モードでの G シリーズカードとはいくつかの点で異なります。

- トランスポンダモードに設定された G シリーズカードは、ユーザが SONET/SDH 回線をプロビジョニングするときに、CTC のプロビジョニング可能なカードリストに表示されません。
- トランスポンダモードに設定された G シリーズカードはクロスコネクトカード (たとえば、XC10G) を必要としませんが、TCC2/TCC2P カードを必要とします。
- トランスポンダに設定された G シリーズのポートは、フロー制御のポーズ フレームには応答せず、ポーズ フレームを透過的にカードに通します。SONET/SDH モードでは、ポートはポーズ フレームに応答し、ポーズ フレームをカードに通しません。
- TL1 によるプロビジョニングではトランスポンダモードの設定はサポートされていません。ただし、トランスポンダモードおよびポート情報は、TL1 コマンドの RTRV-G1000 で表示できます。
- すべての SONET/SDH 関連のアラームは、カードがトランスポンダモードに設定されている場合には抑制されます。

## ■ G シリーズギガビットイーサネットトランスポンダモード

- トランスポンダモードの G1000-4 や G1K-4 カードには、スロット番号やクロスコネクタの制約はありません。
- ファシリティと端末のループバックは、単方向のトランスポンダモードでは完全にはサポートされていませんが、両方の双方向トランスポンダモードではサポートされています。
- イーサネットの自動ネゴシエーションはサポートされておらず、単方向トランスポンダモードではプロビジョニングできません。自動ネゴシエーションは、両方の双方向トランスポンダモードでサポートされています。
- エンドツーエンドのリンク完全性機能はトランスポンダモードでは使用できません。



(注)

通常の SONET/SDH モードでは、G シリーズカードはエンドツーエンドのリンク完全性機能をサポートします。この機能はイーサネットや SONET/SDH 障害により、対応するイーサネットポートの送信レーザーをディセーブルにしてオフにします。トランスポンダモードでは、イーサネットポート上の信号損失は、対応するポートの送信信号には影響を与えません。

G シリーズカードのトランスポンダモードでの動作は、G シリーズカードの SONET/SDH モードでの動作に類似している点もあります。

- G シリーズのイーサネット統計情報は、両方のモードのポートで使用可能です。
- イーサネットポートレベルのアラームや条件は、両方のモードのポートで使用可能です。
- ジャンボフレームや非ジャンボフレーム動作は、両方のモードで同一です。
- すべての既存のカウンタや PM パラメータに対する収集、レポート、スレッショールド条件は、両方のモードで同一です。
- SNMP および RMON のサポートは両方のモードで同一です。

## E シリーズカードのアプリケーション

ONS 15454、ONS 15454 SDH、ONS 15327 のすべてで E シリーズ カードをサポートします。E シリーズ カードには、ONS 15454 および ONS 15454 SDH の E100T-12/E100T-G および E1000-2/E1000-2-G が含まれます。E100T-G と以前の E100T-12 の機能は同じです。E1000-2-G と以前の E1000-2 も機能は同じです。XC10G カードを使用している ONS 15454 には、G バージョン (E100T-G または E1000-2-G) の E シリーズ イーサネット カードが必要です。ONS 15454 または ONS 15454 SDH は、最大 10 枚の E シリーズ カードをサポートします。E シリーズ イーサネット カードは任意の多目的スロットに装着できます。

ONS 15327 の E シリーズ カードは、E10/100-4 です。E シリーズの中でこのカードだけが、ML シリーズ カードとの相互運用性を可能にする、LEX カプセル化の設定をサポートします。詳細については、第 20 章「ONS イーサネット カード上の POS」を参照してください。



(注)

ONS 15454 および ONS 15454 SDH の E シリーズ カードは、LEX カプセル化をサポートしません。



(注)

E シリーズ カード (ONS 15327 または ONS 15454) のどちらも G シリーズ カードと相互運用できません。

## E シリーズカードのモード

E シリーズ カードは、マルチカード EtherSwitch グループ、シングルカード EtherSwitch、またはポートマップの 3 つのモードのどれか 1 つで動作します。マルチカード EtherSwitch グループまたはシングルカード EtherSwitch モードの E シリーズ カードは、VLAN (仮想 LAN)、IEEE 802.1Q、STP、IEEE 802.1D などのレイヤ 2 機能をサポートします。ポートマップ モードは、E シリーズ カードを、ストレート マッパー カードとして動作するように設定し、これらのレイヤ 2 機能はサポートしません。複数の E シリーズ カードを使用するノード内では、E シリーズ カードはそれぞれ、3 つのモードのいずれかで動作できます。カードのモードを確認するには、CTC のイーサネット カードビューで、Provisioning > Ether Card タブをクリックします。



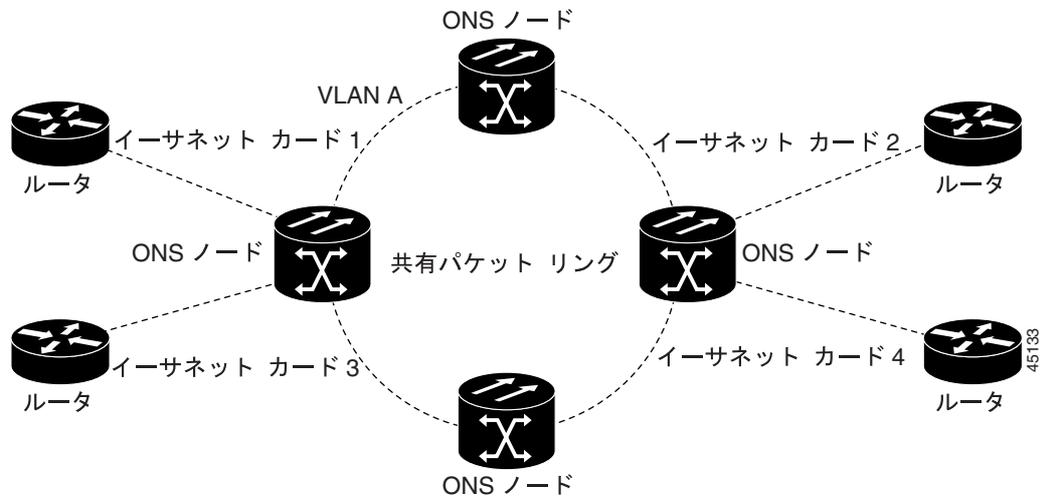
(注)

ポートマップ モードでは、他の E シリーズ モードに固有の問題を回避できます。これについては、フィールド通知『E-Series Ethernet Line Card Packet Forwarding Limitations』で詳しく説明します。

## E シリーズのマルチカード EtherSwitch グループ

マルチカード EtherSwitch グループでは、2 つ以上のイーサネット カードが 1 つのレイヤ 2 スイッチとして機能するようにプロビジョニングします。図 23-11 に、マルチカード EtherSwitch の構成を示します。マルチカード EtherSwitch は、ONS 15454 または ONS 15454 SDH-E シリーズ カードの 2 つのイーサネット回線ポイント間の帯域幅を STS-6c に、ONS 15327 E シリーズ カード間の帯域幅を STS-3c に制限しますが、ノードとカードを追加して共有パケット リングを作成できます。

図 23-11 マルチカード EtherSwitch 構成



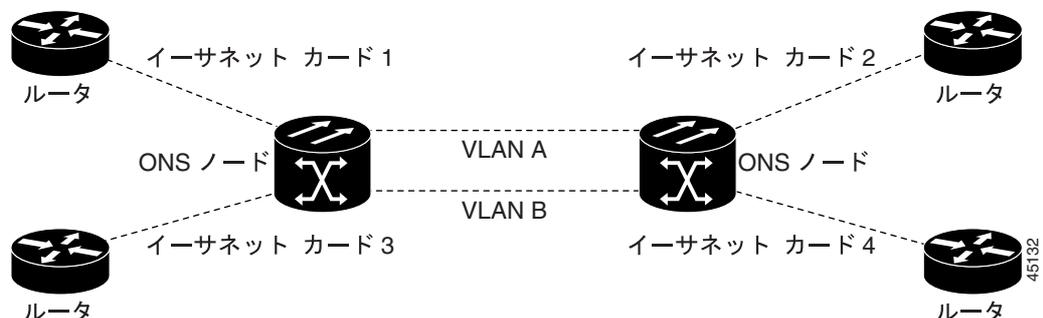
## 注意

2本の STS-3c/VC4-2c マルチカード EtherSwitch 回線をイーサネットカード上で終端させ、その後最初の回線を削除する場合には、カードに STS-1/VC4 回線をプロビジョニングする前に、もう 1 本の STS-3c/VC4-2c 回線を削除する必要があります。最初の STS-3c/VC4-2c 回線を削除しただけで STS-1/VC4 回線を作成しようとする、STS-1/VC4 回線は動作しませんが、アラームはこの状態を表示しません。この状況を回避するために、2 本目の STS-3c/VC4-2c を削除してから、STS-1/VC4 回線を作成します。

## E シリーズシングルカード EtherSwitch

すべての E シリーズカードでは、シングルカード EtherSwitch を使用すると、各イーサネットカードでは ONS ノード内に 1 つのスイッチ エンティティしか存在できません。図 23-12 に、シングルカード EtherSwitch の構成を示します。

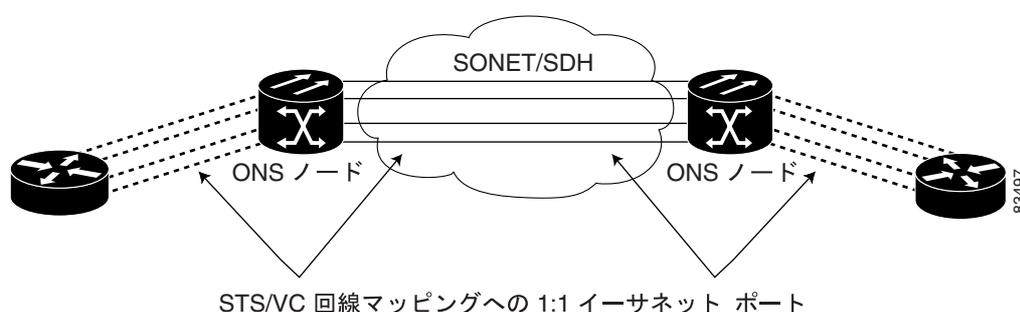
図 23-12 シングルカード EtherSwitch 構成



## ポートマップ (リニア マッパー)

ポートマップモード (リニア マッパー) では、特定の E シリーズイーサネットポートをカード固有の STS/VC 回線の 1 つにマップするように E シリーズカードを設定します (図 23-13)。ポートマップモードでは、レイヤ 1 の転送で、ユニキャスト、マルチキャスト、および混合トラフィックの低遅延を実現できます。E100T-G カードまたは E10/100-4 カード上のイーサネットとファストイーサネットは、回線レート速度で動作します。E1000-2-G カードの最大帯域幅が STS-12c/VC4-4c であるため、ギガビットイーサネットの転送は最大で 600 Mbps に制限されます。また、イーサネットフレームは最大 1522 バイトまでのサイズがサポートされ、IEEE 802.1Q タグ付きフレームが転送できます。Q-in-Q フレーム (IEEE 802.1Q in IEEE 802.1Q ラップフレーム) の大きな最大フレームサイズはサポートされません。

図 23-13 E シリーズカードのイーサネットポートから STS/VC 回線へのマッピング



ポートマップモードでは、シングルカードモードまたはマルチカードモードの E シリーズカードでサポートされているレイヤ 2 機能 (STP、VLAN、MAC [メディア アクセス制御] アドレス学習など) は使用できません。このモードを使用すると、クロスコネクトおよび TCC2/TCC2P カード切り替えでのサービスに影響する時間を大幅に短縮できます。

ポートマップモードでは、マルチカードモードとシングルカードモードと同じ方法では VLAN をサポートしません。マルチカードモードおよびシングルカードモードの E シリーズカードのポートは、特定の VLAN に加入することが可能ですが、ポートマップモードの E シリーズカードには、レイヤ 2 機能がありません。このモードでは、ポート間でマップされた接続で外部の VLAN を透過的に転送するだけです。ポートマップモードの E シリーズカードは、転送する VLAN のタグを検査しないため、1 ~ 4096 の範囲の VLAN がポートマップモードで転送できます。

ポートマップモードでは、イーサネットフレームヘッダーの検査または検証を実行しません。イーサネットの CRC は検証され、無効なイーサネット CRC を持ったフレームはすべて廃棄されます。

また、ポートマップモードでは、任意の 2 枚の E シリーズカード (E100T-G、E1000-2-G、および E10/100-4 [ONS 15327 の E シリーズカード]) 間に STS/VC 回線を作成できます。ポートマップモードでは、ONS 15454 の E シリーズカードを ML シリーズカードまたは G シリーズカードに接続できません。ただし、LEX カプセル化がプロビジョニングされた ONS 15327 E10/100-4 カードは ML シリーズカードに接続できます。



(注) E シリーズカード (ONS 15327 または ONS 15454) のどちらも G シリーズカードとは相互運用できません。

## ■ E シリーズカードのアプリケーション

## E シリーズモードで使用可能な回線サイズ

表 23-1 に、ONS 15454、ONS 15454 SDH、および ONS 15327 の E シリーズモードで使用可能な回線サイズを示します。

表 23-1 ONS 15454 および ONS 15327 E シリーズイーサネットの回線サイズ

ONS 15327 E シリーズポートマップおよびシングルカード EtherSwitch	ONS 15327 E シリーズマルチカード EtherSwitch	ONS 15454 E シリーズポートマップおよびシングルカード EtherSwitch	ONS 15454 E シリーズマルチカード EtherSwitch	ONS 15454 SDH E シリーズポートマップおよびシングルカード EtherSwitch	ONS 15454 SDH E シリーズマルチカード EtherSwitch
STS-1	STS-1	STS-1	STS-1	VC4	VC4
STS-3c	STS-3c	STS-3c	STS-3c	VC4-2c	VC4-2c
STS-6c	—	STS-6c	STS-6c	VC4-4c	—
STS-12c	—	STS-12c	—	—	—

## E シリーズモードで使用可能な合計帯域幅

表 23-1 に、ONS 15454、ONS 15454 SDH、および ONS 15327 の E シリーズモードで使用可能な合計帯域幅を示します。

表 23-2 ONS 15454 および ONS 15327 E シリーズの使用可能な合計帯域幅

ONS 15327 E シリーズポートマップおよびシングルカード EtherSwitch	ONS 15327 E シリーズマルチカード EtherSwitch	ONS 15454 E シリーズポートマップおよびシングルカード EtherSwitch	ONS 15454 E シリーズマルチカード EtherSwitch	ONS 15454 SDH E シリーズポートマップおよびシングルカード EtherSwitch	ONS 15454 SDH E シリーズマルチカード EtherSwitch
STS-12c の合計	STS-3c の合計	STS-12c の合計	STS-6c の合計	VC4-4c の合計	VC4-2c の合計

## E シリーズカードの IEEE 802.3z フロー制御

E100T-G または E10/100-4 (任意のモードで動作) と E1000-2-G (ポートマップモードで動作) は、IEEE 802.3z 対称フロー制御をサポートし、接続されているイーサネット装置と自動ネゴシエーションする際に対称フロー制御を提案します。フロー制御を機能させるには、E シリーズのポートと接続されているイーサネット装置を自動ネゴシエーション (AUTO) モードに設定する必要があります。接続されているイーサネット装置でフロー制御がイネーブルになっていることも必要です。フロー制御メカニズムでは、E シリーズカードは、外部装置から送信されたポーズフレームに回答し、ポーズフレームを外部装置に送信します。

E100T-G または E10/100-4 (任意のモードで動作) および E1000-2-G (ポートマップモードで動作) の場合、フロー制御では送受信装置のスループットが STS 回線の帯域幅のスループットと一致します。同様のことが ONS 15454、ONS 15454 SDH、および ONS 15327 に適用されます。たとえば、ルータがポートマップモードの E シリーズカードのギガビットイーサネットに送信するとします。ルータから送信されるデータレートは 622 Mbps を超える場合もありますが、ポートマップモードの E シリーズカードポートに割り当てられる ONS 15454 回線の帯域幅は、最大で STS-12c (622.08 Mbps) です。このシナリオでは、ONS 15454 はポーズフレームを送信し、送信ルータに一定の期間送信を遅らせるように要求します。



(注) ポートマップモードの E シリーズカードと SmartBits テストセット間のフロー制御をイネーブルにするには、SmartBits テストセットで MII レジスタのビット 5 を手動で 0 に設定します。ポートマップモードの E シリーズカードと Ixia テストセット間のフロー制御をイネーブルにするには、接続されている Ixia ポートの Properties メニューで Enable the Flow Control を選択します。

## E シリーズの VLAN サポート

CTC ソフトウェアを使用して、E シリーズ VLAN をプロビジョニングできます。特定のセットのポートで、ONS ノードに対するブロードキャストドメインを定義します。VLAN ポートの定義には、すべてのイーサネットとパケット交換の SONET/SDH ポートタイプが含まれます。VLAN の IP アドレスディスカバリ、フラッディング、および転送はすべて、これらのポートに制限されます。



注意

VLAN の数が多すぎると (100 以上)、トラフィックが停止する可能性があります。

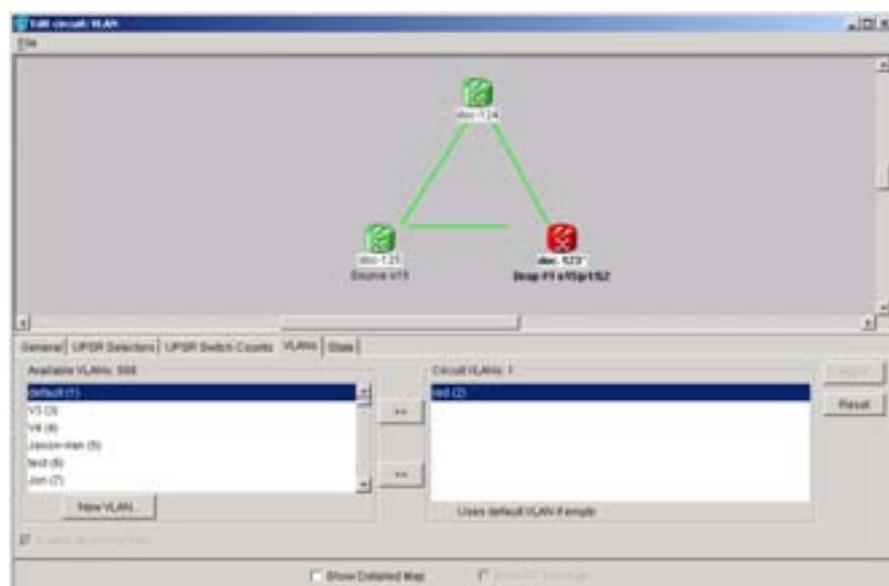
IEEE 802.1Q ベースの VLAN メカニズムでは、一般的な SONET/SDH 転送インフラストラクチャ上で加入者 LAN トラフィックを論理的に分離します。各加入者はそれぞれのサイトにイーサネットポートを 1 つずつ持ち、それぞれの加入者が 1 つの VLAN を割り当てられます。加入者の VLAN データは共有回線上を流れますが、加入者にはサービスは専用のデータ転送のように見えます。



(注) ポートマップモードは VLAN をサポートしません。

回線で使用される VLAN の数と使用可能な VLAN の合計数は、CTC の VLAN カウンタに表示されます (図 23-14)。

図 23-14 使用可能な VLAN を示す Edit Circuit ダイアログボックス



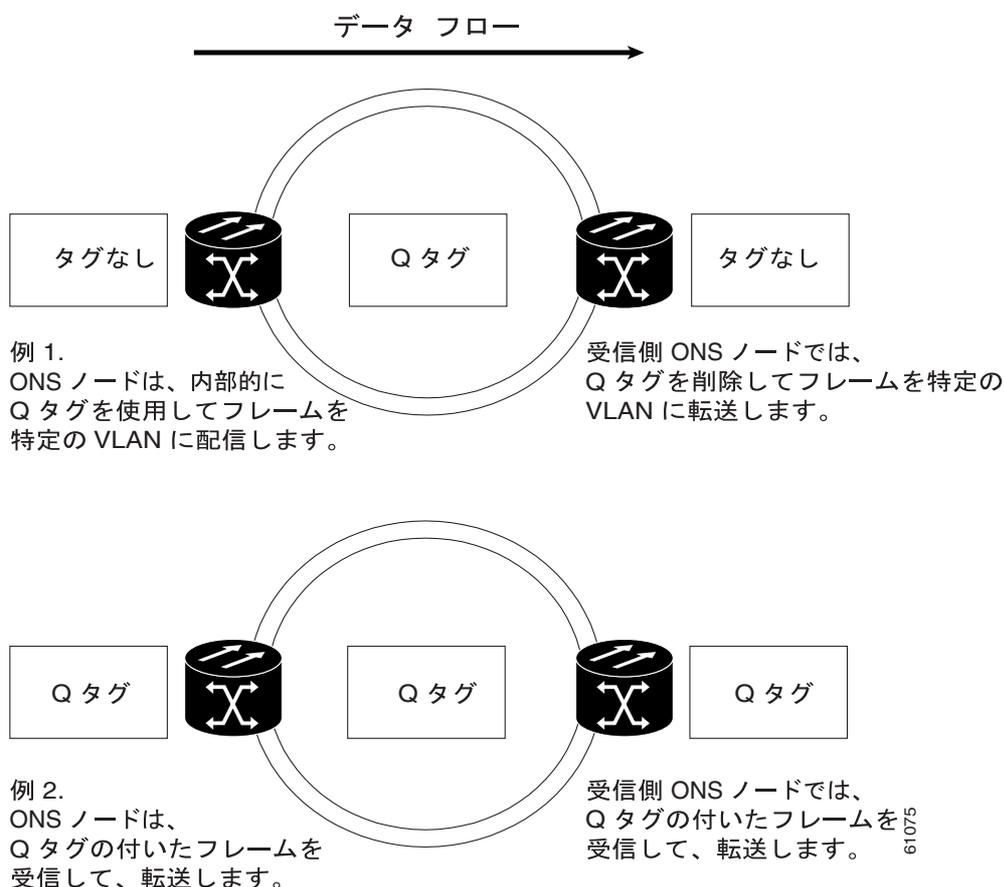
## EシリーズカードのQタギング (IEEE 802.1Q)

シングルカードモードとマルチカードモードのEシリーズカードは、IEEE 802.1Qをサポートします。IEEE 802.1Qを使用すると、同じ物理ポートに複数の802.1Q VLANを収容できます。各IEEE 802.1Q VLANはそれぞれ別の論理ネットワークを表します。ポートマップモードのEシリーズカードはIEEE 802.1Qタグ(Qタグ)を転送しますが、これらのタグの削除や追加は行いません。

ONSノードは、IEEE 802.1Qをサポートするイーサネット装置とも、IEEE 802.1Qをサポートしないイーサネット装置とも相互運用できます。Eシリーズイーサネットポートに接続されている装置がIEEE 802.1Qをサポートしない場合、ONSノードはQタグを内部でのみ使用します。ONSノードはこれらのQタグを特定のポートに関連付けます。

IEEE 802.1Qをサポートしないイーサネット装置を使用している場合、ONSノードはONSネットワークに入るタグなしのイーサネットフレームを取得し、Qタグを使用してそのパケットをONSネットワークの入力ポートと関連付けられたVLANに割り当てます。受信側のONSノードは、フレームがONSネットワークを出る時に、(古いイーサネット装置が、IEEE 802.1Qパケットを不正なフレームであると誤って識別しないように)Qタグを削除します。ONSネットワークの入力ポートと出力ポートは、Untagに設定して削除できるようにする必要があります。Untagは、ONSポートのデフォルト設定です。図23-15の例1は、ONSネットワーク内でのみQタグを使用する例を示しています。

図23-15 VLANを経由するQタグの推移



ONS ノードは、IEEE 802.1Q をサポートする外部のイーサネット装置によって付加された Q タグを使用します。パケットは、既存の Q タグが付いて ONS ネットワークに入ります。ONS ノードは ONS ネットワーク内でこの同じ Q タグを使用してパケットを転送し、パケットが ONS ネットワークを出るときには Q タグが付加された状態のままにします。この処理が行われるためには、ONS ネットワークの入力ポートと出力ポートを Tagged に設定しておく必要があります。図 23-15 の例 2 は、Q タグを使用して、ONS ネットワークに出入りするパケットの処理の様子を表しています。

