Sun Fire™ B1600
ブレードシステムシャーシ
ソフトウェア設定マニュアル

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No. 817-1888-10
2003 年 4 月, Revision A

コメントの宛先: docfeedback@sun.com

原典: *Sun Fire B1600 Blade System Chassis Software Setup Guide*
Part No: 816-3361-11
Revision A

目次

はじめに

このマニュアルでは、Sun Fire B1600 ブレードシステムシャーシのコンポーネントのソフトウェアを設定して、システムシャーシをネットワークに組み込む方法について説明します。

このマニュアルは、経験のある Solaris システム管理者を対象とします。

お読みになる前に

このマニュアルで説明する作業を行う前に、ブレードシステムシャーシをラックに取り付けて、必要なケーブルをすべて接続しておいてください。システムハードウェアの設置方法については、『Sun Fire B1600 ブレードシステムシャーシハードウェア設置マニュアル』を参照してください。

このマニュアルの構成

第 1 章では、Sun Fire B1600 ブレードシステムシャーシのソフトウェアの概要を示し、第 2 章以降の手順を実行する前に行う必要のある作業について説明します。

第 2 章では、システムシャーシの準備設定作業の手順について説明します。

第 3 章では、データ用と管理用のネットワークを分離していない単純なネットワーク環境にシステムシャーシを接続する場合の、システムシャーシの簡易な設定方法について説明します。

第 4 章では、サーバーブレードの電源投入およびコンソールへのアクセス、予備診断の実行方法について説明します。

第 5 章では、データと管理のトラフィックを分離しているネットワーク環境にシステムシャーシを接続する方法について説明します。

第 6 章では、管理ネットワークから直接かつ安全にブレードを管理できるように設定して、第 5 章のシステムシャーシ設定を改良する方法について説明します。

第 7 章は、ISP (インターネットサービスプロバイダ) を対象とします。この章では、サーバーブレードを異なるユーザー (サーバーブレードのテナント) に割り当て、テナント自身がほかのユーザーのブレードにアクセスすることなく各自のブレードを管理できるように設定する方法について説明します。

付録 A では、ほかの章の手順を実行する際に必要となる、スイッチでの作業方法について説明します。

付録 B では、ラップトップコンピュータからシステムシャーシのコマンド行インタフェースに接続する方法について説明します。

付録 C は、『Solaris のインストール (上級編)』および『Solaris DHCP の管理』の説明を補足します。この付録の手順を実行すると、システムシャーシのサーバーブレードが IP アドレスを動的に受け取るように、データネットワーク上の DHCP サーバーを設定できます。

付録 D では、Web Start でフラッシュアーカイブを使用して、あるサーバーブレードのオペレーティング環境およびアプリケーションソフトウェアをほかのサーバーブレードに複製する方法について説明します。

付録 E では、システムコントローラの sc> プロンプトから実行できるコマンドの一覧を示します。

付録 F では、アクティブシステムコントローラとスタンバイシステムコントローラの関係について説明します。

お読みになったあとで

このマニュアルを読んだあとは、必要に応じて、ブレードシステムシャーシに関する次の 2 冊のマニュアルを参照してください。

- シャーシのシステムコントローラのコマンド行インタフェースの使用方法については、『Sun Fire B1600 ブレードシステムシャーシ管理マニュアル』を参照してください。
- シャーシの統合スイッチの管理方法については、『Sun Fire B1600 ブレードシステムシャーシスイッチ管理マニュアル』を参照してください。このマニュアルでは、統合スイッチのハードウェアおよびアーキテクチャーについて説明しています (第 1 章)。また、スイッチの初期設定方法 (第 2 章) および Web グラフィカルユーザーインタフェースや SNMP を使用したスイッチの管理方法 (第 3 章)、コマンド行インタフェースからスイッチを管理するためのすべてのコマンドの使用方法 (第 4 章) について説明しています。

UNIX コマンド

このマニュアルには、UNIX® の基本的なコマンド、およびシステムの停止、システムの起動、デバイスの構成などの基本的な手順の説明は記載されていません。

基本的なコマンドや手順についての説明は、次のマニュアルを参照してください。

- 『Sun 周辺機器 使用の手引き』
- Solaris™ オペレーティング環境についてのオンライン AnswerBook2™

書体と記号について

書体または記号	意味	例
AaBbCc123	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例。	.login ファイルを編集します。 ls -a を実行します。 % You have mail.
AaBbCc123	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して表します。	**マシン名% su** Password:
AaBbCc123 または**ゴシック**	コマンド行の可変部分。実際の名前や値と置き換えてください。	rm *filename* と入力します。 rm **ファイル名** と入力します。
『 』	参照する書名を示します。	『Solaris ユーザーマニュアル』
「 」	参照する章、節、または、強調する語を示します。	第 6 章「データの管理」を参照。 この操作ができるのは「スーパーユーザー」だけです。
\	枠で囲まれたコード例で、テキストがページ行幅をこえる場合に、継続を示します。	% **grep '^#define \ XV_VERSION_STRING'**

シェルプロンプトについて

シェル	プロンプト
UNIX の C シェル	**マシン名**%
UNIX の Bourne シェルと Korn シェル	$
スーパーユーザー (シェルの種類を問わない)	#
システムコントローラシェル	sc>
統合スイッチシェル	Console#

関連マニュアル

用途	マニュアル名	Part No.
安全に関する注意事項	『Sun Fire B1600 Blade System Chassis Compliance and Safety Manual』(マルチリンガル版)	816-3364
設置の概要(折り込みポスター)	『Sun Fire B1600 Blade System Chassis Quick Start Guide』(英語版)	816-3625
ハードウェアの設置	『Sun Fire B1600 ブレードシステムシャーシハードウェア設置マニュアル』	817-1904
ソフトウェアの設定	『Sun Fire B1600 ブレードシステムシャーシソフトウェア設定マニュアル』(このマニュアル)	817-1888
システムシャーシの管理およびコンポーネントの交換	『Sun Fire B1600 ブレードシステムシャーシ管理マニュアル』	817-1898
スイッチの管理	『Sun Fire B1600 ブレードシステムシャーシスイッチ管理マニュアル』	817-1893
最新情報	『Sun Fire B1600 Blade System Chassis Product Notes』(英語版)	816-4174

Sun のオンラインマニュアル

各言語対応版を含むサンの各種マニュアルは、次の URL から表示または印刷、購入できます。

`http://www.sun.com/documentation`

コメントをお寄せください

弊社では、マニュアルの改善に努力しており、お客様からのコメントおよびご忠告をお受けしております。コメントは下記宛に電子メールでお送りください。

docfeedback@sun.com

電子メールの表題にはマニュアルの Part No. (817-1888-10) を記載してください。

なお、現在日本語によるコメントには対応できませんので、英語で記述してください。

第1章

システムシャーシの設定の準備

この章では、システムシャーシの設定手順の概要について説明します。また、システムシャーシの特徴と、システムコントローラおよびスイッチの役割について説明します。この章の後半 (最後の節を除く) では、システムシャーシを設定する前に行う必要のある作業について説明します。最後の節では、#. エスケープシーケンスを使用して、ユーザーインタフェースを切り替える方法について説明します。

この章は次の節で構成されています。

1.1 ソフトウェア設定手順の概要

この節では、システムシャーシの設定手順の概要について説明します。

注 – システムシャーシを設定するには、システムコントローラのコマンド行インタフェースを使用する必要があります。このインタフェースを使用して、2 つのスイッチおよびサーバーブレードのコンソールにアクセスします。スイッチまたはブレードのコンソールでは、#. を入力すると、アクティブシステムコントローラの sc> プロンプトに戻ります。

---

1. **サーバーブレードにオペレーティング環境をインストールするために、ネットワークインストールサーバーを作成します。**

   サーバーブレードにオペレーティング環境をインストールするには、ネットワークインストールサーバーからブレードを起動する必要があります。そのため、シャーシのソフトウェア設定を開始する前に、『Solaris のインストール (上級編)』に記載されているネットワークインストールサーバーの作成手順を実行します。このマニュアルは、Solaris メディアキットに付属しています。また、使用するネットワークにネットワークインストールサーバーがすでに存在する場合は、このネットワークインストールサーバーにサーバーブレード用の Solaris イメージを追加します。

   ブレードシステムシャーシのコンポーネントに動的に IP アドレスを割り当てる場合は、次の節を参照してください。

   - 1-11 ページの 1.6 節「シャーシに必要な IP 情報」
   - 1-12 ページの 1.7 節「DHCP サーバーを使用した SSC の IP アドレスの自動設定」

   また、付録 C の補足情報を参照して、データネットワーク上にネットワークインストールサーバーと DHCP サーバーの両方を設定してください。

2. **シャーシのシステムコントローラの 1 つにシリアル接続を設定します。**

   または、DHCP サーバーを設定してシステムコントローラに IP 情報を割り当てます。この情報によって、システムコントローラに telnet でアクセスできるようになります。

   シャーシのシステムコントローラの 1 つにシリアル接続を設定する方法については、『Sun Fire B1600 ブレードシステムシャーシハードウェア設置マニュアル』を参照してください。

3. **システムコントローラにログインして、パスワードと日付および時刻を設定します。**

   パスワードと日付および時刻の設定は必須です (第 2 章を参照)。

4. **各スイッチにログインして、パスワードを 1 つ以上設定します。**

   この手順の詳細は、第 2 章を参照してください。

5. **IP 環境を準備します。**

   シャーシのシステムコントローラおよびスイッチ、サーバーブレードの IP を受信するために、ネットワークの IP 環境を準備する必要があります (第 3 章を参照)。

6. **基本的な設定を行います。**

   第 3 章の手順に従って、あとで調整できる基本的な設定を行います。第 3 章の手順では、システムシャーシの 2 つのスイッチを利用して、各サーバーブレードからネットワークに 2 つの接続を確立する方法について説明します。

7. **必要に応じて、データと管理のネットワークが分離されたネットワーク環境でシステムシャーシを使用できるように設定します。**

   第 5 章の手順に従って設定します。第 5 章の手順では、インターネットネットワークマルチパス (IPMP) によってシステムシャーシの 2 つのスイッチを利用して、各サーバーブレードからデータネットワークに 2 つの完全な冗長接続を確立する方法について説明します。

8. **必要に応じて、各ブレードがデータネットワークへの冗長接続 (第 5 章を参照) と管理ネットワークへの冗長接続の両方を確立するようにシステムシャーシを設定します。**

   第 6 章の手順に従って設定します。

9. **必要に応じて、各サーバーブレードを別々の所有者に割り当てるようにシステムシャーシを設定し、各所有者がシステムコントローラまたはスイッチ、ほかの所有者のブレードにアクセスすることなく、自身のブレードを管理できるようにします。**

   第 7 章の手順に従って設定します。

1.2 Sun Fire B1600 ブレードシステムシャーシ

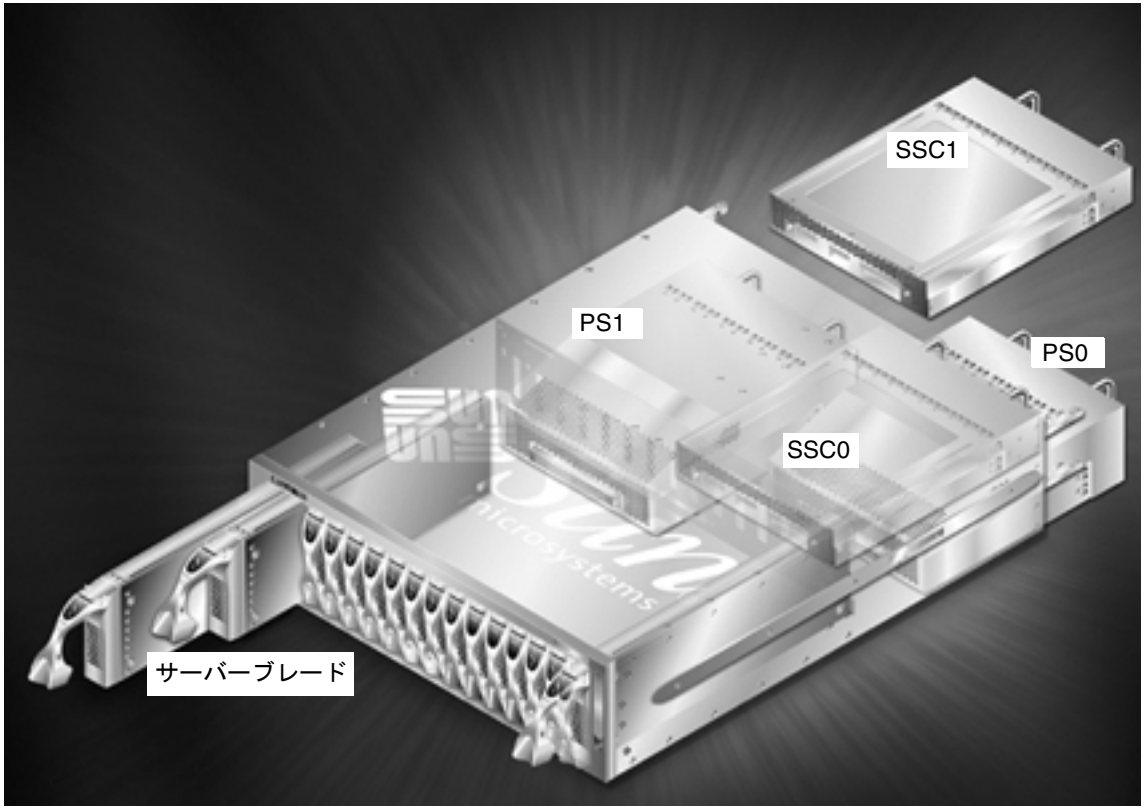

図 1-1 Sun Fire B1600 ブレードシステムシャーシ

Sun Fire B1600 ブレードシステムシャーシは、主にインターネットサービスプロバイダ向けに設計された、高さ 3 U の 16 サーバーシャーシです。高性能のサーバーをできるだけ高い密度で配置する必要がある企業ネットワークでの使用にも適しています。

このシャーシは、最大で 16 台のサーバーブレードを収容することができ、2 台の電源装置 (PSU) と 2 台のスイッチ/システムコントローラ (SSC) 装置を備えています。

1.3 ブレードシステムシャーシのソフトウェア

ブレードシステムシャーシの主なソフトウェアコンポーネントは、次の 3 つです。

- 2 つのシステムコントローラ (SSC0 に 1 つ、SSC1 に 1 つ)
- 2 つのスイッチ (SSC0 に 1 つ、SSC1 に 1 つ)
- サーバーブレード

1.3.1 アクティブシステムコントローラおよびスタンバイシステムコントローラ

図 1-1 に示すとおり、シャーシは 2 台の SSC を備えています。システムシャーシの出荷時の構成では、SSC0 のシステムコントローラが「アクティブ」で、SSC1 のシステムコントローラが「スタンバイ」になっています。

しかし、アクティブシステムコントローラを含む SSC を物理的に取り外した場合、またはアクティブシステムコントローラの主要なソフトウェアアプリケーションに重大な障害が発生した場合には、もう一方の SSC のスタンバイシステムコントローラが自動的にアクティブになります。

また、アクティブシステムコントローラのコマンド行から、スタンバイシステムコントローラをアクティブに切り替えることもできます。詳細は、『Sun Fire B1600 ブレードシステムシャーシ管理マニュアル』を参照してください。

システムコントローラソフトウェアの将来のバージョンでは、システムコントローラソフトウェアがスタンバイシステムコントローラを常時監視して、他のシステムコントローラに比べてアクティブシステムコントローラがアクティブの役割に適していないと判断した場合に、スタンバイシステムコントローラに処理を自動的に引き継ぐ機能が追加される予定です。

2 つのシステムコントローラはエイリアス IP アドレスを共有し、個別にプライベート IP アドレスを持つこともできます。エイリアス IP アドレスは、常にアクティブシステムコントローラのアドレスになります。ネームサービスには、このアドレスを設定します。システムコントローラは、アクティブシステムコントローラの役割を引き継ぐと、自身にこのエイリアスアドレスを割り当て、MAC アドレスとエイリアス IP アドレスの両方を含むブロードキャストによって、広域なネットワークにエイリアス IP アドレスを持つデバイスであることを通知します。

各システムコントローラにプライベート IP アドレスを割り当てると、アクティブシステムコントローラに telnet で接続するときに、エイリアス IP アドレスの代わりにプライベート IP アドレスを使用できます。プライベート IP アドレスが割り当てられ

ていても、スタンバイシステムコントローラに telnet で接続することはできません。ただし、システムコントローラにプライベート IP アドレスを割り当てると (第 3 章を参照)、ネットワーク管理者はシステムコントローラに個別に ping を実行して、ネットワーク上にシステムコントローラが存在することを迅速に確認できるので便利です。

1.3.2 冗長化された 2 つのスイッチ

シャーシ内のアクティブシステムコントローラは常に 1 つですが、SSC 内のスイッチは常に両方ともアクティブになっています。これは、ブレードシステムシャーシの重要な機能です。各サーバーブレードは、2 つの (各スイッチに 1 つずつの) Gigabit ネットワークインタフェースを備えています。したがって、一方のインタフェース上でネットワーク接続の障害 (スイッチの障害など) が発生しても、もう一方がサービスを継続します。

この二重化された接続を利用して広域なネットワークにシャーシを接続するように設定する方法については、第 3 章および第 5 章を参照してください。

注 – アクティブシステムコントローラは常に 1 つだけですが、シャーシのスイッチは常に両方ともアクティブになっています。

1.3.3 サーバーブレード

サーバーブレードは、論理的には標準的なサンのエントリレベルサーバーと同じものです。標準的なネットワークおよび sysid 設定方法 (TFTP および DHCP など) は、すべてサーバーブレードにも適用され、次に示す Solaris オペレーティング環境のネットワークインストール方法も使用できます。

- Web Start インストール
- 対話式インストール
- カスタム JumpStart インストール
- Web Start のフラッシュインストール

これらの Solaris のインストール方法については、『Solaris のインストール (上級編)』の第 3 章を参照してください。

1.4 システムコントローラおよびスイッチ、サーバーブレードの役割

1.4.1 システムコントローラの役割

アクティブシステムコントローラには 2 つの役割があります。システムシャーシのサブコンポーネントと通信してその動作状態を監視することと、シリアル接続または telnet 接続を介して「Advanced Lights Out Management」ソフトウェアと呼ばれるシャーシ設定の中心になるソフトウェアへのコマンド行インタフェースを提供することです。このソフトウェアは、シャーシ内のアクティブシステムコントローラ上で動作するアプリケーションです。

このマニュアルの第 2 章では、システムコントローラの Advanced Lights Out Management ソフトウェアにログインする方法について説明します。

ログインすると、次の機能を使用できるようになります。

- システムシャーシとそのコンポーネントを監視および管理するための、アクティブシステムコントローラ固有のコマンドセット。このコマンドについては、付録 E および『Sun Fire B1600 ブレードシステムシャーシ管理マニュアル』を参照してください。
- システムシャーシ内の 2 つの統合スイッチのコンソール。スイッチのコマンド行インタフェース固有のコマンドについては、付録 A および『Sun Fire B1600 ブレードシステムシャーシスイッチ管理マニュアル』を参照してください。
- システムシャーシに取り付けたサーバーブレードのコンソール。

このマニュアルは、最初の設定を行うときに、出荷キットのマニュアル CD に収録されたほかのマニュアルを参照しなくてもブレードシステムシャーシを設定できるように作成されています。

ただし、マニュアル CD には、出荷キットに付属する印刷されたマニュアルのオンライン版だけでなく、Advanced Lights Out Management ソフトウェアのオンラインマニュアル (『Sun Fire B1600 ブレードシステムシャーシ管理マニュアル』) および統合スイッチのオンラインコマンドリファレンスマニュアル (『Sun Fire B1600 ブレードシステムシャーシスイッチ管理マニュアル』) も収録されています。

アクティブシステムコントローラとスタンバイシステムコントローラの関係、およびその制限事項については、付録 F を参照してください。

1.4.2 スイッチの役割

図 1-2 に、各スイッチの Ethernet ポートおよび各サーバーブレードの Ethernet インタフェースをすべて示します。各サーバーブレードは、SSC0 および SSC1 のスイッチに対するインタフェースを 1 つずつ備えています。各スイッチは、各サーバーブレードに対するポートを 1 つずつ備えています。これには、SNP0 ～ SNP15 のラベルが付いています。データネットワークのアップリンクポートには、NETP0 ～ NETP7 のラベルが付いています。

注 – データネットワークのアップリンクポートとサーバーブレードのポートには、直接的な関連はありません。この 2 つのポートグループの間にある高速ミッドプレーンが、グループ間のすべてのトラフィックを切り替えます。図 1-2 ではこれを、SNP ポートおよび NETP ポートからスイッチファブリックへの黒い太線として示しています。

この図には、スイッチの内部管理ポート (NETMGT) と、SSC の背面にある NETMGT というラベルの付いた外部 RJ-45 ポートも示されています。

外部 NETMGT ポートは、システムコントローラ (図で SC と示されている部分) およびスイッチの両方に Ethernet 接続を提供します。スイッチのコマンド行インタフェースおよび Web インタフェースでは、スイッチの内部管理ポートも NETMGT として識別されます。内部スイッチの NETMGT ポートおよびシステムコントローラと、外部 NETMGT ポートは、小さいハブによって接続されています。図の Ethernet ポートおよび SC インタフェースに付いている 1 および 2 の番号は、これらのポートのデフォルトの VLAN[1] 構成を示しています。データネットワークに対応するデフォルトの VLAN は VLAN 1 です。管理ネットワークに対応するデフォルトの VLAN は VLAN 2 です。

SC の VLAN ID はスイッチからは設定できません。SC の VLAN ID は、`setupsc` コマンド (第 3 章を参照) を使用した、システムコントローラの対話式の設定手順の中で指定します。このコマンドを実行すると、SC の VLAN を使用可能にするかどうかを含む、一連の質問が表示されます。yes と答えると、SC インタフェースに VLAN ID を指定するためのプロンプトが表示されます。デフォルトは、スイッチのデフォルトの管理 VLAN である VLAN 2 です。SC インタフェースは、スイッチのポートとは異なります。このインタフェースの VLAN を使用可能にすると、指定した VLAN のタグの付いたフレームだけが送受信されるようになります。

図 1-2 のスイッチには、パケットフィルタが示されています。パケットフィルタは、初期状態では、内部 NETMGT ポートとすべてのサーバーブレードポートの間を遮断しています。パケットフィルタは、データネットワークを介してブレードにアクセスする外部ユーザーによる攻撃から、管理ネットワークを保護します。

---

1. VLAN (Virtual Local Area Network : 仮想ローカルエリアネットワーク) とは、自己完結型の論理的なネットワークおよびブロードキャストドメインで、1 つ以上のネットワークインフラストラクチャーデバイスのポートのグループをソフトウェアで設定することによって定義します。

デフォルトでは、サーバーブレードとスイッチの NETMGT ポート間を通過できるネットワークトラフィックはありません。ただし、特定のプロトコルに関するルールを指定することによって、一部のトラフィックにパケットフィルタの通過を許可することができます。ルールの指定方法については、付録 A を参照してください。

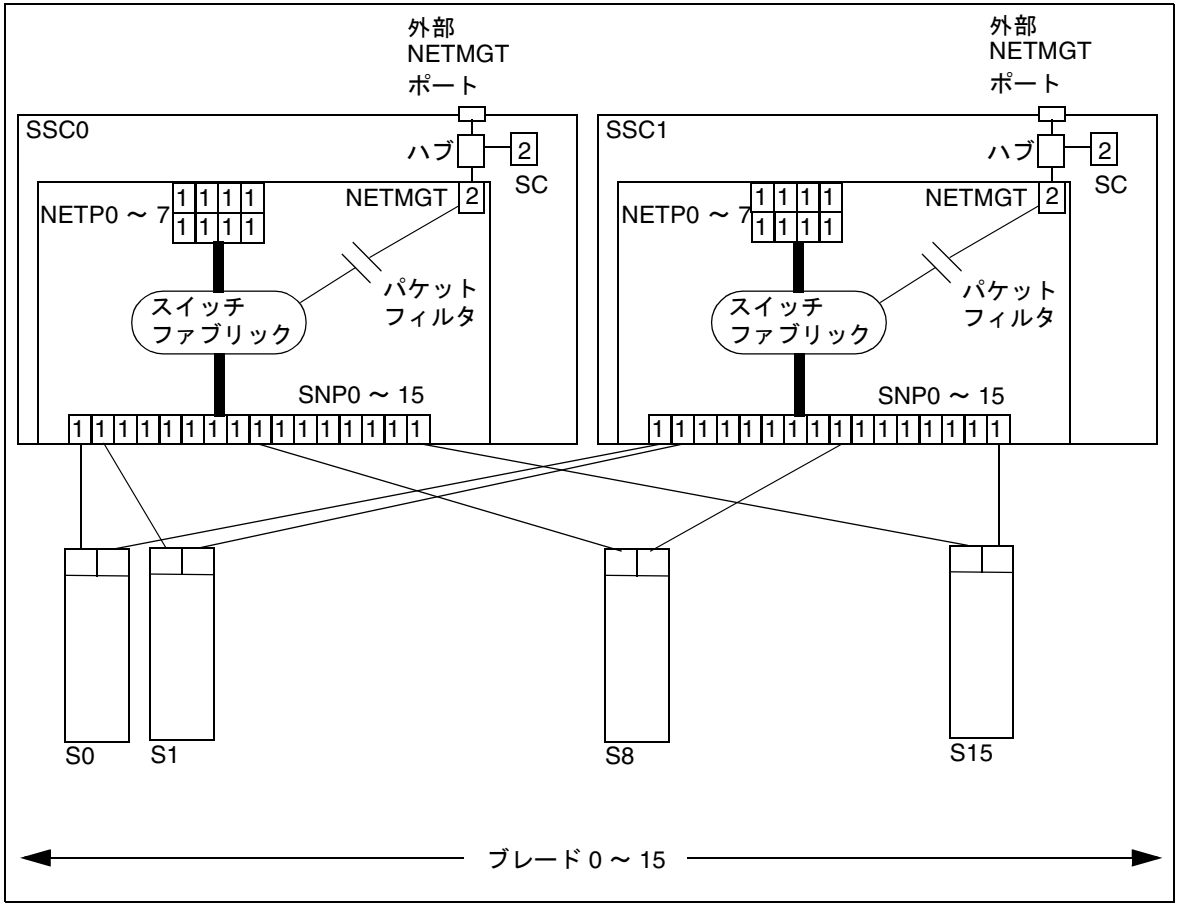

図 1-2　　システムシャーシの Ethernet ポートおよびインタフェースとデフォルトの VLAN 番号

1.4.3 サーバーブレードの役割

サーバーブレードは、ソフトウェアアプリケーションを実行するための処理能力を提供します。入出力には主にネットワークを使用しますが、システムコントローラと各ブレード間の内部シリアル接続を使用して、システムコントローラのコマンド行インタフェースからブレードのコンソールにアクセスすることもできます。

すべてのブレードは、シャーシの 2 つの内部スイッチへの Gigabit Ethernet インタフェースを 1 つずつ備えていて、スイッチも外部ネットワークへの Gigabit Ethernet インタフェースを備えています。

ブレードは、通常、ローカルディスクにオペレーティングシステムソフトウェアおよび構成情報を保持します。ブレードのローカルの記憶装置にはユーザーのデータは格納されませんが、代わりに遠隔の記憶装置を使用できます。

出荷時のデフォルトの状態では、サーバーブレードは、ローカルハードディスクに格納されているオペレーティング環境のスタブを使用して起動します。起動されたサーバーブレードは、ネットワーク上でオペレーティング環境をインストールしたネットワークインストールサーバーを検索します。

ネットワークインストールサーバーから最初のサーバーブレードを起動したときに、ブレード上で実行するアプリケーションソフトウェアを追加できます。ソフトウェアの追加後に、『Solaris のインストール (上級編)』の手順に従って Web Start 用フラッシュアーカイブを作成します。Sun Fire B1600 ブレードシステムシャーシ内の Sun Fire B100s Solaris サーバーブレードで、この Web Start 用フラッシュアーカイブを使用すると、1 台のブレードのオペレーティング環境およびアプリケーションソフトウェアをほかのブレードに複製できます。したがって、シャーシ全体のサーバーブレードの設定作業にかかる時間を大幅に短縮できます。

Web Start のフラッシュアーカイブの詳細は、付録 D を参照してください。

1.5 ソフトウェア設定のための準備作業

ブレードシステムシャーシを設置して電源を入れ、初期設定を実行するときは、SSC0 へのシリアル接続を設定するか (デフォルトでは、アクティブシステムコントローラ)、DHCP サーバーを使用してシャーシのアクティブシステムコントローラに自動的に IP を割り当てる必要があります。DHCP サーバーを使用して IP を割り当てた場合は、アクティブシステムコントローラに telnet で接続してシャーシの初期設定を実行できます。

シリアル接続を設定するためのケーブル配線については、『Sun Fire B1600 ブレードシステムシャーシハードウェア設置マニュアル』を参照してください。

DHCP サーバーの使用方法については、1-12 ページの 1.7 節「DHCP サーバーを使用した SSC の IP アドレスの自動設定」を参照してください。

注 – シャーシ内の 2 つの SSC に電源が入り、どちらの SSC も正常に動作している場合は、デフォルトで SSC0 がアクティブシステムコントローラ、SSC1 がスタンバイシステムコントローラになっています。これは、シリアル接続によるシャーシの初期設定を行う場合は、SSC0 へのシリアル接続が必要であることを意味します。

ただし、ブレードシステムシャーシを毎日稼動させることを考慮して、両方の SSC にシリアル接続を設定することをお勧めします。こうしておくと、アクティブな SSC に何らかの障害が発生した場合でも、シャーシへのシリアル接続を失うことがありません。

このマニュアルの第 2 章および第 3 章では、SSC0 へのシリアル接続または telnet 接続を設定した場合のシャーシの設定方法について説明します。

1.6 シャーシに必要な IP 情報

使用しているネットワーク環境に Sun Fire B1600 ブレードシステムシャーシを組み込むには、アクティブシステムコントローラのエイリアス IP アドレスのほかに、シャーシの各 Ethernet インタフェースの IP アドレスおよびネットマスク、デフォルトゲートウェイを設定する必要があります。

ネームサービスにはシステムコントローラのエイリアス IP アドレスを設定しますが、システムコントローラはプライベート IP アドレスを持つこともできます。プライベート IP アドレスは、ネームサービスに設定する必要はありません。システムコントローラは、アクティブシステムコントローラの役割を引き継ぐと、自身にエイリアス IP アドレスを割り当て、MAC アドレスおよびエイリアス IP アドレスの両方を含むブロードキャストによって、広域なネットワークにエイリアス IP アドレスを持つデバイスであることを通知します。

