Sun Fire™ B1600 블레이드 시스템 섀시 소프트웨어 설치 설명서

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054 U.S.A.
650-960-1300

문서 번호 817-1889-10
2003년 4월, 개정판 A

이 문서에 대한 의견은 docfeedback@sun.com으로 보내주십시오.

목차

머리말

본 설명서에서는 네트워크에 시스템 섀시를 설치하기 위해 Sun Fire B1600 블레이드 시스템 섀시에 있는 구성 부품의 소프트웨어를 구성하는 방법을 설명합니다.

이 설명서는 숙련된 Solaris 시스템 관리자를 대상으로 작성되었습니다.

이 설명서를 읽기 전에

이 설명서의 지침을 수행하기 전에 랙에 블레이드 시스템 섀시를 설치하고, 필요한 모든 케이블을 연결했는지 확인하십시오. 시스템 하드웨어를 설치하는 방법은 *Sun Fire B1600 블레이드 시스템 섀시 하드웨어 설치 설명서*를 참조하십시오.

이 책의 구성

1장에서는 Sun Fire B1600 블레이드 시스템 섀시의 소프트웨어에 대해 개괄적으로 설명하고, 이 설명서 나머지 부분의 지침을 수행하기 전에 해야 할 사항들에 대해 설명합니다.

2장에서는 시스템 섀시 설치를 위한 준비 작업을 수행하는 방법을 설명합니다.

3장에서는 데이터 네트워크와 관리 네트워크를 분리하지 않고 시스템 섀시를 단순한 네트워크에 설치하려는 경우 시스템 섀시를 구성하는 가장 빠른 방법을 설명합니다.

4장에서는 서버 블레이드의 전원을 켜고 해당 콘솔에 연결한 다음 예비 진단을 실행하는 방법을 설명합니다.

5장에서는 데이터 트래픽과 관리 트래픽이 분리된 네트워크 환경에 시스템 섀시를 설치하는 방법을 설명합니다.

6장에서는 관리 네트워크에서 안전하게 직접 블레이드를 관리할 수 있도록 5장에 나온 시스템 섀시 구성을 개선하는 방법을 설명합니다.

7장은 인터넷 서비스 제공업체(ISP)를 대상으로 합니다. 이 장에서는 서버 블레이드를 여러 고객(서버 블레이드 고객이라고 함)에게 할당하는 방법과 이들 고객이 다른 고객의 블레이드에 대한 액세스 권한 없이도 자신의 블레이드를 관리할 수 있는 방법을 설명합니다.

부록 A에서는 이후 장의 지침을 수행할 때 필요한 일부 스위치 작업들을 수행하는 방법을 설명합니다.

부록 B에서는 랩탑 컴퓨터에서 시스템 섀시의 명령행 인터페이스에 연결하는 방법을 설명합니다.

부록 C는 *Solaris Advanced Installation Guide*와 *DHCP Administration Guide*의 내용을 보완합니다. 이 부록에는 시스템 섀시의 서버 블레이드가 IP 주소를 동적으로 할당받을 수 있도록 데이터 네트워크의 DHCP 서버를 구성하는 방법이 나와 있습니다.

부록 D에서는 Web Start Flash 아카이브를 사용하여 한 서버 블레이드의 운영 환경과 응용 프로그램 소프트웨어를 다른 블레이드에 복제하는 방법을 설명합니다.

부록 E에는 시스템 컨트롤러의 `sc>` 프롬프트에서 사용할 수 있는 명령들이 나와 있습니다.

부록 F에서는 활성 시스템 컨트롤러와 대기 시스템 컨트롤러간의 관계에 대해 자세히 설명합니다.

이 설명서를 읽은 후에

이 설명서를 읽은 후에는 블레이드 시스템 섀시에 관한 다른 두 가지 설명서를 참조할 필요가 있습니다.

- 섀시의 시스템 컨트롤러의 명령행 인터페이스를 사용하는 자세한 방법은 *Sun Fire B1600 블레이드 시스템 섀시 관리 안내서*를 참조하십시오.
- 섀시의 내장 스위치를 관리하는 자세한 방법은 *Sun Fire B1600 블레이드 시스템 섀시 스위치 관리 안내서*를 참조하십시오. 이 설명서에서는 내장 스위치의 하드웨어 및 아키텍처에 대해 설명합니다(1장). 또한 스위치 초기 구성을 수행하는 방법(2장), 웹 그래픽 사용자 인터페이스 또는 SNMP를 사용하여 스위치를 관리하는 방법(3장), 그리고 명령행 인터페이스에서 스위치를 관리하기 위해 사용되는 명령들을 실행하는 방법(4장)도 설명합니다.

UNIX 명령 사용

이 설명서에는 기본적인 UNIX® 명령 및 절차에 대한 내용은 포함되어 있지 않습니다.

이와 관련된 내용은 다음을 참조하십시오.

- *Solaris Handbook for Sun Peripherals*
- Solaris™ 운영 환경에 대한 AnswerBook2™ 온라인 설명서

활자체 규정

활자체*	의미	예제
AaBbCc123	컴퓨터 화면에 나타나는 명령, 파일 및 디렉토리의 이름	.login 파일을 편집합니다. ls -a를 수행하여 모든 파일을 나열합니다. % You have mail.
AaBbCc123	컴퓨터 출력과 대조되는, 사용자가 직접 입력하는 내용	% **su** Password:
AaBbCc123	책 제목, 새 단어 또는 용어, 강조할 단어. 실제 이름이나 값으로 대체할 명령행 변수	사용 설명서 6장을 참조하십시오. 이들을 클래스 옵션이라고 합니다. 이 작업은 수퍼유저만 수행할 수 있습니다. 파일을 삭제하려면 *rm filename*을 입력하십시오.

* 사용 중인 브라우저의 설정이 이 설정과 다를 수도 있습니다.

셸 프롬프트

셸	프롬프트
C 셸	*machine-name*%
C 셸 수퍼유저	*machine-name*#
Bourne 셸과 Korn 셸	$
Bourne 셸과 Korn 셸 수퍼유저	#
시스템 컨트롤러 셸	sc>
내장 스위치 셸	Console#

관련 문서

분야	제목	문서 번호
준수 규정 및 안전	*Sun Fire B1600 Blade System Chassis Compliance and Safety Manual*	816-3364
설치 개요(접는 낱장 인쇄물)	*Sun Fire B1600 Blade System Chassis Quick Start Guide*	816-3625
하드웨어 설치	*Sun Fire B1600 블레이드 시스템 섀시 하드웨어 설치 설명서*	817-1930
소프트웨어 설치	*Sun Fire B1600 블레이드 시스템 섀시 소프트웨어 설치 설명서*(본 설명서)	817-1887
시스템 섀시 관리 및 구성 부품 교체	*Sun Fire B1600 블레이드 시스템 섀시 관리 안내서*	817-1897
스위치 관리	*Sun Fire B1600 블레이드 시스템 섀시 스위치 관리 안내서*	817-1892
최신 정보	*Sun Fire B1600 Blade System Chassis Product Notes*	816-4174

Sun 설명서 얻기

다음 사이트에서 Sun 설명서(번역본 포함)를 읽거나 인쇄 및 구입할 수 있습니다.

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

Sun에 대한 고객의 의견

Sun은 설명서 개선에 노력을 기울이고 있으며 여러분의 의견과 제안을 환영합니다. 다음 주소로 의견을 보내주십시오.

`docfeedback@sun.com`

전자 우편의 제목에 설명서의 문서 번호(817-1889-10)를 명시해 주시기 바랍니다.

1장

시스템 섀시 구성 작업 준비

이 장에서는 시스템 섀시 구성 절차를 개괄적으로 설명합니다. 그런 다음 시스템 섀시에 대해 소개하고 시스템 컨트롤러와 스위치의 역할에 대해서도 설명합니다. 마지막 단원을 제외한 이 장의 나머지 부분에서는 시스템 섀시를 구성하기 전에 수행해야 할 사항에 대해 설명합니다. 마지막 단원에서는 #. 탈출 문자열을 사용하여 여러 가지 사용자 인터페이스 사이를 이동하는 방법을 설명합니다.

이 장은 다음 단원으로 구성되어 있습니다.

1.1 소프트웨어 설치 개요

이 단원에서는 시스템 섀시를 설정하는 절차를 요약 설명합니다.

참고 – 시스템 섀시를 구성하려면 시스템 컨트롤러의 명령행 인터페이스를 사용해야 합니다. 또한 이 인터페이스에서 두 스위치와 서버 블레이드의 콘솔에 액세스할 필요가 있습니다. 스위치 콘솔 또는 블레이드 콘솔 위치에 있을 때 활성 시스템 컨트롤러의 `sc>` 프롬프트로 돌아가려면 **#.**을 입력하십시오.

---

1. **운영 환경을 서버 블레이드에 설치하기 위해 네트워크 설치 서버를 생성합니다.**

   서버 블레이드에 운영 환경을 설치하려면 해당 블레이드를 네트워크 설치 서버에서 시동해야 합니다. 그러므로 섀시에 소프트웨어를 설치하기 전에 먼저 *Solaris Advanced Installation Guide*(이 설명서는 Solaris 미디어 키트와 함께 제공됩니다)에 나온 네트워크 설치 서버 생성 절차를 수행합니다. 네트워크 설치 서버가 이미 네트워크에 있는 경우에는 서버 블레이드용 Solaris 이미지를 기존 네트워크 설치 서버에 추가합니다.

   블레이드 시스템 섀시의 구성 부품에 대해 IP 주소를 동적으로 할당하려면 아래 내용을 참조하십시오.

   - 1-11페이지의 단원 1.6, "섀시에 필요한 IP 정보"
   - 1-12페이지의 단원 1.7, "DHCP 서버를 사용하여 SSC IP 주소를 자동으로 할당하기",

   그리고 부록 C의 추가 정보를 참조하여 데이터 네트워크에 네트워크 설치 서버와 DHCP 서버를 구성하는 작업을 완료합니다.

2. **섀시의 시스템 컨트롤러 중 하나에 직렬 연결을 설정합니다.**

   또는 시스템 컨트롤러에 IP 구성 정보를 제공하도록 DHCP 서버를 구성합니다. 그런 후에 텔넷을 사용하여 시스템 컨트롤러에 액세스할 수 있습니다.

   섀시의 시스템 컨트롤러 중 하나에 직렬 연결을 설정하려면 *Sun Fire B1600 블레이드 시스템 섀시 하드웨어 설치 설명서*를 참조하십시오.

3. **시스템 컨트롤러에 로그인하여 암호와 날짜, 시간을 설정합니다.**

   부록2의 지침에 따라 암호와 날짜, 시간을 설정합니다.

4. **각 스위치에 로그인하여 최소 하나의 암호를 설정합니다.**

   이 작업을 수행하는 방법은 부록2을 참조하십시오.

5. **IP 환경 준비**

   새시의 시스템 컨트롤러, 스위치 및 서버 블레이드를 받아들일 수 있도록 네트워크의 IP 환경을 준비해야 합니다(부록 3 참조).

6. **간단한 설정 작업을 수행합니다.**

   우선 간단한 설정을 구성한 후 나중에 이를 수정할 수 있도록 부록 3에 나와있는 지침을 수행합니다. 이 장에서는 새시에 있는 두 개의 스위치를 활용하여 서버 블레이드에 각각 두 개의 네트워크 연결을 설정하는 방법을 설명합니다.

7. **필요할 경우, 데이터 네트워크와 관리 네트워크가 분리된 환경에 사용할 수 있도록 시스템 새시를 설정합니다.**

   이렇게 하는 방법은 부록 5에 나와있는 지침을 참조하십시오. 이 장에서는 IPMP(IP 네트워크 다중 경로 지정)를 사용하여 각 서버 블레이드에 데이터 네트워크에 대한 이중화된 연결을 설정함으로써 시스템 새시의 두 스위치를 활용하는 방법을 설명합니다.

8. **필요할 경우, 각 블레이드가 데이터 네트워크와 관리 네트워크에 대해 각각 이중화된 연결을 갖도록 시스템 새시를 설정합니다(부록 5 참조).**

   이렇게 하는 방법은 부록 6에 나와있는 지침을 참조하십시오.

9. **필요할 경우, 개별 서버 블레이드를 서로 다른 소유자에게 할당하고, 각 소유자가 시스템 컨트롤러나 스위치, 또는 다른 소유자의 블레이드에 액세스하지 않고도 자신의 블레이드를 관리할 수 있도록 시스템 새시를 설정합니다.**

   이렇게 하는 방법은 부록 7에 나와있는 지침을 참조하십시오.

1.2 Sun Fire B1600 블레이드 시스템 섀시

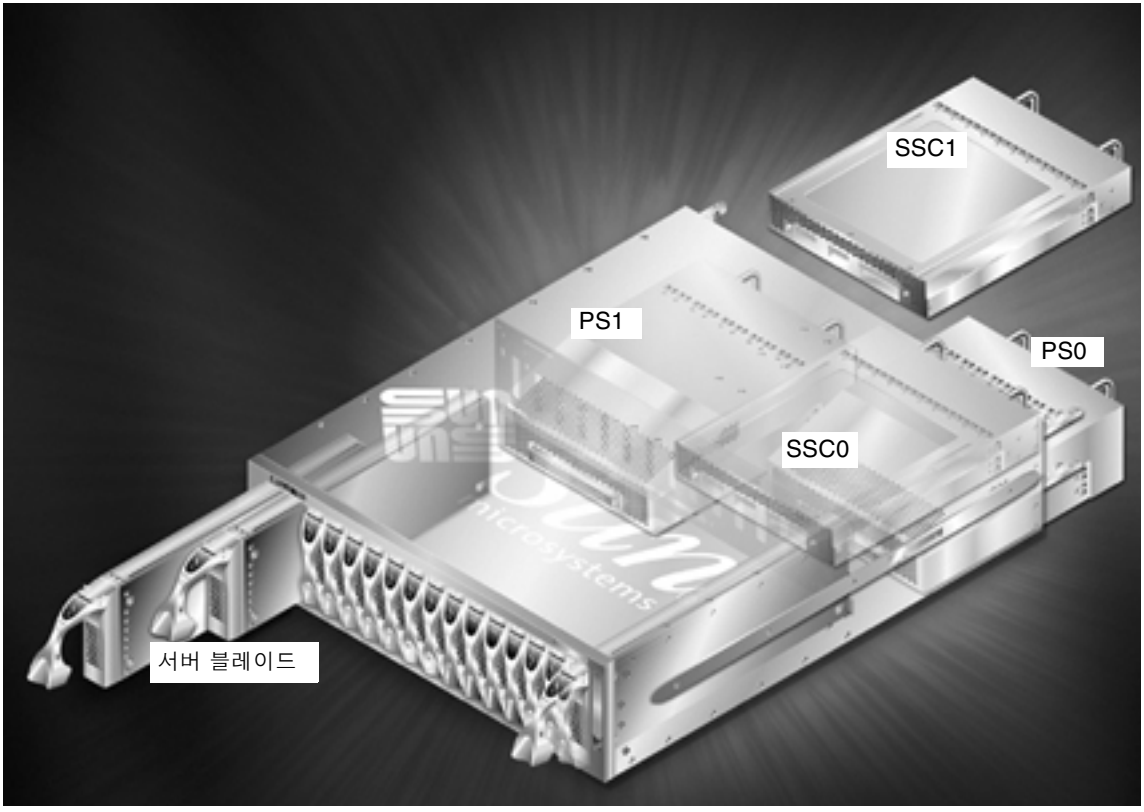


그림 1-1 Sun Fire B1600 블레이드 시스템 섀시

Sun Fire B1600 블레이드 시스템 섀시는 주로 인터넷 서비스 공급업체가 사용하도록 설계되었으며, 16개의 서버를 수용할 수 있는 3U 높이의 섀시입니다. 또한 고성능 서버의 밀도를 극대화할 필요가 있는 기업 네트워크에도 적합합니다.

이 섀시는 최대 16개의 서버 블레이드를 수용할 수 있는 외에도, 두 개의 전원 공급 장치(PSU)와 두 개의 스위치 및 시스템 컨트롤러(SSC) 장치를 갖추고 있습니다.

1.3 블레이드 시스템 섀시를 위한 소프트웨어

블레이드 시스템 섀시에는 다음에 사용되는 세 개의 주요 소프트웨어 구성 요소가 있습니다.

- 두 개의 시스템 컨트롤러(SSC0에 하나, SSC1에 하나)
- 두 개의 스위치(SSC0에 하나, SSC1에 하나)
- 서버 블레이드

1.3.1 활성 및 대기 시스템 컨트롤러

그림 1-1에 나타난 바와 같이 SSC 장치는 두 개가 있습니다. 시스템 섀시의 공장 출하시 기본 설정에서, SSC0의 시스템 컨트롤러는 활성 상태이고 SSC1의 시스템 컨트롤러는 대기 상태입니다.

그러나 활성 시스템 컨트롤러가 있는 SSC를 제거하거나 기본 소프트웨어 응용 프로그램에 심각한 오류가 발생하면 다른 SSC에 있는 대기 시스템 컨트롤러가 자동으로 활성화됩니다.

활성 시스템 컨트롤러의 명령행에서 강제로 대기 시스템 컨트롤러를 활성 상태로 바꾸는 것도 가능합니다. 이렇게 하는 방법은 *Sun Fire B1600 블레이드 시스템 섀시 관리 안내서*를 참조하십시오.

향후 출시될 시스템 컨트롤러 소프트웨어에서는 활성 시스템 컨트롤러를 지속적으로 모니터링하여 활성 컨트롤러가 대기 컨트롤러보다 맡은 역할을 수행하기에 적합하지 않다고 판단될 경우 대기 시스템 컨트롤러가 활성 시스템 컨트롤러의 역할을 자동으로 넘겨받게 됩니다.

두 시스템 컨트롤러는 하나의 별칭 IP 주소를 공유하며 각각 전용 IP 주소를 하나씩 가질 수 있습니다. 별칭 IP 주소는 활성 시스템 컨트롤러가 어느 것이든 해당 컨트롤러의 주소가 됩니다. 이름 서비스에 지정해야 하는 주소가 바로 이 주소입니다. 한 시스템 컨트롤러가 활성 컨트롤러의 역할을 맡게되면 자신에게 이 별칭 주소를 할당하고, 자신의 MAC 주소와 별칭 IP 주소를 포함하는 브로드캐스트를 통해 상위 네트워크에 자신이 이 별칭 IP 주소의 소유자임을 알립니다.

각 시스템 컨트롤러에 전용 IP 주소를 할당한 경우, 별칭 IP 주소 대신 이 전용 IP 주소를 사용하여 활성 시스템 컨트롤러에 텔넷 연결할 수 있습니다. 대기 시스템 컨트롤러에는 전용 IP 주소가 있더라도 텔넷 연결할 수 없습니다. 그러나 두 시스템 컨트롤러가 각각 전용 IP 주소를 갖고있을 경우, 네트워크 관리자가 각 시스템 컨트롤러에 ping 신호를 보내 네트워크 연결 여부를 확인할 수 있으므로 전용 IP 주소를 할당해 두는 것이 좋습니다(부록 3 참조).

1.3.2 스위치 이중화 구성

섀시의 시스템 컨트롤러는 특정 시점에 항상 하나만 작동하지만 두 SSC의 스위치들은 항상 작동합니다. 이 점은 블레이드 시스템 섀시 설계의 중요한 특징입니다. 각 서버 블레이드에는 개별 스위치마다 하나씩 두 개의 기가비트 네트워크 인터페이스가 있습니다. 따라서 한 인터페이스에 네트워크 연결 장애(예: 스위치 장애)가 발생하더라도 다른 하나가 계속 서비스를 제공합니다.

섀시를 구성할 때 이 이중화된 연결을 활용하는 방법은 부록 3과 부록 5을 참조하십시오.

참고 – 섀시의 시스템 컨트롤러는 특정 시점에 항상 하나만 작동하지만 두 스위치는 모두 항상 작동한다는 점에 유의하십시오.

1.3.3 서버 블레이드

서버 블레이드는 기본급의 표준 Sun 서버와 논리적으로 동등합니다. 네트워크 및 sysid 구성을 위한 모든 표준 방법(예: TFTP와 DHCP)을 서버 블레이드에 사용할 수 있으며, 다음과 같은 Solaris 운영 환경 설치 방법도 사용할 수 있습니다.

- Web Start 설치
- 대화식 설치
- 맞춤식 점프스타트 설치
- Web Start Flash 설치

이와 같은 Solaris 설치 방법에 대해서는 *Solaris Advanced Installation Guide* 3장을 참조하십시오.

1.4 시스템 컨트롤러, 스위치 및 서버 블레이드의 역할

1.4.1 시스템 컨트롤러의 역할

활성 시스템 컨트롤러는 두 가지 역할을 수행합니다. 첫째, 시스템 섀시의 하위 구성 부품들의 작동 상태를 모니터링합니다. 둘째, 직렬 연결 또는 텔넷을 통해 기본 섀시 구성 소프트웨어인 "Advanced Lights Out Management Software"에 대한 명령행 인터페이스를 제공합니다. 이 소프트웨어는 섀시의 활성 시스템 컨트롤러에서 실행되는 응용 프로그램입니다.

시스템 컨트롤러에서 Advanced Lights Out Management Software에 로그인하는 방법은 이 설명서 2장에 설명되어 있습니다.

시스템 컨트롤러에 로그인하면 아래와 같은 기능에 액세스할 수 있습니다.

- 시스템 섀시 및 그 구성 부품의 모니터링과 관리를 위한 활성 시스템 컨트롤러 고유 명령들. 이러한 명령에 대한 자세한 내용은 부록 E 및 *Sun Fire B1600 블레이드 시스템 섀시 관리 안내서*를 참조하십시오.
- 시스템 섀시에 있는 두 내장 스위치의 콘솔. 스위치의 명령행 인터페이스에서 사용할 수 있는 명령에 대해서는 부록 A 및 *Sun Fire B1600 블레이드 시스템 섀시 스위치 관리 안내서*를 참조하십시오.
- 시스템 섀시에 있는 서버 블레이드의 콘솔.

무엇보다도 이 설명서는 배송 키트에 포함된 설명서 CD에 있는 다른 설명서들을 참조하지 않고도 블레이드 시스템 섀시를 설정할 수 있도록 작성되었습니다.

그러나 설명서 CD에는 배송 키트에 포함된 모든 설명서 인쇄본의 온라인 버전 외에도, Advance Lights Out Management Software에 대한 온라인 설명서(*Sun Fire B1600 블레이드 시스템 섀시 관리 안내서*)와 내장 스위치에 대한 온라인 명령 참조 설명서(*Sun Fire B1600 블레이드 시스템 섀시 스위치 관리 안내서*)도 들어 있습니다.

활성 시스템 컨트롤러와 대기 시스템 컨트롤러간의 관계, 그리고 이러한 관계의 한계성에 대한 자세한 내용은 부록 F를 참조하십시오.

1.4.2 스위치의 역할

그림 1-2에는 개별 스위치의 모든 이더넷 포트와 개별 서버 블레이드의 모든 이더넷 인터페이스가 나와 있습니다. 각 서버 블레이드는 SSC0의 스위치에 대한 인터페이스 하나와 SSC1의 스위치에 대한 인터페이스 하나를 갖고 있습니다. 그리고 각 스위치는 개별 서버 블레이드에 대해 하나씩의 포트를 가집니다. 이 포트들은 SNP0 ~ SNP15로 표시되어 있습니다. 데이터 네트워크 업링크 포트는 NETP0 ~ NETP7로 표시되어 있습니다.

참고 – 데이터 네트워크 업링크 포트와 서버 블레이드 포트 사이에는 직접적인 연결이 없습니다. 대신 이 두 가지 포트 사이에 고속의 중앙판이 있어서 둘 사이의 모든 트래픽을 처리합니다. 이 연결은 그림에서 SNP 포트 및 NETP 포트와 스위치 패브릭 사이에 그려진 굵은 검정 선으로 표시되어 있습니다.

또한 이 그림에는 스위치의 내부 관리 포트(NETMGT)와 외부 RJ-45 포트(SSC의 뒷면에 NETMGT라고 표시됨)가 나와 있습니다.

외부 NETMGT 포트는 시스템 컨트롤러(그림에 SC로 표시)와 스위치에 이더넷 연결을 제공합니다. 스위치의 내부 관리 포트도 스위치 명령행 인터페이스와 해당 웹 인터페이스에서 NETMGT로 표시되어 있습니다. 미니 허브가 내부 스위치 NETMGT 포트와 시스템 컨트롤러를 외부 NETMGT 포트에 연결해 줍니다. 그림에서 이더넷 포트와 SC 인터페이스 내부의 번호 1과 2는 스위치 포트의 기본 VLAN[1] 구성을 나타냅니다. 데이터 네트워크의 기본 VLAN은 VLAN 1입니다. 관리 네트워크의 기본 VLAN은 VLAN 2입니다.

시스템 컨트롤러의 VLAN ID는 스위치에서 구성할 수 없으며, `setupsc` 명령을 사용하여 시스템 컨트롤러를 대화식으로 설정하는 과정의 일부로서 구성됩니다(부록 3 참조). 이 명령을 실행하면 SC에 VLAN을 사용하겠느냐는 질문을 포함한 여러 질문을 사용자에게 묻습니다. "예"라고 대답하면 해당 SC 인터페이스의 VLAN ID를 지정하라는 메시지가 표시되며, 이 질문에 대한 기본값은 스위치의 기본 관리 VLAN인 VLAN 2입니다. SC 인터페이스는 스위치 포트가 아닙니다. 이 인터페이스에 VLAN 기능을 설정하여 얻는 효과는 사용자가 지정한 VLAN으로 태그 지정된 프레임만 송수신하도록 구성할 수 있다는 점입니다.

마지막으로, 그림 1-2의 스위치에 패킷 필터가 있다는 사실을 주목하십시오. 이 패킷 필터는 무엇보다도 내부 NETMGT 포트와 모든 서버 블레이드 포트 사이의 차단막 역할을 합니다. 이 필터는 데이터 네트워크를 통해 블레이드에 액세스한 외부 사용자의 공격으로부터 관리 네트워크를 보호해 줍니다.

기본적으로는 어떠한 네트워크 트래픽도 서버 블레이드와 스위치의 NETMGT 포트 사이를 통과할 수 없게 되어 있습니다. 그러나 특정 프로토콜과 관련된 규칙을 지정하면 해당 트래픽이 패킷 필터를 통과하도록 허용할 수 있습니다. 이렇게 하는 방법은 부록 A를 참조하십시오.

---

1. VLAN은 가상 LAN(Virtual Local Area Network)을 말합니다. 즉, 하나 이상의 네트워크 인프라 장비의 포트들을 소프트웨어를 사용하여 구성한 독립형 논리 네트워크이자 브로드캐스트 도메인입니다.

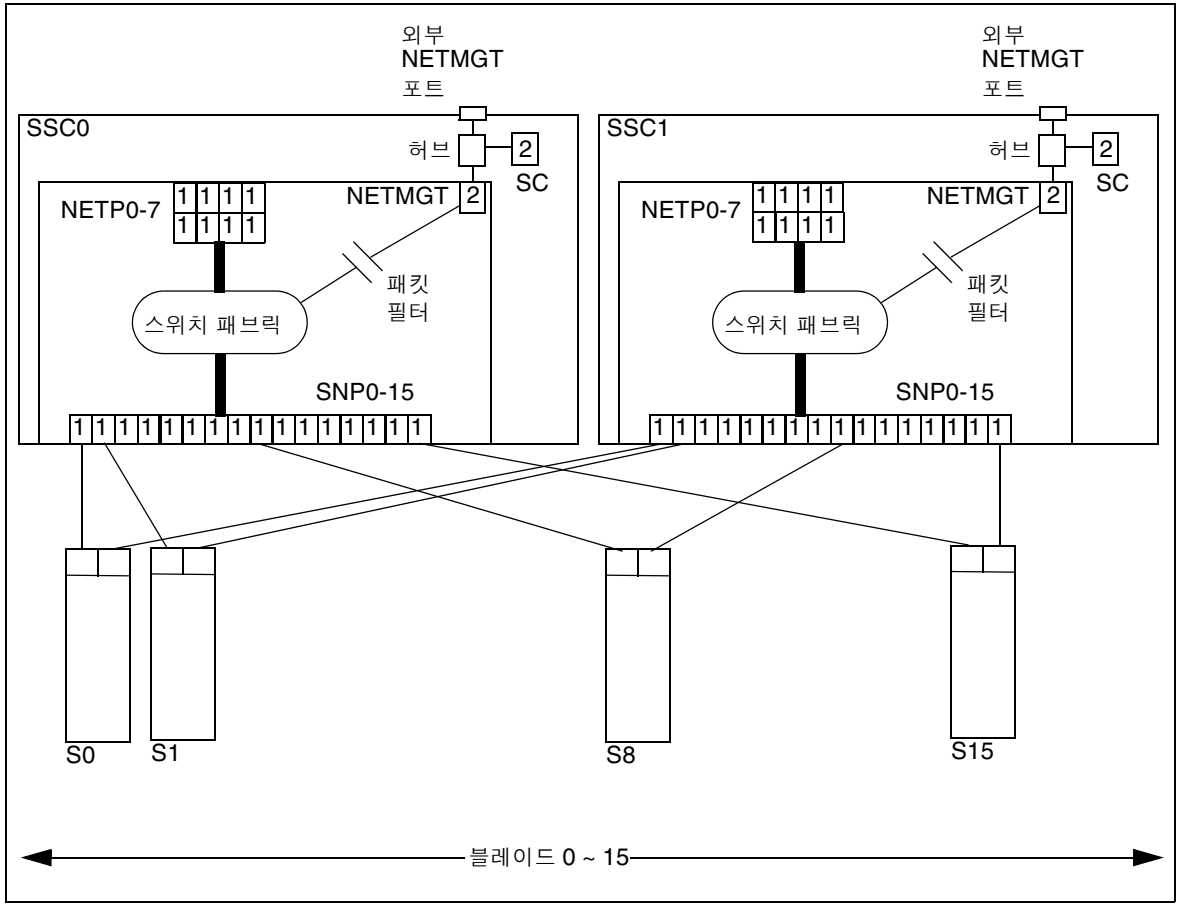


그림 1-2 시스템 섀시의 이더넷 포트와 인터페이스, 그리고 해당 기본 VLAN 번호

1.4.3 서버 블레이드의 역할

서버 블레이드는 소프트웨어 응용 프로그램을 실행하기 위한 컴퓨팅 능력을 제공합니다. 서버 블레이드의 주요 입출력 수단은 네트워크이지만, 시스템 컨트롤러와 각 블레이드간의 내부 직렬 연결을 통해 시스템 컨트롤러의 명령행 인터페이스에서 서버 블레이드의 콘솔에 액세스할 수 있습니다.

모든 블레이드는 새시의 두 내부 스위치 각각에 대해 하나의 기가비트 이더넷 인터페이스를 가지며, 스위치는 외부 네트워크에 대한 기가비트 이더넷 인터페이스도 갖고 있습니다.

