SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers

XSCF User's Guide

Part No.: E25381-01,
Manual Code: C120-E332-11EN
January 2012

Disclaimer: The only warranties granted by Oracle and Fujitsu Limited, and/or any affiliate of either of them in connection with this document or any product or technology described herein are those expressly set forth in the license agreement pursuant to which the product or technology is provided. EXCEPT AS EXPRESSLY SET FORTH IN SUCH AGREEMENT, ORACLE OR FUJITSU LIMITED, AND/OR THEIR AFFILIATES MAKE NO REPRESENTATIONS OR WARRANTIES OF ANY KIND (EXPRESS OR IMPLIED) REGARDING SUCH PRODUCT OR TECHNOLOGY OR THIS DOCUMENT, WHICH ARE ALL PROVIDED AS IS, AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. Unless otherwise expressly set forth in such agreement, to the extent allowed by applicable law, in no event shall Oracle or Fujitsu Limited, and/or any of their affiliates have any liability to any third party under any legal theory for any loss of revenues or profits, loss of use or data, or business interruptions, or for any indirect, special, incidental or consequential damages, even if advised of the possibility of such damages.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Avis de non-responsabilité : les seules garanties octroyées par Oracle et Fujitsu Limited et/ou toute société affiliée de l'une ou l'autre entité en rapport avec ce document ou tout produit ou toute technologie décrits dans les présentes correspondent aux garanties expressément stipulées dans le contrat de licence régissant le produit ou la technologie fournis. SAUF MENTION CONTRAIRE EXPRESSÉMENT STIPULÉE DANS CE CONTRAT, ORACLE OU FUJITSU LIMITED ET LES SOCIÉTÉS AFFILIÉES À L'UNE OU L'AUTRE ENTITÉ REJETTENT TOUTE REPRÉSENTATION OU TOUTE GARANTIE, QUELLE QU'EN SOIT LA NATURE (EXPRESSE OU IMPLICITE) CONCERNANT CE PRODUIT, CETTE TECHNOLOGIE OU CE DOCUMENT, LESQUELS SONT FOURNIS EN L'ÉTAT. EN OUTRE, TOUTES LES CONDITIONS, REPRÉSENTATIONS ET GARANTIES EXPRESSES OU TACITES, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE À LA QUALITÉ MARCHANDE, À L'APTITUDE À UNE UTILISATION PARTICULIÈRE OU À L'ABSENCE DE CONTREFAÇON, SONT EXCLUES, DANS LA MESURE AUTORISÉE PAR LA LOI APPLICABLE. Sauf mention contraire expressément stipulée dans ce contrat, dans la mesure autorisée par la loi applicable, en aucun cas Oracle ou Fujitsu Limited et/ou l'une ou l'autre de leurs sociétés affiliées ne sauraient être tenues responsables envers une quelconque partie tierce, sous quelque théorie juridique que ce soit, de tout manque à gagner ou de perte de profit, de problèmes d'utilisation ou de perte de données, ou d'interruptions d'activités, ou de tout dommage indirect, spécial, secondaire ou consécutif, même si ces entités ont été préalablement informées d'une telle éventualité.

LA DOCUMENTATION EST FOURNIE « EN L'ÉTAT » ET TOUTE AUTRE CONDITION, DÉCLARATION ET GARANTIE, EXPRESSE OU TACITE, EST FORMELLEMENT EXCLUE, DANS LA MESURE AUTORISÉE PAR LA LOI EN VIGUEUR, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE À LA QUALITÉ MARCHANDE, À L'APTITUDE À UNE UTILISATION PARTICULIÈRE OU À L'ABSENCE DE CONTREFAÇON.

Contents

Preface

This manual describes the system monitor and control facility, known as eXtended System Control Facility (XSCF), which is used to control, monitor, operate, and service SPARC Enterprise M3000/M4000/M5000/M8000/M9000 servers and domains from Oracle and Fujitsu.

XSCF may also be referred to as the System Control Facility (SCF). Unless otherwise stated in this manual, the SPARC Enterprise system is described as "the server" or "the system".

Some references to server names and document names are abbreviated for readability. For example, if you see a reference to the M9000 server, note that the full product name is the SPARC Enterprise M9000 server. And if you see a reference to the *XSCF Reference Manual*, note that the full document name is the *SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers XSCF Reference Manual*.

Before reading this document, you should read the overview guide for your server and the *SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers Administration Guide*.

At publication of this document, servers described herein were shipping with XCP 1110 firmware installed. That might no longer be the latest available version, or the version now installed. Always see the Product Notes that apply to the firmware on your server, and those that apply to the latest firmware release.

This chapter includes the following sections:

Audience

This guide is written for experienced system administrators with working knowledge of computer networks and advanced knowledge of the Oracle Solaris Operating System (Oracle Solaris OS).

Related Documentation

All documents for your server are available online at the following locations:

Documentation	Link
Sun Oracle software-related manuals (Oracle Solaris OS, and so on)	`http://www.oracle.com/documentation`
Fujitsu documents	`http://www.fujitsu.com/sparcenterprise/manual/`
Oracle M-series server documents	`http://www.oracle.com/technetwork/documentation/sparc-mseries-servers-252709.html`

The following table lists titles of related documents.

Related SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers Documents
SPARC Enterprise M3000 Server Site Planning Guide
SPARC Enterprise M4000/M5000 Servers Site Planning Guide
SPARC Enterprise M8000/M9000 Servers Site Planning Guide
SPARC Enterprise Equipment Rack Mounting Guide
*SPARC Enterprise M3000 Server Getting Started Guide**
*SPARC Enterprise M4000/M5000 Servers Getting Started Guide**
*SPARC Enterprise M8000/M9000 Servers Getting Started Guide**
SPARC Enterprise M3000 Server Overview Guide
SPARC Enterprise M4000/M5000 Servers Overview Guide
SPARC Enterprise M8000/M9000 Servers Overview Guide
*SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers Important Legal and Safety Information**

Related SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers Documents
SPARC Enterprise M3000 Server Safety and Compliance Guide
SPARC Enterprise M4000/M5000 Servers Safety and Compliance Guide
SPARC Enterprise M8000/M9000 Servers Safety and Compliance Guide
External I/O Expansion Unit Safety and Compliance Guide
SPARC Enterprise M4000 Server Unpacking Guide[*]
SPARC Enterprise M5000 Server Unpacking Guide[*]
SPARC Enterprise M8000/M9000 Servers Unpacking Guide[*]
SPARC Enterprise M3000 Server Installation Guide
SPARC Enterprise M4000/M5000 Servers Installation Guide
SPARC Enterprise M8000/M9000 Servers Installation Guide
SPARC Enterprise M3000 Server Service Manual
SPARC Enterprise M4000/M5000 Servers Service Manual
SPARC Enterprise M8000/M9000 Servers Service Manual
External I/O Expansion Unit Installation and Service Manual
SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers Administration Guide
SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers XSCF User's Guide
SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers XSCF Reference Manual
SPARC Enterprise M4000/M5000/M8000/M9000 Servers Dynamic Reconfiguration (DR) User's Guide
SPARC Enterprise M4000/M5000/M8000/M9000 Servers Capacity on Demand (COD) User's Guide
SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers Product Notes[†]
SPARC Enterprise M3000 Server Product Notes
SPARC Enterprise M4000/M5000 Servers Product Notes
SPARC Enterprise M8000/M9000 Servers Product Notes
External I/O Expansion Unit Product Notes
SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers Glossary

[*] This is a printed document.

[†] Beginning with the XCP 1100 release.

Text Conventions

This manual uses the following fonts and symbols to express specific types of information.

Font/symbol	Meaning	Example
`AaBbCc123`	What you type, when contrasted with on-screen computer output. This font represents the example of command input in the frame.	`XSCF>` **`adduser jsmith`**

`AaBbCc123`	The names of commands, files, and directories; on-screen computer output.
	This font represents the example of command output in the frame.
		`XSCF>` **`showuser -p`**
		`User Name:     jsmith`
		`Privileges:    useradm`
		`               auditadm`

Italic	Indicates the name of a reference manual, a variable, or user-replaceable text.	See the *SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers XSCF User's Guide.*
" "	Indicates names of chapters, sections, items, buttons, or menus.	See Chapter 2, "System Features"

Syntax of the Command-Line Interface (CLI)

The command syntax is as follows:

- A variable that requires input of a value must be put in Italics.
- An optional element must be enclosed in [].
- A group of options for an optional keyword must be enclosed in [] and delimited by `|`.

Documentation Feedback

If you have any comments or requests regarding this document, go to the following websites:

- For Oracle users:

`http://www.oracle.com/goto/docfeedback`

Include the title and part number of your document with your feedback:

SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers XSCF User's Guide, part number E25381-01

- For Fujitsu users:

`http://www.fujitsu.com/global/contact/computing/sparce_index.html`

CHAPTER 1

XSCF Overview

This chapter provides an overview of the system monitoring and control facility (eXtended System Control Facility, or XSCF).

1.1 XSCF Features

The XSCF firmware is a system monitoring and control facility consisting of a dedicated processor (Note 1) that is independent from the system processor. While input power is supplied to the server, the XSCF constantly monitors the server even if no domain is active. The XSCF provides an interface between the user and the server.

The XSCF is the firmware running on the Service Processor in the server. In the rest of this chapter, although XSCF firmware programs are called XSCF firmware, or XSCF, they all have the same meaning. The board with the installed XSCF firmware is called the XSCFU (also referred to as the "XSCF Unit") or Service Processor.

The XSCF uses different functions to achieve high system availability. The XSCF firmware is a single centralized point for the management of hardware configuration, control of hardware monitoring, cooling system (fan units), domain status monitoring, power on and power off of peripheral devices (Note 2), and error monitoring. The XSCF centrally controls and monitors the server. The XSCF also has a partitioning function to configure and control domains, and it has a function to monitor the server through an Ethernet connection so that the user can control the server remotely. Another function is to report failure information to the system administrator and a remote control input/output function.

In the SPARC Enterprise M3000 server (the M3000 server; the entry-level server) and the SPARC Enterprise M4000/M5000 (the M4000/M5000 servers; the midrange servers), a single XSCF Unit is installed in the server. In the SPARC Enterprise M8000/M9000 servers (the M8000/M9000 servers; the high-end servers), two XSCF Units are installed in the server and they are duplicated. Also, in the M3000 server, the XSCF Unit is fixed to the Motherboard Unit (MBU). For details of the server differences, see Section 1.2.1, "Major Differences Among the Server Models" on page 1-14.

Note – (1) Processors on server boards are called CPUs.

Note – (2) Only the system model with a special interface can power on and off the peripheral devices. (See Remote Cabinet Interface (RCI) in External Interfaces.)

Redundant XSCFs (High-End Servers Only)

The high-end servers use a redundant configuration of XSCF Units, thereby providing high system reliability. The XSCF that controls the server is called the Active XSCF or Active XSCF Unit, while the other XSCF acts as a backup and is called the Standby XSCF or Standby XSCF Unit. The Active XSCF and the Standby XSCF monitor each other, and if an error is detected, they determine when a failover switching to Active or Standby should be performed.

