

# Cisco Systems Intelligent Gigabit Ethernet Switch Module for IBM **@**server BladeCenter

カッパー・イーサネット・スイッチング・  
テクノロジーを BladeCenter シャーシに統合

構成および  
トラブルシューティング

CMS および CLI を  
使用した構成例



Rufus Credle  
Yoko Fujiwara  
Matt Slavin  
Kenichi Tanaka  
Mark Welch





International Technical Support Organization

**Cisco Systems Intelligent Gigabit Ethernet Switch  
Module for IBM @server BladeCenter**

**お願い：**本書および本書で紹介する製品をご使用になる前に、『特記事項』（vii ページ）に記載されている情報をお読みください。

本書は、Cisco Systems Intelligent Gigabit Ethernet Switch Module for the IBM **@server** BladeCenter に適用されます。

IBM 発行のマニュアルに関する情報のページ  
<http://www.ibm.com/jp/manuals/>

こちらから、日本語版および英語版のオンライン・ライブラリーをご利用いただけます。また、マニュアルに関するご意見やご感想を、上記ページよりお送りください。今後の参考にさせていただきます。  
(URL は、変更になる場合があります)

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： REDP-3869-00  
International Technical Support Organization  
Cisco Systems Intelligent Gigabit Ethernet Switch  
Module for IBM Eserver BladeCenter

発行： 日本アイ・ビー・エム株式会社

担当： ナショナル・ランゲージ・サポート

第 1 刷 2006.7



# 目次

特記事項 .....	vii
商標 .....	viii
前書き .....	ix
この redbook の執筆チーム .....	ix
執筆にご協力ください .....	xi
コメントをお寄せください .....	xii
 第 1 章 要旨 .....	1
 第 2 章 IBM eServer BladeCenter の概要 .....	3
2.1 IBM eServer BladeCenter のアーキテクチャー .....	6
2.1.1 ミッドプレーン .....	6
2.1.2 管理モジュールのイーサネット .....	6
2.1.3 Gigabit Ethernet パス .....	7
2.2 IBM eServer HS20 のアーキテクチャー .....	8
2.3 スタンドアロン構成ツール .....	10
 第 3 章 Cisco Systems Intelligent Gigabit Ethernet Switch Module .....	11
3.1 製品説明 .....	12
3.2 提案の価値 .....	12
3.3 製品の機能 .....	13
3.3.1 スイッチ管理 .....	13
3.3.2 ポート機構 .....	14
3.3.3 パフォーマンス機能 .....	14
3.3.4 冗長性 .....	14
3.3.5 VLAN サポート .....	15
3.3.6 セキュリティ .....	15
3.3.7 サービス品質 (QoS) およびサービス・クラス (CoS) .....	16
3.3.8 モニター .....	16
3.3.9 ネットワーク・ケーブル .....	17
3.3.10 サポートされる IEEE ネットワーク標準 .....	17
 第 4 章 Cisco Systems Intelligent Gigabit Ethernet Switch Module のアーキテクチャー ....	19
4.1 Cisco Systems Intelligent Gigabit Ethernet Switch Module のブロック・ダイアグラム ....	22
 第 5 章 Cisco Systems IGESM の管理とユーザー・オリエンテーション .....	23
5.1 Cisco Systems IGESM のユーザー・インターフェース .....	24
5.1.1 コマンド行インターフェース .....	25
5.1.2 Cisco Systems Intelligent Gigabit Ethernet Switch Module ホーム .....	29
5.1.3 Cisco Systems IGESM Cluster Management Suite .....	29
5.1.4 Cisco Systems Intelligent Gigabit Ethernet Switch Module のツール .....	39
5.1.5 Cisco Systems Intelligent Gigabit Ethernet Switch Module のヘルプ・リソース .....	40
5.2 システム管理に関する考慮事項 .....	40
5.2.1 アウト・オブ・バンド管理の定義 .....	40
5.2.2 インバンド管理の定義 .....	41
5.2.3 Cisco Systems IGESM への管理トラフィックのパス .....	41
5.2.4 Cisco Cluster Management Suite .....	45
5.2.5 CiscoWorks LAN Management Solution .....	53
5.2.6 CiscoView .....	54

5.2.7 IBM Director および Remote Deployment Manager .....	55
5.3 管理パスに関する詳細説明.....	56
5.3.1 管理に関する詳細説明の概要 .....	56
5.3.2 この詳細説明を執筆した理由 .....	56
5.3.3 一般的な管理パスの設計上の考慮事項 .....	58
5.3.4 考慮事項: IGESM の管理に管理モジュールのアップリンクを使用する場合 .....	60
5.3.5 考慮事項: IGESM アップリンクを使用した IGESM の管理.....	63
5.3.6 考慮事項: 特定の BladeCenter 内に複数の IGESM がある場合 .....	64
5.3.7 シナリオ 1 (推奨).....	66
5.3.8 シナリオ 2 (推奨).....	67
5.3.9 シナリオ 3 (推奨).....	70
5.3.10 シナリオ 4 (考えられる代替案).....	72
5.3.11 シナリオ 5 (非推奨).....	74
5.3.12 シナリオ 6 (非推奨).....	76
5.3.13 シナリオ 7 (評価テスト環境として使用可能).....	78
<b>第 6 章 IBM eServer BladeCenter システムの初期セットアップ .....</b>	<b>83</b>
6.1 IBM eServer BladeCenter システム .....	84
6.1.1 管理モジュールのファームウェア .....	84
6.1.2 管理モジュールのネットワーク・インターフェース .....	84
6.1.3 入出力モジュールの管理タスク .....	87
6.2 ブレード・サーバーの初期構成.....	93
6.2.1 ファームウェアの更新 .....	93
6.2.2 オペレーティング・システム .....	95
6.2.3 Broadcom Advanced Control Suite のインストール.....	100
6.3 この例で使用したファームウェアとデバイス・ドライバ.....	102
<b>第 7 章 Cisco Systems IGESM の構成およびネットワーク統合.....</b>	<b>103</b>
7.1 構成および統合の概要.....	104
7.1.1 Cisco Systems スイッチに習熟したユーザー向けの説明 .....	104
7.2 管理ネットワークに関する考慮事項.....	109
7.3 この章で使用される例の基本構成.....	110
7.3.1 本書の制作に使用されたハードウェアとソフトウェア .....	110
7.3.2 事前構成の準備 (基本構成情報) .....	111
7.4 BladeCenter を Cisco インフラストラクチャーに接続するためのガイドライン.....	121
7.4.1 ガイドラインとコメント .....	121
7.4.2 構成例に関する予備情報 .....	125
7.5 トポロジーと構成の例.....	129
7.5.1 トポロジー 1: デュアル IGESM、2 つの 6500 に対する 4 ポート・アグリゲーション .....	129
7.5.2 トポロジー 2: デュアル Cisco Systems IGESM、2 つの 6500 に対する 2 ポート・アグリゲーション .....	145
7.5.3 トポロジー 3a: デュアル Cisco Systems IGESM、RSPAN を使用した 2 ポート・アグリゲーション .....	170
7.5.4 トポロジー 3b: 直接相互接続の使用を除いてはトポロジー 3a と同様.....	186
7.6 各種ブレード・サーバー構成.....	199
7.7 トランク・フェイルオーバー機能の説明と構成.....	203
7.7.1 トランク・フェイルオーバーの概要 .....	203
7.7.2 トランク・フェイルオーバーを使用したトポロジー 1 の例 .....	205
7.7.3 トランク・フェイルオーバーを使用したトポロジー 2 の例 .....	207
7.8 Serial over LAN 機能の説明および構成.....	209
7.8.1 Serial over LAN の概要 .....	210
7.8.2 Serial over LAN の構成 .....	211

<b>第 8 章 Cisco Systems IGESM のトラブルシューティング</b> .....	213
8.1 基本的な規則と固有の現象.....	214
8.1.1 基本的な規則.....	214
8.1.2 具体的な問題と解決策.....	214
8.2 IGESM のトラブルシューティングの概要.....	216
8.2.1 トラブルシューティングに関する全般的な注意.....	217
8.2.2 テクニカル・サポートに役立つ情報.....	218
8.3 ハードウェアの問題が考えられる場合のトラブルシューティング.....	218
8.4 ソフトウェアの問題が考えられる場合のトラブルシューティング.....	221
8.5 構成の問題が考えられる場合のトラブルシューティング.....	221
8.6 便利な IOS CLI トラブルシューティング・コマンド.....	223
8.6.1 データの収集.....	223
8.6.2 管理.....	226
8.6.3 トラブルシューティング.....	226
<b>第 9 章 サービスおよびサポート</b> .....	235
9.1 IBM に連絡する.....	236
9.2 オンライン・サービス.....	236
9.3 発注について.....	236
9.4 その他のサポート・サイト.....	237
<b>付録 A. ヒント</b> .....	239
ブレード・サーバーの NIC の番号付け.....	239
マルチホーム・サーバー上でのデフォルト・ゲートウェイの構成.....	240
重複 IP アドレス: その 1.....	241
重複 IP アドレス: その 2.....	242
チーミングソフトウェアの選択項目がキャンセルできない.....	243
Cisco Systems IGESM が switch: プロンプトで停止する.....	244
ブレード・サーバー間を切り替えるためのキー・シーケンス.....	245
ネイティブ VLAN ミスマッチ・メッセージ.....	245
Cisco Systems IGESM 上での RSPAN の使用.....	246
IGESM からの管理モジュール設定値の検出.....	246
Redhat tg3 ドライバーに関連して起こりうる問題.....	249
Hyperterm からのコンソールポートアクセスに関する問題.....	249
デフォルトの EtherChannel ロード・バランシングが最適でない場合がある.....	250
IGESM IP アドレス情報の制御.....	250
A.1 12.1(14) 以降のコードの使用.....	251
BladeCenter に関するその他のヒント.....	251
<b>関連資料</b> .....	253
IBM Redbooks.....	253
その他の資料.....	253
オンライン・リソース.....	254
IBM Redbooks を入手する方法.....	256
IBM が提供するヘルプ.....	256
<b>省略語および頭字語</b> .....	257
<b>索引</b> .....	259





# 特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権（特許出願中のものを含む）を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒106-0032 東京都港区六本木 3-2-31 IBM World Trade Asia Corporation Licensing

以下の保証は、国または地域の法律に沿わない場合は、適用されません。IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾：

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。お客様は、IBM のアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。

## 商標

以下は、IBM Corporation の商標です。

AIX®  
BladeCenter™  
Domino®  
Electronic Service Agent™  
Enterprise Storage Server®  
@server®  
eServer®

eServer™  
HelpCenter®  
HelpWare®  
ibm.com®  
IBM®  
IntelliStation®  
NetVista™

Redbooks (ロゴ) ™  
Redbooks™  
ServerGuide™  
ThinkPad®  
Tivoli®  
TotalStorage®  
xSeries®

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

Java およびすべての Java 関連の商標およびロゴは、Sun Microsystems, Inc. の米国およびその他の国における商標または登録商標です。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

Intel および Intel Inside (ロゴ) は、Intel Corporation の米国およびその他の国における商標です。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.

# 前書き

この IBM® Redpaper では、Cisco Systems Intelligent Gigabit Ethernet Switch Module for the IBM® eServer® BladeCenter™ の位置付けを示し、お客様の既存データ・ネットワークへのシームレスなインターフェースを提供するこの製品が、BladeCenter の提案する価値をどのように高めるかについて説明します。

本書では、数種類のネットワーク・トポロジを対象に、Cisco Systems Intelligent Gigabit Ethernet Switch Module の計画、インストール、および構成に役立つ情報を示します。トポロジーの例を示して、スイッチ・モジュールをさまざまなネットワークに統合するための方法をいくつか解説しています。

また、Cisco Systems Intelligent Gigabit Ethernet Switch Module および BladeCenter のアーキテクチャ、および既存の Cisco Data Center で完全な相互運用性を実現する各製品のテクノロジーの連携についても説明します。

本書の対象読者としては、既存のネットワークに Cisco Systems Intelligent Gigabit Ethernet Switch Module を正しく統合するために本書を使用する、経験を積んだシステム管理者とネットワーク管理者を想定しています。

この Redpaper の執筆時点で、Cisco Systems Intelligent Gigabit Ethernet Switch Module は IOS の 12.1(14) バージョンをサポートしています。このスイッチは、12.1(22) バージョンもサポートします。サポートされる IOS の最新バージョンについては、ibm.com® にある次のサポート・サイトをご覧ください。

<http://www.ibm.com/servers/eserver/support/bladecenter/index.html>

## この redbook の執筆チーム

この redbook は、International Technical Support Organization, San Jose Center、および Cisco San Jose に勤務する、世界中から集まった専門家のチームによって制作されました。



**Rufus Credle** は、International Technical Support Organization, Raleigh Center に勤務する認定上級 IT スペシャリスト、認定プロフェッショナル・サーバー・スペシャリストです。研修生を指揮して、ネットワーク・オペレーティング・システム、ERP ソリューション、音声テクノロジー、高可用性クラスタリング・ソリューション、Web アプリケーション・サーバー、パーベイスブ・コンピューティング、IBM および OEM の e-business アプリケーションに関する Redbooks™ を制作しています。これらはすべて、IBM eServer™ xSeries® システムおよび IBM eServer BladeCenter システムを実行する製品です。Rufus 氏は IBM でのキャリアの中でさまざまな業務に携わり、業務管理、財務管理、システム・エンジニアリング、営業とマーケティング、IT サービスなどの分野で活躍しました。セントオーガスティン大学でビジネス・マネージメントの理学士号を取得しました。Rufus 氏は、IBM に 24 年間勤務しています。



**Yoko Fujiwara** は、東京の晴海に勤務する、日本 IBM の IBM eServer xSeries 技術支援の主任 IT スペシャリストです。IA サーバーのプレセールス技術支援に 6 年の経験があり、2002 年の製品販売開始以来 BladeCenter を中心とした職務に携わっています。専門分野はシステム管理などです。IBM Redbook *「Implementing Systems Management Solutions Using IBM Director」* (SG24-6188) の共著者であり、Cisco Certified System Network Associate などの認定を受けています。



**Matt Slavin** は、オクラホマ州タルサに勤務するシステム・エンジニアで、Cisco Systems の戦略的アライアンス・グループの一員として働いています。コンピューターおよびネットワークの業界で 25 年を超える経験があり、いくつかのハイレベル技術支援業務を担当しました。MCSE、MCNE、CCNA、CCIP などの業界認定を受けています。Matt 氏が現在関心を持っている分野はインフラストラクチャーの設計およびサポートで、特にワイヤレス・ネットワークとセキュリティに重点を置いています。



**Kenichi Tanaka** は、日本 IBM 幕張事業所に勤務する、日本 IBM システムズ・エンジニアリングのネットワーク・システム部門に所属する IT スペシャリストです。ネットワークに 3 年の経験があり、ネットワーク製品、設計、および実装に関する技術支援を提供しています。専門分野には、Cisco ネットワーク製品と F5 Networks のロード・バランサーが含まれます。Cisco Certified Network Professional などの業界認定を受けており、東京都立大学で電子情報工学の学位を取得しました。



**Mark Welch** は、ノースカロライナ州 RTP の IBM に勤務する、IBM eServer BladeCenter 開発グループの主任開発者です。Mark 氏は、IBM ネットワーク・ハードウェア部門、IBM グローバル・サービス、および IBM eServer xSeries サーバーで 15 年を超えるネットワーク経験があります。専門分野は、ネットワークの相互運用性とテストです。フロリダ・アトランティック大学でコンピューター・プログラミングの応用理学士号を取得し、Cisco System Network Associate、Nortel Networks Certified Design Specialist、Nortel Networks Certified Account Specialist などの認定を受けています。

このプロジェクトにご協力いただいた次の方々に感謝いたします。

Margaret Ticknor、Jeanne Tucker、Tamikia Barrow  
International Technical Support Organization, Raleigh Center

Deanna Polm、Sangam Racherla、Maritza Dubec  
International Technical Support Organization, San Jose Center

Ishan Sehgal、Worldwide BladeCenter Marketing, IBM Systems and Technology Group  
IBM RTP

Ed Bowen、主任技術者、Internetworking Alliance  
IBM RTP

Mauricio Arregoces、技術マーケティング・マネージャー、エンタープライズ・ソリューション設計  
Cisco Systems San Jose

Ted Odgers、ビジネス開発、Cisco Systems Strategic Alliance Group  
Cisco Systems RTP

Glenn Wilkinson、マネージャー、Cisco Systems Strategic Alliance Group  
Cisco Systems RTP

Anthony Sager、ビジネス開発ディレクター、CTO Cisco Alliance  
IBM Poughkeepsie

Vinay Gundi、ソフトウェア・エンジニア、エンタープライズ・ソリューション設計  
Cisco Systems San Jose

Chris Verne、マネージャー、BladeCenter エコシステム開発、IBM Systems Group  
IBM RTP

Norm Strole、STSM-BladeCenter 開発  
IBM RTP

Mark Allen、エンタープライズ・ソリューション設計  
Cisco Systems San Jose

Albert Mitchell、技術リーダー、EAG Desktop Switch Business Unit  
Cisco Systems San Jose

Charles Wu、ソフトウェア・エンジニア、EAG Desktop Switch Business Unit  
Cisco Systems San Jose

Edward Suffern、BladeCenter イーサネット・スイッチング  
IBM RTP

Pritesh Patel、マネージャー、ソフトウェア開発、EAG Desktop Switch Business Unit  
Cisco Systems San Jose

Amit Sanyal、製品マーケティング・マネージャー、EAG Desktop Switch Business Unit  
Cisco Systems San Jose

Damon West、IBM PC Institute  
IBM RTP

Chris Durham、BladeCenter 開発、IBM Systems Group  
IBM RTP

Khalid Ansari、ストレージ・ネットワークング・サポート、LAN/ATM スイッチ・サポート、  
BISC チーム  
IBM RTP

Robert Jakes、BISC チーム - (Blade Infrastructure Solutions Center)  
IBM RTP

Kazumasa Norihashi、ネットワーク・システム担当マネージャー、Systems Design Center  
日本 IBM

Nobukazu Kamei、マネージャー、xSeries 技術支援  
日本 IBM

Vahid Mehr、ビジネス開発マネージャー、Cisco Systems Strategic Alliance Group  
Cisco San Jose

Derek Owens、システム・エンジニア、Cisco Systems Strategic Alliance Group  
Cisco New York

## 執筆にご協力ください

2 週間から 6 週間の研修プログラムに加わりませんか。特定の製品またはソリューションを扱う IBM Redbook の作成を手伝い、最先端のテクノロジーを実地体験できます。IBM の技術プロフェッショナル、ビジネス・パートナー、およびお客様と、チームとして協働できます。

ご協力いただければ、製品の受容性とおお客様の満足度の向上につながります。また、IBM 開発研究所の技術者と技術交流することもできます。生産性と市場性が向上します。

研修プログラムの詳細は、次の URL でプログラムのインデックスをご覧の上、オンラインにてお申し込みください。

[ibm.com/redbooks/residencies.html](http://ibm.com/redbooks/residencies.html)

## コメントをお寄せください

お客様のコメントを大切にしています。

弊社では、Redbooks を可能な限り役に立つものにしていきたいと考えています。当 Redbooks や他の Redbook に関するコメントを、次のいずれかの方法でお送りください。

- ▶ 次のアドレスにある「**Contact us**」をクリックして、オンラインの Redbook レビュー・フォームにアクセスしてください。

[ibm.com/redbooks](http://ibm.com/redbooks)

- ▶ 次の宛先に、E メールでコメントをお寄せください。

[redbook@us.ibm.com](mailto:redbook@us.ibm.com)

- ▶ 次の宛先に、手紙でコメントをお寄せください。

IBM Corporation, International Technical Support Organization  
Dept. HQ7 Building 662  
P.O. Box 12195  
Research Triangle Park, NC 27709-2195



## 要旨

IBM と Cisco は、サーバーおよびネットワーク・テクノロジーの統合に関連したお客様の要件に対応するために、戦略的アライアンスに力を注いでいます。Cisco Systems Intelligent Gigabit Ethernet Switch Module for IBM **@server** BladeCenter (Cisco Systems IGESM) は、このアライアンスにおける重要な第一歩です。この BladeCenter スイッチ・モジュールにより、BladeCenter のお客様が、世界クラスである Cisco の銅・イーサネット・スイッチング・テクノロジーを BladeCenter シャーシに統合された形でご利用いただけます。さらに、業界に普及している CiscoWorks などの SNMP ベース管理ツールを使用すれば、お客様の既存データ・ネットワークへのシームレスなインターフェースが提供され、BladeCenter の提案する価値が一層高まります。

BladeCenter シャーシに取り付けられた Cisco Systems IGESM は、基本的な L2 スwitch 機能に加えて、一般的な商品のスイッチング・ソリューションにはない重要な付加価値を提供します。次のような付加価値があります。

<b>BackboneFast</b>	レイヤー 2 ネットワークの迅速なコンバージェンスの支援
<b>UplinkFast</b>	レイヤー 2 ネットワークの迅速なコンバージェンスの支援
<b>UDLD</b>	UniDirectional Link Detection、スパンニング・ツリー・プロトコル (STP) のループが生じる可能性を低減
<b>CDP</b>	Cisco Discovery Protocol (管理およびトラブルシューティングを支援)
<b>ISL</b>	VLAN トランッキング (Cisco プロプライエタリー)
<b>PAgP</b>	Port Aggregation Protocol (Cisco EtherChannel)
<b>VTP</b>	VLAN Trunking Protocol (GVRP に類似)
<b>DTP</b>	Dynamic Trunking Protocol (トランクのタイプおよび状態の自動ネゴシエーション)
<b>RADIUS</b>	スイッチへのアクセスの集中管理制御
<b>TACACS+</b>	スイッチへのアクセスの集中管理制御
<b>VMPS</b>	VLAN Management Policy Server (一部の Cisco スイッチの場合のみ)
<b>PVST+</b>	Per-VLAN Spanning Tree
<b>802.1w</b>	高速再構成スパンニング・ツリー (802.1D の拡張)



それぞれの Cisco Systems IGESM は、14 基のブレード・スロットそれぞれにギガビット/秒イーサネット (GbE) 接続を 1 つずつ提供し、さらに BladeCenter 外部への GbE アップリンク・インターフェースを 4 つ提供します。お客様は、1 つの BladeCenter に Cisco Systems IGESM を最小 1 つ、最大 4 つ取り付けることができます。4 つの Cisco Systems IGESM を取り付けると、お客様は 16 の GbE アップリンク・インターフェース、および 56 の GbE 内部スイッチング機能を使用できます。Cisco Systems IGESM の柔軟性により、お客様のパフォーマンスと冗長性に関するさまざまな要件に対応できます。

Cisco と IBM は、Cisco Data Center ネットワーク・アーキテクチャーと IBM のオンデマンド稼働環境の統合について、ベスト・プラクティスのテストと文書化を積極的に行っています。これにより、お客様の高可用性、スケーラビリティ、セキュリティ、および管理の容易性に関する要件が確実に満たされます。IBM Tivoli® および Cisco の管理製品の統合と、これらのアーキテクチャーの組み合わせによって、運用費用を削減しながら価値の高いソリューションが実現します。Cisco Systems IGESM は、これらのソリューションに不可欠な部分です。Cisco Systems IGESM を使用すれば、お客様は世界最大手のサーバーおよびネットワーク企業との支援のもとでソリューションの投資保護を実現できます。



## IBM eServer BladeCenter の概要

IBM *@server* BladeCenter の革新的なモジュラー・テクノロジー、先進的な高密度と高可用性は、現実には生じるさまざまな問題の解決を支援するための設計です。

サーバーの統合を目指す組織のために、BladeCenter はサーバーを集中化して柔軟性を高め、保守を容易にし、コストを削減して、人的資源の合理化を実現します。新しい e-commerce アプリケーションと e-business アプリケーションのデプロイを必要としている企業が、柔軟性、スケーラビリティ、および可用性を保ちながら、処理を高速化できます。ファイルおよび印刷のサービス提供、コラボレーションなどの企業要件を満たすために、BladeCenter は信頼性、柔軟な拡張性、およびコスト効率性を備えた設計になっています。さらに、高可用性クラスタリングを必要とする計算主体のアプリケーションを実行するお客様は、BladeCenter を使用すれば高度なスケーラビリティとパフォーマンスが得られます。

IBM eServer BladeCenter 製品ファミリーは、複数のコンピューティング・リソースをコスト効率の高い高密度格納装置に統合するモジュラー設計を採用して、次のようなプラットフォームを提供します。

- ▶ 取り付け、配置、および再配置に要する時間が短縮されます。
- ▶ 便利な管理ツールによって、管理コストが削減されます。
- ▶ 最高レベルの可用性と信頼性を発揮します。
- ▶ XpandonDemand スケールアウト機能を備えています。
- ▶ 1U ソリューションと比較して、スペース所要量と冷却要件が軽減されます。

Cisco Systems Intelligent Gigabit Ethernet Switch Module が BladeCenter 環境で動作するためにどのように設計されているか詳しく知るには、後続の節をお読みになり、BladeCenter のアーキテクチャーを理解してください。BladeCenter とそのコンポーネントについて詳しい情報が必要な場合は、IBM Redpaper 『The Cutting Edge: IBM *@server* BladeCenter』 (REDP-3581) をお読みになることをお勧めします。この Redpaper は、次の URL で入手できます。

<http://www.redbooks.ibm.com/redpapers/abstracts/redp3581.html>

図 2-1 に、BladeCenter シャーシ、HS40、HS20、および JS20 を示します。

▶ IBM eServer BladeCenter シャーシ

BladeCenter は、アプリケーション・サービス提供、ストレージの柔軟性、および長期にわたる投資保護を実現するために最大限のパフォーマンス、可用性、および管理の容易性を備えた高密度ブレード・ソリューションです。

▶ HS40

HS40 は、4 プロセッサの SMP 機能を必要とする高性能エンタープライズ・アプリケーション向けの 4-way ブレード・サーバーです。BladeCenter シャーシは、7 台までの 4-way サーバーをサポートし、ERP およびデータベース・アプリケーションに最適です。

▶ HS20

IBM の効率的な 2-way ブレード・サーバー設計により、サーバーのパフォーマンスを犠牲にせずに高密度を実現しています。Domino®、Web サーバー、Microsoft® Exchange、ファイルおよび印刷、アプリケーション・サーバーなどに最適です。

▶ JS20

JS20 は、64 ビット・コンピューティングを必要とするアプリケーション向けの 2-way ブレード・サーバーです。計算主体のアプリケーションとトランザクションの Web サービス提供に最適です。

BladeCenter プラットフォーム用のブレードの開発が進行中です。

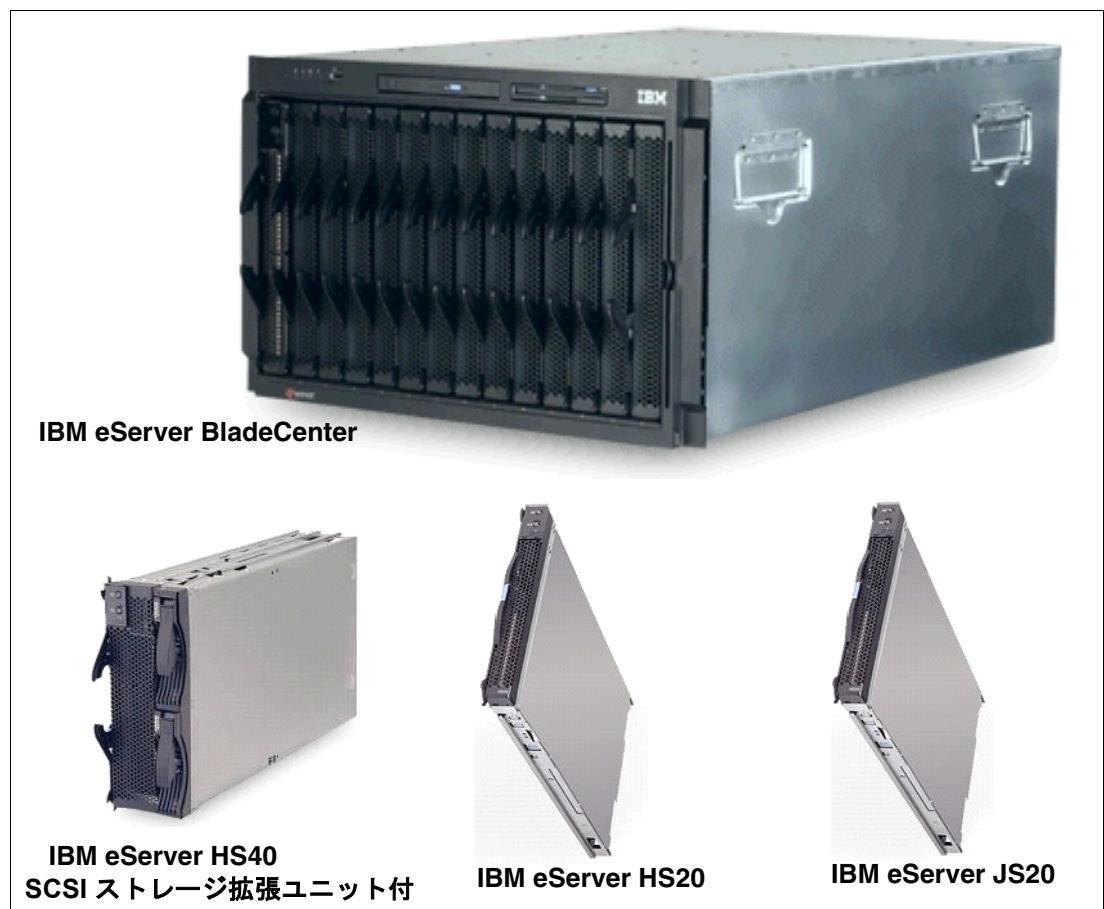


図 2-1 IBM eServer BladeCenter およびブレード

BladeCenter テクノロジーについて詳しくは、次の Web サイトをご覧ください。

<http://www.ibm.com/servers/eserver/bladecenter/index.html>

## IBM eServer BladeCenter のストレージ・ソリューション

IBM は、厳しいビジネス要件に対応する、インストールの容易な大容量のテスト済みストレージ製品を BladeCenter 向けに幅広く提供しています。これにより、次のものを含む広範囲の IBM TotalStorage® ストレージ・ソリューション製品からお客様に合ったものを選択できます。

- ▶ ファイバー・チャネル製品および Storage Area Network
- ▶ Network Attached Storage
- ▶ Enterprise Storage Server®

IBM TotalStorage が提供する、お客様固有の要件に合わせて設計された接続性のある保護された完全なストレージ・ソリューションによって、ストレージ環境の管理が容易になり、コストを削減でき、ビジネス効率とビジネスの継続性を高めることができます。

BladeCenter ストレージ・ソリューションについて詳しくは、次の Web サイトをご覧ください。

<http://www.pc.ibm.com/us/eserver/xseries/storage.html>

## IBM eServer BladeCenter のシステム管理

BladeCenter への投資からライフ・サイクルを通じて最大限の価値を得るためには、高可用性と低コストを維持する、合理的で効率的なシステム管理が必要です。

### 管理の基礎

高い評価を得ている業界標準ベースのワークグループ・ソフトウェアである IBM Director は、xSeries、IntelliStation®、NetVista™、および ThinkPad® の各ハードウェアを対象に広範囲の管理機能を提供し、コストの削減と生産性の向上に役立ちます。

### IBM Director

IBM Director は、インテリジェント・システム管理のために設計されたハードウェアです。この製品は業界で最も優れたツールを備えており、可用性の向上、資産のトラッキング、パフォーマンスの最適化、およびリモート保守機能によって、ユーザーの時間と費用を節約できます。

### 高度なサーバー管理

次に示す、他にはないソフトウェア・ユーティリティのコレクションを使用して、高度なサーバー管理を実行し、可用性を最大限に高めることができます。

- ▶ Server Plus Pack
- ▶ Application Workload Manager
- ▶ Scalable Systems Manager
- ▶ Real-Time Diagnostics
- ▶ Electronic Service Agent™
- ▶ Tape Drive Management Assistant

### デプロイメント管理および更新管理

IBM デプロイメント・ツールを使用すれば、サーバーとクライアントの実行準備に伴う面倒な作業を最小限に減らすことができます。次のようなツールがあります。

- ▶ Remote Deployment Manager
- ▶ Software Distribution Premium Edition
- ▶ ServerGuide™
- ▶ UpdateXpress

BladeCenter のシステム管理について詳しくは、次の Web サイトをご覧ください。

[http://www.ibm.com/servers/eserver/xseries/systems\\_management/xseries\\_sm.html](http://www.ibm.com/servers/eserver/xseries/systems_management/xseries_sm.html)

## 2.1 IBM eServer BladeCenter のアーキテクチャー

ここでは、BladeCenter のシャーシとコンポーネントのアーキテクチャー設計について解説します。

### 2.1.1 ミッドプレーン

図 2-2 では、BladeCenter のミッドプレーンについて説明します。ミッドプレーンには、冗長機能を提供する 2 つの類似したセクション（上部および下部）があります。プロセッサ・ブレード（ブレード・サーバー）は、ミッドプレーンの前部に接続されます。その他の主要コンポーネントはすべて、ミッドプレーンの後部に接続されます。

プロセッサ・ブレードには 2 つのコネクターがあり、1 つはミッドプレーンの上部セクション、もう 1 つは下部セクションに接続されます。その他のコンポーネントはすべて、1 つのセクションのみ（上部または下部）に接続されます。ただし、冗長性のために他方のミッドプレーン・セクションに接続できる、別の対応するコンポーネントが存在します。

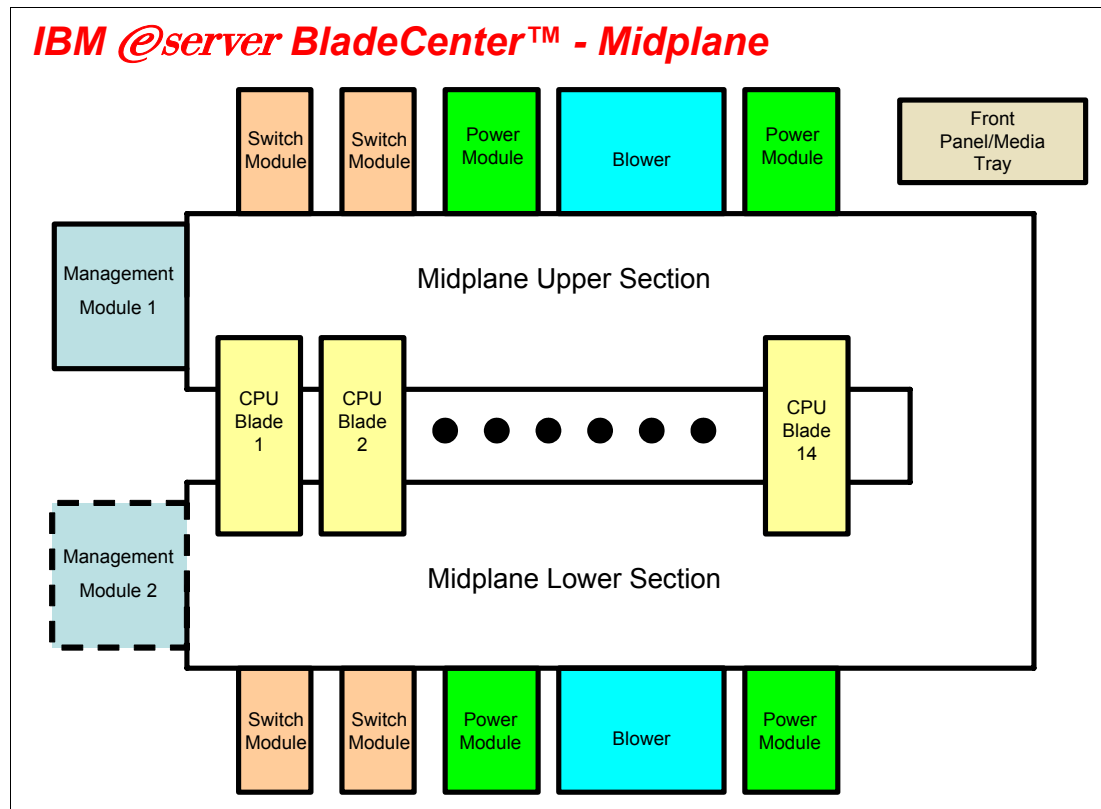


図 2-2 ミッドプレーンの図

### 2.1.2 管理モジュールのイーサネット

7 ページの図 2-3 では、管理モジュール・インターフェースについて説明します。スイッチ・モジュールは、100 Mb イーサネット・インターフェースを使用するアクティブ管理モジュールによって構成されます。それぞれの管理モジュールには、100 Mb イーサネット・

インターフェースが4つ（それぞれのスイッチ・モジュールごとに1つ）あります。それぞれのスイッチ・モジュールには、100 Mb イーサネット・インターフェースが2つ（それぞれの管理モジュールごとに1つ）あります。次のリストに、具体的なルーティングを示します。

- ▶ 管理モジュール1 イーサネット 1 → スイッチ・モジュール1 イーサネット 15
- ▶ 管理モジュール1 イーサネット 2 → スイッチ・モジュール2 イーサネット 15
- ▶ 管理モジュール1 イーサネット 3 → 拡張スイッチ・モジュール3 イーサネット 15
- ▶ 管理モジュール1 イーサネット 4 → 拡張スイッチ・モジュール4 イーサネット 15
- ▶ 管理モジュール2 イーサネット 1 → スイッチ・モジュール1 イーサネット 16
- ▶ 管理モジュール2 イーサネット 2 → スイッチ・モジュール2 イーサネット 16
- ▶ 管理モジュール2 イーサネット 3 → 拡張スイッチ・モジュール3 イーサネット 16
- ▶ 管理モジュール2 イーサネット 4 → 拡張スイッチ・モジュール4 イーサネット 16

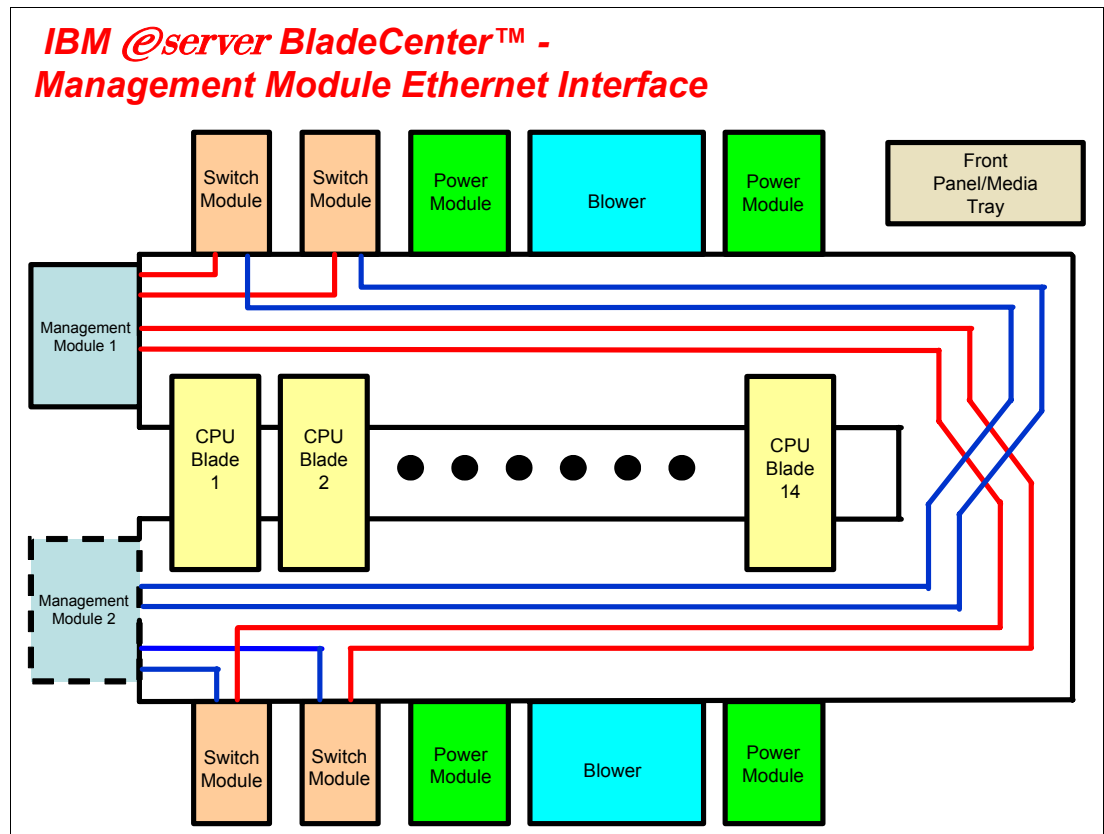


図2-3 管理モジュールのイーサネット・インターフェース

### 2.1.3 Gigabit Ethernet パス

8 ページの図 2-4 では、Gigabit Ethernet パスについて説明します。それぞれのプロセッサ・ブレードに、最小2つ、最大4つの EtherLAN インターフェースがあります。特に、BladeCenter HS20 プロセッサ・ブレードには、SERDES ベースの Gb イーサネット・インターフェースが2つ（それぞれのミッドプレーン・コネクタごとに1つ）あります。ドーターカードを取り付けた場合は、さらに2つのネットワーク・インターフェースを追加できます。それぞれのスイッチ・モジュール（SW モジュール）が、それぞれのプロセッサ・ブレードから LAN 入力を1つ受信し、入力の合計数は14です。次に、このルーティングの部分リストを示します。

- ▶ プロセッサ・ブレード1 LAN 1 → スイッチ・モジュール1 入力1
- ▶ プロセッサ・ブレード1 LAN 2 → スイッチ・モジュール2 入力1
- ▶ プロセッサ・ブレード1 LAN 3 → 拡張スイッチ・モジュール3 入力1

- ▶ プロセッサ・ブレード 1 LAN 4 → 拡張スイッチ・モジュール 4 入力 1
- ▶ プロセッサ・ブレード 2 LAN 1 → スイッチ・モジュール 1 入力 2
- ▶ プロセッサ・ブレード 2 LAN 2 → スイッチ・モジュール 2 入力 2
- ▶ プロセッサ・ブレード 2 LAN 3 → 拡張スイッチ・モジュール 3 入力 2
- ▶ プロセッサ・ブレード 2 LAN 4 → 拡張スイッチ・モジュール 4 入力 2

プロセッサ・ブレード上では、LAN 1 と LAN 2 がオンボード SERDES G ビット・イーサネット・インターフェースであり、すべてのプロセッサ・ブレードに対してスイッチ・モジュール 1 とスイッチ・モジュール 2 にそれぞれ配線されます。LAN 3 と LAN 4 はそれぞれ、拡張スイッチ・モジュール 3 と 4 に接続し、これはドーターカードが取り付けられている場合のみ使用されます。1 つ以上のプロセッサ・ブレードにドーターカードを取り付けない限り、スイッチ・モジュール 3 と 4 は必要ありません。さらに、これらのスイッチ・モジュールは、プロセッサ・ブレードによって生成される LAN インターフェースと互換であることが必要です。ファイバー・チャネル・ドーターカードを BladeCenter HS20 プロセッサ・ブレードに取り付ける場合は、スイッチ・モジュール 3 と 4 もファイバー・チャネル・ベースであることが必要で、残りの BladeCenter HS20 プロセッサ・ブレードに取り付けるドーターカードは、すべてファイバー・チャネルであることが必要です。

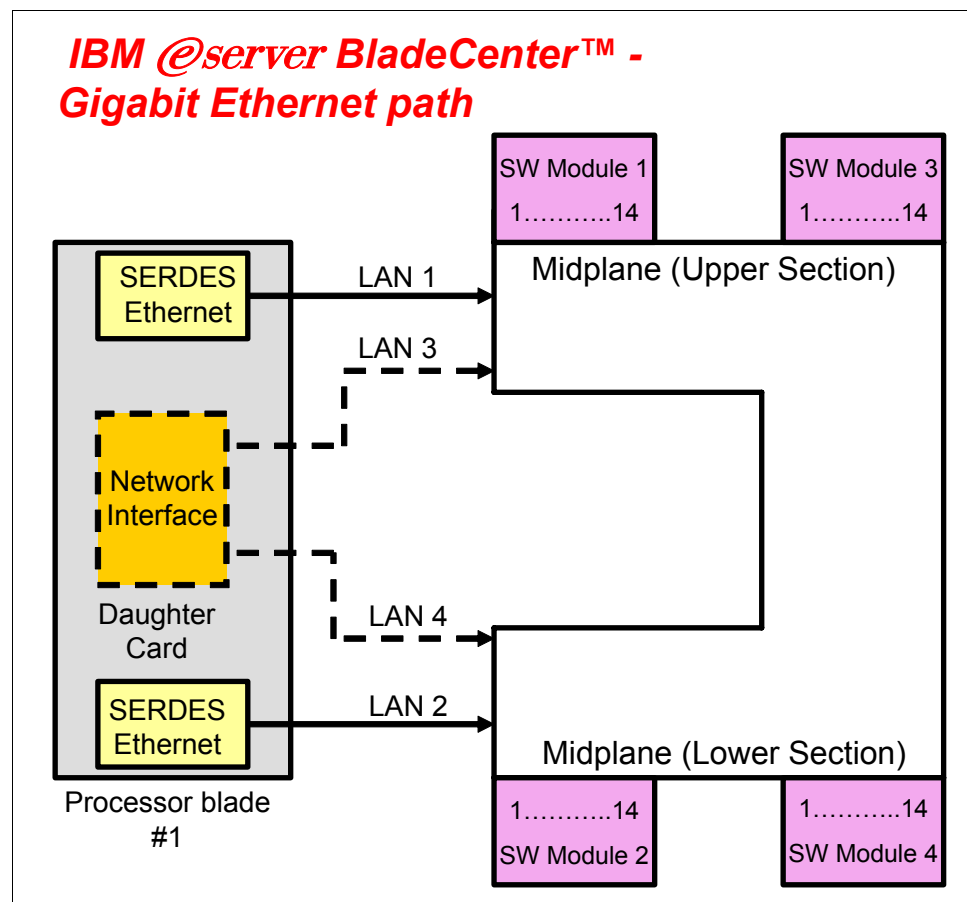


図 2-4 Gigabit Ethernet パス

## 2.2 IBM eServer HS20 のアーキテクチャー

ここでは、IBM @server BladeCenter HS20 のアーキテクチャー設計について説明します。この説明では、標準的なデュアル・プロセッサ・サーバーのブレード設計を単に一例として示します。







## 2.3 スタンドアロン構成ツール

BladeCenter ハードウェアは、Web ブラウザーや Telnet クライアントなどの標準ソフトウェアを使用して構成できます。これらのソフトウェアは、主流となっているすべての OS プラットフォーム上で使用できます。この構成を可能にするために、管理モジュールと Ethernet Switch Module の両方に組み込まれた Web と ANSI の両インターフェースが活用されます。Web インターフェースからは、非常に広範囲の機能を備えたツールにアクセスできます。このツールにはさまざまな構成サブメニューがあり、お客様はその 1 つ (Switch Tasks) を使用して Ethernet Switch Module をセットアップできます。基本設定 (Ethernet Switch Module の IP アドレス、外部ポートの使用可能化など) の構成は、I2C バスを活用して行われます。拡張メニューを使用して、モジュールを微調整できます。このためには、Web ブラウザーの別のウィンドウを開くか、ANSI インターフェースへの接続を可能にする Java™ アプレットを実行します (管理システムに Java 2 V1.4 がインストールされている必要があります)。この機能を実現するために、BladeCenter バックプレーンを経由して管理モジュールと Ethernet Switch Module を接続する 10/100 Mb 内部リンクが活用されます (管理モジュールの内部ネットワーク・インターフェースのデフォルト静的 IP アドレスは、192.168.70.126 であることに注意してください)。これらの機能を完備したツールにアクセスするには、Web ブラウザーまたは Telnet クライアントに Ethernet Switch Module 自体の IP を指定します (後部ベイ 1 に接続したモジュールのデフォルトは 192.168.70.127 ですが、DHCP ベースのアドレッシングを構成できます)。この拡張機能を使用するには、Ethernet Switch Module の外部ポート (実動 LAN 上にある) を経由して管理システムを接続する必要があるため、セキュリティに不安が生じる可能性があります。この理由から、お客様は管理モジュール・インターフェースの「Switch Tasks」で外部ポート経由の構成制御を使用不可に設定できます。図 2-6 を参照してください。

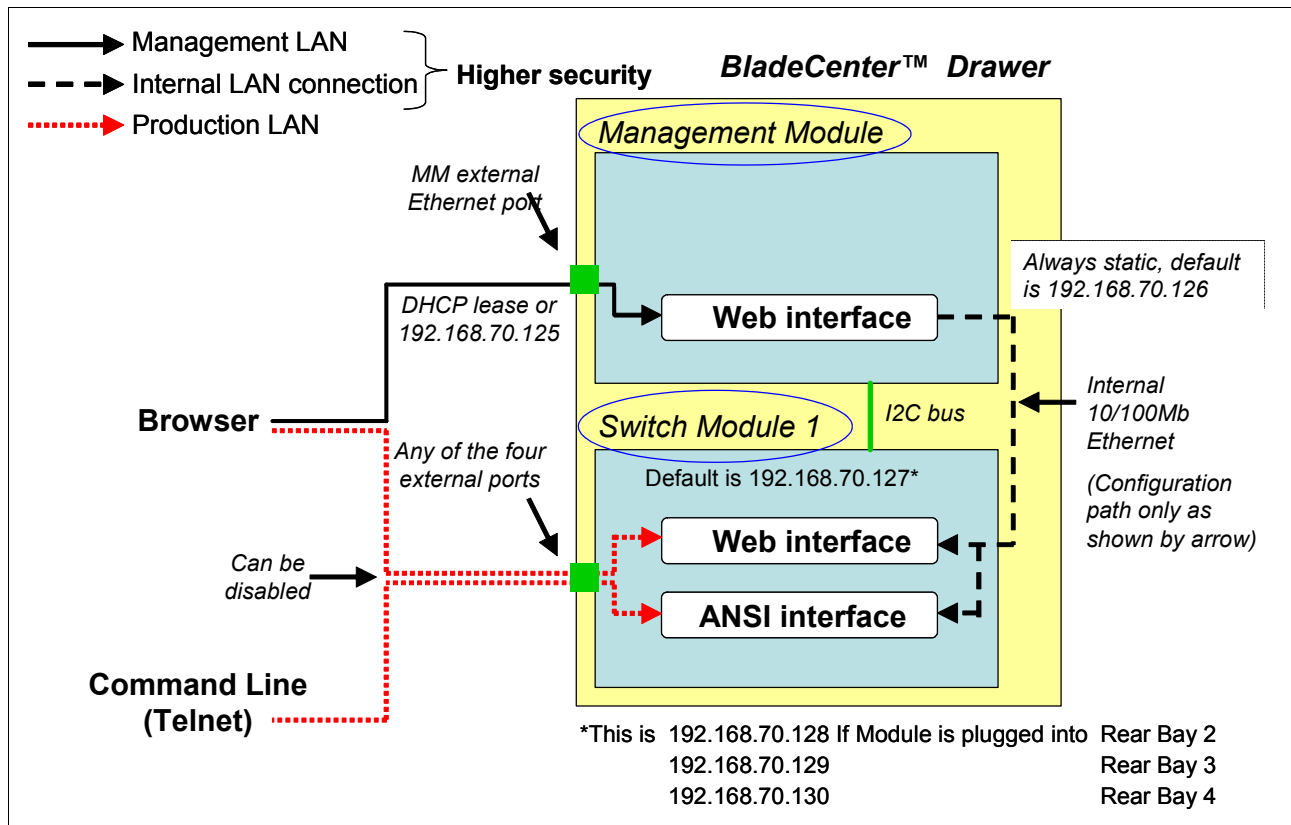


図 2-6 スタンドアロン構成ツール



## Cisco Systems Intelligent Gigabit Ethernet Switch Module

この章では、Cisco Systems Intelligent Gigabit Ethernet Switch Module に組み込まれている機能について説明します。これらの機能により、BladeCenter のお客様は、IBM @server BladeCenter に統合された Cisco の世界最高クラスのイーサネット・スイッチング・テクノロジーを利用できます。

## 3.1 製品説明

Cisco Systems Intelligent Gigabit Ethernet Switch Module (図 3-1) は、BladeCenter サーバー・シャーシにレイヤー 2 スイッチング機能を提供します。この製品は最大 250 の仮想 LAN を提供するので、ネットワーク・リソース、トラフィック・パターン、および帯域幅に関連して、さまざまなユーザーを VLAN に割り当てることができます。また、EtherChannel リンクを自動的に作成するためのトランッキング・プロトコル (IEEE 802.1Q) とリンク・アグリゲーションもサポートします。ポートのセキュリティにより、特定のポートのみへのアクセス許可を受けたメディア・アクセス制御 (MAC) アドレスのみにトラフィックを制限できます (Internet Group Management Protocol (IGMP) スヌープ)。BladeCenter シャーシのスイッチ・モジュール・ベイに、4 つまでの Cisco Systems Intelligent Gigabit Ethernet Switch Module を取り付けることができます。これらのモジュールは、通常操作を中断せずにホット・プラグによって BladeCenter に接続できます。スイッチは、BladeCenter ミッドプレーン上にある 14 の内部 GbE (ギガビット) インターフェース (サーバー・ポート) を経由してサーバー・ブレードに接続します。外部通信用に 4 つの外部銅 GbE インターフェースが備わっており、これらのインターフェースは他の Cisco 装置と完全に互換性があります。GbE スwitch の管理は、BladeCenter 管理モジュールとの通信用の内部 100 Mbps ポート 2 つを経由して行われます。Web ベースまたは Telnet ベースのインターフェースを使用して、診断および Cisco Systems Intelligent Gigabit Ethernet Switch Module と BladeCenter 管理モジュール間の直接接続が可能です。また、標準の Cisco 管理アプリケーションをすべてサポートします。

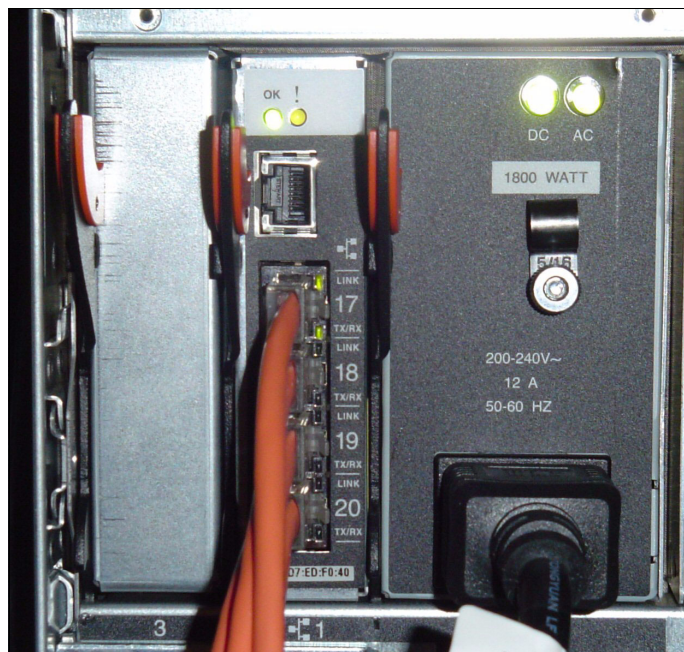


図3-1 Cisco Systems Intelligent Gigabit Ethernet Switch Module (製品番号13N2281)

## 3.2 提案の価値

Cisco Systems Intelligent Gigabit Ethernet Switch Module が IBM eServer BladeCenter に向いている理由は？ 次のポイントからその答えは明らかです。

### 製品の長所

この製品には次のような長所があります。

- ▶ BladeCenter 統合インテリジェント・スイッチ・モジュールは、既存の Cisco Data Center に対して完全な相互運用性を備えています。

- ▶ 業界最先端の Cisco ネットワーキング機能を統合して、データ・センターの複雑さを軽減し、ネットワーキングの管理の容易性を高めます。
- ▶ BladeCenter アライアンス・パートナーのリーダーシップ力を利用して、お客様は最高の技術を使用した製品を選択できます。

### 先進的な機構および機能

次に示す先進的な機構および機能を備えています。

- ▶ BladeCenter は Cisco Systems Intelligent Gigabit Ethernet Switch Module とともに提供されます。この製品は、Cisco Catalyst 製品ファミリー全体にわたるレイヤー 2+ 機能を完備したスイートです。
- ▶ スイッチ・モジュールは Cisco Internetworking Operating System (IOS) を実行するので、このスイッチ・モジュールはデータ・センターのネットワーク管理ツールに他の Cisco ネットワーキング・エレメントと同様に表示されます。

### 競争上の利点

次のような競争上の利点があります。

- ▶ BladeCenter は、イーサネット・スイッチングの完全な統合を実現し、インフラストラクチャの複雑さを軽減します。
- ▶ インテリジェントな Gigabit Ethernet スイッチングをシャーシに組み込んで提供しているブレード・ベンダーは、他にはありません。

## 3.3 製品の機能

ここでは、Cisco Systems Intelligent Gigabit Ethernet Switch Module の各機能の具体的な役割と、サポートされるネットワーク・プロトコルについて説明します。

### 3.3.1 スイッチ管理

Cisco Systems Intelligent Gigabit Ethernet Switch Module には次のようなスイッチ管理機能があります。

- ▶ Cisco Discovery Protocol (CDP) バージョン 1 および 2 によって、スイッチと他の Cisco ネットワーク・デバイスとの間でネットワーク・トポロジーのディスカバリーとマッピングを行います。
- ▶ Network Time Protocol (NTP) によって、外部ソースからの整合したタイム・スタンプをすべてのスイッチに提供します。
- ▶ Trivial File Transfer Protocol (TFTP) サーバーへ指定されたユニキャスト要求によって、TFTP サーバーからソフトウェア・アップグレードを取得します。
- ▶ デフォルト構成がフラッシュ・メモリーに格納されているので、最小限のユーザー介入によってスイッチをネットワークに接続し、トラフィックを転送できます。
- ▶ Cluster Management Suite (CMS) Web インターフェース・セッションによるインバンド管理アクセス。
- ▶ 最大 16 の同時 Telnet 接続を経由したインバンド管理アクセスによって、複数のコマンド行インターフェース (CLI) ベースのセッションをネットワーク上で確立できます。
- ▶ 最大 5 つの同時暗号化セキュア・シェル (SSH) 接続を経由したインバンド管理アクセスによって、複数の CLI ベースのセッションをネットワーク上で確立できます。このオプションは、暗号ソフトウェア・イメージにのみ含まれており、次の Web サイトから入手できます。

<http://www.ibm.com/support/us/>

- ▶ SNMP バージョン 1、2c、および 3 の get 要求と set 要求によるインバンド管理アクセス。

### 3.3.2 ポート機構

次に示す機構は、Cisco Systems Intelligent Gigabit Ethernet Switch Module のポートです。

- ▶ バックボーン、エンド・ステーション、およびサーバーへの 10/100/1000 Mbps 接続用の外部 1000BASE-T コネクタ 4 つ
- ▶ 内部全二重ギガビット・ポート 14 個 (BladeCenter 装置内のブレード・サーバーそれぞれに 1 つずつ接続)
- ▶ 管理モジュールに接続する内部全二重 100 Mbps ポート 2 つ

### 3.3.3 パフォーマンス機能

Cisco Systems Intelligent Gigabit Ethernet Switch Module には次のようなパフォーマンス機能があります。

- ▶ 10/100/1000 ポートの速度の自動検知、およびポートの二重モードの自動ネゴシエーションにより、帯域幅を最適化します。
- ▶ 全二重モードで動作する Gigabit Ethernet ポート上での IEEE 802.3x フロー制御。
- ▶ Fast EtherChannel および Gigabit EtherChannel により、フォールト・トレランスが強化され、スイッチ、ルーター、およびサーバー間で最大 4 Gbps の帯域幅が得られます。
- ▶ 1530 バイトまでのフレーム・サイズのサポート。
- ▶ ポートごとのブロードキャスト・ストーム制御により、障害のあるエンド・ステーションが、ブロードキャスト・ストームによって全体のシステム・パフォーマンスを低下させることを防ぎます。
- ▶ Port Aggregation Protocol (PAgP) および Link Aggregation Control Protocol (LACP) による、EtherChannel リンクの自動作成。
- ▶ Internet Group Management Protocol (IGMP) スヌープのサポートにより、IP マルチキャスト・トラフィックのフラグディングを制限します。
- ▶ Multicast VLAN registration (MVR) は、マルチキャスト VLAN にマルチキャスト・ストリームを継続的に送信する一方で、帯域幅とセキュリティ確保のために加入者 VLAN からストリームを分離します。
- ▶ IGMP フィルタリングにより、スイッチ・ポート上のホストが所属できるマルチキャスト・グループのセットを制御します。
- ▶ 保護ポート (専用 VLAN エッジ・ポート) オプションにより、トラフィックの転送を同じスイッチ上の指定されたポートに限定します。
- ▶ 動的アドレス学習により、セキュリティが強化されます。

### 3.3.4 冗長性

次に、Cisco Systems Intelligent Gigabit Ethernet Switch Module に組み込まれた冗長性機能について説明します。

- ▶ UniDirectional link detection (UDLD) は、すべてのイーサネット・ポート上で、ポートの障害によって生じる単一方向リンクを検出して使用不可にします。
- ▶ IEEE 802.1D スパニング・ツリー・プロトコル (STP) により、冗長バックボーン接続が提供され、ループのないネットワークが実現します。

- ▶ IEEE 802.1s 多重 STP (MSTP) により、複数の VLAN をスパンニング・ツリー・インスタンスにグループ化し、データ・トラフィックとロード・バランシングのために複数の転送パスを使用できます。
- ▶ IEEE 802.1w 高速 STP (RSTP) は、ルートおよび指定されたポートを即時に転送状態に遷移させて、スパンニング・ツリーの迅速なコンバージェンスを実現します。
- ▶ Per-VLAN Spanning Tree (PVST)+、Rapid PVST+、および MSTP の各モードで、オプションのスパンニング・ツリー機能が利用できます。

### 3.3.5 VLAN サポート

このスイッチは、250 ポート・ベースの VLAN をサポートし、該当するネットワーク・リソース、トラフィック・パターン、および帯域幅に関連した VLAN にユーザーを割り当てることができます。VLAN サポートの特長は次のとおりです。

- ▶ スイッチは最大 4094 の VLAN ID をサポートするので、サービス・プロバイダーのネットワークは IEEE 802.1Q 規格によって許される数の VLAN をサポートできます。
- ▶ すべてのポート上で IEEE 802.1Q トランッキング・プロトコルを使用して、ネットワークの移動、追加、および変更に対応し、ブロードキャストおよびマルチキャストのトラフィックの管理と制御を行い、ユーザーとネットワーク・リソースのセキュリティを高めるための VLAN グループを設定してネットワーク・セキュリティを確保します。
- ▶ VLAN Management Policy Server (VMPS) による動的 VLAN メンバーシップ。
- ▶ VLAN Trunking Protocol (VTP) プルーニングにより、トラフィックを受信するステーションに向かうリンクのみにフラッドイングされるトラフィックを制限して、ネットワーク・トラフィックを削減します。
- ▶ Dynamic Trunking Protocol (DTP) により、2 つのデバイス間のリンク上でトランッキングをネゴシエーションし、使用するトランッキング・カプセル化 (802.1Q) のタイプをネゴシエーションします。
- ▶ 音声 VLAN により、Cisco IP 電話からの音声トラフィック用のサブネットを作成します。
- ▶ VLAN 1 の最小化により、個々の VLAN トランク・リンク上で VLAN 1 を使用不可に設定でき、スパンニング・ツリーのループやストームのリスクが減ります。

### 3.3.6 セキュリティ

Cisco Systems Intelligent Gigabit Ethernet Switch Module には、次のようなセキュリティ機能が組み込まれています。

- ▶ ブリッジ・プロトコル・データ単位 (BPDU) ガードにより、無効な構成が行われた場合に Port Fast 構成のポートをシャットダウンします。
- ▶ 保護ポート・オプションにより、トラフィックの転送を同じスイッチ上の指定されたポートに限定します。
- ▶ 管理インターフェース、Cluster Management Suite、およびコマンド行インターフェースへのパスワード保護アクセス（読み取り専用および書き込み専用のアクセス）により、無許可の構成変更を防止します。
- ▶ ポート・セキュリティ・オプションにより、ポートにアクセスできるステーションの MAC アドレスを制限および識別します。
- ▶ ポート・セキュリティ・エージングにより、ポート上のセキュア・アドレスのエージング時間を設定できます。
- ▶ マルチレベル・セキュリティにより、セキュリティ・レベル、通知、および結果のアクションを選択できます。

- ▶ MAC ベースのポート・レベル・セキュリティにより、スイッチ・ポートの使用を特定のソース・アドレスのグループに制限し、無許可のステーションからスイッチへのアクセスを防止します。
- ▶ Terminal Access Controller Access Control System Plus (TACACS+)。これは、TACACS サーバーによってネットワーク・セキュリティを管理するためのプロプライエタリー機能です。
- ▶ IEEE 802.1X ポート・ベース認証により、無許可のデバイスがネットワークにアクセスできないようにします。
- ▶ VLAN の割り当てを指定した IEEE 802.1X ポート・ベース認証により、802.1X の認証を受けるユーザーを指定の VLAN に制限できます。
- ▶ ポート・セキュリティを指定した IEEE 802.1X ポート・ベース認証により、ポートを認証し、すべての MAC アドレス（クライアントのものを含む）を対象にネットワーク・アクセスを管理できます。
- ▶ 音声 VLAN を指定した IEEE 802.1X ポート・ベース認証により、ポートの許可または無許可の状態に関係なく、音声 VLAN への IP 電話のアクセスを許可できます。
- ▶ ゲスト VLAN を指定した IEEE 802.1X ポート・ベース認証により、802.1X に準拠しないユーザーに制限付きのサービスを提供できます。
- ▶ 標準および拡張の IP アクセス制御リスト (ACL) による、セキュリティ・ポリシーの定義。

### 3.3.7 サービス品質 (QoS) およびサービス・クラス (CoS)

次に、Cisco Systems Intelligent Gigabit Ethernet Switch Module のサービス品質 (QoS) とサービス・クラス (CoS) を示します。

- ▶ 分類
  - IEEE 802.1p サービス・クラス (CoS) は、ギガビット・ポート上で 8 つの優先キューを使用し、データ・アプリケーション、音声アプリケーション、およびテレフォニー・アプリケーションからのミッション・クリティカルなトラフィックや時間依存トラフィックに優先順位を付けます。
  - IP Differentiated Services Code Point (IP DSCP) と CoS は、ポートごとに優先順位付けを行って、ミッション・クリティカルなアプリケーションのパフォーマンスを保護します。
  - ネットワーク・エッジでハイパフォーマンス QoS を実現するためのフロー・ベースの packets 分類 (MAC、IP、および TCP/UDP の各ヘッダーの情報に基づく分類) により、ネットワーク・トラフィックのさまざまなタイプに応じてサービス・レベルを差別化でき、ネットワーク内のミッション・クリティカルなトラフィックに優先順位を付けることができます。
  - IEEE 802.1p CoS スケジューリングのサポートにより、優先順位の高い音声トラフィックを分類し、優先して処理できます。
- ▶ 発信キューの発信ポリシングおよびスケジューリング
  - すべてのスイッチ・ポート上に 4 つの発信キューがあります。厳密な優先順位と、加重ラウンドロビン (WRR) の CoS ポリシーをサポートします。

### 3.3.8 モニター

次に、Cisco Systems Intelligent Gigabit Ethernet Switch Module のモニター機能について説明します。

- ▶ ポートとスイッチの状況を視覚的に表現するスイッチ LED。

- ▶ Switch Port Analyzer (SPAN) および Remote Switch Port Analyzer (RSPAN) のサポートによる、ネットワークのローカル・モニターとリモート・モニター。
- ▶ 組み込みリモート・モニター (RMON) エージェントの 4 つのグループ (ヒストリー、統計、アラーム、およびイベント) による、ネットワーク・モニターおよびトラフィック分析。
- ▶ MAC アドレス通知による、スイッチが学習または除去した MAC アドレスのトラッキング。
- ▶ 認証または許可エラー、リソースの問題、およびタイムアウト・イベントに関するシステム・メッセージをログに記録する SYSLOG 機能。
- ▶ レイヤー 2 traceroute による、ソース・デバイスから宛先デバイスまでにパケットがたどった物理パスの識別。

### 3.3.9 ネットワーク・ケーブル

次に、Cisco Systems Intelligent Gigabit Ethernet Switch Module のサポートされるネットワーク・ケーブルのリストを示します。

- ▶ 10BASE-T:
  - UTP カテゴリー 3、4、5 (最長 100 メートル)
  - 100 オーム STP (最長 100 メートル)
- ▶ 100BASE-TX:
  - UTP カテゴリー 5 (最長 100 メートル)
  - EIA/TIA-568 100 オーム STP (最長 100 メートル)
- ▶ 1000BASE-T:
  - UTP カテゴリー 6 (最長 100 メートル) 1 GB デバイスの標準
  - UTP カテゴリー 5e (最長 100 メートル)
  - UTP カテゴリー 5 (最長 100 メートル)
  - EIA/TIA-568B 100 オーム STP (最長 100 メートル)

### 3.3.10 サポートされる IEEE ネットワーク標準

Cisco Systems Intelligent Gigabit Ethernet Switch Module は、次の IEEE 標準をサポートします。

- ▶ IEEE 802.1D スパンニング・ツリー・プロトコル
- ▶ IEEE 802.1p タグ付きパケット
- ▶ IEEE 802.1Q タグ付き VLAN (VLAN が使用可能になっているときにすべてのポート上でフレームのタグ付けを行う)
- ▶ IEEE 802.2 論理リンク制御
- ▶ IEEE 802.3 10BASE-T イーサネット
- ▶ IEEE 802.3u 100BASE-TX ファースト・イーサネット
- ▶ IEEE 802.3x 全二重フロー制御







# Cisco Systems Intelligent Gigabit Ethernet Switch Module のアーキテクチャー

ここでは、Cisco Systems Intelligent Gigabit Ethernet Switch Module (Cisco Systems IGESM) for the IBM **@server** BladeCenter のシステム概要について説明します。

まず、Cisco Systems IGESM 自体を中心に説明します。このスイッチはレイヤー 2 スイッチで、レイヤー 2 から 4 ままでが可視です。20 ページの図 4-1 に、Cisco Systems Intelligent Gigabit Ethernet Switch Module のアーキテクチャー概要を示します。Cisco Systems IGESM には、ブレード・サーバーに接続する 14 の内部 1 Gbps リンク、およびアップストリーム・スイッチに接続する 4 つの外部ギガビット・ポートがあります。スイッチ・モジュールには、管理モジュールへの 100 Mbps 接続が 2 つ備わっています。Cisco Systems IGESM と管理モジュールの間の接続を経由して、Cisco Systems IGESM を管理できます。また、出荷時にはキャップでふさがれているコンソール・ポートを使用して、Cisco Systems IGESM を他の Catalyst スイッチと同様に管理することもできます。コンソール・ポートは、コマンド行インターフェース (CLI) を使用してソフトウェアを構成したり、スイッチに関する問題のトラブルシューティングを行ったりするために、端末または PC を接続できるサービス・ポートです。

**注：**この Redpaper の制作時点では、コンソール・ポートは IBM によって公式にはサポートされていません。ただし、IBM はテストの完了後にこの機能をサポートする予定です。

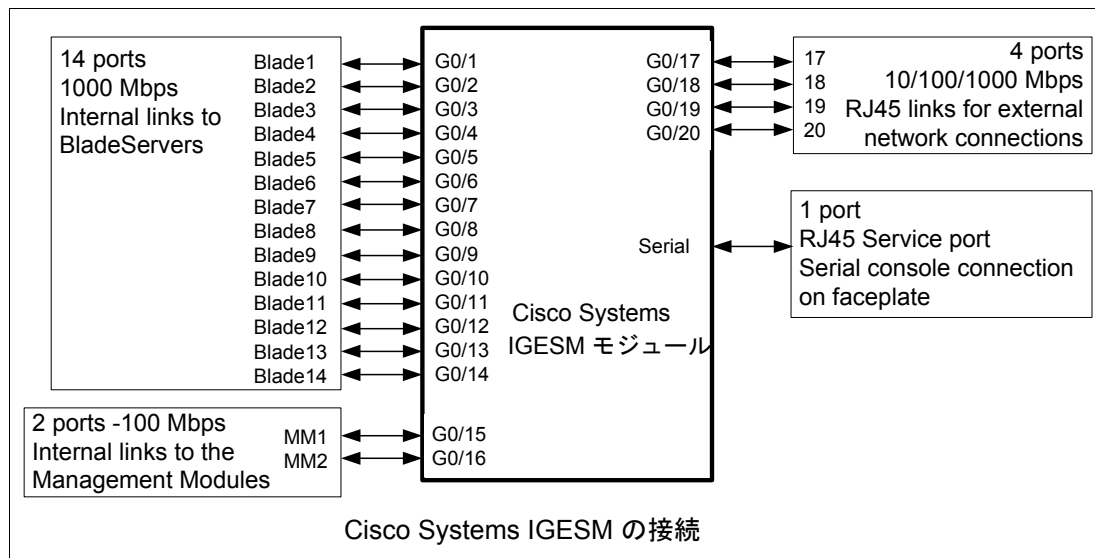


図 4-1 Cisco Systems IGESM のアーキテクチャー概要

次に、BladeCenter シャーシ内で Cisco Systems IGESM をブレード・サーバーに接続する方法を解説します。図 4-2 は、イーサネット接続のアーキテクチャーを示しています。2つの Cisco Systems IGESM を BladeCenter シャーシ内に格納できます。それぞれの Cisco Systems IGESM は 4 つのアップリンク・ポートを備え、これらをグループ化して 802.3ad リンク・アグリゲーションをサポートできます。ブレード・サーバーには 2 つの NIC があり、NIC 1 は Cisco Systems IGESM 1 に接続し、NIC 2 は Cisco Systems IGESM 2 に接続します。ブレード・サーバーを Cisco Systems IGESM に接続するリンクは、BladeCenter シャーシのバックプレーン上にあります。Cisco Systems IGESM には、管理モジュールへのリンクが 2 つあります。それぞれのリンクは、別々の管理モジュールに接続します。

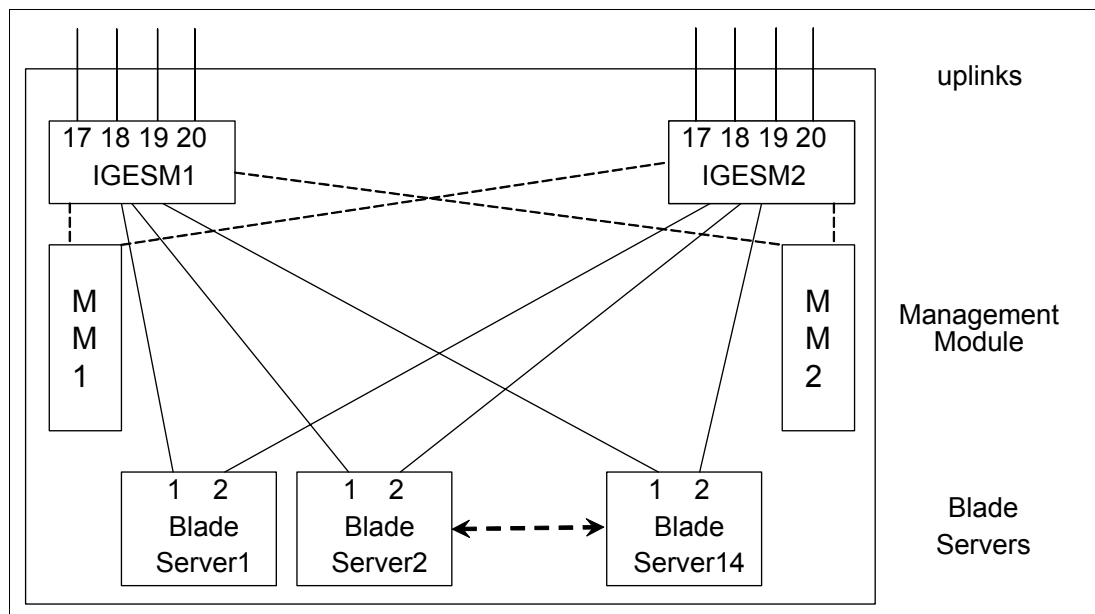


図 4-2 イーサネット接続

## Cisco Systems IGESM 内部のレイヤー 2 トラフィック・フロー

図 4-3 は、Cisco Systems IGESM 内部のレイヤー 2 トラフィック・フローを示しています。Cisco Systems IGESM 内にハードコーディングされたフィルターが、外部ポートと管理モジュール・ポート間のトラフィックすべてをブロックします。同じ BladeCenter シャーシ内にある 2 つの Cisco Systems IGESM が、管理モジュール間でレイヤー 2 フレームを交換します。ただし、Cisco Systems IGESM は管理モジュールによって交換される BPDU をブロックします。

この図は、次のことも示しています。

- ▶ CDP が使用可能になると、同じ BladeCenter シャーシ内にある 2 つの Cisco Systems IGESM は、外部ポートに接続せずに相互のディスカバリーを行うことができます。CLI から **show cdp neighbors** コマンドを実行すれば、相互間の接続を検査できます。
- ▶ 内部ブレード・ポートは、管理モジュール・ポートと同じ VLAN 上にあってはなりません。このことを守らなければ、重複 IP アドレスの問題が生じます。『重複 IP アドレス：その 1』(241 ページ)、および『重複 IP アドレス：その 2』(242 ページ) を参照してください。

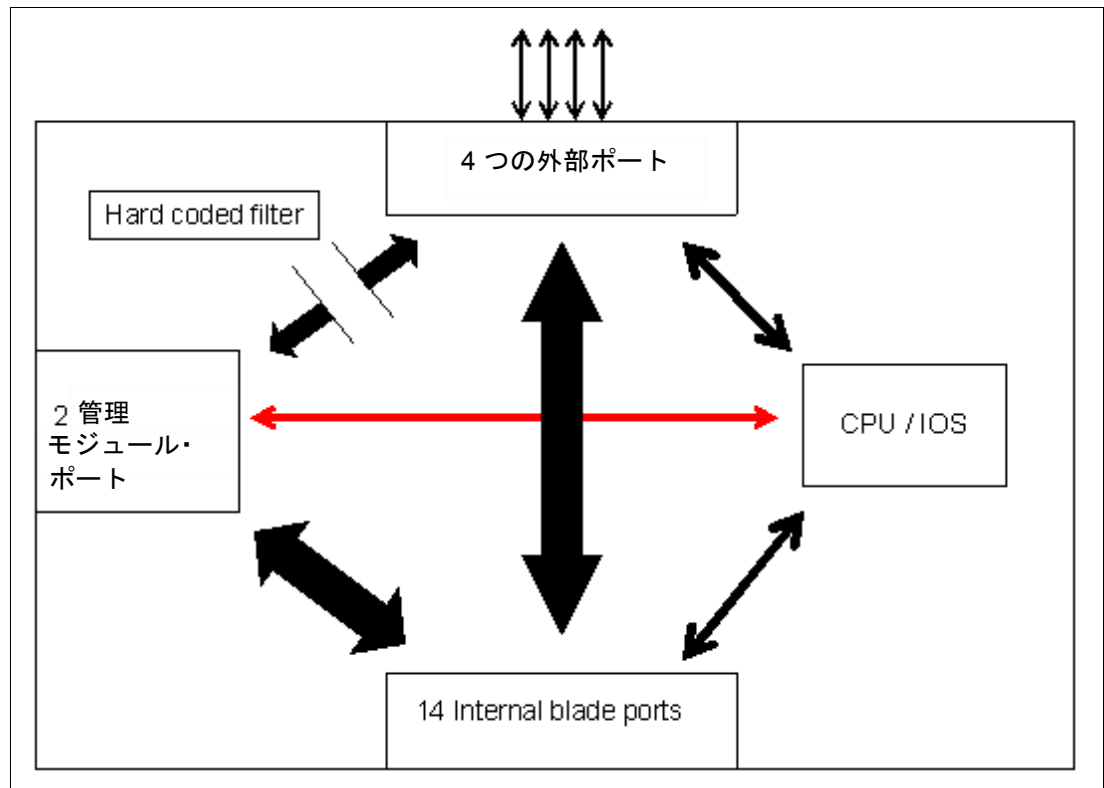


図 4-3 Cisco Systems IGESM 内のレイヤー 2 フレーム・フロー

## 4.1 Cisco Systems Intelligent Gigabit Ethernet Switch Module のブロック・ダイアグラム

22 ページの図 4-4 は、Cisco Systems Intelligent Gigabit Ethernet Switch Module のブロック・ダイアグラムを示しています。

Cisco Systems IGESM には、スイッチング用の ASIC が 2 つあります。パケット・バッファ用の 1 MB のオンチップ・キャッシュを備え、12 個の Gigabit Ethernet ポートをサポートします。2 つの ASIC は 10 ギガビット・リンクによって相互接続され、これは 22 ページの図 4-4 では 10 Gigabit Ethernet 接続として示されています。

それぞれのスイッチング ASIC には、ブレード・サーバー用の Gigabit Ethernet ポートが 7 つ、外部ポート用のポートが 2 つあります。また、管理モジュールへのポートもあります。ASIC と管理モジュール間の接続のリンクアップ速度は 100 Mbps です。

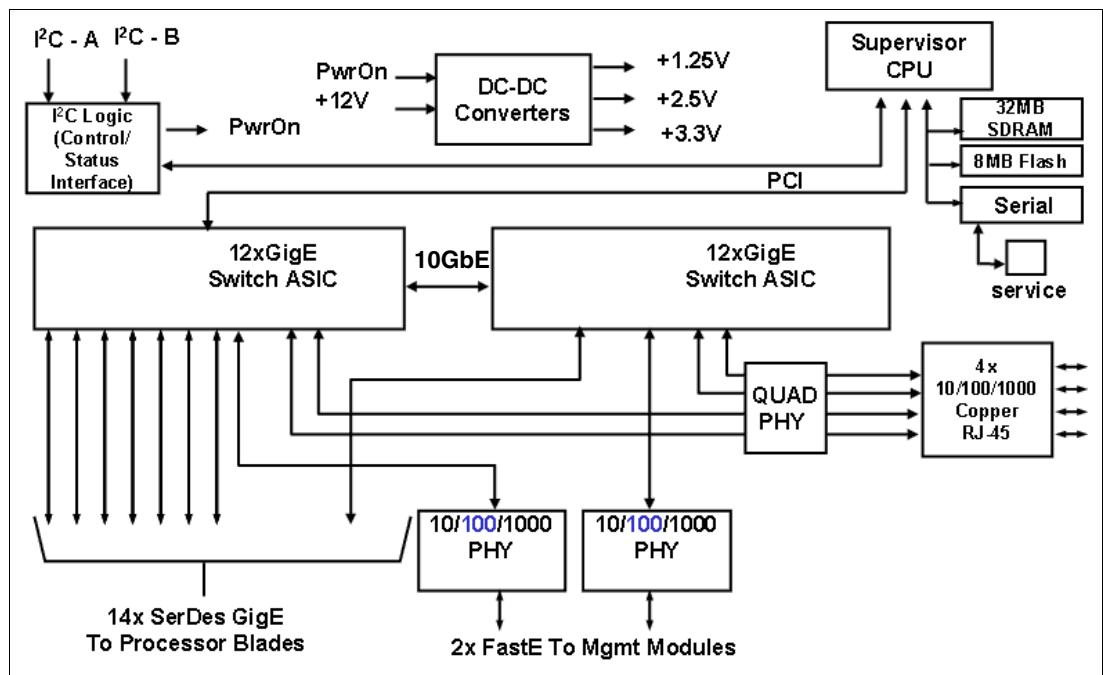


図 4-4 Cisco Systems IGESM ブロック・ダイアグラム



## Cisco Systems IGESM の管理と ユーザー・オリエンテーション

この章では、IBM @server BladeCenter 内の Cisco Systems Intelligent Gigabit Ethernet Switch Module (IGESM) の管理と配置に役立つツールとアプリケーションについて説明します。また、IGESM に接続してアクセスするための管理パスと規則についても説明します。

本書ですでに説明したとおり、本書の情報は IOS の 12.1(14) バージョンを実行する 4 ポート・銅・ベースの IGESM に適用されます。4 ポート SFP ベースの IGESM、または IGESM 12.1(22) 以上のコードを実行する 4 ポート・銅・ベースの IGESM を使用する場合は、これらのソリューションに該当する資料を参照してください。

## 5.1 Cisco Systems IGESM のユーザー・インターフェース

ここでは、スイッチ・モジュールの管理インターフェース、およびそれぞれのタスクの内容について説明します。

スイッチ・モジュールの構成と管理には、次のインターフェースを使用できます。

- ▶ コマンド行インターフェース (CLI)

CLI からスイッチおよびスイッチ・クラスター・メンバーの構成とモニターを行うことができます。CLI には、リモート管理ステーションから Telnet または SSH 経由でアクセスできます。また、スイッチ・モジュールのコンソール・ポートに直接接続した管理ステーション上で、端末エミュレーション・ソフトウェアを使用して CLI にアクセスすることもできます。

CLI を使用すると、必要なそれぞれの構成プロセスをより詳細に設定でき、詳しい結果が示されます。また、CLI には構成の検査とトラブルシューティングを行うためのさまざまなコマンドが備わっており、これらのコマンドは Cluster Management Suite GUI では使用できません。CLI を使用すると、CMS よりも柔軟にスイッチ・モジュールを構成できます。CLI はスクリプトに対応しており、実行に必要なオーバーヘッドが小さくて済みます。

また、Cisco Systems IGESM にはコンソール・ポートが組み込まれています。コンソール・ポートは、CLI を使用してソフトウェアを構成したり、スイッチに関する問題のトラブルシューティングを行ったりするために、端末または PC を接続できるサービス・ポートです。

**注：**新品の IGESM 上では、コンソール・ポートは小さい金属プレートによって隠されており、コネクタにアクセスするにはこの金属プレートを取り外す必要があります。このプレートは、IGESM 背面のポート g0/17 のすぐ上にあります。プレートを取り外すには、小型のねじ回しなどの適切な工具を使用してください。

このポートは標準の Cisco コンソール・ケーブル (IGESM には付属していません) を使用し、接続のデフォルト値は 9600、N、8、および 1 で、フロー制御は行いません。

- ▶ Cluster Management Suite (CMS) (IGESM 用の IOS の 12.1(14) バージョンでのみ使用可能)

CMS は、Netscape Communicator や Microsoft Internet Explorer などの Web ブラウザーを使用して、ネットワーク内のどこからでも起動できるグラフィカル・ユーザー・インターフェースです。CMS はスイッチにインストールされ、リモート管理ステーションに追加のソフトウェアをインストールする必要はありません。CMS を使用して、スタンドアロン・スイッチ、特定のクラスター・メンバー、またはスイッチ・クラスター全体の構成とモニターを行うことができます。また、ネットワーク・トポロジを表示してリンク情報を収集でき、スイッチ・イメージを表示してスイッチ・レベルとポート・レベルの設定値を変更できます。

CMS は、小規模から中規模の環境でスイッチ・モジュールを管理するために便利です。CMS を使用すれば、直観的なインターフェースとガイド・モードやウィザードなどの援助機能によって、セットアップを容易に行うことができます。

表 5-1 に、各インターフェースの特徴を要約します。

表 5-1 管理インターフェース

	コマンド行インターフェース (CLI)	Cluster Management Suite (CMS)
インターフェース・タイプ	テキスト・ベース	グラフィカル
利点	詳細さと制御能力	直観的で開始が容易
アクセス用のインターフェース	Telnet、SSH	Java プラグインを備えた Web ブラウザー
使用するポート	Telnet: 23 SSH: 22	HTTP 80 (デフォルト) 0 から 65535 までの値に変更できますが、ウェルノウン・ポート (1 から 1023) は除外する必要があります。
許可されるセッション番号	16 (Telnet を使用)、5 (SSH を使用)	N/A
ネットワーク・トポロジー・ビューアー	なし	あり
スクリプト対応	あり	なし
トラブルシューティング情報とデバッグ	完備	限定

### 5.1.1 コマンド行インターフェース

CLI は、多くの Cisco スイッチのユーザーに幅広く使用されている堅固なインターフェースです。ここでは、103 ページの第 7 章、『Cisco Systems IGESM の構成およびネットワーク統合』で説明するサンプル構成を実行するために役立つ、いくつかの基本的なコマンドについて説明します。また、構成の検査やトラブルシューティングのために便利なコマンドの例も示します。

CLI の各コマンドとその機能の詳しいリストについては、『Cisco Systems Intelligent Gigabit Ethernet Switch Module for the IBM @server BladeCenter System Command Reference』（Cisco Systems Intelligent Gigabit Ethernet Switch Module に付属）を参照してください。この資料はダウンロードすることも可能で、本書の巻末にあるオンライン・リソースのリストに含まれています。

#### CLI へのアクセス

スイッチ・モジュールの CLI にアクセスするには、次の 2 とおりの方法があります。

- ▶ Telnet
  - Telnet クライアントから直接アクセスする
  - 管理モジュール Web ブラウザーからセッションを起動する
  - IBM Director からセッションを起動する
- ▶ SSH (拡張暗号ソフトウェア・イメージにのみ含まれる)
  - SSH クライアントから直接アクセスする

図 5-1 は、Microsoft Windows® 2000 Telnet クライアントから Cisco スイッチ・モジュールに直接アクセスする例です。



User Access Verification

Username: USERID

Password:

CIGESM#2#

図 5-1 C:/WINNT/system32/cmd.exe - Telnet 192.168.70.128

## CLI コマンドのモード

Cisco IOS ユーザー・インターフェースには、さまざまなモードがあります。使用可能なコマンドは、現在使用しているモードによって異なります。表 5-2 では、これらのモードについて説明します。

- ▶ 主なコマンド・モード
- ▶ このモードの機能
- ▶ モードに応じた表示プロンプト
- ▶ アクセス方法
- ▶ モードを終了する方法

この表に示す例では、ホスト名 Switch を使用します。

表 5-2 CLI モード

モード	機能	プロンプト	開始方法	終了方法
ユーザー EXEC	限定された特権	Switch>	特権レベル 14 以下のユーザーのデフォルト。	<b>logout</b> または <b>quit</b> と入力します。
特権 (使用可能) EXEC	スーパーユーザー権限	Switch#	スイッチ・モジュールのデフォルト・ユーザー (USERID) のデフォルト設定での権限。 ユーザー・モードで <b>Enable</b> と入力します。 いずれかの構成モードから戻るときは <b>Ctrl+Z</b> を押します。	終了するには <b>disable</b> または <b>exit</b> と入力します。
グローバル 構成	グローバルな変更、つまりシステム全体に影響を及ぼす変更の実行	Switch(config)#	特権モードで <b>config terminal</b> と入力します。	終了して特権 EXEC モードに戻るには、 <b>exit</b> または <b>end</b> と入力するか、 <b>Ctrl+Z</b> を押します。
インターフェース 構成	インターフェース固有の構成のセットアップ	Switch(config-if)#	グローバル構成モードで <b>interface_name</b> を入力します。	終了してグローバル構成モードに戻るには、 <b>exit</b> と入力します。 終了して特権 EXEC モードに戻るには、 <b>Ctrl+Z</b> を押すか <b>end</b> と入力します。
VLAN 構成	VLAN の構成	Switch(config-vlan)#	グローバル構成モードで <b>vlan #</b> を入力します。	終了してグローバル構成モードに戻るには、 <b>exit</b> と入力します。 終了して特権 EXEC モードに戻るには、 <b>Ctrl+Z</b> を押すか <b>end</b> と入力します。

CLI の編集

表 5-3 に、キー・ストロークを使用する標準的な編集コマンドを示します。

表 5-3 編集キー・ストローク

目的	キー・ストローク
1 文字前に戻る	Ctrl+B
1 文字先に進む	Ctrl+F
1 文字削除する	Ctrl+D
1 ワード前に戻る	ESC+B
1 ワード先に進む	ESC+F
1 ワード削除する	Ctrl+W
行の先頭に移動する	Ctrl+A
行の末尾に移動する	Ctrl+E
カーソルから先頭までを削除する	Ctrl+U
カーソルから末尾までを削除する	Ctrl+K

ヘルプの表示

それぞれのコマンド・モードで使用可能なコマンドのリスト、または任意のコマンドに関連したキーワードと引数のリストを表示するには、表 5-4 に示すコマンドを使用します。

表 5-4 ヘルプ・コマンド

コマンド	機能
<code>?</code>	任意のコマンド・モードで、ヘルプ・システムの要旨を表示します。
<code>abbreviated-command-entry?</code>	特定の文字ストリングから始まるコマンドのリストを表示します。
<code>abbreviated-command-entry</code> + Tab	部分的なコマンド名を補完します。
<code>?</code>	特定のコマンド・モードで使用可能なコマンドをすべてリストします。
<code>command ?</code>	コマンドに関連したキーワードをリストします。
<code>command keyword ?</code>	キーワードに関連した引数をリストします。

コマンドの取り消しまたは機能の無効化

前に発行したコマンドのアクションを取り消す場合や、機構または機能を無効にする場合は、no 形式を使用します。たとえば、次のようにインターフェース構成モードで no shutdown を実行すると、インターフェースのシャットダウンが取り消されます。

```
CIGESM1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
CIGESM1(config)#interface g0/17
CIGESM1(config-if)#no shutdown
```

また、コマンドの再呼び出し（上下の矢印キーを使用）を行い、行の先頭に **no** を追加するだけで、コマンドを無効にすることができます。

## 構成の保管

行った構成または変更を保管するには、次の特権 EXEC コマンドを入力します。

```
Switch# copy running-config startup-config
```

このコマンドは、フラッシュ・メモリーにある現行構成セットを、始動構成セットとして NVRAM にコピーします。このコマンドを発行しなかった場合、またはコマンドが失敗した場合は、行った変更の内容はスイッチの次の再ロード時に失われます。

## 便利なコマンド

ここでは、構成およびトラブルシューティングに使用される代表的なコマンドの例をいくつか示します。ここにリストするコマンドはすべて、特権 EXEC モードで実行できます。

### 現行構成とシステム状況の検査

表 5-5 に示すコマンドは、現行設定値と状況を検査するために役立ちます。

表 5-5 現行構成の検査

コマンド	目的
<b>show version</b>	ソフトウェアのバージョン、システムのアップタイムなどを検査します。
<b>show platform summary</b>	スイッチが取り付けられているベイを表示します。また、すべてのポートの管理に関して管理モジュールがどのように構成されているか、および IGESM の IP アドレスの保存に関する管理モジュールの設定値が「Enabled」または「Disabled」のどちらに設定されているかを表示します。
<b>show running-config</b>	スイッチ・モジュールの現行構成を検査します。
<b>show interface status</b>	ポート状況を検査します。
<b>show cdp neighbors</b>	外部スイッチ間の物理接続を検査します。

また、表 5-6 で説明するコマンドを使用して、操作とスイッチの処理を検査することもできます。

表 5-6 操作の検査

コマンド	目的
<b>show logging</b>	システム・ヒストリーを検査します。
<b>terminal monitor</b> <b>terminal no monitor</b> (端末モニターを使用不可にする)	端末ウィンドウにスイッチ・メッセージを表示します。

### トラブルシューティング情報の収集

**show tech-support** コマンドを実行して、トラブルシューティング情報を収集できます。このコマンドは、**crashinfo** ファイルなどのデータを収集します。このファイルに保管されている情報は、IOS イメージの障害（破損）を引き起こした問題をテクニカル・サポート担当者がデバッグするために役立ちます。また、**show version** コマンドの結果や、**show running-config** コマンドの結果などのデータも収集します。

注：端末ソフトウェアのロギング機能を使用して、端末ウィンドウの表示内容をファイルに保管できます。ログ・ファイルに *more* 行が出力されないようにするには、次のコマンドを発行します。

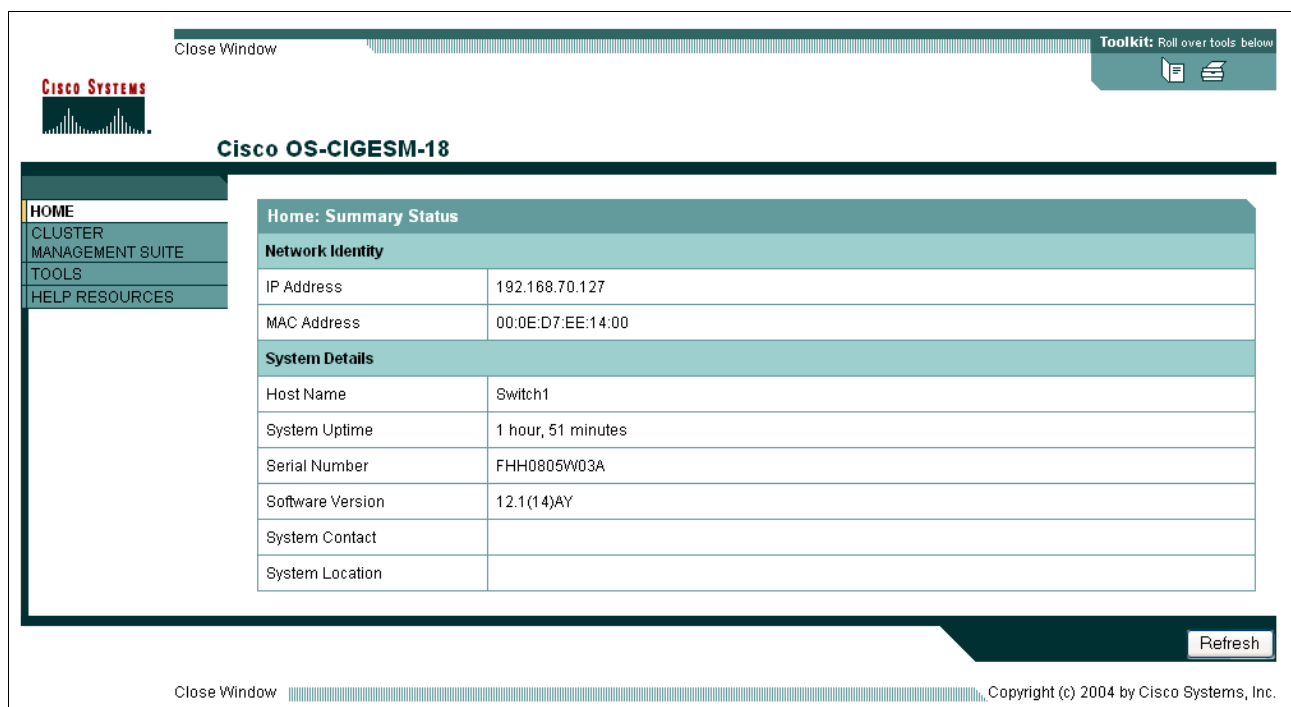
```
switch#terminal length 0
```

## 5.1.2 Cisco Systems Intelligent Gigabit Ethernet Switch Module ホーム

スイッチ・モジュールに IP アドレスを割り当てた後、スイッチ・モジュールの Web インターフェースである Cisco Systems Intelligent Gigabit Ethernet Switch Module ホームを開くことができます。このインターフェースを開くには、スイッチの IP アドレスを Web ブラウザーに入力し、スイッチのユーザー ID とパスワードを入力します。IOS の 12.1(14) バージョンの場合は、29 ページの図 5-2 に示すようなウィンドウが開きます。

メインペインには、スイッチの IP アドレス、MAC アドレス、およびスイッチ管理をサポートするその他の情報（ホスト名、シリアル番号、IOS バージョン、アップタイムなど）が表示されます。

左側のメニューから、Cluster Management Suite を起動したり、診断とモニターのツールを実行したり、ヘルプ・リソースにアクセスしたりすることもできます。



The screenshot shows the Cisco OS-CIGESM-18 web interface. The top bar includes a 'Close Window' button and a 'Toolkit: Roll over tools below' menu. The main content area is titled 'Home: Summary Status' and contains two tables. The first table, 'Network Identity', shows the IP Address as 192.168.70.127 and the MAC Address as 00:0E:D7:EE:14:00. The second table, 'System Details', shows the Host Name as Switch1, System Uptime as 1 hour, 51 minutes, Serial Number as FHH0805W03A, Software Version as 12.1(14)AY, System Contact, and System Location. A 'Refresh' button is located at the bottom right of the main content area. The bottom bar includes another 'Close Window' button and a copyright notice: 'Copyright (c) 2004 by Cisco Systems, Inc.'