フル構成のシャーシは、37 個以上の IP アドレス (2 個のプライベード SC アドレスを含む) を使用します。

1. アクティブシステムコントローラのエイリアス IP アドレス 1 個 (SSC0 または SSC1 にかかわらず、アクティブシステムコントローラが使用するアドレス)
2. SSC0 のシステムコントローラのプライベート IP アドレス 1 個
3. SSC1 のシステムコントローラのプライベート IP アドレス 1 個
4. SSC0 のスイッチの IP アドレス 1 個
5. SSC1 のスイッチの IP アドレス 1 個
6. 各ブレードの一次 (Gigabit Ethernet) インタフェース `ce0` の IP アドレス 16 個
7. 各ブレードの二次 (Gigabit Ethernet) インタフェース `ce1` の IP アドレス 16 個

第 5 章または第 6 章、第 7 章で説明するように、シャーシにインターネットマルチパス (IPMP) 機能を設定する場合は、フル構成のシャーシのブレードには 65 個以上の IP アドレスが必要になります。

1.7 DHCP サーバーを使用した SSC の IP アドレスの自動設定

デフォルトでは、アクティブな SSC 内のシステムコントローラは、DHCP サーバーからアクティブシステムコントローラおよびスタンバイシステムコントローラの IP 設定情報を取得することを試みます。

各 SSC 内のスイッチも、デフォルトでは、DHCP サーバーから自身の IP 設定情報を取得することを試みます。

システムコントローラは、IP アドレスを最大で 3 個使用します。

- エイリアス IP アドレス 1 個 (SSC0 または SSC1 にかかわらず、アクティブシステムコントローラが使用するアドレス)
- SSC0 のシステムコントローラのプライベート IP アドレス 1 個 (任意)
- SSC1 のシステムコントローラのプライベート IP アドレス 1 個 (任意)

各スイッチには IP アドレスが 1 個ずつ必要です。

注 – データネットワークと管理ネットワークを分離する場合は、SSC の設定に使用する DHCP サーバーが管理ネットワーク上に存在し、サーバーブレードの設定に使用する DHCP サーバーがデータネットワーク上に存在する必要があります。サーバーブレードの IP アドレスを提供するように DHCP サーバーを設定する方法については、付録 C を参照してください。

1.7.1 SSC の「固定」IP アドレスの設定

アクティブシステムコントローラは、3 個の IP アドレス (SSC0、SSC1、エイリアス IP アドレス) を求める DHCP 要求を送信します。

各スイッチは、1 個の IP アドレスを求める DHCP 要求を送信します。

5 個の「固定」IP アドレス (5 個の変化しない IP アドレス) を使用するには、DHCP サーバーの 5 個の特定のアドレスをシステムコントローラおよびスイッチのクライアント識別子に関連付ける必要があります。

アクティブかどうかにかかわらず、各システムコントローラにはクライアント識別子が設定されています。これは、各システムコントローラが、任意でプライベート IP アドレスを持つことができるためです。プライベート IP アドレスを割り当てると、ネットワーク管理者は、各システムコントローラに ping を実行することでネットワーク上にシステムコントローラが存在することを確認できるので便利です。

表 1-1 に、シャーシのシステムコントローラおよびスイッチのクライアント識別子を示します。

表 1-1 システムコントローラおよび統合スイッチのクライアント識別子

デバイス	クライアント識別子
アクティブシステムコントローラ	SUNW,SSC_ID=*serial number of chassis*
SSC0 のシステムコントローラ (プライベート IP)	SUNW,SSC_ID=*serial number of chassis*,0
SSC1 のシステムコントローラ (プライベート IP)	SUNW,SSC_ID=*serial number of chassis*,1
SSC0 のスイッチ	SUNW,SWITCH_ID=*serial number of chassis*,0
SSC1 のスイッチ	SUNW,SWITCH_ID=*serial number of chassis*,1

注 – シャーシのシリアル番号は、シャーシ背面の右側にあるラベルに印刷されています。クライアント識別子には、シャーシのラベルに印刷された番号の最後の 6 桁だけを使用します。

シャーシのシリアル番号は、システムコントローラのコマンド行で `showfru ch` コマンドを実行して確認することもできます。`/ManR/Sun_serial_No` フィールドに表示されるのがシリアル番号です。

『Solaris DHCP の管理』(816-1249) の手順に従って「固定」IP アドレスを作成する際には、SSC と同じネットワークにある DHCP サーバーで、前述の表のクライアント識別子に割り当てる 5 個の IP アドレスを 1 組設定します。クライアント識別子に割り当てた IP アドレスは控えておいてください。アクティブシステムコントローラまたはスイッチに telnet で接続するときに、この IP アドレスが必要になります。また、Web ベースのグラフィカルユーザーインタフェースからスイッチにアクセスするときにも、この IP アドレスが必要です。

1.7.2 SSC の動的 IP アドレスの設定

シャーシのシステムコントローラおよびスイッチに「固定」IP アドレスを設定しない場合は、DHCP サーバーによって 1 組の動的 IP アドレスを割り当てるように設定します。デバイスが DHCP 要求を発行すると、クライアント識別子に動的 IP アドレスが割り当てられます。詳細は、『Solaris DHCP の管理』(816-1249) を参照してください。

DHCP サーバーが 1 組の動的 IP アドレスを提供するように設定した場合、システムコントローラまたはいずれかのスイッチに telnet で接続するか、いずれかのスイッチに Web ベースのグラフィカルユーザーインタフェースでアクセスするときには、システムコントローラおよび 2 つのスイッチに割り当てられた IP アドレスを確認する必要があります (1-14 ページの 1.7.3 節「telnet 接続のためのシャーシの IP アドレスの確認」を参照)。

1.7.3 telnet 接続のためのシャーシの IP アドレスの確認

シリアル接続ではなく telnet 接続を介してアクティブシステムコントローラにはじめてログインする場合で、シャーシのコンポーネントに「固定」IP アドレスではなく動的 IP アドレスを割り当てた場合には、DHCP サーバーがシステムコントローラに割り当てた IP アドレスを確認する必要があります。

使用している DHCP サーバーが Solaris システムである場合は、pntadm コマンドを実行すると、シャーシが属するネットワーク上のすべてのデバイスを対応する IP アドレスとともに一覧表示することができます。

次のように入力します。

```
# pntadm -P network address
pntadm -P 129.156.203.0
Client ID                                  Flags   Client IP        Server IP      Lease Expiration

53554E572C5353435F49443D313233343536[1]      00     129.156.203.240   129.156.202.163 01/03/2003
53554E572C5357495443485F49443D3132333435362C30[2]  00     129.156.203.241   129.156.202.163 01/03/2003
53554E572C5357495443485F49443D3132333435362C31[3]  00     129.156.203.242   129.156.202.163 01/03/2003
```

出力例の説明

1. アクティブシステムコントローラのクライアント ID
2. SSC0 のスイッチのクライアント ID
3. SSC1 のスイッチのクライアント ID

network address には、使用している管理ネットワークのネットワークアドレスを指定します。一覧に表示されたデバイスは、クライアント識別子を示す 16 進数表記の文字列によって識別できます。

出力例の最初に表示されているデバイスはアクティブシステムコントローラ (エイリアス IP アドレスを使用) で、2 番目のデバイスは SSC0 のスイッチ、3 番目のデバイスは SSC 1 のスイッチです。どのデバイスにどのクライアント IP アドレスが割り当てられているかを確認するには、出力された 16 進数表記の文字列を該当する英数字に変換する必要があります。

(出力例では、見やすくするために、「Lease Expiration」の右側の 2 列を省略しています。省略した列は、「Macro」および「Comments」です。)

表 1-2 アクティブシステムコントローラのクライアント ID の変換例

	アクティブシステムコントローラ	シャーシのシリアル番号
16 進数	53554E572C5353435F49443D	313233343536
英数字	SUNW,SSC_ID=	123456

表 1-3 SSC0 の SC[1] (任意のプライベート IP アドレス) のクライアント ID の変換例

	アクティブシステムコントローラ	シャーシのシリアル番号	SSC0 の接尾辞
16 進数	53554E572C5353435F49443D	313233343536	2C30
英数字	SUNW,SSC_ID=	123456	,0

1. システムコントローラ

表 1-4 SSC1 のスイッチのクライアント ID の変換例

	SSC1 のスイッチ	シャーシのシリアル番号	SSC1 の接尾辞
16 進数	53554E572C5357495443485F49443D	313233343536	2C31
英数字	SUNW,SWITCH_ID=	123456	,1

1.7.4 telnet 接続を使用したシステムコントローラへのアクセス

必要な IP アドレスを DHCP サーバーに設定したあと、アクティブシステムコントローラに telnet 接続するには、次の手順を実行します。

1. **シャーシにすでに電源が入っている場合は、IEC 電源ケーブルを取り外してシャーシの電源を入れ直します。**

2. シャーシに電源が入ったら、遠隔の端末で次のように入力します。

```
% telnet alias ip address または host name
Trying alias ip address
Connected to alias ip address または host name
Escape character is '^]'

Sun Advanced Lights Out Manager for Blade Servers 1.0
ALOM-B 1.0

username:
```

alias ip address には、アクティブシステムコントローラの IP アドレスを入力します。または、ホスト名で指定することもできます。

1.8 スイッチまたはブレードのコンソールから sc> プロンプトへの切り替え

シャーシの設定作業に進む前に、ブレードまたはスイッチのコンソールからシステムコントローラの sc> プロンプトに切り替えるためのエスケープシーケンスを控えておくと役立ちます。このエスケープシーケンスは #. です。ハッシュ記号「#」を入力してからピリオド「.」を入力します。

このマニュアルの手順を実行するときには、sc> プロンプトからサーバーブレードおよびスイッチのコンソールにアクセスします。

次の手順

第 2 章に進んで、システムシャーシの準備設定手順を実行します。

第2章

SSC のパスワードおよび日付、時刻の設定

この章では、ブレードシステムシャーシをネットワーク環境に組み込む前に、アクティブシステムコントローラおよび両方のスイッチにログインして実行しておく必要のある準備作業について説明します。

アクティブシステムコントローラは設定しますが、スタンバイシステムコントローラを設定する必要はありません。アクティブシステムコントローラが設定情報をスタンバイシステムコントローラに通知して、必要な場合にスタンバイシステムコントローラに処理を引き継ぐことができるようにするためです。

スイッチのユーザーログインおよびパスワードの情報は、システムコントローラのユーザーログインおよびパスワードの情報とは別のものです。したがって、これらの情報は別々に設定する必要があります。

この章は次の節で構成されています。

- 2-2 ページの 2.1 節「システムコントローラへのログインとパスワードおよび時刻の設定」
- 2-4 ページの 2.2 節「デフォルトユーザーでのスイッチへのログインとパスワードの設定」

この 2 つの節の手順を、すべて実行してください。

注 – システムシャーシを設定するには、アクティブシステムコントローラへのコマンド行インタフェースを使用します。このインタフェースから、2 つのスイッチおよびサーバーブレードのコンソールにアクセスする必要もあります。スイッチまたはブレードのコンソールでは、**#.** を入力して、アクティブシステムコントローラの `sc>` プロンプトに切り替えます。

2.1 システムコントローラへのログインとパスワードおよび時刻の設定

この節では、アクティブシステムコントローラにユーザー admin (デフォルトユーザー) でログインし、そのパスワードを指定する方法について説明します。

注 – システムコントローラに設定するユーザーログインおよびパスワードの情報は、スイッチに設定するユーザーログインおよびパスワードの情報とは別のものです。スイッチの情報を設定する方法については、2-4 ページの 2.2 節「デフォルトユーザーでのスイッチへのログインとパスワードの設定」を参照してください。

この節の手順は、アクティブシステムコントローラへのシリアル接続または telnet 接続の設定が完了していることを前提とします。スタンバイシステムコントローラへの telnet 接続は設定できません。エイリアス IP アドレスを使用して telnet で接続すると、常にアクティブシステムコントローラに接続します。

シリアル接続を使用する場合、シャーシの出荷時のデフォルトの設定では、SSC0 のシステムコントローラがアクティブシステムコントローラであることに注意してください。スタンバイシステムコントローラである SSC1 に接続すると、スタンバイシステムコントローラに接続したことを示すメッセージが表示されます。この場合は、SSC0 に接続してください。どのような場合でも、両方の SSC へのシリアル接続を維持することをお勧めします。

ブレードシステムシャーシの設定を開始するには、次の手順を実行します。

1. username: プロンプトで、デフォルトユーザー名 (admin) を入力します。

```
Sun Advanced Lights Out Manager for Blade Servers 1.0
ALOM-B 1.0

username: admin
```

2. sc> プロンプトで、デフォルトユーザーのパスワードを設定します。

   デフォルトユーザー (admin) は事前設定されており、削除することはできません。このユーザーは、はじめは自身のパスワードを設定する権限だけを持っています。パスワードを設定すると、すべての権限を取得します。ブレードシステムシャーシの設定を続けるには、デフォルトユーザー (admin) のパスワードを設定する必要があります。

   指定する最初のパスワードは、次の条件を満たす必要があります。

- 大文字または小文字の英字で始まり、2 文字以上の大文字または小文字の英字を含むこと
- 6 ~ 8 文字であること
- 1 文字以上の数字またはピリオド (.)、下線 (_)、ハイフン (-) を含むこと
- デフォルトユーザーのログイン名 (admin) またはそれを逆順に並べた名前 (nimda)、前後をつなげて並べ変えた名前ではないこと (たとえば、dmina および minad、inadm、nadmi はすべて禁止)

システムコントローラの名前付きユーザーの設定方法については、『Sun Fire B1600 ブレードシステムシャーシ管理マニュアル』を参照してください。

ユーザー admin のパスワードを設定するには、次のように入力します。

```
sc> password
Enter current password:
Enter new password:
Enter new password again:
New password set for user admin successfully
sc>
```

3. アクティブシステムコントローラに日付および時刻を設定します。

注 – 日付および時刻を設定するときは、協定世界時 (UTC) を使用する必要があります。サーバーブレードは、システムコントローラの UTC からのオフセットを使用して、その地域のタイムゾーンのローカル時刻を算出します。サーバーブレードは、この時刻をシステムコントローラから受信します。

日付と時刻は、同じコマンド (setdate コマンド) で設定します。次に、このコマンドの構文を示します。

```
sc> setdate [mmdd]HHMM[.SS] | mmddHHMM[cc]yy[.SS]
```

記号の意味は、次のとおりです。

mm には月を指定 (2 桁)
dd には日を指定 (2 桁)
HH には時を指定 (2 桁)
MM には分を指定 (2 桁)
SS には秒を指定 (2 桁)

- **時刻を設定します (24 時間制)。**
  時 (2 桁)、分 (2 桁) の順に続けて入力します。たとえば、時刻を 11 時 42 分に設定するには、次のように入力します。

```
sc> setdate 1142
```

- **月および日、時刻 (24 時間制で分まで) を設定します 。**
  月 (2 桁)、日 (2 桁)、時 (2 桁)、分 (2 桁) の順に続けて入力します。たとえば、日付および時刻を 3 月 27 日午前 11 時 42 分に設定するには、次のように入力します。

```
sc> setdate 03271142
```

- **月および日、時刻 (24 時間制)、年、秒を設定します。**
  月 (2 桁)、日 (2 桁)、時 (2 桁)、分 (2 桁)、年 (4 文字 (2002) または 2 文字 (02)) の順に続けて入力します。任意でピリオドと秒 (2 桁) を続けて入力します。たとえば、日付および時刻を 2002 年 3 月 27 日午前 11 時 42 分 47 秒に設定するには、次のように入力します。

```
sc> setdate 2703114202.47
```

2.2 デフォルトユーザーでのスイッチへのログインとパスワードの設定

この節では、スイッチへのログイン方法とパスワードの設定および保存方法について説明します。

注 – スイッチに設定するユーザーログインおよびパスワードの情報は、システムコントローラに設定するユーザーログインおよびパスワードの情報とは別のものです。

---

1. **次のように入力します。**

```
sc> console sscn/swt
```

n には、SSC0 または SSC1 のどちらのスイッチを設定するかによって、0 または 1 を指定します。たとえば、SSC0 のスイッチを設定するには、次のように入力します。

```
sc> console ssc0/swt
```

2. ユーザー名およびパスワードの入力を求めるプロンプトが表示されたら、両方に admin を入力します。

```
Username admin
Password *****

CLI session with the host is opened.
To end the CLI session, enter [Exit].
```

3. console# プロンプトで、次のように入力します。

```
Console#configure
```

4. 次の 3 つのパスワードを設定します。最初のパスワードは、必ず設定してください。

   a. スイッチの特権実行コマンドモードを使用するためのパスワードを設定します。

   このコマンドモードでは、スイッチのすべての設定の参照および変更が可能です。デフォルトユーザー admin (手順 2 を参照) は、特権実行の権限を持っています。セキュリティーのため、このユーザーのパスワードを変更することをお勧めします。次のように入力します。

```
Console(config)#username admin password 0 password
```

   password には、1 ～ 8 文字の文字列を指定します。0 は、パスワードをプレーンテキストで指定することをスイッチに通知します。パスワードのプレーンテキストまたは暗号化テキストの使用方法については、『Sun Fire B1600 ブレードシステムシャーシスイッチ管理マニュアル』を参照してください。

b. **ユーザー** guest **のパスワードを設定します。**

ユーザー guest は、スイッチの一部の設定および状態情報を参照することができ、ping コマンドを実行することもできます。このユーザーはスイッチの設定を変えることはできません。このユーザーのデフォルトのパスワードは、guest です。このユーザーの新しいパスワードを設定するには、次のように入力します。

```
Console(config)#username guest password 0 password
```

password には、1 ～ 8 文字の文字列を指定します。0 は、パスワードをプレーンテキストで指定することをスイッチに通知します。

c. enable **コマンドのパスワードを設定します。**

enable コマンドを使用すると、guest でログインしたユーザーが特権実行の権限を取得できるようになります。このユーザーがコマンド行で enable を入力すると、パスワードを求めるプロンプトが表示されます。enable コマンドのデフォルトのパスワードは、super です。このコマンドの新しいパスワードを設定するには、次のように入力します。

```
Console(config)#enable password level 15 0 password
```

password には、1 ～ 8 文字の文字列を指定します。15 を指定すると、enable コマンドの実行を許可されたユーザーに特権実行の権限が与えられます。
0 は、パスワードをプレーンテキストで指定することを通知します。

注 – 統合スイッチのその他のコマンドモードについては、『Sun Fire B1600 ブレードシステムシャーシスイッチ管理マニュアル』を参照してください。

---

5. **次のように入力して、スイッチの設定モードを終了します。**

```
Console(config)#end
```

または

```
Console(config)#exit
```

6. **スイッチの設定を変更したので、ここで設定を保存します。**

保存するには、ファームウェアが保持している現在の設定情報 (running-config) を起動時の設定情報 (startup-config) にコピーします。

次のように入力します。

```
Console#copy running-config startup-config
Startup configuration file name []:filename
Write to FLASH Programming
-Write to FLASH finish
Success

Console#
```

filename には、新しい起動時の設定を保存するファイルの名前を指定します。

7. **DHCP を使用してスイッチの IP を設定している場合は、次のいずれかを実行して 2 番目のスイッチを設定することをお勧めします。**

- 2 番目のスイッチに対しても、手順 1 ～手順 6 を実行します。
- A-9 ページの A.9 節「最初のスイッチから 2 番目のスイッチへの設定のコピー」の手順を実行します。スイッチの設定をコピーすると、設定したログインとパスワードの情報もコピーされます。

DHCP を使用していない場合は、この時点では 2 番目のスイッチを設定する必要はありません。この設定がいつ必要であるかについては、第 3 章で説明しますが、最初のスイッチにさらに設定を行ったあとで設定をすべてコピーします。

次の手順

第 3 章に進んで単純なネットワークへの接続を実行してから、第 4 章の手順に従ってサーバーブレードを設定します。

さらに高度なネットワークの設定が必要な場合は、第 5 章および第 6 章、第 7 章を参照してください。

第3章

システムシャーシの単純なネットワークへの接続

この章は次の節で構成されています。

3.1 システムシャーシの 2 つのスイッチの利用

この章では、Sun Fire B1600 ブレードシステムシャーシを、データネットワークと管理ネットワークを分離していない単純なネットワーク環境で使用する方法について説明します。この章の手順を実行すると、システムシャーシの 2 つのスイッチを利用して、各サーバーブレードがネットワークに 2 つの接続を確立できます。

図 3-1 に、Sun Fire B1600 ブレードシステムシャーシを含むネットワークの例を示します。以降の手順では、この図および図に記された IP アドレスを使用します。

また、この章では、`/etc/hosts` ファイルの例と `/etc/ethers` および `/etc/netmasks` ファイルの例も示します。この例は、ネットワーク環境にシャーシを組み込むために、ネームサーバーのファイルを編集する方法を示しています。この管理ファイルの例を参考にして、図 3-1 に示すネットワーク例の IP アドレスおよびホスト名を、実際に使用する IP アドレスおよびホスト名に置き換えてください。

注 – 使用しているネットワーク環境にシステムシャーシを統合する方法を検討するときには、シャーシが 2 つのスイッチを備えていて、各サーバーブレードが各スイッチに対するインタフェースを 1 つずつ持っていることに注意してください。シャーシのアクティブシステムコントローラは常に 1 つだけですが、スイッチは常に両方ともアクティブです。つまり、正常に動作しているシャーシでは、常に両方のスイッチがサーバーブレードにネットワーク接続を提供します。一方のスイッチに障害が発生しても、もう一方のスイッチはネットワーク接続を維持します。

この章では、ブレードの各 Ethernet インタフェースに異なる IP アドレスを設定して、ネットワークの冗長性を利用する方法について説明します。アクティブシステムコントローラに障害が発生した場合でも、障害が発生したシステムコントローラを含む SSC 内のスイッチはネットワーク接続の提供を継続することにも注意してください。

システムシャーシ内の 2 番目のスイッチが提供する冗長性を利用するため、次のように運用することをお勧めします。

- システムシャーシは、常に 2 台の SSC を取り付けた状態で動作させます。
- データネットワークの 8 つのアップリンクポートから広域なネットワークのサブネットへのケーブル接続と、2 番目のスイッチの 8 つのアップリンクポートのケーブル接続を同一にします。
- 最初のスイッチの設定を 2 番目のスイッチにコピーします。実行方法については、A-9 ページの A.9 節「最初のスイッチから 2 番目のスイッチへの設定のコピー」を参照してください。

- DHCP サーバーからシャーシの IP ネットワークを割り当てるように設定している場合は、各サーバーブレードの 2 つの Ethernet インタフェース (ce0 および ce1) に IP アドレスを指定します。
- ネームサーバーの /etc/hosts ファイル (図 3-2 を参照) でシャーシの静的な IP を設定する (DHCP を使用しない) 場合は、各サーバーブレードの 2 つの Ethernet インタフェース (ce0 および ce1) に IP アドレスを指定します。
- 起動サーバーの /etc/ethers ファイルでシャーシの静的な IP を設定する (DHCP を使用しない) 場合は、各サーバーブレードの 2 つの Ethernet インタフェースに MAC および IP アドレスを指定します。
- 各サーバーブレードからシャーシの 2 つの統合スイッチへの冗長インタフェースを最大限に利用するには、IPMP (IP ネットワークマルチパス) を使用する必要があります。詳細は、第 5 章を参照してください。

3.1.1 各ブレードの 2 つの Ethernet インタフェースの MAC アドレスの確認

起動サーバーの /etc/ethers ファイルを設定するときには、各サーバーブレードの ce0 および ce1 の MAC アドレスが必要です。これを確認するには、次の手順を実行します。

1. アクティブシステムコントローラにログインします (第 2 章を参照)。
2. sc> プロンプトで次のように入力します。

```
sc> showplatform -v
```

3. このコマンドの出力に、s0 ～ s15 のラベルの付いた各サーバーブレードの ce0 の MAC アドレスが表示されます。

   ce1 の MAC アドレスは、各サーバーブレードの ce0 の次の番号に相当する 16 進数を計算して求めます。

3.2 DHCP を使用するネットワーク環境の準備

システムシャーシのサーバーブレードおよびシステムコントローラ、スイッチは、DHCP サーバーから直接 IP アドレスを受け取ることができます。

DHCP サーバーからシャーシのスイッチおよびシステムコントローラの IP アドレスを割り当てるように設定する方法については、第 1 章を参照してください。

DHCP サーバーからサーバーブレードの IP アドレスを割り当てるように設定する方法については、付録 C を参照してください。

注 – DHCP を使用してサーバーブレードの IP を設定すると、IPMP を使用してネットワークの回復機能を構成することはできなくなります。

DHCP サーバーから各サーバーブレードの各インタフェースに IP アドレスを割り当てるように設定していることを確認してください。DHCP サーバーで IP の構成パラメタを動的に割り当てる方法については、『Solaris DHCP の管理』(816-1249) を参照してください。このマニュアルは、次のサンのマニュアル Web サイトで入手できます。

`http://docs.sun.com`

動的に割り当てられた IP アドレスに対応するようにネットワークインストールサーバーを設定する方法については、『Solaris のインストール (上級編)』および『Solaris DHCP の管理』(816-1249)、付録 C を参照してください。

3.3 静的 IP アドレスおよびホスト名を使用するネットワーク環境の準備

図 3-1 に、2 台の SSC と 16 台のブレード用のスロットを備えた Sun Fire B1600 ブレードシステムシャーシを示します。システムシャーシの各ブレードの `ce0` インタフェースは、SSC0 のスイッチに接続し、各ブレードの `ce1` インタフェースは、SSC1 のスイッチに接続します。スイッチの 8 つのアップリンクポートの 1 つ以上を、ネットワークインストールサーバーおよびネームサーバーが接続されている外部スイッチに接続します。この外部スイッチには、Sun Fire B1600 ブレードシステムシャーシから広域なネットワークへのデフォルトゲートウェイになるルーター (IP アドレス : 192.168.1.1) を接続します。2 台の SSC の 100 Mbps のネットワーク管理ポート (シャーシの背面の NETMGT のラベルが付いたポート) も外部スイッチに接続します。

システムシャーシに割り当てられた IP アドレスは、すべて同じサブネットに含まれています。

図 3-1 に示すような単純なネットワーク環境にシステムシャーシを組み込むには、Solaris ネームサーバー上にある `/etc/hosts` および `/etc/ethers`、`/etc/netmasks` ファイルを編集する必要があります。

- 図 3-2 は、図 3-1 に示すネットワーク構成の IP アドレスおよびホスト名を含む `/etc/hosts` ファイルの例です。
- 図 3-3 は、図 3-1 に示すネットワーク例の IP ネットワーク番号に対応するネットマスクを含む `/etc/netmasks` ファイルの例です。

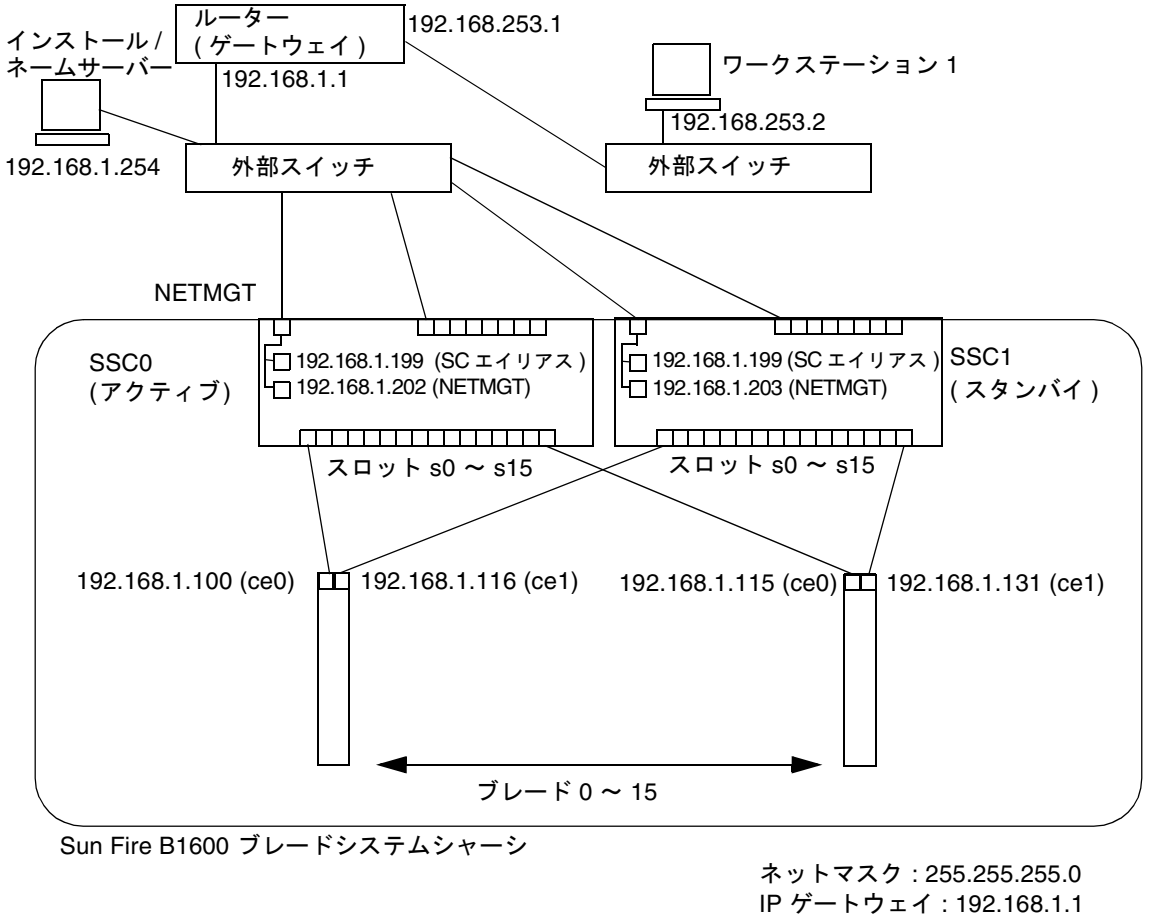

図 3-1　VLAN を使用しない構成の例

```
# Internet host table
127.0.0.1      localhost
192.168.1.254  datanet-nameserver   # Data network name server
192.168.1.1    datanet-router-1     # Data network router (default gateway)
192.168.253.1  datanet-router-253   # Data network router (client side)
192.168.253.2  dataclient-ws1       # Data client network workstation

192.168.1.199   medusa-sc           # Medusa - active SC (alias IP address)
192.168.1.200   medusa-ssc0         # Medusa - SSC0/SC (private IP address)
192.168.1.201   medusa-ssc1         # Medusa - SSC1/SC (private IP address)
192.168.1.202   medusa-swt0         # Medusa - SSC0/SWT
192.168.1.203   medusa-swt1         # Medusa - SSC1/SWT

192.168.1.100   medusa-s0-0
192.168.1.101   medusa-s1-0
192.168.1.102   medusa-s2-0
192.168.1.103   medusa-s3-0
192.168.1.104   medusa-s4-0
192.168.1.105   medusa-s5-0
192.168.1.106   medusa-s6-0
192.168.1.107   medusa-s7-0
192.168.1.108   medusa-s8-0
192.168.1.109   medusa-s9-0
192.168.1.110   medusa-s10-0
192.168.1.111   medusa-s11-0
192.168.1.112   medusa-s12-0
192.168.1.113   medusa-s13-0
192.168.1.114   medusa-s14-0
192.168.1.115   medusa-s15-0
192.168.1.116   medusa-s0-1
192.168.1.117   medusa-s1-1
192.168.1.118   medusa-s2-1
192.168.1.119   medusa-s3-1
192.168.1.120   medusa-s4-1
192.168.1.121   medusa-s5-1
192.168.1.122   medusa-s6-1
192.168.1.123   medusa-s7-1
192.168.1.124   medusa-s8-1
192.168.1.125   medusa-s9-1
192.168.1.126   medusa-s10-1
192.168.1.127   medusa-s11-1
192.168.1.128   medusa-s12-1
192.168.1.129   medusa-s13-1
192.168.1.130   medusa-s14-1
192.168.1.131   medusa-s15-1
```