External Interfaces

The following connectors (ports) and LEDs act as the external interface of the XSCF Unit. The user, system administrator, and field engineer (FE) can use these ports for server monitoring and XSCF firmware operations:

- One Serial port that can be used for the command-line interface (CLI) (Note 1)
- Two Ethernet ports (XSCF-LAN ports) (10Base-T / 100Base-T (TX))

  CLI and the browser user interface (BUI) can be used with these ports for server monitoring and operations. (Note 1)
- USB port that an FE or a system administrator can use to save and restore hardware information
- Two UPS Controller (UPC) ports to connect the entire system with an Uninterruptible Power Supply Unit (UPS)

  A UPS is connected for backup power control purposes in the event of a power outage. In the M8000/M9000 servers, the UPC interface ports are in the cabinet.

- Remote Cabinet Interface (RCI) port to perform power supply interlock by connecting a system and an I/O device with an RCI device

  The RCI is the power and system control interface that connects a peripheral device with an RCI connector to the server, and performs such functions as power supply interlock and alarm notification and recognition. For the information whether the RCI function is supported on your server, see the *SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers Product Notes*.

- Three types of LEDs that indicate the XSCF Unit status: ACTIVE LED, READY LED, and CHECK LED

  In the M3000/M4000/M5000 servers, there are two types of LEDs: READY LED and CHECK LED.

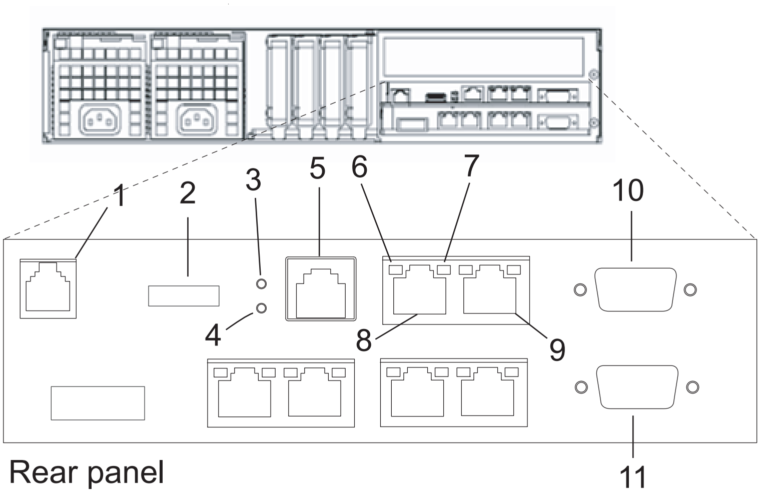
Note – (1) In this manual, XSCF CLI functions are called "XSCF Shell," and XSCF BUI functions are called "XSCF Web".

Rear Panel on the Entry-Level Server

FIGURE 1-1 is an outline drawing of the rear panel of the M3000 server. The XSCF Unit of the M3000 server is not a removable unit but is fixed on the Motherboard unit. The external interface of the XSCF Unit is exposed on a part of rear panel of the server (1 to 11 in FIGURE 1-1).

Of the rear panel of the M3000 server, this section focuses on the external interface which has relevance to XSCF Unit. For details about the other units or interfaces of the rear panel and the mounting location of XSCF Unit, see the *SPARC Enterprise M3000 Server Overview Guide* and the *SPARC Enterprise M3000 Server Service Manual*.

FIGURE 1-1 Outline Drawing of the Rear Panel (In the Entry-level Server)



Number	Description	Number	Description
1	RCI port	7	ACT LED
2	USB port	8	LAN 1 port (XSCF-LAN#1 port)
3	READY LED	9	LAN 0 port (XSCF-LAN#0 port)
4	CHECK LED	10	UPC 1 port
5	Serial port	11	UPC 0 port
6	Link Speed LED		

RCI Port

When connecting a peripheral device with an RCI connector to the server, the RCI port is used for interlocking with a power supply and error monitoring.

Note – To use the RCI function, peripheral devices with the RCI connector and the server on which the RCI function is supported are required. For the information whether the RCI function is supported on your server, see the *SPARC Enterprise M3000/M4000/M5000/M8000/M9000 Servers Product Notes*.

USB Port

The USB port (type A) is used to connect a USB device. The port is compatible with USB 1.1. The port can be used by a system administrator or an FE to save and restore the hardware information, or to collect log data. For the USB handling, see Section 2.3, "Save and Restore XSCF Configuration Information" on page 2-195 and Section 8.2.2, "Method of Collecting the Log Information" on page 8-27.

READY LED

The READY LED lights up in green. When the power supply is turned on, the READY LED blinks. This blinking LED state indicates that the XSCF has been started and is being initialized. When XSCF initialization is completed, the LED stays lit.

CHECK LED

The CHECK LED lights up in orange. While the XSCF is operating normally, the LED remains off. If an abnormality occurs in the XSCF Unit, the CHECK LED turns on. The CHECK LED can set to blink using an XSCF Shell command. This can be used to identify the XSCF Unit even if there is no failure. For details on the LED-related commands of the XSCF Shell, see Chapter 5 and the XSCF Reference Manual.

Note – The Check LED turns on immediately after the server input power is turned on.

Serial Port

The serial port (RS-232C port) uses an RJ-45 connector. The serial port is used with the XSCF Shell to configure server settings and display the server status. An RS-232C serial cross cable is used in the serial port. The connection between the serial port and a PC requires an RJ-45 / RS-232C conversion cable or a conversion connector. For details on serial port connections, see Chapter 3 and the *Installation Guide* for your server.

XSCF-LAN Port (Ethernet Port)

There are two XSCF-LAN ports. Both use an RJ-45 connector and are compatible with 10BASE-T/100BASE-T (TX). The XSCF-LAN ports are used with the XSCF Shell and XSCF Web to perform system administrator operations, output the system status, perform domain operations, and display the console. With a connection between the PC/workstation and LAN, the XSCF-LAN ports are used with the XSCF Shell and XSCF Web by system administrators or FEs to configure the system settings, display the system status, and perform component replacement tasks. For details on using the LAN ports, see Section 1.3, "Types of Connection to XSCF" on page 1-15 and Chapter 3.

Link Speed LED

Located on each of the XSCF-LAN ports, the Link Speed LED is a LAN LED that lights up in green. The Link Speed LED is turned on when a 100-Mbps LAN connection is established, and it is not turned on when a 10-Mbps LAN connection is established.

ACT LED

Located on each of the XSCF-LAN ports, the ACT LED is a LAN LED that lights up in green. When the communication state is Link up, the ACT LED lights up. When the communication state is Link down, the ACT LED light is off. The ACT LED light is off while data is being sent/received though the associated LAN connection. So, the ACT LED looks as if it is blinking.

UPC Port

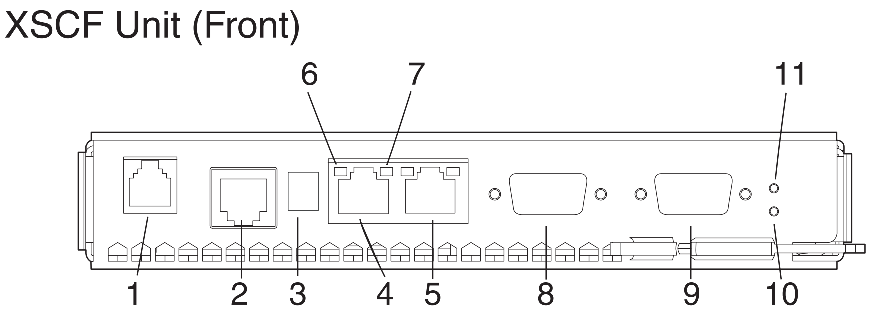
There are two UPC ports. These ports are a connection between the XSCF Unit and the UPS. The UPC port is used only when a UPS is connected. For details on the connectors, see the *Service Manual* for your server.

XSCF Unit Panel (Front) on the Midrange Servers

FIGURE 1-2 is an outline drawing of the XSCF Unit front panel on the M4000/M5000 servers.

The XSCF Unit of the M4000/M5000 servers is a removable unit. In the M4000/M5000 servers, for details on mounting the XSCF Unit, see the *SPARC Enterprise M4000/M5000 Servers Service Manual*.

FIGURE 1-2 Outline Drawing of the XSCF Unit Front Panel (In the Midrange Servers)



Number	Description	Number	Description
1	RCI port	7	ACT LED
2	Serial port	8	UPC#1 port
3	USB port	9	UPC#0 port
4	ETHERNET#1 port (XSCF-LAN#1 port)	10	CHECK LED
5	ETHERNET#0 port (XSCF-LAN#0 port)	11	READY LED
6	Link Speed LED		

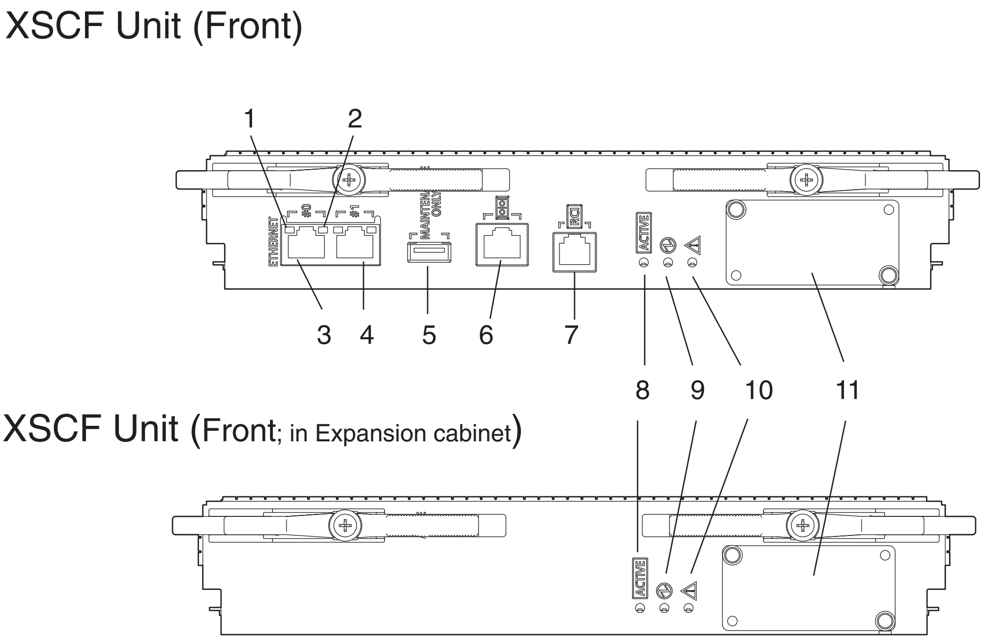
The RCI port, serial port, USB port, XSCF-LAN ports, Link Speed LED, ACT LED, UPC ports, CHECK LED, and READY LED shown in FIGURE 1-2 have the same functions as those of the M3000 server. For descriptions of their functions, see the explanation of FIGURE 1-1.

XSCF Unit Front Panels on the High-End Servers

FIGURE 1-3 includes an outline drawing of the XSCF Unit front panel on the M8000/M9000 servers. For connections between the model and an expansion cabinet, an XSCF Unit as shown at the bottom of FIGURE 1-3 is mounted in the expansion cabinet.