ポートの Tagged および Untag の設定手順の詳細については、『Cisco ONS 15454 Procedure Guide』、『Cisco ONS 15454 SDH Procedure Guide』、または『Cisco ONS 15327 Procedure Guide』を参照してください。



注意

ONS ノードは、別のノードのネットワークビューにノードが表示されているときは、そのノードが同じ SONET/SDH ネットワークに存在するかあるいは DCC を通じて接続されているかに関係なく、必ず VLAN を伝播しています。たとえば、DCC で接続されていない 2 つの ONS ノードが同じログイン ノードグループに属している場合、VLAN はその 2 つの ONS ノード間で伝播されます。ONS ノードが同じ SONET/SDH リングに属していない場合でも、VLAN は伝播されます。

## E シリーズカードの優先キューイング (IEEE 802.1Q)

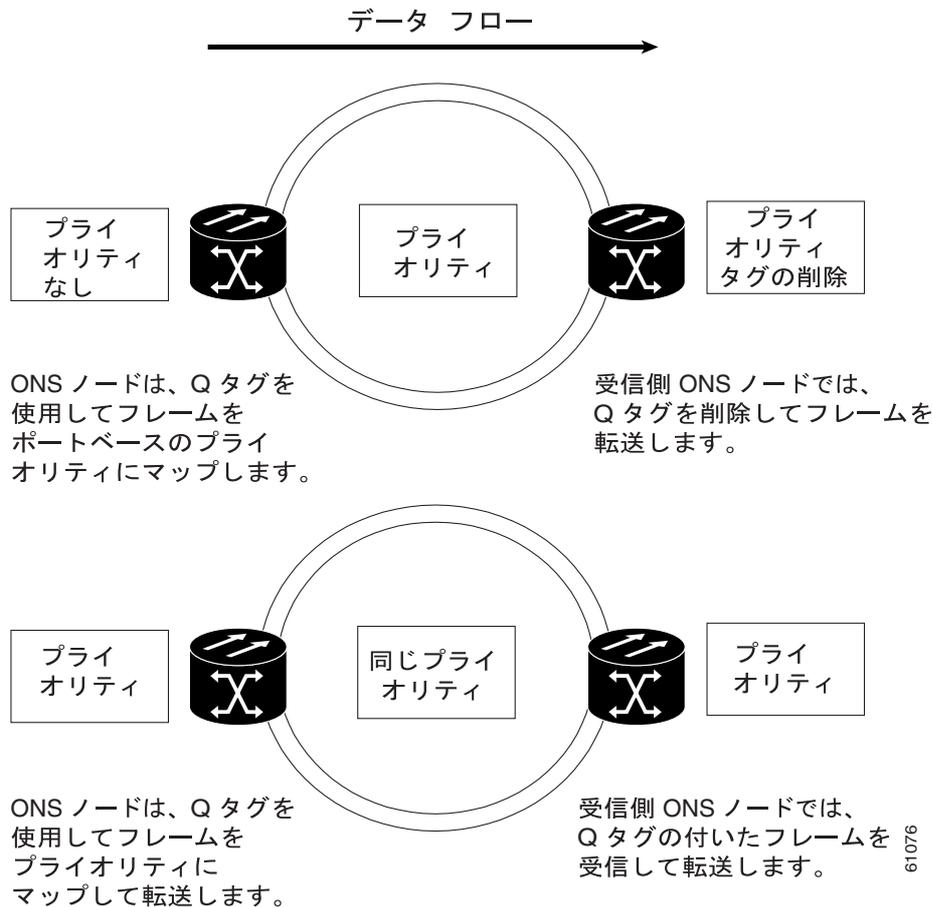
優先キューイングを行わないネットワークでは、すべてのパケットを First-in-first-out (FIFO; 先入れ先出し) の原則に基づいて処理します。優先キューイングを行うと、イーサネットトラフィックがプライオリティ レベル別にマッピングされるため、ネットワーク輻輳の影響が緩和されます。E シリーズカードは優先キューイングをサポートします。E シリーズカードは IEEE 802.1Q で指定されている 8 つのプライオリティを 2 つのキュー (ロー プライオリティとハイ プライオリティ) にマップします (表 23-3)。

表 23-3 優先キューイング

ユーザのプライオリティ	キュー	割り当て帯域幅
0、1、2、3	ロー	30%
4、5、6、7	ハイ	70%

Q タグは、ネットワークを通じて優先キューイング情報を伝送します (図 23-16)。

図 23-16 優先キューイングのプロセス



ONS ノードでは、「漏出パケット」アルゴリズムを使用して重み付けプライオリティを設定します。完全プライオリティとは反対に、重み付けプライオリティでは、優先順位の高いパケットに帯域幅へのアクセスをより多く提供しますが、優先順位の低いパケットをまったく優先使用しないわけではありません。ネットワーク輻輳の期間中、帯域幅のおよそ 70 % がハイプライオリティのキューに、残りの 30 % はロープライオリティのキューに振り分けられます。過度に輻輳しているネットワークでは、パケットが廃棄されます。



(注) IEEE 802.1Q は、以前は IEEE 802.1P と呼ばれていました。



(注) ポートマップモードの E シリーズカードおよび G シリーズカードは優先キューイング (IEEE 802.1Q) をサポートしません。

## E シリーズのスパニングツリー (IEEE 802.1D)

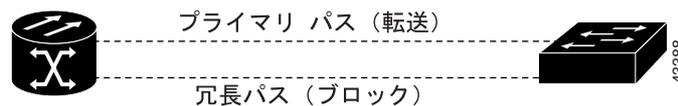
E シリーズカードでは IEEE 802.1D の STP を実行します。E シリーズカードは、回線ごとに一般的な STP を合計 8 つの STP インスタンスまでサポートします。VLAN 単位の STP はサポートされません。シングルカードモードでは、回線の作成中に回線単位で STP をディセーブルまたはイネーブルにできます。STP をディセーブルにすると、使用可能な STP インスタンスの数が保持されます。

STP は、イーサネットポートおよび OC-N/STM-N ポートを含むすべてのパケット交換ポートで動作します。イーサネットポート上では、STP はデフォルトでイネーブルになっていますが、ディセーブルにすることもできます。ユーザはまた、ポイントツーポイント構成でシングルカード EtherSwitch (束になっていない) として設定したイーサネットカードで、回線単位で STP をディセーブルまたはイネーブルにできます。ただし、回線単位で STP 保護をオフにすると、SONET/SDH システムは、その回線でイーサネットトラフィックを保護しなくなるため、イーサネットトラフィックはイーサネットネットワークの別のメカニズムによって保護される必要があります。OC-N/STM-N インターフェイスポートでは、ONS ノードはデフォルトで STP を有効化し、ユーザが STP をディセーブルにすることはできません。

イーサネットカードは、イーサネットポート上で STP をイネーブルにし、接続されているイーサネット装置への冗長パスを作成できます。STP では、機器とファシリティの両方が障害から保護されるようにカードを接続します。

STP はネットワークループを検出して排除します。STP が、2 つのネットワークホスト間で複数のパスを検出した場合は、2 つのネットワークホスト間のパスが 1 つだけになるまでポートをブロックします (図 23-17)。パスを 1 つにすることで、ブリッジループの発生を回避できます。これは、必然的にループを含む共有パケットリングにとって重要です。

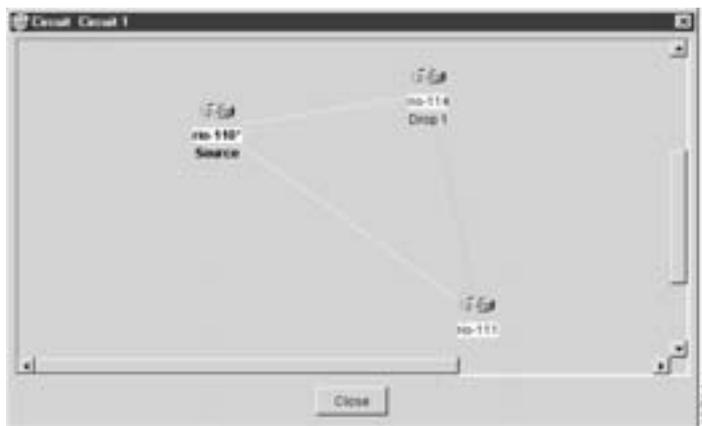
図 23-17 STP ブロックパス



ループを削除するために STP では、広域ネットワークのすべてのスイッチにわたるツリーを定義します。STP は、一定の冗長データパスをスタンバイ (ブロック) 状態にします。STP のあるネットワークセグメントが到達不能になると、STP アルゴリズムは STP トポロジを再構成し、ブロックされたパスを再度有効にして、リンクを再確立します。STP 操作はエンドステーションに透過的であり、単一の LAN セグメントへの接続と、複数のセグメントがあるスイッチド LAN への接続は、エンドステーションでは区別されません。ONS ノードは、回線ごとに 1 つの STP インスタンス、ONS ノードごとに最大 8 つの STP インスタンスをサポートします。

Circuit ウィンドウのスパニングツリーマップには、転送スパンとブロックスパンが表示されます (図 23-18)。

図 23-18 Circuit ウィンドウのスパニングツリー マップ



(注)

緑色は、転送スパンを表し、紫はブロック（保護）スパンを表します。パケット リング構成の場合は、1 つ以上のスパンが紫色になります。



注意

STP 保護がイネーブル化されている複数の回線では、それらの回線が 1 枚の共通カードを通過し、同じ VLAN を使用する場合には、ブロッキングが発生します。



(注)

E シリーズカードのポートマップ モードは STP (IEEE 802.1D) をサポートしません。

## E シリーズカードの複数インスタンス スパニングツリーと VLAN

ONS ノードでは、ループトポロジーで VLAN をサポートするために STP の複数のインスタンスを動作させます。SONET/SDH リング上の別個の回線を、それぞれの VLAN グループ専用の回線にできます。各回線はそれぞれ独自の STP を実行して、複数リング環境で VLAN 接続を維持します。

### 回線単位のスパニングツリー

ポイントツーポイント構成のシングルカード EtherSwitch E シリーズカードでは、回線単位でも STP をディセーブルまたはイネーブルにできます。この機能で、スパニング ツリー保護回線を同一カード上の保護されていない回線と混在させることができます。また、同一ノードにある 2 枚のシングルカード EtherSwitch E シリーズカードで、相互ノード回線を構成することもできます。

### E シリーズカードのスパニングツリー パラメータ

デフォルトの STP パラメータは、ほとんどの状況に適するように設定されています (表 23-4)。デフォルトの STP パラメータを変更する場合は、その前に Cisco Technical Assistance Center (Cisco TAC) に相談してください。連絡方法については、「テクニカル サポート」(p.xxvii) を参照してください。

表 23-4 スパニングツリーのパラメータ

パラメータ	説明
BridgeID	コンフィギュレーション Bridge Protocol Data Unit (BPDU; ブリッジ プロトコル データ ユニット)を送信する ONS ノードの一意の ID。ブリッジ ID は、ブリッジのプライオリティと ONS ノードの MAC アドレスを組み合わせたものです。
TopoAge	最後にトポロジが変更されてからの経過時間 (秒)
TopoChanges	ノードが起動してから STP トポロジが変更された回数
DesignatedRoot	特定の STP インスタンスの STP の指定ルート
RootCost	指定ルートへのパス コストの合計
RootPort	ルートに到達するために使用するポート
MaxAge	受信したプロトコル情報が廃棄されるまでの最大保持時間
HelloTime	スパニングツリーのルートであるブリッジまたはスパニングツリーのルートになるうとするブリッジによってコンフィギュレーション BPDU が送信される間隔 (秒)
HoldTime	指定したポートで設定情報を送信する間の最小経過時間 (秒)
ForwardDelay	リスニング ステートおよびラーニング ステートのポートの経過時間

## E シリーズカードのスパニングツリー設定

スパニングツリー設定を表示するには、ノード ビューで、**Provisioning > Etherbridge > Spanning Trees** タブをクリックします (表 23-5)。

表 23-5 スパニングツリーの構成

カラム	デフォルト値	値の範囲
Priority	32768	0 ~ 65535
Bridge Max Age	20 秒	6 ~ 40 秒
Bridge Hello Time	2 秒	1 ~ 10 秒
Bridge Forward Delay	15 秒	4 ~ 30 秒

## E シリーズカードの回線構成

E シリーズのイーサネット回線では、ポイントツーポイント（ストレート）共有パケットリング、またはハブアンドスポーク構成を通じて ONS ノードをリンクできます。ノードが 2 つの場合は、通常、ポイントツーポイント構成で接続します。3 つ以上のノードは、通常、共有パケットリング構成かハブアンドスポーク構成で接続します。イーサネットの手動クロスコネクタを使用すると、個々のイーサネット回線を ONS ノードの光インターフェイス上の STS/VC チャネルに相互接続したり、ONS 以外の SONET/SDH ネットワーク セグメントをブリッジングすることもできます。E シリーズの回線を設定する方法については、『Cisco ONS 15454 Procedure Guide』、『Cisco ONS 15454 SDH Procedure Guide』、または『Cisco ONS 15327 Procedure Guide』を参照してください。

## E シリーズカードの回線保護

E シリーズの回線設定と SONET/SDH ネットワーク トポロジーのさまざまな組み合わせによって、異なるレベルの E シリーズ回線保護を提供します。表 23-6 に、使用可能な保護を詳しく示します。

表 23-6 E シリーズ回線設定の保護

構成	UPSR (SNCP)	BLSR (MS-SPRing)	1 + 1
ポイントツーポイント マルチカード EtherSwitch	なし	SONET/SDH	SONET/SDH
ポイントツーポイント シングルカード EtherSwitch	SONET/SDH	SONET/SDH	SONET/SDH
ポイントツーポイント ポートマップ モード	SONET/SDH	SONET/SDH	SONET/SDH
共有パケットリング マルチカード EtherSwitch	STP	SONET/SDH	SONET/SDH
共通制御カード スイッチ	STP	STP	STP



(注) STS/STM 回線サイズを選択してから、イーサネット接続を行ってください。

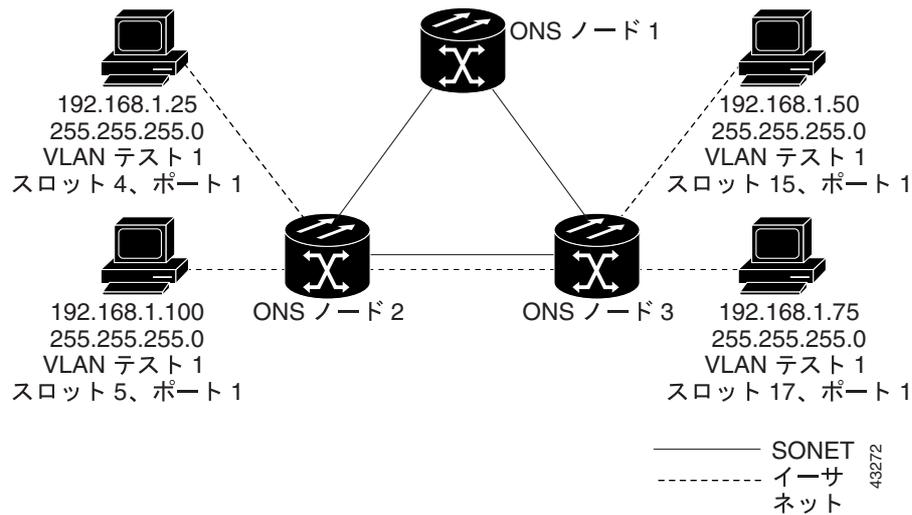


(注) STS-12c/VC4-4c イーサネット回線を作成する場合は、イーサネットカードをシングルカード EtherSwitch モードまたはポートマップ モードに設定する必要があります。マルチカード モードは STS-12c/VC4-4c イーサネット回線をサポートしません。

## E シリーズカードのポイントツーポイントイーサネット回線

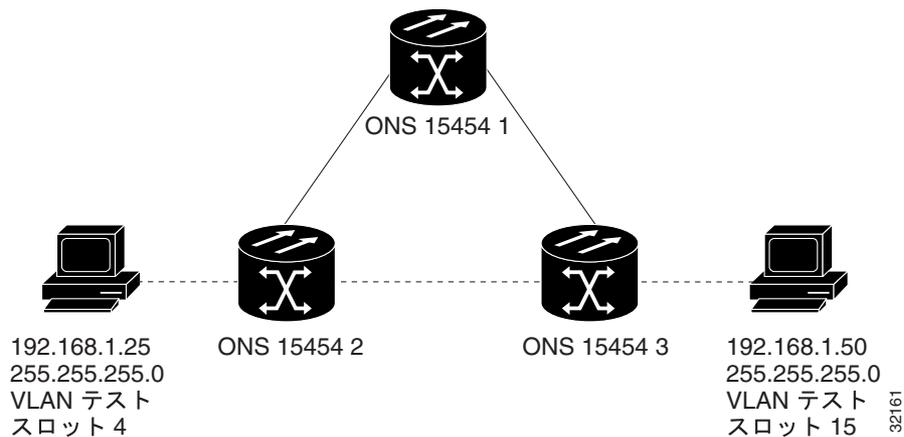
ONS ノードでは、ポイントツーポイント（ストレート）のイーサネット回線をシングルカード、ポートマップ、またはマルチカードの回線として設定できます（図 23-19）。

図 23-19 マルチカード EtherSwitch のポイントツーポイント回線



シングルカード EtherSwitch モードとポートマップ モードでは、イーサネット回線の 2 つのエンドポイント間で STS-12c の全帯域幅を利用できます（図 23-20）。

図 23-20 シングルカード EtherSwitch またはポートマップのポイントツーポイント回線

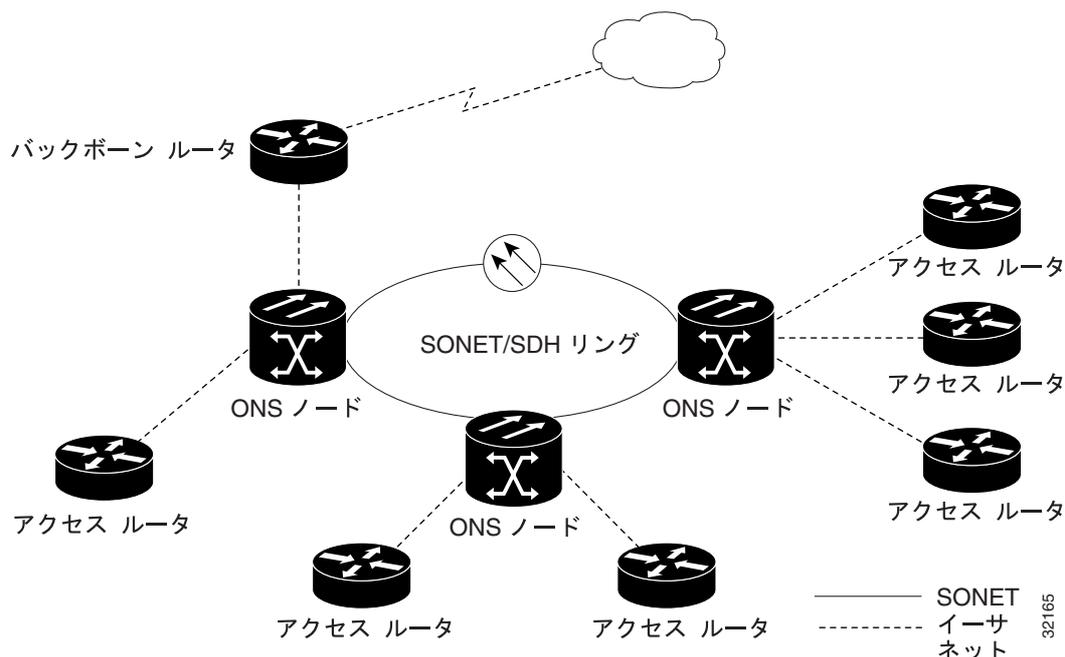


**(注)** ポートマップ回線、ポイントツーポイント回線は E シリーズのポートベースの VLAN に加入できませんが、外部 VLAN を転送できます。

## E シリーズ カードの共有パケット リング イーサネット回線

共有パケット リングでは、送信元ノードと宛先ノード以外にも、イーサネット STS 回線にアクセスするノードを追加できます。追加ノードの E シリーズ カードポートは、回線の VLAN および帯域幅を共有できます。図 23-21 に共有パケット リングを示します。実際のネットワーク アーキテクチャは、この例とは異なる場合があります。

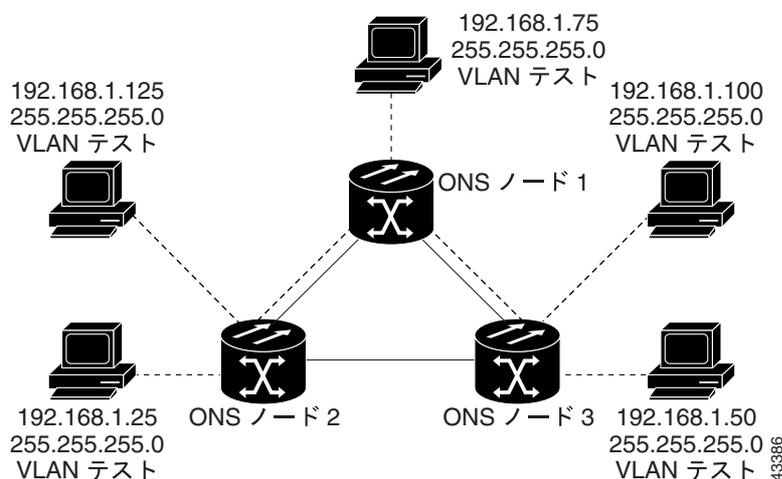
図 23-21 共有パケット リング イーサネット回線



## E シリーズ カードのハブアンドスポーク イーサネット回線のプロビジョニング

ハブアンドスポーク構成は、ポイントツーポイント回線（スポーク）を集約ポイント（ハブ）に接続します。多くの場合、ハブは高速接続にリンクしており、スポークはイーサネット カードです。図 23-22 にハブアンドスポーク リングを示します。実際のネットワーク アーキテクチャは、この例とは異なる場合があります。

図 23-22 ハブアンドスポーク構成のイーサネット回線



## E シリーズカードのイーサネット手動クロスコネク

ONS ノードで 通常のイーサネット回線のプロビジョニングを行うためには、CTC でノード間のエンドツーエンドでそれらを確認できる必要があります。ONS ノード間に他のベンダーの機器が配置されている場合、そのベンダーの OSI/TARP ベースの機器では、ONS ノードにおける TCP/IP ベースの DCC のトンネリングは使用できません。矛盾した DCC を回避するために、ONS 以外のネットワークを使用してイーサネット回線を STS チャネルに手動で相互接続する必要があります。手動クロスコネクを使用すると、ONS 以外のネットワークを利用しながら、イーサネット回線を ONS ノード間で実行できます。



(注)

ここでは「クロスコネク」および「回線」を次のような意味で使用します。「クロスコネク」は、1 つの ONS ノード内の接続を表し、回線が ONS 15454 に出入りできることを意味します。回線は、トラフィック送信元 (トラフィックが ONS 15454 ネットワークに入る場所) からドロップまたは送信先 (トラフィックが ONS 15454 ネットワークを出る場所) までの一連の接続を表します。

## RMON 仕様アラーム スレッシュホールド

ONS ノードには、ネットワーク オペレータが Network Management System (NMS; ネットワーク管理システム) でネットワークの状態をモニタリングできる RMON 機能があります。

ONS ノードの RMON MIB (管理情報ベース) の 1 つは、アラーム グループです。アラーム グループは、alarmTable から構成されます。NMS は、alarmTable を使用して、ネットワーク パフォーマンスのアラームが発生するスレッシュホールドを検索します。スレッシュホールドは、現在の 15 分の間隔と、現在の 24 時間の間隔に適用されます。RMON は、イーサネット コリジョンなどいくつかの変数をモニタリングし、その間隔の間に変数がスレッシュホールドを超えるとイベントをトリガーします。たとえば、スレッシュホールドが 1000 コリジョンに設定されている場合、15 分の間隔の間に 1001 のコリジョンが発生するとイベントがトリガーされます。CTC により、イーサネットの統計のスレッシュホールドをプロビジョニングできます。

RMON アラーム スレッシュホールドの手順については、『Cisco ONS 15454 Troubleshooting Guide』、『Cisco ONS 15454 Troubleshooting Guide』、または『Cisco ONS 15327 Troubleshooting Guide』を参照してください。