Network Identity	
IP Address	192.168.70.127
MAC Address	00:0E:D7:EE:14:00

System Details	
Host Name	Switch1
System Uptime	1 hour, 51 minutes
Serial Number	FHH0805W03A
Software Version	12.1(14)AY
System Contact	
System Location	

図 5-2 Cisco Systems Intelligent Gigabit Ethernet Switch Module ホーム (12.1(14) IOS)

## 5.1.3 Cisco Systems IGESM Cluster Management Suite

CMS の一般的な操作手順については、「Cisco Systems Intelligent Gigabit Ethernet Switch Module for the IBM @server BladeCenter Software Configuration Guide」に説明があります。詳細はオンライン・ヘルプに記載されています。CMS の要約情報は、次の URL にあります。

<http://www.cisco.com/warp/public/cc/techno/media/lan/ether/sgth/>

データ・シートとプレゼンテーションは、次の URL にあります。

<http://www.cisco.com/warp/public/cc/techno/media/lan/ether/sgth/prodlit/index.shtml>

CMS にアクセスするには、まず 29 ページの 5.1.2、『Cisco Systems Intelligent Gigabit Ethernet Switch Module ホーム』で説明したように、Cisco Systems Intelligent Gigabit Ethernet Switch Module ホームにログオンする必要があります。

CMS は、CIGESM 用の IOS の 12.1(14) バージョンでのみ使用できます。

スイッチ・モジュールのホーム・ページで、「Cluster Management Suite」をクリックします。スイッチのユーザー ID とパスワードを入力すると、30 ページの図 5-3 に示すようなウィンドウに進みます。

お願い：このセッションには Java 1.4 プラグインが必要です。必要な場合は、プラグインをダウンロードしてインストールするためのオプションが表示されます。この例で CMS へのアクセスに使用したシステムは Java 1.4.2\_03 プラグインを実行しており、表示されました。「Continue」をクリックしたところ、インターフェースにアクセスできました。

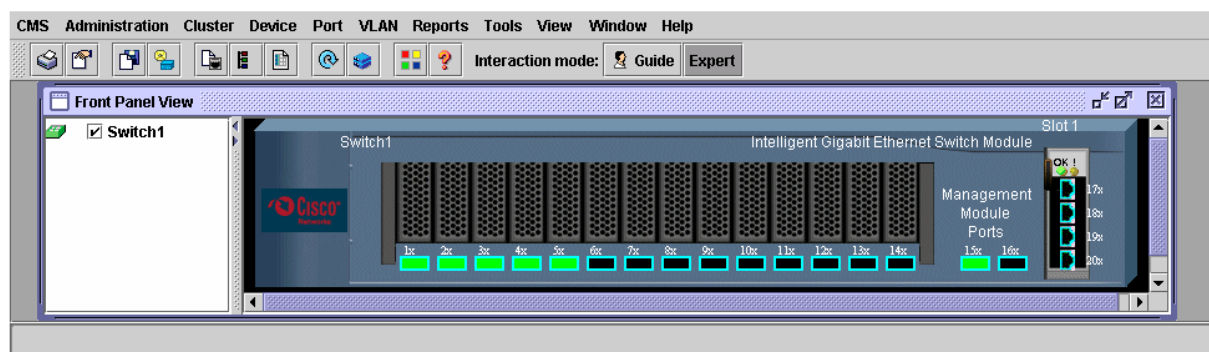


図 5-3 Cisco Systems Intelligent Gigabit Ethernet Switch Module Cluster Management Suite

CMS のフロント・パネル・ビューでは、次の機能を使用できます。

メニュー・バー

単一のスイッチ、およびスイッチ・クラスターを管理するためのオプションすべてのリストがあります。

ツールバー・ボタン

よく使われるスイッチおよびクラスターの構成オプション、および凡例やオンライン・ヘルプなどの情報ウィンドウのボタンがあります。

ポートおよびデバイスのポップアップ・メニュー

ポートのポップアップ・メニューには、スイッチ・ポートの構成とモニターに固有のオプションがあり、デバイスのポップアップ・メニューには、スイッチとクラスターの構成とモニターに関するオプションがあります。

次の図に、メニュー・バーのオプションを示します。CMS を使用する前に、これらのオプションをよく確認しておくことをお勧めします。メニュー・バーのオプションには、次のものがあります。

- ▶ CMS (図 5-3)
  - Page Setup
  - Print Preview
  - Print
  - Guide

- Expert
- Preferences

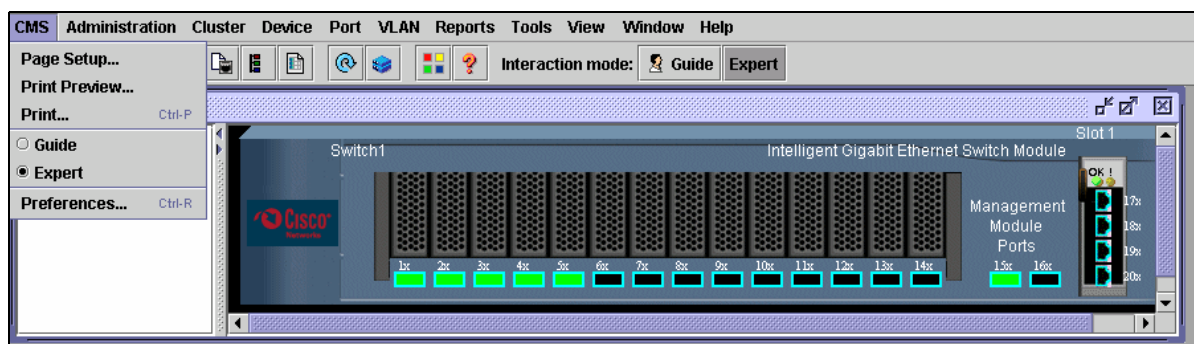


図 5-4 CMS メニュー

- ▶ Administration (31 ページの図 5-4)
  - IP Addresses
  - SNMP
  - System Time
  - HTTP Port
  - Users and Passwords
  - Console Baud Rate
  - MAC Addresses
  - ARP
  - Save Configuration
  - Restore Configuration
  - Software Upgrade
  - System Reload
  - Event Notification

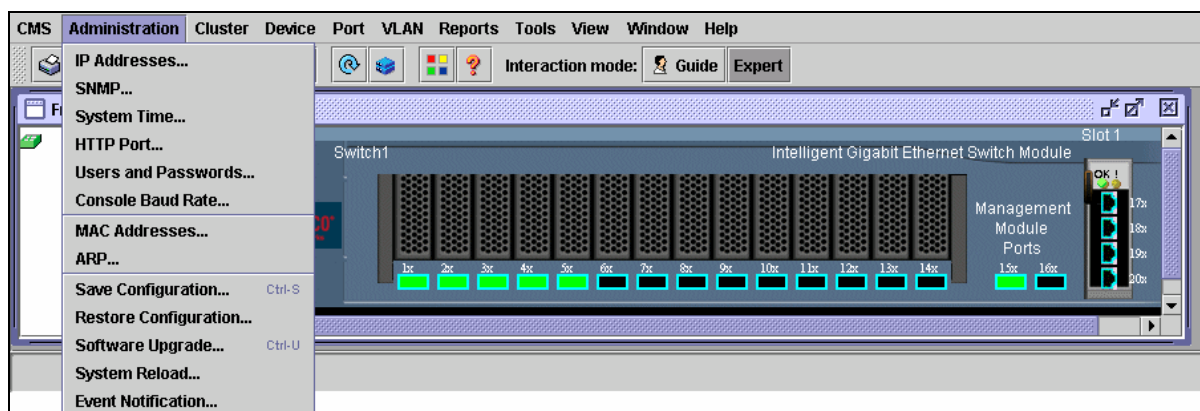


図 5-5 「Administration」メニュー

- ▶ Cluster (図 5-6)
  - Create Cluster

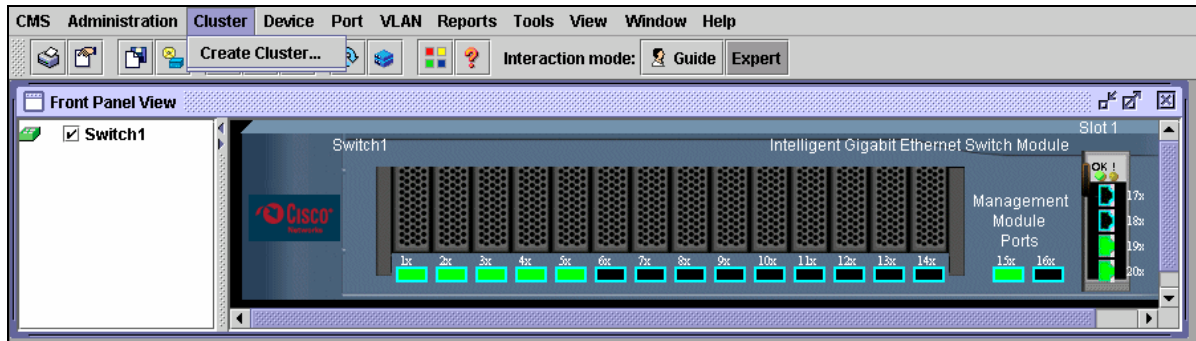


図 5-6 「Cluster」メニュー

- ▶ Device (図 5-7)
  - Host Name
  - STP
  - IGMP Snooping
  - ACL (読み取り書き込みモードでガイド・モードが使用可能)
  - Security Wizard
  - QoS
  - AVVID Wizards

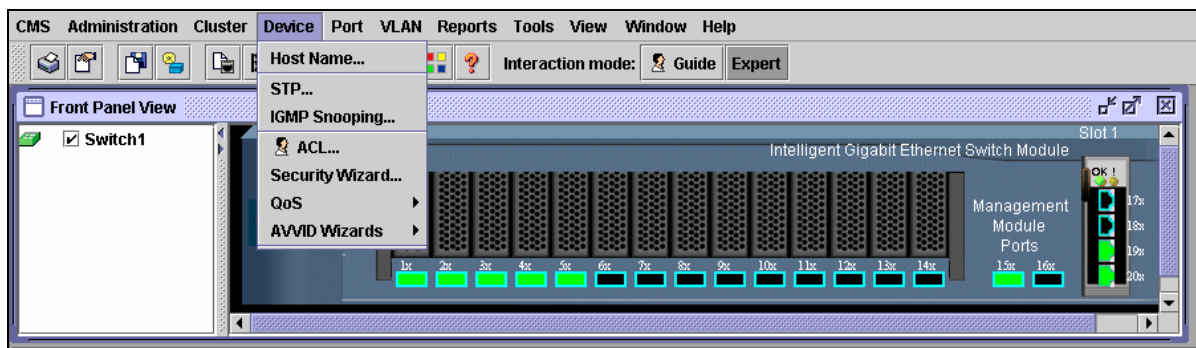


図 5-7 「Device」メニュー

- ▶ Port (図 5-8)
  - Port Settings
  - Port Search
  - Port Security
  - EtherChannels
  - SPAN
  - Protected Port
  - Flooding Control

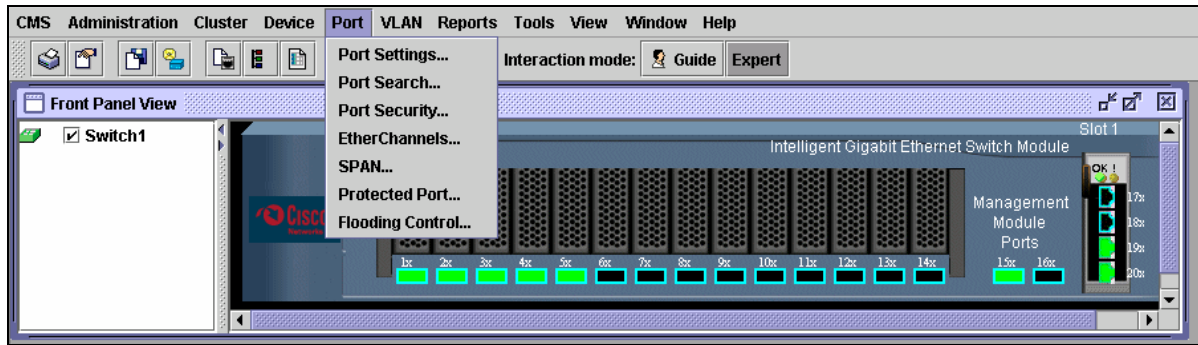


図 5-8 「Port」メニュー

- ▶ VLAN (図 5-9)
  - VLAN (読み取り書き込みモードでガイド・モードが使用可能)
  - Management VLAN
  - VMPS
  - Voice VLAN

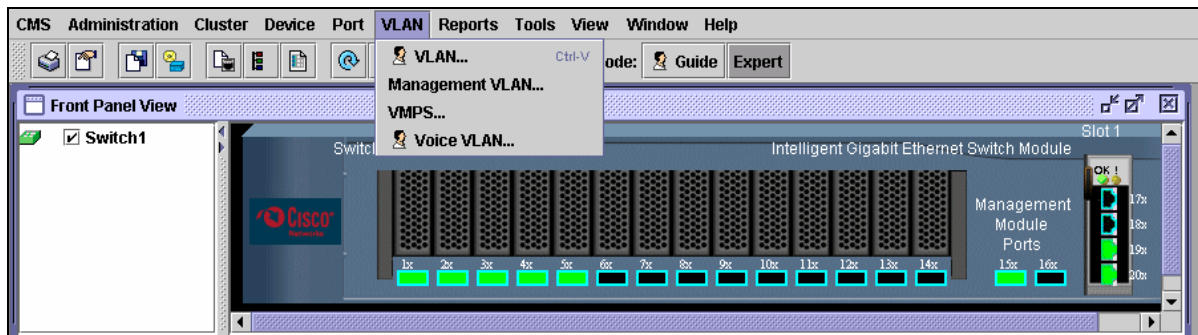


図 5-9 「VLAN」メニュー

- ▶ Reports (図 5-10)
  - Inventory
  - Port Statistics
  - Bandwidth Graphs
  - Link Graphs
  - Link Reports
  - Multicast
  - Resource Monitor
  - System Messages

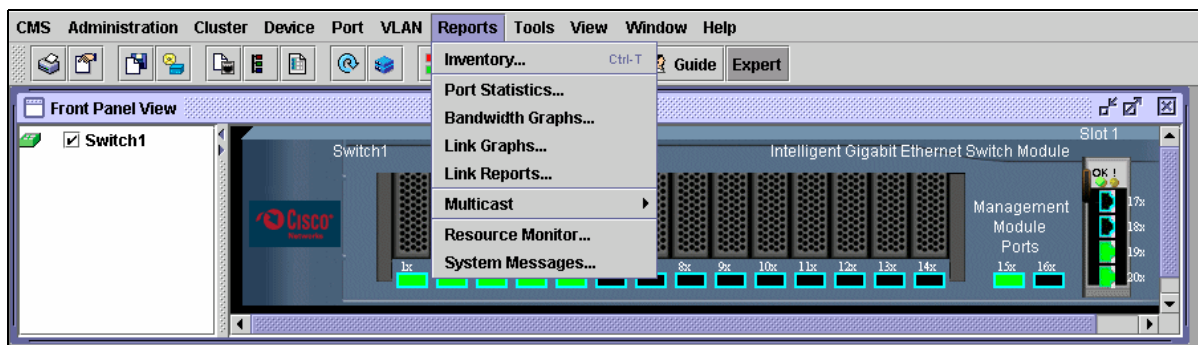


図 5-10 「Reports」メニュー



- ▶ Tools (図 5-11)
  - Ping and Trace

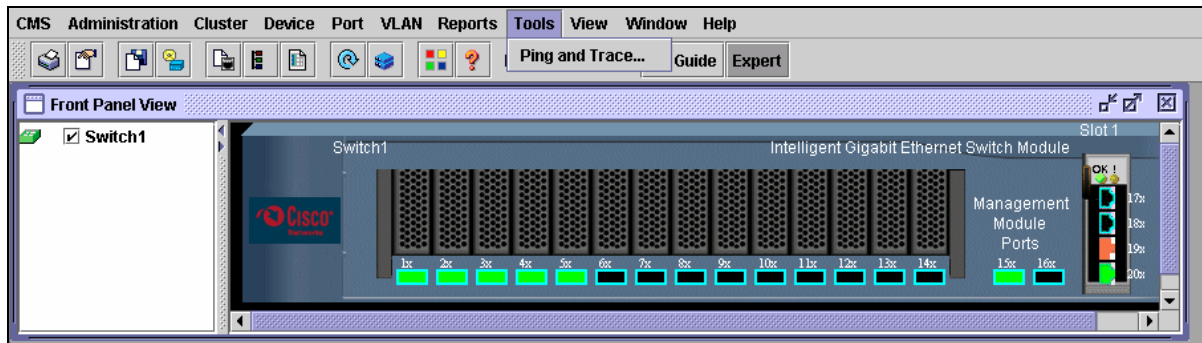


図 5-11 「Tools」メニュー

- ▶ View (図 5-12)
  - Refresh
  - Front Panel

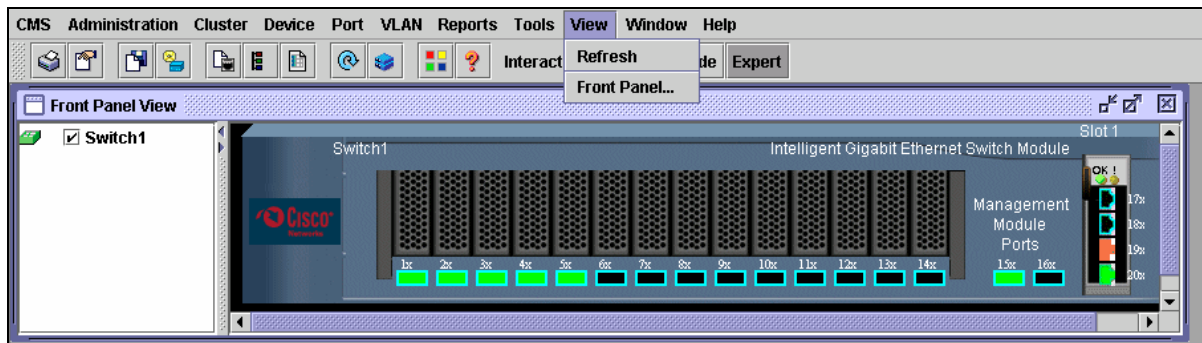


図 5-12 「View」メニュー

- ▶ Window (図 5-13)
  - フロント・パネル・ビュー

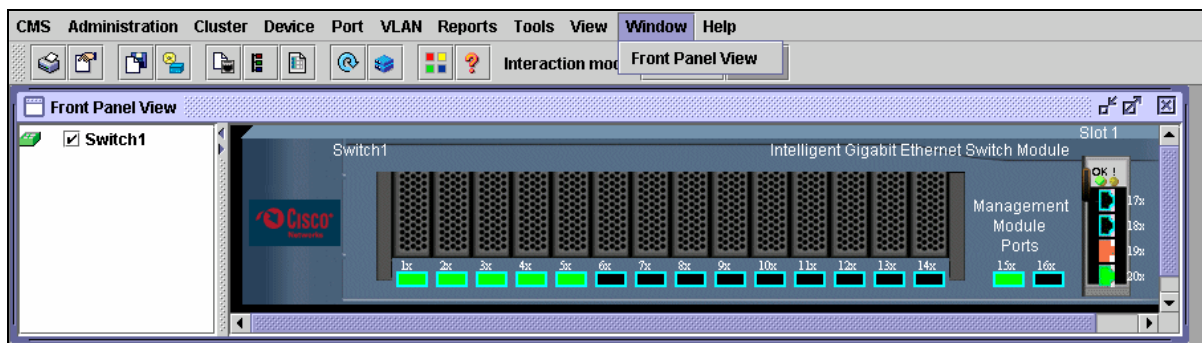


図 5-13 「Window」メニュー

- ▶ Help (図 5-14)
  - Overview
  - What's New?
  - Help For Active Window
  - Contents
  - Legend
  - About

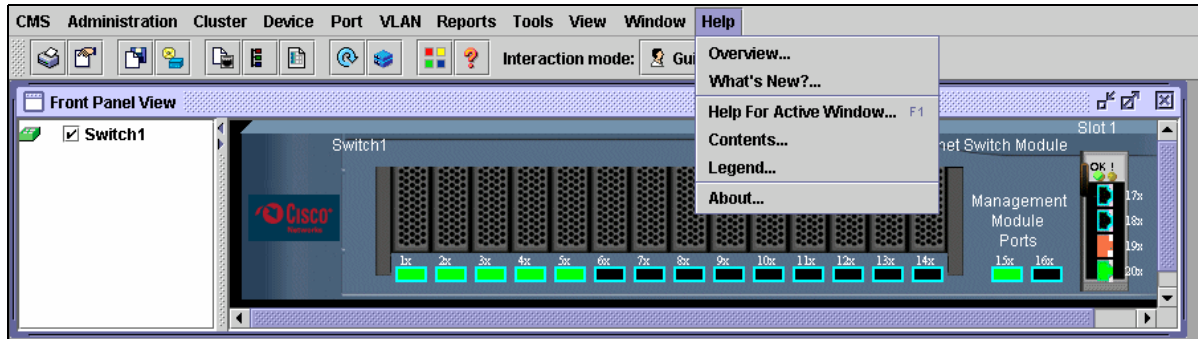


図 5-14 「Help」メニュー

スイッチ・モジュールを右クリックすると、図 5-15 に示すようなデバイスのポップアップ・メニューが開きます。選択したスイッチ・モジュールは、黄色い線で囲まれます。

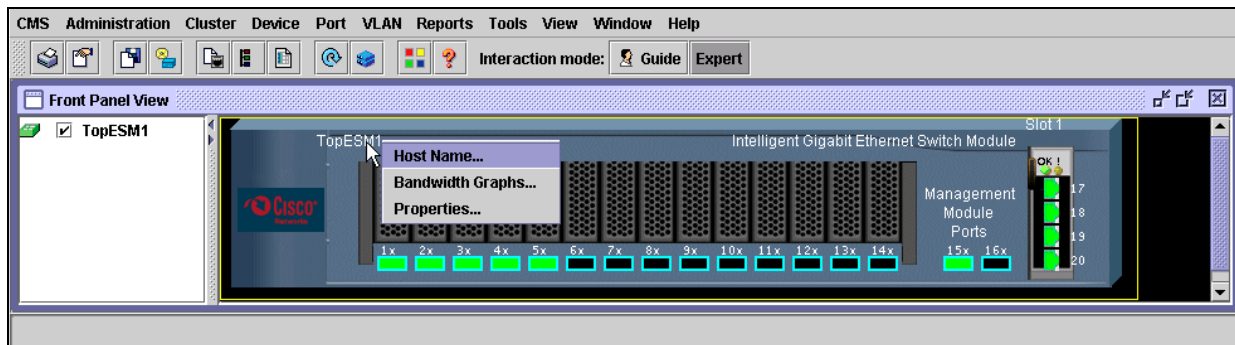


図 5-15 デバイスのポップアップ・メニュー

ポップアップ・メニューから次の各項目を選択すると、スイッチ・モジュールの設定値とパフォーマンス・データを確認および構成できます。

- ▶ Host Name (図 5-16)
- ▶ Bandwidth Graphs (36 ページの図 5-17)
- ▶ Properties (36 ページの図 5-18)

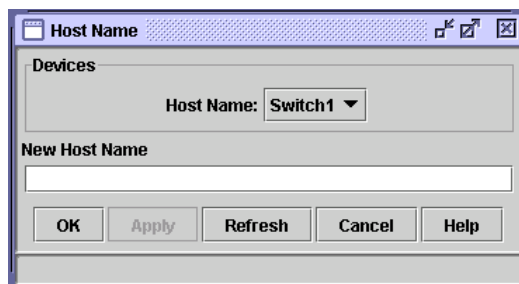


図 5-16 デバイスのポップアップ・メニュー: Host Name

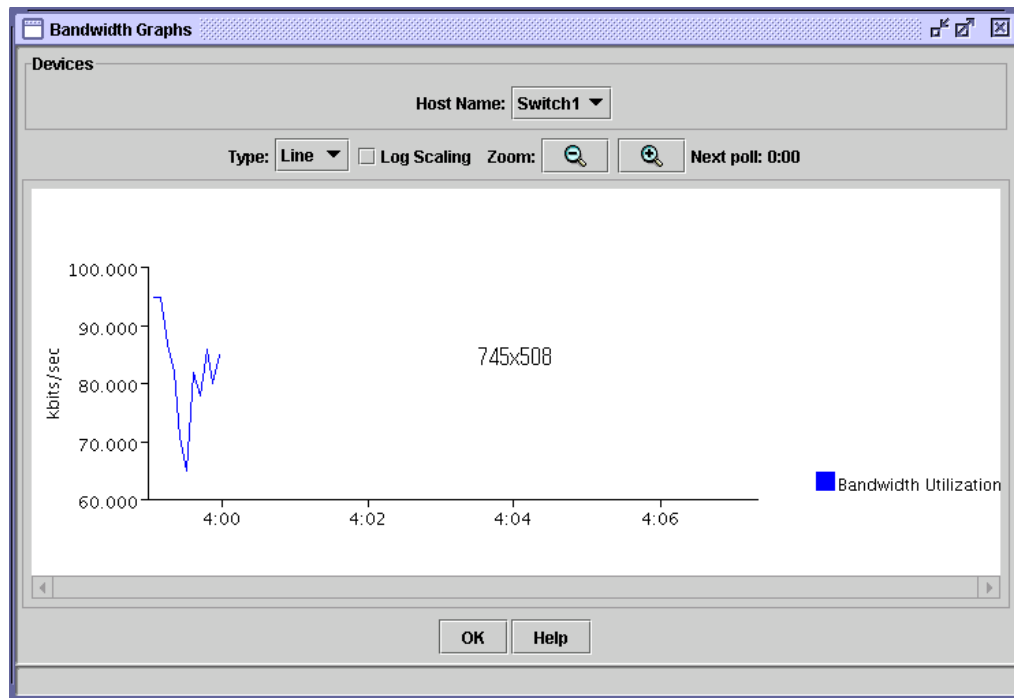


図5-17 デバイスのポップアップ・メニュー: *Bandwidth Graphs*

図5-18 デバイスのポップアップ・メニュー: *Device Properties*

図 5-19 に示すようなポートのアイコンを右クリックすると、ポートのポップアップ・メニューが開きます。Shift または Ctrl を使用して複数のポートを選択すると、これらのポートを同時に構成できます。また、ポップアップ・メニューから「Select All Ports」を使用して、すべてのポートを選択することもできます。選択したポートは、黄色い線で囲まれます。

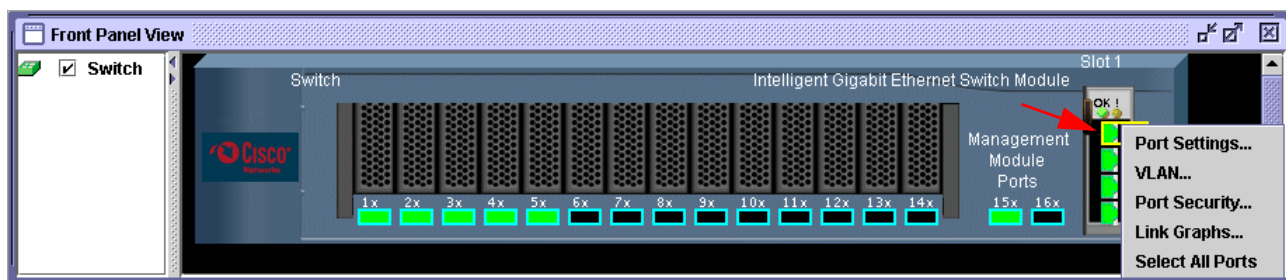


図5-19 ポートのポップアップ・メニュー

ポップアップ・メニューから、次のメニュー項目を表示および構成できます。

- ▶ Port Settings ( 図 5-20)
- ▶ VLAN (38 ページの図 5-21)
- ▶ Port Security (38 ページの図 5-22)
- ▶ Link Graphs (38 ページの図 5-23)

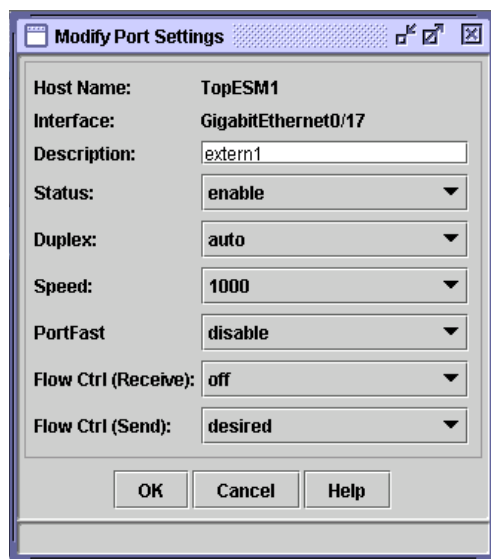


図5-20 ポートのポップアップ・メニュー : Modify Port Settings

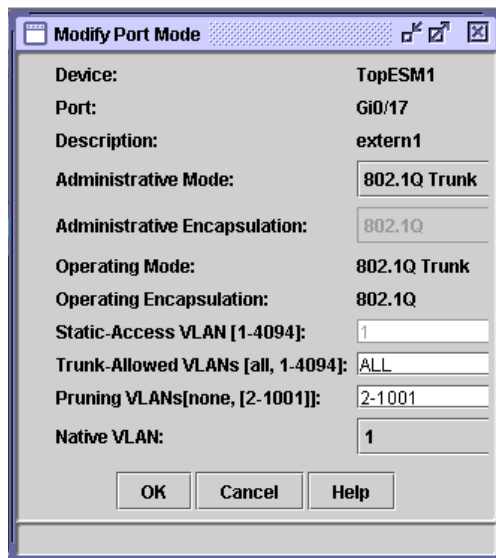


図 5-21 ポートのポップアップ・メニュー : VLAN

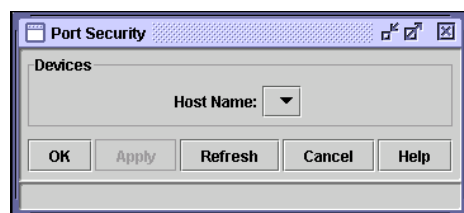


図 5-22 ポートのポップアップ・メニュー : Port Security

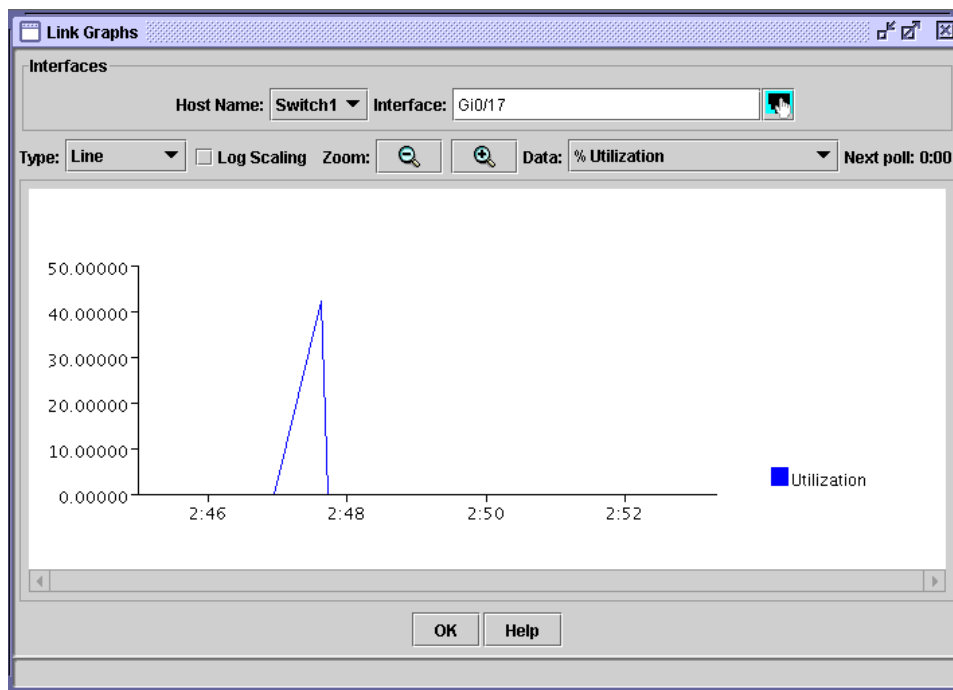


図 5-23 ポートのポップアップ・メニュー : Link Graphs

## 5.1.4 Cisco Systems Intelligent Gigabit Ethernet Switch Module のツール

スイッチ管理ホーム・ページで「Tools」をクリックすると、図 5-24 に示すようなウィンドウが表示されます。このウィンドウを使用して、スイッチへの Telnet セッションを開始したり、モニター情報やトラブルシューティング情報を入手したりできます。「Tools」ウィンドウには次のメニューがあります。

<b>Telnet</b>	スイッチ・モジュールへの Telnet セッションを開きます。
<b>Extended Ping</b>	ping ダイアログを開きます。このダイアログでは、拡張 ping を発行できます。このツールは、スイッチ・モジュールと別のスイッチとの間の接続についてトラブルシューティングを行う際に便利です。
<b>Diagnostic Log</b>	システム・メッセージ・ログからの出力を表示し、特権 EXEC コマンドをデバッグします。
<b>Monitor Switch</b>	コマンドのリストを指定した特権モードでコマンド行インターフェースを開きます。このメニューを使用すれば、CLI コマンドをより柔軟な方法で対話式に発行できます。0 から 15 までのさまざまな特権レベルを選択することもできます。
<b>Show Interfaces</b>	<b>show the interfaces</b> CLI コマンドを発行します。このコマンドは、すべてのインターフェースの状況と構成を表示し、トラブルシューティングに便利です。

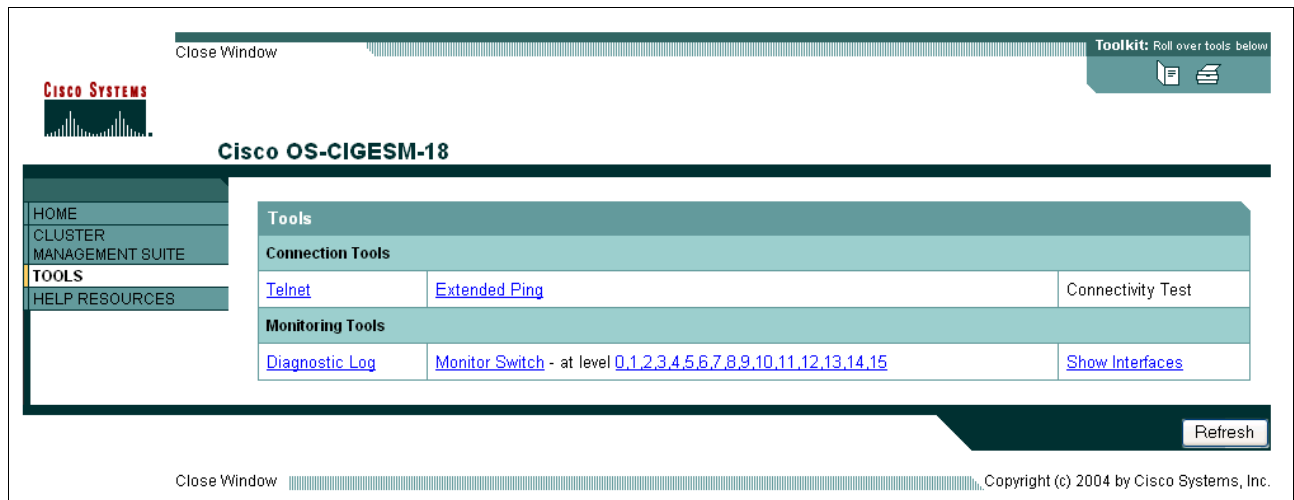


図 5-24 Cisco Systems Intelligent Gigabit Ethernet Switch Module のツール

## 5.1.5 Cisco Systems Intelligent Gigabit Ethernet Switch Module のヘルプ・リソース

「Help Resources」メニュー (図 5-25) にアクセスすると、他のヘルプ・リソースと製品資料のリンクが表示されます。

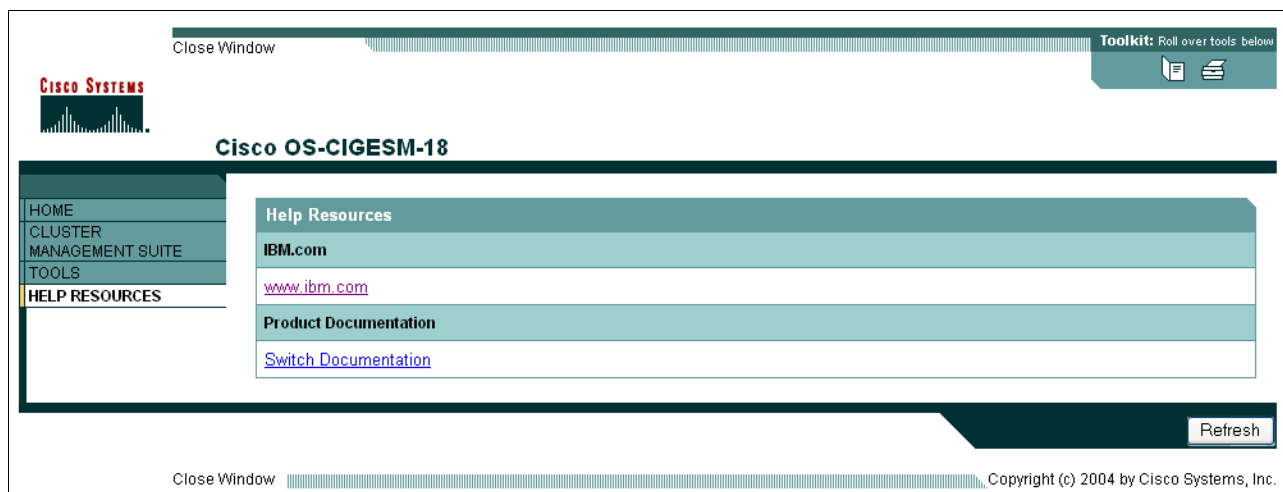


図 5-25 Cisco Systems Intelligent Gigabit Ethernet Switch Module のヘルプ・リソース

## 5.2 システム管理に関する考慮事項

ここでは、Cisco Systems IGESM のシステム管理機能の一部、およびシステム管理ツールについて解説します。IGESM の管理パスに関する考慮事項の詳しい説明については、56 ページの 5.3、『管理パスに関する詳細説明』を参照してください。

**重要：**実際に BladeCenter 内の IGESM を適切に管理するためには、BladeCenter 内の管理モジュールの適切な管理も必要です。つまり、管理モジュールのいくつかの設定値、および必要な IGESM 構成設定値を理解し、適切に構成しなければ、IGESM を正しく配置することは事実上不可能です。

### 5.2.1 アウト・オブ・バンド管理の定義

すべてのデバイスに対して（物理的に）分離した管理インターフェースを用意し、管理トラフィックのみを伝送することがよく行われます。この方式は **アウト・オブ・バンド管理** と呼ばれ、別個のイーサネット接続を使用する場合や、完全に異なる物理接続（コンソール・ポートなど）を使用する場合があります。管理モジュールを経由したイーサネット・ベースのアウト・オブ・バンド管理のために BladeCenter を構成する方法について詳しくは、60 ページの 5.3.4、『考慮事項：IGESM の管理に管理モジュールのアップリンクを使用する場合』を参照してください。

イーサネット・スイッチを管理するほかに、ブラウザを使用して管理モジュールにログオンすることによって、BladeCenter 内のブレード・サーバーすべてを管理することもできます。BladeCenter 内では、サーバー管理トラフィック（通常はサーバー・コンソール・アクセス）は別個のバスを経由して流れます。このバスは I2C バスで、BladeCenter のデータ・トラフィック・バスとは常に分離されています。

BladeCenter は少なくとも 1 つの管理モジュールとともに出荷され、外部イーサネット・インターフェースをサポートします。デフォルトでは、このインターフェースを使用してブ

レード・サーバー、イーサネット・スイッチ、および管理モジュール自体の管理が行われます。IGESM はこのパス経由で管理することも、専用の外部アップリンクによって管理することもできます。（これらの管理パスの規則に関する詳しい説明は、56 ページの 5.3、『管理パスに関する詳細説明』を参照してください）

デフォルトでは、イーサネット内部スイッチ管理ポートは VLAN 1 に配置されます。通常、セキュリティ上の理由から VLAN 1 は使用しないように Cisco は勧告していますが、管理目的で VLAN 1 を使用することはよくあります。また、ブレード・サーバー・インターフェースのいずれかによって共用されていない VLAN に、IGESM 用の管理インターフェースを配置することも非常に重要です。

**重要：**IGESM 管理 VLAN を使用するようにブレード・サーバーを構成すると、予期しない重複 IP アドレスが報告される可能性があります。これは、管理モジュールが内部接続上のデバイスのプロキシとして動作しようとするために起こります。77 ページの図 5-51 に、この詳しい説明があります。

## 5.2.2 インバンド管理の定義

お客様によっては、2 つ目の操作モードである **インバンド管理** を使用することがあります。この場合、管理トラフィックはデータ・トラフィック・パスを経由して移動します（IGESM アップリンク）。

BladeCenter スイッチがインバンド管理用に構成されている場合でも、BladeCenter 管理モジュールの内部インターフェースに接続したスイッチの内部ポート構成は、同じ管理 VLAN に配置されるように自動的に変更されます。このため、予期しない結果が生じることがあります。（インバンド管理の構成について詳しくは、63 ページの 5.3.5、『考慮事項：IGESM アップリンクを使用した IGESM の管理』を参照してください。）インバンド管理を構成すると、他のクライアント/サーバー・トラフィックと限られた帯域幅を共用する必要性が生じます。適切に管理しなければ、ブロードキャスト・トラフィックによって管理モジュールの CPU に過大な負担がかかり、そのために他の重大な問題が生じる可能性があります。

## 5.2.3 Cisco Systems IGESM への管理トラフィックのパス

ここでは、Cisco Systems IGESM に接続して管理するためのさまざまな方法について説明します。次の説明でいう管理トラフィックには、管理ワークステーションと Cisco Systems IGESM の間の HTTP、Telnet、TFTP、および SNMP ベースのトラフィックが含まれます。詳しくは、56 ページの 5.3、『管理パスに関する詳細説明』を参照してください。

42 ページの図 5-26 は、Cisco Systems IGESM に接続する際に使用できる最も一般的なパスを示しています。

### パスの要約

パス 1 と 2 は、Cisco Systems IGESM への従来型のアウト・オブ・バンド管理パスとして分類されます（管理トラフィックがデータ・トラフィックと同じ物理接続を使用しないので、アウト・オブ・バンドと呼ばれます）。

パス 3 と 4 は、Cisco Systems IGESM への従来型のインバンド管理パスとして分類されます。

パス 5 は、場合によってはアウト・オブ・バンド管理の 1 形式として分類され、端末サーバーを経由して管理ネットワークまたは経路指定された実動ネットワークに接続されることも、接続されないこともあります。



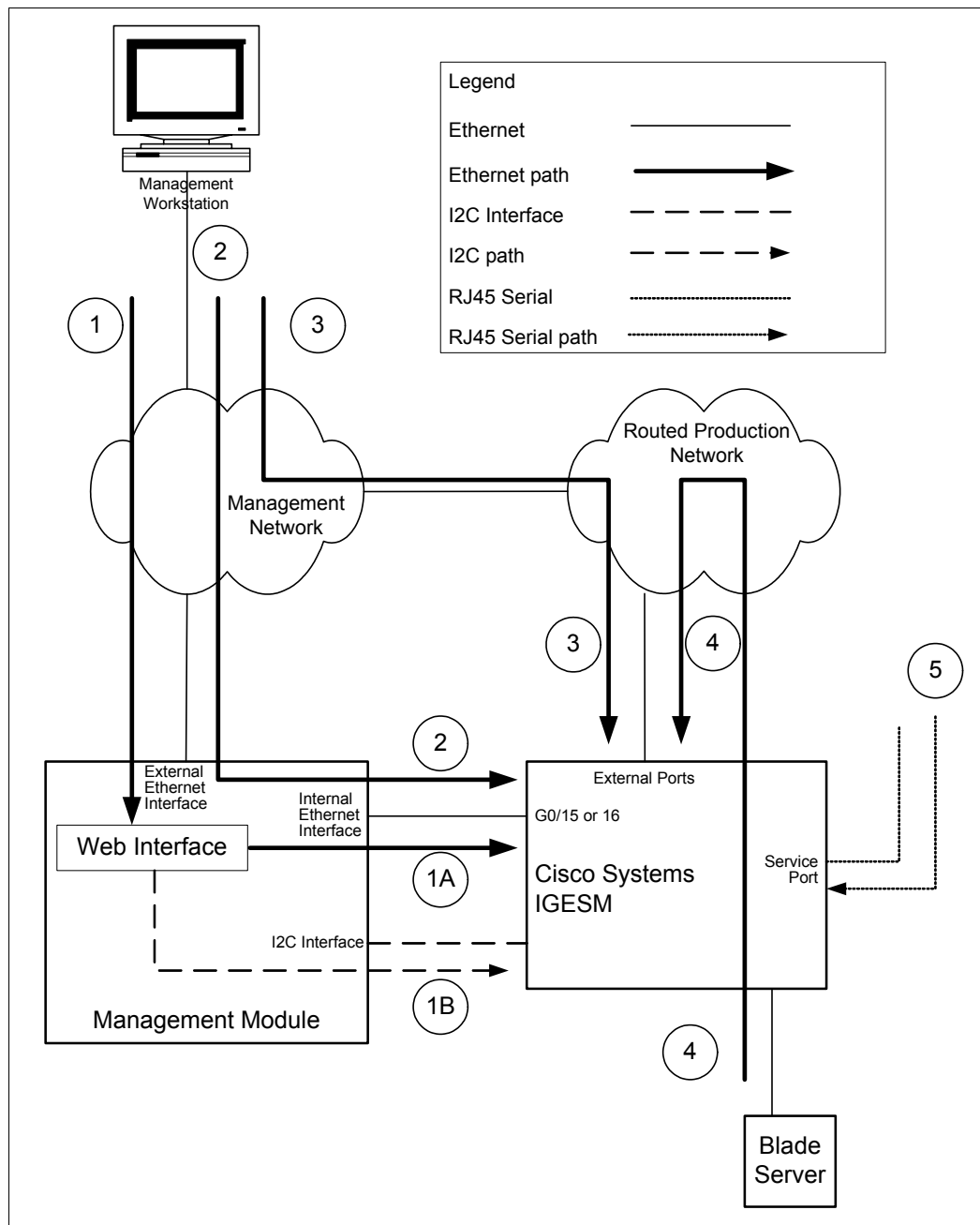


図 5-26 Cisco Systems IGESM への管理パス

## パス 1 の詳細

パス 1 は、いずれかの管理ワークステーションから、管理ネットワークを通り、管理モジュールの外部イーサネット・インターフェースを経由して管理モジュールに至ります。(管理ワークステーションは、管理モジュールの外部 IP アドレスを直接ブラウザに指定します。) Web インターフェースを経由して管理モジュールに接続した後、Cisco Systems IGESM を実際に管理するためにパス 1 は 2 つの方向に分かれることがあります。

### パス 1A

このパスは、管理モジュール内の Web ベースのインターフェースから使用できる一部のツールによって使用されるパスです (たとえば、管理モジュールのインターフェースから IGESM への Telnet セッションまたは HTTP セッションを起動するツールなど)。ツールの起

動後、管理モジュールは外部管理ネットワークから Cisco Systems IGESM への単なるパススルーとして機能し、パスは管理モジュールと Cisco Systems IGESM の間のイーサネット接続を経由するので、実質的にはパス 2 になります。このパスが機能するためには、Cisco Systems IGESM の管理 IP アドレスが、管理モジュールの内部および外部の両イーサネット・インターフェース上で使用されているものと同じ IP サブネット内にあることが必要です。

管理モジュールを経由したアウト・オブ・バンド管理のために BladeCenter を構成する方法について詳しくは、60 ページの 5.3.4、『考慮事項：IGESM の管理に管理モジュールのアップリンクを使用する場合』を参照してください。

### パス 1B

これは、管理モジュールが特定のタスクのために Cisco Systems IGESM ( および BladeCenter の他コンポーネント ) と通信するために使用する、非常に特別なパス (I2C インターフェース) です。これは通常のデータ・パスには含まれず、管理モジュールから BladeCenter 内の他コンポーネント、およびパス 1B の特定のケースでは Cisco Systems IGESM への非常に特別な命令のみに使用されます。技術的な観点からは、このパスは Cisco Systems IGESM に対して管理モジュールが特定の操作を行うときに使用されます (たとえば、Cisco Systems IGESM の IP アドレスの設定、または Cisco Systems IGESM のデフォルト値へのリセット)。通常、HTTP、Telnet、または Cisco Systems IGESM に対する ping テストに関連したものを除く、管理モジュール Web ベース・インターフェースの Cisco Systems IGESM 管理ツールは、すべてパス 1B に含まれます。パス 1B は、Cisco Systems IGESM 上で設定されている管理 IP アドレスに関係なく使用できることに注意してください。

### パス 2 の詳細

パス 2 は、管理ネットワーク上のいずれかの管理ワークステーションから Cisco Systems IGESM へのパスで、この接続のパススルーとして管理モジュールを使用します。(管理ワークステーションは、Cisco Systems IGESM の管理 IP アドレスを Web、Telnet、SNMP などのアプリケーションに直接指定します。) この場合、Cisco Systems IGESM と管理ワークステーション間の管理トラフィックは、管理ネットワークを通り、管理モジュールを経由して、管理モジュールと Cisco Systems IGESM の間の内部イーサネット・ネットワークに至ります (戻りパスも同じ)。パス 1A の場合と同様に、このパスが機能するためには、Cisco Systems IGESM の管理 IP アドレスが、管理モジュールの内部および外部の両イーサネット・インターフェース上で使用されているものと同じ IP サブネット内にあることが必要です。

管理モジュールを経由したアウト・オブ・バンド管理のために BladeCenter を構成する方法について詳しくは、60 ページの 5.3.4、『考慮事項：IGESM の管理に管理モジュールのアップリンクを使用する場合』を参照してください。

### パス 3 の詳細

パス 3 は、管理ネットワークと経路指定された実動ネットワークの間の接続を使用して、Cisco Systems IGESM と管理ワークステーションの間でトラフィックを伝送します。(管理ワークステーションは、Cisco Systems IGESM の外部で使用可能な管理 IP アドレスを Web、Telnet、SNMP などのアプリケーションに直接指定します。) この場合、管理モジュールは Cisco Systems IGESM の管理の目的では完全にバイパスされ、管理トラフィックは Cisco Systems IGESM の外部 GigE 接続を両方向に流れます。

Cisco Systems IGESM にパス 3 を経由してアクセスするには、管理モジュールの「*advanced management*」Web ページで、「*External ports*」を「*Enabled*」に設定し、「*Management over all ports*」を「*Enabled*」に設定する必要があります。これらのいずれかが使用不可に設定されている場合、パス 3 は機能しません。

このシナリオでは、Cisco Systems IGESM の IP アドレスは、管理モジュールによって使用される IP アドレスとは別の IP サブネット上にあることが必要です。これら (管理モジュールと Cisco Systems IGESM) が同じ IP サブネット上にある場合、管理モジュールは Cisco Systems IGESM のプロキシとして動作しようとするため、ネットワークに混乱が生じる可

能性があります。また、Cisco Systems IGESM 上の管理 VLAN をデフォルトの VLAN1 以外のものに変更することもお勧めします。これは、外部接続を経由した Cisco Systems IGESM へのアクセスに使用される IP サブネットを含む VLAN にあることが必要です。たとえば、Cisco Systems IGESM の管理 IP アドレスが 10.200.200.X (24 ビット・マスク) である場合、使用する Cisco Systems IGESM の管理 VLAN は、10.200.200.X サブネットワークのトラフィックを、経路指定された実動ネットワークに伝送する必要があります。

Cisco Systems IGESM の管理 VLAN を変更するには、次の手順で行います。

1. Cisco Systems IGESM 上で新規 VLAN を作成します (**vlan XX**)。
2. 新規 VLAN へのインターフェースを作成します (**interface vlan XX**)。
3. 新規 VLAN インターフェース上で **no shut** を実行します。

その後、この新規の管理 VLAN をアップリンク接続に追加し (**switchport trunk allowed vlan yy,zz,XX...**)、経路指定された実動ネットワークに追加する必要があります。Cisco Systems IGESM 上の管理 VLAN インターフェースの実際の管理 IP アドレスを変更する方法としては、管理モジュールの Web インターフェースを使用することをお勧めします (Cisco Systems IGESM は管理モジュールによって使用されるサブネットとは異なる IP サブネット上にありますが)。Cisco Systems IGESM 上で直接 IP アドレスを変更すると、239 ページの付録 A、『ヒント』に示すような問題が生じます。

インバンド管理のために BladeCenter を構成する方法については、63 ページの 5.3.5、『考慮事項: IGESM アップリンクを使用した IGESM の管理』を参照してください。

## パス 4 の詳細

ブレード・サーバーは Cisco Systems IGESM にアクセスするステーションであると説明しましたが、パス 4 は、経路指定された実動ネットワーク上にあるほぼすべてのデバイスが、経路指定された実動ネットワークから Cisco Systems IGESM にアクセスできることを示しています。(管理ワークステーションとして機能するデバイスは、Cisco Systems IGESM の外部で使用可能な管理 IP アドレスを Web、Telnet、SNMP などのアプリケーションに直接指定します。)ほとんどの場合 (72 ページのシナリオ 4 を除く)、ブレード・サーバーが Cisco Systems IGESM に接続するためには、まず Cisco Systems IGESM をパススルーし、経路指定された実動ネットワークに入り、その後 Cisco Systems IGESM の IP アドレスを含むサブネットに戻る経路をたどる必要があります。ブレード・サーバーが、Cisco Systems IGESM の管理 IP アドレスに使用されるものと同じ IP サブネット/VLAN 上に配置されることはあまりないので、この点に注意することが重要です。(分離の理由については、239 ページの付録 A、『ヒント』を参照してください)

また、パス 3 の場合と同様に、Cisco Systems IGESM にパス 4 を経由してアクセスするには、管理モジュールの「*advanced management*」Web ページで、「*External ports*」を「*Enabled*」に設定し、「*Management over all ports*」を「*Enabled*」に設定する必要があります。これらのいずれかが使用不可に設定されている場合、パス 4 は機能しません。

パス 3 について説明したことと同じ IP サブネットと管理 VLAN に関する規則が、パス 4 にも適用されます。

インバンド管理のために BladeCenter を構成する方法については、63 ページの 5.3.5、『考慮事項: IGESM アップリンクを使用した IGESM の管理』を参照してください。

## パス 5 の詳細

パス 5 は、Cisco Systems IGESM のフェース・プレートにある サービス・ポート (RJ45 シリアル・コンソール接続) を使用します。パス 1B の場合と同様に、このパスは Cisco Systems IGESM の管理 IP アドレスとは独立しています。また、パス 5 の使用は管理モジュールの設定値とも完全に独立しています。この接続は、シリアル・ポートを備えた PC を直接接続する単純な方法で行うこともでき (9600、N、8、および 1、フロー制御なし)、応用的な方法として、IP ネットワークに接続したターミナル・サーバーにサービスポートを接続

する方法も可能です (Cisco Systems IGESM サービス・ポート経由の管理を遠隔地から実行するという目的に使用できます)。

この接続の正しい使用法を確認するには、『Hyperterm からのコンソールポートアクセスに関する問題』(249 ページ) を参照してください。

### 特定の管理パスのために行う構成の影響

これまでに説明した特定のパスを使用するための構成を行うには、他の使用可能なパスに及ぼす影響を考慮した選択が必要です。

たとえば、インバンド・アクセス用の構成 (前述のパス 3 または 4) では、パス 1A と 2 が使用できなくなります。逆に、パス 1A またはパス 2 専用の構成では、パス 3 または 4 が使用できなくなります。

パス 1B とパス 5 は、これらの選択とはほぼ無関係で、アウト・オブ・バンド・パス (パス 1 と 2) またはインバンド・パス (パス 3 と 4) を選択する場合に必要な構成選択の影響は受けません。

56 ページの 5.3、『管理パスに関する詳細説明』では、IGESM の望ましい管理パスの選択と管理について詳しく説明しています。

最後に 1 つ注意点があります。管理モジュールと Cisco Systems IGESM をインバンド管理用に構成し、管理モジュールの内部イーサネット・インターフェースを Cisco Systems IGESM によって使用されている IP サブネットに設定した場合、管理モジュールを Cisco Systems IGESM によって実際に管理できるように見えますが、事実は異なります。Cisco Systems IGESM には特定のハードコーディングされたフィルターが備わっており、アップストリーム・ポート (g0/17 から 20) のいずれかから入るトラフィックが管理モジュール方向のポート (g0/15 から 16) から出ることと、その逆を禁止しています。(これにより、予期しないスパンニング・ツリー・ループも防止されます。) 管理モジュールの管理は、管理モジュールの外部イーサネット・インターフェース経由でのみ行うことができます。

## 5.2.4 Cisco Cluster Management Suite

Cisco Cluster Management Suite (CMS) は、IGESM 用 IOS の 12.1(14) バージョンで使用できる、BladeCenter スイッチに組み込まれた Web ベースのネットワーク管理ソフトウェアで、小規模から中規模の企業および事業所のネットワーク向けに設計されています。このソフトウェアは、繰り返しが多く時間のかかるネットワーク管理タスクを単純化し、モニターおよびトラブルシューティング用のツールを提供して、多数のスイッチの配置と構成にかかる時間を短縮できます。

Cisco CMS ソフトウェアは、BladeCenter Cisco スイッチ (IOS の 12.1(14) バージョンを実行) に組み込まれており、各種混合した Cisco スイッチを単一の GUI 画面で管理できます。Cisco スイッチ・クラスターリング・テクノロジーにより、ユーザーは任意の標準 Web ブラウザーを使用して Cisco CMS にアクセスし、これらのスイッチを物理的な隣接性に関係なく 16 台まで一度に管理できます。

詳しい情報は、次の URL にあります。

[http://www.cisco.com/en/US/products/hw/switches/ps628/products\\_data\\_sheet09186a00800913ce.html](http://www.cisco.com/en/US/products/hw/switches/ps628/products_data_sheet09186a00800913ce.html)

### Cisco CMS ソフトウェアに当てはまらないこと

Cluster Management Suite のクラスターという用語は、ときどき違うものを意味していると誤解されることがあります。このソフトウェアの場合、クラスターという用語は、スイッチを単に管理のために単一の GUI 画面にまとめて表示することを意味しています。データ・

パスの可用性を高めるためのサーバーのクラスタリングやスイッチのクラスタリングとは関係なく、単にスイッチを管理するための手段です。

サーバーのクラスタリングは、サーバー上でクラスタリング・ソフトウェアを使用して実現でき、データ・パスの高可用性は、適切なネットワーク設計と、トランク・フェイルオーバーや NIC チーミングなどの機能を使用して実現できます。

### 新規クラスターの作成

新規クラスターを作成するには、次の手順で行います。

1. 管理サブネット上のスイッチに IP アドレスを割り当てます。これは、管理モジュールを使用して行うことができます。87 ページの図 6-4 を参照してください。
2. クラスタリング・ソフトウェアを実行する他のスイッチに、このスイッチを接続します。これは直接接続でなくても構いません。CMS はデフォルトで 3 ホップ先までのデバイスを管理します。ホップ・カウントは、メニュー・バーから「Cluster」→「Hop Count」で、1 から 7 までに調整できます。
3. 「Cluster」→「Create Cluster」を選択します（図 5-27）。

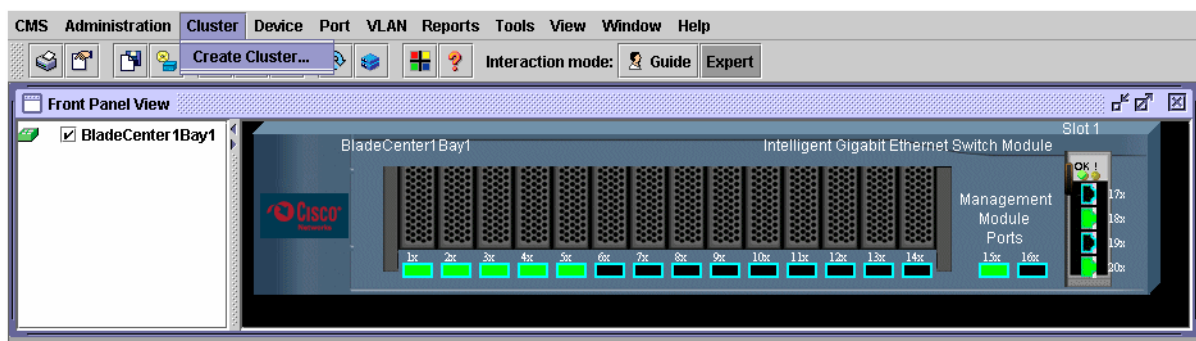


図 5-27 Cisco Cluster Management Suite のウィンドウ

4. 「Create Cluster」ウィンドウに、コマンド・スイッチ番号を入力します。この番号は、ネットワーク内に存在する他のどのコマンド・スイッチ番号とも異なっている必要があります（図 5-28）。
5. 新規クラスター名を入力します。この例では、RedpaperCluster を使用しました。
6. 「OK」をクリックします。

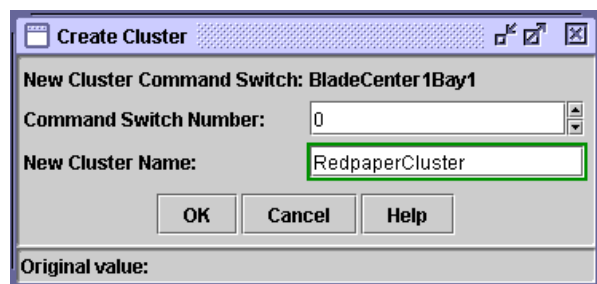


図 5-28 「Create Cluster」ウィンドウ

コマンド・スイッチが作成された後、フロント・パネル・ビュー（図 5-29）に、クラスターと、クラスター内のスイッチすべてのホスト名が表示されます。

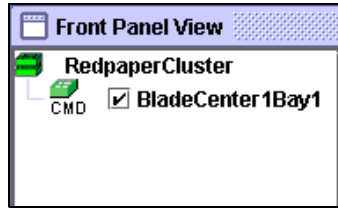


図 5-29 フロント・パネル・ビュー

### クラスターへの追加

クラスターにデバイスを追加するには、次の手順で行います。

1. メニュー・バーの「Cluster」→「Add To Cluster」を選択します（図 5-30）。

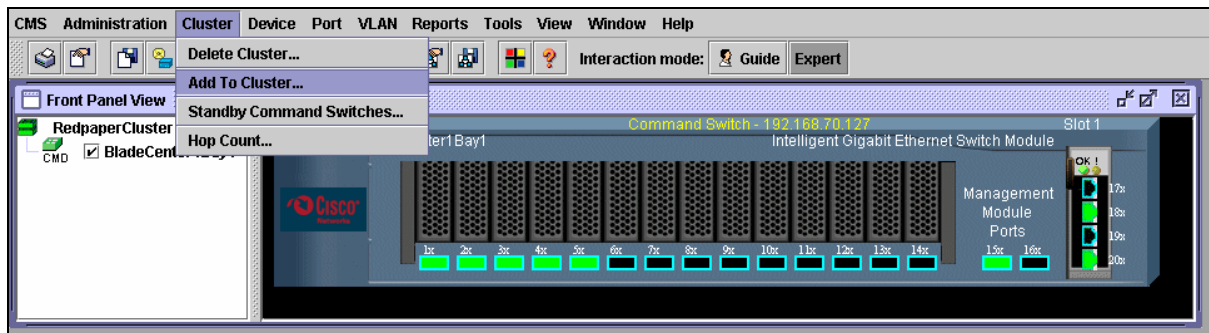


図 5-30 Cisco Cluster Management Suite のウィンドウ

2. 「Current Candidates」リスト（図 5-31）から、クラスターに追加するスイッチを選択します。リストにあるスイッチをすべて選択するには、「Select All」をクリックします。

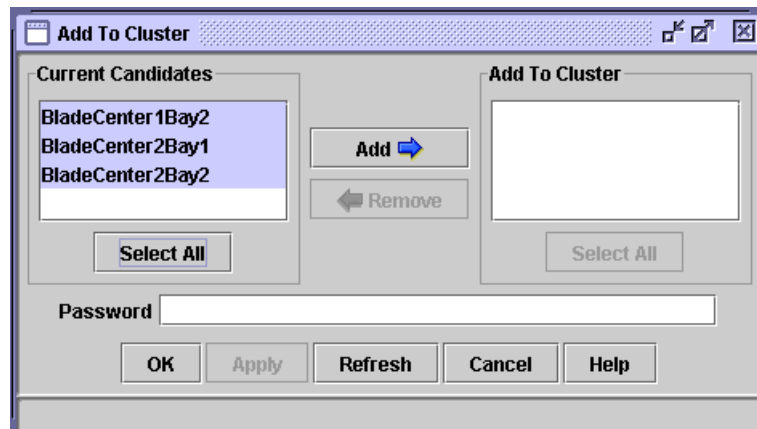


図 5-31 「Add To Cluster」ウィンドウ

3. 「Add」をクリックして、選択項目を「Add To Cluster」リストに移動します。

このリストからスイッチを除去するには、スイッチを選択して「Remove」をクリックします。リストからスイッチをすべて除去するには、「Select All」をクリックし、「Remove」をクリックします。

**注：**ポップアップ・メニューからこのウィンドウを要求した場合は、ウィンドウが開いたときに、選択したデバイスが「Add To Cluster」リストに表示されます。

4. スイッチにパスワードが構成されている場合は、「Password」フィールドにパスワードを入力します。

**注：**メンバー・スイッチに異なるパスワードが設定されている場合は、同じパスワードを使用するグループごとにこれらのスイッチを追加する必要があります。

5. 「OK」をクリックします。パスワードが必須の場合にパスワードを入力していなければ、入力するようにプロンプトが出されます。
6. メニュー・バーから、「Administration」→「Save Configuration」を選択して、変更内容を不揮発性メモリーに保管します。スイッチのリセットまたは電源オフを行う前に、変更内容が不揮発メモリーに保管されるまで約 1 分待ちます。

デバイスが正常に追加されると、そのラベルが緑色に変わります（図 5-32）。

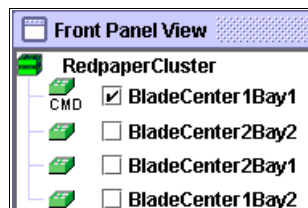


図 5-32 フロント・パネル・ビュー

7. フロント・パネル・ビューに表示するデバイスのボックスをクリックします（図 5-33）。CMS はデバイスを照会し、表示します。表示順序は再配列できます。このためには、ボックスのチェック・マークを外し、上から下の順にデバイスを表示したい順序でボックスをクリックします。

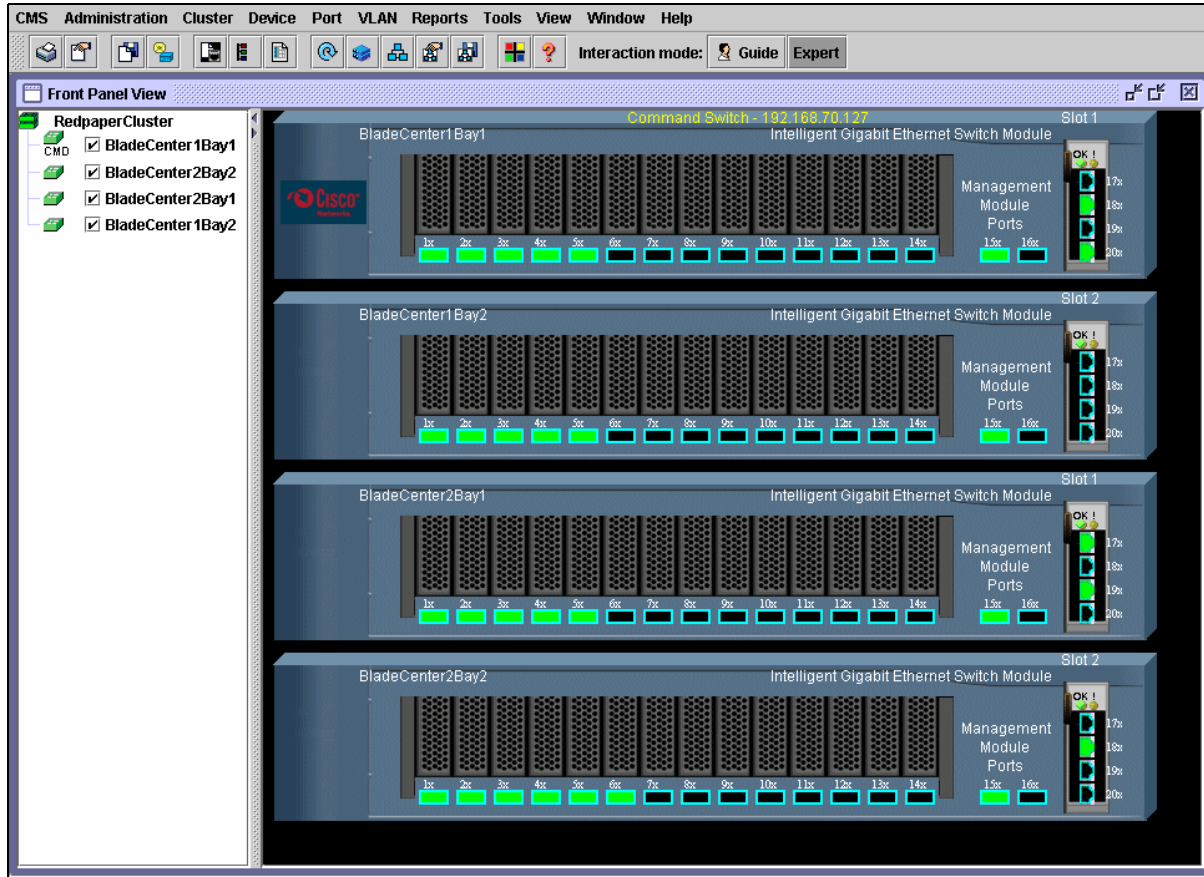


図 5-33 Cisco Cluster Management Suite のウィンドウ

8. これで、クラスター内の任意のデバイスを管理できます。このためには、スイッチのグラフィックをクリックしてからメニュー・バーのタスクをクリックするか、メニュー・バーのタスクを選択してからデバイスのホスト名を選択します（図 5-34）。この例では、VLAN を選択しました。



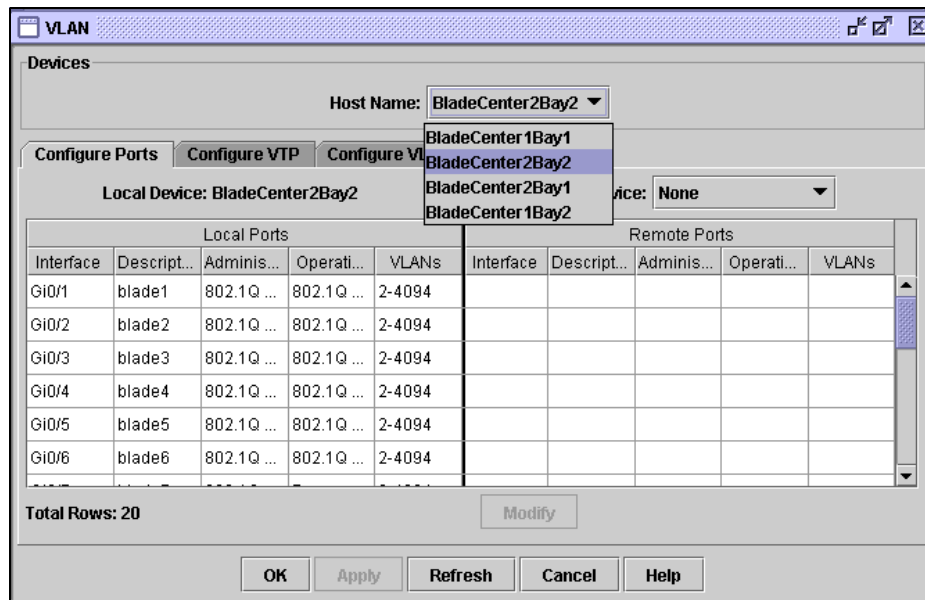


図 5-34 「VLAN Devices」 ウィンドウ

## クラスター・トポロジー・ビュー

クラスターを作成した後、グラフィカル表現でクラスターを表示できます。メニュー・バーの「Topology」アイコンをクリックして、トポロジーを表示します（図 5-35 を参照）。

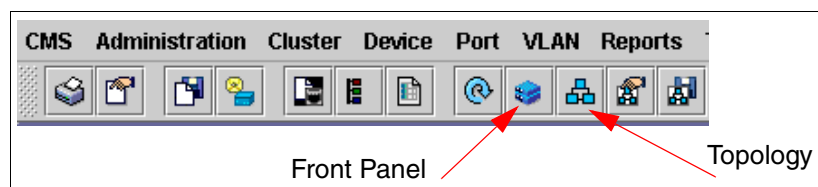


図 5-35 アイコン・バー

注：フロント・パネル・ビューに戻るには、「Front Panel」アイコンをクリックします。

「Topology」アイコンをクリックすると、図 5-36 に示すようなウィンドウが表示されます。

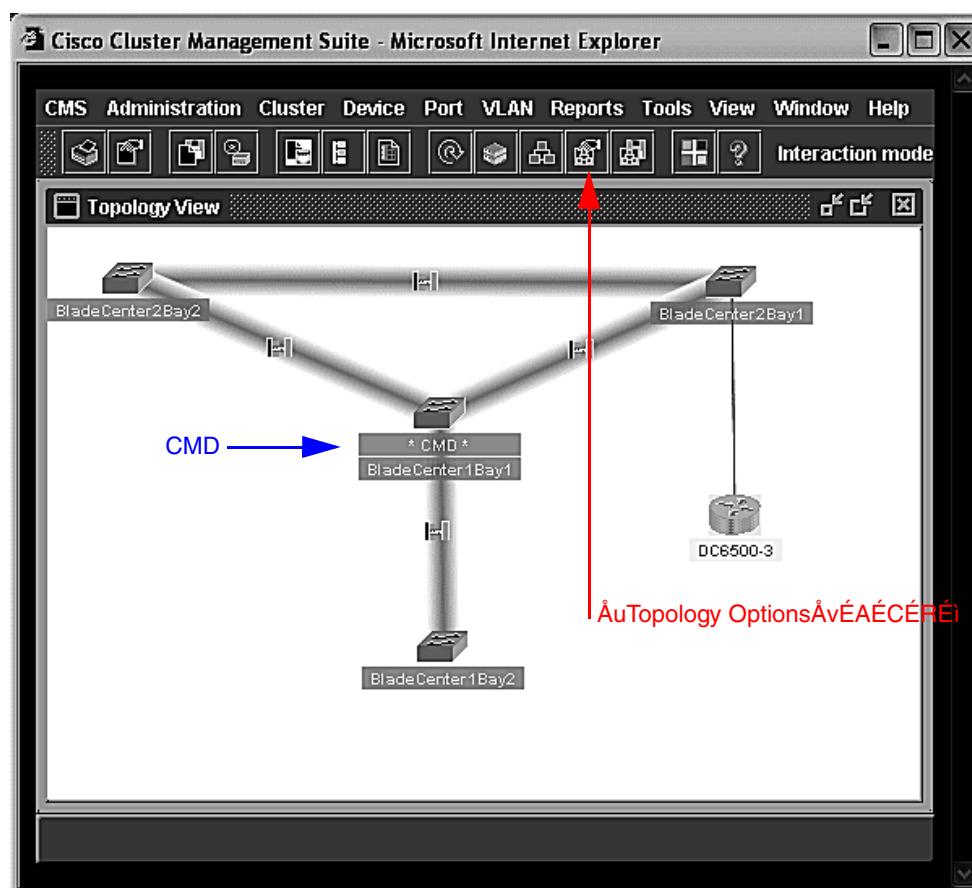


図 5-36 「Topology View」ウィンドウ

コマンド・スイッチとクラスター・メンバーからなるネットワーク・マップが表示され、コマンド・スイッチには「CMD」というラベルが付いています。このビューには、クラスター候補、隣接デバイス、隣接クラスター、およびノードとリンクの情報も表示されることがあります。図 5-36 は、次のようなセットアップの一例のスナップショットです。

- ▶ BladeCenter1Bay1 は、コマンド・スイッチ (CMD) です。BladeCenter2Bay1 および BladeCenter2Bay2 への直接外部接続があります。
- ▶ BladeCenter1Bay1 は、管理モジュールを経由して BladeCenter1Bay2 に接続されています。
- ▶ BladeCenter2Bay1 と BladeCenter2Bay2 は、管理モジュールを経由して相互に接続されています。
- ▶ 6500 スイッチは、BladeCenter2Bay1 に接続されています。6500 はクラスターのメンバーではなく、隣接デバイスです。

トポロジー・ビューの内容は、「Topology Options」ウィンドウで選択したオプションによって異なります。アイコン・バーの「Topology Options」アイコンをクリックすれば（または、「View」→「Topology Options」をクリック）、ネットワーク・トポロジーの情報を追加できます。

これにより、図 5-37 に示すようなウィンドウが開きます。この図では、選択可能なフィルター・オプションがすべて使用可能に設定されている点に注意してください。

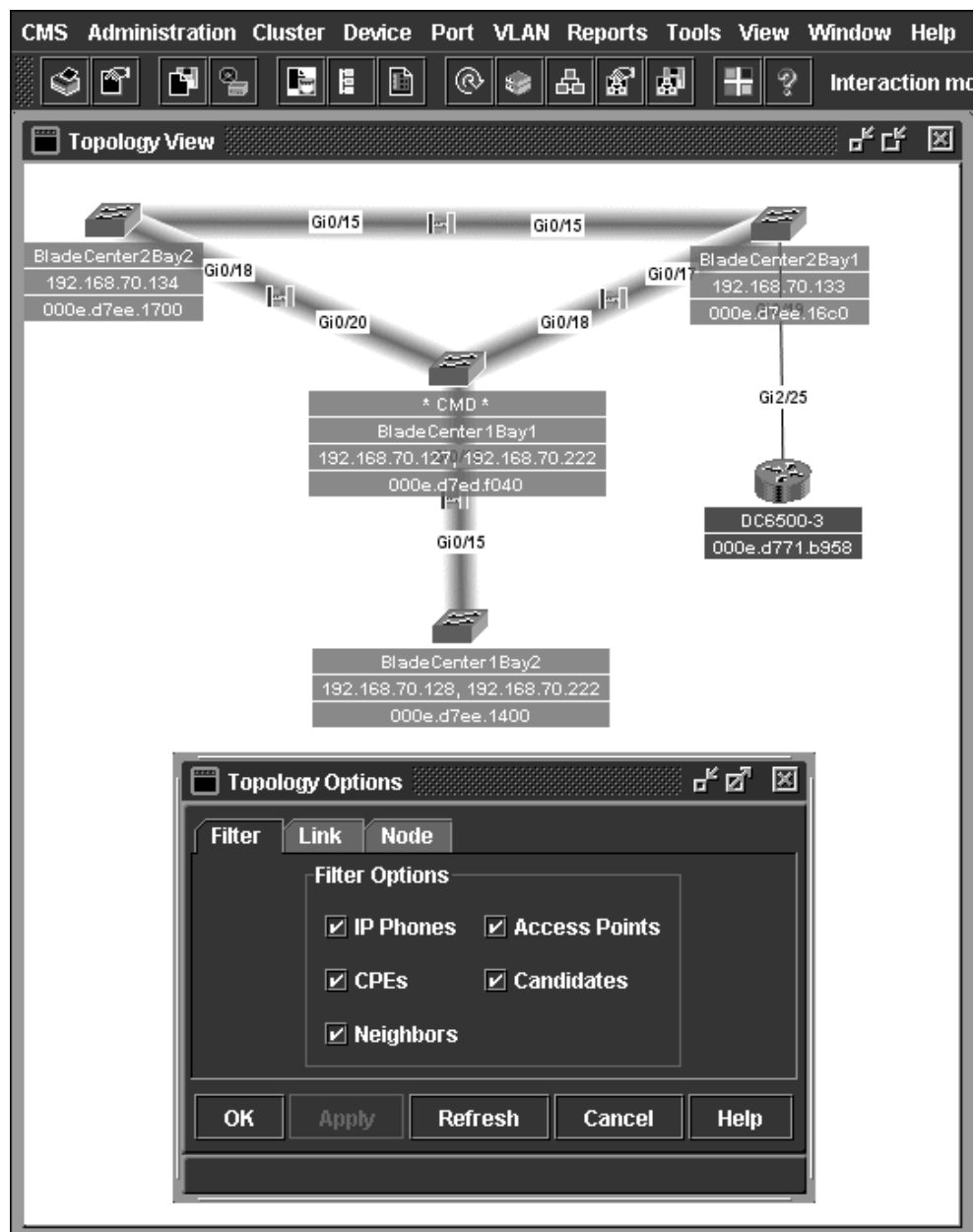


図 5-37 「Topology View」 ウィンドウ

デバイスを右クリックすると、管理用の選択項目があるポップアップ・ウィンドウが開きます（図 5-38）。

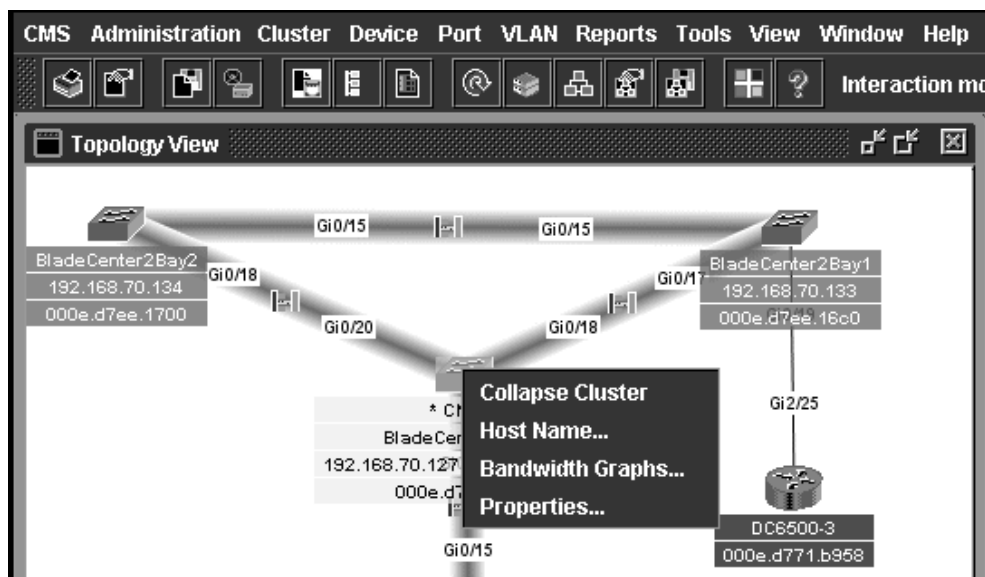


図5-38 トポロジー・ビュー

リンクを右クリックすると、管理用の選択項目があるポップアップ・ウィンドウが開きます（図 5-39）。

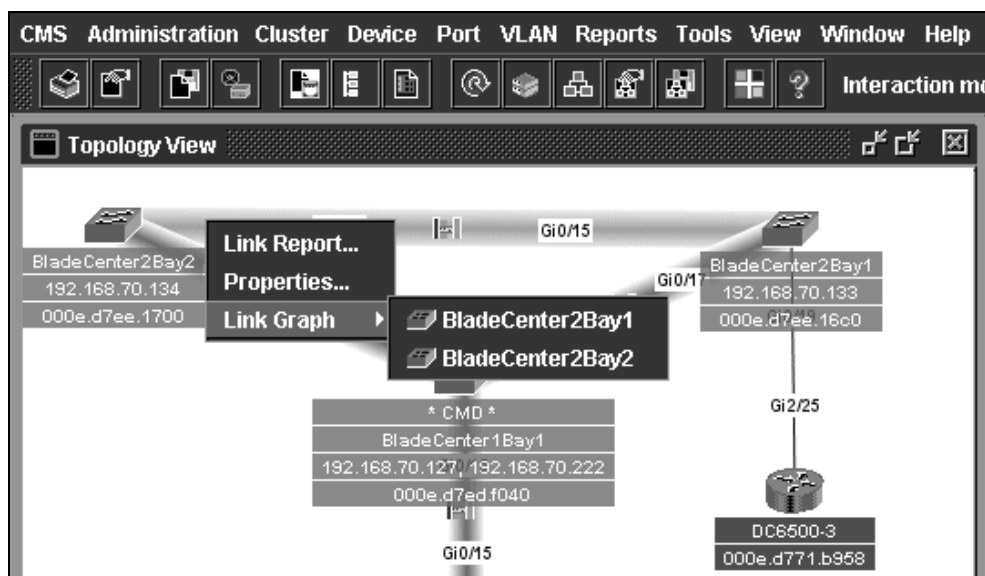


図5-39 「Topology View」ウィンドウ

## 5.2.5 CiscoWorks LAN Management Solution

CiscoWorks LAN Management Solution (LMS) は、ネットワークを管理するネットワーク・オペレーターを支援する、基本から拡張までのデバイス管理アプリケーションの基礎を提供します。このソリューションには CiscoView、CiscoWorks Resource Manager Essentials、および CiscoWorks Campus Manager が含まれ、IGESM を対象にこれらのアプリケーションすべての使用がサポートされています。

本書では、CiscoWorks LAN Management Solution のコンポーネントである CiscoView 5.5 について説明します。このアプリケーションの幅広いテストは行っていないが、ネットワーク内の IGESM のモニターと管理にこのアプリケーションを使用できることを例示します。

CiscoWorks LAN Management Solution (LMS) について詳しくは、次の URL にアクセスしてください。

<http://www.cisco.com/en/US/products/sw/cscowork/ps2425/index.html>

## 5.2.6 CiscoView

CiscoView は、Web ベースのデバイス管理アプリケーションで、幅広い Cisco インターネットワーキング製品を対象に、動的な状況情報、モニター情報、および構成情報を提供します。CiscoView はデバイス・シャーシの物理ビューを表示し、モジュールとポートの状況の一覧を色分けして示します。モニター機能は、パフォーマンスなどの統計を表示します。必要なセキュリティー特権が付与されていれば、構成機能を使用してデバイスに広範囲の変更を加えることができます。

この Redpaper に記載したトポロジーと構成を開発およびテストするには、CiscoView バージョン 5.5 を使用し、スイッチング・デバイスへのアクセスと管理のために Cisco Systems Intelligent Gigabit Ethernet Switch Module 用の最新デバイス・パッケージをロードしました。

デバイス・パッケージは、次の Web サイトからダウンロードできます。

<http://www.cisco.com/cgi-bin/tablebuild.pl/cview50>

ファイル名（本書の執筆時点での）は、cigesm.cv50.v1-1.zip です。

**注：**この情報にアクセスするには、Cisco Connection Online (CCO) のユーザー ID とパスワードが必要です。CCO ID は、次のページにアクセスして登録を行うことによって取得できます。

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

**注：**CiscoWorks Resource Manager Essentials と CiscoWorks Campus Manager も Cisco Systems Intelligent Gigabit Ethernet Switch Module に対してサポートされていますが、本書の制作時点ではテストされていませんでした。IGESM のサポートに必要な IDU をダウンロードするためのリンクは、次の URL にあります。

<http://www.cisco.com/kobayashi/sw-center/cw2000/lan-planner.shtml>

- ▶ それぞれのモジュールごとのアプリケーション・レベル更新に含まれる、バージョン 10 以上の IDU が IGESM をサポートします。
- ▶ CiscoWorks をサポートする IGESM の最低コードは 12.1(14)AY1 です。

## CiscoWorks Resource Manager Essentials

Resource Manager Essentials は、Cisco スイッチ、アクセス・サーバー、およびルーター用のネットワーク管理ソリューションを提供する、Web ベース・アプリケーションのスイートです。Resource Manager Essentials のブラウザー・インターフェースを使用すれば、ネットワークのアップタイムに不可欠な情報に容易にアクセスでき、時間のかかる管理タスクが単純化されます。

Resource Manager Essentials の内容は次のとおりです。

- ▶ Inventory Manager
- ▶ Change Audit
- ▶ Device Configuration Manager

- ▶ Software Image Manager
- ▶ Availability Manager
- ▶ Syslog Analyzer
- ▶ Cisco Management Connection

## CiscoWorks Campus Manager

運用時の使用に対応するように設計された Campus Manager は、複雑な物理インフラストラクチャーや論理インフラストラクチャーを構成、管理、および把握するためのレイヤー 2 ツールを備えています。

Campus Manager を使用して、管理者はネットワークの関係を容易に変更、モニター、および制御できるので、ビジネスに不可欠な拡張ネットワーク・サービスをユーザーと顧客に提供する作業が効率化されます。

## 5.2.7 IBM Director および Remote Deployment Manager

IBM は、BladeCenter の日常的な操作を効率的に管理するために役立つ、次の 2 つのソフトウェア製品を提供しています。

- ▶ IBM Director。これは、IBM の Intel® ベース・サーバーすべてのお客様を対象に無料で提供されています。
- ▶ Remote Deployment Manager (RDM)。これは有料でお客様に提供されます。RDM は IBM Director に統合されており、この製品は RDM の前提条件です。

IBM ソフトウェア管理ツールは、BladeCenter の配置と管理を簡単、迅速に行えるように設計されていますが、これらのツールを使用しないこともできます。この場合は、管理モジュール Web インターフェースを使用します（標準の Web ブラウザーから使用可能）。その後、標準のインストール方式（たとえば、CD からブートしてセットアップを実行するか、無人ネットワーク・インストールを行う）を使用して、ブレード・サーバーにオペレーティング・システムをデプロイできます。

BladeCenter のストラテジーを完全に実装するために、ブレードの管理とデプロイには IBM Director と Remote Deployment Manager (RDM) を両方とも使用することをお勧めします。

IBM Director の機能の中でも、ハードウェア管理は特に優れています。IBM Director は、Service Location Protocol (SLP) と呼ばれる特殊なプロトコルを使用して、BladeCenter 管理モジュールと直接対話します。これにより、BladeCenter シャーシおよび取り付け済みのブレードを IBM Director データベースに登録することが可能です。BladeCenter を IBM Director に登録した後、シャーシとブレードを Director コンソールから管理できます。したがって、管理モジュール Web インターフェースから使用できるアクションを Director コンソールから実行できます（ブレードのリモート・コンソール・リダイレクトなど、いくつかの機能を除く）。たとえば、ブレードの電源オン/オフ、ハードウェア構成などのアクションを実行できます。また、シャーシから発生するイベントが通知されます（ハードウェア・ヘルス、アラート、ブレードの挿入など）。

これとは対照的に、RDM は新規システム上で最初からオペレーティング・システムをデプロイする役割を担います。RDM は Preboot Execution Environment (PXE) プロトコルを使用します。これはネットワーク・アダプターの標準機能で、マシンの BIOS によるサポートも必要とします。PXE プロトコルを使用して、インストール対象のサーバーはネットワークからブートし、RDM サーバーがオペレーティング・システム OS（Microsoft オペレーティング・システムの場合は DOS、Linux® の場合は Linux）のインストールを開始するための基本環境を提供します。前提条件の 1 つは動的ホスト構成プロトコル (DHCP) サーバーです。これは、RDM サーバーとして使用されているものと同じサーバー上になくても構いません。

IBM Director を使用すれば、Tivoli、HP OpenView、Microsoft SMS、CA Unicenter、BMC、および NetIQ との上位統合によって、既存のエンタープライズ管理構造を最大限に活用できます。

詳しくは、次の Web サイトをご覧ください。

<http://www.redbooks.ibm.com/redpapers/pdfs/redp3776.pdf>

[http://www.ibm.com/servers/eserver/xseries/systems\\_management/xseries\\_sm.html](http://www.ibm.com/servers/eserver/xseries/systems_management/xseries_sm.html)

## 5.3 管理パスに関する詳細説明

ここでは、Cisco Systems IGESM と管理モジュールの相互作用、および IGESM への管理接続の安定性を確保するために必要な規則について詳しく説明します。

### 5.3.1 管理に関する詳細説明の概要

この詳細説明の目的は、推奨されるパスを明らかにすることです。特に、IBM BladeCenter 内の Cisco Systems IGESM に伝送され、これを通過するさまざまなタイプのトラフィックに対する管理パスを示します。7 とおりの考えられるシナリオの例を示し、いくつかの設計を推奨する理由、およびいくつかを推奨しない理由を詳しく説明します。

注意点として、ここでの説明は、執筆時点で有効であったことです。コードやハードウェアの将来の改訂によって、ここで定義した操作が変更されることがあり、この節の一部または全体が無効になる可能性があります。

参考のため、この節の内容は、IOS 改訂 12.1(14)AY4 を実行する IGESM 型式番号 13N2286 (これは管理モジュールによって報告される番号ですが、13N2281 とも呼ばれます) を基準として検証されました。使用された管理モジュールは、日付 7-22-04、改訂 16 のファームウェア・リリース BRET67D を実行するモデル 02R1606 です。

### 5.3.2 この詳細説明を執筆した理由

BladeCenter の設計により、IGESM を管理するために使用できるパスは 2 とおりあります (管理モジュールのアップリンク・ポート経由、または IGESM のアップリンク・ポート経由)。IGESM と管理モジュールの間には常に内部リンクが存在するため、設計によっては予期しない結果が生じることがあり、IGESM の管理 VLAN インターフェースに対して無秩序な接続が行われる可能性があります。

さらに具体的に説明すると、IGESM は常に自身と管理モジュールの間でパスを提供しようとし、管理モジュールは常に IGESM の管理 IP アドレス (およびその内部 IP サブネット上にある、その他いくつかの IP アドレス) のプロキシとして機能しようとするのが原因で、設計によっては問題が生じます。最終的な結果として、管理モジュールは、その内部サブネット上で管理する IP アドレスに対する、アップリンク・ポート上での ARP 要求に応答します (これには、管理モジュールの eth1 インターフェース、および BladeCenter 内の各スイッチ・ベイの IP アドレスが含まれます)。

管理モジュールのアップリンクと IGESM のアップリンクが同じ VLAN 上の同じ IP サブネットに配置されていて、IGESM に対する「External management over all ports」が「Enabled」に設定されている場合 (管理モジュールの機能設定)、管理モジュールと IGESM の両方が IGESM の IP アドレスに対する ARP 要求に応答しようとし、この条件下では、管理モジュールの ARP 応答がアップストリーム・デバイスに受け入れられると、IGESM 管理トラフィックは管理モジュールを通過しようとし、管理モジュールは IGESM に実際にトラフィックを渡す場合も渡さない場合もあります。また、ARP はブロードキャスト・ベースなので、IGESM は管理モジュールの応答を認識し、自身の IP アドレスを所有してい

ることを公表する Gratuitous ARP を発信します。管理モジュールはこれを認識して同じように応答を返し、IGESM の IP アドレスを所有するアップストリーム・ネットワーク上で ARP の競合が起こります。

以降この節では主に、こうした問題を回避して、管理接続の安定性が確保されるように IGESM をインフラストラクチャーに統合する方法を説明します。

**注：**これらの問題はすべて、BladeCenter からのアップストリーム外部ネットワーク上で起こります。

IP サブネットのプロキシとなる管理モジュールは、別の（内部の）影響も及ぼします。ブレード・サーバーが IGESM の管理インターフェースによって使用されている IP サブネットと VLAN に配置されている場合、ブレード・サーバーは IP インターフェースの起動にほぼ確実に失敗します。これは、ほとんどの OS が IP インターフェースの起動時にまず、固有の IP アドレスを探すための ARP 要求を発信するからです（すでにそのアドレスが他に使用されていないことを確認するため）。ブレード・サーバーが、IGESM の管理 VLAN に使用されているものと同じ VLAN/IP サブネット上に存在する場合、管理モジュールはこの ARP 要求に応答を返し、ブレード・サーバーの OS は TCP スタックをシャットダウンします。これは、重複する IP アドレスがネットワーク上にすでに存在すると見なされるからです。

この内部の問題に関してさらに重大と考えられる点は、ブレード・サーバーがすでに稼働中の場合に、管理モジュールと IGESM が同じ VLAN に配置されると、通常ブレード・サーバーはリブートされるまで正常に動作を続けることです。ブレード・サーバーは再起動すると、その IP アドレスを所有するものが存在するかどうかの確認を再試行し、管理モジュールがブレード・サーバーからの初期 ARP に応答すると確認は失敗します。（ブレード・サーバーは、自身の IP アドレスに対するこの ARP 応答を認識し、すでにその IP アドレスが他に所有されていると見なします）

ブレード・サーバーを IGESM 管理インターフェースと同じ VLAN に配置するために起こる最後の問題は、特定のケースで（管理モジュールが同じ IP サブネットも使用している場合）、一部のユーザー・データ・トラフィックが IGESM のアップリンク・ポートを正しく経由せずに、管理モジュールを通過しようと実際に試みることです（これは失敗します）。

**ヒント：**こうした内部問題が起こらないようにする最も良い方法は、IGESM 上で管理インターフェース VLAN として定義されている VLAN からブレード・サーバーを分離することです。

ここで説明するシナリオのために、次の 3 種類のトラフィックを定義します。

▶ データ・トラフィック

これは、実動ネットワークから IGESM のアップリンク・ポートを経由して伝送され、BladeCenter 内に取り付けられているブレード・サーバーを出入りするユーザー・データです。

▶ 管理モジュール・トラフィック

これは、管理モジュールとの間でやり取りされる管理トラフィックで、管理モジュールへのアクセスのために管理モジュールのアップリンク・ポートを経由して伝送されます。

▶ IGESM トラフィック

これは、IGESM の管理のために IGESM との間でやり取りされる管理トラフィックで、管理モジュールのアップリンク接続を経由するか、IGESM のアップリンク接続を経由して伝送されます。

IGESM はポート g0/15 と 16 のシャットダウンを許可しませんが（常に稼働するようにハードコーディング済み）、接続の相手側（MM ETH1 インターフェース）を使用不可に設定で



きます。これにより、管理モジュールから BladeCenter 内のデバイスへの内部イーサネット接続がすべて使用不可になります。これは、ポートをシャットダウンするのではなく、インバンド内部要求への応答を停止するからです。このことは、他の Ethernet Switch Module や SAN モジュールすべて、さらに管理モジュールからブレード・サーバーへの Serial over LAN 接続（構成されている場合）にも当てはまります。このようにイーサネット・アクセスが完全に失われるため、ETH1 インターフェースを使用不可にする方法は、たとえば BladeCenter 内の他のデバイスに対する内部イーサネット管理アクセス、または Serial over LAN が必要ない場合など、非常に限定された状況でしか役に立たず、したがって通常はお勧めしません。

### 5.3.3 一般的な管理パスの設計上の考慮事項

インバンド管理とアウト・オブ・バンド管理の概念については、すでに説明しました。次に、これらのパスに関連した Cisco Systems IGESM と従来型のスタンドアロン Cisco スイッチの微妙な違いについて詳しく説明します。

従来型の Cisco スイッチは、管理目的の接続を 2 とおりの方法で行います。

- ▶ コンソール・ポート経由（アウト・オブ・バンド）
- ▶ ネットワーク接続経由（インバンド）

BladeCenter 内の Cisco Systems IGESM には、3 とおりの接続方法があります。

- ▶ コンソール・ポート経由（アウト・オブ・バンド）。
- ▶ 管理モジュールを通る内部ネットワーク接続経由。これは、トラフィックの伝送にネットワーク接続を使用しますが、データ・パス・ネットワーク接続は使用しません。これは IGESM のデフォルトのネットワーク・ベース管理パスで、図 5-40 に示されているパス 1 と 2 です。
- ▶ 外部アップリンク・ネットワーク接続経由（インバンド）。これは、図 5-40 に示されているパス 3 と 4 です。

これは小さな違いに見えるかもしれませんが、実際にはとても重要です。これらのパスの違いと、どちらか 1 つを使用するように構成する（*両方を同時に使用するように構成することはできません*）方法を理解することは、IGESM を実稼働環境に正しく配置するために不可欠です。