The XSCF Unit of the M8000/M9000 servers is a removable unit. In the M8000/M9000 servers, for details on mounting the XSCF Unit, see the *SPARC Enterprise M8000/M9000 Servers Service Manual*.

FIGURE 1-3 Outline Drawing of the XSCF Unit Front Panel (In High-End Servers)



Number	Description	Number	Description
1	Link Speed LED	7	RCI port
2	ACT LED	8	ACTIVE LED
3	ETHERNET#0 port (XSCF-LAN#0 port)	9	READY LED
4	ETHERNET#1 port (XSCF-LAN#1 port)	10	CHECK LED
5	USB port	11	Connector that connects the XSCF Unit for base cabinet with the XSCF Unit for expansion cabinet
6	Serial port		

The Link Speed LED, ACT LED, XSCF-LAN ports, USB port, serial port, RCI port, READY LED, and CHECK LED shown in FIGURE 1-3 have the same functions as those of the M3000 server. For descriptions of their functions, see the explanation of FIGURE 1-1.

ACTIVE LED

The ACTIVE LED lights up in green. If the XSCF Unit is in a redundant configuration, the ACTIVE LED indicates the active XSCF Unit.

Connector That Connects the XSCF Unit for the Base Cabinet With the XSCF Unit for the Expansion Cabinet

The connector for connecting between XSCF Units is used to connect the Base cabinet to an Expansion cabinet on the M9000 server. Field engineers should connect this connector.

1.2 XSCF Functions

This section describes XSCF functions.

Monitoring the Server Status and RAS Function (Fault Management)

XSCF constantly monitors the server status, so the system can operate with stability. If XSCF detects a system abnormality, it collects a hardware log immediately and analyzes it to locate the fault and determine the failure status by using the Fault Management Architecture (FMA). XSCF displays the status and, if necessary, degrades the faulty parts, degrades the faulty domains, or resets the system to prevent another problem from occurring. XSCF thereby maintains high system reliability, availability, and serviceability (RAS).

XSCF Shell and XSCF Web

XSCF provides the XSCF Shell and XSCF Web that enable the user to display the server status, operate the system, operate domains, and display the console.

XSCF Unit Diagnosis

When the input power is turned on or the XSCF is reset, XSCF performs initial diagnostics for the XSCF itself, checks for abnormalities, displays any detected abnormality, and reports it to the user. While the system is operating, the error detection facility of the XSCF continues to monitor itself, and if any errors are detected, it will report them.

Initial System Configuration Function

XSCF configures the initial hardware settings of the XSCF Unit and initializes hardware as required to start the Oracle Solaris Operating System (Oracle Solaris OS). XSCF also controls the initial system configuration information.

XSCF User Account Control

XSCF controls the user accounts for XSCF operations.

The basic types of user account privileges controlled by XSCF are listed below. The server provides the XSCF Shell and XSCF Web, but their privileges depend on the user privilege (type).

- System administrator
- Domain administrator
- Operator
- Field engineer

For details on the user privileges, see the *Administration Guide*.

Security

XSCF provides an encryption function using Secure Shell (SSH) or Secure Sockets Layer (SSL) and an audit function. Any operation error or unauthorized attempt to access XSCF functionality is recorded in a log. The system administrator can use this information for troubleshooting system errors and unauthorized login attempts.

Power Control for the Server System and Domains

XSCF has power-on and power-off control of the server. The user can press the POWER switch on the operator panel to turn on or off the whole system, or the user can use XSCF to turn on and off the supply of power to the whole system or individual domains.

The user can power on and off the server by using XSCF as follows:

- Power on/off the server or a domain

  The user can turn on, turn off, or reset the server by using the XSCF Shell command from a remote terminal, which is connected to XSCF over a LAN or serial connection. When the user instructs power off, the Oracle Solaris OS is automatically shut down, and then power will be turned off.

- Automatically shut down and cancel a power on operation when an error is detected

  If a system abnormality occurs, the Oracle Solaris OS is automatically shut down, and the subsequent power on will not be started. This can minimize damage to the system.

- Control power during power failure and power restoration

  XSCF performs the following operations when a power failure occurs that causes the system to turn off:

  - When a power failure occurs:

  XSCF performs emergency power off when the power failure occurs. When a UPS is connected, any running domains may also be shut down automatically. For a momentary power failure, XSCF may allow the system to continue working without any shutting down.

  - When power is restored:

  The system can be set up such that XSCF automatically turns on the power to the server, then starts up the domains, relieving the system administrator of extra work.

For details on operation settings for a power failure, see Section 4.4.10, "Shutdown Wait Time Administration" on page 4-23.

Support of Hot-Swapping of Components

XSCF supports maintenance work with the XSCF Shell during hot-swapping of components. For details on the XSCF Shell, see Chapter 5.

Component Configuration Recognition and Temperature/Voltage Monitoring

XSCF monitors component information such as the configuration status and the serial numbers of components in the server. If an abnormality is detected in the component configuration, it is displayed and reported to the user. XSCF periodically monitors and displays the temperature inside the server, the ambient temperature, component temperatures, voltage levels, and FAN status.

Internal Cabinet Configuration, Recognition, and Domain Configuration Control Functions

To use XSCF, you can display the system configuration status, and create and change domain configuration definitions. It also provides domain start and stop functions, mainly for its own use. In the server, the user can configure a domain as a single Physical System Board (PSB) that has CPU, memory, and I/O device, or a PSB logically divided, which are the eXtended System Boards: (XSBs). The user assigns a domain and the Logical System Boards (LSBs) number that can be referenced from the domain to the XSBs for control of the domain configuration. The type of the PSB not logically divided is called Uni-XSB and the type of the PSB logically divided into four is called Quad-XSB.

For details on domain configuration, see the *Overview Guide* for your server and Chapter 2. Also, for each term, see *Glossary*.

Note – In the M3000 server, the domain configuration control function is not available. The M3000 server consists of a single PSB (Uni-XSB) equipped with one CPU, and operates with one domain only. Unlike the M4000/M5000/M8000/M9000 servers, the user cannot configure a domain by logically dividing the PSB.

Dynamic Reconfiguration Function

XSCF supports dynamic system board configuration change operations while the domains are operating. Dynamic reconfiguration (DR) of a domain can be achieved using XSCF. For details on DR, see the *Dynamic Reconfiguration User's Guide*.

Note – In the M3000 server, the DR function is not available.

Console Redirection Function

XSCF provides a function that displays the OS console of the Oracle Solaris OS of each domain. With an SSH (Secure Shell) or telnet connection to XSCF, the user can access the console of any domain in the system. For details on the console, see Chapter 3.

Capacity on Demand Function

Capacity on Demand is an option to purchase spare processing resources (CPUs) for your server. The spare resources are provided in the form of one or more CPUs on COD boards that are installed on your server. When you need the spare processing resources (CPUs) for the server, XSCF assists the operation to add or delete the resources. For details on COD, see the *COD User's Guide*.

Note – In the M3000 server, the COD function is not available.

Functions for Monitoring and Notification During Operation

XSCF constantly monitors the system operating status, FAN status, ambient temperature, etc. Using the network function of the cabinet, XSCF accesses the server to provide the following services:

- Monitoring the server even when the Oracle Solaris OS is inactive.
- Enabling remote operation of the server.
- Reporting error messages by email to specified addresses. For details, see Chapter 6.
- Trapping notification with the SNMP Agent functions. For details, see Chapter 7.

Hardware Fault Information Collection (Hardware Log Collection)

XSCF collects hardware fault information and saves it on the XSCF itself.
The XSCF hardware failure log makes it possible to identify the location of a failure.
The log also provides assistance in anticipating failures on the server and immediately reports precise information about failures to the user.
For details on error messages and their contents, see Appendix A and Appendix B .
The displayed messages types are as follow:

- An initial diagnostic message is displayed at system startup.
- XSCF monitors the network configuration. If an error is detected, an error message is generated and displayed.
- XSCF monitors the status of the power supply, FAN, voltage, system board, memory, CPU, and other components. If an error is detected in a component, an error message is generated and displayed. Based on the error message, the system administrator can easily identify the component that needs to be replaced.
- XSCF monitors the temperatures of the cabinet and CPU. If an abnormal temperature is detected, an error message is generated and displayed. The error messages make it possible to prevent the system from rising to a higher temperature and to prevent system instability.

Firmware Update Function

The web browser and commands can be used to download new firmware image (XSCF firmware and OpenBoot PROM firmware) without stopping the domain and to update firmware without stopping other domains. To complete updating the OpenBoot PROM firmware in the target domain, the domain must be rebooted. For details on updating firmware, see Chapter 8.

1.2.1 Major Differences Among the Server Models

TABLE 1-1 shows the major differences related to XSCF, among the models of the M3000/M4000/M5000/M8000/M9000 servers.

TABLE 1-1 Major Differences Between the Models

Item / Model	**M3000 server (Entry-level)**	**M4000/M5000 servers (Midrange)**	**M8000/M9000 servers (High-end)**
XSCF Unit	Fixed on MBU. Replaceable in units of MBU.	Replaceable	Replaceable
XSCF redundancy	Not available	Not available	Available
Number of domains	1	Max 2 (M4000) Max 4 (M5000)	Max 16 (M8000) Max 24 (M9000)
Number of CPUs	1	Max 4 (M4000) Max 8 (M5000)	Max 16 (M8000) Max 32 (M9000) Max 64 (M9000 with expansion cabinet)
Mounted processor	SPARC64 VII+ SPARC64 VII	SPARC64 VII+ SPARC64 VII SPARC64 VI	SPARC64 VII+ SPARC64 VII SPARC64 VI
System board division	Not available	Available	Available
Memory mirroring	Not available	Available	Available
DR	Not available	Available	Available
COD option	Not available	Available	Available

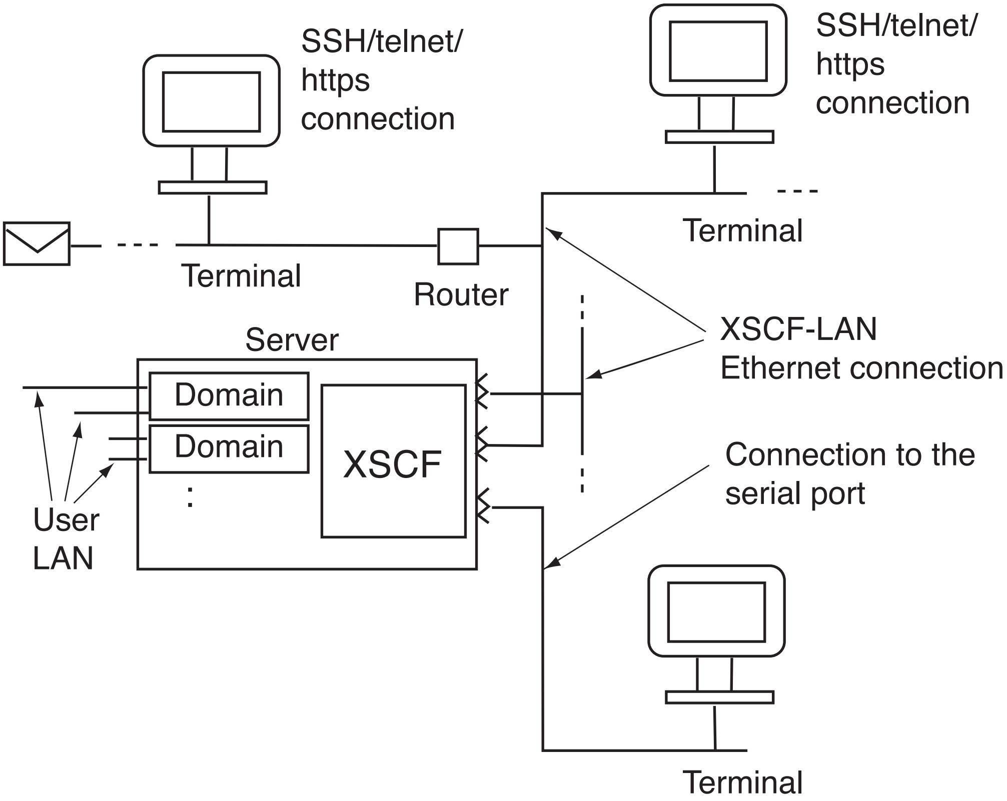
For an overview of the system board and the component, see the *Overview Guide* and the *Service Manual* for your server.