일반적으로 블레이드에는 운영 체제 소프트웨어와 구성 정보를 담기 위한 로컬 디스크 저장 장치가 있습니다. 하지만 고객들은 사용자 데이터를 블레이드의 로컬 저장 장치에 보관하기보다는 원격 저장 시스템에 보관하는 것이 보통입니다.

공장 출하시 기본 설정인 경우, 서버 블레이드는 로컬 하드 디스크에 저장된 운영 환경 스텁을 사용하여 시동됩니다. 시동이 완료되면 블레이드는 네트워크에서 네트워크 설치 서버를 찾아 이것을 이용하여 운영 환경을 설치합니다.

네트워크 설치 서버를 통해 첫번째 서버 블레이드를 시동한 후에는 블레이드에서 사용할 응용 프로그램 소프트웨어를 추가할 수 있습니다. 그 다음에는 *Solaris Advanced Installation Guide* 에 나온 설명에 따라 Web Start Flash 아카이브를 생성합니다. Sun Fire B1600 블레이드 시스템 새시의 Sun Fire B100s Solaris 서버 블레이드에서 Web Start Flash 아카이브를 사용하여 한 블레이드의 운영 환경 및 응용 프로그램 소프트웨어를 다른 블레이드로 복제할 수 있습니다. 따라서 새시에 있는 전체 서버 블레이드를 구성하는 데 드는 시간이 단축됩니다.

Web Start Flash 아카이브를 사용하는 자세한 방법은 부록 D를 참조하십시오.

1.5 소프트웨어를 구성하기 전에

블레이드 시스템 새시를 설치하고 전원을 켠 후에 초기 구성을 수행하려면 SSC0(기본적으로 활성 시스템 컨트롤러)에 직렬 연결을 설정하거나, 새시의 활성 시스템 컨트롤러에 대한 IP 구성 작업을 자동으로 수행하도록 DHCP 서버를 설정해야 합니다. 이렇게 DHCP 서버를 설정한 후에는 활성 시스템 컨트롤러에 텔넷 연결하여 새시를 처음 설정할 수 있습니다.

직렬 연결 설정을 위한 케이블 연결 방법은 *Sun Fire B1600 블레이드 시스템 새시 하드웨어 설치 설명서*를 참조하십시오.

DHCP 서버를 사용하는 방법은 1-12페이지의 단원 1.7, "DHCP 서버를 사용하여 SSC IP 주소를 자동으로 할당하기"를 참조하십시오.

참고 – 새시의 두 SSC에 전원이 들어오고 정상적으로 작동하며 어느 SSC도 손상되지 않은 경우, 기본적으로 SSC0의 시스템 컨트롤러가 활성 컨트롤러가 되고 SSC1의 시스템 컨트롤러가 대기 컨트롤러가 됩니다. 따라서 직렬 연결을 사용하여 처음으로 새시를 설정하려면 적어도 SSC0에 대한 직렬 연결이 있어야 합니다.

그러나 블레이드 시스템 새시의 일상적 작동을 위해서는 두 SSC 모두에 직렬 연결을 설정하는 것이 좋습니다. 그렇게 해두면 활성 SSC가 작동하지 않는 경우가 생기더라도 새시에 대한 직렬 연결을 유지할 수 있습니다.

이 설명서의 부록2과 부록 3에서는 SSC0에 직렬 연결 또는 텔넷 연결을 설정한 후에 새시를 구성하는 방법을 설명합니다(SSC0에 활성 시스템 컨트롤러가 있다고 전제함).

1.6 새시에 필요한 IP 정보

네트워크 환경에 Sun Fire B1600 블레이드 시스템 새시를 설치하기 위해서는, 활성 시스템 컨트롤러에 대한 별칭 IP 주소와 새시의 각 이더넷 인터페이스에 대한 IP주소, 넷마스크 및 기본 게이트웨이 등을 제공하도록 네트워크 환경을 구성해야 합니다.

시스템 컨트롤러의 별칭 IP 주소는 이름 서비스에 지정됩니다. 하지만 시스템 컨트롤러는 그 외에도 전용 IP 주소를 각각 하나씩 가질 수 있습니다(이 주소는 이름 서비스에 지정할 필요가 없습니다). 한 시스템 컨트롤러가 활성 컨트롤러의 역할을 맡게되면 자신에게 이 별칭 주소를 할당하고, 자신의 MAC 주소와 별칭 IP 주소를 포함하는 브로드캐스트를 통해 상위 네트워크에 자신이 이 별칭 IP 주소의 소유자임을 알립니다.

내부 장비가 모두 탑재된 하나의 새시는 최소 37개의 IP 주소를 사용합니다(두 개의 전용 SC 주소 포함).

1. 활성 시스템 컨트롤러를 위한 별칭 IP 주소 1개(활성 시스템 컨트롤러가 SSC0에 있든 SSC1에 있든 이 주소가 사용됨)
2. SSC0의 시스템 컨트롤러를 위한 전용 IP 주소 1개
3. SSC1의 시스템 컨트롤러를 위한 전용 IP 주소 1개
4. SSC0의 스위치를 위한 IP 주소 1개
5. SSC1의 스위치를 위한 IP 주소 1개
6. 각 블레이드의 `ce0` 기본 인터페이스(기가비트 이더넷)를 위한 IP 주소 16개
7. 각 블레이드의 `ce1` 보조 인터페이스(기가비트 이더넷)를 위한 IP 주소 16개

부록 5, 부록 6 및 부록 7에 설명된 섀시 구성들의 경우 인터넷 다중 경로 지정(IPMP) 기능을 사용하므로 내부 장비가 모두 탑재된 섀시는 블레이드에 사용하기 위해 최소 64개 이상의 IP 주소를 필요로 합니다.

1.7 DHCP 서버를 사용하여 SSC IP 주소를 자동으로 할당하기

기본적으로 활성 SSC의 시스템 컨트롤러는 자신 및 대기 시스템 컨트롤러의 IP 구성 정보를 DHCP 서버에서 찾으려고 합니다.

각 SSC의 스위치들 역시 기본적으로 해당 IP 구성 정보를 DHCP 서버에서 찾으려고 합니다.

시스템 컨트롤러는 최대 3개의 IP 주소를 사용합니다.

- 별칭 IP 주소 1개(활성 시스템 컨트롤러가 SSC0에 있든 SSC1에 있든 이 주소가 사용됨)
- SSC0의 시스템 컨트롤러를 위한 전용 IP 주소 1개(옵션)
- SSC1의 시스템 컨트롤러를 위한 전용 IP 주소 1개(옵션)

각 스위치는 하나의 IP 주소를 필요로 합니다.

참고 – 데이터 네트워크와 관리 네트워크를 구분하려는 경우, SSC 구성에 사용되는 DHCP 서버는 관리 네트워크에 있어야 하고 서버 블레이드 구성에 사용되는 DHCP 서버는 데이터 네트워크에 있어야 합니다. 서버 블레이드에 IP 주소를 할당하도록 DHCP 서버를 구성하는 방법은 부록 C를 참조하십시오.

1.7.1 고정 IP 주소로 SSC 구성하기

활성 시스템 컨트롤러는 3개의 IP 주소(SSC0, SSC1 및 별칭 IP 주소)에 대한 DHCP 요청을 발송합니다.

각 스위치는 1개의 IP 주소에 대한 DHCP 요청을 발송합니다.

5개의 고정 IP 주소(즉 변경되지 않는 5개의 IP 주소)를 사용하려면 DHCP 서버 상의 5개의 주소를 시스템 컨트롤러 및 스위치의 클라이언트 식별자에 매핑해야 합니다.

시스템 컨트롤러는 각각 하나의 전용 IP 주소를 선택적으로 가질 수 있으므로 두 시스템 컨트롤러에 대해 클라이언트 식별자가 각각 하나씩 존재하며, 아울러 활성 시스템 컨트롤러에 대해서도 클라이언트 식별자가 존재합니다. (전용 IP 주소가 있을 경우 네트워크 관리자들이 ping 명령을 사용하여 이들의 네트워크 연결을 확인할 수 있으므로 전용 IP 주소를 할당하는 것이 좋습니다.)

표 1-1에는 새시의 시스템 컨트롤러와 스위치의 클라이언트 식별자가 나와 있습니다.

표 1-1 시스템 컨트롤러 및 내장 스위치의 클라이언트 식별자

장치	클라이언트 식별자
활성 시스템 컨트롤러	SUNW,SSC_ID=*새시 일련 번호*
SSC0의 시스템 컨트롤러(전용 IP)	SUNW,SSC_ID=*새시 일련 번호,0*
SSC0의 시스템 컨트롤러(전용 IP)	SUNW,SSC_ID=*새시 일련 번호,1*
SSC0의 스위치	SUNW,SWITCH_ID=*새시 일련 번호,0*
SSC1의 스위치	SUNW,SWITCH_ID=*새시 일련 번호,1*

참고 – 새시의 일련 번호는 새시 오른쪽 뒷면의 레이블에 인쇄되어 있습니다. 새시 레이블에 인쇄된 번호 중 뒤 6자리만 클라이언트 식별자로 사용됩니다.

(새시의 일련 번호를 찾는 또 다른 방법은 시스템 컨트롤러의 명령행에서 `showfru ch` 명령을 수행한 후 `/ManR/Sun_serial_No` 필드를 확인하면 됩니다.)

Solaris DHCP Administration Guide(806-5529)에 나온 고정 IP 주소 생성 지침에 따라, SSC와 동일한 네트워크에 DHCP 서버를 구성한 다음 위에 나열된 클라이언트 식별자에 매핑되는 5개의 IP 주소를 지정하십시오. 그리고 각 클라이언트 식별자에 매핑시킨 IP 주소를 기록해 두십시오. 활성 시스템 컨트롤러 또는 두 스위치에 텔넷 연결하려면 이 주소를 알아야 합니다. 스위치의 웹 기반 그래픽 사용자 인터페이스에 액세스하려는 경우에도 이 주소가 필요합니다.

1.7.2 동적 IP 주소로 SSC 구성하기

섀시의 시스템 컨트롤러와 스위치에 고정 IP 주소를 지정하는 대신 동적 IP 주소를 할당하도록 DHCP 서버를 구성할 수 있습니다. 이 주소들은 장치가 DHCP 요청을 수행한 후에 클라이언트 식별자와 매핑됩니다. 이를 수행하는 방법은 *Solaris DHCP Administration Guide*(806-5529)를 참조하십시오.

동적 IP 주소를 할당하도록 DHCP 서버를 구성한 경우에는 어떤 IP 주소가 시스템 컨트롤러에 할당되고 어떤 IP 주소가 두 스위치에 할당되었는지 알아야 합니다. 그래야만 텔넷을 통해 시스템 컨트롤러 또는 스위치에 액세스하거나 스위치의 웹 기반 그래픽 사용자 인터페이스에 액세스할 수 있습니다(1-14페이지의 단원 1.7.3, "텔넷을 사용하기 위해 섀시의 IP 주소 확인하기" 참조).

1.7.3 텔넷을 사용하기 위해 섀시의 IP 주소 확인하기

섀시 구성 부품에 고정 IP 주소가 아닌 동적 IP 주소를 할당한 상태에서 직렬 연결을 사용하지 않고 텔넷을 통해 활성 시스템 컨트롤러에 로그인하려는 경우, DHCP 서버가 시스템 컨트롤러에 할당한 IP 주소를 알아야 합니다.

사용 중인 DHCP 서버가 Solaris 시스템인 경우, `pntadm` 명령을 사용하면 섀시가 속한 네트워크의 모든 장치들이 해당 IP 주소와 함께 나열됩니다.

다음을 입력합니다.

```
# 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
```

샘플 출력 힌트:

1. 활성 시스템 컨트롤러의 클라이언트 식별자
2. SSC0에 있는 스위치의 클라이언트 식별자
3. SSC1에 있는 스위치의 클라이언트 식별자

여기서 *network address*는 관리 네트워크의 네트워크 주소입니다. 목록의 각 장치는 클라이언트 식별자를 나타내는 16진수 문자열로 구분됩니다.

이 예제에서 첫번째 장치는 활성 시스템 컨트롤러(별칭 IP 주소를 사용하는 컨트롤러), 두번째 장치는 SSC0의 스위치, 세번째 장치는 SSC1의 스위치입니다. 어느 장치에 어떤 클라이언트 IP 주소가 할당되었는지 확인하려면 16진수 문자열을 영숫자 일반 문자열로 변환해야 합니다.

(예제 출력에서는 공간이 부족하여 Lease Expiration 열 오른쪽의 두 열이 생략되었습니다. 생략된 열은 Macro 열과 Comments 열입니다.)

표 1-2 활성 시스템 컨트롤러의 클라이언트 식별자 변환 예제

	활성 시스템 컨트롤러	섀시 일련 번호
16진수	53554E572C5353435F49443D	31323334356
영숫자	SUNW,SSC_ID=	123456

표 1-3 SSC0에 있는 SC[1]의 클라이언트 식별자(고정 IP 주소용) 변환 예제

	활성 시스템 컨트롤러	섀시 일련 번호	SSC0를 나타내는 접미어
16진수	53554E572C5353435F49443D	31323334356	2C30
영숫자	SUNW,SSC_ID=	123456	,0

1. 시스템 컨트롤러

표 1-4 SSC1에 있는 스위치의 클라이언트 식별자 변환 예제

	SSC1의 스위치	섀시 일련 번호	SSC1를 나타내는 접미어
16진수	53554E572C5357495443485F49443D	31323334356	2C31
영숫자	SUNW,SWITCH_ID=	123456	,1

1.7.4 텔넷을 사용하여 시스템 컨트롤러에 액세스하기

DHCP 서버가 IP 주소를 할당하도록 구성한 경우, 활성 시스템 컨트롤러에 텔넷으로 연결하려면 다음을 수행하십시오.

1. **섀시의 전원이 이미 켜져있는 경우 IEC 전원 케이블을 뽑아서 섀시의 전원을 껐다 켜야 합니다.**

2. 섀시에 전원이 들어오면 원격 터미널에 다음과 같이 입력합니다.

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

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

username:
```

여기서 *alias ip address*는 활성 시스템 컨트롤러의 IP 주소입니다. 또는 그 대신에 명령행에 호스트 이름을 지정할 수도 있습니다.

1.8 스위치 콘솔 또는 블레이드 콘솔에서 sc> 프롬프트로 돌아가기

섀시 구성 작업을 시작하기 전에, 블레이드 콘솔 또는 스위치 콘솔에서 시스템 컨트롤러의 sc> 프롬프트로 돌아가는 탈출 문자열을 알아두는 것이 유용합니다. 탈출 문자열은 #(우물 '#'자와 마침표 '.')입니다.

이 설명서의 지침을 수행할 때 서버 블레이드나 스위치의 콘솔에는 sc> 프롬프트를 통해 액세스해야 합니다.

다음에 수행할 작업

2장으로 가서 시스템 섀시 예비 설정 작업을 수행하십시오.

2장

SSC의 암호, 날짜 및 시간 설정

이 장에서는 활성 시스템 컨트롤러와 두 스위치에 로그인하여 네트워크 환경에 맞게 블레이드 시스템 새시를 구성하기 위한 준비 작업을 수행하는 방법을 설명합니다.

활성 시스템 컨트롤러는 구성해야 하지만 대기 시스템 컨트롤러는 별도로 구성할 필요가 없습니다. 필요시 대기 시스템 컨트롤러가 활성 컨트롤러의 역할을 떠맡을 수 있도록 활성 시스템 컨트롤러는 자동으로 구성 정보를 대기 시스템 컨트롤러에 전달하여 줍니다.

스위치의 사용자 로그인 및 암호 정보는 시스템 컨트롤러의 사용자 로그인 및 암호 정보와는 별개입니다. 따라서 별도로 구성해야 합니다.

이 장은 다음 단원으로 구성되어 있습니다.

두 단원의 모든 지침을 수행하십시오.

참고 – 시스템 새시를 구성하려면 활성 시스템 컨트롤러의 명령행 인터페이스를 사용해야 합니다. 그러나 이 인터페이스에서 두 스위치 또는 서버 블레이드의 콘솔에 액세스해야 할 경우도 있습니다. 스위치 콘솔 또는 블레이드 콘솔 위치에 있을 때 시스템 컨트롤러의 `sc>` 프롬프트로 돌아가려면 **#.**을 입력하십시오.

2.1 시스템 컨트롤러 로그인, 암호 설정, 시간 설정

이 단원에서는 기본 사용자 admin으로 활성 시스템 컨트롤러에 로그인하는 방법과 이 사용자의 암호를 설정하는 방법을 설명합니다.

참고 – 시스템 컨트롤러에서 구성한 사용자 로그인 및 암호 정보는 스위치에서 구성한 사용자 로그인 및 암호 정보와 완전히 별개입니다. 스위치에서 이 정보를 구성하는 방법은 2-4페이지의 단원 2.2, "기본 사용자로 스위치에 로그인하여 암호 설정하기"를 참조하십시오.

이 단원은 활성 시스템 컨트롤러에 대한 직렬 연결 또는 텔넷 연결을 설정했다고 전제합니다. (대기 시스템 컨트롤러에는 텔넷 연결을 설정할 수 없습니다.) 별칭 IP 주소를 사용하여 텔넷으로 연결하면 현재 활성인 시스템 컨트롤러에 연결됩니다.

직렬 연결을 사용하는 경우, 공장 출하시 기본 설정 상태의 새시에서 활성 시스템 컨트롤러는 SSC0에 들어 있습니다. SSC1에 대기 시스템 컨트롤러가 있는 상태에서 SSC1에 연결하면 대기 시스템 컨트롤러에 연결되었음을 알리는 메시지가 표시됩니다. 이 경우 SSC0에 대한 연결을 설정하십시오. 어떤 경우에도 두 SSC의 직렬 연결은 유지하는 것이 좋습니다.

블레이드 시스템 새시 설정 작업을 시작하려면 다음을 수행하십시오.

1. username: **프롬프트에서 기본 사용자 이름** admin**을 입력합니다.**

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

username: admin
```

2. sc> **프롬프트에서 기본 사용자의 암호를 설정합니다.**

   기본 사용자(admin)는 미리 구성되어 있으며 삭제할 수 없습니다. 이 사용자는 처음에는 자신의 암호를 구성하는 권한만 갖고 있습니다. 하지만 암호를 설정한 후에 전체 사용자 권한을 얻게 됩니다. 블레이드 시스템 새시 구성 작업을 진행하려면 기본 사용자 admin의 암호를 설정해야 합니다.

   처음 암호를 지정할 때는 다음 조건을 충족해야 합니다.

   - 영문 대문자 또는 소문자로 시작하고 최소 2개 이상의 영문 대문자 또는 소문자를 포함할 것

- 최소 6자 이상일 것(최대 8자까지 가능)
- 최소 하나 이상의 숫자, 마침표(.), 밑줄(_) 또는 하이픈(-)을 포함할 것
- 기본 사용자 로그인 이름(admin), 거꾸로 표기한 기본 사용자 로그인 이름(nimda), 또는 이 이름을 재배열한 것으로 연속하여 읽으면 문자의 순서가 그대로 유지되는 경우는 사용할 수 없음(예를 들어, dmina, minad, inadm, nadmi는 모두 사용할 수 없음)

시스템 컨트롤러의 사용자를 설정하는 자세한 방법은 *Sun Fire B1600 블레이드 시스템 새시 관리 안내서*를 참조하십시오.

사용자 admin의 암호를 설정하려면 다음을 입력합니다.

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

3. 활성 시스템 컨트롤러의 날짜 및 시간을 설정합니다.

참고 – 날짜 및 시간을 설정할 때는 국제 표준시(UTC)를 사용해야 합니다. 서버 블레이드는 시스템 컨트롤러의 UTC에서 시간을 상쇄하여 해당 시간대에 맞춰 현지 시간을 계산합니다. 그리고 서버 블레이드는 시스템 컨트롤러로부터 시간을 가져옵니다.

날짜 및 시간을 설정하는 명령은 setdate 명령입니다. 이 명령의 구문은 다음과 같습니다.

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

여기서:

mm - 월(2자릿수)
dd - 일(2자릿수)
HH - 시(2자릿수)
MM - 분(2자릿수)
SS - 초(2자릿수)

- **시간을 설정하는 경우(24시간 기준)**

  시(2자리)와 분(2자리)을 차례로 입력합니다. 예를 들어, 시간을 11:42로 설정하려면 다음을 입력합니다.

```
sc> setdate 1142
```

- **월, 일 및 시간을 설정하는 경우(24시간 기준. 가장 가까운 분 자리로 반올림)**

  월(2자리), 일(2자리), 시(2자리), 분(2자리)을 차례로 입력합니다. 예를 들어, 3월 27일 11.42 am을 설정하려면 다음을 입력합니다.

```
sc> setdate 03271142
```

- **월, 일, 시간(24시간 기준), 연도 및 초를 설정하는 경우**

  월(2자리), 일(2자리), 시(2자리), 분(2자리), 연도(4문자 또는 2문자. 예를 들어, "2002" 또는 "02"), 그리고 선택 사항으로 마침표와 초(2자리)를 차례로 입력합니다. 예를 들어, 날짜 및 시간을 2002년 3월 27일 11:42 am 47초로 설정하려면 다음을 입력합니다.

```
sc> setdate 2703114202.47
```

2.2 기본 사용자로 스위치에 로그인하여 암호 설정하기

이 단원에서는 스위치에 로그인하여 암호를 설정 및 저장하는 방법을 설명합니다.

참고 – 스위치에서 구성한 사용자 로그인 및 암호 정보는 시스템 컨트롤러에서 구성한 사용자 로그인 및 암호 정보와 완전히 별개입니다.

---

1. 다음을 입력합니다.

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

여기서 *n*은 구성하려는 스위치가 SSC0 또는 SSC1 중 어디에 속하는지에 따라 0 또는 1로 지정합니다. 예를 들어, SSC0의 스위치를 구성하려면 다음을 입력합니다.

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

2. 사용자 이름과 암호를 입력하라는 프롬프트가 나타나면 두 가지 모두에 admin을 입력합니다.

```
Username admin
Password *****

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

3. console# **프롬프트에서 다음을 입력합니다.**

```
Console#configure
```

4. 다음 세 가지 스위치 암호 중에서 적어도 첫번째 것을 설정합니다.

a. 아래와 같이 암호를 설정하여 스위치의 권한 실행 명령 모드에 대한 액세스 권한을 스스로에게 부여합니다.

이 명령 모드는 스위치 구성 전체를 보거나 변경할 수 있는 모드입니다. 기본 사용자 admin (단계 2 참조)은 권한 실행 모드에 대한 권한을 갖고 있습니다. 보안을 위해 이 사용자의 암호를 변경하는 것이 좋습니다. 다음을 입력합니다.

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

여기서 *password*는 1-8자의 문자열이어야 합니다. 0은 암호가 일반 텍스트로 지정되었음을 나타냅니다. 일반 텍스트 또는 암호화된 텍스트를 암호로 사용하는 방법은 *Sun Fire B1600 블레이드 시스템 섀시 스위치 관리 안내서*를 참조하십시오.)

b. 사용자 guest의 암호를 설정합니다.

사용자 guest는 일부 스위치 구성 및 상태 정보를 보거나 ping 명령을 실행할 수 있습니다. 이 사용자는 스위치의 구성 설정을 변경할 수 없습니다. 이 사용자의 기본 암호는 guest입니다. 새 암호를 설정하려면 다음을 입력합니다.

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

*password*는 1-8자의 문자열이어야 합니다. 0은 암호가 일반 텍스트로 지정되었음을 나타냅니다.

c. enable 명령의 암호를 설정합니다.

guest로 로그인한 사용자는 enable 명령을 사용하여 권한 실행 모드에 대한 권한을 얻을 수 있습니다. 이 사용자가 명령행에 enable을 입력하면 암호를 입력하라는 프롬프트가 나타납니다. enable 명령의 기본 암호는 super입니다. 새 암호를 설정하려면 다음을 입력합니다.

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

여기서 *password*는 1-8자의 문자열이어야 합니다. 숫자 15는 enable 명령을 실행하도록 승인된 모든 사용자가 권한 실행 모드에 대한 권한을 가짐을 나타냅니다. 0은 암호가 일반 텍스트로 지정되었음을 나타냅니다.

참고 – 내장 스위치에서 사용할 수 있는 기타 명령 모드에 대한 자세한 내용은 *Sun Fire B1600 블레이드 시스템 섀시 스위치 관리 안내서*를 참조하십시오.

---

5. 다음을 입력하여 스위치의 구성 모드에서 빠져나옵니다.

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

또는

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

6. 스위치의 구성을 변경했으므로 이제 구성을 저장해야 합니다.

저장하려면 실행 구성 펌웨어를 시동 구성 펌웨어로 복사하면 됩니다.

다음을 입력합니다.

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

Console#
```

여기서 *filename*은 새 시동 구성 파일에 지정할 이름입니다.

7. DHCP를 사용하여 스위치의 IP 구성을 제공하는 경우, 이제 다음 작업 중 하나를 수행하여 두번째 스위치를 구성할 것을 권장합니다.

- 두번째 스위치에서 위의 단계 1 ~ 단계 6을 반복합니다.
- A-9페이지의 단원 A.9, "첫번째 스위치의 구성을 두번째 스위치에 복사하기"에 나와있는 지침을 수행합니다. 스위치 구성을 복사하면 앞에서 구성한 로그인 및 암호 정보도 함께 복사됩니다.

DHCP를 사용하지 않는 경우, 지금 두번째 스위치를 구성할 필요는 없습니다. 3장에 언제 이 작업을 수행해야 하는지 나오지만, 구성을 복사하기 전에 먼저 첫번째 스위치에 대해 몇 가지 구성 작업을 더 해야 합니다.

다음에 수행할 작업

3장으로 가서 단순한 네트워크에 새시를 설치하는 작업을 수행한 다음, 4장의 지침에 따라 서버 블레이드를 설정합니다.

보다 복잡한 네트워크에 새시를 설치해야 할 경우에는 5장, 6장 및 7장을 참조하십시오.

3장

간단한 네트워크에 시스템 섀시 설치

이 장은 다음 단원으로 구성되어 있습니다.

3.1 시스템 섀시에서 두 개의 스위치 활용하기

이 장에서는 데이터 네트워크와 관리 네트워크가 분리되지 않은 간단한 네트워크에서 사용할 수 있도록 Sun Fire B1600 블레이드 시스템 섀시를 구성하는 방법을 설명합니다. 이 장의 지침에 따라, 섀시에 있는 두 개의 스위치를 활용하여 서버 블레이드에 각각 두 개의 네트워크 연결을 설정할 수 있습니다.

그림 3-1에는 Sun Fire B1600 블레이드 시스템 섀시가 포함된 예제 네트워크가 나와 있습니다. 그 아래 단원에서는 이 도표와 도표에 표시된 IP 주소를 사용하여 사용자가 수행할 절차에 대해 설명합니다.

또한 이 장에는 예제 `/etc/hosts` 파일과 예제 `/etc/ethers` 및 `/etc/netmasks` 파일이 나와 있습니다. 이러한 예제에서는 네트워크 환경에 섀시를 설치하기 위해 이름 서버에 있는 파일들을 편집하는 방법을 설명합니다. 이 예제 관리 파일들은 참조용으로 사용할 수 있습니다. 그림 3-1에 나와있는 예제 네트워크에 사용되는 IP 주소와 호스트 이름을 사용자의 IP 주소와 호스트 이름으로 대체하십시오.

참고 – 시스템 섀시를 네트워크 환경에 설치하는 방법을 고려할 때에는, 섀시에 두 개의 스위치가 있고 각 서버 블레이드에는 개별 스위치별로 하나씩의 인터페이스가 있음을 유념해야 합니다. 섀시의 시스템 컨트롤러는 특정 시점에 항상 하나만 작동하지만 스위치는 항상 둘 다 작동합니다. 다시 말하면, 정상적으로 작동하는 섀시에서는 *두* 스위치가 모두 서버 블레이드에 지속적인 네트워크 연결을 제공함을 의미합니다. 즉, 스위치 하나가 장애를 일으키더라도 다른 스위치는 계속해서 네트워크 연결을 제공합니다.

이 장에서는 블레이드의 각 이더넷 인터페이스에 상이한 IP 주소를 설정하여 네트워크 이중화 구성을 활용하는 방법에 대해 설명합니다. 또한, 활성 시스템 컨트롤러에 장애가 발생하더라도 컨트롤러 장애가 발생한 SSC 내의 스위치는 계속 네트워크 연결을 제공한다는 점에도 유의하십시오.

시스템 섀시 내의 두번째 스위치가 제공하는 이중화 구성을 활용하려면 다음과 같이 할 것을 권장합니다.

- 항상 두 개의 SSC가 설치된 상태에서 시스템 섀시를 작동하십시오.
- 8개 데이터 네트워크 업링크 포트로부터 상위 네트워크의 서브넷으로 연결되는 케이블 회선을 두번째 스위치의 8개 업링크 포트에도 동일하게 설정하십시오.
- 첫번째 스위치의 구성을 두번째 스위치에도 복사하십시오. 이렇게 하는 방법에 대해서는 A-9 페이지의 단원 A.9, "첫번째 스위치의 구성을 두번째 스위치에 복사하기"를 참조하십시오.

- DHCP 서버를 사용하여 섀시의 IP 네트워크 구성을 제공하는 경우, 각 서버 블레이드의 두 이더넷 인터페이스(ce0 및 ce1)에 IP 주소를 지정하십시오.
- 이름 서버의 /etc/hosts 파일을 설정하여 섀시에 비-DHCP 방식으로 고정 IP 구성을 제공하는 경우, 각 서버 블레이드의 두 이더넷 인터페이스(ce0 및 ce1)에 IP 주소를 지정하십시오.
- 부트 서버의 /etc/ethers 파일을 설정하여 섀시에 비-DHCP 방식으로 고정 IP 구성을 제공하는 경우, 각 서버 블레이드의 두 이더넷 인터페이스에 MAC 및 IP 주소를 지정하십시오.
- 섀시의 이중 내장 스위치와 각 서버 블레이드 간의 이중화된 인터페이스의 장점을 극대화하려면 IPMP(IP 네트워크 다중 경로 지정)를 사용해야 합니다. 자세한 내용은 5장을 참조하십시오.

3.1.1 각 블레이드의 두 이더넷 인터페이스의 MAC 주소 알아내기

부트 서버의 /etc/ethers 파일을 설정하려면 각 서버 블레이드의 ce0와 ce1의 MAC 주소를 알아야 합니다. 이를 알아내려면 다음을 수행하십시오.

1. **활성 시스템 컨트롤러에 로그인합니다(2장 참조).**
2. sc> **프롬프트에서 다음을 입력합니다.**

```
sc> showplatform -v
```

3. **출력에 각 서버 블레이드의** ce0 **MAC 주소가 표시됩니다(s0 ~ s15으로 표기됨).**

   ce1의 MAC 주소는 각 블레이드의 ce0에 사용된 숫자 다음에 오는 십육진수가 됩니다.