## CE-100T-8 イーサネットの運用

この章では、ONS 15454 および ONS 15454 SDH でサポートされている CE-100T-8 (キャリア イーサネット) カードの運用について説明します。ONS 15454 SONET に取り付けられた CE-100T-8 カードは SONET 動作にのみ限定されていて、ONS 15454 SDH に取り付けられた CE-100T-8 カードは SDH 動作にのみ限定されます。別バージョンの CE-100T-8 カードは、ONS15310-CL でサポートされています。

プロビジョニングは、Cisco Transport Controller (CTC) または Transaction Language One (TL1) を使用して行います。Cisco IOS は、CE-100T-8 カードではサポートされていません。

イーサネット カードの仕様については、『Cisco ONS 15454 Reference Manual』または『Cisco ONS 15454 SDH Reference Manual』を参照してください。イーサネット カードの回線の詳細な設定手順については、『Cisco ONS 15454 Procedure Guide』または『Cisco ONS 15454 SDH Procedure Guide』を参照してください。TL1 プロビジョニング コマンドについては、『Cisco ONS SONET TL1 Command Guide』または『Cisco ONS SDH TL1 Command Guide』を参照してください。

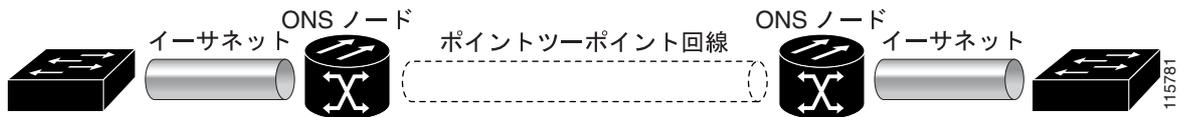
この章では、次の内容について説明します。

- [CE-100T-8 の概要 \(p.24-2\)](#)
- [CE-100T-8 のイーサネットの機能 \(p.24-3\)](#)
- [CE-100T-8 の SONET/SDH 回線および機能 \(p.24-8\)](#)

## CE-100T-8 の概要

CE-100T-8 は、8 個の 10/100 イーサネットポートを備えたレイヤ 1 マッパー カードです。このカードは、各ポートをポイントツーポイント設定で一意の SONET 回線にマップします。図 24-1 に、CE-100T-8 のアプリケーション例を示します。この例では、スイッチのファストイーサネットポートからのデータトラフィックがポイントツーポイント回線を経由して別のスイッチのファストイーサネットポートに伝送されます。

図 24-1 CE-100T-8 のポイントツーポイント回線



CE-100T-8 カードを使用して、従来の SONET/SDH 回線のように、イーサネット専用回線サービスを提供して管理できます。CE-100T-8 カードのアプリケーションには、キャリアクラスのエーサネット専用回線サービスおよびハイアベイラビリティ転送があります。

CE-100T-8 カードは、イーサネット上でカプセル化および転送可能な任意のレイヤ 3 プロトコル (IP や IPX など) を伝送します。データネットワークからのイーサネットフレームは、イーサネットケーブルで CE-100T-8 カード上の標準 RJ-45 ポートに送信されます。CE-100T-8 カードは、Packet-over-SONET/SDH (POS) カプセル化を使用して SONET/SDH ペイロードにイーサネットフレームを透過的にマップします。次に、カプセル化されたイーサネットを内部に持つ POS 回線は、他の SONET Synchronous Transport Signal (STS; 同期転送信号) や SDH Synchronous Transport Mode (STM; 同期転送モード) と同じように、光カードに多重化されます。ペイロードが宛先ノードに達すると、逆のプロセスが行われ、宛先の CE-100T-8 カードの標準 RJ-45 ポートからイーサネットケーブルおよびイーサネットデータネットワークヘデータが送信されます。POS プロセスについては第 20 章「ONS イーサネットカード上の POS」を参照してください。

CE-100T-8 カードは、ITU-T G.707 および Telcordia GR-253 規格標準をサポートします。このカードではソフトリセットが可能で、多くの場合エラーが発生しません。ソフトリセット中にプロビジョニングが変更された場合、またはソフトウェアのアップグレード中にファームウェアが置き換えられる場合、リセットはハードリセットに相当します。CTC を使用した CE-100T-8 カードのソフトリセットの詳細については、『Cisco ONS 15454 Procedure Guide』または『Cisco ONS 15454 SDH Procedure Guide』を参照してください。

## CE-100T-8 のイーサネットの機能

CE-100T-8 カードには、10BASE-T イーサネットおよび 100BASE-TX イーサネット メディア用に標準 RJ-45 コネクタを使用するフロントエンド イーサネット ポートが 8 基装備されています。イーサネット ポート 1 ~ 8 の各ポートは、対応する番号の POS ポートにそれぞれマップされます。CE-100T-8 カードのコンソール ポートは機能しません。

CE-100T-8 カードは、正常なイーサネット フレームには変更を加えないで SONET/SDH ネットワークに転送します。ヘッダー内の情報は、カプセル化や転送によって影響を受けません。たとえば、IEEE 802.1Q が含まれた情報は、影響を受けずにプロセスを通過します。

ONS 15454 SONET/SDH CE-100T-8 および ONS 15310-CL CE-100T-8 は、Cyclic Redundancy Check (CRC; 巡回冗長検査)を含めて最大 1548 バイトのイーサネット フレーム サイズをサポートします。Maximum Transmission Unit (MTU; 最大伝送ユニット) サイズは最大 1500 バイト (標準イーサネット MTU) に設定されており、変更できません。標準イーサネット フレームが IEEE 802.1Q タグまたは Multiprotocol Label Switching (MPLS; マルチプロトコル ラベル スイッチング) タグで拡張されるベビー ジャイアント フレームもサポートされています。フルジャンボ フレームはサポートされません。

CE-100T-8 カードは、特定の種類のエラーが発生しているイーサネット フレームを、SONET/SDH 上で転送せずに廃棄します。エラーになったイーサネット フレームとは、破損して CRC エラーになったフレームや、イーサネット規格の最小のフレーム長である 64 バイトに満たない短いフレームなどです。



(注)

多くのイーサネット属性も、Network Element (NE; ネットワーク要素) のデフォルト機能によって利用できます。NE のデフォルト機能の詳細については、『Cisco ONS 15454 Reference Manual』または『Cisco ONS 15454 SDH Reference Manual』の付録「Network Element Defaults」を参照してください。

## 自動ネゴシエーション、フロー制御、およびフレームバッファリング

CE-100T-8 では、イーサネット リンク自動ネゴシエーションがデフォルトでオンに設定されています。また、ポートのデュプレックス モードや速度が auto になっているときもオンに設定されます。CTC のカード レベルの Provisioning タブを使用して、リンク速度、デュプレックス、およびフロー制御を手動で設定することもできます。

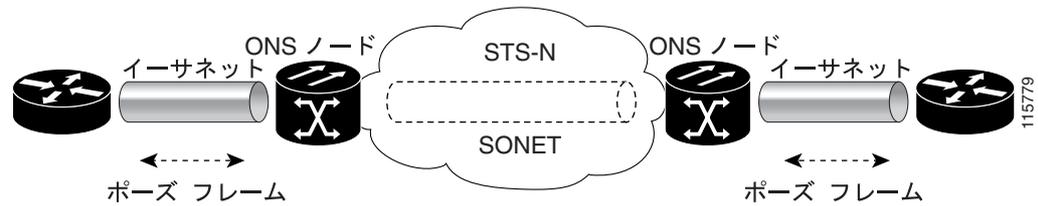
CE-100T-8 は、IEEE 802.3x フロー制御とフレームバッファリングをサポートし、データトラフィックの輻輳を緩和できます。フロー制御はデフォルトでオンに設定されています。

オーバーサブスクライブを避けるために、各ポートでバッファメモリを利用できます。イーサネット ポートのバッファメモリがキャパシティに近づくと、CE-100T-8 は IEEE 802.3x のフロー制御を使用して、接続されているイーサネット装置にポーズフレームを送信します。フロー制御と自動ネゴシエーション フレームは、ファストイーサネット インターフェイスおよび接続されているイーサネット装置に対してローカルです。これらのフレームは、POS ポートを経由して送信されません。

CE-100T-8 カードには対称フロー制御機能があります。この機能により、接続されているイーサネット装置とフロー制御を自動ネゴシエーションする際に、対称フロー制御が提案されます。対称フロー制御により、CE-100T-8 カードは、外部装置から送信されたポーズフレームに応答し、ポーズフレームを外部装置に送信できます。

ポーズフレームは、送信元に一定期間パケットの送信を停止するように指示します。送信側のステーションは、要求された時間が経過してから、残りのデータを送信します。図 24-2 は、CE-100T-8 カードと接続されているスイッチで送受信されているポーズフレームを示しています。

図 24-2 フロー制御



このフロー制御メカニズムでは、送受信装置のスループットが、STS 回線の帯域幅のスループットと一致します。たとえば、1 台のルータが CE-100T-8 カード上のイーサネット ポートに送信を行うとします。この特定のデータ レートは 51.84 Mbps を超える場合がありますが、CE-100T-8 ポートに割り当てられている SONET 回線は STS-1 (51.84 Mbps) のみです。この例では、CE-100T-8 はポーズ フレームを送信し、ルータからの送信を一定期間遅らせるように要求します。フロー制御と十分なポート単位のバッファリング機能を使用すると、フレーム損失の大部分を制御できるため、回線 レートの最大容量(STS-1)未満でプロビジョニングされる、専用回線サービスが効率良く行えます。

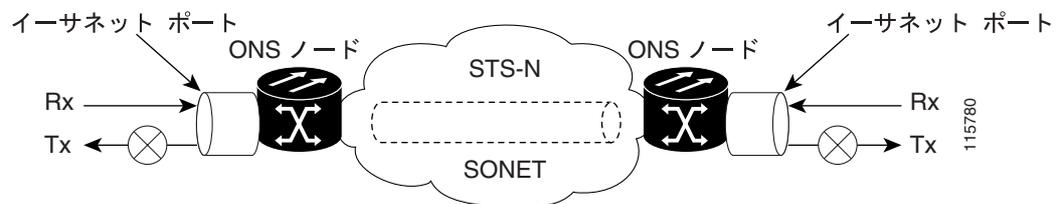
## イーサネット リンク完全性のサポート

CE-100T-8 は、エンドツーエンドのイーサネット リンク完全性をサポートします (図 24-3)。この機能は、イーサネット専用回線サービスの提供と、接続されているイーサネット装置でのレイヤ 2 およびレイヤ 3 プロトコルの適切な運用に不可欠です。

エンドツーエンドのイーサネット リンク完全性では、エンドツーエンドのパスの一部に障害が発生すると、パス全体で障害が発生したことになります。リモートイーサネット ポートが SONET/SDH ネットワーク上で転送できない場合、またはリモートイーサネット ポートが無効な場合には、CE-100T-8 カードのイーサネット ポートが無効になります。

パス全体の障害は、パスの各端にある送信ペアがオフになっていることで確認できます。接続されているイーサネット装置は、ディセーブルになった送信ペアを搬送波損失と認識し、その結果非アクティブリンクまたはリンク障害とみなします。

図 24-3 エンドツーエンドのイーサネット リンク完全性のサポート



(注)

搬送波損失状態を無視するように設定できるネットワーク装置もあります。搬送波損失状態を無視するように設定された装置が一方の端で CE-100T-8 カードに接続されている場合は、障害を回避してトラフィックをルーティングするために代替方法 (レイヤ 2 またはレイヤ 3 のキープアライブメッセージの使用など) を用意する必要があります。通常、このような代替方法の応答時間は、エラー状態の識別にリンク状態を使用する方法よりもかなり長くなります。

## イーサネット ポートおよび SONET/SDH ポートの管理状態とサービス状態およびソーク時間

CE-100T-8 カードは、イーサネット ポートおよび SONET/SDH 回線の管理状態とサービス状態をサポートします。カードと回線のサービス状態の詳細については、『Cisco ONS 15454 Reference Manual』または『Cisco ONS 15454 SDH Reference Manual』の付録「Administrative and Service States」を参照してください。

イーサネット ポートには、In-Service, Automatic In-service ( IS,AINS ) 管理状態を含む、ESM サービス状態を設定できます。IS, AINS は、ポートを最初に Out-of-Service and Autonomous, Automatic In-Service ( OOS-AU,AINS ) 状態に設定します。このサービス状態では、アラーム レポートは抑制されますが、トラフィックは伝送され、ループバックは許可されます。ソーク期間が終了すると、ポートの状態が In-Service and Normal ( IS-NR ) に変わります。アラームがレポートされるかどうかに関係なく、発生した障害状態は、CTC の Conditions タブまたは TL1 の RTRV-COND コマンドを使用して取得できます。

イーサネット ポートのアラームおよび状態である、CARLOSS および TPTFAIL の 2 つは、ポートが稼動中になるのを防ぎます。アラーム レポートが抑制されている場合でも、イーサネット ポートが IS,AINS 状態に設定されて CE-100T-8 回線がプロビジョニングされているときに、これが発生します。これは、CE-100T リンク完全性機能がアクティブで、パス上のすべての SONET およびイーサネット エラーが解決されるまで両端でリンクがイネーブルにならないようになっているからです。リンク完全性機能によりエンドツーエンドパスがダウンした状態にある限り、両方のポートの状態は、AINS から IS への変更を抑制するために必要な 2 つの状態のうちの少なくとも 1 つになります。したがって、ポートは AINS 状態のままとなり、アラーム レポートが抑制されます。

また、ESM は CE-100T-8 カードの SONET/SDH 回線にも適用されます。SONET/SDH 回線の状態が IS,AINS に設定されて、回線状態が IS に変わる前にイーサネット エラーが発生した場合、イーサネット エラーが両端で解決されるまで、リンク完全性は回線の状態が IS に変わるのも防止します。管理状態が IS,AINS である限り、サービス状態は OOS-AU,AINS となります。イーサネット エラーまたは SONET エラーがなくなると、リンク完全性機能が両端でイーサネット ポートをイネーブルにします。同時に、AINS カウントダウンが通常どおりに開始されます。経過時間中に別の状態が発生しない場合は、各ポートの状態が IS-NR 状態に変わります。AINS カウントダウン中、ソーク時間の残り時間が CTC および TL1 で使用できます。ソーク期間に状態が再度発生すると、AINS ソーキング ロジックが最初から再開します。

IS,AINS 状態にプロビジョニングされた SONET/SDH 回線は、回線の両端のイーサネット ポートの状態が IS-NR に変わるまで最初の Out-of-Service ( OOS ) 状態のままです。AINS から IS への変更が完了するかどうかに関係なく、リンク完全性機能によりイーサネット ポートがオンになると、SONET/SDH 回線はイーサネット トラフィックを転送し統計情報をカウントします。

## IEEE 802.1Q CoS および IP ToS キューイング

CE-100T-8 は、優先キューイングを行うための IEEE 802.1Q Class of Service ( CoS; サービス クラス ) スレッシュホールドおよび IP Type of Service ( ToS; サービス タイプ ) ( IP Differentiated Services Code Point [DSCP] ) スレッシュホールドを参照しています。CE-100T-8 の CoS スレッシュホールドおよび ToS スレッシュホールドは、ポート レベルごとにプロビジョニングします。これにより、ユーザは、CE-100T-8 に接続されているデータ ネットワークの既存のオープンスタンダード Quality of Service ( QoS; サービス品質 ) 方式に基づくプライオリティ処理を提供できます。QoS 処理は、イーサネット ポートと POS ポートの両方に適用されます。

設定されているスレッシュホールドを超えるプライオリティの packets またはフレームはプライオリティ トラフィックとして処理されます。このプライオリティ トラフィックは、通常のキューではなく、プライオリティ キューに送信されます。バッファリングが発生すると、プライオリティ

キューの packets が、通常のキューの packets よりも優先されます。その結果、Voice over IP (VoIP) など、遅延に影響されやすいトラフィックなどのプライオリティトラフィックが低遅延となります。

これらのプライオリティは個別のキューに置かれるため、優先キューイング機能は、レートベースの CIR/EIR マーク付けされたトラフィックの分離には使用しないでください (メトロイーサネットサービスプロバイダーのエッジでときどき行われます)。その結果、同じアプリケーションの packets が順序正しく配信されなくなることがあります。これは、一部のアプリケーションではパフォーマンスの問題の原因になります。

IP ToS タグ付き packets の場合、CE-100T-8 は IP ToS で指定されている 256 のプライオリティのいずれもプライオリティまたはベストエフォートにマップします。CTC の **Provisioning > Ether Ports** タブを使用してカードレベルビューで別の ToS を設定できます。CTC で指定された ToS クラスより高い ToS クラスは、できるだけ遅延を発生させないキューであるプライオリティキューにマップされます。デフォルトでは、ToS は最高値の 255 に設定されます。その結果、デフォルトではすべてのトラフィックが同じプライオリティで処理されます。

表 24-3 に、IP ToS 設定例でプライオリティキューにマップされる値を示します (ToS 設定の範囲は 0 ~ 255 ですが、一部の設定のみを示しています)。

表 24-1 IP ToS プライオリティ キューのマッピング

CTC での ToS 設定	プライオリティ キューに送信される ToS 値
255 (デフォルト)	なし
250	251 ~ 255
150	151 ~ 255
100	101 ~ 255
50	51 ~ 255
0	1 ~ 255

CoS タグ付きフレームの場合、CE-100T-8 は CoS で指定されている 8 のプライオリティをプライオリティまたはベストエフォートにマップできます。CTC の **Provisioning > Ether Ports** タブを使用してカードレベルビューで別の CoS を設定できます。CTC で指定された CoS クラスより高い CoS クラスは、できるだけ遅延を発生させないキューであるプライオリティキューにマップされます。デフォルトでは、CoS が最高値の 7 に設定されます。その結果、デフォルトではすべてのトラフィックが同じプライオリティで処理されます。

表 24-3 に、CoS 設定でプライオリティキューにマップされる値を示します。

表 24-2 CoS プライオリティ キューのマッピング

CTC での CoS 設定	プライオリティ キューに送信される CoS 値
7 (デフォルト)	なし
6	7
5	6、7
4	5、6、7
3	4、5、6、7
2	3、4、5、6、7
1	2、3、4、5、6、7
0	1、2、3、4、5、6、7

VLAN タグなしのイーサネット フレームは、ToS および CoS 優先キューイングの両方がカードでアクティブな場合、ToS ベースの優先キューイングを使用します。CE-100T-8 カードで CoS および ToS 優先キューイングをアクティブにするには、カードの ToS 設定は 255 (デフォルト) より小さく、CoS 設定は 7 (デフォルト) より小さくする必要があります。ToS 設定が 255 (デフォルト) の場合には ToS 優先キューイングがディセーブルになるため、この場合には CoS 設定が使用されません。

VLAN タグ付きのイーサネット フレームは、ToS および CoS 優先キューイングの両方がカードでアクティブな場合、CoS ベースの優先キューイングを使用します。ToS 設定は無視されます。CoS 設定が 7 (デフォルト) の場合には CoS ベースの優先キューイングがディセーブルになるため、この場合には ToS 設定が使用されます。

CE-100T-8 カードの ToS 設定が 255 (デフォルト) で CoS 設定が 7 (デフォルト) の場合、カードで優先キューイングがアクティブでなくなり、データはデフォルトの通常のトラフィック キューに送信されます。CE-100T-8 カードに送られるデータに ToS 値や CoS 値がタグ付けされていない場合にも、データはデフォルトの通常のトラフィック キューに送信されます。

**(注)**

CE-100T-8 でフロー制御がイネーブル (デフォルト) に設定されている場合、優先キューイングは効果がありません。フロー制御がイネーブルの場合に、6 キロバイトの単一プライオリティ First-in first-out (FIFO; 先入れ先出し) パッファが満たされると、ポーズ フレームが送信されます。その結果、パケット順序のプライオリティは、フロー制御のポーズ フレームを受信してバッファリングを行う外部装置の責任となります。

**(注)**

CE-100T-8 で STS-3C 回線がプロビジョニングされている場合、優先キューイングは効果がありません。STS-3c 回線はファスト イーサネットよりもデータ容量が大きいため、CE-100T-8 バッファリングは必要ありません。優先キューイングはバッファリングの際にのみ影響します。

## RMON および SNMP のサポート

CE-100T-8 カードには、ネットワーク オペレータが Network Management System (NMS; ネットワーク管理システム) でネットワークの状態をモニタリングできる Remote Monitoring (RMON) 機能があります。CE-100T-8 は ONG RMON を使用します。ONG RMON には、標準 RMON MIB からの統計情報、履歴、アラーム、イベント MIB (管理情報ベース) グループが含まれます。RMON スレッシュホールドのプロビジョニングにアクセスするには、TL1 または CTC を使用します。CTC での RMON スレッシュホールドのプロビジョニングについては、『Cisco ONS 15454 Procedure Guide』 (NTP-A279) および『Cisco ONS 15454 Troubleshooting Guide』、または『Cisco ONS 15454 SDH Procedure Guide』 および『Cisco ONS 15454 SDH Troubleshooting Guide』を参照してください。

## 統計情報およびカウンタ

CE-100T-8 のイーサネット統計情報および POS 統計情報は、**Performance > Ether Ports** または **Performance > POS Ports** を選択してすべて表示できます。

## CE-100T-8 の SONET/SDH 回線および機能

CE-100T-8 には 1 ~ 8 の番号が付いた POS ポートが 8 基装備されています。ポートの番号は CTC または TL1 で管理できます。各 POS ポートは対応するイーサネット ポートに静的にマップされます。カードレベルの **Provisioning > POS Ports** タブをクリックして、管理状態、フレーミングタイプ、およびカプセル化タイプを設定できます。カードレベルの **Performance > POS Ports** タブをクリックして、POS ポートの統計情報、利用率、および履歴を表示できます。

### 利用可能な回線サイズと組み合わせ

各 POS ポートは、独立した Contiguous Concatenation (CCAT) または Virtual Concatenation (VCAT; パーチャル コンカチネーション) 回線を終端します。イーサネット以外のラインカードに対して SONET/SDH 回線を作成するのと同じように、CTC または TL1 を使用してこれらのポートに対して SONET/SDH 回線を作成します。表 24-3 および 表 24-4 に、CE-100T-8 で利用可能な回線サイズを示します。

表 24-3 ONS 15454 の CE-100T-8 でサポートされている SONET 回線サイズ

CCAT	VCAT 高次	VCAT 低次
STS-1	STS-1-1v	VT1.5- <i>n</i> V (n= 1 ~ 64)
STS-3c	STS-1-2v	
	STS-1-3v	

表 24-4 ONS 15454 SDH の CE-100T-8 でサポートされている SDH 回線サイズ

CCAT	VC-3 VCAT	VC-12 VCAT
VC-3	VC-3-1v	VC-12- <i>n</i> V (n= 1 ~ 63)
VC-4	VC-3-2v	
	VC-3-3v	

1 本の回線の最大スループットは 100 Mbps になります。この最大スループットは、155 Mbps の帯域幅を持つより大きな STS-3c または VC-4 回線がプロビジョニングされた場合でも同様です。これは、ファストイーサネットポートのハードウェア制限によるものです。また、VCAT 回線も同様に制限されます。表 24-5 に、ワイヤスピードのサービスの配信に必要な最小 SONET 回線サイズを示します。

表 24-5 イーサネット速度に対する最小 SONET 回線サイズ

イーサネット ワイヤ スピード	CCAT 高次	VCAT 高次	VCAT 低次
回線レート 100BASE-T	STS-3c	STS-1-3v、STS-1-2v <sup>1</sup>	VT1.5- <i>x</i> V (x=56 ~ 64)
サブレート 100BASE-T	STS-1	STS-1-1v	VT1.5- <i>x</i> V (x=1 ~ 55)
回線レート 10BASE-T	STS-1	適用されない	VT1.5-7v
サブレート 10BASE-T	適用されない	適用されない	VT1.5- <i>x</i> V (x=1 ~ 6)

1. STS-1-2v は合計で 98 Mbps の転送容量を提供します。

表 24-6 に、10 Mbps および 100 Mbps ワイヤ スピード サービスに必要な最小 SDH 回線サイズを示します。

表 24-6 SDH 回線サイズおよびイーサネット サービス

イーサネット ワイヤ スピード	CCAT	VC-3 VCAT	VC-12 VCAT
回線レート 100BASE-T	VC-4	VC-3-3v、VC-3-2v <sup>1</sup>	VC-12-xv (x=50 ~ 63)
サブレート 100BASE-T	VC-3	VC-3-1v	VC-12-xv (x=1 ~ 49)
回線レート 10BASE-T	VC-3	VC-3-1v	VC-12-5v
サブレート 10BASE-T	適用されない	適用されない	VC-12-xv (x=1 ~ 4)