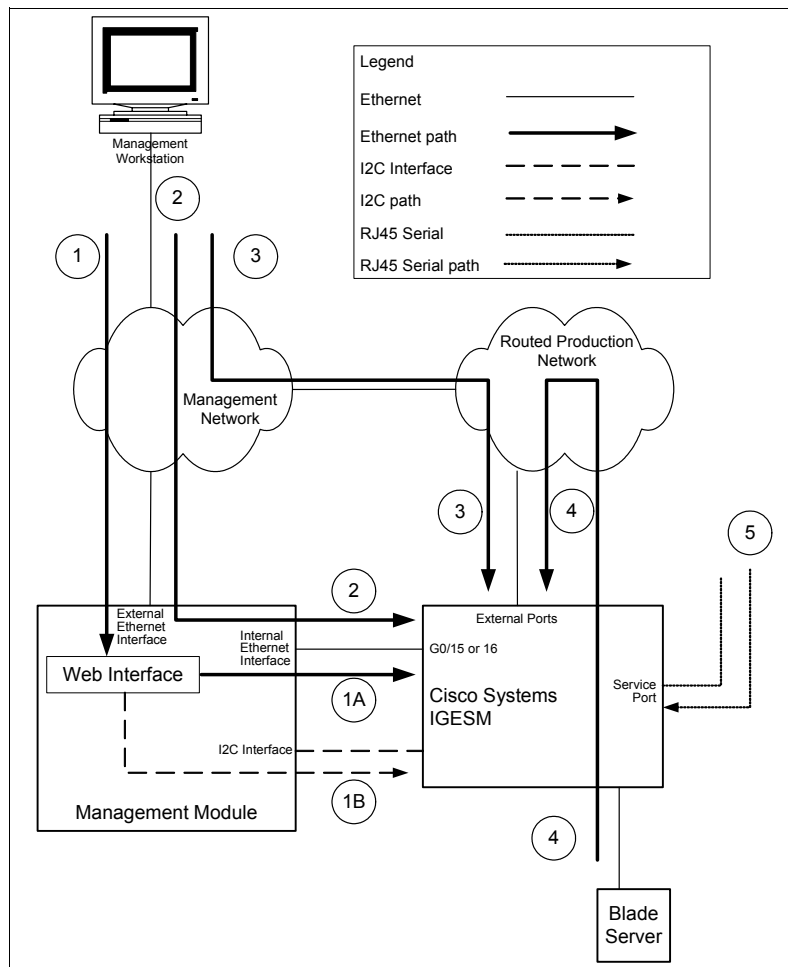


図 5-40 管理パスのフロー

前述のとおり、これら 2 つのネットワーク・ベース管理パスの重要な性質は、使用するパスの選択が二者択一であることです。管理モジュール・アップリンク（シナリオ 1、2、および場合によっては 7 に示すもの）、または IGESM 自身のアップリンク（シナリオ 3 および 4 に示すもの）を経由して IGESM を管理するように、明示的に構成する必要があります。両方のパスを同時に使用するように IGESM 管理を構成すると、通常は IGESM に接続しようとする際に接続が断続的になる問題が生じます。シナリオ 5 および 6 は、両方のパスを同時に使用可能に設定して構成した場合の不適切な構成例を示しています。

**注：**これらのシナリオの説明は、66 ページから始まります。

ここで最初に説明する、IGESM を管理するためのおそらく最も単純なアプローチは、管理モジュールのアップリンク・ポートを使用して IGESM を管理することです（59 ページの図 5-40 のパス 1 と 2）。この接続は、この節のシナリオ 1、2、および 7 に例示されており、またこの後でさらに詳しく説明します。配置が容易なので、IGESM 自身のアップリンクによって IGESM を管理するよりも、管理モジュールのアップリンクを使用して IGESM を管理する方法が望ましく、シナリオ 1 と 2 は両方ともお客様の要件に応じて同等に推奨されます。

すでに説明したとおり、2 番目のアプローチは、IGESM を自身の外部アップリンク接続 G0/17 から 20 経由で管理することです（59 ページの図 5-40 のパス 3 と 4）。この接続はシナリオ 3 から 6 に例示されており、この後で詳しく説明します。

重要な注意点として、シナリオ 3 から 6 はすべて、IGESM 自体のアップリンク・ポートを経由して IGESM を管理する例を示しており、このパスを使用する場合にはシナリオ 3 と 4 のみが推奨されます。IGESM アップリンク管理を使用する場合にはシナリオ 3 の選択が推奨されますが、シナリオ 4 も実行可能なオプションと考えられます。

シナリオ 5 と 6 は、IGESM アップリンクを使用して IGESM を管理する際に設計によって起こりうる問題を示すことだけを目的に記載したもので、したがって推奨されるソリューションではありません。

要約すると、この選択の過程では、望ましい管理パスを選択し、正しく動作するように適切に構成する必要があります。すでに説明したとおり、IGESM のアップリンクを使用して IGESM を管理する（シナリオ 3 と 4）よりも、管理モジュールのアップリンクを使用して IGESM を管理する（シナリオ 1 と 2）方法が推奨されます。ただし、シナリオ 3 と 4 は、真のインバンド管理を必要とするユーザーには確実に役立つオプションです。

管理モジュールのアップリンクを経由した管理の構成に関する規則は、60 ページの 5.3.4、『考慮事項：IGESM の管理に管理モジュールのアップリンクを使用する場合』に示されています。

IGESM のアップリンクを経由した管理の構成に関する規則は、その後の 63 ページの 5.3.5、『考慮事項：IGESM アップリンクを使用した IGESM の管理』に示されています。

## VLAN のベスト・プラクティス

ここで説明している他のさまざまな推奨事項には、VLAN の使用法と分離に関するいくつかのベスト・プラクティスが密接に関連しています。

機能するであろう VLAN の使用法はいろいろと考えられますが（たとえば、すべてを単一の VLAN ネットワークに配置するなど）、これらは良い設計でしょうか。堅固なセキュリティ、予測可能なトラフィック・フロー、高可用性は考慮しているでしょうか。この点を念頭に置き、堅固でセキュアなネットワークを設計する際には、いくつかの事項に常に注意する必要があります（IGESM に関係するものに限らず、すべての設計で）。

- ▶ 通常、管理トラフィックまたはデータ・トラフィックの伝送には VLAN 1 を使用しないようにします。
- ▶ 管理トラフィックとデータ・トラフィックを同じ VLAN 内で伝送しないようにします。
- ▶ 管理用の VLAN の使用は、その VLAN を使用する必要があるポートのみに限定します。不要なリンクから、その VLAN をプルーニングなどの方法でブロックします。
- ▶ トランクの相手側で必要な VLAN のみをトランク上で伝送し、その他すべての VLAN をプルーニングまたはブロックします。

これらの推奨事項の根拠について詳しくは、次の URL にある「Virtual LAN Security Best Practices」資料を参照してください。

[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_white\\_paper09186a008013159f.shtml](http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml)

### 5.3.4 考慮事項：IGESM の管理に管理モジュールのアップリンクを使用する場合

シナリオ 1、2、および 7（7 は後述する特殊なケースです）は、BladeCenter 内の IGESM への管理パスを提供するために管理モジュールのアップリンクを使用する場合の情報を示しています。

**注：**これらのシナリオの説明は、66 ページから始まります。

シナリオ 1 と 2 でこのパスを使用するには、次の 4 つの基本的な考慮事項に注意する必要があります。

1. IGESM アップリンク経由での管理を使用不可に設定します。

管理モジュールの「External management over all ports」を必ず「Disabled」に設定します。これにより、管理インターフェース VLAN の IP アドレスに対する、ポート 15 および 16 以外からの ARP 要求に IGESM が応答しなくなります。代わりに、管理モジュールは IGESM への MAC アドレスを尋ねる要求に対してプロキシとして機能し、すべての管理トラフィックは管理モジュールを通してポート G0/15（また、冗長管理モジュールがアクティブの場合は G0/16）経由で IGESM に流れます。

2. ブレード・サーバー側のすべてのポートから IGESM 管理 VLAN を分離します。

IGESM と管理モジュールの間で使用される VLAN が、BladeCenter シャーシ内のいずれかのブレード・サーバーによって使用されないようにします。これが必要である理由は、管理モジュールが内部 IGESM 管理 VLAN 上のデバイスのプロキシとして機能できるため、この管理 VLAN に配置されているいずれかのデバイス（ブレード・サーバーなど）に対して管理モジュールがプロキシとなる可能性があるからです。最終的に、IGESM 管理インターフェース VLAN と同じ VLAN と IP サブネット上に配置されているブレード・サーバーが、重複 IP アドレスを認識することになります（管理モジュールが、そのサブネット上のデバイスへのパスであると公表しようとするため）。

3. IGESM 管理 VLAN を IGESM アップストリーム接続からブロックします。

管理 VLAN インターフェース上で IGESM によって使用される VLAN が、IGESM のアップリンクによって伝送されないようにします。管理モジュール経由で IGESM を管理する際にこのパスをブロックしなければ、IGESM への接続が断続的になる可能性があります。シナリオ 1 の場合（物理的に分離された管理ネットワークとデータ・ネットワーク）、このことは問題にならないと考えられます。シナリオ 2 の場合は、IGESM アップリンクによって伝送されないように IGESM 管理インターフェース VLAN を除去することが不可欠です。

4. IP サブネットの選択が正しいことを確認します。

IGESM によって使用される IP サブネットが、管理モジュール上で自身の IP アドレスに使用されるサブネットと同じであることを確認してください。これは、管理モジュールのアップリンクを使用して IGESM を管理するシナリオの場合には絶対に必要です。

これら 4 つの規則を守ることによって、IGESM がお客様の管理ネットワークに直接接続されている場合と同じように、管理モジュールのアップリンク・ポート経由で IGESM の管理とアクセスを正しく行うことができます。つまり、まず管理モジュールに接続してからその後で IGESM に接続する必要はなく、実際に Telnet またはブラウザのセッションに IGESM の IP アドレスを直接指定し、他の Cisco スイッチの場合と同様に IGESM に直接接続（管理モジュールを通るパスを経由して）できます。

管理モジュールを使用して IGESM への管理パスを提供する場合に、混乱しやすい点の 1 つは、IGESM 管理トラフィックのフローが管理モジュールを経由して IGESM に到達するために、管理モジュールのポートに接続されたアップストリーム・スイッチのポート上で定義される VLAN が、IGESM 上のインターフェース VLAN と同じでなくても構わないという点です。（図 5-41 を参照してください）

この理由は、管理 VLAN インターフェースが IGESM 上で定義されていても、この VLAN は常に管理モジュール側のポート（G0/15 と g0/16）を経由して、トランク上のネイティブ VLAN として伝送されるからです。これは、g0/15 と g0/16 が 802.1Q トランクとしてハードコーディングされており、管理 VLAN インターフェースが常にネイティブ VLAN に割り当てられるためです。したがって、この VLAN はタグなしであり、管理モジュールにそのように認識されます。

IGESM 方向の管理モジュールのインターフェース（ETH1）には、これは単純なアクセス・リンクと見なされ、IGESM 上でその VLAN が何と呼ばれていても関係ありません。これ

は、このインターフェースが単にネイティブ VLAN 上で伝送されるタグなしパケットを探し、そのパケットを受信するからです。その後、これらのパケットはアップストリーム・スイッチに面する ETH0 インターフェースから発信されます。

異なる VLAN を使用した場合でも接続は機能しますが、これは非常に紛らわしいので、通常は IGESM (interface vlan X) と、管理モジュールに接続したスイッチ上のアップストリーム・ポート (switchport access vlan X) の両方で、同じ VLAN を定義することをお勧めします。

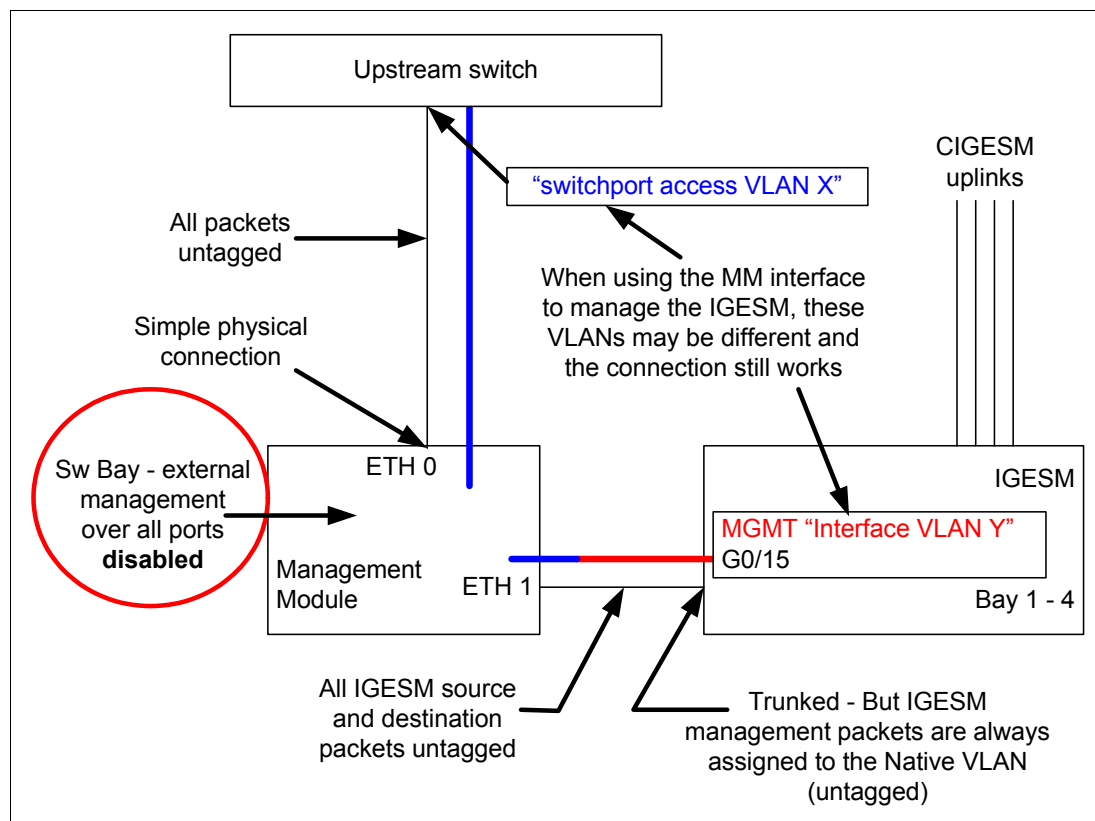


図5-41 管理モジュール経由の IGESM への管理パスに関する考慮事項

この規則には1つ例外があります。IGESM の初期評価期間中に、簡単な単一の VLAN ネットワークをテスト目的でセットアップすることがよくあります。この節のシナリオ7では、このアプローチの可能性と影響について説明します。

話題は少し異なりますが、次のような疑問点が生じるかもしれません。タグなしデータを管理モジュールに伝送することのみが目的ならば、ポート g0/15 と g0/16 はどうしてトランクとしてハードコーディングされているのか？ どうして、混乱が生じないように単純なアクセス・リンクとしてハードコーディングされていないのか？

1つの理由は、BladeCenter が Serial over LAN (SoL) という機能をサポートしていることです。この機能を使用して、ユーザーは管理モジュールに Telnet でログインしてから、特殊な VLAN 上で IGESM を経由して個々のブレード・サーバーに接続できます。SoL VLAN は IGESM の管理 VLAN と別個であることが必要なので (フローを分離するため)、SoL を使用する場合は、2つの VLAN の伝送を管理モジュールと IGESM の間のリンクによって行う必要があります。複数の VLAN を単一の物理リンク上で伝送しながら、フローの分離を保つためには、トランク接続 (この場合は 802.1Q) を使用するしか方法がありません。SoL を使用する場合、IGESM 管理トラフィックは常にネイティブ VLAN (タグなし) 上にあり、一方で SoL VLAN はそれとは別の VLAN (タグ付き) になります。

### 5.3.5 考慮事項：IGESM アップリンクを使用した IGESM の管理

この節のシナリオ 3 から 6 では、IGESM のアップリンクを使用して BladeCenter 内の IGESM への管理パスを提供する方法を説明します。IGESM の管理に IGESM アップリンクを使用する実稼働環境では、シナリオ 3 と 4 のみが推奨されることに注意してください。シナリオ 5 と 6 は、IGESM の管理に IGESM アップリンク・ポートを使用する場合に生じる可能性がある問題を示すためだけに記載してあります。

IGESM アップリンク・ポートを使用して IGESM を管理するには、次の 5 つの基本的な考慮事項に注意する必要があります。

1. IGESM アップリンク経由での管理を使用可能に設定します。

管理モジュールの「External management over all ports」を必ず「Enabled」に設定してください。これにより IGESM は、管理インターフェース VLAN の IP アドレスに対する、アップリンク・ポートからの ARP 要求に応答できます。

2. ブレード・サーバー方向のすべてのポートから IGESM 管理 VLAN を分離します。

IGESM が管理のために使用する VLAN が、BladeCenter シャーシ内のいずれかのブレード・サーバーによって使用されていないことを確認してください。これは、ブレード・サーバーに対する管理モジュールのプロキシの問題を避けるために必要です。IGESM 自身のアップリンク（管理モジュールのアップリンクでなく）を経由して IGESM を管理する場合には、このことはあまり問題になりませんが、それでもこの規則を守ることをお勧めします。（この規則の例外は、シナリオ 4 で説明します）

3. IGESM 管理 VLAN の伝送は IGESM アップリンク上で行います。

IGESM が管理 VLAN として使用する VLAN が、IGESM からアップストリーム・スイッチ（複数の場合もある）へのアップリンクのうち少なくとも 1 つによって伝送されるようにします。これは、EtherChannel バンドルによって伝送される場合や、802.1Q トランクの一部として伝送される場合、または単純なアクセス・タイプの接続として伝送される場合があります。

4. IGESM 管理 VLAN が管理モジュールのアップストリーム VLAN と同じでないようにします。

IGESM によって管理 VLAN インターフェース上で使用される VLAN が、管理モジュール側で管理モジュールへのアップストリーム接続に使用される VLAN と同じにならないようにしてください。ここでは IGESM 自身のアップリンクを使用して IGESM を管理しようとしているので、IGESM 管理インターフェースの VLAN は、管理モジュールのサポートに使用される VLAN と分離する必要があります。

5. IP サブネットの選択が正しいことを確認します。

IGESM によって使用される IP サブネットが、管理モジュール上で自身の IP アドレスに対して定義されたサブネットと異なることを確認してください。ステップ 3 の場合と同様に、IGESM 自身のアップリンクを使用して IGESM を管理しようとしているので、管理モジュールへの IGESM 管理パスを分離することが重要です。管理モジュールと IGESM の間で IP サブネットが異なっていれば、この分離は完全になります。

これら 5 つの規則を守ることによって、IGESM 自身のアップリンク（g0/17 から 20）を経由して IGESM の管理とアクセスを正しく行うことができます。

図 5-42 は、IGESM を管理するために IGESM アップリンクを使用する場合の重要な属性を示しています。この場合、IGESM 管理 VLAN に割り当てられた VLAN はアップリンクによって伝送されますが、ポート g0/15 または 16 を経由して管理モジュールに伝送されるので、BladeCenter の動作に影響を及ぼす可能性があります。この内部リンクが使用されることと、管理モジュールが BladeCenter 内のデバイスのプロキシとして動作しようとするのが、IGESM の管理に IGESM アップリンクを使用する場合にシナリオ 3 と 4 のみが実現性のあるオプションと考えられる主な理由です。

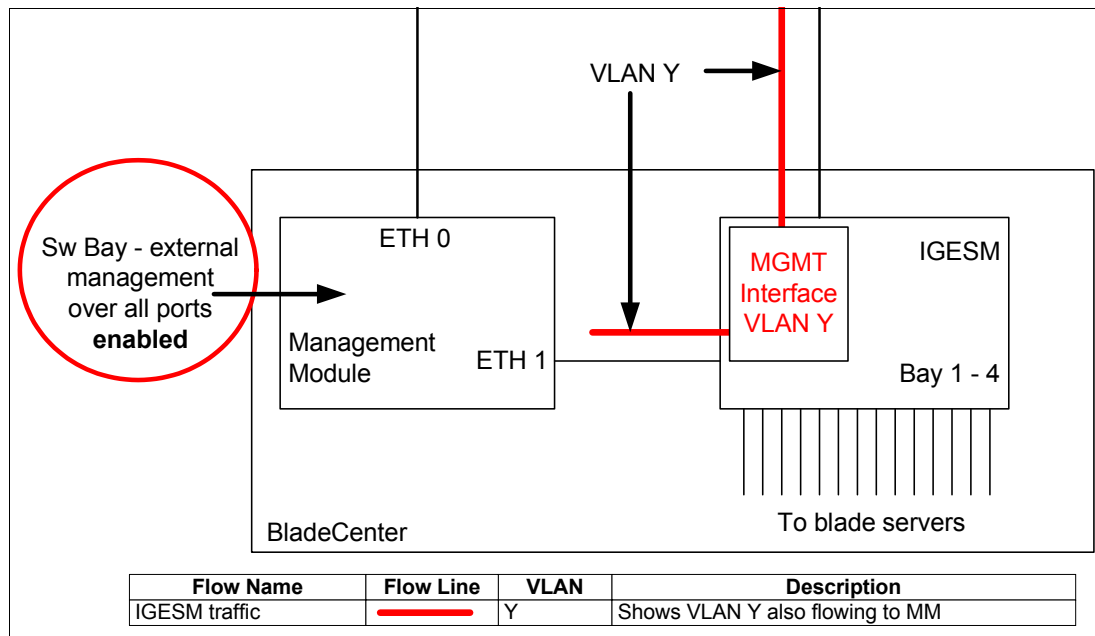


図5-42 IGESM アップリンクと管理モジュールへの内部リンクを経由した管理の考察

### 5.3.6 考慮事項：特定の BladeCenter 内に複数の IGESM がある場合

BladeCenter シャーシに複数の IGESM を取り付ける場合、最も一般的な（推奨される）アプローチは、IGESM を管理モジュールのアップリンク経由、または IGESM のアップリンク経由のどちらで管理するかに関係なく、すべての IGESM を同じ IP サブネット内の同じ管理 VLAN に配置することです。この単純なアプローチを順守すれば、本書で説明する推奨シナリオを正しく動作させることができます。

ユーザーは、IGESM を異なる管理 VLAN に配置したい場合があります。たとえば、異なるグループがいくつかの IGESM を管理し、これらのグループが BladeCenter 内の各 IGESM 間で VLAN の分離を必要とする場合などです。これを実行することは簡単に見えますが、実際には予期しないエラー・メッセージが IGESM 上で生成される結果になる可能性があります。

単一シャーシ内の IGESM を異なる管理 VLAN に配置する場合の問題は、管理モジュールがそれぞれの IGESM<sup>1</sup> に接続し、それぞれの IGESM が常にポート g0/15 と g0/16 上の管理 VLAN をネイティブ VLAN にするために、異なる管理 VLAN が存在すると、それぞれの IGESM がネイティブ VLAN のミスマッチに関する問題をそれぞれのログとコンソール・ポートに報告することです。

<sup>1</sup> アップリンク・ポートからのトラフィックが g0/15 と 16 を流れないようにブロックするハード・フィルターは、一方の IGESM から発信されて管理モジュールを通り、シャーシ内の他方の IGESM に移動するパケットには影響を及ぼしません。

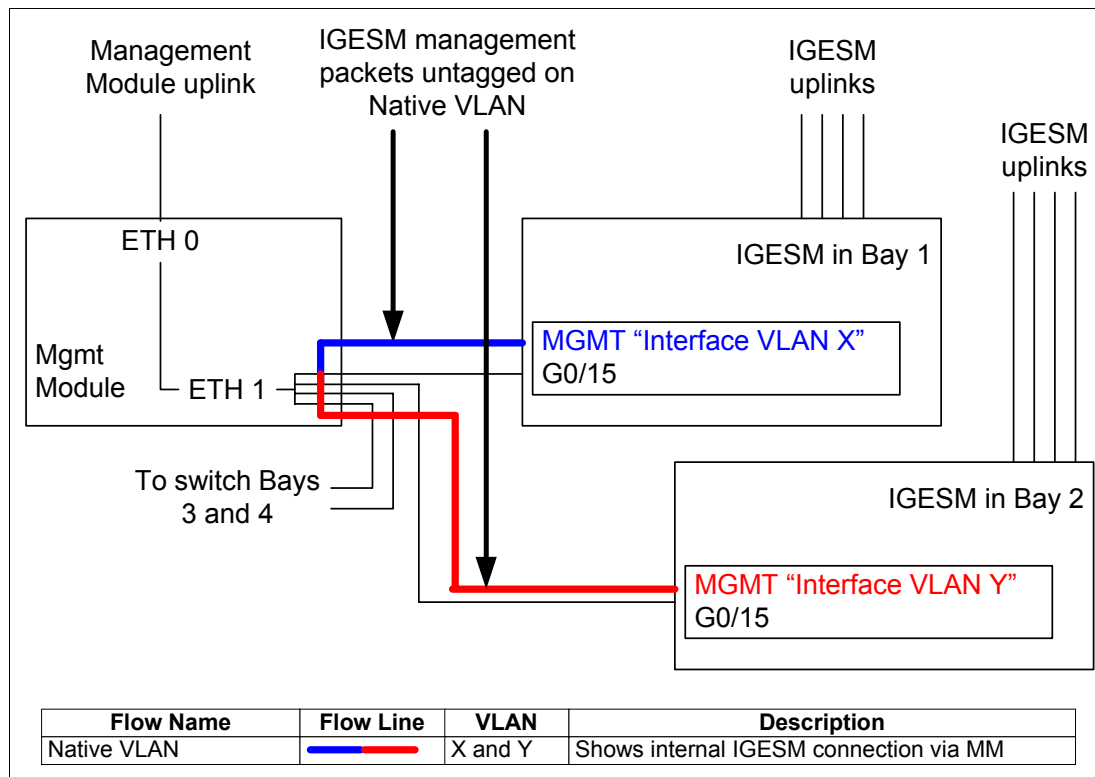


図5-43 異なる IGESM 上で異なる管理 VLAN を使用する場合の考察

同じ BladeCenter 内にあるそれぞれの IGESM を異なる管理 VLAN に配置する必要がある場合は、管理モジュール方向のポート（g0/15 と g0/16）上で CDP をオフにすることによって、ネイティブ VLAN のミスマッチ・メッセージを停止できます。このためには、これら 2 つのポートに対してコマンド **no cdp enable** を実行します。

ネイティブ VLAN のミスマッチ・メッセージが IGESM に表示されるその他の理由としては、IGESM とその接続先のアップストリーム・スイッチとの間でネイティブ VLAN のミスマッチが生じている場合があります。図 5-43 で解説した問題は、同じ BladeCenter 内の異なる IGESM 上で異なる管理 VLAN の使用を試みた場合に固有のものです。すべての IGESM を同じ VLAN に配置しているときに、ネイティブ VLAN のミスマッチ・メッセージが表示される場合は、問題は他のところにあり、標準のトラブルシューティング手法を使用して解決する必要があります。

ここから、さまざまなシナリオを紹介します。



### 5.3.7 シナリオ 1（推奨）

- ▶ 管理モジュールのアップリンクを使用した IGESM の管理
- ▶ 物理的に分離した管理ネットワークとデータ・ネットワーク

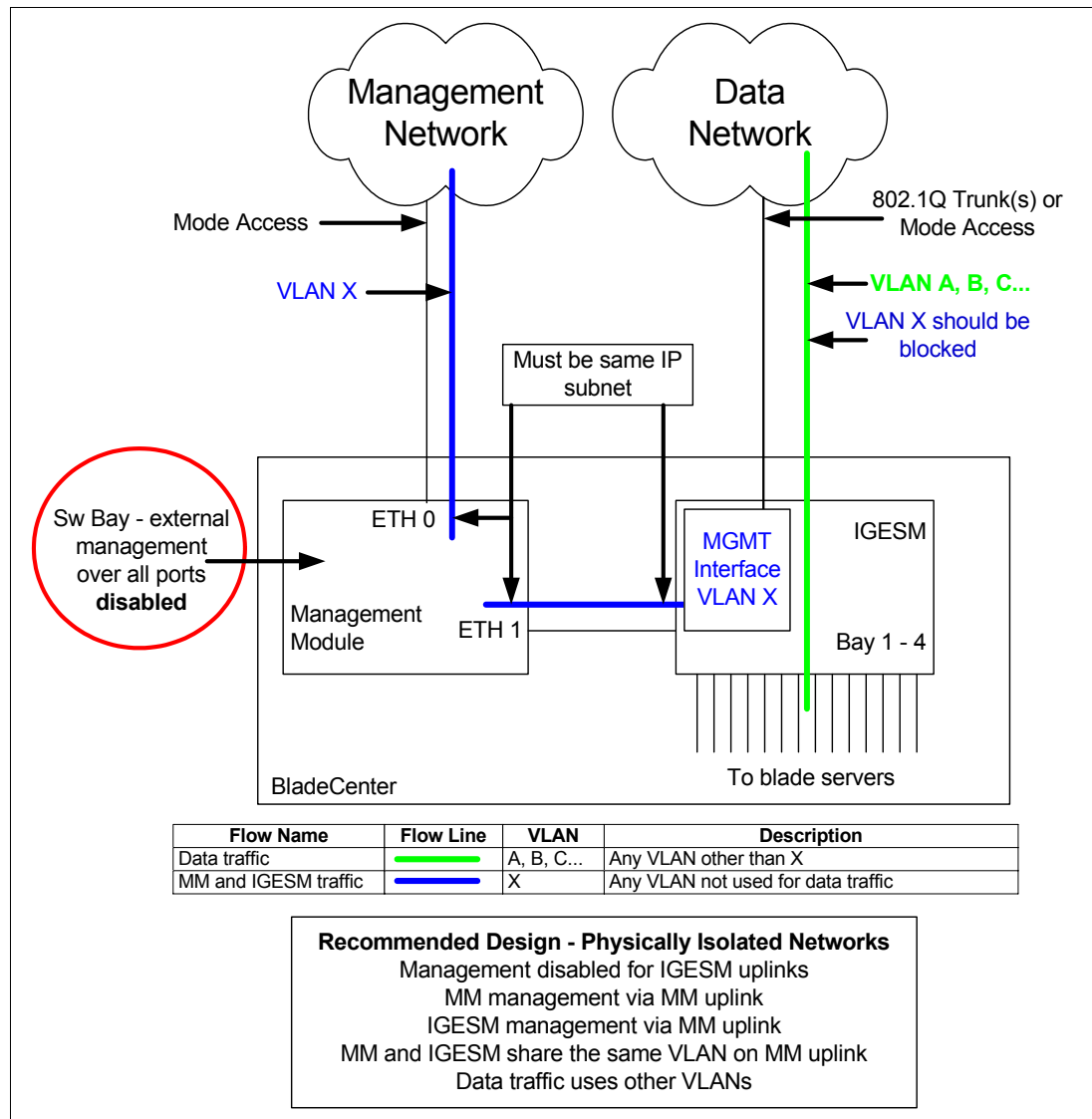


図5-44 シナリオ1: 物理的に分離した管理ネットワークとデータ・ネットワーク。管理モジュールがパスを提供する

このシナリオの規則については、60 ページの 5.3.4、『考慮事項：IGESM の管理に管理モジュールのアップリンクを使用する場合』を参照してください。

シナリオ 1 と 2 は、すべての管理トラフィックが管理モジュールのアップリンク・ポートを使用し、このトラフィックをデータ・トラフィックから分離しているので、最も配置およびサポートしやすい設計です。この設計では、IGESM 自身のアップリンク・ポートを経由して IGESM を管理しないので、アップリンク・ポート上で IGESM を管理するための機能は使用不可に設定する必要があります。このためには、それぞれの IGESM ごとに、管理モジュールの「advanced management」セクションで「External management over all ports」の設定値を「Disabled」に変更します。

この構成が正しく動作するためには、IGESM によって使用される IP アドレスが、管理モジュールによって使用されるものと同じ IP サブネット内にいることが必要です。

この物理的に分離された管理ネットワークとデータ・ネットワークからなる環境では、IGESM アップリンク上で管理 VLAN をブロックすることは必須ではありませんが、このようにすれば、もし 2 つのアップストリーム・ネットワークが物理的に併合されたときに問題を防止できます。このシナリオは、物理的に分離されたネットワーク（それぞれのネットワークごとにスイッチとルーターが異なる）を対象としていること注意してください。シナリオ 2 に示すような、論理的に分離されたネットワーク（共用のスイッチとルーターが、データおよび管理のトラフィックを VLAN によって分離している）を正しく動作させるためには、IGESM アップリンクを通らないように管理 VLAN をブロックする必要があります。

アップストリーム・ネットワークは物理的に分離されていますが、ブレード・サーバーの通信に使用される VLAN は、管理モジュールおよび IGESM によって使用される VLAN とは異なる必要があります。77 ページの図 5-51 は、この分離が必要である理由を示しています。

### 5.3.8 シナリオ 2（推奨）

- ▶ 管理モジュールのアップリンクを使用した IGESM の管理
- ▶ 共通の管理ネットワークとデータ・ネットワーク

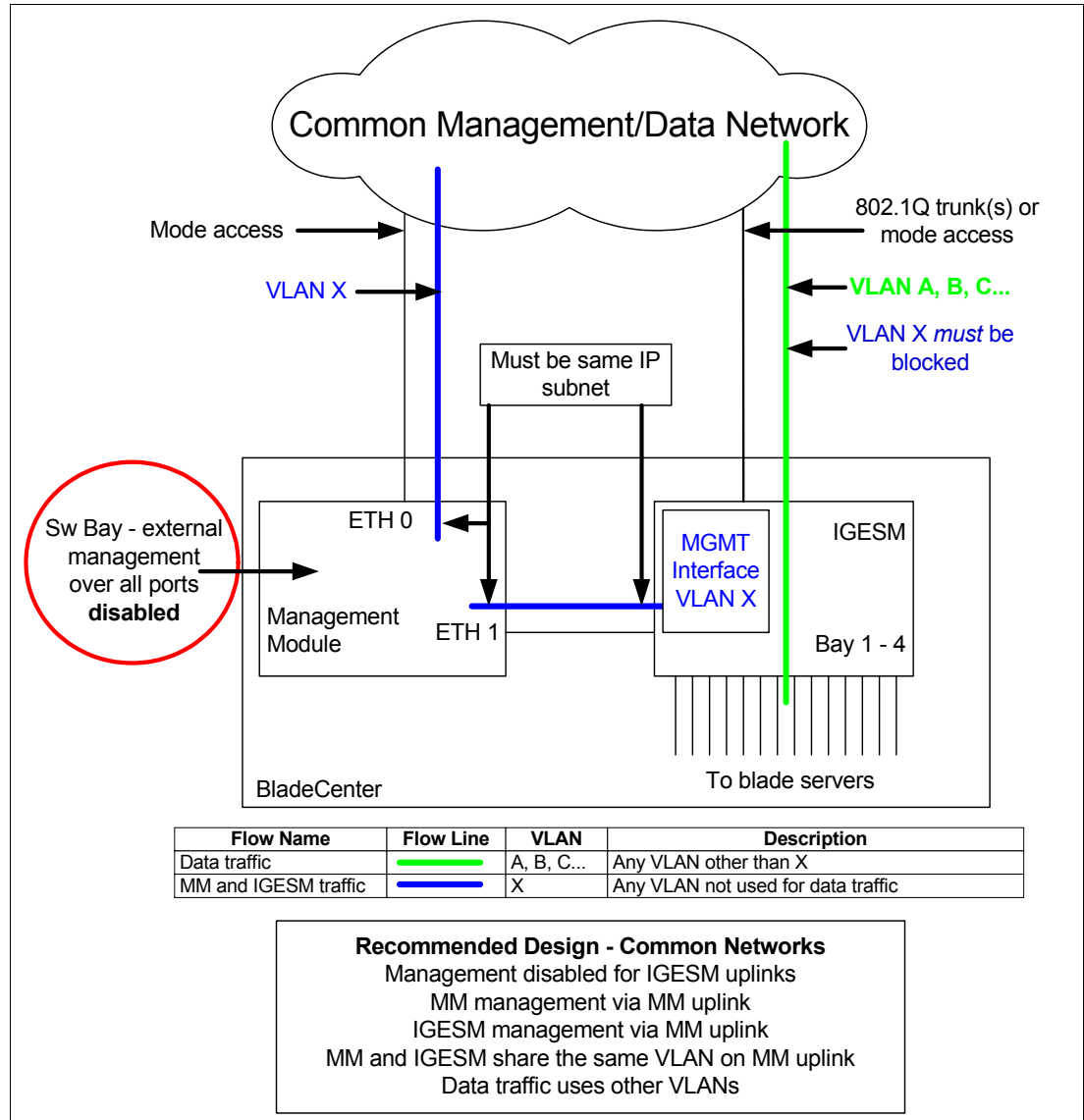


図5-45 シナリオ2: 物理的に共通する管理ネットワークとデータ・ネットワーク。管理モジュールがパスを提供する

このシナリオの規則については、60 ページの 5.3.4、『考慮事項: IGESM の管理に管理モジュールのアップリンクを使用する場合』を参照してください。

シナリオ 1 で説明したように、この設計は、すべての管理トラフィックが管理モジュールのアップリンク・ポートを使用し、このトラフィックをデータ・トラフィックから分離しているので、最も簡単に配置およびサポートできる設計の 1 つです。この設計では、IGESM 自身のアップリンク・ポートを経由して IGESM を管理しないので、アップリンク・ポート上で IGESM を管理するための機能は使用不可に設定する必要があります (このためには、それぞれの IGESM ごとに、管理モジュールの「advanced management」セクションで「External management over all ports」の設定値を「Disabled」に変更します)。

IGESM 上の管理インターフェース VLAN の選択は重要です。この VLAN は、いずれかのブレード・サーバーとの間でトラフィックをやり取りするために使用される VLAN に設定してはなりません。

管理モジュールのアップリンク・ポートに接続されるアップストリーム・スイッチ上での VLAN 設定も、このシャーシ内のブレード・サーバーによって使用されない VLAN のいずれかにすることができます。ただし、IGESM 上の管理 VLAN と同じ VLAN に設定すれば、混乱を避けるために役立ちます。（この規則の例外は、シナリオ 7 を参照してください）

シナリオ 1 の場合と同様に、この構成が正しく動作するためには、IGESM によって使用される IP アドレスが、管理モジュールによって使用されるものと同じ IP サブネット内にある必要があります。

シナリオ 1 とシナリオ 2 の重要な違いの 1 つは、このシナリオではアップストリーム・ネットワークが共通インフラストラクチャーであるため、VLAN の分離に頼ってトラフィック・タイプの分離を実現している点です。このためには、IGESM とそのアップストリーム・スイッチの間のアップリンクを通らないように VLAN X をブロックする必要があります。このブロックを行わないと、IGESM を管理する際に接続が断続的になる問題が発生する可能性があります。

### 5.3.9 シナリオ 3（推奨）

- ▶ IGESM アップリンクを使用した IGESM の管理
- ▶ IGESM、管理モジュール、およびデータのトラフィックはそれぞれの VLAN に分離

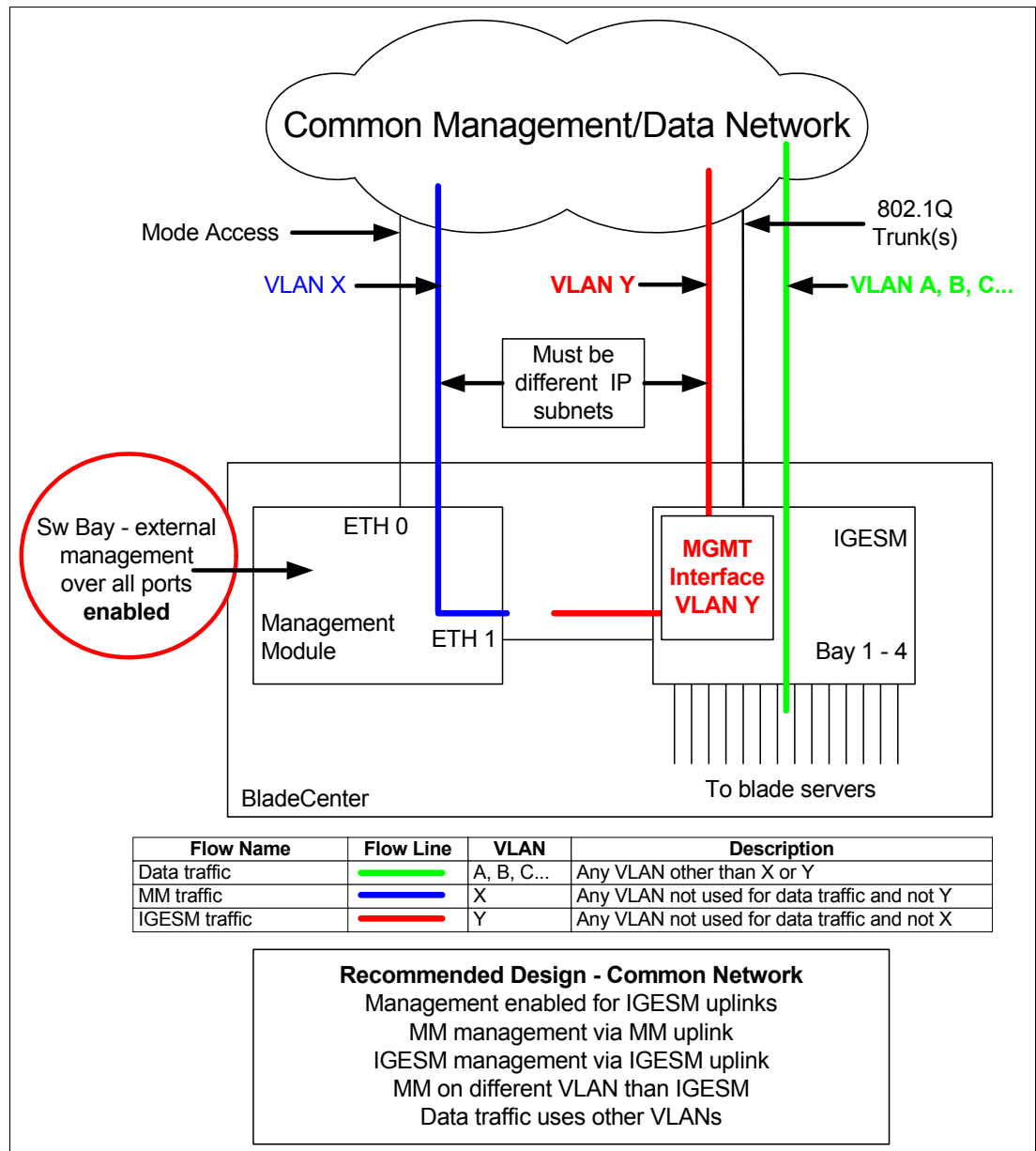


図5-46 シナリオ3: 物理的に共通の管理ネットワークとデータ・ネットワーク。IGESM アップリンクがIGESM 管理パスを提供する

このシナリオの規則については、63 ページの 5.3.5、『考慮事項 : IGESM アップリンクを使用した IGESM の管理』を参照してください。

シナリオ3は、IGESM の管理に IGESM アップリンクを使用する場合に推奨される設計です。この設計では、IGESM 自身のアップリンク・ポートを経由して IGESM を管理するので、IGESM のアップリンク・ポート上で IGESM を管理する機能を使用可能に設定する必要があります。（それぞれの IGESM ごとに、管理モジュールの「advanced management」セクションで「External management over all ports」の設定値を「Enabled」にする必要があります）

最も重要な点は、それぞれの管理パス（IGESM および管理モジュールの）が分離した VLAN 上にあり、したがって分離した IP サブネット上にあることと、ブレード・サーバーへのデータ・トラフィックに使用されるパスが、これらの VLAN をどちらも使用しないことです。

これはユーザー・トラフィックと管理トラフィックを分離するというネットワーク設計のベスト・プラクティスに従っており、管理モジュールが IGESM にプロキシ・サポートを提供しようとすることを防止している（VLAN と IP サブネットの分離によって）ので完全に安定しており、十分推奨されます。

IGESM とアップストリーム・ネットワークの間のリンクは、この例では 802.1Q トランクとして示されていることに注意してください。このトラフィック分離の要件を満たす方法は、他にもあります。たとえば、VLAN Y を IGESM ポート g0/17 上の単一のアクセス・リンクに配置し、IGESM ポート g0/18、19、または 20 の任意の組み合わせで構成される 802.1Q トランク・ポートに VLAN A、B、C などを配置します。これにより、最終的に管理 VLAN をブレード・サーバーの VLAN から分離する要件が同じように満たされるので、この構成は機能します。

ただし、IGESM の管理インターフェースに冗長性がないため、この方法はあまり実用的ではありません。ポート g0/17 がダウン状態になると、IGESM への管理接続が失われます。より論理的なアプローチとしては、IGESM からのアップリンクによって 1 つまたは 2 つの EtherChannel バンドルを作成し、これらを 802.1Q トランクとして構成して、必要なすべての VLAN（管理 VLAN とブレード・サーバー VLAN の両方）を伝送します。

最後に 1 つ注意点があります。IGESM と管理モジュールの間の赤い線は、技術上、VLAN Y が実際には管理モジュールに伝送されている（リンク上のネイティブ VLAN によって）ことを改めて示すためのものです。このシナリオでは、そのことは問題になりません。これは、管理モジュール上の IP サブネットが、IGESM 管理インターフェース (VLAN Y) 上で使用されているものとは異なるため、管理モジュールが VLAN Y 上のデバイスのプロキシとして動作しようとする可能性がないからです（管理モジュールは自身の IP サブネット上にあるデバイスのみのプロキシになるため）。

### 5.3.10 シナリオ 4 (考えられる代替案)

- ▶ IGESM アップリンクを使用した IGESM の管理
- ▶ IGESM トラフィックとデータ・トラフィックの VLAN は共通

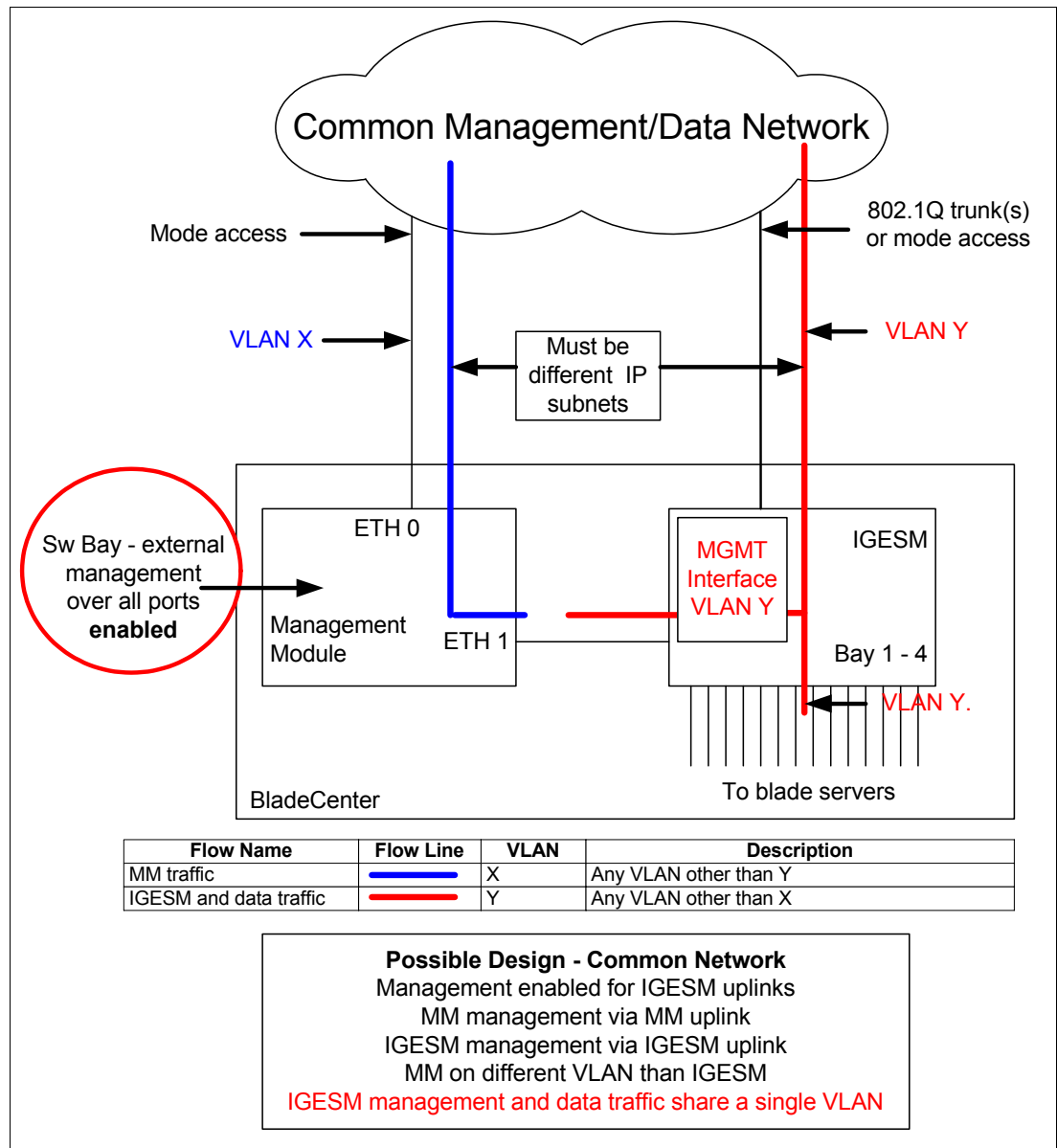


図5-47 シナリオ4: 物理的に共通の管理ネットワークとデータ・ネットワーク。IGESM アップリンクがIGESM 管理パスを提供する

このシナリオの規則については、63 ページの 5.3.5、『考慮事項 : IGESM アップリンクを使用した IGESM の管理』を参照してください。

シナリオ 4 では、管理 VLAN はブレード・サーバーと IGESM の両方によって共有されます。管理モジュール上の IP サブネット (ETH0 と ETH1 の両方の) が、IGESM とブレード・サーバーによって使用される IP サブネットとは異なっている限り (これらが別々の VLAN であれば、そのようにする必要があります)、この設計は機能します。

何らかの理由で、この設計のブレード・サーバーが管理モジュールと同じ IP サブネットに配置された場合 (異なる VLAN 内にあるにもかかわらず) は、ブレード・サーバーがネッ

トワーク上のデバイスに接続する際に問題が生じる可能性が高くなります。これは、管理モジュールが **IP ARP** 要求（ブレード・サーバーから発信され、内部接続を経由して管理モジュールに至る）のプロキシとして動作しようとするからで、ブレード・サーバー自身の **IP** アドレスに重複が生じたり、デフォルト・ゲートウェイの **MAC** アドレスが誤っていたりする可能性があり、接続の確立に失敗する結果になります。

この設計についてもう 1 つ考えられる欠点は、ネットワーク設計のベスト・プラクティスではデータ・トラフィックと管理トラフィックに分離した **VLAN** を使用するよう勧められているにもかかわらず、ここでは **VLAN Y** でデータ・トラフィックと管理トラフィックを混合している点です。こうした問題から、**IGESM** アップリンクを管理に使用する場合はシナリオ 3 が推奨されますが、シナリオ 4 も必要に応じて代替として使用できます。



### 5.3.11 シナリオ 5（非推奨）

- ▶ IGESM アップリンクを使用した IGESM の管理
- ▶ IGESM と管理モジュールのトラフィックの VLAN は共通

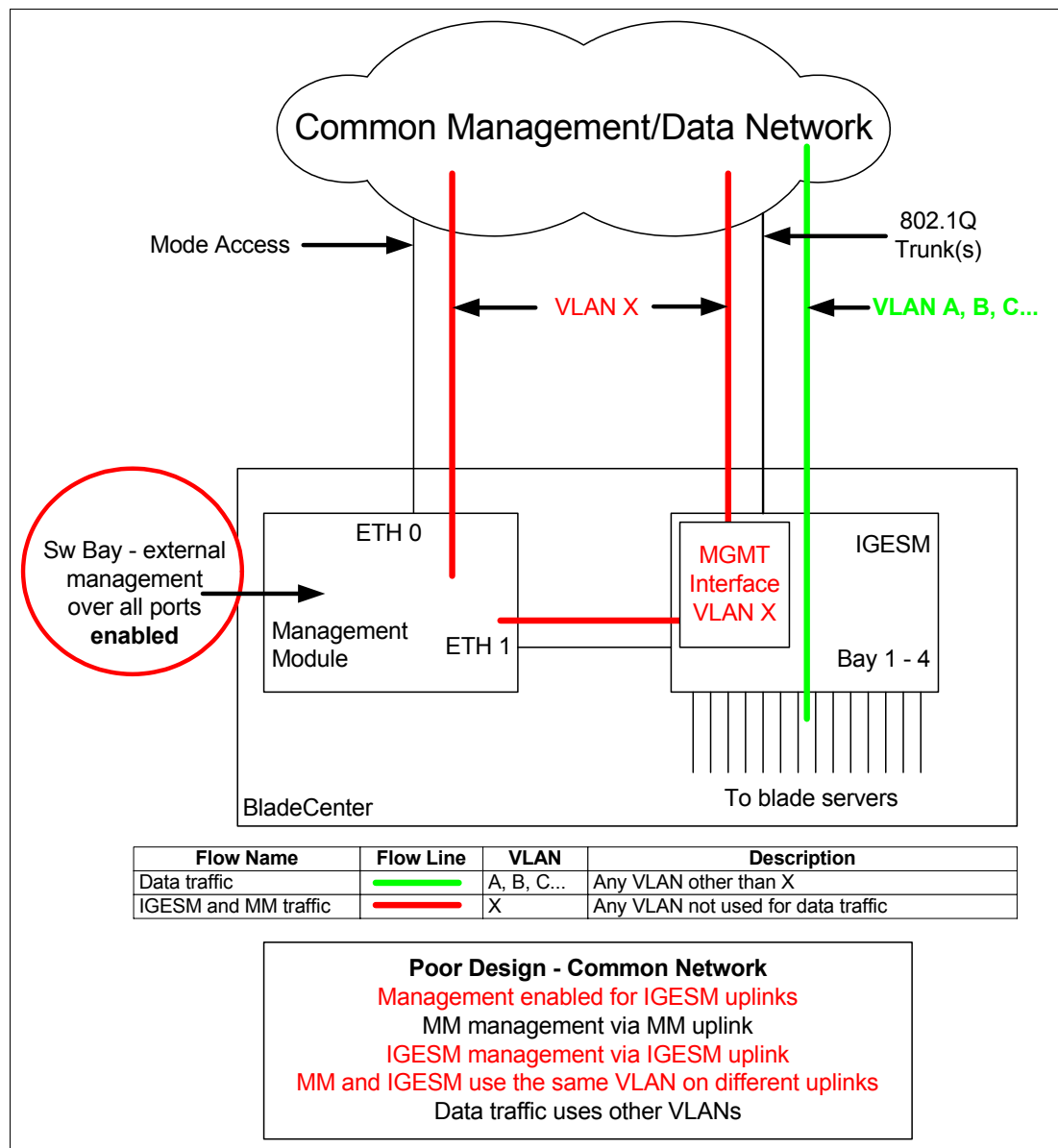


図5-48 シナリオ5: 物理的に共通の管理ネットワークとデータ・ネットワーク。管理モジュールのアップリンクとIGESMのアップリンクがIGESM管理パスを提供する

シナリオ5では、IGESM上のアップリンク・ポートを使用してIGESMを管理し、管理モジュールのアップリンク・ポートを使用して管理モジュールを管理しようと試みますが、これらを同じVLANに配置し、場合によっては同じIPサブネットに配置します。

この設計では、管理モジュールとIGESMの両方がIGESMのIPアドレスの制御を争ったときに（それぞれがIGESMのIPアドレスに対するGratuitous ARPをアップストリーム・ネットワークに向けて発信するために）、IGESMへの最適なパスに関してアップストリーム・デバイスに混乱が生じる可能性があります。この設計は、成功するときと失敗するときがあります。アップストリーム・デバイスが、IGESM宛ての packets をそのアップリンク経由でIGESMに直接送信する場合（成功）もあれば、管理モジュールに送信する場合もあり

(Gratuitous ARP が競合している間に)、このとき管理モジュールはこのデータを IGESM に渡すことも渡さないこともあります (失敗)。図 5-49 に、こうした問題の例を示します。

この設計の結果は予期できず制御できないので、この設計は推奨されません。

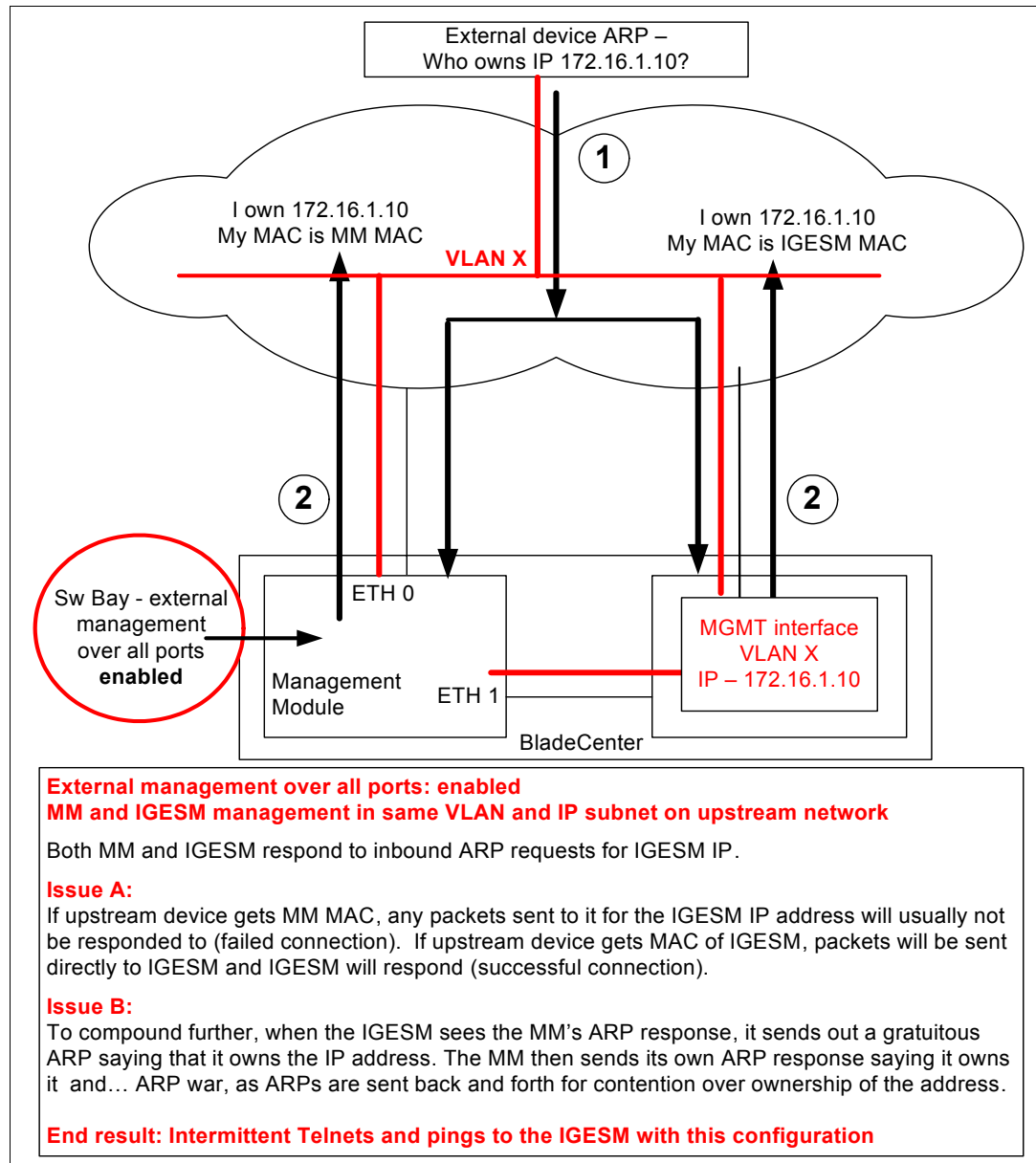


図 5-49 アップストリームの問題: シナリオ 5 が推奨されない理由

### 5.3.12 シナリオ 6（非推奨）

- ▶ IGESM アップリンクを使用した IGESM の管理
- ▶ IGESM、管理モジュール、およびデータのトラフィックの VLAN はすべて共通

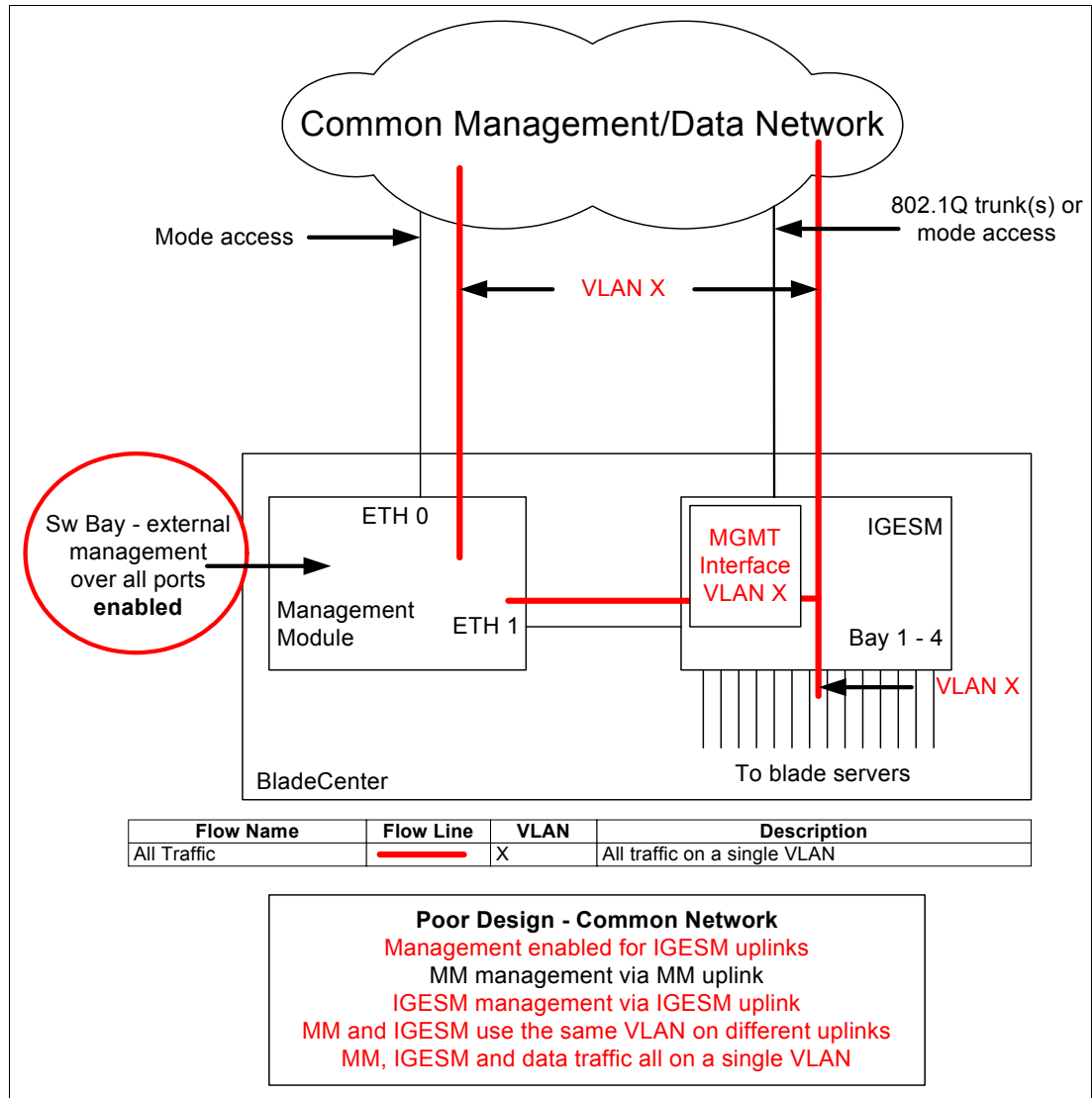


図5-50 シナリオ6: 物理的に共通の管理ネットワークとデータ・ネットワーク。管理モジュールのアップリンクとIGESMのアップリンクがIGESM管理パスを提供する

シナリオ6は、考えられる最悪の設計です。問題はシナリオ5（75ページの図5-49）で説明したとおりですが、すべてのトラフィックを単一のVLAN/IPサブネット上で伝送するため、データ・トラフィックと管理トラフィックの混合も生じます。さらに、ブレード・サーバーは管理モジュールと共通のVLANを共用し、たいていはIPサブネットも共用するので、管理モジュールがBladeCenter内のブレード・サーバーのプロキシとして動作しようとする可能性があり、そのために正しい接続に失敗します（77ページの図5-51）。

ここで説明した問題が起こる可能性を考えると、この設計は推奨されず、ほぼ確実にBladeCenterの動作不良を引き起こします。



### 5.3.13 シナリオ 7（評価テスト環境として使用可能）

- ▶ 管理モジュールのアップリンクを使用した IGESM の管理
- ▶ 管理モジュールおよびデータのトラフィックの VLAN はすべて共通
- ▶ IGESM は内部では異なる VLAN 上にあるが、管理モジュールのアップリンク VLAN を管理のために共有

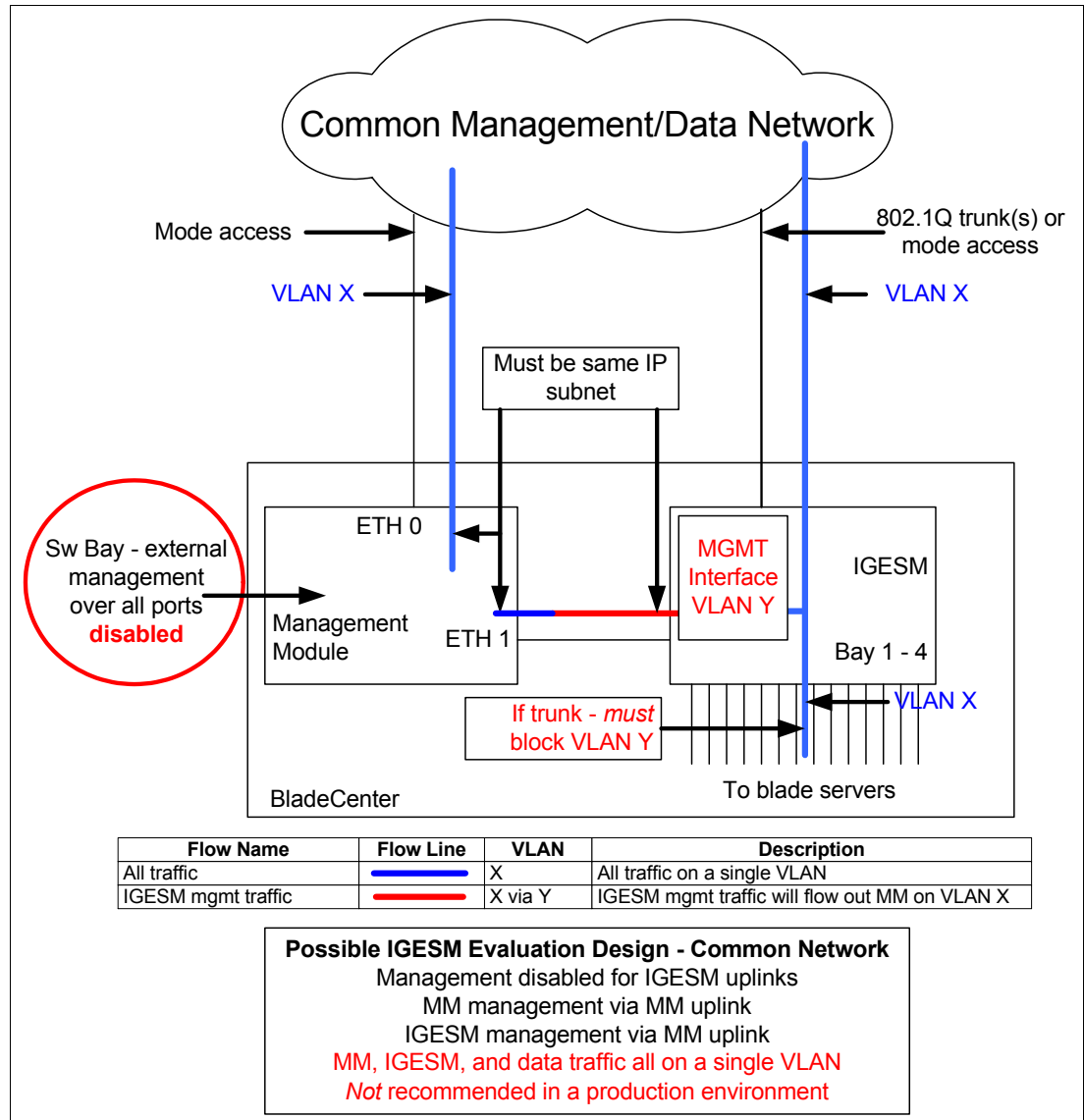


図5-52 シナリオ7: テスト環境のみ。管理モジュールのアップリンクがIGESM 管理パスを提供する

注：この構成には、既知の注意点があります。ブレード・サーバー側のポート（g0/1 から 14）がトランクを構成している場合は、これらのトランク・ポートから IGESM の管理 VLAN Y をブロックする必要があります。ブレード・サーバー方向のポート上で VLAN Y をブロックしなければ、ブレード・サーバーから IGESM の IP アドレスへの ping 要求が失敗し、またブレード・サーバーから IGESM への Telnet が断続的に失敗する可能性があります。ただし、ブレード・サーバー方向のポートがアクセス用に設定されている場合（また、Y 以外の VLAN の場合）、この注意点は該当しません。

このシナリオの基本的な規則については、60 ページの 5.3.4、『考慮事項: IGESM の管理に管理モジュールのアップリンクを使用する場合』を参照してください。このシナリオは、次に説明する規則のいくつかに違反しますが、それでも評価目的には利用できます。

前述のとおり、このシナリオは単一の VLAN テスト・ネットワーク上で IGESM を評価するために役立つ場合があります。ただし、すべてのトラフィックに同じ VLAN を共用するので、実稼働環境での使用は推奨されません。

この設計について、重要な点が 2 つあります。

- ▶ IGESM と管理モジュールが IGESM IP アドレスの管理に関して競合する（IGESM の IP アドレスの制御権に対する ARP の競合）ことを防ぐため、IGESM アップリンク経由での管理は**使用不可に設定する必要があります**。この環境では、管理モジュールのみが IGESM への管理パスを提供するようにします。
- ▶ 管理モジュールと IGESM によって使用される IP サブネットは、同じであることが必要です。

IGESM のデフォルトでは、管理 VLAN インターフェースは VLAN 1 で、ブレード・サーバーに向かうポートおよびアップリンクは、デフォルトで VLAN 2 になることがよくあります（リンクの相手側の構成によって異なる）。

テスト環境でよく使用されるアプローチの 1 つは、すべてのトラフィックを VLAN 1 に配置することです。すべてのトラフィックを単一の VLAN（特に VLAN 1）に配置することはベスト・プラクティスに反しますが、限定されたテスト環境には適している場合があります。この種のテスト環境の要件によっては、最初に IGESM 用の管理 VLAN を新規に作成し、次に IGESM の管理インターフェースを新規に作成した VLAN に変更してから、ブレード・サーバーとアップリンク方向のポートを VLAN 1 に配置する必要があります。

次の手順は、VLAN 1 をすべてのユーザー・トラフィックおよび管理トラフィックに使用し、管理モジュールに接続するための IGESM 内部 VLAN として VLAN 4000 を使用するテスト環境をセットアップする場合の例です。*VLAN 4000 は、例示目的にのみ選択されたものです。*

## シナリオ 7 の構成手順の概要

1. IGESM の管理インターフェース VLAN を変更します。
2. IGESM のアップリンク方向のポートを変更します。
3. IGESM のブレード・サーバー方向のポートを変更します。

### IGESM の管理インターフェース VLAN の変更

ポート g0/15 と g0/16 経由でトラフィックを伝送するために IGESM によって使用される VLAN を変更するには、最初のステップとして新規 VLAN を作成します。この例では、この VLAN をこの IGESM 内で他の用途に割り当てないようにする必要があります。VLAN の作成後、新規 VLAN を使用する管理インターフェースを新規に作成する必要があります。インターフェースの新規作成後、この新規インターフェースに対して **no shutdown** を実行すると、IGESM の IP アドレスがこの新規インターフェースに移動し、g0/15 と 16 のリンク上にある管理 VLAN（ネイティブ VLAN）がこの新規 VLAN に自動的に変更されます。

構文の上では、IGESM の管理 VLAN の変更は次のように行われます。

```
conf t
```

```
    IGESM を構成モードにします。
```

```
vlan 4000
```

```
    管理に使用する新規 VLAN を作成します。
```

この例では、VLAN 4000 を使用しました。これは単なる例です。どの VLAN を選択する場合にも、この IGESM 内でその VLAN を他の用途に使用してはなりません（このシナリオ特有の制限）。

```
interface vlan 4000
```

新規 VLAN に基づいて、管理インターフェースを新規に作成します。

```
no shutdown
```

新規の管理 VLAN を起動します。

以前の VLAN インターフェースから IP アドレスを移動します。

以前の VLAN インターフェースをシャットダウンします。

ネイティブ VLAN をポート g0/15 と 16 から 4000 に変更します。

g0/15 と 16 上で伝送される VLAN のリストに VLAN 4000 を追加します。

```
end
```

構成モードを終了します。

```
write
```

構成を NVRAM に保管します。

BladeCenter 内に複数の IGESM が存在する場合は、このシャーシ内の IGESM すべてが、同じ管理 VLAN を使用する準備ができるまでネイティブ VLAN のミスマッチ・メッセージの報告を開始します。詳しくは、64 ページの 5.3.6、『考慮事項：特定の BladeCenter 内に複数の IGESM がある場合』を参照してください。

### **IGESM のアップリンク方向のポートの変更**

このテスト・ネットワークの目標はすべてを単一の VLAN に配置することで、これを最も簡単に実現する方法は、使用中のアップリンク・ポートをアクセス・モードに設定し、アクセス VLAN をこの目的の VLAN に設定することです。この接続の相手側を適切に構成する必要があります。また、使用する単一の VLAN としてネイティブ VLAN を設定して、この接続をトランク・タイプの接続にすることもできます。アップリンク上でトランクを使用する場合は、このトランクから IGESM 管理 VLAN をブロックする必要があります。この VLAN を伝送するアップリンク・ポート（g0/17 から g0/20）上で、次のコマンドを使用します。

```
conf t
```

IGESM を構成モードにします。

```
interface g0/17
```

これは、使用するすべてのアップリンク上で実行する必要があります。複数のアップリンクを使用している場合、このステップではそのことを考慮に入れる必要があります。

```
switchport mode access
```

ポートをアクセス用に設定します。前述のように、このリンクの相手側も適切に構成する必要があります。

```
switchport access VLAN 1
```

アップリンク・ポート（複数の場合もある）VLAN 1 用に設定します。

```
end
```

構成モードを終了します。

```
write
```

構成を NVRAM に保管します。

## IGESM のブレード・サーバー方向のポートの変更

前述のこのシナリオの目標に基づいて、ブレード・サーバーのポート（g0/1 から 14）も VLAN 1 に配置する必要があります。次に、先頭のスロット 1 のブレード・サーバーをアクセス VLAN 1 に配置する例を示します。

```
conf t
```

IGESM を構成モードにします。

```
interface g0/1
```

このテストに使用するブレード・サーバー方向のポートすべてに対して実行する必要があります。

```
switchport mode access
```

ポートをアクセス用に設定します。

```
switchport access VLAN 1
```

ブレード・サーバー方向のポート（複数の場合もある）を VLAN 1 用に設定します。

```
end
```

構成モードを終了します。

```
write
```

構成を NVRAM に保管します。

ブレード・サーバーに向かうポートをトランクのままにする場合は、IGESM の管理 VLAN をこのトランクからブロックする必要があります。詳しくは、この節の最初に説明した注意点を参照してください。

**重要：**このシナリオの中ですでに説明したとおり、ユーザー・トラフィックと管理トラフィックの両方を伝送するために単一の VLAN を使用することはベスト・プラクティスとは考えられず、このような設計を実動ネットワーク内で使用することは推奨されません。







## IBM eServer BladeCenter システムの初期セットアップ

この章では、ネットワーク・トポロジーと構成されるハードウェアについて解説し、Cisco Systems Intelligent Gigabit Ethernet Switch Module (IGESM) for the IBM @server BladeCenter の実装に役立つテスト済みの作動可能な構成を示します。

本書ですでに説明したとおり、本書の情報は IOS の 12.1(14) バージョンを実行する 4 ポート・銅線ベースの IGESM に適用されます。4 ポート・ファイバーベースの IGESM、または IGESM 12.1(22) 以上のコードを実行する 4 ポート銅線ベースの IGESM を使用する場合は、これらのソリューションに該当する資料を参照してください。

## 6.1 IBM eServer BladeCenter システム

ここでは、BladeCenter を操作するための準備について段階を追って説明します。

### 6.1.1 管理モジュールのファームウェア

BladeCenter に必要なハードウェアを取り付けた後、IBM eServer BladeCenter - 管理モジュール・ファームウェア更新バージョン 1.10 以降を使用して、管理モジュールを更新する必要があります。次の Web サイトにアクセスして、ファームウェアを入手します。

<http://www.ibm.com/pc/support/site.wss/document.do?lnocid=MIGR-54939>

または、次の Web サイトで最新バージョンを検索します。

<http://www.ibm.com/servers/eserver/support/xseries/index.html>

*readme* ファイルに記載されている、インストールとセットアップの手順のとおりに行います。*.pkt* 拡張子の付いたファイルのみをインストールする必要があります。インストール後、管理モジュールを再始動する必要があります、図 6-1 を参照してください。

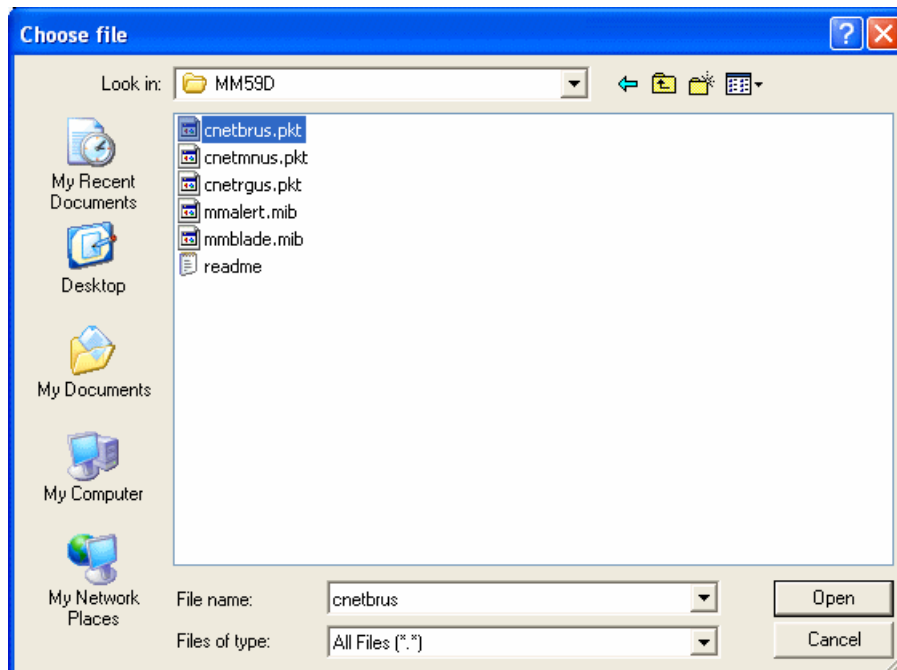


図 6-1 管理モジュールのファームウェア更新ファイル

### 6.1.2 管理モジュールのネットワーク・インターフェース

ここでは、管理モジュールの外部および内部のネットワーク・インターフェースを構成して、管理サブネット上に配置します。外部ネットワーク・インターフェースの IP アドレスは、BladeCenter 外部のネットワークに所属します。このアドレスは、外部デバイスから管理モジュールに接続するために使用されます。

## 管理モジュールへの物理接続の確立

管理モジュールの管理は、モジュールの前面にある外部 10/100 Mbps イーサネット・ポートを経由して行う必要があります。管理モジュールへの物理接続を確立するには、次のいずれかの方法を使用します。

- ▶ カテゴリー 3、4、5、またはそれ以上の対より線（シールドなし）（UTP）ストレート・ケーブルを使用して、管理モジュールのイーサネット・ポートを、アクセス可能な管理ステーションのあるネットワーク内のスイッチに接続する。
- ▶ カテゴリー 3、4、5、またはそれ以上のクロスケーブルを使用して、管理ステーション（PC、ラップトップ）を管理モジュールの外部イーサネット・ポートに直接接続する。

## 管理モジュール Web インターフェースへのアクセス

管理モジュールへの物理接続を確立した後、管理モジュールと同じサブネット内で使用可能な IP アドレスを指定して、管理ステーションを構成します。デフォルトでは、サブネットは 192.168.70.0/24 です。管理モジュールを管理するには、主に次の 2 つの方法を使用できます。

- ▶ HTTP Web インターフェース
- ▶ IBM Director

本書では、管理モジュール Web インターフェースを使用した管理モジュールの初期構成とスイッチ・モジュール構成の例を示します。

管理モジュールに対する管理セッションを確立し、初期スイッチ・モジュール設定値を構成するには、次の手順で行います。

1. Web ブラウザーを開き、構成済み IP アドレスを使用して管理モジュールに接続します。管理モジュールの外部インターフェースのデフォルト IP アドレスは、192.168.70.125 です。内部インターフェースのデフォルト IP アドレスは 192.168.70.126 である点に注意してください。
2. ユーザー ID とパスワードを入力します。デフォルトは USERID と PASSWORD です（大 / 小文字の区別があり、文字 O の代わりにゼロ）。「OK」をクリックします。
3. 初期ウィンドウで、「Continue」をクリックして管理セッションにアクセスします。

IBM BladeCenter Documentation CD に収録されている「*BladeCenter Management Module User's Guide*」を参照することもできます。

## 管理モジュールのネットワーク・インターフェースの構成

管理モジュール Web インターフェースにアクセスした後、外部および内部のネットワーク・インターフェースを構成できます。BladeCenter 管理モジュール Web インターフェースから、「MMControl」→「Network Interfaces」をクリックします。

BladeCenter Management Module

Bay 1: WMN315734255

Monitors

System Status
Event Log
LEDs
Hardware VPD
Firmware VPD

Blade Tasks

Power/Restart
On Demand
Remote Control
Firmware Update
Configuration
Serial Over LAN

I/O Module Tasks

Power/Restart
Management
Firmware Update

MM Control

External Network Interface (eth0) ?

Interface: Enabled

DHCP Disabled - Use static IP configuration

\*\*\* Currently the static IP configuration is active for this interface.

\*\*\* This static configuration is shown below.

Hostname

BC1-MGMT-B

Static IP Configuration

IP address

192.168.70.131

Subnet mask

255.255.255.0

Gateway address

0.0.0.0

[Advanced Ethernet Setup](#)
[IP Configuration Assigned by DHCP Server](#)

図 6-2 管理モジュールの「External Network Interface」ウィンドウ

BladeCenter 管理モジュールのデフォルトの IP アドレスは、192.168.70.125 です。管理ネットワークに複数の BladeCenter が存在する場合は、外部ネットワーク・インターフェース (eth0) を変更する必要があります。変更しなければ、IP アドレスの競合が発生するため、管理モジュールにアクセスできなくなります。図 6-2 では、外部インターフェースを同じデフォルト管理サブネットに配置し、固有の IP アドレスを使用して構成しました。

外部インターフェースを構成した後、別の固有の IP アドレスを使用して内部インターフェースを構成する必要があります。内部ネットワーク・インターフェース (eth1) (図 6-3) の目的は、イーサネット・リンク経由で BladeCenter デバイスと通信することです。内部インターフェースを外部インターフェースと同じネットワークに構成しなければ、管理モジュールからスイッチ・モジュールへの IP 接続ができなくなるので注意してください。

MM Control

General Settings
Login Profiles
Alerts
Port Assignments
Network Interfaces
Network Protocols
Security
Configuration File
Firmware Update
Restore Defaults
Restart MM

Log Off

Internal Network Interface (eth1) ?

Interface

Enabled

\*\*\* This network interface always uses a static IP configuration.

Static IP Configuration

IP address

192.168.70.132

Subnet mask

255.255.255.0

Gateway address

0.0.0.0

図 6-3 管理モジュールの「Internal Network Interface」ウィンドウ

ページの一番下にある「Save」をクリックします。変更を実装するためには、管理モジュールを再始動する必要があります。

86 Cisco Systems Intelligent Gigabit Ethernet Switch Module

### 6.1.3 入出力モジュールの管理タスク

ここでは、Cisco Systems IGESM をセットアップし、構成します。

#### IGESM のセットアップと構成

IGESM は、シャーシの背面にある 4 つの BladeCenter スイッチ・ベイのいずれかに取り付けることができます。ベイ 1 は、ブレード HS20 のイーサネット・ネットワーク・インターフェース・コントローラー (NIC) のいずれかに接続します。ベイ 2 は、その他のイーサネット NIC に接続します。それぞれの NIC は、スイッチのいずれか 1 つだけに接続するギガビット全二重リンクです。HS40 の場合は、標準として合計 4 つの NIC を装備しており、2 つの NIC が 1 つのスイッチにリンクします。Gigabit Ethernet 拡張カードをブレードに取り付ける場合は、ベイ 3 またはベイ 4 のスイッチが必要です。このカードは、ブレードに 2 つの NIC を追加します。一方の NIC はベイ 3 へ、他方の NIC はベイ 4 への専用ギガビット全二重リンクを備えています。ベイ 1 の Cisco Systems Intelligent Gigabit Ethernet Switch Module を管理するには、BladeCenter 管理モジュールから「I/O Module Tasks」→「Management」をクリックします。図 6-4 に示すようなウィンドウが開きます。

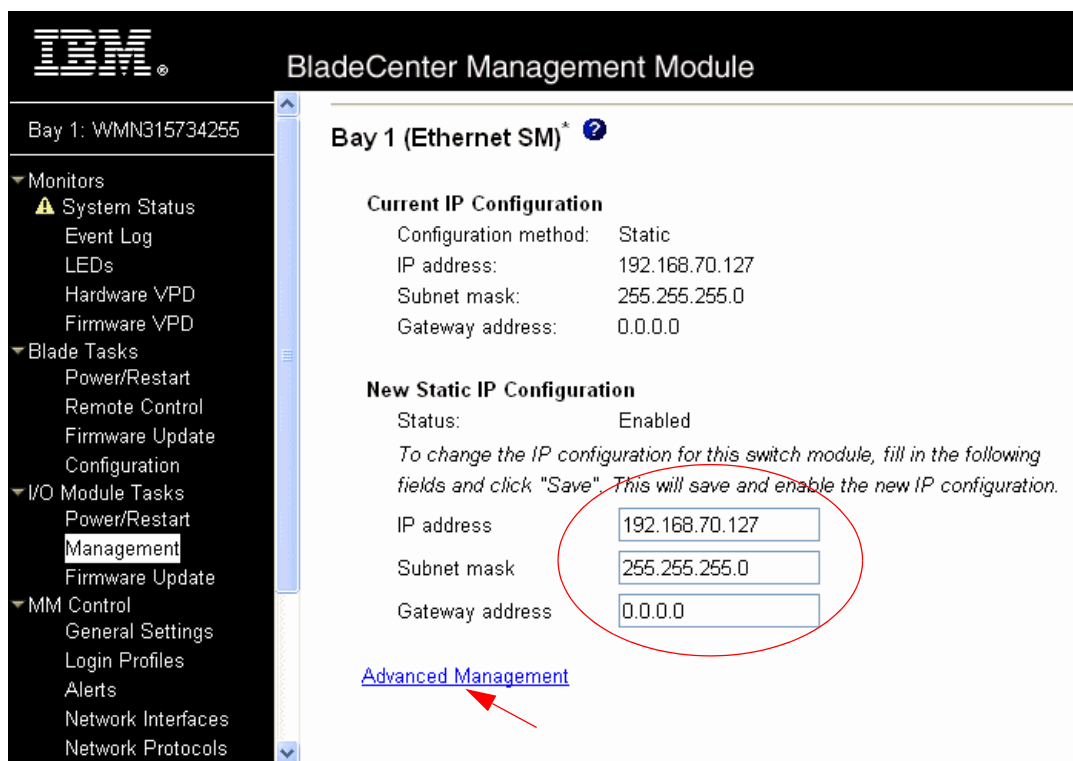


図 6-4 I/O Module Tasks: Management (Bay 1 Ethernet SM) ウィンドウ

管理モジュールの場合と同様に、スイッチには固有の IP アドレスが必要で、アウト・オブ・バンド管理の場合は管理モジュールと同じサブネット上にある必要があります (40 ページの 5.2.1、『アウト・オブ・バンド管理の定義』)。他のネットワークへの接続が必要な場合は、ゲートウェイ・アドレスを入力します。インバンド管理 (41 ページの 5.2.2、『インバンド管理の定義』) を行う場合、IP アドレスは管理モジュールと異なるサブネット内にある必要があります。また、インバンド管理を構成する際には、スイッチ上で構成される VLAN が確実に IGESM のアップリンクによって伝送されるようにする必要があります。

インバンド (IGESM のアップリンク経由で IGESM を管理) またはアウト・オブ・バンド (管理モジュールのアップリンク経由で IGESM を管理) の選択と構成について詳しくは、56 ページの 5.3、『管理パスに関する詳細説明』を参照してください。

これらの変更を即時に適用するには、「Save」をクリックします。リブートまたはリセットは不要です。

## 管理モジュールからの IGESM アップリンク・ポートの使用可能化

ここでは、Cisco Systems Intelligent Gigabit Ethernet Switch Module のイーサネット・ポートを BladeCenter 管理モジュールから使用可能に設定します。87 ページの図 6-4 に示す「I/O Module Tasks」→「Management (Bay 1 Ethernet SM)」ウィンドウで、「Advanced Management」をクリックします。必要な場合は、「Advanced Setup」セクションまでスクロールダウンします。データをスイッチから送信するためには、少なくとも「External ports」を「Enabled」に設定する必要があります (図 6-5)。変更を即時に適用するには、「Save」をクリックします。

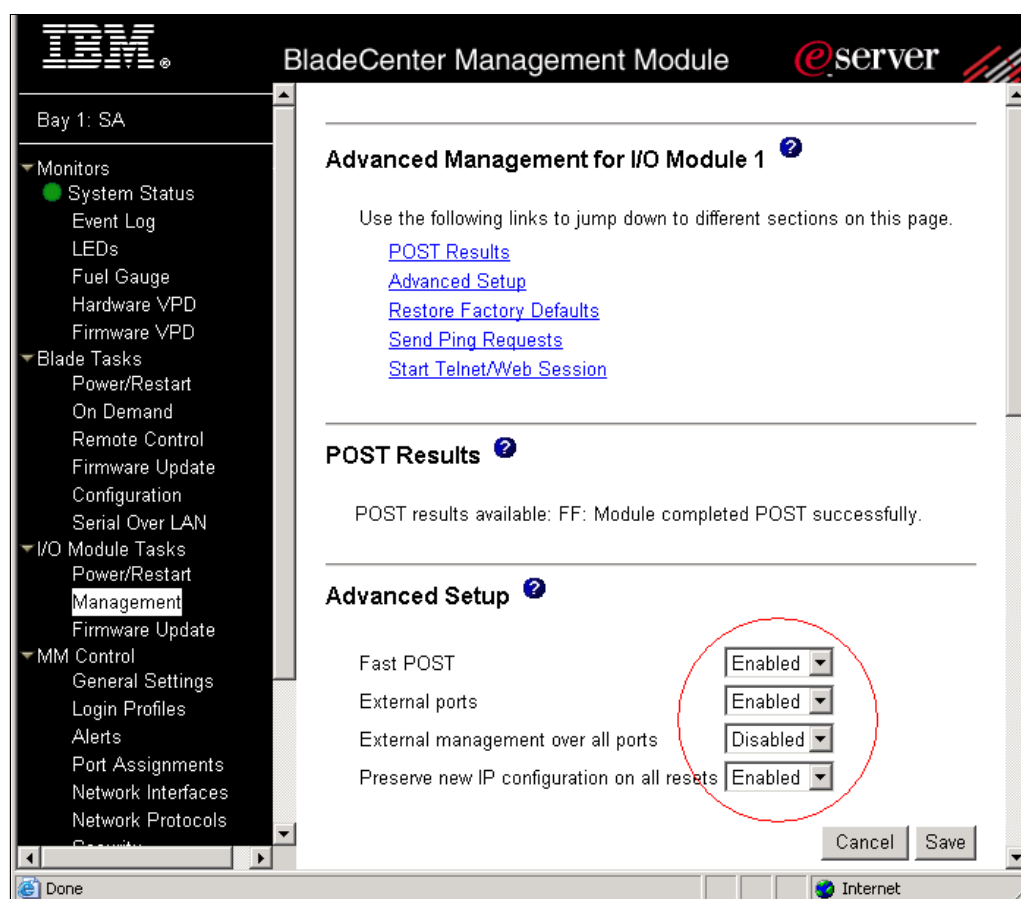


図 6-5 I/O Module Tasks: Management - Advanced Setup

この例では、「Advanced Setup」の「External Management over all ports」を除くすべてのオプションを使用可能に設定しました。次のリストを検討して、使用可能にする必要がある項目を判別してください。

### ▶ Fast POST

このモジュールの高速 POST を使用可能または使用不可に設定するには、このフィールドを使用します。高速 POST を使用可能に設定すると、メモリー診断がバイパスされます。使用不可に設定すると、メモリー診断が POST 中に実行されます。

► External ports

この入出力モジュールの外部ポートを使用可能または使用不可に設定するには、このフィールドを使用します。外部ポートを使用不可に設定すると、トラフィックがこれらのポートを通過できなくなります。

このフィールドを「Disabled」に設定した場合は、ポート g0/17 から 20 に対して **no shutdown** を実行すると、「Shutdown not allowed」などのエラー・メッセージが表示されます。

► External management over all ports

このモジュールの外部からの構成管理を使用可能または使用不可に設定するには、このフィールドを使用します。このフィールドを「Disabled」に設定すると、管理モジュールのポートのみをこのモジュールの構成の変更に使用できます（つまり、アウト・オブ・バンド管理）。このフィールドを「Enabled」に設定すると、すべてのポート（内部、外部、および管理モジュールのポートを含む）を管理に使用でき、この場合はいくつかの規則に従う必要があります。

この設定値を使用して IGESM 管理パスを定義する方法については、56 ページの 5.3、『管理パスに関する詳細説明』を参照してください。

► Preserve new IP configuration on all resets

モジュールの出荷時のデフォルト値が復元された場合、または管理モジュール以外のソースからリセットが開始された場合に、ユーザー定義の IP 構成を保持するかどうか指定するには、このフィールドを使用します。このフィールドを「Enabled」に設定する場合は、このスイッチの管理モジュール設定の中で、このスイッチ・モジュールに対して有効な IP 構成が入力されていることを確認してください。このフィールドを「Disabled」に設定した場合は、スイッチの出荷時のデフォルト値が復元されたとき、または管理モジュール以外のソースによってスイッチのリセットが開始されたときに、出荷時のデフォルト IP 構成がアクティブになります。この場合は、管理モジュールに保管されている IGESM のユーザー定義 IP 構成は使用されません。

この値を「Disabled」に設定すると、IGESM は NVRAM に保管された IP 情報を以降の IGESM のリブート時に使用できるようになりますが、管理モジュールのリブート時には、管理モジュールが持っている IGESM の IP アドレスが引き続き IGESM に適用されるので注意してください。このため、IGESM を再ロードするときに、管理モジュールの再ロード時とは異なる IP 情報が使用されないように、この設定値は「Enabled」のままにすることを強くお勧めします。

この設定値を「Disabled」として有効に使用するには、管理モジュールの IGESM 設定に保管されている情報を、IGESM の NVRAM に保管されている情報と同じにする必要があります。これにより、管理モジュールまたは IGESM のどちらかが再ロードされても関係なく、正しい IP 情報が IGESM 上で使用されます。

## IGESM ファームウェアのダウンロード

ここでは、スイッチ・モジュールの最新バージョンのファームウェアをロードします。

### Cisco スイッチ・ソフトウェアのレベルの判別

Cisco スイッチ・モジュールを BladeCenter 装置に取り付けた後、最新の Cisco スイッチ・オペレーティング・システムがモジュールにインストールされていることを確認してください。スイッチ・モジュールにインストールされている Cisco スイッチ・オペレーティング・システム・ソフトウェアのレベルを判別するには、次の手順で行います。

1. IGESM コマンドラインインターフェースにログオンします。
2. **show version** コマンドを実行します。
3. 現行リビジョンについて、戻されたバージョン情報を確認します。



このプロジェクトの大部分では、Cisco Systems IGESM ファームウェアのビルド 12.1 [14] AY を使用しました。

### 最新レベルのスイッチ・ソフトウェアの入手

IBM から入手可能な最新レベルの Cisco スイッチ・オペレーティング・システム・ソフトウェアを判別するには、次の手順で行います。

1. <http://www.ibm.com/pc/support/site.wss/> にアクセスします。
2. 「Downloads and drivers」をクリックします。
3. 「Downloads and drivers」ウィンドウの「Quick path」フィールドに、スイッチ・マシンの型式番号を入力し（たとえば、8832-21x）、「Go」をクリックします。結果ウィンドウが開き、入手可能な最新ソフトウェアのリンクのリストが表示されます。
4. **show version** コマンドからメモを取っておいたソフトウェアのレベルを、入手可能なソフトウェアの最新レベルと比較します。2つのソフトウェア・レベルが一致しない場合は、Web から最新レベルをダウンロードし、ご使用のスイッチにインストールします。

### スイッチ・ソフトウェアのアップグレード

スイッチ・ソフトウェアのアップグレードは、TFTP サーバー・アプリケーションを使用していきます。通常、このソフトウェアはオペレーティング・システムのもとでアプリケーションとして実行されます。ご使用のサーバーにこのソフトウェアがインストールされていることを確認した後、IBM Web サイトから TFTP サーバー上のディレクトリにソフトウェア・イメージをダウンロードします。TFTP サーバーを使用可能に設定し、デフォルト・ディレクトリをイメージがある場所に設定してください。

TFTP サーバーからスイッチにソフトウェア・イメージ・ファイルを転送するには、管理モジュールから Telnet セッションを確立する必要があります。接続が確立されていることを確認するには、TFTP サーバーを ping します。3つのネットワーク・エンティティ（TFTP サーバー、管理モジュール、およびスイッチの IP アドレス）がすべて同じサブネット上にある場合に、Telnet セッションは最適に実行されます。そうでなければ、ルーターを使用する必要があります。管理モジュールのグラフィカル・インターフェースを使用して、管理モジュールの外部ネットワーク・インターフェース（eth0）と Cisco Systems Intelligent Gigabit Ethernet Switch Module の IP アドレスを構成し、これらを TFTP サーバーと同じサブネット上に配置してください。

### TFTP サーバーのインストール

ここでは、ファームウェアを Cisco Systems Intelligent Gigabit Ethernet Switch Module に転送する方法を説明します。数種類の優れた製品が WWW 上で入手できるので、本書でいずれか特定の TFTP 製品の使用を推奨することはありません。ただし、例を示すために本書では SolarWinds TFTP を使用します。SolarWinds の TFTP サーバーは、Microsoft の Windows 95、98、NT、ME、2000、および XP の各オペレーティング・システム上で稼働します。

SolarWinds TFTP は、次の Web サイトから入手しました。

[http://www.solarwinds.net/Tools/Free\\_tools/TFTP\\_Server/](http://www.solarwinds.net/Tools/Free_tools/TFTP_Server/)

「TRY NOW」をクリックし、このページにあるフォームに入力します。ダウンロードしたファイルを実行してコードをインストールし、マシンをリブートします。デフォルト構成では、インストール先のマシンからファイルを転送することができません。次の手順で、SolarWinds を構成します。