3.2 DHCP를 사용한 네트워크 환경 준비

시스템 섀시의 서버 블레이드, 시스템 컨트롤러 및 스위치는 DHCP 서버로부터 IP 주소를 동적으로 받습니다.

섀시의 스위치 및 시스템 컨트롤러에 IP 주소를 제공하도록 DHCP 서버를 구성하는 방법은 1장을 참조하십시오.

서버 블레이드에 IP 주소를 할당하도록 DHCP 서버를 구성하는 방법은 부록 C를 참조하십시오.

참고 – DHCP를 사용하여 서버 블레이드의 IP 설정을 구성하는 경우, 네트워크 복원성을 얻기 위해 IPMP를 사용할 수 없습니다.

반드시 각 서버 블레이드의 개별 인터페이스에 IP 주소를 할당하도록 DHCP 서버를 구성하십시오. IP 구성 매개 변수를 동적으로 제공하도록 DHCP 서버를 설정하는 방법은 *Solaris DHCP Administration Guide*(806-5529)를 참조하십시오. 이 문서가 있는 Sun 설명서 웹 사이트 주소는 다음과 같습니다.

`http://docs.sun.com`

동적으로 할당된 IP 주소로 작동하도록 네트워크 설치 서버를 구성하려면 *Solaris Advanced Installation Guide* 및 *Solaris DHCP Administration Guide*(806-5529)는 물론 부록 C도 참조할 필요가 있습니다.

3.3 고정 IP 주소 및 호스트 이름으로 네트워크 환경 준비하기

그림 3-1에는 두 개의 SSC가 설치되어 있고 16개의 블레이드를 수용하도록 슬롯이 구성된 Sun Fire B1600 블레이드 시스템이 나와 있습니다. 시스템 섀시 각 블레이드의 `ce0` 인터페이스는 SSC0의 스위치에 연결되어 있고, 각 블레이드의 `ce1` 인터페이스는 SSC1의 스위치에 연결되어 있습니다. 스위치의 8개 업링크 포트 중 하나 이상이 네트워크 설치 서버(이름 서버 포함)가 연결된 외부 스위치에 연결되어 있습니다. 이 외부 스위치에는 Sun Fire B1600 블레이드 시스템 섀시에서 상위 네트워크로 통하는 기본 게이트웨이 역할을 하는 라우터(IP 주소 192.168.1.1)가 연결되어 있습니다. 마지막으로, 두 SSC의 100Mbps 네트워크 관리 포트(섀시 후면에 NETMGT로 표기됨)도 외부 스위치에 연결되어 있습니다.

시스템 섀시에 할당된 모든 IP 주소는 동일한 서브넷에 있습니다.

그림 3-1에 묘사된 것과 같은 간단한 네트워크 환경에 시스템 섀시를 설치하려면 Solaris 이름 서버의 `/etc/hosts`, `/etc/ethers` 및 `/etc/netmasks` 파일을 편집해야 합니다.

- 그림 3-2는 그림 3-1에 묘사된 네트워크 구성에 사용된 IP 주소와 호스트 이름이 들어있는 예제 `/etc/hosts` 파일입니다.

■ 그림 3-3은 그림 3-1의 예제 네트워크에서 사용된 IP 네트워크 번호에 대한 넷마스크가 들어 있는 예제 `/etc/netmasks` 파일입니다.

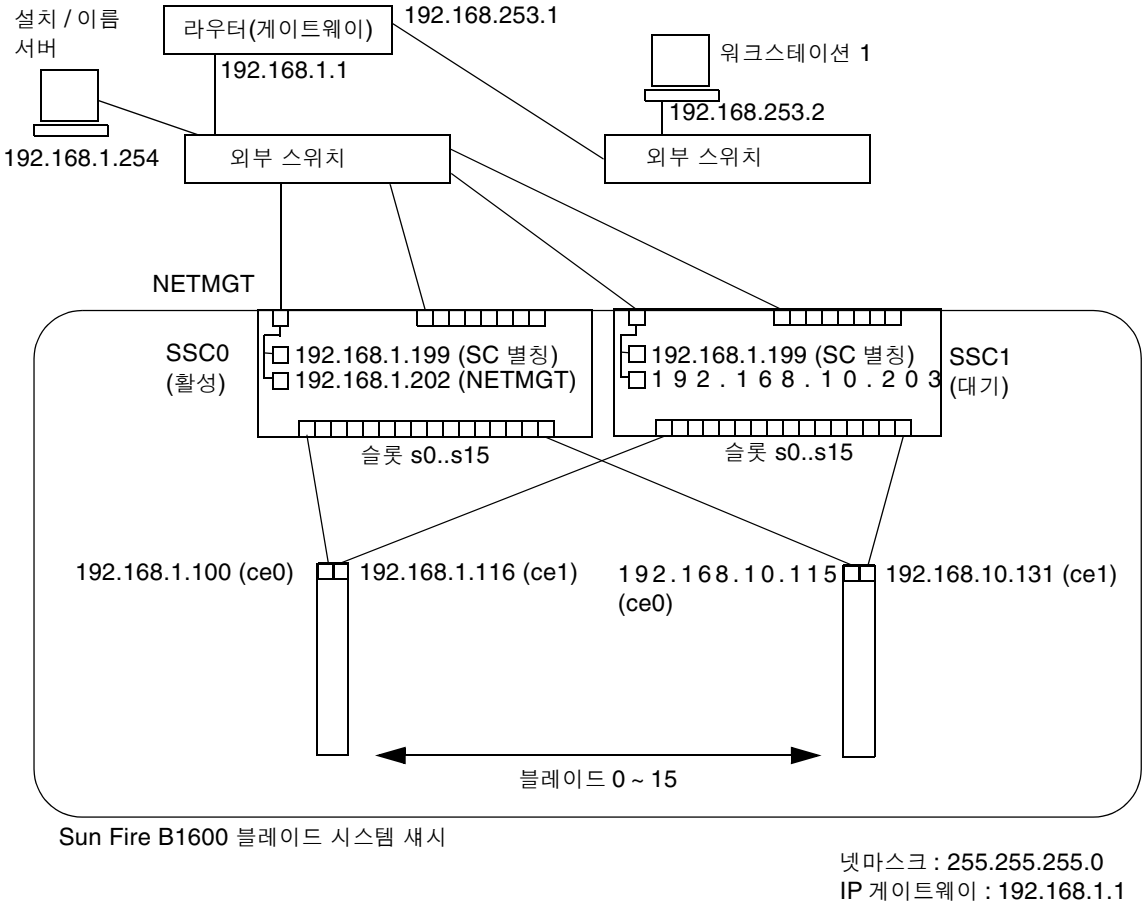


그림 3-1 VLAN을 사용하지 않는 구성의 예

```
# 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
192.168.10.116   medusa-s0-1
192.168.10.117   medusa-s1-1
192.168.10.118   medusa-s2-1
192.168.10.119   medusa-s3-1
192.168.10.120   medusa-s4-1
192.168.10.121   medusa-s5-1
192.168.10.122   medusa-s6-1
192.168.10.123   medusa-s7-1
192.168.10.124   medusa-s8-1
192.168.10.125   medusa-s9-1
192.168.10.126   medusa-s10-1
192.168.10.127   medusa-s11-1
192.168.10.128   medusa-s12-1
192.168.10.129   medusa-s13-1
192.168.10.130   medusa-s14-1
192.168.10.131   medusa-s15-1
```

그림 3-2 이름 서버의 `/etc/hosts` 파일 예제

```
#
# 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
#
```

그림 3-3 이름 서버의 /etc/netmasks 파일 예제

3.4 시스템 컨트롤러 및 스위치 구성

이 단원의 지침을 수행하려면 활성 시스템 컨트롤러(기본적으로 SSC0의 시스템 컨트롤러)에 대한 직렬 연결 또는 텔넷 연결이 있어야 합니다.

시스템 컨트롤러에 로그인하는 방법은 위의 1장과 2장을 참조하십시오.

시스템 컨트롤러에 대한 직렬 연결을 설정하는 방법은 *Sun Fire B1600 블레이드 시스템 섀시 하드웨어 설치 설명서*를 참조하십시오.

활성 시스템 컨트롤러에 대한 텔넷 연결을 설정하는 방법은 1장을 참조하십시오.

3.4.1 시스템 컨트롤러 설정

참고 – 명령행 인터페이스는 활성 시스템 컨트롤러에서만 사용할 수 있습니다. 그러나 이 단원에서 설명하는 setupsc 명령은 두 시스템 컨트롤러를 모두 구성합니다. 시스템 컨트롤러는 특정 시점에 항상 하나만 작동하지만 스위치는 항상 둘 다 작동한다는 점에 유의하십시오.

1. **2장의 지침에 따라 활성 시스템 컨트롤러에 로그인합니다.**

2. setupsc **명령을 실행합니다.**

   sc> 프롬프트에서 다음을 입력합니다.

```
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]?
```

   setupsc를 실행했을 때 질문이 나타나면 Enter를 눌러 기본 응답을 받아들입니다. 기본 응답은 질문 끝 부분에 꺾쇠 괄호로 표시되며, y는 '예', n은 '아니요'를 나타냅니다.

   처음 네 개 질문에 대해 기본값인 y로 대답합니다.

3. **화면에 시스템 컨트롤러(SC)가 DHCP를 사용하여 네트워크 구성을 받도록 설정할 것인지 묻는 질문이 나타나면 '예' 또는 '아니요'로 대답합니다.**

   '예'로 대답했으면 단계 5로 갑니다.

   '아니요'로 대답한 후 다음을 묻는 질문이 나타나면 차례로 해당 값을 지정합니다.

   - SC의 IP 주소. 활성 시스템 컨트롤러(SSC0 또는 SSC1)가 상위 네트워크와 통신하기 위해 사용할 IP 주소를 말합니다.
   - 시스템 컨트롤러의 IP 넷마스크
   - 시스템 컨트롤러의 기본 게이트웨이

4. SC의 사설 IP 주소를 구성하겠냐는 질문에 '예' 또는 '아니요'로 대답합니다.

활성 및 대기 시스템 컨트롤러 모두 사설 IP 주소를 가질 수 있습니다. 이 사설 IP 주소는 서로 달라야 하며 SC의 IP 주소(단계 3에서 지정)와도 달라야 합니다.

두 시스템 컨트롤러의 상태를 점검하는 방법으로 이 주소를 핑 테스트할 수 있으므로 이들 주소를 지정해두는 것이 좋습니다. 또한 활성 시스템 컨트롤러의 공개 네트워크 주소를 통해서 뿐만 아니라 사설 IP 주소를 이용해서도 활성 시스템 컨트롤러에 텔넷 연결할 수 있습니다. 대기 시스템 컨트롤러에는 사설 IP 주소가 있어도 텔넷 연결할 수 없습니다.

5. SC에 VLAN을 사용하겠냐는 질문에 '예' 또는 '아니요'로 대답합니다.

'예'라고 대답하면 시스템 컨트롤러의 이더넷 포트는 다음 질문에서 지정하는 VLAN으로 태그된 프레임만 수신하고 전송합니다.

a. 화면에 질문이 나타나면 관리 VLAN의 VLAN ID(1부터 4094 사이의 수)를 지정합니다.

스위치의 관리 VLAN에 사용하려는 것과 동일한 숫자를 지정합니다. 스위치의 관리 VLAN의 기본 숫자는 2입니다. VLAN 1은 데이터 네트워크의 기본 VLAN 값이므로 사용하지 않는 것이 좋습니다.

6. 시스템 관리 시스템(SMS)의 IP 주소를 묻는 질문이 나타나면 해당 주소를 지정합니다.

Enter를 눌러 다음 질문으로 이동하거나 Sun Fire B1600용 Sun Management Center 소프트웨어 또는 Sun SNMP Management Agent를 실행하는 데 사용되는 네트워크 관리 스테이션의 주소를 입력합니다.

7. 관리 시스템 인터페이스를 구성하겠냐고 물어보면 '예' 또는 '아니요'로 대답합니다.

'예'라고 대답하면 새시 구성 부품의 작동이 정지되었을 때 해당 구성 부품을 자동으로 재시작할 것인지, 그리고 서버 블레이드를 새시에 삽입하는 즉시 자동으로 블레이드의 전원이 켜지게 할 것인지 등을 묻는 질문이 이어집니다.

a. 질문이 표시되면, 작동이 정지되었을 때 해당 장치를 자동으로 재시작하도록 모든 현장 교체형 장치(두 SSC와 모든 서버 블레이드)를 설정할지 여부를 대답합니다.

'아니요'로 대답하면 작동이 정지되었을 때 자동으로 재시작하도록 설정할 현장 교체형 장치가 하나도 없는지를 묻는 질문이 나타납니다. 다시 '아니요'로 대답하면 작동이 정지되었을 때 해당 장치를 자동으로 재시작할지 여부를 각각의 현장 교체형 장치마다 묻습니다.

b. 섀시 전원이 켜지는 즉시, 그리고 전원이 들어온 섀시에 서버 블레이드를 삽입하는 즉시 해당 블레이드의 전원이 자동으로 켜지도록 모든 서버 블레이드를 설정할지 묻는 질문에 답합니다.

'아니요'로 대답하면 새시 전원을 켜거나 슬롯에 블레이드를 삽입했을 때 자동으로 전원이 켜지도록 설정할 블레이드가 하나도 없는지를 묻는 질문이 나타납니다. 다시 '아니요'로 대답하면 새시 전원을 켜거나 슬롯에 블레이드를 삽입했을 때 해당 블레이드의 전원을 자동으로 켤지 여부를 각각의 블레이드마다 묻습니다.

8. 시스템 컨트롤러 매개 변수를 구성하겠냐고 물어 보면 '예' 또는 '아니요'로 대답합니다.

'예'라고 대답하면, 텔넷 인터페이스를 통한 이벤트 보고, 시스템 컨트롤러 명령 프롬프트 설정, 시스템 컨트롤러 사용자 세션의 시간 초과 설정, 암호 입력 시 별표(*) 표시 여부, 그리고 시스템 컨트롤러가 네트워크 시간 프로토콜(NTP)을 사용하게 할지 등을 묻는 질문이 이어집니다.

a. CLI 이벤트 보고 기능을 사용하겠냐는 질문이 나타났을 때 SSC에 대한 텔넷 연결을 통해 이벤트 보고를 수신하려는 경우 `y`를 누릅니다.

SSC의 직렬 연결을 통한 이벤트 보고 기능은 해제할 수 없다는 점에 유의하십시오.

b. 단계 a에서 `y`를 입력한 경우, 표시할 이벤트 레벨을 묻는 질문에 대한 기본 응답을 받아들여 심각도 레벨 2 이상의 이벤트를 표시하도록 지정합니다.

레벨 2를 지정하면 MINOR, MAJOR 및 CRITICAL 이벤트가 표시됩니다.

c. 시스템 컨트롤러의 명령행 프롬프트를 지정하거나 기본값을 받아들입니다.

d. 명령행 인터페이스의 시간 초과 값을 지정합니다.

기본값인 0을 지정하면 사용자 입력이 없어도 사용자 세션이 시간 초과되지 않습니다.

e. 사용자가 암호를 입력할 때 화면에 별표(*)가 표시되도록 할 것인지 지정합니다.

f. 네트워크 시간 프로토콜(NTP)을 사용할 것인지 지정합니다.

네트워크에 시간 서버가 있고 그 시간 서버를 사용하려는 경우 '예'라고 대답합니다. 그리고 나서 1차 및 2차 NTP 서버의 IP 주소를 입력하라는 메시지가 표시되면 해당 주소를 입력합니다.

9. 네트워크 변경 사항을 즉시 적용하겠냐고 물어보면 '예' 또는 '아니요'로 대답합니다.

이 질문은 시스템 컨트롤러의 네트워크 설정을 변경한 경우에만 나타납니다. 텔넷 연결을 통해 시스템 컨트롤러를 구성 중일 때 '예'라고 대답하면 텔넷 연결이 끊길 수도 있다는 점에 유의하십시오.

10. 3-14페이지의 단원 3.4.3, "SSC0 및 SSC1의 스위치 설정"의 지침에 따라 스위치를 설정합니다.

```
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 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>
```

그림 3-4 setupsc의 출력 및 응답 예제(비-DHCP 구성)

```
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]?
Do you want the network changes to take effect immediately [y]?
sc>
```

그림 3-5 setupsc의 출력 및 응답 예제(DHCP 구성)

3.4.2 시스템 컨트롤러 구성 보기

시스템 컨트롤러의 구성을 보려면 showsc -v 명령을 실행합니다. 그러면 시스템 컨트롤러의 모든 설정 가능한 속성들이 나열됩니다.

- **다음을 입력합니다.**

```
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

Output continued on next page
```

그림 3-6 블레이드가 세 개 있는 섀시의 기본 구성(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>
```

그림 3-7 블레이드가 세 개 있는 섀시의 기본 구성(*계속*)

3.4.3 SSC0 및 SSC1의 스위치 설정

이 단원에서는 스위치의 IP 주소, 넷마스크 및 기본 게이트웨이를 구성하는 방법을 설명합니다. 스위치는 기본적으로 자신의 IP 구성을 DHCP에서 받으려고 합니다. 그러므로 스위치의 IP 정보를 제공하도록 DHCP 서버를 구성했다면 이 단원은 그냥 지나가십시오.

1. 다음을 입력하여 SSC0의 스위치에 로그인합니다.

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

2. 나타나는 화면에서 스위치의 사용자 이름과 암호를 입력합니다.

3. **기본적으로 스위치의 IP 주소 및 넷마스크는 DHCP에 의해 설정됩니다. 아래와 같이 입력하여 이들을 수동으로 설정할 수도 있습니다.**

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

여기서 *vlan id*는 스위치의 네트워크 관리 포트 NETMGT가 포함된 VLAN의 번호(기본 스위치 구성의 경우 2)이며, *ip address*는 스위치에 지정할 IP 주소이고, *netmask*는 설정하려는 넷마스크입니다.

예를 들어, 그림 3-1의 SSC0 스위치에 대한 IP 주소와 넷마스크를 지정하려면 다음을 입력합니다.

```
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. **기본적으로 기본 게이트웨이는 DHCP에 의해 설정됩니다.**

아래와 같이 입력하여 수동으로 설정할 수도 있습니다.

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

여기서 *ip address*는 기본 게이트웨이로 지정하려는 장치의 IP 주소입니다.

5. 새 스위치 구성을 저장합니다.

스위치 콘솔에 아래와 같이 입력합니다.

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

Console#
```

여기서 *filename*은 새 시동 구성이 포함될 파일에 지정하는 이름입니다.

6. exit을 입력하여 첫번째 스위치에서 로그아웃합니다.

그 다음에 #.을 입력하여 스위치의 명령행 인터페이스에서 나와 시스템 컨트롤러의 sc> 프롬프트로 돌아갑니다.

7. 이제 A-9페이지의 단원 A.9, "첫번째 스위치의 구성을 두번째 스위치에 복사하기"의 지침에 따라 두번째 스위치를 구성합니다.

아니면 SSC1의 스위치에 대해 단계 1부터 단계 6까지를 다시 수행합니다.

다음에 수행할 작업

4장의 지침에 따라 서버 블레이드를 설정합니다.

4장

서버 블레이드 설치 및 초기 진단 수행

이 장에서는 서버 블레이드의 전원을 켠 다음 콘솔에 액세스하는 방법을 설명합니다. 그런 다음 *Sun Fire B1600 블레이드 시스템 새시 소프트웨어 설치 설명서*에서 설명된 Advanced Lights-out Management Software를 제외한 여러 가지 도구를 사용하여 초기 진단을 수행하는 방법을 설명합니다.

Solaris 시스템에서 진단을 수행하는 일반적인 방법은 *OpenBoot Command Reference Manual*과 *Sun VTS Users Guide*를 참조하십시오. 이러한 설명서는 Solaris 미디어 키트와 함께 제공된 Software Supplement CD나 다음 사이트에서 찾아볼 수 있습니다.

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

이 장은 다음 단원으로 구성되어 있습니다.

참고 – 블레이드 콘솔 위치에 있을 때 활성 시스템 컨트롤러의 `sc>` 프롬프트로 돌아가려면 **#.**을 입력하십시오.

4.1 서버 블레이드 전원 켜기

공장 출하시의 기본 설정 상태인 서버 블레이드에 전원을 공급하면 해당 로컬 하드 디스크에 있는 운영 환경 스텁에서 블레이드가 자동적으로 시동됩니다. 그런 다음 블레이드는 운영 환경 설치 작업을 완료할 네트워크 설치 서버를 검색합니다.

네트워크 설치 서버를 설정하려면 *Solaris Advanced Installation Guide*에 나와있는 지침을 따르십시오.

이 설명서의 부록 D에는 시스템 섀시에 있는 일련의 서버 블레이드를 Web Start Flash 아카이브를 사용하여 신속하게 구성하는 방법에 대한 추가 정보가 나와 있습니다.

준비가 되면 서버 블레이드의 전원을 켠 다음 아래 지침에 따라 해당 블레이드를 시동하십시오.

1. **서버 블레이드를 켭니다.**

   다음을 입력합니다.

```
sc> poweron sn
```

   여기서 *n*은 서버 블레이드가 들어있는 슬롯의 번호입니다.

2. **시동 프로세스를 보거나 작업을 수행할 수 있도록 서버 블레이드의 콘솔에 로그인합니다.**

   sc> 프롬프트에 다음을 입력하여 블레이드의 콘솔에 액세스합니다.

```
sc> console sn
```

   여기서 *n*은 블레이드가 들어있는 슬롯의 번호입니다.

   다음 수행할 작업은 *Solaris Advanced Installation Guide*에서 선택한 Solaris 설치 방법에 따라 달라집니다.

3. **필요할 경우 시동 프로세스를 직접 수행하거나 진단 작업을 실행하기 위해 시동 프로세스를 중단시킬 수 있습니다.**

   시동 프로세스를 중단시키려면[1] 다음을 입력합니다.

```
sc> break sn
```

   여기서 *n*은 블레이드가 들어있는 슬롯의 번호입니다.

4. **서버 블레이드에 초기 진단 작업을 수행하려면 이 장에 나와있는 나머지 지침을 수행합니다.**

참고 – 블레이드 콘솔 위치에 있을 때 활성 시스템 컨트롤러의 sc> 프롬프트로 돌아가려면 **#.**을 입력하십시오.

4.2 POST 진단(전원 인가 후 자가 검사) 사용

이 단원에서는 시동시 서버 블레이드에 기본적으로 수행되는 POST 진단 작업을 제어하는 방법을 설명합니다.

4.2.1 진단 검사의 범위 제어

POST 진단에는 3가지 수준의 진단 검사가 있습니다.

- max (최고 수준)
- min (최소 수준)
- off (검사 안함)

OpenBoot PROM 변수 diag-level을 사용하여 원하는 수준을 설정할 수 있습니다. diag-level은 기본적으로 min으로 설정되어 있습니다. 이 값을 설정하려면 다음을 입력하십시오.

```
ok diag-level level
```

여기서 *level*은 min, max 또는 off로 지정합니다.

---

1. break 명령을 받아들이지 않도록 블레이드를 구성하는 방법은 kbd(1) MAN 페이지를 참조하십시오.

4.2.2 시스템 컨트롤러에서 블레이드의 진단 설정 무시하기

시스템 컨트롤러의 bootmode 명령을 사용하여 diag-level 및 diag-switch? 설정을 일시적으로 무시할 수 있습니다.

- **시동시 진단 작업을 수행하지 않도록 설정된 상태일 때 서버 블레이드가 이 작업을 수행하게 하려면 다음과 같이 합니다.**

  a. #.을 입력하여 시스템 컨트롤러의 명령행 인터페이스로 돌아갑니다.

  b. 다음을 입력합니다.

```
sc> bootmode diag sn
```

  여기서 *n*은 구성할 블레이드의 슬롯 번호입니다.

  이 명령은 하나의 시동 프로세스에 대해서만 diag-switch?를 true로 설정하고 diag-level을 min으로 설정하는 것과 동일한 작업을 수행합니다. 블레이드의 diag-level이 max 또는 min으로 설정된 경우 bootmode 명령은 블레이드 설정을 변경하지 않습니다.

- **시동시 진단 작업을 수행하도록 설정된 상태일 때 진단 작업을 수행하지 않고 서버 블레이드를 시동하려면 다음과 같이 합니다.**

  a. #.을 입력하여 시스템 컨트롤러의 명령행 인터페이스로 돌아갑니다.

  b. 다음을 입력합니다.

```
sc> bootmode skip_diag sn
```

  여기서 n은 구성할 블레이드의 슬롯 번호입니다.

  이 명령은 diag-switch?를 false로 설정하는 것과 동일한 작업을 수행합니다.

4.2.3 POST 진단 실행

OpenBoot PROM(OBP) 변수 diag-switch?가 true로 설정된 경우 POST 진단은 서버의 전원이 켜지면 자동적으로 수행됩니다. 그러나 diag-switch?의 기본 설정은 false입니다.

POST 진단을 초기화하려면 diag-switch? 변수를 true로 설정하고 diag-level 변수를 max 또는 min으로 설정해야 합니다(off로 설정하면 안됩니다). 이렇게 했으면 서버 블레이드를 재설정해야 합니다. 아래 지침을 수행하십시오.

1. **서버 블레이드의** ok **프롬프트에서 다음을 입력합니다.**

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

2. **#.을 입력하여 시스템 컨트롤러의 명령행 인터페이스로 돌아갑니다.**

3. **블레이드의 전원을 껐다가 다시 켭니다.**

   다음을 입력합니다.

```
sc> poweroff sn
```

   여기서 *n*은 블레이드가 들어있는 슬롯의 번호입니다.

   그런 다음 다음을 입력합니다.

```
sc> poweron sn
```

4. **블레이드의 전원을 켠 후 가능하다면 2-3초 내에 블레이드의 콘솔에 액세스하여 진단 결과를 확인합니다.**

   다음을 입력합니다.

```
sc> console sn
```

5. **시동이 완료되면 #.을 입력하여 시스템 컨트롤러의 명령행 인터페이스로 돌아간 후에 다음을 입력하여 부트 타임 콘솔의 결과를 확인할 수 있습니다.**

```
sc> consolehistory boot sn
```

   POST 진단 중에 오류가 발견되면 해당 장애를 설명하는 오류 메시지가 표시됩니다.

   POST에서 "치명적"인 오류(예: 내장 메모리 또는 CPU 등의 하드웨어 장애)가 발견되면 서버 블레이드의 전원이 꺼지고 블레이드의 고장 LED에 불이 들어옵니다.

4.3 OpenBoot Diagonostics(obdiag) 사용

OpenBoot Diagonostics를 실행하려면 다음을 수행하십시오.

1. **ok 프롬프트에서 다음을 입력합니다.**

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

2. **유형:**

```
ok obdiag
```

그러면 OpenBoot Diagnostics 메뉴가 나타납니다.

```
                                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=
```

그림 4-1 obdiag 메뉴

각 검사에 대한 설명은 표 4-1에 나와 있습니다. 수행하려는 검사의 번호를 사용하여 test 명령을 실행합니다. 예를 들어, 기본 이더넷 포트에 대한 검사를 실행하려면 다음을 입력합니다.

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

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

3. **검사를 마치면 OpenBoot Diagnostics를 종료한 다음** `auto-boot?` **값을 true로 되돌립니다.**
   다음을 입력합니다.

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

각 검사의 기능이 아래에 설명되어 있습니다.

표 4-1 Open Boot Diagnostics 검사

1	`bscv@0,0`	BSC(블레이드 지원 칩) 검사
2	`ide@d`	IDE 컨트롤러 검사
3	`network@a`	기본 이더넷 인터페이스 검사
4	`network@b`	보조 이더넷 인터페이스 검사
5	`pmu@3`	전원 관리 장치 검사
6	`rtc@0,70`	실시간 클럭 장치 검사
7	`serial@0,3f8`	시스템 컨트롤러에 대한 직렬 인터페이스 검사

4.4 기타 OpenBoot PROM 명령 사용

이 단원에는 사용할 수 있는 OpenBoot PROM 명령과 그에 대한 설명이 나와 있습니다.

`show-devs` *명령*

OpenBoot PROM의 `show-devs` 명령은 OBP 장치 트리에 있는 장치를 나열합니다.

printenv *명령*

OpenBoot PROM의 printenv 명령은 시스템 NVRAM에 저장된 OpenBoot PROM 구성 변수를 보여줍니다. 표시 내용에는 이러한 변수의 현재 값과 기본값이 포함됩니다. 또한 변수를 지정하여 해당 변수에 대한 현재 값만 표시되게 할 수도 있습니다. 예를 들어, printenv diag-level을 입력하면 diag-level 변수에 대한 현재 값이 표시됩니다.

watch-clock *명령*

watch-clock 명령은 초당 하나씩 증가하는 숫자 카운터를 표시합니다. 정상 작동시에는 이 초 카운터가 0에서 59까지 반복적으로 증가합니다. 다음은 watch-clock 명령을 사용했을 때 출력되는 결과의 예제 스냅샷입니다.

```
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 *및* watch-net-all *명령*

watch-net 및 watch-net-all 명령은 블레이드의 이더넷 인터페이스상의 이더넷 패킷을 모니터링합니다. 오류가 없이 수신된 패킷은 마침표(.)로 표시됩니다. 프레이밍 오류나 순환 중복 검사(CRC) 오류 등과 같은 오류는 X로 표시되고 그에 대한 설명이 함께 표시됩니다.

다음 예제는 watch-net 및 watch-net-all 명령의 출력 결과를 보여줍니다.

```
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 *명령*

probe-ide 명령을 사용하면 블레이드의 IDE 컨트롤러는 4개의 해당 IDE 장치 각각에 대해 질의를 전송합니다(실제로는 IDE 컨트롤러에는 항상 한 개의 장치만 연결되어 있습니다). 기본 마스터 장치에 대해 not present가 응답되면 하드 디스크에 문제가 생겼거나 IDE 컨트롤러와 하드 디스크간의 연결에 이상이 있는 것입니다.

그림 4-2 probe-ide 출력 메시지

```
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 사용

SunVTS(Sun Validation and Test Suite)는 하드웨어 컨트롤러, 장치 및 플랫폼의 구성 및 기능을 확인할 때 사용하는 온라인 진단 도구입니다. SunVTS는 *Software Supplement for the Solaris Operating Environment* CD에 들어 있습니다.

이 소프트웨어는 다음과 같은 Solaris 프롬프트에서 실행해야 합니다.

- 명령행 인터페이스
- 윈도우 데스크탑 환경의 그래픽 인터페이스

SunVTS 소프트웨어를 사용하면 원격으로 연결된 서버에서 검사 세션을 확인하고 관리할 수 있습니다. 아래 표에는 일부 검사 목록이 나와 있습니다.

표 4-2 SunVTS 검사

SunVTS 검사	설명
disktest	로컬 디스크 드라이브를 검사합니다.
fputest	부동 소수점 처리 장치(FPU)를 검사합니다.
nettest	시스템의 CPU 보드와 시스템의 네트워크 어댑터에 있는 네트워킹 하드웨어를 검사합니다.
pmem	물리적 메모리를 검사합니다(읽기 작업만).
vmem	가상 메모리(스왑 파티션과 물리적 메모리의 조합)를 검사합니다.
bsctest	서버 블레이드에 있는 BSC(블레이드 지원 칩)를 검사합니다.