図 3-2　ネームサーバーの /etc/hosts ファイルの例

```
#
# The netmasks file associates Internet Protocol (IP) address
# masks with IP network numbers.
#
#       network-number  netmask
#
# The term network-number refers to a number obtained from the
# Internet Network Information Center. Currently this number is
# restricted to being a class A, B, or C network number. In the
# future we intend to support arbitrary network numbers
# as described in the Classless Internet Domain Routing
# guidelines.
#
# Both the network-number and the netmasks are specified in
# "decimal dot" notation, e.g:
#
#               128.32.0.0 255.255.255.0
#
192.168.1.0     255.255.255.0
192.168.253.0   255.255.255.0
#
```

図 3-3　ネームサーバーの /etc/netmasks ファイルの例

3.4　システムコントローラおよびスイッチの設定

この節の手順を実行するには、アクティブシステムコントローラ (デフォルトでは SSC0 のシステムコントローラ) へのシリアル接続または telnet 接続が必要です。

システムコントローラへのログイン方法については、第 1 章および第 2 章を参照してください。

システムコントローラへのシリアル接続の設定方法については、『Sun Fire B1600 ブレードシステムシャーシハードウェア設置マニュアル』を参照してください。

アクティブシステムコントローラへの telnet 接続の設定方法については、第 1 章を参照してください。

3.4.1 システムコントローラの設定

注 – アクセスできるのは、アクティブシステムコントローラのコマンド行インタフェースだけです。しかし、この節で説明する `setupsc` コマンドを実行すると、両方のシステムコントローラが設定されます。アクティブシステムコントローラは常に 1 つだけですが、スイッチは常に両方ともアクティブです。

1. **第 2 章の手順に従って、アクティブシステムコントローラにログインします。**
2. **`setupsc` コマンドを実行します。**

   `sc>` プロンプトで次のように入力します。

```
sc> setupsc
Entering Interactive setup mode.
Use Ctrl-z to exit & save. Use Ctrl-c to abort.

Do you want to configure the enabled interfaces [y]?
Should the SC network interface be enabled [y]?
Should the SC telnet interface be enabled for new connections[y]?
Do you want to configure the network interface [y]?
```

   `setupsc` を実行したときに表示される質問に対して、ENTER キーを押してデフォルトの返答を受け入れます。デフォルトの返答は、質問の最後に角括弧で囲んで示されます。`y` は「yes」を、`n` は「no」を意味します。

   最初の 4 つの質問に対して、デフォルトの返答である `y` を受け入れます。

3. **システムコントローラ (SC) のネットワーク構成に DHCP を使用するかどうかの質問が表示されたら、yes または no で答えます。**

   yes と答えた場合は、手順 5 に進みます。

   no と答えた場合はプロンプトが表示されるので、次の情報を順に指定します。

   - SC の IP アドレス (SSC0 または SSC1 にかかわらず、アクティブシステムコントローラが広域なネットワークとの通信に使用する IP アドレス)
   - システムコントローラの IP ネットマスク
   - システムコントローラのデフォルトゲートウェイ

4. **SC のプライベート IP アドレスを設定するかどうかの質問が表示されたら、yes または no で答えます。**

   アクティブシステムコントローラおよびスタンバイシステムコントローラは、両方ともプライベート IP アドレスを持つことができます。プライベート IP アドレスは、それぞれ異なったものを使用する必要があります。また、手順 3 で指定した SC の IP アドレスとも異なっている必要があります。

   システムコントローラにプライベート IP アドレスを指定すると、これらのアドレスを指定して ping を実行することで 2 つのシステムコントローラの健全性を確認できるので便利です。また、アクティブシステムコントローラ用のネットワークアドレスを使用するのと同様に、プライベート IP アドレスを使用して、アクティブシステムコントローラに telnet で接続することもできます。スタンバイシステムコントローラには、プライベート IP アドレスが割り当てられていても、telnet で接続することはできません。

5. **SC の VLAN を使用可能にするかどうかの質問が表示されたら、yes または no で答えます。**

   yes と答えると、システムコントローラの Ethernet ポートは、次の質問に対して指定した VLAN のタグの付いたフレームだけを送受信します。

   a. **プロンプトが表示されたら、管理 VLAN 用の VLAN ID (1 ～ 4094 の数字) を指定します。**

      スイッチの管理 VLAN と同じ番号を使用してください。スイッチの管理 VLAN のデフォルトの番号は 2 です。VLAN 1 はデータネットワークに対する デフォルトの VLAN なので、VLAN 1 を使用することはお勧めしません。

6. **プロンプトが表示されたら、システム管理システム (SMS) の IP アドレスを指定します。**

   ENTER キーを押して次の質問へ進むか、Sun Fire B1600 用の Sun Management Center ソフトウェアまたは Sun SNMP Management Agent が動作するネットワーク管理ホストのアドレスを入力します。

7. **システムを管理するインタフェースを設定するかどうかの質問が表示されたら、yes または no で答えます。**

   yes と答えると、ハングアップしたときにシャーシのコンポーネントを自動的に再起動するかどうかの質問と、サーバーブレードをシャーシに挿入したときに自動的に電源を入れるかどうかの質問が表示されます。

   a. **プロンプトが表示されたら、ハングアップしたときにすべての FRU (2 台の SSC およびすべてのサーバーブレード) を自動的に再起動するかどうかを指定します。**

      no と答えると、プロンプトが表示されて、ハングアップしたときにすべての FRU を自動的に再起動しないように設定するかどうかの質問が表示されます。再び no と答えると、ハングアップしたときの自動的な再起動を、FRU ごとに指定できます。

b. プロンプトが表示されたら、シャーシの電源を入れたとき、または電源の入ったシャーシにブレードを挿入したときに、すべてのサーバーブレードに自動的に電源を入れるかどうかを指定します。

no と答えると、プロンプトが表示されて、シャーシの電源を入れたとき、またはブレードを電源の入ったシャーシのスロットに挿入したときに、すべてのブレードの電源を入れないように設定するかどうかの質問が表示されます。再び no と答えると、シャーシの電源を入れたときまたはブレードをスロットに挿入したときの自動的な電源投入を、ブレードごとに指定できます。

8. システムコントローラのパラメタを設定するかどうかの質問が表示されたら、yes または no で答えます。

yes と答えた場合は、telnet インタフェースを介したイベントレポートおよびシステムコントローラのコマンドプロンプトの設定、システムコントローラのユーザーセッションのアイドル状態のタイムアウト時間、ユーザーがパスワードを入力したときに * 記号を画面に表示するかどうか、システムコントローラが時間情報プロトコル (NTP) を使用するかどうかに関する質問が表示されます。

a. CLI のイベントレポートを使用可能にするかどうかの質問が表示されたら、SSC への telnet 接続を介してイベントレポートを受信する場合は y と入力します。

SSC のシリアル接続を介したイベントレポートを使用不可にすることはできません。

b. 手順 a で y と入力した場合は、表示するイベントのレベルにデフォルトの値を受け入れます。デフォルトでは、重要度レベル 2 以上のイベントが表示されます。

レベル 2 では、MINOR および MAJOR、CRITICAL のイベントが表示されます。

c. システムコントローラのコマンド行プロンプトを指定するか、デフォルトを受け入れます。

d. コマンド行インタフェースのタイムアウト時間を指定します。

デフォルトは 0 で、アイドル状態が続いてもユーザーセッションはタイムアウトしません。

e. ユーザーがパスワードを入力したときに、画面上に * 記号を表示するかどうかを指定します。

f. NTP を使用可能にするかどうかを指定します。

ネットワーク上に時刻サーバーがあって、それを使用する場合は、yes と答えます。プロンプトが表示されたら、一次 NTP サーバーおよび二次 NTP サーバーの IP アドレスを入力します。

9. ネットワークの設定変更をすぐに有効にするかどうかの質問が表示されたら、yes または no で答えます。

この質問は、システムコントローラのネットワーク設定を変更した場合にだけ表示されます。telnet 接続を使用しているシステムコントローラの設定を変更した場合に yes と答えると、telnet 接続が失われることがあります。

10. 3-14 ページの 3.4.3 節「SSC0 および SSC1 のスイッチの設定」の手順に従って、スイッチを設定します。

```
sc> setupsc
Entering Interactive setup mode.
Use Ctrl-z to exit & save. Use Ctrl-c to abort.

Do you want to configure the enabled interfaces [y]?
Should the SC network interface be enabled [y]?
Should the SC telnet interface be enabled for new connections[y]?
Do you want to configure the network interface [y]?
Should the SC use DHCP to obtain its network configuration [n]?
Enter the SC IP address [192.156.203.139]:
Enter the SC IP netmask [255.255.255.0]:
Enter the SC IP gateway [192.168.1.1]:
Do you want to configure the the SC private addresses [y]?
Enter the SSC0/SC IP private address [192.168.1.200]:
Enter the SSC1/SC IP private address [192.168.1.201]:
Do you want to enable a VLAN for the SC [y]?
Enter VLAN ID [2]: 2
Enter the SMS IP address [0.0.0.0]:
Do you want to configure the managed system interface [y]? y
Should all frus be configured to be automatically restarted if hung
[y]?
Should all of the blades be configured to power on automatically [y]?
Do you want to configure the System Controller parameters [y]?
Do you want to enable CLI event reporting via the telnet interface [y]?
Enter the level of events to be displayed over the CLI.
(0 = critical, 1 = major, 2 = minor) [2]:
Enter the CLI prompt [sc>]:
Enter the CLI timeout (0, 60 - 9999 seconds) [0]:
Should the password entry echo *'s [y]?
Do you want to enable NTP [y]?
Enter the IP address of the primary NTP server [192.168.130.26]:
Enter the IP address of the secondary NTP server [192.168.130.26]:
Do you want the network changes to take effect immediately [y]?
sc>
```

図 3-4　　setupsc からの出力および返答の例 (DHCP 構成でない場合)

```
sc> setupsc
Entering Interactive setup mode.
Use Ctrl-z to exit & save. Use Ctrl-c to abort.

Do you want to configure the enabled interfaces [y]?
Should the SC network interface be enabled [y]?
Should the SC telnet interface be enabled for new connections[y]?
Do you want to configure the network interface [y]?
Should the SC use DHCP to obtain its network configuration [n]? y
Do you want to enable a VLAN for the SC [y]?
Enter VLAN ID [2]: 2
Enter the SMS IP address [0.0.0.0]:
Do you want to configure the managed system interface [n]?
Do you want to configure the managed system interface [y]? n
Do you want to configure the System Controller parameters [y]? n
Do you want the network changes to take effect immediately [y]?
sc>
```

図 3-5　setupsc からの出力および返答の例 (DHCP 構成の場合)

3.4.2 システムコントローラの設定の表示

システムコントローラの設定を表示するには、showsc -v コマンドを実行します。システムコントローラの設定可能なすべてのプロパティーが一覧表示されます。

- 次のように入力します。

```
sc> showsc -v
Sun Advanced Lights Out Manager for Blade Servers 1.0
ALOM-B 1.0

Release: 0.2.0, Created: 2003.01.10.11.03

Parameter                                  Running Value      Stored Value
-------------------------------------------------------------------------
Bootable Image:                            0.2.0 (Jan 10 03)
Current Running Image:                     0.2.0 (Jan 10 03)
SC IP address:                              192.156.203.139   129.156.203.139
SC IP netmask address:                     255.255.255.0      255.255.255.0
SC IP gateway address:                     192.168.1.1        192.168.1.1
SSC1/SC (Active) IP private address:       192.168.1.200      192.168.1.200
SSC0/SC (Standby) IP private address:      192.168.1.201      192.168.1.201
SMS IP address:                            0.0.0.0            0.0.0.0
SC VLAN:                                   Disabled           Disabled
SC DHCP:                                   Enabled            Enabled
SC Network interface is:                   Enabled            Enabled
SC Telnet interface is:                    Enabled            Enabled
NTP:                                       Disabled           Disabled
Blade auto restart when hung:
S0                                         Disabled           Disabled
S1                                         Disabled           Disabled
S2                                         Disabled           Disabled
Blade auto poweron:
S0                                         Disabled           Disabled
S1                                         Disabled           Disabled
S2                                         Disabled           Disabled
The CLI prompt is set as:                  sc>                sc>
Event Reporting via telnet interface:      Enabled            Enabled
The CLI event level is set as:             CRITICAL           CRITICAL
The CLI timeout (seconds) is set at:       0                  0
Mask password with *'s:                    Disabled           Disabled

次のページへ続く
```

図 3-6　3 台のブレードを取り付けたシャーシのデフォルトの設定 (showsc -v)

```
FRU   Software Version             Software Release Date
-------------------------------------------------------
S0     v1.1T30-SUNW,Serverblade1    Oct 24 2002 16:22:2
S1     v1.1T30-SUNW,Serverblade1   Oct 24 2002 16:22:24
S2     v1.1T30-SUNW,Serverblade1   Oct 24 2002 16:22:24
S3     Not Present
S4     Not Present
S5     Not Present
S6     Not Present
S7     Not Present
S8     Not Present
S9     Not Present
S10    Not Present
S11    Not Present
S12    Not Present
S13    Not Present
S14    Not Present
S15    Not Present
sc>
```

図 3-7　3 台のブレードを取り付けたシャーシのデフォルトの設定 (前ページの続き)

3.4.3　SSC0 および SSC1 のスイッチの設定

この節では、スイッチの IP アドレスおよびネットマスク、デフォルトゲートウェイを設定する方法について説明します。デフォルトでは、スイッチは DHCP から IP 設定情報を取得します。そのため、DHCP サーバーでスイッチの IP 情報を設定した場合は、この節の手順を省略してください。

1. SSC0 のスイッチにログインするには、次のように入力します。

```
sc> console ssc0/swt
```

2. プロンプトが表示されたら、スイッチのユーザー名およびパスワードを入力します。

3. デフォルトでは、スイッチの IP アドレスおよびネットマスクは DHCP によって設定されます。手動で設定するには、次のように入力します。

```
Console#configure
Console(config)#interface vlan vlan id
Console(config-if)#ip address ip address netmask
Console(config-if)#exit
```

vlan id には、スイッチのネットワーク管理ポートである NETMGT を含む VLAN の番号 (デフォルトのスイッチ設定を使用している場合は 2) を指定します。*ip address* には、使用するスイッチの IP アドレスを指定します。*netmask* には、ネットマスクを指定します。

たとえば、図 3-1 に示す SSC0 のスイッチの IP アドレスおよびネットマスクを指定するには、次のように入力します。

```
Console#configure
Console(config)#interface vlan 2
Console(config-if)#ip address 192.168.1.202 255.255.255.0
Console(config-if)#exit
```

4. デフォルトでは、デフォルトゲートウェイは DHCP によって設定されます。

手動で設定するには、次のように入力します。

```
Console(config)#ip default-gateway ip address
Console(config)#exit
```

ip address には、デフォルトゲートウェイとして指定したデバイスの IP アドレスを指定します。

5. 新しいスイッチの設定を保存します。

スイッチのコンソールで次のように入力します。

```
Console#copy running-config startup-config
Startup configuration file name []:filename
Write to FLASH Programming
-Write to FLASH finish
Success

Console#
```

filename には、新しい起動時の設定を保存するファイルの名前を指定します。

6. **exit と入力して最初のスイッチからログアウトします。**

   次に #. を入力して、スイッチのコマンド行インタフェースを終了し、システムコントローラの sc> プロンプトに戻ります。

7. **A-9 ページの A.9 節「最初のスイッチから 2 番目のスイッチへの設定のコピー」の手順に従って、2 番目のスイッチを設定します。**

   または、SSC1 のスイッチに対しても手順 1 ～手順 6 を実行します。

次の手順

第 4 章の手順に従って、サーバーブレードを設定します。

第4章

サーバーブレードの設定および初期診断の実行

この章では、サーバーブレードの電源投入およびコンソールへのアクセス方法について説明します。また、このマニュアルで説明する Advanced Lights-out Management ソフトウェア以外の、さまざまなツールを使用した予備診断の実行方法についても説明します。

Solaris システムの診断の実行に関する一般的な情報については、『OpenBoot コマンド・リファレンスマニュアル』および『SunVTS ユーザーマニュアル』を参照してください。これらのマニュアルは、Solaris メディアキットに付属するソフトウェアサプリメント CD に収録されています。また、次の Web サイトから入手することもできます。

`http://www.sun.com/documentation`

この章は次の節で構成されています。

注 – ブレードのコンソールでは、**#.** を入力して、アクティブシステムコントローラの `sc>` プロンプトに切り替えます。

4.1 サーバーブレードへの電源投入

出荷時のデフォルトの状態のサーバーブレードに電源を入れると、ブレードは自身のローカルハードディスク上のオペレーティング環境のスタブから自動的に起動します。次に、ブレードはネットワークインストールサーバーを検索し、そこからオペレーティング環境のインストール処理を実行します。

ネットワークインストールサーバーの設定手順については、『Solaris のインストール (上級編)』を参照してください。

Web Start でフラッシュアーカイブを使用して、システムシャーシ内のサーバーブレードの設定にかかる時間を短縮する方法については、このマニュアルの付録 D を参照してください。

準備ができたら、次の手順に従って、サーバーブレードの電源を入れて起動します。

1. **サーバーブレードの電源を入れます。**

   次のように入力します。

```
sc> poweron sn
```

   n には、サーバーブレードが取り付けられているスロット番号を指定します。

2. **サーバーブレードのコンソールにログインし、起動処理を監視するか、起動処理に割り込みます。**

   sc> プロンプトで次のように入力して、ブレードのコンソールにアクセスします。

```
sc> console sn
```

   n には、ブレードが取り付けられているスロット番号を指定します。

   次の作業は、『Solaris のインストール (上級編)』で選択した Solaris のインストール方法によって異なります。

3. **必要な場合は、起動処理に割り込んで、起動処理を制御するか診断を実行します。**

起動処理に割り込む[1]には、次のように入力します。

```
sc> break sn
```

n には、ブレードが取り付けられているスロット番号を指定します。

4. **必要に応じて、この章の以降の手順に従ってサーバーブレードの初期診断を実行します。**

注 – ブレードのコンソールでは、**#.** を入力して、アクティブシステムコントローラの sc> プロンプトに切り替えます。

4.2 電源投入時自己診断 (POST)

この節では、POST 診断処理の制御方法について説明します。デフォルトでは、サーバーブレードの起動時には POST 診断が実行されます。

4.2.1 診断テストのレベルの制御

POST 診断には、3 つのレベルの診断テストがあります。

- max (最高レベル)
- min (最低レベル)
- off (テストなし)

OpenBoot PROM 変数 diag-level を使用して、必要なレベルを設定します。diag-level のデフォルトの設定は min です。レベルを設定するには、次のように入力します。

```
ok diag-level level
```

level には、min または max、off を指定します。

---

1. ブレードを break コマンドを受け入れないように設定する方法については、kbd(1) のマニュアルページを参照してください。

4.2.2 システムコントローラからのブレードの診断設定の上書き

システムコントローラの bootmode コマンドを使用して、diag-level および diag-switch? の設定を一時的に変更することができます。

- **起動時の診断の実行が設定されていない場合に、診断を実行してサーバーブレードを起動するには、次の手順を実行します。**

  a. #. を入力して、システムコントローラのコマンド行インタフェースに切り替えます。

  b. 次のように入力します。

```
sc> bootmode diag sn
```

  n には、設定を変更するブレードが取り付けられているスロット番号を指定します。

  このコマンドを実行すると、次の起動時のみ、diag-switch? を true に設定し、diag-level を min に設定した場合と同じ処理が実行されます。ブレードの diag-level に max または min が設定されている場合は、上記の bootmode コマンドはブレードの設定を変更しません。

- **診断の実行が設定されている場合に、診断を実行せずにサーバーブレードを起動するには、次の手順を実行します。**

  a. #. を入力して、システムコントローラのコマンド行インタフェースに切り替えます。

  b. 次のように入力します。

```
sc> bootmode skip_diag sn
```

  n には、設定を変更するブレードが取り付けられているスロット番号を指定します。

  このコマンドを実行すると、diag-switch? を false に設定した場合と同じ処理が実行されます。

4.2.3 POST 診断の実行

OpenBoot PROM (OBP) 変数の diag-switch? を true に設定すると、サーバーに電源を入れたときに POST 診断が自動的に実行されます。ただし、diag-switch? のデフォルトの設定は false です。

POST 診断を初期化するには、diag-switch? 変数を true に、diag-level を max または min (off でない値) に設定する必要があります。この設定を完了したら、サーバーブレードをリセットしてください。次の手順を実行します。

1. サーバーブレードの ok プロンプトで、次のように入力します。

```
ok setenv diag-switch? true
```

2. #. を入力して、システムコントローラのコマンド行インタフェースに切り替えます。

3. サーバーブレードの電源を入れ直します。

   次のように入力します。

```
sc> poweroff sn
```

   n には、ブレードのスロット番号を指定します。

   続けて次のように入力します。

```
sc> poweron sn
```

4. ブレードの電源を入れてから、可能であれば 2 ～ 3 秒以内にブレードのコンソールにアクセスして診断の出力を参照します。

   次のように入力します。

```
sc> console sn
```

5. 起動が完了したときに起動時のコンソール出力を確認するには、#. を入力してシステムコントローラのコマンド行インタフェースに切り替え、次のように入力します。

```
sc> consolehistory boot sn
```

   POST は、エラーを検出すると、障害を説明するエラーメッセージを表示します。

POST は、「重大な」エラー (オンボードメモリーまたは CPU に関するハードウェア障害など) を検出した場合には、サーバーブレードの電源を切って、ブレードの障害 LED を点灯させます。

4.3 OpenBoot 診断 (obdiag) の使用

OpenBoot 診断を実行するには、次の手順を実行します。

1. ok プロンプトから、次のように入力します。

```
ok setenv auto-boot? false
ok reset-all
```

2. 次のように入力します。

```
ok obdiag
```

OpenBoot 診断メニューが表示されます。

```
                                obdiag
1 bscv@0,0              2 ide@d                 3 network@a
4 network@b             5 ide@d                 6 rtc@0,70
7 serial@0,3f8

       Commands: test test-all except help what setenv exit

              diag-passes=1 diag-level=max test-args=
```

図 4-1 obdiag メニュー

表 4-1 に、テストの説明を示します。実行するテストに対応する番号を書き留めて、test コマンドでその番号を指定してください。たとえば、一次 Ethernet ポートのテストを実行するには、次のように入力します。

```
obdiag> test 3
Hit the spacebar to interrupt testing
Testing /pci@1f,0/network@a ..........................passed
Pass:1 (of 1) Errors:0 (of 0) Tests Failed:0 Elapsed Time: 0:0:0:2

Hit any key to return to the main menu.
```

3. テストが完了したら、OpenBoot 診断を終了して、auto-boot? を true に戻します。

次のように入力します。

```
obdiag> exit
ok setenv auto-boot? true
ok auto-boot? true
ok boot
```

次に、各テストの機能を示します。

表 4-1　OpenBoot 診断テスト

1	bscv@0,0	ブレードサポートチップをテストします。
2	ide@d	IDE コントローラをテストします。
3	network@a	一次 Ethernet インタフェースをテストします。
4	network@b	二次 Ethernet インタフェースをテストします。
5	pmu@3	電源管理装置をテストします。
6	rtc@0,70	リアルタイムクロック装置をテストします。
7	serial@0,3f8	システムコントローラのシリアルインタフェースをテストします。

4.4 その他の OpenBoot PROM コマンドの使用

この節では、実行できる OpenBoot PROM コマンドと、各コマンドの機能について説明します。

show-devs コマンド

OpenBoot PROM の show-devs コマンドを使用すると、OBP デバイスツリー上の装置を一覧表示できます。

printenv コマンド

OpenBoot PROM の printenv コマンドを使用すると、システムの NVRAM に格納されている OpenBoot PROM 構成変数を表示できます。この表示には、構成変数の現在の値とともにデフォルト値が示されます。構成変数を指定して、その構成変数の現在の値だけを表示することもできます。たとえば、printenv diag-level を実行すると、diag-level 変数の現在の値が出力されます。

watch-clock コマンド

watch-clock コマンドは、1 秒ごとに増分される数値を表示します。通常の運用時には、秒カウンタは 0 ～ 59 の間で増分を繰り返します。次に、watch-clock コマンドの出力例を示します。

```
ok watch-clock
Watching the 'seconds' register of the real time clock chip.
It should be 'ticking' once a second.
Type any key to stop.
4
```

watch-net および watch-net-all コマンド

watch-net および watch-net-all コマンドは、ブレードの Ethernet インタフェース上の Ethernet パケットを監視します。正常なパケットを受信すると、ピリオド (.) が表示されます。フレームエラー、巡回冗長検査 (CRC) エラーなどのエラーがあった場合は、X とエラーに関連する説明が表示されます。

次に、watch-net および watch-net-all コマンドの出力例を示します。

```
ok watch-net
1000 Mbps FDXLink up
Link is -- up
Looking for Ethernet Packets.
'.' is a Good Packet. 'X' is a Bad Packet.
Type any key to stop.
.............................
ok
```

```
ok watch-net-all
/pci@1f,0/network@b
1000 Mbps FDXLink up
Link is -- up
Looking for Ethernet Packets.
'.' is a Good Packet. 'X' is a Bad Packet.
Type any key to stop.
.............................
/pci@1f,0/network@a
1000 Mbps FDXLink up
Link is -- up
Looking for Ethernet Packets.
'.' is a Good Packet. 'X' is a Bad Packet.
Type any key to stop.
.............................
ok
```

probe-ide コマンド

probe-ide コマンドを実行すると、ブレードの IDE コントローラは 4 つの IDE 装置に問い合わせを送信しますが、実際には IDE コントローラに接続されている装置は 1 つだけです。一次マスターデバイスに「not present」と表示された場合には、ハードディスクか、IDE コントローラからハードディスクへの接続に問題があります。

図 4-2 probe-ide の出力メッセージ

```
ok probe-ide
 Device 0  ( Primary Master )
           ATA Model: TOSHIBA MK3019GAB

 Device 1  ( Primary Slave )
      Not Present

 Device 2  ( Secondary Master )
      Not Present

 Device 3  ( Secondary Slave )
      Not Present
```

4.5 SunVTS の使用

SunVTS (Sun Validation and Test Suite) は、ハードウェアコントローラや装置、プラットフォームの設定および機能に問題がないかどうかを検査するためのオンライン診断ツールです。SunVTS は、Software Supplement for the Solaris Operating Environment CD に含まれています。

SunVTS は、Solaris プロンプトから、次のいずれかの方法で実行します。

- コマンド行インタフェース
- ウィンドウ化されたデスクトップ環境でのグラフィカルインタフェース

SunVTS ソフトウェアによって、遠隔接続されたサーバーのテストセッションの表示および制御が可能になります。SunVTS には、次の表に示すようなテストがあります。

表 4-2　SunVTS テスト

SunVTS テスト	説明
disktest	ローカルディスクドライブを検査します。
fputest	浮動小数点ユニットを検査します。
nettest	システムの CPU ボード上、およびシステムに取り付けられたネットワークアダプタ上のネットワーク関連ハードウェアを検査します。
pmem	物理メモリーをテストします (読み取りのみ)。
vmem	仮想メモリー (スワップパーティションと物理メモリーの組み合わせ) をテストします。
bsctest	サーバーブレード上のブレードサポートチップをテストします。

4.5.1　SunVTS がインストールされていることの確認

SunVTS がサーバーブレードにインストールされているかどうかを確認するには、次のように入力します。

```
# pkginfo -l SUNWvts
```

- SunVTS ソフトウェアがインストールされている場合は、パッケージに関する情報が表示されます。
- SunVTS ソフトウェアがインストールされていない場合は、次のエラーメッセージが表示されます。

```
ERROR: information for "SUNWvts" was not found
```

4.5.2　SunVTS のインストール

SunVTS は、Software Supplement for the Solaris Operating Environment CD に含まれています。SunVTS をインストールする方法については、『Sun ハードウェアマニュアル』を参照してください。SunVTS ソフトウェアをインストールするときにデフォルトで使用されるディレクトリは /opt/SUNWvts です。

4.5.3 SunVTS の実行

SunVTS のグラフィカルユーザーインタフェースを使用してワークステーションから SunVTS セッションを実行し、Sun Fire B100s サーバーブレードをテストするには、次の手順を実行します。

1. **ワークステーションで `xhost` コマンドを使用して、ローカルのディスプレイからサーバーブレードにアクセスします。**

   次のように入力します。

```
# /usr/openwin/bin/xhost + remote_hostname
```

   remote_hostname には、サーバーブレードのホスト名を指定します。

2. **スーパーユーザーまたは root で、サーバーブレードに遠隔ログインします。**

3. **次のように入力します。**

```
# cd /opt/SUNWvts/bin
# ./sunvts -display local_hostname:0
```

   local_hostname には、使用しているワークステーションの名前を指定します。

注 – ディレクトリ `/opt/SUNWvts/bin` は、SunVTS ソフトウェアのデフォルトのディレクトリです。SunVTS ソフトウェアを別のディレクトリにインストールした場合は、そのパスを指定してください。

SunVTS ソフトウェアを起動すると、SunVTS カーネルがテスト対象のシステム装置をプローブし、その結果をテスト選択パネルに表示します。システム上のハードウェア装置のそれぞれに、関連する SunVTS テストがあります。

実行する各テストに適したチェックボックスを選択することで、テストセッションを調整できます。

第5章

システムシャーシのデータ用と管理用に分離されたネットワークへの接続

この章は次の節で構成されています。

5.1 システムシャーシの 2 つのスイッチの利用

この章では、Sun Fire B1600 ブレードシステムシャーシを、データネットワークと管理ネットワークを分離した環境で使用する方法について説明します。この章の手順を実行すると、システムシャーシの 2 つのスイッチを利用して、各サーバーブレードがネットワークに 2 つの接続を確立できます。

図 5-1 に、Sun Fire B1600 ブレードシステムシャーシを含むネットワークの例を示します。以降の手順では、この図および図に記された IP アドレスを使用します。

また、この章では、`/etc/hosts` ファイルの例と `/etc/netmasks` ファイルの例も示します。この例は、システムシャーシに取り付けられたサーバーブレードの Solaris の設定 (この章の後半で説明) を容易にするために、ネームサーバーのファイルを編集する方法を示しています。この管理ファイルの例を参考にして、図 5-1 に示すネットワーク例の IP アドレスおよびホスト名を、実際に使用する IP アドレスおよびホスト名に置き換えてください。