1.3 Types of Connection to XSCF

This section outlines types of connection to the XSCF.

XSCF enables access to the server over a serial port or from networks connected to XSCF-LAN. FIGURE 1-4 outlines the connections to the XSCF.

FIGURE 1-4 Connections to XSCF (In the Midrange Servers)



Note – In the systems with two XSCF Units, the XSCF Unit is in a redundant configuration, and there are physically twice as many XSCF-LAN ports and serial ports. Also, in the entry-level server, there is only one domain.

The following connections in the XSCF Unit connection configuration shown in FIGURE 1-4 are described below:

- Serial port connection
- XSCF-LAN Ethernet connection

Serial Port Connection

The serial port enables workstations, PCs, and ASCII terminals to connect to the XSCF through the serial (RS-232C) port. The user can use the XSCF Shell and access the domain console through the XSCF Shell.

XSCF-LAN Ethernet Connection

XSCF-LAN Ethernet enables workstations and PCs to connect to the XSCF through the XSCF-LAN port. The following can be used with XSCF-LAN Ethernet:

- XSCF Shell via a SSH or telnet connection
- XSCF Web from a web browser running on the terminal
- Domain console access
- Mail reports
- SNMP notification

For details on these XSCF functions, see the following chapters:

- Settings for each function: Chapter 2
- Shell terminal and console connections: Chapter 3
- XSCF Shell: Chapter 5
- XSCF mail functions: Chapter 6
- XSCF SNMP Agent functions: Chapter 7
- XSCF Web: Chapter 9

1.3.1 Examples of LAN Connection Operations

The XSCF Unit has two 10/100 Mbps XSCF-LAN two ports. TABLE 1-2 to TABLE 1-4 outlines three XSCF-LAN operation examples.

TABLE 1-2 XSCF-LAN Operation Examples 1

LAN Name	Operation
XSCF-LAN#0 port	• For system administrator operation The system administrator can control the server, control domains, and display the console using the XSCF Shell.
XSCF-LAN#1 port	• For field engineer operation. Field engineers can configure the server and perform maintenance tasks using the XSCF Shell. • For remote maintenance service operation

TABLE 1-3 XSCF-LAN Operation Examples 2

LAN Name	Operation
XSCF-LAN#0 port	• For system administrator operation • For remote maintenance service operation
XSCF-LAN#1 port	Not used

Note – The serial port is used by maintenance engineers.

TABLE 1-4 XSCF-LAN Operation Examples 3

LAN Name	Operation
XSCF-LAN#0 port	• For system administrator operation • For maintenance operation • For remote maintenance service operation
XSCF-LAN#1 port	Same as above

Note – The two XSCF-LAN ports are used for the same purpose (alternate path configuration). For details on these connections, see Chapter 3.

Caution – IMPORTANT - The IP address of XSCF-LAN#0 and the IP address of XSCF-LAN#1 must be specified in different subnet addresses.

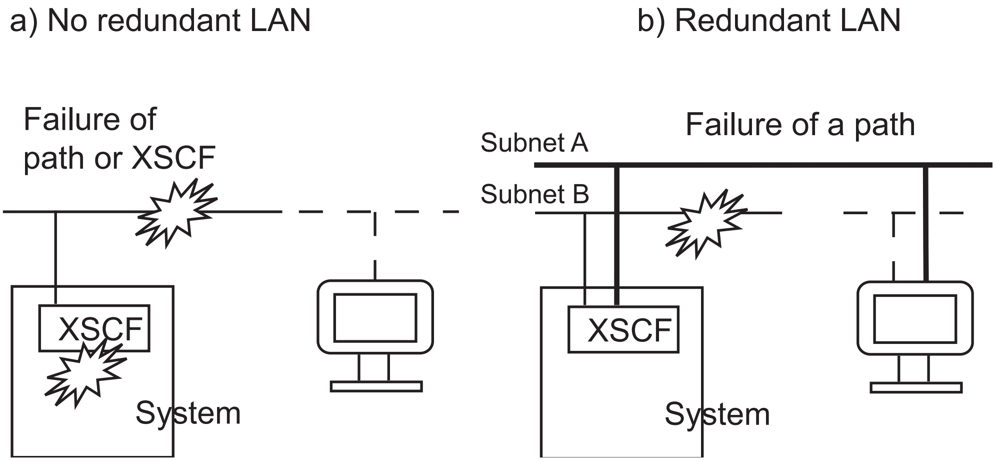
XSCF-LAN Redundancy

In the M3000/M4000/M5000/M8000/M9000 servers, the XSCF-LAN paths can be made redundant (duplicated). If a LAN failure occurs, it contributes significantly to reducing system availability. However, in a system equipped with a duplicate LAN, the routes (paths) in the remaining network can be used even if one subnetwork is faulty. In this way, high system availability can be achieved.

FIGURE 1-5 and FIGURE 1-6 show the network, which belongs to one or two different subnets. In FIGURE 1-5 and FIGURE 1-6, the ordinary lines represent subnetwork connections and the thick lines represent network connections.

FIGURE 1-5 shows configurations with a single mounted XSCF Unit: one where the LAN is not redundant, and the other with a redundant LAN.

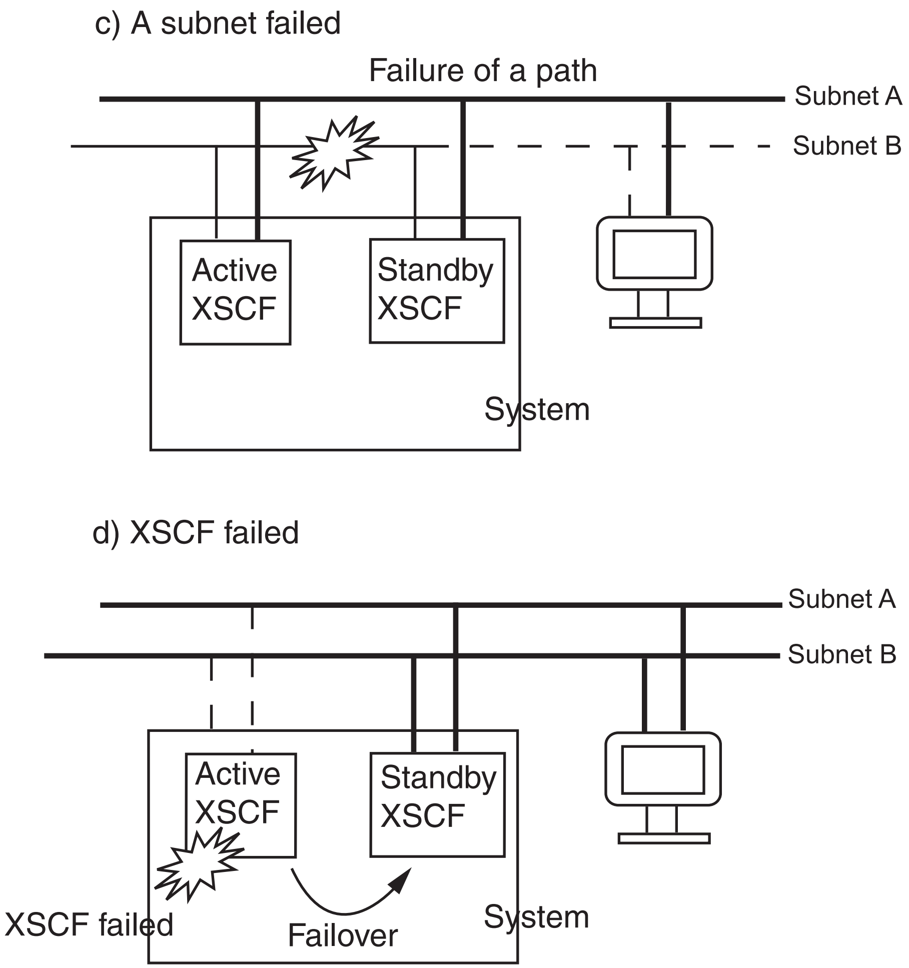
FIGURE 1-5 XSCF-LAN Redundancy (In Entry-level and Midrange Servers)



In the configuration examples shown in FIGURE 1-6, the XSCF-LANs are redundant and the XSCF Unit is in a redundant configuration.

In the configuration with a single XSCF Unit, XSCF-LAN cannot be used by any XSCF Unit failure even if the XSCF-LANs are redundant (duplicated). If one subnetwork is faulty, the remaining path can be used (FIGURE 1-6-c). If the active XSCF Unit is faulty, XSCF initiates failover (FIGURE 1-6-d). Therefore, high network availability can be achieved.

FIGURE 1-6 Two XSCF-LANs and Two XSCF Units Configuration (In High-End Servers)



c) A subnet failed

d) XSCF failed

For details on LAN configurations and connections, see Chapter 3. For details on specifying IP addresses, see Chapter 2.

1.3.2 NTP Configuration and Time Synchronization

The system uses the XSCF Unit clock for the system standard time.

The domains in the server synchronize their times based on the XSCF Unit clock when the domains are started. The XSCF Unit clock can be adjusted to the exact time through a network connection to an external NTP server. In that way, the XSCF Unit becomes the NTP server and an NTP client.

Only domains may specify XSCF as an NTP server. Also, when the XSCF is used as an NTP server, XSCF permits only the confirmation of the time synchronization to the inquiry from the NTP client.

Note – Alternatively, the domains can synchronize their times through a connection to an external NTP server. However, there is a possibility that time differences exist between the XSCF and the domain. If you connect the domain to an external NTP, connect the high rank NTP server that supplies the time of the same accuracy as the domain as for XSCF.
For details about NTP server setting, see Chapter 2.

TABLE 1-5 outlines XSCF and domain time synchronization methods.