1. VC-3-2v は合計で 98 Mbps の転送容量を提供します。

CE-100T-8 での使用可能な回線数と合計の帯域幅は、設定する回線サイズの組み合わせによって異なります。表 24-7 に、ONS 15454 の CE-100T-8 で使用可能な CCAT 高次回線サイズの組み合わせを示します。

表 24-7 SONET の CCAT 高次回線サイズの組み合わせ

STS-3c 回線の数	STS-1 回線の最大数
なし	8
1	7
2	6
3	3
4	なし

表 24-8 に、ONS 15454 SDH の CE-100T-8 で使用可能な CCAT 高次回線サイズの組み合わせを示します。

表 24-8 SDH の CCAT 高次回線サイズの組み合わせ

VC-4 回線の数	VC-3 回線の最大数
なし	8
1	7
2	6
3	3
4	なし

表 24-9 に、ONS 15454 の CE-100T-8 で使用可能な VCAT 高次回線サイズの組み合わせを示します。

表 24-9 STS-1-3v および STS-1-2v SONET の VCAT 高次回線の組み合わせ

STS-1-3v 回線の数	STS-1-2v 回線の最大数
なし	4
1	3
2	2
3	1
4	なし

表 24-10 に、ONS 15454 SDH の CE-100T-8 で使用可能な VC-3-3v および VC-3-2v 回線サイズの組み合わせを示します。

表 24-10 SDH の VC-3-3v および VC-3-2v の VCAT 回線の組み合わせ

VC-3-3v 回線の数	VC-3-2v 回線の最大数
なし	4
1	3
2	2
3	1
4	なし

CCAT 高次、VCAT 高次、および VCAT 低次回線を組み合わせることができます。CE-100T-8 は、最大 8 本の低次 VCAT 回線をサポートします。

使用可能な SONET 回線サイズは VT1.5- $X$ v です。 $X$  の範囲は 1 ~ 64 です。最大の低次 VCAT SONET 回線サイズ VT1.5-64v では、最大で 4 本の回線が利用できます。表 24-11 に、SONET における最大密度でのサービスの組み合わせについて詳細に説明します。

使用可能な SDH 回線サイズは VC-12- $X$ v です。 $X$  の範囲は 1 ~ 63 です。最大の低次 VCAT SDH 回線サイズ VC-12-63v では、最大で 4 本の回線が利用できます。表 24-12 に、SDH における最大密度でのサービスの組み合わせについて詳細に説明します。

表 24-11 SONET の CE-100T-8 サービス密度の実例

サービスの組み合わせ	STS-3c または STS-1-3v	STS-1-2v	STS-1	VT1.5-xV	アクティブなサービスの数
1	4	0	0	0	4
2	3	1	1	0	5
3	3	0	3	0	6
4	3	0	0	$4(x=1 \sim 21)^1$	7 <sup>1</sup>
5	2	2	2	0	6
6	2	1	4	0	7
7	2	1	1	$4(x=1 \sim 21)^1$	8 <sup>1</sup>
8	2	0	6	0	8
9	2	0	3	$3(x=1 \sim 28)$	8
10	2	0	0	$6(x=1 \sim 28)$	8
11	1	3	3	0	7
12	1	2	5	0	8
13	1	2	2	$3(x=1 \sim 28)$	8
14	1	1	1	$5(x=1 \sim 28)$	8
15	1	0	7	0	8
16	1	0	3	$4(x=1 \sim 42)$	8
17	1	0	0	$7(x=1 \sim 42)$	8
18	0	4	4	0	8
19	0	3	3	$2(x=1 \sim 42)$	8
20	0	0	8	0	8

表 24-11 SONET の CE-100T-8 サービス密度の実例 ( 続き )

サービスの組み合わせ	STS-3c または STS-1-3v	STS-1-2v	STS-1	VT1.5-xV	アクティブなサービスの数
21	0	0	4	4 ( x=1 ~ 42 )	8
22	0	0	0	8 ( x=1 ~ 42 )	8

- この低次 VCAT 回線の組み合わせは、カード上に作成された最初の 2 本の回線のどちらかが低次 VCAT 回線の場合に実現できます。カード上に作成された最初の 2 本の回線が高次 VCAT または CCAT 回線の場合、最大で 3 本の低次 VCAT 回線がカード上で作成できます。

表 24-12 SDH の CE-100T-8 サービス密度の例

サービスの組み合わせ	VC-4 または VC-3-3v	VC-3-2v	VC-3	VC-12-xv	アクティブなサービスの数
1	4	0	0	0	4
2	3	1	1	0	5
3	3	0	3	0	6
4	3	0	0	3 ( x=1 ~ 21 )	6
5	2	2	2	0	6
6	2	1	4	0	7
7	2	1	1	3 ( x=1 ~ 21 )	7 <sup>1</sup>
8	2	0	6	0	8
9	2	0	3	3 ( x=1 ~ 21 )	8
10	2	0	0	6 ( x=1 ~ 21 )	8
11	1	3	3	0	7
12	1	2	5	0	8
13	1	2	2	3 ( x=1 ~ 21 )	8 <sup>1</sup>
14	1	1	1	5 ( x=1 ~ 21 )	8 <sup>1</sup>
15	1	0	7	0	8
16	1	0	3	2 ( x=1 ~ 32 ) および 2 ( x=1 ~ 31 )	8
17	1	0	0	7 ( x=1 ~ 28 )	8
18	0	4	4	0	8
19	0	3	3	1 ( x=1 ~ 32 ) および 1 ( x=1 ~ 31 )	8
20	0	0	8	0	8
21	0	0	4	2 ( x=1 ~ 32 ) および 2 ( x=1 ~ 31 )	8
22	0	0	0	4 ( x=1 ~ 32 ) および 4 ( x=1 ~ 31 )	8

- これらのサービスの組み合わせでは、VC-3 回線を作成する前に VC-12-xv 回線を作成する必要があります。

## CE-100T-8 プール

CE-100T-8 回線の合計容量は、4 つのプールに分けられます。各プールの最大容量は、SONET の場合 STS-1 が 3 本で、SDH の場合 VC-3 が 3 本です。

### STS/VT 割り当てタブまたは VC4/VC LO 割り当てタブでの CE-100T-8 プール情報の表示

CTC のカード レベル ビューのメンテナンスタブで、ONS 15454 SONET の STS/VT 割り当てタブおよび ONS 15454 SDH の VC4/VC LO 割り当てタブに、プロビジョニングされた回線が 4 つのプールをどのように実装するかが表示されます。いずれの画面でも、POS Port テーブルの行には、各ポートごとに 3 つのカラムが表示されます。各行には、ポート番号、回線サイズとタイプ、帯域幅を使用するプールが表示されます。Pool Utilization テーブルは 4 つのカラムで構成され、プール番号、そのプールでの回線タイプ、使用されているプール容量、および追加容量が使用可能かどうかを表示します。

図 24-4 にタブの SDH バージョンを、図 24-5 にタブの SONET バージョンを示します。

図 24-4 SDH の CE-100T-8 割り当てタブ

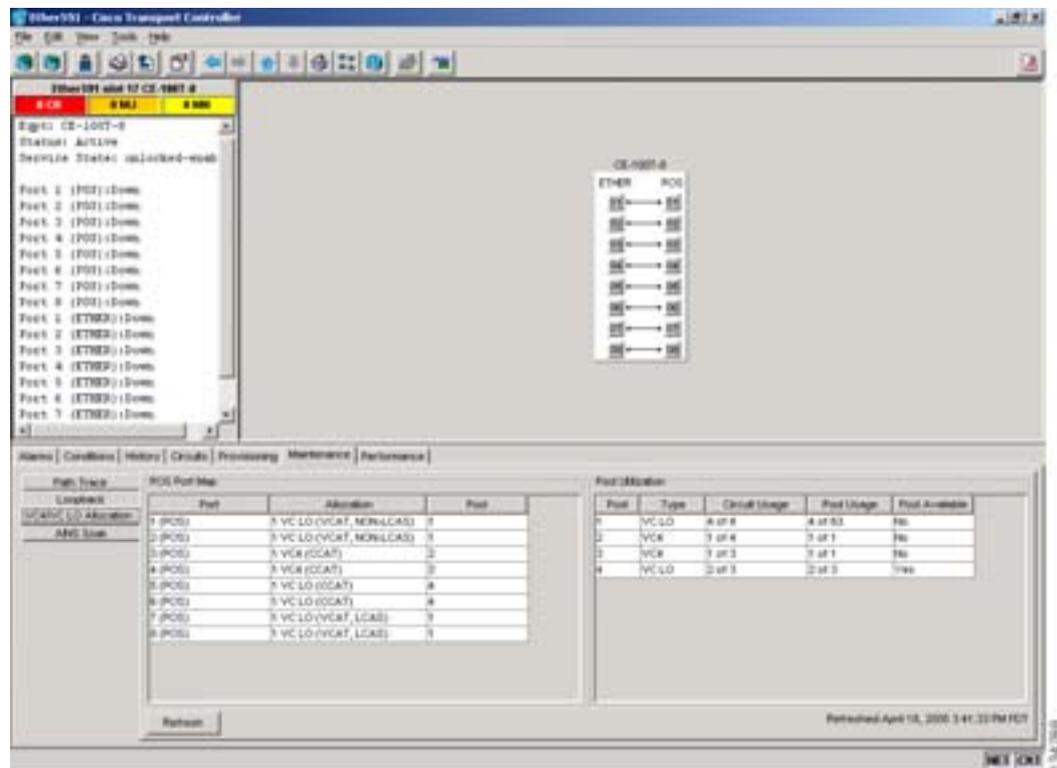
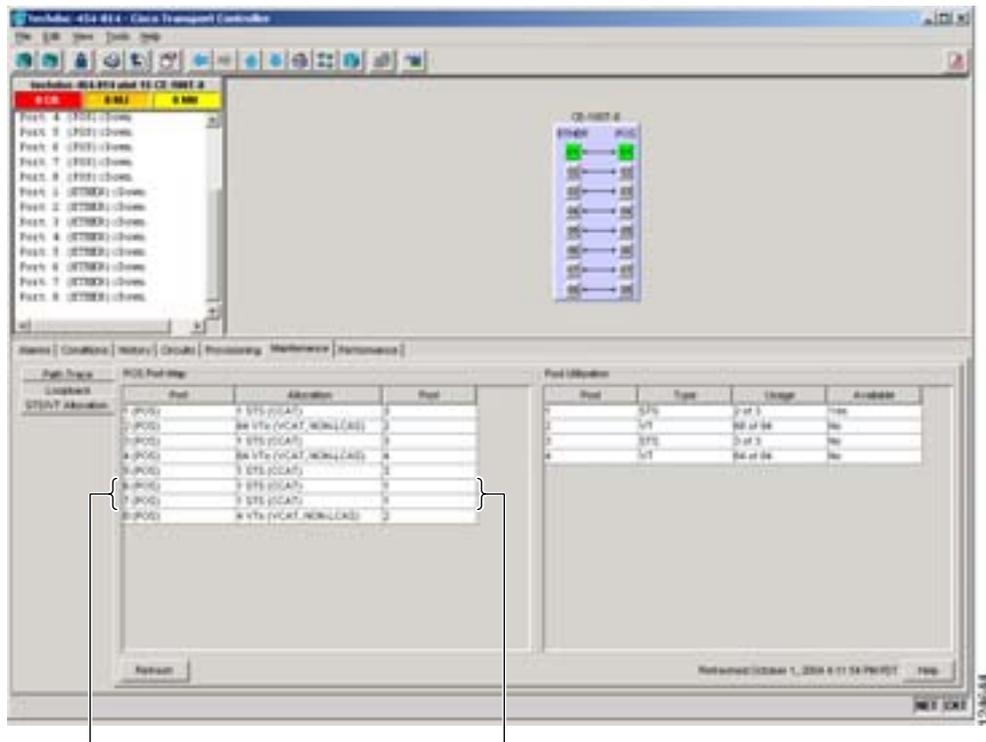


図 24-5 CE-100T-8 の STS/VT 割り当てタブ



ポート 6 とポート 7 は  
両方ともプール 1 に所属

## CE-100T-8 プール割り当ての例

回線のプロビジョニングのために 1 つのプールに十分な容量がない場合には、その回線のプロビジョニングに必要な帯域幅を解放するのにこの情報が役立ちます。4 つのプールのなかの既存の回線の配分を表示して、該当の回線のために帯域幅を解放するのに削除する必要のある回線を決定できます。

たとえば、図 24-5 に示すように、SONET CE-100T-8 カードで STS-3c または STS-1-3v をプロビジョニングする必要がある場合、STS-3c または STS-1-3v に相当する帯域幅は 4 つのプールのいずれからでも使用可能ではありません。帯域幅を解放するために同じプールから回線を削除する必要があります。帯域幅が使用可能でも複数のプール間で散在している場合、回線はプロビジョニングできません。POS Port Map テーブルを参照すると、どの回線がどのプールに属するかがわかります。図 24-5 の Pool カラムと Port カラムには、ポート 6 およびポート 7 は両方ともプール 1 を使用しており、他の回線はプール 1 を使用していないことが表示されています。これらの 2 つの STS-1 回線を削除すると、単一のプールから STS-3c または STS-1-3v に相当する帯域幅が解放されます。

削除する回線をテーブルの情報から決定しない場合、ポート 3、ポート 5、およびポート 6 の STS-1 回線を削除することが考えられます。この場合、STS-3c または STS-1-3v に相当する帯域幅が解放されますが、必要な帯域幅が単一のプールから得られないため、STS-3c または STS-1-3v 回線をプロビジョニングできません。

## CE-100T-8 プール プロビジョニング規則

すべての VCAT 回線メンバーは同じプールからのメンバーである必要があります。3 個のプールに高次回線をサポートするのに十分な帯域幅が存在する場合には、4 個のメモリ プールの内の 1 つは低次 VCAT 回線用に予約されます。高次 CCAT 回線は、単一のメモリ プールから使用可能なすべての容量を使用してから、新しいプールの容量を使用します。要求された回線サイズをサポートするのに十分な帯域幅がメモリ プールにある場合には、それらのプールが代わりに最初の 3 本の高次 VCAT 回線に割り当てられます。余分な帯域幅を防ぐために、最初に高次 VCAT 回線をプロビジョニングしてこれらの回線を平等に分配します。

## CE-100T-8 の VCAT の特性

ML-100T-8 カードおよび CE-100T-8 カード (ONS 15310-CL バージョンおよび ONS 15454 SONET/SDH バージョンの両方) は、ITU-T G.7042 規格の Link Capacity Adjustment Scheme (LCAS; リンク キャパシティ調整方式) がハードウェア ベースでサポートされています。このサポートにより、VCG の他のメンバーに影響を与えることなく (エラーなしで) CTC または TL1 を使用して高次および低次 VCAT 回線サイズを動的に変更できます。

ONS 15454 SONET/SDH ML シリーズ カードには、Software-based LCAS (SW-LCAS; ソフトウェアベースの リンク キャパシティ調整方式) があります。この方式は、ML-100T-8 カードおよび CE-100T-8 カード (ONS 15310-CL バージョンおよび ONS 15454 SONET/SDH バージョンの両方) でもサポートされていますが、反対側が ONS 15454 SONET/SDH ML シリーズ カードで終端されている回線でのみサポートされます。

CE-100T-8 カードでは、VCAT 回線の各メンバーに対して独立したルーティングおよび保護優先を行うことができます。完全に保護されているまたは保護されていない、または Protection Channel Access (PCA) (PCA が使用可能な場合) を使用する VCAT 回線の容量の合計を制御することもできます。アラームは、Virtual Concatenation Group (VCG) ごとだけでなく、メンバーごとにサポートされています。



(注)

CE-100T-8 の最大許容 VCAT 遅延差は 48 ミリ秒です。VCAT 遅延差は、VCG メンバー間の相対的な到着時間を計算したものです。

## CE-100T-8 の POS カプセル化、フレーム化、および CRC

CE-100T-8 は Cisco EoS LEX (LEX) を使用します。LEX は ONS イーサネット カードの基本カプセル化方式です。このカプセル化では、プロトコル フィールドは、Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) の Request For Comments (RFC; コメント要求) 1841 で規定された値に設定されます。ユーザは、Frame-mapped Generic Framing Procedure (GFP-F) フレーミング (デフォルト) または High-Level Data Link Control (HDLC; ハイレベル データリンク制御) フレーミングをプロビジョニングできます。GFP-F フレーミングでは、32 ビット CRC (デフォルト) または CRC なし (なし) も設定できます。GFP-F 上で LEX が使用される場合、LEX は ITU-T G.7041 に基づいた GFP-F 上の標準マップ イーサネットです。HDLC フレーミングは設定済み 32 ビット CRC を提供します。カプセル化、フレーム化、および CRC の情報を含め、ONS イーサネット カードの相互運用性の詳細については、「ONS イーサネット カード上の POS」の章を参照してください。

CE-100T-8 カードは GFP-F のヌル モードをサポートします。GFP-F の CMF はカウントされてから廃棄されます。

## CE-100T-8 のループバック、J1 パス トレース、および SONET/SDH アラーム

CE-100T-8 カードは、ターミナル ループバックとファシリティ ループバックをサポートします。また、OC-N カードと同様の方法で SONET/SDH アラームをレポートし、J1 パス トレース バイトを転送およびモニタリングします。次のパス 終端機能がサポートされています。

- H1 および H2 連結表示
- C2 信号ラベル
- Bit Interleaved Parity 3 (BIP-3; ビット インターリーブド パリティ 3) 生成
- G1 パス ステータス表示
- C2 パス 信号ラベルの読み取り / 書き込み
- Loss Of Pointer (LOP; ポインタ 損失)、未実装、ペイロード 不一致、Alarm Indication Signal (AIS; アラーム 表示 信号) 検出、および Remote Defect Indication (RDI; リモート 障害 表示) を含む、パス レベルのアラームと条件
- 高次 CCAT パスの J1 パス トレース
- メンバー レベルでの高次 VCAT 回線の J2 パス トレース
- メンバー レベルでの低次 VCAT 回線の J2 パス トレース
- 低次パスの拡張信号ラベル





## CE-1000-4 イーサネットの動作

---

この章では、Cisco ONS 15454 および Cisco ONS 15454 SDH でサポートされている CE-1000-4 (キャリア イーサネット) カードの動作について説明します。ONS 15454 SONET に取り付けられた CE-1000-4 カードは SONET 動作にのみ限定されていて、ONS 15454 SDH に取り付けられた CE-1000-4 カードは SDH 動作にのみ限定されます。

CE-1000-4 カードをプロビジョニングするには、Cisco Transport Controller (CTC) または Transaction Language One (TL1) を使用します。Cisco IOS は、CE-1000-4 カードではサポートされていません。

イーサネットカードの仕様については、『*Cisco ONS 15454 Reference Manual*』または『*Cisco ONS 15454 SDH Reference Manual*』を参照してください。イーサネットカードの回線の詳細な設定手順については、『*Cisco ONS 15454 Procedure Guide*』または『*Cisco ONS 15454 SDH Procedure Guide*』を参照してください。TL1 プロビジョニング コマンドについては、『*Cisco ONS SONET TL1 Command Guide*』または『*Cisco ONS SDH TL1 Command Guide*』を参照してください。

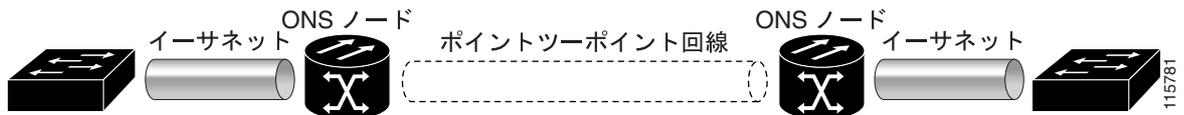
この章では、次の内容について説明します。

- [CE-1000-4 の概要 \(p.25-2\)](#)
- [CE-1000-4 イーサネットの機能 \(p.25-3\)](#)
- [CE-1000-4 の SONET/SDH 回線および機能 \(p.25-7\)](#)

## CE-1000-4 の概要

CE-1000-4 は、4 個のギガビット イーサネット ポートを備えたレイヤ 1 マッパー カードです。このカードは、各ポートをポイントツーポイント設定で一意的 SONET 回線にマップします。図 25-1 に、CE-1000-4 のアプリケーション例を示します。この例では、スイッチのギガビット イーサネット ポートからのデータトラフィックがポイントツーポイント回線を經由して別のスイッチのギガビット イーサネット ポートに伝送されます。

図 25-1 CE-1000-4 のポイントツーポイント回線



CE-1000-4 カードを使用して、従来の SONET/SDH 回線のように、イーサネット専用回線サービスを提供して管理できます。CE-1000-4 カードは、キャリアクラスのイーサネット専用回線サービスおよびハイアベイラビリティ転送を提供します。

CE-1000-4 カードは、イーサネット上でカプセル化と転送が可能な任意のレイヤ 3 プロトコル (IP や IPX など) を伝送します。データネットワークからのイーサネット フレームは、CE-1000-4 カード上の GBIC (ギガビット インターフェイス コンバータ) に送信されます。CE-1000-4 カードは、Packet-over-SONET/SDH (POS) カプセル化を使用して SONET/SDH ペイロードにイーサネット フレームを透過的にマップします。次に、カプセル化されたイーサネットを持つ POS 回線は、他の SONET Synchronous Transport Signal (STS; 同期転送信号) や SDH Synchronous Transport Mode (STM; 同期転送モード) と同じように、光カードに多重化されます。ペイロードが宛先ノードに達すると、逆のプロセスが行われ、宛先の CE-1000-4 カードの GBIC からデータネットワークのイーサネット ヘッダが送信されます。POS プロセスについては第 20 章「ONS イーサネット カード上の POS」を参照してください。

CE-1000-4 カードは、ITU-T G.707 および Telcordia GR-253 ベースの規格をサポートします。このカードではソフトリセットが可能で、エラーが発生しません。ソフトリセット中にプロビジョニングが変更された場合、またはソフトウェアのアップグレード中にファームウェアが置き換えられた場合は、エラーとなることがあります。この場合、リセットはハードリセットと同じになります。CTC を使用した CE-1000-4 カードでソフトリセットを実行するには、『Cisco ONS 15454 Procedure Guide』または『Cisco ONS 15454 SDH Procedure Guide』を参照してください。

## CE-1000-4 イーサネットの機能

CE-1000-4 カードには、ギガビットイーサネット用に標準 GBIC コネクタを使用するフロントエンドイーサネットポートが4つ装備されています。イーサネットポート1～4の各ポートは、対応する番号のPOSポートにそれぞれマップされます。これらのイーサネットポートは、ダイジチェーン接続できます。

イーサネットポートレベルでは、次の特性を設定できます。

- ポート名
- 管理状態
- Automatic In-Service (AINS) ソーク時間
- フロー制御
- フロー制御の水準点
- 自動ネゴシエーション

CE-1000-4 カードは、有効なイーサネットフレームに変更を加えずに SONET/SDH ネットワークに転送します。ヘッダー内の情報は、カプセル化や転送によって影響を受けません。たとえば、IEEE 802.1Q 情報は、影響を受けずにプロセスを通過します。

CE-1000-4 は、デフォルトではイーサネットの Cyclic Redundancy Check (CRC; 巡回冗長検査) を含めて最大 10004 バイトのジャンボフレームをサポートします。CTC では、イーサネット CRC を含めて最大 1548 バイトのイーサネットフレームサイズも設定できます。



(注)

イーサネット属性の多くは、Network Element (NE; ネットワーク要素) のデフォルト機能によって利用できます。NE のデフォルト機能の詳細については、『Cisco ONS 15454 Reference Manual』または『Cisco ONS 15454 SDH Reference Manual』の付録「Network Element Defaults」を参照してください。

### 自動ネゴシエーションおよびフレームバッファリング

CE-1000-4 カードでは、イーサネットリンク自動ネゴシエーションがデフォルトでオンに設定されています。また、カードレベルの CTC の Provisioning タブを使用して、自動ネゴシエーションをイネーブルおよびディセーブルにできます。

CE-1000-4 は、Field Programmable Gate Array (FPGA) バッファリングをサポートし、データトラフィックの輻輳を緩和できます。FPGA バッファリングは、SONET/SDH オーバーサブスクライブをサポートします。バッファがキャパシティに近づくと、CE-1000-4 カードは IEEE 802.3x のフロー制御を使用して、接続されているイーサネット装置にポーズフレームを送信します。フロー制御と自動ネゴシエーションフレームは、ギガビットイーサネットインターフェイスおよび接続されているイーサネット装置に対してローカルです。これらのフレームは、POSポートを経由して送信されません。