注 – 第 3 章の注にも示しましたが、使用しているネットワーク環境にシステムシャーシを統合する方法を検討するときには、Sun Fire B1600 ブレードシステムシャーシが 2 つのスイッチを備えていることに注意してください。シャーシのアクティブシステムコントローラは常に 1 つだけですが、スイッチは常に両方ともアクティブです。つまり、正常に動作しているシャーシでは、常に両方のスイッチがサーバーブレードにネットワーク接続を提供します。何らかの理由で一方のスイッチに障害が発生しても、もう一方のスイッチはネットワーク接続を継続します。また、いずれかのシステムコントローラに障害が発生した場合でも、障害が発生したシステムコントローラを含む SSC モジュール内のスイッチはネットワーク接続を継続します。スイッチとシステムコントローラは物理的には同じ格納装置内にありますが、スイッチはシステムコントローラから独立して動作します。

この章では、IPMP (IP ネットワークマルチパス) と VLAN を組み合わせて 2 つのスイッチを利用し、ブレードからデータネットワークおよび管理ネットワークへの完全な冗長接続を確立する構成方法について説明します。

システムシャーシ内の 2 番目のスイッチが提供する冗長性を利用するため、次のように運用することをお勧めします。

- システムシャーシは、常に 2 台の SSC を取り付けた状態で動作させます。
- 8 つのアップリンクポートから広域なネットワークのサブネットへのケーブル接続と、2 番目のスイッチの 8 つのアップリンクポートのケーブル接続を同一にします。

- 最初のスイッチの構成ファイルを冗長スイッチにコピーしてから、冗長スイッチの IP アドレスおよびネットマスク、デフォルトゲートウェイを設定します。コピーする方法については、A-9 ページの A.9 節「最初のスイッチから 2 番目のスイッチへの設定のコピー」を参照してください。
- ネームサーバーの `/etc/hosts` ファイルで、IPMP (IP ネットワークマルチパス) 構成に対応する IP アドレスを指定します (図 5-2 を参照)。IPMP は、各サーバーブレードからデータネットワークおよび管理ネットワークへの冗長インタフェースをサポートします。図 5-2 のブレードの IP アドレスの数は、第 3 章の `/etc/hosts` ファイルの例 (図 3-2) よりも少なくなっています。これは、IPMP を使用すると、各サーバーブレードに必要な公開インタフェースが 1 つだけになるためです。
- ネームサーバーの `/etc/ethers` ファイルを設定する場合は、各サーバーブレードの 2 つの Ethernet インタフェースに MAC および IP アドレスを指定します。

5.2 DHCP を使用するネットワーク環境の準備

注 – DHCP を使用して各サーバーブレードの 2 つのインタフェースの IP を設定すると、IPMP を使用して物理ネットワークへの冗長接続または VLAN への複数接続を構成することはできなくなります。

DHCP を使用する場合は、システムコントローラおよびスイッチ用の DHCP サーバーが管理ネットワーク上に存在し、ブレード用の DHCP サーバーがデータネットワーク上に存在する必要があります。

ネットワークインストールサーバーおよび DHCP サーバーの設定については、第 1 章および第 3 章、付録 C を参照してください。

5.3 静的 IP アドレスを使用するネットワーク環境の準備

図 5-1 のネットワーク構成は、前述の章の構成例に類似していますが、2 台の SSC の 100 Mbps ネットワーク管理ポート (NETMGT) がデータアップリンクポートとは別のスイッチに接続している点が異なります。この新しい外部スイッチは、シャーシのデータアップリンクポートが接続されているスイッチとは別のサブネットに含まれています。このサブネットはネットワーク管理トラフィック専用なので、シャーシのシステムコントローラおよびスイッチもこのサブネットに含まれます。管理 VLAN (VLAN 2) には、システムコントローラのインタフェースと 2 つのスイッチの管理ポートが含まれます。すべてのサーバーブレードとアップリンクポートは、VLAN 1 上にあります。

図 5-1 には、各ブレードの `ce0` インタフェースから SSC0 のスイッチへの接続と、各ブレードの `ce1` インタフェースから SSC1 のスイッチへの接続も示します。この図では、各サーバーブレードのインタフェースに、1 個ではなく 4 個の IP アドレスが割り当てられていることに注意してください。これら 4 個のアドレスは IPMP ドライバが使用するもので、インタフェースに冗長接続の機能を与えます (5-9 ページの 5.5 節「ネットワーク回復のために IPMP を使用するサーバーブレードの設定」を参照)。

図 3-1 (第 3 章を参照) と同様に、図 5-1 の各スイッチの 8 つのアップリンクポートの 1 つ以上を、インストールサーバーおよびネームサーバーが接続されている外部スイッチに接続します。この外部スイッチには、Sun Fire B1600 ブレードシステムシャーシから広域なネットワークへのデフォルトゲートウェイになるルーター (IP アドレス : 192.168.1.1) も接続します。

注 – 図 5-1 に、スイッチの管理ポート (NETMGT) からサーバーブレードポートへの直接的なネットワーク接続が示されていないことに注意してください。これは、デフォルトでは、管理ネットワークからサーバーブレードを直接管理することはできないことを意味します。データネットワークから不正な攻撃を受ける可能性を考慮した、管理ネットワークを保護するためのセキュリティー機能です。サーバーブレードから管理ポートへの特定のトラフィックを許可する方法については、第 6 章および付録 A を参照してください。

図 5-1 のようなデータネットワークと管理ネットワークが分離された環境に Sun Fire B1600 ブレードシステムシャーシを組み込むには、先にデータネットワークおよび管理ネットワーク上で使用している Solaris ネームサーバーの `/etc/hosts` および `/etc/ethers`、`/etc/netmasks` ファイルを編集する必要があります。

- 図 5-2 は、図 5-1 に示す環境のデータネットワーク上にあるブレードシステムシャーシの IP アドレスおよびホスト名を含む `/etc/hosts` ファイルの例です。

- 図 5-2 は、図 5-1 に示す管理ネットワーク上にあるシステムシャーシのコンポーネント (2 台の SSC およびスイッチ) の IP アドレスおよびホスト名を含む `/etc/hosts` ファイルの例です。
- 図 5-3 は、図 5-1 に示すネットワーク例の IP ネットワーク番号に対応するネットマスクを含む `/etc/netmasks` ファイルの例です。

注 – ネームサーバーの `/etc/hosts` ファイルに登録する必要があるのは、IPMP が使用するテスト IP アドレスではなく、各サーバーブレードの公開 IP アドレスだけです。ただし、各ブレードのテストアドレスが予約済みであることをコメントに明示して、ほかのネットワーク管理者にそのアドレスを使用できないことを知らせる必要があります (図 5-2 を参照)。

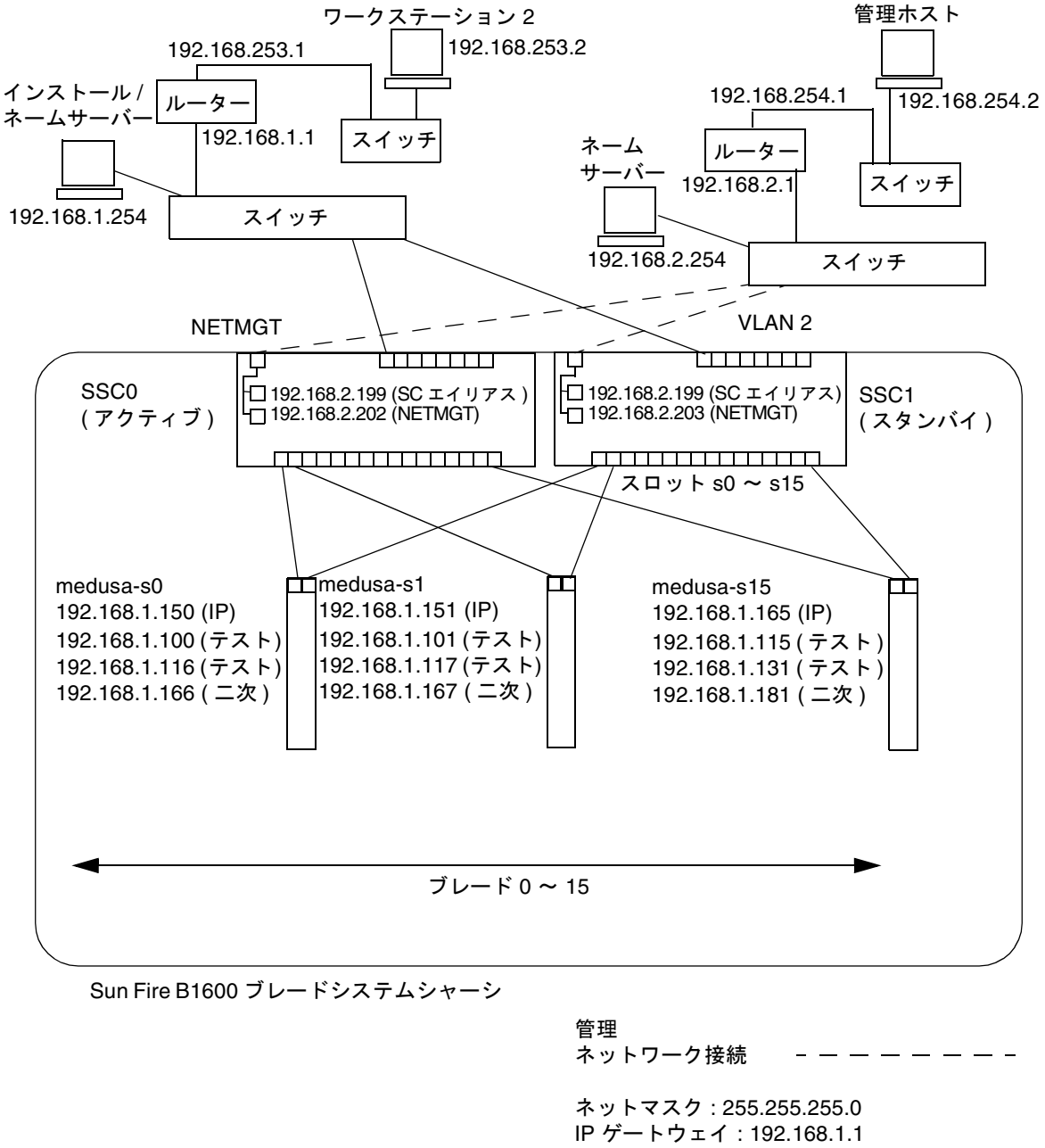

図 5-1　管理 VLAN を使用したネットワーク構成の例

```
# Internet host table

127.0.0.1       localhost

192.168.1.254   datanet-nameserver    # loghost
192.168.1.1     datanet-router-1      # Data network router
                                      # (default gateway)
192.168.2.199   medusa-sc             # Medusa - alias address for active SC

192.168.253.1   datanet-router-253    # Data network router (client side)
192.168.253.2   dataclient-ws1        # Data client network workstation

# 192.168.1.100 -> 192.168.1.131 are reserved for private use by the
# Sun Fire B1600 Blade System Chassis called Medusa. They are test addresses for
# the IPMP driver on each server blade.
#
# Published IP addresses for server blades in Medusa.
192.168.1.150   medusa-s0
192.168.1.151   medusa-s1
192.168.1.152   medusa-s2
192.168.1.153   medusa-s3
192.168.1.154   medusa-s4
192.168.1.155   medusa-s5
192.168.1.156   medusa-s6
192.168.1.157   medusa-s7
192.168.1.158   medusa-s8
192.168.1.159   medusa-s9
192.168.1.160   medusa-s10
192.168.1.161   medusa-s11
192.168.1.162   medusa-s12
192.168.1.163   medusa-s13
192.168.1.164   medusa-s14
192.168.1.165   medusa-s15
```

図 5-2　ネームサーバーの `/etc/hosts` ファイルの例 (データネットワーク)

```
#
# The netmasks file associates Internet Protocol (IP) address
# masks with IP network numbers.
#
#       network-number  netmask
#
# The term network-number refers to a number obtained from the
# Internet Network Information Center. Currently this number is
# restricted to being a class A, B, or C network number.
#
# Routing guidelines.
#
# Both the network-number and the netmasks are specified in
# "decimal dot" notation, e.g:
#
#               128.32.0.0 255.255.255.0
#
192.168.1.0     255.255.255.0

192.168.2.0     255.255.255.0
192.168.253.0   255.255.255.0
```

図 5-3　ネームサーバーの /etc/netmasks ファイルの例 (データネットワーク)

5.4　システムコントローラおよびスイッチの設定

図 5-1 のシステムコントローラおよびスイッチを設定する方法については、3-7 ページの 3.4 節「システムコントローラおよびスイッチの設定」を参照してください。ただし、システムコントローラおよびスイッチに割り当てる IP アドレスは、管理サブネットに含める必要があることに注意してください。

5.5 ネットワーク回復のために IPMP を使用するサーバーブレードの設定

この節では、各サーバーブレードからシャーシのスイッチへの冗長接続を利用するために、Solaris IPMP (IP ネットワークマルチパス) 機能を設定する方法について説明します。サーバーブレードの 2 つの 1000 Mbps Ethernet インタフェースには、それぞれ `ce0` および `ce1` のラベルが付いています。`ce0` は SSC0 のスイッチに接続し、`ce1` は SSC1 のスイッチに接続します。Sun Fire B1600 ブレードシステムシャーシが完全に動作している場合は、常に両方のスイッチがアクティブになっています。

サーバーブレードの IPMP ドライバは、両方の Ethernet インタフェースからデフォルトゲートウェイに定期的に ping を実行します。何らかの理由で ping が失敗し、ping を実行するのに使用したインタフェースでネットワークへのパスが無効になったことが示された場合、IPMP ドライバは、有効なインタフェースだけを使用してネットワークトラフィックを送信するように対処します。両方のインタフェースをアクティブにすることもできますが、この場合は別々の IP アドレスが必要です。また、一方をスタンバイインタフェースにして、アクティブなインタフェースに障害が発生した場合にその IP アドレスを引き継ぐこともできます。

アクティブ/アクティブ構成のインタフェースには、各インタフェースに 1 個の IP アドレスと 1 個のテストアドレスの、合計 4 個の IP アドレスが必要です。アクティブ/スタンバイ構成のインタフェースには、3 個の IP アドレスが必要です。いずれの構成でも、IPMP が ping 処理を実行するため、2 個のテストアドレスが非公開に使用されます。一方のインタフェースのテストアドレスに対する ping に応答がない場合には、IPMP はインタフェースに障害が発生したと認識して、すべてのデータトラフィックを有効なインタフェースに送信します。アクティブ/アクティブ構成の場合は、無効なインタフェースの使用を停止するだけです。アクティブ/スタンバイ構成で、アクティブなインタフェースが無効になった場合は、スタンバイインタフェースに IP アドレスが割り当てられて、スタンバイインタフェースがアクティブインタフェースになります。

シャーシが正常に動作しているときにはシャーシのスイッチは両方ともアクティブなので、この章ではアクティブ/アクティブ構成の実行手順について説明します。アクティブ/スタンバイ構成の設定手順については、『IP ネットワークマルチパスの管理』(816-1250) を参照してください。

ブレードの各物理インタフェースに必要な IP アドレスは、次のとおりです。

- 一次 IP アドレス
- 二次 IP アドレス (アクティブ/アクティブ構成の場合にだけ必要)

  一次および二次 IP アドレスは、どちらもネームサーバーに登録できます。このアドレスは、ネットワーク上のほかの装置とブレードとの通信に使用します。

- 前述の ping 処理を行うには、IP アドレスが 2 個 (各インタフェースに 1 個) 必要です。このマニュアルでは、この 2 個のアドレスを「テスト」アドレスと呼びます。テストアドレスは、IPMP ドライバ以外には公開しません (ネームサーバーに登録しません)。

この章では、2 つの物理インタフェースに対して IPMP を設定する方法について説明します。次の章では、仮想 IPMP インタフェースの複数の組を設定し、各組によって別々の VLAN への冗長インタフェースを提供する方法について説明します。

5.5.1 サーバーブレードの設定

この節では、サーバーブレードの IPMP を構成して、2 つの Ethernet インタフェースでデータの送受信を行う方法について説明します。手順を理解しやすくするために、ここでは 5-4 ページの 5.3 節「静的 IP アドレスを使用するネットワーク環境の準備」に示すネットワーク構成の例を使用します。

表 5-1 に、図 5-1 のシステムシャーシのスロット 0 に取り付けたサーバーブレードの IPMP ドライバに設定する必要のある情報を示します。

注 – この節の手順は、ネットワークへの冗長接続が必要なサーバーブレードごとに実行する必要があります。

表 5-1 サーバーブレードの IPMP 設定の例

IPMP 構成変数	スロット 0 のサーバーブレードの値の例
ネットワークアダプタインタフェース	ce0 (アクティブ) ce1 (アクティブ)
インタフェースグループ名	medusa_grp0
IP アドレスおよびホスト名 (一次)	192.168.1.150 (medusa-s0)
二次 IP アドレスおよびホスト名 (二次)	192.168.1.166 (medusa-s0-sec)
テスト IP アドレスおよびホスト名 (ce0)	192.168.1.100 (medusa-s0-0)
テスト IP アドレスおよびホスト名 (ce1)	192.168.1.116 (medusa-s0-1)
ネットマスク	255.255.255.0
サーバーブレードによるネットワークルーティングの実行	実行しない

1. 第 3 章の手順に従って、Solaris の準備設定を実行します。

   この設定を実行したら、サーバーブレードのコンソールから **#.** を入力して sc> プロンプトに戻ります。

2. スーパーユーザーで、インタフェースを設定するサーバーブレードのコンソールにログインします。

   sc> プロンプトで、次のように入力します。

```
sc> console sn
```

   n には、ログインするサーバーブレードが取り付けられているスロット番号を指定します。

3. サーバーブレードの /etc/hosts ファイルを編集して、ブレードの 2 個のテスト IP アドレスを追加します。

   表 5-1 のアドレスの例を使用するブレードでは、次に示すファイルの例の最後の 2 行を追加する必要があります。

```
#
# /etc/hosts on the server blade in system chassis Medusa, slot 0
#
127.0.0.1       localhost       loghost

192.168.1.150   medusa-s0       # Data Address
192.168.1.166   medusa-s0-sec   # Secondary Data Address
192.168.1.100   medusa-s0-0     # Test Address for ce0
192.168.1.116   medusa-s0-1     # Test Address for ce1
```

4. サーバーブレードの /etc/netmasks ファイルにネットマスクを設定します。

   表 5-1 のアドレスの例を使用するブレードでは、次の行を追加する必要があります。

```
192.168.1.0     255.255.255.0
```

5. サーバーブレードはルーティングの実行には使用しないため、ルーティングを使用不可にします。

   次のように入力します。

```
# touch /etc/notrouter
# ndd -set /dev/ip ip_forwarding 0
```

6. 次のように入力して、ネットワークインタフェースを作成します。

```
# ifconfig ce0 plumb
# ifconfig ce1 plumb
```

7. medusa_grp0 という名前の IPMP グループを作成して、ネットワークインタフェース ce0 および ce1 を含めます。

```
# ifconfig ce0 group medusa_grp0
# ifconfig ce1 group medusa_grp0
```

このコマンドを実行したとき、次の syslog メッセージが表示されることがあります。

```
Sep  3 00:49:58 medusa-s0 in.mpathd[298]: Failures cannot be
detected on ce0 as no IFF_NOFAILOVER address is available
```

このメッセージは、インタフェースのテストアドレスが確立されるまでは障害が検出されないことを単に警告するものです。

8. ce0 および ce1 にデータ転送用のアドレスを作成し、インタフェースの障害が検出された場合にフェイルオーバーを実行するように指定します。

```
# ifconfig ce0 medusa-s0 netmask + broadcast + failover up
Setting netmask of ce0 to 255.255.255.0

# ifconfig ce1 medusa-s0-sec netmask + broadcast + failover up
Setting netmask of ce1 to 255.255.255.0
```

9. 各ネットワークインタフェースのテストアドレスを設定します。

このアドレスは、mpathd がインタフェースの障害を検出するために使用するものです。-failover フラグの指定が必要です。このフラグによって、in.mpathd がこのアドレスをテストアドレス (ほかのインタフェースに渡すことができないため、フェイルオーバーしないアドレス) として使用するようになります。

```
# ifconfig ce0 addif medusa-s0-0 netmask + broadcast + -failover
deprecated up
Created new logical interface ce0:1
Setting netmask of ce0:1 to 255.255.255.0

# ifconfig ce1 addif medusa-s0-1 netmask + broadcast + -failover
deprecated up
Created new logical interface ce1:1
Setting netmask of ce1:1 to 255.255.255.0
```

10. **再起動しても新しいインタフェース設定が消えないように、/etc ディレクトリに hostname.ce0 ファイルおよび hostname.ce1 ファイルを作成します。**

hostname.ce0 ファイルの例は、次のとおりです。

```
medusa-s0 netmask + broadcast + \
group medusa_grp0 up \
addif medusa-s0-0 deprecated -failover \
netmask + broadcast + up
```

hostname.ce1 ファイルの例は、次のとおりです。

```
medusa-s0-sec netmask + broadcast + \
group medusa_grp0 up \
addif medusa-s0-1 deprecated -failover \
netmask + broadcast + up
```

11. **2 つのネットワークアダプタの設定を確認します。**

次のように入力します。

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
ce0: flags=9040843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.1.150 netmask ffffff00 broadcast 192.168.1.255
        groupname medusa_grp0
        ether 0:3:ba:19:26:3
ce0:1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4, NOFAILOVER> mtu 1500 index 2
        inet 192.168.1.100 netmask ffffff00 broadcast 192.168.1.255
ce1: flags=9040843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
        inet 192.168.1.166 netmask ffffff00 broadcast 192.168.1.255
        groupname medusa_grp0
        ether 0:3:ba:19:26:4
ce1:1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4, NOFAILOVER> mtu 1500 index 3
        inet 192.168.1.116 netmask ffffff00 broadcast 192.168.1.255
```

この出力は、4 個のアドレス (表 5-1 のアドレスの例) が定義されていることを示しています。ce0:1 および ce1:1 に対応する IPMP テストアドレスには、NOFAILOVER と記されています。これは、障害が発生した場合に、障害の発生していないインタフェースへの転送が行われないことを意味します。

12. シャーシから 1 台の SSC を一時的に取り外して、IPMP をテストします。

この操作によって、コンソール上に次のエラーメッセージが表示されます。

```
Sep 3 01:08:50 medusa-s0 in.mpathd[29]: NIC failure detected on
ce0 of group medusa_grp0
Sep 3 01:08:50 medusa-s0 in.mpathd[29]: Successfully failed over
from NIC ce0 to NIC ce1
```

注 – デフォルトの設定では、IPMP デーモンがネットワーク障害を検出してから回復するまでに約 10 秒かかります。IPMP デーモンの設定は、`/etc/default/mpathd` ファイルに定義されています。

第6章

ブレードの管理および VLAN タグの追加

この章では、管理ネットワークからサーバーブレードを安全に管理できるようにシステムシャーシを設定する方法について説明します。

この章は次の節で構成されています。

6.1 概要

この章では、第 5 章の設定を調整して、セキュリティーレベルを低下させることなく、ネットワーク管理者が管理ネットワーク (telnet によるサーバーブレードへの直接接続) からサーバーブレードの管理作業を実行できるように設定する方法について説明します。

図 6-1 には、シャーシのスイッチのサーバーブレードポートから管理ポート (NETMGT) への点線が示されています。また、サーバーブレードから各スイッチの管理ポートへも点線が示されています。これらの点線は、管理 VLAN (VLAN 2) のメンバーであるコンポーネントまたはデバイス間のリンクを表します。デフォルトの VLAN 2 には、スイッチの管理ポート (NETMGT) は含まれていますが、サーバーブレードポートは含まれていません。そのため、図 6-1 のようなネットワーク環境に対応するようにシャーシを設定するには、サーバーブレードポートを手動で再設定する必要があります。ポートを手動で再設定する方法については、6-5 ページの 6.3 節「システムコントローラおよびスイッチの設定」を参照してください。

また、デフォルトでは、ネットワークトラフィックは、サーバーブレードポートからスイッチのパケットフィルタを通過して管理ポートに到達することはできません。これはセキュリティーのための機能なので、スイッチを設定してトラフィックのパケットフィルタの通過を許可するときには、十分に注意する必要があります。特定のプロトコルだけがパケットフィルタを通過できるように設定する方法については、A-15 ページの A.11 節「スイッチのパケットフィルタを使用したブレードの安全な管理」を参照してください。

この章の手順では、管理ネットワーク (VLAN 2) にサーバーブレードを接続する方法について説明するとともに、各ブレードがデータネットワークへの冗長接続 (第 5 章を参照) だけでなく管理ネットワーク (VLAN 2) への冗長接続も確立するように、サーバーブレードの IPMP 設定を変更する方法について説明します。

6.2 ネットワーク環境の準備

この節では、第 5 章の構成図に、概要の節で説明した設定の拡張と、各ブレードから管理ネットワークへの冗長接続を確立するために必要な IPMP 情報の例を追加した図を示します。また、管理ネットワーク上のネームサーバーの `/etc/hosts` ファイルの例も示します。データネットワークの管理ファイルは、第 5 章と同じです。ただし、管理ネットワークのネームサーバーの `/etc/hosts` ファイルには、シャーシの 2 つの SSC およびスイッチに対する IP アドレスだけでなく、各サーバーブレードの管理サブネットの IP アドレスを含める必要があります (図 6-2)。

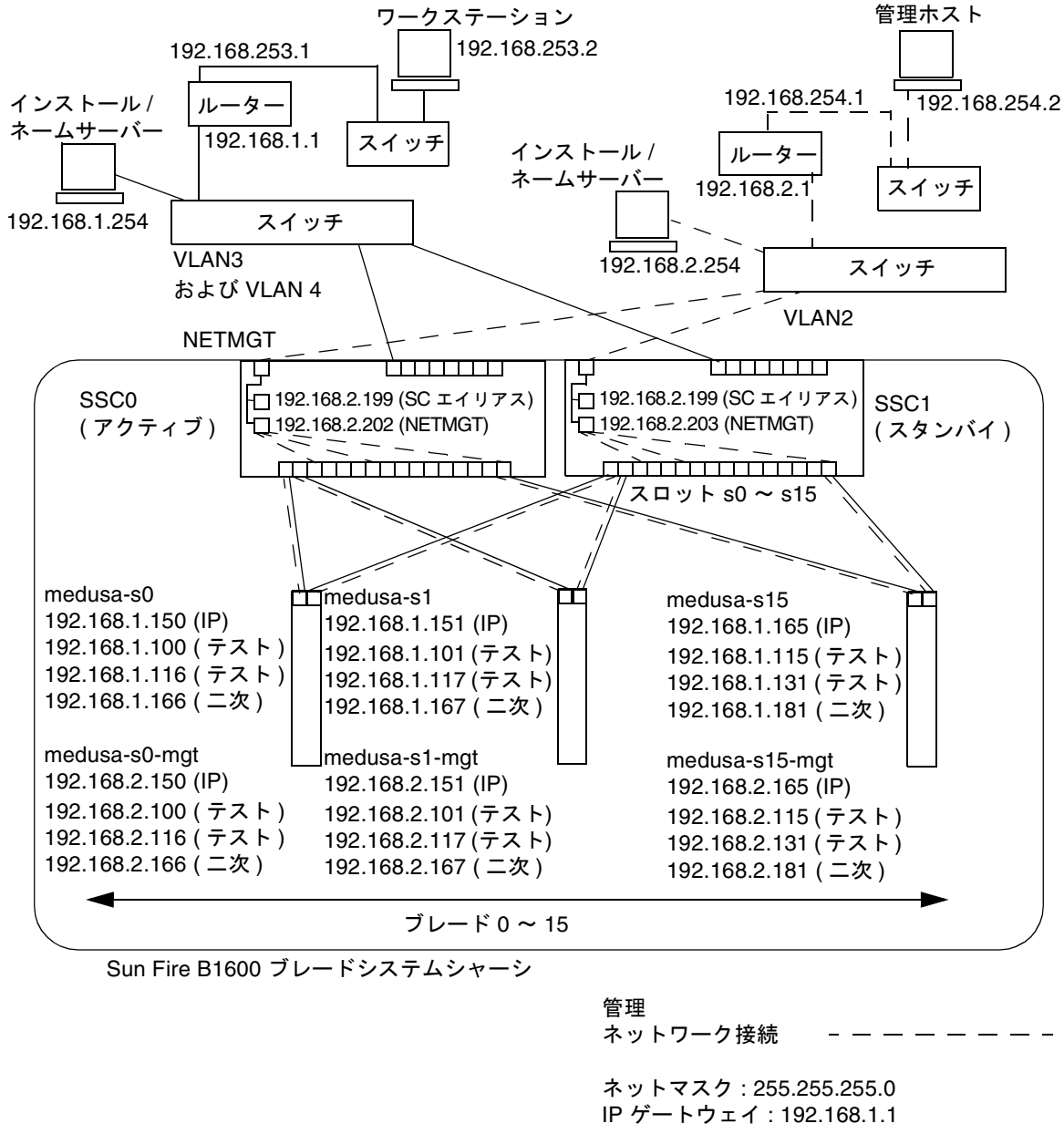

図 6-1　サーバーブレードを含む管理 VLAN を使用したネットワーク構成の例

```
# Internet host table
# This is the sample /etc/hosts file for the name-server on the management
# network.

192.168.2.1      mgtnet-router-1    # Management network router
#                                     (default gateway)
192.168.2.254   mgtnet-nameserver  # Management network install/name server
192.168.254.1   mgtnet-router-254  # Management network router (client side)
192.168.254.2   mgtnet-ws          # Management network workstation

192.168.2.199   medusa-sc          # Medusa - alias IP address for active SC
192.168.2.200   medusa-ssc0        # Medusa - ssc0/sc
192.168.2.201   medusa-ssc1        # Medusa - ssc1/sc
192.168.2.202   medusa-swt0        # Medusa - ssc0/swt
192.168.2.203   medusa-swt1        # Medusa - ssc1/swt

# 192.168.2.100 -> 192.168.2.131 are reserved for private use by the
# Sun Fire B1600 Blade System Chassis called medusa. They are test addresses for
# the IPMP driver on each server blade.