TABLE 1-5 XSCF Unit and Domain Time Synchronization

Client	Primary NTP Server	Time Synchronization Method
Domain	XSCF Unit	The domain time is adjusted to the XSCF Unit clock time. XSCF Unit operates as the NTP server.
	External NTP server	The domain time is adjusted to the standard time of the external NTP server.
XSCF	No connection	The XSCF Unit time is the time in initial system settings or the time set by the `setdate`(8) command. For details on the `setdate`(8) command, see the *XSCF Reference Manual*.
	External NTP server	The XSCF Unit time is adjusted to the standard time of the external NTP server.

1.3.3 The CD-RW/DVD-RW Drive Unit and Tape Drive Unit

In the M3000 server, one domain monopolizes the DVD drive unit. In the M4000/M5000 servers, the domain that uses a minimum XSB number of number 0 of the MotherBoard Unit (MBU#0) can use the CD-RW/DVD-RW drive unit and tape drive unit (hereafter collectively called DVD drive/tape drive unit).

In the M8000/M9000 servers, a basic cabinet and an expansion cabinet contain one DVD drive/tape drive unit respectively, and they are assigned to a single operating domain of each cabinet. The DVD drive/tape drive unit can be used by assigning it to a specific card port on the I/O unit. To assign a different port, specify the unit by using the XSCF Shell. For details on this DVD drive/tape drive unit setting, see Chapter 2.

Note – Do not use the CD_RW/DVD-RW drive unit and the tape drive unit at the same time.

1.4 XSCF User Interfaces

This section describes the XSCF user interfaces.

1. XSCF Shell (Ethernet Connection):

A set of XSCF Shell commands you can use from a PC or a terminal connected to the XSCF over an XSCF-LAN Ethernet connection using SSH or `telnet`. Also, you can switch to domain console.

2. XSCF Shell (Serial Connection):

A set of XSCF Shell commands you can use from a PC or terminal directly connected to the XSCF by a serial cable. Also, you can switch to domain console.

3. XSCF Web:

A set of browser user interface (BUI) operations you can use from a web browser connected to the XSCF over the XSCF-LAN Ethernet.

4. XSCF SNMP Agent functions:

SNMP manager commands used to monitor the operation of the server's network functions.

5. XSCF mail functions:

Sends email reports of the system status.

For details about connecting to XSCF consoles, see Chapter 3.

Caution – IMPORTANT – To use the function as explained previously, you must create your XSCF account. Create your account before you start using the XSCF functionality. In addition, create an account for your field engineer (FE) with the privilege of fieldeng during initial setup.

To use these XSCF interfaces, users need to log in to XSCF with an XSCF user account, and then enter a password. When a user successfully logs into XSCF but the user leaves the session without any activity for a specified length of time, XSCF automatically logs the user out. XSCF monitors user operations and keeps a detailed access record containing the names of users who logged in and login times. For details on the user privilege required for control of this access record, see Section 1.4.1, "User Accounts and User Privileges" on page 1-23.

For details on login, see Chapter 5. For details on authentication and Web functions, see Chapter 9. For details on user account registration and mail function settings, see Chapter 2.

TABLE 1-6 outlines XSCF Functions and Connection Ports.

TABLE 1-6 XSCF Functions and Connection Ports

Functions	Contents	Serial port	XSCF-LAN Ethernet
XSCF Shell	• Monitors the server The status of the system can be checked. • System power can be controlled from a remote location The system power can be turned on and off and the system can be rebooted from a remote location. • Displays the server configuration The internal configuration of the server can be checked. • Set up the server Many server settings can be set. • Supports system maintenance Issues instructions for firmware update operation and component replacement. • OS console function You can access to the OS console and/or OpenBoot PROM prompt.	S	S

TABLE 1-6 XSCF Functions and Connection Ports *(Continued)*

Functions	Contents	Serial port	XSCF-LAN Ethernet
XSCF Web	Provides the same functions as the functions of the XSCF Shells, but provides graphical displays for easier operation.	_	S
Mail report	Mail notification in the event of a failure enables prompt action to be taken.	_	S
SNMP trap report	Enables consolidated control for system administration in conjunction with SNMP manager.	_	S

Note – Symbols: S: Supported. — : Not supported.

1.4.1 User Accounts and User Privileges

The system administrator and field engineers log in to XSCF with XSCF user accounts that allow them to refer to the status of any part of the entire system and work on all parts of the system. Each domain administrator uses an XSCF user account that enables system control of one domain.

For the server, the system administrator must consider both a user account that controls the whole system and a user account that administers each domain. When a user is registered, the user is assigned a privilege that controls the XSCF operations available to that user. This is referred to as the user privilege of the registered user account.

For example, to set up a domain administrator, the user privilege for the domain is specified. Moreover, you can provide system monitoring privileges, for instance, without system operation privileges. You can also limit privileges to specific domains.

TABLE 1-7 lists user privilege names and outlines the user privileges.

TABLE 1-7 User Privilege Names and Descriptions

User privilege	Outline	Description of Defined Contents
domainop@*n*	Reference of the status of any part of one entire domain_*n*	• Can refer to the status of any hardware mounted in a domain_*n*. • Can refer to the status of any part of a domain_*n*. • Can refer to the information of all system boards mounted.
domainmgr@*n*	Power supply operations and reference of the status of only one domain_*n*	• Can power on, power off, and reboot a domain_*n*. • Can refer to the status of any hardware mounted in a domain_*n*. • Can refer to the status of any part of a domain_*n*. • Can refer to the information of all system boards mounted.
domainadm@*n*	Control of only one domain_*n*	• Can operate all hardware mounted in a domain_*n*. • Can refer to the status of any hardware mounted in a domain_*n*. • Can operate all of a domain. • Can refer to the status of any part of a domain_*n*. • Can refer to the information of all system boards mounted.
platop	Reference of the status of any part of the entire system	• Can refer to the status of any part of the entire server but cannot change it.
platadm	Control of the entire system	• Can operate all hardware in the system. • Can configure all XSCF settings except the useradm and auditadm privilege settings. • Can add and delete hardware in a domain. • Can do the power operation of a domain. • Can refer to the status of any part of the entire server.
useradm	User account control	• Can create, delete, invalidate, and validate user accounts. • Can change user passwords and password profiles. • Can change user privileges.
auditop	Reference of the Audit status	• Can refer to the XSCF access monitoring status and monitoring methods.

TABLE 1-7 User Privilege Names and Descriptions *(Continued)*

User privilege	Outline	Description of Defined Contents
auditadm	Audit control (Note)	• Can monitor and control XSCF access. • Can delete an XSCF access monitoring method.
fieldeng	Field engineer operations	• Allows field engineers to perform the maintenance tasks or change the server configuration.
none	None	• When the local privilege for a user is set to none, that user has no privileges, even if the privileges for that user are defined in LDAP. • Setting a user's privilege to none prevents the user's privileges from being looked up in LDAP.

Note – (@*n*) "@domain number" is added behind the privilege name for the target domain privilege. (Example: The domainadm for domain ID 1 is domainadm@1). Also, a user account can have privileges over multiple domains, and not just the target domain.

For details on user privileges, see the *Administration Guide*. For details on setting up user accounts and setting user privileges, see Section 2.2.2, "User Account Administration" on page 2-36.

CHAPTER 2

Setting Up XSCF

This chapter explains how to set up XSCF.

2.1 XSCF Setup Summary

Each XSCF function must be configured before it can be used. Make the following settings:

- User Account Administration (required)
- Network Configuration (required)
- Time Administration (required)
- SSH/telnet Administration (optional)
- Mail Administration (optional)
- LDAP Administration (optional)
- Active Directory Administration (optional)
- LDAP/SSL Administration (optional)
- Https Administration (optional)
- Log Archiving Administration (optional)
- Audit Administration (optional)
- SNMP Administration (optional)
- Remote Maintenance Service Setting (optional) (see the following Note 1)
- Domain Configuration (required) (see the following Note 2)
- System Board Configuration (required) (see the following Note 3)
- Domain Mode Configuration (optional)
- Locale Administration (optional)

- Altitude Administration (required)
- DVD Drive/Tape Drive Unit Administration (optional)
- COD Administration (optional) (see the following Note 4)

Note – (1) This document does not provide details on the remote maintenance service functions. For the information of the remote maintenance service, see the Product Notes for your server.

Note – (2) Domain configuration is not required in the M3000 server. Some of the options can be configured. For details, see Section 2.2.13, "Domain Configuration" on page 2-146.

Note – (3) In the M3000 server, system board cannot be configured. System board has been configured by default and you cannot change the setting. However, you can refer to the system board information.

Note – (4) In the M3000 server, COD is not available.

After the XSCF is set up, the settings are automatically saved in XSCF internally and in the operator panel. Once you have configured the XSCF, it requires no day-to-day management. However, you can save or restore the XSCF setup configuration information. For details of saving or restoring XSCF configuration information, see Section 2.3, "Save and Restore XSCF Configuration Information" on page 2-195.

About Setup Flow

The XSCF Shell or XSCF Web can be used to set up XSCF.

Each setting items and the step summary are explained in Section 2.1.1, "Setup Summary by the XSCF Shell" on page 2-3 and Section 2.1.2, "Setup Summary Using the XSCF Web" on page 2-12. Details on each step are provided in Section 2.2, "Specifying the XSCF Settings" on page 2-15.

2.1.1 Setup Summary by the XSCF Shell

This section describes the step summary of setup using the XSCF Shell. This procedure contains examples of command usage and setting items. For details on settings, see the corresponding parts of Section 2.2, "Specifying the XSCF Settings" on page 2-15.

Note – Establish one-to-one communication between the PC and XSCF during the initial setup.

---

1. **Connect to XSCF by serial connection and log in.**

   To configure XSCF, the system administrator or a field engineer first uses the XSCF default user account. Before an appropriate user account for the user environment is created, log in with the following default user account and password:

- Default user account: default

  The user privileges are useradm, platadm.

- Default password:

  The default password is not input directly on the keyboard. Instead, after the default user account is input, the mode switch of the operator panel is operated as follows.

  a. **If Locked, change to Service. (Or if Service, change to Locked)**

  b. **Press return. Keep the status for more than 5 seconds.**

  c. **Change to Locked. (Or change to Service)**

  d. **Press return.**

  This mode switch operation is done within one minute. When one minute is passed, the authentication timeout occurs.

  - To begin the configuration, connect the XSCF Shell over a serial connection using any terminal software. The shell can be used immediately following connection to the serial port.

```
<Terminal screen image>
login:
```

  - Log in with the default user account. Follow the instructions to change the mode switch of the operator panel, and operate the mode switch within one minute.

```
login: default
Change the panel mode switch to Service and press return...
  (Operation : Locked state -> Service -> Return)
Leave it in that position for at least 5 seconds. Change the panel
mode switch to Locked, and press return...
 (Operation : Wait more than 5 seconds -> Service state ->
Locked -> Return)
XSCF>
```

When the server is running normally, the mode switch is set to the Locked position.

2. **Set the password policy.**

• Display and set a password policy.	showpasswordpolicy(8), setpasswordpolicy(8) (See Section 2.2.2, "User Account Administration" on page 2-36)

(This table includes the example of setting items and command used. It is similar thereafter.)