4.5.1 SunVTS 설치 여부 확인

서버 블레이드에 SunVTS가 설치되어 있는지 확인하려면 다음을 입력하십시오.

```
# pkginfo -l SUNWvts
```

- SunVTS 소프트웨어가 설치된 경우 설치된 소프트웨어에 대한 정보가 표시됩니다.
- SunVTS 소프트웨어가 설치되지 않은 경우 다음과 같은 오류 메시지가 표시됩니다.

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

4.5.2 SunVTS 설치

SunVTS는 *Software Supplement for the Solaris Operating Environment* CD에 들어 있습니다. 설치 방법은 *Sun Hardware Platform Guide*를 참조하십시오. SunVTS 소프트웨어를 설치할 기본 디렉토리는 `/opt/SUNWvts`입니다.

4.5.3 SunVTS 실행

워크스테이션에서 SunVTS 그래픽 사용자 인터페이스를 통해 SunVTS 세션을 실행하여 Sun Fire B100s 서버 블레이드 검사 작업을 수행하려면 아래의 절차를 따르십시오.

1. **워크스테이션에서 `xhost` 명령을 실행하여 서버 블레이드에 원격 액세스합니다.**

   다음을 입력합니다.

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

   여기서 *remote_hostname*은 서버 블레이드의 호스트 이름입니다.

2. **수퍼유저 또는 루트 사용자로 서버 블레이드에 원격 로그인합니다.**

3. **다음을 입력합니다.**

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

   여기서 *local_hostname*은 사용하고 있는 워크스테이션의 이름입니다.

참고 – `/opt/SUNWvts/bin` 디렉토리는 SunVTS 소프트웨어의 기본 설치 디렉토리입니다. 소프트웨어를 다른 디렉토리에 설치한 경우, 그 경로를 대신 사용하십시오.

SunVTS 소프트웨어를 시작하면 SunVTS 커널은 검사할 시스템에 어떤 장치가 있는지 확인하여 그 결과를 Test Selection 패널에 표시합니다. 시스템의 각 하드웨어 장치에는 그와 관련된 SunVTS 검사 작업이 있습니다.

실행할 각 검사 작업의 확인란을 선택하여 검사 세션을 세밀하게 조정할 수 있습니다.

5장

데이터 네트워크 및 관리 네트워크가 분리된 환경에 시스템 섀시 설치

이 장은 다음 단원으로 구성되어 있습니다.

5.1 시스템 섀시에서 두 개의 스위치 활용하기

이 장에서는 데이터 네트워크와 관리 네트워크가 분리된 환경에서 사용할 수 있도록 Sun Fire B1600 블레이드 시스템 섀시를 구성하는 방법을 설명합니다. 이 장의 지침에 따라, 섀시에 있는 두 개의 스위치를 활용하여 서버 블레이드에 각각 두 개의 네트워크 연결을 설정할 수 있습니다.

그림 5-1에는 Sun Fire B1600 블레이드 시스템 섀시가 포함된 예제 네트워크가 나와 있습니다. 그 아래 단원에서는 이 도표와 도표에 표시된 IP 주소를 사용해서 사용자가 수행할 절차에 대해 설명합니다.

또한 이 장에는 예제 `/etc/hosts` 파일과 예제 `/etc/netmasks` 파일이 나와 있습니다. 이러한 예제에서는 이름 서버에 있는 파일들을 편집하여 시스템 섀시의 서버 블레이드에 Solaris를 구성하는 절차를 간소화하는 방법을 설명합니다(서버 블레이드 구성 절차는 이 장의 마지막 부분에 나와 있습니다). 이 예제 관리 파일들은 참조용으로 사용할 수 있습니다. 그림 5-1에 나와 있는 예제 네트워크에 사용되는 IP 주소와 호스트 이름을 사용자의 IP 주소와 호스트 이름으로 대체하십시오.

참고 – 3장에서 언급된 바와 같이 시스템 섀시를 네트워크 환경에 설치하는 방법을 고려할 때에는, Sun Fire B1600 블레이드 시스템 섀시에 두 개의 스위치가 있음을 유념해야 합니다. 섀시의 시스템 컨트롤러는 특정 시점에 항상 하나만 작동하지만 스위치는 항상 둘 다 작동합니다. 다시 말하면, 정상적으로 작동하는 시스템 섀시에서는 두 스위치가 모두 서버 블레이드에 지속적인 네트워크 연결을 제공함을 의미합니다. 즉, 스위치 하나가 장애를 일으키더라도 다른 스위치는 계속해서 네트워크 연결을 제공합니다. 또한 시스템 컨트롤러 중 하나에 장애가 발생하더라도 해당 SSC 모듈에 속한 스위치는 계속해서 네트워크 연결을 제공합니다. 동일한 모듈에 설치되어 있다 하더라도 시스템 컨트롤러와 스위치는 서로 개별적으로 작동합니다.

이 장에서는 VLAN과 IPMP(IP 네트워크 다중 경로 지정)를 사용하여 데이터 네트워크 및 관리 네트워크와 블레이드간에 이중화된 연결을 설정함으로써 두 개의 스위치를 활용하는 방법을 설명합니다.

시스템 섀시 내의 두번째 스위치가 제공하는 이중화 구성을 활용하려면 다음과 같이 할 것을 권장합니다.

- 항상 두 개의 SSC가 설치된 상태에서 시스템 섀시를 작동하십시오.
- 8개 업링크 포트로부터 상위 네트워크의 서브넷으로 연결되는 케이블 회선을 두번째 스위치의 8개 업링크 포트에도 동일하게 설정하십시오.

- 스위치의 IP 주소, 넷마스크 및 기본 게이트웨이를 설정하기 전에 첫번째 스위치의 구성 파일을 두번째 스위치에도 복사하십시오. 이렇게 하는 방법은 A-9페이지의 단원 A.9, "첫번째 스위치의 구성을 두번째 스위치에 복사하기"를 참조하십시오.
- 데이터 네트워크 및 관리 네트워크와 각 서버 블레이드간의 이중화된 인터페이스를 지원하는 IPMP(IP 네트워크 다중 경로 지정) 구성에 적합한 IP 주소를 이름 서버의 `/etc/hosts` 파일에서 지정하십시오(그림 5-2 참조). 그림 5-2에는 3장의 예제 `/etc/hosts` 파일(그림 3-2 참조)에 나열된 IP 주소보다 적은 수의 블레이드 IP 주소가 나와 있습니다. 이는 IPMP를 사용할 경우 각 서버 블레이드에 대해 하나의 인터페이스만 있으면 되기 때문입니다.
- 이름 서버의 `/etc/ethers` 파일을 설정할 때는 서버 블레이드의 두 이더넷 인터페이스 모두에 MAC 주소와 IP 주소를 지정하십시오.

5.2 DHCP를 사용한 네트워크 환경 준비

참고 – DHCP를 사용하여 각 서버 블레이드의 두 인터페이스에 대한 IP 설정을 구성하는 경우, 물리적 네트워크에 대한 이중화된 연결을 구성하거나 VLAN에 대한 다중 연결을 구성하기 위해 IPMP를 사용할 수 없습니다.

DHCP를 사용할 경우 시스템 컨트롤러 및 스위치용 DHCP 서버는 관리 네트워크에 위치하고 블레이드용 DHCP 서버는 데이터 네트워크에 위치하도록 구성하십시오.

네트워크 설치 서버 및 DHCP 서버를 설정하는 방법은 1장, 3장 및 부록 C를 참조하십시오.

5.3 고정 IP 주소를 사용한 네트워크 환경 준비

그림 5-1은 이전 장에 나와있는 예제 구성과 유사한 네트워크를 보여주지만, 두 SSC의 100Mbps 네트워크 관리 포트(NETMGT)는 데이터 업링크 포트가 연결된 스위치가 아닌 다른 스위치에 연결되어 있습니다. 이 새로운 외부 스위치는 섀시의 데이터 업링크 포트가 연결된 스위치와는 다른 서브넷에 위치하고 있습니다. 이 서브넷은 네트워크 관리 트래픽 전용 서브넷으로 섀시의 시스템 컨트롤러와 스위치를 모두 포함하고 있습니다. 관리 VLAN(VLAN 2)은 두 시스템 컨트롤러 인터페이스와 두 스위치 관리 포트를 모두 포함하고 있는 반면, 모든 서버 블레이드 포트와 업링크 포트는 VLAN 1에 위치합니다.

또한 그림 5-1에는 각 블레이드의 `ce0` 인터페이스와 SSC0 스위치간의 연결, 그리고 각 블레이드의 `ce1` 인터페이스와 SSC1 스위치간의 연결이 나와 있습니다. 각 서버 블레이드 인터페이스에는 하나의 IP 주소가 아닌 4개의 IP 주소가 할당되어 있음에 유의하십시오. 이 4개의 주소는 각 인터페이스가 이중화된 연결로서의 역할을 수행할 수 있도록 IPMP 드라이버에 의해 사용됩니다(5-9페이지의 단원 5.5, "네트워크 복원성을 얻기 위해 IPMP를 사용하여 서버 블레이드 설정하기" 참조).

그림 3-1에서와 같이(3장 참조), 그림 5-1에 나와있는 각 스위치의 8개 업링크 포트 중 하나 이상이 네트워크 설치 서버(이름 서버 포함)가 연결된 외부 스위치에 연결되어 있습니다. 이 외부 스위치에는 Sun Fire B1600 블레이드 시스템 섀시에서 상위 네트워크로 통하는 기본 게이트웨이 역할을 하는 라우터(IP 주소 192.168.1.1)가 연결되어 있습니다.

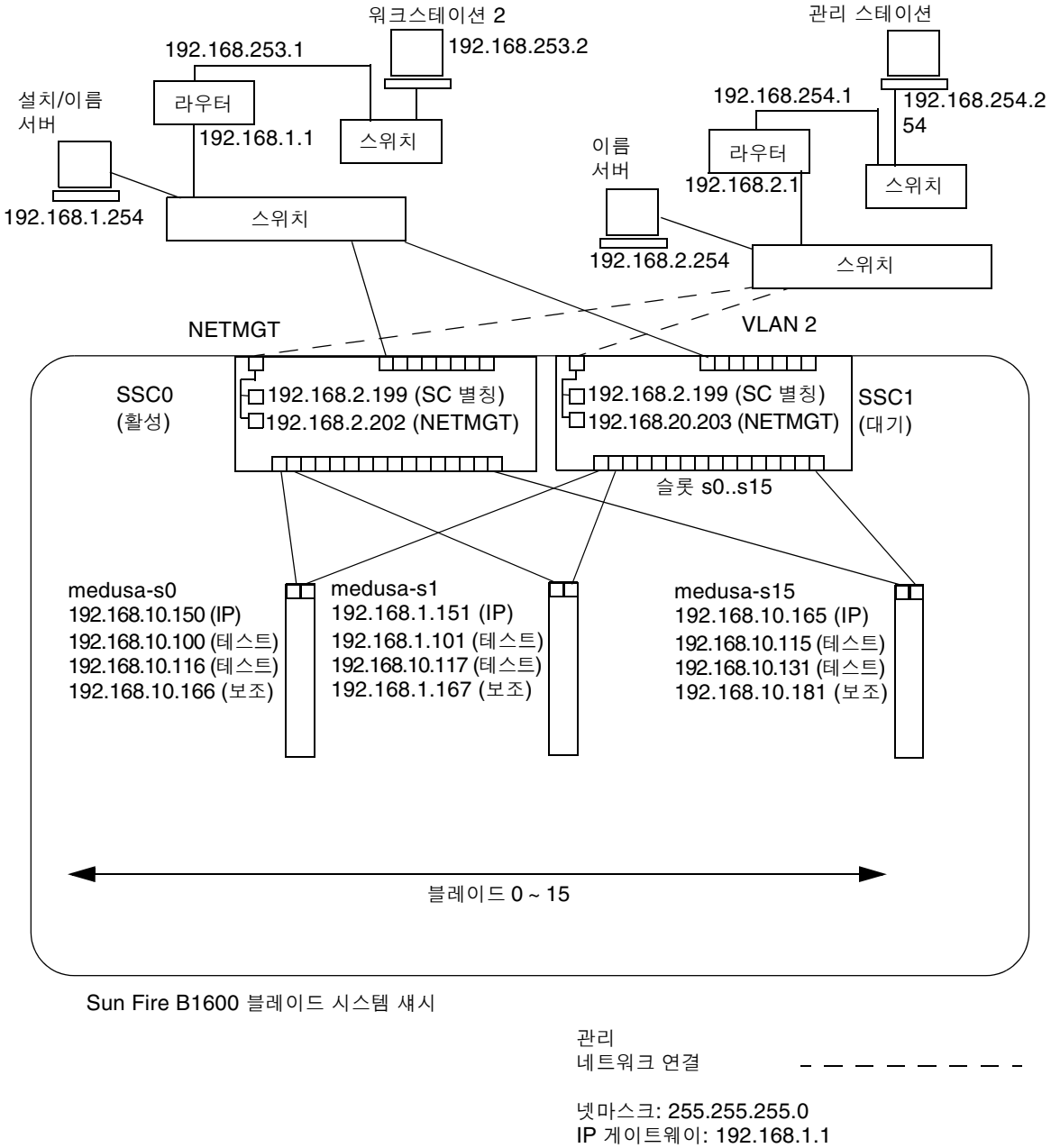
참고 – 그림 5-1에서는 스위치의 관리 포트(NETMGT)가 서버 블레이드 포트에 직접 연결되지 않은 점에 유의하십시오. 이것은 기본적으로 관리 네트워크 상에서는 서버 블레이드를 직접 관리할 수 없음을 의미합니다. 이것은 데이터 네트워크를 통해 올 수 있는 적대적 공격으로부터 관리 네트워크를 보호하기 위한 보안 기능입니다. 서버 블레이드에서 관리 포트로 가는 트래픽을 허용하는 방법은 부록 A와 6장을 참조하십시오.

Sun Fire B1600 블레이드 시스템 섀시를 그림 5-1에 설명된 것과 같은 환경(즉, 데이터 네트워크와 관리 네트워크가 분리된 환경)에 설치하려면, 데이터 네트워크와 관리 네트워크의 Solaris 이름 서버에서 `/etc/hosts`, `/etc/ethers` 파일과 `/etc/netmasks` 파일을 편집해야 합니다.

- 그림 5-2는 그림 5-1에 설명된 데이터 네트워크의 블레이드 시스템 섀시에서 사용된 IP 주소와 호스트 이름이 들어있는 예제 `/etc/hosts` 파일입니다.

- 그림 5-2는 그림 5-1에 설명된 관리 네트워크의 시스템 섀시 구성 부품(두 개의 SSC와 스위치)에 사용된 IP 주소와 호스트 이름이 들어있는 예제 `/etc/hosts` 파일입니다.
- 그림 5-3은 그림 5-1의 예제 네트워크에서 사용된 IP 네트워크 번호에 대한 넷마스크가 들어있는 `/etc/netmasks` 예제 파일입니다.

참고 – 각 서버 블레이드의 공개 IP 주소(IPMP가 사용하는 테스트 IP 주소가 아닌 다른 주소)만 이름 서버의 `/etc/hosts` 파일에 등록하면 됩니다. 아울러 각 블레이드의 테스트 주소에 대한 설명을 제공하여 다른 네트워크 관리자가 이 주소를 사용하지 않도록 해야 합니다(그림 5-2 참조).



Sun Fire B1600 블레이드 시스템 섀시

관리
네트워크 연결 - — — — — — —

넷마스크: 255.255.255.0
IP 게이트웨이: 192.168.1.1

그림 5-1 관리 VLAN을 사용하는 네트워크 구성 예제

```
# 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
```

그림 5-2 데이터 네트워크 이름 서버의 `/etc/hosts` 파일 예제

```
#
# 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
```

그림 5-3 데이터 네트워크 이름 서버의 /etc/netmasks 파일 예제

5.4 시스템 컨트롤러 및 스위치 구성

그림 5-1에서 설명된 유형의 구성에서 시스템 컨트롤러와 스위치를 구성하려면 3-7페이지의 단원 3.4, "시스템 컨트롤러 및 스위치 구성"에 나와있는 지침을 수행하십시오. 그러나 시스템 컨트롤러와 스위치에 할당하는 IP 주소는 관리 서브넷에 위치해야 함을 명심하십시오.

5.5 네트워크 복원성을 얻기 위해 IPMP를 사용하여 서버 블레이드 설정하기

이 단원에서는 섀시의 스위치와 각 서버 블레이드간의 이중화된 연결을 활용하기 위해 Solaris IP 네트워크 다중 경로 지정(IPMP) 기능을 사용하는 방법을 설명합니다. 서버 블레이드에 있는 두 개의 1000Mbps 이더넷 인터페이스는 각각 `ce0`과 `ce1`으로 표시되어 있으며, `ce0`은 SSC0의 스위치에, `ce1`은 SSC1의 스위치에 연결되어 있습니다. Sun Fire B1600 블레이드 시스템 섀시가 정상적으로 작동 중일 때는 두 스위치가 모두 작동합니다.

서버 블레이드의 IPMP 드라이브는 두 이더넷 인터페이스에서 기본 게이트웨이에 ping 신호를 주기적으로 보냅니다. 어떠한 이유에서든 둘 중 하나의 ping 작업이 실패할 경우(즉, ping 작업을 수행한 인터페이스의 네트워크 경로를 더 이상 사용할 수 없는 경우), IPMP 드라이버는 사용 가능한 나머지 인터페이스로만 네트워크 트래픽을 보냅니다. 두 인터페이스 모두를 활성 상태로 설정할 수 있으며, 이 경우 각각의 인테페이스에 개별 IP 주소가 필요합니다. 또는, 하나의 인터페이스를 대기 인터페이스로 두어 활성 인터페이스에 장애가 발생했을 경우 그 IP 주소를 넘겨받도록 설정할 수도 있습니다.

활성/활성 구성에는 4개의 IP 주소가 필요합니다. 즉, 각각의 인터페이스에 하나의 IP 주소와 하나의 테스트 주소가 필요합니다. 활성/대기 구성에는 3개의 IP주소가 필요합니다. 어떠한 구성에서든 IPMP 드라이버는 두 개의 전용 테스트 주소를 사용하여 ping 작업을 수행합니다. 특정 인터페이스의 테스트 주소에 대한 ping 신호에 응답이 없을 경우, IPMP 드라이버는 해당 인터페이스에 장애가 발생했음을 감지하고 모든 네트워크 트래픽을 사용 가능한 나머지 인터페이스로 보냅니다. 활성/활성 구성인 경우, IPMP 드라이버는 장애가 발생한 인터페이스의 사용을 중단합니다. 활성/대기 구성일 때 활성 인터페이스를 사용할 수 없게 되면, IPMP 드라이버는 활성 인터페이스의 IP주소를 대기 인터페이스에 할당하여 활성 인터페이스로 전환시킵니다.

정상 작동시 섀시의 두 스위치는 모두 작동 상태이므로, 이 장에서는 활성/활성 구성으로 설정하는 방법을 설명합니다. 활성/대기 구성으로 설정하는 방법은 *IP Network Multipathing Administration Guide*(816-0850)를 참조하십시오.

블레이드의 각 물리적 인터페이스에 필요한 IP 주소는 다음과 같습니다.

- 기본 IP 주소.
- 보조 IP 주소. 이 주소는 활성/활성 구성에서만 필요합니다.

  기본 IP 주소와 보조 IP 주소는 모두 이름 서버에 등록됩니다. 이 주소들은 네트워크상의 다른 장치들이 블레이드와 통신하는 데 사용됩니다.

- 위에서 설명한 ping 작업을 위해 두 개의 다른 IP 주소가 필요합니다. 이 설명서에서는 이 두 주소를 "테스트" 주소로 칭하겠습니다. 이 주소들은 IPMP 드라이버 전용 주소(즉, 이름 서버에 등록되지 않는 주소)입니다.

이 장에서는 두 개의 물리적 인터페이스에 대해 IPMP를 설정하는 방법을 설명합니다. 다음 장에서는 여러 쌍의 가상 IPMP 인터페이스를 설정하는 방법을 설명합니다. 각 인터페이스 쌍은 개별 VLAN에 대한 이중화된 인터페이스 역할을 합니다.

5.5.1 서버 블레이드 구성

이 단원에서는 두 개의 이더넷 인터페이스가 모두 데이터를 송수신할 수 있도록 서버 블레이드의 IPMP를 구성하는 방법을 설명합니다. 설명을 위한 목적으로, 이 단원의 지침에서는 5-4페이지의 단원 5.3, "고정 IP 주소를 사용한 네트워크 환경 준비"에 나온 네트워크 시나리오를 사용한 구성 예제를 설명합니다.

표 5-1에는 그림 5-1에 설명된 시스템 새시에서 슬롯 0에 있는 서버 블레이드의 IPMP 드라이버에 적용할 정보가 요약되어 있습니다.

참고 – 이중화된 네트워크 연결이 필요한 각 서버 블레이드에 대해 이 단원에 설명된 지침을 수행해야 합니다.

표 5-1 서버 블레이드의 IPMP 구성 예제

IPMP 구성 변수	슬롯 0의 예제 서버 블레이드에 대한 값
네트워크 어댑터 인터페이스	`ce0` (활성) `ce1` (활성)
인터페이스 그룹 이름	`medusa_grp0`
IP 주소 및 호스트 이름(기본)	192.168.1.150 (`medusa-s0`)
보조 IP 주소 및 호스트 이름(보조)	192.168.1.166 (`medusa-s0-sec`)
테스트 IP 주소 및 호스트 이름(`ce0`)	192.168.1.100 (medusa-s0-0)
테스트 IP 주소 및 호스트 이름(`ce1`)	192.168.10.116 (medusa-s0-1)
Netmask	255.255.255.0
서버 블레이드가 네트워크 라우팅을 수행합니까?	아니요

1. **3장에 나와있는 방법에 따라 Solaris 예비 설치를 수행합니다.**

   설치를 마치고 나면 #.을 입력하여 서버 블레이드 콘솔에서 sc> 프롬프트로 돌아갑니다.

2. **인터페이스를 구성할 서버 블레이드의 콘솔에 루트로 로그인합니다.**

   sc> 프롬프트에서 다음을 입력합니다.

```
sc> console sn
```

   여기서 *n*은 로그인하려는 서버 블레이드가 들어있는 슬롯의 번호입니다.

3. **서버 블레이드의 /etc/hosts 파일을 편집하여 블레이드의 두 IP 테스트 주소를 추가합니다.**

   표 5-1의 예제 주소를 사용하는 블레이드의 경우, 다음 파일의 마지막 2행을 추가해야 합니다.

```
#
# /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. **서버 블레이드의 /etc/netmasks 파일에서 넷마스크를 설정합니다.**

   표 5-1의 예제 주소를 사용하는 블레이드의 경우, 다음 행을 추가해야 합니다.

```
192.168.1.0     255.255.255.0
```

5. **서버 블레이드가 라우팅에 사용되지 않으므로 라우팅 기능을 해제합니다.**

   다음을 입력합니다.

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

6. **다음을 입력하여 네트워크 인터페이스를 생성합니다.**

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

7. **네트워크 인터페이스** ce0**과** ce1**을 포함하는 IPMP 그룹** medusa_grp0**을 생성합니다.**

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

이러한 명령을 실행하면 다음과 같은 syslog 메시지가 표시될 수 있습니다.

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

이 메시지는 단지 인터페이스의 테스트 주소를 설정하기 전에는 장애를 감지할 수 없음을 경고하는 내용입니다.

8. **데이터 전송을 위해** ce0 **및** ce1**에 주소를 할당하고, 인터페이스 장애가 감지됐을 경우 이 주소를 장애 복구용으로 사용하도록** failover**로 설정합니다.**

```
# 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. 각 네트워크 인터페이스의 테스트 주소를 설정합니다.

이 주소는 mpathd가 인터페이스 장애를 감지하는 데 사용됩니다. 테스트 주소를 설정할 때는 -failover 플래그를 사용해야 합니다. 그러면 in.mpathd가 이 주소를 테스트 주소(즉, 다른 인터페이스에 할당되지 않으므로 장애 복구가 되지않는 주소)로 사용하게 됩니다.

```
# 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. 새로운 인터페이스 구성이 재시동 이후에도 유지되게 하려면 /etc 디렉토리에 hostname.ce0 및 hostname.ce1 파일을 만듭니다.

hostname.ce0 파일의 예제가 다음에 나와 있습니다.

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

hostname.ce1 파일의 예제가 다음에 나와 있습니다.

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

11. 두 네트워크 어댑터의 구성을 점검합니다.

다음을 입력합니다.

```
# 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 192.168.10.100 netmask ffffff00 broadcast 192.168.1.255
ce1: flags=9040843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
        inet 192.168.10.166 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 192.168.10.116 netmask ffffff00 broadcast 192.168.1.255
```

위에 표시된 출력은 4개의 주소(표 5-1에서 사용된 예제 주소)가 정의되었음을 보여줍니다. `ce0:1` 및 `ce1:1`과 연관된 두 IPMP 테스트 주소는 NOFAILOVER로 표시되어 있습니다. 즉, 이들 주소는 장애 발생 시 온전한 다른 인터페이스에 할당되지 않습니다.

12. 섀시에서 한 개의 SSC를 임시로 제거하여 IPMP를 테스트해 봅니다.

그러면 다음과 같은 오류 메시지가 콘솔에 표시됩니다.

```
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
```

참고 – IPMP 데몬이 네트워크 장애를 감지하고 기본 구성으로 복구하는 데는 약 10초가 소요됩니다. IPMP 데몬의 구성은 `/etc/default/mpathd` 파일에 정의되어 있습니다.

6장

블레이드 관리 추가 및 VLAN 태그 지정

이 장에서는 관리 네트워크에서 안전하게 서버 블레이드를 관리할 수 있도록 시스템 섀시를 구성하는 방법을 설명합니다.

이 장은 다음 단원으로 구성되어 있습니다.

6.1 소개

이 장에서는 관리 네트워크의 보안을 약화시키지 않고 네트워크 관리자가 관리 네트워크에서 (즉, 서버 블레이드에 직접 텔넷 연결하여) 서버 블레이드 관리 작업을 수행할 수 있도록 5장의 구성을 개선하는 방법을 설명합니다.

그림 6-1에는 새시 내 스위치의 서버 블레이드 포트와 관리 포트(NETMGT)를 잇는 점선이 표시되어 있습니다. 또한 서버 블레이드 자체와 각 스위치의 관리 포트를 잇는 점선도 있습니다. 이 점선들은 관리 VLAN(VLAN 2)에 속하는 구성 부품 또는 장치간의 연결을 나타냅니다. 기본적으로 스위치의 관리 포트(NETMGT)를 포함하는 VLAN 2는 서버 블레이드 포트를 갖고 있지 않습니다. 따라서 그림 6-1에서와 같은 네트워크 환경을 지원하도록 새시를 구성하려면 이러한 포트들을 수동으로 재구성해야 합니다. 이 작업을 수행하는 방법은 6-5페이지의 단원 6.3, "시스템 컨트롤러 및 스위치 구성"을 참조하십시오.

또한 기본적으로 서버 블레이드 포트에서 스위치의 패킷 필터를 거쳐 관리 포트로 가는 네트워크 트래픽은 허용되지 않습니다. 이것은 보안 기능이므로 특정 트래픽이 패킷 필터를 통과할 수 있게 스위치를 구성할 때는 신중을 기해야 합니다. A-15페이지의 단원 A.11, "스위치의 패킷 필터를 사용한 블레이드의 보안 관리"에서는 원하는 프로토콜만이 패킷 필터를 통과할 수 있게 설정하는 방법을 설명합니다.

마지막으로, 이 장에서는 관리 네트워크(VLAN 2)에 서버 블레이드를 포함시키는 방법을 설명합니다. 따라서 각 블레이드가 데이터 네트워크는 물론 관리 네트워크(VLAN 2)에 대해서도 이중화된 연결을 갖도록(5장 참조) 서버 블레이드의 IPMP 설정를 수정하는 방법도 설명합니다.

6.2 네트워크 환경 준비

이 단원의 구성 예제에는 이전 장에서 보여준 구성 예제에 위 지침에서 언급한 개선안을 추가하였고, 각 블레이드와 관리 네트워크간의 이중화 연결을 구축하는 데 필요한 IPMP 정보 예제도 포함하였습니다. 이 단원에는 또한 관리 네트워크에 속한 이름 서버의 예제 `/etc/hosts` 파일도 나와 있습니다. 데이터 네트워크의 관리 파일은 5장과 동일합니다. 그러나 관리 네트워크 이름 서버의 `/etc/hosts` 파일에는 새시의 두 SSC와 스위치는 물론 각 서버 블레이드에 대한 관리 서브넷 IP 주소가 포함되어야 합니다(그림 6-2 참조).

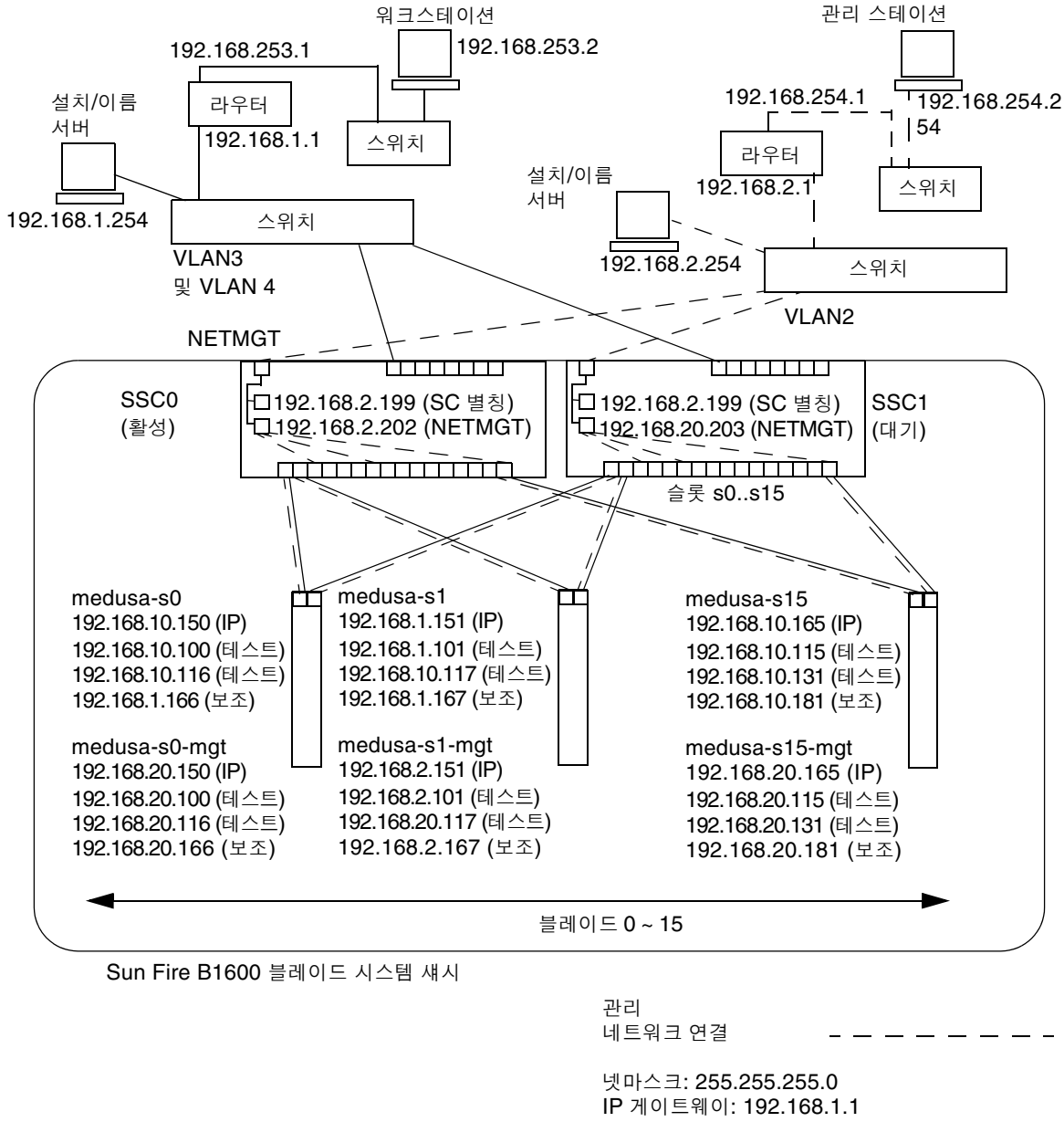


그림 6-1 서버 블레이드를 포함하는 관리 VLAN을 가진 네트워크 구성 예제