1. 「File」→「Configure」をクリックします (図 6-6)。

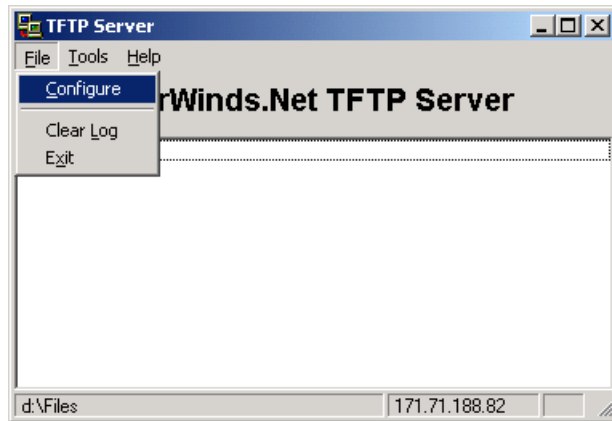


図 6-6 「TFTP Server」 ウィンドウ

2. TFTP ルート・ディレクトリーを、更新する Cisco スイッチ・ファームウェアの場所に変更します (図 6-7)。

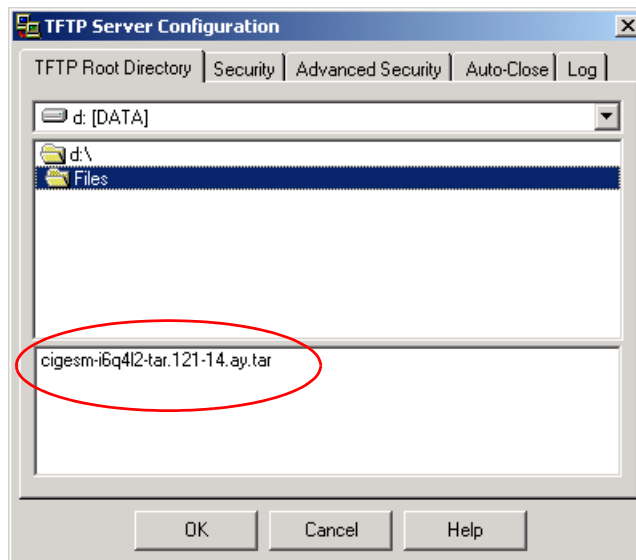


図 6-7 スイッチ・ファームウェアの場所

3. 「**Security**」 タブをクリックし、TFTP サーバーの設定を「**Transmit and Receive files**」に変更します。「**OK**」をクリックして保管します。これで、TFTP サーバーが稼働します。

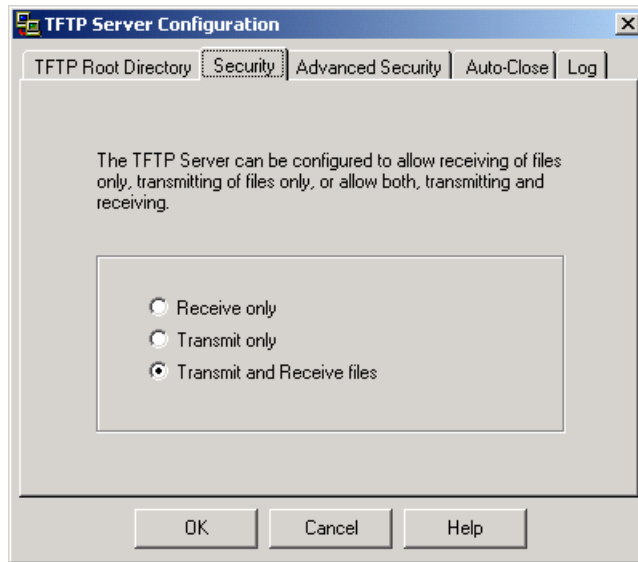


図 6-8 「TFTP Server Configuration」 ウィンドウの「Security」タブ

### コードのアップグレード

Telnet セッションを開始するには、次の手順で説明するように、管理モジュールのグラフィカル・インターフェースを使用します。また、外部スイッチ・ポート上でのリモート管理が使用可能に設定されている場合は、接続されたワークステーションの DOS プロンプトから次のようにして Telnet セッションを開きます。

1. 『管理モジュール Web インターフェースへのアクセス』（85 ページ）で説明したように、管理モジュール Web インターフェースにアクセスしてログオンします。
2. 「I/O Module Tasks」メニューから、「**Management**」をクリックします。「BladeCenter Management Module」ウィンドウが開きます。
3. スイッチが存在するベイの「**Advanced Management**」をクリックします。
4. Telnet セッションを開始するには、「**Start Telnet Session**」をクリックします。

**注：**このアプリケーションを実行するには Java 1.4 プラグインが必要です。インストールされていない場合は、インターネット接続が使用可能ならばプラグインがダウンロードされます。インターネット・セッションが使用可能でない場合は、プラグインを別途ダウンロードし、インストールしてください。

スイッチ・ソフトウェアをアップグレードするには、次の手順で行います。

1. ユーザー ID とパスワードを入力します。ユーザー ID と初期パスワードが割り当てられていない場合は、デフォルトのユーザー ID (USERID) を「User ID」フィールドに入力し、デフォルトのパスワード (PASSWORD、ここで O はゼロ) を「Password」フィールドに入力して、Enter を押します。
2. CLI を使用して、次のコマンドを入力し、Enter を押します。  

```
archive download-sw tftp://xxxx/yyyy
```

(xxxx は TFTP サーバーの IP アドレス、yyyy はダウンロードするイメージ、たとえば cigesm-i6q4l2-tar.121-14.ay.tar)
3. ダウンロードが正常に行われると、次のようなメッセージが表示されます。  

```
New software image installed in flash:/cigesm-i6q4l2-mz.121-14.AY
Configuring system to use new image...done.
```

4. ダウンロードが完了したら、CLI プロンプトに `reload` と入力して Enter を押し、`y` と入力して Enter を押します。

## 6.2 ブレード・サーバーの初期構成

ここでは、IBM eServer BladeCenter HS20 を操作するための準備を行います。

### 6.2.1 ファームウェアの更新

BladeCenter HS20 のファームウェアを更新するには、主に 2 とおりの方法があります。

- ▶ 更新ディスクセット

ファームウェア・ディスクセット・イメージをダウンロードします。更新ディスクセットを作成し、これを使用して HS20 をブートします。更新はそれぞれのファームウェアごとに 1 つずつ実行する必要があります。

- ▶ UpdateXpress CD

IBM UpdateXpress を使用すれば、サーバー・ファームウェアを効率よく容易に更新できます。UpdateXpress は自動開始プログラムを収録した CD で、このプログラムを使用してシステム・ファームウェアと Windows デバイス・ドライバを CD に定義された最新レベルに維持できます。UpdateXpress は、現在適用されているデバイス・ドライバとファームウェアのレベルを自動的に検出して表示します。その後、特定のアップグレードを選択するか、UpdateXpress がアップグレードの必要なものとして検出した項目すべてを自動的に更新するかを指定できます。

### UpdateXpress

この例では、IBM UpdateXpress バージョン 3.03 を使用して、HS20 サーバーのファームウェア更新を実行しています。UpdateXpress V3.03 を入手するには、次の Web サイトにアクセスしてください。

<http://www.ibm.com/pc/support/site.wss/document.do?lnodocid=MIGR-53046>

**注：**更新は必要に応じてリリースされるので、UpdateXpress CD は構成の時点で最新レベルの更新を常に提供するとは限りません。このことは、ファームウェアとデバイス・ドライバの両方に当てはまります。UpdateXpress CD より後にリリースされた更新については、次の IBM Support Web サイトを確認してください。

<http://www.ibm.com/servers/eserver/support/xseries/index.html>

### 始めに

出荷時のままのシステムでない限り、IBM UpdateXpress を開始する前にシステムをバックアップする必要があります。IBM UpdateXpress CD は DOS 始動可能（ブート可能）CD で、この CD を使用してシステムを始動できます。また、ハード・ディスクからサーバーを始動し、サーバーの始動後に CD 上のファイルにアクセスすることもできます。

システムの更新は、必ず次の順序で行ってください。

1. デバイス・ドライバを更新します。（ハード・ディスクから始動し、IBM UpdateXpress CD にアクセスします）
2. ファームウェアを更新します。（UpdateXpress CD から始動します）

ファームウェアを更新する前に、ご使用のサーバーが正常に再始動できることを確認してください。

**注：**この例では、出荷時のままの HS20 システムを使用しました。このため、最初にファームウェアを HS20 サーバーにアップロードしました。HS20 にそれぞれのオペレーティング・システムをロードした後、UpdateXpress を起動し、サポートされるデバイス・ドライバを使用してオペレーティング・システムを更新しました。

### ファームウェアの更新

ここでは、サポートされるサーバー HS20 Type 8832 のファームウェアを更新する作業を行います。このファームウェアを更新するには、次の手順で行います。

1. UpdateXpress CD からシステムを始動します。

**注：**始動可能 CD モードでは、「Help」ボタンは使用できません。オンライン・ヘルプを表示するには、UpdateXpress CD の ¥help¥Xpress ディレクトリーにアクセスしてください。

インストール済みのファームウェア・コンポーネントすべてが表示されます。更新または検証の必要なファームウェア・コンポーネントが存在する場合は、自動的に選択されます。ファームウェアが CD にあるファームウェアと同レベルの場合、そのファームウェアのチェック・ボックスは外されます。

**注：**「Firmware Update」ウィンドウには 60 秒のカウントダウン・タイマーが表示されます。タイマーがゼロに達すると、選択済みのファームウェア・コンポーネントが自動的に更新されます。タイマーを停止するには、いずれかのキーを押してください。

2. 更新するファームウェア・コンポーネントを選択または選択解除します。
3. 「Apply Update」をクリックします。
4. UpdateXpress CD を CD-ROM ドライブから取り出します。その後、サーバーを再始動します。

UpdateXpress がサーバーのファームウェアの更新を完了した後などは、管理モジュール Web インターフェースの「Monitors」→「Firmware VPD」を選択して、現行ファームウェア・レベルを確認する必要があります。95 ページの図 6-9 に示すようなウィンドウが開きます。

BladeCenter Management Module

Bay 1: WMN315795789

▼ Monitors

System Status
Event Log
LEDs
Hardware VPD
**Firmware VPD**

▼ Blade Tasks

Power/Restart
On Demand
Remote Control
Firmware Update
Configuration
Serial Over LAN

▼ I/O Module Tasks

Power/Restart
Management
Firmware Update

▼ MM Control

General Settings
Login Profiles
Alerts
Port Assignments
Network Interfaces
Network Protocols
Security
Configuration File
Firmware Update
Restore Defaults
Restart MM

Log Off

Blade Server Firmware VPD

Bay(s)	Name	Firmware Type	Build ID	Released	Revision
1	SN#ZJ1TS73BC148	BIOS	BSE117AUS	02/24/2004	1.04
		Diagnostics	BSYT13AUS	02/11/2004	1.02
		Blade sys. mgmt. proc.	BR8T30A	n/a	30
2	SN#ZJ1TS73A913Y	BIOS	BSE117AUS	02/24/2004	1.04
		Diagnostics	BSYT13AUS	02/11/2004	1.02
		Blade sys. mgmt. proc.	BR8T30A	n/a	30
3	SN#ZJ1TS73BB103	BIOS	BSE117AUS	02/24/2004	1.04
		Diagnostics	BSYT13AUS	02/11/2004	1.02
		Blade sys. mgmt. proc.	BR8T30A	n/a	30
4	SN#ZJ1TS73AB132	BIOS	BSE117AUS	02/24/2004	1.04
		Diagnostics	BSYT13AUS	02/11/2004	1.02
		Blade sys. mgmt. proc.	BR8T30A	n/a	30

I/O Module Firmware VPD

Bay	Type	Firmware Type	Build ID	Released	Revision
1	Ethernet SM	Boot ROM	BRCSMB12.1	01/15/2004	14E
		Main Application 1	BRCSMI12.1	03/22/2004	14AY

Management Module Firmware VPD

Bay	Name	Firmware Type	Build ID	File Name	Released	Revision
1	WMN315795789	Main application	BRET59D	CNETMNUS.PKT	03-19-04	16
		Boot ROM	BRBR59D	CNETBRUS.PKT	03-19-04	16
		Remote control	BRRG59D	CNETRGUS.PKT	03-19-04	16
2	Redundant MM	Main application	BRET59D	CNETMNUS.PKT	03-19-04	16
		Boot ROM	BRBR59D	CNETBRUS.PKT	03-19-04	16
		Remote control	BRRG59D	CNETRGUS.PKT	03-19-04	16

図 6-9 「BladeCenter Firmware VPD」 ウィンドウ

## 6.2.2 オペレーティング・システム

ここでは、BladeCenter HS20 のために使用するオペレーティング・システムの準備をします。

### Microsoft Windows 2000 Server インストール CD の作成

Microsoft Windows 2000 Server または Advanced Server をインストールするには、Service Pack 3 以降が組み込まれた市販バージョンが必要です。ただし、ユーザーまたはユーザーの顧客がコーポレート契約を結んでいる場合は、CD 更新を受け取ると、最新の Service Pack が組み込まれた Windows 2000 Server CD が提供されます。詳しくは、Microsoft の窓口にお問い合わせください。Microsoft Windows 2000 Server オペレーティング・システムの初期のバージョンは、BladeCenter HS20 にはロードできません。これは、このオペレーティング・システムのビルドに USB ドライバーのサポートが組み込まれていなかったからです。この問題を解決するために、本書の例では Service Pack 3 以降を組み込んだブート可能な Windows 2000 Server CD を作成しました。これらのサービス・パックには、HS20 のロードに必要な USB

ドライバが組み込まれています。Service Pack 3 を含むブート可能 CD-ROM を作成するには、次の手順で行います。

1. Windows 2000 マシン上で、サービス・パックをダウンロードし、/x オプションを指定して（例：W2Ksp3.exe /x）サービス・パックを d:\images\sp3 などのディレクトリーに解凍します。これにより、サービス・パックがインストールされずに解凍されます。このマシンから、新規 CD-ROM イメージを作成することが必要なので注意してください。イメージは次の URL からダウンロードしました。  
<http://www.microsoft.com/windows2000/downloads/servicepacks/sp3/sp3lang.asp>
2. Windows 2000 CD の i386 ディレクトリーを、CD 書き込み機能のあるマシンの d:\images\bootcd\i386 ディレクトリーにコピーします。
3. /s オプションを指定して、d:\images\bootcd ディレクトリーに対してサービス・パックを適用します。次のコマンドを使用しました。  
`d:\images\sp3\update\update /s:d:\images\bootcd`
4. 適切なアプリケーションを使用して、Windows 2000 インストール CD-ROM からブート・セクターを抽出します。いくつかの CD 書き込みアプリケーションにこの機能があります。
5. CD 書き込み機能のあるマシンの d:\images\bootsect ディレクトリーにブート・セクターをコピーします。
6. 次のファイルが d:\images\bootcd ディレクトリーにあることを確認します。存在しないファイルは、オリジナルの CD-ROM から d:\images\bootcd ディレクトリーにコピーする必要があります。
  - CDROM\_NT.5。
  - CDROM\_IA.5、CDROM\_IS.5、または CDROM\_IP.5。これは、Windows 2000 のバージョン (Advanced、Standard、または Professional) によって異なります。
  - CDROMSP3.TST。
  - オプションで、ファイル Autorun.inf、Read1st.me、readme.doc、および setup.exe をオリジナルの CD-ROM からコピーします。
7. ブート可能 CD-ROM の作成が可能な CD ライター・ソフトウェアを使用します。
8. CD ライター・アプリケーションの設定は次のものを使用します。使用する CD ライター・アプリケーションによっては、これらの設定の呼び方が少し異なるか、まったく存在しない場合があります。
  - ロード・セグメントを 07C0 に設定します。
  - セクター・カウントを 4 に設定します。
  - エミュレーション・モードをエミュレーションなしに設定します。
  - Joliet 拡張を使用可能に設定します。
  - CD フォーマットをモード 1 に設定します。
  - ファイル/ディレクトリーの長さを ISO レベル 2 に設定します。
  - ファイル・システムを ISO9660 に設定します。
  - 記録方式としてディスク・アット・ワンスを選択します。
  - d:\images\bootsect ディレクトリーにあるブート・セクター・ファイルを選択します。
9. CD-ROM を書き込んでディスクをファイナライズします。



## UpdateXpress を使用した Windows 2000 デバイス・ドライバのインストール

デバイス・ドライバを BladeCenter HS20 にインストールするには、主に次のような方式があります。

- ▶ 更新ディスクまたはインストーラー・アプリケーション。

ディスク・イメージをダウンロードし、更新ディスクを作成するか、インストーラー・アプリケーションをダウンロードし、インストールを実行します。それぞれのデバイス・ドライバごとに、インストールを行う必要があります。

- ▶ UpdateXpress CD。

UpdateXpress V3.3 は、前にファームウェアのために使用しましたが、Windows Server 2003、Windows 2000 Server、または Windows NT® 4.0 を実行するサポート対象のサーバーのデバイス・ドライバを更新するためにも使用できます。93 ページの 6.2.1、『ファームウェアの更新』を参照してください。

ここでは、UpdateXpress V3.3 を使用して、サポート対象のサーバー (Windows Advanced Server 2000 を実行する HS20 Type 8832) のデバイス・ドライバを更新します。

デバイス・ドライバを更新するには、次の手順で行います。

1. システムを始動します。
2. UpdateXpress CD を CD-ROM ドライブに挿入します。

**注：**CD-ROM が UpdateXpress を自動的に始動しない場合は、DOS を使用して CD の UpdateXpress ディレクトリーまでナビゲートし、launch.exe を実行してください。

UpdateXpress は、検出したサポート対象のデバイス・ドライバをすべて表示します。デバイス・ドライバを更新する必要がない場合は選択不可として表示され、更新する必要がある場合はチェック・マーク付きの項目として表示されます。UpdateXpress によって検出されたインストール済みデバイス・ドライバのバージョンが CD 上のバージョンと同レベルの場合は、チェック・マークのないチェック・ボックスがそのデバイス・ドライバに対して表示されます。

3. 特定のデバイス・ドライバのチェック・ボックスを選択するか、チェック・マークを外します。
4. 「Apply Update」をクリックします。選択したデバイス・ドライバが更新されます。
5. 開いたファイルをすべて保管し、開いたソフトウェアをすべて閉じます。
6. システムを再始動します。

## Microsoft Windows 2000 Broadcom ドライバのインストール

Windows 2000 には、Broadcom Ethernet NIC の実行に必要なドライバが付属していません。NIC を使用可能にするには、ドライバを更新する必要があります。

ご使用の Microsoft Windows 2000 システム用の Broadcom NetXtreme Gigabit Ethernet ドライバを入手するには、次の URL にアクセスします。

<http://www.ibm.com/pc/support/site.wss/document.do?ln docid=MIGR-43815>

本書の例では、この Web サイトから BCM570x ベースのサーバーおよびアダプター用の Broadcom NetXtreme Gigabit Ethernet ソフトウェア CD バージョン 7.0.5 を入手しました。ご



使用のオペレーティング・システム環境をセットアップするには、バージョン 7.0.5 以降を入手する必要があります。このバージョンは、次のマシンをサポートします。

- ▶ BladeCenter HS20 Type 8678 (すべて)
- ▶ IntelliStation E Pro 6216 (すべて)、6226 (すべて)
- ▶ IntelliStation Z Pro 6221 (すべて)
- ▶ IntelliStation M Pro 6219 (すべて)
- ▶ xSeries 205 8480 (すべて)
- ▶ xSeries 225 8647 (すべて)
- ▶ xSeries 235 8671 (すべて)
- ▶ xSeries 255 8685 (すべて)
- ▶ xSeries 305 8673 (すべて)
- ▶ xSeries 335 8676 (すべて)、8830 (すべて)
- ▶ xSeries 440 8687 (すべて)

注：本書の例では、BladeCenter HS20 Type 8832 を使用しています。このタイプはサポート対象のマシンのリストにはありませんが、IBM サポートの検索エンジンによって、BCM570x ベースのサーバーおよびアダプター用 Broadcom NetXtreme Gigabit Ethernet ソフトウェア CD バージョン 7.0.5 の場所が指示されました。ドライバーをロードしたところ、エラーを出さずに正常に機能しました。

## Red Hat Linux AS 2.1 Broadcom ドライバーのインストール

ここでは、Red Hat Linux AS 2.1 をインストールします。オペレーティング・システムのロード後、ネットワーク・ドライバーは即時に機能しました。ただし、最新の Linux 用 Broadcom デバイス・ドライバーをダウンロードし、例 6-1 の指示のとおりに行ってインストールしました。最新の Broadcom デバイス・ドライバーは、次の URL から入手しました。

<http://www.ibm.com/pc/support/site.wss/document.do?lnodocid=MIGR-54186>

例 6-1 HS20 用 Broadcom デバイス・ドライバーの RPM インストール

```
[root@localhost root]# mount /dev/sda /mnt/floppy
[root@localhost root]# ls -al /mnt/floppy
total 285
drwxr-xr-x  2 root  root    7168 Dec 31  1969 .
drwxr-xr-x  4 root  root    4096 Apr 13 16:22 ..
-rwxr-xr-x  1 root  root   279887 Jan  6 20:06 basplnx-6.2.1-1.src.i386.rpm
[root@localhost root]#
[root@localhost root]# cp /mnt/floppy/basplnx-6.2.1-1.src.i386.rpm /tmp
[root@localhost root]#
[root@localhost root]# cd /tmp
[root@localhost tmp]# rpm -ivh basplnx-6.2.1-1.src.i386.rpm
1:basplnx                               ##### [100%]
[root@localhost tmp]#
[root@localhost tmp]# cd /usr/src/redhat/
[root@localhost redhat]#
[root@localhost redhat]# rpm -bb ./SPECS/basplnx.spec
Executing(%prep): /bin/sh -e /var/tmp/rpm-tmp.4397
drwxr-xr-x root/root          0 2004-01-06 12:05:14 ./
-rw-r--r-- root/root       5648 2004-01-06 12:05:13 ./basp.4.gz
-rwxr-xr-x root/root     26544 2004-01-06 12:05:13 ./baspcfg
-rw-r--r-- root/root      1921 2004-01-06 12:05:13 ./baspcfg.8.gz
-rw-r--r-- root/root      2240 2004-01-06 12:05:13 ./bcmtype.h
-rw-r--r-- root/root       6913 2004-01-06 12:05:13 ./blf.c
-rw-r--r-- root/root       1312 2004-01-06 12:05:13 ./blfcore.h
-rw-r--r-- root/root     53116 2004-01-06 12:05:13 ./blfcore.o
-rw-r--r-- root/root        122 2004-01-06 12:05:13 ./blfopt.h
-rw-r--r-- root/root       1795 2004-01-06 12:05:13 ./blfver.h
```

```

-rw-r--r-- root/root      4622 2004-01-06 12:05:14 ./Makefile
drwxr-xr-x root/root          0 2004-01-06 12:05:09 ./nice-2.2.16/
-rw-r--r-- root/root    77592 2004-01-06 12:05:14 ./nice-2.2.16/3c59x.c
-rw-r--r-- root/root    79140 2004-01-06 12:05:14 ./nice-2.2.16/acenic.c
-rw-r--r-- root/root    73926 2004-01-06 12:05:14 ./nice-2.2.16/eeepro100.c
-rw-r--r-- root/root   430585 2004-01-06 12:05:14 ./nice-2.2.16/acenic_firmware.h
-rw-r--r-- root/root    14528 2004-01-06 12:05:14 ./nice-2.2.16/acenic.h
drwxr-xr-x root/root          0 2004-01-06 12:05:09 ./nice-2.4.16/
-rw-r--r-- root/root   101644 2004-01-06 12:05:14 ./nice-2.4.16/3c59x.c
-rw-r--r-- root/root    79195 2004-01-06 12:05:14 ./nice-2.4.16/eeepro100.c
-rw-r--r-- root/root     6194 2004-01-06 12:05:13 ./nicext.h
-rw-r--r-- root/root    60792 2004-01-06 12:05:13 ./pal.c
-rw-r--r-- root/root    11513 2004-01-06 12:05:13 ./pal.h
-rw-r--r-- root/root    22076 2004-01-06 12:05:13 ./readme.txt
-rw-r--r-- root/root    11322 2004-01-06 12:05:13 ./release.txt
drwxr-xr-x root/root          0 2004-01-06 12:05:09 ./scripts/
-rwxr-xr-x root/root     2722 2004-01-06 12:05:14 ./scripts/basp
-rwxr-xr-x root/root     3332 2004-01-06 12:05:14 ./scripts/baspteam
-rwxr-xr-x root/root     3924 2004-01-06 12:05:14 ./scripts/baspiif
-rwxr-xr-x root/root     2729 2004-01-06 12:05:14 ./scripts/team-sample
-rwxr-xr-x root/root     2723 2004-01-06 12:05:14 ./scripts/team-gec
-rwxr-xr-x root/root     2859 2004-01-06 12:05:14 ./scripts/team-vlan
drwxr-xr-x root/root          0 2004-01-06 12:05:14 ./
-rw-r--r-- root/root     5648 2004-01-06 12:05:13 ./basp.4.gz
-rwxr-xr-x root/root    26544 2004-01-06 12:05:13 ./baspcfg
-rw-r--r-- root/root     1921 2004-01-06 12:05:13 ./baspcfg.8.gz
-rw-r--r-- root/root     2240 2004-01-06 12:05:13 ./bcmtypes.h
-rw-r--r-- root/root     6913 2004-01-06 12:05:13 ./blf.c
-rw-r--r-- root/root     1312 2004-01-06 12:05:13 ./blfcore.h
-rw-r--r-- root/root    53116 2004-01-06 12:05:13 ./blfcore.o
-rw-r--r-- root/root      122 2004-01-06 12:05:13 ./blfopt.h
-rw-r--r-- root/root     1795 2004-01-06 12:05:13 ./blfver.h
-rw-r--r-- root/root     4622 2004-01-06 12:05:14 ./Makefile
drwxr-xr-x root/root          0 2004-01-06 12:05:09 ./nice-2.2.16/
-rw-r--r-- root/root    77592 2004-01-06 12:05:14 ./nice-2.2.16/3c59x.c
-rw-r--r-- root/root    79140 2004-01-06 12:05:14 ./nice-2.2.16/acenic.c
-rw-r--r-- root/root    73926 2004-01-06 12:05:14 ./nice-2.2.16/eeepro100.c
-rw-r--r-- root/root   430585 2004-01-06 12:05:14 ./nice-2.2.16/acenic_firmware.h
-rw-r--r-- root/root    14528 2004-01-06 12:05:14 ./nice-2.2.16/acenic.h
drwxr-xr-x root/root          0 2004-01-06 12:05:09 ./nice-2.4.16/
-rw-r--r-- root/root   101644 2004-01-06 12:05:14 ./nice-2.4.16/3c59x.c
-rw-r--r-- root/root    79195 2004-01-06 12:05:14 ./nice-2.4.16/eeepro100.c
-rw-r--r-- root/root     6194 2004-01-06 12:05:13 ./nicext.h
-rw-r--r-- root/root    60792 2004-01-06 12:05:13 ./pal.c
-rw-r--r-- root/root    11513 2004-01-06 12:05:13 ./pal.h
-rw-r--r-- root/root    22076 2004-01-06 12:05:13 ./readme.txt
-rw-r--r-- root/root    11322 2004-01-06 12:05:13 ./release.txt
drwxr-xr-x root/root          0 2004-01-06 12:05:09 ./scripts/
-rwxr-xr-x root/root     2722 2004-01-06 12:05:14 ./scripts/basp
-rwxr-xr-x root/root     3332 2004-01-06 12:05:14 ./scripts/baspteam
-rwxr-xr-x root/root     3924 2004-01-06 12:05:14 ./scripts/baspiif
-rwxr-xr-x root/root     2729 2004-01-06 12:05:14 ./scripts/team-sample
-rwxr-xr-x root/root     2723 2004-01-06 12:05:14 ./scripts/team-gec
-rwxr-xr-x root/root     2859 2004-01-06 12:05:14 ./scripts/team-vlan
Executing(%build): /bin/sh -e /var/tmp/rpm-tmp.4397
gcc -DLINUX -D__KERNEL__ -DMODULE -I/lib/modules/2.4.9-e.24smp/build/include -Wall -Wstrict-prototypes -O2
-c blf.c
gcc -DLINUX -D__KERNEL__ -DMODULE -I/lib/modules/2.4.9-e.24smp/build/include -Wall -Wstrict-prototypes -O2
-c pal.c
ld -r -o basp.o blf.o pal.o blfcore.o

```

```

Executing(%install): /bin/sh -e /var/tmp/rpm-tmp.67022
mkdir -p /var/tmp/basplnx-buildroot/dev
mknod /var/tmp/basplnx-buildroot/dev/basp c 0 0
mkdir -p /var/tmp/basplnx-buildroot/usr/bin
cp -f baspcfg /var/tmp/basplnx-buildroot/usr/bin
mkdir -p /var/tmp/basplnx-buildroot/etc/init.d
cp -f scripts/basp /var/tmp/basplnx-buildroot/etc/init.d
mkdir -p /var/tmp/basplnx-buildroot/etc/basp/samples
cp -f scripts/baspteam /var/tmp/basplnx-buildroot/etc/basp
cp -f scripts/baspif /var/tmp/basplnx-buildroot/etc/basp
cp -f scripts/team-sample /var/tmp/basplnx-buildroot/etc/basp/samples
cp -f scripts/team-gec /var/tmp/basplnx-buildroot/etc/basp/samples
cp -f scripts/team-vlan /var/tmp/basplnx-buildroot/etc/basp/samples
mkdir -p /var/tmp/basplnx-buildroot/usr/src/nice-2.2.16
cp -f nice-2.2.16/* /var/tmp/basplnx-buildroot/usr/src/nice-2.2.16
cp -f nicext.h /var/tmp/basplnx-buildroot/usr/src/nice-2.2.16
mkdir -p /var/tmp/basplnx-buildroot/usr/src/nice-2.4.16
cp -f nice-2.4.16/* /var/tmp/basplnx-buildroot/usr/src/nice-2.4.16
cp -f nicext.h /var/tmp/basplnx-buildroot/usr/src/nice-2.4.16
mkdir -p /var/tmp/basplnx-buildroot/usr/share/man/man4
cp -f basp.4.gz /var/tmp/basplnx-buildroot/usr/share/man/man4
mkdir -p /var/tmp/basplnx-buildroot/usr/share/man/man8
cp -f baspcfg.8.gz /var/tmp/basplnx-buildroot/usr/share/man/man8
mkdir -p /var/tmp/basplnx-buildroot/lib/modules/`uname -r`/kernel/net/basp
cp -f basp.o /var/tmp/basplnx-buildroot/lib/modules/`uname -r`/kernel/net/basp
mkdir -p /var/tmp/basplnx-buildroot/lib/modules/`uname -r`/build/include/linux
cp -f nicext.h /var/tmp/basplnx-buildroot/lib/modules/`uname -r`/build/include/linux
Processing files: basplnx-6.2.1-1
Executing(%doc): /bin/sh -e /var/tmp/rpm-tmp.67022
Finding Provides: (using /usr/lib/rpm/find-provides)...
Finding Requires: (using /usr/lib/rpm/find-requires)...
PreReq: /bin/sh /bin/sh /bin/sh rpmlib(PayloadFilesHavePrefix) <= 4.0-1 rpmlib(CompressedFileNames) <= 3.0.4-1
Requires(interp): /bin/sh /bin/sh /bin/sh
Requires(rpmlib): rpmlib(PayloadFilesHavePrefix) <= 4.0-1 rpmlib(CompressedFileNames) <= 3.0.4-1
Requires(post): /bin/sh
Requires(preun): /bin/sh
Requires(postun): /bin/sh
Requires: ld-linux.so.2 libc.so.6 /bin/sh libc.so.6(GLIBC_2.0) libc.so.6(GLIBC_2.1) libc.so.6(GLIBC_2.1.3)
Wrote: /usr/src/redhat/RPMS/i386/basplnx-6.2.1-1.i386.rpm
Executing(%clean): /bin/sh -e /var/tmp/rpm-tmp.3526

[root@localhost redhat]# rpm -ivh RPMS/i386/basplnx-6.2.1-1.i386.rpm
Preparing... ##### [100%]
 1:basplnx ##### [100%]
[root@localhost redhat]#

```

---

## 6.2.3 Broadcom Advanced Control Suite のインストール

ネットワーク・インターフェース・カード (NIC) チーミングは、IBM eServer サーバーに高可用性とフォールト・トレランスを提供する方式の 1 つです。この例では、Broadcom Advanced Server Program (BASP) を使用して、ロード・バランシング、フォールト・トレランス、および VLAN タグ付けとともにチーミング機能を実装します。

NIC チーミングを使用可能にするには、HS20 上で Broadcom Advanced Control Suite アプリケーションを使用する必要があります。このプログラムはドライバーと一緒に含まれており、次の URL からダウンロードできます。

<http://www.ibm.com/pc/support/site.wss/document.do?lnDocid=MIGR-43815>

スイートをインストールするには、次の手順で行います。

1. Broadcom Advanced Control Suite アプリケーション・ファイルを解凍した場所まで移動します（デフォルトは C:\¥Drivers¥BcomXXX、ここで XXX はコード・レベル）。Launch.exe を実行します。101 ページの図 6-10 に示すようなウィンドウが表示されます。

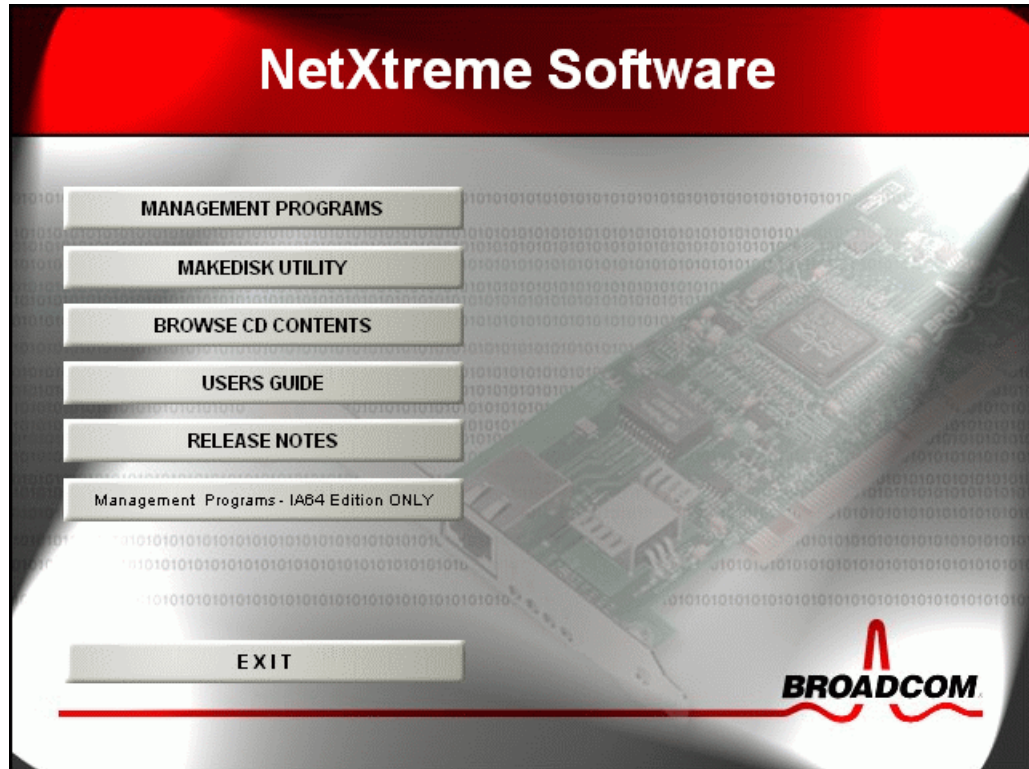


図 6-10 Broadcom 選択ウィンドウ

2. 「MANAGEMENT PROGRAMS」をクリックします。図 6-11 のようなウィンドウが開きます。

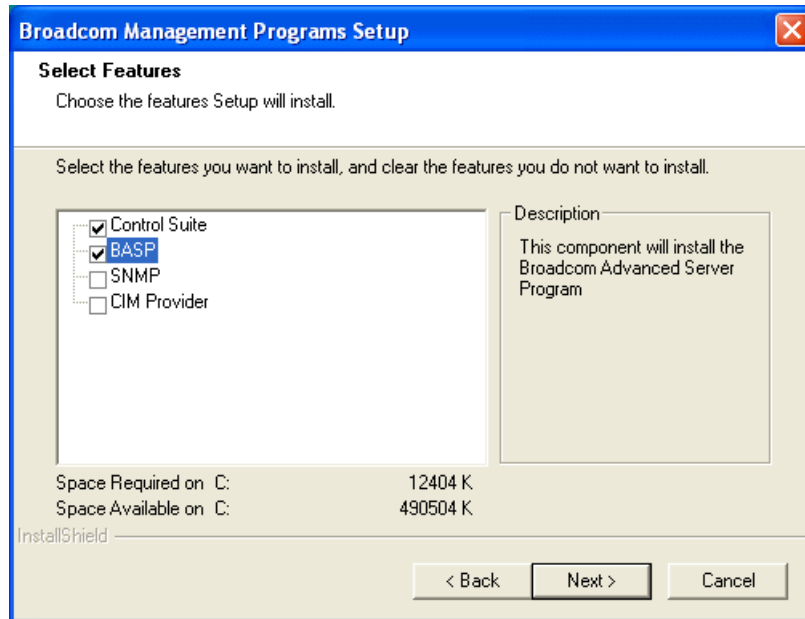


図 6-11 「Select Features」 ウィンドウ

3. 「Control Suite」と「BASP」を選択します。「Next」をクリックして先に進み、「Finish」をクリックします。

## 6.3 この例で使用したファームウェアとデバイス・ドライバー

この例では、次のファームウェアとドライバーを環境に適用しました。

- ▶ IBM eServer BladeCenter 管理モジュール：
  - 管理モジュール・ファームウェア更新バージョン 1.10
- ▶ BladeCenter HS20(8832) ファームウェア
  - BladeCenter HS20 (Type 8832) - フラッシュ BIOS 更新バージョン 1.04
  - BladeCenter HS20 (Type 8678、8832) - ブレード・サーバー統合システム管理プロセスのファームウェア更新バージョン 1.04
  - Broadcom NetXtreme ファームウェア・レベル 3.21
- ▶ Cisco Systems Intelligent Gigabit Ethernet Switch Module ファームウェア：
  - Cisco Systems IGESM ファームウェア・ビルド・レベル 12.1 [14] AY
- ▶ Windows 2000 Advanced Server 用 BladeCenter HS20(8832) デバイス・ドライバー：
  - Broadcom NetXtreme デバイス・ドライバー 7.33.00
  - Broadcom Advanced Server Program 7.12.01
  - Broadcom Advanced Control Suite 7.0.8

(すべて、BCM570x ベースのサーバーおよびアダプター用 Broadcom NetXtreme Gigabit Ethernet ソフトウェア CD バージョン 7.0.5 に含まれる)
- ▶ Red Hat Linux AS 2.1 用 BladeCenter HS20(8832) デバイス・ドライバー：
  - Broadcom BCM5700 Linux ドライバー・バージョン 7.1.22
  - Linux 用 Broadcom Advanced Server Program (BASP) ドライバー・バージョン 6.2.1



## Cisco Systems IGESM の構成 およびネットワーク統合

この章では、組み込みの Cisco Systems Intelligent Gigabit Ethernet Switch Module (Cisco Systems IGESM) を使用して、IBM *@server* BladeCenter をデータ・センター・タイプの環境に組み入れる、数種類のシナリオの構成について解説します。Cisco コマンド行インターフェース (CLI) と Cluster Management Suite (該当する場合) の両方を使用する構成の例を示します。

この章の主な目的は、次の 2 つです。

- ▶ 数種類のトポロジーの例とステップバイステップの構成手順を示します。
- ▶ ブレード・サーバーをこれらのトポロジーに組み込む方法について、例を挙げて説明します。

全般的に、ここに示すブレード・サーバーの構成は、単に *可能な* 構成のオプションと考えてください。

たとえば、4 種類の接続技法を使用する 4 台のブレード・サーバーなどが例に示されていても、1 つの BladeCenter 内でこれらの構成をすべて一度に行うことを承認するものではありません。これらは、可能なオプションのいくつかを示す構成例としてのみ提供されています。

ほとんどの設計と同様に、常にシンプルを心掛けることが成功の秘訣です。

本書ですでに説明したとおり、本書の情報は IOS の 12.1(14) バージョンを実行する 4 ポート銅線ベースの IGESM に適用されます。4 ポート SFP ベースの IGESM、または IGESM 12.1(22) 以上のコードを実行する 4 ポート銅線ベースの IGESM を使用する場合は、これらのソリューションに該当する資料を参照してください。

## 7.1 構成および統合の概要

本書で説明する Cisco Systems IGESM モジュールは、標準ベースのレイヤー 2 スイッチで、レイヤー 2 から 4 の情報に基づいた QoS 機能を備え、Cisco Systems Internet Operating System (IOS) を使用します。このモジュールは、BladeCenter 内での使用に専用化されたホット・プラグ可能モジュールで、従来の Cisco スイッチに関連した機能のほとんどを備えています。

### 7.1.1 Cisco Systems スイッチに習熟したユーザー向けの説明

この節は、IOS を使用する Cisco スイッチに習熟したユーザーを対象としています。Cisco Systems IGESM は、Enhanced Image (EI) ソフトウェアを実行する Cisco 2950 スイッチに備わっている機能セットをベースとしていますが、Cisco Systems IGESM とスタンドアロンの 2950 にはいくつかの違いがあります。この理由は主に、BladeCenter に組み込まれるという性質、および管理モジュールとの相互作用です。

次に、これらの相違点のいくつかについて解説します。

**Cisco Systems IGESM のポートには特定の役割が指定されており、役割は変更できない**

図 7-1 と 105 ページの図 7-2 は、IBM BladeCenter 内の Cisco Systems IGESM に対する 2 種類のポート接続の例を示しています。その後、各種のポート固有の役割と制約事項について説明します。

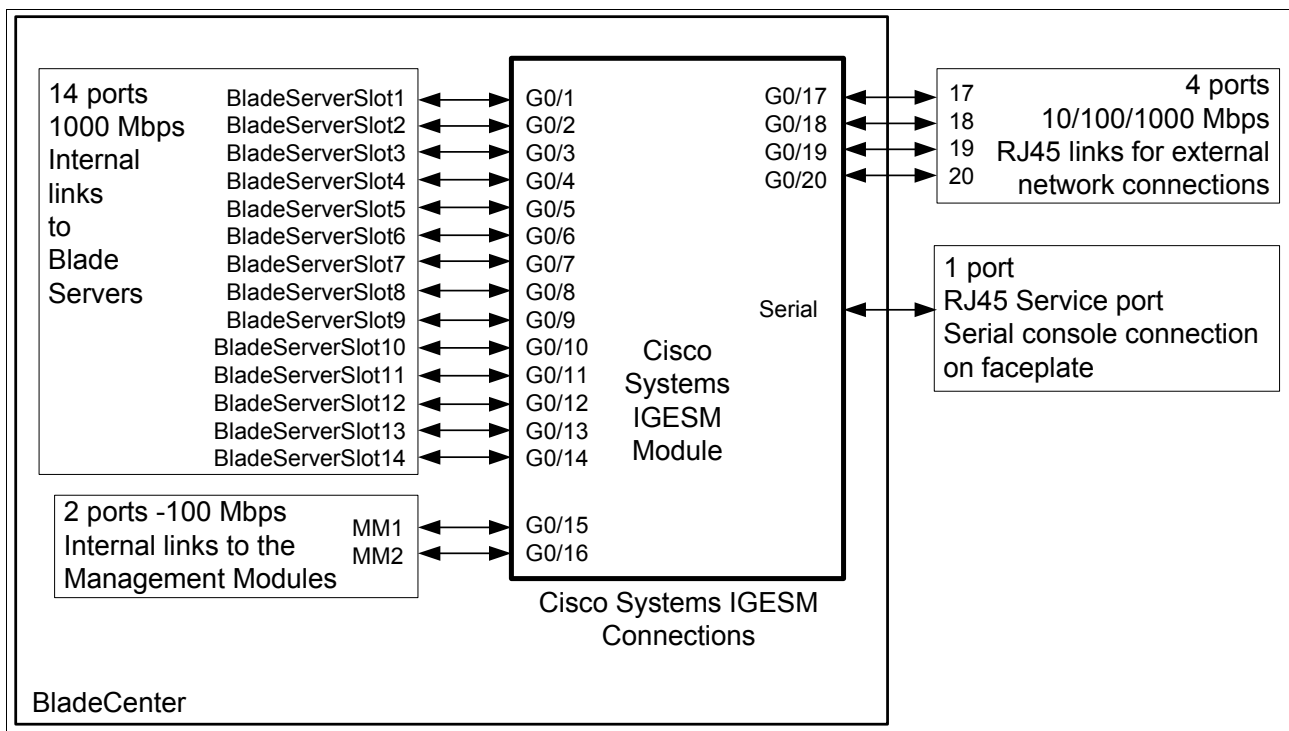


図 7-1 Cisco Systems IGESM 上での接続

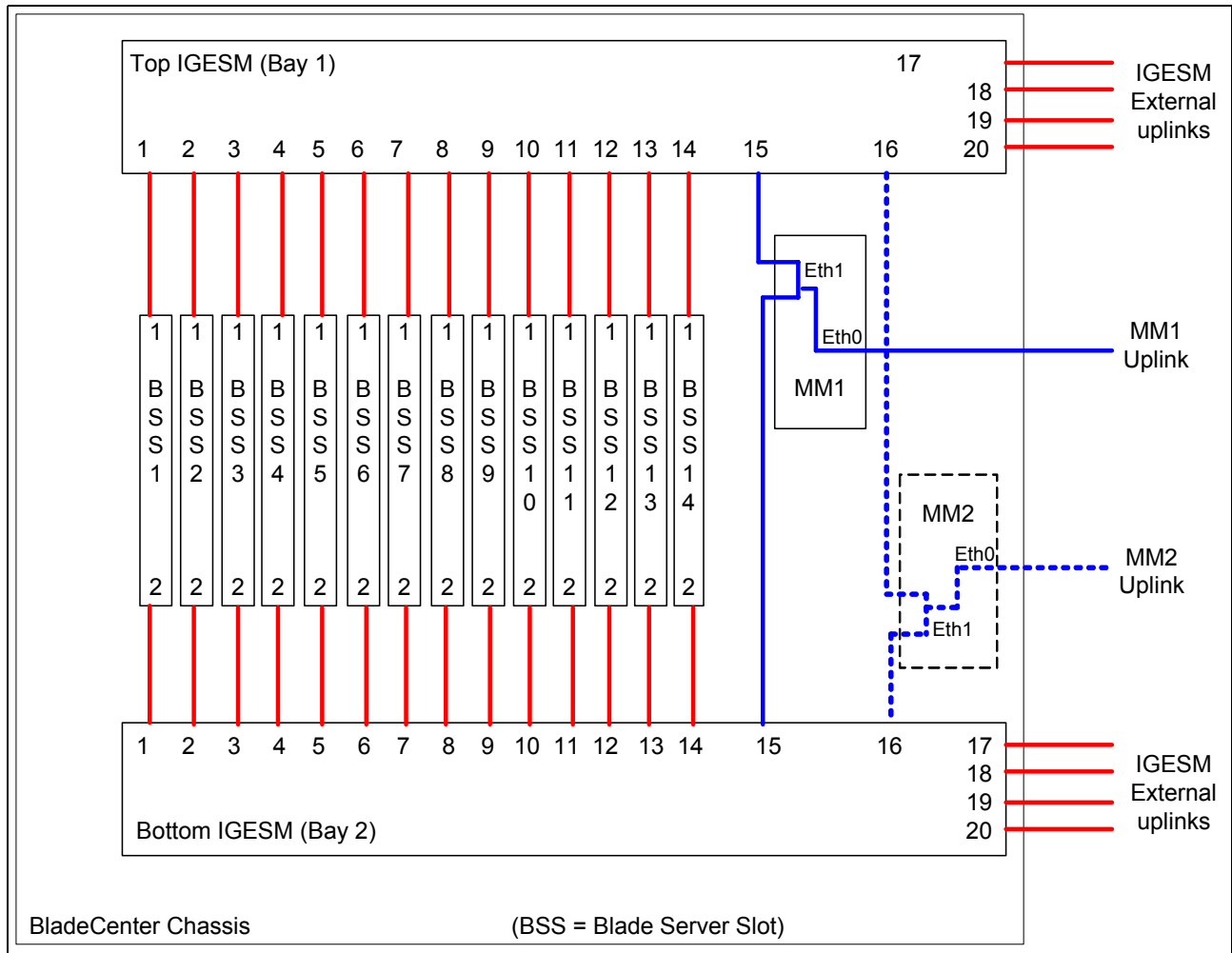


図 7-2 BladeCenter 内でのポート接続の全体図

ポート G0/1 から G0/14: それぞれ、ブレード・サーバーのスロット 1 から 14 に接続します。

- ▶ ブレード・サーバーに接続するポートの事前設定デフォルト値は、次のとおりです (ポート g0/1 から g0/14 を含み、示されているものは g0/1 の場合)。

```
description bladel1
switchport access vlan 2
switchport trunk native vlan 2
switchport trunk allowed vlan 2-4094
switchport mode trunk
spanning-tree portfast trunk
spanning-tree bpduguard enable
```

- ▶ 自動ネゴシエーションにハードコーディング済みですが、ブレード・サーバーに対しては 1000/ 全二重のみをサポートします。この設定は現時点では変更できませんが、コードの将来の改訂により、これらのポートをネゴシエーションなし条件に設定し、リンクを強制的に 1000/ 全二重にする機能がサポートされる可能性があります。
- ▶ ポートはデフォルトでトランク・リンク (switchport mode trunk) として動作し、VLAN 2 から 4094 を伝送します (switchport trunk allowed vlan 2-4094)。

これらのデフォルト (trunk port with native VLAN 2) に変更を加えなければ、特別なソフトウェア (たとえば、この章で後述する BASP チューニング・ソフトウェア) を使用せずにサーバーがこのポートに接続されたとき、サーバーは VLAN 2 上に配置されます。別



の VLAN を使用するには、BASP ソフトウェアを使用してブレード・サーバー側で VLAN を割り当てるか、Cisco Systems IGESM 上のポートを変更してアクセス・ポートにし (**switchport mode access**)、アクセス VLAN を目的の VLAN に設定します (**switchport access vlan x**)。また、デフォルト VLAN をトランクのままにし、ネイティブ VLAN を他の値に変更することによって、デフォルト VLAN を変更することもできます。

- ▶ ブレード・サーバーのポートに対して、Portfast および BPDU フィルターがデフォルトで使用可能に設定されます。Portfast と BPDU フィルターは、ユーザーが使用不可に設定できます。
- ▶ ブレード・サーバーのポートすべてに、その機能と一致したデフォルト記述が提供されています。

ポート G0/15 から G0/16; それぞれ、管理モジュール 1 と 2 に接続します。

- ▶ 管理モジュールに接続するポートの事前設定デフォルト値は、次のとおりです (ポート g0/15 と g0/16 を含み、示されているものは g0/15 の場合)。

```
description mgmt1
switchport trunk allowed vlan 1
switchport mode trunk
switchport nonegotiate
spanning-tree cost 100
```

- ▶ 速度は 100 全二重にハードコーディング済みで、変更できません。
- ▶ ポートの管理シャットダウンを行うことはできません。
  - これは、BladeCenter 管理モジュールへのリンクが管理者の不注意によってダウン状態にならないように、設計によって決められています。
  - これらのポートのどちらか一方 (g0/15 または g0/16) のみが一度にアクティブになる点に注意してください (アクティブな管理モジュールはどの時点でもただ 1 つ)。ほとんどの場合は、管理モジュール 1 に接続するポート 15 がアクティブ・ポートで、ポート 16 は次のように表示されます。

```
GigabitEthernet0/16 is down, line protocol is down (notconnect)
```

- ▶ この g0/16 の状況は、第 2 の管理モジュールがアクティブであるというイベント通知を Cisco Systems IGESM が受け取ったときに限って up/up に変更されます。
- ▶ 両方のポートがトランクとしてハードコーディング済みで、アクセス・ポートに設定することはできません。
- ▶ 管理 VLAN (デフォルトは VLAN 1) は、ポート g0/15 および g0/16 上では常にスパンニング・ツリー転送状態にあります。これは、Cisco Systems IGESM と管理モジュールとの間の通信を確保するためです。その他の VLAN はすべて、ループが検出された場合は STP によってブロック状態になる可能性があります。

アップリンク・ポート (g0/17 から 20) のいずれかに入ったパケットが管理モジュール・ポート (g0/5 から 16) の方向に抜けること、およびその逆を防止する隠しフィルター (管理者が表示または制御できない) が存在することに注意してください。これにより、パケットが無限ループに入らないようになります (スパンニング・ツリー・ループの防止)。

スパンニング・ツリー・ポートのコストは、デフォルトで 100 に設定されます (前述の非管理 VLAN のみに影響)。この値はユーザーが変更できますが、予期しない STP ブロックが発生する可能性があるため、変更しないことをお勧めします。

- ▶ ポート g0/15 と g0/16 の VLAN 特性の変更は、管理 VLAN の変更によってのみ可能です。別の管理 VLAN をアクティブにすると (たとえば、新規 VLAN を作成し、新規 VLAN インターフェースを作成してから、**no shut** を実行する)、ポート g0/15 と g0/16 はこの VLAN を自動的にネイティブ VLAN にし、これらのポートのトランク・リンクを通過で

きるようにします (switchport trunk allowed vlan X)。これは設計によって決まっており、これら 2 つのポートのネイティブ VLAN 設定を制御する方法はこれだけです。

ポート G0/17 から G0/20: それぞれ、外部ポート 17 から 20 に接続します。

- ▶ 外部接続に向かうポートの事前設定デフォルト値は、次のとおりです (ポート g0/17 から g0/20 を含み、示されているものはポート g0/17 の場合)。

```
description extern1
switchport trunk native vlan 2
```

- ▶ これらのポートのデフォルトは、新規 BladeCenter の場合は **shutdown** です。これらのポートを初めて起動する場合は、管理モジュール Web インターフェースを使用し、「I/O tasks」、「Advanced settings」のもとで「External Ports」を「Enabled」に設定する必要があります。

管理モジュールを使用してこれらのポートを使用可能に設定しなければ、**no shutdown** を実行しようとしたときに、% Shutdown not allowed on this interface というエラー・メッセージが表示されます。このメッセージが出ないようにするには、管理モジュールにログインし、それぞれの IGESM ごとに「Advanced Settings」に進んで、「External ports」を「Enabled」に設定する必要があります。

- ▶ デフォルトのネイティブ VLAN は 2 に設定されます。

RJ45 サービス・ポート:

- ▶ これは、ほとんどの Cisco 製品に備わっている標準の RJ45 シリアル・コンソール・ポートです。
  - デフォルト設定値: 9600、N、8、1
  - 最高 115,200 bps までの速度をサポート
- ▶ 初期の出荷時には、キャップ・プレートがコンソール・ポートの RJ45 ジャックに取り付けられており、ケーブルを挿入する前にこのプレートを取り外す必要があります。このキャップは、担当者以外がこのポートにイーサネット・ケーブルを接続する可能性を減らすためのものです。

このポートの使用上起こりうる問題と予備手段については、『Hyperterm からのコンソールポートアクセスに関する問題』(249 ページ) を参照してください。

**重要:** 前に示したデフォルトのポート設定値は、Cisco Systems IGESM 上で **write erase/reload** を実行した後に作成されます。**default int** コマンドを config term モードで使用しても、ここに示したような結果は得られず、デフォルトに設定されるポートからすべての構成が完全に除去されるので注意してください。この違いにより、**default int** コマンドは Cisco Systems IGESM 上では注意して使用する必要があります。

## write erase 後のデフォルト値は他のほとんどの Cisco スイッチと異なる

前述のとおり、Cisco Systems IGESM によって使用されるデフォルト・インターフェース値は、他のほとんどの Cisco スイッチとは異なります。前に示したインターフェースのデフォルト値のほかに、Cisco Systems IGESM によって使用される標準的でない Cisco デフォルト値のいくつかを次のリストに示します。

- ▶ SNMP のデフォルト値:
  - snmp-server community public RO
  - snmp-server community private RW

- ▶ ほとんどの Cisco スイッチのデフォルト値は、単一の VLAN (VLAN1) です。Cisco Systems IGESM には、次の 2 つのデフォルト VLAN があります。
  - 管理 - VLAN 1
  - 操作 - VLAN 2

本書の別の個所で説明したとおり、デフォルトではブレード・サーバー・ポートから VLAN 1 が除去されています。これは、ブレード・サーバーと Cisco Systems IGESM の管理 VLAN の間で分離を維持するために重要です。

このことが重要である理由について詳しくは、56 ページの 5.3、『管理パスに関する詳細説明』を参照してください。
- ▶ スパニング・ツリーのデフォルト設定値：
  - spanning-tree mode rapid-pvst

Rapid-PVST は、レイヤー 2 ネットワークの問題から迅速にリカバリーするために 802.1w を実装しています。この同じ高速リカバリーを実行するために、802.1w より前では追加のコマンドを多数実行する必要がありましたが、その必要はなくなりました。

  - no spanning-tree optimize bpdu transmission
  - spanning-tree extend system-id
- ▶ デフォルト・ユーザー（ユーザー名は USERID、パスワードは PASSWORD で、O の代わりに数字のゼロ）が作成されます。
  - username USERID privilege 15 secret 5 \$1\$7/1C\$.lbXvHc5lyBHDzAZ9WpfT0

## 管理 VLAN の IP アドレス情報は write erase 時に失われない

管理モジュールの特定の機能（入出力モジュールの「Advanced Setup」にある）を使用可能に設定すると、その直接の効果として、Cisco Systems IGESM がクリアされた後（write erase/reload または GUI を使用して）、BladeCenter 管理モジュールはその Cisco Systems IGESM に関して現在保管されている IP 情報を提供できるようになります。この目的は、管理モジュールから Cisco Systems IGESM へのアクセスを常に確保することです。このアクション（Cisco Systems IGESM にデフォルト・アドレスを提供する、または提供しない）は、管理モジュール Web インターフェースから部分的に制御できます（「Preserve new IP configuration on all resets」という機能を使用可能または使用不可に設定する方法について詳しくは、『IGESM IP アドレス情報の制御』（250 ページ）を参照してください）。

また、この設定を使用不可に変更する場合は、IGESM 自身のアップリンクを経由して IGESM を管理する予定であることが前提になります。この理由について詳しくは、63 ページの 5.3.5、『考慮事項：IGESM アップリンクを使用した IGESM の管理』を参照してください。

新規 BladeCenter に対して管理モジュールが提供するデフォルトの Cisco Systems IGESM IP アドレッシングは、次のとおりです。

- ▶ スイッチ・ベイ 1: 192.168.70.127/24
- ▶ スイッチ・ベイ 2: 192.168.70.128/24
- ▶ スイッチ・ベイ 3: 192.168.70.129/24
- ▶ スイッチ・ベイ 4: 192.168.70.130/24

BladeCenter 内で相互作用が生じるため、通常は Cisco Systems IGESM 上で管理 IP アドレスを直接変更することはお勧めしません。代わりに、必ず管理モジュールの Web ベース GUI を使用して変更するようにしてください。

特に、Cisco Systems IGESM の CLI を使用してアドレスを同じサブネット上の別のアドレスに変更すると、重複する IP アドレスが実際には存在しないにもかかわらず報告される状態

が発生することがあります。これは、Cisco Systems IGESM の内部ポートからその IP サブネット上のいずれかのアドレスに対して出されたアドレス解決プロトコル (ARP) 要求に、管理モジュールが応答するために起こります。この状態が発生しないようにするには、Cisco Systems IGESM の IP アドレスの変更を必ず管理モジュール GUI から行ってください。詳しくは、239 ページの付録 A、『ヒント』を参照してください。

管理モジュール GUI の使用法については、84 ページの 6.1.2、『管理モジュールのネットワーク・インターフェース』を参照してください。

## 7.2 管理ネットワークに関する考慮事項

ここでは、BladeCenter に関する非常に重要なトピックである、管理 VLAN の選択と BladeCenter 内での使用について解説します。

BladeCenter には管理 VLAN に関する具体的な要件がいくつかありますが、まず管理トラフィックに適した VLAN を選択することの重要さと、この選択にネイティブ VLAN が果たす役割について、あらかじめ全般的に理解しておく役に立ちます。管理 VLAN とネイティブ VLAN の選択に関する分かりやすい解説については、『Best Practices』資料の「Switch Management Interface and Native VLAN」の節を参照してください（このためには、Cisco のユーザー ID とパスワードが必要です）。この資料は、次の URL で入手できます。

[http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products\\_white\\_paper09186a00801b49a4.shtml](http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products_white_paper09186a00801b49a4.shtml)

BladeCenter 内で IGESM を使用する際の管理ネットワークの構成について具体的な情報を入力するには、56 ページの 5.3、『管理パスに関する詳細説明』を参照してください。

### BladeCenter 特有の観点から見た管理 VLAN

BladeCenter に関する説明では、管理 VLAN はそれぞれの Cisco Systems IGESM 上にあるただ 1 つのアクティブ VLAN インターフェース（デフォルトは VLAN 1）を指し、スイッチを管理するために可能な方法の 1 つとして IP 経由での接続に使用されます。この同じ管理 VLAN は、Cisco Systems IGESM のポート g0/15 と g0/16 に直接結合され、これによって Cisco Systems IGESM を管理モジュールに接続します。

管理モジュールには特定の役割があり、その役割の 1 つは、Cisco Systems IGESM を管理するために管理モジュール経由で Cisco Systems IGESM に接続できるようにすることです。この役割の副次作用として、管理モジュールは Cisco Systems IGESM への内部接続上で、現行サブネット内にあるすべてのアドレスに対する ARP 要求に応答します（Cisco Systems IGESM のプロキシとして動作する）。ブレード・サーバーが同じ VLAN 上の同じ IP サブネット内にある場合は、自身のアドレスを所有するものが存在しないことをブレード・サーバーが確認する際に、管理モジュールがブレード・サーバーの ARP に応答し、結果として通常は重複 IP アドレスが報告されます。詳しくは、76 ページの 5.3.12、『シナリオ 6（非推奨）』を参照してください。

もう 1 つの副次作用は、DHCP クライアントとして稼働するブレード・サーバーが IGESM 管理 VLAN に配置されたときに発生します。ほとんどの場合、DHCP サーバーが IP アドレスをクライアントに発行する前に、そのアドレスがすでに使用中かどうかを検査する Gratuitous ARP を送信します。管理モジュールがこの Gratuitous ARP を内部インターフェース上で検出すると、そのアドレスを所有していると応答し（サブネットのプロキシとして動作しているため）、DHCP サーバーはそのアドレスに使用中のマークを付け、別の IP アドレスの使用を試みます（同じ結果になります）。結果として、DHCP プールが使い尽くされ、サブネット上で使用可能な IP アドレスがなくなります。

内部管理ネットワークの設計によって生じるさらにもう 1 つの副次作用は、管理モジュールが少なくとも一部のパケットのブリッジとなることです。（Cisco Systems IGESM 上で **show cdp neighbor** コマンドを実行すると、実際には管理モジュール経由のブリッジ接続であっても、他の Cisco Systems IGESM が直接接続されているものとして示されます）

このことを念頭に置いて、次に示す 1 つの単純な規則を守ることを強くお勧めします。

*BladeCenter 内のブレード・サーバーは、Cisco Systems IGESM によって使用されている管理 VLAN から常に分離すること。*

このために、Cisco Systems IGESM のデフォルト構成では VLAN 1 がブレード・サーバー・ポートから分離されています。ただしこの構成は、VLAN 1 をブレード・サーバー・ポートに単に追加することは禁止していません。

管理 VLAN のデフォルト VLAN は 1 なので、前述の規則に基づいて、ブレード・サーバーを VLAN 1 に配置しないでください。

管理 VLAN を 1 以外のものに変更する場合は（新規 VLAN を作成して、その新規 VLAN へのインターフェースを作成し、新規インターフェースに対して **no shutdown** を実行する）、ブレード・サーバーをこの新規 VLAN に配置しないでください。

管理 VLAN とネイティブ VLAN の選択に関する前述の「Best Practices」資料には、管理トラフィックとユーザー・トラフィックの分離を保つ理由が他にもいくつか示されていますが、それらを差し置いても BladeCenter の要件は、これらのネットワーク（管理 VLAN と、ブレード・サーバーによって使用される VLAN）の分離を保つ必要がある重大な理由であるといえます。

## Cisco Systems IGESM を管理するためのパス

BladeCenter 内の Cisco Systems IGESM を管理するために使用できるさまざまなパスについては、56 ページの 5.3、『管理パスに関する詳細説明』を参照してください。

## 7.3 この章で使用される例の基本構成

この環境で使用できる構成の組み合わせを具体的に説明する前に、本書の制作時に使用された構成と操作の基本をいくつか説明する必要があります。

### 7.3.1 本書の制作に使用されたハードウェアとソフトウェア

次に、本書の制作時に使用されたハードウェアとソフトウェアのリストを示します。6500 とそのコンポーネントの選択は、高可用性とハイパフォーマンスを最も重視する、ミッション・クリティカルなデータ・センター環境に BladeCenter を配置することを想定して行われたことに注意してください。

#### **IBM eServer BladeCenter の構成**

BladeCenter の構成は次のとおりです。

- ▶ それぞれ次のものを装備する、2 つの IBM eServer BladeCenter シャーシ（8677-1xx）
  - BladeCenter シャーシごとに 5 つの HS20（8832-21x）
    - 2 つの 2.8 Ghz CPU（#73P5983）アップグレード
    - 1 つの 40 GB ハード・ディスク（#48P7063）
    - 2 つの 256 MB DIMM および 2 つの 1 GB DIMM（#33L5039）アップグレード

- 1 つの Gigabit Ethernet 拡張カード (#73P9030) (この章の制作時には不使用)
- BladeCenter シャーシごとに 4 つの 1800 ワット・パワー・サプライ (#13N0570) アップグレード
- 2 つの Cisco Systems Intelligent Gigabit Ethernet Switch Module (#13N2281)
- 2 つの BladeCenter 管理モジュール (#48P7055)

### **Cisco Systems Intelligent Gigabit Ethernet Switch Module**

次のコードを実行する、2 つの Cisco Systems IGESM を使用します。

▶ IOS バージョン : 12.1(14)AY

イメージ名 : cigesm-i6q4l2-mz.121-14.AY.bin

本書の最新の更新時点で利用可能なコードの現行改訂は、12.1(14)AY4 です。最新のバグ修正がすべて適用され、新機能が利用可能になるように、この改訂、またはこれより新しい改訂をインストールすることを強くお勧めします。

### **Cisco Catalyst 6500 スイッチのハードウェアとソフトウェア**

それぞれ次のものを備えた、2 つの Cisco Catalyst 6509 を使用します。

▶ IOS バージョン : 12.2(17d)SXB

イメージ名 : s72033-jk9sv-mz.122-17d.SXB.bin

▶ スロット 2 のモジュール : 48 CEF720 48 ポート 10/100/1000mb イーサネット

- 型式番号 : WS-X6748-GE-TX
  - ハードウェア : 1.4
  - ファームウェア : 12.2(14r)S5
  - ソフトウェア : 12.2(17d)SXB
- サブモジュール : Centralized Forwarding Card - WS-F6700-CFC (Hw 2.0)

▶ スロット 5 のモジュール : Supervisor Engine 720

- 型式番号 : WS-SUP720-BASE
  - ハードウェア : 2.1
  - ファームウェア : 7.7(1)
  - ソフトウェア : 12.2(17d)SXB
- サブモジュール : Policy Feature Card 3 - WS-F6K-PFC3A (Hw 1.1)
- サブモジュール : MSFC3 ドーターボード - WS-SUP720 (Hw 1.2)

▶ スロット 6 のモジュール : CEF720 4 ポート 10 Gigabit Ethernet

- 型式番号 : WS-X6704-10GE
  - ハードウェア : 1.2
  - ファームウェア : 12.2(14r)S5
  - ソフトウェア : 12.2(17d)SXB
- サブモジュール : Centralized Forwarding Card - WS-F6700-CFC (Hw 1.1)
- 2 つの 10GBASE-LR XENPAK モジュール

▶ 1 つの DS-CAC-2500W パワー・サプライ

▶ 1 つの WS-C6K-9SLOT-FAN2 ファン・トレイ

## **7.3.2 事前構成の準備 (基本構成情報)**

すべての構成とテストは、クリーン・システム上で行われました。Cisco Systems IGESM および 6500 の場合は、装置を出荷時のデフォルト値に復元するために、CLI インターフェー

ス・コマンド **write erase** を使用し、vlan.dat ファイルを削除し、スイッチに対して **reload** を実行しました。

**重要:** 前述の操作を実行すると、ここに示したデバイスの構成データがすべて失われるため、実動システム上で行った場合はネットワークのダウン時間が発生します。これらのコマンドをここに記載した目的は、本書のためのテストを研究所で開始する前に行った準備作業を紹介することのみです。

**重要:** 実動ネットワーク内で作業する場合は、発行するコマンドの影響を必ず理解しておいてください。コマンドの動作を完全に理解していなければ、ネットワークがダウン状態になる可能性があります。

**注:** 使用可能な機能とコマンド構文は、コードのバージョンによって異なることがあります。本書は、前述したコードの改訂からの機能と構文を使用して制作されたので、他の改訂とは異なっている場合があります。当該製品に使用できる機能とコマンドの完全な最新リストについては、IBM または Cisco の Web サイトをご覧ください。

## すべての例に共通する基本構成オプション

ここでは、すべての例に共通して設定される構成オプションのいくつかをリストします。これらはデモンストレーションのみを目的としており、個々のユーザーの環境では同じものを使用できる場合もできない場合もあります。

すべての構成例では、次に示す VLAN からいくつかを組み合わせて構成します。VLAN 2、10、15、20、25、30、35、40、45、および 50

次に示すブレード・サーバーに、VLAN が次のように配置されます（正確な番号と配置は、それぞれの例のトランキングや SLB チューニングなどによって異なります）。

- ▶ BladeServer1: VLAN 10、15、20、25
- ▶ BladeServer2: VLAN 10、20
- ▶ BladeServer3: VLAN 30
- ▶ BladeServer4: VLAN 35、40、45、50

**注:** ここで選択されている VLAN は、デモンストレーションのみを目的としており、個々のユーザーのネットワークには存在する場合もしない場合もあります。

すべての構成で、VLAN 2 が g0/15 および g0/16 を除くすべてのトランク・リンクのネイティブ VLAN である（ネイティブ VLAN にはタグが付かない）ことを前提としています（これは、Cisco Systems IGESM のデフォルトです）。

すべての構成で、トランクによって伝送される VLAN は、必要なものだけに限られていることを前提としています（これはセキュリティ上推奨されます）。

ここに示した構成はすべて、6500-1 を強制的にすべての VLAN のスパンニング・ツリー・ルートにしています。既存のネットワーク上で、目的のスイッチ（VLAN のロード・バランシングを行っている場合は複数のスイッチ）がすでにルートとして構成されていることがよくあります。ルート・ブリッジの正しい選択方法を理解していることは非常に重要で、Cisco Systems IGESM をルート・ブリッジにすることはお勧めしません。Cisco Systems IGESM がルート・ブリッジになると、レイヤー 2 ネットワーク内のデータ・フローが最適でなくなる可能性があります。

## Cisco Systems IGESM の基本構成

構成を消去した後、例の構成に合うように Cisco Systems IGESM1 と Cisco Systems IGESM2 を準備するために必要な作業は、次に示す 2 つだけです。

- ▶ **config term** モードで、それぞれの Cisco Systems IGESM に正しいホスト名を追加します。
  - Cisco Systems IGESM1 に対して : **hostname CIGESM1**
  - Cisco Systems IGESM2 に対して : **hostname CIGESM2**
- ▶ それぞれのサーバーを IBMLAB VTP ドメインに配置します。
  - それぞれの Cisco Systems IGESM に対して : **vtp domain IBMLAB**

新品の BladeCenter の場合は、管理モジュールに接続し、それぞれの IGESM ごとに「I/O module tasks」の「Advanced Settings」に進み、少なくとも一度は「External Ports」を「Enable」（デフォルトは「Disabled」）に設定する必要があります。

### 管理モジュール Web インターフェースの使用

管理モジュール Web インターフェースを使用して、Cisco Systems IGESM の外部ポートを初めて使用可能に設定するには、次の手順で行います。

1. ペイ 1 の管理モジュールの外部 IP アドレス（デフォルトは 192.168.70.125）をブラウザに指定し、次の信用証明情報を使用してログオンします。ID=USERID、Password=PASSWORD（ここで、パスワードの中の 0 は数字のゼロ）
2. ウィンドウの左側の「I/O module tasks」の下で、「Management」をクリックします。
3. ウィンドウの右側で、「Bay 1」を選択し、「Advanced Management」を選択します。
4. ウィンドウの右側にある「Advanced Setup」の下で、「External Ports」を「Enable」に変更し、「Save」をクリックします。
5. 他の Cisco Systems IGESM に対して手順を繰り返します。

## Cat 6500 の基本構成

それぞれの例では、Cisco Systems IGESM の構成は消去されており、それぞれの例を開始する前に基本構成が適用されました。6500 の場合は、スイッチは出荷時のデフォルト値にリセットされました。その後、すでに存在する Cisco ネットワークをシミュレートするために、次の構成が適用されました（前述のとおり、これは単なる例であり、ユーザーの実動ネットワークとは異なると考えられます）。

この基本構成については、次のようにいくつかの注意点があります。

- ▶ VLAN 2 は両方のスイッチに事前に追加済みです。
- ▶ VLAN 10、15、20、25、20、25、40、45、および 50 がすでに作成済みです。
- ▶ 外部スイッチ上で *ping* 可能なポイントを提供する目的で、L3 インターフェースがそれぞれの VLAN（10、15、20 など）ごとに作成済みです。
- ▶ ブレード・サーバーには通常、少なくとも 1 つのデフォルト・ゲートウェイがあります。使用するデフォルト・ゲートウェイの数の選択はユーザーの任意ですが（このことについて詳しくは、『マルチホーム・サーバー上でのデフォルト・ゲートウェイの構成』（240 ページ）を参照）、この構成ではデフォルト・ゲートウェイ・アドレスに Hot Standby Router Protocol（HSRP）を使用する必要があります。これは、デフォルト・ゲートウェイを指示するブレード・サーバーの高可用性を保つために役立ちます。この例で



は、デフォルト・ゲートウェイは 6500 上に配置され、他のネットワークへのパスがブレード・サーバーに常に存在するように、両方の 6500 上で HSRP が構成されています。

- ▶ 6500-1 の基本構成に使用される IP アドレスは、次のとおりです。
  - 6500-1、VLAN 10 アドレス : 10.1.10.251/24  
HSRP アドレス : 10.1.10.254/24
  - 6500-1、VLAN 15 アドレス : 10.1.15.251/24  
HSRP アドレス : 10.1.15.254/24
  - 6500-1、VLAN 20 アドレス : 10.1.20.251/24  
HSRP アドレス : 10.1.20.254/24
  - 6500-1、VLAN 25 アドレス : 10.1.25.251/24  
HSRP アドレス : 10.1.25.254/24
  - 6500-1、VLAN 30 アドレス : 10.1.30.251/24  
HSRP アドレス : 10.1.30.254/24
  - 6500-1、VLAN 35 アドレス : 10.1.35.251/24  
HSRP アドレス : 10.1.35.254/24
  - 6500-1、VLAN 40 アドレス : 10.1.40.251/24  
HSRP アドレス : 10.1.40.254/24
  - 6500-1、VLAN 45 アドレス : 10.1.45.251/24  
HSRP アドレス : 10.1.45.254/24
  - 6500-1、VLAN 50 アドレス : 10.1.50.251/24  
HSRP アドレス : 10.1.50.254/24
- ▶ 6500-3 の基本構成に使用される IP アドレスは、次のとおりです。
  - 6500-3、VLAN 10 アドレス : 10.1.10.253/24  
HSRP アドレス : 10.1.10.254/24
  - 6500-3、VLAN 15 アドレス : 10.1.15.253/24  
HSRP アドレス : 10.1.15.254/24
  - 6500-3、VLAN 20 アドレス : 10.1.20.253/24  
HSRP アドレス : 10.1.20.254/24
  - 6500-3、VLAN 25 アドレス : 10.1.25.253/24  
HSRP アドレス : 10.1.25.254/24
  - 6500-3、VLAN 30 アドレス : 10.1.30.253/24  
HSRP アドレス : 10.1.30.254/24
  - 6500-3、VLAN 35 アドレス : 10.1.35.253/24  
HSRP アドレス : 10.1.35.254/24
  - 6500-3、VLAN 40 アドレス : 10.1.40.253/24  
HSRP アドレス : 10.1.40.254/24
  - 6500-3、VLAN 45 アドレス : 10.1.45.253/24  
HSRP アドレス : 10.1.45.254/24

– 6500-3、VLAN 50 アドレス : 10.1.50.253/24

HSRP アドレス : 10.1.50.254/24

- ▶ この例では、基本構成の一部として、6500-1 という名前のスイッチが強制的に 1 次ルート・スイッチになります。このためには、**spanning-tree vlan X,Y,Z root primary** コマンドを実行します。ただし、X、Y、および Z は、スイッチ上で使用される VLAN です。6500-3 は、**spanning-tree vlan X,Y,Z root secondary** として構成されます。
- ▶ VTP ドメイン名は、基本構成の一部として IBMLAB に設定されます。データ・センター全体で同じ VTP ドメイン・ネームを使用することをお勧めします。また、基本構成の一部として、両方の 6500 が VTP 透過モードに設定されます。

### 6500-1 の基本構成

例 7-1 は、6500-1 の実行構成を簡略に示したリストで、それぞれの例に使用される基本構成を示しています。次の例で使用されている基本インターフェースすべてに対して、**no shutdown** コマンドが発行されていることに注意してください。

#### 例 7-1 6500-1 の基本構成

---

```
hostname DC6500-1
!
vtp domain IBMLAB
vtp mode transparent
!
spanning-tree mode rapid-pvst
spanning-tree vlan 1-2,10,15,20,25,30,35,40,45,50 priority 8192
!
enable password ese
!
vlan 2
!
vlan 10
    name Web
!
vlan 15
    name User
!
vlan 20
    name Application
!
vlan 25
    name Backup
!
vlan 30,35,40,45,50
!
interface Port-channel1
    switchport
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan 1,2,10,15,20,25,30,35,40,45,50
    switchport mode trunk
    switchport nonegotiate
!
interface TenGigabitEthernet6/1
    no ip address
    switchport
    switchport trunk encapsulation dot1q
    switchport trunk allowed vlan 1,2,10,15,20,25,30,35,40,45,50
    switchport mode trunk
    switchport nonegotiate
    channel-group 1 mode active
```

```

no shutdown
!
interface TenGigabitEthernet6/2
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2,10,15,20,25,30,35,40,45,50
switchport mode trunk
switchport nonegotiate
channel-group 1 mode active
no shutdown
!
interface Vlan1
ip address 192.168.70.1 255.255.255.0
no ip redirects
no shutdown
!
interface Vlan10
ip address 10.1.10.251 255.255.255.0
no ip redirects
no ip proxy-arp
arp timeout 200
standby 1 ip 10.1.10.254
standby 1 timers 1 3
standby 1 priority 110
standby 1 preempt delay minimum 60
standby 1 authentication cisco
no shutdown
!
interface Vlan15
ip address 10.1.15.251 255.255.255.0
no ip redirects
no ip proxy-arp
arp timeout 200
standby 1 ip 10.1.15.254
standby 1 timers 1 3
standby 1 priority 110
standby 1 preempt delay minimum 60
standby 1 authentication cisco
no shutdown
!
interface Vlan20
ip address 10.1.20.251 255.255.255.0
no ip redirects
no ip proxy-arp
arp timeout 200
standby 1 ip 10.1.20.254
standby 1 timers 1 3
standby 1 priority 110
standby 1 preempt delay minimum 60
standby 1 authentication cisco
no shutdown
!
interface Vlan25
ip address 10.1.25.251 255.255.255.0
no ip redirects
no ip proxy-arp
arp timeout 200
standby 1 ip 10.1.25.254
standby 1 timers 1 3

```

```

standby 1 priority 110
standby 1 preempt delay minimum 60
standby 1 authentication cisco
no shutdown
!
interface Vlan30
ip address 10.1.30.251 255.255.255.0
no ip redirects
no ip proxy-arp
arp timeout 200
standby 1 ip 10.1.30.254
standby 1 timers 1 3
standby 1 priority 110
standby 1 preempt delay minimum 60
standby 1 authentication cisco
no shutdown
!
interface Vlan35
ip address 10.1.35.251 255.255.255.0
no ip redirects
no ip proxy-arp
arp timeout 200
standby 1 ip 10.1.35.254
standby 1 timers 1 3
standby 1 priority 110
standby 1 preempt delay minimum 60
standby 1 authentication cisco
no shutdown
!
interface Vlan40
ip address 10.1.40.251 255.255.255.0
no ip redirects
no ip proxy-arp
arp timeout 200
standby 1 ip 10.1.40.254
standby 1 timers 1 3
standby 1 priority 110
standby 1 preempt delay minimum 60
standby 1 authentication cisco
no shutdown
!
interface Vlan45
ip address 10.1.45.251 255.255.255.0
no ip redirects
no ip proxy-arp
arp timeout 200
standby 1 ip 10.1.45.254
standby 1 timers 1 3
standby 1 priority 110
standby 1 preempt delay minimum 60
standby 1 authentication cisco
no shutdown
!
interface Vlan50
ip address 10.1.50.251 255.255.255.0
no ip redirects
no ip proxy-arp
arp timeout 200
standby 1 ip 10.1.50.254
standby 1 timers 1 3

```

```

standby 1 priority 110
standby 1 preempt delay minimum 60
standby 1 authentication cisco
no shutdown
!
line vty 0 4
password ese
login
!

```

---

### 6500-3 の基本構成

例 7-2 は、6500-3 の実行構成を簡略に示したリストで、それぞれの例に使用される基本構成を示しています。次の例で使用されている基本インターフェースすべてに対して、**no shutdown** コマンドが発行されていることに注意してください。

#### 例 7-2 6500-3 の基本構成

---

```

hostname DC6500-3
!
vtp domain IBMLAB
vtp mode transparent
!
spanning-tree mode rapid-pvst
spanning-tree vlan 1-2,10,15,20,25,30,35,40,45,50 priority 28672
!
enable password ese
!
vlan 2
!
vlan 10
name Web
!
vlan 15
name User
!
vlan 20
name Application
!
vlan 25
name Backup
!
vlan 30,35,40,45,50
!
interface Port-channel1
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2,10,15,20,25,30,35,40,45,50
switchport mode trunk
switchport nonegotiate
!
!
interface TenGigabitEthernet6/1
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2,10,15,20,25,30,35,40,45,50
switchport mode trunk
switchport nonegotiate
channel-group 1 mode active
no shutdown

```

```

!
interface TenGigabitEthernet6/2
no ip address
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,2,10,15,20,25,30,35,40,45,50
switchport mode trunk
switchport nonegotiate
channel-group 1 mode active
no shutdown
!
interface Vlan1
ip address 192.168.70.3 255.255.255.0
no ip redirects
no shutdown
!
interface Vlan10
ip address 10.1.10.253 255.255.255.0
no ip redirects
no ip proxy-arp
arp timeout 200
standby 1 ip 10.1.10.254
standby 1 timers 1 3
standby 1 priority 110
standby 1 preempt delay minimum 60
standby 1 authentication cisco
no shutdown

!
interface Vlan15
ip address 10.1.15.253 255.255.255.0
no ip redirects
no ip proxy-arp
arp timeout 200
standby 1 ip 10.1.15.254
standby 1 timers 1 3
standby 1 priority 110
standby 1 preempt delay minimum 60
standby 1 authentication cisco
no shutdown
!
interface Vlan20
ip address 10.1.20.253 255.255.255.0
no ip redirects
no ip proxy-arp
arp timeout 200
standby 1 ip 10.1.20.254
standby 1 timers 1 3
standby 1 priority 110
standby 1 preempt delay minimum 60
standby 1 authentication cisco
no shutdown
!
interface Vlan25
ip address 10.1.25.253 255.255.255.0
no ip redirects
no ip proxy-arp
arp timeout 200
standby 1 ip 10.1.25.254
standby 1 timers 1 3

```

```

standby 1 priority 110
standby 1 preempt delay minimum 60
standby 1 authentication cisco
no shutdown
!
interface Vlan30
ip address 10.1.30.253 255.255.255.0
no ip redirects
no ip proxy-arp
arp timeout 200
standby 1 ip 10.1.30.254
standby 1 timers 1 3
standby 1 priority 110
standby 1 preempt delay minimum 60
standby 1 authentication cisco
no shutdown
!
interface Vlan35
ip address 10.1.35.253 255.255.255.0
no ip redirects
no ip proxy-arp
arp timeout 200
standby 1 ip 10.1.35.254
standby 1 timers 1 3
standby 1 priority 110
standby 1 preempt delay minimum 60
standby 1 authentication cisco
no shutdown
!
interface Vlan40
ip address 10.1.40.253 255.255.255.0
no ip redirects
no ip proxy-arp
arp timeout 200
standby 1 ip 10.1.40.254
standby 1 timers 1 3
standby 1 priority 110
standby 1 preempt delay minimum 60
standby 1 authentication cisco
no shutdown
!
interface Vlan45
ip address 10.1.45.253 255.255.255.0
no ip redirects
no ip proxy-arp
arp timeout 200
standby 1 ip 10.1.45.254
standby 1 timers 1 3
standby 1 priority 110
standby 1 preempt delay minimum 60
standby 1 authentication cisco
no shutdown
!
interface Vlan50
ip address 10.1.50.253 255.255.255.0
no ip redirects
no ip proxy-arp
arp timeout 200
standby 1 ip 10.1.50.254
standby 1 timers 1 3

```

```
standby 1 priority 110
standby 1 preempt delay minimum 60
standby 1 authentication cisco
no shutdown
line vty 0 4
password ese
login
!
```

---

## 7.4 BladeCenter を Cisco インフラストラクチャーに接続するためのガイドライン

ここでは、BladeCenter を Cisco インフラストラクチャーに接続する際に考慮することについて説明します。初期構成を変更する前に、この節全体をよくお読みになることを強くお勧めします。また、239 ページの付録 A、『ヒント』、および 56 ページの 5.3、『管理パスに関する詳細説明』も検討することをお勧めします。

この章で説明するトポロジーは、ネイティブ・モードで稼働する Cisco 6500 で構成される外部インフラストラクチャーに BladeCenter を接続する場合を示しています（6500 のすべての制御に IOS を使用）。6500 には他にも可能なコード構成があります（たとえば、IOS と CatOS の両方を実行するハイブリッド・モード）。プラットフォームの選択とコードの選択にはさまざまな可能性があります、データ・センター環境での使用に最適なオプションとして、ネイティブ・モードの 6500 が選択されました。

**重要：**次のリンクには、CatOS と IOS の比較に関する情報があり、さらに本書で使用しているさまざまなコマンドの各種構文が示されています。このリンクは、CatOS ベースのスイッチに接続する BladeCenter を配置しようとしているユーザーに役立ちます。

[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_white\\_paper09186a00800c8441.shtml](http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a00800c8441.shtml)

IBM と Cisco の両方から、データ・センターのアーキテクチャーに関するいくつかの優れた資料、および「Best Practices」ガイドが提供されています。Cisco データ・センター・インフラストラクチャーへの統合に関するさまざまな資料と説明を見つけるには、次の Web サイトが便利です。

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

さらに支援が必要な場合は、次の Web サイトにある「6500 IOS Best Practices」ガイドをご覧ください（CCO ID が必要）。

[http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products\\_white\\_paper09186a00801b49a4.shtml](http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products_white_paper09186a00801b49a4.shtml)

### 7.4.1 ガイドラインとコメント

次に、この章の例で使用される各種 BladeCenter コンポーネントに関連したコメントと推奨事項を示します。

#### ケーブル・タイプの選択（クロスまたはストレート）

Cisco Systems IGESM と外部 Cisco スwitch の間で使用するケーブル・タイプの選択（クロスまたはストレート）は重要です。本書の制作時に、研究所ではストレート・ケーブルとクロスケーブルの両方とも正しく機能することが確認されましたが、場合によっては（リンク



速度 / 全二重の特性をハードコーディングする場合など) クロスケーブルしか機能しないこともあります。このため、Cisco Systems IGESM とアップストリーム・スイッチの間ではクロスケーブルを使用することを強くお勧めします。こうすれば、考えられるすべての条件下でこのリンクが常に確実に機能します。

**注:** 特定のアップストリーム・モジュールを使用して IGESM に接続する際に、自動 MDIX 機能がクロスケーブルまたはそれ以外のどちらかに応じた構成を正しく行わず、ストレート・ケーブルのみが機能するという報告がありました。このシナリオに該当する場合は、ストレート・ケーブルを使用して構いません。この問題については、現時点ではまだ調査中です。この問題に関する最新情報については、IBM サポートにお問い合わせください。

## 速度 / 二重モードの選択

ポートの速度と二重モードについて、自動ネゴシエーションを行うか、設定済みの値を強制するか判断は、たびたび議論になることです。研究所のテスト結果では、Cisco Systems IGESM は外部 Cisco スイッチに接続する際にリンクのネゴシエーションを正しく行うことができました。特に、ギガビット接続の場合は、自動ネゴシエーションを使用することを強くお勧めします。

**重要:** Cisco Systems IGESM を外部スイッチに 100 Mb の速度で接続することもできますが、実稼働環境では、可能な限り最高のスループットが得られるように 1000BaseT 接続の使用を強くお勧めします (データ・センター環境に適したすべての Cisco プラットフォーム上で使用可能)。

## トランクおよびアグリゲーションという用語の使用

業界用語や頭字語は、よく混乱の原因になります。このような用語の 1 つが、トランクまたはトランキングという語です。いくつかのテクノロジーを表すためにこの同じ用語が使用されていますが、最も一般的な意味は、パフォーマンスと信頼性を高めるためにリンクを束ねることと、複数の VLAN を単一の接続上で伝送することです。このように混乱を招くもう 1 つの用語は、アグリゲーションまたはリンク・アグリゲーションという用語です。

この章の説明ではすべて、これらの用語の次に示す IEEE 定義に従います。

- ▶ **トランクまたはトランキング:** 単一の接続上で複数の VLAN を伝送すること。接続は単一リンクの場合もあれば、リンクのグループがアグリゲートされてリンク・アグリゲーション・グループを形成する場合があります。VLAN トランキングの IEEE 仕様は 802.1Q です。
- ▶ **アグリゲーションまたはリンク・アグリゲーション:** スループットの向上または信頼性の強化、あるいはその両方の目的で、複数の物理リンクを 1 つの論理リンクに束ねること。リンク・アグリゲーションは、Cisco 関連では EtherChannel と呼ばれることがよくあります。リンク・アグリゲーションの IEEE 仕様は 802.3ad です (現在は 802.3-2002 の一部)。

## ネイティブ VLAN という用語の使用

ネイティブ VLAN という用語は、802.1Q トランク内の単一、指定済み、タグなしの VLAN を表すためにこの章全体で使用されます。802.1Q 仕様はこの用語を定義していませんが、トランク上でのタグなし VLAN の概念はこの仕様の中で定義されています。Cisco は、特に 802.1Q タグ付けを解釈できないデバイスとの後方互換性を提供することによって、このリンク経由で少なくとも何らかの通信を可能にする VLAN を表すために、この用語を採用しています。

多くの Cisco ネットワークでは、802.1Q トランク接続に対してこのネイティブ VLAN がデフォルトで VLAN 1 に設定されることがよくあります。ネイティブ VLAN を使用する場合は、トランク・リンクの両側が同じネイティブ VLAN の使用に合意していることが重要です。Cisco Systems IGESM は、ブレード・サーバーと外部接続すべてをデフォルトでネイティブ VLAN 2 に設定しますが、その他の Cisco スイッチのほとんどは、ネイティブ VLAN を VLAN 1 に設定することに注意してください。ネイティブ VLAN のミスマッチ・メッセージが表示されないようにするには、このことを考慮する必要があります。

## リンク・アグリゲーション (EtherChannel) のサポート

Cisco Systems IGESM は Port Aggregation Protocol (PAgP) をサポートしますが、Cisco Systems IGESM と Cisco デバイスの間でリンク・アグリゲーションを実行する方式としては、IEEE 標準である Link Aggregation Control Protocol (LACP) が推奨されます。使用する外部 Cisco スイッチが LACP をサポートしない場合は (6500 の場合、LACP サポートは IOS バージョン 12.1(13)E から開始されました)、LACP をサポートする新しいコードにスイッチをアップグレードするか、PAgP または静的アグリゲーションの使用を選択できます。(PAgP と静的アグリゲーションの使用については、この章では説明していませんが、両方とも IGESM によってサポートされます)

必要な機能セットが提供されているかどうか、使用する Cisco IOS の改訂のリリース・ノートを必ず確認することをお勧めします。

本書の例では、それぞれの 6500 内で単一のモジュールを使用して、LACP チャネル経由でそれぞれのモジュールを接続しています。これは単に本書での便宜のために行われていることであり、実際にはこのアグリゲーションを複数の 6500 モジュールに分割して、単一のモジュールに障害が起こった場合の可用性を高めることを強くお勧めします。

**重要:** アグリゲーション・スイッチ (本書では 6500-1 と 6500-3) を接続するリンクは、ネットワークの動作と正常性のためにきわめて重要です。このため、すでに説明したとおり、これら 2 つのスイッチ間のリンクは複数のモジュールにわたって分割する必要があります。これにより、いずれかのシャーシ内で単一のモジュールに障害が起こっても、このリンク全体がダウン状態にならなくなります。

アグリゲーション・グループの一部であるポートは、同じ特性を備えている必要があります (速度、二重モード、トランク設定、同じ VLAN の伝送)。異なる特性を備えたポートを使用すると、Cisco Systems IGESM と Cisco スイッチの間でアグリゲーションの形成に失敗するなど、予期しない問題が生じます。

リンク・アグリゲーションの使用法を示すこの章の例は、レイヤー 2 リンク・アグリゲーションのみに関するものです。

アグリゲートされたリンク上でトラフィックのロード・バランシング方法を制御するためのオプションは、いくつか存在します。ここでは、デフォルトのロード・バランシングの使用を前提としています。

EtherChannel ロード・バランシングをデフォルト以外のものに変更する手順については、『デフォルトの EtherChannel ロード・バランシングが最適でない場合がある』(250 ページ)を参照してください。

## スパンニング・ツリー

Cisco Systems IGESM は、現行のスパンニング・ツリー IEEE 標準 (たとえば、802.1D、802.1s、802.1w) のほかに、Cisco オリジナルのスパンニング・ツリーの拡張 (PVST+) をサポートして、スイッチまたはリンクの障害発生時に迅速なコンバージェンスを可能にしています。現在は、最大 64 のスパンニング・ツリー・インスタンスがサポートされています。

前述のとおり、Cisco Systems IGESM のデフォルトは *Rapid-PVST* と呼ばれるもので、これは Cisco オリジナルの拡張（UplinkFast や BackboneFast など）の代わりに 802.1w を使用して、リンクまたはスイッチのダウン状態からの迅速なリカバリーを実現しています。

本書の制作時には、デフォルトのデータのフローが STP の許可したデフォルト・パス以外の望ましいパスになるように、STP ポート・コストに変更を加える必要がときどき生じました。STP ポート・コストについて簡単に説明すると、本書で使ったコードのバージョンに対しては次の値を適用しました。

- ▶ 単一の 1 Gbps リンクに対するデフォルト STP コスト : 4
- ▶ デュアル 1 Gbps EtherChannel (2 Gbps) リンクに対するデフォルト STP コスト : 3
- ▶ クワッド 1 Gbps EtherChannel (4 Gbps) リンクに対するデフォルト STP コスト : 3
- ▶ 単一の 10 Gbps リンクに対するデフォルト STP コスト : 2
- ▶ デュアル 10 Gbps EtherChannel (20 Gbps) リンクに対するデフォルト STP コスト : 1

スパンニング・ツリーの詳細、およびその動作と構成については、次の資料を参照してください。

[http://www.cisco.com/en/US/products/hw/switches/ps628/products\\_configuration\\_guide\\_chapter09186a00801a6baa.html](http://www.cisco.com/en/US/products/hw/switches/ps628/products_configuration_guide_chapter09186a00801a6baa.html)

## BladeCenter HS20 NIC チーミングの考慮事項

NIC チーミングは、Single Point of Failure を解消してハイパフォーマンスやフォールト・トレランスを得るために使用されるサーバー・ベースのテクノロジーです。チーミングにより、同じサーバー内の物理 NIC を 1 つの仮想アダプター（または複数の仮想アダプター）に論理的にグループ化できます。

Broadcom Advanced Server Program (BASP) は 3 種類のチーミングをサポートします。BladeCenter HS20 NIC は、*Smart Load Balancing* (SLB、または *Server Load Balancing* と呼ばれる) および SLB Auto-Fallback Disable という BASP チーミングのみをサポートします。HS40 はこれらをサポートでき、さらにリンク・アグリゲーションに関連して他の 2 つのオプションをサポートできると考えられますが (HS20 はそれぞれの IGESM に単一の NIC を提供しますが、HS40 はそれぞれの IGESM に 2 つの NIC を提供するため)、本書の制作時には HS40 を使用したテストは行われませんでした。

## IP アドレッシングと MAC アドレッシング

SLB チームの作成時に、仮想アダプター上で IP アドレスが構成され、チーム・メンバーの物理 NIC 上では構成されません。

SLB チーミングは、アクティブ/アクティブとアクティブ/スタンバイの両方の構成をサポートします。どちらの構成でも、仮想チームの MAC アドレスとして、ただ 1 つのアクティブ NIC の MAC アドレスがすべての ARP 要求への応答に使用されます。このことは、すべてのトラフィックの受信に 1 つの NIC が使用されることを意味します。アクティブ/アクティブ構成では、チーム MAC アドレスとして使用する NIC MAC アドレスを指定することはできません。これはチーミング・ドライバーによって決定され、本書のためのテスト中には NIC の 1 つに固定されませんでした。つまり、着信トラフィックに使用されるパスがアクティブ/アクティブ構成では変更される可能性があります。アクティブ/スタンバイの場合は、着信トラフィックは常にアクティブ NIC によって伝送されます。パケットを伝送するために、アクティブ/アクティブ・モードでは両方の NIC を使用できますが、アクティブ/スタンバイ構成ではアクティブ NIC のみを使用できます。

## フォールト・トレランス

アクティブ/アクティブ・チーム内のいずれかのアクティブ・アダプター上でリンクが失われた場合は、負荷分散が再評価され、残りのチーム・メンバーに再度割り当てられます。アクティブ/スタンバイ・チームの場合は、アクティブ・アダプターがダウン状態になるとスタンバイ・アダプターがアクティブになります。この場合は、既存のアプリケーション・

セッションが維持されます。フェイルオーバー時には、ダウン状態になった NIC と通信するエンドポイントに、SLB チームの他のメンバーから指定 ARP が送信されます。この ARP には、チーム MAC アドレスがソース・アドレスとして含まれています。

BASP は、NIC のリンクダウンによってリンク消失を検出します。BladeCenter の範囲外でのリンク消失（たとえば、IGESM とアップリンク・スイッチの間）の場合は、IOS 12.1(14)AY4 以上のトランク・フェイルオーバー機能を使用する必要があります。（この機能について詳しくは、203 ページの 7.7、『トランク・フェイルオーバー機能の説明と構成』を参照してください）トランク・フェイルオーバーを実装しない場合は、エンドツーエンド接続のフォールト・トレランスを確保するため、物理的な高可用性が得られるようにアップリンクを構成する必要があります。この例は、この章のトポロジー 2 に示します。

### ロード・バランシング

アクティブ/アクティブ構成では、アウトバウンド・トラフィックのロード・バランシングが可能です。これは、ただ 1 つのアクティブ NIC の MAC が ARP 要求に応答し、着信トラフィックは常にその MAC に送られるからです。構成例のテストを行ったところ、システムがサーバーと同じ VLAN にあって、経路指定されたネットワークにない場合は、ロード・バランシングが機能することが分かりました。これは、ロード・バランシングがターゲット MAC アドレスに基づいて行われることを示しています。MAC アドレスに基づくロード・バランシングは、サーバーが同じレイヤー 2 ネットワーク内で他のシステムと通信する場合に有効です。ただし、他のシステムがレイヤー 2 ネットワークより外にある場合（ルーターの向こう側）、サーバーはデフォルト・ゲートウェイとして設定されたルーターを経由してシステムと通信する必要があります。これらのリモート・システムとの通信時には、サーバーはすべてのトラフィックをルーターに送信し、このルーターがトラフィックをシステムに送信します。これらのシステムに向かうトラフィックはすべて、ロード・バランシング・チーム内の同じ NIC を使用して伝送され、MAC アドレスに基づくアルゴリズムを使用する場合にロード・バランシングは行われません。ロード・バランシングが必要な場合は、このことを念頭に置いてネットワーク構成を検討することを強くお勧めします。