3. **Create an XSCF user account, password and privileges.**

- Create at least one user account with the user privileges of platadm and useradm:

```
XSCF> adduser yyyy
XSCF> password yyyy
XSCF> setprivileges xxxxxx
(See Section 2.2.2, "User Account Administration" on page 2-36)
```

(The screen is an operating procedure image.)

- The default user account is publicly available information. When installation is completed, create an appropriate user account for the user environment and log in again with the new user account. For details on the user privileges, see the *Administration Guide*.
- When you add the user account, use the `showuser(8)` command with `-l` option to confirm that there is no illegal user account in the user account list.

Note – In preparation for maintenance work, please create an account for a field engineer (FE) with the privilege of fieldeng during the initial set up.

4. **Set the time.**

• Set and display the time zone.	showtimezone(8), settimezone(8),
• Set and display the XSCF time.	showdate(8), setdate(8)

• Reset and display the time subtraction between the XSCF and the domain.	showdateoffset(8)
	resetdateoffset(8)
	(See Section 2.2.6, “Time Administration” on page 2-92)

- When the system time is updated, the XSCF reset is done and the XSCF session is disconnected. Please log in again to the XSCF using the new user account.
- NTP settings (setntp(8)) are done after the Network settings or the Domain Configuration.

5. **Configure the SSH/telnet settings.**

• Select SSH or telnet, and set SSH access control from domain.	setssh(8), settelnet(8),
• Display and specify the timeout monitoring period.	showautologout(8), setautologout(8) (See Section 2.2.7, “SSH/Telnet Administration” on page 2-104)

- XSCF reset is required to enable SSH, to disable telnet, and to set the SSH access control from domain. Go to the next step when you reset it later. If you want to reset XSCF immediately, use the rebootxscf(8) command. After the XSCF reset, the XSCF session is disconnected. Log in again to the XSCF.
- You can enable SSH and telnet at the same time. However, the telnet connection is not a secure connection protocol. We recommend that when you enable SSH that you disable telnet.

6. **Confirm the XSCF host public key.**

- Before using SSH for XSCF-LAN connection, record the fingerprint. Or, copy the text data of the host public key and save the data to a specific directory of the client. (The following screen is an example.)

```
XSCF> showssh
SSH status: enabled
SSH DSCP: accept
RSA key:
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEArmf46B4xSvunUNZPWOi4mRbqO9hsunxHitwR/
0P6NTQbNK8BqCpCsyzK6nfjrARztO1rgXIdFfXLDEIY2hudEkuMCjyorX1HK+d8WH
C7eydTCM8Edwwtwm0Q4o66peB/QwI/OL4lDCNRg+4aGyWUHZBwmiwahum+7MJDCKs
fKKM=
Fingerprint:
1024 14:75:fd:5c:e1:68:79:f6:db:cb:a7:36:25:53:25:9a
DSA key:
ssh-dss
AAAAB3NzaC1kc3MAAACBAMMG1ewTyceFX7EnKuDIp1BVnuxf+UTtALVinkfXLQbUn
gn84G8xp9GPnWOpNqiWXxAL8wInQrpz9wFd7n4sZk74HALM+gIhpjbpdXR76FpEvO
MzCi6qYuv4yQ/0+uKCHmJEfzIOvQnDoofVElXYRKxTIyQY5+mtsf+44IoGzJbxAAA
AFQCTNSxe0+5hbDziCOlgvch7FdUM3QAAAIBKGSbFr3XMYxubT7ViDHHIFgFpjEMw
DREJD05g7XwlslgFX4Ff2nqItepyfnok/CeDi1bv1Xs0JGAGsbcwpBeKe7YcSepM3
xe8vGXSIdVqGbfDvqbO9P1q1n58qEKTA2Cj5L9a+6usSYfKHOSDhnvX3R8/Hk+Iiy
6EUaVSaJUHjgAAAIAZ+qQahRLAMuOq5FCuQ000xgfZzExRBIa1Q7sBhMTrg1dksKP
+yPN9YjIw6QJXUD69acCWHD+nIKBTnSdO/NdwxDRKU2+9cOvNriUpbs5RoZgiCNCd
7nMMQUMFTzc78nd3w+pcjD5mBB6kELKuQurWbIDELTgYJcfm52C9TlR5WA==
Fingerprint:
1024 e2:66:1a:c8:8f:37:6f:ec:6c:2a:d4:93:a7:6f:dc:5c
```

7. Installing the user public key.

- Before using the SSH user key for an XSCF-LAN connection, generate a user private key and a user public key for a created XSCF user account with your client software. Then install the user public key to XSCF.

• Generate the SSH user key. (Set in client)	showssh(8), setssh(8)
• Display, Install, and Delete the SSH user public key.	(See Section 2.2.7, “SSH/Telnet Administration” on page 2-104)

8. **Configure the network.**

• Display and set the DSCP.	`showdscp`(8), `setdscp`(8),
• Display XSCF network settings (enable/disable, IP address, netmask) and configure/remove an XSCF network.	`shownetwork`(8), `setnetwork`(8)
• Display and set XSCF host name.	`showhostname`(8), `sethostname`(8)
• Display XSCF route settings (destination IP address, gateway, netmask, interface) and configure an XSCF route.	`showroute`(8), `setroute`(8)
• Display and make the DNS settings (name servers, search paths, add/delete).	`shownameserver`(8) , `setnameserver`(8)
• Display and set the IP packet filtering rules.	`showpacketfilters`(8) , `setpacketfilters`(8)
• Apply network settings.	`applynetwork`(8) (See Section 2.2.1, “Network Configuration” on page 2-16)

- Perform the `applynetwork`(8) command to apply the network settings. To complete the network settings, the XSCF reset is required. Go to the next step when you reset it later. When you want to reset it now, perform the `rebootxscf`(8) command to apply the settings. Then, the XSCF reset is done and the XSCF session is disconnected. Please connect the XSCF and log in to the XSCF again.

- Here, when you set up the XSCF by the XSCF-LAN connection, please change the cable from the serial port to the XSCF-LAN port. (Change the serial cable to the LAN cable.) When you use the controller that converts the RS-232C interface and LAN interface, you do not need to change the cable. Reconnect to the XSCF using the new user account and the new IP address and login to the XSCF again.

  For details on connecting the SSH, telnet, and serial port, and login to the XSCF, see Chapter 3. Moreover, the telnet connection is not a secure connection protocol. We recommend that you use SSH.

  During login using SSH on XSCF Shell (Ethernet connection), you are prompted to confirm the authenticity of the fingerprint of the host public key. The reply is "yes" if the fingerprint is the same as the memo in Step 6. If the reply is not the same, please confirm that the IP address is correct and not duplicated. There is a possibility that IP address spoofing has occurred.

```
RSA key fingerprint is xxxxxx
Connecting? [yes|no] : yes
```

Type the passphrase you have already set in the case that you would be using SSH with user key authentication.

```
Enter passphrase for key '/home/nana/.ssh/id_rsa' :xxxxxxxx
Warning: No xauth data; using fake authentication data for X11
forwarding.
Last login: Fri Sep 1 10:19:37 2006 from client
```

9. **Configure the mail settings.**

• Display mail notification settings, and configure and test mail notification.	`showsmtp`(8), `setsmtp`(8), `showemailreport`(8), `setemailreport`(8) (See Section 2.2.12, "Mail Administration" on page 2-143)

After this, configure the user accounts.

To manage user accounts, you can either configure the XSCF local accounts or you can configure the user accounts to authenticate against a remote user database, such as Lightweight Directory Access Protocol (LDAP), Active Directory, or LDAP/SSL.

Note – Lightweight Directory Access Protocol (LDAP): Protocol used to access directories and databases in TCP/IP networks.
Active Directory: Active Directory is a distributed directory service from Microsoft Corporation.
LDAP/SSL: LDAP/SSL is a distributed directory service like Active Directory. LDAP/SSL offers enhanced security to LDAP users by way of Secure Socket Layer (SSL) technology.

Before using an LDAP, an Active Directory, or an LDAP/SSL server, download a certificate, create a public key, and perform user registration in the applicable directory in the user environment.

If you are an Active Directory user, you cannot upload a user public key. When you set the user public key to XSCF before XCP1100, delete the user public key. The Active Directory users can access to XSCF via SSH by using the password authentication and can login to XSCF.

This manual does not provide details on LDAP, Active Directory, and LDAP/SSL, so see the available LDAP, Active Directory, and LDAP/SSL manuals.

10. **Configure the LDAP settings.**

- Configure XSCF as an LDAP client.

• Display and set LDAP client information.	showldap(8), setldap(8) (See Section 2.2.3, "LDAP Administration" on page 2-44)

11. **Configure the Active Directory settings.**

- Configure XSCF as an Active Directory client.

• Display and set Active Directory client information.	showad(8), setad(8) (See Section 2.2.4, "Active Directory Administration" on page 2-49)

12. **Configure the LDAP/SSL settings.**

- Configure XSCF as an LDAP/SSL client.

• Display and set LDAP/SSL client information.	showldapssl(8), setldapssl(8) (See Section 2.2.5, "LDAP/SSL Administration" on page 2-71)

13. **Configure the user account settings.**

- Configure XSCF local account.

• Add or delete a user account. • Change a user account password. • Display user account information. • Enable or disable a user account. • Specify a user privilege. • Display lockout settings and configure lockout for user accounts	adduser(8), deleteuser(8), password(8), showuser(8), enableuser(8), disableuser(8), setprivileges(8), showloginlockout(8), setloginlockout(8) (See Section 2.2.2, "User Account Administration" on page 2-36)

14. **Configure the log archiving settings.**

• Display log archiving settings and configure log archiving.	`showarchiving`(8), `setarchiving`(8) (See Section 2.2.10, "Log Archiving Administration" on page 2-127)

15. **Configure the audit settings.**

• Display audit settings and configure auditing.	`showaudit`(8), `setaudit`(8) (See Section 2.2.9, "Audit Administration" on page 2-120)

Note – The auditadm privilege is required for the audit settings.

16. **Configure the SNMP settings.**

• Display Agent settings and configure Agent. • Display and specify the notification destination server.	`showsnmp`(8), `setsnmp`(8), `showsnmpusm`(8), `setsnmpusm`(8), `showsnmpvacm`(8), `setsnmpvacm`(8) (See Section 2.2.11, "SNMP Administration" on page 2-132)

17. **Make the settings for using the remote maintenance service.**

Note – This document does not provide details on the remote maintenance service functions. For the information of the remote maintenance service, see the Product Notes for your server.

18. **Configure the system board settings.**

• Display and set a memory mirror mode. • Display and specify system boards separately from the XSB. (Uni-XSB or Quad-XSB displaying and settings.)	`showfru`(8), `setupfru`(8) (See Section 2.2.14, "System Board Configuration" on page 2-175)

In the M3000 server, the system board cannot be configured. The system board has been configured by default and you cannot change the settings. However, you can refer to the system board information.