```
# 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
 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
```

그림 6-2 관리 네트워크 이름 서버의 `/etc/hosts` 파일 예제

6.3 시스템 컨트롤러 및 스위치 구성

이전 장의 지침에 따라 시스템 새시의 시스템 컨트롤러 및 스위치를 이미 설정한 경우 바로 6-5 페이지의 단원 6.3.1, "SSC0과 SSC1 스위치의 관리 VLAN에 서버 블레이드 추가하기"로 이동하십시오.

그렇지 않으면, 5장에 나와있는 지침을 수행하되 SSC1의 스위치는 구성하지 마십시오. 아래 지침(6-5페이지의 단원 6.3.1, "SSC0과 SSC1 스위치의 관리 VLAN에 서버 블레이드 추가하기")에 SSC0의 스위치의 전체 구성을 SSC1의 스위치로 복사하는 작업이 포함되어 있습니다.

6.3.1 SSC0과 SSC1 스위치의 관리 VLAN에 서버 블레이드 추가하기

이 단원에서는 관리 VLAN에 서버 블레이드를 추가하는 방법을 설명합니다. 관리 VLAN은 기본적으로 VLAN 2가 됩니다. 즉, VLAN2에 관리 포트 NETMGT가 포함됩니다. VLAN 1도 스위치에 기본적으로 설정됩니다. 이 VLAN에는 스위치의 모든 서버 블레이드 포트와 업링크 포트가 포함됩니다. 그러나 스위치의 VLAN 구성을 사용하는 방법을 설명하기 위해 이 단원에서는 데이터 네트워크로 VLAN 1대신 VLAN 3을 사용합니다.

이 단원의 지침에서 관리 VLAN(VLAN 2)과 데이터 VLAN(VLAN 3)은 태그를 갖습니다. 하지만 이 지침에는 블레이드 시동을 위한 추가 VLAN(VLAN 4)을 생성하는 방법도 나와 있습니다. 이 추가 VLAN은 Solaris 운영 환경 네트워크 설치 프로세스 동안 블레이드에 의해 생성되는 태그가 없는 트래픽을 처리합니다.

시동 VLAN(VLAN 4)의 트래픽은 시스템 새시를 떠날 때 태그를 지정하거나 지정하지 않을 수 있습니다. 이 단원의 예제 명령에서는 태그가 지정됩니다. (이 지침은 새시 외부의 장치가 VLAN을 인식한다고 전제하며, VLAN 4에는 서버 블레이드가 사용하는 네트워크 설치 서버가 포함되어 있다고 전제합니다.)

참고 – 본 단원에 나온 지침을 수행하는 중에 스위치를 재설정하려는 경우, 먼저 구성을 저장해야 합니다. 그렇지 않으면 변경 사항을 모두 잃게 됩니다. 구성을 저장하려면 A-9페이지의 단원 A.8, "스위치 설정 저장"에 나와있는 지침을 참조하십시오.

---

1. **SSC0의 스위치를 구성하기 위해 `sc>` 프롬프트에서 콘솔로 로그인합니다.**

   다음을 입력하여 SSC0의 스위치에 로그인합니다.

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

2. **사용자 이름과 암호를 묻는 프롬프트가 표시되면 이름과 암호를 입력합니다.**

3. **스위치 명령행 인터페이스의 `Console#` 프롬프트에서 다음을 입력합니다.**

```
Console#configure
```

4. **다음을 입력하여 스위치의 VLAN 데이터베이스로 들어갑니다.**

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

5. **다음을 입력하여 데이터 네트워크와 시동 네트워크에 대하여 VLAN을 설정합니다.**

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

6. **다음을 입력하여 VLAN 데이터베이스를 종료합니다.**

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

7. **관리 VLAN(VLAN 2), 데이터 VLAN(VLAN 3), 그리고 시동에 사용할 VLAN(VLAN 4)에 서버 블레이드 포트 `SNP0`을 추가합니다.**

   다음 명령을 입력합니다.

```
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)#
```

   위 과정의 의미는 다음과 같습니다.

- `interface ethernet SNP0` 명령은 구성하려는 블레이드 포트를 지정합니다. 이 예제에서, 인터페이스는 블레이드 포트 `SNP0`입니다.
- `switchport allowed vlan add 2 tagged` 명령은 이 블레이드 포트를 VLAN 2(관리 네트워크)에 추가하고, 태그 지정된 트래픽을 관리 네트워크에 전달할 수 있도록 허가합니다.
- `switchport allowed vlan add 3 tagged` 명령은 포트를 VLAN 3(새 데이터 네트워크)에 추가하고, 태그 지정된 트래픽을 데이터 네트워크에 전달할 수 있도록 허가합니다.
- `switchport allowed vlan add 4` 명령은 포트를 VLAN 4에 추가합니다. 이 명령은 또한 태그가 지정되지 않은 패킷을 받아서 VLAN 4로 태그를 지정하도록 포트를 설정합니다. 이렇게 함으로써, 시동 중에 블레이드가 생성한 태그가 없는 트래픽이 네트워크 설치 서버에 도달할 수 있는 경로가 마련됩니다. 다음 명령에서는 이 VLAN을 원시 VLAN, 다시 말해서 태그가 없는 모든 프레임이 전달되는 VLAN으로 설정하게 됩니다.
- `switchport native vlan 4` 명령은 포트가 수신하는 태그가 없는 모든 프레임이 VLAN 4로 전송되도록 설정합니다. (OBP 및 점프스타트에서는 서버 블레이드가 태그가 없는 프레임을 전송합니다.)
- `switchport allowed vlan remove 1` 명령은 VLAN 1(모든 서버 블레이드 포트 및 업링크 포트에 대한 스위치의 기본 VLAN)에서 포트를 제거합니다.

나머지 모든 서버 블레이드 포트(`SNP1 ~ SNP15`)에 대하여 단계 7을 반복합니다. 이 모든 포트는 관리 네트워크와 데이터 네트워크 양쪽에 모두 포함되어야 합니다.

구성한 포트를 점검하기 위해 다음을 입력합니다.

```
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. 트렁크로 결합할 데이터 업링크 포트가 있다면 지금 결합합니다.

A-14페이지의 단원 A.10, "복원성 및 성능 향상을 위한 트렁크 연결 설정"에 나와있는 지침을 수행합니다.

9. 다음 명령을 입력하여 트렁크화되지 않은 모든 데이터 업링크 포트를 데이터 VLAN(VLAN 3)과 시동 VLAN(VLAN 4)에 추가합니다.

```
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` 명령은 구성하려는 업링크 포트를 지정합니다.
- `switchport allowed vlan add 3 tagged` 명령은 이 업링크 포트를 데이터 네트워크(VLAN 3)에 추가합니다.
- `switchport allowed vlan add 4` 명령은 이 업링크 포트를 블레이드 시동에 사용되는 태그가 없는 VLAN(VLAN 4)에 추가합니다. 다음 명령에서는 이 VLAN을 원시 VLAN, 즉 태그가 없는 모든 프레임이 전달되는 VLAN으로 설정하게 됩니다.
- `switchport native vlan 4` 명령은 외부 데이터 포트가 수신하는 태그가 없는 모든 프레임을 VLAN 4로 전송하도록 설정합니다. 이 명령의 효과는 일시적입니다. 이후 명령에서 다시 포트가 태그가 없는 프레임을 수신하지 못하게 설정하게 됩니다. 이 명령을 입력해야 하는 이유는 `switchport mode trunk` 명령이 실행될 때까지 스위치에 원시 VLAN이 필요하기 때문입니다.
- `switchport allowed vlan remove 1` 명령은 이 업링크 포트를 VLAN 1(기본 VLAN)에서 제거합니다. 이 VLAN은 이 단계(즉, 태그가 없는 원시 VLAN인 VLAN 4가 생성된 후)에서만 제거할 수 있습니다.
- `switchport ingress-filtering` 명령, `switchport mode trunk` 명령, 그리고 `switchport acceptable-frame-types tagged` 명령은 포트가 자신이 속한 VLAN에 대한 태그를 갖지 않는 모든 프레임을 거부하도록 설정합니다.
- `no switchport gvrp` 명령은 포트가 자신이 속한 VLAN(이 경우, VLAN 3)을 다른 스위치에 알리기 위해 GVRP를 사용하는 것을 금지합니다.
- `switchport forbidden vlan add 2` 명령은 네트워크에 있는 다른 스위치의 GVRP 요청으로 인해 업링크 포트가 vlan 2에 추가되는 것을 금지합니다.

구성한 포트를 점검하기 위해 다음을 입력합니다.

```
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. 아래 명령을 입력하여 모든 트렁크를 데이터 VLAN(VLAN 3)에 추가합니다.

트렁크 연결을 사용하는 자세한 방법은 부록 A을 참조하십시오.

아래 예제에 나온 트렁크의 이름은 port-channel 11입니다. interface port-channel 11 명령은 구성할 트렁크를 지정합니다.

```
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. 모든 업링크 포트를 VLAN 3에 개별적으로 또는 트렁크로 추가합니다(단계 9 및 단계 10 참조).

예를 들어, 포트 NETP1, NETP2 및 NETP3이 트렁크 1로 결합되고 NETP4와 NETP5가 트렁크 2로 결합된 경우, 포트 NETP0, NETP6, NETP7과 트렁크 1, 트렁크 2를 VLAN 3에 추가해야 합니다.

12. **A-15페이지의 단원 A.11, "스위치의 패킷 필터를 사용한 블레이드의 보안 관리"에 나와있는 지침을 수행합니다.**

13. **SSC0의 스위치 구성에 대해 수행한 변경 사항을 저장합니다.**

    이렇게 하는 방법은 A-9페이지의 단원 A.8, "스위치 설정 저장"에 나와있는 지침을 참조하십시오.

14. **SSC0의 스위치 구성을 SSC1의 스위치에 복사합니다.**

    A-9페이지의 단원 A.9, "첫번째 스위치의 구성을 두번째 스위치에 복사하기"에 나와있는 지침을 수행합니다.

15. **#.을 입력하여 스위치의 명령행 인터페이스를 종료하고 시스템 컨트롤러로 돌아옵니다.**

16. **sc> 프롬프트에서 다음을 입력하여 SSC1의 스위치에 로그인합니다.**

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

17. **사용자 이름과 암호를 입력합니다.**

18. **SSC1의 스위치에 대해 IP 주소, 넷마스크, 기본 게이트웨이를 설정합니다.**

    이렇게 하는 방법은 A-6페이지의 단원 A.6, "스위치의 IP 주소, 넷마스크 및 기본 게이트웨이 설정"에 나와있는 지침을 참조하십시오.

19. **SSC1의 스위치 구성에 대해 수행한 변경 사항을 저장합니다.**

    이렇게 하는 방법은 A-9페이지의 단원 A.8, "스위치 설정 저장"에 나와있는 지침을 참조하십시오.

20. **#.을 입력하여 스위치 명령행 인터페이스를 종료하고 sc> 프롬프트로 돌아옵니다.**

21. **6-10페이지의 단원 6.4, "네트워크 복원성을 얻기 위해 IPMP를 사용하여 서버 블레이드 설정하기(VLAN 태그 지정)"에 나와있는 지침을 수행합니다.**

6.4 네트워크 복원성을 얻기 위해 IPMP를 사용하여 서버 블레이드 설정하기(VLAN 태그 지정)

이전 단원에서 수행한 스위치 구성에서는 데이터 네트워크와 관리 네트워크를 분리하기 위해 태그가 있는 VLAN을 사용합니다. 이 스위치 구성에서 IPMP를 사용하려면 서버 블레이드가 속한 *각각의* VLAN에 대해 4개의 IP 주소가 필요합니다. 다시 말해서, 관리 VLAN에 대해 4개, 데이터 VLAN에 대해 4개를 합하여 전부 8개의 IP 주소가 필요합니다.

이것은 IPMP 드라이버가 각 VLAN에 대해 별도의 논리적 이더넷 인터페이스 쌍을 사용하여 태그가 있는 VLAN을 지원하기 때문입니다. 이러한 논리적 인터페이스는 다음의 간단한 공식에 따라 직접 이름을 지정해야 합니다.

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

여기서 *VLAN id*는 VLAN의 번호(새시의 서버 블레이드가 연결된 스위치 포트에 대해 구성된 바에 따라)이며, *instance*는 논리적 인터페이스가 물리적 인터페이스 ce0과 ce1 중 어느 것과 연관되어 있는가에 따라 0 또는 1로 지정합니다.

이러한 논리적 이더넷 인터페이스 쌍을 생성하여 얻어지는 효과는 하나의 네트워크에 대한 프레임이 해당 네트워크에는 전달되지만 다른 네트워크에는 전달되지 않는다는 점입니다. IPMP 드라이버는 스위치에 전송할 프레임이 있을 때마다 해당 프레임을 수신할 VLAN으로 프레임의 태그를 지정한 다음, 수신할 VLAN의 두 논리적 인터페이스 중 하나를 사용하여 이 프레임을 전송합니다. 그러면 해당 프레임을 전송한 서버 블레이드에 할당된 전용 포트를 통해 스위치 중 하나가 이 프레임을 수신합니다. 그리고, 이 VLAN 태그를 갖는 프레임을 수신하도록 스위치가 구성된 경우, 스위치는 프레임을 해당 VLAN에 전달합니다.

중요한 사실은 서버 블레이드의 IPMP 드라이버가 특정 VLAN으로 프레임을 전송했으며, 이 과정에서 해당 VLAN에 대한 이중화된 가상 연결을 사용했다는 점입니다. 이때, 서버 블레이드가 속한 다른 어느 VLAN도 해당 프레임을 수신하지 못합니다.

6.4.1 서버 블레이드 구성(VLAN 태그 지정)

이 단원에서는 두 이더넷 인터페이스가 각각 두 개의 논리적 인터페이스(하나는 데이터 VLAN용, 하나는 관리 VLAN용)를 제공하도록 서버 블레이드에서 IPMP를 구성하는 방법을 설명합니다.

설명을 위한 목적으로, 이 단원의 지침에서는 6-2페이지의 단원 6.2, "네트워크 환경 준비"에 나온 네트워크 시나리오를 사용한 구성 예제를 설명합니다. 이 지침에서는 5장에 나와있는 IPMP를 사용한 서버 블레이드 구성 작업은 이미 수행했다고 전제합니다.

표 6-1에는 그림 6-1에 설명된 시스템 섀시에서 슬롯 0에 있는 서버 블레이드의 IPMP 드라이버에 적용할 정보가 요약되어 있습니다.

참고 – 데이터 네트워크와 관리 네트워크에 대한 이중화된 연결이 필요한 각 서버 블레이드에 대해 이 단원의 지침을 수행해야 합니다.

표 6-1 서버 블레이드에 대한 IPMP 구성 예제(VLAN 태그 지정)

IPMP 구성 변수	슬롯 0 예제 서버 블레이드의 값
인터페이스 그룹 이름	`medusa_grp0-mgt` `medusa_grp0`
IP 주소 및 호스트 이름(`ce2000/1`) IP 주소 및 호스트 이름(`ce3000/1`)	192.168.2.150 (medusa-s0-mgt) 192.168.1.150 (medusa-s0)
네트워크 어댑터 인터페이스	ce2000 (활성) ce2001 (활성) ce3000 (활성) ce3001 (활성)
IP 주소 및 호스트 이름(관리 네트워크) IP 주소 및 호스트 이름(데이터 네트워크)	192.168.2.150 (medusa-s0-mgt) 192.168.1.150 (medusa-s0)
보조 IP 주소 및 호스트 이름(관리 네트워크) 보조 IP 주소 및 호스트 이름(데이터 네트워크)	192.168.2.166 (medusa-s0-mgt-sec) 192.168.1.166 (medusa-s0-sec)
테스트 IP 주소 및 호스트 이름(`ce2000`) 테스트 IP 주소 및 호스트 이름(`ce2001`)	192.168.2.100 medusa-s0-0 192.168.2.116 medusa-s0-1
테스트 IP 주소 및 호스트 이름(`ce3000`) 테스트 IP 주소 및 호스트 이름(`ce3001`)	192.168.1.100 medusa-s0-0 192.168.1.116 medusa-s0-1
Netmask	255.255.255.0
서버 블레이드가 네트워크 라우팅을 수행합니까?	아니오

1. **3장에 나와있는 방법에 따라 Solaris 예비 설치를 수행합니다.**

   설치를 마치고 나면, #.을 입력하여 서버 블레이드 콘솔에서 `sc>` 프롬프트로 돌아갑니다.

2. **인터페이스를 구성할 서버 블레이드의 콘솔에 로그인합니다.**

   `sc>` 프롬프트에서 다음을 입력합니다.

```
sc> console sn
```

   여기서 *n*은 로그인하려는 서버 블레이드가 들어있는 슬롯의 번호입니다.

3. **서버 블레이드의** `/etc/hosts` **파일을 편집하여 관리 인터페이스의 IP 주소를 추가합니다.**

   표 6-1의 예제 주소를 사용하는 블레이드의 경우, 다음 파일의 마지막 2행을 추가해야 합니다.

```
#
# /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. **서버 블레이드의** `/etc/netmasks` **파일에서 넷마스크를 설정합니다.**

   표 6-1의 예제 주소를 사용하는 블레이드의 경우, 다음 행을 추가해야 합니다.

```
192.168.1.0     255.255.255.0
192.168.2.0     255.255.255.0
```

5. **서버 블레이드가 라우팅에 사용되지 않으므로 라우팅 기능을 해제합니다.**

   다음을 입력합니다.

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

6. **다음을 입력하여 기존 네트워크 인터페이스를 삭제합니다.**

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

이들 인터페이스 중 이전에 구성하지 않은 인터페이스가 있으면 다음 오류 메시지가 표시됩니다.

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

7. **다음을 입력하여 새 인터페이스를 생성합니다.**

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

8. **새 인터페이스를 포함하는 IPMP 장애 복구 그룹을 생성합니다.**

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

이 명령들을 실행하면 다음 유형의 `syslog` 메시지가 표시될 수 있습니다.

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

이 메시지는 단지 인터페이스의 테스트 주소를 설정하기 전에는 장애를 감지할 수 없음을 경고하는 내용입니다.

9. **데이터 전송을 위해 각각의 새 인터페이스에 주소를 할당하고 인터페이스 장애가 감지됐을 경우 이 주소를 장애 복구용으로 사용하도록** `failover`**로 설정합니다.**

```
# 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. **각 네트워크 인터페이스의 테스트 주소를 설정합니다.**

이 주소는 `mpathd`가 인터페이스 장애를 감지하는 데 사용됩니다. 호스트 응용 프로그램이 데이터 통신용으로 이 주소를 사용하지 못하도록 명령행에 `deprecated`라는 단어를 포함시킵니다(아래 참조).

또한 `-failover` 플래그도 사용해야 합니다. 그러면 `in.mpathd`가 이 주소를 테스트 주소(즉, 다른 인터페이스에 할당되지 않으므로 장애 복구가 되지않는 주소)로 사용하게 됩니다.

```
# 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. **새 인터페이스 구성이 재시동 이후에도 유지되게 하려면** `/etc` **디렉토리에** `hostname.ce2000`, `hostname.ce2001`, `hostname.ce3000` **및** `hostname.ce3001` **파일을 만듭니다.**

`hostname.ce2000` 파일의 예제가 다음에 나와 있습니다.

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

`hostname.ce2001` 파일의 예제가 다음에 나와 있습니다.

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

`hostname.ce3000` 파일의 예제가 다음에 나와 있습니다.

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

`hostname.ce3001` 파일의 예제가 다음에 나와 있습니다.

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

12. 다음을 입력하여 두 네트워크 어댑터의 구성을 점검합니다.

```
# 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 192.168.20.100 netmask ffffff00 broadcast 192.168.2.255
ce2001: flags=9040843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
mtu 1500 index 4
        inet 192.168.20.166 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 192.168.20.116 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 192.168.10.100 netmask ffffff00 broadcast 192.168.1.255
ce3001: flags=9040843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
mtu 1500 index 6
        inet 192.168.10.166 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 192.168.10.116 netmask ffffff00 broadcast 192.168.1.255
```

위에 표시된 출력은 8개의 주소(표 6-1에서 사용된 예제 주소)가 정의되었음을 보여줍니다. 4개의 IPMP 테스트 주소는 NOFAILOVER로 표시되어 있습니다. 즉, 이들 주소는 장애 발생 시 온전한 다른 인터페이스에 할당되지 않습니다.

13. 섀시에서 한 개의 SSC를 임시로 제거하여 IPMP를 테스트해 봅니다.

그러면 다음과 같은 오류 메시지가 콘솔에 표시됩니다.

```
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
```

참고 – IPMP 데몬이 네트워크 장애를 감지하고 기본 구성으로 복구하는 데는 약 10초가 소요됩니다. IPMP 데몬의 구성은 `/etc/default/mpathd` 파일에 정의되어 있습니다.

7장

다수의 고객을 위한 스위치 구성 예제

이 장은 다음 단원으로 구성되어 있습니다.

참고 – 본 단원의 지침을 수행하는 중에 스위치를 재설정해야 할 경우에는 먼저 구성을 저장해야 합니다. 그렇지 않으면 변경 사항을 모두 잃게 됩니다. 구성을 저장하려면 A-9페이지의 단원 A.8, "스위치 설정 저장"에 나와있는 지침을 참조하십시오.

7.1 소개

이 장은 다음 작업을 수행해야 하는 인터넷 서비스 제공업체(ISP)를 대상으로 작성되었습니다.

- 다수의 고객에게 서버 블레이드 할당하기
- 고객이 자신의 블레이드를 관리할 수 있도록 허용하기
- 한 고객이 다른 고객 네트워크의 데이터를 수신하지 못하도록 방지하기
- 한 고객이 다른 고객 블레이드의 콘솔에 액세스하지 못하도록 방지하기
- 고객이 두 내장 스위치의 콘솔에 액세스하지 못하도록 방지하기

이 장에서는 서버 블레이드를 다수의 고객에게 할당하기 위해 VLAN을 사용하는 두 개의 스위치 구성 예제를 보여줍니다. 이 장의 나머지 부분에서 ISP의 고객은 서버 블레이드 고객을 말하는 것으로 가정합니다.

이 스위치 구성들에서는 하나의 ISP만이 시스템 컨트롤러 및 스위치 명령행 인터페이스에 대한 로그인 및 암호 액세스 권한을 갖는다고 전제합니다. ISP의 고객은 NETMGT 포트를 포함하는 자체 관리 네트워크를 갖기 때문에 스위치의 NETMGT 포트에 `ping` 작업을 수행할 수 있습니다. 그러나 고객에게 스위치에 대한 로그인 및 암호 액세스 권한을 부여하지 않는 한 고객은 스위치에 액세스할 수 없습니다. 또한 고객이 텔넷을 통해 SCO의 네트워크 포트에 액세스할 수 없도록 VLAN 구성이 사용됩니다.

이 장은 주로 ISP를 주요 독자로 하지만, Sun Fire B1600 블레이드 시스템 섀시에서 VLAN을 사용하여 네트워크 트래픽을 제어하는 방법에 대하여 일반적인 관심을 갖고있는 네트워크 관리자에게도 유용할 수 있습니다.

이 장은 블레이드에서 IPMP를 구성하는 지침은 제공하지 않습니다. 복잡한 VLAN 설정에서 IPMP 인터페이스를 구성하는 방법은 부록 6을 참조하십시오.

참고 – 이 장의 지침은 VLAN의 사용과 관련되어 있습니다. 이들 지침은 상위 네트워크에서 태그가 있는 VLAN을 사용한다고 전제합니다. 즉, 이 장의 구성에서는 네트워크 전반에 걸쳐 Solaris를 설치하는 것을 지원하지 않습니다. 이 경우, 스위치의 VLAN이 태그가 없는 트래픽을 처리해야 하기 때문입니다. 이 장의 지침은 스위치에서 VLAN을 사용하는 방법을 예시하기 위해서만 제공되었습니다.

네트워크로 발송하는 프레임에서 VLAN 태그를 제거하고 네트워크에서 수신되는 프레임에 VLAN 태그를 추가하도록 스위치를 구성하는 방법은 7-10페이지의 단원 7.2.4, "각 고객에게 데이터 네트워크 포트 할당하기" 및 7-16페이지의 단원 7.3.4, "고객 간의 데이터 네트워크 포트 공유"를 참조하십시오.

7.2 시나리오 A: 자체 블레이드와 데이터 포트를 갖는 3명의 고객

이 시나리오에서는 인터넷 서비스 제공업체(ISP)가 블레이드 시스템 새시를 소유하고 있으며 그것을 관리하는 전반적인 책임을 지고 있다고 전제합니다. 따라서 ISP만이 NETMGT를 통해 스위치의 명령행 인터페이스에 액세스할 수 있는 권한을 갖습니다.

이 시나리오는 또한 고객 1, 고객 2, 고객 3이라는 세 명의 고객을 가정합니다. 각 고객은 자신에게 독점적으로 할당된 하나의 데이터 VLAN을 보유합니다. 이 데이터 VLAN에는 다수의 서버 블레이드(다시 말하면, 스위치에 있는 다수의 서버 블레이드용 다운링크 포트)와 다수의 외부 데이터 포트가 포함됩니다.

고객은 또한 하나의 관리 VLAN을 갖고있어 이를 통해 자신의 블레이드에 안전하게 액세스할 수 있습니다.

스위치 구성은 표 7-1에 요약되어 있습니다.

표 7-1 시나리오 A: 자체 서버 블레이드와 데이터 포트를 갖는 3명의 고객

네트워크 관리자	관리 포트	서버 블레이드 포트	업링크 포트	데이터 VLAN ID	관리 VLAN ID
인터넷 서비스 제공업체	NETMGT	없음	없음	없음	2
고객 1	NETMGT	SNP0, SNP1, SNP2	NETP0, NETP1	11	21
고객 2	NETMGT	SNP3, SNP4, SNP5, SNP6, SNP7, SNP8, SNP9	NETP2, NETP3, NETP4	12	22
고객 3	NETMGT	SNP10, SNP11, SNP12, SNP13, SNP14, SNP15	NETP5, NETP6, NETP7	13	23

본 단원의 나머지 부분에서는 표 7-1에 나와있는 구성을 구축하는 방법을 설명합니다. 이 부분은 다음의 하위 단원으로 구성되어 있습니다.

- 7-6페이지의 단원 7.2.1, "모든 VLAN의 생성 및 이름 지정"
- 7-7페이지의 단원 7.2.2, "각 고객에게 관리 포트(NETMGT) 할당하기"

- 7-8페이지의 단원 7.2.3, "각 고객에게 서버 블레이드 포트 할당하기"
- 7-10페이지의 단원 7.2.4, "각 고객에게 데이터 네트워크 포트 할당하기"

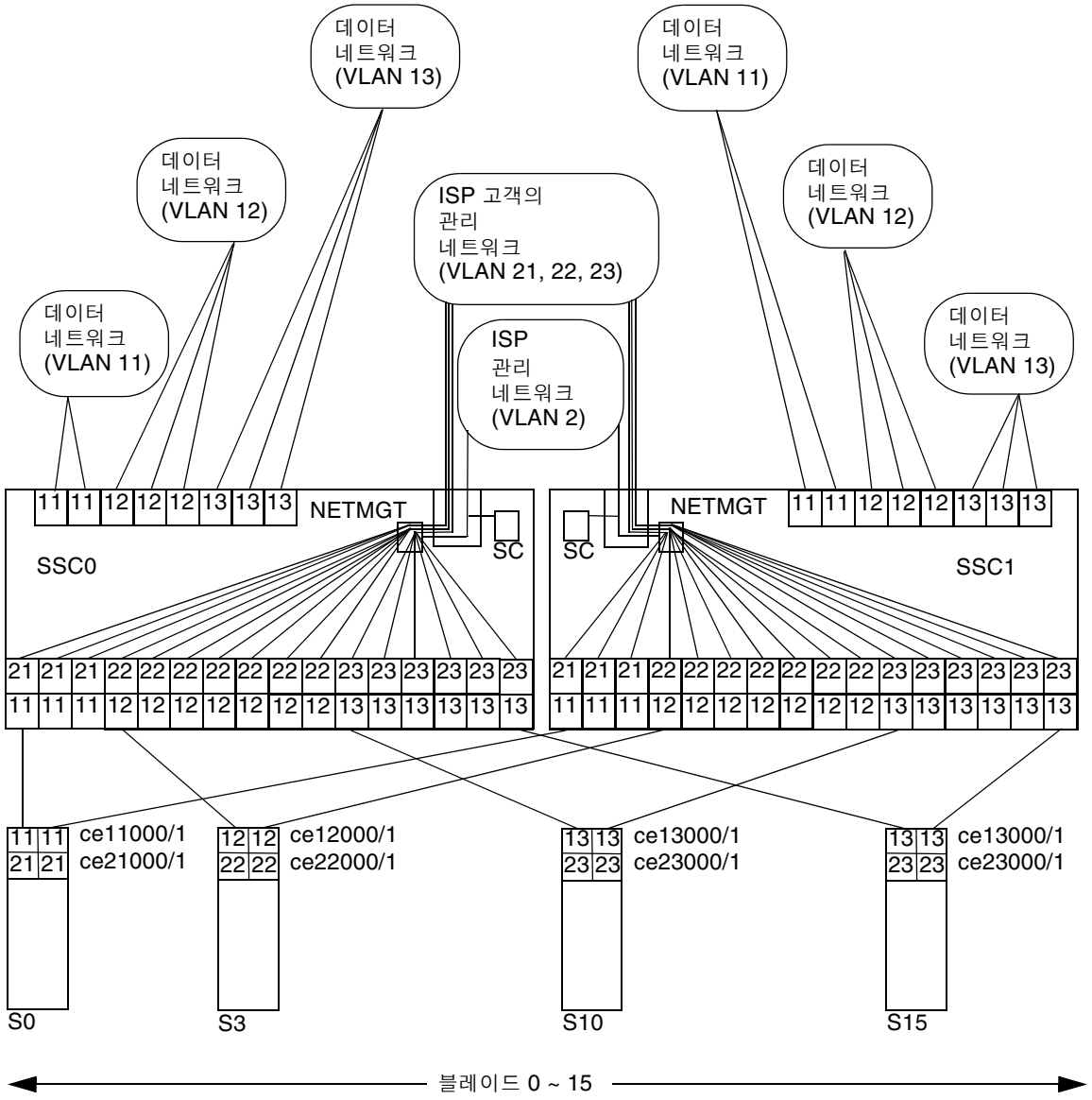


그림 7-1 시나리오 A: 고객의 데이터 LAN 및 관리 VLAN과 ISP의 관리 VLAN

그림 7-1은 표 7-1과 동일한 내용을 보여주는 그림입니다. 중앙에 있는 것은 ISP의 관리 VLAN인 VLAN 2입니다. 이 VLAN은 ISP의 네트워크 관리자가 독점적으로 관리합니다. 이 VLAN에는 스위치의 NETMGT 포트가 포함되어 있으며, 이 포트를 통해 ISP 네트워크 관리자는 텔넷 또는 웹 연결을 사용하여 전체 스위치를 구성할 수 있습니다. 또한 ISP는 이 VLAN에 포함된 시스템 컨트롤러를 사용하여 전체 새시를 구성하고, `sc>` 프롬프트에서 개별 서버 블레이드와 두 스위치의 콘솔에 연결할 수 있습니다. 그러나, 시스템 컨트롤러는 `sc>` 프롬프트에서 `setupsc` 명령을 실행하여 VLAN에 포함시키며, 이 작업은 스위치 구성 절차의 일부가 아님을 유의하십시오.