192.168.2.150   medusa-s0-mgt
192.168.2.151   medusa-s1-mgt
192.168.2.152   medusa-s2-mgt
192.168.2.153   medusa-s3-mgt
192.168.2.154   medusa-s4-mgt
192.168.2.155   medusa-s5-mgt
192.168.2.156   medusa-s6-mgt
192.168.2.157   medusa-s7-mgt
192.168.2.158   medusa-s8-mgt
192.168.2.159   medusa-s9-mgt
192.168.2.160   medusa-s10-mgt
192.168.2.161   medusa-s11-mgt
192.168.2.162   medusa-s12-mgt
192.168.2.163   medusa-s13-mgt
192.168.2.164   medusa-s14-mgt
192.168.2.165   medusa-s15-mgt
```

図 6-2　ネームサーバーの /etc/hosts ファイルの例 (管理ネットワーク)

6.3 システムコントローラおよびスイッチの設定

これまでの章の手順に従って、システムシャーシのシステムコントローラおよびスイッチの設定を完了している場合は、6-5 ページの 6.3.1 節「SSC0 および SSC1 のスイッチの管理 VLAN にサーバーブレードを追加する方法」 に進んでください。

まだ設定を完了していない場合は、第 5 章の手順に従ってください。ただし、SSC1 のスイッチは設定しません。これは、次の手順 (6-5 ページの 6.3.1 節「SSC0 および SSC1 のスイッチの管理 VLAN にサーバーブレードを追加する方法」) に SSC0 のスイッチの全設定を SSC1 のスイッチにコピーする手順が含まれているためです。

6.3.1 SSC0 および SSC1 のスイッチの管理 VLAN にサーバーブレードを追加する方法

この節では、サーバーブレードを管理 VLAN に追加する方法について説明します。デフォルトでは、管理 VLAN は VLAN 2 です (つまり、デフォルトの VLAN 2 には管理ポート NETMGT が含まれています)。また、スイッチには、デフォルトで VLAN 1 も設定されています。VLAN 1 には、すべてのスイッチのサーバーブレードとアップリンクのポートが含まれています。ただし、スイッチの VLAN 設定機能の使用方法を示すため、この節の手順では、VLAN 1 の代わりに VLAN 3 をデータネットワークに使用します。

この節の手順では、管理 VLAN (VLAN 2) およびデータ VLAN (VLAN 3) にはタグが付いています。また、ブレードの起動用として追加の VLAN (VLAN 4) を作成する方法についても説明します。VLAN 4 は、Solaris オペレーティング環境のネットワークインストール中にブレードによって生成される、タグの付いていないトラフィックに対処します。

起動 VLAN (VLAN 4) のトラフィックには、システムシャーシから送信するときにタグを付けることも付けないこともできます。この節のコマンド例では、このトラフィックにタグを付けます。この手順では、シャーシの外部の装置が VLAN を認識し、VLAN 4 にサーバーブレードが使用するネットワークインストールサーバーが含まれていることを前提とします。

注 – この節の手順を実行している途中でスイッチをリセットする場合は、はじめに設定を保存する必要があります。設定を保存しないと、変更はすべて失われます。設定を保存する手順については、A-9 ページの A.8 節「スイッチの設定の保存」を参照してください。

---

1. sc> プロンプトからコンソールにログインし、SSC0 のスイッチを設定します。
   SSC0 のスイッチにログインするには、次のように入力します。

```
sc> console ssc0/swt
```

2. プロンプトが表示されたら、ユーザー名およびパスワードを入力します。
3. スイッチのコマンド行の Console# プロンプトで、次のように入力します。

```
Console#configure
```

4. 次のように入力して、スイッチの VLAN データベースにアクセスします。

```
Console(config)#vlan database
```

5. 次のように入力して、データネットワークおよび起動ネットワークの VLAN を設定します。

```
Console(config-vlan)#vlan 3 name Data media ethernet
Console(config-vlan)#vlan 4 name Boot media ethernet
```

6. 次のように入力して、VLAN データベースを終了します。

```
Console(config-vlan)#end
```

7. サーバーブレードポート SNP0 を、管理 VLAN (VLAN 2) およびデータ VLAN (VLAN 3)、起動 VLAN (VLAN 4) に追加します。
   追加するには、次のコマンドを実行します。

```
Console#configure
Console(config)#interface ethernet SNP0
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#switchport allowed vlan add 3 tagged
Console(config-if)#switchport allowed vlan add 4
Console(config-if)#switchport native vlan 4
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#exit
Console(config)#
```

これらのコマンドの意味は、次のとおりです。

- interface ethernet SNP0 コマンドは、設定するブレードポートを指定します (この例では、インタフェースにブレードポート SNP0 を指定しています)。
- switchport allowed vlan add 2 tagged コマンドを実行すると、このブレードポートは VLAN 2 (管理ネットワーク) のメンバーになって、タグの付いたトラフィックが管理ネットワークへ通過できるようになります。
- switchport allowed vlan add 3 tagged コマンドを実行すると、このポートは VLAN 3 (新しいデータネットワーク) のメンバーになって、タグの付いたトラフィックがデータネットワークへ通過できるようになります。
- switchport allowed vlan add 4 コマンドを実行すると、このポートは VLAN 4 のメンバーになります。ポートは、タグの付いていないパケットを受信して、そのパケットに VLAN 4 のメンバーとしてタグを付けます。これによって、起動中にブレードによって生成されたタグの付いていないトラフィックを、ネットワークインストールサーバーへ送信するためのパスを提供します。この VLAN は、次のコマンドでネイティブ VLAN に設定します。ネイティブ VLAN とは、タグの付いていないすべてのフレームが転送される VLAN のことです。
- switchport native vlan 4 コマンドを実行すると、このポートは受信したタグの付いていないすべてのフレームを VLAN 4 に送信します (OBP および JumpStart のために、サーバーブレードをタグの付いていないフレームの送信に対応させます)。
- switchport allowed vlan remove 1 コマンドを実行すると、そのポートが VLAN 1 (スイッチのすべてのサーバーブレードポートおよびアップリンクポートに対するデフォルトの VLAN) から削除されます。

ほかのすべてのサーバブレードポート (SNP1 ～ SNP15) に対しても手順 7 を実行します。これらのポートは、すべて管理ネットワークおよびデータネットワークの両方に含める必要があります。

設定したポートを確認するには、次のように入力します。

```
Console#show interfaces switchport ethernet SNP0
Information of SNP0
 Broadcast threshold: Enabled, 256 packets/second
 Lacp status: Disabled
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 4
 Priority for untagged traffic: 0
 Gvrp status: Disabled
 Allowed Vlan:    2(t), 3(t), 4(u)
 Forbidden Vlan:
Console#
```

8. いくつかのデータアップリンクポートをトランクにまとめる場合は、この段階でまとめます。

   この手順の詳細は、A-14 ページの A.10 節「回復力と性能を向上させるトランク接続の設定」を参照してください。

9. 次のコマンドを実行して、トランクにまとめられていないデータアップリンクポートをデータ VLAN (VLAN 3) および起動 VLAN (VLAN 4) に追加します。

```
Console#configure
Console(config)#interface ethernet NETP0
Console(config-if)#switchport allowed vlan add 3 tagged
Console(config-if)#switchport allowed vlan add 4
Console(config-if)#switchport native vlan 4
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport mode trunk
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#no switchport gvrp
Console(config-if)#switchport forbidden vlan add 2
Console(config-if)#end
Console(config)#
```

   - interface ethernet NETP0 コマンドは、設定するアップリンクポートを指定します。
   - switchport allowed vlan add 3 tagged コマンドを実行すると、このアップリンクポートはデータネットワーク (VLAN 3) に追加されます。
   - switchport allowed vlan add 4 コマンドを実行すると、このアップリンクポートは、ブレードの起動に使用するタグの付いていない VLAN (VLAN 4) に追加されます。この VLAN は、次のコマンドでネイティブ VLAN に設定します。ネイティブ VLAN とは、このデータポートがタグの付いていないすべてのフレームを転送する VLAN のことです。
   - switchport native vlan 4 コマンドを実行すると、外部データポートは受信したタグの付いていないすべてのフレームを VLAN 4 に送信します。このコマンドの効果は一時的なもので、このあとに実行するコマンドによって、ポートはタグの付いていないフレームを受け入れなくなります。switchport mode trunk コマンドが実行されるまでは、スイッチがネイティブ VLAN を使用できるようにする必要があるため、このコマンドを実行しています。
   - switchport allowed vlan remove 1 コマンドを実行すると、このアップリンクポートが VLAN 1 (デフォルトの VLAN) から削除されます。VLAN 1 は、この時点、つまり VLAN 4 (ネイティブの、タグなし VLAN) を作成したあとでのみ削除できます。

- switchport ingress-filtering コマンドおよび switchport mode trunk コマンド、switchport acceptable-frame-types tagged コマンドを実行すると、ポートは、その VLAN のメンバーであることを示すタグが付いていないフレームを拒否するようになります。
- no switchport gvrp コマンドを実行すると、ポートは、GVRP を使用して、接続されているもう一方のスイッチにどの VLAN (この場合は VLAN 3) のメンバーであるかを通知することができなくなります。
- switchport forbidden vlan add 2 コマンドを実行すると、ネットワーク上のもう一方のスイッチからの GVRP 要求に応じて、アップリンクポートを VLAN 2 に追加することができなくなります。

設定したポートを確認するには、次のように入力します。

```
Console#show interfaces switchport ethernet NETP0
Information of NETP0
 Broadcast threshold: Enabled, 256 packets/second
 Lacp status: Disabled
 VLAN membership mode: Trunk
 Ingress rule: Enabled
 Acceptable frame type: Tagged frames only
 Native VLAN: 4
 Priority for untagged traffic: 0
 Gvrp status: Disabled
 Allowed Vlan:    3(t), 4(t)
 Forbidden Vlan:    2,
Console#
```

10. 次のコマンドを実行して、トランクをデータ VLAN (VLAN 3) に追加します。

トランク接続の使用方法の詳細は、付録 A を参照してください。

次の例では、トランクは port-channel 1 と呼ばれています。
interface port-channel 1 コマンドで、設定するトランクを指定します。

```
Console(config)#interface port-channel 1
Console(config-if)#switchport allowed vlan add 3 tagged
Console(config-if)#switchport allowed vlan add 4
Console(config-if)#switchport native vlan 4
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport mode trunk
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#no switchport gvrp
Console(config-if)#switchport forbidden vlan add 2
Console(config-if)#end
Console(config)#
```

11. すべてのアップリンクポートを、個々にまたはトランクとして VLAN 3 に追加します (手順 9 および手順 10 を参照)。

    たとえば、ポート NETP1 および NETP2、NETP3 がトランク 1 にまとめられ、NETP4 および NETP5 がトランク 2 にまとめられている場合は、ポート NETP0 および NETP6、NETP7 とトランク 1 およびトランク 2 を VLAN 3 に追加する必要があります。

12. A-15 ページの A.11 節「スイッチのパケットフィルタを使用したブレードの安全な管理」の手順を実行します。

13. SSC0 のスイッチの設定に対して行った変更を保存します。

    この手順の詳細は、A-9 ページの A.8 節「スイッチの設定の保存」を参照してください。

14. SSC0 のスイッチの設定を SSC1 のスイッチにコピーします。

    この手順の詳細は、A-9 ページの A.9 節「最初のスイッチから 2 番目のスイッチへの設定のコピー」を参照してください。

15. #. を入力して、スイッチのコマンド行インタフェースを終了し、システムコントローラに戻ります。

16. sc> プロンプトから、次のように入力して SSC1 のスイッチにログインします。

```
sc> console ssc1/swt
```

17. ユーザー名およびパスワードを入力します。

18. SSC1 のスイッチの IP アドレスおよびネットマスク、デフォルトゲートウェイを設定します。

    この手順の詳細は、A-6 ページの A.6 節「スイッチの IP アドレスおよびネットマスク、デフォルトゲートウェイの設定」を参照してください。

19. SSC1 のスイッチの設定に対して行った変更を保存します。

    この手順の詳細は、A-9 ページの A.8 節「スイッチの設定の保存」を参照してください。

20. #. を入力して、スイッチのコマンド行インタフェースを終了し、sc> プロンプトに戻ります。

21. 6-11 ページの 6.4 節「ネットワーク回復のために IPMP を使用するサーバーブレードの設定 (VLAN タグ)」の手順を実行します。

6.4 ネットワーク回復のために IPMP を使用するサーバーブレードの設定 (VLAN タグ)

前の節で実行したスイッチの設定手順では、タグの付いた VLAN を使用して、データネットワークと管理ネットワークを分離しました。このスイッチ構成で IPMP を使用するには、そのサーバーブレードがメンバーになっている各 VLAN 用の IP アドレスが 4 個ずつ必要です。つまり、管理 VLAN 用に 4 個、データ VLAN 用に 4 個の、合計 8 個の IP アドレスが必要です。

これは、IPMP ドライバが、各 VLAN に個別の論理 Ethernet インタフェースの組を使用することによってタグ付き VLAN をサポートするためです。この論理インタフェースには、次の簡単な計算式を使用して、個別に手動で名前を付ける必要があります。

`ce`(*VLAN id* x 1000) + *instance*

VLAN id には、サーバーブレードを接続するシャーシ内のスイッチポートに設定した VLAN の番号を指定します。*instance* には、論理インタフェースが物理インタフェース `ce0` と `ce1` のどちらに関連するかによって、0 または 1 を指定します。

論理 Ethernet インタフェースの組を作成すると、あるネットワークに対するフレームを確実に送信して、ほかのネットワークには送信しないようにすることができます。IPMP ドライバは、スイッチに送信するフレームを受信すると、そのフレームの宛先になる VLAN のタグを付けて、使用できる 2 つの論理インタフェースのいずれかで転送します。次に、いずれかのスイッチは、フレームの送信元のサーバーブレード用のポートでそのフレームを受信します。そして、スイッチがタグで指定された VLAN のフレームに対応するように設定されていれば、フレームをその VLAN に転送します。

サーバーブレードの IPMP ドライバは、VLAN への冗長仮想接続を使用して、フレームを特定の VLAN に転送します。そのサーバーブレードがメンバーになっているほかの VLAN は、そのフレームを受信できません。

6.4.1 サーバーブレードの設定 (VLAN タグ)

この節では、2 つの Ethernet インタフェースが 2 つの有効な論理インタフェース (データ VLAN および管理 VLAN に 1 つずつ) を提供するようにサーバーブレードの IPMP を設定する方法について説明します。

手順を理解しやすくするために、ここでは 6-2 ページの 6.2 節「ネットワーク環境の準備」に示すネットワーク構成の例を使用します。この例では、第 5 章の IPMP に対するサーバーブレードの設定がすでに完了していることを前提とします。

表 6-1 に、図 6-1 のシステムシャーシのスロット 0 に取り付けたサーバーブレードの IPMP ドライバに設定する必要のある情報を示します。

注 – この節の手順は、データネットワークと管理ネットワークへの冗長接続が必要なサーバーブレードごとに実行する必要があります。

表 6-1 サーバーブレードの IPMP 設定の例 (VLAN タグ)

IPMP 構成変数	スロット 0 のサーバーブレードの値の例
ネットワークアダプタインタフェース	ce2000 (アクティブ) ce2001 (アクティブ) ce3000 (アクティブ) ce3001 (アクティブ)
インタフェースグループ名	medusa_grp0-mgt medusa_grp0
IP アドレスおよびホスト名 (ce2000/1) IP アドレスおよびホスト名 (ce3000/1)	192.168.2.150 (medusa-s0-mgt) 192.168.1.150 (medusa-s0)
IP アドレスおよびホスト名 (管理ネットワーク) IP アドレスおよびホスト名 (データネットワーク)	192.168.2.150 (medusa-s0-mgt) 192.168.1.150 (medusa-s0)
二次 IP アドレスおよびホスト名 (管理ネットワーク) 二次 IP アドレスおよびホスト名 (データネットワーク)	192.168.2.166 (medusa-s0-mgt-sec) 192.168.1.166 (medusa-s0-sec)
テスト IP アドレスおよびホスト名 (ce2000) テスト IP アドレスおよびホスト名 (ce2001)	192.168.2.100 (medusa-s0-0) 192.168.2.116 (medusa-s0-1)
テスト IP アドレスおよびホスト名 (ce3000) テスト IP アドレスおよびホスト名 (ce3001)	192.168.1.100 (medusa-s0-0) 192.168.1.116 (medusa-s0-1)
ネットマスク	255.255.255.0
サーバーブレードによるネットワークルーティングの実行	実行しない

1. **第 3 章の手順に従って、Solaris の準備設定を実行します。**

   この設定を実行したら、サーバーブレードのコンソールから #. を入力して sc> プロンプトに戻ります。

2. インタフェースを設定するサーバーブレードのコンソールにログインします。

   sc> プロンプトで、次のように入力します。

```
sc> console sn
```

   n には、ログインするサーバーブレードが取り付けられているスロット番号を指定します。

3. サーバーブレードの /etc/hosts ファイルを編集して、管理インタフェース用のテスト IP アドレスを追加します。

   表 6-1 のアドレスの例を使用するブレードでは、次に示すファイルの例の最後の 2 行を追加する必要があります。

```
#
# /etc/hosts on the server blade in system chassis Medusa, slot 0
#
127.0.0.1       localhost          loghost

192.168.1.150   medusa-s0          # Data Address
192.168.1.166   medusa-s0-sec      # Secondary Data Address
192.168.1.100   medusa-s0-0        # Test Address for ce0
192.168.1.116   medusa-s0-1        # Test Address for ce1

192.168.2.150   medusa-s0-mgt       # Data Address
192.168.2.166   medusa-s0-mgt-sec   # Secondary Data Address
192.168.2.100   medusa-s0-mgt-0     # Test Address for ce0
192.168.2.116   medusa-s0-mgt-1     # Test Address for ce1
```

4. サーバーブレードの /etc/netmasks ファイルにネットマスクを設定します。

   表 6-1 のアドレスの例を使用するブレードでは、次の行を追加する必要があります。

```
192.168.1.0     255.255.255.0
192.168.2.0     255.255.255.0
```

5. サーバーブレードはルーティングの実行には使用しないため、ルーティングを使用不可にします。

   次のように入力します。

```
# touch /etc/notrouter
# ndd -set /dev/ip ip_forwarding 0
```

6. 次のように入力して、既存のネットワークインタフェースを unplumb します。

```
# ifconfig ce0 unplumb
# ifconfig ce1 unplumb
```

片方または両方のインタフェースがあらかじめ設定されていないと、次のエラーメッセージが表示されることがあります。

```
ifconfig: unplumb: SIOCGLIFFLAGS: ce1: no such interface
```

7. 次のように入力して、新しいインタフェースを作成します。

```
# ifconfig ce2000 plumb
# ifconfig ce2001 plumb
# ifconfig ce3000 plumb
# ifconfig ce3001 plumb
```

8. 新しいインタフェースを含む IPMP のフェイルオーバーグループを作成します。

```
# ifconfig ce2000 group medusa_grp0-mgt
# ifconfig ce2001 group medusa_grp0-mgt
# ifconfig ce3000 group medusa_grp0
# ifconfig ce3001 group medusa_grp0
```

このコマンドを実行したとき、次の syslog メッセージが表示されることがあります。

```
Sep  3 00:49:58 medusa-s0 in.mpathd[298]: Failures cannot be
detected on ce0 as no IFF_NOFAILOVER address is available
```

このメッセージは、インタフェースのテストアドレスが確立されるまでは障害が検出されないことを単に警告するものです。

9. 新しいインタフェースにデータ転送用のアドレスを作成し、インタフェースの障害が検出された場合にフェイルオーバーを実行するように指定します。

```
# ifconfig ce2000 medusa-s0-mgt netmask + broadcast + failover up
Setting netmask of ce2000 to 255.255.255.0
#
# ifconfig ce2001 medusa-s0-mgt-sec netmask + broadcast + failover
up
Setting netmask of ce2001 to 255.255.255.0
#
# ifconfig ce3000 medusa-s0 netmask + broadcast + failover up
Setting netmask of ce3000 to 255.255.255.0
#
# ifconfig ce3001 medusa-s0-sec netmask + broadcast + failover up
Setting netmask of ce3001 to 255.255.255.0
```

10. 各ネットワークインタフェースのテストアドレスを設定します。

このアドレスは、mpathd がインタフェースの障害を検出するために使用するものです。ホストアプリケーションがデータの通信にこのアドレスを使用しないように、コマンド行で deprecated と指定します (次の例を参照)。

-failover フラグの指定も必要です。このフラグによって、in.mpathd がこのアドレスをテストアドレス (ほかのインタフェースに渡すことができないため、フェイルオーバーがないアドレス) として使用するようになります。

```
# ifconfig ce2000 addif medusa-s0-mgt-0 netmask + broadcast +
-failover deprecated up
Created new logical interface ce2000:1
Setting netmask of ce2000:1 to 255.255.255.0
# ifconfig ce2001 addif medusa-s0-mgt-1 netmask + broadcast +
-failover deprecated up
Created new logical interface ce2001:1
Setting netmask of ce2001:1 to 255.255.255.0
# ifconfig ce3000 addif medusa-s0-0 netmask + broadcast + -failover
deprecated up
Created new logical interface ce3000:1
Setting netmask of ce3000:1 to 255.255.255.0
# ifconfig ce3001 addif medusa-s0-1 netmask + broadcast + -failover
deprecated up
Created new logical interface ce3001:1
Setting netmask of ce3001:1 to 255.255.255.0
```

11. **再起動しても新しいインタフェース設定が消えないように、/etc ディレクトリに hostname.ce2000 および hostname.ce2001、hostname.ce3000、hostname.ce3001 という名前のファイルを作成します。**

hostname.ce2000 ファイルの例は、次のとおりです。

```
medusa-s0-mgt netmask + broadcast + \
group medusa_grp0-mgt failover up \
addif medusa-s0-mgt-0 netmask + broadcast + \
deprecated -failover up
```

hostname.ce2001 ファイルの例は、次のとおりです。

```
medusa-s0-mgt-sec netmask + broadcast + \
group medusa_grp0-mgt failover up \
addif medusa-s0-mgt-1 netmask + broadcast + \
deprecated -failover up
```

hostname.ce3000 ファイルの例は、次のとおりです。

```
medusa-s0 netmask + broadcast + \
group medusa_grp0 failover up \
addif medusa-s0-0 netmask + broadcast + \
deprecated -failover up
```

hostname.ce3001 ファイルの例は、次のとおりです。

```
medusa-s0-sec netmask + broadcast + \
group medusa_grp0 failover up \
addif medusa-s0-1 netmask + broadcast + \
deprecated -failover up
```

12. 次のように入力して、2 つのネットワークアダプタの設定を確認します。

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
ce2000: flags=9040843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
mtu 1500 index 3
        inet 192.168.2.150 netmask ffffff00 broadcast 192.168.2.255
        groupname medusa_grp0-mgt
        ether 0:3:ba:19:26:3
ce2000:1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER> mtu 1496 index 3
        inet 192.168.2.100 netmask ffffff00 broadcast 192.168.2.255
ce2001: flags=9040843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
mtu 1500 index 4
        inet 192.168.2.166 netmask ffffff00 broadcast 192.168.2.255
        groupname medusa_grp0-mgt
        ether 0:3:ba:19:26:4
ce2001:1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER> mtu 1496 index 4
        inet 192.168.2.116 netmask ffffff00 broadcast 192.168.2.255
ce3000: flags=9040843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
mtu 1500 index 5
        inet 192.168.1.150 netmask ffffff00 broadcast 192.168.1.255
        groupname medusa_grp0
        ether 0:3:ba:19:26:3
ce3000:1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER> mtu 1496 index 5
        inet 192.168.1.100 netmask ffffff00 broadcast 192.168.1.255
ce3001: flags=9040843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
mtu 1500 index 6
        inet 192.168.1.166 netmask ffffff00 broadcast 192.168.1.255
        groupname medusa_grp0
        ether 0:3:ba:19:26:4
ce3001:1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER> mtu 1496 index 6
        inet 192.168.1.116 netmask ffffff00 broadcast 192.168.1.255
```

この出力は、8 個のアドレス (表 6-1 のアドレスの例) が定義されていることを示しています。4 個の IPMP テストアドレスには、NOFAILOVER と記されています。これは、障害が発生した場合に、障害の発生していないインタフェースへの転送が行われないことを意味します。

13. シャーシから 1 台の SSC を一時的に取り外して、IPMP をテストします。

この操作によって、コンソール上に次のエラーメッセージが表示されます。

```
Sep  4 20:12:16 medusa-s0 in.mpathd[31]: NIC failure detected on
ce3001 of group medusa_grp0
Sep  4 20:12:16 medusa-s0 in.mpathd[31]: Successfully failed over
from NIC ce3001 to NIC ce3000
```

注 – デフォルトの設定では、IPMP デーモンがネットワーク障害を検出してから回復するまでに約 10 秒かかります。IPMP デーモンの設定は、/etc/default/mpathd ファイルに定義されています。

第7章

複数のテナントに対するスイッチ設定の例

この章は次の節で構成されています。

注 – この節の手順を実行している途中でスイッチをリセットする場合は、はじめに設定を保存する必要があります。設定を保存しないと、変更はすべて失われます。設定を保存する方法については、A-9 ページの A.8 節「スイッチの設定の保存」を参照してください。

7.1 概要

この章は、主に、次の設定作業を行う必要がある ISP (インターネットサービスプロバイダ) を対象とします。

- サーバーブレードを別々のユーザーに割り当てる
- サーバーブレードを割り当てられたユーザーが、自身のブレードを管理できるようにする
- ユーザーが、ほかのユーザーのネットワークからデータを受信できないようにする
- ユーザーが、ほかのユーザーのブレードのコンソールにアクセスできないようにする
- ユーザーが、どちらの統合スイッチのコンソールにもアクセスできないようにする

この章では、スイッチの 2 つの構成例を使用して、VLAN によってサーバーブレードを別々のユーザーに割り当てる方法を示します。この章では、ISP のユーザーを特定のサーバーブレードの「テナント」と呼びます。

この章のスイッチ設定では、ISP だけが SC およびスイッチのコマンド行インタフェースへのログイン名およびパスワードを持っていることを前提としています。ISP のユーザーは、スイッチの NETMGT ポートに対して `ping` を実行できます。これは、ユーザー自身の管理ネットワークに NETMGT ポートが含まれているためです。ただし、ISP がユーザーにスイッチへのログイン名およびパスワードを付与しないかぎり、ユーザーはスイッチにアクセスできません。VLAN 構成では、ユーザーが telnet 接続で SC ネットワークにアクセスすることはできません。

この章は主に ISP を対象としていますが、一般的なネットワーク管理者が VLAN を使用して Sun Fire B1600 ブレードシステムシャーシのネットワークトラフィックを制御する場合にも役立つことがあります。

この章では、ブレードの IPMP の設定方法については説明しません。複雑な VLAN 構成を実現するための IPMP の設定については、第 6 章を参照してください。

注 – この章の説明は、VLAN の使用方法に関するものです。広域なネットワークで、タグ付き VLAN を使用することを前提としています。この章の構成では、ネットワーク間の Solaris のインストールはサポートしていません。ネットワーク間の Solaris のインストールでは、スイッチにタグの付いていないトラフィックを扱う VLAN を設定する必要があるためです。この章では、スイッチの VLAN 機能の使用方法だけを説明します。

ネットワークに送信するフレームから VLAN のタグを削除し、ネットワークから受信するタグの付いていないフレームには VLAN のタグを追加するようにスイッチを設定する方法については、7-10 ページの 7.2.4 節「データネットワークポートの各テナントへの割り当て」および 7-16 ページの 7.3.4 節「データネットワークポートのテナント間での共有」を参照してください。

7.2 例 A : ブレードおよびデータポートを所有する 3 つの異なるテナント

この例では、ISP がブレードシステムシャーシを所有し、全責任をもって管理していることを前提とします。したがって、スイッチの NETMGT のコマンド行インタフェースには、ISP だけがアクセスできます。

また、この例では、テナント 1 および テナント 2、テナント 3 の 3 つのテナントを想定しています。各テナントには、1 つのデータ VLAN が排他的に割り当てられています。このデータ VLAN には、複数のサーバーブレードポート (スイッチのサーバーブレードダウンリンクポート) および外部データポートが含まれます。

各テナントは、テナント自身のブレードにセキュリティー保護されたアクセスを提供する管理 VLAN を持っています。

スイッチ設定の概要を、表 7-1 に示します。

表 7-1 例 A : サーバーブレードおよびデータポートを所有する 3 つのテナント

ネットワーク管理者	管理ポート	サーバーブレードポート	アップリンクポート	データ VLAN ID	管理 VLAN ID
インターネットサービスプロバイダ	NETMGT	なし	なし	なし	2
テナント 1	NETMGT	SNP0、SNP1、SNP2	NETP0、NETP1	11	21
テナント 2	NETMGT	SNP3、SNP4、SNP5、SNP6、SNP7、SNP8、SNP9	NETP2、NETP3、NETP4	12	22
テナント 3	NETMGT	SNP10、SNP11、SNP12、SNP13、SNP14、SNP15	NETP5、NETP6、NETP7	13	23

この節では、表 7-1 の構成の設定方法について説明します。内容は次のとおりです。

- 7-6 ページの 7.2.1 節「すべての VLAN の作成および命名」

- 7-7 ページの 7.2.2 節「管理ポート (NETMGT) の各テナントへの割り当て」
- 7-8 ページの 7.2.3 節「サーバーブレードポートの各テナントへの割り当て」
- 7-10 ページの 7.2.4 節「データネットワークポートの各テナントへの割り当て」

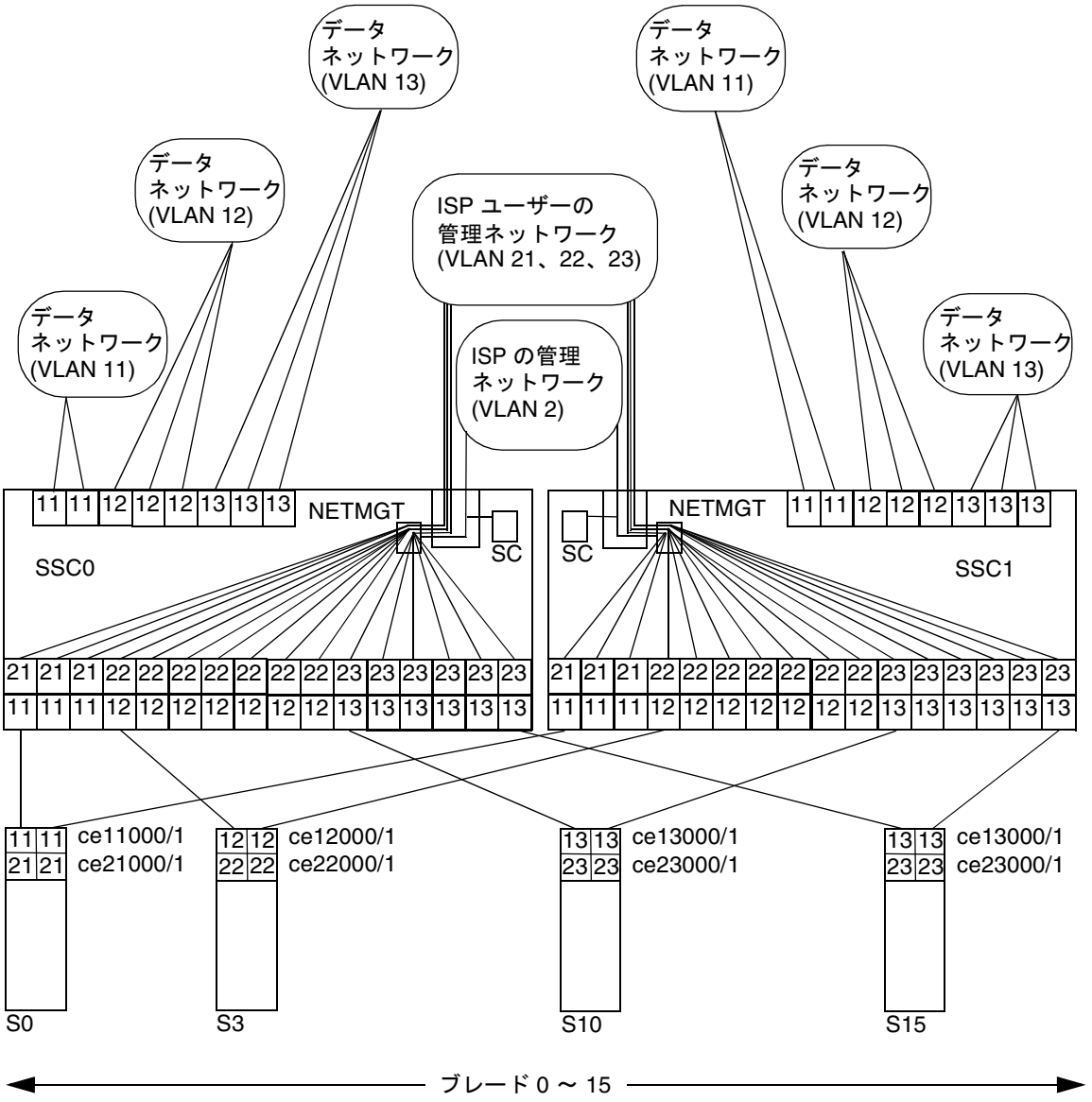

図 7-1　例 A : テナントのデータおよび管理 VLAN と ISP の管理 VLAN

図 7-1 は、表 7-1 と同じ情報を表した図です。中央の VLAN 2 が ISP の管理 VLAN です。この VLAN は、ISP のネットワーク管理者だけが使用します。この管理 VLAN には、スイッチの NETMGT ポートが含まれています。そのため、ISP のネットワーク管理者は、telnet または Web を介してスイッチのすべての情報を設定できます。また、この管理 VLAN にはシステムコントローラも含まれています。そのため、ISP はシャーシのすべての情報を設定し、sc> プロンプトからすべてのサーバーブレードおよび 2 つのスイッチのコンソールにアクセスすることができます。ただし、システムコントローラの VLAN への対応付けを管理するには、sc> プロンプトで特別に `setupsc` コマンドを実行して設定します。これは、スイッチの設定プロセスには含まれていません。