### IEEE 802.1q タグ付き VLAN

BASP が提供するもう 1 つの機能は、IEEE 802.1q タグ付き VLAN サポート（トランキンク）です。この機能自体は、実際には SLB の一部ではなく、複数の VLAN を単一の物理 NIC、またはチームに構成された仮想アダプターに割り当てるために使用されます。これにより、1 つの物理 NIC 上で複数のレイヤー 3 インターフェースを構成でき、トラフィックをタイプごとに互いに分離できます。ブレード・サーバー・レベルで VLAN を使用すれば、適切なセキュリティとサービス品質（QoS）ポリシーを施行するためにも役立ちます。また、この機能を使用する際には、NIC に接続した Cisco Systems IGESM ポートをトランク・ポートとして構成し、VLAN を適切に構成する必要があります。さらに、最高のパフォーマンスを維持するためには、BASP 仮想アダプター上で構成される 8 つの VLAN ごとに、64 MB のシステム・メモリーがサーバーに必要なので注意してください。

BASP NIC チーミングについて詳しくは、BACS オンライン・ヘルプ、および「*BCM570X Broadcom NetXtreme Gigabit Ethernet Teaming*」ホワイト・ペーパーを参照してください。この資料は、次の URL で入手できます。

<http://www.broadcom.com/collateral/wp/570X-WP100-R.pdf>

**重要：**ここまでの説明の一部は、BASP 7.12.01（本書執筆時の最新リリース）を使用する特定の環境でのテストに基づく「現状のまま」の情報を含んでおり、異なる環境や将来のソフトウェア・リリースでは異なる場合があります。

## 7.4.2 構成例に関する予備情報

具体的な構成例を説明する前に、この章の構成すべての基礎となるいくつかのことを説明する必要があります。

## この章に示す例に関する注意点

**重要:** ここに示す例は、目的のタスクを完了するためのステップとコマンドです。実動スイッチには、これらのコマンドと競合する構成コマンドがすでに設定されている可能性があります。外部スイッチと Cisco Systems IGESM の構成担当者は、変更内容とその結果を完全に理解している必要があります。コマンドを完全に理解していなければ、ネットワークがダウン状態になる可能性があります。

ここに示す例では、レイヤー 2 ネットワークが存在し、BladeCenter をこのレイヤー 2 ネットワークに接続しようとしていることを前提とします。必要に応じて、STP によってブロックされるポートに関するコメントが記されています。

この例では、ネットワーク・アーキテクチャの設計には立ち入らず、特定の特性を備えた Cisco インフラストラクチャーに対する BladeCenter のインターフェースの詳細に重点を置きます。適切なネットワーク設計と階層化アーキテクチャー・アプローチの必要性和効果について、管理者が理解していることが前提です。

BladeCenter は、1 つから 4 つまでの Cisco Systems IGESM をサポートします。この章の例ではすべて、2 つの IGESM を使用します。

## この章で使用される構成シーケンス

これらの例の制作時には、次に示す基本的な手順に従いました。

1. 構成するリンクをシャットダウンする、または配線を切断する (127 ページの表 7-1)。
2. 外部スイッチを構成する。
  - 必要な VLAN を構成する。
  - 必要なアグリゲーション・リンクを構成する。
  - 必要な VLAN トランッキング・オプションを構成する。
  - 構成を NVRAM に保管する。
  - 次の外部スイッチに対して手順を繰り返す。
3. Cisco Systems IGESM を構成する。
  - 必要な VLAN を構成する。
  - 必要なアグリゲーション・リンクを構成する。
  - 必要な VLAN トランッキング・オプションを構成する。
  - 必要なアクセス・リンクを構成する。
  - 構成を NVRAM に保管する。
  - 次の Cisco Systems IGESM に対して手順を繰り返す。
4. サーバー・ブレード上のブレード・サーバー・ポートを構成する。
  - 必要なチーミングまたは SLB、あるいはその両方を構成する。
  - 必要な VLAN/ トランッキングを構成する。
  - 必要なアクセス・リンクを構成する。
  - 必要な IP アドレスを構成する。
  - 次のブレード・サーバーに対して手順を繰り返す。
5. ステップ 1 で使用不可にしたリンクを再度使用可能にする、または再配線する (128 ページの表 7-2)。
6. 構成が正しく動作していることを確認する。

## それぞれの例ごとに実行する切断手順の概要

初期構成を実行するとき、またはスパンニング・ツリーに影響を及ぼす可能性がある変更を既存構成に加えるときには (リンク・アグリゲーションの変更など)、構成を変更する前に、接続を切断 (またはシャットダウン) することをお勧めします。こうすれば、構成を追加したり変更したりする処理に伴って、一時的なスパンニング・ツリー・ループや、ネットワークのダウン状態が発生する可能性が減ります。

表 7-1 に、接続を使用不可にするための 3 とおりの基本的なオプションを示します。ユーザーの状況に最も適合するものを選択してください。たとえば、構成を実行する際に物理的に装置のある場所にいない場合は、ケーブルを物理的に切断するオプションは適していません。

表 7-1 事前構成ステップ: 構成するリンクを使用不可にする

説明とコメント	CLI を使用	管理モジュール Web インターフェースを使用	CMS ユーザー・インターフェースを使用
オプション 1: 外部 Cisco Systems IGESM インターフェースを使用不可にします。	CLI インターフェースから実行します。単一ポートを使用不可にする場合: <b>config t</b> <b>interface g0/17</b> <b>shutdown</b> <b>end</b> g0/17 から g0/20 までの範囲のポートを使用不可にする場合: <b>config t</b> <b>interface range g0/17 - 20</b> <b>shutdown</b> <b>end</b> 他の Cisco Systems IGESM に対して手順を繰り返します。	管理モジュール Web インターフェースから次の手順で行います。 1. ウィンドウの左側の「I/O module tasks」の下で、「 <b>Management</b> 」をクリックします。 2. 右側にある「 <b>Bay 1</b> 」を選択し、「 <b>Advanced Management</b> 」を選択します。 3. 右側にある「Advanced Setup」の下で、「External Ports」を「 <b>Disable</b> 」に変更し、「 <b>Save</b> 」をクリックします。 他の Cisco Systems IGESM に対して手順を繰り返します。	CMS インターフェースから次の手順で行います。 1. 上部メニュー・バーの「 <b>Port</b> 」→「 <b>Port Settings</b> 」をクリックします。 2. Ctrl キーを押したまま、ポート <b>Gi0/17</b> から <b>Gi0/20</b> をクリックします。 3. 「 <b>Modify</b> 」をクリックします。 4. 「Status」の隣にある「 <b>disable</b> 」を選択します。 5. 「 <b>OK</b> 」をクリックします。 6. 「 <b>Apply</b> 」をクリックします。 他の Cisco Systems IGESM に対して手順を繰り返します。
オプション 2: 外部スイッチ上でインターフェースを使用不可にします。	使用可能モードから実行します。単一ポートを使用不可にする場合: <b>config t</b> <b>interface g2/25</b> <b>shutdown</b> <b>end</b> g2/25 から g2/28 までの範囲のポートを使用不可にする場合: <b>config t</b> <b>interface range g2/25 - 28</b> <b>shutdown</b> <b>end</b> 他の外部スイッチに対して手順を繰り返します。	N/A	N/A
オプション 3: Cisco Systems IGESM または外部スイッチのどちらかから接続ケーブルを引き抜きます。	N/A	N/A	N/A

## それぞれの例ごとに実行する再接続手順の概要

表 7-2 に、接続の両側の構成が完了した後で実行する手順を示します。これは、127 ページの表 7-1 で使用した手順の逆です。

表 7-2 構成後の手順：デバイスの再接続

説明とコメント	CLI を使用	管理モジュール Web インターフェースを使用	CMS ユーザー・インターフェースを使用
オプション 1: Cisco Systems IGESM インターフェースを再度使用可能にします。	<p>CLI インターフェースから次の手順で行います。 単一ポートを使用可能にする場合： <b>config t</b> <b>interface g0/17</b> <b>no shutdown</b> <b>end</b></p> <p>g0/17 から g0/20 までの範囲のポートを使用可能にする場合： <b>config t</b> <b>interface range g0/17 - 20</b> <b>no shutdown</b> <b>end</b></p> <p>他の Cisco Systems IGESM に対して手順を繰り返します。</p>	<p>管理モジュール Web インターフェースから次の手順で行います。</p> <ol style="list-style-type: none"> <li>1. ウィンドウの左側の「I/O module tasks」の下で、「Management」をクリックします。</li> <li>2. 右側にある「Bay 1」を選択し、「Advanced Management」を選択します。</li> <li>3. 右側にある「Advanced Setup」の下で、「External Ports」を「Enable」に変更し、「Save」をクリックします。</li> </ol> <p>他の Cisco Systems IGESM に対して手順を繰り返します。</p>	<p>CMS インターフェースから次の手順で行います。</p> <ol style="list-style-type: none"> <li>1. 上部ツールバーの「Port」→「Port Settings」をクリックします。</li> <li>2. キーボードの Ctrl キーを押したまま、ポート <b>Gi0/17</b> から <b>Gi0/20</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Status」の隣の下矢印をクリックして、「enable」を選択します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」をクリックします。</li> </ol> <p>他の Cisco Systems IGESM に対して手順を繰り返します。</p>
オプション 2: 外部スイッチ上でインターフェースを再度使用可能にします。ただし、新しい 6500 コードの場合は、インターフェースに対してではなくポート・チャネルに対して <b>no shut</b> を実行する必要があります。	<p>使用可能モードから次の手順で行います。 単一ポートを使用可能にする場合： <b>config t</b> <b>interface g2/25</b> <b>no shutdown</b> <b>end</b></p> <p>g2/25 から g2/28 までの範囲のポートを使用可能にする場合： <b>config t</b> <b>interface range g2/25 - 28</b> <b>no shutdown</b> <b>end</b></p> <p>他の外部スイッチに対して手順を繰り返します。</p>	N/A	N/A
オプション 3: それぞれのポートにケーブルを再接続します。	N/A	N/A	N/A

## 7.5 トポロジーと構成の例

ここでは、数種類のトポロジーを示し、これらのトポロジーを選択する理由と、ステップバイステップの構成オプションを説明します。

### 7.5.1 トポロジー 1: デュアル IGESM、2 つの 6500 に対する 4 ポート・アグリゲーション

この例（131 ページの図 7-3）では、BladeCenter 内のブレード・サーバーと IGESM 上で実行されるオペレーティング・システムと機能の構成によっては、2 つの Cisco Systems IGESM を使用する場合に BladeCenter から引き出すことができる最大限のパフォーマンス、および冗長性が得られます。ここでは、2 つの Cisco Systems IGESM を使用します。それぞれ、4 つのポートすべてが LACP によって単一のリンクにアグリゲートされ、それぞれ別個の Cisco スイッチに接続します。この構成では、スパンニング・ツリー・ブロック状態になるポートはありません。これは、それぞれの Cisco Systems IGESM がレイヤー 2 ネットワークに対してただ 1 つの（ただし、アグリゲートされた）接続を行うからです。

**重要:** このトポロジーは、ブレード・サーバー NIC に対する高可用性を必要とする環境ではお勧めしません。これは、全アップリンク・スイッチまたはアグリゲーション・スイッチの障害発生時に接続が失われる可能性があり、ブレード・サーバー NIC がこのアップストリームでの障害を Cisco Systems IGESM 経由でセンズできないからです（NIC チーミングまたはトランク・フェイルオーバーを使用しなければ）。この設計を使用して高可用性を得るには、サーバー上で NIC チーミング（BASP ソフトウェアが提供する）を使用し、IGESM 上でトランク・フェイルオーバー（12.1(14)AY4 以上が提供する）を使用します。この章では、さまざまな形式の NIC チーミングを示しますが、トランク・フェイルオーバーは示しません。トランク・フェイルオーバーの説明、および実装方法については、203 ページの 7.7、『トランク・フェイルオーバー機能の説明と構成』を参照してください。

#### このトポロジーにブレード・サーバーを接続するための構成

**重要:** この章に示すブレード・サーバーの構成は、トポロジーの説明には含まれません。サーバーをこのトポロジーに接続するために可能ないくつかの方法を理解するための参考として、ここに示す構成を使用してください。これらの例は、ブレード・サーバーを構成するために必要な方法とは解釈しないでください。ある特定のサーバー接続例を確認することのみが目的の場合は、その特定の例および関連した Cisco Systems IGESM のアップストリーム接続を検討し、その他のブレード・サーバー構成は無視して構いません。

次のリストに、この例のブレード・サーバー構成（131 ページの図 7-3 を参照）を示します。

- ▶ BladeServer1: 802.1Q トランク・リンクによって複数の VLAN を NIC に伝送する。  
この構成は、複数の VLAN がブレード・サーバー内の個々の NIC にアクセスできるようにする方法を示すものです。NIC ごとに複数の VLAN を使用して、トラフィック・タイプを互いに分離する方法の 1 つを例示しています。  
Broadcom チーミング・ソフトウェアが必要ですが、冗長性は使用されません。
- ▶ BladeServer2: 個別の接続を経由した、アクセス・ポートから NIC への接続。  
この接続は、それぞれの NIC を標準アクセス・リンクとして使用方法を示すものです。（ブレード・サーバーの観点からは、VLAN、トランッキング、または冗長性は使用されません。）これは、従来はほとんどのサーバーを接続する標準的な方法だったもので、単純で効率的ですが、柔軟性はあまりありません。



この構成は、Windows 2000 に備わっているストック・ネットワーク構成ツールを使用しています。チーミング・ソフトウェアは使用しません。

トランク・フェイルオーバーに適した NIC チーミングの例は、ここには示しません。このためには、同じ VLAN をブレード・サーバー上の両方の NIC に伝送する必要があります。トランク・フェイルオーバーの使用に適した例については、トポロジー 2 の例にある、サーバー 3 と 4 のブレード・サーバー構成を参照してください。

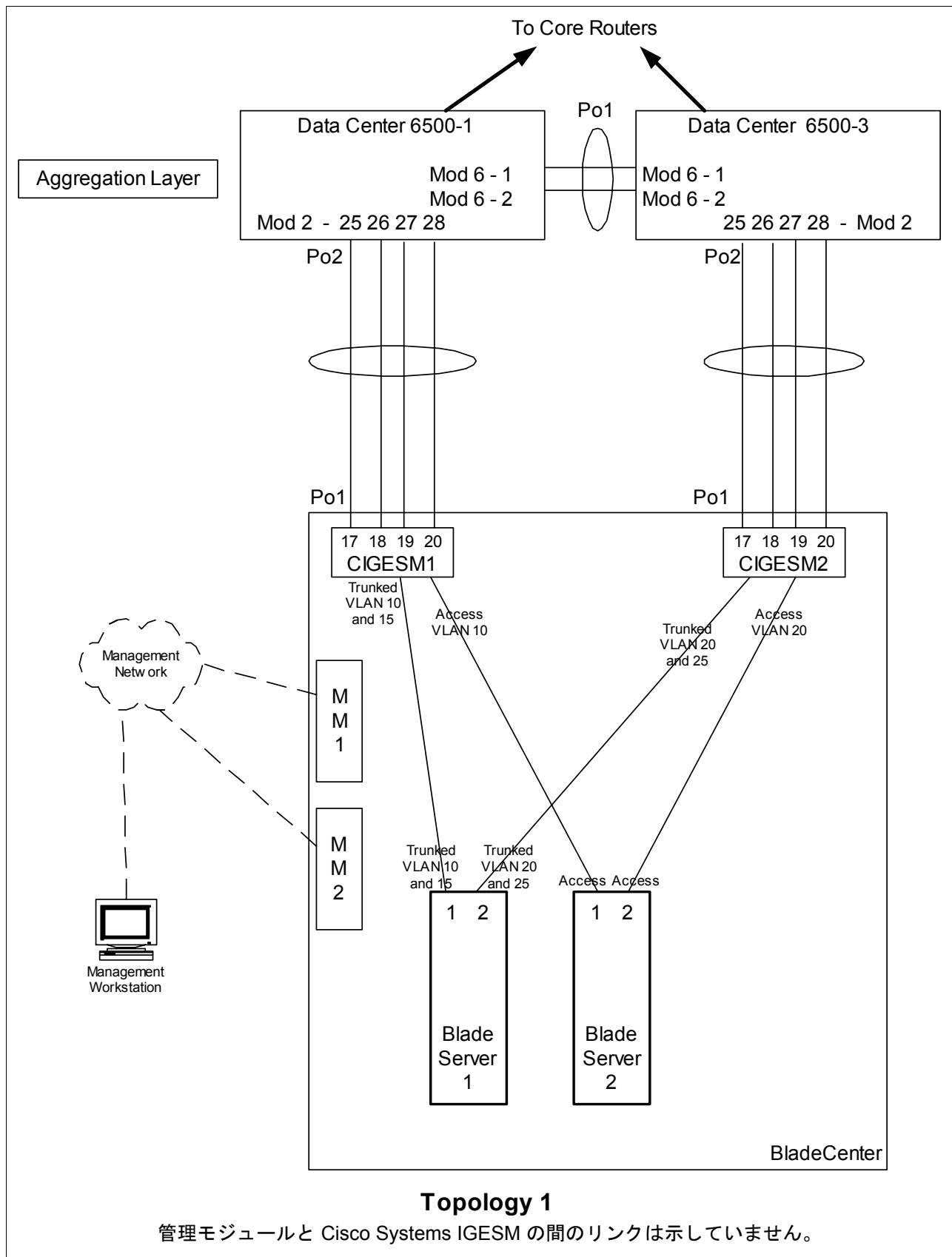


図 7-3 トポロジー 1

## ステップ 1: リンクをダウン状態にする

構成に変更を加える前に、リンクを使用不可にする必要があります（127 ページの表 7-1）。

## ステップ 2: 外部スイッチの構成

この例では、次のことを前提としています。

- ▶ 6500 の構成の大部分は、基本構成に含まれています（『Cat 6500 の基本構成』（113 ページ）を参照）。これは、本書の目的が、一般的な Cisco デバイスではなく BladeCenter コンポーネントを構成する方法を説明することであるからです。ここでは特に、BladeCenter に接続する 6500 ポートの構成を中心に説明します。
- ▶ VLAN 2 は、6500 上で基本構成の一部としてすでに作成済みです。
- ▶ 基本構成の一部として VTP ドメインがすでに命名済みで、透過に設定されています。
- ▶ 基本構成の一部として、スパンニング・ツリー・ルート・コマンドがすでに設定済みです（6500-1 を 1 次ルート、6500-3 を 2 次ルートにする）。
- ▶ ユーザーはすでにスイッチにログオンしており、スイッチは使用可能モードです。
- ▶ コマンドは示されたとおりの順序で実行されます。
- ▶ Cisco Systems IGESM への接続に使用される 6500 内の Cisco スイッチ・モジュールは 1000Base-T をベースとしており、ポートは 1 Gbps 全二重のままにします。
- ▶ 6500 間のアグリゲーション・リンクが基本構成の一部としてすでに作成済みで、必要な VLAN（たとえば、2、10、15、20）を伝送しています。

表 7-3 外部スイッチの構成

説明とコメント	6500-1 上での手順	6500-3 上での手順
ステップ 2.1: リンク・アグリゲーションを作成します。これは、6500 とそれぞれの Cisco Systems IGESM の間のポート・チャネル用です。インターフェースに説明を付けるようにすることを常にお勧めします。個々のポートとポート・チャネルの両方に対して、適所に <b>spanning-tree guard root</b> が追加されていることに注意してください。	<pre>config t int range g2/25 - 28 switchport spanning-tree guard root description To-BladeCenter CIGESM1 channel-group 2 mode active</pre> <p>これにより、<i>Port-Channel2</i> という名前の論理インターフェースが作成され、インターフェース g2/25 から g2/28 がこのインターフェースに配置されます。</p>	<pre>config t int range g2/25 - 28 switchport spanning-tree guard root description To-BladeCenter CIGESM2 channel-group 2 mode active</pre> <p>これにより、<i>Port-Channel2</i> という名前の論理インターフェースが作成され、インターフェース g2/25 から g2/28 がこのインターフェースに配置されます。</p>
ステップ 2.2: 新規に作成したポート・チャネル上で VLAN およびトランキングのオプションを構成します。必要な VLAN はすべて基本構成の一部として作成済みで、その時点で IP アドレスが追加済みです。このステップでは、ステップ 2.1 で作成した、アグリゲートされたリンクを 802.1Q トランクとしてセットアップし、必要な VLAN が伝送されるようにします。	<pre>int port-channel 2 description EtherChannel to CIGESM1 switchport trunk encapsulation dot1q switchport trunk native vlan 2 switchport trunk allowed vlan 2,10,15 switchport mode trunk spanning-tree guard root end</pre> <p>注：6500-1 と Cisco Systems IGESM の間のポート・チャネル・インターフェース上でルート・ガードを構成することにより、ネットワークの安定性を確保できます。</p>	<pre>int port-channel 2 description EtherChannel to CIGESM2 switchport trunk encapsulation dot1q switchport trunk native vlan 2 switchport trunk allowed vlan 2,20,25 switchport mode trunk spanning-tree guard root end</pre> <p>お願い：6500-3 と Cisco Systems IGESM の間のポート・チャネル・インターフェース上でルート・ガードを構成することにより、ネットワークの安定性を確保できます。</p>

説明とコメント	6500-1 上での手順	6500-3 上での手順
ステップ 2.3: 構成を NVRAM に保管します。 <sup>a</sup>	<code>copy running-config startup-config</code>	<code>copy running-config startup-config</code>

a. 構成を保管しないと、保管する前にスイッチを再始動した場合に、ネットワークのダウン状態が発生する可能性があります。（最後に保管を行ってからの変更内容はすべて失われます）

## ステップ 3: Cisco Systems IGESM の構成

ここでは、この例の Cisco Systems IGESM を構成するために必要な一連のアクションについて、段階を追って説明します。主に、ベイ 1 の Cisco Systems IGESM を構成する部分と、ベイ 2 の Cisco Systems IGESM を構成する部分の 2 つに分かれています。

この例に示す両方の Cisco Systems IGESM 構成について、次のことが前提になっています。

- ▶ ユーザーはすでに Cisco Systems IGESM にログオンしており、スイッチは使用可能モードになっています（または CMS にログインし、その GUI を使用している）。
- ▶ コマンドは示されたとおりの順序で実行されます。
- ▶ Cisco Systems IGESM は、『Cisco Systems IGESM の基本構成』（113 ページ）に示すとおりの基本構成から開始されます。
- ▶ ブレード・サーバー上で使用されているオペレーティング・システムは Windows 2000 です。ブレード・サーバー上でどちらのポートが「第 1」と見なされ、どちらのポートが「第 2」と見なされるかはいくつかの要因に依存し、使用されているオペレーティング・システムも少なからず関係しているため、このことは重要です。ブレード・サーバーの接続名と、その名前を得る方法については、239 ページの付録 A、『ヒント』を参照してください。
- ▶ BladeServer1 上では、Broadcom BASP ソフトウェアによるトランキング（ロード・バランシングではない）を両方のポートが使用します。第 1 のポートは VLAN 10 と 15 用に構成され、第 2 のポートは VLAN 20 と 25 用に構成されます。
- ▶ BladeServer2 上では、Cisco Systems IGESM のポート設定によって、両方のポートが単純なアクセス・リンクになり、それぞれ VLAN 10 と 20 に配置されます。

### ステップ 3.1: 第 1 の Cisco Systems IGESM (CIGESM1) の構成

表 7-4 では、CIGESM1 を構成するための手順を説明し、CLI と CMS の両方のコマンドを示します。

**重要：** Cisco Systems IGESM 上でサポートされる CMS の現行バージョンでは、トランクに配置される VLAN を完全に制御する機能に制限があります。許可するように設定していても、トランクには常に VLAN 1 と、1001 から 1005 が含まれます。このため、実動構成のトランク上で許可される VLAN を制御しようとしている場合、この機能の使用は適さない場合があります。

表 7-4 CIGESM1 の構成

説明とコメント	CIGESM1 に対する IOS CLI からのアクション	CIGESM1 に対する CMS からのアクション
<p>ステップ 3.1.1: <i>CIGESM1</i> に対して必要な <i>VLAN</i> を構成します。</p> <p>VLAN 10 と 15 を作成し、名前を付けます。</p>	<p>使用可能モードから実行します。</p> <pre> <b>config t</b> <b>vlan 10</b> <b>name Web</b> <b>vlan 15</b> <b>name User</b> </pre>	<p>CMS インターフェース内で、次の手順で行います。</p> <ol style="list-style-type: none"> <li>1. 上部ツールバーの「VLAN」→「VLAN」をクリックします。</li> <li>2. 「Configure VLANs」タブをクリックします。</li> <li>3. 「Create」をクリックします。</li> <li>4. 「VLAN ID」フィールドに 10 と入力します。</li> <li>5. 「VLAN Name」フィールドに Web と入力します。</li> <li>6. 「OK」をクリックします。</li> <li>7. 「Create」をクリックします。</li> <li>8. 「VLAN ID」フィールドに 25 と入力します。</li> <li>9. 「VLAN Name」フィールドに User と入力します。</li> <li>10. 「OK」をクリックします。</li> <li>11. 「Apply」をクリックします。</li> <li>12. 「Refresh」をクリックして新規 VLAN を表示します。</li> </ol>
<p>ステップ 3.1.2: <i>6500-1</i> へのリンク・アグリゲーションを構成します。</p> <p>この例では、LACP を使用してアグリゲーションを構成します。</p> <p>CMS を使用してポート・チャネルに名前を割り当てる方法はないと考えられるので、注意してください。</p>	<pre> <b>int range g0/17 - 20</b> <b>description To-6500-1</b> <b>channel-group 1 mode active</b> </pre> <p>これにより、<i>Port-Channel1</i> という名前の論理インターフェースが作成され、インターフェース <i>g0/17</i> から <i>g0/20</i> がこのインターフェースに配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部ツールバーの「Port」→「EtherChannels」をクリックします。</li> <li>2. 「Create」をクリックします。</li> <li>3. ポート <b>Gi0/17</b> から <b>Gi0/20</b> までの隣にあるチェック・ボックスを選択します。</li> <li>4. 「Group [1-6]」フィールドに 1 と入力して、使用するポート・チャネルを選択します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> </ol>
<p>ステップ 3.1.3: <i>6500-1</i> への <i>802.1Q</i> トランッキングを構成し、許可される <i>VLAN</i> を追加します。個々の <i>VLAN</i> を許可する行では、番号とコンマの間にスペースを入れることはできないので注意してください。</p> <p>また、デフォルトでは <i>VLAN 2</i> がこれらのポートのネイティブ <i>VLAN</i> です。</p>	<pre> <b>int port-channel 1</b> <b>description</b> <b>EtherChannel-To-6500-1</b> <b>switchport trunk native vlan 2</b> <b>switchport trunk allowed vlan 2,10,15</b> <b>switchport mode trunk</b> </pre> <p>注: <i>VLAN</i> 番号は、コマンドと同じ行に指定する必要があります。</p>	<ol style="list-style-type: none"> <li>1. 上部ツールバーの「VLAN」→「VLAN」をクリックします。</li> <li>2. Ctrl キーを押したまま、ポート <b>Gi0/17</b> から <b>Gi0/20</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Trunk-Allowed VLAN」フィールドに 2,10,15 と入力します。</li> <li>5. 「Native VLAN」フィールドが 2 に設定されていることを確認します。</li> <li>6. 「OK」をクリックします。</li> <li>7. 「Apply」または「OK」をクリックします。</li> <li>8. <b>重要</b>: CMS の現行バージョンの制限により、許可される <i>VLAN</i> には常に <i>VLAN 1</i> と 1001 から 1005 が含まれます。このため、6500 側の設定値とミスマッチが生じる可能性があります。その結果としてアグリゲーションがダウン状態になることがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> を実行することです。</li> </ol>

説明とコメント	CIGEMS1 に対する IOS CLI からのアクション	CIGEMS1 に対する CMS からのアクション
<p>ステップ 3.1.4: <i>BladeServer1</i> への <i>802.1Q</i> トランキングを構成し、許可される VLAN を追加します。この Cisco Systems IGESM の場合は、ポート <i>g0/1</i> (<i>BladeServer1</i> の第 1 の NIC に接続する) のみのトランキングを行います。<i>BladeServer2</i> の第 1 の NIC は、アクセス・リンクになります (次のステップを参照)。</p>	<pre>int g0/1 switchport trunk allowed vlan 2,10,15</pre> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要がありますので注意してください。</p>	<ol style="list-style-type: none"> <li>1. 上部ツールバーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/1</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Trunk-Allowed VLAN」フィールドに 2,10,15 と入力します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> </ol> <p><b>重要:</b> ステップ 3.1.3 で説明したように、CMS の現行バージョンの制限により、許可される VLAN には常に VLAN 1 と 1001 から 1005 が含まれます。このため、ブレード・サーバー側の設定値とのミスマッチが生じる可能性があります。その結果としてトランクが期待どおり動作しないことがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> を実行することです。</p>
<p>ステップ 3.1.5: <i>BladeServer2</i> へのアクセス・リンクを構成し、アクセス VLAN を設定します。この Cisco Systems IGESM の場合は、ポート <i>g0/2</i> (<i>BladeServer2</i> の第 1 の NIC に接続する) のみがアクセス・リンクになります。</p>	<pre>int g0/2 switchport mode access switchport access vlan 10 end</pre> <p>これにより、<i>BladeServer2</i> の第 1 の NIC が VLAN 10 に配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/2</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Administrative Mode」フィールドの「Static Access」を選択します。</li> <li>5. 「Static-Access VLAN」フィールドに 10 と入力します。</li> <li>6. 「OK」をクリックします。</li> <li>7. 「Apply」または「OK」をクリックします。</li> </ol>
<p>ステップ 3.1.6: <i>Cisco Systems IGESM</i> の構成を <i>NVRAM</i> に保管します。このステップを実行しなければ、<i>BladeCenter</i> の電源をオフにした場合、または <i>Cisco Systems IGESM</i> をその他の方法で再始動した場合に、<i>Cisco Systems IGESM</i> に対する変更がすべて失われます。</p>	<pre>copy running-config startup-config</pre>	<ol style="list-style-type: none"> <li>1. 上部ツールバーの「Administration」→「Save Configuration」をクリックします。</li> <li>2. 「Source」は「Running Configuration」に設定されたままにします。</li> <li>3. 「Destination」は「Startup Configuration」を選択します。</li> <li>4. 「Save」をクリックします。</li> </ol>

### ステップ 3.2: 第 2 の Cisco Systems IGESM (CIGESM2) の構成

表 7-5 では、CIGESM2 を構成するために使用されるステップバイステップの手順を説明し、CLI と CMS の両方のコマンドを示します。

**重要:** Cisco Systems IGESM 上でサポートされる CMS の現行バージョンでは、トランクに配置される VLAN を完全に制御する機能に制限があります。許可するように設定していても、トランクには常に VLAN 1 と、1001 から 1005 が含まれます。このため、実動構成のトランク上で許可される VLAN を制御しようとしている場合、この機能の使用は適さない場合があります。

表 7-5 CIGESM2 の構成

説明とコメント	CIGESM2 に対する IOS CLI からのアクション	CIGESM2 に対する CMS からのアクション
ステップ 3.2.1: CIGESM2 に対して必要な VLAN を構成します。VLAN 20 と 25 を作成し、名前を付けます。	使用可能モードから次の手順で行います。 <pre> config t vlan 20  name Application vlan 25  name Backup </pre>	CMS インターフェースから次の手順で行います。 <ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. 「Configure VLANs」タブをクリックします。</li> <li>3. 「Create」をクリックします。</li> <li>4. 「VLAN ID」フィールドに 20 と入力します。</li> <li>5. 「VLAN Name」フィールドに Application と入力します。</li> <li>6. 「OK」をクリックします。</li> <li>7. 「Create」をクリックします。</li> <li>8. 「VLAN ID」フィールドに 25 と入力します。</li> <li>9. 「VLAN Name」フィールドに User と入力します。</li> <li>10. 「OK」をクリックします。</li> <li>11. 「Apply」をクリックします。</li> <li>12. 「Refresh」をクリックして新規に作成した VLAN を表示します。</li> </ol>
ステップ 3.2.2: 6500-3 へのリンク・アグリゲーションを構成します。 この例では、LACP を使用してアグリゲーションを構成します。	<pre> int range g0/17 - 20 description To-6500-3 channel-group 1 mode active </pre> <p>これにより、<i>Port-Channel1</i> という名前の論理インターフェースが作成され、インターフェース g0/17 から g0/20 がこのインターフェースに配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「Port」→「EtherChannels」をクリックします。</li> <li>2. 「Create」をクリックします。</li> <li>3. ポート Gi0/17 から Gi0/20 までの隣にあるチェック・ボックスを選択します。</li> <li>4. 「Group [1-6]」フィールドに 1 と入力して、使用するポート・チャネルを選択します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> </ol>

説明とコメント	CIGEMS2 に対する IOS CLI からのアクション	CIGEMS2 に対する CMS からのアクション
<p>ステップ 3.2.3: 6500-3 への 802.1Q トランッキングを構成します。</p> <p>個々の VLAN を許可する行では、番号とコンマの間にスペースを入れることはできないので注意してください。（この例の中では折り返されている場合がありますが、コマンドと同じ行に入力する必要があります）</p> <p>また、デフォルトでは VLAN 2 がこれらのポートのネイティブ VLAN です。</p>	<pre>int port-channel 1 description EtherChannel-To-6500-3 switchport trunk native vlan 2 switchport trunk allowed vlan 2,20,25 switchport mode trunk</pre> <p>（この例の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があります）</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. Ctrl キーを押したまま、ポート Gi0/17 から Gi0/20 をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Trunk-Allowed VLAN」フィールドに 2,20,25 と入力します。</li> <li>5. 「Native VLAN」フィールドが 2 に設定されていることを確認します。</li> <li>6. 「OK」をクリックします。</li> <li>7. 「Apply」または「OK」をクリックします。</li> </ol> <p><b>重要：</b>CMS の現行バージョンの制限により、許可される VLAN には常に VLAN 1 と 1001 から 1005 が含まれます。このため、6500 側の設定値とミスマッチが生じる可能性があり、その結果としてアグリゲーションがダウン状態になることがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>
<p>ステップ 3.2.4: CIGESM2 に接続する BladeServer1 への 802.1Q トランッキングを構成します。</p> <p>この Cisco Systems IGESM の場合は、ポート g0/1 (BladeServer1 の第 2 の NIC に接続する) のみのトランッキングを行います。</p> <p>BladeServer2 の第 2 の NIC は、アクセス・リンクになります（次のステップを参照）。</p>	<pre>int g0/1 switchport trunk allowed vlan 2,20,25</pre> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート Gi0/1 をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Trunk-Allowed VLAN」フィールドに 2,20,25 と入力します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> </ol> <p><b>重要：</b>ステップ 3.1.3 で説明したように、CMS の現行バージョンの制限により、許可される VLAN には常に VLAN 1 と 1001 から 1005 が含まれます。このため、ブレード・サーバー側の設定値とのミスマッチが生じる可能性があり、その結果としてトランクが期待どおり動作しないことがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>



説明とコメント	CIGEMS2 に対する IOS CLI からのアクション	CIGEMS2 に対する CMS からのアクション
<p>ステップ 3.2.5: ブレード・サーバーの CIGEMS2 へのアクセス・リンクを構成します。</p> <p>この Cisco Systems IGESM の場合は、ポート g0/2 (BladeServer2 の第 2 の NIC に接続する) のみがアクセス・リンクになります。</p>	<pre>int g0/2 switchport mode access switchport access vlan 20 end</pre> <p>これにより、BladeServer2 の第 2 の NIC が VLAN 20 に配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/2</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Administrative Mode」フィールドの「Static Access」を選択します。</li> <li>5. 「Static-Access VLAN」フィールドに 20 と入力します。</li> <li>6. 「OK」をクリックします。</li> <li>7. 「Apply」または「OK」をクリックします。</li> </ol>
<p>ステップ 3.2.6: Cisco Systems IGESM の構成を NVRAM に保管します。</p> <p>このステップを実行しなければ、BladeCenter の電源をオフにした場合、または Cisco Systems IGESM をその他の方法で再始動した場合に、Cisco Systems IGESM に対する変更がすべて失われます。</p>	<pre>copy running-config startup-config</pre>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「Administration」→「Save Configuration」をクリックします。</li> <li>2. 「Source」は「Running Configuration」に設定されたままにします。</li> <li>3. 「Destination」は「Startup Configuration」を選択します。</li> <li>4. 「Save」をクリックします。</li> </ol>

## ステップ 4: ブレード・サーバー上のインターフェースの構成

ここでは、この例に使用するブレード・サーバーを構成するために必要なアクションのリストを示します。

この例では、次のことを前提としています。

- ▶ ブレード・サーバー上で使用されているオペレーティング・システムは Windows 2000 です。ブレード・サーバー上でどちらのポートが「第 1」と見なされ、どちらのポートが「第 2」と見なされるかはいくつかの要因に依存し、使用されているオペレーティング・システムも少なからず関係しているので、このことは重要です。ブレード・サーバーの接続名と、その名前を得る方法については、239 ページの付録 A、『ヒント』を参照してください。
- ▶ ユーザーは管理者または同等なユーザーとして Windows 2000 にすでにログオンしています。管理モジュール上で KVM インターフェースを使用する構成の場合にブレード・サーバーを選択する方法については、239 ページの付録 A、『ヒント』を参照してください。
- ▶ コマンドは示されたとおりの順序で実行されます。
- ▶ BladeServer1: Cisco Systems IGESM へのトランク接続。
  - Broadcom Advanced Server Program (BASP、または Broadcom Advanced Control Suite と呼ばれる) ソフトウェアが BladeServer1 にインストール済みです。BladeServer1 は、BASP ソフトウェアを使用して VLAN 10、15、20、および 25 に対応する論理インターフェースを作成し、すべての IP 構成はこれらの論理インターフェースに対して実行されます (物理インターフェースに対してではなく)。
  - 両方のポートが、Broadcom BASP ソフトウェアによるトランッキングを使用します (一方、ロード・バランシングは使用しません)。第 1 のポートは VLAN 10 および 15 用に構成され、第 2 のポートは VLAN 20 および 25 用に構成されます。

- 次の IP アドレスを使用します (24 ビット・マスク)。
  - 第 1 のポート、VLAN 10 から CIGESM1 へ10.1.10.1 (デフォルト・ゲートウェイ = 10.1.10.254)
  - 第 1 のポート、VLAN 15 から CIGESM1 へ10.1.15.1
  - 第 2 のポート、VLAN 20 から CIGESM2 へ10.1.20.1
  - 第 2 のポート、VLAN 25 から CIGESM2 へ10.1.25.1
- 複数のデフォルト・ゲートウェイを使用する (たとえば、それぞれの VLAN に 1 つ、または複数の VLAN に 1 つ) かどうかの選択は、ユーザーの任意であることに注意してください。マルチホーム・システム上でのデフォルト・ゲートウェイについては、239 ページの付録 A、『ヒント』を参照してください。
- ▶ BladeServer2: Cisco Systems IGESM へのアクセス・リンク接続。
  - どちらのポートも BASP ソフトウェアを使用せず、すべての構成がインターフェースに対して直接実行されます。
  - Cisco Systems IGESM のポート設定によって、両方のポートが単純なアクセス・リンクになり、それぞれ VLAN 10 と 20 に配置されます。
  - 次の IP アドレスを使用します (24 ビット・マスク)。
    - 第 1 のポート、CIGESM1 へ10.1.10.2 (デフォルト・ゲートウェイ = 10.1.10.254)
    - 第 2 のポート、CIGESM2 へ10.1.20.2
  - 複数のデフォルト・ゲートウェイを使用する (たとえば、それぞれの VLAN に 1 つ) かどうかの選択は、ユーザーの任意であることに注意してください。マルチホーム・システム上でのデフォルト・ゲートウェイについては、239 ページの付録 A、『ヒント』を参照してください。

### BladeServer1 を構成するためのステップバイステップの手順

表 7-6 に、BladeServer1 を構成するためのステップバイステップの手順を示します。

表 7-6 複数の VLAN を使用する 802.1Q トランク用の BladeServer1 の構成

説明とコメント	BladeServer1 上での手順 両方のイーサネット・ポート上で VLAN を使用する BASP
ステップ 4.1.1: BASP ソフトウェアを起動します。 このステップは、必要なソフトウェアがすでにインストールされていることを前提としています。	<ul style="list-style-type: none"> <li>▶ 「スタート」 → 「プログラム」 → 「Broadcom」 → 「Broadcom Advanced Control Suite」をクリックします。</li> </ul> <p>これは、ソフトウェアのデフォルト・インストールを使用したことを前提としています。また、ウィンドウ右下隅の時計の近くにあるアイコン (「Control Suite」というラベルの付いたアイコンが見つかるまでカーソルを動かします)、またはコントロール・パネルにあるアイコンを使用して、このソフトウェアを起動することもできます。</p>
ステップ 4.1.2: それぞれ単一のインターフェースを含む 2 つのチームを作成し、名前を付けます。 このプロセスは、SLB を構成する場合と同じように見えるかもしれませんが、実際には異なります。これは、それぞれのチームに含まれる NIC はただ 1 つで、VLAN を割り当てるためだけにチームを作成しているからです (これにより、インターフェースを 802.1Q トランク・インターフェースにします)。	<ol style="list-style-type: none"> <li>1. ツールバーの「Tools」 → 「Create a Team」をクリックします。</li> <li>2. 「name」フィールドに ToCIGESM1 と入力し、「Next」をクリックします。 注: 「Team Type」はデフォルト値のままにしてください (Smart Load Balance and Fail Over)。</li> <li>3. ウィンドウ左側の一番上にある NIC を選択し、上にある右向きの矢印をクリックして、この NIC を「Load Balance Members」に追加します。</li> <li>4. 「Finish」をクリックします。</li> </ol> <p>第 2 の NIC に対してステップ 4.1.2 を繰り返し、チームに ToCIGESM2 という名前を付けます。</p>

説明とコメント	BladeServer1 上での手順 両方のイーサネット・ポート上で VLAN を使用する BASP
<p>ステップ 4.1.3a: チーム <i>CIGESM1</i> に必要な VLAN を作成します。</p> <p>CIGESM1 に接続するチームに VLAN 10 と 15 を作成し、名前を付けます。</p>	<ol style="list-style-type: none"> <li>1. ツールバーの「Tools」→「Configure a Team」をクリックします。</li> <li>2. 「ToCIGESM1」を選択し、「OK」をクリックします。</li> <li>3. ウィンドウ右側にある「Add VLAN」ボタンをクリックします。</li> <li>4. 「VLAN ID」フィールドに、10 と入力します。</li> <li>5. 「VLAN Name」フィールドに、VLAN10-WEB と入力します。 名前は記述的にする必要がありますが、任意の名前を指定できます。また、「Untagged VLAN」というラベルの付いたボックスはクリアされたままにしてください。</li> <li>6. 「OK」をクリックしてこの VLAN を作成します。 このチームの第 2 の VLAN に対して、ステップ 4.1.3a を繰り返します。「VLAN ID」を 15 に設定し、VLAN15-USER という名前を付けます。</li> </ol>
<p>ステップ 4.1.3b: チーム <i>CIGESM2</i> に必要な VLAN を作成します。</p> <p>CIGESM2 に接続するチームに VLAN 20 と 25 を作成し、名前を付けます。</p>	<ol style="list-style-type: none"> <li>1. ツールバーの「Tools」→「Configure a Team」をクリックします。</li> <li>2. 「ToCIGESM2」を選択し、「OK」をクリックします。</li> <li>3. ウィンドウ右側にある「Add VLAN」ボタンをクリックします。</li> <li>4. 「VLAN ID」フィールドに、20 と入力します。</li> <li>5. 「VLAN Name」フィールドに、VLAN20-APPS と入力します。 名前は記述的にする必要がありますが、任意の名前を指定できます。また、「Untagged VLAN」というラベルの付いたボックスはクリアされたままにしてください。</li> <li>6. 「OK」をクリックしてこの VLAN を作成します。 このチームの第 2 の VLAN に対して、ステップ 4.1.3b を繰り返します。「VLAN ID」を 25 に設定し、VLAN25-BACKUP という名前を付けます。</li> </ol>
<p>ステップ 4.1.4: 行った変更を BASP に保管します。</p> <p>このステップでは、Windows 2000 内で次の 4 つの新規論理インターフェースを作成します。</p> <ul style="list-style-type: none"> <li>▶ ToCIGESM1/VLAN10-WEB</li> <li>▶ ToCIGESM1/VLAN15-USER</li> <li>▶ ToCIGESM2/VLAN20-APPS</li> <li>▶ ToCIGESM2/VLAN25-BACKUP</li> </ul> <p>注: 「Apply」または「OK」をクリックせずに BASP プログラムを終了すると、構成変更が失われます。</p>	<ol style="list-style-type: none"> <li>1. メイン BASP ウィンドウの「Apply」をクリックします。</li> <li>2. ネットワーク接続の一時的な中断についての警告が出されたら、「Yes」ボタンをクリックします。 この時点で、BASP ソフトウェアは Windows 2000 ネットワーキングに使用される新規論理インターフェースを作成します。</li> </ol>

説明とコメント	BladeServer1 上での手順 両方のイーサネット・ポート上で VLAN を使用する BASP
<p>ステップ 4.1.5: <i>それぞれの VLAN 上で必要な IP アドレスを構成します。</i></p> <p>このステップでは、IP アドレッシング情報を追加する方法をユーザーが知っていることが前提となります。</p> <p>使用されるデフォルト・ゲートウェイは、6500 の基本 HSRP 構成の一部であることに注意してください。</p> <p>また、実動システム上では、通常は 1 つ以上の DNS サーバーを構成します。これはこの環境の一部としては含まれていませんが、ほとんどの実動ネットワークに組み込む必要があります。</p> <p>このステップでは、IP アドレッシングを物理インターフェースに直接適用することはサポートされません。</p>	<ol style="list-style-type: none"> <li>1. Windows で、「スタート」→「設定」→「ネットワークとダイヤルアップ接続」をクリックします。 元の物理ネットワーク・インターフェースとともに、4 つの新しく作成した論理インターフェースが表示されます。</li> <li>2. <b>ToCIGESM1/VLAN10-WEB</b> インターフェースを選択し、IP アドレスを次のように構成します。 <ul style="list-style-type: none"> <li>– IP アドレス : 10.1.10.1</li> <li>– マスク : 255.255.255.0</li> <li>– デフォルト・ゲートウェイ : 10.1.10.254</li> </ul> </li> <li>3. <b>ToCIGESM1/VLAN15-USER</b> インターフェースを選択し、IP アドレスを次のように構成します。 <ul style="list-style-type: none"> <li>– IP アドレス : 10.1.15.1</li> <li>– マスク : 255.255.255.0</li> </ul> </li> <li>4. <b>ToCIGESM1/VLAN20-APPS</b> インターフェースを選択し、IP アドレスを次のように構成します。 <ul style="list-style-type: none"> <li>– IP アドレス : 10.1.20.1</li> <li>– マスク : 255.255.255.0</li> </ul> </li> <li>5. <b>ToCIGESM1/VLAN25-BACKUP</b> インターフェースを選択し、IP アドレスを次のように構成します。 <ul style="list-style-type: none"> <li>– IP アドレス : 10.1.25.1</li> <li>– マスク : 255.255.255.0</li> </ul> </li> </ol>

### BladeServer2 を構成するためのステップバイステップの手順

表 7-7 に、BladeServer2 を構成するためのステップバイステップの手順を示します。

表 7-7 標準インターフェース接続用の BladeServer2 の構成

説明とコメント	BladeServer2 上での手順 BASP ソフトウェアを使用せず、両方の Eth ポート上で物理アクセス・リンクを使用
<p>ステップ 4.2.1: <i>必要なインターフェース上で IP アドレスを直接構成します。</i></p> <p>このステップでは、IP アドレッシング情報を追加する方法をユーザーが知っていることが前提となります。</p> <p>使用されるデフォルト・ゲートウェイは、6500 の基本 HSRP 構成の一部であることに注意してください。</p> <p>また、実動システム上では、通常は 1 つ以上の DNS サーバーを構成します。これはこの環境の一部としては含まれていませんが、ほとんどの実動ネットワークに組み込む必要があります。</p>	<p>この手順は、2 つの NIC を備えたスタンドアロン・サーバーの構成と異なる点はありません。</p> <ol style="list-style-type: none"> <li>1. 「<b>Local Area Connection</b>」 インターフェースを選択し、IP アドレスを次のように構成します。 <ul style="list-style-type: none"> <li>– IP アドレス : 10.1.10.2</li> <li>– マスク : 255.255.255.0</li> <li>– デフォルト・ゲートウェイ : 10.1.10.254</li> </ul> </li> <li>2. 「<b>Local Area Connection 2</b>」 インターフェースを選択し、IP アドレスを次のように構成します。 <ul style="list-style-type: none"> <li>– IP アドレス : 10.1.20.2</li> <li>– マスク : 255.255.255.0</li> </ul> </li> </ol>

### ステップ 5: デバイスの再接続

これは、接続を完全に動作させるために行う最後のステップです。この手順は、ステップ 1 で使用したすべての手順の逆です。リンクを再確立する方法については、128 ページの表 7-2 を参照してください。

## ステップ 6: 構成の検証

ここでは、正しく要求どおりの動作が行われることを検証するためのオプションを示します。

### ブレード・サーバーの正しい動作の検証

BladeServer1 上でチーミングと VLAN の構成が適切に行われているかどうか、BASP アプリケーションを検討します (図 7-4 を参照)。この例では、BladeServer2 に BASP 構成は存在しません (図 7-5 を参照)。

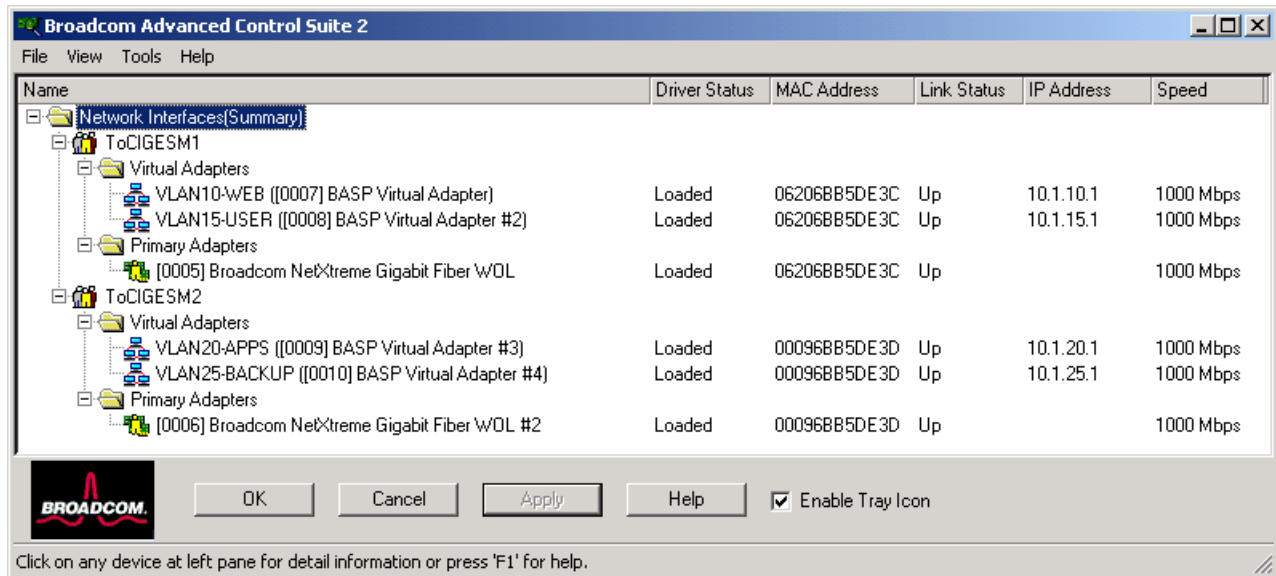


図 7-4 BladeServer1 の BASP 構成

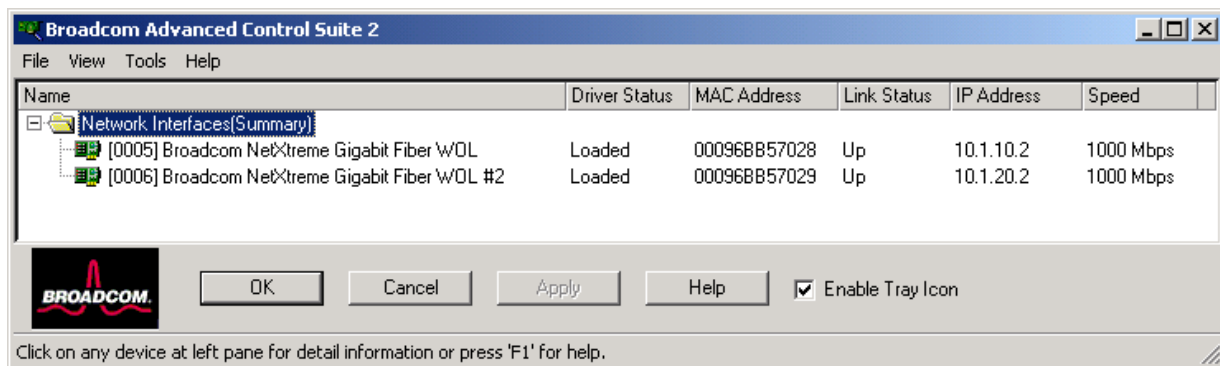


図 7-5 BladeServer2 の BASP 構成 (BASP は BladeServer2 では使用されない)

Windows 2000 ネットワーキング・ツールを使用して、論理ネットワークと物理ネットワークを確認します。143 ページの図 7-6 と 143 ページの図 7-7 は、BladeServer1 と BladeServer2 を示しています。

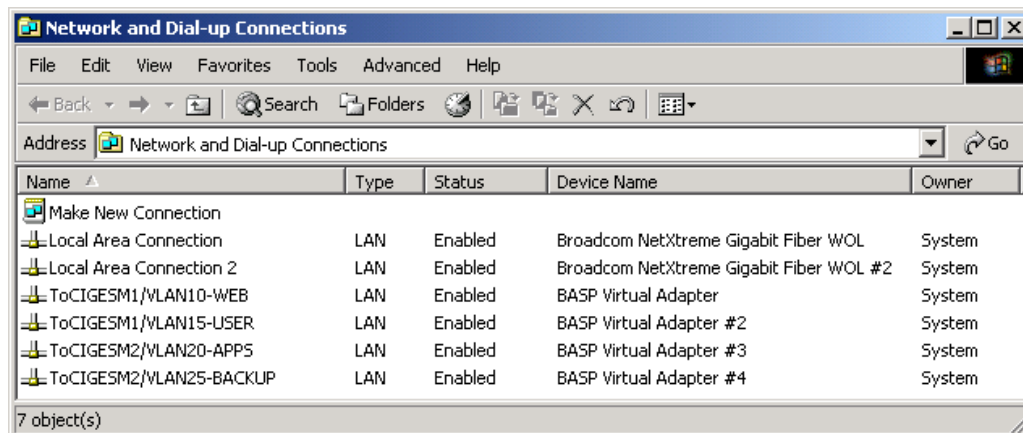


図 7-6 BladeServer1 の物理インターフェースと論理インターフェースを示す Windows 2000 ネットワーキング

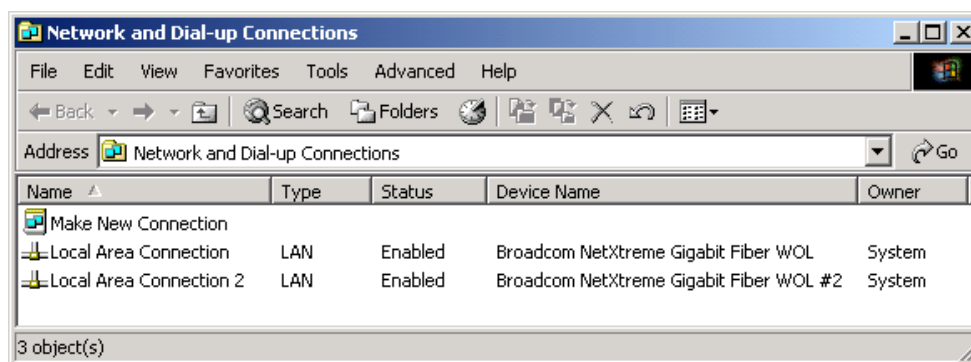


図 7-7 BladeServer2 の物理インターフェースのみを示す Windows 2000 ネットワーキング

CMD プロンプトから（「スタート」→「ファイル名を指定して実行」→cmd→「OK」）、**ipconfig** コマンドを実行し、それぞれのブレード・サーバー上で適切なインターフェースに正しい IP 構成が指定されていることを確認します（これらが逆になっていないことを確認してください。つまり、名前が変更されていないとすると、*Local Area Connection* に必要な IP アドレスが、*Local Area Connection 2* という名前の接続に対して指定されていないか調べます）。チームに構成されたインターフェースの場合は、**ipconfig** によって報告される IP アドレスが、予想される論理インターフェース上のものであることを確認します。

さまざまなボックスから ping テストを実行します。

次に示すテストは、同じ VLAN 上のブレード・サーバー間の接続をテストします。ping は該当する Cisco Systems IGESM まで進むだけで、他のブレード・サーバーに戻ります（アグリゲーション・スイッチまでは進みません）。

- ▶ BladeServer1 から 10.1.10.2（BladeServer2 の VLAN 10 接続）への ping
- ▶ BladeServer1 から 10.1.20.2（BladeServer2 の VLAN 20 接続）への ping

次に示すとおり、Cisco Systems IGESM を経由して 6500 に至る接続をテストします。

- ▶ BladeServer1 から 10.1.10.254（6500 上の HSRP アドレス）への ping
- ▶ BladeServer1 から 10.1.15.254（6500 上の HSRP アドレス）への ping
- ▶ BladeServer1 から 10.1.20.254（6500 上の HSRP アドレス）への ping
- ▶ BladeServer1 から 10.1.25.254（6500 上の HSRP アドレス）への ping
- ▶ BladeServer2 から 10.1.10.254（6500 上の HSRP アドレス）への ping
- ▶ BladeServer2 から 10.1.20.254（6500 上の HSRP アドレス）への ping

この時点で、ここに示したとおりに ping を実行できることが必要です。これらのアドレスを ping できない場合は、前述の構成検査に異常がなければ、次の節に進んでこの構成に含まれる他のコンポーネントを検査してください。

注: この構成では（この例に示す）、Cisco Systems IGESM の管理 VLAN を直接 ping することはできません。これは、管理 VLAN がブレード・サーバーとは異なる VLAN 上にあるからです。また、いくつかの理由から、Cisco Systems IGESM によって使用されている管理 VLAN と同じ VLAN にブレード・サーバーを配置しないことを強くお勧めします。

## Cisco Systems IGESM での正しい動作の確認

次のコマンドを使用して、Cisco Systems IGESM の構成を確認してください。

- ▶ 正しいスイッチを使用していることを確認するには、**show platform summary** コマンドを使用します（現在使用しているスロットが表示されます。例：スロット 1 = CIGESM1、スロット 2 = CIGESM2）。
- ▶ **show run** コマンドを実行して、ここまでのステップで入力した目的の構成と一致していることを確認します。
- ▶ **show logging** コマンドを実行して、予期しないエラーが発生しなかったかどうか調べます。
- ▶ CIGESM1 および CIGESM2 上で、**show int g0/1 status** コマンドを実行します。次のように表示されることを確認します。

```
status - connected および vlan - trunk
```

- ▶ CIGESM1 上で、**show int g0/2 status** コマンドを実行して、次のように表示されることを確認します。

```
status - connected および vlan - 10
```

- ▶ CIGESM2 上で、**show int g0/2 status** コマンドを実行して、次のように表示されることを確認します。

```
status - connected および vlan -20
```

- ▶ **show interface trunk module 0** コマンドを実行し、正しい出力が得られることを確認します（両方の Cisco Systems IGESM に対する出力が*同様*であることが必要です）。

Port	Mode	Encapsulation	Status	Native vlan
Gi0/1	on	802.1q	trunking	2
Gi0/2	off	802.1q	not-trunking	2
.	.	.	.	.
Gi0/17	on	802.1q	trunk-inbndl	2 (Pol)
Gi0/18	on	802.1q	trunk-inbndl	2 (Pol)
Gi0/19	on	802.1q	trunk-inbndl	2 (Pol)
Gi0/20	on	802.1q	trunk-inbndl	2 (Pol)

- ▶ コマンド **show etherchannel summary** を実行して、正しい出力が得られることを確認します（両方の Cisco Systems IGESM に対する出力が*同様*であることが必要です）。

```
Flags: D - down          P - in port-channel
       I - stand-alone  s - suspended
       H - Hot-standby (LACP only)
       R - Layer3       S - Layer2
       u - unsuitable for bundling
       U - in use       f - failed to allocate aggregator
       d - default port

Number of channel-groups in use: 1
Number of aggregators:          1
Group  Port-channel  Protocol  Ports
```

```

-----+-----+-----+-----+-----+-----+
1      Po1(SU)          LACP      Gi0/17(P)  Gi0/18(Pd) Gi0/19(P)
                                   Gi0/20(P)

```

- ▶ コマンド **show etherchannel 1 port-channel** を実行して、正しい出力が得られることを確認します（両方の Cisco Systems IGESM に対する出力が *同様* であることが必要です）。

```

Port-channels in the group:
-----
Port-channel: Po1      (Primary Aggregator)
-----
Age of the Port-channel   = 01d:05h:15m:50s
Logical slot/port        = 1/0          Number of ports = 4
HotStandBy port = null
Port state                = Port-channel Ag-Inuse
Protocol                  = LACP
Ports in the Port-channel:
Index  Load  Port      EC state      No of bits
-----+-----+-----+-----+-----+
0      00    Gi0/17    Active        0
0      00    Gi0/18    Active        0
0      00    Gi0/19    Active        0
0      00    Gi0/20    Active        0

```

- ▶ **show cdp neighbors** コマンドの出力を確認します。この表示は次のようになっている必要があります（CIGESM2 の場合はデバイス ID が異なる）。Cisco Systems IGESM は、管理モジュール・インターフェースを介して相互を認識できることに注意してください。

```

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID        Local Intrfce  Holdtme  Capability  Platform  PortID
DC6500-1         Gig 0/20      179      R S I       WS-C6506  Gig 2/28
DC6500-1         Gig 0/19      179      R S I       WS-C6506  Gig 2/27
DC6500-1         Gig 0/18      179      R S I       WS-C6506  Gig 2/26
DC6500-1         Gig 0/17      179      R S I       WS-C6506  Gig 2/25
CIGESM2          Gig 0/15      141      S I         OS-CIGESM-Gig 0/15

```

### 外部スイッチ上での正しい動作の確認 (6500-1 および 6500-3)

次に、6500 の正しい構成と動作の確認に使用できるコマンドをいくつか示します。

Cisco Systems IGESM について前述したものと同一コマンドのセットを実行できます。当然、出力に多少の違いはありますが、ポートのチャンネルとトランクが適切に設定されていて、正しい VLAN を伝送していることを確認できます。また、管理ダウン状態のポートについても注意してください。次のアドレスを ping することが必要です。

- ▶ BladeServer1 の 10.1.10.1 への ping
- ▶ BladeServer1 の 10.1.15.1 への ping
- ▶ BladeServer1 の 10.1.20.1 への ping
- ▶ BladeServer1 の 10.1.25.1 への ping
- ▶ BladeServer2 の 10.1.10.2 への ping
- ▶ BladeServer2 の 10.1.20.2 への ping

## 7.5.2 トポロジー 2: デュアル Cisco Systems IGESM、2 つの 6500 に対する 2 ポート・アグリゲーション

この例（148 ページの図 7-8 を参照）では、BladeCenter からのアップリンクが 2 つのアグリゲーション・スイッチ間で分割されます。このトポロジーは典型的な高可用性構成で、アグリゲーション・スイッチまたはチャンネル・リンクのいずれか 1 つが失われても、NIC チーミング / トランク・フェイルオーバーの構成に関係なく、トラフィックは失われません。



BladeCenter Cisco Systems IGESM はスパンニング・ツリーに参加し、両方の Cisco Systems IGESM の EtherChannel ポート 19 と 20 がブロッキングに関与します (6500-1 がスパンニング・ツリーのルートであることが前提)。

それでも、NIC チーミング/トランク・フェイルオーバーを構成しない場合に高可用性が問題になるケースが 1 つあります。それは、単一の Cisco Systems IGESM からのアップリンクが両方ともダウン状態になり、Cisco Systems IGESM 自体はダウン状態にならなかった場合です。このケースでは、ブレード・サーバーがアップストリームの障害を検出できず、問題が発生します。NIC チーミングとトランク・フェイルオーバーを使用すれば、この問題は起こらなくなります。

このトポロジは、NIC チーミングを使用しない場合、または実行できない場合 (たとえば、ブレード・サーバーに接続するそれぞれの NIC 上で異なる VLAN が必要な場合) にお勧めします。

## このトポロジにブレード・サーバーを接続するための構成

**重要:** この章に示すブレード・サーバーの構成は、必ずしもトポロジの説明には含まれるとは限りませんが、代わりにこの節にこれらの構成を示します。この説明は、サーバーをこのトポロジに接続するために可能ないくつかの方法を理解するための参考として使用してください。これらの例は、ブレード・サーバーを構成するために必要な唯一の方法とは解釈しないでください。ある特定のサーバー接続例を確認することのみが目的の場合は、その特定の例および関連した Cisco Systems IGESM のアップストリーム接続のみを検討し、その他のブレード・サーバー構成は無視して構いません。

次に、この例のブレード・サーバー構成 (148 ページの図 7-8 を参照) を示します。

- ▶ **BladeServer1:** 802.1Q トランク・リンクによって複数の VLAN を NIC に伝送する。

この構成は、複数の VLAN がブレード・サーバー内の個々の NIC にアクセスできるようにする方法を示すものです。NIC ごとに複数の VLAN を使用して、トラフィック・タイプを互いに分離する方法の 1 つを例示しています。

Broadcom チーミング・ソフトウェアが必要ですが、冗長性は使用されません。

- ▶ **BladeServer2:** 個別の接続を経由した、アクセス・ポートから NIC への接続。

この構成は、それぞれの NIC を標準アクセス・リンクとして使用方法を示すものです (VLAN、トランピング、または冗長性は、ブレード・サーバーの観点からは使用されません)。これは、従来はほとんどのサーバーを接続する標準的な方法だったもので、単純で効率的ですが、柔軟性はあまりありません。

この構成は、Windows 2000 に備わっているストック・ネットワーク構成ツールを使用して行います (チーミング・ソフトウェアは使用しません)。

- ▶ **BladeServer3:** SLB/ チーム接続を経由した、アクセス・ポートから NIC への接続。

この構成は、他のアップストリーム・ネットワーク (Cisco Systems IGESM) には単一のアクセス NIC として認識されるように、複数の NIC を使用方法を示すものです。NIC を結合するためにチーミング・ドライバーを使用しますが、特殊な VLAN 構成は使用しません。Cisco Systems IGESM の観点からは、両方の接続は静的 VLAN が割り当てられた単純なアクセス・ポートとして構成されます。

- この構成は、Broadcom チーミング・ソフトウェアを使用してリンクのバインドと平衡化を行います。Cisco Systems IGESM は、チームに構成されたポートが配置される先の VLAN を設定します (このサーバーに接続する両方の Cisco Systems IGESM に対して、同じ VLAN を設定する必要があります)。
- この章に示す BladeServer3 の例は、アクティブ/アクティブ、または Server Load Balancing と呼ばれる機能を使用しているため、両方のインターフェースがトラ

フィックを同時に伝送できます。この逆がアクティブ/スタンバイ（ここには示しません）です。これはホット・スタンバイとも呼ばれ、リンクの一方のみが一度に稼働します。

- ▶ **BladeServer4:** チーム /SLB 接続上で複数の VLAN をサーバーに伝送する 802.1Q トランク・リンク。

この構成は、単一の NIC として認識されるように複数の NIC を使用しながら、この単一の論理 NIC 上で複数の VLAN を使用する方法を示すものです。この構成では、チーミング・ドライバーを使用して NIC を結合し、目的の VLAN を作成します。Cisco Systems IGESM の観点からは、両方の接続がトランク・ポートとして構成され、共通の VLAN のセットを伝送します（このサーバーの 4 つの論理 NIC に接続する両方の Cisco Systems IGESM ポートに対して、同じ VLAN を構成する必要があります）。

- この例では、Broadcom チーミング・ソフトウェアを使用してリンクのバインドと平衡化を行い、本書に例示するさまざまな VLAN を代表する論理インターフェースを作成します。
- この章に示す BladeServer4 の例は、アクティブ/アクティブ、または Server Load Balancing と呼ばれる機能を使用しているため、両方のインターフェースがトラフィックを同時に伝送できます。この逆がアクティブ/スタンバイ（ここには示しません）です。これはホット・スタンバイとも呼ばれ、リンクの一方のみが一度に稼働します。

**重要:** ブレード・サーバー 3 と 4 の可用性を最大限にするためには、トランク・フェイルオーバーも構成する必要があります（この例には示しません）。トランク・フェイルオーバー機能の構成の詳細と要件については、203 ページの 7.7、『トランク・フェイルオーバー機能の説明と構成』を参照してください。

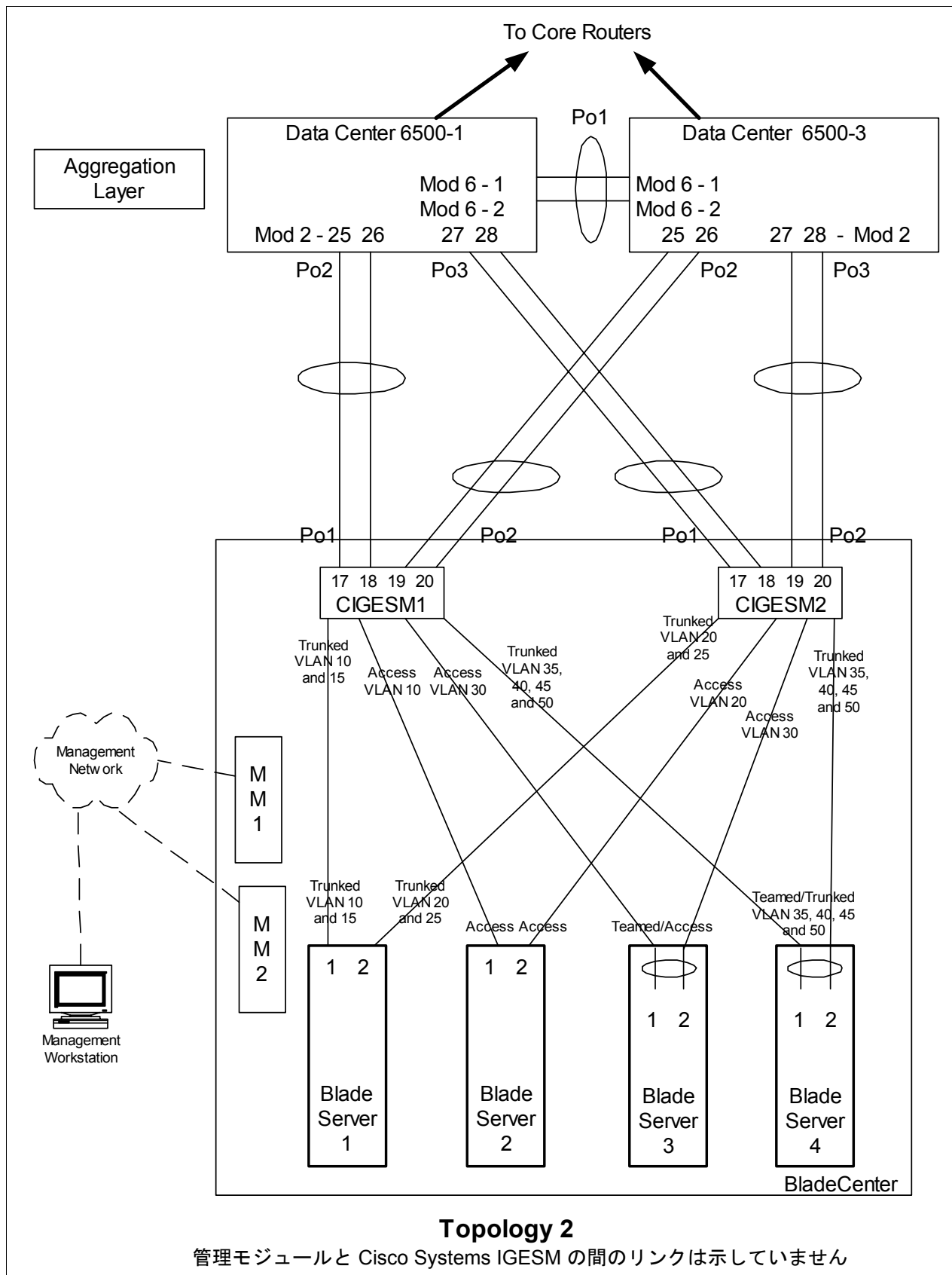


図 7-8 トポロジー 2

## ステップ 1: リンクをダウン状態にする

構成変更を行う前に、必ずリンクを使用不可にすることをお勧めします。必要な手順については、127 ページの表 7-1 を参照してください。

## ステップ 2: 外部スイッチの構成

この例では、次のことを前提としています。

- ▶ 6500 の構成の大部分は、基本構成に含まれています（『Cat 6500 の基本構成』（113 ページ）を参照）。これは、本書の目的が、一般的な Cisco デバイスではなく BladeCenter コンポーネントを構成する方法を説明することであるからです。ここでは特に、BladeCenter に接続する 6500 ポートの構成方法を中心に説明します。
- ▶ VLAN 2 は、6500 上で基本構成の一部としてすでに作成済みです。
- ▶ 基本構成の一部として VTP ドメインがすでに命名済みで、透過に設定されています。
- ▶ 基本構成の一部として、スパンニング・ツリー・ルート・コマンドがすでに設定済みです（6500-1 を 1 次ルート、6500-3 を 2 次ルートにする）。
- ▶ ユーザーはすでにスイッチにログオンしており、スイッチは使用可能モードです。
- ▶ コマンドは示されたとおりの順序で実行されます。
- ▶ Cisco Systems IGESM への接続に使用される 6500 内の Cisco スイッチ・モジュールは 1000Base-T をベースとしており、ポートは 1Gbps 全二重のままにします。
- ▶ 6500 間のアグリゲーション・リンクが基本構成の一部としてすでに作成済みで、必要な VLAN（たとえば、2、10、15、20）を伝送しています。

表 7-8 外部スイッチの構成

説明とコメント	6500-1 上での手順	6500-3 上での手順
ステップ 2.1: 6500 から Cisco Systems IGESM へのリンク・アグリゲーションを構成します。 これは、6500 とそれぞれの Cisco Systems IGESM の間のポート・チャネル用です。インターフェースに説明を付けるようにすることを常にお勧めします。また、個々のポートとポート・チャネルの両方に対して、適所に <b>spanning-tree guard root</b> が追加されていることに注意してください。	<pre>config t int range g2/25 -26 switchport spanning-tree guard root description to-BladeCenter CIGESM1 channel-group 2 mode active</pre> <p>これにより、<i>Port-Channel2</i> という名前の論理インターフェースが作成され、インターフェース g2/25 と g2/26 がこのインターフェースに配置されます。</p> <pre>int range g2/27 - 28 switchport spanning-tree guard root description to-BladeCenter CIGESM2 channel-group 3 mode active</pre> <p>これにより、<i>Port-Channel3</i> という名前の論理インターフェースが作成され、インターフェース g2/27 と g2/28 がこのインターフェースに配置されます。</p>	<pre>config t int range g2/25 -26 switchport spanning-tree guard root description to-BladeCenter CIGESM1 channel-group 2 mode active</pre> <p>これにより、<i>Port-Channel2</i> という名前の論理インターフェースが作成され、インターフェース g2/25 と g2/26 がこのインターフェースに配置されます。</p> <pre>int range g2/27 - 28 switchport spanning-tree guard root description to-BladeCenter CIGESM2 channel-group 3 mode active</pre> <p>これにより、<i>Port-Channel3</i> という名前の論理インターフェースが作成され、インターフェース g2/27 と g2/28 がこのインターフェースに配置されます。</p>

説明とコメント	6500-1 上での手順	6500-3 上での手順
<p>ステップ 2.2: <i>VLAN</i> と <i>トラッキング</i> のオプションを構成します。</p> <p>必要な <i>VLAN</i> はすべて基本構成の一部として作成済みで、その時点で <i>IP</i> アドレスが追加済みです。このステップでは、ステップ 2.1 で作成した、アグリゲートされたリンクを <i>802.1Q</i> トランクとしてセットアップし、必要な <i>VLAN</i> が伝送されるようにします。</p> <p>それぞれのアグリゲーションに異なる <i>VLAN</i> が配置されていることに注意してください。前述のとおり、<i>VLAN</i> を制御することがセキュリティのために推奨されます（ただし、ネットワーク管理者の作業量が増えることがあります）。</p>	<pre> int port-channel 2 description EtherChannel to CIGESM1 switchport trunk encapsulation dot1q switchport trunk native vlan 2 switchport trunk allowed vlan 2,10,15,30,35,40,45,50 switchport mode trunk spanning-tree guard root  注：6500 と Cisco Systems IGESM の間の ポート・チャネル・インターフェース上 でルート・ガードを構成することによ り、ネットワークの安定性を確保できま す。  int port-channel 3 description EtherChannel to CIGESM2 switchport trunk encapsulation dot1q switchport trunk native vlan 2 switchport trunk allowed vlan 2,20,25,30,35,40,45,50 switchport mode trunk spanning-tree guard root end </pre>	<pre> int port-channel 2 description EtherChannel to CIGESM1 switchport trunk encapsulation dot1q switchport trunk native vlan 2 switchport trunk allowed vlan 2,10,15,30,35,40,45,50 switchport mode trunk spanning-tree guard root  注：6500 と Cisco Systems IGESM の間の ポート・チャネル・インターフェース上 でルート・ガードを構成することによ り、ネットワークの安定性を確保できま す。  int port-channel 3 description EtherChannel to CIGESM2 switchport trunk encapsulation dot1q switchport trunk native vlan 2 switchport trunk allowed vlan 2,20,25,30,35,40,45,50 switchport mode trunk spanning-tree guard root end </pre>
<p>ステップ 2.3: 構成を <i>NVRAM</i> に保管します。</p> <p>注：構成を保管しなければ、保管の前にスイッチを再始動した場合に、ネットワークのダウン状態が発生する可能性があります（最後に保管を行ってからの変更はすべて失われます）。</p>	<pre>copy running-config startup-config</pre>	<pre>copy running-config startup-config</pre>

### ステップ 3: Cisco Systems IGESM の構成

ここでは、この例の Cisco Systems IGESM を構成するために必要な一連のアクションについて、段階を追って説明します。主に、ベイ 1 の Cisco Systems IGESM を構成する部分と、ベイ 2 の Cisco Systems IGESM を構成する部分の 2 つに分かれています。

この例に示す両方の Cisco Systems IGESM 構成について、次のことが前提になっています。

- ▶ ユーザーはすでに Cisco Systems IGESM にログオンしており、スイッチは使用可能モードになっています（または CMS にログオンし、その GUI を使用している）。
- ▶ コマンドは示されたとおりの順序で実行されます。
- ▶ Cisco Systems IGESM は、『Cisco Systems IGESM の基本構成』（113 ページ）の例に示すとおりの基本構成から開始されます。
- ▶ ブレード・サーバー上で使用されているオペレーティング・システムは Windows 2000 です。ブレード・サーバー上でどちらのポートが第 1 と見なされ、どちらのポートが第 2 と見なされるかはいくつかの要因に依存し、使用されているオペレーティング・システムも少なからず関係しているので、このことは重要です。ブレード・サーバーの接続名

と、その名前を得る方法については、239 ページの付録 A、『ヒント』を参照してください。

- ▶ BladeServer1 上では、Broadcom BASP ソフトウェアによるトランキング（ロード・バランシングではない）を両方のポートが使用します。第 1 のポートは VLAN 10 と 15 用に構成され、第 2 のポートは VLAN 20 と 25 用に構成されます。
- ▶ BladeServer2 上では、Cisco Systems IGESM のポート設定によって、両方のポートが単純なアクセス・リンクになり、それぞれ VLAN 10 と 20 に配置されます。
- ▶ BladeServer3 上では、両方のポートが Broadcom BASP ソフトウェアによってチームに構成され、OS には単一の論理リンクとして認識されます。これらのポートは、このサーバーへの Cisco Systems IGESM のポートで構成されているとおり、アクセス VLAN 30 を使用します。
- ▶ BladeServer4 では、両方のポートが Broadcom BASP ソフトウェアによってチームに構成され、OS には単一の論理リンクとして認識されます。これらのポートは、802.1Q トランキングを使用して VLAN 35、40、45、および 50 をサポートします。

### ステップ 3.1: 第 1 の Cisco Systems IGESM (CIGESM1) の構成

表 7-9 では、CIGESM1 を構成するために使用されるステップバイステップの手順を説明し、CLI と CMS の両方のコマンドを示します。

**重要：** Cisco Systems IGESM 上でサポートされる CMS の現行バージョンでは、トランクに配置される VLAN を完全に制御する機能に制限があります。許可するように設定していても、トランクには常に VLAN 1 と、1001 から 1005 が含まれます。この制限があるため、実動構成のトランク上で許可される VLAN を制御しようとしている場合、この機能の使用は適さない場合があります。

表 7-9 CIGESM1 の構成

説明とコメント	CIGEMS1 に対する IOS CLI からのアクション	CIGEMS1 に対する CMS からのアクション
<p>ステップ 3.1.1: <i>CIGESM1</i> に対して必要な <i>VLAN</i> を構成します。 VLAN 10、15、30、35、40、45、および 50 を作成します（このデモンストレーションでは、VLAN 10 と 15 のみに名前を付けます）。</p>	<p>使用可能モードから次の手順で行います。</p> <pre>config t vlan 10  name Web vlan 15  name User vlan 30,35,40,45,50</pre> <p>VLAN 番号とコンマの間にスペースを入れないことに注意してください。</p>	<p>CMS インターフェースから次の手順で行います。</p> <ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「<b>VLAN</b>」→「<b>VLAN</b>」をクリックします。</li> <li>2. 「<b>Configure VLANs</b>」タブをクリックします。</li> <li>3. 「<b>Create</b>」をクリックします。</li> <li>4. 「<b>VLAN ID</b>」フィールドに 10 と入力します。</li> <li>5. 「<b>VLAN Name</b>」フィールドに Web と入力します。</li> <li>6. 「<b>OK</b>」をクリックします。</li> <li>7. 「<b>Create</b>」をクリックします。</li> <li>8. 「<b>VLAN ID</b>」フィールドに 15 と入力します。</li> <li>9. 「<b>VLAN Name</b>」フィールドに User と入力します。</li> <li>10. 「<b>OK</b>」をクリックします。</li> <li>11. 「<b>Create</b>」をクリックします。</li> <li>12. 「<b>VLAN ID</b>」フィールドに 30 と入力します（名前のフィールドはデフォルトのままにします）。</li> <li>13. 「<b>OK</b>」をクリックします。</li> <li>14. 前の 3 つのステップを繰り返して、VLAN 35、40、45、および 50 を作成します。</li> <li>15. 「<b>Apply</b>」をクリックします。</li> <li>16. 「<b>Refresh</b>」をクリックして新規に作成した VLAN を表示します。</li> </ol>
<p>ステップ 3.1.2: 6500 へのリンク・アグリゲーションを構成します。</p> <p>この例では、LACP を使用してアグリゲーションを構成します。</p> <p>ポート g0/17 と g0/18 は 6500-1 に接続します。</p> <p>ポート g0/19 と g0/20 は 6500-3 に接続します。</p>	<pre>int range g0/17 -18 description To-6500-1 channel-group 1 mode active</pre> <p>これにより、<i>Port-Channel1</i> という名前の論理インターフェースが作成され、インターフェース g0/17 と g0/18 がこのインターフェースに配置されます。</p> <pre>int range g0/19 - 20 description To-6500-3 channel-group 2 mode active</pre> <p>これにより、<i>Port-Channel2</i> という名前の論理インターフェースが作成され、インターフェース g0/19 と g0/20 がこのインターフェースに配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「<b>Port</b>」→「<b>EtherChannels</b>」をクリックします。</li> <li>2. 「<b>Create</b>」をクリックします。</li> <li>3. ポート <b>Gi0/17</b> と <b>Gi0/18</b> の隣にあるチェック・ボックスを選択します。</li> <li>4. 「<b>Group [1-6]</b>」フィールドに 1 と入力して、使用するポート・チャネルを選択します。</li> <li>5. 「<b>OK</b>」をクリックします。</li> <li>6. 「<b>Create</b>」をクリックします。</li> <li>7. ポート <b>Gi0/19</b> と <b>Gi0/20</b> の隣にあるチェック・ボックスを選択します。</li> <li>8. 「<b>Group [1-6]</b>」フィールドに 2 と入力して、使用するポート・チャネルを選択します。</li> <li>9. 「<b>OK</b>」をクリックします。</li> <li>10. 「<b>Apply</b>」または「<b>OK</b>」をクリックします。</li> </ol>

説明とコメント	CIGEMS1 に対する IOS CLI からのアクション	CIGEMS1 に対する CMS からのアクション
<p>ステップ 3.1.3: 6500 への 802.1Q トランッキングを構成し、許可される VLAN を追加します。個々の VLAN を許可する行では、番号とコンマの間にスペースを入れることはできないので注意してください。</p> <p>また、デフォルトでは VLAN 2 がこれらのポートのネイティブ VLAN です。</p>	<pre>int port-channel 1 description EtherChannel-To-6500-1 switchport trunk native vlan 2 switchport trunk allowed vlan 2,10,15,30,35,40,45,50 switchport mode trunk</pre> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p> <pre>int port-channel 2 description EtherChannel-To-6500-3 switchport trunk native vlan 2 switchport trunk allowed vlan 2,10,15,30,35,40,45,50 switchport mode trunk</pre>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. 「po1」をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Trunk-Allowed VLAN」フィールドに 2,10,15,30,35,40,45,50 と入力します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> </ol> <p>po2 に対してこの手順を繰り返します。  <b>重要:</b> CMS の現行バージョンの制限により、許可される VLAN には常に VLAN 1 と 1001 から 1005 が含まれます。このため、6500 側の設定値とミスマッチが生じる可能性があり、その結果としてアグリゲーションがダウン状態になることがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>
<p>ステップ 3.1.4: BladeServer1 への 802.1Q トランッキングを構成し、許可される VLAN を追加します。</p>	<pre>int g0/1 switchport trunk allowed vlan 2,10,15</pre> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p> <p>これにより、VLAN 2、10、および 15 が BladeServer1 の第 1 の NIC に到達できます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/1</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Trunk-Allowed VLAN」フィールドに 2,10,15 と入力します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> </ol> <p><b>重要:</b> ステップ 3.1.3 で説明したように、CMS の現行バージョンの制限により、許可される VLAN には常に VLAN 1 と 1001 から 1005 が含まれます。このため、ブレード・サーバー側の設定値とのミスマッチが生じる可能性があり、その結果としてトランクが期待どおり動作しないことがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>



説明とコメント	CIGEMS1 に対する IOS CLI からのアクション	CIGEMS1 に対する CMS からのアクション
ステップ 3.1.5: <i>BladeServer2</i> へのアクセス・リンクを構成し、アクセス VLAN を設定します。	<pre>int g0/2 switchport mode access switchport access vlan 10</pre> <p>これにより、BladeServer2 の第 1 の NIC が VLAN 10 に配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/2</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Administrative Mode」フィールドの「Static Access」を選択します。</li> <li>5. 「Static-Access VLAN」フィールドに 10 と入力します。</li> <li>6. 「OK」をクリックします。</li> <li>7. 「Apply」または「OK」をクリックします。</li> </ol>
ステップ 3.1.6: <i>BladeServer3</i> へのアクセス・リンクを構成し、アクセス VLAN を設定します。	<pre>int g0/3 switchport mode access switchport access vlan 30</pre> <p>これにより、BladeServer3 の第 1 の NIC が VLAN 30 に配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/3</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Administrative Mode」フィールドの「Static Access」を選択します。</li> <li>5. 「Static-Access VLAN」フィールドに 30 と入力します。</li> <li>6. 「OK」をクリックします。</li> <li>7. 「Apply」または「OK」をクリックします。</li> </ol>
ステップ 3.1.7: <i>BladeServer4</i> への 802.1Q トランキングを構成し、許可される VLAN を追加します。	<pre>int g0/4 switchport trunk allowed vlan 2,35,40,45,50 end</pre> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/4</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Trunk-Allowed VLAN」フィールドに 2,35,40,45,50 と入力します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> </ol> <p><b>重要:</b> ステップ 3.1.3 で説明したように、CMS の現行バージョンの制限により、許可される VLAN には常に VLAN 1 と 1001 から 1005 が含まれます。このため、ブレード・サーバー側の設定値とのミスマッチが生じる可能性があります。その結果としてトランクが期待どおり動作しないことがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>
ステップ 3.1.8: <i>Cisco Systems IGESM</i> の構成を NVRAM に保管します。 このステップを実行しなければ、BladeCenter の電源をオフにした場合、または Cisco Systems IGESM をその他の方法で再始動した場合に、Cisco Systems IGESM に対する変更がすべて失われます。	<b>copy running-config startup-config</b>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「Administration」→「Save Configuration」をクリックします。</li> <li>2. 「Source」は「Running Configuration」に設定されたままにします。</li> <li>3. 「Destination」は「Startup Configuration」を選択します。</li> <li>4. 「Save」をクリックします。</li> </ol>

### ステップ3.2: 第2のCisco Systems IGESM (CIGESM2) の構成

表 7-10 では、CIGESM2 を構成するために使用されるステップバイステップの手順を説明し、CLI と CMS の両方のコマンドを示します。

**重要 :** Cisco Systems IGESM 上でサポートされる CMS の現行バージョンでは、トランクに配置される VLAN を完全に制御する機能に制限があります。許可するように設定していても、トランクには常に VLAN 1 と、1001 から 1005 が含まれます。この制限があるため、実動構成のトランク上で許可される VLAN を制御しようとしている場合、この機能の使用は適さない場合があります。

表 7-10 CIGESM2 の構成

説明とコメント	CIGESM2 に対する IOS CLI からのアクション	CIGESM2 に対する CMS からのアクション
<p>ステップ 3.2.1: CIGESM2 に対して必要な VLAN を構成します。VLAN 20、25、30、35、40、45、および 50 を作成します (このデモンストレーションでは、VLAN 20 と 25 のみに名前を付けます)。</p>	<p>使用可能モードから次の手順で行います。</p> <pre> config t vlan 20   name Application vlan 25   name Backup vlan 30,35,40,45,50           </pre> <p>VLAN 番号とコンマの間にスペースを入れないことに注意してください。</p>	<p>CMS インターフェースから次の手順で行います。</p> <ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. 「Configure VLANs」タブをクリックします。</li> <li>3. 「Create」をクリックします。</li> <li>4. 「VLAN ID」フィールドに 20 と入力します。</li> <li>5. 「VLAN Name」フィールドに Application と入力します。</li> <li>6. 「OK」をクリックします。</li> <li>7. 「Create」をクリックします。</li> <li>8. 「VLAN ID」フィールドに 25 と入力します。</li> <li>9. 「VLAN Name」フィールドに Backup と入力します。</li> <li>10. 「OK」をクリックします。</li> <li>11. 「Create」をクリックします。</li> <li>12. 「VLAN ID」フィールドに 30 と入力します (名前のフィールドはデフォルトのままにします)。</li> <li>13. 「OK」をクリックします。</li> <li>14. 前の 3 つのステップを繰り返して、VLAN 35、40、45、および 50 を作成します。</li> <li>15. 「Apply」をクリックします。</li> <li>16. 「Refresh」をクリックして新規に作成した VLAN を表示します。</li> </ol>

説明とコメント	CIGEMS2 に対する IOS CLI からのアクション	CIGEMS2 に対する CMS からのアクション
<p>ステップ 3.2.2: 6500 へのリンク・アグリゲーションを構成します。</p> <p>この例では、LACP を使用してアグリゲーションを構成します。ポート g0/17 と g0/18 は 6500-1 に接続します。ポート g0/19 と g0/20 は 6500-3 に接続します。</p>	<pre> <b>int range g0/17 -18</b> <b>description To-6500-1</b> <b>channel-group 1 mode active</b> </pre> <p>これにより、<i>Port-Channel1</i> という名前の論理インターフェースが作成され、インターフェース g0/17 と g0/18 がこのインターフェースに配置されます。</p> <pre> <b>int range g0/19 - 20</b> <b>description To-6500-3</b> <b>channel-group 2 mode active</b> </pre> <p>これにより、<i>Port-Channel2</i> という名前の論理インターフェースが作成され、インターフェース g0/19 と g0/20 がこのインターフェースに配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「Port」→「EtherChannels」をクリックします。</li> <li>2. 「Create」をクリックします。</li> <li>3. ポート <b>Gi0/17</b> と <b>Gi0/18</b> の隣にあるチェック・ボックスを選択します。</li> <li>4. 「Group [1-6]」フィールドに 1 と入力して、使用するポート・チャネルを選択します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Create」をクリックします。</li> <li>7. ポート <b>Gi0/19</b> と <b>Gi0/20</b> の隣にあるチェック・ボックスを選択します。</li> <li>8. 「Group [1-6]」フィールドに 2 と入力して、使用するポート・チャネルを選択します。</li> <li>9. 「OK」をクリックします。</li> <li>10. 「Apply」または「OK」をクリックします。</li> </ol>
<p>ステップ 3.2.3: 6500 への 802.1Q トランッキングを構成し、許可される VLAN を追加します。</p> <p>個々の VLAN を許可する行では、番号とコンマの間にスペースを入れることはできないので注意してください。</p> <p>また、デフォルトでは VLAN 2 がこれらのポートのネイティブ VLAN です。</p>	<pre> <b>int port-channel 1</b> <b>description EtherChannel-To-6500-1</b> <b>switchport trunk native vlan 2</b> <b>switchport trunk allowed vlan 2,20,25,30,35,40,45,50</b> <b>switchport mode trunk</b> </pre> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p> <pre> <b>int port-channel 2</b> <b>description EtherChannel-To-6500-3</b> <b>switchport trunk native vlan 2</b> <b>switchport trunk allowed vlan 2,20,25,30,35,40,45,50</b> <b>switchport mode trunk</b> </pre>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. 「po1」をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Trunk-Allowed VLAN」フィールドに 2,20,25,30,35,40,45,50 と入力します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> <li>7. po2 に対してこの手順を繰り返します。</li> </ol> <p><b>重要:</b> CMS の現行バージョンの制限により、許可される VLAN には常に VLAN 1 と 1001 から 1005 が含まれます。このため、6500 側の設定値とミスマッチが生じる可能性があり、その結果としてアグリゲーションがダウン状態になることがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>

説明とコメント	CIGEMS2 に対する IOS CLI からのアクション	CIGEMS2 に対する CMS からのアクション
<p>ステップ 3.2.4: <i>BladeServer1</i> への 802.1Q トランキングを構成し、許可される VLAN を追加します。</p>	<p><b>int g0/1</b>  <b>switchport trunk allowed vlan 2,20,25</b></p> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p> <p>これにより、VLAN 2、20、および 25 が <i>BladeServer1</i> の第 2 の NIC に到達できます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/1</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Trunk-Allowed VLAN」フィールドに 2,20,25 と入力します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> </ol> <p><b>重要:</b> ステップ 3.1.3 で説明したように、CMS の現行バージョンの制限により、許可される VLAN には常に VLAN 1 と 1001 から 1005 が含まれます。このため、ブレード・サーバー側の設定値とのミスマッチが生じる可能性があります。その結果としてトランクが期待どおり動作しないことがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>
<p>ステップ 3.2.5: <i>BladeServer2</i> へのアクセス・リンクを構成し、アクセス VLAN を設定します。</p>	<p><b>int g0/2</b>  <b>switchport mode access</b>  <b>switchport access vlan 20</b></p> <p>これにより、<i>BladeServer2</i> の第 2 の NIC が VLAN 20 に配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/2</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Administrative Mode」フィールドの「Static Access」を選択します。</li> <li>5. 「Static-Access VLAN」フィールドに 20 と入力します。</li> <li>6. 「OK」をクリックします。</li> <li>7. 「Apply」または「OK」をクリックします。</li> </ol>
<p>ステップ 3.2.6: <i>BladeServer3</i> へのアクセス・リンクを構成し、アクセス VLAN を設定します。</p>	<p><b>int g0/3</b>  <b>switchport mode access</b>  <b>switchport access vlan 30</b></p> <p>これにより、<i>BladeServer3</i> の第 2 の NIC が VLAN 30 に配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/3</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Administrative Mode」フィールドの「Static Access」を選択します。</li> <li>5. 「Static-Access VLAN」フィールドに 30 と入力します。</li> <li>6. 「OK」をクリックします。</li> <li>7. 「Apply」または「OK」をクリックします。</li> </ol>

説明とコメント	CIGEMS2 に対する IOS CLI からのアクション	CIGEMS2 に対する CMS からのアクション
<p>ステップ 3.2.7: <i>BladeServer4</i> への <i>802.1Q</i> トランキングを構成し、許可される VLAN を追加します。</p>	<pre>int g0/4 switchport trunk allowed vlan 2,35,40,45,50 end</pre> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p> <p>これにより、VLAN 2、35、40、45、および 50 が <i>BladeServer4</i> の第 2 の NIC に到達できます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/4</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Trunk-Allowed VLAN」フィールドに <b>2,35,40,45,50</b> と入力します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> </ol> <p><b>重要:</b> ステップ 3.1.3 で説明したように、CMS の現行バージョンの制限により、許可される VLAN には常に VLAN 1 と 1001 から 1005 が含まれます。このため、ブレード・サーバー側の設定値とのミスマッチが生じる可能性があります。その結果としてトランクが期待どおり動作しないことがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>
<p>ステップ 3.2.8: <i>Cisco Systems IGESM</i> の構成を <i>NVRAM</i> に保管します。</p> <p>このステップを実行しなければ、<i>BladeCenter</i> の電源をオフにした場合、または <i>Cisco Systems IGESM</i> をその他の方法で再始動した場合に、<i>Cisco Systems IGESM</i> に対する変更がすべて失われます。</p>	<pre>copy running-config startup-config</pre>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「Administration」→「Save Configuration」をクリックします。</li> <li>2. 「Source」は「Running Configuration」に設定されたままにします。</li> <li>3. 「Destination」は「Startup Configuration」を選択します。</li> <li>4. 「Save」をクリックします。</li> </ol>

## ステップ 4: ブレード・サーバー上のインターフェースの構成

ここでは、この例に使用するブレード・サーバーを構成するために必要な一連のアクションについて、段階を追って説明します。

この例では、次のことを前提としています。

- ▶ ブレード・サーバー上で使用されているオペレーティング・システムは **Windows 2000** です。ブレード・サーバー上でどちらのポートが「第 1」と見なされ、どちらのポートが「第 2」と見なされるかはいくつかの要因に依存し、使用されているオペレーティング・システムも少なからず関係しているので、このことは重要です。ブレード・サーバーの接続名と、その名前を得る方法については、239 ページの付録 A、『ヒント』を参照してください。
- ▶ ユーザーは管理者または同等なユーザーとして **Windows 2000** にすでにログオンしています。管理モジュール上で **KVM** インターフェースを使用する構成の場合にブレード・サーバーを選択する方法については、239 ページの付録 A、『ヒント』を参照してください。
- ▶ コマンドは示されたとおりの順序で実行されます。

▶ BladeServer1: Cisco Systems IGESM へのトランク接続。

- Broadcom Advanced Server Program (BASP、または Broadcom Advanced Control Suite と呼ばれる) ソフトウェアが BladeServer1 にインストール済みです。BladeServer1 は、BASP ソフトウェアを使用して VLAN 10、15、20、および 25 に対応する論理インターフェースを作成し、すべての IP 構成はこれらの論理インターフェースに対して実行されます (物理インターフェースに対してではなく)。
- 両方のポートが、Broadcom BASP ソフトウェアによるトランキングを使用します (一方、ロード・バランシングは使用しません)。第 1 のポートは VLAN 10 および 15 用に構成され、第 2 のポートは VLAN 20 および 25 用に構成されます。
- 次の IP アドレスを使用します (24 ビット・マスク)。