19. **Configure the domain settings.**

• Display domain information and specify the domain configuration. (DCL displaying and settings, configuration policy settings, System board settings)	`showboards`(8), `showdcl`(8), `setdcl`(8)
• Add, delete, or move a system board.	`addboard`(8), `deleteboard`(8), moveboard(8) (See Section 2.2.13, "Domain Configuration" on page 2-146)

- In the M3000 server, you cannot perform operations such as setting the domain configuration, or adding or deleting the system board. The domain has been configured by default and cannot be changed. However, you can set the configuration policy and display the domain information.
- The Domain Component List (DCL) is definition data for the hardware resources that constitute a domain. There is one DCL per the logical system board. Each domain has up to 16 logical system boards. The DCL is used to add a hardware resource that constitutes a domain and to display resource configuration information. For details on the DCL, see Section 2.2.13, "Domain Configuration" on page 2-146, the *Administration Guide*, and the Dynamic Reconfiguration User's Guide.
- In the configuration policy settings, a degradation range applicable to errors detected during initial hardware diagnosis can be specified.

20. **Configure the domain mode settings.**

• Display and make the domain mode settings. (Diagnostic level, Break signal sending on/off, enable/disable Host watchdog monitoring, automatic boot setting, CPU operational mode)	`showdomainmode`(8), `setdomainmode`(8) (See Section 2.2.15, "Domain Mode Configuration" on page 2-178)

The automatic boot setting configures whether to automatically boot the Oracle Solaris OS or to stop in the OpenBoot PROM mode (ok prompt). It is the same operation as to set true or false in `auto-boot?`, which is the OpenBoot PROM environmental variable.

21. Configure the Locale settings.

- Display and set the Locale.	`showlocale`(8), `setlocale`(8) (See Section 2.2.16, "Locale Administration" on page 2-190)

22. Configure the Altitude Administration settings.

- Display altitude settings and configure altitude.	`showaltitude`(8), `setaltitude`(8) (See Section 2.2.17, "Altitude Administration" on page 2-191)

Note – Normally, the Altitude Administration is set up by FE. Also, the privilege of fieldeng is required.

---

23. Configure the DVD drive/tape drive unit settings.

- Display DVD drive/tape drive unit information, including connection information, and configure the devices.	`cfgdevice`(8) (See Section 2.2.18, "DVD Drive/Tape Drive Unit Administration" on page 2-192)

24. Configure the capacity on demand (COD) settings.

- Display and set the COD.	For COD settings and command information, see the *COD User's Guide* and the *XSCF Reference Manual*.

Note – In the M3000 server, COD is not available.

2.1.2 Setup Summary Using the XSCF Web

This section describes the setup summary using the XSCF Web. This procedure contains examples of the windows that are used. For details on settings, see the corresponding parts of Section 2.2, "Specifying the XSCF Settings" on page 2-15.

Before attempting to establish a connection to the XSCF and log in from the web browser window of the XSCF Web, perform Step 1 - Step 8 in Section 2.1.1, “Setup Summary by the XSCF Shell” on page 2-3, and enable https in Section 2.2.8, “Https Administration” on page 2-113. If you have already performed Step 1 to Step 8 in Section 2.1.1, “Setup Summary by the XSCF Shell” on page 2-3, start the procedure in this section at Step 9.

In addition, establish one-to-one communication between the PC and the XSCF during initial setup.

1. **Connect to and log in to XSCF (serial). (Same as Step 1 in** Section 2.1.1, “Setup Summary by the XSCF Shell” on page 2-3**.)**

2. **Set the password policy. (Same as Step 2 in** Section 2.1.1, “Setup Summary by the XSCF Shell” on page 2-3**.)**

3. **Create an XSCF user account, password and privileges. (Same as Step 3 in** Section 2.1.1, “Setup Summary by the XSCF Shell” on page 2-3**.)**

4. **Set the time. (Same as Step 4 in** Section 2.1.1, “Setup Summary by the XSCF Shell” on page 2-3**.)**

5. **Make the SSH/telnet settings. (Same as Step 5 in** Section 2.1.1, “Setup Summary by the XSCF Shell” on page 2-3**.)**

6. **Confirm the XSCF host public key. (Same as Step 6 in** Section 2.1.1, “Setup Summary by the XSCF Shell” on page 2-3**.)**

7. **Install the user public key. (Same as Step 7 in** Section 2.1.1, “Setup Summary by the XSCF Shell” on page 2-3**.)**

8. **Configure the network. (Same as Step 8 in** Section 2.1.1, “Setup Summary by the XSCF Shell” on page 2-3**.)**

9. **Make the https settings.**

• Enable or disable the https. • Import the web certificate.	sethttps(8) (See Section 2.2.8, “Https Administration” on page 2-113)

To enable https, the XSCF reset is required. Reset the XSCF by using the rebootxscf(8) command. After the XSCF reset, the XSCF session is disconnected. Log in again to the XSCF.

- Change to the XSCF-LAN connection when you connect the serial cable.

10. **Establish a connection to XSCF and log in from a web browser.**

- Specify the host name or the IP address of the XSCF during the network configuration, in a web browser running on a PC with an XSCF-LAN port used to establish a connection to the XSCF.

```
<Web browser screen image>
URL https://192.168.111.111/ (The IP address of XSCF is input by number)
Alternatively:
https://XSCF-host-name/ (Not the host name of a domain)
```

(This screen image is an example and differs from the actual screen display.)

Note – The web browser window for the XSCF Web is called the XSCF Web console.

- Log in.

```
<Web browser screen image>
login:yyyy
Password:xxxxxxxx
```

(This screen image is an example and differs from the actual screen display.)

Note – When connecting using https, a warning message appears in the web browser until the certificate is installed.

---

11. **Open the XSCF Administration window.**

```
<Web browser screen image>
XSCF Web console
- Remote Maintenance Service Administration
- Firmware Update
```

(This screen image is an example and differs from the actual screen display.)

- The remaining setting items are the same as those applicable to setup using the XSCF Web. Referring to the setup flow, proceed to Step 9 and later steps in Section 2.1.1, “Setup Summary by the XSCF Shell” on page 2-3. For details on the commands used to make settings, see the corresponding parts of Section 2.2, “Specifying the XSCF Settings” on page 2-15.

2.2 Specifying the XSCF Settings

This section describes the XSCF settings in detail.

XSCF settings can be made in the following ways:

- On the PC connected to the serial port, or you can specify the IP address of the XSCF to establish a connection to the XSCF, and then use the XSCF Shell over an Ethernet or a user LAN connection.
- Specify the host name or the IP address of the XSCF in a web browser running on a PC with an XSCF-LAN connection in order to establish a connection to the XSCF, and then use the XSCF Web (see the following note).

Note – If the XSCF Web is not supported, or you want to set a function that is not supported on the XSCF Web, use the XSCF Shell to make these settings. For the support information, see the Product Notes for your server.

To describe the XSCF settings, each subsequent section is formatted as follows:

1. Each section first uses tables to explain terms, setting items, functions, and XSCF Shell commands.
2. Each section then provides setting examples. When you set up by using XSCF Web, see the "Web browser operation" sections. When you set up by using XSCF Shell, see the "Command operation" sections.
   - For details on individual XSCF Shell commands, options, and privileges, see the *XSCF Reference Manual* or the man page. You can display the man page by executing the man command on XSCF. The man page is the same as the *XSCF Reference Manual*.
   - For details on the screen layout, start procedure, and operation of the XSCF Web, see Chapter 9.
   - For details the connection between a PC and XSCF, the connection to a terminal, or how to log in to XSCF, see Chapter 3.

2.2.1 Network Configuration

Network Configuration is used to specify items relating to network interfaces like XSCF-LANs and Domain-SP Communication Protocol(DSCP), also, routing, and DNS.

TABLE 2-1 lists terms used in Initial Configuration.

TABLE 2-1 Network Configuration Terms

Term	Explanation
XSCF network interface	General term for an interface required in XSCF network configuration. Such interfaces include the following: [First XSCF Unit] • XSCF-LAN#0 (Active side) • XSCF-LAN#1 (Active side) • Inter SCF Network (ISN) (Active side) (If the XSCF Unit is redundant) [Second XSCF Unit] (If the XSCF Unit is redundant) • XSCF-LAN#0 (Standby side) • XSCF-LAN#1 (Standby side) • ISN (Standby side) Takeover IP address (If the XSCF Unit is redundant) • XSCF-LAN#0s • XSCF-LAN#1s Domain-SP Communication Protocol (DSCP): • XSCF side (One IP address is required.) • Domain side (One IP address is required for each domain, therefore, the IP addresses for the maximum number of domains are required.)
ISN	This network is between two XSCF Units (active and standby). ISN is used for a system with a redundant XSCF configuration.
Takeover IP address	A takeover IP address (virtual IP address) is set between each XSCF#*x*-LAN#0’s Unique addresses of two XSCF Units. The XSCF#*x*-LAN#1s are also the same. Even if the active XSCF and the standby XSCF are switched, the IP address takeover can be done at each "LANs".
DSCP	This interface protocol is used between XSCF and a domain. DSCP settings are made with XSCF. The network of the domains and the XSCF connected by DSCP might be called DSCP links.

Note – Systems with two XSCF Units can only be M8000/M9000 servers.

TABLE 2-2 lists setting items and the corresponding shell commands.

To complete the network settings, the XSCF reset is required. Reset the XSCF by using the rebootxscf(8) command. After the XSCF is reset, the XSCF session is disconnected. Please log in again to the XSCF.

TABLE 2-2 Network Configuration

Item	Description	Shell Command	Remarks
Display network	Displays XSCF network interfaces. Also, displays the following network status: • Number of bytes of the receive queue buffer. • Number of bytes of the send queue buffer. • Local address and port. • Host address and Socket port number.	`shownetwork` `showdscp`	If the XSCF Unit is redundant, the connection status of the other side is not displayed.
Enable/disable network	Enables or disables an XSCF network interface (see TABLE 2-1).	`setnetwork` `setdscp`	• When the XSCF Unit is a redundant model, Defaults of IP address of ISN are the following: XSCF#0:192.168.1.1 XSCF#1:192.168.1.2 • No default setting has been specified for the other interfaces. • You can use a single LAN port for XSCF-LAN. For network connection examples, see Chapter 3. • You can remove the configuration, XSCF-LAN, Takeover IP address, and netmask
IP address	Specifies the following IP address of the XSCF network interfaces (see TABLE 2-1). • One or both of the XSCF-LAN ports • DSCP • ISN, Takeover IP address (if a redundant XSCF Unit is used)		
netmask	Sets a netmask for an XSCF network interface.		
Display host name	Displays a host name and the host name informations. A Fully Qualified Domain Name (FQDN) can be displayed	`showhostname`	

TABLE 2-2 Network Configuration *(Continued)*

Item	Description	Shell Command	Remarks
Host name/domain name	Sets a host name and a domain name for the XSCF Unit. FQDN cannot be specified for the host name. A host name can be specified up to 64 characters. A domain name can be specified up to 254 characters with the host name included, with label elements delimited by a "." (period). A label element can contain alphanumeric characters (a to z, A to Z, 0 to 9), "-" (hyphen) and "." (period). Each label element must always begin with an alphabetic character and end with an alphanumeric character. However, you cannot use a "." (period) in a host name.	`sethostname`	No default setting has been specified.
Display route	Displays the XSCF routing environment as follows: Network interface (see TABLE 2-1), Destination IP address, Gateway, netmask, Flags. The meanings of the Flags are as follows: U : route is up H : target is a host G : use gateway R : reinstate route for dynamic routing C : cache entry ! : reject route	`showroute`	
Add/delete route	Adds a route to or deletes a route from an XSCF network interface. Specify the following: • Network interface • Destination IP address (Destination) • Gateway • netmask	`setroute`	The setting of routing information in each interface can be set up to eight respectively.
Display DNS	Displays XSCF name servers and search paths.	`shownameserver`	

TABLE 2-2 Network Configuration *(Continued)*

Item	Description	Shell Command	Remarks
Add/delete DNS	Add or delete the IP address of a name server and the domain name of a search path. Up to three name servers can be registered. Names can be solved in the order specified. Up to five search paths can be registered. Domain names are assigned in the order specified and they are referred to the DNS server.	`setnameserver`	No default setting has been specified. If the DNS connection is necessary, this setting is done.
Display IP packet filtering rules	Displays IP packet filtering rules.	`showpacketfilters`	
IP packet filtering rules	Sets IP packet filtering rules for XSCF-LANs to permit the IP packets to go through or to drop the IP packets.	`setpacketfilters`	You can set the IP filtering rules to the input packets, not to the output packets.
Apply network	Apply network settings.	`applynetwork`	

In systems with two XSCF Units, the two XSCF Units are connected by system internal ports, which are the RS-232C (serial) ports and the LAN ports. Each XSCF Unit monitors the status of the other one and they exchange system information through these communication paths. When the system is initially set up, the user must specify the IP address for internal LAN routes.