참고 – 이 시나리오에서, ISP 네트워크 관리자는 시스템 컨트롤러 또는 스위치의 명령행 인터페이스에 대한 암호 액세스 권한을 고객에게 부여하지 않는다고 전제합니다. 시스템 컨트롤러와 스위치 인터페이스에 대한 액세스를 통제하는 것은 네트워크 관리자의 책임입니다.

그림에서 VLAN 2 위에는 ISP의 개별 고객을 위한 3개의 관리 VLAN이 있습니다. 이들 고객 각각은 자체 서버 블레이드에 대한 전용 관리 VLAN에 액세스할 수 있습니다. 따라서 예를 들어, 고객 1(21번 관리 VLAN)은 슬롯 0, 1, 2의 서버 블레이드에, 고객 2(22번 관리 VLAN)는 슬롯 3 ~ 9의 서버 블레이드에, 그리고 고객 3(23번 관리 VLAN)은 슬롯 10 ~ 15의 서버 블레이드에 텔넷 연결할 수 있습니다.

그림 맨 아래에는 각 고객의 첫번째 서버 블레이드가 표시되어 있습니다. 이러한 블레이드 각각은 해당 데이터 네트워크에 대한 2개의 논리적 인터페이스와, 해당 관리 네트워크에 대한 2개의 논리적 인터페이스를 필요로 합니다. 이러한 논리적 인터페이스는 IPMP를 통해 제공되어야 합니다(부록 6 참조). 이 그림에는 IPMP 구성에 맞는 방식으로 인터페이스 번호가 지정되어 있습니다. 예를 들어, 고객 1의 서버 블레이드에는 VLAN 11(데이터 네트워크)에 대한 2개의 논리적 인터페이스와 VLAN 21(관리 네트워크)에 대한 2개의 논리적 인터페이스가 포함되어 있습니다. 부록 6에서 제시된 공식에 따라, 고객 1의 블레이드 각각의 인터페이스 번호는 `ce11000`과 `ce21000`(SSC0의 스위치와 `ce0` 연결용), 그리고 `ce11001`과 `ce21001`(SSC1의 스위치와 `ce1` 연결용)로 지정되어 있습니다.

마지막으로 이 시나리오에서 ISP의 고객은 각각 전용 네트워크 업링크 포트를 가집니다. 고객 1은 NETP0과 NETP1, 고객 2는 NETP2, NETP3 및 NETP4, 고객 3은 NETP5, NETP6 및 NETP7을 가집니다. 이러한 포트는 각 고객의 서버 블레이드가 속한 데이터 네트워크 VLAN에 포함되어 해당 고객 전용으로 지정됩니다. 그러므로 예를 들어, 고객 3의 데이터 네트워크 VLAN(13)은 서버 블레이드 포트 SNP 10 ~ SNP15와 업링크 포트 NETP5, NETP6 및 NETP7을 갖게 됩니다.

참고 – 서로 다른 고객에 속한 업링크가 동일한 외부 스위치에 연결되면, 스패닝 트리 프로토콜이 그러한 연결의 일부를 차단하게 됩니다. 따라서 각 고객별로 다른 외부 스위치를 사용하는 것이 좋습니다. 또는 스패닝 트리 프로토콜을 끌 수도 있습니다(7-11페이지의 단원 7.2.5, "스패닝 트리 끄기" 참조).

7.2.1 모든 VLAN의 생성 및 이름 지정

1. **다음을 입력하여 SSC0의 스위치에 로그인합니다.**

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

2. **사용자 이름을 묻는 프롬프트가 표시되면** admin**을 입력합니다.**

   암호에 다시 admin을 입력합니다.

3. **스위치가 공장 출하시 기본 설정을 사용하고 있는지 확인합니다.**

   이를 수행하는 방법은 A-4페이지의 단원 A.4, "스위치가 공장 출하시 기본 설정을 사용하는지 확인하기"를 참조하십시오.

4. **공장 출하시 기본 설정으로 돌아갔거나 아직 자신의 암호를 설정하지 않았으면 지금 암호를 설정합니다.**

   이를 수행하는 방법은 2-4페이지의 단원 2.2, "기본 사용자로 스위치에 로그인하여 암호 설정하기"를 참조하십시오.

5. **고객(tenant)의 데이터 VLAN을 생성하고 이름을 지정합니다.**

   다음을 입력합니다.

```
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. 고객(tenant)의 관리 VLAN을 생성하고 이름을 지정합니다.

다음을 입력합니다.

```
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 각 고객에게 관리 포트(NETMGT) 할당하기

1. ISP의 관리 VLAN(2) 및 모든 고객의 관리 VLAN(21, 22, 23)과 프레임을 송수신할 수 있도록 스위치의 관리 포트(NETMGT)를 구성합니다.

ISP는 기본 관리 VLAN인 VLAN 2를 사용합니다.

다음을 입력합니다.

```
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
```

위 과정의 의미는 다음과 같습니다.

- `interface ethernet NETMGT` 명령은 구성하려는 관리 포트가 NETMGT임을 알려줍니다.
- `switchport allowed vlan add 21` 명령은 NETMGT를 고객 1의 관리 VLAN (21)에 추가하고, 태그 지정된 프레임을 이 VLAN에 전달할 수 있도록 허가합니다.

- `switchport allowed vlan add 22` 명령은 NETMGT를 고객 2의 관리 VLAN(22)에 추가하고, 태그 지정된 프레임을 이 VLAN에 전달할 수 있도록 허가합니다.
- `switchport allowed vlan add 23` 명령은 NETMGT를 고객 3의 관리 VALN(23)에 추가하고, 태그 지정된 프레임을 이 VLAN에 전달할 수 있도록 허가합니다.
- `switchport ingress-filtering` 명령, `switchport mode trunk` 명령, 그리고 `switchport acceptable-frame-types tagged` 명령은 NETMGT가 자신이 속한 VLAN(VLAN 21, 22, 23 및 기본 관리 VLAN, VLAN 2)에 대해 태그 지정된 프레임만 송수신하도록 설정합니다.
- `no switchport gvrp` 명령은 NETMGT가 자신이 속한 VLAN을 다른 스위치에 알리기 위해 GVRP를 사용하는 것을 금지합니다.

2. 서버 블레이드에서 관리 네트워크로 가는 트래픽이 통과할 수 있도록 스위치의 IP 패킷 필터를 구성합니다.

이 작업을 수행하는 방법은 A-15페이지의 단원 A.11, "스위치의 패킷 필터를 사용한 블레이드의 보안 관리"를 참조하십시오.

7.2.3 각 고객에게 서버 블레이드 포트 할당하기

1. 고객 1에 대해, VLAN 11 또는 21로 태그 지정된 프레임만 송수신하도록 서버 블레이드 포트를 구성합니다.

다음을 입력합니다.

```
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
```

이 명령들을 고객 1에 속하는 다른 2개의 서버 블레이드 포트(SNP 1과 SNP 2)에도 수행합니다.

2. **고객 2에 대해, VLAN 12 또는 22로 태그 지정된 프레임만 송수신하도록 서버 블레이드 포트를 구성합니다.**

   다음을 입력합니다.

```
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
```

   이 명령들을 고객 2에 속하는 다른 서버 블레이드 포트(SNP 4 ~ SNP 9)에도 수행합니다.

3. **고객 3에 대해, VLAN 13 또는 23으로 태그 지정된 프레임만 송수신하도록 서버 블레이드 포트를 구성합니다.**

   다음을 입력합니다.

```
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
```

   이 명령들을 고객 3에 속하는 다른 서버 블레이드 포트(SNP 11 ~ SNP 15)에도 수행합니다.

7.2.4 각 고객에게 데이터 네트워크 포트 할당하기

참고 – Sun Fire B1600 블레이드 시스템 섀시에 연결된 네트워크 장치는 VLAN을 인식해야 합니다. 이러한 이유 때문에, 이 지침에는 네트워크 포트가 자신이 속한 VLAN에 대해 태그 지정된 프레임만 송수신하도록 설정하는 `switchport mode trunk` 명령이 포함됩니다.

1. **고객 1의 네트워크 포트가 VLAN 11로 태그 지정된 프레임만 송수신하도록 구성합니다.**

   NETP0에 대해 다음을 입력합니다.

```
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
```

   이 명령들을 NETP1에도 수행합니다.

2. **고객 2의 네트워크 포트가 VLAN 12로 태그 지정된 프레임만 송수신하도록 구성합니다.**

   NETP0에 대해 다음을 입력합니다.

```
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
```

   이 명령들을 NETP3과 NETP4에도 수행합니다.

3. **고객 3의 네트워크 포트가 VLAN 13으로 태그 지정된 프레임만 송수신하도록 구성합니다.**

   NETP0에 대해 다음을 입력합니다.

```
Console#configure
Console(config)#interface ethernet NETP 5
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
```

이 명령들을 NETP5, NETP6 및 NETP7에도 수행합니다.

7.2.5 스패닝 트리 끄기

서로 다른 고객에 속한 업링크가 동일한 외부 스위치에 연결되면, 스패닝 트리 프로토콜이 그러한 연결의 일부를 차단하게 됩니다. 따라서 각 고객별로 다른 외부 스위치를 사용하는 것이 좋습니다. 또는 스패닝 트리 프로토콜을 끌 수도 있습니다. 스패닝 트리를 끄려면 다음을 입력하십시오.

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

7.2.6 스위치 설정 저장 및 두번째 스위치에 구성 복사

1. **스위치 설정을 저장합니다.**

   이렇게 하는 방법은 부록 A에 나와있는 지침을 참조하십시오.

2. **스위치 구성을 두번째 스위치에 복사합니다.**

   이렇게 하는 방법은 부록 A에 나와있는 지침을 참조하십시오.

7.3 시나리오 B: 각각 8개의 블레이드를 갖고 4개의 데이터 포트를 공유하는 2명의 고객

이 시나리오에서는 인터넷 서비스 제공업체(ISP)가 블레이드 시스템 새시를 소유하고 있으며 그것을 관리할 전반적인 책임을 지고 있다고 전제합니다. 또한 고객 1과 고객 2라는 2명의 고객이 있습니다. 두 고객에게는 할당된 데이터 VLAN이 있고, 이 VLAN은 서버 블레이드 8개(즉, 스위치의 서버 블레이드 포트 8개)와 스위치의 외부 데이터 포트 4개를 가집니다. 다시 말해서 2명의 고객은 4개의 외부 데이터 포트를 공유하며 어느 누구도 독점적 사용권은 없습니다.

이 시나리오의 스위치 구성은 표 7-2에 요약되어 있습니다.

표 7-2 시나리오 B: 각각 8개의 서버 블레이드와 4개의 데이터 포트를 갖는 2명의 고객

네트워크 관리자	관리 포트	서버 블레이드 포트	외부 데이터 포트	데이터 VLAN ID	관리 VLAN ID
인터넷 서비스 제공업체	NETMGT	없음	없음	없음	2
고객 1	NETMGT	SNP0, SNP1, SNP2, SNP3, SNP4, SNP5, SNP6, SNP7	NETP0 ~ NETP3	11	21
고객 2	NETMGT	SNP8, SNP9, SNP10, SNP11, SNP12, SNP13, SNP14, SNP15	NETP0 ~ NETP3	12	22

본 단원의 나머지 부분에서는 표 7-2에 나와있는 구성을 구축하는 방법을 설명합니다. 이 부분은 다음 하위 단원으로 구성되어 있습니다.

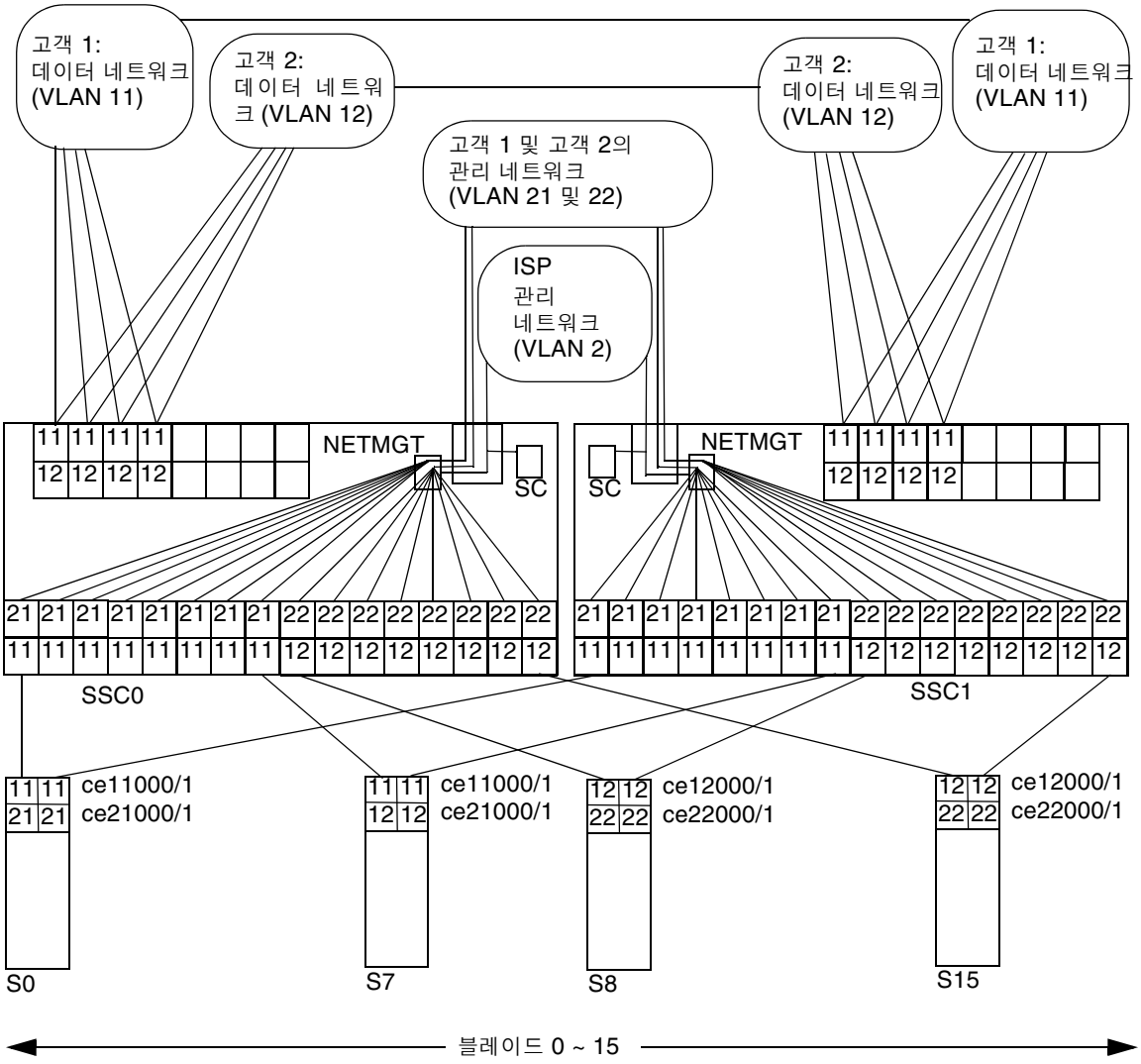


그림 7-2 시나리오 B: 공유 업링크 포트를 갖는 두 고객의 데이터 LAN과 관리 VLAN

그림 7-2는 표 7-2와 동일한 내용을 보여주는 그림입니다. 이 시나리오는 모든 네트워크 업링크 포트를 서버 블레이드 고객들간에 공유한다는 점을 제외하고 시나리오 A와 원칙적으로 동일합니다. 달리 말하면 2개의 고객 데이터 VLAN(고객 1은 VLAN 11, 고객 2는 VLAN 12)은 모두 업링크 포트 NETP0 ~ NETP3을 포함합니다. 그렇다 하더라도 한 고객이 다른 고객의 서버 블레이드 데이터를 수신하는 결과는 발생하지 않습니다. 그 이유는 NETP0 ~ NETP3 포트를 통과하는 모든 프레임은 VLAN 11(고객 1) 또는 VLAN 12(고객 2)로 태그 지정되기 때문입니다.

7.3.1 모든 VLAN의 생성 및 이름 지정

1. 고객(tenant)의 데이터 VLAN을 생성하고 이름을 지정합니다.

다음을 입력합니다.

```
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. 고객(tenant)의 관리 VLAN을 생성하고 이름을 지정합니다.

다음을 입력합니다.

```
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 각 고객에게 관리 포트(NETMGT) 할당하기

1. ISP의 관리 VLAN(2) 및 두 고객의 관리 VLAN(21과 22) 모두와 프레임을 송수신할 수 있도록 스위치의 관리 포트(NETMGT)를 구성합니다.

다음을 입력합니다.

```
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. 서버 블레이드에서 관리 네트워크로 가는 트래픽이 통과할 수 있도록 스위치의 IP 패킷 필터를 구성합니다.

이 작업을 수행하는 방법은 A-15페이지의 단원 A.11, "스위치의 패킷 필터를 사용한 블레이드의 보안 관리"를 참조하십시오.

7.3.3 각 고객에게 서버 블레이드 포트 할당하기

1. 고객 1에 대해, VLAN 11 또는 21로 태그 지정된 프레임만 송수신하도록 서버 블레이드 포트를 구성합니다.

다음을 입력합니다.

```
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
```

고객 1에 속한 다른 7개 서버 블레이드 포트(SNP1 ~ SNP7)에도 이 명령들을 수행합니다.

2. 고객 2에 대해, VLAN 12 또는 22로 태그 지정된 프레임만 송수신하도록 서버 블레이드 포트를 구성합니다.

다음을 입력합니다.

```
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
```

고객 2에 속한 다른 7개 서버 블레이드 포트(SNP9 ~ SNP15)에도 이 명령들을 수행합니다.

7.3.4 고객 간의 데이터 네트워크 포트 공유

참고 – 이 단원은 Sun Fire B1600 블레이드 시스템 섀시에 연결된 네트워크 장치가 VLAN을 인식한다고 전제합니다. 이러한 이유 때문에, 이 지침에는 네트워크 포트가 자신이 속한 VLAN에 대해 태그 지정된 프레임만 송수신하도록 설정하는 `switchport mode trunk` 명령이 포함됩니다.

---

1. **VLAN 11 또는 VLAN 12로 태그 지정된 프레임만 송수신하도록 네트워크 포트를 구성합니다.**

   NETP0에 대해 다음을 입력합니다.

```
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 ~ NETP3에도 이 명령들을 수행합니다.**

3. **스위치 설정을 저장합니다.**

   이렇게 하는 방법은 부록 A에 나와있는 지침을 참조하십시오.

4. **스위치 구성을 두번째 스위치에 복사합니다.**

   이렇게 하는 방법은 부록 A에 나와있는 지침을 참조하십시오.

부록 **A**

스위치에서 수행해야 할 유용한 작업들

본 부록은 스위치의 명령행 인터페이스에서만 수행 가능한 일부 작업들을 수행하는 방법을 설명합니다. 특히 블레이드 시스템 새시를 구성할 때 이 정보가 필요합니다.

스위치 명령행 인터페이스에 로그인하는 방법은 2장을 참조하십시오.

이 장은 다음 단원으로 구성되어 있습니다.

A.1 명령 프롬프트 이동

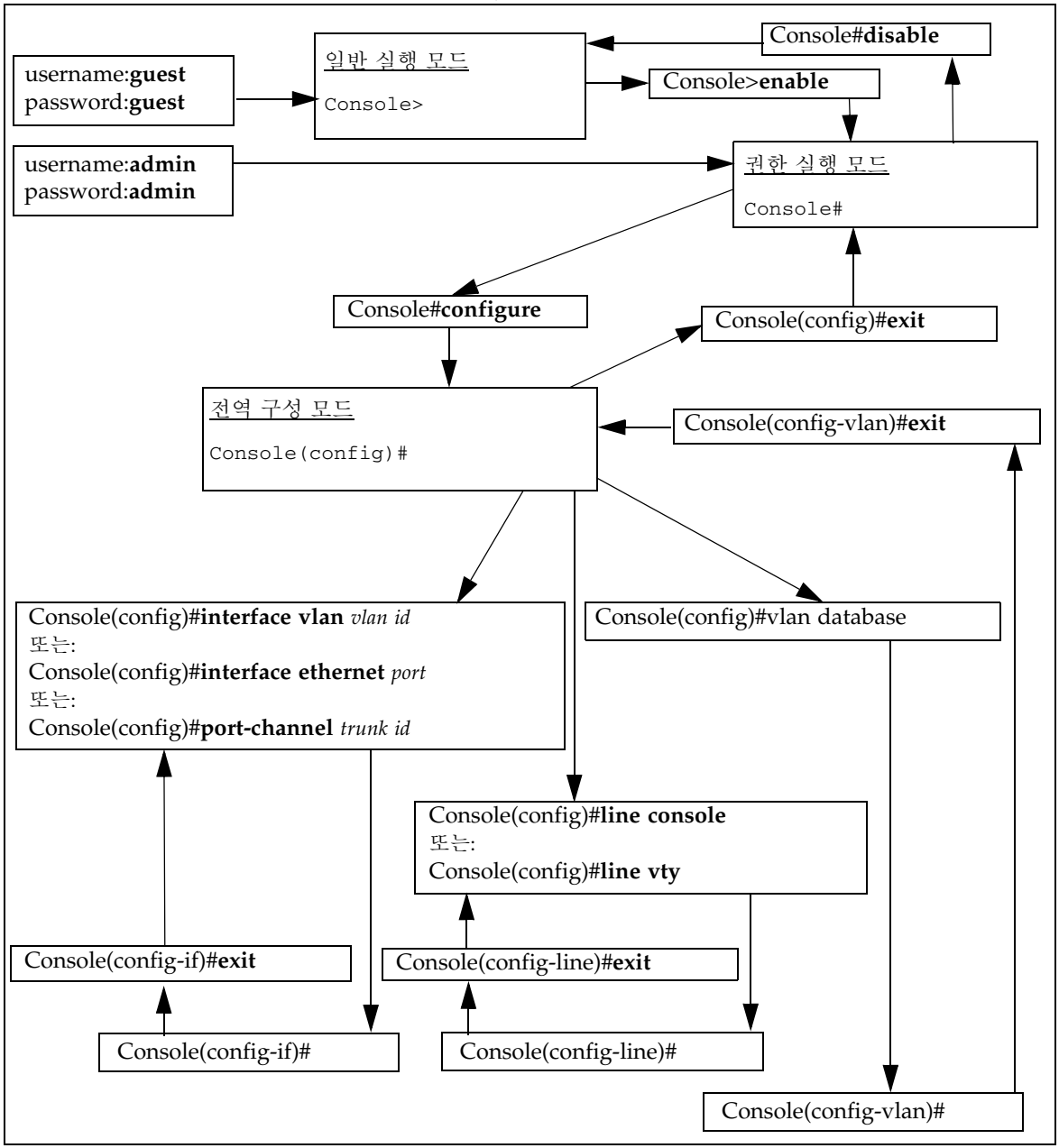


그림 A-1 스위치의 명령 프롬프트 맵

A.2 명령행 인터페이스 종료

A.2.1 스위치에서 시스템 컨트롤러로 돌아가기

- **스위치의 명령행 인터페이스를 종료하고 시스템 컨트롤러의 명령행 인터페이스로 돌아가려면 "#" 문자 바로 뒤에 "." 문자를 입력합니다.**

  스위치 명령행 인터페이스의 어느 위치에 있든지 "#." 탈출 문자열을 입력하면 시스템 컨트롤러의 명령행 인터페이스로 돌아갑니다.

  예를 들어, 다음을 입력합니다(입력한 문자가 화면에 표시되지는 않습니다).

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

A.2.2 스위치의 로그인 프롬프트로 돌아가기

- **스위치의 로그인 프롬프트로 돌아가려면** Console# **프롬프트에 도달할 때까지** exit **또는** end**를 입력한 후 다음을 입력합니다.**

```
Console#exit
```

A.3 스위치 명령행 인터페이스에 대한 온라인 도움말 보기

- **온라인 도움말 사용 방법을 보려면 언제든지** help**를 입력합니다.**
- **상황에 맞는 온라인 도움말을 보려면 언제든지 ?를 입력합니다. 그러면 명령 또는 매개변수 목록이 표시됩니다. 명령 프롬프트에서 ?를 입력하면 현재 명령 모드에서 사용할 수 있는 명령들의 목록이 표시됩니다. 명령에 사용되는 매개변수를 알고 싶으면 명령의 첫번째 단어 뒤에 ?를 입력합니다. 그러면 입력할 수 있는 매개변수의 목록과 각각에 대한 설명이 표시됩니다. 명령을 불완전하게 입력한 후에 ?를 입력하면 앞서 입력한 명령 부분이 콘솔에 자동으로 표시됩니다. 따라서 사용자는 해당 정보를 다시 입력할 필요가 없습니다.**

VLAN을 구성하는 명령 모드로 이동하기 위해 vlan database 명령을 사용하는 과정에 도움말 정보를 표시하는 예제가 아래에 나와 있습니다.

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

여기서 <cr>은 더 이상 필요한 매개변수가 없으며 ENTER를 눌러 명령 프롬프트로 돌아가야 함을 나타냅니다.

A.4 스위치가 공장 출하시 기본 설정을 사용하는지 확인하기

스위치의 공장 출하시 기본 설정에 대한 내용은 *Sun Fire B1600 블레이드 시스템 섀시 스위치 관리 안내서*를 참조하십시오.

스위치를 공장 출하시 기본 설정으로 복원하려면 다음과 같이 하십시오.

1. **스위치가 공장 출하시 기본 설정을 사용하고 있는지 확인하기 위해 다음을 입력합니다.**

```
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
```

이 명령 출력의 맨 아래 줄에서 file name 열에 "Factory_Default_Config.cfg"가 표시되면 스위치가 기본 설정을 사용하고 있는 것입니다.

2. **스위치가 공장 출하시 기본 설정을 사용하게 하려면 다음을 입력합니다.**

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

3. **공장 출하시 기본 설정을 사용하여 스위치를 재시동합니다.**

다음을 입력합니다.

```
Console#reload
```

4. **사용자 이름과 암호를 입력하라는 메시지가 표시되면 두 가지 모두에 대해** admin**을 입력합니다.**

A.5 스위치 재설정

스위치를 재설정하는 일반적인 이유는 실행 구성을 일부 변경한 후에 변경 사항을 취소하고 시동 구성으로 되돌아가기 위해서 입니다.

스위치를 재설정하는 또 다른 이유는 새 구성 파일을 생성 또는 다운로드한 후에 새 파일을 기본 시동 파일로 지정하기 위해서 입니다.

참고 – 스위치를 재설정하기 전에, 보존하고자 하는 구성 변경 사항을 저장해 두십시오.

- **스위치의 명령행에서 스위치를 재설정하려면 다음을 입력합니다.**

```
Console#reload
```

- **또는, 시스템 컨트롤러의 명령행에서 스위치를 재설정할 수도 있습니다.**
  sc> 프롬프트에서 다음을 입력합니다.

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

여기서 *n*은 재설정하는 SSC가 SSC0인지 또는 SSC1인지에 따라 0 또는 1로 지정합니다.

A.6 스위치의 IP 주소, 넷마스크 및 기본 게이트웨이 설정

1. 다음을 입력하여 IP 주소 및 넷마스크를 설정합니다.

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

여기서:

- *vlan id*는 스위치의 네트워크 관리 포트인 NETMGT가 속한 VLAN의 번호(기본적으로 2)입니다. 공장 출하시 기본 설정을 사용 중인 경우 2로 지정하십시오.
- *ip address*는 스위치가 사용할 IP 주소입니다.
- *netmask*는 설정하려는 넷마스크(예: 255.255.255.0)입니다.

2. 다음을 입력하여 기본 게이트웨이를 설정합니다.

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

여기서 *ip address*는 기본 게이트웨이로 지정하려는 장치의 IP 주소입니다.

3. 기본 게이트웨이 설정에 대한 변경 사항을 최종 적용하기 위해 다음을 입력합니다.

```
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#
```

위의 출력 예제의 콜론(:) 문자는 생략된 정보를 나타냅니다. 기본 게이트웨이의 설정은 show running-config 명령 출력의 끝 부분에 있습니다.

A.7 VLAN 설정

스위치에는 기본적으로 관리 포트(NETMGT)를 포함하는 관리 VLAN(VLAN 2)과 다른 모든 포트를 포함하는 데이터 VLAN이 있습니다.

VLAN을 사용하는 자세한 방법은 5장, 6장 및 7장을 참조하십시오.

추가 VLAN을 생성하려면 VLAN을 설정하고 여기에 개별적으로 포트를 추가해야 합니다.

1. Console# **프롬프트에서 다음을 입력합니다.**

```
Console#configure
```

2. 다음을 입력하여 vlan 구성 모드로 전환합니다.