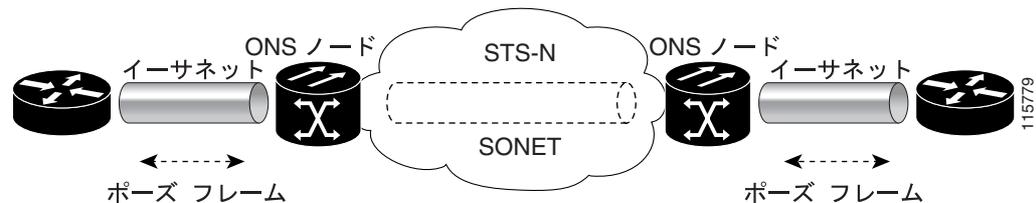
### フロー制御

CE-1000-4 カードは IEEE 802.3x フロー制御をサポートします。このカードでは、対称フロー制御と非対称フロー制御をイネーブルにし、フロー制御をディセーブルにできます。この設定は、ポートレベルの CTC で実行されます。

デフォルトでは、CE-1000-4 カードは対称フロー制御機能を使用します。この機能により、接続されているイーサネット装置とフロー制御を自動ネゴシエーションする際に、対称フロー制御のみが提案されます。対称フロー制御により、CE-1000-4 カードは、外部装置から送信されたポーズフレームに応答し、ポーズフレームを外部装置に送信できます。

ポーズフレームは、送信元に一定期間パケットの送信を停止するように指示します。送信側のステーションは、要求された時間が経過してから、残りのデータを送信します。図 25-2 は、CE-1000-4 カードと接続されているスイッチで送受信されているポーズフレームを示しています。

図 25-2 フロー制御



このフロー制御メカニズムでは、送受信装置のスループットが、STS 回線の帯域幅のスループットと一致します。たとえば、1 台のルータが CE-1000-4 カード上のギガビットイーサネットポートに送信を行うとします。この特定のデータレートは 51.84 Mbps を超える場合がありますが、CE-1000-4 ポートに割り当てられている SONET 回線は STS-1 (51.84 Mbps) のみである可能性があります。この例では、CE-1000-4 カードはポーズフレームを送信し、ルータからの送信を一定期間遅らせるように要求します。フロー制御と十分なポート単位のバッファリング機能を使用すると、フレーム損失の大部分を制御できるため、回線レートの最大容量 (STS-1) 未満でプロビジョニングされる専用回線サービスが効率良く行えます。

非対称により、CE-1000-4 はフロー制御ポーズを受信できますが、フロー制御ポーズを生成できません。このモードは、フロー制御ポーズは受信できませんが、フロー制御ポーズを送信できるリンクパートナーをサポートします。CE-1000-4 には、フロー制御ポーズを送信するモードはありますが、フロー制御ポーズを受信できません。

パススルーモードでは、送信フロー制御フレームはイーサネットインターフェイスポートによって生成されず、受信フロー制御フレームは透過的に通過します。パススルーモードは、Ethernet over SONET/SDH 転送を使用して、クライアントの間のエンドツーエンドフロー制御をサポートします。

## フロー制御のスレッショールドプロビジョニング

CE-1000-4 カードでは、フロー制御のスレッショールドプロビジョニングが可能であり、ユーザは 3 つの基準 (バッファサイズ) 設定、すなわち、デフォルト、低遅延、カスタム設定から 1 つを選択できます。デフォルトは、通常の使用に最適です。低遅延は、STS-1 での Voice-over-IP (VoIP) のようなサブプレートのアプリケーションに適しています。バッファリングが十分でない、ベストエフォートトラフィック、またはアクセスする回線が長距離である接続装置では、高遅延を設定します。

フロー制御高 (Flow Ctrl Hi) の設定は接続されているイーサネット装置に「Pause On」フレームを送るための基準であり、このフレームは装置に一時的に送信を停止させる信号を送信します。フロー制御低 (Flow Ctrl Lo) の設定は接続されているイーサネット装置に「Pause Off」フレームを送るための基準であり、このフレームは装置に送信を再開させる信号を送信します。デフォルトの水準点の設定値は、高いスレッショールドで 485、低いスレッショールドで 25 です。低遅延の水準点の設定値は、高いスレッショールドで 10、低いスレッショールドで 5 です。

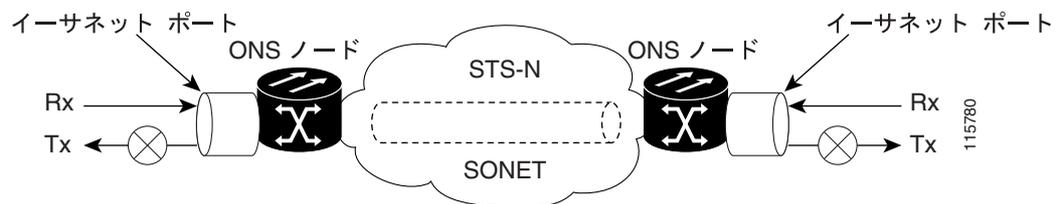
カスタム設定では、Flow Ctrl Lo および Flow Ctrl Hi に対して、1 ~ 511 の範囲の正確なバッファサイズのスレッシュホールドを両方のスレッシュホールドに設定できます。ただし、低いスレッシュホールドは高いスレッシュホールドよりも小さい値に設定する必要があります。

## イーサネット リンク完全性のサポート

CE-1000-4 は、エンドツーエンドのイーサネット リンク完全性をサポートします (図 25-3)。この機能は、イーサネット専用回線サービスの提供と、接続されているイーサネット装置でのレイヤ 2 およびレイヤ 3 プロトコルの適切な動作に不可欠です。Ethernet over SONET/SDH 接続が、接続されているイーサネット装置からのイーサネット ケーブルと同様に動作するように、リンク完全性は実行されます。

エンドツーエンドのイーサネットリンク完全性では、エンドツーエンドのパスの一部に障害が発生すると、パス全体で障害が発生します。リモート イーサネット ポートが信号を受信しないか、または遠端障害の端の近くで SONET/SDH が検出された場合、CE-1000-4 カードのイーサネットポート トランスミッタが無効になります。パス全体の障害は、パスの各端にある送信ペアがオフになっていることで確認できます。接続されているイーサネット装置は、ディセーブルになった送信ペアを搬送波損失と認識し、その結果非アクティブ リンクまたはリンク障害とみなします。ポート トランスミッタがディセーブルの場合、Transport Fail アラームも発生します。両方のイーサネットポートが信号を受信しない場合に、リンク完全性は二重の障害をサポートします。

図 25-3 エンドツーエンドのイーサネット リンク完全性のサポート



搬送波損失状態を無視するように設定できるネットワーク装置もあります。搬送波損失状態を無視するように設定された装置が一方の端で CE-1000-4 カードに接続されている場合は、障害を回避してトラフィックをルーティングするために代替方法 (レイヤ 2 またはレイヤ 3 のキープアライブメッセージの使用など) を用意する必要があります。通常、このような代替方法の応答時間は、エラー状態の識別にリンク状態を使用する方法よりもかなり長くなります。

## イーサネット ポートおよび SONET/SDH ポートの管理状態とサービス状態およびソーク時間

CE-1000-4 カードは、イーサネット ポートおよび SONET/SDH 回線の管理状態とサービス状態をサポートします。カードと回線のサービス状態の詳細については、『Cisco ONS 15454 Reference Manual』または『Cisco ONS 15454 SDH Reference Manual』の付録「Administrative and Service States」を参照してください。

イーサネット ポートには、In-Service, Automatic In-service (IS,AINS) 管理状態を設定できます。IS, AINS は、ポートを最初に Out-of-Service and Autonomous, Automatic In-Service (OOS-AU,AINS) 状態に設定します。このサービス状態では、アラーム レポートは抑制されますが、トラフィックは伝送され、ループバックは許可されます。ソーク期間が終了すると、ポートの状態が In-Service and Normal (IS-NR) に変わります。

デフォルトのソーク期間は、8 時間 0 分です。Provisioning タブ > Ether Ports タブ、または Provisioning タブ > POS Ports タブを選択して AINS ソーク期間を設定できます。Maintenance タブ > AINS Soak タブを選択して、AINS ソーク期間と IS までの残りの時間を表示できます。

アラームがレポートされるかどうかに関係なく、発生した障害状態は、CTC の Conditions タブまたは TL1 の RTRV-COND コマンドを使用して取得できます。イーサネット ポートのアラーム / 状態の CARLOSS と TPTFAIL の 2 つは、ポートが稼働するのを防ぎます。アラーム レポートが抑制されている場合でも、イーサネット ポートが IS,AINS 状態に設定されて CE-1000-4 回線がプロビジョニングされているときに、これが発生します。これは、CE-1000-4 リンク完全性機能がアクティブで、パス上のすべての SONET/SDH およびイーサネット エラーが解決されるまで両端でリンクがイネーブルにならないようになっているためです。リンク完全性機能によりエンドツーエンド パスがダウンした状態にある場合、両方のポートの状態は、AINS から IS への変更を抑制するために必要な 2 つの状態のうちの少なくとも 1 つになります。したがって、ポートは AINS 状態のままとなり、アラーム レポートが抑制されます。

また、ESM は CE-1000-4 カードの SONET/SDH 回線にも適用されます。SONET/SDH 回線の状態が IS,AINS に設定されて、回線状態が IS に変わる前にイーサネット エラーが発生した場合、イーサネット エラーが両端で解決されるまで、リンク完全性は回線の状態が IS に変わるのも防止します。管理状態が IS,AINS である限り、サービス状態は OOS-AU,AINS となります。イーサネット エラーまたは SONET エラーがなくなると、リンク完全性機能が両端でイーサネット ポートをイネーブルにします。同時に、AINS カウントダウンが通常どおりに開始されます。経過時間中に別の状態が発生しない場合は、各ポートの状態が IS-NR 状態に変わります。AINS カウントダウン中、ソーク時間の残り時間が CTC および TL1 で使用できます。ソーク期間に状態が再度発生すると、AINS ソーキング ロジックが最初から再開します。

IS,AINS 状態にプロビジョニングされた SONET/SDH 回線は、回線の両端のイーサネット ポートの状態が IS-NR に変わるまで最初の Out-of-Service (OOS) 状態のままです。AINS から IS への変更が完了するかどうかに関係なく、リンク完全性機能によりイーサネット ポートがオンになると、SONET/SDH 回線はイーサネット トラフィックを転送し統計情報をカウントします。

## RMON および SNMP のサポート

CE-1000-4 カードには、ネットワーク オペレータが Network Management System (NMS; ネットワーク管理システム) でネットワークの状態をモニタリングできる RMON 機能と SNMP (簡易ネットワーク管理プロトコル) 機能があります。CE-1000-4 は ONG RMON を使用します。ONG RMON には、標準 RMON MIB からの統計情報、履歴、アラーム、およびイベント MIB (管理情報ベース) グループが含まれます。RMON スレッシュホールドのプロビジョニングにアクセスするには、TL1 または CTC を使用します。CTC での RMON スレッシュホールドのプロビジョニングについては、『Cisco ONS 15454 Procedure Guide』または『Cisco ONS 15454 SDH Procedure Guide』を参照してください。

## 統計情報およびカウンタ

CE-1000-4 のイーサネット統計情報および POS 統計情報は、Performance > Ether Ports タブまたは Performance > POS Ports タブを選択してすべて表示できます。

## CE-1000-4 の SONET/SDH 回線および機能

CE-1000-4 には 1 ~ 4 の番号が付いた POS ポートが 4 つ装備されています。ポートの番号は CTC または TL1 で管理できます。各 POS ポートは対応するイーサネット ポートに統計的にマップされます。CE-1000-4 カードは、ONS 15454 内の互換スロットに STS-48c の総帯域幅を、または ONS 15454 SDH 内の互換スロットに STM-16 の総帯域幅を提供します。

POS ポート レベルでは、次の特性を設定できます。

- ポート名
- 管理状態
- AINS ソーク時間
- フレーミング タイプ
- カプセル化 CRC



(注)

フレーミング タイプが GFP に設定されている場合、カプセル化 CRC をオンおよびオフ (CRC ありまたは CRC なし) にできます。フレーミング タイプが High-Level Data Link Control (HDLC; ハイレベル データリンク制御) に設定されている場合、CRC は常にオンです。

カード レベルの Provisioning > POS Ports タブをクリックして、管理状態、フレーミング タイプ、カプセル化タイプを設定できます。カード レベルの Performance > POS Ports タブをクリックして、POS ポートの統計情報、利用率、履歴を表示できます。

CE-1000-4 カードの特定のサイズと互換カード スロットについては、『Cisco ONS 15454 Reference Manual』または『Cisco ONS 15454 SDH Reference Manual』の「Ethernet Cards」の章を参照してください。

## CE-1000-4 VCAT の特性

CE-1000-4 カードでは、Software Link Capacity Adjustment Scheme (SW-LCAS; ソフトウェア リンク キャパシティ 調整方式) がサポートされています。これにより、CE-1000-4 カードは ONS 15454 SONET/SDH ML シリーズ カードとの互換性を持ち、SW-LCAS もサポートします。CE-1000-4 カードでは、ハードウェア ベースの標準 LCAS がサポートされません。CE-1000-4 も SW-LCAS がイネーブルの状態では動作しません。このモードでは、ML シリーズ カードに SW-LCAS が設定されていない場合、CE-1000-4 は ONS 15454 SONET/SDH の G シリーズ カード、CE-100T-8 カード、ML シリーズ カードと互換性があります。イーサネット カードの互換性の詳細については、[第 20 章「ONS イーサネット カード上の POS」](#)を参照してください。

CE-1000-4 カードはフレキシブル VCAT グループ (VCG) と固定 (ピュアまたは非フレキシブル) VCG をサポートします。フレキシブル VCG は SW-LCAS に、固定 VCG は LCA なしに対応します。フレキシブル VCG では、CE-1000-4 は次の動作を実行できます。

- グループからメンバーを追加または削除します。
- メンバーを IS 状態または OOS 状態にします。これもグループからメンバーを追加または削除します。
- VCG からクロスコネクト回線を追加または削除します。
- グループからエラー メンバーを自動的に削除します。

VCG からメンバーを追加または削除すると、サービスに影響します。関連付けられたメンバーがグループ内に存在しない場合、クロスコネクト回線を追加または削除してもサービスに影響しません。

CE-1000-4 カードも固定 (ピュアまたは非フレキシブル) VCG をサポートします。非フレキシブル VCG では、CE-1000-4 はより制限され、次の動作のみを実行できます。

- メンバーを IS 状態または OOS 状態にします。
- メンバーに関連付けられたクロスコネクト回線を追加または削除します。

非フレキシブル VCG では、CE-1000-4 の制限事項には次が含まれます。

- グループからメンバーを追加または削除できません。
- グループからエラー メンバーを自動的に削除できません。

CE-1000-4 カードでは、VCAT 回線の各メンバーに対して独立したルーティングおよび保護優先を行うことができます。完全に保護されているまたは保護されていない、または Protection Channel Access (PCA) (PCA が使用可能な場合) を使用する VCAT 回線の容量の合計を制御することもできます。アラームは、Virtual Concatenation Group (VCG) ごとだけでなく、メンバーごとにサポートされています。

CE-1000-4 カードでは、共通ファイバでの VCAT のルーティングとスプリット ファイバ (ダイバース) での VCAT のルーティングがサポートされます。共通ファイバのルーティングは、2 ファイバ Bidirectional Line Switched Ring (BLSR; 双方向ライン スイッチ型リング) 保護方式および APS と互換性があります。これは、Unidirectional Path Switch Ring (UPSR; 単方向パス スイッチ型リング) と 4 ファイバ BLSR 保護方式はサポートしません。スプリットファイバルーティングでは、UPSR、2 ファイバ BLSR、4 ファイバ BLSR、リニア スイッチ (1+1) のすべての保護タイプがサポートされます。

VCAT スプリットファイバルーティングでは、CCAT および VCAT の共通ファイバルーティングが必要とするパスと同じパスを経由する必要はなく、SONET/SDH ネットワーク経由で各メンバーを個別にルーティングできます。これにより、ネットワーク帯域幅をより効率よく使用できます。ただし、パス長と遅延が異なるので、VCG の各メンバーの到着時間にわずかにズレが生じます。VCAT 遅延差は、VCG メンバー間の相対的な到着時間を計算したものです。CE-1000-4 カードの VCAT スプリットファイバルーティングの最大許容遅延差は、約 120 ミリ秒です。サポートされている最大遅延差を超えた場合、Loss of Alignment (アラインメント損失) アラームが生成されます。

CTC 回線設定プロセス中に、スプリットファイバルーティングを選択すると、遅延差補償機能が自動的にイネーブルになります。CCAT および VCAT の共通ファイバルーティングは、遅延差をイネーブルにしたり、サポートする必要がありません。



#### 注意

遅延差補償機能がイネーブルの場合、60 ミリ秒未満の保護スイッチは保証されません。補償時間をスイッチング時間に追加できます。



#### (注)

TL-1 の場合、スプリットファイバルーティングのサポートをイネーブルするには、EXPBUFFERS パラメータを ENT-VCG でオンに設定する必要があります。

## CE-1000-4 の POS カプセル化、フレーム化、および CRC

CE-1000-4 は Cisco EoS LEX (LEX) を使用します。LEX は ONS イーサネット カードの基本カプセル化方式です。この専用の HDLC ベースのカプセル化では、プロトコル フィールドは、Internet Engineering Task Force (IETF; インターネット技術特別調査委員会) の Request For Comments (RFC; コメント要求) 1841 で指定された値に設定されます。

ユーザは、CE-1000-4 上でフレーミングを、Frame-mapped Generic Framing Procedure (GFP-F) フレーミング (デフォルト) または HDLC フレーミングのいずれかとしてプロビジョニングできます。

GFP-F フレーミングでは、32 ビット CRC (デフォルト) または CRC なし (なし) も設定できます。GFP-F 上で LEX が使用される場合、LEX は ITU-T G.7041 に基づいた GFP-F 上の標準マップ イーサネットです。

HDLC フレーミングは設定済み 32 ビット CRC を提供します。

カプセル化、フレーム化、CRC の情報を含め、ONS イーサネット カードの相互運用性の詳細については、「[ONS イーサネット カード上の POS](#)」の章を参照してください。

## CE-1000-4 のループバック、J1 パストレース、および SONET/SDH アラーム

CE-1000-4 カードは、ターミナルループバックとファシリティループバックをサポートします。また、OC-N カードと同様の方法で SONET/SDH アラームをレポートし、J1 パストレース バイトを転送およびモニタリングします。次のパス終端機能がサポートされています。

- H1 および H2 連結表示
- Bit Interleaved Parity 3 (BIP-3; ビット インターリーブド パリティ 3) 生成
- G1 パス ステータス表示
- C2 パス信号ラベル (読み取り専用)
- Loss Of Pointer (LOP; ポインタ損失)、未実装、ペイロード不一致、Alarm Indication Signal (AIS; アラーム表示信号) 検出、および Remote Defect Indication (RDI; リモート障害表示) を含む、パス レベルのアラームと条件
- 高次回線パスの J1 パストレース
- 低次パスの拡張信号ラベル





## コマンド リファレンス

---

この付録では、Cisco IOS コマンドのコマンド リファレンスまたは ML シリーズ カードに固有の Cisco IOS コマンドの特徴について説明します。標準的な Cisco IOS Release 12.2 コマンドの詳細については、<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/> から入手できる Cisco IOS のマニュアルを参照してください。

■ [no] bridge bridge-group-number protocol {drpri-rstp | ieee | rstp}

## [no] bridge *bridge-group-number* protocol {drpri-rstp | ieee | rstp}

ブリッジグループで使用するプロトコルを定義するには、**bridge protocol** グローバル コンフィギュレーション コマンドを使用します。ブリッジグループでプロトコルを使用しない場合、このコマンドは必要ありません。ブリッジグループからプロトコルを削除するには、このコマンドの **no** 形式を、適切なキーワードおよび引数と一緒に使用します。

シンタックスの説明	パラメータ	説明
	<b>drpri-rstp</b>	ML シリーズ カードの Dual Resilient Packet Ring Interconnect (DRPRI; 二重復元パケットリング相互接続) 機能をイネーブルにするプロトコル
	<b>ieee</b>	IEEE 802.1D Spanning Tree Protocol (STP; スパニングツリー プロトコル)
	<b>rstp</b>	IEEE 802.1D Rapid Spanning Tree Protocol (RSTP; 高速スパニングツリー プロトコル)
	<i>bridge-group-number</i>	プロトコルに割り当てられるブリッジグループの識別番号

### デフォルト

**コマンドモード**      グローバル コンフィギュレーション

**使用上のガイドライン**      プロトコル DRPRI-RSTP は、ML シリーズ カードを DRPRI の一部として設定する場合にのみ使用します。DRPRI が設定されているブリッジグループでは、プロトコルは 1 つに制限されるため、そのブリッジグループには、RSTP または STP を併せて実装することはできません。

**例**      次の例では、ブリッジグループ番号 100 のブリッジグループに DRPRI プロトコルを割り当てます。

```
Router(config)# bridge 100 protocol drpri-rstp
```

**関連コマンド**      bridge-group

## [no] clock auto

システム クロック パラメータを Advanced Timing, Communications, and Control/Advanced Timing, Communications, and Control Plus (TCC2/TCC2P) カードから自動的に設定するかどうかを決定するには、**clock auto** コマンドを使用します。このコマンドがイネーブルになっていると、夏時間と時間帯が両方とも自動的に設定され、システム クロックが定期的に TCC2/TCC2P カードに同期されます。この機能をディセーブルにする場合は、このコマンドの **no** 形式を使用します。

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト** デフォルトの設定は **clock auto** です。

**コマンド モード** グローバル コンフィギュレーション

**使用上のガイドライン** このコマンドの **no** 形式は、夏時間、時間帯、またはクロックを手動で設定するために必須です。また、**no** 形式は、Network Time Protocol (NTP) が Cisco IOS で設定されている場合は必須です。ONS 15454 SONET/SDH も Cisco Transport Controller (CTC) から設定され、NTP または SNTP (簡易ネットワーク タイム プロトコル) サーバを使用してノードの日付と時刻が設定できるようになっています。

**例** Router(config)# **no clock auto**

**関連コマンド**

- clock
- clock timezone
- clock set

# interface spr 1

Resilient Packet Ring (RPR; 復元パケットリング) のために ML シリーズ カード上で Shared Packet Ring (SPR; 共有パケットリング) を作成するには、このコマンドを使用します。インターフェイスがすでに作成されている場合は、このコマンドによって spr インターフェイス コンフィギュレーション モードに入ります。有効な spr インターフェイス番号は 1 のみです。

---

## デフォルト

---

**コマンド モード**      グローバル コンフィギュレーション

---

**使用上のガイドライン**      このコマンドを使用すると、RPR/SPR で使用する仮想インターフェイスを作成できます。さらに、**spr wrap** や **spr station-id** などのコマンドを SPR コンフィギュレーション コマンドモードから RPR に適用できます。

---

**例**      次の例では、共有パケットリング インターフェイスを作成します。

```
Router(config)# interface spr 1
```

---

## 関連コマンド

spr drpri-id  
spr-intf-id  
spr station-id  
spr wrap

## [no] ip radius nas-ip-address {hostname | ip-address}

ML シリーズ カードを使用すると、ユーザは各 ML シリーズ カードに対して個別の nas-ip-address を設定できます。これにより、Remote Authentication Dial In User Service (RADIUS) サーバが同一 ONS ノード内の ML シリーズ カードを個別に識別できます。ONS ノードに ML シリーズ カードが 1 つしかない場合は、このコマンドを使用するメリットはありません。ONS ノードのパブリック IP アドレスは、サーバに送信される RADIUS パケット内の nas-ip-address として機能します。

サーバに要求を送信した特定の ML シリーズ カードを識別できると、サーバのデバッグ時に便利です。nas-ip-address は、主に RADIUS 認証およびアカウントिंग要求の検証に使用されます。

この値が設定されていない場合、nas-ip-address は、**ip radius-source** コマンドで設定された値を使用して通常の Cisco IOS メカニズムによって設定されます。値が設定されていない場合は、サーバへの最良のルートとなる IP アドレスが使用されます。サーバにルーティングされているアドレスが使用できない場合は、サーバの IP アドレスが使用されます。

---

### デフォルト

---

**コマンド モード**      グローバル コンフィギュレーション

---

**使用上のガイドライン**      このコマンドを使用すると、ユーザは RADIUS パケット内にある属性 4 (nas-ip-address) の IP アドレスまたはホスト名を指定できます。

---

**例**      次の例では、RADIUS パケットの 属性 4 の IP アドレスを作成します。

```
Router# configure terminal
Router (config)# [no] ip radius nas-ip-address 10.92.92.92
```