第 1 のポート、 VLAN 10 から CIGESM1 へ 10.1.10.1 (デフォルト・ゲートウェイ = 10.1.10.254)

第 1 のポート、 VLAN 15 から CIGESM1 へ 10.1.15.1

第 2 のポート、 VLAN 20 から CIGESM2 へ 10.1.20.1

第 2 のポート、 VLAN 25 から CIGESM2 へ 10.1.25.1

複数のデフォルト・ゲートウェイを使用する (たとえば、それぞれの VLAN に 1 つ、または複数の VLAN に 1 つ) かどうかの選択は、ユーザーの任意であることに注意してください。マルチホーム・システム上でのデフォルト・ゲートウェイについては、239 ページの付録 A、『ヒント』を参照してください。

▶ BladeServer2: Cisco Systems IGESM へのアクセス・リンク接続。

- どちらのポートも BASP ソフトウェアを使用せず、すべての構成がインターフェースに対して直接実行されます。
- Cisco Systems IGESM のポート設定によって、両方のポートが単純なアクセス・リンクになり、それぞれ VLAN 10 と 20 に配置されます。
- 次の IP アドレスを使用します (24 ビット・マスク)。

第 1 のポート、 CIGESM1 へ : 10.1.10.2 (デフォルト・ゲートウェイ = 10.1.10.254)

第 2 のポート、 CIGESM2 へ : 10.1.20.2

複数のデフォルト・ゲートウェイを使用する (たとえば、それぞれの VLAN に 1 つ) かどうかの選択は、ユーザーの任意であることに注意してください。マルチホーム・システム上でのデフォルト・ゲートウェイについては、239 ページの付録 A、『ヒント』を参照してください。

▶ BladeServer3 の場合 : Server Load Balancing (SLB) - アクセス接続。

- Broadcom Advanced Server Program (BASP、または Broadcom Advanced Control Suite と呼ばれる) ソフトウェアが BladeServer3 にインストール済みです。BladeServer3 は BASP ソフトウェアを使用して、単一のチームに構成された論理インターフェースを VLAN 30 用に作成し、IP 構成はこの単一の論理インターフェースに対して実行されます (物理インターフェースに対してではなく)。
- この論理ポートは、CIGESM1 (ポート g0/3) と CIGESM2 (ポート g0/3) の両方に接続し、それぞれの Cisco Systems IGESM のアクセス・ポート設定を使用して VLAN 30 に配置されます。すべての IP 構成は、この単一の論理インターフェースに対して実行されます (物理インターフェースに対してではなく)。
- 次の IP アドレスを使用します (24 ビット・マスク)。

BASP 論理ポート、 CIGESM1 へ : 10.1.30.3 (デフォルト・ゲートウェイ = 10.1.30.254)

▶ BladeServer4 の場合 : Server Load Balancing (SLB) - トランク接続。

- Broadcom Advanced Server Program (BASP、または Broadcom Advanced Control Suite と呼ばれる) ソフトウェアが BladeServer4 にインストール済みです。BladeServer4 は BASP ソフトウェアを使用して、単一のチームに構成されたエレメントを作成しま

す。さらにこれを使用して、BladeServer4 上で使用されるそれぞれの VLAN (VLAN 35、40、45、および 50) ごとに 1 つずつ、4 つの論理インターフェースが作成されます。また、すべての IP 構成はこれら 4 つの論理インターフェースに対して実行されます (物理インターフェースに対してではなく)。

- この論理ポートは、CIGESM1 (ポート g0/4) と CIGESM2 (ポート g0/4) の両方に接続し、それぞれの Cisco Systems IGESM のポート設定によって LAN 35、40、45、および 50 を使用します。
- 次の IP アドレスを使用します (24 ビット・マスク)。

第 1 のポート、 CIGESM1 への VLAN 10: 10.1.35.4 (デフォルト・ゲートウェイ = 10.1.35.254)

第 1 のポート、 CIGESM1 への VLAN 15: 10.1.40.4

第 2 のポート、 CIGESM2 への VLAN 20: 10.1.45.4

第 2 のポート、 CIGESM2 への VLAN 25: 10.1.50.4

複数のデフォルト・ゲートウェイを使用する (たとえば、それぞれの VLAN に 1 つ、または複数の VLAN に 1 つ) かどうかの選択は、ユーザーの任意であることに注意してください。マルチホーム・システム上でのデフォルト・ゲートウェイについては、239 ページの付録 A、『ヒント』を参照してください。

### BladeServer1 を構成するためのステップバイステップの手順

表 7-11 に、BladeServer1 を構成するためのステップバイステップの手順を示します。

表 7-11 複数の VLAN を使用する 802.1Q トランク用の BladeServer1 の構成

説明とコメント	BladeServer1 上での手順 両方のイーサネット・ポート上で VLAN を使用する BASP
ステップ 4.1.1: BASP ソフトウェアを起動します。 このステップは、必要なソフトウェアがすでにインストールされていることを前提としています。	「スタート」→「プログラム」→「Broadcom」→「Broadcom Advanced Control Suite」をクリックします。 これは、ソフトウェアのデフォルト・インストールを使用したことを前提としています。また、ウィンドウ右下隅の時計の近くにあるアイコン (「Control Suite」というラベルの付いたアイコンが見つかるまでカーソルを動かします)、またはコントロール・パネルにあるアイコンを使用して、このソフトウェアを起動することもできます。
ステップ 4.1.2: それぞれ単一のインターフェースを含む 2 つのチームを作成し、名前を付けます。 このプロセスは、SLB を構成する場合と同じように見えるかもしれませんが、実際には異なります。これは、それぞれのチームに含まれる NIC はただ 1 つで、VLAN を割り当てるためだけにチームを作成しているからです (これにより、インターフェースを 802.1Q トランク・インターフェースにします)。	1. ツールバーの「Tools」→「Create a Team」をクリックします。 2. 「name」フィールドに ToCIGESM1 と入力し、「Next」をクリックします。 注: 「Team Type」はデフォルト値のままにしてください (Smart Load Balance and Fail Over)。 3. ウィンドウ左側の一番上にある NIC を選択し、上にある右向きの矢印をクリックして、この NIC を「Load Balance Members」に追加します。 ▶ 「Finish」をクリックします。 第 2 の NIC に対してステップ 4.1.2 を繰り返し、チームに ToCIGESM2 という名前を付けます。
ステップ 4.1.3a: チーム CIGESM1 に必要な VLAN を作成します。 CIGESM1 に接続するチームに VLAN 10 と 15 を作成し、名前を付けます。	1. ツールバーの「Tools」→「Configure a Team」をクリックします。 2. 「ToCIGESM1」を選択し、「OK」をクリックします。 3. ウィンドウ右側にある「Add VLAN」ボタンをクリックします。 4. 「VLAN ID」フィールドに、10 と入力します。 5. 「VLAN Name」フィールドに、VLAN10-WEB と入力します。 名前は記述的にする必要がありますが、任意の名前を指定できます。また、「Untagged VLAN」というラベルの付いたボックスはクリアされたままにしてください。 6. 「OK」をクリックしてこの VLAN を作成します。 このチームの第 2 の VLAN に対して、ステップ 4.1.3a を繰り返します。「VLAN ID」を 15 に設定し、VLAN15-USER という名前を付けます。

説明とコメント	BladeServer1 上での手順 両方のイーサネット・ポート上で VLAN を使用する BASP
<p>ステップ 4.1.3b: チーム <i>CIGESM2</i> に必要な <i>VLAN</i> を作成します。</p> <p><i>CIGESM2</i> に接続するチームに <i>VLAN 20</i> と <i>25</i> を作成し、名前を付けます。</p>	<ol style="list-style-type: none"> <li>1. ツールバーの「Tools」→「Configure a Team」をクリックします。</li> <li>2. 「ToCIGESM2」を選択し、「OK」をクリックします。</li> <li>3. ウィンドウ右側にある「Add VLAN」ボタンをクリックします。</li> <li>4. 「VLAN ID」フィールドに、20 と入力します。</li> <li>5. 「VLAN Name」フィールドに、<b>VLAN20-APPS</b> と入力します。 名前は記述的にする必要がありますが、任意の名前を指定できます。また、「Untagged VLAN」というラベルの付いたボックスはクリアされたままにしてください。</li> <li>6. 「OK」をクリックしてこの VLAN を作成します。 このチームの第 2 の VLAN に対して、ステップ 4.1.3b を繰り返します。「VLAN ID」を 25 に設定し、<b>VLAN25-BACKUP</b> という名前を付けます。</li> </ol>
<p>ステップ 4.1.4: 行った変更を <i>BASP</i> に保管します。</p> <p>このステップでは、Windows 2000 内で次の 4 つの新規論理インターフェースを作成します。</p> <ul style="list-style-type: none"> <li>▶ ToCIGESM1/VLAN10-WEB</li> <li>▶ ToCIGESM1/VLAN15-USER</li> <li>▶ ToCIGESM2/VLAN20-APPS</li> <li>▶ ToCIGESM2/VLAN25-BACKUP</li> </ul> <p>注: 「Apply」または「OK」をクリックせずに <i>BASP</i> プログラムを終了すると、構成変更が失われます。</p>	<ol style="list-style-type: none"> <li>1. メイン <i>BASP</i> ウィンドウの「Apply」をクリックします。</li> <li>2. ネットワーク接続の一時的な中断についての警告が出されたら、「Yes」ボタンをクリックします。 この時点で、<i>BASP</i> ソフトウェアは Windows 2000 ネットワーキングに使用される新規論理インターフェースを作成します。</li> </ol>
<p>ステップ 4.1.5: それぞれの <i>VLAN</i> 上で必要な <i>IP</i> アドレスを構成します。</p> <p>このステップでは、IP アドレッシング情報を追加する方法をユーザーが知っていることが前提となります。</p> <p>使用されるデフォルト・ゲートウェイは、6500 の基本 HSRP 構成の一部であることに注意してください。</p> <p>また、実動システム上では、通常は 1 つ以上の DNS サーバーを構成します。これはこの環境の一部としては含まれていませんが、ほとんどの実動ネットワークに組み込む必要があります。</p> <p>このステップでは、IP アドレッシングを物理インターフェースに直接適用することはサポートされません。</p>	<ol style="list-style-type: none"> <li>1. Windows で、「スタート」→「設定」→「ネットワークとダイヤルアップ接続」をクリックします。 元の物理ネットワーク・インターフェースとともに、4 つの新しく作成した論理インターフェースが表示されます。</li> <li>2. <b>ToCIGESM1/VLAN10-WEB</b> インターフェースを選択し、IP アドレスを次のように構成します。 <ul style="list-style-type: none"> <li>– IP アドレス: 10.1.10.1</li> <li>– マスク: 255.255.255.0</li> <li>– デフォルト・ゲートウェイ: 10.1.10.254</li> </ul> </li> <li>3. <b>ToCIGESM1/VLAN15-USER</b> インターフェースを選択し、IP アドレスを次のように構成します。 <ul style="list-style-type: none"> <li>– IP アドレス: 10.1.15.1</li> <li>– マスク: 255.255.255.0</li> </ul> </li> <li>4. <b>ToCIGESM1/VLAN20-APPS</b> インターフェースを選択し、IP アドレスを次のように構成します。 <ul style="list-style-type: none"> <li>– IP アドレス: 10.1.20.1</li> <li>– マスク: 255.255.255.0</li> </ul> </li> <li>5. <b>ToCIGESM1/VLAN25-BACKUP</b> インターフェースを選択し、IP アドレスを次のように構成します。 <ul style="list-style-type: none"> <li>– IP アドレス: 10.1.25.1</li> <li>– マスク: 255.255.255.0</li> </ul> </li> </ol>



## BladeServer2 を構成するためのステップバイステップの手順

表 7-12 に、BladeServer2 を構成するためのステップバイステップの手順を示します。

表 7-12 標準インターフェース接続用の BladeServer2 の構成

説明とコメント	BladeServer2 上での手順 BASP ソフトウェアを使用せず、両方のイーサネット・ポート上で物理アクセス・リンクを使用
<p>ステップ 4.2.1: 必要なインターフェース上で IP アドレスを直接構成します。</p> <p>このステップでは、IP アドレッシング情報を追加する方法をユーザーが知っていることが前提となります。</p> <p>使用されるデフォルト・ゲートウェイは、6500 の基本 HSRP 構成の一部であることに注意してください。</p> <p>また、実動システム上では、通常は 1 つ以上の DNS サーバーを構成します。これはこの環境の一部としては含まれていませんが、ほとんどの実動ネットワークに組み込む必要があります。</p>	<p>この手順は、2 つの NIC を備えたスタンドアロン・サーバーの構成と異なる点はありません。</p> <ol style="list-style-type: none"> <li>1. 「<b>Local Area Connection</b>」 インターフェースを選択し、IP アドレスを次のように構成します。 <ul style="list-style-type: none"> <li>– IP アドレス : 10.1.10.2</li> <li>– マスク : 255.255.255.0</li> <li>– デフォルト・ゲートウェイ : 10.1.10.254</li> </ul> </li> <li>2. 「<b>Local Area Connection 2</b>」 インターフェースを構成し、IP アドレスを次のように構成します。 <ul style="list-style-type: none"> <li>– IP アドレス : 10.1.20.2</li> <li>– マスク : 255.255.255.0</li> </ul> </li> </ol>

## BladeServer3 を構成するためのステップバイステップの手順

表 7-13 に、BladeServer3 を構成するためのステップバイステップの手順を示します。

表 7-13 単一の VLAN を使用するアクセス・リンク用の BladeServer3 の構成 (SLB を使用)

説明とコメント	BladeServer3 上での手順 両方のイーサネット・ポート上で SLB のために VLAN を使用する BASP
<p>ステップ 4.3.1: BASP ソフトウェアを起動します。</p> <p>このステップは、必要なソフトウェアがすでにインストールされていることを前提としています。</p>	<p>「スタート」 → 「プログラム」 → 「Broadcom」 → 「Broadcom Advanced Control Suite」 をクリックします。</p> <p>これは、ソフトウェアのデフォルト・インストールを使用したことを前提としています。また、ウィンドウ右下隅の時計の近くにあるアイコン（「Control Suite」というラベルの付いたアイコンが見つかるまでカーソルを動かします）を使用してこのソフトウェアを起動することもできます。</p>
<p>ステップ 4.3.2: 両方の NIC を使用してチームを作成します。</p>	<ol style="list-style-type: none"> <li>1. ツールバーの「Tools」 → 「Create a Team」 をクリックします。</li> <li>2. 「name」 フィールドに ToBoth-VLAN30 と入力し、「Next」 をクリックします。 注：「Team Type」 はデフォルト値のままにしてください（Smart Load Balance and Fail Over）。</li> <li>3. ウィンドウ左側の先頭にある NIC を選択し、上にある右向きの矢印をクリックして、この NIC を「Load Balance Members」 に追加します。</li> <li>4. ウィンドウ左側の 2 番目にある NIC を選択し、上にある右向きの矢印をクリックして、この NIC を「Load Balance Members」 に追加します。</li> <li>5. 「Finish」 をクリックします。</li> </ol>

説明とコメント	BladeServer3 上での手順 両方のイーサネット・ポート上で SLB のために VLAN を使用する BASP
<p>ステップ 4.3.4: 行った変更を BASP に保管します。</p> <p>このステップでは、Windows 2000 内で次に示す単一の新規論理インターフェースを作成します。</p> <p>► ToBoth-VLAN30</p> <p>注: 「Apply」または「OK」をクリックせずに BASP プログラムを終了すると、構成変更が失われます。</p>	<ol style="list-style-type: none"> <li>1. メイン BASP ウィンドウの「Apply」をクリックします。</li> <li>2. ネットワーク接続の一時的な中断についての警告が出されたら、「Yes」ボタンをクリックします。</li> </ol> <p>この時点で、BASP ソフトウェアは Windows 2000 ネットワーキングに使用される新規論理インターフェースを作成します。</p>
<p>ステップ 4.3.5: それぞれの VLAN 上で必要な IP アドレスを構成します。</p> <p>このステップでは、IP アドレッシング情報を追加する方法をユーザーが知っていることが前提となります。</p> <p>使用されるデフォルト・ゲートウェイは、6500 の基本 HSRP 構成の一部であることに注意してください。</p> <p>また、実動システム上では、通常は 1 つ以上の DNS サーバーを構成します。これはこの環境の一部としては含まれていませんが、ほとんどの実動ネットワークに組み込む必要があります。</p> <p>このステップでは、IP アドレッシングを物理インターフェースに直接適用することはサポートされません。</p>	<ol style="list-style-type: none"> <li>1. Windows で、「スタート」→「設定」→「ネットワークとダイヤルアップ接続」をクリックします。</li> </ol> <p>元の物理ネットワーク・インターフェースとともに、新規の論理インターフェースが表示されます。</p> <ol style="list-style-type: none"> <li>2. <b>ToCIGESM1/ToBoth-VLAN30</b> インターフェースを選択し、IP アドレスを次のように構成します。 <ul style="list-style-type: none"> <li>– IP アドレス: 10.1.30.3</li> <li>– マスク: 255.255.255.0</li> <li>– デフォルト・ゲートウェイ: 10.1.30.254</li> </ul> </li> </ol>

### BladeServer4 を構成するためのステップバイステップの手順

表 7-14 に、BladeServer4 を構成するためのステップバイステップの手順を示します。

表 7-14 複数の VLAN と SLB を使用する 802.1Q トランク用の BladeServer4 の構成

説明とコメント	BladeServer4 上での手順 両方のイーサネット・ポート上でチーミングと VLAN を使用する BASP
<p>ステップ 4.4.1: BASP ソフトウェアを起動します。</p> <p>このステップは、必要なソフトウェアがすでにインストールされていることを前提としています。</p>	<p>「スタート」→「プログラム」→「Broadcom」→「Broadcom Advanced Control Suite」をクリックします。</p> <p>これは、ソフトウェアのデフォルト・インストールを使用したことを前提としています。また、ウィンドウ右下隅の時計の近くにあるアイコン（「Control Suite」というラベルの付いたアイコンが見つかるまでカーソルを動かします）を使用してこのソフトウェアを起動することもできます。</p>
<p>ステップ 4.4.2: チームを作成し、名前を付けます。</p>	<ol style="list-style-type: none"> <li>1. ツールバーの「Tools」→「Create a Team」をクリックします。</li> <li>2. 「name」フィールドに ToBoth-Trunked と入力し、「Next」をクリックします。</li> <li>3. ウィンドウ左側の先頭にある NIC を選択し、上にある右向きの矢印をクリックして、この NIC を「Load Balance Members」に追加します。</li> <li>4. ウィンドウ左側の 2 番目にある NIC を選択し、上にある右向きの矢印をクリックして、この NIC を「Load Balance Members」に追加します。</li> <li>5. 「Finish」をクリックします。</li> </ol>

説明とコメント	BladeServer4 上での手順 両方のイーサネット・ポート上でチームングと VLAN を使用する BASP
<p>ステップ 4.4.3: チーム <i>ToBoth-Trunked</i> に必要な VLAN を作成します。 チーム <i>ToBoth-Trunked</i> のために VLAN 35、40、45、および 50 を作成し、名前を付けます。</p>	<ol style="list-style-type: none"> <li>1. ツールバーの「Tools」→「Configure a Team」をクリックします。 存在するチームはただ 1 つなので、BASP ソフトウェアは「Team Configuration」ページに直接進みます。</li> <li>2. ウィンドウ右側にある「Add VLAN」ボタンをクリックします。</li> <li>3. 「VLAN ID」フィールドに、35 と入力します。</li> <li>4. 「VLAN Name」フィールドに、VLAN35 と入力します。 名前は記述的にする必要がありますが、任意の名前を指定できます。また、「Untagged VLAN」というラベルの付いたボックスはクリアされたままにしてください。</li> <li>5. 「OK」をクリックしてこの VLAN を作成します。 このチームの残りの VLAN に対して、ステップ 4.4.3a を繰り返します。 値を次のように設定します。 <ul style="list-style-type: none"> <li>– 「VLAN ID」を 40 に設定し、VLAN40 という名前を付けます。</li> <li>– 「VLAN ID」を 45 に設定し、VLAN45 という名前を付けます。</li> <li>– 「VLAN ID」を 50 に設定し、VLAN50 という名前を付けます。</li> </ul> </li> </ol>
<p>ステップ 4.4.4: 行った変更を BASP に保管します。 このステップでは、Windows 2000 内で次の 4 つの新規論理インターフェースを作成します。</p> <ul style="list-style-type: none"> <li>▶ ToBoth-Trunked/VLAN35</li> <li>▶ ToBoth-Trunked/VLAN40</li> <li>▶ ToBoth-Trunked/VLAN45</li> <li>▶ ToBoth-Trunked/VLAN50</li> </ul> <p>注: 「Apply」または「OK」をクリックせずに BASP プログラムを終了すると、構成変更が失われます。</p>	<ol style="list-style-type: none"> <li>1. メイン BASP ウィンドウの「Apply」をクリックします。</li> <li>2. ネットワーク接続の一時的な中断についての警告が出されたら、「Yes」ボタンをクリックします。 この時点で、BASP ソフトウェアは Windows 2000 ネットワーキングに使用される新規論理インターフェースを作成します。</li> </ol>
<p>ステップ 4.5.5: それぞれの VLAN 上で必要な IP アドレスを構成します。 このステップでは、IP アドレッシング情報を追加する方法をユーザーが知っていることが前提となります。 使用されるデフォルト・ゲートウェイは、6500 の基本 HSRP 構成の一部であることに注意してください。 また、実動システム上では、通常は 1 つ以上の DNS サーバーを構成します。これはこの環境の一部としては含まれていませんが、ほとんどの実動ネットワークに組み込む必要があります。 このステップでは、IP アドレッシングを物理インターフェースに直接適用することはサポートされません。</p>	<ol style="list-style-type: none"> <li>1. Windows で、「スタート」→「設定」→「ネットワークとダイヤルアップ接続」をクリックします。 元の物理ネットワーク・インターフェースとともに、4 つの新しく作成した論理インターフェースが表示されます。</li> <li>2. <b>ToBoth-Trunked/VLAN35</b> インターフェースを選択し、IP アドレスを次のように構成します。 <ul style="list-style-type: none"> <li>– IP アドレス: 10.1.35.4</li> <li>– マスク: 255.255.255.0</li> <li>– デフォルト・ゲートウェイ: 10.1.35.254</li> </ul> </li> <li>3. <b>ToBoth-Trunked/VLAN40</b> インターフェースを選択し、IP アドレスを次のように構成します。 <ul style="list-style-type: none"> <li>– IP アドレス: 10.1.40.4</li> <li>– マスク: 255.255.255.0</li> </ul> </li> <li>4. <b>ToBoth-Trunked/VLAN45</b> インターフェースを選択し、IP アドレスを次のように構成します。 <ul style="list-style-type: none"> <li>– IP アドレス: 10.1.45.4</li> <li>– マスク: 255.255.255.0</li> </ul> </li> <li>5. <b>ToBoth-Trunked/VLAN50</b> インターフェースを選択し、IP アドレスを次のように構成します。 <ul style="list-style-type: none"> <li>– IP アドレス: 10.1.50.4</li> <li>– マスク: 255.255.255.0</li> </ul> </li> </ol>

## ステップ 5: デバイスの再接続

これは、接続を完全に動作させるために行う最後のステップです。この手順は、ステップ 1 で使用したすべての手順の逆です。リンクを再確立する方法について詳しくは、128 ページの表 7-2 を参照してください。

## ステップ 6: 構成の検証

ここでは、正しく要求どおりの動作が行われることを検証するためのオプションを示します。

### ブレード・サーバーの正しい動作の検証

BladeServer1、3、および 4 上でチームングと VLAN の必要な構成が行われているかどうか、BASP アプリケーションを検討します（165 ページの図 7-9、166 ページの図 7-11、および 166 ページの図 7-12 を参照）。VLAN が存在していて、正しいチームに所属していることを確認します。BladeServer2 に BASP 構成は存在しません（165 ページの図 7-10 を参照）。

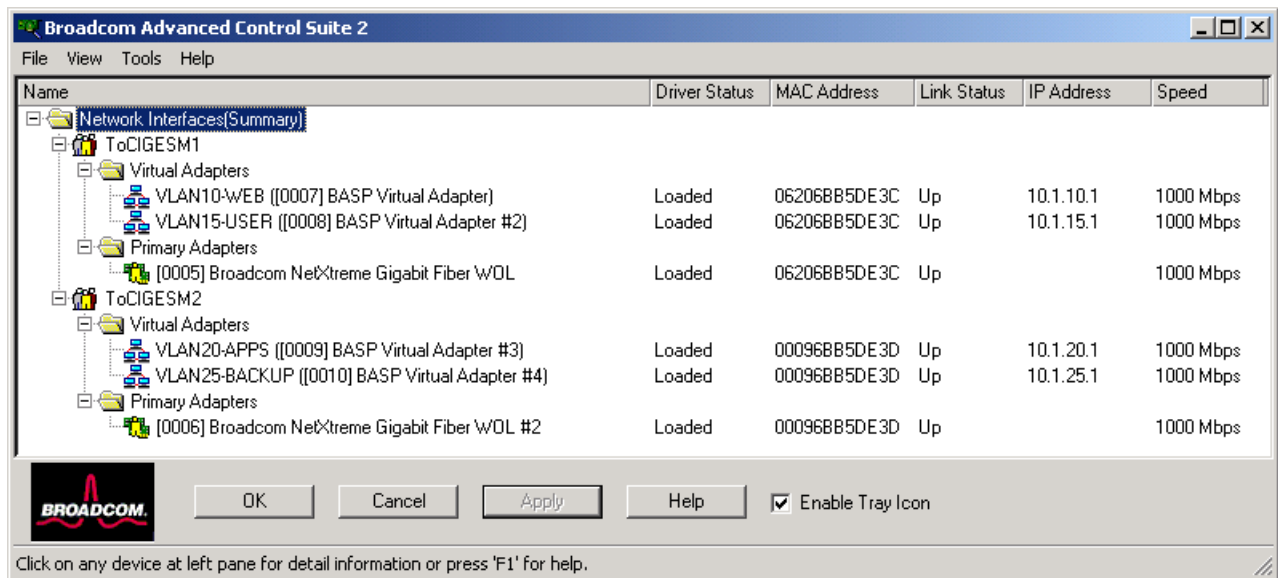


図 7-9 BladeServer1 の BASP 構成

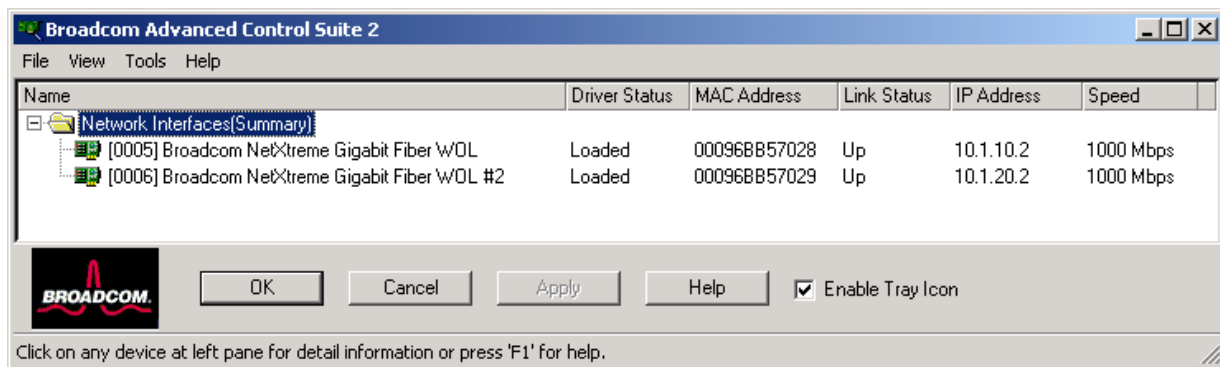


図 7-10 BladeServer2 の BASP 構成 (BASP は BladeServer2 では使用されない)

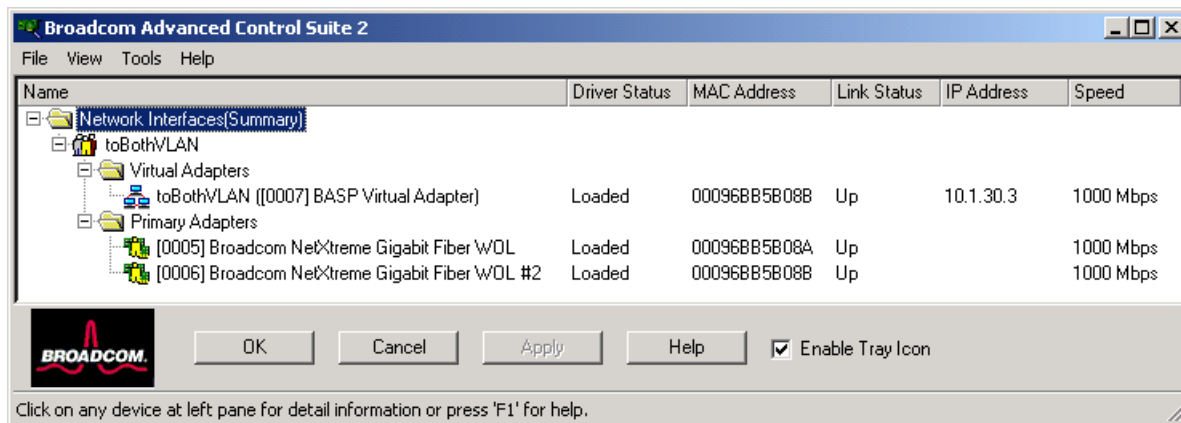


図 7-11 BladeServer3 のBASP 構成

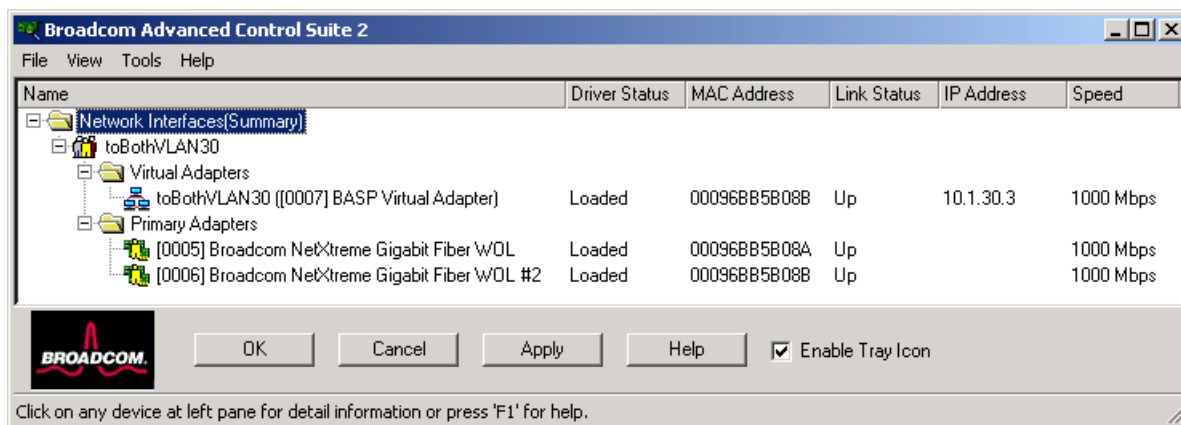


図 7-12 BladeServer4 のBASP 構成

Windows 2000 ネットワーキング・ツールを使用して、論理ネットワークと物理ネットワークを確認します。次の図は、BladeServer 1、2、3、および 4 を示しています。

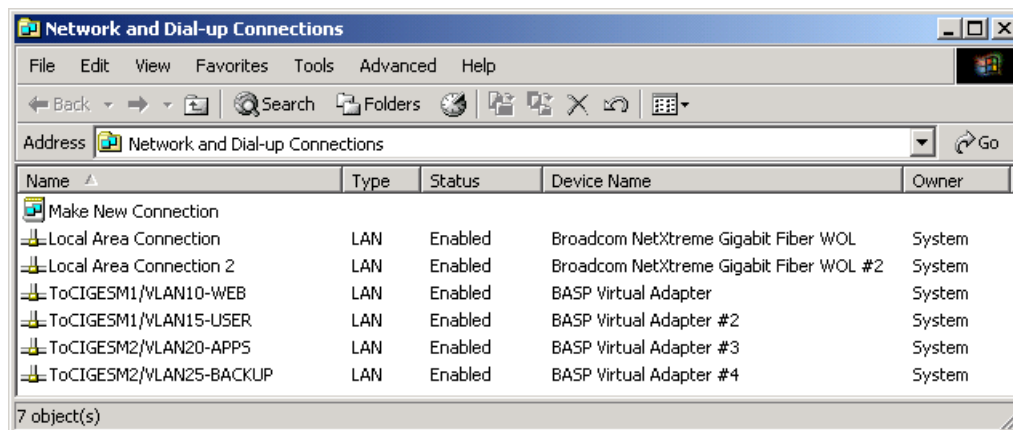


図 7-13 BladeServer1 の物理インターフェースと論理インターフェースを示す Windows 2000 ネットワーキング

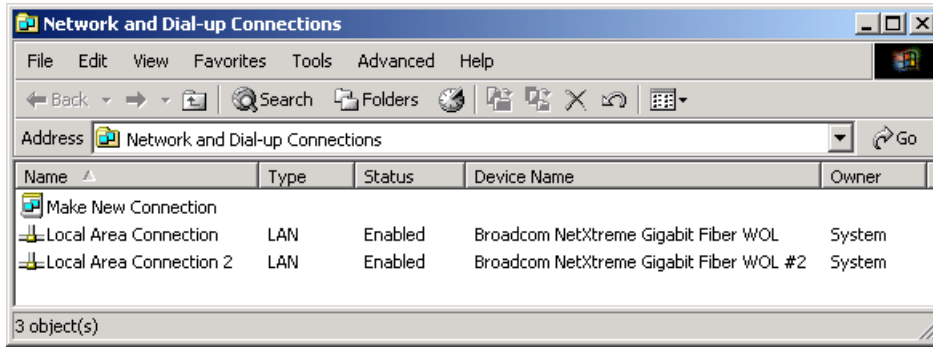


図 7-14 BladeServer2 の物理インターフェースのみを示す Windows 2000 ネットワーキング

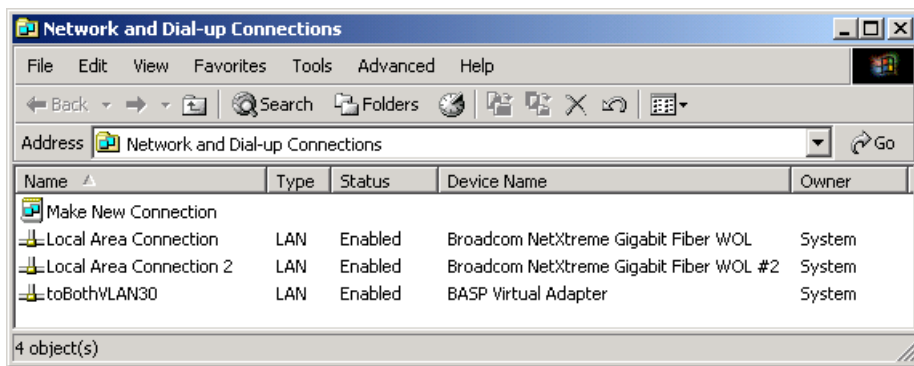


図 7-15 BladeServer3 の物理インターフェースのみを示す Windows 2000 ネットワーキング

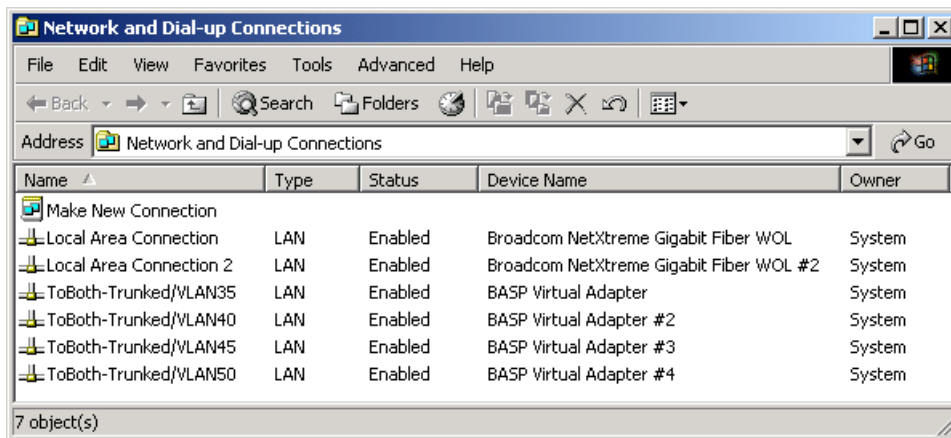


図 7-16 BladeServer4 の物理インターフェースのみを示す Windows 2000 ネットワーキング

CMD プロンプトから（「スタート」→「ファイル名を指定して実行」→cmd→「OK」）、**ipconfig** コマンドを実行し、それぞれのブレード・サーバー上で適切なインターフェースに正しい IP 構成が指定されていることを確認します（これらが逆になっていないことを確認してください。つまり、名前が変更されていないとすると、*Local Area Connection* に必要な IP アドレスが、*Local Area Connection 2* という名前の接続に対して指定されていないか調べます）。チームに構成されたインターフェースの場合は、**ipconfig** によって報告される IP アドレスが、予想される論理インターフェース上のものであることを確認します。

さまざまなボックスから ping テストを実行します。

次に示すテストは、同じ VLAN 上のブレード・サーバー間の接続をテストします。ping は該当する Cisco Systems IGESM まで進むだけで、他のブレード・サーバーに戻ります（アグリゲーション・スイッチまでは進みません）。

- ▶ BladeServer1 から 10.1.10.2（BladeServer2 の VLAN 10 接続）への ping
- ▶ BladeServer1 から 10.1.20.2（BladeServer2 の VLAN 20 接続）への ping

次に示すとおり、Cisco Systems IGESM を経由して 6500 に至る接続をテストします。

- ▶ BladeServer1 から 10.1.10.254（6500 上の HSRP アドレス）への ping
- ▶ BladeServer1 から 10.1.15.254（6500 上の HSRP アドレス）への ping
- ▶ BladeServer1 から 10.1.20.254（6500 上の HSRP アドレス）への ping
- ▶ BladeServer1 から 10.1.25.254（6500 上の HSRP アドレス）への ping
- ▶ BladeServer2 から 10.1.10.254（6500 上の HSRP アドレス）への ping
- ▶ BladeServer2 から 10.1.20.254（6500 上の HSRP アドレス）への ping
- ▶ BladeServer3 から 10.1.30.254（6500 上の HSRP アドレス）への ping
- ▶ BladeServer4 から 10.1.35.254（6500 上の HSRP アドレス）への ping
- ▶ BladeServer4 から 10.1.40.254（6500 上の HSRP アドレス）への ping
- ▶ BladeServer4 から 10.1.45.254（6500 上の HSRP アドレス）への ping
- ▶ BladeServer4 から 10.1.50.254（6500 上の HSRP アドレス）への ping

この時点で、ここに示したとおりに ping を実行できることが必要です。これらのアドレスを ping できない場合は、前述の構成検査に異常がなければ、次の節に進んでこの構成に含まれる他のコンポーネントを検査してください。

この時点で、SLB を実行するサーバー（BladeServer3 および BladeServer4）上でリンクのダウンを試すこともできます。目的のブレード・サーバーから、サブネットの該当する HSRP アドレスへの連続 ping（-t オプション）を開始し、Cisco Systems IGESM に進んで、どちらか一方の Cisco Systems IGESM 上で G0/3 と G0/4 のシャットダウンを試行します（両方の g0/3 ポートまたは両方の g0/4 ポートを同時にダウン状態にしないでください。このようにすると、関連したブレード・サーバーがすべての接続を失うからで、これは SLB 接続のポートをすべて強制終了した場合に予期される動作です）。1 つか 2 つの ping が失われることがあります。全般的には g0/3 または g0/4 のどちらかをダウン状態にしても関係なく ping が継続する必要があります。

この構成では（この例に示す）、Cisco Systems IGESM 上の管理 VLAN を ping することはできません。これは、管理 VLAN がブレード・サーバーとは異なる VLAN 上にあるからです。また、いくつかの理由から、Cisco Systems IGESM によって使用されている管理 VLAN と同じ VLAN にブレード・サーバーを配置しないことを強くお勧めします。

### **Cisco Systems IGESM での正しい動作の確認**

次のコマンドを使用して、Cisco Systems IGESM の構成を確認してください。

正しいスイッチを使用していることを確認するには、**show platform summary** コマンドを使用します（現在使用しているスロットが表示されます。例：スロット 1 = CIGESM1、スロット 2 = CIGESM2）。

**show run** コマンドを実行して、ここまでのステップで入力した目的の構成と一致していることを確認します。

**show logging** コマンドを実行して、予期しないエラーが発生しなかったかどうか調べます。

CIGESM1 上での作業：

- ▶ **show int g0/1 status** を実行します。status - connected および vlan - trunk が表示されます。
- ▶ **show int g0/2 status** を実行します。status - connected および vlan - 10 が表示されます。

- ▶ **show int g0/3 status** を実行します。status - connected および vlan -30 が表示されます。
- ▶ **show int g0/4 status** を実行します。status - connected および vlan - trunk が表示されます。

CIGESM2 上での作業：

- ▶ **show int g0/1 status** を実行します。status - connected および vlan - trunk が表示されます。
- ▶ **show int g0/2 status** を実行します。status - connected および vlan -20 が表示されます。
- ▶ **show int g0/3 status** を実行します。status - connected および vlan -30 が表示されます。
- ▶ **show int g0/4 status** を実行します。status - connected および vlan - trunk が表示されます。

**show interface trunk module 0** コマンドを実行し、正しい出力が得られることを確認します（両方の Cisco Systems IGESM に対する出力が *同様* であることが必要です）。

Port	Mode	Encapsulation	Status	Native vlan
Gi0/1	on	802.1q	trunking	2
Gi0/2	off	802.1q	not-trunking	2
Gi0/3	off	802.1q	not-trunking	2
Gi0/4	on	802.1q	trunking	2
.	.	.	.	.
Gi0/17	on	802.1q	trunk-inbndl	2 (Po1)
Gi0/18	on	802.1q	trunk-inbndl	2 (Po1)
Gi0/19	on	802.1q	trunk-inbndl	2 (Po2)
Gi0/20	on	802.1q	trunk-inbndl	2 (Po2)

**show etherchannel summary** コマンドを実行して、正しい出力が得られることを確認します（両方の Cisco Systems IGESM に対する出力が *同様* であることが必要です）。

```
Flags: D - down          P - in port-channel
       I - stand-alone s - suspended
       H - Hot-standby (LACP only)
       R - Layer3        S - Layer2
       u - unsuitable for bundling
       U - in use        f - failed to allocate aggregator
       d - default port
```

```
Number of channel-groups in use: 2
Number of aggregators:          2
```

Group	Port-channel	Protocol	Ports
1	Po1(SU)	LACP	Gi0/17(Pd) Gi0/18(P)
2	Po2(SU)	LACP	Gi0/19(Pd) Gi0/20(P)

**show etherchannel 1 port-channel** コマンドを実行して、正しい出力が得られることを確認します（両方の Cisco Systems IGESM に対する出力が *同様* であることが必要です）。  
port-channel 2 に対して手順を繰り返します。

Port-channels in the group:

```
-----
Port-channel: Po1    (Primary Aggregator)
-----
Age of the Port-channel   = 00d:03h:36m:48s
Logical slot/port        = 1/0           Number of ports = 2
HotStandBy port = null
Port state                = Port-channel Ag-Inuse
Protocol                  = LACP
```



```

Ports in the Port-channel:
Index   Load   Port      EC state   No of bits
-----+-----+-----+-----+-----
0       00      Gi0/17    Active     0
0       00      Gi0/18    Active     0

```

**show cdp neighbors** コマンドの出力を確認します。この表示は次のようになっている必要があります (CIGESM2 の場合はデバイス ID が異なる)。Cisco Systems IGESM は、管理モジュール・インターフェースを介して相互を認識できることに注意してください。

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge  
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
DC6500-1	Gig 0/18	127	R S I	WS-C6506	Gig 2/26
DC6500-1	Gig 0/17	127	R S I	WS-C6506	Gig 2/25
DC6500-3	Gig 0/20	177	R S I	WS-C6506	Gig 2/26
DC6500-3	Gig 0/19	177	R S I	WS-C6506	Gig 2/25
CIGESM2	Gig 0/15	159	S I	OS-CIGESM-Gig	0/15

### 外部スイッチ上での正しい動作の確認 (6500-1 および 6500-3)

ここでは、6500 の正しい構成と動作の確認に使用できるコマンドをいくつか示します。

基本的には、Cisco Systems IGESM について前述したものと同一コマンドのセットを実行できます。当然、出力に多少の違いはありますが、ポートのチャンネルとトランクが適切に設定されていて、正しい VLAN を伝送していることを確認できます。また、管理ダウン状態のポートについても注意してください。

次のアドレスを ping できることが必要です。

- ▶ BladeServer1 の 10.1.10.1 への ping
- ▶ BladeServer1 の 10.1.15.1 への ping
- ▶ BladeServer1 の 10.1.20.1 への ping
- ▶ BladeServer1 の 10.1.25.1 への ping
- ▶ BladeServer2 の 10.1.10.2 への ping
- ▶ BladeServer2 の 10.1.20.2 への ping
- ▶ BladeServer3 の 10.1.30.3 への ping
- ▶ BladeServer4 の 10.1.35.4 への ping
- ▶ BladeServer4 の 10.1.40.4 への ping
- ▶ BladeServer4 の 10.1.45.4 への ping
- ▶ BladeServer4 の 10.1.50.4 への ping

この時点で、冗長性を検査することもできます。このためには、ネットワークのさまざまなエレメントをダウン状態にして (リンクまたはデバイス、またはその両方)、ネットワークが期待どおり動作するかどうか確認します。

## 7.5.3 トポロジー 3a: デュアル Cisco Systems IGESM、RSPAN を使用した 2 ポート・アグリゲーション

このトポロジー (174 ページの図 7-18) はトポロジー 2 と類似していますが、それぞれの Cisco Systems IGESM 上に専用 RSPAN ポートを設けるオプションを示しています。この設計の欠点は、スパンニング・ツリー・コストによって 2 つの EtherChannel アップリンクが転送状態になったとき、EtherChannel アップリンクの 1 つに障害が起これば、標準を上回るオーバー・サブスクリプションが発生し、パフォーマンスに影響する可能性があることです。

トポロジー 2 の場合と同様に、このトポロジーでも高可用性が問題になるケースが 1 つあります。それは、単一の Cisco Systems IGESM からのアップリンクがすべてダウン状態にな

り、Cisco Systems IGESM 自体はダウン状態にならなかった場合です。このケースでは、ブレード・サーバー NIC がアップストリームの障害を検出できず、問題が発生します。正しく構成された NIC チーミングとトランク・フェイルオーバーを使用すれば、この問題は解決します。

### このトポロジー例の RSPAN に関する簡単な説明

**重要：**RSPAN の使用に関しては特有の規則があります。これらの規則を守らなければ、予期せず望ましくない結果が生じる可能性があります。RSPAN のガイドラインと使用法は、次のロケーションで確認できます。

[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_configuration\\_guide\\_chapter09186a008007f323.html](http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008007f323.html)

[http://www.cisco.com/en/US/products/hw/switches/ps628/products\\_configuration\\_guide\\_chapter09186a00801a6ba9.html](http://www.cisco.com/en/US/products/hw/switches/ps628/products_configuration_guide_chapter09186a00801a6ba9.html)

**重要：**ここで説明する、このトポロジーのためにテストされた RSPAN リフレクター・ポートは、Cisco Systems IGESM に備わっている 4 つの外部ポートの 1 つです。未使用のブレード・サーバー・ポート（たとえば、g0/14）をリフレクター・ポートの役割に使用することも可能ですが、ブレード・サーバーを接続していた内部ポートを使用すると予期せず望ましくない動作が発生する可能性があるため、最大限に注意する必要があります。本書のためのテストはすべて、外部ポート（g0/17 から g0/20）の 1 つをリフレクター・ポートとして使用して行われました。

**重要：**すでに説明したとおり、環境に実装する前に RSPAN を理解しておくことが重要です。よく見過ごされる重要な点の 1 つとして、RSPAN 用に使用される VLAN は、BladeCenter 内のブレード・サーバー・ポートから削除 / 除去する必要があります。

**注：**「Cisco Systems Intelligent Gigabit Ethernet Switch Module for the IBM @server BladeCenter Software Configuration Guide」（Cisco Systems Intelligent Gigabit Ethernet Switch Module に付属）は、現時点では Cisco Systems IGESM 上で RSPAN を構成する正しい手順を反映していません（少なくとも、RSPAN セッションの宛先として使用される VLAN 上で **remote-span** を実行するステップを説明していません）。この資料はレビュー中で、正しい手順を反映して近日中に更新される予定です。これと同じことが、2950 上での RSPAN の使用に関して現在入手可能な Cisco 資料にも当てはまります。

**重要：**本書の制作時に行われた、Cisco Systems IGESM 上での RSPAN のテストにより、バージョン 12.1(14)AY のコードを使用すると問題が生じる可能性があることが分かりました（予期しないワイヤー速度トラフィック・ストリーミング）。この問題は、バージョン 12.1(14)AY1 以上では解決されました。RSPAN を 12.1(14)AY コードと組み合わせて使用しないことを強くお勧めします。すでに RSPAN が構成済みで、12.1(14)AY に関連したストリーミング・データの問題が生じている場合は、RSPAN を使用するモニター・セッションを削除すれば、この状態が解消します（**config term** モードで、コマンド **no monitor session x** を実行。ただし x は、RSPAN 用に構成されたモニター・セッション番号）。

この例では、単純な RSPAN を実行して、BladeServer1 への最初の接続上でやり取りされるトラフィックすべてを VLAN 500 にリダイレクトし、ポート・チャネル・リンクを経由して

6500-1 に伝送し、トラフィックはそこからポート g2/2 に接続されたスニファァーに送信されます。

172 ページの図 7-17 は、この例に示す RSPAN 構成で生じるフローを示しています。

1 つ注意点として、リフレクター・ポートの役割を果たす g0/19 には、ケーブルが接続されていません。リフレクター・ポートの役割は、モニター対象のポートからトラフィックを取り出し、RSPAN VLAN（この例では VLAN 500）に送ることができるように、内部ループバックとして機能することです。その後、このトラフィックはネットワーク内の別の場所にあるリモート・モニター・デバイスに移送されます。

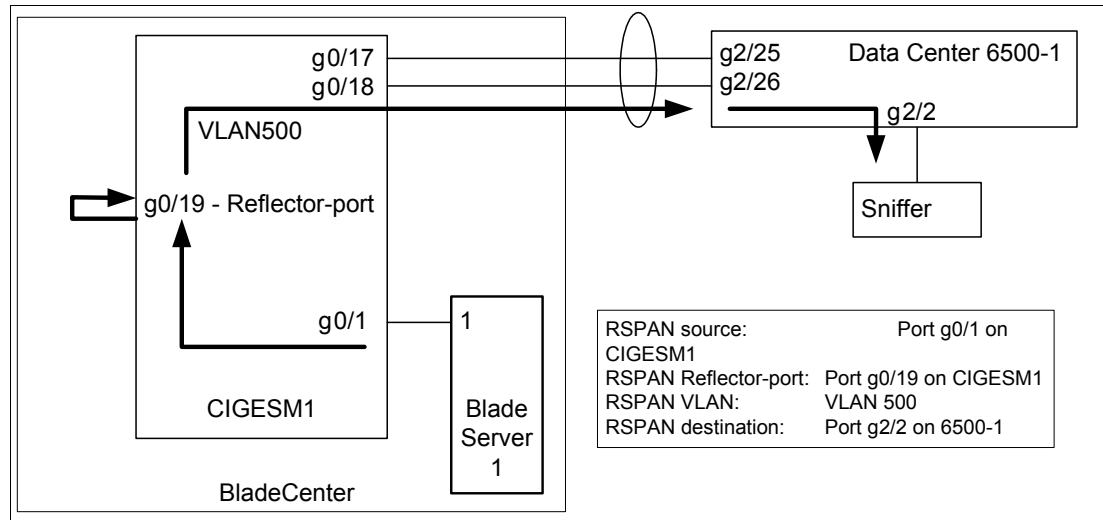


図 7-17 この例の目的の RSPAN データ・フロー

## このトポロジーにブレード・サーバーを接続するための構成

**重要:** この章に示すブレード・サーバーの構成は、トポロジーの説明には含まれませんが、代わりにこの節にこれらの構成を示します。この説明は、サーバーをこのトポロジーに接続するために可能ないくつかの方法を理解するための参考として使用してください。これらの例は、ブレード・サーバーを構成するために必要な方法とは解釈しないでください。ある特定のサーバー接続例を確認することのみが目的の場合は、その特定の例および関連した Cisco Systems IGESM のアップストリーム接続のみを検討して、その他のブレード・サーバー構成は無視して構いません。

次のリストに、この例のブレード・サーバー構成（174 ページの図 7-18 を参照）を示します。

- ▶ **BladeServer1:** 802.1Q トランク・リンクによって複数の VLAN を NIC に伝送する。  
この構成は、複数の VLAN がブレード・サーバー内の個々の NIC にアクセスできるようにする方法を示すものです。NIC ごとに複数の VLAN を使用して、トラフィック・タイプを互いに分離する方法の 1 つを例示しています。  
Broadcom チーミング・ソフトウェアが必要ですが、冗長性は使用されません。
- ▶ **BladeServer2:** 個別の接続を経由した、アクセス・ポートから NIC への接続。  
この構成は、それぞれの NIC を標準アクセス・リンクとして使用方法を示すものです（VLAN、トランキング、または冗長性は、ブレード・サーバーの観点からは使用されません）。これは、従来はほとんどのサーバーを接続する標準的な方法だったもので、単純で効率的ですが、柔軟性はあまりありません。

この構成は、Windows 2000 に備わっているストック・ネットワーク構成ツールを使用して行います（チーミング・ソフトウェアは使用しません）。

► **BladeServer3: SLB/ チーム接続を経由した、アクセス・ポートから NIC への接続。**

この構成は、他のアップストリーム・ネットワーク（Cisco Systems IGESM）には単一のアクセス NIC として認識されるように、複数の NIC を使用する方法を示すものです。NIC を結合するためにチーミング・ドライバーを使用しますが、特殊な VLAN 構成は使用しません。Cisco Systems IGESM の観点からは、両方の接続は静的 VLAN が割り当てられた単純なアクセス・ポートとして構成されます。

- この構成は、Broadcom チーミング・ソフトウェアを使用して、リンクのバインドと平衡化を行います。チームに構成されたポートが配置される先の VLAN は、Cisco Systems IGESM が設定します（これは、このサーバーに接続する両方の Cisco Systems IGESM ポートについて同じであることが必要です）。
- この章に示す BladeServer3 の例は、アクティブ/アクティブ、または Server Load Balancing と呼ばれる機能を使用しているため、両方のインターフェースがトラフィックを同時に伝送できます。この逆がアクティブ/スタンバイ（ここには示しません）です。これはホット・スタンバイとも呼ばれ、リンクの一方のみが一度に稼働します。

► **BladeServer4: チーム /SLB 接続上で複数の VLAN をサーバーに伝送する 802.1Q トランク・リンク。**

この構成は、単一の NIC として認識されるように複数の NIC を使用しながら、この単一の論理 NIC 上で複数の VLAN を使用する方法を示すものです。この構成では、チーミング・ドライバーを使用して NIC を結合し、目的の VLAN を作成します。Cisco Systems IGESM の観点からは、両方の接続がトランク・ポートとして構成され、共通の VLAN のセットを伝送します（このサーバーの 4 つの論理 NIC に接続する両方の Cisco Systems IGESM ポートに対して、同じ VLAN を構成する必要があります）。

- この例では、Broadcom チーミング・ソフトウェアを使用してリンクのバインドと平衡化を行い、本書に例示するさまざまな VLAN を代表する論理インターフェースを作成します。
- この章に示す BladeServer4 の例は、アクティブ/アクティブ、または Server Load Balancing と呼ばれる機能を使用しているため、両方のインターフェースがトラフィックを同時に伝送できます。この逆がアクティブ/スタンバイ（ここには示しません）です。これはホット・スタンバイとも呼ばれ、リンクの一方のみが一度に稼働します。

**重要:** ブレード・サーバー 3 と 4 の可用性を最大限にするためには、トランク・フェイルオーバーも構成する必要があります（この例には示しません）。トランク・フェイルオーバー機能の構成の詳細と要件については、203 ページの 7.7、『トランク・フェイルオーバー機能の説明と構成』を参照してください。

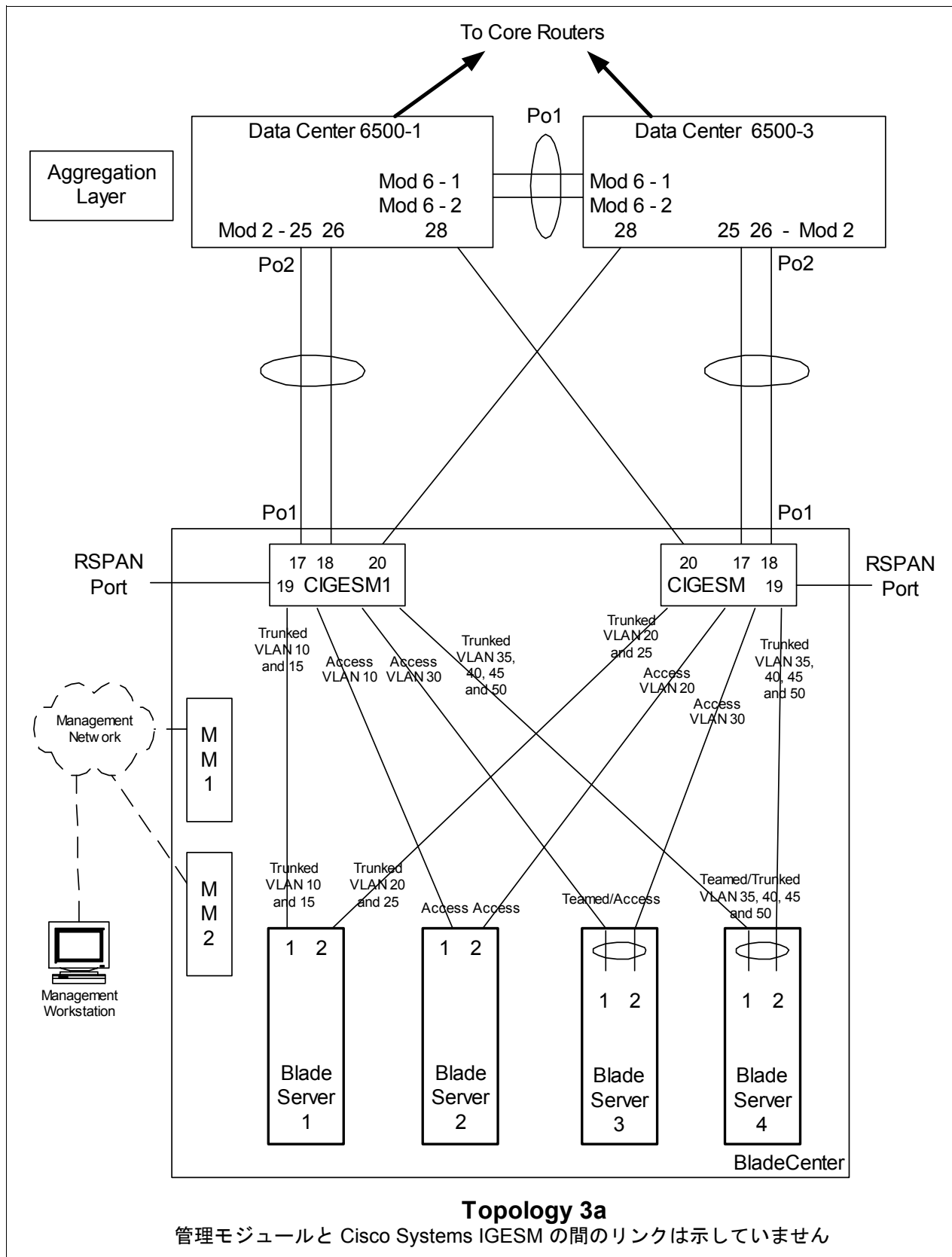


図 7-18 トポロジー 3a: デュアル Cisco Systems IGESM、RSPAN を使用した 2 ポート・アグリゲーション

## ステップ 1: リンクをダウン状態にする

構成変更を行う前に、必ずリンクを使用不可にすることをお勧めします。必要な手順については、127 ページの表 7-1 を参照してください。

## ステップ 2: 外部スイッチの構成

この例では、次のことを前提としています。

- ▶ 6500 の構成の大部分は、基本構成に含まれています（『Cat 6500 の基本構成』（113 ページ）を参照）。これは、本書の目的が、一般的な Cisco デバイスではなく BladeCenter コンポーネントを構成する方法を説明することであるからです。ここでは特に、BladeCenter に接続する 6500 ポートの構成方法を中心に説明します。
- ▶ VLAN 2 は、6500 上で基本構成の一部としてすでに作成済みです。
- ▶ 基本構成の一部として VTP ドメインがすでに命名済みで、透過に設定されています。
- ▶ 基本構成の一部として、スパンニング・ツリー・ルート・コマンドがすでに設定済みです（6500-1 を 1 次ルート、6500-3 を 2 次ルートにする）。
- ▶ ユーザーはすでにスイッチにログオンしており、スイッチは使用可能モードです。
- ▶ コマンドは示されたとおりの順序で実行されます。
- ▶ Cisco Systems IGESM への接続に使用される 6500 内の Cisco スイッチ・モジュールは 1000Base-T をベースとしており、ポートは 1Gbps 全二重のままにします。
- ▶ 6500 間のアグリゲーション・リンクが基本構成の一部としてすでに作成済みで、必要な VLAN（たとえば、2、10、15、20）を伝送しています。

表 7-15 外部スイッチの構成

説明とコメント	6500-1 上での手順	6500-3 上での手順
ステップ 2.1: 6500 から Cisco Systems IGESM へのリンク・アグリゲーションと単一リンクを構成します。 これは、6500 とそれぞれの Cisco Systems IGESM の間のポート・チャネル用です。インターフェースに説明を付けるようにすることを常にお勧めします。また、個々のポートとポート・チャネルの両方に対して、適所に Spanning-Tree guard root が追加されていることに注意してください。	<pre>config t int range g2/25 -26 switchport spanning-tree guard root description to-BladeCenter CIGESM1 channel-group 2 mode active</pre> これにより、 <i>Port-Channel2</i> という名前の論理インターフェースが作成され、インターフェース g2/25 と g2/26 がこのインターフェースに配置されます。  <pre>int g2/28 switchport spanning-tree guard root description to-BladeCenter CIGESM2</pre>	<pre>config t int range g2/25 -26 switchport spanning-tree guard root description to-BladeCenter CIGESM2 channel-group 2 mode active</pre> これにより、 <i>Port-Channel2</i> という名前の論理インターフェースが作成され、インターフェース g2/25 と g2/26 がこのインターフェースに配置されます。  <pre>int g2/28 switchport spanning-tree guard root description to-BladeCenter CIGESM1</pre>

説明とコメント	6500-1 上での手順	6500-3 上での手順
<p>ステップ 2.2: <i>VLAN</i> と <i>トラッキング</i> のオプションを構成します。</p> <p>必要な VLAN はすべて基本構成の一部として作成済みで、その時点で IP アドレスが追加済みです。このステップでは、ステップ 2.1 で作成した、アグリゲートされたリンクを 802.1Q トランクとしてセットアップし、必要な VLAN が伝送されるようにします。</p> <p>それぞれのアグリゲーションに異なる VLAN が配置されていることに注意してください。前述のとおり、VLAN を制御することがセキュリティのために推奨されます（ただし、ネットワーク管理者の作業量が増えることがあります）。</p>	<pre> int port-channel 2 description EtherChannel to CIGESM1 switchport trunk encapsulation dot1q switchport trunk native vlan 2 switchport trunk allowed vlan 2,10,15,30,35,40,45,50,500 switchport mode trunk spanning-tree guard root </pre> <p>注：6500 と Cisco Systems IGESM の間のポート・チャネル・インターフェース上でルート・ガードを構成することにより、ネットワークの安定性を確保できます。</p> <p>また、前記の許可される VLAN への VLAN 500 の追加は、RSPAN のデモンストラーションをサポートするために 6500-1 上でのみ行われています。</p> <pre> int g2/28 description Trunk to CIGESM2 switchport trunk encapsulation dot1q switchport trunk native vlan 2 switchport trunk allowed vlan 2,10,15,20,25,30,35,40,45,50 switchport mode trunk spanning-tree guard root </pre>	<pre> int port-channel 2 description EtherChannel to CIGESM2 switchport trunk encapsulation dot1q switchport trunk native vlan 2 switchport trunk allowed vlan 2,20,25,30,35,40,45,50 switchport mode trunk spanning-tree guard root </pre> <p>注：6500 と Cisco Systems IGESM の間のポート・チャネル・インターフェース上でルート・ガードを構成することにより、ネットワークの安定性を確保できます。</p> <pre> int g2/28 description Trunk to CIGESM1 switchport trunk encapsulation dot1q switchport trunk native vlan 2 switchport trunk allowed vlan 2,10,15,20,25,30,35,40,45,50 switchport mode trunk spanning-tree guard root end </pre>
<p>ステップ 2.3: <i>CIGESM1</i> 上で定義した <i>RSPAN VLAN</i> をサポートするための構成。</p> <p>テスト目的で、CIGESM1 のポート g0/1（ステップ 3 で定義される）へのトラフィックを取り込むスニフアーが g2/2 に配置されます。</p>	<pre> vlan 500 remote-span  monitor session 5 source remote vlan 500  monitor session 5 destination interface g2/2 </pre> <pre> int g2/2 no shutdown end </pre> <p>前記の 2 つの monitor コマンドは、本書では折り返されていますが、それぞれ個々の行に入力する必要があります。</p> <p>VLAN 500 を RSPAN VLAN として使用する設定は、この後のステップで CIGESM1 に対して定義されます。VLAN の選択、使用するセッションの選択、および宛先ポートとしての g2/2 の選択は、すべて任意です。</p>	<p>この例では、CIGESM1 から 6500-1 への RSPAN のみを示しています。</p>

説明とコメント	6500-1 上での手順	6500-3 上での手順
ステップ 2.4: 構成を NVRAM に保管します。 <b>注:</b> 構成を保管しなければ、保管の前にスイッチを再起動した場合に、ネットワークのダウン状態が発生する可能性があります（最後に保管を行ってからの変更はすべて失われます）。	<code>copy running-config startup-config</code>	<code>copy running-config startup-config</code>

### ステップ 3: Cisco Systems IGESM の構成

ここでは、この例の Cisco Systems IGESM を構成するために必要な一連のアクションについて、段階を追って説明します。主に、ベイ 1 の Cisco Systems IGESM を構成する部分と、ベイ 2 の Cisco Systems IGESM を構成する部分の 2 つに分かれています。

この例に示す両方の Cisco Systems IGESM 構成について、次のことが前提になっています。

- ▶ ユーザーはすでに Cisco Systems IGESM にログオンしており、スイッチは使用可能モードになっています（または CMS にログオンし、その GUI を使用している）。
- ▶ コマンドは示されたとおりの順序で実行されます。
- ▶ Cisco Systems IGESM は、『Cisco Systems IGESM の基本構成』（113 ページ）の例に示すとおりの基本構成から開始されます。
- ▶ ブレード・サーバー上で使用されているオペレーティング・システムは Windows 2000 です。ブレード・サーバー上でどちらのポートが「第 1」と見なされ、どちらのポートが「第 2」と見なされるかはいくつかの要因に依存し、使用されているオペレーティング・システムも少なからず関係しているので、このことは重要です。ブレード・サーバーの接続名と、その名前を得る方法については、239 ページの付録 A、『ヒント』を参照してください。
- ▶ BladeServer1 上では、Broadcom BASP ソフトウェアによるトランキンク（ロード・バランシングではない）を両方のポートが使用します。第 1 のポートは VLAN 10 と 15 用に構成され、第 2 のポートは VLAN 20 と 25 用に構成されます。
- ▶ BladeServer2 上では、Cisco Systems IGESM のポート設定によって、両方のポートが単純なアクセス・リンクになり、それぞれ VLAN 10 と 20 に配置されます。
- ▶ BladeServer3 上では、両方のポートが Broadcom BASP ソフトウェアによってチームに構成され、OS には単一の論理リンクとして認識されます。これらのポートは、このサーバーへの Cisco Systems IGESM のポートで構成されているとおり、アクセス VLAN 30 を使用します。
- ▶ BladeServer4 では、両方のポートが Broadcom BASP ソフトウェアによってチームに構成され、OS には単一の論理リンクとして認識されます。これらのポートは、802.1Q トランキンクを使用して VLAN 35、40、45、および 50 をサポートします。

#### ステップ 3.1: 第 1 の Cisco Systems IGESM (CIGESM1) の構成

178 ページの図 7-16 では、CIGESM1 を構成するために使用されるステップバイステップの手順を説明し、CLI と CMS の両方のコマンドを示します。



**重要：** Cisco Systems IGESM 上でサポートされる CMS の現行バージョンでは、トランクに配置される VLAN を完全に制御する機能に制限があります。許可するように設定していても、トランクには常に VLAN 1 と、1001 から 1005 が含まれます。この制限があるため、実動構成のトランク上で許可される VLAN を制御しようとしている場合、この機能の使用は適さない場合があります。

表 7-16 CIGESM1 の構成

説明とコメント	CIGEMS1 に対する IOS CLI からのアクション	CIGEMS1 に対する CMS からのアクション
<p>ステップ 3.1.1: CIGESM1 に対して必要な VLAN を構成します。VLAN 10、15、30、35、40、45、および 50 を作成します（このデモンストレーションでは、VLAN 10 と 15 のみに名前を付けます）。</p>	<p>使用可能モードから次の手順で行います。</p> <pre>config t vlan 10   name Web vlan 15   name User vlan 30,35,40,45,50</pre> <p>VLAN 番号とコンマの間にスペースを入れないことに注意してください。</p>	<p>CMS インターフェースから次の手順で行います。</p> <ol style="list-style-type: none"> <li>1. 上部ツールバーの「VLAN」→「VLAN」をクリックします。</li> <li>2. 「Configure VLANs」タブをクリックします。</li> <li>3. 「Create」をクリックします。</li> <li>4. 「VLAN ID」フィールドに 10 と入力します。</li> <li>5. 「VLAN Name」フィールドに Web と入力します。</li> <li>6. 「OK」をクリックします。</li> <li>7. 「Create」をクリックします。</li> <li>8. 「VLAN ID」フィールドに 15 と入力します。</li> <li>9. 「VLAN Name」フィールドに User と入力します。</li> <li>10. 「OK」をクリックします。</li> <li>11. 「Create」をクリックします。</li> <li>12. 「VLAN ID」フィールドに 30 と入力します（名前のフィールドはデフォルトのままにします）。</li> <li>13. 「OK」をクリックします。</li> <li>14. 前の 3 つのステップを繰り返して、VLAN 35、40、45、および 50 を作成します。</li> <li>15. 「Apply」をクリックします。</li> <li>16. 「Refresh」をクリックして新規に作成した VLAN を表示します。</li> </ol>
<p>ステップ 3.1.2: 6500-1 へのリンク・アグリゲーションを構成します。</p> <p>この例では、LACP を使用してアグリゲーションを構成します。ポート g0/17 と g0/18 は 6500-1 に接続します。</p>	<pre>int range g0/17 -18 description To-6500-1 channel-group 1 mode active</pre> <p>これにより、<i>Port-Channel1</i> という名前の論理インターフェースが作成され、インターフェース g0/17 と g0/18 がこのインターフェースに配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部ツールバーの「Port」→「EtherChannels」をクリックします。</li> <li>2. 「Create」をクリックします。</li> <li>3. ポート Gi0/17 と Gi0/18 の隣にあるチェック・ボックスを選択します。</li> <li>4. 「Group [1-6]」フィールドに 1 と入力して、使用するポート・チャネルを選択します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> </ol>

説明とコメント	CIGEMS1 に対する IOS CLI からのアクション	CIGEMS1 に対する CMS からのアクション
<p>ステップ 3.1.3: 6500 への 802.1Q トランッキングを構成し、<i>EtherChannel</i> と単一トランク・リンクの両方に許可される VLAN を追加します。</p> <p>個々の VLAN を許可する行では、番号とコンマの間にスペースを入れることはできないので注意してください。</p> <p>また、デフォルトでは VLAN 2 がこれらのポートのネイティブ VLAN です。</p>	<pre> int port-channel 1 description EtherChannel-To-6500-1 switchport trunk native vlan 2 switchport trunk allowed vlan 2,10,15,30,35,40,45,50,500 switchport mode trunk </pre> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p> <p>前に示したように許可される VLAN に VLAN 500 を追加する目的は、RSPAN トラフィックを Cisco Systems IGESM から 6500 に伝送することです。VLAN 500 は任意選択です。</p> <pre> int g0/20 description Trunk-to-6500-3 switchport trunk native vlan 2 switchport trunk allowed vlan 2,10,15,30,35,40,45,50 switchport mode trunk </pre>	<ol style="list-style-type: none"> <li>1. 上部ツールバーの「VLAN」→「VLAN」をクリックします。</li> <li>2. 「po1」をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Trunk-Allowed VLAN」フィールドに 2,10,15,30,35,40,45,50,500 と入力します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> <li>7. 上部メニュー・バーの「Port」→「Port Settings」をクリックします。</li> <li>8. スクロールダウンして、ポート <b>gi0/20</b> を強調表示します。</li> <li>9. 「Modify」をクリックします。</li> <li>10. 説明を <b>Trunk-to-6500-3</b> に変更します。</li> <li>11. 上部ツールバーの「VLAN」→「VLAN」をクリックします。</li> <li>12. 「g0/20」をクリックします。</li> <li>13. 「Modify」をクリックします。</li> <li>14. 「Trunk-Allowed VLAN」フィールドに 2,10,15,30,35,40,45,50 と入力します。</li> <li>15. 「Native VLAN」フィールドが 2 に設定されていることを確認します。</li> <li>16. 「OK」をクリックします。</li> <li>17. 「Apply」または「OK」をクリックします。</li> </ol> <p><b>重要：</b> CMS の現行バージョンの制限により、許可される VLAN には常に VLAN 1 と 1001 から 1005 が含まれます。このため、6500 側の設定値とミスマッチが生じる可能性があり、その結果としてアグリゲーションがダウン状態になることがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>

説明とコメント	CIGEMS1 に対する IOS CLI からのアクション	CIGEMS1 に対する CMS からのアクション
<p>ステップ 3.1.4: <i>CIGESM1</i> のポート <i>g0/19</i> に対する <i>RSPAN</i> の構成。</p> <p><i>RSPAN</i> をいくつかの方法で構成して、単一ポート、複数のポート、あるいは <i>VLAN</i> からのトラフィックも取り込むことができます。このステップでは、可能なすべての方法を説明するのではなく、具体例を 1 つ示します。この例では、ポート <i>g0/1</i> 上でやり取りされるトラフィックをすべて取り込み、6500-1 のポート <i>g2/2</i> に接続されたスニファァーに取り込んで表示できるようにします。Cisco Systems IGESM のポート <i>g0/19</i> が、この例のリフレクター・ポートとして使用されます。6500-1 に必要なコマンドは、175 ページの表 7-15 に示してあります。</p> <p><b>重要:</b> リリース 12.1(14)AY を実行する Cisco Systems IGESM 上では、<i>RSPAN</i> の使用はお勧めしません。このリリースには <i>RSPAN</i> に関する問題があり、ネットワーク通信が中断する可能性があります。この問題について詳しくは、239 ページの付録 A、『ヒント』を参照してください。</p>	<p><i>RSPAN</i> <i>VLAN</i> を作成し、<i>RSPAN</i> をサポートするように設定します。</p> <pre><b>vlan 500</b> <b>remote-span</b></pre> <p>モニターするポート（この例では <i>g0/1</i>）を構成し、リフレクター・ポートの機能を実行するポート（<i>g0/19</i>）を設定します。</p> <pre><b>monitor session 1 source interface g0/1</b></pre> <pre><b>monitor session 1 destination remote vlan 500 reflector-port g0/19</b></pre> <p>前記の 2 つの <i>monitor</i> コマンドは、それぞれ単一の行に入力する必要があります。</p> <p><b>重要:</b> <i>RSPAN</i> が使用するリモート <i>VLAN</i> は、Cisco Systems IGESM 上の他のアクセス・ポートによって使用されていたり、Cisco Systems IGESM 上で管理 <i>VLAN</i> として定義されていたりしてはなりません。このトポロジー例の最初に説明した、<i>RSPAN</i> のセットアップに関する規則を確認してください。</p>	<p>CMS は、現時点では <i>RSPAN</i> の構成をサポートしません。<i>RSPAN</i> の構成には CLI を使用してください。</p>
<p>ステップ 3.1.5: <i>BladeServer1</i> への <i>802.1Q</i> トランキングを構成し、許可される <i>VLAN</i> を追加します。</p>	<pre><b>int g0/1</b> <b>switchport trunk allowed vlan 2,10,15</b></pre> <p>本書の中では <i>VLAN</i> 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要がありますので注意してください。</p> <p>これにより、<i>VLAN</i> 2、10、および 15 が <i>BladeServer1</i> の第 1 の NIC に到達できます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「<b>VLAN</b>」→「<b>VLAN</b>」をクリックします。</li> <li>2. ポート <b>Gi0/1</b> をクリックします。</li> <li>3. 「<b>Modify</b>」をクリックします。</li> <li>4. 「<b>Trunk-Allowed VLAN</b>」フィールドに <b>2,10,15</b> と入力します。</li> <li>5. 「<b>OK</b>」をクリックします。</li> <li>6. 「<b>Apply</b>」または「<b>OK</b>」をクリックします。</li> </ol> <p><b>重要:</b> ステップ 3.1.3 で説明したように、CMS の現行バージョンの制限により、許可される <i>VLAN</i> には常に <i>VLAN</i> 1 と 1001 から 1005 が含まれます。このため、ブレード・サーバー側の設定値とのミスマッチが生じる可能性があります。その結果としてトランクが期待どおり動作しないことがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>

説明とコメント	CIGEMS1 に対する IOS CLI からのアクション	CIGEMS1 に対する CMS からのアクション
ステップ 3.1.6: <i>BladeServer2</i> へのアクセス・リンクを構成し、アクセス VLAN を設定します。	<pre>int g0/2 switchport mode access switchport access vlan 10</pre> <p>これにより、BladeServer2 の第 1 の NIC が VLAN 10 に配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部ツールバーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/2</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Administrative Mode」フィールドの「Static Access」を選択します。</li> <li>5. 「Static-Access VLAN」フィールドに 10 と入力します。</li> <li>6. 「OK」をクリックします。</li> <li>7. 「Apply」または「OK」をクリックします。</li> </ol>
ステップ 3.1.7: <i>BladeServer3</i> へのアクセス・リンクを構成し、アクセス VLAN を設定します。	<pre>int g0/3 switchport mode access switchport access vlan 30</pre> <p>これにより、BladeServer3 の第 1 の NIC が VLAN 30 に配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部ツールバーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/3</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Administrative Mode」フィールドの「Static Access」を選択します。</li> <li>5. 「Static-Access VLAN」フィールドに 30 と入力します。</li> <li>6. 「OK」をクリックします。</li> <li>7. 「Apply」または「OK」をクリックします。</li> </ol>
ステップ 3.1.8: <i>BladeServer4</i> への 802.1Q トランキングを構成し、許可される VLAN を追加します。	<pre>int g0/4 switchport trunk allowed vlan 2,35,40,45,50 end</pre> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p>	<ol style="list-style-type: none"> <li>1. 上部ツールバーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/4</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Trunk-Allowed VLAN」フィールドに 2,35,40,45,50 と入力します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> </ol> <p><b>重要:</b> ステップ 3.1.3 で説明したように、CMS の現行バージョンの制限により、許可される VLAN には常に VLAN 1 と 1001 から 1005 が含まれます。このため、ブレード・サーバー側の設定値とのミスマッチが生じる可能性があります。その結果としてトランクが期待どおり動作しないことがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>
ステップ 3.1.9: <i>Cisco Systems IGESM</i> の構成を NVRAM に保管します。 このステップを実行しなければ、BladeCenter の電源をオフにした場合、または Cisco Systems IGESM をその他の方法で再始動した場合に、Cisco Systems IGESM に対する変更がすべて失われます。	<b>copy running-config startup-config</b>	<ol style="list-style-type: none"> <li>1. 上部ツールバーの「Administration」→「Save Configuration」をクリックします。</li> <li>2. 「Source」は「Running Configuration」に設定されたままにします。</li> <li>3. 「Destination」は「Startup Configuration」を選択します。</li> <li>4. 「Save」をクリックします。</li> </ol>

### ステップ3.2: 第2のCisco Systems IGESM (CIGESM2)の構成

表 7-17 では、CIGESM2 を構成するために使用されるステップバイステップの手順を説明し、CLI と CMS の両方のコマンドを示します。

**重要:** Cisco Systems IGESM 上でサポートされる CMS の現行バージョンでは、トランクに配置される VLAN を完全に制御する機能に制限があります。許可するように設定していても、トランクには常に VLAN 1 と、1001 から 1005 が含まれます。この制限があるため、実動構成のトランク上で許可される VLAN を制御しようとしている場合、この機能の使用は適さない場合があります。

表 7-17 CIGESM2 の構成

説明とコメント	CIGESM2 に対する IOS CLI からのアクション	CIGESM2 に対する CMS からのアクション
ステップ 3.2.1: CIGESM2 に対して必要な VLAN を構成します。VLAN 20、25、30、35、40、45、および 50 を作成します (このデモンストレーションでは、VLAN 20 と 25 のみに名前を付けます)。	<p>使用可能モードから次の手順で行います。</p> <pre> <b>config t</b> <b>vlan 20</b>   <b>name Application</b> <b>vlan 25</b>   <b>name Backup</b> <b>vlan 30,35,40,45,50</b> </pre> <p>VLAN 番号とコンマの間にスペースを入れないことに注意してください。</p>	<p>CMS インターフェースから次の手順で行います。</p> <ol style="list-style-type: none"> <li>1. 上部ツールバーの「VLAN」→「VLAN」をクリックします。</li> <li>2. 「Configure VLANs」タブをクリックします。</li> <li>3. 「Create」をクリックします。</li> <li>4. 「VLAN ID」フィールドに 20 と入力します。</li> <li>5. 「VLAN Name」フィールドに Application と入力します。</li> <li>6. 「OK」をクリックします。</li> <li>7. 「Create」をクリックします。</li> <li>8. 「VLAN ID」フィールドに 25 と入力します。</li> <li>9. 「VLAN Name」フィールドに Backup と入力します。</li> <li>10. 「OK」をクリックします。</li> <li>11. 「Create」をクリックします。</li> <li>12. 「VLAN ID」フィールドに 30 と入力します (名前のフィールドはデフォルトのままにします)。</li> <li>13. 「OK」をクリックします。</li> <li>14. 前の 3 つのステップを繰り返して、VLAN 35、40、45、および 50 を作成します。</li> <li>15. 「Apply」をクリックします。</li> <li>16. 「Refresh」をクリックして新規に作成した VLAN を表示します。</li> </ol>
ステップ 3.2.2: 6500-3 へのリンク・アグリゲーションを構成します。この例では、LACP を使用してアグリゲーションを構成します。ポート g0/17 と g0/18 は 6500-3 に接続します。	<pre> <b>int range g0/17 -18</b> <b>description To-6500-3</b> <b>channel-group 1 mode active</b> </pre> <p>これにより、Port-Channel という名前の論理インターフェースが作成され、インターフェース g0/17 と g0/18 がこのインターフェースに配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部ツールバーの「Port」→「EtherChannels」をクリックします。</li> <li>2. 「Create」をクリックします。</li> <li>3. ポート Gi0/17 と Gi0/18 の隣にあるチェック・ボックスを選択します。</li> <li>4. 「Group [1-6]」フィールドに 1 と入力して、使用するポート・チャネルを選択します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> </ol>

説明とコメント	CIGEMS2 に対する IOS CLI からのアクション	CIGEMS2 に対する CMS からのアクション
<p>ステップ 3.2.3: 6500 への 802.1Q トランッキングを構成し、<i>EtherChannel</i> と単一リンク・リンクの両方に許可される VLAN を追加します。</p> <p>個々の VLAN を許可する行では、番号とコンマの間にスペースを入れることはできないので注意してください。</p> <p>また、デフォルトでは VLAN 2 がこれらのポートのネイティブ VLAN です。</p> <p>単一リンクのコストを <i>EtherChannel</i> のルート・コストより高い値に変更することによって、最適なフローを強制する必要がありますので注意してください。</p> <p>この構成では、6500-1 と 6500-3 へのルート・コストは両方とも等しい (4) ので、最適なフロー (6500-3 への) を保証するために、0/20 を 8 に設定します。これにより、デフォルト・フローが 6500-3 への高帯域幅リンクに強制されます。</p> <p><b>お願い:</b> CMS の場合は、ポート全体ではなく VLAN に対する STP ポート・コストの指定のみが可能です。VLAN ごとにこの設定を行うことは面倒な作業です。このため、STP ポート・コストを制御する手段としては CLI の方が適していると考えられます。</p>	<pre> int port-channel 1 description EtherChannel-To-6500-3 switchport trunk native vlan 2 switchport trunk allowed vlan 2,20,25,30,35,40,45,50 switchport mode trunk </pre> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p> <pre> int g0/20 description Trunk-to-6500-1 switchport trunk native vlan 2 switchport trunk allowed vlan 2,20,25,30,35,40,45,50 switchport mode trunk spanning-tree cost 8 </pre>	<ol style="list-style-type: none"> <li>1. 上部ツールバーの「VLAN」→「VLAN」をクリックします。</li> <li>2. 「po1」をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Trunk-Allowed VLAN」フィールドに 2,20,25,30,35,40,45,50 と入力します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> <li>7. 上部ツールバーの「Port」→「Port Settings」をクリックします。</li> <li>8. スクロールダウンして、ポート <b>gi0/20</b> を強調表示します。</li> <li>9. 「Modify」をクリックします。</li> <li>10. 説明を Trunk-to-6500-1 に変更します。</li> <li>11. 上部ツールバーの「VLAN」→「VLAN」をクリックします。</li> <li>12. 「g0/20」をクリックします。</li> <li>13. 「Modify」をクリックします。</li> <li>14. 「Trunk-Allowed VLAN」フィールドに 2,20,25,30,35,40,45,50 と入力します。</li> <li>15. 「Native VLAN」フィールドが 2 に設定されていることを確認します。</li> <li>16. 「OK」をクリックします。</li> <li>17. 「Apply」または「OK」をクリックします。</li> </ol> <p><b>重要:</b> CMS の現行バージョンの制限により、許可される VLAN には常に VLAN 1 と 1001 から 1005 が含まれます。このため、6500 側の設定値とミスマッチが生じる可能性があり、その結果としてアグリゲーションがダウン状態になることがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>
<p>ステップ 3.2.4: CIGESM2 に対して RSPAN を構成します。</p>	<p>このトポロジーの場合、RSPAN リフレクター・ポートをそれぞれの Cisco Systems IGESM 専用にしてもいますが、CIGESM1 上での使用例のみを示します。CIGESM2 に対しては RSPAN コマンドは実行しません。</p>	<p>N/A</p>

説明とコメント	CIGEMS2 に対する IOS CLI からのアクション	CIGEMS2 に対する CMS からのアクション
<p>ステップ 3.2.5: <i>BladeServer1</i> への <i>802.1Q</i> トランキングを構成し、許可される <i>VLAN</i> を追加します。</p>	<p><b>int g0/1</b>  <b>switchport trunk allowed vlan 2,20,25</b></p> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p> <p>これにより、VLAN 2、20、および 25 が <i>BladeServer1</i> の第 2 の NIC に到達できます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「<b>VLAN</b>」→「<b>VLAN</b>」をクリックします。</li> <li>2. ポート <b>Gi0/1</b> をクリックします。</li> <li>3. 「<b>Modify</b>」をクリックします。</li> <li>4. 「<b>Trunk-Allowed VLAN</b>」フィールドに 2,20,25 と入力します。</li> <li>5. 「<b>OK</b>」をクリックします。</li> <li>6. 「<b>Apply</b>」または「<b>OK</b>」をクリックします。</li> </ol> <p><b>重要:</b> ステップ 3.1.3 で説明したように、CMS の現行バージョンの制限により、許可される VLAN には常に VLAN 1 と 1001 から 1005 が含まれます。このため、ブレード・サーバー側の設定値とのミスマッチが生じる可能性があります、その結果としてトランクが期待どおり動作しないことがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>
<p>ステップ 3.2.6: <i>BladeServer2</i> へのアクセス・リンクを構成し、アクセス <i>VLAN</i> を設定します。</p>	<p><b>int g0/2</b>  <b>switchport mode access</b>  <b>switchport access vlan 20</b></p> <p>これにより、<i>BladeServer2</i> の第 2 の NIC が VLAN 20 に配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「<b>VLAN</b>」→「<b>VLAN</b>」をクリックします。</li> <li>2. ポート <b>Gi0/2</b> をクリックします。</li> <li>3. 「<b>Modify</b>」をクリックします。</li> <li>4. 「<b>Administrative Mode</b>」フィールドの「<b>Static Access</b>」を選択します。</li> <li>5. 「<b>Static-Access VLAN</b>」フィールドに 20 と入力します。</li> <li>6. 「<b>OK</b>」をクリックします。</li> <li>7. 「<b>Apply</b>」または「<b>OK</b>」をクリックします。</li> </ol>
<p>ステップ 3.2.7: <i>BladeServer3</i> へのアクセス・リンクを構成し、アクセス <i>VLAN</i> を設定します。</p>	<p><b>int g0/3</b>  <b>switchport mode access</b>  <b>switchport access vlan 30</b></p> <p>これにより、<i>BladeServer3</i> の第 2 の NIC が VLAN 30 に配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「<b>VLAN</b>」→「<b>VLAN</b>」をクリックします。</li> <li>2. ポート <b>Gi0/3</b> をクリックします。</li> <li>3. 「<b>Modify</b>」をクリックします。</li> <li>4. 「<b>Administrative Mode</b>」フィールドの「<b>Static Access</b>」を選択します。</li> <li>5. 「<b>Static-Access VLAN</b>」フィールドに 30 と入力します。</li> <li>6. 「<b>OK</b>」をクリックします。</li> <li>7. 「<b>Apply</b>」または「<b>OK</b>」をクリックします。</li> </ol>

説明とコメント	CIGEMS2 に対する IOS CLI からのアクション	CIGEMS2 に対する CMS からのアクション
<p>ステップ 3.2.8: <i>BladeServer4</i> への <i>802.1Q</i> トランキングを構成し、許可される <i>VLAN</i> を追加します。</p>	<pre>int g0/4 switchport trunk allowed vlan 2,35,40,45,50 end</pre> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p> <p>これにより、VLAN 2、35、40、45、および 50 が <i>BladeServer4</i> の第 2 の NIC に到達できます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/4</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Trunk-Allowed VLAN」フィールドに <b>2,35,40,45,50</b> と入力します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> </ol> <p><b>重要:</b> ステップ 3.1.3 で説明したように、CMS の現行バージョンの制限により、許可される VLAN には常に VLAN 1 と 1001 から 1005 が含まれます。このため、ブレード・サーバー側の設定値とのミスマッチが生じる可能性があります。その結果としてトランクが期待どおり動作しないことがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>
<p>ステップ 3.2.9: <i>Cisco Systems IGESM</i> の構成を <i>NVRAM</i> に保管します。</p> <p>このステップを実行しなければ、<i>BladeCenter</i> の電源をオフにした場合、または <i>Cisco Systems IGESM</i> をその他の方法で再始動した場合に、<i>Cisco Systems IGESM</i> に対する変更がすべて失われます。</p>	<pre>copy running-config startup-config</pre>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「Administration」→「Save Configuration」をクリックします。</li> <li>2. 「Source」は「Running Configuration」に設定されたままにします。</li> <li>3. 「Destination」は「Startup Configuration」を選択します。</li> <li>4. 「Save」をクリックします。</li> </ol>

## ステップ 4: ブレード・サーバー上のインターフェースの構成

ここに示すブレード・サーバー構成は、トポロジー 2 と同一です。このトポロジーにアクセスするためにブレード・サーバーを構成する方法については、『ステップ 4: ブレード・サーバー上のインターフェースの構成』（158 ページ）を参照してください。

## ステップ 5: デバイスの再接続

これは、接続を完全に動作させるために行う最後のステップです。この手順は、ステップ 1 で使用したすべての手順の逆です。リンクを再確立する方法について詳しくは、128 ページの表 7-2 を参照してください。

## ステップ 6: 構成の検証

このステップは、EtherChannel の数が少ないことと、RSPAN が追加されていることを除いては、トポロジー 2 の検証ときわめて類似しています。詳しくは、『ステップ 6: 構成の検証』（165 ページ）を参照してください。



## RSPAN セッションの検証の簡単な要約

CIGESM1 上で、コマンド **show monitor** を実行し、構成が正しいかどうか出力を検討します。

```
Session 1
-----
Type                : Remote Source Session
Source Ports        :
    Both            : Gi0/1
Reflector Port      : Gi0/19
Dest RSPAN VLAN:    500
```

6500-1 上で、コマンド **show monitor** を実行し、構成が正しいかどうか出力を検討します。

```
Session 5
-----
Type                : Remote Destination Session
Source RSPAN VLAN : 500
Destination Ports  : Gi2/2
```

スニファアまたはその他のネットワーク・モニターを 6500-1 のポート g2/2 に接続し、BladeServer 1 から vlan 10 のデフォルト・ゲートウェイへの連続 ping を開始して (**ping 10.1.10.254 -t**)、これらの ping をスニファアによって取り込むことができるかどうか確認します。

規則および SPAN と RSPAN の構成方法について詳しく知るには、次の資料を参照してください。

[http://www.cisco.com/en/US/products/hw/switches/ps628/products\\_configuration\\_guide\\_chapter09186a00801a6ba9.html](http://www.cisco.com/en/US/products/hw/switches/ps628/products_configuration_guide_chapter09186a00801a6ba9.html)

[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_configuration\\_guide\\_chapter09186a008007f323.html](http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008007f323.html)

## 7.5.4 トポロジー 3b: 直接相互接続の使用を除いてはトポロジー 3a と同様

このトポロジー (187 ページの図 7-19) はトポロジー 3a と同様ですが、2 つの Cisco Systems IGESM 間の直接接続によって冗長性が提供される点が異なります。この例では、それぞれの Cisco Systems IGESM を他の Cisco Systems IGESM に対するアグリゲーション・スイッチへのバックアップ・パスとして使用するの、Cisco Systems IGESM から 6500 への 1 次アップリンクのいずれかに障害が起こった場合にトラフィックを正しく受け渡すことができるように、それぞれの Cisco Systems IGESM (およびこれらのアップリンク) にすべての VLAN を組み込む必要があります。

トポロジー 3a の利点は、1 次ルート・スイッチに障害が起こった場合に、トラフィックが 2 次ルート・スイッチに直接切り替わることです。トポロジー 3b の利点は、配線作業の一部を省くことができ、アップストリーム・スイッチ上で必要なポートの数が少ないことです。最適なトラフィック・パスの観点から見ると、専用 RSPAN ポートが必要な場合は 3a のトポロジーが推奨されます。

このため、ここに示す例は可能な方法としてのみ紹介するもので、あまりお勧めしません。

**重要:** RSPAN を環境に実装する前に、RSPAN の使用規則を理解しておくことが重要です。RSPAN の正しい使用法を理解していなければ、予期せず望ましくない結果が生じる可能性があります。RSPAN の配置に取りかかる前に、170 ページの 7.5.3、『トポロジー 3a: デュアル Cisco Systems IGESM、RSPAN を使用した 2 ポート・アグリゲーション』の情報を確認してください。

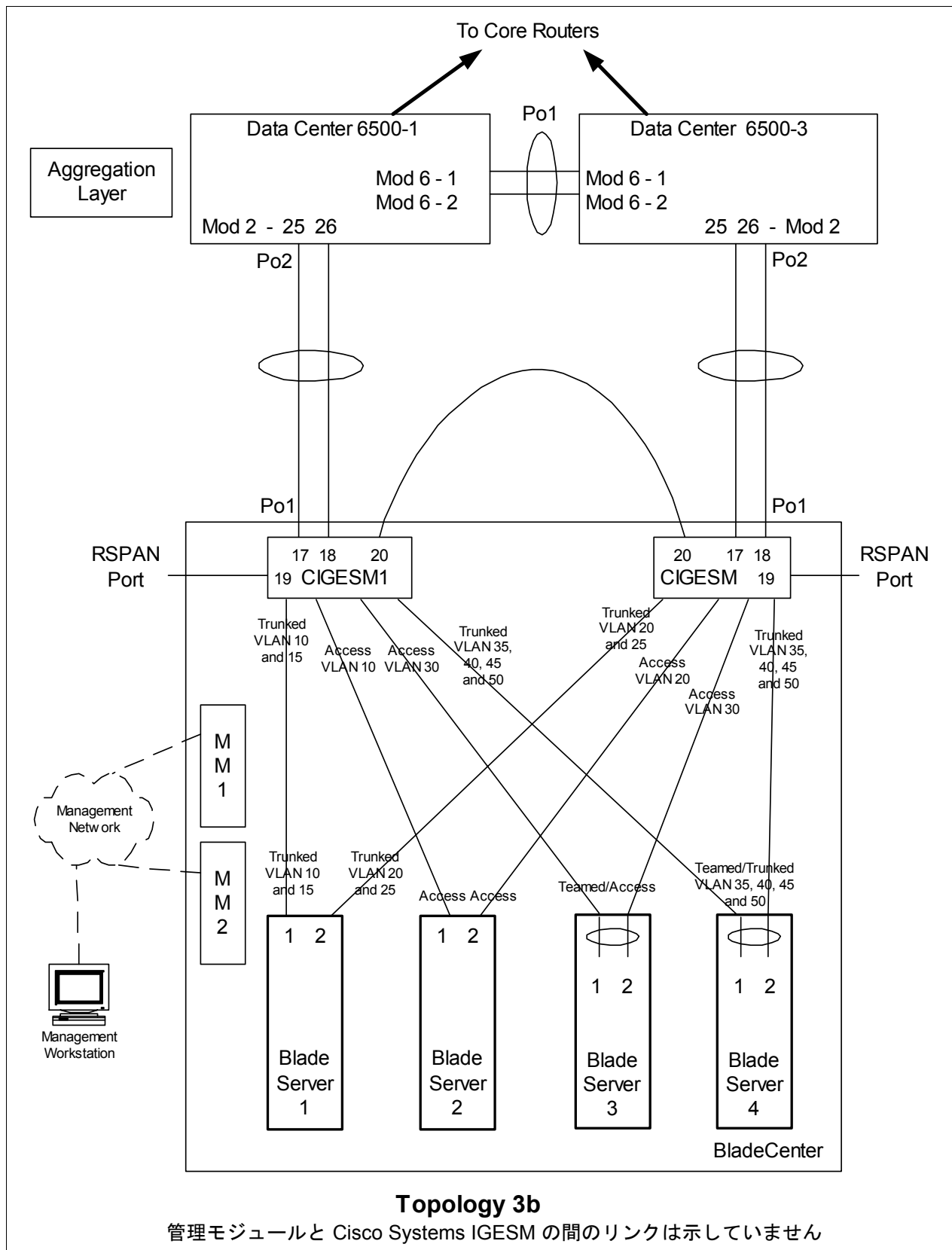


図 7-19 トポロジー 3b: デュアル Cisco Systems IGESM、相互リンクと RSPAN を使用した 2 ポート・アグリゲーション

## ステップ 1: リンクをダウン状態にする

構成変更を行う前に、必ずリンクを使用不可にすることをお勧めします。必要な手順については、127 ページの表 7-1 を参照してください。

## ステップ 2: 外部スイッチの構成

この例では、次のことを前提としています。

- ▶ 6500 の構成の大部分は、基本構成に含まれています（『Cat 6500 の基本構成』（113 ページ）を参照）。これは、本書の目的が、一般的な Cisco デバイスではなく BladeCenter コンポーネントを構成する方法を説明することであるからです。ここでは特に、BladeCenter に接続する 6500 ポートの構成方法を中心に説明します。
- ▶ VLAN 2 は、6500 上で基本構成の一部としてすでに作成済みです。
- ▶ 基本構成の一部として VTP ドメインがすでに命名済みで、透過に設定されています。
- ▶ 基本構成の一部として、スパンニング・ツリー・ルート・コマンドがすでに設定済みです（6500-1 を 1 次ルート、6500-3 を 2 次ルートにする）。
- ▶ ユーザーはすでにスイッチにログオンしており、スイッチは使用可能モードです。
- ▶ コマンドは示されたとおりの順序で実行されます。
- ▶ Cisco Systems IGESM への接続に使用される 6500 内の Cisco スイッチ・モジュールは 1000Base-T をベースとしており、ポートは 1Gbps 全二重のままにします。
- ▶ 6500 間のアグリゲーション・リンクが基本構成の一部としてすでに作成済みで、必要な VLAN（たとえば、2、10、15、20）を伝送しています。