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

3. VLAN을 생성합니다.

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

여기서 *vlan identifier*는 1 ~ 4094 사이의 숫자입니다.

4. 다음을 입력하여 VLAN에 이름을 부여합니다.

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

여기서 *vlan identifier*는 VLAN의 번호이며, *name*은 VLAN에 부여할 이름입니다.

5. 개별 포트에 추가하여 VLAN에 포함시킬 포트를 지정합니다.

a. 이 작업을 수행하려면 먼저 다음을 입력하여 구성 모드로 돌아갑니다.

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

b. 그런 다음 다음을 입력하여 구성 인터페이스 모드로 전환합니다.

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

여기서 *port*는 VLAN에 포함시킬 포트의 이름입니다.

c. 다음을 입력하여 VLAN을 포트에 추가합니다.

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

d. 새 VLAN에 포함시킬 각 포트에 대하여 단계 a ~ 단계 c를 반복합니다.

A.8 스위치 설정 저장

참고 – 스위치를 재시동한 후에도 유지하고자 하는 모든 스위치 설정을 저장하도록 하십시오.

- **변경 사항을 저장하려면 실행 구성 펌웨어를 시동 구성 펌웨어에 복사합니다.**
  이 작업을 수행하려면 스위치 콘솔에 다음을 입력합니다.

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

Console#
```

여기서 *default filename*은 현재 시동 구성 파일이고 *filename*은 새 시동 구성 파일에 부여할 이름입니다. 새 파일 이름을 지정하는 대신 ENTER를 입력하면 실행 구성이 현재 시동 구성 파일에 기록됩니다.

A.9 첫번째 스위치의 구성을 두번째 스위치에 복사하기

하나의 스위치에서 다른 스위치로 구성 파일을 복사하려면 TFTP를 사용해야 합니다. 따라서 네트워크에 TFTP 서버를 설정해 두어야 합니다. 이 단원에서는 이 작업을 수행하는 방법을 설명한 다음, 파일을 전송하는 방법을 설명합니다.

스위치에 VLAN을 설정하여 네트워크를 여러 지역으로 나누었고 아울러 IP 네트워크 다중 경로 지정(IPMP)을 사용하여 서버 블레이드에 이중화된 네트워크 연결을 설정한 경우, 두번째 스위치의 구성을 첫번째 스위치의 구성과 동일하게 만들어야 합니다.

주의 – 두번째 내장 스위치의 VLAN 구성이 첫번째 스위치의 VLAN 구성과 동일하지 않으면 두번째 스위치를 통과하는 데이터는 첫번째 스위치의 VLAN 정의와 무관하게 행동합니다. 마찬가지로 첫번째 스위치의 패킷 필터를 두번째 스위치에 복사하지 않으면 해당 패킷 필터가 수행하는 관리 네트워크 보호 기능이 상실됩니다.

Sun Fire B1600 블레이드 시스템 섀시의 두번째 스위치가 첫번째 스위치와 동일한 구성을 갖게 하려면 이 단원의 지침을 따르십시오.

A.9.1 TFTP 서버 설정

네트워크의 Solaris 시스템이 TFTP 요청을 처리하도록 구성하려면 다음을 수행하십시오.

1. **TFTP 서버로 설정할 시스템에서 루트로 로그인합니다.**

2. **텍스트 편집기를 사용하여** /etc/inetd.conf **파일에서 다음 행을 삭제합니다.**

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

3. **동일한 시스템의 Solaris 프롬프트에서 다음과 같이 입력하여 TFTP 홈 디렉토리를 작성합니다.**

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

4. **다음을 입력하여** inetd**를 다시 시작합니다.**

```
# pkill -HUP inetd
```

5. **TFTP가 작동하는지 확인합니다.**

   확인하려면 TFTP를 사용하여 /tftpboot 디렉토리에서 파일을 가져와 봅니다. 아래 지침을 수행합니다.

a. TFTP 서버로 사용하는 시스템에서 임의의 파일(예: Solaris /etc/release **파일)을** /tftpboot **디렉토리로 복사합니다.**

Solaris 프롬프트에서 다음을 입력하여 /etc/release 파일을 복사합니다.

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

여기서 *filename*은 TFTP 서버에서 외부와 공유할 파일의 이름입니다.

b. 방금 복사한 파일을 전체 사용자에 대해 읽기 전용으로 만듭니다.

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

여기서 *filename*은 TFTP 서버에서 외부와 공유할 파일의 이름입니다.

c. 생성한 TFTP 서버에서 파일을 가져옵니다.

다른 시스템의 Solaris 프롬프트에서 다음 명령을 입력합니다.

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

여기서 *tftp server*는 앞에서 설정한 TFTP 서버를 실행 중인 시스템의 호스트 이름 또는 IP 주소이고, *filename*은 TFTP 서버에서 가져올 파일의 이름입니다.

d. get **명령을 입력했던 Solaris 시스템에서 다시 다음을 입력하여 파일의 내용을 확인합니다.**

```
# cat filename
```

여기서 *filename*은 TFTP 서버에서 가져온 파일의 이름입니다.

참고 – TFTP는 FTP와 다르다는 점에 유의하십시오. TFTP와 FTP는 서로 다른 오류 메시지를 표시하며, FTP에서 사용할 수 있는 cd 명령이나 ls 명령 또는 그 외의 대부분의 명령을 사용할 수 없습니다.

A.9.2 스위치 구성 파일 전송

TFTP 서버를 생성하고 아울러 SSC0 또는 SSC1의 스위치 구성 작업을 완료한 경우, 해당 스위치의 구성을 두번째 스위치로 복사하십시오.

이렇게 하려면 아래 지침을 수행하십시오. 아래 지침은 SSC0의 스위치 구성을 SSC1의 스위치로 복사한다고 가정하지만 물론 SSC1의 스위치에서 SSC0으로 복사할 수도 있습니다.

1. **2장, 3장, 5장, 6장 및 7장의 지침에 따라 필요에 맞게 스위치 0을 구성합니다.**

2. **스위치 0의 구성을 예를 들어** standard.cfg **파일에 저장합니다.**

   이 작업을 수행하려면 스위치 Console# 프롬프트에서 다음을 입력합니다.

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

Console#
```

3. standard.cfg **파일을 TFTP 서버로 업로드합니다.**

   다음을 수행합니다.

   a. **TFTP 서버에 루트로 로그인합니다.**

   b. /tftpboot **디렉토리로 이동합니다.**

   c. standard.cfg**라는 이름으로 비어있는 파일을 생성합니다.**

```
#>standard.cfg
```

4. **전체 사용자에 대해 이 파일의 읽기/쓰기를 허용합니다.**

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

5. 스위치의 명령행 인터페이스에서 다음을 입력합니다.

```
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#
```

여기서 *filename*은 두 경우 모두 standard.cfg(스위치 구성을 저장한 파일의 이름)이고 *IP address*는 TFTP 서버의 IP 주소입니다.

6. TFTP 서버에서 텍스트 편집기를 사용하여 standard.cfg **파일을 엽니다.**

스위치 0의 호스트 이름 항목을 스위치 1의 호스트 이름으로 변경합니다.

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

스위치에 IP 주소를 수동으로 할당하려는 경우, 스위치 0이 아닌 스위치 1의 IP 주소와 넷마스크를 포함하도록 IP 주소 및 넷마스크 항목을 변경해야 합니다.

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

DHCP를 사용하는 경우에는 IP 주소나 넷마스크 또는 DHCP 클라이언트 식별자를 변경할 필요가 없습니다. IP 주소와 넷마스크는 DHCP 서버가 자동으로 할당합니다. DHCP 클라이언트 식별자는 스위치가 재설정될 때마다 활성 시스템 컨트롤러가 자동으로 할당합니다.

7. 이 파일을 적당한 이름으로 바꿔 저장합니다(예: standard1.cfg**).**

8. 스위치 1에 로그인한 다음, 스위치에 DHCP가 할당한 IP 주소가 없을 경우 임시 관리 IP 주소를 설정합니다.

스위치 1에 대하여 이미 로그인 및 암호 정보를 구성했으면 해당 정보를 사용하여 로그인합니다. 그렇지 않으면 공장 출하시 기본 사용자 이름(admin)과 암호(admin)를 사용하여 로그인합니다.

IP 매개변수를 설정하려면 A-6페이지의 단원 A.6, "스위치의 IP 주소, 넷마스크 및 기본 게이트웨이 설정"에 나와있는 지침을 수행합니다.

9. **TFTP 서버에서 스위치 1로** standard1.cfg **파일을 다운로드합니다.**

   다음을 입력합니다.

```
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. **이 파일을 스위치 1의 시동 구성으로 설정합니다.**

    다음을 입력합니다.

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

11. **스위치 펌웨어를 다시 로드합니다.**

    다음을 입력합니다.

```
Console#reload
```

A.10 복원성 및 성능 향상을 위한 트렁크 연결 설정

다수의 외부 데이터 포트가 동일한 스위치에 연결되어 있을 경우 이들을 트렁크로 결합하는 것이 좋습니다. 그러면 복원성과 성능이 향상됩니다.

예를 들어, 하나의 외부 스위치에 대하여 4개의 별도 연결이 있고 그러한 연결 중 하나가 케이블 고장으로 인해 장애가 발생한 경우, 해당 연결을 사용하는 모든 통신이 두절됩니다. 그러나 이 외부 스위치에 대한 4개의 연결 모두를 포함하는 트렁크를 설정한 경우, 하나의 연결에 장애가 발생하더라도 트렁크에 설정된 나머지 연결을 통해 통신이 정상적으로 수행됩니다.

장애가 발생한 연결이 없는 한, 내장 스위치는 트렁크의 모든 연결을 동일한 네트워크에 대한 단일 고 대역폭 연결로 간주합니다.

참고 – 외부 스위치, 허브 또는 라우터에 대해 이중화된 연결이 있는데 이 연결을 트렁크로 만들지 않은 경우, 내장 스위치의 스패닝 트리 기능은 하나를 제외한 모든 연결을 차단합니다. 그러므로 네트워크는 여전히 이중화 구성의 혜택을 보게된다 하더라도, 사용 중인 하나의 연결이 잘못되기 전까지 나머지 연결은 어느 것도 사용할 수 없게 됩니다.

다음 예제 명령은 NETP2, NETP3 및 NETP4 포트를 포함하는 트렁크를 생성합니다.

```
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 스위치의 패킷 필터를 사용한 블레이드의 보안 관리

스위치에는 기본적으로 서버 블레이드에서 스위치의 관리 포트(NETMGT)로 이동하는 모든 트래픽을 차단하는 패킷 필터가 있습니다. 이 필터는 서버 블레이드를 통해 올 수 있는 모든 적대적 공격으로부터 관리 네트워크를 보호합니다(예를 들어, 해커가 공용 네트워크에서 블레이드 중 하나에 몰래 침입한 경우). 그러나 한편으로는 서버 블레이드에서 관리 포트로 가는 관리 트래픽을 허용하는 패킷 필터를 구성할 때까지는 관리 포트를 통해 서버 블레이드와 직접 통신할 수 없음을 의미하기도 합니다. 이 단원에서는 이러한 패킷 필터를 구성하는 방법을 설명합니다.

참고 – 기본적으로 패킷 필터는 서버 블레이드에서 관리 포트(NETMGT)로 가는 모든 트래픽을 막습니다. 패킷 필터를 통과시킬 트래픽을 결정할 때에는 신중을 기해야 하며, 어떤 경우에도 반드시 필요한 프로토콜만 통과를 허용해야 합니다.

다음 지침은 DHCP, BOOTP, TFTP, SUNRPC, SNMP 및 NFS 프레임이 서버 블레이드에서 패킷 필터를 통해 관리 포트로 통과하도록 허용하는 데 사용되는 명령에 대해 설명합니다. 이 프로토콜들은 관리 포트를 통해 서버 블레이드를 관리하기 위해 필요한 최소한의 프로토콜입니다.

1. **DHCP 및 BOOTP 프레임이 패킷 필터를 통과하도록 허용합니다.**

   스위치 콘솔에서 다음을 입력합니다.

```
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 프레임이 패킷 필터를 통과하도록 허용합니다.**

   다음을 입력합니다.

```
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 프레임이 패킷 필터를 통과하도록 허용합니다.**

   다음을 입력합니다.

```
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 프레임이 패킷 필터를 통과하도록 허용합니다.**

   다음을 입력합니다.

```
Console#configure
Console(config)#ip filter permit udp 1610.0.0 0.0.0.0 0.0.0.0
0.0.0.0 0.0
Console(config)#ip filter permit tcp 1610.0.0 0.0.0.0 0.0.0.0
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
```

참고 – 161 포트는 관리 대상 장치에 SNMP 요청을 보내기 위한 포트이고, 162 포트는 관리 대상 장치의 SNMP 트랩을 수신하기 위한 포트임에 유의하십시오. SNMP 트랩은 관리 대상 장치에서 시작됩니다. SNMP 명령은 SNMP 관리 스테이션에서 시작됩니다.

5. **NFS 프레임이 패킷 필터를 통과하도록 허용합니다.**

   다음을 입력합니다.

```
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
```

참고 – ip filter permit 명령을 사용하는 자세한 방법은 *Sun Fire B1600 블레이드 시스템 섀시 스위치 관리 안내서*를 참조하십시오. 개별 프로토콜과 관련된 포트 번호 목록은 Unix 시스템의 /etc/services 파일 또는 /etc/inet/services 파일을 참조하십시오. IP 서비스와 관련된 전체 포트 번호 목록은 Internet Assigned Numbers Authority 웹 사이트 (http://www.iana.org)를 참조하십시오.

A.12 스위치의 사용자 설정

1. **스위치 콘솔에서 다음을 입력합니다.**

```
Console#configure
```

2. **다음을 입력합니다.**

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

여기서 *username*은 로그인할 때 사용자가 입력할 이름입니다.

첫번째 명령의 숫자 15는 새 사용자가 권한 실행 모드에 액세스할 수 있음을 의미합니다. 사용자에게 일반 실행 모드에 대한 액세스 권한만 부여하려면 15 대신 0을 입력합니다.

3. **다음을 입력합니다.**

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

여기서 *username*은 로그인할 때 사용자가 입력할 이름이고 *password*는 새 사용자의 암호입니다.

이 명령에서 0은 *password*로 지정한 값이 암호화되지 않았음을 의미합니다. 암호화된 형식으로 값을 지정하려는 경우, 암호 앞에 7을 두어 암호화된 형식으로 암호를 지정했음을 나타내야 합니다.

A.12.1 스위치의 기본 사용자 이름 및 암호

전체 액세스 권한을 갖는 기본 사용자의 이름은 admin입니다.
암호는 admin입니다.

방문자 액세스를 위한 기본 사용자 이름은 guest입니다(제한된 권한만 가짐).
암호는 guest입니다.

guest 액세스를 전체 액세스로 전환하는 enable 명령의 기본 암호는 super입니다.

A.13 스위치 및 스위치 구성 정보 보기

본 단원은 다음 정보로 구성되어 있습니다.

A.13.1 IP 주소 및 VLAN ID 확인

● **관리 포트의 IP 주소 및 VLAN ID를 확인하려면** Console# **프롬프트에서 다음을 입력합니다.**

```
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 구성 확인

● **스위치의 VLAN 구성을 확인하려면** Console# **프롬프트에서 다음을 입력합니다.**

```
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 로그인한 사용자 목록 보기

- **명령행 인터페이스와 웹 인터페이스에 로그인한 사용자의 목록을 보려면** Console# **프롬프트에서 다음을 입력합니다.**

```
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 현재 구성 또는 시동 구성 확인

- **스위치의 현재 구성을 보려면** Console# **프롬프트에서 다음을 입력합니다.**

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

스위치를 마지막 시동한 이후 스위치 설정을 변경한 사용자가 있을 경우, 실행 구성이 시동 구성과 다르게 됩니다.

- **가장 최근에 시동했을 때 스위치가 사용한 구성(또한 다음 시동시에도 사용하게 될 구성)을 보려면** Console# **프롬프트에서 다음을 입력합니다.**

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

A.13.5 펌웨어 버전 번호 확인

- **펌웨어 및 기타 버전 정보를 확인하려면** Console# **프롬프트에서 다음을 입력합니다.**

```
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 :0.0.60.7
 Boot rom version :1.00.00.8
 Operation code version :1.0.00.6
Console#
```

A.13.6 MAC 주소 및 일반 시스템 정보 보기

- **MAC 주소, 펌웨어 및 기타 버전 정보를 확인하려면** Console# **프롬프트에서 다음을 입력합니다.**

```
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#
```

부록 **B**

랩탑을 사용하여 시스템 컨트롤러에 직렬 연결 설정

본 부록은 Sun Fire B1600 블레이드 시스템 섀시의 두 스위치 및 시스템 컨트롤러(SSC) 모듈 중 하나에 랩탑 컴퓨터를 사용하여 연결함으로써 섀시의 명령행 관리 인터페이스에 액세스하는 방법을 설명합니다.

본 부록은 다음 단원으로 구성되어 있습니다.

참고 – 이 장의 지침을 수행하기 전에 블레이드 시스템 섀시를 랙 또는 캐비닛에 설치했는지 확인하십시오(*Sun Fire B1600 하드웨어 설치 설명서* 참조).

B.1 랩탑에 연결

참고 – 랩탑의 직렬 포트 대신 병렬 포트(25핀)를 사용해서는 안됩니다. 직렬 포트는 D유형 9핀 숫커넥터입니다.

1. **섀시와 함께 제공된 RJ-45/RJ-45 패치 케이블을 SSC의 직렬 포트에 연결합니다.**
2. **패치 케이블의 다른 쪽 끝을 Sun Fire B1600과 함께 제공된 은색 DB25(25웨이 DSUB 수/암 8 POS RJ-45) 어댑터(부품 번호 530-2889-0x)의 RJ-45 커넥터에 연결합니다.**

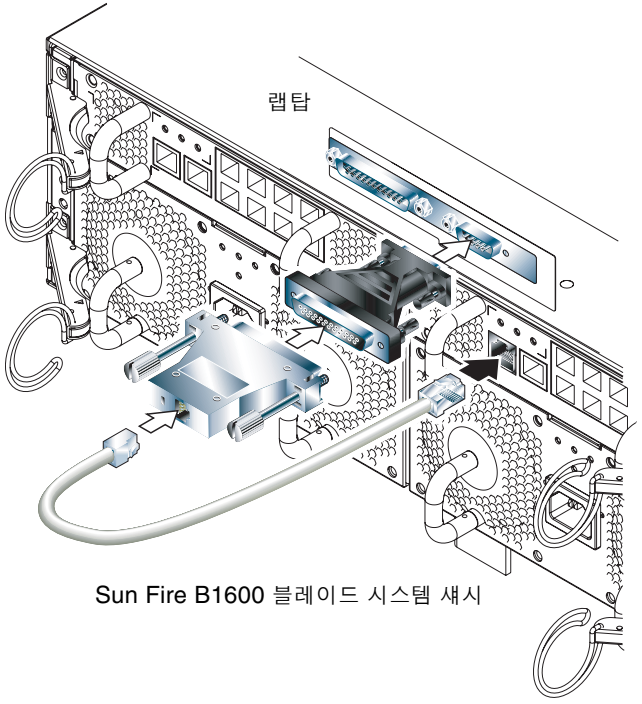


그림 B-1 랩탑의 직렬 포트에 SSC 연결

3. **25웨이 암커넥터와 9웨이 D유형 암커넥터를 가진 어댑터에 25웨이 D유형 숫커넥터를 연결합니다.**

   Sun에서는 25x9웨이 D유형 암/암 어댑터를 제공하지 않습니다. 그러나 이러한 종류의 어댑터는 가정용 컴퓨터 공급업체나 전자 대리점에서 쉽게 구입하실 수 있습니다. 어댑터가 갖추어야 할 핀 연결 구성은 표 B-1에 나와 있습니다.

표 B-1 25x9웨이 D유형 암/암 어댑터가 갖추어야 할 핀 연결

9웨이 암커넥터	25웨이 암커넥터
핀 1	핀 8
핀 2	핀 3
핀 3	핀 2
핀 4	핀 20
핀 5	핀 7
핀 6	핀 6
핀 7	핀 4
핀 8	핀 5
핀 9	핀 22

4. **마지막으로, 9웨이 암커넥터를 랩탑의 직렬 포트에 연결합니다.**

B.1.1 Microsoft Windows HyperTerminal 사용

참고 – 평소에 랩탑의 직렬 포트를 초소형 휴대 장치에 연결하여 사용하는 경우, 본 단원의 지침을 수행하기 전에 Hot Sync Manager를 닫아야 합니다. 그러지 않을 경우 Sun Fire B1600 블레이드 시스템 섀시와의 통신에 직렬 포트를 사용하지 못하게 됩니다.

본 단원에서 설명하는 지침은 Microsoft Windows 98 및 HyperTerminal Applet 버전 3.0이 설치된 랩탑 PC에서 검증되었습니다.

1. **Microsoft Windows의 HyperTerminal을 실행합니다.**
2. **HyperTerminal 창에서 Hypertrm.exe 아이콘을 두번 누릅니다.**

3. **Connection Description 창에서 랩탑에 생성할 HyperTerminal 연결의 이름을 지정합니다.**

   그런 다음 연결에 사용할 아이콘을 선택하고 OK를 누릅니다.

4. **Connect to... 창에서 "Connect using" 옵션의 화살표를 누른 다음 서버 연결에 사용할 포트를 선택합니다.**

   다른 포트를 사용해야 할 특별한 이유가 없는 한 DIRECT TO COM1을 선택합니다. OK를 누릅니다.

5. **COM1 Properties Port Settings 창에서 아래와 같이 매개변수를 설정합니다.**

   초당 비트 수: 9600
   데이터 비트: 8
   패리티: None
   정지 비트: 1
   흐름 제어: "Xon/Xoff" 또는 "None"으로 지정합니다.

   참고 – 흐름 제어 옵션으로 "Hardware"를 선택하지 마십시오.

   OK를 누릅니다.

6. **그러면 HyperTerminal 세션이 활성화됩니다. File 메뉴에서 Properties를 선택합니다.**

7. **Properties 창에서 Settings 탭을 누릅니다.**

   Settings 탭에서 Emulation 옵션의 화살표를 누른 다음 VT100을 선택합니다. Telnet terminal 옵션에는 VT100을 지정합니다. OK를 누릅니다.

   참고 – 이제 Sun Fire B1600 블레이드 시스템 섀시 및 블레이드에 소프트웨어를 설치할 수 있습니다(2장 참조).

부록 **C**

서버 블레이드의 IP 주소 구성을 위한 DHCP 설정

본 부록은 *Solaris Advanced Installation Guide*와 *DHCP Administration Guide*의 내용을 보완합니다. 이 부록에는 시스템 섀시의 서버 블레이드가 IP 주소를 동적으로 할당받을 수 있도록 데이터 네트워크의 네트워크 설치 서버와 DHCP 서버를 구성하는 방법이 나와 있습니다.

본 부록의 내용은 사용자가 Solaris 이미지를 네트워크 설치 서버에 추가하였고 데이터 네트워크 상에 DHCP 서버가 있음을 전제로 합니다.

본 부록은 다음 단원으로 구성되어 있습니다.

C.1 네트워크 설치 서버 작업

- **네트워크 설치 서버에서 -d 옵션과 함께** add_install_client **명령을 실행합니다.**

  이 명령은 DHCP를 지원하는 inetboot 파일을 Solaris 이미지에서 /tftpboot 디렉토리로 복사합니다. 이 명령을 실행하려면 다음을 입력합니다.

```
# 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
```

  여기서 *path*는 네트워크 설치 서버에서 Solaris 이미지의 위치입니다. (위 예제에서 두번째 명령이 다음 행으로 넘어간 점에 유의하십시오.) 위 예제의 출력에는 예제 IP 데이터가 사용되었습니다.

C.2 DHCP 서버 작업

1. **DHCP 서버에서, Solaris 점프스타트를 실행하는 동안 블레이드에 전달할 옵션을 생성합니다.**

   (이 정보는 비-DHCP 점프스타트 실행시 /etc/bootparams 파일에서 얻을 수 있는 정보입니다.)

표 C-1에 생성해야 할 옵션 목록이 나와 있습니다.

표 C-1 점프스타트 실행시 블레이드에 전달해야 할 DHCP 옵션

옵션 이름	설명
SrootIP4	루트 서버의 IP 주소
SrootNM	루트 서버의 호스트 이름
SrootPTH	부트 이미지 경로(예: `/images/2.8/Solaris_8/Tools/Boot`)
SinstIP4	네트워크 설치 서버의 IP 주소
SinstNM	네트워크 설치 서버의 호스트 이름
SsysidCF	sysidcfg 파일의 위치(예: configsrv:/config)
SjumpsCF	프로파일 및 rules.ok 디렉토리의 위치(예: `configsrv:/config`)
SbootFIL	커널 경로(예: `/platform/sun4u/kernel/sparcv9/uni`)
Sterm	설치시 사용되는 터미널 유형

다음은 표 C-1에 나와있는 옵션을 생성하는 데 사용되는 명령 예제입니다.

```
# 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. 필요한 옵션(단계 1에서 생성한 옵션 포함)이 들어있는 매크로를 생성합니다.

표 C-2 생성해야 할 매크로

매크로 이름	매크로 내용(한 매크로에 다른 매크로를 포함할 수 있음)
Solaris	SrootIP4, SrootNM, SinstIP4, SinstNM, Sterm, SjumpsCF, SsysidCF
sparc	SrootPTH, SinstIP4
sun4u	Solaris, sparc
SUNW.Serverblade1	SbootFIL, sun4u
*network name**	Subnet, Router, Broadcst ¼Þ BootSrvA

여기서 **network name*은 클라이언트가 들어있는 네트워크를 나타내는 IP 주소입니다. DHCP 서버의 기본 인터페이스가 들어있는 서브넷을 제외한 각 클라이언트 서브넷마다 위 매크로 중 하나를 생성해야 합니다.

다음은 원하는 매크로를 생성하는 데 사용되는 명령 예제입니다.

```
# dhtadm -A -m Solaris -d ':SrootIP4=192.168.160.12:SrootNM=
"bootsrv":SinstIP4=192.168.160.15:SinstNM="installsrv":Sterm=
"xterm":SjumpsCF="configsrv:/config":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=192.168.160.255:BootSrvA=
192.168.160.12:'
```

3. 클라이언트의 호스트 이름과 IP 주소를 호스트 데이터베이스(/etc/hosts)에 추가합니다.

4. SUNW.Serverblade1 매크로를 클라이언트에 매핑합니다.

다음을 입력합니다.

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

여기서:

*MACaddress*는 클라이언트의 MAC 주소입니다.

*DHCP server*는 DHCP 서버의 호스트 이름입니다.

*network name*은 클라이언트가 들어있는 네트워크를 나타내는 IP 주소입니다(위 예제의 명령행이 다음 행으로 넘어간 점에 유의하십시오).

C.3 서버 블레이드 작업

서버 블레이드에 각각 2개의 IP 주소를 할당하도록 네트워크 환경을 구성한 경우, 본 단원의 내용을 수행하십시오. 본 단원의 내용은 구성하려는 서버 블레이드가 네트워크에서 시동되었고, 해당 기본(ce0) 인터페이스의 IP 구성이 할당되었음을 전제로 합니다.

1. **시스템 컨트롤러의 sc> 프롬프트에서 블레이드 콘솔에 액세스합니다.**

   다음을 입력합니다.

```
sc> console sn
```

   여기서 *n*은 구성하려는 블레이드의 슬롯 번호입니다.

2. **Solaris 프롬프트에서 다음을 입력합니다.**

```
# ifconfig ce1 plumb
```

3. **마지막으로, 다음을 입력합니다.**

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

부록 **D**

Web Start Flash 아카이브를 사용하여 Solaris 블레이드 설치하기

본 부록은 *Solaris 8 Advanced Installation Guide*의 네트워크 설치 서버 구성 관련 내용을 보완합니다.

네트워크 설치 서버에서 첫번째 Solaris 블레이드를 시동한 후에는 블레이드에서 사용할 응용 프로그램 소프트웨어를 추가할 수 있습니다. 그런 다음 *Solaris Advanced Installation Guide*의 지침에 따라 Web Start Flash 아카이브를 생성합니다.

Sun Fire B1600 블레이드 시스템 섀시에 있는 Sun Fire B100s Solaris 서버 블레이드의 Web Start Flash 아카이브를 사용하여 한 블레이드의 운영 환경 및 응용 프로그램 소프트웨어를 다른 블레이드로 복제할 수 있습니다.

본 부록은 다음 단원으로 구성되어 있습니다.

D.1 Web Start Flash 아카이브를 사용한 신속한 블레이드 구성

Flash 아카이브는 Solaris 시스템의 스냅샷입니다. 따라서 해당 시스템의 모든 파일, 더 정확히 말하자면 사용자가 지정한 모든 파일을 포함합니다. 블레이드에 모든 소프트웨어를 설치한 후 해당 블레이드를 사용하기 전에 Flash 아카이브를 생성해야 합니다. 관련 소프트웨어와 그 사용 목적에 따라, 해당 소프트웨어를 설치한 후 그 소프트웨어를 구성하기 전에 Flash 아카이브를 생성해야 할 경우도 있습니다. 예를 들어, 데이터베이스 관리 소프트웨어의 경우, 소프트웨어를 설치한 후 데이터베이스를 만들기 전에 생성한 Flash 아카이브가 데이터베이스 서버에 필요합니다.

블레이드에서 어떤 소프트웨어 응용 프로그램을 사용할 것인지 아직 모르는 경우에도, Web Start Flash 아카이브를 사용하여 Solaris를 여러 블레이드에 복제할 수 있습니다. 이 방식이 개별적으로 점프스타트를 수행하는 것 보다 더 빠릅니다.

D.1.1 Web Start Flash 아카이브 생성

블레이드에 있는 소프트웨어의 Flash 아카이브를 생성하려면 *Solaris Advanced Installation Guide*에 나온 Flash 아카이브 생성 지침을 따르십시오.

D.1.2 다른 블레이드에 아카이브 이미지 설치

다른 블레이드에 아카이브 이미지를 설치하려면 *Solaris Advanced Installation Guide*에 나온 Flash 아카이브 설치 지침을 따르십시오.

D.1.3 Web Start Flash 아카이브 설치 능률 향상시키기

Web Start Flash 아카이브 설치 능률을 향상시키기 위해 서버 블레이드간의 기가비트 연결을 활용할 수 있습니다.

이렇게 하려면 생성한 Flash 아카이브의 위치를 NFS를 사용하여 공유해야 합니다. 즉, 첫번째 블레이드의 소프트웨어 아카이브 이미지를 공유합니다. 아래 지침을 수행하십시오.

1. **이미지를 복제할 블레이드의 Solaris 프롬프트에서 다음을 입력합니다.**

```
#share -F ufs flash location
```

여기서 *flash location*은 블레이드 Flash 아카이브의 위치입니다. 예를 들면 다음과 같습니다.