---

**関連コマンド**

- aaa new-model
- aaa authentication login

# microcode fail system reload

マイクロコード障害の際に、フラッシュメモリに情報を保存してリブートするように ML シリーズカードを設定します。保存される情報は、Cisco TAC で使用されます。TAC への連絡については、「[テクニカル サポート](#)」( p.xxvii ) を参照してください。

---

## デフォルト

---

**コマンドモード**      グローバル コンフィギュレーション

---

**使用上のガイドライン**      このコマンドと機能は、ML シリーズカード固有のもので。

---

**例**                              ML-Series(config)# **microcode fail system-reload**

---

## 関連コマンド

## [no] pos pdi holdoff *time*

Virtual Concatenation (VCAT; バーチャル コンカチネーション)メンバー回線が Virtual Concatenation Group (VCG) に追加された場合に、Path Defect Indication (PDI; パス障害表示) を遠端に送信しないで待機する時間をミリ秒単位で指定するには、このコマンドを使用します。デフォルト値を使用するには、このコマンドの no 形式を使用します。

### シンタックスの説明

パラメータ	説明
<i>time</i>	ミリ秒単位の遅延時間 (100 ~ 1000)

### デフォルト

デフォルト値は 100 ミリ秒です。

### コマンドモード

インターフェイス コンフィギュレーション モード (Packet-over-SONET/SDH [POS] のみ)

### 使用上のガイドライン

通常、この値は Peer Terminal Equipment (PTE) の設定と一致するように設定します。このコマンドの時間単位は 1 ミリ秒です。

### 例

```
Gateway(config)# int pos0  
Gateway(config-if)# pos pdi holdoff 500
```

### 関連コマンド

pos trigger defects

## [no] pos report *alarm*

アラームおよび信号をコンソールに記録するかどうかを指定するには、このコマンドを使用します。このコマンドは、アラームが Advanced Timing Communications, and Control/Advanced Timing, Communications, and Control Plus (TCC2/TCC2P) および CTC にレポートされるかどうかに影響しません。このような条件は、Telcordia GR-253 に従ってソークされ、クリアされます。特定のアラームや信号のレポート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。

### シンタックスの説明

パラメータ	説明
<i>alarm</i>	コンソールに記録される SONET/SDH アラームです。アラームの種類は次のとおりです。
<code>all</code>	すべてのリンク ダウン アラーム障害
<code>ber_sd_b3</code>	PBIP BER SD スレッシュホールド超過障害
<code>ber_sf_b</code>	PBIP BER SF スレッシュホールド超過障害
<code>encap</code>	パス信号ラベル カプセル化ミスマッチ障害
<code>pais</code>	パス アラーム表示信号障害
<code>plop</code>	パス ポインタ喪失障害
<code>ppdi</code>	パス ペイロード障害表示障害
<code>pplm</code>	ペイロードラベル ミスマッチ パス
<code>prdi</code>	パス リモート障害表示障害
<code>ptim</code>	パス トレース ID ミスマッチ障害
<code>puneq</code>	ゼロと同等のパス ラベル障害

### デフォルト

デフォルトではすべてのアラームをレポートします。

### コマンドモード

インターフェイス コンフィギュレーション モード (Packet-over SONET/SDH [POS] のみ)

### 使用上のガイドライン

通常、この値は Peer Terminal equipment (PTE) の設定と一致するように設定します。

### 例

```
Gateway(config)# int pos0
Gateway(config-if)# pos report all
Gateway(config-if)# pos flag c2 1
03:16:51: %SONET-4-ALARM: POS0: PPLM
Gateway(config-if)# pos flag c2 0x16
03:17:34: %SONET-4-ALARM: POS0: PPLM cleared
```

### 関連コマンド

pos trigger defects

## [non] pos trigger defects *condition*

関連付けられた Packet-over-SONET/SDH (POS) リンク状態が条件によって変わるように指定するには、このコマンドを使用します。これらの条件は、**pos trigger delay** コマンドで指定した遅延を使用してソークまたはクリアされます。特定の条件でのトリガー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。

シンタックスの説明	パラメータ	説明
	<i>condition</i>	リンク状態を変更する SONET/SDH 状態です。状態は次のとおりです。  <b>all</b> すべてのリンク ダウン アラーム障害  <b>ber_sd_b3</b> Path Bit Interleaved Parity (PBIP; パス ビット インターリーブド パリティ) Bit Error Rate (BER; ビット エラー レート) Signal Degrade (SD; 信号劣化) スレッシュホールド超過障害  <b>ber_sf_b</b> PBIP BER SF スレッシュホールド超過障害  <b>encap</b> パス信号ラベル カプセル化ミスマッチ障害  <b>pais</b> パス アラーム表示信号障害  <b>plop</b> パス ポインタ喪失障害  <b>ppdi</b> パス ペイロード障害表示障害  <b>pplm</b> ペイロードラベル ミスマッチ パス  <b>prdi</b> パス リモート障害表示障害  <b>ptim</b> パス トレース ID ミスマッチ障害  <b>puneq</b> ゼロと同等のパス ラベル障害

**デフォルト** デフォルトではすべての状態をレポートします。すべての状態のリストについては、上記の説明のリストを参照してください。

**コマンドモード** インターフェイス コンフィギュレーション モード (Packet-over SONET/SDH [POS] のみ)

**使用上のガイドライン** 通常、この値は Peer Terminal Equipment (PTE) の設定と一致するように設定します。

**例**

```
Gateway(config)# int pos0
Gateway(config-if)# pos trigger defects all
```

**関連コマンド** pos trigger delay

## [no] pos trigger delay *time*

関連付けられた Packet-over-SONET/SDH (POS) リンク状態が条件によって変わるように指定するには、このコマンドを使用します。pos trigger defects コマンドで指定した条件は、遅延を使用してソークまたはクリアされます。デフォルト値を使用するには、このコマンドの no 形式を使用します。

### シンタックスの説明

パラメータ	説明
<i>time</i>	ミリ秒単位の遅延時間 (200 ~ 2000)

### デフォルト

デフォルト値は 200 ミリ秒です。

### コマンドモード

インターフェイス コンフィギュレーション モード (Packet-over SONET/SDH [POS] のみ)

### 使用上のガイドライン

通常、この値は Peer Terminal Equipment (PTE) の設定と一致するように設定します。このコマンドの最小単位は 50 ミリ秒です。

### 例

```
Gateway(config)# int pos0
Gateway(config-if)# pos trigger delay 500
```

### 関連コマンド

pos trigger defects

## [no] pos scramble-spe

スクランブリングをイネーブルにするには、このコマンドを使用します。

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト** デフォルト値はカプセル化によって異なります。

カプセル化	スクランブリング
LEX	pos scramble-atm
PPP/HDLC	no pos scramble-spe

**コマンド モード** インターフェイス コンフィギュレーション モード ( Packet-over SONET/SDH [POS] のみ )

**使用上のガイドライン** 通常、この値は Peer Terminal Equipment ( PTE ) の設定と一致するように設定します。このコマンドによって pos flag c2 の設定が変わる可能性があります。

**例**

```
Gateway(config)# int pos0
Gateway(config-if)# pos scramble-spe
```

**関連コマンド関連** pos flag c2

## [no] pos vcat defect {immediate | delayed}

Virtual Concatenation (VCAT; バーチャル コンカチネーション) 障害処理モードを、状態の変化を検出したらただちに処理するように設定するか、または `pos trigger delay` で指定した時間の間待機するように設定します。デフォルト値を使用するには、このコマンドの `no` 形式を使用します。

シンタックスの説明	パラメータ	説明
	<code>immediate</code>	ステートの変化を検出したらただちに障害を処理します。
	<code>delayed</code>	コマンド <code>pos trigger delay</code> で指定した時間が経過してから障害を処理します。遅延を設定していて、かつ回線が Resilient Packet Ring (RPR; 復元パケットリング) 上にある場合は、RPR 障害処理も指定した遅延時間だけ遅れます。

**デフォルト** デフォルトの設定は `immediate` です。

**コマンドモード** POS インターフェイス設定

**使用上のガイドライン** VCAT 回線が非保護 SONET/SDH 回線を使用している場合は、`immediate` を使用する必要があります。SONET 保護回路 (Bidirectional Line Switch Ring [BLSR; 双方向ラインスイッチ型リング] または Unidirectional Path Switch Ring [UPSR; 単方向パススイッチ型リング]) または SDH 保護回路 (Subnetwork Connection Protection [SNCP; サブネットワーク接続保護] または Multiplex Section-Shared Protection Ring [MS-SPRing; 多重化セクション共有保護リング]) を使用している場合、`delayed` を使用する必要があります。

**例** 次の例では、ML シリーズ カードを `delayed` に設定しています。

```
Router(config)# interface pos 1
Router(config-if)# pos vcat defect delayed
```

**関連コマンド**

```
interface spr 1
spr wrap
interface pos 1
pos trigger delay
```

## [no] pos vcat resequence {enable | disable}

Software Link Capacity Adjustment Scheme (SW-LCAS; ソフトウェア リンク キャパシティ 調整方式) の H4 バイト シーケンス番号の再シーケンス機能をイネーブルまたはディセーブルにします。Release 4.6.2 以降のソフトウェアを実行している ML シリーズ カードが、Release 4.6.0 または 4.6.1 のソフトウェアを実行している ML シリーズ カードと相互運用している場合は、Release 4.6.2 以降のソフトウェアを実行している ML シリーズ カードの設定に **pos vcat resequence disable** コマンドを追加する必要があります。

シンタックスの説明	パラメータ	説明
	Enable	Virtual Concatenation (VCAT; バーチャル コンカチネーション) グループにメンバーを追加した際または VCAT グループからメンバーを削除した際に行う H4 バイト シーケンス番号の再シーケンスをイネーブルにします。両メンバーがアップ状態の場合は、メンバー 0 のシーケンス番号がゼロ (0) になり、メンバー 1 のシーケンス番号が 1 になります。1 つのメンバーだけがアップ状態の場合は、そのメンバーのシーケンス番号はゼロ (0) になります。
	Disable	VCAT グループにメンバーを追加した際または VCAT グループからメンバーを削除した際に行う H4 バイト シーケンス番号の再シーケンスをディセーブルにします。メンバー 0 のシーケンス番号は必ずゼロ (0) になり、メンバー 1 のシーケンス番号は必ず 1 になります。

**デフォルト** デフォルトの設定は Enable です。

**コマンド モード** Packet-over-SONET/SDH (POS) ポート設定ごと

**使用上のガイドライン** このコマンドの no 形式ではモードがデフォルトに設定されます。

**例** 次の例では、POS ポート 0 に対して H4 バイト シーケンス番号の再シーケンスをディセーブルにします。

```
Router(config)# int pos 0
Router(config)# pos vcat resequence disable
```

**関連コマンド** なし

## show controller pos *interface-number* [details]

Packet-over-SONET/SDH (POS) コントローラの状態を表示するには、このコマンドを使用します。インターフェイスの SONET および POS の追加情報を取得するには、details 引数を使用します。

シンタックスの説明	パラメータ	説明
	<i>interface-number</i>	POS インターフェイスの番号 (0 ~ 1)

### デフォルト

コマンドモード    イネーブル EXEC

使用上のガイドライン    このコマンドは、POS と SONET の問題を診断して特定するために使用できます。

### 例

#### Continuous Concatenation Circuit (CCAT) の Show Controller の出力例

```
Router# show controller pos 0
Interface POS0
Hardware is Packet/Ethernet over Sonet
Concatenation: CCAT
Circuit state: IS
PATH
  PAIS      = 0          PLOP      = 0          PRDI      = 0          PTIM = 0
  PPLM      = 0          PUNEQ     = 0          PPDI      = 0          PTIU = 0
  BER_SF_B3 = 0          BER_SD_B3 = 0          BIP(B3)   = 20         REI  = 2
  NEWPTR    = 0          PSE       = 0          NSE       = 0

Active Alarms : None
Demoted Alarms: None
Active Defects: None
Alarms reportable to CLI: PAIS PLOP PUNEQ PTIM PPLM PRDI PPDI BER_SF_B3 BER_SD_B3
VCAT_OOU_TPT LOM SQM
Link state change defects: PAIS PLOP PUNEQ PTIM PPLM PRDI PPDI BER_SF_B3
Link state change time   : 200 (msec)

DOS FPGA channel number : 0
Starting STS (0 based)  : 0
VT ID (if any) (0 based): 255
Circuit size            : VC4
RDI Mode                : 1 bit
C2 (tx / rx)           : 0x01 / 0x01
Framing                 : SDH

Path Trace
Mode                    : off
Transmit String         :
Expected String         :
Received String         :
Buffer                  : Stable
Remote hostname         :
Remote interface        :
Remote IP addr          :

B3 BER thresholds:
SFBER = 1e-4,   SDBER = 1e-7
```

```

5 total input packets, 73842 post-HDLC bytes
0 input short packets, 73842 pre-HDLC bytes
0 input long packets , 0 input runt packets
67 input CRCerror packets , 0 input drop packets
0 input abort packets
0 input packets dropped by ucode

0 total output packets, 0 output pre-HDLC bytes
0 output post-HDLC bytes

Carrier delay is 200 msec

```

## VCAT の Show Controller の出力例

```

Router# show controller pos 1
Interface POS1
Hardware is Packet/Ethernet over Sonet
Concatenation: VCAT
VCG State: VCG_NORMAL
LCAS Type:NO LCAS
Defect Processing Mode: IMMEDIATE
PDI Holdoff Time: 100 (msec)
Active Alarms : None
Demoted Alarms: None

***** Member 1 *****
ESM State: IS
VCG Member State: VCG_MEMBER_NORMAL
  PAIS      = 0          PLOP      = 0          PRDI      = 0          PTIM = 0
  PPLM      = 0          PUNEQ     = 0          PPDI      = 0          PTIU = 0
  BER_SF_B3 = 0          BER_SD_B3 = 0          BIP(B3)   = 16         REI  = 17
  NEWPTR    = 0          PSE       = 0          NSE       = 0

Active Alarms : None
Demoted Alarms: None
Active Defects: None
Alarms reportable to CLI: PAIS PLOP PUNEQ PTIM PPLM PRDI PPDI BER_SF_B3 BER_SD_B3
VCAT_OOU_TPT LOM SQM
Link state change defects: PAIS PLOP PUNEQ PTIM PPLM PRDI PPDI BER_SF_B3
Link state change time : 200 (msec)

DOS FPGA channel number : 2
Starting STS (0 based) : 3
VT ID (if any) (0 based) : 255
Circuit size : VC4
RDI Mode : 1 bit
C2 (tx / rx) : 0x01 / 0x01
Framing : SDH

Path Trace
Mode : off
Transmit String :
Expected String :
Received String :
Buffer : Stable
Remote hostname :
Remote interface:
Remote IP addr :

B3 BER thresholds:
SFBER = 1e-4, SDBER = 1e-7

***** Member 2 *****
ESM State: IS
VCG Member State: VCG_MEMBER_NORMAL
  PAIS      = 0          PLOP      = 0          PRDI      = 0          PTIM = 0

```

## ■ show controller pos interface-number [details]

```

PPLM      = 0          PUNEQ      = 0          PPDI      = 0          PTIU = 0
BER_SF_B3 = 0          BER_SD_B3 = 0          BIP(B3)  = 15         REI = 35
NEWPTR    = 0          PSE       = 0          NSE       = 0

Active Alarms : None
Demoted Alarms: None
Active Defects: None
Alarms reportable to CLI: PAIS PLOP PUNEQ PTIM PPLM PRDI PPDI BER_SF_B3 BER_SD_B3
VCAT_OOU_TPT LOM SQM
Link state change defects: PAIS PLOP PUNEQ PTIM PPLM PRDI PPDI BER_SF_B3
Link state change time : 200 (msec)

DOS FPGA channel number : 3
Starting STS (0 based)  : 24
VT ID (if any) (0 based): 255
Circuit size           : VC4
RDI Mode               : 1 bit
C2 (tx / rx)          : 0x01 / 0x01
Framing                : SDH

Path Trace
Mode                   : off
Transmit String       :
Expected String       :
Received String       :
Buffer                 : Stable
Remote hostname       :
Remote interface      :
Remote IP addr        :

B3 BER thresholds:
SFBER = 1e-4,   SDBER = 1e-7

13 total input packets, 5031 post-HDLC bytes
0 input short packets, 5031 pre-HDLC bytes
0 input long packets , 0 input runt packets
0 input CRCerror packets , 0 input drop packets
0 input abort packets
0 input packets dropped by ucode

13 total output packets, 5031 output pre-HDLC bytes
5031 output post-HDLC bytes

Carrier delay is 200 msec

```

## 関連コマンド

```

show interface pos

clear counters

```

## show interface pos *interface-number*

Packet-over-SONET/SDH (POS) の状態を表示するには、このコマンドを使用します。

シンタックスの説明	パラメータ	説明
	<i>interface-number</i>	POS インターフェイスの番号 (0 ~ 1)

### デフォルト

コマンドモード    イネーブル EXEC

使用上のガイドライン    このコマンドは、POS と SONET/SDH の問題を診断して特定するために使用できます。

### 例

```
Gateway# show interfaces pos0
POS0 is up, line protocol is up
  Hardware is Packet/Ethernet over Sonet
  Description: foo bar
  MTU 4470 bytes, BW 155520 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation HDLC, crc 32, loopback not set
  Keepalive set (10 sec)
  Scramble enabled
  Last input 00:00:09, output never, output hang never
  Last clearing of "show interface" counters 05:17:30
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec

    2215 total input packets, 223743 post-HDLC bytes
    0 input short packets, 223951 pre-HDLC bytes
    0 input long packets , 0 input runt packets
    0 input CRCerror packets , 0 input drop packets
    0 input abort packets
    0 input packets dropped by ucode

    0 packets input, 0 bytes
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
      0 parity
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

    2216 total output packets, 223807 output pre-HDLC bytes
    224003 output post-HDLC bytes

    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 applique, 8 interface resets
    0 output buffer failures, 0 output buffers swapped out
    0 carrier transitions
```

関連コマンド    show controller pos  
clear counters

## show ons alarm

Cisco IOS CLI (コマンドライン インターフェイス) セッションを実行している ML シリーズ カード上でアクティブなすべてのアラームを表示するには、このコマンドを使用します。

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト**

**コマンドモード** イネーブル EXEC

**使用上のガイドライン** このコマンドは、カードの問題を診断して特定するために使用できます。

**例**

```
router# show ons alarm
Equipment Alarms
Active: CONTBUS-IO-A CTNEQPT-PBWORK

Port Alarms
  POS0 Active: None
  POS1 Active: None
  FastEthernet0 Active: None
  FastEthernet1 Active: None
  FastEthernet2 Active: None
  FastEthernet3 Active: None
  FastEthernet4 Active: None
  FastEthernet5 Active: None
  FastEthernet6 Active: None
  FastEthernet7 Active: None
  FastEthernet8 Active: None
  FastEthernet9 Active: None
  FastEthernet10 Active: None
  FastEthernet11 Active: None

POS0

Active Alarms : None
Demoted Alarms: None

POS1 VCG State: VCG_NORMAL
VCAT Group
Active Alarms : None
Demoted Alarms: None

Member 0
Active Alarms : None
Demoted Alarms: None

Member 1
Active Alarms : None
Demoted Alarms: None
```

**関連コマンド**

- show controller pos
- show ons alarm defects
- show ons alarm failures

## show ons alarm defect eqpt

装置層の障害を表示するには、このコマンドを使用します。

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト**

**コマンドモード** イネーブル EXEC

**使用上のガイドライン** 装置層のアクティブな障害と、問題の可能性のある障害を表示するには、このコマンドを使用します。

**例**

```
router# show ons alarm defect eqpt
Equipment Defects
Active: CONTBUS-IO-B
Reportable to TCC/CLI: CONTBUS-IO-A CONTBUS-IO-B CTNEQPT-PBWORK CTNEQPT-PBPROT EQPT
RUNCFG-SAVENEED ERROR-CONFIG
```

**関連コマンド** show ons alarm failures

# show ons alarm defect port

ポート層の障害を表示するには、このコマンドを使用します。

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト**

**コマンドモード** イネーブル EXEC

**使用上のガイドライン** リンク層のアクティブな障害と、問題の可能性のある障害を表示するには、このコマンドを使用します。TPTFAIL 障害は Packet-over-SONET/SDH (POS) ポート上でのみ発生し、CARLOSS 障害はイーサネット ポート上でのみ発生します。

**例**

```
router# show ons alarm defect port
Port Defects
  POS0
  Active: TPTFAIL
  Reportable to TCC: CARLOSS TPTFAIL
  POS1
  Active: TPTFAIL
  Reportable to TCC: CARLOSS TPTFAIL
  GigabitEthernet0
  Active: None
  Reportable to TCC: CARLOSS TPTFAIL
  GigabitEthernet1
  Active: None
  Reportable to TCC: CARLOSS TPTFAIL
```

**関連コマンド**

- show interface
- show ons alarm failures

## show ons alarm defect pos *interface-number*

リンク層の障害を表示するには、このコマンドを使用します。

シンタックスの説明	パラメータ	説明
	<i>interface-number</i>	インターフェイスの番号 (0 ~ 1)

### デフォルト

コマンドモード    イネーブル EXEC

使用上のガイドライン    Packet-over-SONET/SDH (POS) 層のアクティブな障害と、問題の可能性のある障害を表示するには、このコマンドを使用します。

例

```
router# show ons alarm defect pos0
POS0
Active Defects: None
Alarms reportable to TCC/CLI: PAIS PRDI PLOP PUNEQ PPLM PTIM PPDI BER_SF_B3 BER_SD_B3
```

関連コマンド

- show controller pos
- show ons alarm failures

## show ons alarm failure eqpt

装置層の障害を表示するには、このコマンドを使用します。

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト**

**コマンドモード** イネーブル EXEC

**使用上のガイドライン** 装置層のアクティブな障害を表示するには、このコマンドを使用します。EQPT アラームが存在する場合は、アラームの原因である Board Fail 障害が表示されます。

**例**

```
router# show ons alarm failure eqpt
Equipment
Active Alarms: None
```

**関連コマンド** show ons alarm defect

## show ons alarm failure port

ポート層の障害を表示するには、このコマンドを使用します。

**シンタックスの説明** このコマンドには、引数またはキーワードはありません。

**デフォルト**

**コマンドモード** イネーブル EXEC

**使用上のガイドライン** リンク層のアクティブな障害を表示するには、このコマンドを使用します。

**例**

```
router# show ons alarm failure port
Port Alarms
  POS0 Active: TPTFAIL
  POS1 Active: TPTFAIL
  GigabitEthernet0 Active: None
  GigabitEthernet1 Active: None
```

**関連コマンド** show interface  
show ons alarm defect

# show ons alarm failure pos *interface-number*

リンク層の障害を表示するには、このコマンドを使用します。

シンタックスの説明	パラメータ	説明
	<i>interface-number</i>	インターフェイスの番号 (0 ~ 1)

## デフォルト

コマンドモード    イネーブル EXEC

**使用上のガイドライン**    Packet-over-SONET/SDH (POS) 層にある特定のインターフェイスのアクティブな障害を表示するには、このコマンドを使用します。Telcordia GR-253 に規定されているようにアラームが降格されたかどうかも表示されます。

**例**

```
router# show ons alarm failure pos 0
POS0
Active Alarms : None
Demoted Alarms: None
```

**関連コマンド**

```
show controller pos
show ons alarm defect
```

## spr drpri-id { 0 | 1 }

Dual Resilient Packet Ring Interconnect( DRPRI; 二重復元パケットリング相互接続)保護機能用の ML シリーズカードペアを区別するために、0 または 1 の DRPRI 識別番号を作成します。

### デフォルト

**コマンドモード** Shared Packet Ring ( SPR; 共有パケットリング) インターフェイス設定

**使用上のガイドライン** DRPRI ペアの 2 枚のカードは同じ SPR ステーション ID を共有するため、DRPRI 識別番号を使用すると、DRPRI ペア的一方を簡単に特定できます。

**例** 次の例では、ゼロ (0) という DRPRI 識別番号を ML シリーズカードの SPR インターフェイスに割り当てます。

```
Router(config)# interface spr 1
Router(config-if)# spr drpri-id 0
```