表 7-18 外部スイッチの構成

説明とコメント	6500-1 上での手順	6500-3 上での手順
ステップ 2.1: 6500 から Cisco Systems IGESM へのリンク・アグリゲーションと単一リンクを構成します。 これは、6500 とそれぞれの Cisco Systems IGESM の間のポート・チャネル用です。インターフェースに説明を付けるようにすることを常にお勧めします。また、個々のポートとポート・チャネルの両方に対して、適所に Spanning-Tree guard root が追加されていることに注意してください。	<pre>config t int range g2/25 -26 switchport spanning-tree guard root description to-BladeCenter CIGESM1 channel-group 2 mode active</pre> <p>これにより、<i>Port-Channel2</i> という名前の論理インターフェースが作成され、インターフェース g2/25 と g2/26 がこのインターフェースに配置されます。</p>	<pre>config t int range g2/25 -26 switchport spanning-tree guard root description to-BladeCenter CIGESM2 channel-group 2 mode active</pre> <p>これにより、<i>Port-Channel2</i> という名前の論理インターフェースが作成され、インターフェース g2/25 と g2/26 がこのインターフェースに配置されます。</p>

説明とコメント	6500-1 上での手順	6500-3 上での手順
<p>ステップ 2.2: <i>VLAN</i> と <i>トラッキング</i> のオプションを構成します。</p> <p>必要な VLAN はすべて基本構成の一部として作成済みで、その時点で IP アドレスが追加済みです。このステップでは、ステップ 2.1 で作成した、アグリゲートされたリンクを 802.1Q トランクとしてセットアップし、必要な VLAN が伝送されるようにします。</p> <p>6500 のいずれかと Cisco Systems IGESM の間でアップリンクの 1 つに今後障害が起こった場合に対処するために、両方の Cisco Systems IGESM 上で VLAN すべて (VLAN 500 を除く) を伝送する必要があることに注意してください。</p>	<pre> int port-channel 2 description EtherChannel to CIGESM1 switchport trunk encapsulation dot1q switchport trunk native vlan 2 switchport trunk allowed vlan 2,10,15,20,25,30,35,40,45,50,500 switchport mode trunk spanning-tree guard root </pre> <p>注: 6500 と Cisco Systems IGESM の間のポート・チャネル・インターフェース上でルート・ガードを構成することにより、ネットワークの安定性を確保できます。</p> <p>また、前記の許可される VLAN への VLAN 500 の追加は、RSPAN のデモンストラーションをサポートするために 6500-1 上でのみ行われています。</p>	<pre> int port-channel 2 description EtherChannel to CIGESM2 switchport trunk encapsulation dot1q switchport trunk native vlan 2 switchport trunk allowed vlan 2,10,15,20,25,30,35,40,45,50 switchport mode trunk spanning-tree guard root </pre> <p>注: 6500 と Cisco Systems IGESM の間のポート・チャネル・インターフェース上でルート・ガードを構成することにより、ネットワークの安定性を確保できます。</p>
<p>ステップ 2.3: <i>CIGESM1</i> 上で定義した <i>RSPAN VLAN</i> をサポートするための構成。</p> <p>テスト目的で、CIGESM1 のポート g0/1 (ステップ 3 で定義される) へのトラフィックを取り込むスニファァーが g2/2 に配置されます。</p>	<pre> vlan 500 remote-span  monitor session 5 source remote vlan 500  monitor session 5 destination interface g2/2  int g2/2 no shutdown end </pre> <p>前記の 2 つの monitor コマンドは、本書では折り返されていますが、それぞれ個々の行に入力する必要があります。</p> <p>VLAN 500 を RSPAN VLAN として使用する設定は、この後のステップで CIGESM1 に対して定義されます。VLAN の選択、使用するセッションの選択、および宛先ポートとしての g2/2 の選択は、すべて任意です。</p>	<p>この例では、CIGESM1 から 6500-1 への RSPAN のみを示しています。</p>
<p>ステップ 2.4: 構成を <i>NVRAM</i> に保管します。</p> <p>注: 構成を保管しなければ、保管の前にスイッチを再起動した場合に、ネットワークのダウン状態が発生する可能性があります (最後に保管を行ってからの変更はすべて失われます)。</p>	<pre> copy running-config startup-config </pre>	<pre> copy running-config startup-config </pre>

## ステップ 3: Cisco Systems IGESM の構成

ここでは、この例の Cisco Systems IGESM を構成するために必要な一連のアクションについて、段階を追って説明します。主に、ベイ 1 の Cisco Systems IGESM を構成する部分と、ベイ 2 の Cisco Systems IGESM を構成する部分の 2 つに分かれています。

この例に示す両方の Cisco Systems IGESM 構成について、次のことが前提になっています。

- ▶ ユーザーはすでに Cisco Systems IGESM にログオンしており、スイッチは使用可能モードになっています（または CMS にログオンし、その GUI を使用している）。
- ▶ コマンドは示されたとおりの順序で実行されます。
- ▶ Cisco Systems IGESM は、『Cisco Systems IGESM の基本構成』（113 ページ）の例に示すとおりの基本構成から開始されます。
- ▶ ブレード・サーバー上で使用されているオペレーティング・システムは Windows 2000 です。ブレード・サーバー上でどちらのポートが「第 1」と見なされ、どちらのポートが「第 2」と見なされるかはいくつかの要因に依存し、使用されているオペレーティング・システムも少なからず関係しているので、このことは重要です。ブレード・サーバーの接続名と、その名前を得る方法については、239 ページの付録 A、『ヒント』を参照してください。
- ▶ BladeServer1 上では、Broadcom BASP ソフトウェアによるトランキング（ロード・バランシングではない）を両方のポートが使用します。第 1 のポートは VLAN 10 と 15 用に構成され、第 2 のポートは VLAN 20 と 25 用に構成されます。
- ▶ BladeServer2 上では、Cisco Systems IGESM のポート設定によって、両方のポートが単純なアクセス・リンクになり、それぞれ VLAN 10 と 20 に配置されます。
- ▶ BladeServer3 上では、両方のポートが Broadcom BASP ソフトウェアによってチームに構成され、OS には単一の論理リンクとして認識されます。これらのポートは、このサーバーへの Cisco Systems IGESM のポートで構成されているとおり、アクセス VLAN 30 を使用します。
- ▶ BladeServer4 では、両方のポートが Broadcom BASP ソフトウェアによってチームに構成され、OS には単一の論理リンクとして認識されます。これらのポートは、802.1Q トランキングを使用して VLAN 35、40、45、および 50 をサポートします。

### ステップ 3.1: 第 1 の Cisco Systems IGESM (CIGESM1) の構成

191 ページの表 7-19 では、CIGESM1 を構成するために使用されるステップバイステップの手順を説明し、CLI と CMS の両方のコマンドを示します。

**重要：** Cisco Systems IGESM 上でサポートされる CMS の現行バージョンでは、トランクに配置される VLAN を完全に制御する機能に制限があります。許可するように設定していても、トランクには常に VLAN 1 と、1001 から 1005 が含まれます。この制限があるため、実動構成のトランク上で許可される VLAN を制御しようとしている場合、この機能の使用は適さない場合があります。

表 7-19 CIGESM1 の構成

説明とコメント	CIGEMS1 に対する IOS CLI からのアクション	CIGEMS1 に対する CMS からのアクション
<p>ステップ 3.1.1: <i>CIGESM1</i> に対して必要な <i>VLAN</i> を構成します。  <i>VLAN</i> 10、15、20、25、30、35、40、45、および 50 を作成します。  6500 へのアップリンクのいずれかに障害が起こった場合に、いずれかの <i>VLAN</i> のトラフィックをこの Cisco Systems IGESM 経由に切り替えることができるように、ここでは両方の Cisco Systems IGESM 上で使用される <i>VLAN</i> すべてを作成することに注意してください。</p>	<p>使用可能モードから次の手順で行います。</p> <pre>config t vlan 10  name Web vlan 15  name User vlan 20  name Application vlan 25  name Backup vlan 30,35,40,45,50</pre> <p><i>VLAN</i> 番号とコンマの間にスペースを入れないことに注意してください。</p>	<p>CMS インターフェースから次の手順で行います。</p> <ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「<b>VLAN</b>」→「<b>VLAN</b>」をクリックします。</li> <li>2. 「<b>Configure VLANs</b>」タブをクリックします。</li> <li>3. 「<b>Create</b>」をクリックします。</li> <li>4. 「<b>VLAN ID</b>」フィールドに 10 と入力します。</li> <li>5. 「<b>VLAN Name</b>」フィールドに Web と入力します。</li> <li>6. 「<b>OK</b>」をクリックします。</li> <li>7. 「<b>Create</b>」をクリックします。</li> <li>8. 「<b>VLAN ID</b>」フィールドに 15 と入力します。</li> <li>9. 「<b>VLAN Name</b>」フィールドに User と入力します。</li> <li>10. 「<b>OK</b>」をクリックします。</li> <li>11. 「<b>Create</b>」をクリックします。</li> <li>12. 「<b>VLAN ID</b>」フィールドに 20 と入力します。</li> <li>13. 「<b>VLAN Name</b>」フィールドに Application と入力します。</li> <li>14. 「<b>OK</b>」をクリックします。</li> <li>15. 「<b>Create</b>」をクリックします。</li> <li>16. 「<b>VLAN ID</b>」フィールドに 25 と入力します。</li> <li>17. 「<b>VLAN Name</b>」フィールドに Backup と入力します。</li> <li>18. 「<b>OK</b>」をクリックします。</li> <li>19. 「<b>Create</b>」をクリックします。</li> <li>20. 「<b>VLAN ID</b>」フィールドに 30 と入力します ( 名前のフィールドはデフォルトのままにします )。</li> <li>21. 「<b>OK</b>」をクリックします。</li> <li>22. 前の 3 つのステップを繰り返して、<i>VLAN</i> 35、40、45、および 50 を作成します。</li> <li>23. 「<b>Apply</b>」をクリックします。</li> <li>24. 「<b>Refresh</b>」をクリックして新規に作成した <i>VLAN</i> を表示します。</li> </ol>
<p>ステップ 3.1.2: <i>6500-1</i> へのリンク・アグリゲーションを構成します。  この例では、LACP を使用してアグリゲーションを構成します。  ポート <i>g0/17</i> と <i>g0/18</i> は <i>6500-1</i> に接続します。</p>	<pre>int range g0/17 -18 description To-6500-1 channel-group 1 mode active</pre> <p>これにより、<i>Port-Channel1</i> という名前の論理インターフェースが作成され、インターフェース <i>g0/17</i> と <i>g0/18</i> がこのインターフェースに配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「<b>Port</b>」→「<b>EtherChannels</b>」をクリックします。</li> <li>2. 「<b>Create</b>」をクリックします。</li> <li>3. ポート <b>Gi0/17</b> と <b>Gi0/18</b> の隣にあるチェック・ボックスを選択します。</li> <li>4. 「<b>Group [1-6]</b>」フィールドに 1 と入力して、使用するポート・チャネルを選択します。</li> <li>5. 「<b>OK</b>」をクリックします。</li> <li>6. 「<b>Apply</b>」または「<b>OK</b>」をクリックします。</li> </ol>

説明とコメント	CIGEMS1 に対する IOS CLI からのアクション	CIGEMS1 に対する CMS からのアクション
<p>ステップ 3.1.3: 6500 への 802.1Q トランッキングを構成し、<i>EtherChannel</i> と単一リンク・リンクの両方に許可される VLAN を追加します。</p> <p>個々の VLAN を許可する行では、番号とコンマの間にスペースを入れることはできないので注意してください。</p> <p>また、デフォルトでは VLAN 2 がこれらのポートのネイティブ VLAN です。</p>	<pre> <b>int port-channel 1</b> <b>description EtherChannel-To-6500-1</b> <b>switchport trunk native vlan 2</b> <b>switchport trunk allowed vlan</b> <b>2,10,15,20,25,30,35,40,45,50,500</b> <b>switchport mode trunk</b> </pre> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p> <p>前に示したように許可される VLAN に VLAN 500 を追加する目的は、RSPAN トラフィックを Cisco Systems IGESM から 6500 に伝送することです。VLAN 500 は任意選択です。</p> <pre> <b>int g0/20</b> <b>description Trunk-to-CIGESM-2</b> <b>switchport trunk native vlan 2</b> <b>switchport trunk allowed vlan</b> <b>2,10,15,20,25,30,35,40,45,50</b> <b>switchport mode trunk</b> </pre> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. 「po1」をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Trunk-Allowed VLAN」フィールドに 2,10,15,30,35,40,45,50,500 と入力します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> <li>7. 上部メニュー・バーの「Port」→「Port Settings」をクリックします。</li> <li>8. スクロールダウンして、ポート <b>gi0/20</b> を強調表示します。</li> <li>9. 「Modify」をクリックします。</li> <li>10. 説明を <b>Trunk-to-6500-3</b> に変更します。</li> <li>11. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>12. 「g0/20」をクリックします。</li> <li>13. 「Modify」をクリックします。</li> <li>14. 「Trunk-Allowed VLAN」フィールドに 2,10,15,20,25,30,35,40,45,50 と入力します。</li> <li>15. 「Native VLAN」フィールドが 2 に設定されていることを確認します。</li> <li>16. 「OK」をクリックします。</li> <li>17. 「Apply」または「OK」をクリックします。</li> </ol> <p><b>重要：</b> CMS の現行バージョンの制限により、許可される VLAN には常に VLAN 1 と 1001 から 1005 が含まれます。このため、6500 側の設定値とミスマッチが生じる可能性があり、その結果としてアグリゲーションがダウン状態になることがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>

説明とコメント	CIGEMS1 に対する IOS CLI からのアクション	CIGEMS1 に対する CMS からのアクション
<p>ステップ 3.1.4: <i>CIGESM1</i> のポート <i>g0/19</i> に対する <i>RSPAN</i> の構成。</p> <p><i>RSPAN</i> をいくつかの方法で構成して、単一ポート、複数のポート、あるいは <i>VLAN</i> からのトラフィックも取り込むことができます。このステップでは、可能なすべての方法を説明するのではなく、具体例を 1 つ示します。この例では、ポート <i>g0/1</i> 上でやり取りされるトラフィックをすべて取り込み、6500-1 のポート <i>g2/2</i> に接続されたスニファァに取り込んで表示できるようにします。Cisco Systems IGESM のポート <i>g0/19</i> が、この例のリフレクター・ポートとして使用されます。6500-1 に必要なコマンドは、175 ページの表 7-15 に示してあります。</p> <p><b>重要：</b>リリース 12.1(14)AY を実行する Cisco Systems IGESM 上では、<i>RSPAN</i> の使用はお勧めしません。このリリースには <i>RSPAN</i> に関する問題があり、ネットワーク通信が中断する可能性があります。この問題について詳しくは、239 ページの付録 A、『ヒント』を参照してください。</p>	<p><i>RSPAN</i> <i>VLAN</i> を作成し、<i>RSPAN</i> をサポートするように設定します。</p> <pre><b>vlan 500</b> <b>remote-span</b></pre> <p>モニターするポート（この例では <i>g0/1</i>）を構成し、リフレクター・ポートの機能を実行するポート（<i>g0/19</i>）を設定します。</p> <pre><b>monitor session 1 source interface g0/1</b></pre> <pre><b>monitor session 1 destination remote vlan 500 reflector-port g0/19</b></pre> <p>前記の 2 つの <i>monitor</i> コマンドは、それぞれ単一の行に入力する必要があります。</p> <p><b>重要：</b><i>RSPAN</i> が使用するリモート <i>VLAN</i> は、Cisco Systems IGESM 上の他のアクセス・ポートによって使用されていたり、Cisco Systems IGESM 上で管理 <i>VLAN</i> として定義されていたりしてはなりません。このトポロジー例の最初に説明した、<i>RSPAN</i> のセットアップに関する規則を確認してください。</p>	<p>CMS は、現時点では <i>RSPAN</i> の構成をサポートしません。<i>RSPAN</i> の構成には CLI を使用してください。</p>
<p>ステップ 3.1.5: <i>BladeServer1</i> への <i>802.1Q</i> トランキングを構成し、許可される <i>VLAN</i> を追加します。</p>	<pre><b>int g0/1</b> <b>switchport trunk allowed vlan 2,10,15</b></pre> <p>本書の中では <i>VLAN</i> 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p> <p>これにより、<i>VLAN</i> 2、10、および 15 が <i>BladeServer1</i> の第 1 の NIC に到達できます。</p>	<ol style="list-style-type: none"> <li>1. 上部ツールバーの「<b>VLAN</b>」→「<b>VLAN</b>」をクリックします。</li> <li>2. ポート <b>Gi0/1</b> をクリックします。</li> <li>3. 「<b>Modify</b>」をクリックします。</li> <li>4. 「<b>Trunk-Allowed VLAN</b>」フィールドに <b>2,10,15</b> と入力します。</li> <li>5. 「<b>OK</b>」をクリックします。</li> <li>6. 「<b>Apply</b>」または「<b>OK</b>」をクリックします。</li> </ol> <p><b>重要：</b>ステップ 3.1.3 で説明したように、CMS の現行バージョンの制限により、許可される <i>VLAN</i> には常に <i>VLAN</i> 1 と 1001 から 1005 が含まれます。このため、ブレード・サーバー側の設定値とのミスマッチが生じる可能性があります。その結果としてトランクが期待どおり動作しないことがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>



説明とコメント	CIGEMS1 に対する IOS CLI からのアクション	CIGEMS1 に対する CMS からのアクション
ステップ 3.1.6: <i>BladeServer2</i> へのアクセス・リンクを構成し、アクセス VLAN を設定します。	<pre>int g0/2 switchport mode access switchport access vlan 10</pre> <p>これにより、BladeServer2 の第 1 の NIC が VLAN 10 に配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部ツールバーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/2</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Administrative Mode」フィールドの「Static Access」を選択します。</li> <li>5. 「Static-Access VLAN」フィールドに 10 と入力します。</li> <li>6. 「OK」をクリックします。</li> <li>7. 「Apply」または「OK」をクリックします。</li> </ol>
ステップ 3.1.7: <i>BladeServer3</i> へのアクセス・リンクを構成し、アクセス VLAN を設定します。	<pre>int g0/3 switchport mode access switchport access vlan 30</pre> <p>これにより、BladeServer3 の第 1 の NIC が VLAN 30 に配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/3</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Administrative Mode」フィールドの「Static Access」を選択します。</li> <li>5. 「Static-Access VLAN」フィールドに 30 と入力します。</li> <li>6. 「OK」をクリックします。</li> <li>7. 「Apply」または「OK」をクリックします。</li> </ol>
ステップ 3.1.8: <i>BladeServer4</i> への 802.1Q トランキングを構成し、許可される VLAN を追加します。	<pre>int g0/4 switchport trunk allowed vlan 2,35,40,45,50 end</pre> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/4</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Trunk-Allowed VLAN」フィールドに 2,35,40,45,50 と入力します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> </ol> <p><b>重要:</b> ステップ 3.1.3 で説明したように、CMS の現行バージョンの制限により、許可される VLAN には常に VLAN 1 と 1001 から 1005 が含まれます。このため、ブレード・サーバー側の設定値とのミスマッチが生じる可能性があります。その結果としてトランクが期待どおり動作しないことがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>
ステップ 3.1.9: <i>Cisco Systems IGESM</i> の構成を NVRAM に保管します。 このステップを実行しなければ、BladeCenter の電源をオフにした場合、または Cisco Systems IGESM をその他の方法で再始動した場合に、Cisco Systems IGESM に対する変更がすべて失われます。	<b>copy running-config startup-config</b>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「Administration」→「Save Configuration」をクリックします。</li> <li>2. 「Source」は「Running Configuration」に設定されたままにします。</li> <li>3. 「Destination」は「Startup Configuration」を選択します。</li> <li>4. 「Save」をクリックします。</li> </ol>

### ステップ3.2: 第2のCisco Systems IGESM (CIGESM2) の構成

表 7-20 では、CIGESM2 を構成するために使用されるステップバイステップの手順を説明し、CLI と CMS の両方のコマンドを示します。

**重要:** Cisco Systems IGESM 上でサポートされる CMS の現行バージョンでは、トランクに配置される VLAN を完全に制御する機能に制限があります。許可するように設定していても、トランクには常に VLAN 1 と、1001 から 1005 が含まれます。この制限があるため、実動構成のトランク上で許可される VLAN を制御しようとしている場合、この機能の使用は適さない場合があります。

表 7-20 CIGESM2 の構成

説明とコメント	CIGESM2 に対する IOS CLI からのアクション	CIGESM2 に対する CMS からのアクション
<p>ステップ 3.2.1: CIGESM2 に対して必要な VLAN を構成します。VLAN 10、15、20、25、30、35、40、45、および 50 を作成します。6500 へのアップリンクのいずれかに障害が起こった場合に、いずれかの VLAN のトラフィックをこの Cisco Systems IGESM 経由に切り替えることができるように、ここでは両方の Cisco Systems IGESM 上で使用される VLAN すべてを作成することに注意してください。</p>	<p>使用可能モードから次の手順で行います。</p> <pre> config t vlan 10   name Web vlan 15   name User vlan 20   name Application vlan 25   name Backup vlan 30,35,40,45,50 </pre> <p>VLAN 番号とコンマの間にスペースを入れないことに注意してください。</p>	<p>CMS インターフェースから次の手順で行います。</p> <ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」 → 「VLAN」 をクリックします。</li> <li>2. 「Configure VLANs」 タブをクリックします。</li> <li>3. 「Create」 をクリックします。</li> <li>4. 「VLAN ID」 フィールドに 10 と入力します。</li> <li>5. 「VLAN Name」 フィールドに Web と入力します。</li> <li>6. 「OK」 をクリックします。</li> <li>7. 「Create」 をクリックします。</li> <li>8. 「VLAN ID」 フィールドに 15 と入力します。</li> <li>9. 「VLAN Name」 フィールドに User と入力します。</li> <li>10. 「OK」 をクリックします。</li> <li>11. 「Create」 をクリックします。</li> <li>12. 「VLAN ID」 フィールドに 20 と入力します。</li> <li>13. 「VLAN Name」 フィールドに Application と入力します。</li> <li>14. 「OK」 をクリックします。</li> <li>15. 「Create」 をクリックします。</li> <li>16. 「VLAN ID」 フィールドに 25 と入力します。</li> <li>17. 「VLAN Name」 フィールドに Backup と入力します。</li> <li>18. 「OK」 をクリックします。</li> <li>19. 「Create」 をクリックします。</li> <li>20. 「VLAN ID」 フィールドに 30 と入力します ( 名前のフィールドはデフォルトのままにします )。</li> <li>21. 「OK」 をクリックします。</li> <li>22. 前の 3 つのステップを繰り返して、VLAN 35、40、45、および 50 を作成します。</li> <li>23. 「Apply」 をクリックします。</li> <li>24. 「Refresh」 をクリックして新規に作成した VLAN を表示します。</li> </ol>

説明とコメント	CIGEMS2 に対する IOS CLI からのアクション	CIGEMS2 に対する CMS からのアクション
<p>ステップ 3.2.2: 6500-3 へのリンク・アグリゲーションを構成します。</p> <p>この例では、LACP を使用してアグリゲーションを構成します。ポート g0/17 と g0/18 は 6500-3 に接続します。</p>	<pre>int range g0/17 -18 description To-6500-3 channel-group 1 mode active</pre> <p>これにより、<i>Port-Channel</i> という名前の論理インターフェースが作成され、インターフェース g0/17 と g0/18 がこのインターフェースに配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「Port」→「EtherChannels」をクリックします。</li> <li>2. 「Create」をクリックします。</li> <li>3. ポート Gi0/17 と Gi0/18 の隣にあるチェック・ボックスを選択します。</li> <li>4. 「Group [1-6]」フィールドに 1 と入力して、使用するポート・チャネルを選択します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> </ol>
<p>ステップ 3.2.3: 6500 への 802.1Q トランッキングを構成し、<i>EtherChannel</i> と単一リンク・リンクの両方に許可される VLAN を追加します。</p> <p>個々の VLAN を許可する行では、番号とコンマの間にスペースを入れることはできないので注意してください。</p> <p>また、デフォルトでは VLAN 2 がこれらのポートのネイティブ VLAN です。</p> <p>この構成では、トポロジー 3a の場合とは異なり、スパンニング・ツリーを強制する必要はないことに注意してください。これは、6500-3 に向かうデフォルト・パスが望ましいパスになるからです（6500-3 へのコストは 4、6500-1 へのコストは 7）。</p>	<pre>int port-channel 1 description EtherChannel-To-6500-3 switchport trunk native vlan 2 switchport trunk allowed vlan 2,10,15,20,25,30,35,40,45,50 switchport mode trunk</pre> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p> <pre>int g0/20 description Trunk-to-CIGESM1 switchport trunk native vlan 2 switchport trunk allowed vlan 2,10,15,20,25,30,35,40,45,50 switchport mode trunk</pre> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. 「po1」をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Trunk-Allowed VLAN」フィールドに 2,10,15,20,25,30,35,40,45,50 と入力します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> <li>7. 上部メニュー・バーの「Port」→「Port Settings」をクリックします。</li> <li>8. スクロールダウンして、ポート gi0/20 を強調表示します。</li> <li>9. 「Modify」をクリックします。</li> <li>10. 説明を <i>Trunk-to-6500-1</i> に変更します。</li> <li>11. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>12. 「g0/20」をクリックします。</li> <li>13. 「Modify」をクリックします。</li> <li>14. 「Trunk-Allowed VLAN」フィールドに 2,10,15,20,25,30,35,40,45,50 と入力します。</li> <li>15. 「Native VLAN」フィールドが 2 に設定されていることを確認します。</li> <li>16. 「OK」をクリックします。</li> <li>17. 「Apply」または「OK」をクリックします。</li> </ol> <p><b>重要：</b> CMS の現行バージョンの制限により、許可される VLAN には常に VLAN 1 と 1001 から 1005 が含まれます。このため、6500 側の設定値とミスマッチが生じる可能性があり、その結果としてアグリゲーションがダウン状態になることがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>

説明とコメント	CIGEMS2 に対する IOS CLI からのアクション	CIGEMS2 に対する CMS からのアクション
ステップ 3.2.4: <i>CIGEMS2</i> に対して <i>RSPAN</i> を構成します。	このトポロジーの場合、 <i>RSPAN</i> リフレクター・ポートをそれぞれの Cisco Systems IGESM 専用にしてもいますが、 <i>CIGEMS1</i> 上での使用例のみを示します。 <i>CIGEMS2</i> に対しては <i>RSPAN</i> コマンドは実行しません。	N/A
ステップ 3.2.5: <i>BladeServer1</i> への <i>802.1Q</i> トランキングを構成し、許可される <i>VLAN</i> を追加します。	<p><b>int g0/1</b>  <b>switchport trunk allowed vlan 2,20,25</b></p> <p>本書の中では <i>VLAN</i> 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。</p> <p>これにより、<i>VLAN</i> 2、20、および 25 が <i>BladeServer1</i> の第 2 の NIC に到達できます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「<b>VLAN</b>」→「<b>VLAN</b>」をクリックします。</li> <li>2. ポート <b>Gi0/1</b> をクリックします。</li> <li>3. 「<b>Modify</b>」をクリックします。</li> <li>4. 「<b>Trunk-Allowed VLAN</b>」フィールドに 2,20,25 と入力します。</li> <li>5. 「<b>OK</b>」をクリックします。</li> <li>6. 「<b>Apply</b>」または「<b>OK</b>」をクリックします。</li> </ol> <p><b>重要：</b>ステップ 3.1.3 で説明したように、CMS の現行バージョンの制限により、許可される <i>VLAN</i> には常に <i>VLAN</i> 1 と 1001 から 1005 が含まれます。このため、ブレード・サーバー側の設定値とのミスマッチが生じる可能性があります。その結果としてトランクが期待どおり動作しないことがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>
ステップ 3.2.6: <i>BladeServer2</i> へのアクセス・リンクを構成し、アクセス <i>VLAN</i> を設定します。	<p><b>int g0/2</b>  <b>switchport mode access</b>  <b>switchport access vlan 20</b></p> <p>これにより、<i>BladeServer2</i> の第 2 の NIC が <i>VLAN</i> 20 に配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「<b>VLAN</b>」→「<b>VLAN</b>」をクリックします。</li> <li>2. ポート <b>Gi0/2</b> をクリックします。</li> <li>3. 「<b>Modify</b>」をクリックします。</li> <li>4. 「<b>Administrative Mode</b>」フィールドの「<b>Static Access</b>」を選択します。</li> <li>5. 「<b>Static-Access VLAN</b>」フィールドに 20 と入力します。</li> <li>6. 「<b>OK</b>」をクリックします。</li> <li>7. 「<b>Apply</b>」または「<b>OK</b>」をクリックします。</li> </ol>
ステップ 3.2.7: <i>BladeServer3</i> へのアクセス・リンクを構成し、アクセス <i>VLAN</i> を設定します。	<p><b>int g0/3</b>  <b>switchport mode access</b>  <b>switchport access vlan 30</b></p> <p>これにより、<i>BladeServer3</i> の第 2 の NIC が <i>VLAN</i> 30 に配置されます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「<b>VLAN</b>」→「<b>VLAN</b>」をクリックします。</li> <li>2. ポート <b>Gi0/3</b> をクリックします。</li> <li>3. 「<b>Modify</b>」をクリックします。</li> <li>4. 「<b>Administrative Mode</b>」フィールドの「<b>Static Access</b>」を選択します。</li> <li>5. 「<b>Static-Access VLAN</b>」フィールドに 30 と入力します。</li> <li>6. 「<b>OK</b>」をクリックします。</li> <li>7. 「<b>Apply</b>」または「<b>OK</b>」をクリックします。</li> </ol>

説明とコメント	CIGEMS2 に対する IOS CLI からのアクション	CIGEMS2 に対する CMS からのアクション
<p>ステップ 3.2.8: <i>BladeServer4</i> への <i>802.1Q</i> トランキングを構成し、許可される <i>VLAN</i> を追加します。</p>	<pre>int g0/4 switchport trunk allowed vlan 2,35,40,45,50 end</pre> <p>本書の中では VLAN 番号が折り返されている場合がありますが、コマンドと同じ行に入力する必要があるので注意してください。 これにより、VLAN 2、35、40、45、および 50 が <i>BladeServer4</i> の第 2 の NIC に到達できます。</p>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「VLAN」→「VLAN」をクリックします。</li> <li>2. ポート <b>Gi0/4</b> をクリックします。</li> <li>3. 「Modify」をクリックします。</li> <li>4. 「Trunk-Allowed VLAN」フィールドに <b>2,35,40,45,50</b> と入力します。</li> <li>5. 「OK」をクリックします。</li> <li>6. 「Apply」または「OK」をクリックします。</li> </ol> <p><b>重要:</b> ステップ 3.1.3 で説明したように、CMS の現行バージョンの制限により、許可される VLAN には常に VLAN 1 と 1001 から 1005 が含まれます。このため、ブレード・サーバー側の設定値とのミスマッチが生じる可能性があります。その結果としてトランクが期待どおり動作しないことがあります。現時点で唯一の解決策は、CLI にアクセスし、このステップの CLI セクションに示した適切な設定値を指定して <b>switchport trunk allowed vlan</b> コマンドを実行することです。</p>
<p>ステップ 3.2.9: <i>Cisco Systems IGESM</i> の構成を <i>NVRAM</i> に保管します。 このステップを実行しなければ、<i>BladeCenter</i> の電源をオフにした場合、または <i>Cisco Systems IGESM</i> をその他の方法で再始動した場合に、<i>Cisco Systems IGESM</i> に対する変更がすべて失われます。</p>	<pre>copy running-config startup-config</pre>	<ol style="list-style-type: none"> <li>1. 上部メニュー・バーの「Administration」→「Save Configuration」をクリックします。</li> <li>2. 「Source」は「Running Configuration」に設定されたままにします。</li> <li>3. 「Destination」は「Startup Configuration」を選択します。</li> <li>4. 「Save」をクリックします。</li> </ol>

## ステップ 4: ブレード・サーバー上のインターフェースの構成

ここに示すブレード・サーバー構成は、トポロジー 2 と同一です。このトポロジーにアクセスするためにブレード・サーバーを構成する方法については、『ステップ 4: ブレード・サーバー上のインターフェースの構成』（158 ページ）を参照してください。

## ステップ 5: デバイスの再接続

これは、接続を完全に動作させるために行う最後のステップです。この手順は、ステップ 1 で使用したすべての手順の逆です。リンクを再確立する方法について詳しくは、128 ページの表 7-2 を参照してください。

## ステップ 6: 構成の検証

ここでは、トポロジー 3a の検証とほぼ同じことを行いますが、フェイルオーバー・パスが *Cisco Systems IGESM* を通るという点が異なります。詳しくは、『ステップ 6: 構成の検証』（185 ページ）を参照してください。

## 7.6 各種ブレード・サーバー構成

ここでは、この章でこれまでに説明しなかった数種類のブレード・サーバー構成を示します。203 ページの 7.7、『トランク・フェイルオーバー機能の説明と構成』の説明のとおりトランク・フェイルオーバーも構成する場合を除き、SLB を使用する構成（アクティブ/アクティブまたはアクティブ/スタンバイ）をトポロジー 1 で使用することはお勧めしません（129 ページの 7.5.1、『トポロジー 1: デュアル IGESM、2 つの 6500 に対する 4 ポート・アグリゲーション』の説明に注記したとおり）。

### BladeCenter HS20 Windows 2000 上でのアクティブ/スタンバイ SLB チーミング

ここでは、Windows 2000 環境の BladeCenter HS20 上でアクティブ/スタンバイ SLB チーミングを構成するために使用する手順を示します。

構成手順は、前の例の BladeServer3 に使用したアクティブ/アクティブ構成とほぼ同じで、NIC の 1 つをチーム内のスタンバイ・メンバーとして構成することだけが異なります。

アクティブ/スタンバイ SLB チームを作成するには、162 ページの表 7-13 のステップ 4.3.1 から始めます。ステップ 4.3.2 で「Load Balance Members」に NIC を追加した後、もう 1 つの NIC を強調表示し、下にある矢印ボタンをクリックして「Standby Member」に追加します。これにより、図 7-20 に示すようなウィンドウが開きます。「Finish」をクリックし、ステップ 4.4.3 とそれ以降のステップに進みます。BACS アプリケーションを使用して構成を検証する際には、200 ページの図 7-21 に示すようなウィンドウが開きます。それぞれの「Primary Adapters」グループと「Standby Adapters」グループに、NIC が 1 つずつ割り当てられていることを確認してください。

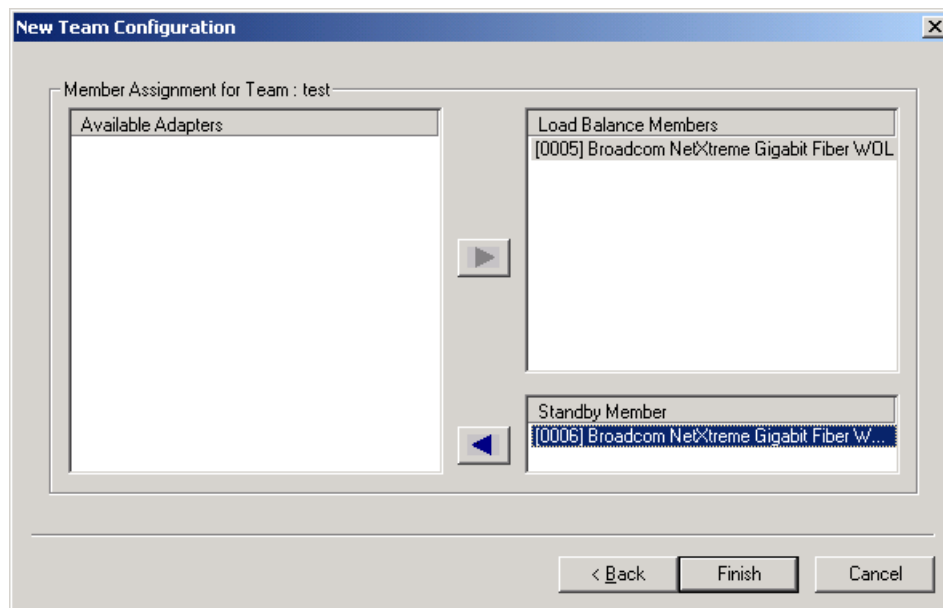


図 7-20 アクティブ/スタンバイ SLB チームの構成

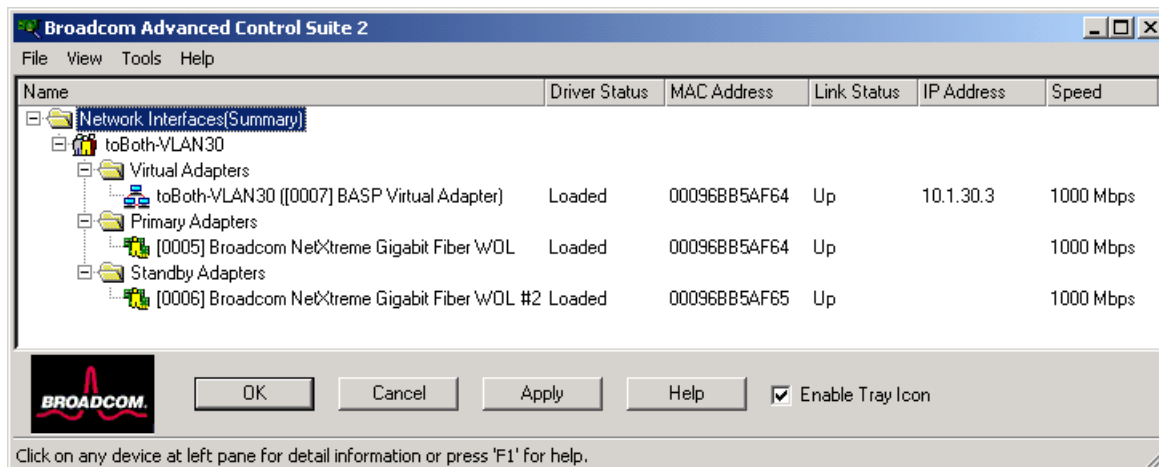


図 7-21 アクティブ/スタンバイ SLB チームの検証

## Red Hat Linux 環境の BladeCenter HS20 上での SLB アクティブ/アクティブ・チーミング

ここでは、Red Hat AS 2.1 を実行する BladeCenter HS20 上のアクセス・ポートとして、Cisco Systems IGESM に接続するための SLB チームを作成する方法を示します。次に一例として説明する構成は、基本的には前のトポロジー例の BladeServer3 と同じ構成です（この例で使われる IP アドレスを除いて）。

- ▶ サーバーは BASP ソフトウェアを使用して、単一のチームに構成された論理インターフェースを VLAN 30 用に作成し、IP 構成はこの単一の論理インターフェースに対して実行されます（物理インターフェースに対してではなく）。
- ▶ この論理ポートは、CIGESM1 と CIGESM2 の両方に接続し、各 Cisco Systems IGESM のアクセス・ポート設定によって、それぞれ VLAN 30 に配置されます。すべての IP 構成は、この単一の論理インターフェースに対して実行されます（物理インターフェースに対してではなく）。
- ▶ 次の IP アドレスを使用します（24 ビット・マスク）。

BASP 論理ポート、CIGESM1 へ: 10.1.30.11（デフォルト・ゲートウェイ = 10.1.30.254）

BACS を使用して Linux 上でチームを作成するには、構成スクリプトを使用してチーミング設定値を構成する必要があります。構成スクリプトを作成するには、`/etc/basp/samples` ディレクトリーから `/etc/basp` ディレクトリーにサンプル・スクリプトをコピーし、これをテンプレートとして使用してください。構成スクリプト名には接頭部として「team-」を付ける必要があります。構成スクリプトを作成した後、初回は `% /etc/init.d/basp start` を使用してチームを手動で開始します。詳しい手順については、BACS の `readme` ファイルを参照してください。

team-sample ファイルを `/etc/basp/sample` ディレクトリーからコピーし、team-toBothVLAN という名前を付けます。ファイルを次のように変更します。変更または追加される項目は、**赤のイタリック体**で示してあります。

```
TEAM_ID=0
TEAM_TYPE=0
TEAM_NAME=toBothVLAN

# 1st physical interface in the team
TEAM_PAO_NAME=eth0
TEAM_PAO_ROLE=0
```

```
# 2nd physical interface in the team
TEAM_PA1_NAME=eth1
TEAM_PA1_ROLE=0

# 3rd physical interface in the team
#TEAM_PA2_NAME=eth2
#TEAM_PA2_ROLE=0

# 1st virtual interface in the team
TEAM_VAO_NAME=sw0
TEAM_VAO_VLAN=0
TEAM_VAO_IP=10.1.30.3
TEAM_VAO_NETMASK=255.255.255.0

# Optional default gateway
# One default gateway is usually specified for the system and it should be
# reachable from one network interface
TEAM_VAO_GW=10.1.30.254
```

## Red Hat Linux 環境の BladeCenter HS20 上での 802.1Q トランク・リンク

ここでは、Red Hat AS 2.1 を実行する BladeCenter HS20 上で、802.1Q トランク・リンクを経由して複数の VLAN を受信するために、BACS を構成して NIC を設定する方法を示します。次に一例として説明する構成は、基本的にはこの章で前のトポロジー例に使用した BladeServer1 と同じ構成です（IP アドレスを除いては）。この構成では、次のことを前提としました。

- ▶ BladeServer1 は、BASP ソフトウェアを使用して VLAN 10、15、20、および 25 に対応する論理インターフェースを作成し、すべての IP 構成はこれらの論理インターフェースに対して実行されます（物理インターフェースに対してではなく）。
- ▶ 両方のポートが、Broadcom BASP ソフトウェアによるトランッキングを使用します（ロード・バランシングは使用しません）。第 1 のポートは VLAN 10 と 15 用に構成され、第 2 のポートは VLAN 20 と 25 用に構成されます。

第 1 のポート、VLAN 10 から CIGESM1 へ 10.1.10.11（デフォルト・ゲートウェイ = 10.1.10.254）

第 1 のポート、VLAN 15 から CIGESM1 へ 10.1.15.11

第 2 のポート、VLAN 20 から CIGESM2 へ 10.1.20.11

第 2 のポート、VLAN 25 から CIGESM2 へ 10.1.25.11

複数のデフォルト・ゲートウェイを使用する（たとえば、それぞれの VLAN に 1 つ、または複数の VLAN に 1 つ）かどうかの選択は、ユーザーの任意であることに注意してください。マルチホーム・システム上でのデフォルト・ゲートウェイについては、239 ページの付録 A、『ヒント』を参照してください。

/etc/basp/sample ディレクトリーにある team-VLAN のコピーを 2 つ作成し、それぞれ team-toCIGESM1 および team-toCIGESM2 という名前を付けます。2 つのチームを作成する際には、それぞれのチームごとに構成スクリプトを作成する必要があります。ファイルを次のように変更します。変更または追加される項目は、**赤のイタリック体**で示してあります。

- ▶ team-toCIGESM1
 

```
TEAM_ID=0
TEAM_TYPE=0
TEAM_NAME=toCIGESM1

# 1st physical interface in the team
TEAM_PA0_NAME=eth0
TEAM_PA0_ROLE=0

# 2nd physical interface in the team
```



```

#TEAM_PA1_NAME=eth1
#TEAM_PA1_ROLE=0

# 3rd physical interface in the team
#TEAM_PA2_NAME=eth2
#TEAM_PA2_ROLE=0

# 1st virtual interface in the team
TEAM_VAO_NAME=sw0
TEAM_VAO_VLAN=10
TEAM_VAO_IP=10.1.10.11
TEAM_VAO_NETMASK=255.255.255.0

# 2nd virtual interface in the team
TEAM_VA1_NAME=sw1
TEAM_VA1_VLAN=15
TEAM_VA1_IP=10.1.15.11
TEAM_VA1_NETMASK=255.255.255.0

# Optional default gateway
# One default gateway is usually specified for the system and it should be
# reachable from one network interface
TEAM_VAO_GW=10.1.10.254
#TEAM_VA1_GW=

```

► team-toCIGESM2

```

TEAM_ID=1
TEAM_TYPE=0
TEAM_NAME=toCIGESM2

# 1st physical interface in the team
TEAM_PAO_NAME=eth1
TEAM_PAO_ROLE=0

# 2nd physical interface in the team
#TEAM_PA1_NAME=eth1
#TEAM_PA1_ROLE=0

# 3rd physical interface in the team
#TEAM_PA2_NAME=eth2
#TEAM_PA2_ROLE=0

# 1st virtual interface in the team
TEAM_VAO_NAME=sw2
TEAM_VAO_VLAN=20
TEAM_VAO_IP=10.1.20.11
TEAM_VAO_NETMASK=255.255.255.0

# 2nd virtual interface in the team
TEAM_VA1_NAME=sw3
TEAM_VA1_VLAN=25
TEAM_VA1_IP=10.1.25.11
TEAM_VA1_NETMASK=255.255.255.0

# Optional default gateway
# One default gateway is usually specified for the system and it should be
# reachable from one network interface
#TEAM_VAO_GW=
#TEAM_VA1_GW=

```

## 7.7 トランク・フェイルオーバー機能の説明と構成

ここでは、トランク・フェイルオーバー機能（IGESM 用の 12.1(14)AY4 以上の IOS で使用可能）について説明し、構成例をいくつか示します。

トランク・フェイルオーバーの操作と構成について詳しくは、「*IGESM Software Configuration Guide*」を参照してください（リンクは本書で後述するオンライン・リソースの項にあります）。

### 7.7.1 トランク・フェイルオーバーの概要

トランク・フェイルオーバー機能（リンク状態トラッキング、およびレイヤー 2 トランク・フェイルオーバーとも呼ばれます）は、12.1(14)AY4 IOS 以降の IGESM 上で使用可能です。

トランク・フェイルオーバーの目的は、NIC チーミング・ソフトウェア（2つの物理 NIC を OS に対して単一の論理 NIC に結合する）を実行するサーバーが、IGESM からのアップリンク・ポートがダウン状態になったことを認識できるようにすることです。これにより、この条件下でトラフィックが消失することを防止できます。

トランク・フェイルオーバーの機能は、構成されたアップストリーム・ポートがダウン状態になったときに、構成されたブレード・サーバーに直接接続したポートをシャットダウンすることです。構成されたグループ内のアップストリーム・リンクがすべてダウン状態になったときに、この機能はダウンストリーム・ポートを `err-disable` 状態（ダウン）にすることによって、シャットダウンを行います。

ほとんどの場合、NIC チーミングを実行しているブレード・サーバーに接続した BladeCenter 内で、すべての CIGESM に対してトランク・フェイルオーバーを構成する必要があります。

#### これらの機能を使用して高可用性を確保するために重要な規則

どのようなネットワーク設計の場合にも、高可用性（HA）を実際に得るためには、十分な検討が必要です。次に、さまざまな障害のシナリオで接続性の維持を図るために重要な設計上の考慮事項をいくつか示します。

- ▶ NIC チーミングをトランク・フェイルオーバーと組み合わせて正しく機能させるには、適切なフェイルオーバーが行われるように CIGESM 間での外部 L2 接続が必要です（これは、同じ L2 ネットワーク /VLAN 上にある 2つのアップストリーム・スイッチ間の接続です）。本書に示す設計では、IGESM の両方のアップリンク接続上、および 6500-1 と 6500-3 の間で、ブレード・サーバーによって使用される VLAN を伝送することによってこれを実現しています。
- ▶ トランク・フェイルオーバーと NIC チーミングを組み合わせて効果的な HA を提供するためには、これらの例の 6500-1 と 6500-3 が何らかの HSRP を実行している必要があります。ブレード・サーバーはこの HSRP アドレスをデフォルト・ゲートウェイとして使用する必要があります。HSRP を使用せず、6500-1 のみがアップストリームのデフォルト・ゲートウェイ・アドレスを制御している場合は、6500-1 がダウン状態になると、トランク・フェイルオーバーはアップストリームの障害を検出してダウンストリーム接続をドロップします。NIC チーミングはこのことを検出し、他の NIC に切り替えて、パケットを 6500-3 に送信しますが、6500-3 はデフォルト・ゲートウェイに到達できないため、パケットをドロップします。

204 ページの図 7-22 に、NIC チーミングとトランク・フェイルオーバーのいくつかの属性を示します。ブレード・サーバー内の NIC の障害、IGESM とブレード・サーバー間のリンクの障害、および IGESM のハード障害（リンクダウン条件を引き起こす）はすべて、トランク・フェイルオーバーの補助なしに NIC チーミングによって検出できることに注意してく

ださい。トランク・フェイルオーバーは、IGESM とアップストリーム・スイッチの間のリンクに障害が発生した場合に作動します（IGESM へのリンクダウン条件を引き起こす、アップストリーム・スイッチのハード障害を含む）。

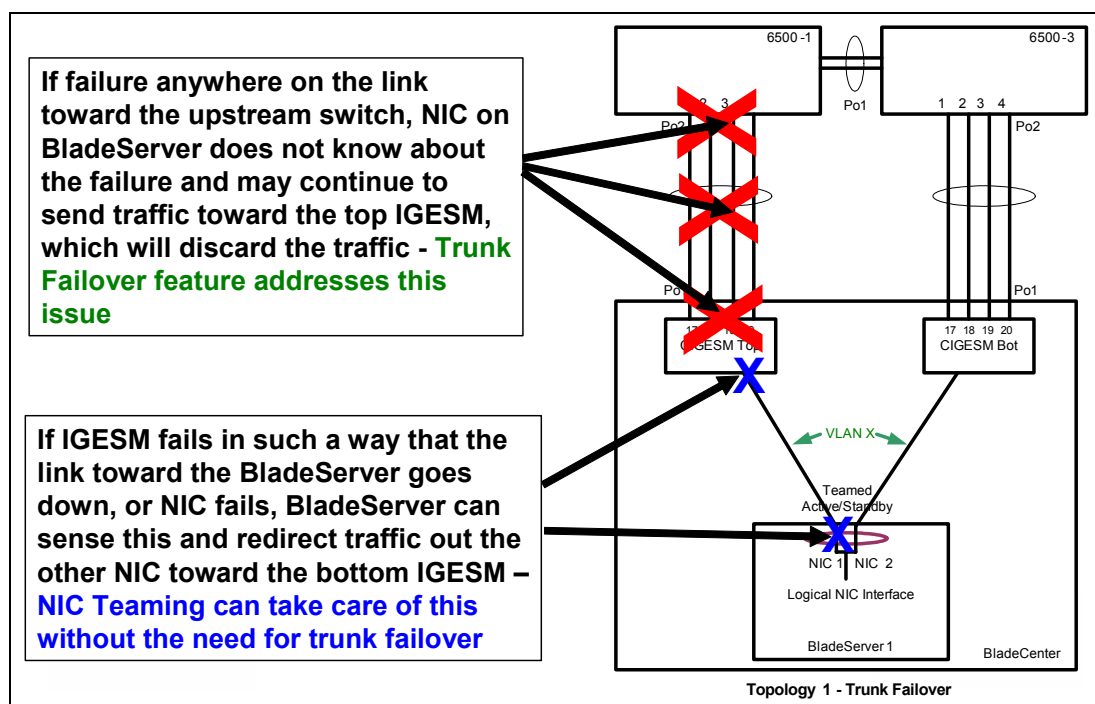


図 7-22 トランク・フェイルオーバーによって保護できる障害

## トランク・フェイルオーバー構成の概要

トランク・フェイルオーバーをサポートするには、IGESM 上で 2 種類の link state コマンドが必要です。

1. グローバル・コマンド（リンク状態グループを使用可能に設定し、2 つまでのグループがサポートされる）。

```
link state track X
```

(X=1 または 2)

2. インターフェース・コマンド（ポートをグループに割り当てる）。

```
link state group X {upstream | downstream}
```

upstream コマンドと downstream コマンドの配置に関する規則は、次のとおりです。

- *upstream* コマンドは、外部アップリンク（g0/17 から g0/20）、または外部アップリンク上の論理インターフェース（Etherchannel）のみに配置できます。
- 通常、*upstream* コマンドは Etherchannel ポートに配置します（int poX）。
- EtherChannel アップリンクを使用しない場合、*upstream* コマンドは物理ポート（G0/17 から 20）のみに配置します。
- *Downstream* コマンドは、g0/1 から g0/14 のみに配置できます。
- *downstream* コマンドの配置は個々の環境によって異なりますが、すべてのブレード・サーバーが NIC チーミングを使用する場合は、すべての内部ポート（G0/1 から 14）が「downstream」コマンドを受信します。

次に示す 3 つ目のタイプのコマンドは、トランク・フェイルオーバー構成の状況を検査するために使用できます。

```
show link state group detail
```

アップストリームおよびダウンストリームに割り当てられたポート、および構成されたトランク・フェイルオーバー・グループの状況を表示します。

**重要:** トランク・フェイルオーバー機能の構成は IGESM CLI からのみ実行でき、CMS から構成したりモニターしたりすることはできません。

## 7.7.2 トランク・フェイルオーバーを使用したトポロジー 1 の例

図 7-23 は、トポロジー 1 でのトランク・フェイルオーバーと NIC チーミングの使用を論理的に図示したものです。

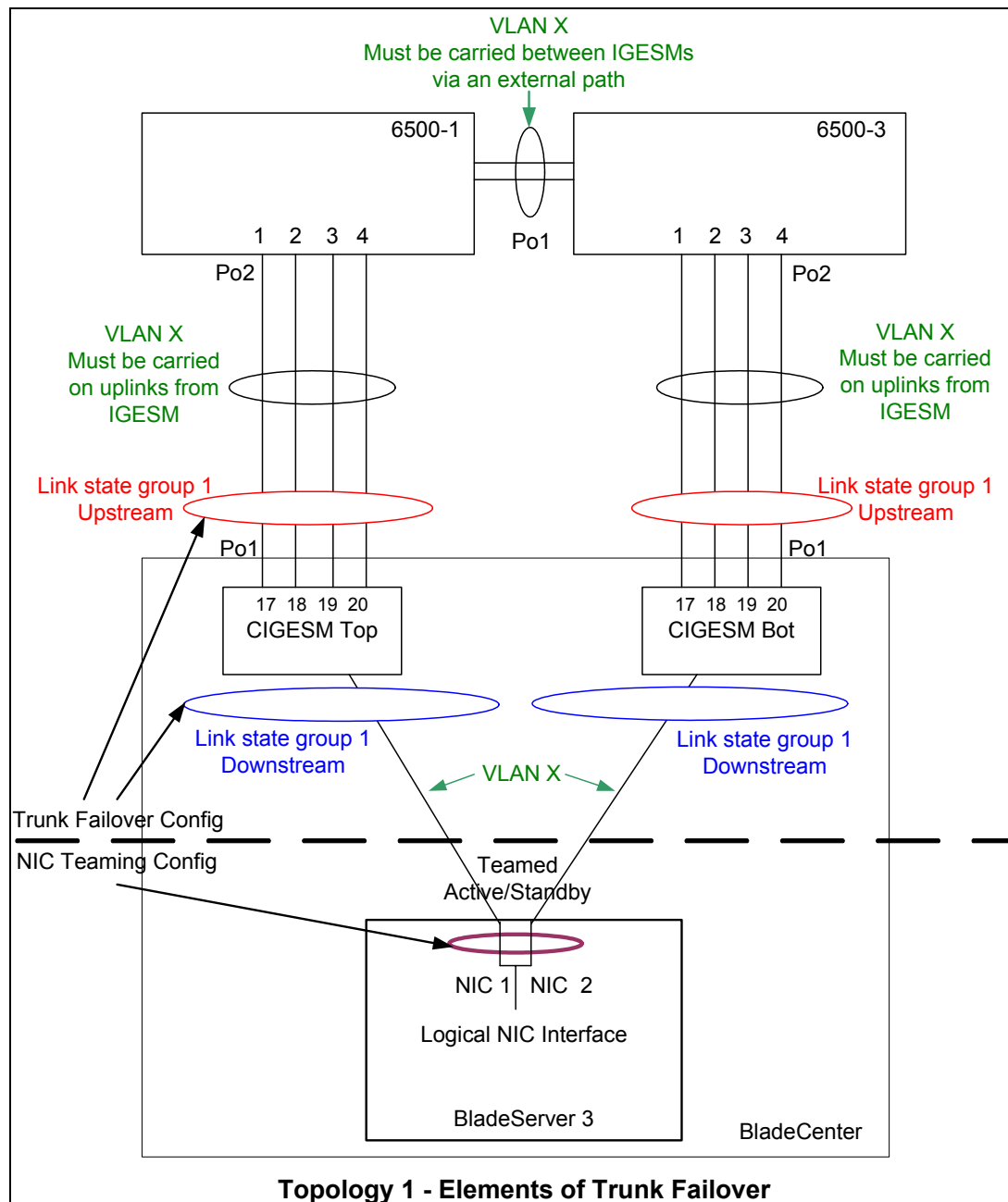


図 7-23 トポロジー 1 - トランク・フェイルオーバーの要素

この図 7-23 に示した例では、それぞれの IGESM 上で単一のリンク状態グループ（グループ 1）が使用されています。この設計では、Po1 の 4 つのポートがすべてダウン状態になった場合、トランク・フェイルオーバーが操作を引き継ぎ、内部のダウンストリームに定義されたポートをシャットダウンします。これにより、NIC チーミングにアップストリームの障害が警告され、この時点で NIC チーミングは他の IGESM に切り替わります。

この例では、チームに構成された NIC に対して単一の VLAN が示されています。チームに構成された NIC に対し、複数の VLAN を伝送することも可能です。複数の VLAN が必要な場合は、6500-1 と 6500-3 の間の Po1 のほかに、両方の NIC およびすべての外部アップリンクにすべての VLAN を伝送する必要があります。

### トポロジー 1 のトランク・フェイルオーバーの例を構成する手順

1. グローバル・コマンドを構成します。
2. アップストリーム・ポートまたは Etherchannel (poX) を構成します。
3. ダウンストリーム・ポートを構成します。

アップストリームの前にダウンストリームを構成すると、アップストリームが構成されるまでダウンストリーム・ポートがダウン状態になります。

### トポロジー 1 のトランク・フェイルオーバー構成の例

```
CIGESM1# configure terminal
CIGESM1(config)# link state track 1
CIGESM1(config)# interface po1
CIGESM1(config-if)# link state group 1 upstream
CIGESM1(config-if)# interface gi0/3
CIGESM1(config-if)# link state group 1 downstream
CIGESM1(config-if)# end
CIGESM1# write
```

### 現行トランク・フェイルオーバー操作の表示

トランク・フェイルオーバーの作動状況を表示するには、show link state group コマンドを使用します。

```
CIGESM1#show link state group detail
Link State Group: 1      Status: Enabled, Up
Upstream Interfaces    : Po1(Up)
Downstream Interfaces  : Gi0/3(Up)

Link State Group: 2      Status: Disabled, Down
Upstream Interfaces    :
Downstream Interfaces  :
```

(Up):Interface up (Dwn):Interface Down (Dis):Interface disabled

この例では、Po1 上の 4 つのポートがすべてダウン状態になると、Gi0/3 が err-disable (ダウン) に設定され、この時点で NIC チーミングが障害をセンスし、トラフィックを他の NIC に切り替えることができます。

前に示した例では、IGESM が 1 つしか構成されていないことに注意してください。ほとんどの実稼働環境では、両方の IGESM 上でトランク・フェイルオーバーを構成する必要があります。

## 7.7.3 トランク・フェイルオーバーを使用したトポロジー 2 の例

206 ページの図 7-23 は、トポロジー 2 でのトランク・フェイルオーバーと NIC チーミングの使用を論理的に図示したものです。

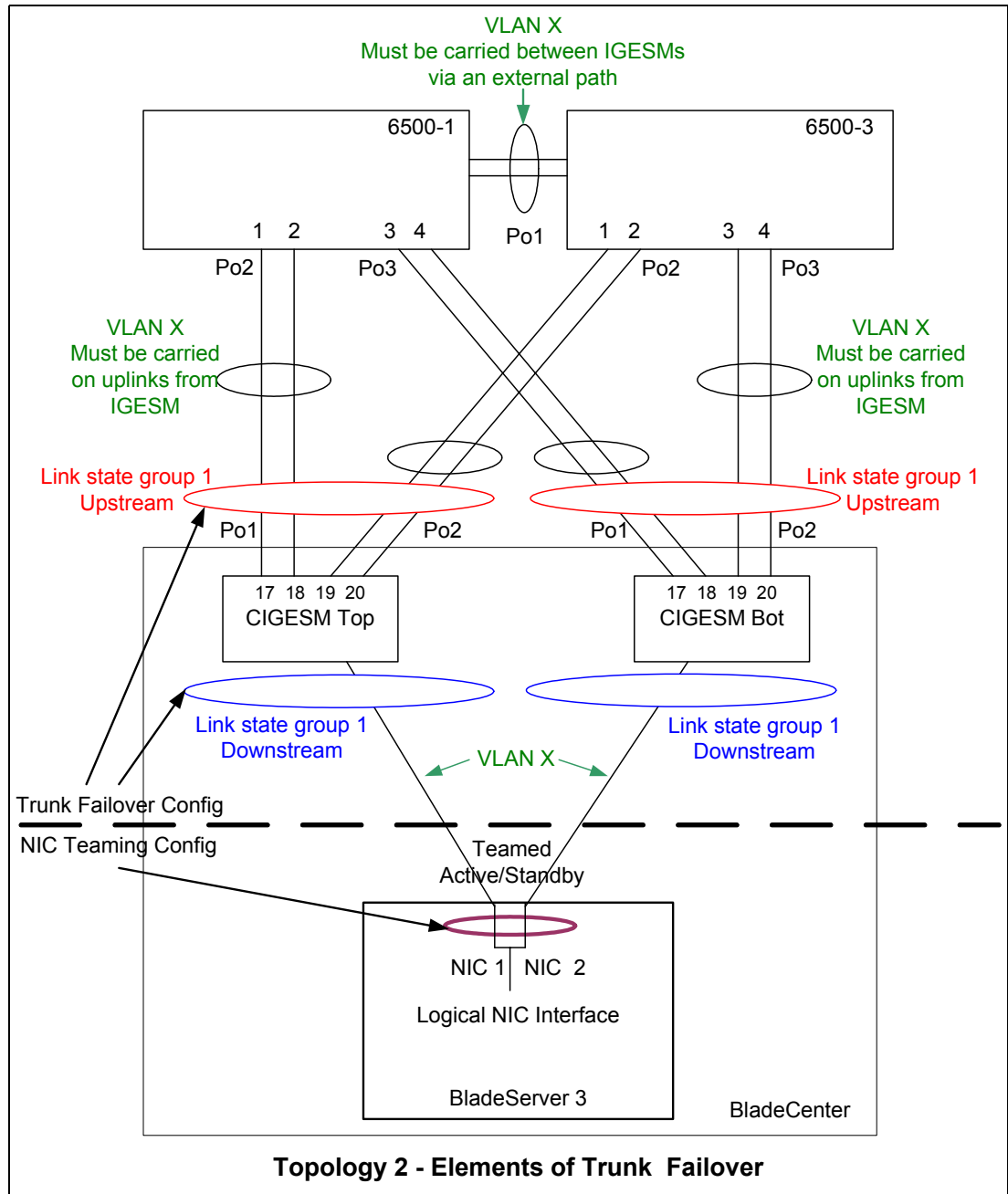


図 7-24 トポロジー 2 - トランク・フェイルオーバーのエレメント

この 206 ページの図 7-23 に示した例では、それぞれの IGESM 上で単一のリンク状態グループ（グループ 1）が使用されています。この設計では、Po1 の 2 つのポートがダウン状態になると、スパンニング・ツリーは Po2 を非ブロックにします。Po1 と Po2 の両方がダウン状態になると、トランク・フェイルオーバーが操作を引き継ぎ、内部のダウンストリームに定義されたポートをシャットダウンします。これにより、NIC チーミングにアップストリームの障害が警告され、この時点でチーミングは他の IGESM に切り替わります。

この例では、チームに構成された NIC に対して単一の VLAN が示されています。チームに構成された NIC に対し、複数の VLAN を伝送することも可能です。複数の VLAN が必要な場合は、6500-1 と 6500-3 の間の Po1 のほかに、両方の NIC およびすべての外部アップリンクにすべての VLAN を伝送する必要があります。

### トポロジー 2 のトランク・フェイルオーバーの例を構成する手順

1. グローバル・コマンドを構成します。
2. アップストリーム・ポートまたは Etherchannel (poX) を構成します。
3. ダウンストリーム・ポートを構成します。

アップストリームの前にダウンストリームを構成すると、アップストリームが構成されるまでダウンストリーム・ポートがダウン状態になります。

### トポロジー 1 のトランク・フェイルオーバー構成の例

```
CIGESM1# configure terminal
CIGESM1(config)# link state track 1
CIGESM1(config)# interface range po1 - 2
CIGESM1(config-if)# link state group 1 upstream
CIGESM1(config-if)# interface gi0/3
CIGESM1(config-if)# link state group 1 downstream
CIGESM1(config-if)# end
CIGESM1# write
```

### 現行トランク・フェイルオーバー操作の表示

トランク・フェイルオーバーの作動状況を表示するには、**show link state group** コマンドを使用します。

```
CIGESM1#show link state group detail
Link State Group: 1      Status: Enabled, Up
Upstream Interfaces   : Po1(Up) Po2(Up)
Downstream Interfaces : Gi0/3(Up)

Link State Group: 2      Status: Disabled, Down
Upstream Interfaces   :
Downstream Interfaces :

(Up):Interface up   (Dwn):Interface Down   (Dis):Interface disabled
```

この例では、Po1 または Po2 のみがダウン状態になった場合、スパンニング・ツリーは必要に応じて他方のリンクを非ブロックにします。Po1 および Po2 の両方がダウン状態になった場合に限り、Gi0/3 が err-disable (ダウン) に設定され、この時点で NIC チーミングが障害をセンスし、トラフィックを他の NIC に切り替えることができます。

前に示した例では、IGESM が 1 つしか構成されていないことに注意してください。ほとんどの実稼働環境では、両方の IGESM 上でトランク・フェイルオーバーを構成する必要があります。

## 7.8 Serial over LAN 機能の説明および構成

ここでは、BladeCenter の Serial over LAN 機能を簡単に紹介し、いくつかの規則について説明し、SoL のために IGESM を構成する例を示します。

*Serial over LAN* を使用するには、管理モジュール、IGESM、および場合によってはブレード・サーバーの BIOS とオペレーティング・システムを構成する必要があります (ブレード・サーバーのモデルによって異なります)。*Serial over LAN* 操作の詳細な説明と、SoL のエレメントすべての構成については、SoL の構成ガイドを参照してください (リンクは本書で後述するオンライン・リソースの項にあります)。



## 7.8.1 Serial over LAN の概要

Serial over LAN (SoL) を使用すると、管理モジュールから特殊な VLAN を経由してブレード・サーバーに至る特殊接続を経由してブレード・サーバーにアクセスできます。この接続は、ブレード・サーバーへのテキスト・ベースのみのインターフェースを提供する目的で行われます。

前述のとおり、*Serial over LAN* の詳しい説明については、*SoL の構成ガイド*を参照してください（リンクは本書で後述するオンライン・リソースの項にあります）。

### Serial over LAN に関する一般的な規則

- ▶ 一部のオペレーティング・システムは SoL をサポートしません。
  - W2K Server はサポートされません。
  - HS シリーズ上では、ほとんどの Linux と Windows Server 2003 がサポートされます。
  - JS20 上では、AIX® および Linux がサポートされます。
- ▶ 一部のブレード・サーバー・モデルでは、OS と BIOS の構成手順を行う必要があります（たとえば、Linux または Windows Server 2003 を実行する HS20）。詳しくは、IBM の SoL 構成ガイドを参照してください。
- ▶ オリジナルの HS 20（モデル 8678）など、一部のブレード・サーバー・モデルはサポートされません。
- ▶ JS20 は、OS の初期インストールのために SoL を必要とします。
  - JS20 には KVM インターフェースがありません。
  - OS のインストール後は、イーサネット・インターフェースを使用して JS20 を管理できます。
- ▶ HS シリーズには KVM インターフェースが組み込まれているので、SoL はオプションです。
- ▶ 一部のサーバー・ブレード上では、ファームウェアのアップグレードが必要です。たとえば、JS20 上で IGESM に SoL を使用するには、Broadcom ファームウェア 2.30 以上が必要です。このファームウェアは、次の URL で入手できます。  
<http://www.ibm.com/pc/support/site.wss/document.do?lnocid=MIGR-56012>
- ▶ すべてのファームウェア（管理モジュール、IGESM、およびブレード・サーバー用）と OS ドライバーを最新リリースにアップグレードすることをお勧めします。  
<http://www.ibm.com/servers/eserver/support/bladecenter/chassis/downloadinghwnonly.html>

### IGESM に対して使用する SoL VLAN を選択するための具体的な規則

- ▶ VLAN ID は 1 から 4094 の間であることが必要です。

**重要：**本書の制作時に入手可能な版の Serial over LAN 構成ガイドには、この最大が 1001 に制限されていると記載されていますが、これは誤りです。

- 1002 から 1005 の SoL VLAN ID は使用できません（IGESM によって予約済み）。
- 1005 より大きな番号の VLAN を使用するには、VTP 透過モード（IGESM のデフォルト）にする必要があります。

- ▶ VLAN 1 と 2 は両方とも IGESM のデフォルト VLAN であり、特に変更しない限りは SoL VLAN に使用してはなりません。
- ▶ この VLAN は、ブレード・サーバーと IGESM アップリンク・ポートの間でユーザー・データを伝送するために使用される VLAN であってはなりません。
- ▶ この VLAN は、IGESM と管理モジュールの間の管理 VLAN であってはなりません。  
IGESM から管理モジュールへのトラフィック用のデフォルト VLAN は VLAN 1 ですが、これはユーザーが変更できます。
- ▶ この VLAN は、管理モジュール上で SoL 用に構成された VLAN と一致している必要があります。
- ▶ SoL VLAN はブレード・サーバーに伝送する必要があります。
- ▶ ブレード・サーバーが単一の VLAN 上にある場合は、SoL が必要ならばポートをアクセス用に設定しないでください。
  - ポートはトランクに設定し、ネイティブ VLAN を目的のアクセス VLAN に設定します。
  - ブレード・サーバーへのトランク上で、許可される SoL VLAN を設定します。

## 7.8.2 Serial over LAN の構成

ここでは、IGESM 上での SoL の構成例を示します。

### Serial over LAN の構成の概要

IBM BladeCenter 内で Serial over LAN を正しく構成するには、いくつかの構成作業が必要です。少なくとも、管理モジュールと IGESM の両方を構成する必要があります。すでに説明したとおり、設置されているブレード・サーバーによっては、Serial over LAN のサポートを追加するために、サーバー上で CMOS/BIOS 設定とオペレーティング・システムの両方をさらに構成する必要が生じることがあります。

ここでは、IGESM のみの構成について説明し、ブレード・サーバー自体や管理モジュールの構成については説明しません。

**重要:** ほとんどの場合、Serial over LAN はスイッチ・ベイ 1 に取り付けられた IGESM 上でのみサポートされます。ブレード・サーバーの少なくとも 1 つのモデルには、Serial over LAN をベイ 2 のスイッチ経由で使用可能に設定するためのジャンパーが備わっています。詳しくは、Serial over LAN の構成ガイドを参照してください。

### IGESM の構成

#### IGESM を SoL 用に構成するためのステップバイステップの手順


表 7-21 に、上部ベイの IGESM を構成するためのステップバイステップの手順を示します。

表 7-21 Serial over LAN 用の IGESM の構成

説明とコメント	IGESM に対する IOS CLI からのアクション
<p>ステップ 1: SoL に使用する目的の VLAN を作成します。 (この例では、VLAN 4094 を使用します) この特定の VLAN を使用するには、スイッチが VTP 透過モードになっている必要があります。 この表のコマンドは、IGESM への Telnet セッションから開始し、IGESM を使用可能モードにして実行します。 SoL VLAN はこの IGESM のみに固有であり、ネットワーク内の他のスイッチから使用できます。これは、このスイッチ上の SoL VLAN が、ステップ 2 のコマンドによって他のスイッチから分離されるからです。 このステップで VLAN の命名はオプションで、単に将来スイッチ構成を検討するユーザーの便宜のために付ける名前です。 ここでどの VLAN を SoL VLAN として定義する場合にも、管理モジュール上で構成された SoL VLAN と一致している必要があります。</p>	<pre>config t vlan 4094 name SoL</pre>
<p>ステップ 2: 外部アップリンクから SoL VLAN を除去します。 これは、ステップ 1 で定義したものと同一 VLAN であることが必要です。 これにより、この BladeCenter への SoL VLAN が分離されます。</p>	<pre>int range g0/17 -20 switchport trunk allowed vlan remove 4094</pre>
<p>ステップ 3: IGESM から管理モジュールとブレード・サーバーに接続するリンクに、SoL VLAN を追加します。 これは、ステップ 1 で定義したものと同一 VLAN であることが必要です。 これにより、IGESM と管理モジュールの間のリンク、およびブレード・サーバーへのリンク上で、SoL トラフィックが使用可能になります。 ブレード・サーバーへのポートは、トランク・モード（アクセスでなく）になっている必要があります。ポートをトランク・リンクにして、ネイティブ VLAN を目的のアクセス VLAN に設定することにより、アクセス・モードのブレード・サーバーをシミュレートできます。</p>	<pre>int range g0/1 -16 switchport trunk allowed vlan add 4094</pre>
<p>ステップ 4: 構成モードを終了し、構成を NVRAM に保管します。 <b>end</b> コマンドは、構成モードを終了します。 このステップを実行しなければ、BladeCenter の電源をオフにしたり、その他の方法で IGESM を再始動したりした場合に、IGESM に対する変更がすべて失われます。</p>	<pre>end write</pre>

IGESM に対して SoL を構成した後、管理モジュールとブレード・サーバー（必要な場合）を構成する必要があります。SoL のすべてのエレメントを構成したら、SoL 接続を経由してブレード・サーバーを接続できるようになります。（詳しくは、Serial over LAN の構成ガイドを参照してください）

**重要：**管理モジュール上で SoL VLAN を構成する際に、保管の後でリポートを要求されることはありません。研究所でのテストの結果、管理モジュール上で SoL VLAN を変更し、構成を保管した後に管理モジュールを再ロードしなければ、SoL VLAN は作動可能にならない場合があります。このため、IGESM 上で SoL VLAN として定義されている VLAN と一致するように SoL VLAN を正しく構成した（保管した）後、管理モジュールを必ず再ロードすることをお勧めします。



## Cisco Systems IGESM の トラブルシューティング

この章では、IGESM をサポートするために利用できるトラブルシューティング技法とコマンドについて説明します。

## 8.1 基本的な規則と固有の現象

トラブルシューティングの詳細に進む前に、まずこの環境での一般的な規則と現象について説明しておくことが重要です。BladeCenter 内の IGESM と管理モジュールの間で行われる対話のために、特定の重要な規則を守る必要があります。これらの規則を守らなければ、IGESM を含む BladeCenter を配置する際に予期しない結果が生じることがあります。ここでは、これらの規則のいくつかを要約して示し、規則を守らない場合の結果を説明します。また、生じる可能性があるいくつかの現象と、考えられる解決策についても説明します。

### 8.1.1 基本的な規則

1. 接続の両側が構成されるまで、IGESM にケーブルを接続しないでください。
  - － 現象：アップストリーム接続が行われない、スパンニング・ツリー・ループによるアップストリーム・ネットワーク障害。
  - － 解決策：接続の両側が正しく構成されるまで、ケーブルは切り離れたまま、ポートはシャットダウンしたままにします。このことは、IGESM とアップストリーム接続の間に限らず、実動ネットワーク内のすべてのスイッチ間接続に当てはまる重要なベスト・プラクティスです。
2. IGESM が管理 VLAN インターフェースのために使用する VLAN 上に、BladeServer を配置しないでください。
  - － 現象：BladeServer 上で重複 IP アドレスが報告される、BladeServer への接続が不安定、BladeServer が DHCP アドレスを取得できない、DHCP サーバーがすべての IP アドレスを予期せず使い切る。さまざまな予期しない BladeServer への接続の問題。
  - － 解決策：データ用と管理用に別個の VLAN を使用します。（詳しくは、56 ページの 5.3、『管理パスに関する詳細説明』を参照してください）
3. IGESM ファームウェア（IOS）コードがアップグレード済みであることを確認します。
  - － 現象：あらゆる予期しない問題、または機能の欠落（トランク・フェイルオーバー、ジャンボ・フレーム、EtherChannel ロード・バランシング）。
  - － 解決策：コードの最新バージョンについて、ファームウェアの readme ファイルを確認します。IOS を最新リリースにアップグレードします。IGESM 用の最新コードを見つけるには、次の URL にアクセスしてください。  
<http://www.ibm.com/support>  
「Support by product」の下にある「**Personal computing**」をクリックします。「Select a product」プルダウン・メニューの「**Servers**」を選択します。「Family」プルダウン・メニューの「**BladeCenter**」を選択します。画面が最新表示されるまで待ち、「**Continue**」をクリックし、スクロールして目的の IGESM コードを見つけます。
4. IGESM 管理パスを決定し（管理モジュール経由または IGESM アップリンク経由）、その構成を行います。
  - － 現象：IGESM IP アドレスへの接続が断続的、または行われない。
  - － 解決策：56 ページの 5.3、『管理パスに関する詳細説明』を参照してください。

### 8.1.2 具体的な問題と解決策

215 ページの表 8-1 に、IGESM を含む BladeCenter を配置する際によく起こる現象と考えられる解決策の一覧を示します。

表 8-1 具体的な問題と推奨事項

BladeCenter 環境と IGESM に固有の現象	考えられる原因 / 解決策
重複 IP アドレスが IGESM 上で報告される	<p><b>原因:</b> 管理モジュール経由でなく IGESM 上で直接 IP アドレスが変更されました。</p> <p><b>解決策:</b> 管理モジュール上で IP アドレスを IGESM に適した設定値に変更し、「Save」をクリックします。この問題について詳しくは、239 ページの付録 A、『ヒント』を参照してください。</p>
重複 IP アドレスが BladeServer 上で報告される	<p><b>原因:</b> サーバーが IGESM 管理 VLAN と同じ VLAN を使用していて、管理モジュールがその VLAN 上にあるすべてのアドレスのプロキシとして動作し、サーバーを混乱させています。</p> <p><b>解決策:</b> VLAN を分離し、サーバーに接続するデータ VLAN のどれとも異なる VLAN を IGESM に対して使用します。(56 ページの 5.3、『管理パスに関する詳細説明』を参照してください)</p>
ネイティブ VLAN のミスマッチが IGESM 上で報告される	<p><b>原因:</b> 1) BladeCenter 内に複数の IGESM があり、IGESM の少なくとも 1 つが、同じ BladeCenter 内で他の IGESM とは異なる管理 VLAN 上にある。2) アップストリームがトランクに構成されており、アップストリーム・スイッチが IGESM とは異なるネイティブ VLAN を使用している。</p> <p><b>解決策:</b> 1) BladeCenter 内の IGESM をすべて同じ管理 VLAN に配置するか、ポート g0/15 および g0/16 上で CDP をオフにします。2) 外部接続の両側が、共通のネイティブ VLAN を一致して使用していることを確認します。(56 ページの 5.3、『管理パスに関する詳細説明』を参照してください)</p>
BladeServer への接続の問題	<p><b>原因:</b> 1) サーバーから他のデバイスへの VLAN の伝送が構成されていません。2) サーバーが IGESM 管理 VLAN と同じ VLAN を使用していて、管理モジュールがその VLAN 上にあるすべてのアドレスのプロキシとして動作し、サーバーを混乱させています。3) BladeServer 上の一部のドライバー（たとえば、Linux tg3 ドライバーの一部のバージョン）が IGESM に正しく接続できないときがあり、IGESM 上で BladeServer 方向のポートが接続されないままになります。</p> <p><b>解決策:</b> 1) ブレード・サーバーから宛先に正しい VLAN が伝送されるようにします。2) VLAN を分離し、サーバーに接続するデータ VLAN を IGESM VLAN として使用しないようにします。(56 ページの 5.3、『管理パスに関する詳細説明』を参照してください) 3) 異なる（作動する）バージョンのドライバーを使用するか、IGESM コードが 12.1(22)AY1 以上である場合はインターフェース・コマンド <b>speed noneg</b> を使用します。</p>
DHCP サーバーがすべての IP アドレスを使い切り、それでも BladeServer がアドレスを取得できない	<p><b>原因:</b> サーバーが IGESM 管理 VLAN と同じ VLAN を使用していて、管理モジュールがその VLAN 上にあるすべてのアドレスのプロキシとして動作し、DHCP サーバーを混乱させています。</p> <p><b>解決策:</b> VLAN を分離し、サーバーに接続するデータ VLAN を IGESM VLAN として使用しないようにします。(56 ページの 5.3、『管理パスに関する詳細説明』を参照してください)</p>
IGESM への接続が断続的、または行われない	<p><b>原因:</b> 管理モジュールの設定により、すべてのポート、管理モジュールからのアップリンク、および IGESM からのアップリンク上で、IGESM が同じ VLAN を使用して管理を行うことが許可されています。</p> <p><b>解決策:</b> すべてのポート上で管理を可能にする場合、管理モジュールは IGESM アップリンク上で伝送されているもの以外の VLAN を使用する必要があります。(56 ページの 5.3、『管理パスに関する詳細説明』を参照してください)</p>

BladeCenter 環境と IGESM に固有の現象	考えられる原因 / 解決策
トランク・フェイルオーバー機能を構成できない	<i>原因:</i> ダウン・レベルの IOS を実行しています。 <i>解決策:</i> 12.1(14)AY4 以上にアップグレードします。
IGESM をアップストリームに接続すると、アップストリーム・ネットワークがダウン状態になる	<i>原因:</i> 実動ネットワーク内で誤った構成またはデフォルト構成の 2 つのスイッチを接続しようとする、ネットワークに問題が生じる可能性があります。これは、未構成の IGESM をアップストリーム・スイッチ上の未構成のポートに接続した場合にも当てはまります。 <i>解決策:</i> 接続を行う前、または接続されたポートを使用可能に設定する前に、リンクの両側を必ず構成してください。このことは、IGESM とアップストリーム接続の間に限らず、実動ネットワーク内のすべてのスイッチ間接続に当てはまる重要なベスト・プラクティスです。
Red Hat および tg3 ドライバーを実行するサーバーがネットワークに接続しない、アップストリーム・ポートをダウン状態にする、またはその両方	<i>原因:</i> tg3 ドライバーの一部のバージョンが原因で、IGESM のポートに問題が起きています。 <i>解決策:</i> 1) Broadcom ドライバーを使用します。2) 正しく機能するバージョンの tg3 ドライバーを入手します。3) IGESM コードが 12.1(22)AY1 以上の場合は、 <b>speed noneg</b> コマンドを使用します。3) IGESM コードが 12.1(22)AY1 以上の場合は、インターフェース・コマンド <b>speed noneg</b> を使用します。
IGESM から外部ポート (g0/17 から 20) を使用可能に設定できない。 「Shutdown not allowed on this interface」と報告される。	<i>原因:</i> 管理モジュールの拡張入力出力モジュール設定の「External ports」が「Disabled」(デフォルト)に設定されています。 <i>解決策:</i> 管理モジュールの「I/O Module tasks」の拡張設定で、「External ports」を「Enabled」に設定し (すべての IGESM に対して)、IGESM に進んで <b>no shut</b> を実行し、インターフェース 17 から 20 を起動します。
アウトバウンド EtherChannel トラフィックにロード・バランシングが適用されず、ほとんどのアウトバウンド・トラフィックが EtherChannel バンドル内の単一ポートを使用している。	<i>原因:</i> デフォルトのアウトバウンド EtherChannel ロード・バランスは、BladeCenter 環境では必ずしも有効になりません。 <i>解決策:</i> 12.1(14)AY4 以降にアップグレードし、グローバル・ロード・バランシングをデフォルトのソース MAC から、ソースと宛先の IP または MAC の XOR に変更します。(たとえば、ソースと宛先の MAC アドレスの XOR に基づいてロード・バランシングを行う場合は、 <b>port-channel load-balance src-dst-mac</b> )
IGESM を取り付けたときに Serial over LAN (SoL) が作動しない、または断続的に作動する。	<i>原因:</i> 1) 管理モジュール、IGESM、または BladeServer 上で SoL が正しく構成されていない。2) 管理モジュール、IGESM、または BladeServer 上でダウン・レベルのファームウェアが使用されている。3) BladeServer 上でダウン・レベルのドライバーが使用されている。4) SoL の構成後に管理モジュールを再始動していない。 <i>解決策:</i> 1) IBM SoL の構成ガイドを使用して、IGESM が存在するときに SoL を正しく構成します。(209 ページの 7.8、『Serial over LAN 機能の説明および構成』を参照してください) 2) すべてのファームウェアが最新レベルであることを確認します。 3) BladeServer 上のドライバーが最新改訂であることを確認します。 4) 管理モジュールに SoL 構成を保管した後、指示が出されなくても、SoL を作動可能にするために管理モジュールを再始動することを強くお勧めします。(初回は作動可能になるまで 2、3 分かかる場合があります)

## 8.2 IGESM のトラブルシューティングの概要

ここでは、一般的なトラブルシューティング手法を説明し、手順を始めるためのオプションを示します。

## 8.2.1 トラブルシューティングに関する全般的な注意

IGESM は BladeCenter 内で高度に統合されているため、基本的なハードウェアのトラブルシューティングの範囲を超えることを行う場合は、複数のチームで連携して取り組む必要が生じることがよくあります。管理グループ間で円滑なコミュニケーションが取れていれば、問題が割合に早く解決する可能性が高いことが経験によって知られています。

それ以外の点では、IGESM のトラブルシューティングは他の製品と同様であり、発生する障害には典型的な基本タイプがあります。タイプのいくつかは次のとおりです。

- ▶ IGESM のハードウェア障害
  - よく起こることはありません。
  - 解決策は、障害のある IGESM の RMA のみです。
- ▶ ソフトウェア障害 (IGESM のバグ)
  - よく起こることはありませんが、他のすべての製品と同じく、ソフトウェア・バグは存在します。
  - コードの各リリースで解決されたバグのリストについては、最新コードの `readme` ファイルを参照してください。
- ▶ IGESM、その他のコンポーネント、またはその両方の構成の誤り
  - これは最もよく起こる問題です。
  - 解決のためには、さまざまな管理グループ間で緊密に協力し合う必要が生じることがよくあります。

トラブルシューティングのときに、どこから始めるか判断するにはどうすればよいでしょうか。ハードウェアまたは構成の問題であって、ソフトウェアのバグではないと判断するにはどうすればよいでしょうか。

真の答えは、*経験*のみです。

考えられるすべてのトラブルシューティング問題に対してステップバイステップの手順をリストする代わりに（数巻にわたって記述しても網羅しきれない可能性があります）、この章では収集する情報と便利なコマンドに関する情報を示し、トラブルシューティングの担当者がこうした問題について経験を積んでいることを前提とします。

**重要：**次に示すコマンドの多くは BladeCenter と接続ネットワークの動作に影響を及ぼすので、これらのコマンドを実行した結果を理解しているユーザーのみが実行するようにしてください。可能なときには、操作にそのような影響を及ぼす可能性があるコマンドを説明するときに警告を示しますが、最終的には結果を理解しているトラブルシューターの判断で使用してください。

本書ではこれ以降、さまざまな種類の問題のトラブルシューティングについて詳しく説明し、便利なトラブルシューティング・コマンドのヒントを示します。



## 8.2.2 テクニカル・サポートに役立つ情報

テクニカル・サポートを依頼する際には、迅速な解決のためにいくつかの情報が役立つことがあります。問題が可能なかぎり迅速に解決するように、問い合わせを開始するときには次に示す情報を収集し、準備しておいてください。

- ▶ 起こっている問題の詳しい説明
- ▶ 使用しているポートと VLAN を示すネットワーク・ダイアグラム（管理モジュールに接続するアップストリーム・ポートに割り当てられた VLAN を含む）
- ▶ 影響を受けているブレード・サーバーのネットワーク構成
- ▶ アップストリーム・デバイスのネットワーク構成
- ▶ BladeCenter 内のそれぞれの IGESM ごとに、次の IGESM CLI コマンドからの出力
  - **show tech-support**
  - **show int status**
  - **show platform summary**
  - **show span root**

この情報を収集するには、通常はいくつかのテクニカル・サポート・チームの協力が必要です。たとえば、ネットワーク・ダイアグラムは通常はネットワーク管理チームから入手し、ブレード・サーバー構成は通常はシステム管理チームから入手します。

サポート担当者の立場からは、次のような質問に対する答えもこのプロセスの助けになります。基本的な例をいくつか示します。

- この問題が発生したのは初めてですか？初めてでない場合は、どれぐらいの頻度で問題が発生しますか？
- 問題は再現できますか、またはランダムに起こっているように見えますか？
- 過去には正しく機能していましたか？機能していた場合は、問題が生じているネットワークまたはシステムに最近何か変更がありましたか？
- 何か修正処置を行いましたか？

これらの回答は、問題の迅速な切り分けに役立ちます。

ここから、さまざまな種類の問題のトラブルシューティングについて詳しい説明を始めます。

## 8.3 ハードウェアの問題が考えられる場合のトラブルシューティング

障害のあるハードウェアのトラブルシューティングは、特に一貫して起こる障害の場合には切り分けが容易なものです。IGESM の背面（コンソール・ポートの上）には障害 LED があり、POST（パワーオン・セルフテスト）時に検出された障害を識別するために使用されます。表 8-2 に、この LED や IGESM の背面にあるその他の LED に関する詳細を示します。

表 8-2 IGESM LED

インディケーター名	色	説明
OK	緑色	スイッチ・モジュールの電源が入っていて、正常に動作しているときに点灯します。
障害	オレンジ色	点灯は、このスイッチのどこかに障害が検出されたことを示します。その他の場合はオフです。

インディケーター名	色	説明
リンク OK	緑色	リンク状況がアップのときは緑色に点灯し、リンク状況がダウンのときはオフになります。それぞれの外部インターフェースごとに、このタイプの LED が 1 つずつあります。
Tx/Rx/ アクティビティ	緑色	インターフェース上のトラフィックに応じて緑色に点滅します。それぞれの外部インターフェースごとに、このタイプの LED が 1 つずつあります。

**注：**スイッチが POST を実行している間は、OK と障害の両方の LED が点灯します。POST が正常に完了すると、障害 LED がオフになります。

管理モジュール・ブラウザーを使用して、「I/O Module tasks」の下にある「Power/Restart」のコードを確認することもできます。220 ページの図 8-1 に、エラー・コードに関する情報があります。ほとんどのクリティカル・エラーを解決するには、RMA が必要です。

これらのエラー・コードに関しては、次の規則があります。

- ▶ 最初のクリティカル・エラー・コードは、後続のエラーによって上書きされません。
- ▶ 非クリティカル・エラーは、後続のクリティカル・エラーによって上書きされます。
- ▶ POST がクリティカル・テストに失敗した場合、ブート・ローダーは IOS をロードしません。スイッチはブート・ローダー（ROMMON）モードのままになります。
  - IOS が破損または欠落している場合にも、ROMMON モードになります。
  - IOS の破損または欠落からリカバリーするための手順については、テクニカル・サポートにご連絡ください。
- ▶ POST 中にクリティカル条件が検出された場合は、IGESM の背面にある障害 LED が点灯します。
- ▶ POST コード FF は、IGESM が正常にブートしたことを示しています。
- ▶ IGESM へのコンソール・ポート接続から、追加のメッセージが見つかる場合があります。

Sub-Test Name	Diagnostic Indicator (in Hex)	Failing Functional Area	Failure Criticality
CPU Cache memory	0x01	Base Internal Functions	Critical
Non-Cache DRAM	0x02	Base Internal Functions	Critical
Internal ASIC packet memory	0x03-0x04	Base Internal Functions	Critical
ASIC PCI memory	0x05-0x06	Base Internal Functions	Critical
data path test: mgmt ports	0x07-0x08	Base Internal Functions	Critical
VPD region read test	0x09	Base Internal Functions	Critical
Flash Memory in Extended Post	0x0A	Base Internal Functions	Critical
Flash Memory in regular POST	0x0B	Base Internal Functions	Critical
Data path test: Internal GE ports	0x81-0x8E	Internal Interface Failure	Non-Critical
Data path test: External ports	0xA1- 0xA8	External Interface Failure	Non-Critical

図8-1 IGESM のエラー・コード

図 8-2 に、入出力モジュールのエラー・コードを含む管理モジュール・ページの表示例を示します。

I/O Modules ?						
Bay	Status	Type*	MAC Address	IP Address	Pwr	POST Status
1	●	Ethernet SM	00:05:5D:71:87:70	192.168.70.51	On	POST results available: FF: Module completed POST
2	●	Ethernet SM	00:09:97:ED:03:00	192.168.70.52	On	POST results available: FF: Module completed POST
3	⚠	Ethernet SM	00:0D:ED:46:B9:00	192.168.70.53	On	POST results not complete: 0B
4	●	Ethernet SM	00:0C:F8:2A:05:00	192.168.70.54	On	POST results available: FF: Module completed POST

図8-2 入出力モジュールの POST 結果

通常のブート POST 以外に、IGESM は管理モジュール GUI から実行できるいくつかの診断機能を備えています。

**重要：**これらの診断を実行するとスイッチのリブートが発生するので、診断は計画停止時にのみ行う必要があります。

**お願い：**「I/O Module tasks」の拡張設定にある「Fast POST」の「Enabled/Disabled」の設定は、現時点では IGESM には影響を及ぼしません。

さまざまなレベルの診断を実行するには、MM GUI にログインし、「I/O Module tasks」に進みます。「Power/Restart」の下で、次のオプションのいずれかを選択します。

#### 1. Run Standard Diagnostics

テストとブートの完了にかかる時間は、通常は 2 分未満です。次のテストを実行します。

- フラッシュ・メモリー・テスト
- CPU キャッシュ・メモリー・テスト
- DRAM テスト

- データ・パス・テスト
- ASIC テスト
- 2. Run Extended Diagnostics  
所要時間は通常は 5 分未満で、通常の POST テストに加えて次のテストを実行します。
  - 拡張 DRAM テスト
- 3. Run Full Diagnostics  
所要時間は通常は 12 分未満で、通常の POST と拡張 POST に加えて次のテストを実行します。
  - 拡張フラッシュ・テスト

## 8.4 ソフトウェアの問題が考えられる場合のトラブルシューティング

ソフトウェアの問題が考えられる場合の最良のトラブルシューティング方法は、最新の IGESM コードの `readme` ファイルを入手して、発生している問題が記載されているかどうか調べることです。

文書化されたバグが見つかった場合は、新しいコードにアップグレードすれば問題は解決します。また、新しいコードにアップグレードすれば、アップグレードされたコードの新機能を利用することもできます。たとえば、バージョン 12.1(14)AY4 以降ではトランク・フェイルオーバーが実行でき、EtherChannel ロード・バランシングが改善されています。

新しい（文書化されていない）バグが発生したと考えられる場合は、テクニカル・サポートにお問い合わせいただき、必要なリソースを利用してこの問題の解決に当たってください。

## 8.5 構成の問題が考えられる場合のトラブルシューティング

構成の問題は最もよくあるトラブルシューティング事例で、通常は管理グループ間での緊密な協力を必要とします。この種のトラブルシューティングに使用できる一般的なツールのいくつかは、次のとおりです。

- ▶ IOS コマンド行インターフェース  
IGESM IOS CLI に習熟している必要があります。
- ▶ 管理モジュール GUI インターフェース  
管理モジュール GUI の知識があると、トラブルシューティングに非常に役立ちます。
- ▶ OS ベースのコマンド  
ほとんどのオペレーティング・システムがネットワークのトラブルシューティング・コマンドをサポートし、すべての主要オペレーティング・システムで何らかの形式の `ping`、`arp dump`、および `traceroute` の各コマンドが使用可能です。
- ▶ 外部ネットワーク管理ソフトウェア  
CiscoWorks、IBM Director などの管理プラットフォームを使用してデータを収集でき、問題の切り分けに役立ちます。
- ▶ その他のサード・パーティー・ツールには、ネットワーク・トラフィックを取り込んで検査するためのネットワーク・スニファー・ツール、さまざまなレベルで接続を迅速にテストするための `ping` スイープ・ツールなどがあります。

次のグループの IOS CLI コマンドは、注記のない限りすべて使用可能モードで実行されます。一部のコマンドは複数のグループに含まれることがあるので、この使用可能なコマンドの部分リストは単に一般的なグループ分けを示しています。これらのコマンドについては、

223 ページの 8.6、『便利な IOS CLI トラブルシューティング・コマンド』で詳しく説明します。

- ▶ データの収集
  - **show running**
  - **show vlan**
  - **show version**
  - **show tech-support**
  - **show platform summary**
  - **show logging**
- ▶ 管理
  - **term mon**
  - **clear counters**
  - **clear log**
  - **clear arp**
  - **clear mac add**
  - **no logging console** (構成モード)
- ▶ トラブルシューティング
  - **ping**
  - **show cdp neighbor**
  - **show int status**
  - **show ip int brief**
  - **shut - no shut** (インターフェース構成モード)
  - **show int g0/X**
  - **show int trunk**
  - **show etherchannel summary**
  - **show spanning-tree blockedports**
  - **show spanning-tree root**
  - **show link state group detail**
  - **show arp**
  - **SPAN および RSPAN**
  - **debug** (注意して使用すること)

図 8-3 に、IOS CLI の操作モードの一部を示します。

Mode	Functions	Prompt	How to get to
User	Limited privilege	Switch>	Telnet or service port
Privilege (Enable)	Super user power	Switch#	Enter <b>Enable</b> from User mode
Global configuration	Make global changes or the change has system-wide impact	Switch(config)#	Enter <b>config terminal</b> from privilege mode
Interface configuration	Set up interface specific config	Switch(config-if)#	Enter <b>interface g0/Y</b> from global config mode (where <b>Y</b> is the port number to be configured)
VLAN configuration	New way to configure VLAN <b>This is the recommended way to create VLANs</b>	Switch(config-vlan)#	Enter <b>vlan X</b> from global config mode (where <b>X</b> = VLAN ID number)
VLAN database	Old way to configure VLAN <b>Recommended to use new way to create VLANs</b>	Switch(vlan)#	Enter <b>vlan database</b> from privilege mode
Bootloader (ROMMON)	Set boot environment	Switch:	POST failure or corrupt IOS

図8-3 CLI の操作モードの部分的なリスト

次に、CLI の使用法に関するヒントの一覧を示します。

- ▶ 左 / 右矢印キー                      コマンド行で左または右に 1 文字移動する

▶ 上/下矢印キー	コマンド・ヒストリーをスクロールする
▶ タブ・キー	コマンドを補完する
▶ Backspace キー	直前の文字を削除する
▶ スペース・バー	一度に 1 ページ分スクロールする
▶ Enter キー	一度に 1 行分スクロールする
▶ ?	ヘルプ
▶ Ctrl+B	1 文字前に戻る
▶ Ctrl+F	1 文字先に進む
▶ Ctrl+A	先頭に移動する
▶ Ctrl+E	末尾に移動する
▶ Esc+B	1 ワード前に戻る
▶ Esc+F	1 ワード先に進む
▶ Ctrl+P	直前の CLI の再呼び出し
▶ Ctrl+N	次の CLI の再呼び出し
▶ Ctrl+D	1 文字削除する
▶ Ctrl+W	1 ワード削除する
▶ Ctrl+I	CLI の再描画
▶ Ctrl+R	CLI の再描画