注 – この例では、ISP のネットワーク管理者が、システムコントローラまたはスイッチのコマンド行インタフェースへのパスワードアクセス権をユーザーに付与しないことを前提とします。システムコントローラおよびスイッチのインタフェースへのアクセスの制御は、ネットワーク管理者が責任をもって行います。

この図の VLAN 2 の上には、ISP の個々のユーザーの管理 VLAN が示されています。各ユーザーは、ユーザー自身のサーバーブレード専用の管理 VLAN にアクセスできます。そのため、たとえば、テナント 1 (管理 VLAN 21) はスロット 0 ～ 2 のサーバーブレードに、テナント 2 (管理 VLAN 22) はスロット 3 ～ 9 のサーバーブレードに、テナント 3 (管理 VLAN 23) はスロット 10 ～ 15 のサーバーブレードに telnet で接続できます。

図の下部には、各ユーザーの最初のサーバーブレードを示しています。各ブレードには、データネットワークへの 2 つの論理インタフェースと、管理ネットワークへの 2 つの論理インタフェースが必要です。論理インタフェースは、IPMP によって提供する必要があります (第 6 章を参照)。この図には、IPMP 設定に必要なインタフェースの番号を示しています。たとえば、テナント 1 のサーバーブレードには、VLAN 11 (データネットワーク) に対する 2 つの論理インタフェースと、VLAN 21 (管理ネットワーク) に対する 2 つの論理インタフェースが設定されています。第 6 章で説明した計算式に従って、テナント 1 の各ブレードのインタフェースには、`ce11000` および `ce21000` (`ce0` から SSC0 のスイッチへの接続) と、`ce11001` および `ce21001` (`ce1` から SSC1 のスイッチへの接続) の番号が付いています。

この例の ISP の各ユーザーは、専用のネットワークアップリンクポートを持っています。テナント 1 は NETP0 および NETP1 のアップリンクポート、テナント 2 は NETP2 および NETP3、NETP4、テナント 3 は NETP5 および NETP6、NETP7 を所有しています。アップリンクポートは、各テナントに属するサーバーブレードで構成するデータネットワークの VLAN に含められることで、特定のテナント専用に限定されます。そのため、たとえばテナント 3 のデータネットワーク VLAN (13) には、サーバーブレードポート SNP10 ～ SNP15 と、アップリンクポート NETP5 および NETP6、NETP7 を含めます。

注 – 異なるテナントに属するアップリンクポートを同じ外部スイッチに接続すると、スパニングツリープロトコルによって一部の接続が切断されます。テナントごとに別々の外部スイッチを使用することをお勧めします。または、スパニングツリープロトコルを終了することもできます (7-11 ページの 7.2.5 節「スパニングツリーの終了」を参照)。

7.2.1 すべての VLAN の作成および命名

1. SSC0 のスイッチにログインするには、次のように入力します。

```
sc> console ssc0/swt
```

2. ユーザー名の入力を求めるプロンプトが表示されたら、admin を入力します。

   パスワードとして、もう一度 admin を入力します。

3. スイッチが出荷時のデフォルトの設定になっていることを確認します。

   詳細は、A-4 ページの A.4 節「スイッチが出荷時のデフォルト設定であることの確認」を参照してください。

4. 出荷時のデフォルトの設定に戻した場合、つまり、まだ自分のパスワードを設定していない場合は、パスワードを設定します。

   詳細は、2-4 ページの 2.2 節「デフォルトユーザーでのスイッチへのログインとパスワードの設定」を参照してください。

5. テナントのデータ VLAN を作成して名前を付けます。

   次のように入力します。

```
Console#configure
Console(config)#vlan database
Console(config-vlan)#vlan 11 name tenant1 media ethernet
Console(config-vlan)#vlan 12 name tenant2 media ethernet
Console(config-vlan)#vlan 13 name tenant3 media ethernet
Console(config-vlan)#end
```

6. テナントの管理 VLAN を作成して名前を付けます。

次のように入力します。

```
Console#configure
Console(config)#vlan database
Console(config-vlan)#vlan 21 name tenant1_managment media ethernet
Console(config-vlan)#vlan 22 name tenant2_managment media ethernet
Console(config-vlan)#vlan 23 name tenant3_managment media ethernet
Console(config-vlan)#end
```

7.2.2 管理ポート (NETMGT) の各テナントへの割り当て

1. ISP の管理 VLAN (2) およびすべてのテナントの管理 VLAN (21、22、23) に対してフレームの送受信を実行できるように、スイッチの管理ポート (NETMGT) を設定します。

ISP は、デフォルトの管理 VLAN (VLAN 2) を使用します。

次のように入力します。

```
Console#configure
Console(config)#interface ethernet NETMGT
Console(config-if)#switchport allowed vlan add 21 tagged
Console(config-if)#switchport allowed vlan add 22 tagged
Console(config-if)#switchport allowed vlan add 23 tagged
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport mode trunk
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#no switchport gvrp
Console(config-if)#end
```

これらのコマンドの意味は、次のとおりです。

- interface ethernet NETMGT コマンドは、管理ポートを設定することを指定します。
- switchport allowed vlan add 21 コマンドを実行すると、テナント 1 の管理 VLAN (21) に NETMGT が追加されて、タグの付いたフレームがその VLAN へ通過できるようになります。
- switchport allowed vlan add 22 コマンドを実行すると、テナント 2 の管理 VLAN (22) に NETMGT が追加されて、タグの付いたフレームがその VLAN へ通過できるようになります。

- `switchport allowed vlan add 23` コマンドを実行すると、テナント 3 の管理 VLAN (23) に NETMGT が追加されて、タグの付いたフレームがその VLAN へ通過できるようになります。
- `switchport ingress-filtering` コマンドおよび `switchport mode trunk` コマンド、`switchport acceptable-frame-types tagged` コマンドを実行すると、NETMGT は、その VLAN (VLAN 21、22、23 およびデフォルトの管理 VLAN である VLAN 2) のメンバーであることを示すタグの付いたフレームだけを送受信するようになります。
- `no switchport gvrp` コマンドを実行すると、NETMGT は、GVRP を使用して、もう一方のスイッチにどの VLAN のメンバーであるかを通知することができなくなります。

2. **トラフィックがサーバーブレードから管理ネットワークへ通過できるように、スイッチの IP パケットフィルタが設定されていることを確認します。**

   詳細は、A-15 ページの A.11 節「スイッチのパケットフィルタを使用したブレードの安全な管理」を参照してください。

7.2.3 サーバーブレードポートの各テナントへの割り当て

1. **テナント 1 のサーバーブレードポートを、VLAN 11 および 21 のタグの付いたフレームだけを送受信するように設定します。**

   次のように入力します。

```
Console#configure
Console(config)#interface ethernet SNP0
Console(config-if)#switchport allowed vlan add 11 tagged
Console(config-if)#switchport allowed vlan add 21
Console(config-if)#switchport native vlan 21
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport mode trunk
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#end
```

   これらのコマンドを、テナント 1 に属するほかの 2 つのサーバーブレードポート (SNP1 および SNP2) に対しても実行します。

2. テナント 2 のサーバーブレードポートを、VLAN 12 および 22 のタグの付いたフレームだけを送受信するように設定します。

   次のように入力します。

```
Console#configure
Console(config)#interface ethernet SNP3
Console(config-if)#switchport allowed vlan add 12 tagged
Console(config-if)#switchport allowed vlan add 22
Console(config-if)#switchport native vlan 22
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport mode trunk
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#end
```

   これらのコマンドを、テナント 2 に属するほかのサーバーブレードポート (SNP4 ～ SNP9) に対しても実行します。

3. テナント 3 のサーバーブレードポートを、VLAN 13 および 23 のタグの付いたフレームだけを送受信するように設定します。

   次のように入力します。

```
Console#configure
Console(config)#interface ethernet SNP10
Console(config-if)#switchport allowed vlan add 13 tagged
Console(config-if)#switchport allowed vlan add 23
Console(config-if)#switchport native vlan 23
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport mode trunk
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#end
```

   これらのコマンドを、テナント 3 に属するほかのサーバーブレードポート (SNP11 ～ SNP15) に対しても実行します。

7.2.4 データネットワークポートの各テナントへの割り当て

注 – Sun Fire B1600 ブレードシステムシャーシを接続するネットワークデバイスは、VLAN を認識できる必要があります。そのため、手順には `switchport mode trunk` コマンドの実行が含まれています。このコマンドを実行すると、特定の VLAN のメンバーであることを示すタグの付いたフレームだけを、ネットワークポートが送受信するようになります。

---

1. **テナント 1 のネットワークポートを、VLAN 11 のタグの付いたフレームだけを送受信するように設定します。**

   NETP0 の場合は、次のように入力します。

```
Console#configure
Console(config)#interface ethernet NETP0
Console(config-if)#switchport allowed vlan add 11
Console(config-if)#switchport native vlan 11
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#switchport mode trunk
Console(config-if)#no switchport gvrp
Console(config-if)#end
```

   NETP1 に対しても、これらのコマンドを実行します。

2. **テナント 2 のネットワークポートを、VLAN 12 のタグの付いたフレームだけを送受信するように設定します。**

   NETP2 の場合は、次のように入力します。

```
Console#configure
Console(config)#interface ethernet NETP2
Console(config-if)#switchport allowed vlan add 12
Console(config-if)#switchport native vlan 12
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#switchport mode trunk
Console(config-if)#no switchport gvrp
Console(config-if)#end
```

   NETP3 および NETP4 に対しても、これらのコマンドを実行します。

3. テナント 3 のネットワークポートを、VLAN 13 のタグの付いたフレームだけを送受信するように設定します。

   NETP5 の場合は、次のように入力します。

```
Console#configure
Console(config)#interface ethernet NETP5
Console(config-if)#switchport allowed vlan add 13
Console(config-if)#switchport native vlan 13
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#switchport mode trunk
Console(config-if)#no switchport gvrp
Console(config-if)#end
```

NETP6 および NETP7 に対しても、これらのコマンドを実行します。

7.2.5 スパニングツリーの終了

異なるテナントに属するアップリンクポートを同じ外部スイッチに接続すると、スパニングツリープロトコルによって一部の接続が切断されます。テナントごとに別々の外部スイッチを使用することをお勧めします。または、スパニングツリープロトコルを終了することもできます。スパニングツリーを終了するには、次のように入力します。

```
Console#configure
Console(config)#no spanning-tree
Console(config)#end
```

7.2.6 スイッチの設定の保存および 2 番目のスイッチへのコピー

1. スイッチの設定を保存します。

   この手順の詳細は、付録 A を参照してください。

2. スイッチの設定を 2 番目のスイッチにコピーします。

   この手順の詳細は、付録 A を参照してください。

7.3 例 B : 8 つのブレードおよび 4 つの共有データポートを所有する 2 つのテナント

この例では、ISP がブレードシステムシャーシを所有し、全責任をもって管理しています。また、この例では、テナント 1 およびテナント 2 の、2 つのテナントを想定しています。2 つのテナントにはデータ VLAN が割り当てられ、その VLAN には 8 つのサーバーブレード (8 つのスイッチのサーバープレートポート) と 4 つのスイッチの外部データポートが含まれています。つまり、2 つのテナントは、4 つの外部データポートを共有します (排他的には使用しません)。

この例のスイッチ設定の概要を、表 7-2 に示します。

表 7-2 例 B : 8 つのサーバーブレードおよび 4 つのデータポートを所有する 2 つのテナント

ネットワーク管理者	管理ポート	サーバーブレードポート	外部データポート	データ VLAN ID	管理 VLAN ID
インターネットサービスプロバイダ	NETMGT	なし	なし	なし	2
テナント 1	NETMGT	SNP0、SNP1、SNP2、SNP3、SNP4、SNP5、SNP6、SNP7	NETP0 ～ NETP3	11	21
テナント 2	NETMGT	SNP8、SNP9、SNP10、SNP11、SNP12、SNP13、SNP14、SNP15	NETP0 ～ NETP3	12	22

この節では、表 7-2 の構成の設定方法について説明します。内容は次のとおりです。

- 7-14 ページの 7.3.1 節「すべての VLAN の作成および命名」
- 7-14 ページの 7.3.2 節「管理ポート (NETMGT) の各テナントへの割り当て」
- 7-15 ページの 7.3.3 節「サーバーブレードポートの各テナントへの割り当て」
- 7-16 ページの 7.3.4 節「データネットワークポートのテナント間での共有」

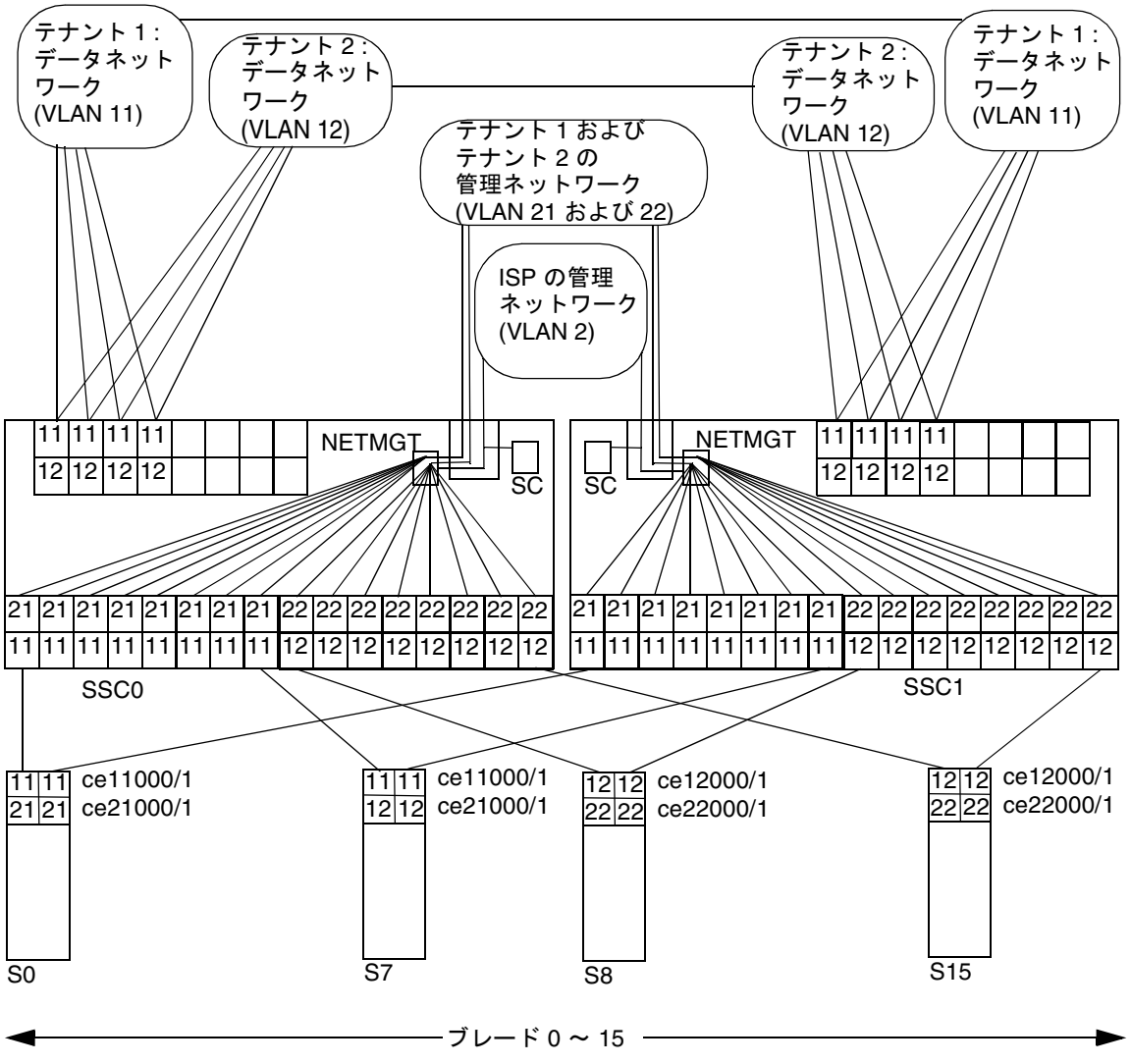

図 7-2　例 B : アップリンクポートを共有する 2 つのテナントのデータおよび管理 VLAN

図 7-2 は、表 7-2 と同じ情報を表した図です。この例は、基本的に例 A と同じです。ただし、すべてのネットワークアップリンクポートがサーバーブレードのテナントによって共有される点が異なります。つまり、2 つのテナントのデータ VLAN (テナント 1 の VLAN 11、テナント 2 の VLAN 12) には、どちらにもアップリンクポート NETP0 ～ NETP3 が含まれています。しかし、テナントがもう一方のテナントの

サーバーブレードからデータを受信することはありません。これは、ポート NETP0 ～ NETP3 から送信されるフレームには、VLAN 11 (テナント 1) または VLAN 12 (テナント 2) のいずれかのタグが付けられるためです。

7.3.1 すべての VLAN の作成および命名

1. テナントのデータ VLAN を作成して名前を付けます。

   次のように入力します。

```
Console#configure
Console(config)#vlan database
Console(config-vlan)#vlan 11 name tenant1 media ethernet
Console(config-vlan)#vlan 12 name tenant2 media ethernet
```

2. テナントの管理 VLAN を作成して名前を付けます。

   次のように入力します。

```
Console#configure
Console(config)#vlan database
Console(config-vlan)#vlan 21 name tenant1_managment media ethernet
Console(config-vlan)#vlan 22 name tenant2_managment media ethernet
Console(config-vlan)#end
```

7.3.2 管理ポート (NETMGT) の各テナントへの割り当て

1. ISP の管理 VLAN (2) および 2 つのテナントの管理 VLAN (21 および 22) に対してフレームの送受信を実行できるように、スイッチの管理ポート (NETMGT) を設定します。

   次のように入力します。

```
Console#config
Console(config)#interface ethernet NETMGT
Console(config-if)#switchport allowed vlan add 21 tagged
Console(config-if)#switchport allowed vlan add 22 tagged
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#switchport mode trunk
Console(config-if)#no switchport gvrp
Console(config-if)#end
```

2. トラフィックがサーバーブレードから管理ネットワークへ通過できるように、スイッチの IP パケットフィルタが設定されていることを確認します。

   詳細は、A-15 ページの A.11 節「スイッチのパケットフィルタを使用したブレードの安全な管理」を参照してください。

7.3.3 サーバーブレードポートの各テナントへの割り当て

1. テナント 1 のサーバーブレードポートを、VLAN 11 および 21 のタグの付いたフレームだけを送受信するように設定します。

   次のように入力します。

```
Console#configure
Console(config)#interface ethernet SNP0
Console(config-if)#switchport allowed vlan add 11 tagged
Console(config-if)#switchport allowed vlan add 21
Console(config-if)#switchport native vlan 21
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport mode trunk
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#end
```

   これらのコマンドを、テナント 1 に属するほかの 7 つのサーバーブレードポート (SNP1 ～ SNP7) に対しても実行します。

2. テナント 2 のサーバーブレードポートを、VLAN 12 および 22 のタグの付いたフレームだけを送受信するように設定します。

   次のように入力します。

```
Console#configure
Console(config)#interface ethernet SNP8
Console(config-if)#switchport allowed vlan add 12 tagged
Console(config-if)#switchport allowed vlan add 22
Console(config-if)#switchport native vlan 12
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport mode trunk
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#end
```

これらのコマンドを、テナント 2 に属するほかの 7 つのサーバーブレードポート (SNP9 ～ SNP15) に対しても実行します。

7.3.4 データネットワークポートのテナント間での共有

注 – この節の手順では、Sun Fire B1600 ブレードシステムシャーシを接続するネットワークデバイスが VLAN を認識できることを前提とします。そのため、手順には `switchport mode trunk` コマンドの実行が含まれています。このコマンドを実行すると、VLAN のメンバーであることを示すタグの付いたフレームだけを、ネットワークポートが送受信するようになります。

---

1. **ネットワークポートを、VLAN 11 および VLAN 12 のタグの付いたフレームだけを送受信するように設定します。**

   NETP0 の場合は、次のように入力します。

```
Console#configure
Console(config)#interface ethernet NETP0
Console(config-if)#switchport allowed vlan add 11 tagged
Console(config-if)#switchport allowed vlan add 21
Console(config-if)#switchport native vlan 21
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#switchport mode trunk
Console(config-if)#no switchport gvrp
Console(config-if)#end
```

2. **NETP1 ～ NETP3 に対しても、これらのコマンドを実行します。**
3. **スイッチの設定を保存します。**

   この手順の詳細は、付録 A を参照してください。

4. **スイッチの設定を 2 番目のスイッチにコピーします。**

   この手順の詳細は、付録 A を参照してください。

付録 A

スイッチで実行する必要のある作業

この付録では、スイッチのコマンド行インタフェースでのみ実行できる作業の手順について説明します。ブレードシステムシャーシを設定するときは、ここで示す作業手順を参照する必要があります。

スイッチのコマンド行インタフェースにログインする方法については、第 2 章を参照してください。

この付録は次の節で構成されています。

A.1 コマンドプロンプトのナビゲーション

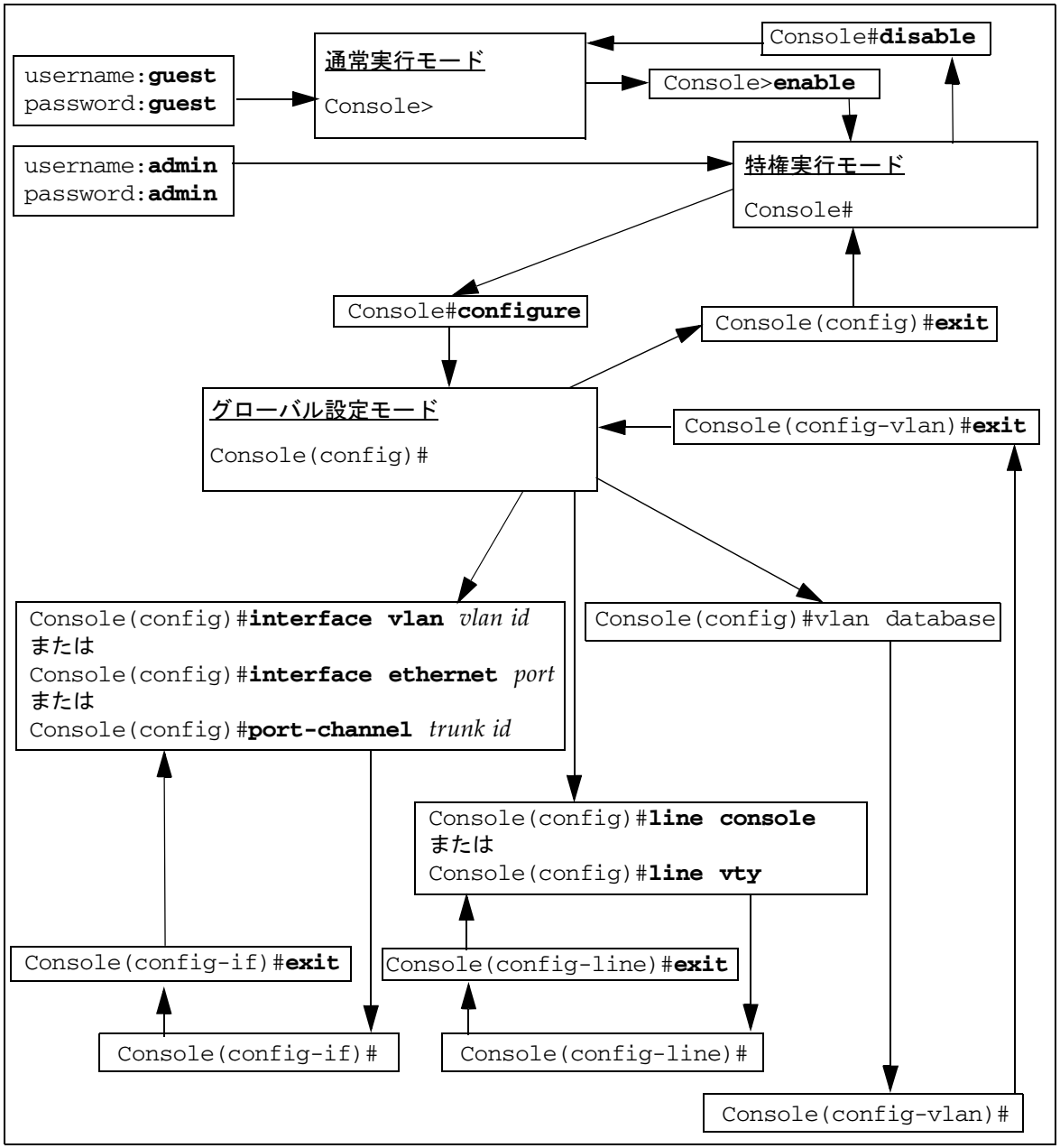

図 A-1 スイッチのコマンドプロンプトのマップ

A.2 コマンド行インタフェースの切り替え

A.2.1 スイッチからシステムコントローラへの切り替え

- スイッチのコマンド行インタフェースを終了してシステムコントローラのコマンド行インタフェースに戻るには、「#」記号を入力してからすぐに「.」を入力します。

  スイッチのコマンド行インタフェースで「#.」エスケープシーケンスを使用すると、システムコントローラのコマンド行インタフェースに戻ります。

  たとえば、次のように入力します (記号は画面には表示されません)。

```
Console(config)##.
```

A.2.2 スイッチのログインプロンプトへの切り替え

- スイッチのログインプロンプトに戻るには、Console# プロンプトが表示されるまで exit または end と入力します。プロンプトが表示されたら、次のように入力します。

```
Console#exit
```

A.3 スイッチ CLI のオンラインヘルプの参照

- **オンラインヘルプの使用方法を参照するには** `help` **を入力します。**
- **オンラインのコンテキストヘルプを参照するには、**`?` **を入力します。この操作によってコマンドまたはパラメタの一覧が表示されます。コマンドプロンプトで** `?` **と入力すると、現在のコマンドモードで使用できるコマンドの一覧が表示されます。コマンドに必要なパラメタを参照するには、そのコマンドの最初の一語を入力して、続けて** `?` **を入力します。これによって、指定できるパラメタの一覧とそのパラメタの説明が表示されます。不完全なコマンドを入力したあとに** `?` **を入力すると、すでに入力した部分はコンソールに表示されます。その情報をもう一度入力する必要はありません。**

  `vlan database` コマンドを使用して VLAN 設定のコマンドモードに入る場合のヘルプ情報の例を、次に示します。

```
Console(config)#vlan
% Incomplete command.
Console(config)#vlan ?
  database  Enter VLAN database mode
Console(config)#vlan database ?
  <cr>
```

<cr> は、これ以上必要なパラメタがないことを示します。ENTER キーを押して、コマンドプロンプトに戻ってください。

A.4 スイッチが出荷時のデフォルト設定であることの確認

スイッチの出荷時のデフォルト設定の詳細は、『Sun Fire B1600 ブレードシステムシャーシスイッチ管理マニュアル』を参照してください。

スイッチを出荷時のデフォルトの設定に戻すには、次の手順を実行します。

1. スイッチが出荷時のデフォルト設定になっているかどうかを確認するには、次のように入力します。

```
Console#whichboot
                    file name  file type       startup  size (byte)
 ------------------------  -------------- ------- --------
                      diag74  Boot-Rom ima    Y      114248
             runtime_v00423  Operation Code  Y      1429204
Factory_Default_Config.cfg  Config File     Y      2574
```

このコマンド出力の最下行で file name 列に「Factory_Default_Config.cfg」と表示された場合は、スイッチはデフォルト設定になっています。

2. スイッチを出荷時のデフォルト設定にするには、次のように入力します。

```
Console#configure
Console(config)#boot system config Factory_Default_Config.cfg
Console(config)#exit
```

3. 出荷時のデフォルト設定で、スイッチを再起動します。

次のように入力します。

```
Console#reload
```

4. ユーザー名およびパスワードの入力を求めるプロンプトが表示されたら、両方に admin を入力します。

A.5 スイッチのリセット

スイッチは、通常、動作時の設定をいくつか変更したあとで起動時の設定に戻す (変更を廃棄する) 場合にリセットします。

また、新しい構成ファイルを作成またはダウンロードして、その新しいファイルをデフォルトの起動ファイルにする場合にも、スイッチをリセットします。

注 – 変更した設定を保持する場合は、スイッチをリセットする前に変更を保存してください。

- スイッチのコマンド行からスイッチをリセットするには、次のように入力します。

```
Console#reload
```

- または、システムコントローラのコマンド行からスイッチをリセットします。

  sc> プロンプトで、次のように入力します。

```
sc>reset sscn/swt
```

  n には、SSC0 と SSC1 のどちらのスイッチをリセットするかによって、0 または 1 を指定します。

A.6 スイッチの IP アドレスおよびネットマスク、デフォルトゲートウェイの設定

1. 次のように入力して、IP アドレスおよびネットマスクを設定します。

```
Console#configure
Console(config)#interface vlan vlan id
Console(config-if)#ip address ip address netmask
Console(config-if)#exit
```