**関連コマンド** interface spr 1

spr-intf-id

spr station-id

spr wrap

## spr-intf-id *shared-packet-ring-number*

POS インターフェイスを SPR インターフェイスに割り当てます。

シンタックスの説明	パラメータ	説明
	<i>shared-packet-ring-number</i>	有効な SPR 番号は 1 のみです。

### デフォルト

**コマンド モード** POS インターフェイス設定

### 使用上のガイドライン

- SPR 番号は必ず 1 に設定します。これは、SPR インターフェイスに割り当てられた SPR 番号と同じです。
- SPR インターフェイスのメンバーは、POS インターフェイスである必要があります。
- SPR インターフェイスは、EtherChannel (ポートチャネル) インターフェイスと同様に設定されます。メンバーの定義には、**channel-group** コマンドではなく、**spr-intf-ID** コマンドを使用してください。さらに、port-channel と同じように、POS インターフェイスではなく SPR インターフェイスを設定します。

**例** 次の例では、SPR グ番号が 1 の SPR インターフェイスに ML シリーズ カードの POS インターフェイスを割り当てます。

```
Router(config)# interface pos 0
Router(config-if)# spr-intf-id 1
```

### 関連コマンド

```
interface spr 1
spr drpri-id
spr station-id
spr wrap
```

■ [no] spr load-balance { auto | port-based }

## [no] spr load-balance { auto | port-based }

ユニキャスト パケットに対して Resilient Packet Ring (RPR; 復元パケットリング) ロード バランシング方式を指定します。

シンタックスの説明	パラメータ	説明
	<b>auto</b>	デフォルトの <b>auto</b> オプションは、MAC (メディア アクセス制御) アドレスまたは IP パケットの送信元アドレスと宛先アドレスに基づいて負荷を分散します。
	<b>port-based</b>	<b>port-based</b> ロード バランシング オプションは、偶数のポートを POS 0 インターフェイスに、奇数のポートを POS 1 インターフェイスにマップします。

**デフォルト** デフォルトの設定は auto です。

**コマンドモード** Shared Packet Ring (SPR; 共有パケット リング) インターフェイス設定

**例** 次の例では、port-based ロード バランシングを使用するように SPR インターフェイスを設定します。

```
Router(config)# interface spr 1
Router(config-if)# spr load-balance port-based
```

**関連コマンド** interface spr 1

## spr station-id *station-id-number*

ステーション ID を設定します。

シンタックスの説明	パラメータ	説明
	<i>station-id-number</i>	Resilient Packet Ring (RPR; 復元パケットリング) に接続した Shared Packet Ring (SPR; 共有パケットリング) インターフェイスごとに異なる番号を設定する必要があります。有効なステーション ID 番号の範囲は、1 ~ 254 です。

### デフォルト

**コマンド モード** Shared Packet Ring (SPR; 共有パケットリング) インターフェイス設定

**使用上のガイドライン** RPR に接続している複数の ML シリーズ カードはすべて同じインターフェイス タイプであり、番号 spr1 を持っています。ステーション ID は、SPR インターフェイスの区別に便利です。

**例** 次の例では、ML シリーズ カードの SPR ステーション ID を 100 に設定します。

```
Router(config)# interface spr 1  
Router(config-if)# spr station-id 100
```

**関連コマンド**

- interface spr 1
- spr drpri-id
- spr-intf-id
- spr wrap

## ■ spr wrap { immediate | delayed }

## spr wrap { immediate | delayed }

Resilient Packet Ring (RPR; 復元パケットリング) ラップモードを、リンクステートの変化を検出したらただちにトラフィックをラップするように設定するか、または障害を登録してリンクのダウンを宣言するための SONET 保護時間を設ける搬送波遅延後にトラフィックをラップするように設定します。

### シンタックスの説明

パラメータ	説明
<b>immediate</b>	リンクステートの変化を検出したらただちに RPR トラフィックをラップします。
<b>delayed</b>	搬送波遅延時間が経過してから RPR トラフィックをラップします。

### デフォルト

デフォルトの設定は immediate です。

### コマンドモード

Shared Packet Ring (SPR; 共有パケットリング) インターフェイス設定

### 使用上のガイドライン

RPR が非保護 SONET/SDH 回線を実行している場合は、immediate を使用する必要があります。SONET 保護回路 (Bidirectional Line Switch Ring [BLSR; 双方向ラインスイッチ型リング] や Unidirectional Path Switch Ring [UPSR; 単方向パススイッチ型リング]) または SDH 保護回路 (Subnetwork Connection Protection [SNCP; サブネットワーク接続保護] や Multiplex Section-Shared Protection Ring [MS-SPRing; 多重化セクション共有保護リング]) の場合は、delayed を使用する必要があります。

### 例

次の例では、ML シリーズカードを delayed に設定しています。

```
Router(config)# interface spr 1
Router(config-if)# spr wrap delayed
```

### 関連コマンド

```
interface spr 1
spr drpri-id
spr-intf-id
spr station-id
```

## xconnect

Ethernet over Multiprotocol Label Switching (EoMPLS) を使用してレイヤ 2 パケットを指定されたポイントツーポイント Virtual Circuit (VC; 仮想回線) にルーティングするには、Customer-Edge (CE; カスタマー エッジ) または Service Provider-edge Customer-located Equipment (PE-CLE) 入力および出力イーサネット ポートまたは宛先および Virtual Connection Identifier (VC ID; 仮想接続 ID) のある dot1Q VLAN (仮想 LAN) サブインターフェイスで、**xconnect** 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。VC を削除するには、このコマンドの **no** 形式を両方のエッジ装置で使用します。

```
xconnect destination vc-id encapsulation mpls
```

```
no xconnect
```



(注)

このコマンドは、**mpls l2transport route** インターフェイス コンフィギュレーション コマンドを置き換えたものです。

### シンタックスの説明

<i>destination</i>	リモート Provider Edge (PE; プロバイダー エッジ) 装置の宛先 Label Distribution Protocol (LDP; ラベル配布プロトコル) IP アドレス。この IP アドレスは、このコマンドを入力するルートの IP アドレスにすることはできません。
<i>vc-id</i>	2 つのピア PE 装置間の仮想接続用に VC ID を割り当てます。指定できる範囲は 1 ~ 4294967295 です。
<b>encapsulation mpls</b>	MPLS データ カプセル化方式を指定します。



(注)

**pw-class** キーワードは、コマンドラインのヘルプ スtring には表示されていますが、サポートされていません。

### デフォルト

ポイントツーポイント接続は設定されていません。

### コマンド モード

インターフェイス コンフィギュレーション

### 使用上のガイドライン

サービス プロバイダー ネットワークの各エッジにある 2 つの PE-CLE 装置上のイーサネット インターフェイスを接続するために、MPLS クラウドで MPLS VC が稼働します。サービス プロバイダー ネットワークの各エッジにある PE 装置でこのコマンドを入力して、双方向仮想接続を確立する必要があります。この接続は、2 つの単一方向 Label Switched Path (LSP; ラベル スイッチド パス) で構成されています。両端で VC が適切に設定されていない場合は、VC が確立されません。

*destination* パラメータの場合、もう一方の PE-CLE 装置の LDP IP アドレスを指定します。コマンドを入力している装置の IP アドレスを入力しないでください。

*vc-id* は、PE 装置の各ペアに対して一意でなければなりません。したがって、大規模なネットワークでは、1 つの VC ID が複数回設定されていないことを確認するために、VC ID を追跡する必要があります。

**例** この例では、インターフェイス PE1 VLAN3 とインターフェイス PE 2 VLAN 4 間の EoMPLS トンネルの確立方法を示しています。PE1 には PE2 がルーティングを通じて検出した IP アドレス 10.0.0.1/32 があり、PE2 には PE1 がルーティングを通じて検出した IP アドレス 20.0.0.1/32 があります。

インターフェイス PE1 での入力

```
Switch(config)# interface vlan 3  
Switch(config-if)# xconnect 20.0.0.1 123 encapsulation mpls
```

インターフェイス PE2 での入力

```
Switch(config)# interface vlan 4  
Switch(config-if)# xconnect 10.0.0.1 123 encapsulation mpls
```

**関連コマンド** `show mpls l2transport route`



## サポートされていない CLI コマンド

---

この付録では、テストされていないかまたはハードウェアの制限があるかのいずれかの理由でこのリリースではサポートされていない CLI (コマンドライン インターフェイス) コマンドについて説明します。サポートされないコマンドは、CLI プロンプトで疑問符 (?) を入力すると表示されます。このリストは完全ではありません。サポートされていないコマンドは、コマンドモードで表示されます。

### サポートされていないイネーブル EXEC コマンド

```
clear ip accounting
show ip accounting
show ip cache
clear ip tcp header-compression
show ip mcache
show ip mpacket
show controller pos pm
show controller pos [variable] pm
```

## サポートされていないグローバル コンフィギュレーション コマンド

access-list aaa <1100-1199>  
access-list aaa <200-299>  
access-list aaa <700-799>  
async-bootp  
boot  
bridge <num> acquire  
bridge <num> address  
bridge cmf  
bridge <num> bitswap-layer3-addresses  
bridge <num> circuit-group  
bridge <num> domain  
bridge <num> lat-service-filtering  
bridge <num> protocol dec  
bridge <num> protocol ibm  
bridge <num> protocol vlan-bridge  
chat-script  
class-map match access-group  
class-map match class-map  
class-map match destination-address  
class-map match mpls  
class-map match protocol  
class-map match qos-group  
class-map match source-address  
clns  
define  
dialer  
dialer-list  
downward-compatible-config  
file  
ip access-list log-update  
ip access-list logging  
ip address-pool  
ip alias  
ip bootp

ip gdp  
ip local  
ip reflexive-list  
ip security  
ip source-route  
ip tcp  
ipc  
map-class  
map-list  
multilink  
netbios  
partition  
policy-map class queue-limit  
priority-list  
queue-list  
iso-igrpiso-igrp  
router mobile  
service compress-config  
service disable-ip-fast-frag  
service exec-callback  
service nagle  
service old-slip-prompts  
service pad  
service slave-log  
set privilege level  
subscriber-policy

## サポートされていない POS インターフェイス コンフィギュレーション コマンド

access-expression  
autodetect  
bridge-group x circuit-group  
bridge-group x input-  
bridge-group x lat-compression  
bridge-group x output-  
bridge-group x subscriber-loop-control  
clock  
cls  
custom-queue-list  
down-when-looped  
fair-queue  
flowcontrol  
full-duplex  
half-duplex  
hold-queue  
ip accounting  
ip broadcast-address  
ip load-sharing per-packet  
ip route-cache  
ip security  
ip tcp  
ip verify  
iso-igrp  
loopback  
multilink-group  
netbios  
pos flag c2  
pos mode gfp  
priority-group  
pulse-time  
random-detect  
rate-limit

serial  
service-policy history  
source  
timeout  
transmit-interface  
tx-ring-limit

## サポートされていないファーストイーサネットまたは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コマンド

access-expression

clns

custom-queue-list

fair-queue

hold-queue

ip accounting

ip broadcast-address

ip load-sharing per-packet

ip route-cache

ip security

ip tcp

ip verify

iso-igrp

keepalive

loopback

max-reserved-bandwidth

multilink-group

netbios

priority-group

random-detect

rate-limit

service-policy history

timeout

transmit-interface

tx-ring-limit

## サポートされていない Port-Channel インターフェイス コンフィギュレーション コマンド

access-expression

carrier-delay

cdp

clns

custom-queue-list

duplex

down-when-looped

encapsulation

fair-queue

flowcontrol

full-duplex

half-duplex

hold-queue

iso-igrp

keepalive

max-reserved-bandwidth

multilink-group

negotiation

netbios

ppp

priority-group

rate-limit

random-detect

timeout

tx-ring-limit

## サポートされていない BVI インターフェイス コンフィギュレーション コマンド

access-expression

carrier-delay

cdp

clns

flowcontrol

hold-queue

iso-igrp

keepalive

l2protocol-tunnel

load-interval

max-reserved-bandwidth

mode

multilink-group

netbios

ntp

mtu

rate-limit

timeout

transmit-interface

tx-ring-limit



## テクニカル サポートの利用方法

---

この付録では、ML シリーズ カードに関する問題の解決方法について説明します。

この付録の内容は次のとおりです。

- [インターネットワーク情報の収集 \(p.C-2\)](#)
- [ML シリーズ カードからのデータの取得 \(p.C-3\)](#)
- [テクニカル サポート担当者へのデータの提供 \(p.C-3\)](#)

問題の解決に役立つため、ご連絡の前に、「[インターネットワーク情報の収集](#)」(p.C-2)をご使用のネットワークの関連情報を収集する際の注意事項として利用してください。



**(注)** 解決できない問題がある場合は、Cisco Technical Assistance Center (TAC) にご連絡ください。詳細は、「[テクニカル サポート](#)」(p.xxvii)を参照してください。

---

## インターネットワーク情報の収集

特定のデータを収集する前に、インターネットワークに関してすでにレポートされているすべての症状の情報（接続切断やホスト応答の遅延など）をまとめます。

次に、特定の情報を収集します。インターネットワーキングの問題をトラブルシューティングするのに必要な標準的な情報は、一般的に 2 つに分類されます。つまり、あらゆる状況に必要な情報と、トポロジー、テクノロジー、プロトコルに特有の情報です。

テクニカル サポート担当者に必ず提供する必要のある情報は次のとおりです。

- データ ネットワークのネットワーク トポロジー マップ、および SONET/SDH トポロジーとプロビジョニング
- ホストとサーバの一覧（ホストとサーバのタイプ、ネットワーク番号、およびホストにインストールされているオペレーティングシステムの説明を含む）
- 関連するすべてのスイッチ ルータとスイッチの設定一覧
- 関連するすべてのスイッチ ルータとスイッチの全仕様
- 関連するすべてのスイッチ ルータとスイッチのソフトウェア バージョン番号（`show version` コマンドで取得）とフラッシュ コード（`show controllers` コマンドで取得）
- ネットワーク層プロトコル、バージョン、およびベンダーの一覧
- SONET/SDH トポロジーの全ノードのアラームと状態の一覧
- ノード装置と構成（クロスコネクト カードのタイプ、ML シリーズ カードのスロット番号、OC-N カード、および TCC2/TCC2P カードを含む）

必要なデータの収集に役立てるために、`show tech-support EXEC` コマンドが Cisco IOS Release 11.1(4) 以降に追加されました。このコマンドは、テクニカル サポート担当者に障害を報告する際に必要となる、スイッチ ルータに関する一般的な情報を表示します。

`show tech-support` コマンドは、`show version`、`show running-config`、`show controllers`、`show stacks`、`show interfaces`、`show buffers`、`show process memory`、および `show process` の各 EXEC コマンドを使用した場合と同じ情報を出力します。

テクニカル サポートで必要とされる特定情報の要件は、状況によって異なります。次のような情報が必要となります。

- 次の一般的な `show` コマンドの出力
  - `show interfaces`
  - `show controllers`
  - `show processes {cpu | mem}`
  - `show buffer`
  - `show mem summary`
- 次のプロトコル固有の `show` コマンドの出力
  - `show protocol route`
  - `show protocol traffic`
  - `show protocol interfaces`
  - `show protocol arp`
- プロビジョニング `show` コマンドの出力
- 関連する `debug` イネーブル EXEC コマンドの出力
- プロトコル固有の `ping` の出力と `trace` コマンドによる診断テストの結果（必要な場合）
- ネットワーク アナライザのトレース結果（必要な場合）
- `exception dump` コマンド、またはシステムが動作可能な場合は `write core` コマンドで取得したコア ダンプ（必要な場合）

## ML シリーズ カードからのデータの取得

ML シリーズ カードから情報を取得するときには、取得に使用するシステムに適した取得方法を選択する必要があります。さまざまなプラットフォームでのヒントを次に示します。

- PC と Macintosh の場合 PC または Macintosh を ML シリーズ カードのコンソール ポートに接続し、出力内容をすべてディスク ファイルに記録します ( 端末エミュレーション プログラムを使用 )。具体的な手順は、システムで使用する通信パッケージによって異なります。
- コンソール ポートに接続された端末またはリモート端末の場合 コンソール ポートに接続された端末またはリモート端末を使用して情報を取得するには、プリンタを端末の AUX ポート ( 存在する場合 ) に接続し、すべての画面出力をプリンタに出力するしかありません。データをファイルに保存する方法がないため、端末の使用は好ましくありません。
- UNIX ワークステーションの場合 UNIX のプロンプトで、コマンド `script filename` を入力し、Telnet を使用して ML シリーズ カードに接続します。UNIX の `script` コマンドは、指定したファイルにすべての画面出力を保存します。出力の保存を中止してファイルを閉じるには、UNIX システムのファイル終了文字 ( 通常は Ctrl-D ) を入力します。



(注) 特定のエラー メッセージまたは動作情報を UNIX の Syslog サーバに自動的に記録させるには、`logging internet-address` コマンドを入力します。`logging` コマンドの使用方法和 Syslog サーバの設定方法の詳細については、Cisco IOS のコンフィギュレーション ガイドとコマンド リファレンスを参照してください。

## テクニカル サポート担当者へのデータの提供

テクニカル サポート担当者へ情報を提供する場合は、できるだけ電子データでお送りください。テクニカル サポート担当者から開発スタッフへの情報の転送が、電子データにより非常に容易になります。一般的な電子形式には、電子メールで送信するデータと FTP ( ファイル転送プロトコル ) で送信するファイルがあります。

テクニカル サポート担当者へデータを提供する場合、次のリスト ( 望ましい順に列挙 ) に従って適切な提供方法を決定します。

- 最も望ましい情報の提供方法は、インターネット経由の FTP サービスによる送信です。FTP を使用できる場合は、ホスト Cisco.com の受信ディレクトリにファイルをコピーします。
- 次に望ましい方法は、データを電子メールで送信する方法です。この方法を使用するときには、事前にテクニカル サポート担当者にご連絡ください。特に、バイナリのコア ダンプや他のサイズの大きなファイルを送信する場合には必ずご連絡ください。
- Kermit などの PC ベースの通信プロトコルを使用してファイルを Cisco.com にアップロードします。この場合も、転送を開始する前にテクニカル サポート担当者にご連絡ください。
- ディスクまたはテープなどのメディアでデータを送付します。
- 最も望ましくない方法は、ファックスまたは郵送によるハードコピーの送付です。



(注) 電子メールを使用する場合は、binhex や zip などの符号化方式は使用しないでください。MIME 準拠のメールだけを使用してください。

■ テクニカル サポート担当者へのデータの提供



## Numerics

802.1D

STP を参照

IEEE 802.1D

STP を参照

## A

ABR 11-10

Access Control List

ACL を参照

access-list コマンド 22-9

ACL

ACL の適用 16-5

概要 16-2

作成

IP ACL 16-3

拡張 IP ACL 16-3

名前付き IP ACL 16-3

名前付き拡張 IP ACL 16-5

名前付き標準 IP ACL 16-4

番号付き標準 IP ACL 16-3

設定時の注意事項 IP ACL 16-3

名前付き IP ACL 16-3

ASBR 11-10

Auto-MDIX 4-7

## B

bandwidth コマンド、トラフィック クラス 14-15, 18-5

BGP、概要 11-28

BPDU RSTP の形式 7-14

bridge irb コマンド 12-3

bridge protocol コマンド 18-10

bridge-group virtual interface

BVI を参照

bridge-group コマンド 4-6, 4-8, 4-9, 4-10, 18-10

BVI

情報の表示 12-7

設定 12-3

説明 12-2

ルーティングのイネーブル化 12-3

bvi コマンド 12-3

## C

CDP、レイヤ 2 プロトコル トンネリング 9-13

CE-1000-4

FPGA バッファリング 25-3

GFP-F フレーミング 25-9

HDLC 25-9

IS, AINS 25-5

J1 パストレース 25-9

LEX カプセル化 25-9

POS ポート 25-7

RMON および SNMP のサポート 25-6

SW-LCAS 25-7

VCAT 特性 25-7

イーサネット機能 25-3

オーバーサブスクライブ 25-3

回線のルーティングおよび保護 25-8

概要 25-2

拡張状態モデル (ESM) 25-6

自動ネゴシエーション 25-3

遅延差補償 25-8

統計情報およびカウンタ 25-6

フレーム バッファリング 25-3

フロー制御 25-3

フロー制御の基準のプロビジョニング 25-4

リンク完全性 25-5

ループバック 25-9

- CE-100T-8
  - IEEE 802.1Q 24-5
  - LCAS 24-14
  - MTU 24-3
  - STS/VT 割り当てタブ 24-12
  - イーサネット機能 24-2
  - 概要 24-1
  - 最大帯域幅 24-12
  - 統計情報およびカウンタ 24-7
  - プール 24-12
  - フレームバッファリング 24-3
  - フロー制御 24-3
  - 優先キューイング (ToS および CoS) 24-5
  - 容量制限 24-12
  - リンク完全性 24-4
- channel-group コマンド 10-4, 10-6
- Cisco HDLC 20-6
- Cisco IOS
  - 1 レベル上に戻る 3-18
  - イネーブル EXEC モード 3-16
  - イメージのアップグレード 1-6
  - インターフェイス コンフィギュレーション モード 3-16
  - グローバル コンフィギュレーション モード 3-16
  - コマンドモード 3-16 3-18
  - コマンドの表示 3-18
  - スタートアップ コンフィギュレーション ファイル 3-11
  - ソフトウェアの基礎 3-16
  - ユーザ EXEC モード 3-16
  - ライン コンフィギュレーション モード 3-17
  - ログイン強化 19-2
- Cisco IOS ソフトウェア イメージ 3-3
- CiscoWorks 22-5
- clear bridge コマンド 6-5
- cos commit コマンド 14-18
- CoS ベース QoS 14-18
- CoS ベース パケットの統計情報 14-28
- CRC 5-4
- CRC エラー
  - SNMP トラップの設定 21-16
  - SNMP を通じたアクセス 21-16
  - 手動による検証 21-20
  - スレッシュホールドの設定の注意事項 21-16
  - モニタリング 21-16
- CTC
  - CTC での Cisco IOS 3-3
  - POS ポートのプロビジョニング情報 2-4
  - POS 統計情報 2-2
  - SONET 回線の設定 2-7
  - SONET アラーム 2-5
  - イーサネット ポートのプロビジョニング情報 2-3
- D
  - Diffusing Update Algorithm ( DUAL ) 11-21
  - DRPRI
    - 概要 1-6, 17-34
    - 設定 17-36
    - 特性 17-35
    - モニタリングと確認 17-42
    - 例 17-37
  - DUAL 有限状態マシン、EIGRP 11-22
- E
  - E シリーズ カード
    - EtherSwitch
      - シングルカード 23-16
      - マルチカード 23-15
    - IEEE 802.1Q 23-20
    - IEEE 802.3z フロー制御 23-18
    - Q タギング 23-20
    - RMON アラームスレッシュホールド 23-30
    - VLAN カウンタ 23-19
    - VLAN サポート 23-19
    - アプリケーション 23-15
    - 回線保護 23-26
    - 共有パケットリング 23-28
    - 手動クロスコネク ト 23-29
    - シングルカード EtherSwitch 23-16
    - スパニングツリー ( STP ) 23-23
    - 専用カプセル化 20-6
    - ハブアンドスポーク構成のイーサネット回線 23-28
    - フロー制御 23-18
    - ポイントツーポイント回線 23-27
    - ポート マップ 23-17
    - マルチカード EtherSwitch 23-15
    - 優先キューイング 23-21

- リニア マッパー 23-17
- レイヤ 2 スイッチング 23-15
- EIGRP
  - インターフェイス パラメータ、設定 11-25
  - コンポーネント 11-22
  - 設定 11-24
  - 説明 11-21
  - デフォルト設定 11-22
  - 認証 11-26
  - モニタリング 11-27
- Enhanced IGRP
  - EIGRP を参照
- EoMPLS 18-1
- EtherChannel
  - カプセル化の設定 10-9
  - サポートされるポート チャネル 10-2
- Ethernet Wire Service (EWS) 9-8
  
- F
  
- FEC
  - カプセル化の設定 10-9
  - サポートされるポート チャネル 10-2
  - 設定 10-3
  - 注意 10-2
- FPGA 2-6
- FPGA バージョン 2-6
  
- G
  
- G シリーズ カード
  - Gigabit EtherChannel (GEC) 23-5
  - STS-24c/VC4-8c の制限 23-8
  - アプリケーション 23-1
  - 回線 23-8
  - 回線の制限 23-8
  - 個別の自動ネゴシエーションおよびフロー制御 23-4
  - 自動ネゴシエーション 23-4
  - 手動クロスコネク ト 23-9
  - トランスポンダ モード 23-10
  - フレーム バッファリング 23-4
  - フロー制御の基準のプロビジョニング 23-4
  - ポイントツーポイントイーサネット回線 23-8
  - リンク完全性 23-6
- G シリーズに対するトランスポンダ モード 23-10
  