<show command> | [ begin | include | exclude ] <REGEXP>

例: *monitor* というワードを含む行を表示する `:sh run | inc monitor`

例: 構成の中でインターフェース *g0/17* から  
始まる行をすべて表示する `:sh run | beg 0/17`

**more** コマンド

(ストリング検索とともに使用) `:more filename | [begin | include | exclude] REGEXP`

## 8.6 便利な IOS CLI トラブルシューティング・コマンド

ここでは、IGESM のトラブルシューティングに便利な IOS コマンドを中心に説明します。

### 8.6.1 データの収集

#### show running

これは最も基本的ですが重要なコマンドの 1 つで、現在実行中の構成を表示します。このコマンドは、構成が期待どおりであることを確認するために使用されます。

構成全体をスクロールするには、スペース・バーを使用します。

```
switch#sh run
Building configuration...

Current configuration : 5907 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
...
```

予期される構成を探してください。たとえば、リストを検討して、目的の VLAN が存在し (vtp 透過モードの場合)、正しいポート上で伝送されていることを確認します。また、予期される EtherChannel、正しい IP アドレッシング、予期される管理 VLAN など、その他の重要な情報についてもこのリストを検討してください。

このコマンドはメモリー内で実行中の構成を表示し、コマンド **show startup** は NVRAM に格納されている構成を表示します。**show running** の情報を NVRAM 内の情報と同期させる（つまり、実行中の構成を NVRAM に保管する）には、**write mem** または **copy running startup** を使用します。

## show vlan

目的の VLAN が存在するかどうか検査します。VLAN がここに存在しない場合は、ポートがその VLAN を使用するように構成されていても、スイッチはその VLAN のデータを伝送しません。

```
switch#sh vlan
VLAN Name                Status        Ports
-----
1 default                 active
2 operational             active        Gi0/1, Gi0/2, Gi0/3, Gi0/6
                        Gi0/7, Gi0/8, Gi0/9, Gi0/10
                        Gi0/11, Gi0/12, Gi0/13, Gi0/14
30 VLAN0030              active        Gi0/15
110 VLAN0110             active
...
```

トランク用に構成され、接続されているポート (**show int status**) は、このリストに表示されません。

## show version

**sh version** は、次の情報を表示します。

- ▶ IGESM 上で実行されているコードのバージョン
- ▶ IGESM が稼働している時間の長さ（最後のブート時から）
- ▶ コードのバージョンと、フラッシュ上でコードがブートされた元場所
- ▶ ベース（最初で最下位の）MAC アドレス（IGESM は複数の MAC を使用するため）
- ▶ 構成レジスター（通常、標準ブートの場合は 0xF）

```
switch#sh version
IOS (tm) CIGESM Software (CIGESM-I6Q4L2-M), Version 12.1(14)AY4, RELEASE SOFTWARE (fc1)
...
switch uptime is 6 days, 54 minutes
System image file is
"flash:/cigesm-i6q4l2-mz.121-14.AY4/cigesm-i6q4l2-mz.121-14.AY4.bin"
...
Base ethernet MAC Address: 00:0F:90:CD:6F:C0
...
Configuration register is 0xF
```

## show tech-support

**show tech-support** は、サポート担当者に役立つ多量の情報をリストします（役に立たないものも含めて）。

**show tech** からの出力は非常に長いので、端末エミュレーターのスクロール・バッファに収まらないことがよくあります。スクロール・データの消失を防ぐには、コマンドを実行する前にデータをファイルに取り込むようにエミュレーターを設定し、ログ・ファイルに取り込んだデータを表示してください。

現在、**show tech-support** の出力に含まれる項目は次のとおりです。

- ▶ **show version**
- ▶ **show running-config**
- ▶ **show stacks**

- ▶ show interfaces
- ▶ show controllers
- ▶ show file systems
- ▶ show flash: all
- ▶ show process memory
- ▶ show process cpu
- ▶ show vlan
- ▶ show clock
- ▶ show etherchannel summary
- ▶ show int trunk
- ▶ show cdp neighbors
- ▶ show spanning-tree summary
- ▶ show mac-address-table count
- ▶ show log
- ▶ show region
- ▶ show buffers

show tech-support に含まれない、有用な項目のいくつかを次に示します。

- ▶ show platform summary
- ▶ show int status
- ▶ show span blocked

## show platform summary

show platform summary は、たとえば管理モジュール上で特定のオプションが構成されたことなど、他の IGESM コマンドが表示できないデータを表示するために重要です。

図 8-4 に、このコマンドの重要な属性のいくつかを示します。

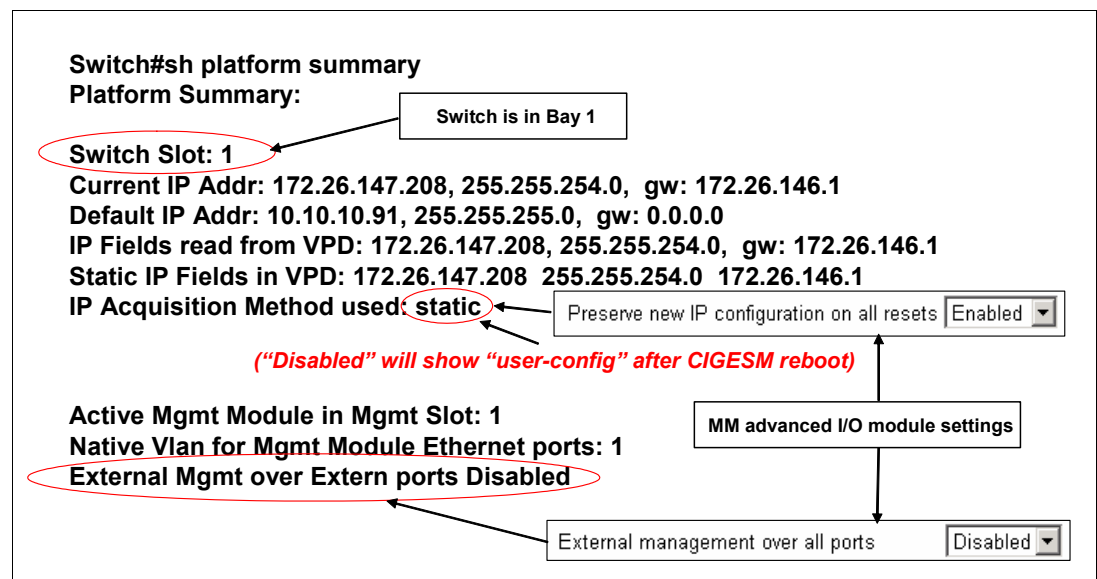


図 8-4 Show platform summary の属性

## show logging

show logging は基本的に、スイッチ上で発生したイベントのローカル・リポジトリで、コンソール・メッセージなどのアクティビティを追跡する FIFO バッファです。このバッファは、大きく構成することも小さく構成することもできます。



何らかの異常や予期しない現象（たとえば、不適切な時期にリンクがダウン状態になった、リンク状態グループが変更された）が過去に発生していないかどうか、ここで確認できます。

## 8.6.2 管理

### **term monitor (term no monitor)**

コンソール出力を現行端末エミュレーション・セッションにリダイレクトします。

Telnet でログインした場合は、このコマンドを最初に実行しない限り、重要なコンソール・メッセージが表示されません（con メッセージを表示したい場合は、Telnet でログインするたびに実行する必要があります）。

### **clear counters**

特定の時点からカウンターを容易にモニターできるように、インターフェース・カウンターをクリアします。

### **clear log**

古いログ・メッセージを消去し、新しく開始できます。

### **clear arp**

arp キャッシュを消去します。IGESM 管理 IP アドレスと外部デバイスへの接続のトラブルシューティング時に便利です。

### **clear mac add**

MAC アドレス・テーブルを消去し、必要なすべての MAC の再学習をスイッチに強制します。

### **no logging console (logging console) - conf t モードから**

コンソール・ポートへの接続時に、メッセージが操作の妨げになっている（スクロールが速すぎ、コマンドの入力の妨げになっている）ときに便利です。

通常の動作時にはコンソール・メッセージがよく必要になるので、完了したら必ず **logging console** に再設定してください。

## 8.6.3 トラブルシューティング

### **ping**

基本的なネットワーク接続をテストするために使用します。次の 2 つのモードがあります。

- ▶ **単純（対話式でない）** : **ping** コマンドと、ping する IP アドレスを入力します。

```
Enter the ping command followed by an address and then the Enter key
switch#Ping 172.26.146.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.26.146.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/12 ms
```

- ▶ **拡張 (対話式)** : オプションを指定せずに **ping** コマンドを入力します。**ping** の実行オプションを指定するためのプロンプトが出されます。この方法では、コマンドの特性を非常に柔軟に制御できます。

**ping** コマンドを入力した後、Enter キーを押して変数を入力します。

```
switch#ping
Protocol [ip]:
Target IP address: 172.26.146.1
Repeat count [5]: 10
Datagram size [100]: 1000
Timeout in seconds [2]: 1
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 10, 1000-byte ICMP Echos to 172.26.146.1, timeout is 1 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 4/4/4 ms
```

## show cdp neighbor

**show cdp neighbor** は、強力なトラブルシューティング・コマンドです。このコマンドは最小で、リンクの両側に接続されているポートを表示します。また、リンクの相手側にあるデバイスのタイプ、リンクの相手側の IOS バージョン、およびリンクの相手側にあるデバイスの IP アドレスも表示できます。(相手側の IOS と IP アドレスを表示するには、**show cdp neighbor** コマンドの末尾にキーワード **detail** を追加する必要があります)

リンクの両側が Cisco デバイスであることが必要です。(CDP は Cisco プロプライエタリー・プロトコルです)

図 8-5 に、このコマンドの属性を示します。

- **Very important tool – Based on Cisco Discovery Protocol**
- **CDP is a Cisco protocol that runs between links and learns information about the connection**
- **Shows connection info from CIGESM to uplinks**
  - Shows device name/model number, ports used, etc.
  - cigesm\_t#sh cdp nei

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge  
S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
c3750-24_A	Gig 0/19	143	S I	WS-C3750-2Fas	1/0/19
c3750-24_A	Gig 0/20	143	S I	WS-C3750-2Fas	1/0/20
c3750-24_A	Gig 0/18	143	S I	WS-C3750-2Fas	1/0/18
c3750-24_A	Gig 0/17	143	S I	WS-C3750-2Fas	1/0/17
cigesm_t	Gig 0/15	164	S I	OS-CIGESM-Gig	0/15

Device name on other side of link

Port on this side of link

Model of device on other side

Remote port number

- **Very handy to confirm cables are plugged into correct ports**
- “show cdp nei detail” gives even more information on device on the other side of the link

図 8-5 show cdp nei コマンドの出力

## show int status

このコマンドは、IGESM の接続状況のスナップショットを提供します（228 ページの図 8-6）。

cigesm_t#sh int status							Port number
Port	Name	Status	Vlan	Duplex	Speed	Type	
Gi0/1	blade1	notconnect	2	full	1000	1000Mbps	SERDES
Gi0/2	blade2	notconnect	2	full	1000	1000Mbps	SERDES
Gi0/3	blade3	notconnect	2	full	1000	1000Mbps	SERDES
Gi0/4	blade4	connected	trunk	full	1000	1000Mbps	SERDES
Gi0/5	blade5	connected	trunk	full	1000	1000Mbps	SERDES
Gi0/6	blade6	notconnect	2	full	1000	1000Mbps	SERDES
Gi0/7	blade7	notconnect	2	full	1000	1000Mbps	SERDES
Gi0/8	blade8	notconnect	2	full	1000	1000Mbps	SERDES
Gi0/9	blade9	notconnect	2	full	1000	1000Mbps	SERDES
Gi0/10	blade10	notconnect	2	full	1000	1000Mbps	SERDES
Gi0/11	blade11	notconnect	2	full	1000	1000Mbps	SERDES
Gi0/12	blade12	notconnect	2	full	1000	1000Mbps	SERDES
Gi0/13	blade13	notconnect	2	full	1000	1000Mbps	SERDES
Gi0/14	blade14	notconnect	2	full	1000	1000Mbps	SERDES
Gi0/15	mgmt1	connected	trunk	full	100	10/100/1000BaseTX	
Gi0/16	mgmt2	notconnect	30	full	100	10/100/1000BaseTX	
Gi0/17	extern1	connected	trunk	a-full	a-100	10/100/1000BaseTX	
Gi0/18	extern2	connected	trunk	a-full	a-100	10/100/1000BaseTX	
Gi0/19	extern3	connected	trunk	a-full	a-100	10/100/1000BaseTX	
Gi0/20	extern4	connected	trunk	a-full	a-100	10/100/1000BaseTX	
Po1		connected	trunk	a-full	a-100		
Po2		connected	trunk	a-full	a-100		

Port number

Status of port

connected = Link up

notconnect= Link down

Err-disable = Link down

If "connected" –

Shows trunk if 802.1Q trunk

Shows VLAN # if access mode

If "notconnected"

Shows native VLAN if trunk

Shows VLAN # if access mode

Speed/duplex setting for port

Leading "a" = Auto-negotiated

図 8-6 show interface status コマンドの出力

## show ip int brief

show ip int brief は show int status と類似していますが、別のフォーマットで管理 VLAN インターフェースを表示します。図 8-7 に、このコマンドの属性のいくつかを示します。

cigesm_b#sh ip int brief						
Interface	IP-Address	OK?	Method	Status	Protocol	
Vlan1	unassigned	YES	NVRAM	administratively down	down	
Vlan30	172.26.147.209	YES	unset	up	up	
GigabitEthernet0/1	unassigned	YES	unset	down	down	
GigabitEthernet0/2	unassigned	YES	unset	down	down	
GigabitEthernet0/3	unassigned	YES	unset	down	down	
GigabitEthernet0/4	unassigned	YES	unset	up	up	
GigabitEthernet0/5	unassigned	YES	unset	up	up	
GigabitEthernet0/6	unassigned	YES	unset	down	down	
...						
GigabitEthernet0/14	unassigned	YES	unset	down	down	
GigabitEthernet0/15	unassigned	YES	unset	up	up	
GigabitEthernet0/16	unassigned	YES	unset	down	down	
GigabitEthernet0/17	unassigned	YES	unset	up	up	
GigabitEthernet0/18	unassigned	YES	unset	up	up	
GigabitEthernet0/19	unassigned	YES	unset	administratively down	down	
GigabitEthernet0/20	unassigned	YES	unset	administratively down	down	
Port-channel1	unassigned	YES	unset	up	up	
Port-channel2	unassigned	YES	unset	down	down	

図 8-7 show ip int brief の出力

## shut - no shut (インターフェース構成モード)

インターフェースの管理シャットダウンまたは立ち上げを行うために使用します。インターフェース構成モードで実行します。

Telnet でログインした場合は、**term mon** を使用してポートのアップ / ダウンのメッセージを確認します。ポートが管理シャットダウン中かどうか確認するには、**show int status** を使用します。

**shut - no shut** は、err-disable 状態のポートをクリアするために非常に便利です。(例外: トランク・フェイルオーバー機能を使用している場合、**shut - no shut** は err-disabled をクリアするための手段にはなりません。アップストリームに定義されたポートがすべてダウン状態になった場合、トランク・フェイルオーバーに対して **err-disable** は異常ではなく、正常な状態です。アップストリームを修正すれば **err-disable** は修正されます)

```
cigesm_t#conf t
Enter configuration commands, one per line. End with CNTL/Z.
cigesm_t(config)#int g0/5
cigesm_t(config-if)#shut
cigesm_t(config-if)#
12:50:36: %LINK-5-CHANGED: Interface GigabitEthernet0/5, changed state to
administratively down
12:50:37: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/5, changed
state to down
cigesm_t(config-if)#no shut
cigesm_t(config-if)#
12:50:46: %LINK-3-UPDOWN: Interface GigabitEthernet0/5, changed state to up
12:50:48: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/5, changed
state to up
```

**重要: shut** は、インターフェースを通過するすべてのトラフィックを効率的にブロックするために使用されます。これによりデータ・フローが中断するので、このコマンドを使用した結果を理解しているユーザーのみが使用する必要があります。

## show int g0/X

図 8-8 は、**sh int g0/X** ( $X$  は 1 から 20 までの番号) コマンドからの出力を示しています。これは、インターフェースのスループットとエラー条件をモニターするために非常に便利です。新しくモニターを開始するためにインターフェースの数値をクリアするには、**clear counters** を使用します。

- **Show status of individual interface along with input/output stats and error stats**

```
cigesm_t#sh int g0/5
GigabitEthernet0/5 is up, line protocol is up (connected)
Hardware is Gigabit Ethernet, address is 000f.90cd.6fc5 (bia 000f.90cd.6fc5)
Description: blade5
...
Full-duplex, 1000Mb/s, link type is auto, media type is unknown 0
...
5871 packets input, 633470 bytes, 0 no buffer
Received 1210 broadcasts (0 multicast)
0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 0 multicast, 0 pause input
0 input packets with dribble condition detected
13265 packets output, 1409452 bytes, 0 underruns
0 output errors, 0 collisions, 4 interface resets
0 babbles, 0 late collision, 0 deferred
0 lost carrier, 0 no carrier, 0 PAUSE output
0 output buffer failures, 0 output buffers swapped out
```

Port link state

Port speed/duplex

Input stats and errors for interface

output stats and errors for interface

図8-8 sh int g0/X コマンドの出力

## show int trunk

図 8-9 に、show int trunk コマンドの属性のいくつかを示します。

- **Lets you know what VLANs can be carried and are being carried on trunk ports**

```
cigesm_t#sh int trunk
```

Port	Mode	Encapsulation	Status	Native vlan
Gi0/15	on	802.1q	trunking	30
Po1	on	802.1q	trunking	1
Po2	on	802.1q	trunking	1

Native VLAN in use on trunk link

Port	Vlans allowed on trunk
Gi0/15	30,4094
Po1	1-29,31-4093
Po2	1-29,31-4093

VLANs that CAN be carried on trunk

Port	Vlans allowed and active in management domain
Gi0/15	30,4094
Po1	1-2,110,333,444,777-779
Po2	1-2,110,333,444,777-779

VLANs that ARE carried on trunk

Make sure any VLANs you want carried show up in this list on the proper interfaces. If they do not, make sure VLAN exists and that it's assigned to be carried on the desired interfaces

Port	Vlans in spanning tree forwarding state and not pruned
Gi0/15	30,4094
Po1	1-2,110,333,444,777-779
Po2	2,110,333,444

VLANs on trunk not being blocked by spanning-tree

図8-9 sh int trunk コマンドの出力

## show etherchannel summary

図 8-10 に、show eth sum コマンドの出力を示します。このコマンドは、単純な ping テストに合格できるかどうかの検査だけでなく、アグリゲーションの正常性を検査するために重要です。

- **Important to monitor the health of the Etherchannel connection**

cigesm\_t#sh eth sum

Flags: D - down P - in port-channel

I - stand-alone s - suspended

H - Hot-standby (LACP only)

R - Layer3 S - Layer2

u - unsuitable for bundling

U - in use f - failed to allocate aggregator

d - default port

Number of channel-groups in use: 2

Number of aggregators: 2

Group Port-channel Protocol Ports

Group	Port-channel	Protocol	Ports
1	Po1(SU)	LACP	Gi0/17(Pd) Gi0/18(P)
2	Po2(SU)	LACP	Gi0/19(P) Gi0/20(Pd)

This example shows a switch with two Etherchannels bundles, one using ports 17 and 18 and one using ports 19 and 20

SU = good

Anything else = problem

Shows ports assigned to bundle

P or Pd = good

Anything else = problem

図8-10 show eth sum コマンドの出力

## show spanning-tree blockedports

このコマンドは、ブロックされているポート、および転送中のポートを、問題が始まる前に確認するために重要です。あらゆるリンクアップ/ダウン条件下で問題が予測可能であることが必要です。

スイッチが2つの EtherChannel ポート (Po1 と Po2) を備えていて、ルート・スイッチが Po1 に接続されている場合の例を次に示します。

cigesm\_t#sh spanning-tree blockedports

Name Blocked Interfaces List

Name	Blocked Interfaces List
VLAN0001	Po2
VLAN0777	Po2
VLAN0778	Po2
VLAN0779	Po2

Number of blocked ports (segments) in the system : 4

## show spanning-tree root

図 8-11 に、show span root コマンドの属性のいくつかを示します。show span blocked コマンドと同様に、障害が起こった場合に転送やブロッキングが変化したことが分かるように、正常動作時のスパンニング・ツリーを確認しておくことが重要です。

- Somewhat of the inverse of the show span blocked command
- Important to know what ports are closest to the root switch

cigesm\_t#sh spanning-tree root

Vlan	Root ID	Root Hello Cost	Max Fwd Time	Age	Dly	Root Port
VLAN0001	32768 000f.f88c.6c00	31	2	20	15	
VLAN0002	32770 000f.90cd.6fc0	0	2	20	15	
VLAN0030	32798 000f.90cd.6fc0	0	2	20	15	
VLAN0110	32878 000f.90cd.6fc0	0	2	20	15	
VLAN0777	32768 000f.f88c.6f08	31	2	20	15	Po1
VLAN0778	32768 000f.f88c.6f09	31	2	20	15	Po1
VLAN0779	32768 000f.f88c.6f0a	31	2	20	15	Po1
VLAN4094	36862 000f.90cd.6fc0	0	2	20	15	

In this example, VLANs not carried off of this switch

This switch is root for these VLANs so there is no entry in "Root port"

VLANs carried off of this switch, Po1 in this design is the closest connection to the root switch

図8-11 show span root コマンドからの出力

## show link state group detail

show link state group detail は、トランク・フェイルオーバー機能の構成と状況を報告します。

```
Switch#show link state group detail
Link State Group: 1      Status: Enabled, Up
Upstream Interfaces   : Po1(Up) Po2(Up)
Downstream Interfaces : Gi0/1(Up) Gi0/2(Up) Gi0/3(Up) Gi0/4(Up)
Gi0/5(Up) Gi0/6(Up) Gi0/7(Up) Gi0/8(Up) Gi0/9(Up) Gi0/10(Up)
Gi0/11(Up) Gi0/12(Up) Gi0/13(Up) Gi0/14(Up)

Link State Group: 2      Status: Disabled, Down
Upstream Interfaces   :
Downstream Interfaces :
(Up):Interface up    (Dwn):Interface Down    (Dis):Interface disabled
```

アップストリーム・インターフェースに、予期されるインターフェースが含まれていることを確認します。すべてが正しく機能していれば、アップストリーム・インターフェースがすべて「up」と表示されます。

ダウンストリーム・インターフェースに、予期されるインターフェースが含まれていることを確認します（目的の構成によっては、すべてのインターフェースが含まれる場合があります）。構成済みのダウンストリーム・インターフェースすべてが AuUpAv と表示されている必要があります。グループに対して構成されたアップストリーム・ポートすべてがダウン状態になると、ダウンストリーム・ポートは AuDisAv になります。

## show arp

IGESM の管理インターフェースとアップストリーム接続との間、または管理モジュールとの間で生じる接続の問題のトラブルシューティングに役立つ show arp は、IGESM の管理 VLAN インターフェースに対する接続の問題のトラブルシューティングにも便利です。

ARP テーブルは、デバイス（この場合は IGESM）が特定の IP アドレスの MAC アドレスを解決できることを示します。

ARP 解決は、デバイスが別の IP アドレスとの対話を試みるとき最初に行われる処理です。（IP アドレスは認識していますが、指定パケットを送信するために MAC アドレスを確認する必要があります）

```
cigesm_t#sh arp
Protocol Address      Age (min) Hardware Addr  Type   Interface
Internet 172.26.146.1        105      0009.6bca.eba3  ARPA   Vlan30
Internet 172.26.147.208      -        000f.90cd.6fc0  ARPA   Vlan30
```

## SPAN および RSPAN

SPAN および RSPAN は、デバイスとの間でやり取りされるパケットを取り込み、分析するために、ネットワーク・スニファと組み合わせて使用できるツールです。また、これらを使用して、IDS（侵入検知システム）にデータを送信することもできます。

重要：リダイレクトされたトラフィックによってリンクのオーバー・サブスクリプションが生じ、その結果としてトラフィックがドロップされる可能性があるため、RSPAN は注意して使用する必要があります。

SPAN は、この IGESM 上のいずれかのポートから特定の物理ポートに、モニター対象のパケットをこの IGESM 上で直接切り替えるために使用されます。

RSPAN は、モニター対象のパケットを特殊な VLAN に切り替え、このスイッチ上にないリモート・ポートに伝送するために使用されます。

SPAN と RSPAN を両方使用して、SPAN/RSPAN の宛先であるポートにスニファを接続します。

SPAN と RSPAN の使用法は、この配置方法について説明した Redpaper の第 7 章、170 ページの 7.5.3、『トポロジー 3a: デュアル Cisco Systems IGESM、RSPAN を使用した 2 ポート・アグリゲーション』に記載されています。

## debug

IGESM 内のさまざまなアクティビティをモニターするために使用される、数多くの debug コマンドが IOS に備わっています。

**警告：** debug コマンドを使用する際には、*最大限*に注意してください。

debug は、経験を積んだ管理者のみが使用することをお勧めします。使用法を誤ると、IGESM の望ましくない動作が予期せず発生し、スイッチへのトラフィックやスイッチを通過するトラフィックのフローが中断されることがあるので、ネットワークがダウン状態になる可能性があります。結果を理解していない限り、使用しないでください。

**debug all** は使用しないでください。

複数のデバッグを同時に実行することができますが、デバッグの数が多すぎるとスイッチの CPU に過大な負荷がかかる可能性があります。

現行デバッグを表示するには、**show debug** を使用します。

デバッグを停止するには、コマンドの **no** 形式を使用します。例：**no debug arp**



実行中の **debug** コマンドすべてを単一のコマンドによって停止するには、**u all** (**undebbug all** の短縮形) を使用します。トラブルシューティングを完了したら、必ず **u all** を実行します。

Telnet でログインしている場合は、**term monitor** を実行するとメッセージが表示されます。

よく使用されるデバッグの例を次に示します。

▶ **debug arp**

IGESM の管理インターフェースとの間でやり取りされる ARP 要求をモニターします。

▶ **debug ip packet**


IGESM との間でやり取りされる (IGESM を通過しない) IP トラフィックをモニターします。

▶ **debug cdp packets**

IGESM と他のデバイスとの間の CDP パケットをモニターします。

▶ **debug ip icmp**

IGESM との間でやり取りされる (IGESM を通過しない) **ping** トラフィックをモニターします。



## サービスおよびサポート

Cisco Systems Intelligent Gigabit Ethernet Switch Module のサポートは、次に示す方法でお客様に提供されています。

## 9.1 IBM に連絡する

U.S.、AP、CAN、および EMEA の場合 : IBM に電話でテクニカル・サポートを依頼する場合は、次のいずれかの番号を使用してください。

- ▶ 米国内では、IBM サポートの電話番号は 1-800-IBM-SERV (426-7378) です。
- ▶ カナダの場合 :
  - サポートについては、HelpPC (800-426-7378) にお電話ください。
  - 詳細または発注については、800-465-7999 にお電話ください。
- ▶ 米国およびカナダ以外では、IBM HelpWare® の番号、ご購入先、またはお近くの IBM オフィスにご連絡ください。

LA の場合 : テクニカル・サポートについては、IBM HelpCenter® にお電話いただくか、IBM HelpWare の番号、ご購入先、またはお近くの IBM オフィスにご連絡ください。

## 9.2 オンライン・サービス

U.S.、AP、CAN、および EMEA でのオンライン・サービスについては、次の Web サイトをご覧ください。

<http://www.ibm.com/support/us/>

LA でのオンライン・サービスについては、次の Web サイトをご覧ください。

<http://www.ibm.com/pc/la>

オンライン・ディレクトリー・サービスについては、次の Web サイトにある「Directory of World Wide Contacts」にアクセスし、国を選択してください。「*technical support*」の下で該当する電話番号を探し、IBM に支援を依頼してください。

<http://www.ibm.com/planetwide/>

## 9.3 発注について

Cisco Systems Intelligent Gigabit Ethernet Switch Module の注文部品番号は 13N2281 です。

- ▶ U.S. の場合 :

PartnerLink を通じたご注文については、800-426-7272、オプション 8 にお電話ください。詳しくは、IBM Remarketer Fulfillment Center (800-426-9735)、またはマーケティング・サポート担当者にお問い合わせください。

- ▶ EMEA の場合 :

配送システムにご注文を入力できるようになりました。ご注文は順次スケジュールに入れます。ご注文に複数の装置が含まれる場合は、配送スケジュールが延長されることがあります。スケジュールが確定するまで、配送に関する確約は行われません。パーソナル・コンピューティング部門ビジネス・パートナーへの本製品の配送は、SAP/Direct Ship の受注システムおよびプロセスによって行われます。

- ▶ オンライン :

本製品は、オンラインの BladeCenter スイッチ・モジュール Web サイトから入手可能です。

[http://www.ibm.com/servers/eserver/bladecenter/switch/more\\_info.html](http://www.ibm.com/servers/eserver/bladecenter/switch/more_info.html)

## 9.4 その他のサポート・サイト

次に、その他の有用な Web サイトのリストを示します（Cisco のユーザー名とパスワードが必要になる場合があります）。

- ▶ TAC メイン・サポート・ページ  
<http://www.cisco.com/en/US/partner/support/index.html>
- ▶ TAC サービス要求ツール  
[http://www.cisco.com/cgi-bin/front.x/case\\_tools/case0open.pl](http://www.cisco.com/cgi-bin/front.x/case_tools/case0open.pl)
- ▶ SVO サブミット  
[http://www.cisco.com/cgi-bin/front.x/agents/svo\\_tools/SV0ToolDispatcher](http://www.cisco.com/cgi-bin/front.x/agents/svo_tools/SV0ToolDispatcher)
- ▶ Cisco CCO – オンライン資料  
<http://www.cisco.com/univercd/home/home.htm>
- ▶ Cisco TAC - Catalyst スイッチのベスト・プラクティス  
<http://www.cisco.com/warp/customer/473/103.html>





## ヒント

ここでは、Cisco Systems Intelligent Gigabit Ethernet Switch Module for the IBM **@server** BladeCenter のセットアップ、構成、および操作の際に役立つヒントを示します。

本書ですでに説明したとおり、本書の情報は IOS の 12.1(14) バージョンを実行する 4 ポート・銅ベースの IGESM に適用されます。4 ポート SFP ベースの IGESM、または IGESM 12.1(22) 以上のコードを実行する 4 ポート・銅ベースの IGESM を使用する場合は、これらのソリューションに該当する資料を参照してください。

### ブレード・サーバーの NIC の番号付け

ブレード・サーバー上のどの接続が、BladeCenter 内のどの Cisco Systems IGESM と結合するかについては、多少の解説が必要です。

実際には、HS20/JS20 ブレード・サーバー上にある第 1 の物理 NIC は常にベイ 1（上部ベイ）の IGESM に結合し、HS20/JS20 ブレード・サーバー上にある第 2 の物理 NIC は常にベイ 2（下部ベイ）の IGESM に結合します。これは BladeCenter 内で配線されており、変更できません。

ところが、ブレード・サーバーを実行するオペレーティング・システムがこれらの物理 NIC に通常適用する論理名は、予期されるものとは逆になる場合があります。次に、このようなことが起こる理由と、どの論理接続がどの物理 NIC に結合しているか判別する方法を説明します。

ほとんどの場合、Windows 2000 では、ローカル・エリア接続 という名前の接続がスイッチ・ベイ 1 の Cisco Systems IGESM に結合し（103 ページの第 7 章、『Cisco Systems IGESM の構成およびネットワーク統合』では CIGESM1 と呼ばれています）、ローカル・エリア接続 2 という名前の接続がスイッチ・ベイ 2 の Cisco Systems IGESM に結合します（第 7 章では CIGESM2 と呼ばれています）。

ほとんどの場合 という表現を使ったのは、すでに説明したとおり、これが当てはまらないケースもあるからです。

Windows 2000 では、ローカル・エリア接続の論理名 が物理 NIC に割り当てられる順序は、それぞれの NIC 用のドライバーがインストールされた 順序 によって決まります。ブレー

ド・サーバー上の NIC のサポートに必要なドライバーは Windows 2000 の標準インストールには含まれておらず、必要なドライバーがロードされるまで、NIC は Windows 2000 デバイス・マネージャーに複数のイーサネット・コントローラーとして総称的にリストされます（疑問符が隣に付いて）。これらの NIC をアクティブにするには、IBM 提供のサード・パーティー・ドライバーをインストールする必要があります。ほとんどのユーザーが通常行う手順では、ドライバーをまずリストの先頭にあるイーサネット・コントローラーにインストールし、その後リストの 2 番目にあるイーサネット・コントローラーにドライバーをインストールします（以降も同様）。この最終的な結果が、前に説明したほとんどの場合のシナリオであり、ローカル・エリア接続という名前の Windows 2000 接続は CIGESM1 に結合し、ローカル・エリア接続 2 という名前の接続は CIGESM2 に結合します。

一方、リストの 2 番目にあるイーサネット・コントローラーにドライバーを最初にインストールし、次にリストの先頭にあるイーサネット・コントローラーにインストールした場合、接続名は逆になり、ローカル・エリア接続という名前の接続が CIGESM2 に結合し、ローカル・エリア接続 2 という名前の接続が CIGESM1 に結合します。

**重要：** 混乱を避けるために、リストの先頭にあるイーサネット・コントローラーからリストの末尾にあるイーサネット・コントローラーまで、ドライバーを常に順序どおりインストールしてください。

Windows Server 2003 の場合はネイティブ Broadcom ドライバーが存在し、これは論理的に分かりやすい順序でロードされる場合もされない場合もあります。ローカル・エリア接続は上部または下部のどちらの NIC とも結合する可能性があり、ローカル・エリア接続 2 は他方の物理 NIC と結合します。

Linux の場合、デフォルトの eth0 はスイッチ・ベイ 2 の Cisco Systems IGESM（第 7 章の例では CIGESM2）と結合し、eth1 はスイッチ・ベイ 1 の Cisco Systems IGESM（第 7 章の例では CIGESM1）と結合します。これは前述のとおり、通常 Windows 2000 インストールとは逆であり、ドライバーのインストール順序による影響を受けることがあります。

**重要：** どの論理 NIC がどの物理 IGESM と結合しているか判別するための補助手段として、先頭の IGESM に Telnet でログインし、対象のブレード・サーバーと結合しているインターフェースを先頭の IGESM 上でシャットダウンできます。この IGESM 側でのシャットダウンにより、ブレード・サーバー側の接続のどちらかがダウン状態として報告されます。オペレーティング・システムが割り当てた論理名と関係なく、ダウン状態として報告されたどちらかが、先頭の IGESM に物理的に接続されているものです。

この手順を逆に使用する（OS から NIC のどちらかを使用不可に設定し、それぞれの IGESM にアクセスしてどちらのポートがダウン状態になったか調べる）ことも有効ですが、ブレード・サーバー側でポートを使用不可に設定すると、ブレード・サーバーの物理インターフェースの性質により、IGESM 側のポートはダウン状態になることもありません。このため、論理リンクと物理リンクの接続性を判別するには最初の方法をお勧めします。

## マルチホーム・サーバー上でのデフォルト・ゲートウェイの構成

BladeCenter 内のほとんどのブレード・サーバー（HS20/JS20）は、デフォルトでネットワークに対して 2 つの接続を使用し、通常はそれぞれ別個の IP サブネットに配置されます。Broadcom チューニング・ソフトウェアを使用すれば、物理接続上で使用可能な数を超えるサブネットをブレード・サーバー上で構成できます。その結果、ブレード・サーバーに複数の IP サブネットが構成されることがよくあります。

よく尋ねられることに、ブレード・サーバーなどのマルチホーム・システム上で構成されるそれぞれの IP サブネットには、デフォルト・ゲートウェイを割り当てる必要があるのか、という質問があります。答えは簡単ではありません。

この章に示す例ではすべて、ただ 1 つのインターフェースにデフォルト・ゲートウェイが指定され、その他のインターフェースのデフォルト・ゲートウェイのフィールドは空白のままです。これは、この解決策がユーザーの環境に最適であるということを意味しているのではなく、環境にはそれぞれ固有の要件があります。これらの例では、単純化のためにこの設定を使用しているに過ぎません。

Microsoft は、マルチホーム・システム上でのデフォルト・ゲートウェイに対するさまざまなアプローチを説明するナレッジ・ベース記事 157025 を公開しました。この記事は、次のアドレスで入手できます。

<http://support.microsoft.com/default.aspx?scid=kb;en-us;157025>

ユーザー個々の環境でこの問題に対処するにはどの方法が最適なのか疑問がある場合、BladeCenter システム管理者はこの資料を検討することをお勧めします。

## 重複 IP アドレス：その 1

構成の選択によっては、既知の競合が存在しなくても、BladeCenter が重複 IP アドレスを報告する場合があります。

ブレード・サーバーが重複アドレスを報告する最も一般的な原因は、ブレード・サーバーのインターフェースの 1 つが、Cisco Systems IGESM の管理 VLAN（デフォルトは VLAN 1）と同じ VLAN に配置され、管理モジュール内部で Cisco Systems IGESM との通信に使用されている管理アドレスと同じサブネット内の IP アドレスを使用していることです。

この場合、管理モジュールはこのサブネット上のすべてのアドレスに対してプロキシとして機能しようとし（外部インターフェース経由で Cisco Systems IGESM への外部アクセスを可能にするために）、内部の管理サブネット全体にあるすべてのアドレスに対する照会に応答します。この場合、ブレード・サーバーがネットワーク内で自身のアドレスが使用可能かどうか検査するときに（自身のアドレスに対する ARP 要求を送信する）、管理モジュールはこのブレード・サーバー・アドレスに対する ARP 要求に応答し、ブレード・サーバーはそのアドレスが使用中であると見なし、このことを Windows 2000 のポップアップ・メッセージによって報告します。

最も簡単な解決策は、ブレード・サーバーを常に Cisco Systems IGESM の管理 VLAN から分離することです（Cisco Systems IGESM のデフォルト管理 VLAN は VLAN 1 です）。ブレード・サーバーがこの VLAN に配置される可能性を減らすために、Cisco Systems IGESM はブレード・サーバーに接続するすべてのポート（g0/1 から g0/14）のデフォルトを次のように設定します。

```
switchport access vlan 2
switchport trunk native vlan 2
switchport trunk allowed vlan 2-4094
```

ただしこの設定は、ブレード・サーバーに接続するポートにユーザーが VLAN 1（または管理 VLAN であるいずれかの VLAN）を追加して、ここに説明した結果を招くことを防止するものではありません。

この問題の原因についての詳しい説明は、76 ページの 5.3.12、『シナリオ 6（非推奨）』を参照してください。



**重要:** ブレード・サーバーと管理モジュールの間でこのような相互作用が起こる可能性があるため、Cisco Systems IGESM 上で管理 VLAN として使用されているものと同じ VLAN に、ブレード・サーバーを配置しないことを強くお勧めします。

## 重複 IP アドレス：その 2

『重複 IP アドレス：その 1』で説明したとおり、構成の選択によっては、既知の競合が存在しなくても、BladeCenter が重複 IP アドレスを報告する場合があります。ここでは、Cisco Systems IGESM が重複 IP アドレスを報告することに伴う問題について説明します。

最もよくある原因は、Cisco Systems IGESM の管理 IP アドレスを Cisco Systems IGESM 上で直接変更しようとしたことです（CLI または CMS のどちらかを使用して）。

管理モジュール Web インターフェース以外の手段を使用して、ユーザーが Cisco Systems IGESM 上の管理 VLAN IP アドレスを管理モジュールから受信したもの以外に変更すると、管理モジュールを経由した Cisco Systems IGESM の管理 IP アドレスへの IP 通信はすべて失敗し、Cisco Systems IGESM は重複 IP アドレスの報告を開始します。この重複 IP アドレスのメッセージは、IP アドレスを元の場所と同じサブネット内のアドレスに変更した場合に限って発生することに注意してください。たとえば、192.168.70.127 から 192.168.70.150 に変更した場合は重複 IP アドレスのメッセージが出されますが、192.168.70.127 から 10.35.15.1 に変更した場合は重複 IP アドレスのメッセージは出されません（ただし、管理モジュールを経由した IGESM への IP 通信は失われる可能性が高くなります）。

この問題の例として、次の一連のイベントを見てみましょう。（これは実際にやった場合の説明のみを目的としており、実動システム上では実行しないでください）

Cisco Systems IGESM の管理 VLAN の現行 IP アドレスを表示して、正しい構成を確認します（この例では、デフォルト IP アドレスを使用します）。

```
CIGESM1#sh run int vlan 1
INTERFACE Vlan1
  ip address 192.168.70.127 255.255.255.0
  no ip route-cache
```

Cisco Systems IGESM から管理モジュールの内部 IP アドレスへの **ping** をテストして、接続が機能していることを確認します。

```
CIGESM1#ping 192.168.70.126
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.70.126, timeout is 2 seconds:
!!!!
```

```
Success rate is 100 percent (5/5)
```

Cisco Systems IGESM の IP アドレスを別のアドレスに変更します。

```
CIGESM1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
CIGESM1(config)#int vlan 1
CIGESM1(config-if)#ip add 192.168.70.150 255.255.255.0
CIGESM1(config-if)#
```

この変更を行ってから少し後に、Cisco Systems IGESM のコンソール上で重複アドレスのメッセージの受信が始まります。

```
1d19h: %IP-4-DUPADDR: Duplicate address 192.168.70.150 on Vlan1, sourced by 0009.6bca.7499
```

次に、元のアドレスに再び変更します。

```
CIGESM1(config-if)#  
CIGESM1(config-if)#ip add 192.168.70.127 255.255.255.0  
CIGESM1(config-if)#
```

重複アドレスのメッセージの受信が続きます。

```
1d19h: %IP-4-DUPADDR: Duplicate address 192.168.70.127 on Vlan1, sourced by  
0009.6bca.7499
```

Cisco Systems IGESM から管理モジュールの内部 IP アドレスへの **ping** をテストすると、失敗します。

```
CIGESM1#ping 192.168.70.126  
Type escape sequence to abort.  
Sending 5, 100-byte ICMP Echos to 192.168.70.126, timeout is 2 seconds:  
.....  
Success rate is 0 percent (0/5)
```

この問題の原因は、重複 IP アドレス : その 1 で報告された重複 IP アドレスのメッセージに関連しています (管理モジュールが自身の内部サブネット上のアドレスに対する ARP 要求に応答する)。この状態が発生しないようにするには、管理 VLAN の IP アドレスの変更を必ず管理モジュールの Web インターフェースから行うようにします。

この問題がすでに発生している場合の解決策は、次のとおりです。

▶ 解決策 1

最も安全で推奨されるアプローチとしては、管理モジュールの Web インターフェースに接続し、ウィンドウの左側にある「I/O Module tasks」の「**Management**」をクリックし、問題が発生しているペイを選択して (この例ではペイ 1)、ペイ 1 の Cisco Systems IGESM に対して表示されている IP アドレスが適切に設定されていることを確認し (そうでなければ、望ましいアドレスに変更します)、「**Save**」をクリックします。これにより、管理モジュールと Cisco Systems IGESM の間で再び IP アドレスの同期が取られ、通信が復元されます。(また、重複 IP アドレスのメッセージは停止します)

▶ 解決策 2

次の手順によって競合を解決することもできますが、Cisco Systems IGESM のリブート中はトラフィックが中断されます。IGESM の IP アドレスを元の値に設定し、構成を保管して、Cisco Systems IGESM を再ロードします。リブートしてオンラインに復帰すると、Cisco Systems IGESM と管理モジュールが同期した状態に戻ります。

**重要:** この問題が発生する可能性を減らすために、Cisco Systems IGESM のアドレスの変更は必ず管理モジュールの Web ベース・インターフェースから行い、IGESM 自身で直接変更しないようにしてください。ただし、管理モジュールと IGESM の構成により、IGESM が自身の IP アドレッシング情報を管理できるようにした場合は、この規則の例外です。(詳しくは、『IGESM IP アドレス情報の制御』(250 ページ)を参照してください)

## チーミングソフトウェアの選択項目がキャンセルできない

Broadcom Advance Control Suite (BACS) と呼ばれる Broadcom ソフトウェアが、ブレード・サーバー上の NIC チーミングの制御に使用されます。このソフトウェアの選択項目の中に、キャンセルなどの方法で選択を取り消すことができないものがいくつか存在し、実行したくないアクションを強制されるように見えることが指摘されています。

このような選択の例を 2 つ示します。

- ▶ 「Team Configuration」ウィンドウの「**Remove VLAN**」をクリックする
- ▶ メニュー・バーの「**Tools**」→「**Delete a team**」を選択する

これらのケースでは、削除する VLAN またはチームを指定するために 244 ページの図 9-1 に示すようなウィンドウが開きますが、操作を取り消すための明示的な手段は提供されません。このような中止できないように見える手順を中止するには、キーボードの Esc キーを押します。

削除する項目がリストに 1 つしか存在しない場合（たとえば、ただ 1 つの VLAN または 1 つのチーム）、BASC ソフトウェアは単にその項目を削除し、元のウィンドウに戻ります。この削除を行いたくない場合、解決策としては、BASC のメインウィンドウで「**Cancel**」をクリックし、変更を保管せずに BASC ソフトウェアを終了するほかにありません。もちろん、このようにすると、最後に「**Apply**」ボタンや「**OK**」ボタンをクリックしてからすでに行っていた他の変更はすべて失われます。

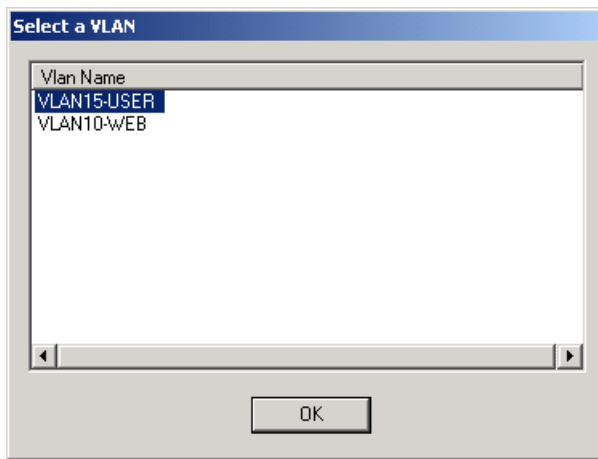


図9-1 取り消すオプションのないBASC ウィンドウの例

## Cisco Systems IGESM が switch: プロンプトで停止する

Cisco Systems IGESM のブート処理中の初期段階に、シリアル・コンソール接続から受信したキー・ストロークがブレイク信号と解釈され、Cisco Systems IGESM が不完全なブート状態になる場合があります、これに伴って **switch:** のみのプロンプトが表示されます。

端末エミュレーター・セッションが開いた状態でコンソール・ポートに接続していて、ブート処理中に端末エミュレーター・セッションに文字が入力されると、次の例のように表示される場合があります。

```
The system has been interrupted prior to initializing the
flash filesystem. The following commands will initialize
the flash filesystem, and finish loading the operating
system software:
    flash_init
    load_helper
    boot
switch:
```

このメッセージ全体が表示されなかったり、**switch:** プロンプトのみが表示されたりする場合があります。どちらの場合も、スイッチはブート処理を完了しておらず、ブート処理が完了するまではトラフィックの交換などの機能を実行しません。

スイッチがこのプロンプトで停止した場合は、**flash\_init** と入力し、フラッシュが初期化されて **switch:** プロンプトに戻るまで待ってから、**boot** と入力すればブート処理を完了できます。

スイッチはフラッシュ・イメージのロードを開始し、ブート・シーケンスを完了して、その後で完全に作動可能になります。

特定の POST 障害条件が発生した場合に、Cisco Systems IGESM がこのプロンプトで停止することがあります。このような状態では、この手順のとおり行うことによって問題が解決することも、解決しないこともあります。

## ブレード・サーバー間を切り替えるためのキー・シーケンス

BladeCenter の管理モジュールには KVM（キーボード / ビデオ / モニター）スイッチが組み込まれており、取り付けられたブレード・サーバーに従来の方法でアクセスできます。ブレード・サーバー間でキーボード、マウス、およびモニターを切り替えるには、アクティブ管理モジュールに接続したキーボードから、次に示すキー・ストロークの組み合わせを使用します。

NumLock NumLock < ブレード・サーバー番号 > Enter

ここで、<blade server number> はブレード・サーバーが取り付けられているブレード・サーバー・ベイの番号です。たとえば、ベイ 2 のブレード・サーバーを選択するには、NumLock キーを 2 回押し、数字 2 のキーを押して、Enter キーを押します。

NumLock NumLock 2 Enter

このシーケンスを使用してブレード・サーバーを選択した後、表示がブランクになることがよくあるので注意してください。通常は、カーソルを動かすとウィンドウが起動します（スクリーン・セーバー・モードから抜ける）。

## ネイティブ VLAN ミスマッチ・メッセージ

Cisco Systems IGESM 上の管理 VLAN を変更すると、Cisco Systems IGESM のコンソールに「native VLAN mismatch」というメッセージが表示されることがあります。これは、Cisco Systems IGESM 上の管理 VLAN を変更すると、ポート g0/15 と g0/16 のネイティブ VLAN も変更されるからです（これらのポートのデフォルト・ネイティブ VLAN は VLAN1）。ポート g0/15 と g0/16 は、管理モジュールを経由して BladeCenter 内にある他のすべての Cisco Systems IGESM に接続します。最初に Cisco Systems IGESM の 1 つに変更を加えた場合は、BladeCenter 内にある他の Cisco Systems IGESM の管理 VLAN（ポート g0/15 と g0/16 上）もすべて変更するまでは、ネイティブ VLAN のミスマッチが残ります。

BladeCenter に存在する Cisco Systems IGESM がただ 1 つの場合は、管理 VLAN を変更したときにこのメッセージは出されません。

**注：**正しい動作のためには、BladeCenter 内にあるすべての Cisco Systems IGESM 上で管理 VLAN が同じであることが必要です。「native VLAN mismatch」メッセージを解消するには、特定の BladeCenter 内ですべての Cisco Systems IGESM の管理 VLAN を同じ VLAN に変更します。単一の BladeCenter 内で IGESM の管理 VLAN が異なる場合の詳細と予備手段については、64 ページの 5.3.6、『考慮事項：特定の BladeCenter 内に複数の IGESM がある場合』を参照してください。

## Cisco Systems IGESM 上での RSPAN の使用

この Redpaper の制作時に行ったテストでは、IOS リリース 12.1(14)AY を使用する場合に、Cisco Systems IGESM 上で RSPAN を構成する際に問題が起きました。環境によっては、アップストリーム・スイッチとモニター対象のポートへのリンクなど、いくつかのインターフェースがワイヤー速度でデータのストリーミングを開始することがあります。その結果、少なくともモニター対象のポート上にあるデバイスへの通信が失われ、アップストリーム・スイッチ上で問題が発生します。

この RSPAN の問題は、IOS のリリース 12.1(14)AY でバグとしてトレースされました。更新バージョンである改訂 12.1(14)AY1 では、この問題は解決されています。この修正（その他の修正も合わせて）を含む最新バージョンの IOS は、次のロケーションからダウンロードできます（将来は変更される場合があります）。

<http://www.ibm.com/pc/support/site.wss/document.do?lnocid=MIGR-55479>

すでに RSPAN が構成済みで、前述したストリーミング・データの問題が生じている場合は、RSPAN に関連したモニター・セッションを削除すれば、この状態が解消します（**config term** モードで、コマンド **no monitor session xx** を実行。ただし *x* は、RSPAN 用に構成されたモニター・セッション番号）。

**重要：** 12.1(14)AY1 以降の改訂のコードを使用していない場合に Cisco Systems IGESM 上で RSPAN 機能を使用するときは、十分に注意することをお勧めします。

## IGESM からの管理モジュール設定値の検出

管理モジュールが IGESM に対してデフォルトで制御する IP アドレッシング情報のほかに、管理モジュールが IGESM 設定値を直接制御する領域があります。ほとんどの場合は管理モジュールにログインしてこれらの設定値を確認できますが、環境によっては、IGESM の管理者が管理モジュールにログインする許可を持っていないことがあります。

IGESM にログインしたユーザーが、IGESM から管理モジュールの設定値を表示する手段があります。

各 IGESM の入出力モジュール構成の拡張セクションにある 4 つの設定値のうち、IGESM との間でやり取りされるデータの管理とフローに直接影響を及ぼすものは 3 つあります。これらは 247 ページの図 9-2 に示すもので、次のように定義されます。

### ► External ports

- *Enabled*: ポート G0/17 から 20 は IGESM 上で制御できます。
- *Disabled* (デフォルト) : 管理モジュール上でこの設定値を「Enable」に変更した後に限って、IGESM 上でポート g0/17 から 20 をダウン状態にしたり起動したりすることができます。

### ► External management over all ports

- *Enabled*: IGESM 管理パスは IGESM のアップリンクを経由します。
- *Disabled* (デフォルト) : IGESM 管理パスは管理モジュールのアップリンクを経由します。

**重要:** この値を「Enabled」または「Disabled」に設定する場合は、望ましい管理パスをサポートするために、他のいくつかの規則を守る必要が生じます。詳しくは、56 ページの 5.3、『管理パスに関する詳細説明』を参照してください。

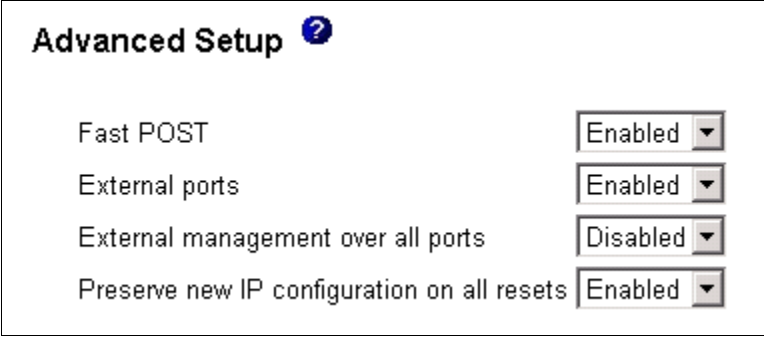
これらの規則を理解せずにこの値を変更すると、IGESM への管理接続が断続的になるか、接続が失われる可能性が高くなります。

► Preserve new IP address on all resets

- *Enabled* (デフォルト) : IP アドレス情報 (IP アドレス、マスク、およびデフォルト・ゲートウェイ) は、管理モジュールの設定によって制御されます。IGESM または管理モジュールがリブートするたびに、IGESM は管理モジュールに格納されている IP 値を取得します (IGESM の NVRAM に格納されている値でなく)。
- *Disabled*: IGESM は、IGESM のリブート時に IGESM の NVRAM に格納されている IP アドレスを取得します。

**重要:** この値を「Enabled」(デフォルト) から「Disabled」に変更すると、IGESM は自身の IP アドレッシング情報を完全に制御できなくなります。IGESM の再ロードが行われるとき (この設定値が「Disabled」の場合)、IGESM は IP アドレッシング情報を自身の NVRAM から取得します。一方、管理モジュールを再ロードすると、IGESM は管理モジュールの IGESM IP アドレッシング情報を使用して更新されます。このため、この値は「Enabled」に設定したままにすることをお勧めします。

管理モジュールの入出力モジュールに対する「Advanced Setup」の「Fast POST」オプションは、POST 中に行われる診断の詳細度のみに影響し、したがってスイッチのブート速度には影響を与えますが、IGESM 上の管理パスやデータ・パスに最終的な影響はありません。



Advanced Setup ?	
Fast POST	Enabled
External ports	Enabled
External management over all ports	Disabled
Preserve new IP configuration on all resets	Enabled

図 9-2 各 IGESM の拡張設定 (管理モジュール上の)

Cisco Systems IGESM 上で実行するコマンドとアクションによって管理モジュールの設定値を検出する方法は、次のとおりです。

- 「External ports」の設定値が「Enabled」または「Disabled」のどちらに設定されているか判別する方法

外部インターフェースの 1 つにアクセスし、IGESM 上で **no shut** を実行した場合に、「Shutdown is not allowed on this interface」というメッセージが戻されれば、管理モジュール上での設定値は「Disabled」です (図 9-3)。ポート 17 から 20 に対して **no shut** を使用できるようにするには、管理モジュールにアクセスしてこの値を「Enabled」に設定する必要があります。

- **Unable to enable external ports from switch**  
switch(config)#int g0/17  
switch(config-if)#no shut  
**% Shutdown not allowed on this interface.**
- **Must enable External ports in advanced setup in MM**
  - Default is Disabled

Advanced Setup	
Fast POST	Enabled
External ports	Disabled
External management over all ports	Disabled
Preserve new IP configuration on all resets	Enabled

図9-3 管理モジュール上の外部ポートの設定値を検出する方法

- ▶ 「External management over all ports」と「Preserve new IP configuration on all resets」の設定値を判別する方法

248 ページの図 9-4 を参照してください。sh platform summary コマンドを使用すればこれらの値が表示されます。これらの値を変更するには、管理モジュールにログオンしてそこで適切な変更を行う必要があります。

```

Switch#sh platform summary
Platform Summary:
Switch Slot: 1
Current IP Addr: 172.26.147.208, 255.255.254.0, gw: 172.26.146.1
Default IP Addr: 10.10.10.91, 255.255.255.0, gw: 0.0.0.0
IP Fields read from VPD: 172.26.147.208, 255.255.254.0, gw: 172.26.146.1
Static IP Fields in VPD: 172.26.147.208 255.255.254.0 172.26.146.1
IP Acquisition Method used: static
Active Mgmt Module in Mgmt Slot: 1
Native Vlan for Mgmt Module Ethernet ports: 1
External Mgmt over Extern ports Disabled
  
```

Switch is in Bay 1

Preserve new IP configuration on all resets: Enabled

MM advanced I/O module settings

External management over all ports: Disabled

("Disabled" will show "user-config" after IGESM reboot)

図9-4 show platform summary コマンドの出力

sh platform summary コマンドは、コマンドを実行している対象のスイッチが取り付けられているベイも表示します。これは、誤ったスイッチ名やIPアドレスが適用されている疑いがある場合や、自分がどのスイッチにログオンしているか分からない場合に便利です。

## Redhat tg3 ドライバーに関連して起こりうる問題

Redhat Linux とそのネイティブの tg3 ドライバーを使用する場合に、いくつかの問題が現場で見つかっています (tg3 ドライバーは、HS20 上の Broadcom NIC 用の Redhat 版ドライバーです)。指摘されている問題には、IGESM の再ロード後にブレード・サーバーから IGESM へのリンクが復帰しない問題 (`sh int status` コマンドを使用すると `^unotconnected^` と表示される) や、リンク・フラップ・エラーによってブレード・サーバーに接続する IGESM 上のポートがシャットダウンされる問題などがあります。

- ▶ IGESM の再ロード後にポートが復帰しない問題が発生した場合、考えられる解決策 / 次善策は次のとおりです。
  - 解決策 1: ibm.com から入手可能な Broadcom ドライバーを使用します。Broadcom から実際に提供されているドライバーは、非常に信頼性が高いことが立証されています。
  - 解決策 2: この問題が発生しない tg3 ドライバーのバージョンを入手します。該当するものは本書の執筆時点では入手できませんが、後日提供される可能性があります。
  - 次善策 1: ブレード・サーバーからポートをダウン状態にし、再起動して (この例では eth0) ポートを再び立ち上げます。

```
ifconfig eth0 down
ifconfig eth0 up
```
  - 次善策 2: この状態が発生しているブレード・サーバーを再ロードします。
- ▶ リンクのフラップによってポートがダウン状態になる問題が IGESM 上で発生している場合 (ブレード・サーバーが IGESM へのリンクを立ち上げようとするとすぐに起こる)、考えられる解決策と次善策は次のとおりです。
  - 解決策 1: ibm.com から入手可能な Broadcom ドライバーを使用します。  
Broadcom から実際に提供されているドライバーは、非常に信頼性が高いことが立証されています。
  - 次善策 1: この問題が発生しない tg3 ドライバーのバージョンを入手します。
    - この問題があることが確認されているバージョン (Linux サーバー上で `コマンド dmesg | grep tg3` を実行すると表示される) の 1 つは、tg3.c:v3.10RH (2004 年 11 月 14 日) です。
    - この問題が生じないことが確認されているバージョンの 1 つ (ただし、前述したポートがダウン状態になる問題があります) は、tg3.c:v3.6RH (2004 年 6 月 12 日) です。

機能する tg3 ドライバーをインストールした後、インターフェースを再び立ち上げるには、障害のある tg3 ドライバーによって `err-disable` 状態になった IGESM 上のインターフェースに対して、さらに `shut` および `no shut` を実行する必要があるので注意してください。

## Hyperterm からのコンソールポートアクセスに関する問題

シリアル・ケーブルと IGESM のコンソール・ポートを使用して IGESM に接続する際に、ポートから出力されるメッセージが表示されるものの、ユーザーが情報を入力できない場合があります。(Enter キーを押しても、コマンドを入力するためのコマンド・プロンプトが出されません。) この問題は、XP 環境で Hyperterm を使用する場合に最も頻繁に起こりますが、Hyperterm と W2K の環境でも少なくとも 1 回確認されました。

この問題が発生した場合は、正しい動作を確実にするために次のようにすることをお勧めします。

- ▶ Hyperterm 内でフロー制御をなしに設定する (通常は正しく動作)。



- ▶ 無料の Hyperterm の完全バージョンにアップグレードする（常に正しく動作）。
- ▶ Hyperterm 以外の端末エミュレーターを使用する（常に正しく動作）。

## デフォルトの EtherChannel ロード・バランシングが最適でない場合がある

デフォルトの EtherChannel ロード・バランス設定（ソース MAC アドレスに基づく）が原因で、場合によってはアウトバウンド・トラフィックの伝送に主に単一のアップリンクしか使用されないことが判明しています。EtherChannel バンドル内で複数のアウトバウンド・リンクが使用できる場合には、これは効率的とはいえません。12.1(14)AY4 以降では、EtherChannel ロード・バランシング用の新しいオプションを使用して、次のいずれかに基づくロード・バランスを設定できます。

- ▶ ソースまたは宛先の MAC
- ▶ ソースおよび宛先の MAC (XOR)
- ▶ ソースまたは宛先の IP (SIP/DIP と呼ばれる)
- ▶ ソースおよび宛先の IP (XOR)

ソースと宛先の MAC アドレスの XOR に基づいて EtherChannel ロード・バランスを設定する例は、次のとおりです（望ましいロード・バランシングが得られる可能性がデフォルトより高くなります）。

```
port-channel load-balance src-dst-mac
```

このグローバル・コマンドは、特定の IGESM 上ですべての EtherChannel に対してアウトバウンドのロード・バランシングを設定します。

## IGESM IP アドレス情報の制御

管理モジュールのデフォルト構成では、IGESM の IP アドレス、マスク、およびデフォルト・ゲートウェイは、管理モジュールによって制御されます。このため、この情報を IGESM 上で直接変更した場合、情報は一時的にのみ変更され、IGESM の次回リブート時、管理モジュールの次回リブート時、またはいずれかのユーザーが管理モジュールに IGESM の IP 情報を次回保管したときに、管理モジュールによって割り当てられた IP 情報に戻ります。

IGESM 上でこの情報を少なくとも部分的に制御できるようにするには、次の手順で行います。

1. 管理モジュールの「Advanced settings」で、「**Preserve new IP configuration during all resets**」を「**Disabled**」に設定し、「**Save**」をクリックします。
2. IGESM にログオンし、IP 情報を目的の情報に変更します。
3. IGESM 構成を NVRAM に保管します (**write mem**)。
4. IGESM を再ロードします。

IGESM の再ロード後、IGESM は自身の IP 情報を IGESM の再ロード時に制御できるようになりますが、これは IGESM が再ロードされる場合に限りです。管理モジュールが再ロードされた場合は、管理モジュールの IGESM IP アドレッシング情報が IGESM に再びプッシュされます。

**重要:** IGESM が自身の IP アドレッシング情報を 100% 制御できるようにする方法はないので、「Preserve new IP configuration during all resets」は「Enabled」のままにすることをお勧めします。この値を「Disabled」に設定する場合は、IGESM または管理モジュールのどちらが再ロードされた場合にも IGESM が同じ IP アドレッシング情報を入手できるように、IGESM の正しい IP アドレッシング情報を管理モジュールに常に保管しておくことを強くお勧めします。

**重要:** IGESM が自身の IP アドレス情報を管理できるようにするには、インバンド管理のために IGESM のアップリンクを使用することが前提となります。この変更の後、管理モジュールは IGESM のプロキシとして正しく機能しなくなるので、管理モジュールのアップリンクを IGESM への管理パスとして使用できなくなります。63 ページの 5.3.5、『考慮事項: IGESM アップリンクを使用した IGESM の管理』を参照してください。

## A.1 12.1(14) 以降のコードの使用

本書は、特に IOS の 12.1(14) バージョンを使用する IGESM を対象として執筆されました。次期メジャー・リリース (12.1(22)) など、将来の IOS のバージョンには、12.1(14) バージョンとは異なる機能が備わっている場合があります。相違点のいくつかは次のとおりです。

- ▶ CMS が CDM (Cisco Device Manager) に置き換えられました。
  - CMS は、IGESM 内のほとんどのオプションを構成する機能を備えています。
  - CMS は Java を必要としますが、CDM は必要としません。
  - CDM は基本的に、限定された構成機能を備えたモニター・ツールです。GUI ベースで構成を行う場合は、CiscoWorks など他のツールを使用することをお勧めします。
- ▶ 12.1(22) は次の機能をサポートします。
  - 完全な 9216 バイトのジャンボ・フレーム
  - Smartport のサポート
  - 構成可能な Auto-MDIX のサポート
  - 12.1(22) 以降の暗号イメージでの SSH V2 のサポート
  - SFP ベースの IGESM のサポート (OS-CIGESM-18-SFP)
  - ポート G0/1 から 14 上でリンク速度 / 二重モードを 1000/ 全二重にハードコーディングするためのサポート

## BladeCenter に関するその他のヒント

BladeCenter に関するその他のヒントについては、次の URL で入手できる「*IBM BladeCenter (Type 8677) and IBM BladeCenter HS20 (Type 8678) Product FAQ Hints and Tips version 2.00*」を参照してください。

<http://www.ibm.com/pc/support/site.wss/document.do?lnocid=MIGR-45277>



# 関連資料

ここに示す資料は、この **redbook** で説明しているトピックをより詳しく解説する資料として特に適切と考えられるものです。

## IBM Redbooks

これらの資料のご注文については、『IBM Redbooks を入手する方法』（256 ページ）を参照してください。ここに示す資料のいくつかは、ソフトコピー形態でのみ入手可能です。

- ▶ *Deploying Apache on IBM @server BladeCenter*, REDP-3588
- ▶ *Deploying Citrix MetaFrame on IBM @server BladeCenter*, REDP-3583
- ▶ *Deploying Lotus Domino on IBM @server BladeCenter*, REDP-3584
- ▶ *Deploying Samba on IBM @server BladeCenter*, REDP-3595
- ▶ *IBM @server BladeCenter Layer 2-7 Network Switching*, REDP-3755
- ▶ *IBM @server BladeCenter Networking Options*, REDP-3660
- ▶ *IBM @server BladeCenter Systems Management*, REDP-3582
- ▶ *IBM @server BladeCenter Systems Management with IBM Director V4.1 and Remote Deployment Manager V4.1*, REDP-3776
- ▶ *IBM Web Infrastructure Orchestration*, SG24-7003
- ▶ *The Cutting Edge: IBM @server BladeCenter*, REDP-3581

## その他の資料

次の関連資料が Cisco Systems Intelligent Gigabit Ethernet Switch Module に付属しています。

- ▶ *IBM @server BladeCenter Type 8677 Installation and User's Guide*
- ▶ *Safety Information*
- ▶ *ラック搭載手順*
- ▶ *Safety Information*
- ▶ *IBM @server BladeCenter Management Module User's Guide*
- ▶ *IBM @server BladeCenter Management Module Installation Guide*
- ▶ *IBM @server BladeCenter HS20 Installation and User's Guide*
- ▶ *Hardware Maintenance Manual and Troubleshooting Guides*
- ▶ *Cisco Systems Intelligent Gigabit Ethernet Switch Module for the IBM @server BladeCenter Installation Guide*
- ▶ *Cisco Systems Intelligent Gigabit Ethernet Switch Module for the IBM @server BladeCenter Software Configuration Guide*
- ▶ *Cisco Systems Intelligent Gigabit Ethernet Switch Module Message Guide*
- ▶ *Cisco Systems Intelligent Gigabit Ethernet Switch Module Command Reference Guide*

## オンライン・リソース

次の Web サイトも、詳しい情報源として関係のあるものです。（一部の Cisco ページには、ユーザー名とパスワードが必要です）

- ▶ Whatis.com（膨大な数の最新 IT 関連用語の定義）  
<http://whatis.techtarget.com/>
- ▶ IBM @server BladeCenter  
<http://www.ibm.com/servers/eserver/bladecenter/index.html>
- ▶ IBM @server BladeCenter サポート  
<http://www.ibm.com/servers/eserver/support/bladecenter/index.html>
- ▶ IBM @server ストレージ  
<http://www.pc.ibm.com/us/eserver/xseries/storage.html>
- ▶ IBM @server システム管理  
[http://www.ibm.com/servers/eserver/xseries/systems\\_management/xseries\\_sm.html](http://www.ibm.com/servers/eserver/xseries/systems_management/xseries_sm.html)
- ▶ IBM サポートおよびダウンロード  
<http://www.ibm.com/support/us/>
- ▶ Cisco スイッチ・クラスタリング・テクノロジー  
<http://www.cisco.com/warp/public/cc/techno/media/lan/ether/sgth/>
- ▶ Cisco スイッチ・クラスタリング・テクノロジー製品資料  
<http://www.cisco.com/warp/public/cc/techno/media/lan/ether/sgth/prodlit/index.shtml>
- ▶ Cisco Cluster Management Suite ソフトウェア  
[http://www.cisco.com/en/US/products/hw/switches/ps628/products\\_data\\_sheet09186a00800913ce.html](http://www.cisco.com/en/US/products/hw/switches/ps628/products_data_sheet09186a00800913ce.html)
- ▶ CiscoWorks LAN Management Solution  
<http://www.cisco.com/en/US/products/sw/cscowork/ps2425/index.html>
- ▶ Cisco Systems Intelligent Gigabit Ethernet Switch Module 用 CiscoView デバイス・パッケージ  
<http://www.cisco.com/cgi-bin/tablebuild.pl/cview50>
- ▶ 管理モジュール・ファームウェア更新バージョン 1.10 - IBM @server BladeCenter  
<http://www.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-54939>
- ▶ IBM @server xSeries サポート  
<http://www.ibm.com/servers/eserver/support/xseries/index.html>
- ▶ IBM パーソナル・コンピューティング・サポート  
<http://www.ibm.com/pc/support/site.wss/>
- ▶ SolarWinds ソフトウェア  
[http://www.solarwinds.net/Tools/Free\\_tools/TFTP\\_Server/](http://www.solarwinds.net/Tools/Free_tools/TFTP_Server/)
- ▶ UpdateXpress CD バージョン 3.03 - サーバー・ダウンロード  
<http://www.ibm.com/pc/support/site.wss/document.do?lndocid=MIGR-53046>
- ▶ Microsoft Windows 2000 Service Pack 3 ダウンロード  
<http://www.microsoft.com/windows2000/downloads/servicepacks/sp3/sp3lang.asp>

- ▶ BCM570x ベースのサーバーおよびアダプター用 Broadcom NetXtreme Gigabit Ethernet Software CD V7.0.5  
<http://www.ibm.com/pc/support/site.wss/document.do?lnodocid=MIGR-43815>
- ▶ Linux 用 Broadcom Advanced Server Program (BASP) ドライバー V6.2.1  
<http://www.ibm.com/pc/support/site.wss/document.do?lnodocid=MIGR-54186>
- ▶ 「Best Practices」資料に記載されているスイッチ管理インターフェースおよびネイティブ VLAN  
[http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products\\_white\\_paper09186a00801b49a4.shtml](http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products_white_paper09186a00801b49a4.shtml)
- ▶ Cisco Business Ready Data Center  
<http://www.cisco.com/go/datacenter>
- ▶ 「6500 IOS Best Practices」ガイド  
[http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products\\_white\\_paper09186a00801b49a4.shtml](http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products_white_paper09186a00801b49a4.shtml)
- ▶ スパンニング・ツリーのエレメント  
[http://www.cisco.com/en/US/customer/tech/tk389/tk621/tech\\_tech\\_notes\\_list.html](http://www.cisco.com/en/US/customer/tech/tk389/tk621/tech_tech_notes_list.html)
- ▶ Cisco Connection Online への登録  
<http://tools.cisco.com/RPF/register/register.do>
- ▶ SPAN および RSPAN の構成  
[http://www.cisco.com/en/US/products/hw/switches/ps628/products\\_configuration\\_guide\\_chapter09186a00801a6ba9.html](http://www.cisco.com/en/US/products/hw/switches/ps628/products_configuration_guide_chapter09186a00801a6ba9.html)  
[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_configuration\\_guide\\_chapter09186a008007f323.html](http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008007f323.html)
- ▶ TAC メイン・サポート・ページ  
<http://www.cisco.com/en/US/partner/support/index.html>
- ▶ TAC サービス要求ツール  
[http://www.cisco.com/cgi-bin/front.x/case\\_tools/case0open.pl](http://www.cisco.com/cgi-bin/front.x/case_tools/case0open.pl)
- ▶ SVO サブミット  
[http://www.cisco.com/cgi-bin/front.x/agents/svo\\_tools/SV0ToolDispatcher](http://www.cisco.com/cgi-bin/front.x/agents/svo_tools/SV0ToolDispatcher)
- ▶ Cisco CCO – オンライン資料  
<http://www.cisco.com/univercd/home/home.htm>
- ▶ Cisco TAC - Catalyst スイッチのベスト・プラクティス  
[http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products\\_white\\_paper09186a00801b49a4.shtml](http://www.cisco.com/en/US/partner/products/hw/switches/ps700/products_white_paper09186a00801b49a4.shtml)
- ▶ IBM @server BladeCenter スイッチ・モジュール  
[http://www.ibm.com/servers/eserver/bladecenter/switch/more\\_info.html](http://www.ibm.com/servers/eserver/bladecenter/switch/more_info.html)
- ▶ Cisco Systems IGESM を対象とした IBM/Cisco Design Guide  
<http://www.ibm.com/services/alliances/cisco/files/cisco-igesm-design-guide.pdf>
- ▶ IBM Serial Over LAN Setup Guide  
<http://www.ibm.com/support/docview.wss?uid=psg1MIGR-54666>
- ▶ IBM/Cisco Systems IGESM Software Configuration Guide

- <http://www.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-55261>
- ▶ IBM/Cisco Systems IGESM Command Reference  
<http://www.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-55260>
- ▶ IBM/Cisco Systems IGESM Message Guide (すべてのエラー・メッセージ)  
<http://www.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-55259>
- ▶ VLAN セキュリティーのベスト・プラクティス  
[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_white\\_paper09186a008013159f.shtml](http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml)
- ▶ IBM/Cisco Systems IGESM IOS コードのダウンロード  
<http://www.ibm.com/pc/support/site.wss/document.do?Indocid=MIGR-58132>
- ▶ Cisco Systems IGESM バージョン 10 以上をサポートする CiscoWorks IDU  
CiscoWorks をサポートする Cisco Systems IGESM の最低コードは 12.1(14)AY1 です。  
<http://www.cisco.com/kobayashi/sw-center/cw2000/lan-planner.shtml>  
各モジュールの「Application-Level Updates」の下にあります。
- ▶ Ethereal (オープン・ソースのネットワーク・スニффイング・ツール)  
<http://www.ethereal.com/>

## IBM Redbooks を入手する方法 (英語版のみ)

次の Web サイトでは、Redbook、Redpaper、ヒント、ドラフト資料、追加資料などを、検索、表示、またはダウンロードできます。

[ibm.com/redbooks](http://ibm.com/redbooks)

## IBM が提供するヘルプ

IBM サポートおよびダウンロード

[ibm.com/support](http://ibm.com/support)

IBM グローバル・サービス

[ibm.com/services](http://ibm.com/services)

# 省略語および頭字語

<b>802.3</b>	10BASE-T イーサネット	<b>IEEE</b>	米国電気電子学会 (Institute of Electrical and Electronics Engineers)
<b>802.3ad</b>	リンク・アグリゲーション	<b>IGESM</b>	Intelligent Gigabit Ethernet Switch Module
<b>802.1D</b>	スパンニング・ツリー・プロトコル (Spanning Tree Protocol)	<b>IGMP</b>	Internet Group Management Protocol
<b>802.1p</b>	サービス・クラス (CoS)	<b>IMB2</b>	Inter Module Buses
<b>802.1Q</b>	トランキンク・プロトコル	<b>IOS</b>	Cisco Internetworking Operating System
<b>802.1s</b>	多重スパンニング・ツリー・プロトコル	<b>IP</b>	インターネット・プロトコル (Internet Protocol)
<b>802.1w</b>	高速再構成スパンニング・ツリー	<b>IP DSCP</b>	IP Differentiated Services Code Point
<b>ARP</b>	アドレス解決プロトコル (Address Resolution Protocol)	<b>ISL</b>	Cisco Inter-Switch Link
<b>BACS</b>	Broadcom Advance Control Suite	<b>ISO</b>	国際標準化機構 (International Organization of Standardization)
<b>BASP</b>	Broadcom Advanced Server Program	<b>ITSO</b>	International Technical Support Organization
<b>BPDU</b>	ブリッジ・プロトコル・データ・ユニット (Bridge Protocol Data Unit)	<b>LACP</b>	Link Aggregation Control Protocol
<b>CDP</b>	Cisco Discovery Protocol	<b>LPC</b>	Low Pin Count
<b>Cisco Systems</b>	Cisco Systems Intelligent Gigabit Ethernet Switch Module	<b>MST</b>	複数インスタンス STP (Multiple Instance STP)
<b>IGESM</b>		<b>MVR</b>	Multicast VLAN registration
<b>CIOB-X2</b>	Champion I/O Bridge	<b>NAS</b>	Network Attached Storage
<b>CLI</b>	コマンドラインインターフェイス (Command-Line Interface)	<b>NIC</b>	イーサネット・ネットワーク・インターフェース・コントローラー (Ethernet Network Interfaces Controllers)
<b>CMIC</b>	Champion Memory and I/O Controller	<b>NTP</b>	Network Time Protocol
<b>CMS</b>	Cluster Management Suite	<b>PagP</b>	Port Aggregation Protocol
<b>CoS</b>	クラス・オブ・サービス (Class of Service)	<b>POST</b>	パワーオン・セルフテスト (Power-On Self-Test)
<b>CSB5</b>	Champion South Bridge	<b>PVST+</b>	Per-VLAN Spanning Tree
<b>CSM</b>	Content Switching Module	<b>PXE</b>	Preboot Execution Environment
<b>DHCP</b>	動的ホスト構成プロトコル (Dynamic Host Configuration Protocol)	<b>QoS</b>	クオリティ・オブ・サービス (Quality of Service)
<b>DOS</b>	ディスク・オペレーティング・システム (Disk Operating System)	<b>RDM</b>	Remote Deployment Manager
<b>DTP</b>	Dynamic Trunking Protocol	<b>RMON</b>	Remote Monitoring
<b>EI</b>	Enhanced Image	<b>RPM</b>	RPM Package Manager
<b>ESM</b>	Ethernet Switch Module	<b>RSPAN</b>	Remote Switch Port Analyzer
<b>ESS</b>	Enterprise Storage Server	<b>RSTP</b>	高速 STP (Rapid STP)
<b>GbE</b>	ギガビット・イーサネット (Gigabit/sec Ethernet)	<b>SAN</b>	Storage Area Networks
<b>HA</b>	高可用性 (High Availability)	<b>SIO</b>	SuperI/O
<b>HSRP</b>	Hot Standby Router Protocol	<b>SLP</b>	Service Location Protocol
<b>IC</b>	Inter-IC: 双方向 2 線シリアル・バス	<b>SMP</b>	対称型マルチプロセッシング (Symmetric Multiprocessing)
<b>IBM</b>	International Business Machines Corporation		
<b>IHS</b>	IBM HTTP Server		



<b>SNMP</b>	Simple Network Management Protocol
<b>SPAN</b>	Switch Port Analyzer
<b>SSH</b>	セキュア・シェル (Secure Shell)
<b>STP</b>	スパンニング・ツリー・プロトコル (Spanning Tree Protocol)
<b>TACACS+</b>	Terminal Access Controller Access Control System Plus
<b>TFTP</b>	Trivial File Transfer Protocol
<b>UDLD</b>	UniDirectional Link Detection
<b>URL</b>	Uniform Resource Locator
<b>USB</b>	ユニバーサル・シリアル・バス (Universal Serial Bus)
<b>UTP</b>	対より線 (シールドなし) (Unshielded Twisted Pair)
<b>VLAN</b>	仮想ローカル・エリア・ネットワー ク (Virtual Local Area Network)
<b>VMPS</b>	VLAN Membership Policy Server
<b>VTP</b>	VLAN Trunking Protocol

# 索引

## 数字

100 オーム STP 17  
1000BASE-T 14, 17  
100BASE-TX 17  
10BASE-T 17  
1800 ワット・パワー・サブライ 111  
64 ビット・コンピューティング 4  
6500 110, 111, 112, 113, 114, 132  
6509 111  
802.1D 1, 14  
802.1Q 2, 15, 122, 151  
802.1Q トランク 122, 129, 146  
802.1s 2, 15  
802.1w 1, 15  
802.1X 16  
802.3x 14  
8677 110  
8832 90, 94, 97, 98, 102, 110

## A

ACL 32  
「Administration」メニュー 31  
ANSI インターフェース 10  
Application Workload Manager 5  
ATI Rage XL ビデオ・コントローラー 9  
Availability Manager 55  
AVVID ウィザード 32

## B

BackboneFast 1  
BCM570x ベースのサーバー 97, 102  
BladeCenter HS20 7, 8, 93  
BladeCenter アライアンス・パートナー 13  
BladeCenter 管理モジュール 92  
BladeCenter シャーシ 1, 4, 6, 12, 55, 110  
BladeCenter 管理モジュール 111  
BMC 56  
Broadcom Advance Control Suite (BACS) 243  
Broadcom Advanced Server Program (BASP) 100, 102, 138, 142, 151, 159, 165  
Broadcom Ethernet NIC 97  
Broadcom NetXtreme Gigabit Ethernet 97, 98  
Broadcom NetXtreme Gigabit Ethernet ソフトウェア CD 97  
Broadcom チーミング 146  
Broadcom チーミング・ソフトウェア 129

## C

CA Unicenter 56  
Campus Manager 55  
CatOS 121  
CCO 54  
CEF720 111  
CEF720 4 ポート 10 Gigabit Ethernet 111  
Centralized Forwarding Card (CFC) 111  
Champion I/O Bridge (CIOB-X2) 9  
Champion Memory and I/O Controller (CMIC) 9  
Champion South Bridge (CSB5) 9  
Change Audit 54

Cisco Catalyst 6509 111  
Cisco Connection Online (CCO) 54, 237  
Cisco Discovery Protocol (CDP) 1, 13, 257  
Cisco EtherChannel 1  
Cisco Internetworking Operating System (IOS) 13, 257, 123  
Cisco IP 電話 15  
Cisco Management Connection 55  
Cisco Systems IGESM 1, 19, 20, 21, 108, 111, 113, 126  
Cisco Systems Intelligent Gigabit Ethernet Switch Module 1, 3, 12, 19, 83, 88, 103, 111  
Cisco Systems Intelligent Gigabit Ethernet Switch Module ホーム 29  
Cisco Systems Internet Operating System (IOS) 104  
Cisco スイッチ・クラスターリング・テクノロジー 45  
Cisco データ・センター・ネットワーク・アーキテクチャー 2  
Cisco ネットワーク 113  
Cisco プロプラエタリー 1, 16  
CiscoView 54  
CiscoWorks 1  
CiscoWorks Campus Manager 54  
CiscoWorks LAN Management Solution (LMS) 53, 54  
CiscoWorks Resource Manager Essentials 54  
CLI 13, 15, 19, 24, 25, 27, 103, 111, 151  
CLI コマンド 25, 39  
CLI コマンドのモード 26  
CLI ベースのセッション 13  
Cluster Management Suite  
CMS を参照  
Cluster Management Suite GUI 24  
「Cluster」メニュー 32  
CMS 13, 15, 24, 29, 30, 45, 103, 151  
CMS のフロント・パネル・ビュー 30, 34  
CMS メニュー 31

## D

DDR-SDRAM メモリー・チャンネル 9  
Device Configuration Manager 54  
「Device」メニュー 32  
DHCP 55  
Director コンソール 55  
Domino 4  
DOS 始動可能 (ブート可能) CD 93  
Dynamic Trunking Protocol (DTP) 1, 15, 257

## E

EEPROM 9  
EIA/TIA-568 17  
EIA/TIA-568B 17  
Electronic Service Agent 5  
Enhanced Image (EI) 104  
Enterprise Storage Server (ESS) 5  
ERP 4  
EtherChannel 32, 123, 146, 185  
EtherChannel リンク 12, 14  
EtherLAN インターフェース 7  
Ethernet Switch Module 10  
EXEC コマンド 39

## F

Fast EtherChannel 14  
「Firmware VPD」 ウィンドウ 89

## G

GbE インターフェース 12  
Gigabit EtherChannel 14  
Gigabit Ethernet 拡張カード 87  
Gigabit Ethernet スイッチング 13  
Gigabit Ethernet パス 7  
GVRP 1

## H

H8S2148 IBM 統合システム管理プロセッサ 9  
Hot Standby Router Protocol (HSRP) 257, 113  
HP OpenView 56  
HS20 4, 87, 93, 94, 110  
HS20 アーキテクチャー 9  
HS40 4  
HTTP Web インターフェース 85  
HTTP ポート 31

## I

I2C 10  
I2C パス 9, 40  
IBM Director 5, 25, 55, 56, 85  
IBM TotalStorage 5  
IBM UpdateXpress 93  
IBM オンデマンド稼働環境 2  
IBM 統合システム管理プロセッサ 9  
IDE チャンネル 9  
IEEE 802.1d スパニング・ツリー・プロトコル 17  
IEEE 802.1D スパニング・ツリー・プロトコル (STP) 14  
IEEE 802.1p CoS スケジューリング 16  
IEEE 802.1p サービス・クラス (CoS) 16  
IEEE 802.1P タグ付きパケット 17  
IEEE 802.1Q 12  
IEEE 802.1Q タグ付き VLAN 17  
IEEE 802.1Q トランッキング・プロトコル 15  
IEEE 802.1s 多重 STP (MSTP) 15  
IEEE 802.1w 高速 STP (RSTP) 15, 257  
IEEE 802.2 論理リンク制御 17  
IEEE 802.3 10BASE-T イーサネット 17  
IEEE 802.3u 100BASE-TX ファースト・イーサネット 17  
IEEE 802.3x 全二重フロー制御 17  
IGMP スヌープ 12, 32  
IGMP フィルタリング 14  
IntelliStation 5  
Inter Module Buses (IMB2) 9  
Internet Group Management Protocol (IGMP) 12, 14  
Inventory Manager 54  
IOS 13, 121, 123  
IP Differentiated Services Code Point (IP DSCP) 16  
ipconfig コマンド 143, 167  
ISL 1

## J

Java 1.4 プラグイン 30, 92  
Java 2 V1.4 10  
Java アプレット 10  
JS20 4

## L

L2 スイッチング 1  
L3 インターフェース 113  
LACP チャンネル 123  
Link Aggregation Control Protocol (LACP) 14, 123  
Low Pin Count (LPC) 9

## M

MAC アドレス 17  
MAC ベースのポート・レベル・セキュリティ 16  
Microsoft 56  
    Exchange 4  
    Internet Explorer 24  
    Windows 2000 97  
MSFC3 ドーターボード 111  
MSTP 15  
Multicast VLAN registration (MVR) 14

## N

NetIQ 56  
Netscape Communicator 24  
NetVista 5  
Network Attached Storage (NAS) 5  
Network Time Protocol (NTP) 13, 257  
NIC 87  
NIC チーミング 100, 243  
NVRAM 126

## P

PCI パス 9  
Per-VLAN Spanning Tree (PVST) 1, 15  
ping およびトレース 34  
ping ダイアログ 39  
Policy Feature Card 3 111  
Port Aggregation Protocol (PAgP) 1, 14, 257, 123  
「Port」メニュー 32  
POST 88  
POST/BIOS コード 9  
Preboot Execution Environment (PXE) 55  
PXE 55

## Q

Quality of Service (QoS) 16, 32, 104

## R

RADIUS 1  
Rapid PVST+ 15  
Rapid-PVST 124  
RDM 55  
Real-Time Diagnostics 5  
Red Hat Linux AS 2.1 98  
Redbooks Web サイト 256  
    Contact us xii  
Remote Deployment Manager (RDM) 5, 55  
Remote Switch Port Analyzer (RSPAN) 17, 170, 172  
「Reports」メニュー 33  
Resource Manager Essentials 54  
RSPAN 186  
RSPAN リフレクター・ポート 171

## S

Scalable Systems Manager 5

SERDES G ビット・イーサネット・インターフェース 8  
SERDES ベースの Gb イーサネット・インターフェース 7  
Server Load Balancing (SLB) 146, 147, 159, 173  
Server Plus Pack 5  
ServerGuide 5  
ServerWorks Grand Champion LE 9  
Service Location Protocol (SLP) 55  
show interfaces 39  
Simple Network Management Protocol (SNMP) 14  
SIO (SuperI/O) 9  
SLB チューニング 112  
SLP 55  
SMP 4  
SNMP 31  
SNMP ベースの管理ツール 1  
Software Distribution Premium Edition 5  
Software Image Manager 55  
SolarWinds TFTP 90  
SPAN 32, 186  
SSH 25  
Storage Area Network (SAN) 5  
STP 32, 126  
STP ループ 1  
SuperI/O (SIO) 9  
Supervisor Engine 720 111  
Switch Port Analyzer (SPAN) 17  
Switch Tasks 10  
switchport 105  
Syslog Analyzer 55  
SYSLOG 機能 17

## T

TACACS+ 1  
Tape Drive Management Assistant 5  
Telnet 12, 13, 24, 25, 39, 90, 92  
Telnet クライアント 10  
Telnet セッション 39, 92  
Terminal Access Controller Access Control System Plus (TACACS+) 16  
TFTP 90  
TFTP サーバー 90  
thin IMB バス 9  
ThinkPad 5  
Tivoli 2, 56  
「Tools」メニュー 34  
traceroute 17  
Trivial File Transfer Protocol (TFTP) 13

## U

UniDirectional Link Detection (UDLD) 1, 14  
UpdateXpress 94, 97  
UpdateXpress CD 93  
UplinkFast 1  
USB バス 9  
UTP 85  
UTP カテゴリー 3 17  
UTP カテゴリー 5 17  
UTP カテゴリー 5e 17  
UTP カテゴリー 6 17

## V

「View」メニュー 34  
VLAN 15, 106, 108, 112  
VLAN Management Policy Server (VMPS) 1, 15  
VLAN Trunking Protocol (VTP) 1, 15

VLAN インターフェース 106  
VLAN タグ付け 100  
VLAN トランッキング 1, 122  
VLAN 割り当て 16  
「VLAN」メニュー 33  
VMPS 33  
VTP ドメイン・ネーム 115  
VTP 透過モード 115

## W

Web サーバー 4  
Web ブラウザー 25  
Windows NT 4.0 97  
Windows Server 2000 97  
Windows Server 2003 97  
「Window」メニュー 34

## X

XENPAK 111  
Xeon 9  
XpandonDemand 3  
xSeries 5

## あ

アウト・オブ・バンド管理 40, 69, 87  
アクセス制御リスト (ACL) 16  
アクティブ・アクティブ 147, 173  
アクティブ・パッシブ 147, 173  
アグリゲーション 122  
アップストリーム・スイッチ 19  
アップストリーム接続 129, 172  
アドレス解決プロトコル (ARP) 31, 109  
アプリケーション管理 41  
アプリケーション・サーバー 4  
アプリケーション・サービス提供 4  
アラーム 17  
暗号ソフトウェア・イメージ 13

## い

イーサネット・インターフェース 6, 7, 40  
イーサネット・スイッチング・テクノロジー 11  
イーサネット・ネットワーク・インターフェース・コントローラー 87  
イーサネット・ポート 85  
イーサネット・モジュール 10  
イベント 17  
イベント通知 31  
色分け 54  
印刷 30  
インターネットワーキング製品 54  
インバンド管理 13, 41, 87  
インベントリ 33

## え

エキスパート 31  
エンタープライズ・アプリケーション 4  
エンド・ステーション 14

## お

音声 VLAN 15, 16, 33  
音声トラフィック 15

## か

ガイド 30

ガイド・モード 24

外部インターフェース 85

外部スイッチ・ポート 92

外部銅線 GbE インターフェース 12

外部ネットワーク・インターフェース (eth0) 86, 90

外部ポート 10, 22, 88, 89

拡張 ping 39

拡張暗号ソフトウェア・イメージ 25

拡張スイッチ・モジュール 8

加重ラウンドロビン (WRR) 16

仮想ローカル・エリア・ネットワーク

VLAN を参照

カテゴリ 3、4、5 ケーブル接続 85

管理 VLAN 33, 41, 87, 106, 108, 109, 144, 168

管理アプリケーション 54

管理サブネット 84

管理モジュール 6, 12, 21, 22, 41, 84, 87, 89, 102, 106, 109

管理モジュール Web インターフェース 55, 85, 92, 94

管理モジュール Web ブラウザー 25

管理モジュールのデフォルト 86

管理モジュールのファームウェア 84

## き

ギガビット/秒イーサネット (GbE) 2

許可エラー 17

## く

クラスター 31

クロスケーブル 85, 121

## け

ゲートウェイ 113

ゲートウェイ・アドレス 87

ゲスト VLAN 16

## こ

高可用性 110, 113, 123, 129, 146, 170

高速 POST 88

高速 STP (RSTP) 15, 257

高速再構成スパンニング・ツリー 1

コマンド 28

コマンド行インターフェース

CLI を参照

コラボレーション 3

コンソール通信速度 31

## さ

サーバー統合 3

サービス・クラス (CoS) 16

最適でないデータ・フロー 112

サブネット 87, 90

## し

システム再ロード 31

システム時刻 31

システム・メッセージ 33

実動ネットワーク 113

自動検知 14

自動ネゴシエーション 14, 122

出荷時のデフォルト値 89

新規 IP 構成の保持 89

診断 12, 29

診断ログ 39

## す

スイッチ ASIC 22

スイッチ状況 16

スイッチの出荷時のデフォルト値 89

スイッチのモニター 39

スイッチ・ソフトウェア 90

スイッチ・モジュール 6, 12

スイッチ・モジュールのコンソール・ポート 24

スイッチ・モジュールのファームウェア 89

スケールアウト 3

ストレージ 4

ストレージ・ソリューション 5

ストレート・ケーブル 121

スパンニング・ツリー 14, 15, 106, 108, 109, 112, 123, 126

スパンニング・ツリー・ストーム 15

スパンニング・ツリー・ブロック状態 129

スパンニング・ツリー・プロトコル (STP) 14

スパンニング・ツリー・ループ 15

すべてのポート上での外部管理 89

## せ

セキュア・シェル (SSH) 13, 24

セキュリティー・ウィザード 32

専用 VLAN エッジ・ポート 14

## そ

ソフトウェア管理ツール 55

ソフトウェア・アップグレード 31

## た

帯域幅 12, 14

帯域幅グラフ 33, 35

タイムアウト・イベント 17

対より線 (シールドなし) (UTP) 85

多重 STP (MSTP) 15

多重スパンニング・ツリー 2

単一モジュール 123

端末エミュレーション 24

## ち

チップ・キャッシュ 22

重複 IP アドレス 241

## つ

ツールバー・ボタン 30

## て

データベース・アプリケーション 4

データ・センター 103

## と

統計 17

動的 VLAN メンバーシップ 15

動的アドレス学習 14

動的ホスト構成プロトコル (DHCP) 55

ドーターカード 7, 8

トラフィック分析 17

トラブルシューティング 28

トランキング 122  
トランク 106, 122

## な

内部ネットワーク・インターフェース 10, 86

## に

入出力バス 9  
入出力モジュール 89

## ね

ネイティブ VLAN 112, 122  
ネットワーク管理 41  
ネットワーク・インターフェース・カード (NIC) チーミング 100  
ネットワーク・インターフェース・コントローラー (NIC) 87  
ネットワーク・セキュリティ 15  
ネットワーク・モニター 17

## は

ハードウェア・アラート 55  
ハードウェア・ヘルス 55  
ハイブリッド・モード 121  
バックボーン 14  
発信キュー 16  
発信ポリシングおよびスケジューリング 16  
凡例 35

## ひ

ヒストリー 17

## ふ

ファイバー・チャネル 5, 8  
ファイバー・チャネル・ドーターカード 8  
ファイルおよび印刷 3, 4  
フォールト・トレランス 14  
フラッシュ・メモリー 13  
フラッシュ制御 32  
ブリッジ・プロトコル・データ単位 (BPDU) 15  
ブレード 19  
ブレードの挿入 55  
ブレード・サーバー 4, 6, 14, 19, 20, 22, 40, 55, 93, 102, 112  
    ポート 106  
    構成 103  
フレーム・サイズ 14  
ブロードキャスト・ストーム 14  
ブロードキャスト・トラフィック 15  
フロー・ベースのパケット分類 16  
フロント・パネル 34

## へ

ヘルプ  
    コマンド 27  
    メニュー 35  
    リソース 40  
編集コマンド 27

## ほ

ポート検索 32  
ポート設定 32  
ポート統計 33

ポートのポップアップ・メニュー 30  
ポート・スイッチ 16  
ポート・セキュリティ 16, 32  
ポート・セキュリティ・エーijing 15  
ポート・セキュリティ・オプション 15  
保護ポート 32  
ホスト名 32, 35  
ホット・スタンバイ 147, 173  
ホット・プラグ可能モジュール 104

## ま

マルチキャスト 33  
マルチキャスト・トラフィック 15  
マルチホーム・サーバー 240  
マルチレベル・セキュリティ 15

## み

ミッドプレーン 6, 7, 12

## め

メディア・アクセス制御 (MAC) 12  
メニュー・バー 30

## も

モジュラー設計 3  
モニター 54  
モニター・ツール 29

## り

リソースの問題 17  
リソース・モニター 33  
リモート・モニター (RMON) 17, 172  
リンク・アグリゲーション 12, 122, 123  
リンク・アグリゲーション・グループ 122  
リンク・グラフ 33  
リンク・レポート 33

## る

ルート・ブリッジ 112

## れ

レイヤー 2 1, 12, 13, 19  
レイヤー 2 traceroute 17  
レイヤー 2 スイッチ 104  
レイヤー 2 ツール 55  
レイヤー 2 ネットワーク 108, 112, 126, 129









# Cisco Systems Intelligent Gigabit Ethernet Switch Module for IBM *@*server BladeCenter

銅線イーサネット・スイッチング・テクノロジーを BladeCenter シャーシに統合

役に立つ構成およびトラブルシューティングの技法

CMS および CLI を使用した構成例

この IBM Redpaper では、Cisco Systems Intelligent Gigabit Ethernet Switch Module for the IBM *@*server BladeCenter の位置付けを示し、お客様の既存データ・ネットワークへのシームレスなインターフェースを提供するこの製品が、BladeCenter の提案する価値をどのように高めるかについて説明します。

本書では、数種類のネットワーク・トポロジを対象に、Cisco Systems Intelligent Gigabit Ethernet Switch Module の計画、インストール、および構成に役立つ情報を示します。トポロジーの例を示して、スイッチ・モジュールをさまざまなネットワークに統合するための方法をいくつか解説しています。

また、Cisco Systems Intelligent Gigabit Ethernet Switch Module および BladeCenter のアーキテクチャー、および既存の Cisco データ・センターで完全な相互運用性を実現するこれら両製品のテクノロジーの連携についても説明します。

本書の対象読者としては、既存のネットワークに Cisco Systems Intelligent Gigabit Ethernet Switch Module を正しく統合するために本書を使用する、経験を積んだシステム管理者とネットワーク管理者を想定しています。

## INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

### 実際の経験に基づく技術情報の構築

IBM Redbook は IBM International Technical Support Organization (ITSO) によって作成されます。世界中の IBM、お客様およびパートナーの専門家が、現実的なシナリオに基づいてタイムリーな技術情報を作成します。推奨事項を特定して、お客様の環境に IT ソリューションを効率よくインプリメントできるようにします。

詳細は次のサイトを参照してください。  
[ibm.com/redbooks](http://ibm.com/redbooks)

SG88-8547-00