   ここでは、次のように指定します。

   - *vlan id* には、スイッチのネットワーク管理ポート NETMGT を含む VLAN の番号 (デフォルトでは 2) を指定します。出荷時のデフォルト設定を使用している場合は、2 を指定します。
   - *ip address* には、使用するスイッチの IP アドレスを指定します。
   - *netmask* には、設定するネットマスク (255.255.255.0 など) を指定します。

2. デフォルトゲートウェイを設定するには、次のように入力します。

```
Console(config)#ip default-gateway ip address
Console(config)#exit
```

   ip address には、デフォルトゲートウェイとして指定したデバイスの IP アドレスを指定します。

3. デフォルトゲートウェイの設定の変更を確認するには、次のように入力します。

```
Console#show running-config
building running-config, please wait.....
:
!
interface ethernet NETMGT
 description External RJ-45 connector NETPMGT
 switchport allowed vlan add 2 untagged
 switchport native vlan 2
 switchport allowed vlan remove 1
 switchport forbidden vlan add 1
 spanning-tree edge-port
!
interface vlan 2
 ip address 129.156.203.3 255.255.255.0
 ip dhcp client-identifier text SUNW,SWITCH_ID=900002,0
!
!
!
ip default-gateway  129.156.203.8
:
Console#
```

この出力例の「:」記号は、情報が省略されていることを示しています。デフォルトゲートウェイは、show running-config コマンドの出力の終わりの方に表示されます。

A.7 VLAN の設定

デフォルトでは、スイッチには、管理ポート (NETMGT) を含む管理 VLAN (VLAN 2) と、その他のすべてのポートを含むデータ VLAN が設定されています。

VLAN の使用方法については、第 5 章および第 6 章、第 7 章を参照してください。

追加の VLAN を作成するには、VLAN を設定してポートを個別に追加する必要があります。

1. Console# プロンプトで、次のように入力します。

```
Console#configure
```

2. 次のように入力して、VLAN 設定モードに入ります。

```
Console(config)#vlan database
```

3. VLAN を作成します。

```
Console(config-vlan)#vlan vlan identifier media ethernet
```

vlan identifier には、1 ～ 4094 の番号を指定します。

4. VLAN に名前を付けるには、次のように入力します。

```
Console(config-vlan)#vlan vlan identifier name media ethernet
```

vlan identifier には、VLAN の番号を指定し、*name* には、その VLAN 用の名前を指定します。

5. VLAN を個々のポートに追加して作成します。

a. この手順を実行するには、最初に次のように入力して設定モードに戻ります。

```
Console(config-vlan)#exit
```

b. 設定モードに戻ったら、次のように入力してインタフェース設定モードに入ります。

```
Console(config)#interface ethernet port
```

port には、VLAN に含めるポートの番号を指定します。

c. 次のように入力して、VLAN をポートに追加します。

```
Console(config-if)#switchport allowed vlan add vlan identifier
```

d. 新しい VLAN に含める各ポートに対して手順 a ～手順 c を実行します。

A.8 スイッチの設定の保存

注 – 次にスイッチを再起動したときにも保持するスイッチ設定は、保存する必要があります。

- **変更した設定を保存するには、ファームウェアが保持している動作時の設定情報を起動時の設定情報にコピーします。**

  スイッチのコンソールで次のように入力します。

```
Console#copy running-config startup-config
Startup configuration file name [default filename]:filename
Write to FLASH Programming
-Write to FLASH finish
Success

Console#
```

default filename には、現在の起動用構成ファイルが表示されます。*filename* に、新しい起動用構成ファイルの名前を指定します。新しいファイル名を指定せずに ENTER キーを押すと、動作時の設定情報が現在の起動用構成ファイルに書き込まれます。

A.9 最初のスイッチから 2 番目のスイッチへの設定のコピー

あるスイッチの構成ファイルを別のスイッチに転送する手順では、TFTP を使用する必要があります。つまり、スイッチの設定をコピーするには、ネットワーク上で TFTP サーバーを使用できるようにする必要があります。この節では、TFTP サーバーの設定方法について説明します。そのあとで、ファイル転送の実行方法について説明します。

ネットワークの領域をそれぞれ分離するようにスイッチの VLAN を設定し、IPMP (IP ネットワークマルチパス) を使用してサーバーブレードをネットワークに冗長接続している場合は、2 番目のスイッチの設定を最初のスイッチと同一にする必要があります。

注意 – 2 番目の統合スイッチの VLAN 設定が最初のスイッチの VLAN 設定と一致しないと、2 番目のスイッチを通過するデータに、最初のスイッチの VLAN 定義が適用されません。同様に、最初のスイッチを 2 番目のスイッチに複製しないと、最初のスイッチのパケットフィルタによる管理ネットワークの保護が失われます。

Sun Fire B1600 ブレードシステムシャーシの 2 番目のスイッチの設定を最初のスイッチと確実に同一にするために、この節の手順を実行してください。

A.9.1 TFTP サーバーの設定

ネットワーク上の Solaris システムを TFTP 要求に対応するように設定するには、次の手順を実行します。

1. **TFTP サーバーとして設定するシステムに、スーパーユーザーでログインします。**
2. **テキストエディタを使用して、`/etc/inetd.conf` ファイルでコメントになっている次の行を有効にします。**

```
tftp  dgram udp6 wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```

3. **同じシステムの Solaris プロンプトで次のように入力して、TFTP のホームディレクトリを作成します。**

```
# mkdir /tftpboot
# chown root /tftpboot
# chmod 755 /tftpboot
# cd /tftpboot
# ln -s . tftpboot
```

4. **次のように入力して、`inetd` を再起動します。**

```
# pkill -HUP inetd
```

5. **TFTP が動作していることを確認します。**

   確認するには、TFTP を使用して `/tftpboot` ディレクトリからファイルを取り出します。次の手順を実行します。

a. TFTP サーバーとして使用しているシステムで、任意のファイル (Solaris の `/etc/release` ファイルなど) を `/tftpboot` ディレクトリにコピーします。

`/etc/release` ファイルをコピーするには、Solaris プロンプトで次のように入力します。

```
# cp /etc/release /tftpboot/filename
```

filename には、TFTP サーバーから取り出せるようにするファイルの名前を指定します。

b. コピーしたファイルが、すべてのユーザーに対して読み取り専用となるように設定します。

```
# chmod 444 /tftpboot/filename
```

filename には、TFTP サーバーから取り出せるようにするファイルの名前を指定します。

c. 作成した TFTP サーバーからファイルを取り出します。

別のシステムの Solaris プロンプトで、次のコマンドを実行します。

```
% tftp tftp server
tftp>get filename
```

tftp server には、設定した TFTP サーバーが動作しているシステムのホスト名または IP アドレスを指定し、*filename* には、TFTP サーバーから取り出すファイルの名前を指定します。

d. `get` コマンドを実行した Solaris システムで、次のように入力してファイルの内容を確認します。

```
# cat filename
```

filename には、TFTP サーバーから転送したファイルの名前を指定します。

注 – TFTP は FTP とは異なります。TFTP は FTP のようなエラーメッセージを表示しません。また、FTP では使用できる `cd` または `ls` コマンドなどのコマンドの多くは、TFTP では使用できません。

A.9.2 スイッチ構成ファイルの転送

TFTP サーバーを作成し、SSC0 または SSC1 のスイッチの設定を完了したら、スイッチの設定情報を 2 番目のスイッチに複製します。

複製するには、次の手順を実行します。この手順では、SSC0 のスイッチの設定情報を SSC1 のスイッチに複製することを想定していますが、SSC1 のスイッチから SSC0 のスイッチに複製することもできます。

1. 第 2 章および第 3 章、第 5 章、第 6 章、第 7 章の手順を実行して、スイッチ 0 で必要な設定を行います。
2. スイッチ 0 の設定情報を、standard.cfg などの名前の付いたファイルに保存します。

   スイッチの Console# プロンプトで、次のように入力します。

```
Console#copy running-config file
Destination configuration file name: standard.cfg
Write to FLASH Programming
-Write to FLASH finish
Success.

Console#
```

3. standard.cfg ファイルを TFTP サーバーにアップロードします。

   次の手順を実行します。

   a. スーパーユーザーで TFTP サーバーにログインします。

   b. /tftpboot ディレクトリに移動します。

   c. standard.cfg という名前の空ファイルを作成します。

```
#>standard.cfg
```

4. すべてのユーザーがこのファイルに対して読み取りおよび書き込みを行えるように設定します。

```
#chmod 666 standard.cfg
```

5. スイッチのコマンド行インタフェースで、次のように入力します。

```
Console#copy file tftp
Choose file type:
1. config: 2.opcode: <1-2>:1
Source file name: filename
TFTP server ip address: IP address
Desitination file name: filename
Console#
```

2 つの *filename* には、どちらも standard.cfg (スイッチ設定を保存したファイル名) を指定し、*IP address* には TFTP サーバーの IP アドレスを指定します。

6. TFTP サーバーで、テキストエディタを使用して standard.cfg ファイルを開きます。

スイッチ 0 のホスト名のエントリを、スイッチ 1 のホスト名を設定するように変更します。

```
!
hostname host name of switch 1
```

スイッチの IP アドレスを手動で割り当てるように設定している場合は、IP アドレスおよびネットマスクのエントリを、スイッチ 0 ではなくスイッチ 1 の IP アドレスおよびネットマスクに変更する必要があります。

```
interface vlan 2
  ip address ip address  netmask
```

DHCP を使用している場合は、IP アドレスおよびネットマスクや DHCP クライアント識別子を変更する必要はありません。IP アドレスおよびネットマスクは、DHCP サーバーによって自動的に割り当てられます。DHCP クライアント識別子は、スイッチをリセットするときにアクティブシステムコントローラによって自動的に割り当てられます。

7. このファイルに適切な名前 (standard1.cfg など) を付けて保存します。

8. スイッチ 1 にログインします。DHCP によってスイッチに IP アドレスが割り当てられていない場合は、一時的に管理 IP アドレスを設定します。

スイッチ 1 のログインおよびパスワード情報をすでに設定している場合は、その情報を使用してログインします。まだ設定していない場合は、出荷時のデフォルトのユーザー名 (admin) とパスワード (admin) を使用してログインします。

IP のパラメタを設定するには、A-6 ページの A.6 節「スイッチの IP アドレスおよびネットマスク、デフォルトゲートウェイの設定」の手順を実行してください。

9. TFTP サーバーからスイッチ 1 に standard1.cfg をダウンロードします。

次のように入力します。

```
Console#copy tftp file
TFTP server ip address:IP address
Choose file type:
1. config: 2.opcode: <1-2>:1
Source file name:standard1.cfg
Destination file name:standard1.cfg
Console#
```

10. このファイルをスイッチ 1 の起動時の設定情報にします。

次のように入力します。

```
Console#configure
Console(config)#boot system config standard1.cfg
Console(config)#exit
Console#
```

11. スイッチのファームウェアを再起動します。

次のように入力します。

```
Console#reload
```

A.10 回復力と性能を向上させるトランク接続の設定

外部データポートがほかの外部データポートと同じスイッチに接続されている場合は、それらのポートをトランクにまとめることをお勧めします。これによって回復力と性能を向上させることができます。

たとえば、同じ外部スイッチへの 4 つの個別の接続があり、接続の 1 つにケーブルの問題による障害が発生した場合には、切断された接続の通信は失われます。しかし、その外部スイッチへの 4 つの接続を 1 つのトランクにまとめて設定すると、1 つの接続に障害が発生しても、トランクのほかの接続上で通信が継続されます。

接続が切断されないかぎり、統合スイッチはトランクのすべての接続を同じネットワークへの 1 つの広帯域幅の接続として扱います。

注 – 外部スイッチまたはハブ、ルーターへの接続が二重化されていて、それらがトランクにまとめられていない場合は、統合スイッチのスパニングツリー機能によって 1 つを除くすべての接続がブロックされます。したがって、ネットワークの冗長性は残りますが、ブロックされていない 1 つの接続に障害が発生するまで重複する接続は動作しません。

次のコマンド例では、NETP2 および NETP3、NETP4 のポートを使用してトランクを作成しています。

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet NETP2
Console(config-if)#channel-group 1
Console(config-if)#exit
Console(config)#interface ethernet NETP3
Console(config-if)#channel-group 1
Console(config-if)#exit
Console(config)#interface ethernet NETP4
Console(config-if)#channel-group 1
Console(config-if)#exit
Console(config)#
```

A.11 スイッチのパケットフィルタを使用したブレードの安全な管理

スイッチは、パケットフィルタを備えています。デフォルトでは、パケットフィルタは、サーバーブレードからスイッチの管理ポート (NETMGT) へのすべてのトラフィックをブロックします。これによって、サーバーブレードから管理ネットワークへの不当な攻撃 (ハッカーによるパブリックネットワークからブレードへのアクセスなど) を回避できます。ただし、管理トラフィックがサーバーブレードから管理ポートへ通過できるようにパケットフィルタを設定しないと、管理ポートを介してサーバーブレードと直接通信することはできません。この節では、パケットフィルタを設定する方法について説明します。

注 – デフォルトでは、パケットフィルタは、サーバーブレードから管理ポート (NETMGT) へのトラフィックの通過を許可しません。トラフィックがパケットフィルタを通過できるように設定するときには、十分に注意して、常に必要なプロトコルだけを使用可能にしてください。

次の手順では、DHCP および BOOTP、TFTP、SunRPC、SNMP、NFS のフレームを、パケットフィルタを介してサーバーブレードから管理ポートへ通過できるようにするためのコマンドについて説明します。これは、管理ポートを介してサーバーブレードを管理するために必要な、最小限のプロトコルです。

1. DHCP および BOOTP のフレームがパケットフィルタを通過できるように設定します。

   スイッチのコンソールで、次のように入力します。

```
Console#configure
Console(config)#ip filter permit udp 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 67-68
```

2. TFTP フレームがパケットフィルタを通過できるように設定します。

   次のように入力します。

```
Console#configure
Console(config)#ip filter permit udp 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 69
Console(config)#ip filter permit udp 0.0.0.0 0.0.0.0 1024-65535
0.0.0.0 0.0.0.0 1024-65535
```

3. SunRPC フレームがパケットフィルタを通過できるように設定します。

   次のように入力します。

```
Console#configure
Console(config)#ip filter permit udp 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 111
Console(config)#ip filter permit tcp 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 111
```

4. SNMP フレームがパケットフィルタを通過できるように設定します。

次のように入力します。

```
Console#configure
Console(config)#ip filter permit udp 0.0.0.0 0.0.0.0 161 0.0.0.0
0.0.0.0
Console(config)#ip filter permit tcp 0.0.0.0 0.0.0.0 161 0.0.0.0
0.0.0.0
Console(config)#ip filter permit udp 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 162
Console(config)#ip filter permit tcp 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 162
```

注 – 161 ポートは管理されるデバイスの SNMP 要求用のポートで、162 ポートは管理されるデバイスの SNMP トラップ用のポートです。SNMP トラップは、管理されるデバイスから送信されます。SNMP コマンドは、SNMP 管理ホストから発行されます。

---

5. NFS フレームがパケットフィルタを通過できるように設定します。

次のように入力します。

```
Console#configure
Console(config)#ip filter permit udp 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 2049
Console(config)#ip filter permit tcp 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 2049
```

注 – `ip filter permit` コマンドの使用方法の詳細は、『Sun Fire B1600 ブレードシステムシャーシスイッチ管理マニュアル』を参照してください。特定のプロトコルに関連するポート番号のリストについては、UNIX システムの `/etc/services` ファイルまたは `/etc/inet/services` ファイルを参照してください。IP サービスに関連するすべてのポート番号のリストについては、Internet Assigned Numbers Authority の Web サイト (`http://www.iana.org`) を参照してください。

A.12 スイッチの名前付きユーザーの設定

1. スイッチのコンソールで、次のように入力します。

```
Console#configure
```

2. 次のように入力します。

```
Console(config)#username username access-level 15
```

username には、ログインするときに入力するユーザー名を指定します。

この最初のコマンドの 15 は、新しいユーザーに特権実行モードへのアクセス権を付与することを示します。ユーザーに通常実行モードへのアクセス権のみを付与するには、15 ではなく 0 を指定してください。

3. 次のように入力します。

```
Console(config)#username username password 0 password
```

username には、ログインするときに入力するユーザー名を指定し、*password* には、新しいユーザーのパスワードを指定します。

このコマンドの 0 は、*password* に指定した文字が暗号化されていないことを示します。値を暗号化形式で入力する場合は、パスワードとする暗号化テキストの前に 7 を指定して、暗号化形式であることを示す必要があります。

A.12.1 スイッチのデフォルトユーザー名およびパスワード

フルアクセス権を持つデフォルトユーザー名は、admin です。
パスワードは、admin です。

限定された権限を持つゲストアクセス用のデフォルトユーザー名は、guest です。
パスワードは、guest です。

ゲストアクセスからフルアクセスに切り替える enable コマンドのデフォルトのパスワードは、super です。

A.13 スイッチおよびその設定に関する情報の表示

この節の内容は、次のとおりです。

A.13.1 IP アドレスおよび VLAN ID の確認

- 管理ポートの IP アドレスおよび VLAN ID を確認するには、Console# プロンプトで次のように入力します。

```
Console#show ip interface
 IP address and netmask: 129.156.223.215 255.255.255.0 on VLAN 2,
 and address mode: User specified.
```

A.13.2 VLAN 設定の確認

- スイッチの VLAN 設定を確認するには、Console# プロンプトで次のように入力します。

```
Console#show vlan

VLAN Type    Name              Status    Ports/Channel groups
---- ------- ----------------- --------- -----------------------------------
   1  Static      DefaultVlan   Active   SNP0    SNP1    SNP2    SNP3    SNP4
                                         SNP5    SNP6    SNP7    SNP8    SNP9
                                         SNP10   SNP11   SNP12   SNP13   SNP14
                                         SNP15   NETP0   NETP1   NETP2   NETP3
                                         NETP4   NETP5   NETP6   NETP7
   2  Static         MgtVlan   Active  NETMGT
```

A.13.3 ログインしているユーザーの確認

- コマンド行インタフェースおよび Web インタフェースにログインしているユーザーを確認するには、Console# プロンプトで次のように入力します。

```
Console#show users
Username accounts:
  Username Privilege
  -------- ---------
     admin        15
     guest         0

 Online users:
  Line        Username Idle time (h:m:s) Remote IP addr.
  ----------- -------- ----------------- ---------------
* 0   console    admin           0:00:00
```

A.13.4 現在または起動時の設定情報の確認

- 現在のスイッチの設定を表示するには、Console# プロンプトで次のように入力します。

```
Console#show running-config
```

最後にスイッチを起動したあとでスイッチの設定を変更した場合、この動作時の設定は起動時の設定と異なります。

- 最後に起動したときのスイッチの設定 (次に起動するときに使用する設定) を表示するには、Console# プロンプトで次のように入力します。

```
Console#show startup-config
```

A.13.5　ファームウェアバージョンの確認

- ファームウェアなどのバージョン情報を確認するには、Console# プロンプトで次のように入力します。

```
Console#show version

Unit1
 Serial number           :
 Service tag             :
 Hardware version        :r0b
 Number of ports         :25
 Main power status       :up
 Redundant power status  :not present

Agent(master)
 Unit id                 :1
 Loader version          :0.0.6.7
 Boot rom version        :1.0.0.8
 Operation code version  :1.0.0.6
Console#
```

A.13.6 MAC アドレスおよび一般的なシステム情報の確認

- MAC アドレスおよび一般的なシステム情報を確認するには、Console# プロンプトで次のように入力します。

```
Console#show system

System description: Sun Fire B1600
System OID string: 1.3.6.1.4.1.42.2.24.1

System information

 System Up time: 0 days, 7 hours, 41 minutes, and 4.4 seconds
 System Name             : [NONE]
 System Location         : [NONE]
 System Contact          : [NONE]
 MAC address             : 08-00-20-7A-92-0B
 Web server              : enable
 Web server port         : 80
 Web secure server       : enable
 Web secure server port  : 443

 POST result

--- Performing Power-On Self Tests (POST) ---
UART Loopback Test ..................... PASS
Timer Test ............................. PASS
DRAM Test .............................. PASS
I2C Initialization ..................... PASS
Runtime Image Check .................... PASS
PCI Device Check ....................... PASS
AN983 Initialization ................... PASS
AN983 Internal Loopback Test ........... PASS
Switch Driver Initialization ........... PASS
Switch Internal Loopback Test .......... PASS
------------------- DONE --------------------
Console#
```

付録B

ラップトップを使用したシステムコントローラへのシリアル接続の設定

この付録では、シャーシのコマンド行管理インタフェースにアクセスするため、ラップトップコンピュータから Sun Fire B1600 ブレードシステムシャーシの 2 台のスイッチ/システムコントローラ (SSC) モジュールの一方に接続する方法について説明します。

この付録は次の節で構成されています。

注 – この付録の手順を実行する前に、ブレードシステムシャーシをラックまたはキャビネットに取り付けておいてください (『Sun Fire B1600 ブレードシステムシャーシハードウェア設置マニュアル』を参照)。

B.1 ラップトップへの接続

注 – ラップトップのパラレルポート (25 ピン) は使用せず、シリアルポートを使用してください。シリアルポートは、9 ピン D タイプのオスコネクタです。

1. RJ-45−RJ-45 パッチケーブル (シャーシに付属) を、SSC のシリアルポートに接続します。
2. パッチケーブルのもう一方の端を、Sun Fire B1600 に付属する銀色の DB-25 (25 ピン DSUB オス/メス 8 POS RJ-45) アダプタ (パーツ番号 530-2889-0x) の RJ-45 コネクタに差し込みます。

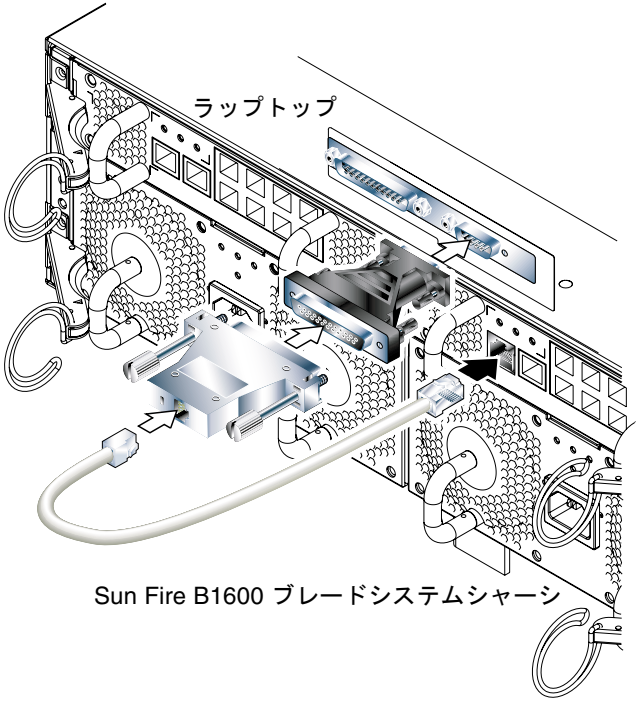

図 B-1　SSC からラップトップのシリアルポートへの接続

3. **25 ピン D タイプのオスコネクタを、一方が 25 ピンメスコネクタで、もう一方が 9 ピン D タイプメスコネクタのアダプタに差し込みます。**

   サンは、25 ピン D タイプメス−9 ピン D タイプメスのアダプタを提供していません。このようなアダプタは、家庭用コンピュータの販売店および電気店で購入できます。表 B-1 に、このアダプタに要求されるピンの相互接続を示します。

表 B-1　25 ピン D タイプメス−9 ピン D タイプメスアダプタのピンの相互接続

9 ピンメスコネクタ	25 ピンメスコネクタ
ピン 1	ピン 8
ピン 2	ピン 3
ピン 3	ピン 2
ピン 4	ピン 20
ピン 5	ピン 7
ピン 6	ピン 6
ピン 7	ピン 4
ピン 8	ピン 5
ピン 9	ピン 22

4. **最後に、9 ピンメスコネクタをラップトップのシリアルポートに接続します。**

B.1.1　Microsoft Windows のハイパーターミナルの使用

注 – 通常、ラップトップのシリアルポートを携帯型装置に接続している場合は、ここで説明する手順を実行する前に、Hot Sync Manager を終了する必要があります。Hot Sync Manager を終了しないと、Sun Fire B1600 ブレードシステムシャーシとの通信に、シリアルポートを使用できません。

ここで説明する手順は、Microsoft Windows 98 および HyperTerminal Applet バージョン 3.0 が動作するラップトップ PC 上で確認したものです。

1. **Windows の ハイパーターミナルユーティリティーを起動します。**
2. **「HyperTerminal」ウィンドウで、Hypertrm.exe のアイコンをダブルクリックします。**

3. 「Connection Description」ウィンドウで、ラップトップ上で作成するハイパーターミナル接続の名前を指定します。

   アイコンを選択して「OK」をクリックします。

4. 「Connect to...」ウィンドウで、「Connect using」オプションの矢印をクリックし、サーバーへの接続に使用するポートを選択します。

   特にほかのポートを使用する理由がないかぎり、「DIRECT TO COM1」を選択します。「OK」をクリックします。

5. 「COM1 Properties Port Settings」ウィンドウで、パラメタを次のように設定します。

   Bits per second : 9600
   Data bits : 8
   Parity: None
   Stop bits : 1
   Flow control : Xon/Xoff または None

注 – フロー制御オプションで、「Hardware」を選択しないでください。

   「OK」をクリックします。

6. これで、ハイパーターミナルセッションがアクティブになりました。「File」メニューから「Properties」を選択します。

7. 「Properties」ウィンドウで、「Settings」タブをクリックします。

   「Settings」タブで、「Emulation」オプションの矢印をクリックし、「VT100」を選択します。「Telnet terminal」オプションでは、「VT100」を指定します。「OK」をクリックします。

注 – これで、Sun Fire B1600 ブレードシステムシャーシおよび各ブレードのソフトウェアを設定する準備ができました (第 2 章を参照)。

付録C

サーバーブレードに IP アドレスを割り当てる DHCP の設定

この付録は、『Solaris のインストール (上級編)』および『Solaris DHCP の管理』の説明を補足します。この付録の手順を実行すると、システムシャーシのサーバーブレードが IP アドレスを動的に受け取るように、データネットワーク上のネットワークインストールサーバーおよび DHCP サーバーを設定できます。

この手順では、ネットワークインストールサーバーに Solaris イメージが追加されていて、データネットワーク上に DHCP サーバーが存在することを前提としています。

この付録は次の節で構成されています。

C.1 ネットワークインストールサーバーでの作業

- **ネットワークインストールサーバーで、`add_install_client` に `-d` オプションを指定して実行します。**

  このコマンドは、DHCP 対応の `inetboot` ファイルを、Solaris イメージから `/tftpboot` ディレクトリへコピーします。このコマンドを実行するには、次のように入力します。

```
# cd path/Solaris_8/Tools
# ./add_install_client -d -s installserv:/images/2.8 -c
configsrv:/config -p configsrv:/config SUNW.Serverblade1 sun4u

To enable SUNW.Serverblade1 in the DHCP server, add an entry to
the server with the following data:

Install server      (SinstNM)  : installserv
Install server IP   (SinstIP4) : 192.168.160.12
Install server path (SinstPTH) : /images/2.8
Root server name    (SrootNM)  : installserv
Root server IP      (SrootIP4) : 192.168.160.12
Root server path    (SrootPTH) : /images/2.8/Solaris_8/Tools/Boot
Profile location    (SjumpsCF) : configsrv:/config
sysidcfg location   (SsysidCF) : configsrv:/config
```

  path には、ネットワークインストールサーバーの Solaris イメージの位置を指定します。この例の 2 番目のコマンドは、2 行に渡っています。この出力例には、構成例の IP データが表示されています。

C.2 DHCP サーバーでの作業

1. **DHCP サーバーで、Solaris JumpStart の実行中にブレードに渡すオプションを作成します。**

   この情報は、DHCP を使用せずに JumpStart を実行したときには `/etc/bootparams` ファイルから収集されます。

表 C-1 に、作成する必要のあるオプションを示します。

表 C-1 JumpStart の実行中にブレードに渡す必要のある DHCP オプション

オプション名	説明
SrootIP4	root サーバーの IP アドレス
SrootNM	root サーバーのホスト名
SrootPTH	起動イメージへのパス (/images/2.8/Solaris_8/Tools/Boot など)
SinstIP4	ネットワークインストールサーバーの IP アドレス
SinstNM	ネットワークインストールサーバーのホスト名
SsysidCF	sysidcfg ファイルの位置 (configsrv:/config など)
SjumpsCF	プロファイルおよび rules.ok ディレクトリの位置 (configsrv:/config など)
SbootFIL	カーネルへのパス (/platform/sun4u/kernel/sparcv9/uni など)
Sterm	インストール時に使用する端末の種類

次に、表 C-1 のオプションを作成するためのコマンドの例を示します。

```
# dhtadm -A -s SrootIP4 -d 'Vendor=SUNW.Serverblade1,2,IP,1,1'
# dhtadm -A -s SrootNM -d 'Vendor=SUNW.Serverblade1,3,ASCII,1,0'
# dhtadm -A -s SrootPTH -d 'Vendor=SUNW.Serverblade1,4,ASCII,1,0'
# dhtadm -A -s SbootFIL -d 'Vendor=SUNW.Serverblade1,7,ASCII,1,0'
# dhtadm -A -s SinstIP4 -d 'Vendor=SUNW.Serverblade1,10,IP,1,1'
# dhtadm -A -s SinstNM -d 'Vendor=SUNW.Serverblade1,11,ASCII,1,0'
# dhtadm -A -s SinstPTH -d 'Vendor=SUNW.Serverblade1,12,ASCII,1,0'
# dhtadm -A -s SsysidCF -d 'Vendor=SUNW.Serverblade1,13,ASCII,1,0'
# dhtadm -A -s SjumpsCF -d 'Vendor=SUNW.Serverblade1,14,ASCII,1,0'
# dhtadm -A -s Sterm -d 'Vendor=SUNW.Serverblade1,15,ASCII,1,0'
```

2. 必要なオプションを含むマクロを作成します。これに、手順 1 で作成したオプションを含めます。

表 C-2 作成する必要のあるマクロ

マクロ名	マクロの内容 (マクロにほかのマクロを含めることもできます)
Solaris	SrootIP4、SrootNM、SinstIP4、SinstNM、Sterm、SjumpsCF、SsysidCF
sparc	SrootPTH、SinstIP4

表 C-2　作成する必要のあるマクロ (続き)

マクロ名	マクロの内容 (マクロにほかのマクロを含めることもできます)
sun4u	Solaris、sparc
SUNW.Serverblade1	SbootFIL、sun4u
*network name**	Subnet、Router、Broadcst、BootSrvA

**network name* には、クライアントが接続しているネットワークを特定する IP アドレスを指定します。これらのマクロの 1 つを、各クライアントのサブネットに対して作成する必要があります。ただし、DHCP サーバーの一次インタフェースを含むサブネットは除きます。