```
#share -F ufs /var/tmp
```

2. **네트워크 설치 서버에서 설치 프로파일을 수정하여 첫번째 블레이드의 Flash 아카이브 위치를 가리키게 합니다.**

부록 **E**

시스템 컨트롤러 명령

본 부록에는 시스템 컨트롤러의 sc> 프롬프트에서 사용할 수 있는 명령들이 나와 있습니다.

본 부록은 다음 단원으로 구성되어 있습니다.

E.1 전체 섀시에 대한 전원 설정 명령

참고 – 활성 시스템 컨트롤러를 제외한 모든 구성 부품의 전원을 한번에 끄거나 제거 가능 또는 대기 상태로 전원을 다운시킬 수 있습니다. 블레이드 시스템 섀시는 단일 명령으로 활성 시스템 컨트롤러의 전원을 끄거나 다운시킬 수 없도록 되어 있습니다. 활성 시스템 컨트롤러의 전원을 끄는 방법은 *Sun Fire B1600 블레이드 시스템 섀시 관리 안내서*를 참조하십시오.

표 E-1 모든 구성 부품의 전원 켜기/끄기/다운 명령

명령 및 옵션(있을 경우)	실행 작업
`sc> poweron ch`	모든 구성 부품의 전원을 켭니다. 이 명령을 사용하여 전원 다운, 제거 가능 또는 대기 전원 상태에서 한 번에 모든 구성 부품의 전원을 복원할 수 있습니다.
`sc> poweroff ch`	활성 시스템 컨트롤러를 제외하고 섀시의 모든 구성 부품의 전원을 끕니다.
`sc> poweroff -f ch`	구성 부품의 운영 체제가 정상적으로 종료하지 못했을 경우에도 활성 시스템 컨트롤러를 제외한 모든 구성 부품의 전원을 끕니다.
`sc> poweroff -y ch`	전원을 끌 것인지 묻는 메시지를 표시하지 않고 활성 시스템 컨트롤러를 제외한 모든 구성 부품의 전원을 끕니다.
`sc> poweroff -s ch`	활성 시스템 컨트롤러를 제외한 모든 구성 부품의 전원을 대기 모드로 다운시킵니다(standbyfru ch 명령과 동일).
`sc> poweroff -r ch`	활성 시스템 컨트롤러를 제외한 모든 구성 부품의 전원을 해당 구성 부품을 안전하게 제거할 수 있는 상태로 다운시킵니다. 또한 -r 옵션은 각 구성 부품의 "제거 가능" LED를 켭니다(removefru ch 명령과 동일).
`sc> standbyfru ch`	활성 시스템 컨트롤러를 제외한 모든 구성 부품의 전원을 대기 모드로 다운시킵니다(poweroff -s ch 명령과 동일).
`sc> standbyfru -f ch`	구성 부품의 운영 체제가 정상적으로 종료하지 못했을 경우에도 활성 시스템 컨트롤러를 제외한 모든 구성 부품의 전원을 대기 모드로 다운시킵니다.

표 E-1 모든 구성 부품의 전원 켜기/끄기/다운 명령

명령 및 옵션(있을 경우)	실행 작업
`sc> standbyfru -y ch`	전원을 다운시킬지 묻는 메시지를 표시하지 않고 활성 시스템 컨트롤러를 제외한 모든 구성 부품의 전원을 대기 모드로 다운시킵니다.
`sc> removefru ch`	활성 시스템 컨트롤러를 제외한 모든 구성 부품의 전원을 해당 구성 부품을 안전하게 제거할 수 있는 상태로 다운시킵니다. 또한 이 명령은 각 구성 부품의 "제거 가능" LED를 켭니다(`poweroff -r ch` 명령과 동일).
`sc> removefru -f ch`	시스템 컨트롤러의 운영 체제가 정상적으로 종료하지 못했을 경우에도, 활성 시스템 컨트롤러를 제외한 모든 구성 부품의 전원을 해당 구성 부품을 안전하게 제거할 수 있는 상태로 다운시킵니다. 이 명령은 또한 각 구성 부품의 "제거 가능" LED를 켭니다.
`sc> removefru -y ch`	활성 시스템 컨트롤러를 제외한 모든 구성 부품의 전원을 해당 구성 부품을 안전하게 제거할 수 있는 상태로 다운시킵니다. 하지만 전원을 다운시킬지 묻는 메시지는 표시하지 않습니다. 이 명령은 또한 각 구성 부품의 "제거 가능" LED를 켭니다.

E.2 시스템 컨트롤러의 전원 설정 명령

참고 – 대기 시스템 컨트롤러만 전원을 끄거나 다운시킬 수 있습니다. 활성 시스템 컨트롤러의 전원을 끄는 방법은 *Sun Fire B1600 블레이드 시스템 섀시 관리 안내서*를 참조하십시오.

표 E-2 SSC 전원 켜기/끄기/다운 명령

명령 및 옵션(있을 경우)	실행 작업
`sc> poweron sscn`	SSC*n*의 전원을 켭니다(여기서 *n*은 대기 시스템 컨트롤러가 SSC0과 SSC1 중 어디에 속하는지에 따라 0 또는 1로 지정합니다). 이 명령을 사용하여 전원 다운, 제거 가능 또는 대기 전원 상태에서 대기 SSC의 전원을 복원할 수 있습니다.
`sc> poweroff sscn`	SSC*n*의 전원을 끕니다(여기서 *n*은 대기 시스템 컨트롤러가 SSC0과 SSC1 중 어디에 속하는지에 따라 0 또는 1로 지정합니다).
`sc> poweroff -f sscn`	시스템 컨트롤러의 운영 체제가 정상적으로 종료하지 못했을 경우에도 대기 시스템 컨트롤러(SSC0 또는 SSC1)의 전원을 끕니다.
`sc> poweroff -y sscn`	전원을 끌 것인지 묻는 메시지를 표시하지 않고 대기 시스템 컨트롤러(SSC0 또는 SSC1)의 전원을 끕니다.
`sc> poweroff -s sscn`	대기 시스템 컨트롤러(SSC0 또는 SSC1)의 전원을 대기 모드로 다운시킵니다(`standbyfru` 명령과 동일).
`sc> poweroff -r sscn`	대기 시스템 컨트롤러의 전원을 해당 컨트롤러를 안전하게 제거할 수 있는 상태로 다운시킵니다. `-r` 옵션은 또한 "제거 가능" LED를 켭니다(`removefru` 명령과 동일).
`sc> standbyfru sscn`	대기 시스템 컨트롤러의 전원을 대기 모드로 다운시킵니다(`poweroff -s` 명령과 동일).
`sc> standbyfru -f sscn`	시스템 컨트롤러의 운영 체제가 정상적으로 종료하지 못했을 경우에도 대기 시스템 컨트롤러의 전원을 대기 모드로 다운시킵니다.
`sc> standbyfru -y sscn`	전원을 다운시킬지 묻는 메시지를 표시하지 않고 대기 시스템 컨트롤러의 전원을 대기 모드로 다운시킵니다.

표 E-2 SSC 전원 켜기/끄기/다운 명령

명령 및 옵션(있을 경우)	실행 작업
`sc> removefru sscn`	대기 시스템 컨트롤러의 전원을 해당 컨트롤러를 안전하게 제거할 수 있는 상태로 다운시킵니다. 이 명령은 또한 SSC 후면 패널의 "제거 가능" LED를 켭니다(`poweroff -r` 명령과 동일).
`sc> removefru -f sscn`	시스템 컨트롤러의 운영 체제가 정상적으로 종료하지 못했을 경우에도, 대기 시스템 컨트롤러의 전원을 해당 컨트롤러를 안전하게 제거할 수 있는 상태로 다운시킵니다. 이 명령은 또한 SSC 후면 패널의 "제거 가능" LED를 켭니다.
`sc> removefru -y sscn`	대기 시스템 컨트롤러의 전원을 해당 컨트롤러를 안전하게 제거할 수 있는 상태로 다운시킵니다. 그러나 전원을 다운시킬지 묻는 메시지는 표시하지 않습니다. 이 명령은 또한 SSC 후면 패널의 "제거 가능" LED를 켭니다.

E.3 서버 블레이드 전원 설정 명령

표 E-3 서버 블레이드 전원 켜기/끄기/다운 명령

명령 및 옵션(있을 경우)	실행 작업
`sc> poweron s`*n*	슬롯 *n*의 블레이드 전원을 켭니다. 이 명령을 사용하여 전원 다운, 제거 준비 또는 대기 전원 상태에서 블레이드의 전원을 복원합니다.
`sc> poweroff s`*n*	슬롯 *n*의 블레이드 전원을 끕니다.
`sc> poweroff -f s`*n*	시스템 컨트롤러의 운영 체제가 정상적으로 종료하지 못했을 경우에도 슬롯 *n*의 블레이드 전원을 끕니다.
`sc> poweroff -y s`*n*	전원을 끌 것인지 묻는 메시지를 표시하지 않고 슬롯 *n*의 블레이드 전원을 끕니다.
`sc> poweroff -s s`*n*	슬롯 *n*의 블레이드 전원을 대기 모드로 다운시킵니다 (`standbyfru` 명령과 동일).
`sc> poweroff -r s`*n*	슬롯 *n*의 블레이드 전원을 해당 블레이드를 안전하게 제거할 수 있는 상태로 다운시킵니다. -r 옵션은 또한 블레이드 전면의 파란색 "제거 가능" LED를 켭니다(`removefru` 명령과 동일).
`sc> standbyfru s`*n*	슬롯 *n*의 블레이드 전원을 대기 모드로 다운시킵니다 (`poweroff -s` 명령과 동일).
`sc> standbyfru -f s`*n*	블레이드의 운영 체제가 정상적으로 종료하지 못했을 경우에도 슬롯 *n*의 블레이드 전원을 대기 모드로 다운시킵니다.
`sc> standbyfru -y s`*n*	전원을 다운시킬지 묻는 메시지를 표시하지 않고 슬롯 *n*의 블레이드 전원을 대기 모드로 다운시킵니다.

표 E-3 서버 블레이드 전원 켜기/끄기/다운 명령

명령 및 옵션(있을 경우)	실행 작업
`sc> removefru s`*n*	슬롯 *n*의 블레이드 전원을 해당 블레이드를 안전하게 제거할 수 있는 상태로 다운시킵니다. 이 명령은 또한 블레이드 전면의 파란색 "제거 가능" LED를 켭니다(`poweroff -r` 명령과 동일).
`sc> removefru -f s`*n*	슬롯 *n*의 블레이드 전원을 해당 블레이드를 안전하게 제거할 수 있는 상태로 다운시킵니다. 이 명령은 블레이드의 운영 체제가 정상적으로 종료하지 못했을 경우에도 해당 블레이드의 전원을 다운시킵니다. 이 명령은 또한 블레이드 전면의 파란색 "제거 가능" LED를 켭니다.
`sc> removefru -y s`*n*	슬롯 *n*의 블레이드 전원을 해당 블레이드를 안전하게 제거할 수 있는 상태로 다운시킵니다. 하지만 전원을 다운시킬지 묻는 메시지는 표시하지 않습니다. 이 명령은 또한 블레이드 전면의 파란색 "제거 가능" LED를 켭니다.

E.4 시스템 컨트롤러, 스위치 및 블레이드 재설정 명령

표 E-4 시스템 섀시 구성 부품 재설정 명령

명령 및 옵션(있을 경우)	실행 작업
`sc> reset s`*n*	슬롯 *n*의 서버 블레이드를 재설정합니다.
`sc> reset s`*n* `s`*y*	슬롯 *n* 및 *y*의 서버 블레이드를 재설정합니다. 재설정할 블레이드는 공백으로 구분하여 지정합니다.
`sc> reset -y s`*n*	블레이드를 재설정할지 묻는 메시지를 표시하지 않고 슬롯 *n*의 블레이드를 재설정합니다.
`sc> reset -x s`*n*	슬롯 *n*의 블레이드에 대해 외부 실행 재설정을 수행합니다.
`sc> reset ssc`*n*`/swt`	SSC*n*의 스위치를 재설정합니다. 여기서 *n*은 0 또는 1로 지정합니다.
`sc> reset -y ssc`*n*`/swt`	스위치를 재설정할지 묻는 메시지를 표시하지 않고 SSC*n*의 스위치를 재설정합니다.
`sc> reset -x ssc`*n*`/swt`	SSC*n*의 스위치에 대해 외부 실행 재설정을 수행합니다.
`sc> reset ssc`*n*`/sc`	대기 시스템 컨트롤러를 재설정합니다. 여기서 n은 대기 시스템 컨트롤러가 SSC0과 SSC1 중 어디에 속하는지에 따라 0 또는 1로 지정합니다.
`sc> reset -f ssc`*n*`/sc`	정상적으로 운영 체제를 종료할 수 없는 경우에도 대기 시스템 컨트롤러를 강제로 재설정합니다. 여기서 *n*은 대기 시스템 컨트롤러가 SSC0 또는 SSC1 중 어디에 속하는가에 따라 0 또는 1로 지정합니다. 이 명령을 실행할 경우 해당 SSC 장치 내의 스위치도 재설정됩니다.
`sc> resetsc`	활성 시스템 컨트롤러를 재설정합니다. 어느 쪽 스위치도 이 재설정 명령으로 영향을 받지는 않습니다. 이 명령을 사용하여 시스템 컨트롤러를 재설정할 경우 현재 사용자 세션이 닫힙니다.
`sc> reset ssc`*n*	대기 시스템 컨트롤러(*n*은 활성 시스템 컨트롤러로 지정할 수 없음), 두 스위치, 그리고 섀시에 설치된 모든 서버 블레이드를 재설정합니다.
`sc> resetsc -y`	시스템 컨트롤러를 재설정할지 묻는 메시지를 표시하지 않고 활성 시스템 컨트롤러를 재설정합니다.

표 E-4 시스템 섀시 구성 부품 재설정 명령

명령 및 옵션(있을 경우)	실행 작업
`sc> break s`*n*	Solaris가 실행 중일 때 `break` 명령을 실행할 경우, Solaris가 부팅된 모드에 따라 블레이드가 Solaris에서 kadb 또는 OBP로 전환됩니다(Solaris가 이 방식으로 Break를 처리하도록 구성된 경우).
`sc> break -y s`*n*	위 설명과 동일하며, 다만 -y 옵션은 `break` 명령을 실행할지 묻는 메시지를 표시하지 않도록 지정합니다.
`sc> break s`*n* *s*y *s*x	위 설명과 동일하며, 다만 이 명령은 블레이드 *n*, *y*, *x*에 대해 break 명령을 적용합니다.

E.5 상태 점검 명령

표 E-5 섀시와 그 구성 부품에 대한 상태 점검 명령

명령 및 옵션(있을 경우)	실행 작업
`showsc [-v]`	활성 시스템 컨트롤러의 구성을 요약하여 표시합니다.
`showplatform [-v]`	각 구성 부품의 상태(정상, 고장, 없음)를 표시합니다. 또한 섀시에 있는 모든 도메인(시스템 컨트롤러, 스위치 및 블레이드)의 운영 체제 작동 상태도 표시합니다. -v 옵션을 사용하면 각 구성 부품의 기본 MAC 주소와 일련 번호도 표시됩니다.
`showenvironment [-v] {[sscn][psn][sn]}`	섀시 내 여러 구성 부품의 환경 센서의 상태를 표시합니다. 예를 들어, 이 명령은 구성 부품의 내부 온도, 팬 속도 및 전원 공급 라인의 전류 수준을 알려줍니다.
`showfru [-g] {sscn|sn|ch|psn}`	지정한 구성 부품(또는 모든 구성 부품)의 FRUID 데이터베이스의 내용을 표시합니다. 각 구성 부품은 자신에 대한 다양한 정보를 유지관리합니다. 여기에는 고정 데이터(예: 하드웨어 버전 정보)와 동적 데이터(예: 구성 부품이 최근 생성한 이벤트 메시지)가 포함됩니다. -g 옵션을 사용하면 지정한 행 수만큼 출력이 표시되고 화면이 잠시 멈춥니다.
`showdate`	시스템 컨트롤러의 현재 날짜 및 시간을 UTC 형식으로 표시합니다.
`showlogs [-b]|[-e] [-g] [-v] {sscn|sn}`	지정한 블레이드, 스위치 또는 시스템 컨트롤러에 대하여 기록된 이벤트를 표시합니다. 처음 *n*개의 이벤트를 보려면 -b 옵션을 지정하고, 마지막 *n*개의 이벤트를 보려면 -e 옵션을 지정하고, 지정한 행 수의 출력을 표시하고 화면을 잠시 멈추려면 -g 옵션을 지정하고, 로그의 모든 이벤트를 보려면 -v 옵션을 지정합니다.
`showlocator`	위치 탐지기 LED가 켜졌는지 또는 꺼졌는지 여부를 알려줍니다.

표 E-5 섀시와 그 구성 부품에 대한 상태 점검 명령

명령 및 옵션(있을 경우)	실행 작업
`consolehistory [-b]|[-e] [-g] [boot|run] sscn/swt|sn`	스위치 콘솔 또는 블레이드 콘솔의 부트 타임 버퍼 또는 런타임 버퍼의 내용을 표시합니다. 해당 정보의 처음 *n* 행을 보려면 -b 옵션을 지정하고, 마지막 *n* 행을 보려면 -e 옵션을 지정하고, 지정한 행 수의 출력을 표시하고 화면을 잠시 멈추려면 -g 옵션을 지정합니다.
`showusers`	시스템 컨트롤러에 현재 로그인한 사용자의 목록을 표시합니다.
`usershow [`*username*`]`	지정한 사용자의 로그인 계정에 대한 세부 정보를 보여줍니다. 사용자를 지정하지 않을 경우 모든 사용자 계정에 대한 세부 정보를 보여줍니다. 출력에는 사용자의 권한과 암호 유무 여부가 표시됩니다.

E.6 시스템 컨트롤러 구성 명령

표 E-6 시스템 컨트롤러 구성 명령

명령 및 옵션(있을 경우)	실행 작업
`setupsc`	대화식으로 활성 시스템 컨트롤러를 구성합니다. (비대화식으로 구성할 수 있는 방법은 없습니다.) 대기 시스템 컨트롤러는 자동으로 활성 컨트롤러와 동일한 구성을 사용합니다.
`flashupdate -s` *IP address* `-f` *path* `[-v] ssc`*n*`|s`*n*	시스템 컨트롤러 또는 서버 블레이드의 펌웨어를 업그레이드합니다. IP address는 펌웨어가 저장되어 있는 TFTP 서버의 IP 주소입니다. Path는 TFTP 서버에서 펌웨어의 위치를 나타내는 경로입니다. -v 옵션을 지정하면 업그레이드 수행 시 상세한 진행 과정을 표시합니다.
`setfailover`	어느 것이 활성 시스템 컨트롤러이고 어느 것이 대기 시스템 컨트롤러인지 알려줍니다. 또한 대기 시스템 컨트롤러와 활성 시스템 컨트롤러의 역할을 강제로 서로 바꿀 것인지 여부를 묻는 메시지를 표시합니다. 활성 시스템 컨트롤러가 어느 것인지 알기 위해 명령을 사용한 경우에는 "아니요"라고 대답하면 됩니다.
`setdefaults [-y]`	대기 시스템 컨트롤러(스위치는 제외)를 공장 출하시 기본 설정으로 되돌립니다. -y 옵션을 지정하면 SSC를 출하시 기본 설정으로 되돌릴지 여부를 묻지않고 명령을 수행합니다.
`setdate [`*mmdd*`]`*HHMM*`[.`*SS*`]|` *mmddHHMM*`[`*cc*`]`*yy*`[.`*SS*`]`	시스템 컨트롤러, 스위치 및 현재 설치된 모든 서버 블레이드의 날짜 및 시간을 설정합니다. 날짜 및 시간을 설정할 때는 국제 표준시(UTC)를 사용해야 합니다. Solaris 서버 블레이드는 UTC에서 시간을 상쇄하여 해당 시간대에 맞춰 현지 시간을 계산합니다. 그리고 블레이드는 UTC 시간을 시스템 컨트롤러로부터 가져옵니다. 변수는 다음과 같습니다. *mm* - 월(2자리수) *dd* - 일(2자리수) *HH* - 시(2자리수) *MM* - 분(2자리수) *SS* - 초(2자리수)
`setlocator on|off`	섀시의 위치 탐지기 LED를 켜거나 끕니다.

E.7 스위치 및 블레이드 관련 명령

참고 – 스위치 콘솔 또는 블레이드 콘솔 위치에 있을 때 활성 시스템 컨트롤러의 sc> 프롬프트로 돌아가려면 **#.**을 입력하십시오.

표 E-7 스위치 및 블레이드 액세스/구성 명령

명령 및 옵션(있을 경우)	실행 작업
`console [-f]|[[-r] sscn/swt|sn`	스위치 또는 블레이드의 콘솔에 액세스합니다. 현재 로그인되어 있는 다른 모든 사용자를 "읽기 전용" 모드로 강제 전환하려면 `-f` 명령을 사용합니다. "읽기 전용" 모드로 로그인하려면 `-r` 명령을 사용합니다.
`consolehistory [-b]|[-e] [-g] [boot|run] sscn/sc|sscn/swt|sn`	지정한 시스템 컨트롤러, 스위치 또는 블레이드의 콘솔에 있는 부트 타임 버퍼 또는 런 타임 버퍼의 내용을 표시합니다. 해당 정보의 처음 *n* 행을 보려면 `-b` 옵션을 지정하고, 마지막 *n* 행을 보려면 `-e` 옵션을 지정하고, 지정한 행 수의 정보를 표시하고 화면을 잠시 멈추려면 `-g` 옵션을 지정합니다.
`bootmode reset_nvram|diag|skip_diag|normal|bootscript="string" sn {sn}`	이 명령은 블레이드의 부트 모드를 지정합니다. 자세한 내용은 *Sun Fire B1600 섀시 관리 안내서*를 참조하십시오.
`flashupdate -s` *IP address* `-f` *path* `[-v] sscn|sn`	활성 시스템 컨트롤러 또는 서버 블레이드의 펌웨어를 업그레이드합니다. *IP address*는 펌웨어가 저장되어 있는 TFTP 서버의 IP 주소입니다. *Path*는 TFTP 서버에서 펌웨어의 위치를 나타내는 경로입니다. `-v` 옵션을 사용하면 업그레이드 수행시 상세한 진행 과정을 표시합니다.

E.8 사용자 계정 관리 명령

표 E-8 사용자 계정 관리 명령

명령 및 옵션(있을 경우)	실행 작업
useradd *username*	승인된 시스템 컨트롤러 사용자 목록에 새 사용자를 추가합니다.
userdel *username*	승인된 시스템 컨트롤러 사용자 목록에서 사용자를 삭제합니다.
userpassword *username*	이 명령은 a-레벨 권한을 가진 사용자가 다른 사용자의 암호를 변경할 때 사용됩니다.
password	이 명령은 사용자가 자신의 암호를 변경할 때 사용됩니다. 즉, 현재 로그인한 계정의 사용자 암호를 변경합니다.
userperm *username* [a][u][c][r]	이 명령은 사용자의 권한 레벨을 지정합니다. c 옵션은 블레이드 및 스위치에 대한 콘솔 액세스 권한을 부여하고, a 옵션은 관리자 권한을 부여하고(해당 사용자가 시스템 컨트롤러의 구성을 변경할 수 있게 됩니다.), u 옵션은 사용자 관리 권한을 부여하고(해당 사용자가 다른 사용자의 계정을 관리할 수 있게 됩니다.), r 옵션은 재설정 권한을 부여합니다(해당 사용자가 섀시의 구성 부품을 재설정하거나 구성 부품의 전원을 끄고 켤 수 있게 됩니다).
usershow [*username*]	지정한 사용자의 로그인 계정에 대한 세부 정보를 보여줍니다. 사용자를 지정하지 않을 경우에는 모든 사용자 계정에 대한 세부 정보를 보여줍니다. 출력에는 사용자의 권한과 암호 유무 여부가 표시됩니다.
showusers	현재 시스템 컨트롤러에 로그인한 모든 사용자를 나열합니다.

부록 **F**

활성 및 대기 시스템 컨트롤러

본 부록에서는 새시의 활성 시스템 컨트롤러와 대기 시스템 컨트롤러간의 관계에 대한 자세한 설명이 제공됩니다. 또한 이 관계의 한계성에 대해서도 설명합니다.

F.1 장애 복구 기능이 수행되는 경우

블레이드 시스템 섀시에는 두 개의 시스템 컨트롤러가 있습니다. 한번에 한 개의 컨트롤러만 작동하기 때문에 ALOM 명령행 인터페이스를 사용하여 하나의 컨트롤러에만 액세스할 수 있습니다. 그러나 나머지 시스템 컨트롤러가 활동하지 않는 상태(즉, 대기 모드)에 있더라도 해당 컨트롤러의 스위치는 계속 활동 중입니다. 또한 다음의 경우 대기 시스템 컨트롤러는 활성 시스템 컨트롤러의 역할을 대신 수행할 수 있습니다.

- 활성 시스템 컨트롤러를 제거했을 경우
- 활성 시스템 컨트롤러의 시스템 컨트롤러 소프트웨어 응용 프로그램에 심각한 오류가 발생했거나 치명적인 하드웨어 장애가 발생했을 경우
- 시스템 컨트롤러간에 역할을 상호 전환하도록 사용자가 강제로 setfailover 명령을 실행했을 경우

F.2 대기 시스템 컨트롤러의 역할

대기 시스템 컨트롤러의 기본 소프트웨어 응용 프로그램은 작동하지 않는 상태에 있지만 그래도 대기 시스템 컨트롤러는 다음과 같은 작업을 수행합니다.

- 활성 시스템 컨트롤러의 상태를 모니터링하고 있다가 활성 시스템 컨트롤러가 제거되었을 경우, 기본 소프트웨어 응용 프로그램에 오류가 발생했을 경우, 하드웨어에 치명적인 장애가 발생했을 경우, 또는 활성 시스템 컨트롤러에 대해 `setfailover` 명령이 수행되었을 경우에 활성 시스템 컨트롤러의 역할을 대신 떠맡습니다.
- 사용자가 활성 시스템 컨트롤러에 `setupsc` 명령을 수행하면서 지정한 구성 매개변수를 수신합니다. 이렇게 해둠으로써 대기 시스템 컨트롤러는 필요시 투명하게 활성 시스템 컨트롤러의 역할을 떠맡을 수 있습니다.
- 모든 이벤트 메시지를 수신하여 대기 시스템 컨트롤러의 이벤트 로그를 항상 최신 상태로 유지합니다.
- 대기 시스템 컨트롤러와 같은 SSC 모듈에 있는 스위치에 대해 활성 시스템 컨트롤러에서 콘솔 연결을 수행할 수 있게 해줍니다. (어떠한 이유로든 대기 시스템 컨트롤러의 시동이 중단된 경우, 대기 시스템 컨트롤러는 연결된 스위치에 대한 콘솔 연결을 제공할 수 없습니다.)

- 섀시 전체에서 사용자 로그인 정보 및 호스트 ID 정보의 무결성을 유지하도록 지원합니다. 호스트 ID 정보는 서버 블레이드에서 사용되며 사용자 로그인 정보는 시스템 컨트롤러에서 사용됩니다. 이 두 정보는 주로 중앙판에 저장되나 두 시스템 컨트롤러도 이러한 정보의 유지관리에 관여합니다.

  사용하던 섀시에 새 SSC(공장 출하시 초기 설정 상태)를 설치할 경우 새 SSC는 현재 중앙판에 저장되어 있는 사용자 로그인 정보와 호스트 ID 정보를 그대로 상속합니다.

  그 반대의 경우, 즉 섀시는 새 것이고(따라서 해당 사용자 로그인 정보와 호스트 ID 정보가 구성되지 않음) SSC는 사용하던 것일 경우 중앙판은 시스템 컨트롤러에서 사용자 로그인 정보와 호스트 ID 정보를 가져옵니다.

  그러나 SSC를 섀시에 설치할 때 둘 다 사용자 로그인 정보와 호스트 ID 정보를 갖고있는 경우, SSC와 섀시가 갖고있는 정보 중 어느 하나라도 서로 다르다면 결과를 예상하기가 힘들어집니다. 이 경우 대기 시스템 컨트롤러가 있다면 중재자 역할을 떠맡게 됩니다. 대기 시스템 컨트롤러는 자신의 사용자 로그인 정보와 호스트 ID 정보를 활성 시스템 컨트롤러가 속한 SSC의 정보 및 중앙판의 정보와 비교합니다. 대기 시스템 컨트롤러의 호스트 ID 정보가 활성 SSC 또는 중앙판에 저장된 정보 중 하나와 일치할 경우 일치하는 정보가 사용됩니다. 마찬가지로 대기 시스템 컨트롤러의 사용자 로그인 정보가 활성 SSC 또는 중앙판에 저장된 정보 중 하나와 일치할 경우 일치하는 정보가 사용됩니다. 두 경우 모두, 대기 시스템 컨트롤러의 정보가 활성 SSC의 정보와 중앙판의 정보 어느 것과도 일치하지 않을 경우 중앙판의 정보가 사용됩니다.

F.3 두 시스템 컨트롤러간의 장애 복구 관계의 한계성

장애 복구 프로세스가 진행되는 동안 서버 블레이드나 스위치의 실행에는 아무런 영향도 미치지 않습니다. 그렇지만 다음 사항을 유념해둘 필요가 있습니다.

- 하나의 시스템 컨트롤러가 다른 시스템 컨트롤러의 역할을 넘겨받을 때 일시적으로(약 15초 정도) 섀시는 활성 시스템 컨트롤러가 없는 상태가 됩니다. 장애 복구 프로세스에 따라 두 시스템 컨트롤러가 모두 재설정되기 때문에 이와 같은 현상이 발생합니다. 그 결과로, 장애 복구 중에는 콘솔 로그가 수집되지 않으며, 새 활성 시스템 컨트롤러에 로그인했을 때 양 시스템 컨트롤러의 이벤트 로그는 비어있게 됩니다.

  장애 복구 프로세스가 진행되는 동안에는 시스템 컨트롤러를 통해 섀시의 구성 부품을 관리하는 것이 불가능합니다. 그러나 스위치 또는 블레이드에 텔넷 연결하거나 스위치의 웹 기반 그래픽 사용자 인터페이스를 사용하는 것은 가능합니다.

  장애 복구 프로세스가 진행되는 중에는 또한 섀시 구성 부품의 펌웨어를 업그레이드하는 작업은 수행할 수 없습니다. 그러므로 시스템 컨트롤러 펌웨어를 업그레이드하려면 업그레이드할 시스템 컨트롤러를 활성 컨트롤러로 설정해야 합니다(현재 활성 시스템 컨트롤러의 sc> 프롬프트에서 `setfailover` 명령을 수행하여).

- 대기 시스템 컨트롤러에는 텔넷 연결이 허용되지 않습니다. 대신 별칭 IP 주소를 사용하십시오. 그러나 장애 복구를 위해 한 시스템 컨트롤러에서 다른 시스템 컨트롤러로 활성 컨트롤러가 전환되면 텔넷 연결이 끊어지게 됨에 유의하십시오.

색인

T

U

V

W