- GEC
  - カプセル化の設定 10-9
  - 設定 10-3, 10-6
  - get-bulk-request 動作 22-4
  - get-next-request 動作 22-4, 22-5
  - get-request 動作 22-4, 22-5
  - get-response 動作 22-4
  - GFP-F フレーミング 1-6, 20-7, 25-9
  - GFP-F フレーミングの設定 5-6
  
- H
  
- HDLC 25-9
- HDLC フレーミングでの CRC の設定 5-6
- hostname コマンド 3-10
  
- I
  
- IEEE 802.1Q トンネリング
  - 説明 9-2
  - 他の機能との互換性 9-5
  - デフォルト 9-5
- IEEE 802.3x
  - フロー制御を参照
- IGMP 11-36
- IGP 11-10
- Interior Gateway Protocol
  - IGP を参照
- Internet Group Membership Protocol
  - IGMP を参照
- IOS
  - Cisco IOS を参照
  - IOS コマンド A-1
  - IP Access Control List
    - ACL を参照
  - ip multicast-routing コマンド 11-37
  - ip pim コマンド 11-37
  - ip radius nas-ip-address 19-19, A-5
  - IP マルチキャスト ルーティング
    - IGMP 11-36
    - PIM 11-36
    - 説明 11-36
  - IP ユニキャスト ルーティング
    - IGP 11-10
    - 管理距離 11-33
    - スタティック ルートの設定 11-33

- IP ルーティング プロトコル、設定作業 11-2
- IP ルート、モニタリング 11-35
- IRB
- BVI 12-2
  - 情報の表示 12-7
  - 設定 12-3
  - 設定についての考慮事項 12-2
  - 説明 12-2
  - モニタリングと確認 12-7
- IS, AINS 25-5
- J**
- J1 バイト 2-7, 25-9
- K**
- keepalive コマンド 5-7
- Kermit プロトコル C-3
- L**
- LCAS 24-14
- LEX カプセル化 20-5, 25-9
- line vty コマンド 3-10
- logging コマンド C-3
- LSA 11-16
- M**
- MAC アドレス 4-2
- match any コマンド 14-13
- match cos コマンド 14-14
- match ip dscp コマンド 14-14
- match ip precedence コマンド 14-14
- MIB
- SNMP によるアクセス 22-5
  - 概要 22-2
- ML シリーズのソフト リセット 3-3
- ML シリーズのハード リセット 3-3
- ML-100T-8 カード
- SDM の設定 15-1
- rmon collection history コマンド 21-5
- MPLS
- VC A-29
  - 設定 18-1
- MSTP トンネリング 9-14
- MSTP、IEEE 802.1D との相互運用性 7-15
- MTU 5-6
- N**
- Not-So-Stubby Area (準スタブ エリア)
- NSSA を参照
- NSSA、OSPF 11-16
- O**
- OSPF
- LSA グループ ページング 11-19
  - network area コマンド 11-3
  - インターフェイス パラメータ、設定 11-14
  - エリア パラメータ、設定 11-16
  - 仮想リンク 11-18
  - 経路集約 11-18
  - 設定 11-3, 11-12
  - 説明 11-10
  - デフォルト設定
    - 設定 11-11
    - メトリック 11-18
    - ルート 11-18
  - プロセス ID 11-3
  - モニタリング 11-21, 11-34
  - ルータ ID 11-20
- P**
- PC、スイッチへの接続 3-7
- Per-VLAN Spanning Tree+ 7-8
- PIM
- 設定 11-37
  - モード 11-36
  - ランデブー ポイント 11-36
- port-channel コマンド 10-2
- POS
- GFP-F フレーミング 1-6, 20-7
  - LEX 20-5
  - ML シリーズの一般的な設定 5-13
  - SONET アラーム 5-7, 5-8
  - インターフェイスの設定 5-4

- 概要 20-2
  - カプセル化タイプ 20-5
  - 説明 5-2
  - 相互運用性 20-3
  - フレーミング 20-7
  - pos report コマンド 5-8
  - pos scramble-spe コマンド 5-10
  - pos trigger delay コマンド 5-9
  - POS チャネル インターフェイス
    - 設定 10-6
    - 注意 10-6
  - PPP/BCP 20-5
  - Protocol Independent Multicast
    - PIM を参照
  - PVST+
    - Per-VLAN Spanning Tree+ を参照
- Q**
- QinQ 9-2
  - QoS ポリシング機能 14-16
- R**
- RADIUS
    - AAA サーバ グループの定義 19-15
    - 概要 19-9
    - サーバの特定 19-10
    - 設定
      - アカウントティング 19-18
      - 許可 19-17
      - サーバ、通信 19-10
      - 通信、グローバル 19-20
      - 認証 19-13
      - 複数の UDP ポート 19-10
    - 設定の表示 19-23
    - 属性
      - ベンダー固有 19-20, 19-22
      - デフォルト設定 19-10
      - ユーザのアクセスしたサービスの追跡 19-18
      - ユーザへのサービスの制限 19-17
  - RADIUS を使用したアカウントティング 19-18
  - RADIUS を使用した許可 19-17
  - RADIUS を使用したログイン認証 19-13
  - Remote Network Monitoring
    - RMON を参照
  - RFC
    - 1058、RIP 11-5
    - 1157、SNMPv1 22-3
    - 1253、OSPF 11-10
    - 1493、Bridge-MIB 22-6
    - 1573、IF-MIB 22-6
    - 1587、NSSA 11-10
  - RIP
    - アダバタイズ 11-5
    - サマリー アドレス 11-9
    - スプリット ホライズン 11-9
    - 設定 11-6
    - 説明 11-5
    - デフォルト設定 11-5
    - 認証 11-8
    - ホップ カウント 11-5
  - RIP のアダバタイズ 11-5
  - RJ-11 と RJ-45 のピンの対応関係 3-6
  - RJ-11/RJ-45 コンソール ケーブル アダプタ 3-6
  - RJ-45 コネクタ、コンソール ポート 3-7
  - RMON
    - CRC エラーのモニタリング 21-16
    - アラームおよびイベントの設定 21-3
    - 概要 21-2
    - ステータスの表示 21-21
    - デフォルト設定 21-3
    - 統計情報
      - グループ イーサネットの収集 21-6
      - グループ履歴の収集 21-5
      - トラップの設定 21-17
  - rmon alarm コマンド 21-4
  - rmon collection stats コマンド 21-6
  - rmon event コマンド 21-3
  - router bgp コマンド 11-4
  - router eigrp コマンド 11-3
  - router isis コマンド 11-31
  - RPF 11-36
  - RPR
    - CoS ベース QoS 14-18
    - Link Fault Propagation ( LFP )
      - 概要 17-30
      - 設定 17-32
      - モニタリングおよび確認 17-33
      - 例 17-30
    - MAC アドレスと VLAN サポート 17-6
    - QoS 14-11, 17-6

- 概要 1-7, 17-2
- 設定 17-7
- デュアル RPR 相互接続
  - DRPRI を参照
- パケット処理動作 17-2
- フレーミング プロセス 17-5
- モニタリングおよび確認 17-19
- リング ラッピング 17-3
- 例 17-8, 17-17
- RSTP
  - BPDU
    - 形式 7-14
    - 処理 7-14
  - IEEE 802.1D との相互運用性
    - 説明 7-15
    - トポロジーの変更 7-15
  - アクティブ トポロジー、決定 7-11
  - 概要 7-10
  - 高速コンバージェンス
    - ポイントツーポイント リンク 7-11
    - ルート ポート 7-11
  - 指定スイッチ、定義 7-10
  - 指定ポート、定義 7-10
  - 提案合意ハンドシェイク プロセス 7-11
  - ポートの役割
    - 説明 7-10
    - 同期化 7-13
  - ルート ポート、定義 7-10
- S
  - script コマンド C-3
  - SDH アラーム 5-7
  - SDM
    - TCAM も参照
    - 設定
      - サイズ 15-3
      - 領域 15-2
  - sdm access-list コマンド 15-3
  - service-policy input コマンド 14-18
  - service-policy output コマンド 14-18
  - service-policy コマンド、トラフィック ポリシー 14-18
  - set cos コマンド 14-17
  - set-request 動作 22-5
  - show bridge verbose コマンド 6-5
  - show bridge コマンド 6-5
  - show interfaces bvi コマンド 12-7
  - show interfaces irb コマンド 12-7
  - show interfaces port-channel コマンド 10-12
  - show ip mroute コマンド 11-37
  - show policy-map コマンド 14-19
  - show rmon alarms コマンド 21-21
  - show rmon events コマンド 21-21
  - show rmon history コマンド 21-21
  - show rmon statistics コマンド 21-21
  - show rmon コマンド 21-21
  - show sdm size コマンド 15-4
  - show snmp group コマンド 22-16
  - show snmp pending コマンド 22-16
  - show snmp sessions コマンド 22-16
  - show snmp user コマンド 22-16
  - show snmp コマンド 22-16
  - show tech-support コマンド C-2
  - show vlans コマンド 8-6
  - SNMP
    - MIB 変数へのアクセス 22-5
    - TFTP サーバによるアクセスの制限 22-14
    - インフォーム
      - イネーブル化 22-13
      - 説明 22-6
      - トラップ キーワード 22-11
      - トラップとの差 22-6
    - エージェント
      - 説明 22-4
      - ディセーブル化 22-8
    - 概要 22-2, 22-5
    - グループ 22-7, 22-10
    - コミュニティ スtringing
      - 概要 22-5
      - 設定 22-8
    - サポートするバージョン 22-3
    - システム コンタクトおよびロケーション 22-14
    - ステータス、表示 22-16
    - 設定の注意事項 22-7
    - 設定例 22-15
    - 通知 22-6
    - デフォルト設定 22-7
    - トラップ
      - ifIndex 番号、判別 21-18
      - イネーブル化 22-11
      - インフォームとの差 22-6

- 概要 22-3, 22-5
- 設定 21-16
- 説明 22-2, 22-6
- タイプ 22-11
- トラップ マネージャ、設定 22-11
- ホスト 22-7
- マネージャの機能 22-4
- ユーザ 22-7, 22-10
- snmp-server community コマンド 22-9
- snmp-server contact コマンド 22-14
- snmp-server enable traps コマンド 22-13
- snmp-server engineID コマンド 22-10
- snmp-server group コマンド 22-10
- snmp-server host コマンド 22-12
- snmp-server location コマンド 22-14
- snmp-server queue-length コマンド 22-13
- snmp-server tftp-server-list コマンド 22-14
- snmp-server trap-source コマンド 22-13
- snmp-server trap-timeout コマンド 22-13
- snmp-server user コマンド 22-11
- SNMPv2C 22-4
- SONET アラーム 5-7
- SSH
  - 設定 19-3
- STP
  - BPDU メッセージ交換 7-3
  - IEEE 802.1Q トランクの限界 7-8
  - インターフェイスのステート
    - 概要 7-6
    - ディセーブル 7-8
    - フォワーディング 7-7, 7-8
    - ブロッキング 7-7
    - ラーニング 7-7
    - リスニング 7-7
  - 下位 BPDU 7-3
  - 概要 7-2
  - 拡張システム ID
    - 概要 7-4
    - 予期しない動作 7-17
  - サポートされているスパニングツリー インスタンスの数 7-3, 7-10
  - 指定スイッチ、定義 7-3
  - 指定ポート、定義 7-3
  - 冗長接続 7-8
  - ステータスの表示 7-22
- 設定
  - Hello タイム 7-20
  - スイッチ プライオリティ 7-19
  - 転送遅延時間 7-21
  - パス コスト 7-18
  - ポート プライオリティ 7-18
  - ルート スイッチ 7-17
  - タイマー、説明 7-5
  - ディセーブル化 7-17
  - デフォルト設定 7-16
  - 転送遅延タイマー 7-7
  - マルチキャスト アドレス、影響 7-8
  - 優位 BPDU 7-3
  - ルート スイッチ
    - 拡張システム ID の影響 7-4
    - 選出 7-4
    - 予期しない動作 7-17
  - ルート ポート、定義 7-3
  - レイヤ 2 プロトコル トンネリング 9-13
  - STP のパス コスト 7-18
  - SW-LCAS 5-4, 25-7
  - Syslog サーバ C-3
- T
- TCAM
  - SDM も参照
  - アプリケーション領域 15-2
  - スイッチング情報 15-2
  - スペース 15-2
- Ternary Content Addressable Memory
  - TCAM も参照
- TFTP
  - サーバによるアクセスの制限 22-14
- V
- VC4/VC LO 割り当て 24-12
- VCAT
  - VCAT グループ (VCG) 25-7
  - 固定 VCG 25-7, 25-8
  - 特性 25-7
  - フレキシブル VCG 25-7
- VC、インターフェイスの割り当て A-29
- VLAN
  - IEEE 802.1Q の設定 8-3

- STP と IEEE 802.1Q トランク 7-8
  - エージング ダイナミック アドレス 7-9
  - サービスプロバイダー ネットワークのカスタマー番号 9-4
  - システムごとの数 8-2
  - トランク ポート 8-2
  - VLAN 固有サービス 9-8
  - VRF Lite
    - 概要 13-2
    - 設定 13-3
    - モニタリングと確認 13-9
    - 例 13-4
  - VTP レイヤ 2 プロトコル トンネリング 9-13
  - vtv 3-5
- X
- xconnect コマンド A-29
- あ
- アダプタ ケーブル 3-6
  - アドレス
    - ダイナミック
      - 加速されたエージング 7-9
      - デフォルトのエージング 7-9
    - マルチキャスト、STP アドレス管理 7-8
  - アラーム 5-7
  - アラーム、RMON 21-3
- い
- イーサネット
    - オーバーサブスクライブ 25-3
    - クロッキング 20-12
    - 自動ネゴシエーション 25-3
    - フレームバッファリング 24-3, 25-3
    - フロー制御 25-3
  - イーサネットの設定作業 4-6
  - イネーブル EXEC モード 3-16
  - イネーブル シークレット パスワード 3-9
  - イネーブル パスワード 3-9
  - イネーブル モード 3-16
  - イベント、RMON 21-3
  - インターネット プロトコル マルチキャスト
    - IP マルチキャスト ルーティングを参照
  - インターフェイス コンフィギュレーション モード 3-16
  - インターフェイス パラメータ、設定
    - EtherChannel 10-3
    - 概要 4-2, 4-4
  - インターフェイス ポート ID 4-3
- え
- エージング タイム、STP 用に加速 7-9
  - エラー メッセージ、記録 C-3
  - エリア境界ルータ
    - ABR を参照
- お
- オーバーサブスクライブ 25-3
- か
- カードの説明 1-2
  - 回線定義 23-9
  - 拡張システム ID、STP 7-4
  - 拡張状態モデル (ESM) 25-6
  - 拡張パフォーマンス モニタリング 14-28
  - 確認
    - IP マルチキャストの動作 11-37
    - VLAN の動作 8-6
  - 仮想 LAN
    - VLAN を参照
  - カプセル化 5-4
    - EtherChannel の設定 10-9
    - IEEE 802.1Q VLAN の設定 8-3
  - 監査証跡 19-2
  - 管理オブション
    - SNMP 22-2
  - 管理距離
    - OSPF 11-18
    - ルーティング プロトコルのデフォルト 11-33
  - 管理ポート
    - コンソール ポートも参照
    - 設定 3-9

- き
- ギガビット イーサネット
    - インターフェイスの設定 4-8, 4-9
    - 自動ネゴシエーションの設定 4-8, 4-9
  - 機能一覧 1-3
  - キューイング 24-5
  - 近接ルータ検出 / 回復、EIGRP 11-22
- く
- グローバル コンフィギュレーション モード 3-16
  - クロッキング許容値 20-12
- け
- 経路集約、OSPF 11-18
  - ケーブル、RJ-11/RJ-45 アダプタ 3-6
- こ
- 高信頼性転送プロトコル、EIGRP 11-22
  - コマンド
    - access-list 22-9
    - bridge irb 12-3
    - bridge priority 6-3
    - bridge protocol drpri-rstp A-2
    - channel-group 10-4, 10-6
    - clear bridge 6-5
    - hostname 3-10
    - interface bvi 12-3
    - interface spr 1 A-4
    - ip multicast-routing 11-37
    - ip pim 11-37
    - ip radius nas-ip-address A-5
    - line vty 3-10
    - microcode fail system-reload A-6
    - rmon collection history 21-5
    - network area 11-3
    - rmon collection stats 21-6
    - rmon event 21-3
    - rmon アラーム 21-4
    - router bgp 11-4
    - router eigrp 11-3
    - show bridge 6-5
    - show bridge verbose 6-5
    - show interfaces bvi 12-7
    - show interfaces irb 12-7
    - show interfaces port-channel 10-12
    - show ip mroute 11-37
    - show rmon 21-21
    - show rmon alarms 21-21
    - show rmon events 21-21
    - show rmon history 21-21
    - show rmon statistics 21-21
    - show sdm size 15-4
    - show snmp 22-16
    - show snmp group 22-16
    - show snmp pending 22-16
    - show snmp sessions 22-16
    - show snmp user 22-16
    - show tech-support C-2
    - show vlan 8-6
    - snmp-server community 22-9
    - snmp-server contact 22-14
    - snmp-server enable traps 22-13
    - snmp-server engineID 22-10
    - snmp-server group 22-10
    - snmp-server host 22-12
    - snmp-server location 22-14
    - snmp-server queue-length 22-13
    - snmp-server tftp-server-list 22-14
    - snmp-server trap-source 22-13
    - snmp-server trap-timeout 22-13
    - snmp-server user 22-11
    - spr drpri-id A-24
    - spr station-id A-27
    - spr wrap A-28
    - spr-intf-id A-25
    - 表示 3-18
    - ブリッジグループ 4-6, 4-8, 4-9, 4-10, 6-3, 18-10
    - ブリッジ プロトコル 6-3, 18-10
    - リファレンスの章 A-1
  - コマンドの短縮 3-18
  - コミュニティ スtring
    - 概要 22-5
    - 設定 22-8
  - コンソール ポートのディセーブル化 19-2
  - コンソール ポートへの接続 3-6
  - コンソール ポート、接続 3-6
  - コンフィギュレーション ファイル
    - TFTP サーバのアクセス制限 22-14

- システム コンタクトおよびロケーションの情報  
22-14
- コンフィギュレーション モード
  - グローバル 3-16
  - ライン 3-17
- さ
- サービスプロバイダー ネットワーク
  - IEEE 802.1Q トンネリング 9-2
  - カスタマー VLAN 9-3
  - レイヤ 2 プロトコル 9-13
- サポート、テクニカル
  - テクニカル サポートを参照
- し
- システム MTU
  - IEEE 802.1Q トンネリング 9-5
- 自動ネゴシエーション 25-3
- 出力プライオリティ マーキング 14-8
- 受動インターフェイス OSPF 11-18
- 自律システム境界ルータ
  - ASBR を参照
- す
- スタートアップ コンフィギュレーション ファイル  
3-11
- スタートアップ コンフィギュレーション ファイルの復元 3-13
- スタティック ルート、設定 11-33
- スタブエリア、OSPF 11-16
- せ
- 接続手順 3-6 3-8
- 設定
  - BVI 12-3
  - EtherChannel カプセル化 10-9
  - IP 11-1
  - IP マルチキャスト 11-36
  - VLAN 8-2
  - インターフェイス、概要 4-2
  - 管理ポート 3-9
- 統合ルーティングとブリッジング
  - IRB を参照
  - ホスト名 3-10
- 設定の注意事項
  - SNMP 22-7
- 設定例
  - RPR 17-8, 17-17
  - SNMP 22-15
- そ
- 送信元 23-9
- 属性、RADIUS
  - ベンダー固有 19-20, 19-22
- ソフトリセット 24-2, 25-2
- 疎モード、PIM 11-36
- た
- 帯域幅コマンドトラフィック クラス 18-5
- ダイナミック アドレス
  - アドレスを参照
- タグ付きパケット、レイヤ 2 プロトコル 9-13
- 端末
  - スイッチへの接続 3-7
  - 端末エミュレーション ソフトウェア 3-6
  - ルータ出力の記録 C-3
- て
- データベースの復元 3-13
- テクニカル サポート
  - FTP サービス C-3
  - show tech-support コマンド C-2
  - データの収集 C-2
  - データの提供 C-3
  - ルータ出力の記録 C-3
- 手順、接続 3-6 3-8
- デフォルト設定
  - EIGRP 11-22
  - OSPF 11-11
  - RADIUS 19-10
  - RIP 11-5
  - RMON 21-3
  - SNMP 22-7

STP 7-16  
 レイヤ 2 プロトコル トンネリング 9-14  
 デフォルトのマルチキャスト QoS 14-26  
 電子メール、テクニカル サポート C-3

## と

## 統計情報

RMON グループ イーサネット 21-6  
 RMON グループ履歴 21-5  
 SNMP 入出力 22-16  
 統計情報、OSPF 11-21, 11-34  
 統合ルーティングとブリッジング

IRB を参照

## トラップ

イネーブル化 22-11  
 概要 22-3, 22-5  
 通知タイプ 22-11  
 定義 22-4  
 マネージャの設定 22-11  
 トラフィック クラス 14-13  
 トラフィック ポリシー  
 インターフェイス、適用 14-18  
 作成 14-14

トランク ポート 8-2

## ドロップ

説明 23-9

## トンネリング

IEEE 802.1Q 9-2  
 定義 9-1  
 レイヤ 2 プロトコル 9-13  
 トンネル ポート  
 IEEE 802.1Q、設定 9-5, 9-15, 9-16  
 説明 9-2  
 他の機能との非互換性 9-5

## に

## 二重タグ付きパケット

IEEE 802.1Q トンネリング 9-3  
 レイヤ 2 プロトコル トンネリング 9-14  
 入力プライオリティ マーキング 14-9

## 認証

## RADIUS

鍵 19-11  
 ログイン 19-13

## ね

ネットワーキング プロトコル、IP マルチキャスト ルーティング 11-36

## ネットワーク管理

RMON 21-1

SNMP 22-1

ネットワーク要素のデフォルト 24-3, 25-3

## は

## バーチャル コンカチネーション

VCAT を参照

パスワード 3-9

## ふ

## ファスト イーサネット

インターフェイスの設定 4-6

プライオリティ マルチキャスト QoS 14-25

## ブリッジ

機能一覧 1-3

設定 6-4

## トランスペアレント

bridge CRB モード 6-8

bridge IRB モード 6-10

IP routing モード 6-6

no IP routing モード 6-8

概要 6-6

モニタリングと確認 6-5

ブリッジグループ、ルーティング 12-2

フレーミングモード 5-4

フレームバッファリング 25-3

フロー制御 24-3, 25-3

プロトコル依存型モジュール、EIGRP 11-22

## ほ

## ボーダー ゲートウェイ プロトコル

BGP を参照

ポート ID 4-3

ポート チャネル 10-2

ポート プライオリティ、STP 7-18

## ま

- マルチキャスト QoS 14-25
- マルチキャスト プライオリティ キューイング  
14-25
- マルチキャスト、IP  
IP マルチキャスト ルーティングを参照

## み

- 密モード、PIM 11-36

## め

- メッセージの記録 C-3
- メディア アクセス制御アドレス  
MAC アドレスを参照
- メトロ タグ 9-3

## も

- モジュラ QoS コマンドライン インターフェイス  
設定 14-13
- 設定、確認 14-19
- 設定（例） 14-20
- モニタリング
  - EIGRP 11-27
  - IEEE 802.1Q トンネリング 9-16
  - IP ルート 11-35
  - OSPF 11-21, 11-34
  - トラフィック フロー 21-2
  - トンネリング 9-16
  - レイヤ 2 プロトコル トンネリング 9-16

## ゆ

- ユーザ EXEC モード 3-16
- 優先キューイング 24-5

## ら

- ランデブー ポイント 11-36

## り

- リモート端末、ルータ出力の記録 C-3
- リンク完全性 24-4, 25-5

## る

- ルータ ID、OSPF 11-20
- ルータ出力の記録 C-3
- ルーティング プロトコルの管理距離 11-33
- ルート計算タイマー、OSPF 11-18

## れ

- レイヤ 2 の機能一覧 1-3
- レイヤ 2 プロトコル トンネリング 9-14
  - 設定 9-14
  - 注意事項 9-14
  - 定義 9-13
  - デフォルト設定 9-14
- レイヤ 3 の機能一覧 1-5

## ろ

- ログイン強化 19-2