次に、必要なマクロを作成するコマンドの例を示します。

```
# dhtadm -A -m Solaris -d
':SrootIP4=192.168.160.12:SrootNM="bootsrv":SinstIP4=192.168.160
.15:SinstNM="installsrv":Sterm="xterm":SjumpsCF="configsrv:/conf
ig":SsysidCF="configsrv:/config":'
# dhtadm -A -m sparc -d
':SrootPTH="/images/2.8/Solaris_8/Tools/Boot":SinstPTH="/images/
2.8":'
# dhtadm -A -m sun4u -d ':Include=Solaris:Include=sparc:'
# dhtadm -A -m SUNW.Serverblade1 -d
':SbootFIL="/platform/sun4u/kernel/sparcv9/unix":Include=sun4u:'
# dhtadm -A -m 192.168.160.0 -d
':Subnet=255.255.255.0:Router=192.168.160.254:Broadcst=192.168.1
60.255:BootSrvA=192.168.160.12:'
```

3. **クライアントのホスト名および IP アドレスをホストデータベース (`/etc/hosts`) に追加します。**

4. **`SUNW.Serverblade1` マクロをクライアントに割り当てます。**

   次のように入力します。

```
# pntadm -A dhcpclient01 -i 01MACaddress -m SUNW.Serverblade1 -s
DHCP server network name
```

   次のように指定します。

   MACaddress には、クライアントの MAC アドレスを指定します。

   DHCP server には、DHCP サーバーのホスト名を指定します。

   network name には、クライアントが接続しているネットワークを特定する IP アドレスを指定します (このコマンド例では、2 行に渡って表示されています)。

C.3 サーバーブレードでの作業

各サーバーブレードに 2 つの IP アドレスが設定されているネットワーク環境では、この節の手順を実行してください。この手順は、設定しているサーバーブレードがネットワークから起動していて、その一次インタフェース (ce0) に IP のパラメタが設定されていることを前提としています。

1. **システムコントローラの** sc> **プロンプトから、ブレードのコンソールにアクセスします。**

   次のように入力します。

```
sc> console sn
```

   n には、設定しているブレードのスロット番号を指定します。

2. Solaris プロンプトで、次のように入力します。

```
# ifconfig ce1 plumb
```

3. 最後に、次のように入力します。

```
# ifconfig ce1 auto-dhcp up
```

付録 D

Web Start のフラッシュアーカイブを使用した Solaris ブレードの設定

この付録は、『Solaris のインストール (上級編)』のネットワークインストールサーバーの設定手順を補足します。

ネットワークインストールサーバーから最初の Solaris ブレードを起動したときに、ブレード上で実行するアプリケーションソフトウェアを追加し、次に『Solaris のインストール (上級編)』の手順を実行して、Web Start のフラッシュアーカイブを作成することができます。

Sun Fire B1600 ブレードシステムシャーシに取り付けた Sun Fire B100s Solaris サーバーブレードの Web Start フラッシュアーカイブを使用すると、あるブレードのオペレーティング環境およびアプリケーションソフトウェアをほかのブレードに複製できます。

この付録は次の節で構成されています。

D.1 Web Start のフラッシュアーカイブを使用したブレードの迅速な設定

フラッシュアーカイブとは Solaris システムのスナップショットです。そのため、フラッシュアーカイブには、システムのすべてのファイル (正確には、指定したすべてのファイル) が含まれます。フラッシュアーカイブは、すべてのソフトウェアをブレードにインストールしたあと、ブレードを使用する前に作成する必要があります。インストールしたソフトウェアおよびブレードの使用目的によっては、そのソフトウェアをインストールしたあと、設定を行う前にフラッシュアーカイブを作成する必要がある場合があります。たとえば、データベースサーバーの場合は、データベース管理ソフトウェアをインストールしたあと、データベースを作成する前にフラッシュアーカイブを作成します。

ブレードで実行するソフトウェアアプリケーションが決まっていない場合は、Web Start でフラッシュアーカイブを使用して、複数のブレードに Solaris を複製できます。この方法は、JumpStart を個々に実行する方法よりも迅速です。

D.1.1 Web Start のフラッシュアーカイブの作成

ブレードのソフトウェアのフラッシュアーカイブを作成する方法については、『Solaris 8 のインストール (上級編)』のフラッシュアーカイブの作成手順を参照してください。

D.1.2 アーカイブしたブレードイメージの別のブレードへのインストール

アーカイブしたイメージを別のブレードへインストールする方法については、『Solaris 8 のインストール (上級編)』のフラッシュアーカイブのインストール手順を参照してください。

D.1.3 Web Start のフラッシュアーカイブインストールの高速化

サーバーブレード間の Gigabit インターコネクトを利用すると、Web Start のフラッシュアーカイブインストールを高速化できます。

Gigabit インターコネクトを利用するには、NFS を使用して、作成したフラッシュアーカイブの位置を共有します (つまり、最初のブレードのソフトウェアのアーカイブされたイメージを共有します)。次の手順を実行します。

1. イメージの複製元になるブレードの Solaris プロンプトで、次のように入力します。

```
#share -F ufs flash location
```

flash location には、ブレードのフラッシュアーカイブの位置を指定します。たとえば、次のように入力します。

```
#share -F ufs /var/tmp
```

2. ネットワークインストールサーバーでインストールプロファイルを変更して、最初のブレードのフラッシュアーカイブの位置を指定します。

付録 E

システムコントローラコマンド

この付録では、システムコントローラの sc> プロンプトから実行できるコマンドの一覧を示します。

この付録は次の節で構成されています。

E.1 シャーシ全体の電源に関するコマンド

注 – アクティブシステムコントローラを除くすべてのコンポーネントの電源は、一度に切断する (停止して取り外し可能またはスタンバイの状態にする) ことができます。ブレードシステムシャーシは、アクティブシステムコントローラの電源を 1 回のコマンドで切断または停止できないように設計されています。アクティブシステムコントローラの電源を停止する方法については、『Sun Fire B1600 ブレードシステムシャーシ管理マニュアル』を参照してください。

表 E-1 すべてのコンポーネントの電源を投入または切断、停止するためのコマンド

コマンドおよびオプション (ある場合)	コマンドの説明
`sc> poweron ch`	すべてのコンポーネントの電源を入れます。このコマンドを実行すると、すべてのコンポーネントを、電源停止または取り外し可能、スタンバイの状態から一度に回復できます。
`sc> poweroff ch`	アクティブシステムコントローラを除く、シャーシのすべてのコンポーネントの電源を切ります。
`sc> poweroff -f ch`	コンポーネントのオペレーティングシステムが正常に停止できなかった場合でも、アクティブシステムコントローラを除くすべてのコンポーネントの電源を切ります。
`sc> poweroff -y ch`	確認のプロンプトを表示せずに、アクティブシステムコントローラを除くすべてのコンポーネントの電源を切ります。
`sc> poweroff -s ch`	アクティブシステムコントローラを除くすべてのコンポーネントの電源を停止して、スタンバイモードにします (`standbyfru ch` コマンドと同じ機能)。
`sc> poweroff -r ch`	アクティブシステムコントローラを除くすべてのコンポーネントの電源を停止して、安全に取り外せる状態にします。`-r` オプションを指定することで、各コンポーネントの取り外し可能 LED も点灯します (`removefru ch` コマンドと同じ機能)。
`sc> standbyfru ch`	アクティブシステムコントローラを除くすべてのコンポーネントの電源を停止して、スタンバイモードにします (`poweroff -s ch` コマンドと同じ機能)。
`sc> standbyfru -f ch`	コンポーネントのオペレーティングシステムが正常に停止できなかった場合でも、アクティブシステムコントローラを除くすべてのコンポーネントの電源を停止して、スタンバイモードにします。

表 E-1 すべてのコンポーネントの電源を投入または切断、停止するためのコマンド (続き)

コマンドおよびオプション (ある場合)	コマンドの説明
`sc> standbyfru -y ch`	確認のプロンプトを表示せずに、アクティブシステムコントローラを除くすべてのコンポーネントの電源を停止して、スタンバイモードにします。
`sc> removefru ch`	アクティブシステムコントローラを除くすべてのコンポーネントの電源を停止して、安全に取り外せる状態にします。このコマンドを実行すると、各コンポーネントの取り外し可能 LED も点灯します (`poweroff -r ch` コマンドと同じ機能)。
`sc> removefru -f ch`	システムコントローラのオペレーティングシステムが正常に停止できなかった場合でも、アクティブシステムコントローラを除くすべてのコンポーネントの電源を停止して、安全に取り外せる状態にします。このコマンドを実行すると、各コンポーネントの取り外し可能 LED も点灯します。
`sc> removefru -y ch`	確認のプロンプトを表示せずに、アクティブシステムコントローラを除くすべてのコンポーネントの電源を停止して、安全に取り外せる状態にします。このコマンドを実行すると、各コンポーネントの取り外し可能 LED も点灯します。

E.2 システムコントローラの電源に関するコマンド

注 – 電源の切断または停止ができるのは、スタンバイシステムコントローラだけです。アクティブシステムコントローラの電源を停止する方法については、『Sun Fire B1600 ブレードシステムシャーシ管理マニュアル』を参照してください。

表 E-2 SSC の電源を投入または切断、停止するためのコマンド

コマンドおよびオプション (ある場合)	コマンドの説明
`sc> poweron sscn`	SSC*n* の電源を入れます。*n* にはスタンバイシステムコントローラの番号 (スタンバイシステムコントローラが SSC0 または SSC1 のどちらにあるかに応じて、0 または 1) を指定します。このコマンドを実行すると、スタンバイ SSC を、電源停止または取り外し可能、スタンバイの状態から回復できます。
`sc> poweroff sscn`	SSC*n* の電源を切ります。*n* には、スタンバイシステムコントローラが SSC0 または SSC1 のどちらにあるかに応じて、0 または 1 を指定します。
`sc> poweroff -f sscn`	システムコントローラのオペレーティングシステムが正常に停止できなかった場合でも、スタンバイシステムコントローラ (SSC0 または SSC1) の電源を切ります。
`sc> poweroff -y sscn`	確認のプロンプトを表示せずに、スタンバイシステムコントローラ (SSC0 または SSC1) の電源を切ります。
`sc> poweroff -s sscn`	スタンバイシステムコントローラ (SSC0 または SSC1) の電源を停止して、スタンバイ電力モードにします (`standbyfru` コマンドと同じ機能)。
`sc> poweroff -r sscn`	スタンバイシステムコントローラの電源を停止して、安全に取り外せる状態にします。`-r` オプションを指定することで、取り外し可能 LED も点灯します(`removefru` コマンドと同じ機能)。
`sc> standbyfru sscn`	スタンバイシステムコントローラの電源を停止して、スタンバイ電力モードにします (`poweroff -s` コマンドと同じ機能)。

表 E-2　SSC の電源を投入または切断、停止するためのコマンド (続き)

コマンドおよびオプション (ある場合)	コマンドの説明
`sc> standbyfru -f sscn`	オペレーティングシステムが正常に停止できなかった場合でも、スタンバイシステムコントローラの電源を停止して、スタンバイ電力モードにします。
`sc> standbyfru -y sscn`	確認のプロンプトを表示せずに、スタンバイシステムコントローラの電源を停止して、スタンバイ電力モードにします。
`sc> removefru sscn`	スタンバイシステムコントローラの電源を停止して、安全に取り外せる状態にします。このコマンドを実行すると、SSC の背面パネルにある取り外し可能 LED も点灯します (`poweroff -r` コマンドと同じ機能)。
`sc> removefru -f sscn`	システムコントローラのオペレーティングシステムが正常に停止できなかった場合でも、スタンバイシステムコントローラの電源を停止して、安全に取り外せる状態にします。このコマンドを実行すると、SSC の背面パネルにある取り外し可能 LED も点灯します。
`sc> removefru -y sscn`	確認のプロンプトを表示せずに、スタンバイシステムコントローラの電源を停止して、安全に取り外せる状態にします。このコマンドを実行すると、SSC の背面パネルにある取り外し可能 LED も点灯します。

E.3 サーバーブレードの電源に関するコマンド

表 E-3　サーバーブレードの電源を投入または切断、停止するためのコマンド

コマンドおよびオプション (ある場合)	コマンドの説明
`sc> poweron s`*n*	スロット *n* のブレードの電源を入れます。このコマンドを実行すると、ブレードを、電源停止または取り外し可能、スタンバイ電源の状態から回復できます。
`sc> poweroff s`*n*	スロット *n* のブレードの電源を切ります。
`sc> poweroff -f s`*n*	ブレードのオペレーティングシステムが正常に停止できなかった場合でも、スロット *n* のブレードの電源を切ります。
`sc> poweroff -y s`*n*	確認のプロンプトを表示せずに、スロット *n* のブレードの電源を切ります。
`sc> poweroff -s s`*n*	スロット *n* のブレードの電源を停止して、スタンバイモードにします (`standbyfru` コマンドと同じ機能)。
`sc> poweroff -r s`*n*	スロット *n* のブレードの電源を停止して、安全に取り外せる状態にします。`-r` オプションを指定することで、ブレードの正面にある青色の取り外し可能 LED も点灯します (`removefru` コマンドと同じ機能)。
`sc> standbyfru s`*n*	スロット *n* のブレードの電源を停止して、スタンバイモードにします (`poweroff -s` コマンドと同じ機能)。
`sc> standbyfru -f s`*n*	ブレードのオペレーティングシステムが正常に停止できなかった場合でも、スロット *n* のブレードの電源を停止して、スタンバイモードにします。
`sc> standbyfru -y s`*n*	確認のプロンプトを表示せずに、スロット *n* のブレードの電源を停止して、スタンバイモードにします。

表 E-3　サーバーブレードの電源を投入または切断、停止するためのコマンド (続き)

コマンドおよびオプション (ある場合)	コマンドの説明
sc> removefru s*n*	スロット *n* のブレードの電源を停止して、安全に取り外せる状態にします。このコマンドを実行すると、ブレードの正面にある青色の取り外し可能 LED も点灯します (poweroff -r コマンドと同じ機能)。
sc> removefru -f s*n*	スロット *n* のブレードの電源を停止して、安全に取り外せる状態にします。このコマンドは、ブレードのオペレーティングシステムが正常に停止できなかった場合でも、電源を停止します。このコマンドを実行すると、ブレードの正面にある青色の取り外し可能 LED も点灯します。
sc> removefru -y s*n*	確認のプロンプトを表示せずに、スロット *n* のブレードの電源を停止して、安全に取り外せる状態にします。このコマンドを実行すると、ブレードの正面にある青色の取り外し可能 LED も点灯します。

E.4 システムコントローラおよびスイッチ、ブレードのリセットに関するコマンド

表 E-4　システムシャーシのコンポーネントをリセットするためのコマンド

コマンドおよびオプション (ある場合)	コマンドの説明
sc> reset s*n*	スロット *n* のサーバーブレードをリセットします。
sc> reset s*n* s*y*	スロット *n* および *y* のサーバーブレードをリセットします。リセットするブレードを空白文字で区切って指定します。
sc> reset -y s*n*	確認のプロンプトを表示せずに、スロット *n* のブレードをリセットします。
sc> reset -x s*n*	スロット *n* のブレードの外部強制リセットを実行します。
sc> reset ssc*n*/swt	SSC*n* のスイッチをリセットします。*n* には、0 または 1 を指定します。
sc> reset -y ssc*n*/swt	確認のプロンプトを表示せずに、SSC*n* のスイッチをリセットします。
sc> reset -x ssc*n*/swt	SSC*n* のスイッチの外部強制リセットを実行します。
sc> reset ssc*n*/sc	スタンバイシステムコントローラをリセットします。*n* には、スタンバイシステムコントローラが SSC0 または SSC1 のどちらにあるかに応じて、0 または 1 を指定します。
sc> reset -f ssc*n*/sc	オペレーティングシステムが正常に停止できなかった場合でも、スタンバイシステムコントローラを強制的にリセットします。*n* には、スタンバイシステムコントローラが SSC0 または SSC1 のどちらにあるかに応じて、0 または 1 を指定します。このコマンドを実行すると、同じ SSC 装置内のスイッチもリセットされます。
sc> resetsc	アクティブシステムコントローラをリセットします。このリセットは、どちらのスイッチにも影響を与えません。このコマンドを実行してシステムコントローラをリセットすると、ユーザーセッションが失われます。

表 E-4　システムシャーシのコンポーネントをリセットするためのコマンド (続き)

コマンドおよびオプション (ある場合)	コマンドの説明
sc> reset ssc*n*	スタンバイシステムコントローラ (*n* にアクティブシステムコントローラを指定することはできない) および両方のスイッチ、シャーシに取り付けられたすべてのサーバーブレードをリセットします。
sc> resetsc -y	確認のプロンプトを表示せずに、アクティブシステムコントローラをリセットします。
sc> break s*n*	Solaris が動作していて、break コマンドによって終了するように設定されている場合は、このコマンドを実行すると、Solaris の起動モードに応じて Solaris ブレードが Solaris から kadb または OBP のいずれかに戻ります。
sc> break -y s*n*	前述のコマンドと同じ機能ですが、-y オプションを指定することで、break コマンドの実行を確認するプロンプトが表示されません。
sc> break s*n* s*y* s*x*	前述のコマンドと同じ機能ですが、このコマンドの対象は、ブレード *n* および *y*、*x* になります。

E.5 監視に関するコマンド

表 E-5 シャーシおよびコンポーネントを監視するためのコマンド

コマンドおよびオプション (ある場合)	コマンドの説明
`showsc [-v]`	アクティブシステムコントローラの設定の概要を表示します。
`showplatform [-v]`	各コンポーネントの状態 (Ok、Faulty、Not Present) を表示します。また、シャーシ内のすべてのドメイン (システムコントローラおよびスイッチ、ブレード) のオペレーティングシステムの状態も表示します。-v オプションを指定すると、コンポーネントの一次 MAC アドレスおよびシリアル番号も表示されます。
`showenvironment [-v] {[ssc`*n*`][ps`*n*`][s`*n*`]}`	シャーシのさまざまなコンポーネントの環境センサーの状態を表示します。コンポーネントの内部温度、ファンの回転速度、電源供給経路の電流レベルなどを表示します。
`showfru [-g] {ssc`*n*`|s`*n*`|ch|ps`*n*`}`	指定したコンポーネントまたはすべてのコンポーネントの FRUID データベースの内容を表示します。各コンポーネントは、自身の詳細な情報を保持しています。この情報には、静的データ (ハードウェアのバージョン情報など) と、動的データ (そのコンポーネントが生成した最新のイベントメッセージなど) が含まれています。-g オプションを指定すると、行数を指定して、その行数分の情報の出力後一時停止させることができます。
`showdate`	システムコントローラの現在の日付および時刻を、UTC 形式で表示します。
`showlogs [-b]|[-e] [-g] [-v] {ssc`*n*`|s`*n*`}`	指定したブレードまたはスイッチ、システムコントローラの記録されたイベントを表示します。-b を指定すると、最初の *n* 件のイベントが表示されます。-e を指定すると、最後の *n* 件のイベントが表示されます。-g を指定すると、行数を指定して、その行数分の情報の出力後一時停止させることができます。-v を指定すると、ログ内のすべてのイベントが表示されます。
`showlocator`	ロケータの点灯または消灯を表示します。

表 E-5　シャーシおよびコンポーネントを監視するためのコマンド (続き)

コマンドおよびオプション (ある場合)	コマンドの説明
`consolehistory [-b]|[-e] [-g] [boot|run] sscn/swt|sn`	スイッチまたはブレードのコンソールの起動時バッファーまたは動作中バッファーの内容を表示します。-b を指定すると、最初の *n* 件の情報が表示されます。-e を指定すると、最後の *n* 件の情報が表示されます。-g を指定すると、行数を指定して、その行数分の情報の出力後一時停止させることができます。
`showusers`	システムコントローラに現在ログインしているユーザーを表示します。
`usershow [username]`	指定したユーザーのログインアカウントの詳細を表示します。ユーザーを指定しないと、すべてのユーザーアカウントの詳細が表示されます。出力には、ユーザーのアクセス権およびパスワードの割り当ての有無が表示されます。

E.6　システムコントローラの設定に関するコマンド

表 E-6　システムコントローラを設定するためのコマンド

コマンドおよびオプション (ある場合)	コマンドの説明
`setupsc`	アクティブシステムコントローラを対話式で設定できます (非対話式で設定することはできません)。スタンバイシステムコントローラは、自動的にアクティブシステムコントローラと同じ設定を使用します。
`flashupdate -s` *IP address* `-f` *path* `[-v] sscn|sn`	システムコントローラまたはサーバーブレードを新しいファームウェアでアップグレードします。*IP address* には、ファームウェアが格納されている TFTP サーバーの IP アドレスを指定します。*Path* には、TFTP サーバー上のファームウェアの位置を指定します。-v オプションを指定すると、アップグレード処理を実行したときに、関連する情報が表示されます。

表 E-6　システムコントローラを設定するためのコマンド (続き)

コマンドおよびオプション (ある場合)	コマンドの説明
`setfailover`	どちらのシステムコントローラがアクティブで、どちらがスタンバイになっているかを表示します。また、現在のスタンバイシステムコントローラがアクティブシステムコントローラから処理を引き継ぐかどうかを確認するプロンプトも表示されます。どちらのシステムコントローラがアクティブであるかを確認するためだけにこのコマンドを実行した場合は「no」と答えます。
`setdefaults [-y]`	アクティブシステムコントローラを出荷時のデフォルトの設定に戻します。スイッチの設定は変更されません。-y オプションを指定すると、確認のプロンプトを表示せずに、SSC の設定を出荷時のデフォルトに戻します。
`setdate [`*mmdd*`]`*HHMM*`[.`*SS*`] | `*mmddHHMM*`[`*cc*`]`*yy*`[.`*SS*`]`	システムコントローラおよびスイッチ、現在挿入されているサーバーブレードの日付および時刻を設定できます。日付および時刻を設定するときには、協定世界時 (UTC) を使用する必要があります。Solaris サーバーブレードは、UTC からのオフセットを使用して、その地域のタイムゾーンのローカル時刻を算出します。ブレードは、システムコントローラから UTC を取得します。変数の意味は、次のとおりです。 *mm* には月を指定 (2 桁) *dd* には日を指定 (2 桁) *HH* には時を指定 (2 桁) *MM* には分を指定 (2 桁) *SS* には秒を指定 (2 桁)
`setlocator on|off`	シャーシのロケータの点灯と消灯を切り替えます。

E.7 スイッチおよびブレードに関するコマンド

注 – スイッチまたはブレードのコンソールでは、**#.** を入力して、アクティブシステムコントローラの sc> プロンプトに切り替えます。

表 E-7 スイッチおよびブレードにアクセスして設定するためのコマンド

コマンドおよびオプション (ある場合)	コマンドの説明
`console [-f]|[[-r] sscn/swt|sn`	スイッチまたはブレードのコンソールにアクセスします。-f オプションを指定すると、現在ログインしているほかのユーザーを、強制的に読み取り専用モードにします。-r オプションを指定すると、そのユーザー自身が読み取り専用モードでログインします。
`consolehistory [-b]|[-e] [-g] [boot|run] sscn/sc|sscn/swt|sn`	指定したシステムコントローラまたはスイッチ、ブレードのコンソールの起動時バッファーまたは動作中バッファーの内容を表示します。-b を指定すると、最初の *n* 件の情報が表示されます。-e を指定すると、最後の *n* 件の情報が表示されます。-g を指定すると、行数を指定して、その行数分の情報の出力後一時停止させることができます。
`bootmode reset_nvram|diag|skip_diag|normal|bootscript="string" sn {sn}`	このコマンドを使用して、ブレードの起動モードを指定できます。詳細は、『Sun Fire B1600 ブレードシステムシャーシ管理マニュアル』を参照してください。
`flashupdate -s` *IP address* `-f` *path* `[-v] sscn|sn`	アクティブシステムコントローラまたはサーバーブレードを新しいファームウェアでアップグレードします。*IP address* には、ファームウェアが格納されている TFTP サーバーの IP アドレスを指定します。*Path* には、TFTP サーバー上のファームウェアの位置を指定します。-v オプションを指定すると、アップグレード処理を実行したときに関連する情報が表示されます。

E.8 ユーザーアカウントの管理に関するコマンド

表 E-8　ユーザーアカウントを管理するためのコマンド

コマンドおよびオプション (ある場合)	コマンドの説明
useradd *username*	システムコントローラへのアクセス権を持つユーザーのリストに名前付きユーザーを追加します。
userdel *username*	システムコントローラへのアクセス権を持つユーザーのリストからユーザーを削除します。
userpassword *username*	a レベルのアクセス権を持つユーザーは、このコマンドを使用して別のユーザーのパスワードを変更できます。
password	このコマンドを実行すると、ユーザーは自分のパスワード (現在ログインしているユーザーのパスワード) を変更できます。
userperm *username* [a][u][c][r]	このコマンドを使用して、名前付きユーザーのアクセス権のレベルを指定します。c を指定すると、ブレードおよびスイッチのコンソールへのアクセス権が付与されます。a を指定すると、管理の権限が付与され、システムコントローラの設定を変更できるようになります。u を指定すると、ユーザー管理の権限が付与され、ユーザーアカウントを管理できるようになります。r を指定すると、リセットの権限が付与され、シャーシのコンポーネントのリセットと電源の投入および切断を実行できるようになります。
usershow [*username*]	指定したユーザーのログインアカウントの詳細を表示します。ユーザーを指定しないと、すべてのユーザーアカウントの詳細が表示されます。出力には、ユーザーのアクセス権およびパスワードの割り当ての有無が表示されます。
showusers	システムコントローラに現在ログインしているすべてのユーザーを表示します。

付録F

アクティブシステムコントローラおよびスタンバイシステムコントローラ

この付録では、シャーシのアクティブシステムコントローラとスタンバイシステムコントローラの関係について説明します。また、この関係の制限事項についても説明します。

F.1 フェイルオーバーの契機になるイベント

ブレードシステムシャーシは、2 つのシステムコントローラを備えています。システムコントローラは、一度に 1 つだけがアクティブになるので、ALOM コマンド行インタフェースによってアクセスできるのは 1 つだけです。ただし、一方のシステムコントローラが休止している (スタンバイモードになっている) ときも、それに関連するスイッチはアクティブです。また、次の場合には、スタンバイシステムコントローラはアクティブシステムコントローラの処理を引き継ぐことができます。

- 現在アクティブなシステムコントローラを取り外した
- アクティブシステムコントローラのシステムコントローラソフトウェアアプリケーションで重大な障害が発生するか、ハードウェアで致命的なエラーが発生した
- ユーザーが `setfailover` コマンドを実行して、システムコントローラの役割を強制的に切り替えた

F.2 スタンバイシステムコントローラの動作

スタンバイシステムコントローラは、主要なソフトウェアアプリケーションは休止していますが、次のように動作しています。

- 現在のアクティブシステムコントローラを監視し、アクティブシステムコントローラが物理的に取り外された場合や、主要なソフトウェアアプリケーションで重大な障害が発生した場合、ハードウェアで致命的なエラーが発生した場合、アクティブシステムコントローラで `setfailover` コマンドが実行された場合には、処理を引き継ぎます。
- ユーザーがアクティブシステムコントローラ上で `setupsc` コマンドを実行して設定した構成パラメタを受信します。これによって、スタンバイシステムコントローラは、透過的にアクティブシステムコントローラの処理を引き継ぐことができるようになります。
- スタンバイシステムコントローラのイベントログが常に最新の状態になるように、すべてのイベントメッセージを受信します。
- アクティブシステムコントローラから、スタンバイシステムコントローラがある SSC モジュール内のスイッチのコンソールへのアクセスを許可します。何らかの理由でスタンバイシステムコントローラの起動が中断された場合は、スタンバイシステムコントローラが関連するスイッチのコンソールへのアクセスを提供できないことに注意してください。

- シャーシ全体のユーザーログインおよびホスト ID 情報の整合性を保持します。サーバーブレードにはホスト ID 情報が必要で、システムコントローラにはユーザーログイン情報が必要です。この 2 組の情報は、主にミッドプレーンに格納されます。ただし、2 つのシステムコントローラも、この情報を保持しています。

  出荷時のデフォルト設定のままの新しい SSC を、すでに使用しているシャーシに取り付けると、新しい SSC は現在ミッドプレーンに格納されているユーザーログインおよびホスト ID 情報を引き継ぎます。

  逆に、ユーザーログインおよびホスト ID が設定されていない新しいシャーシに、以前から使用している SSC を取り付けると、ミッドプレーンはシステムコントローラからユーザーログインおよびホスト ID 情報を取得します。

  SSC をシャーシに取り付けたときに、SSC とシャーシの両方にユーザーログインおよびホスト ID 情報があり、その片方または両方が SSC とシャーシ間で異なっていると、どちらの情報が引き継がれるかを予測することが困難になります。このときスタンバイシステムコントローラが動作していれば調停の役割を果たします。スタンバイシステムコントローラは、自身のユーザーログインおよびホスト ID 情報を、アクティブシステムコントローラの SSC が保持している情報、およびミッドプレーンに格納されている情報と比較します。スタンバイシステムコントローラのホスト ID 情報が、アクティブな SSC またはミッドプレーンに格納されている情報のいずれかと一致した場合は、その情報が優先されます。同様に、スタンバイシステムコントローラのユーザーログイン情報が、アクティブな SSC またはミッドプレーンに格納されている情報のいずれかと一致した場合は、その情報が優先されます。各情報について、スタンバイシステムコントローラのデータが、アクティブな SSC およびミッドプレーンのデータのどちらとも異なる場合は、ミッドプレーンのデータが優先されます。

F.3 2 つのシステムコントローラのフェイルオーバー関係についての制限事項

フェイルオーバー処理中、サーバーブレードまたはスイッチの動作に対する影響はありません。ただし、次の点に注意してください。

- システムコントローラが別のシステムコントローラから処理を引き継ぐときに、シャーシは一時的に (約 15 秒間) アクティブシステムコントローラがない状態になります。これは、フェイルオーバー処理の過程で、両方のシステムコントローラがリセットされるためです。そのため、フェイルオーバー中は、コンソールログは収集されません。また、新しいアクティブシステムコントローラにログインしたとき、両方のシステムコントローラのすべてのイベントログは空になっています。

  フェイルオーバー処理中は、システムコントローラを介してシャーシのコンポーネントのユーザーを管理することはできません。ただし、スイッチまたはブレードへの telnet 接続は可能なので、スイッチの Web ベースのグラフィカルユーザーインタフェースは使用できます。

  フェイルオーバー処理中、シャーシのコンポーネントのファームウェアをアップグレードすることはできません。システムコントローラファームウェアをアップグレードするには、現在アクティブなシステムコントローラの `sc>` プロンプトで `setfailover` コマンドを実行して、アップグレードするシステムコントローラをアクティブシステムコントローラにする必要があります。

- telnet 接続を使用したスタンバイシステムコントローラへのアクセスは許可されません。代わりに、エイリアス IP アドレスを使用してください。ただし、あるシステムコントローラから別のシステムコントローラへのフェイルオーバーが発生すると、telnet 接続は切断されます。

索引

し

す