In the M8000/M9000 servers, up to 33 IP addresses are usually specified: four for XSCF-LAN ports, two for the ISN, two for the Takeover IP addresses, and up to 25 for DSCP on both the XSCF and domain sides. In the M4000/M5000 servers, up to seven IP addresses are usually specified: two for XSCF-LAN ports and up to five for DSCP on both the XSCF and domain sides. In the M3000 server, up to four IP addresses are usually specified: two for XSCF-LAN ports and two for DSCP on both the XSCF and domain sides.

⚠ **Caution – IMPORTANT –** If the XSCF Unit is redundant, issue the commands to setup all XSCF on only the Active XSCF Unit. The command need not be executed on both (Active and Standby) XSCF Units. The XSCF setting cannot be performed on the standby side.

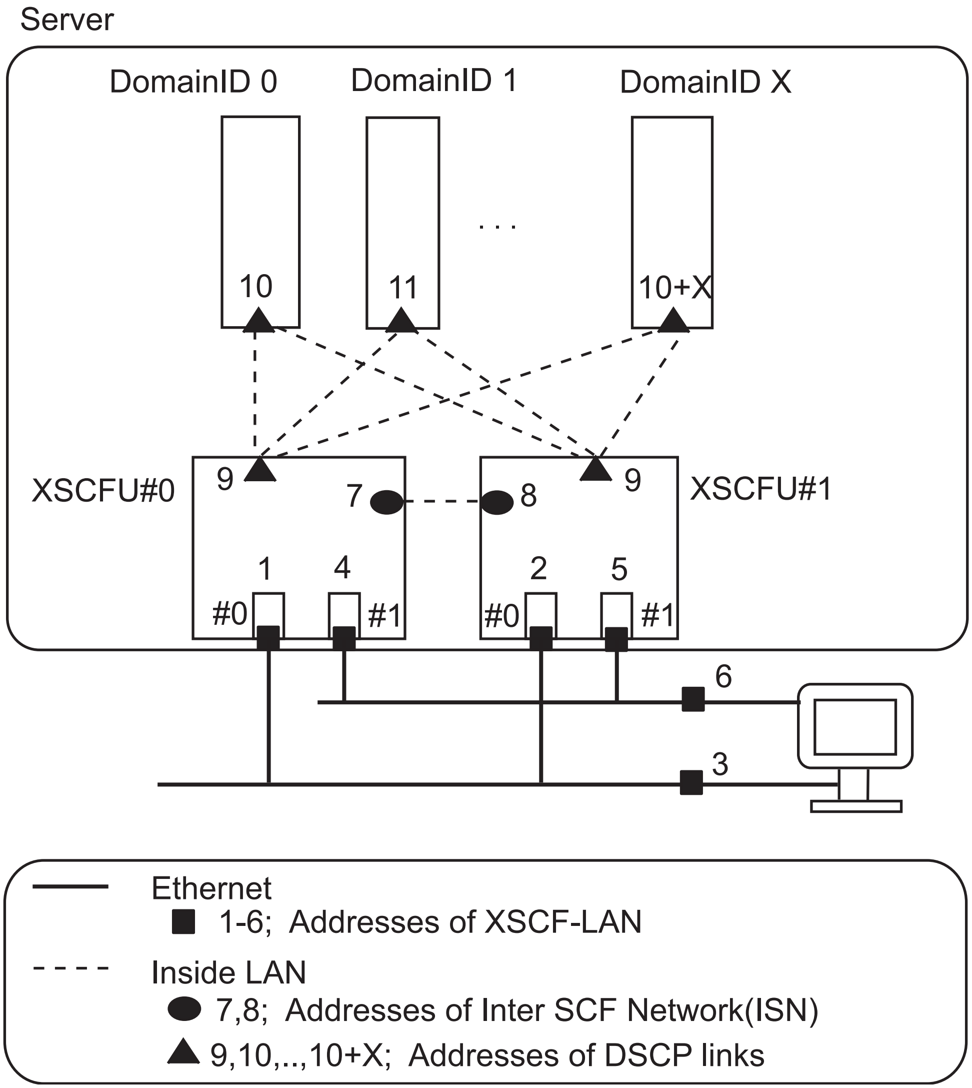
XSCF network interface configuration

The XSCF network interface includes the following.

- LAN (XSCF-LAN) for users to access to XSCF
- LAN (ISN) for the communication between XSCF Units (M8000/M9000 servers only)
- LAN (DSCP) for the communication between XSCF and each domain

FIGURE 2-1 shows the network interface which is required for the XSCF and domain network configuration.

FIGURE 2-1 Network Interface Required for XSCF Network Configuration (In the High-End Servers)


Server
DomainID 0
DomainID 1
DomainID X
. . .
10
11
10+X
XSCFU#0
XSCFU#1
9
9
7
8
1
4
2
5
#0
#1
#0
#1
6
3
Ethernet
■ 1-6; Addresses of XSCF-LAN
Inside LAN
● 7,8; Addresses of Inter SCF Network(ISN)
▲ 9,10,..,10+X; Addresses of DSCP links

Number	Description	Number	Description
1	XSCF-LAN#0 address (XSCFU#0 side)	7	ISN address. (XSCFU#0 side)
2	XSCF-LAN#0 address (XSCFU#1 side)	8	ISN address. (XSCFU#1 side)
3	Takeover IP address between XSCF-LAN#0s	9	DSCP link address (XSCF side)
4	XSCF-LAN#1 address (XSCFU#0 side)	10 or later	DSCP link addresses (Domains side)
5	XSCF-LAN#1 address (XSCFU#1 side)		
6	Takeover IP address between XSCF-LAN#1s		

XSCF network configuration procedure and the reference

The procedure to set up the XSCF network is as follows. Each step offers the detailed procedure reference.

Note – You must set XSCF-LAN, ISN, and DSCP to different subnet addresses. If two XSCF-LAN ports are used, each must be assigned to a different subnet. The ISN address has been set up with the default value (see TABLE 2-2).

---

1. Specify the IP address of Ethernet (XSCF-LAN).

You can use two XSCF-LAN ports in accordance with the network configuration. In the M3000/M4000/M5000 servers, specify either or both of the following IP addresses:

- XSCF-LAN#0 of XSCFU#0 (See "1" in FIGURE 2-1)
- XSCF-LAN#1 of XSCFU#0 (See "4" in FIGURE 2-1)

In the M8000/M9000 servers, subsequently to the XSCFU#0 side, specify the IP address of XSCF-LAN of the XSCFU#1 side (see "2" and "5" in FIGURE 2-1). (See `shownetwork` (8), `setnetwork` (8).)

Use the same subnet address to specify the LAN ports which share the same number in each XSCF unit so that you can connect to both of the XSCF in case the XSCF failover generated.

To make the IP address redundant, specify the same subnet address to the LAN port of XSCFU#0 side and to the LAN port of XSCFU#1 side which share the same LAN port number. Also, The IP address of XSCF-LAN#0 and the IP address of XSCF-LAN#1 must be specified in different subnet addresses.

2. **Perform the following setting to specify the takeover IP address in a redundant XSCF configuration.**

When you specify the takeover IP address, in case the XSCF failover occurred, the control switching between the active side and the standby side performed, and then the IP address will be taken over. The user who accesses the takeover IP address can always connect to the active side XSCF, without being aware of the XSCF switching.

Sets IP address respectively of XSCF-LAN#0 and XSCF-LAN#1. In addition, on each LAN port of XSCF-LAN#0 and XSCF-LAN#1 in the redundant system, specify the takeover IP address one by one (see "3" and "6" in FIGURE 2-1). (See `shownetwork`(8), `setnetwork`(8).)

3. **In a redundant XSCF configuration, specify the two IP addresses of ISN.**

Since ISN is a network for the communication between the redundant XSCF Units, it is necessary to specify the IP address. The ISN address has been set up with the default value (see TABLE 2-2).

If the IP address of XSCF-LAN conflicts with the default subnet address of ISN, you must specify the IP address of ISN (see "7" and "8" in FIGURE 2-1). Also, both ISN addresses must be in the same network subnet. Users cannot access this network. (See `shownetwork`(8), `setnetwork`(8).)

4. **Specify the DSCP address.**

After configured the domain (see Section 2.2.13, “Domain Configuration” on page 2-146), specify the DSCP address.

Specify one DSCP IP address in the XSCF-side, and one for each of the domains (See "9," "10" or later in FIGURE 2-1). By specifying the option, you can specify one DSCP address which is used in all of the DSCP links. In this case, the IP addresses used by the XSCF and each domain-specific DSCP link are automatically selected from within the range of addresses indicated by the DSCP network address.

All DSCP addresses must be in the same network subnet. Since the DSCP is the network for the communication between domain and XSCF, users can’t access to this network. When you changed the DSCP address, you must reset XSCF by using the `rebootxscf`(8) command before domain start up, in order to maintain the consistency between XSCF and the domain. After XSCF resetting, the domain restart is required. (See `showdscp`(8), `setdscp`(8).)

5. **Specify the host name, routing, and DNS.**

In the M8000/M9000 servers, subsequently to the XSCFU#0 side, specify the host name and the routing of the XSCFU#1 side. (See `showhostname`(8), `sethostname`(8), `showroute`(8), `setroute`(8), `shownameserver`(8), and `setnameserver`(8).)

6. **Configure IP packet filtering rules.**

Configure IP packet filtering rules for XSCF-LANs. (See `showpacketfilters`(8), `setpacketfilters`(8).)

7. **Apply network settings.**

(See `applynetwork`(8), `rebootxscf`(8).)

Note – An XSCF reset or failover might prevent any of the setting commands operation from completing. If a reset or failover occurs during the setting operation, log in to the active XSCF to determine if the operation succeeded. If not, try it again

---

Enabling or Disabling the XSCF Network and Specifying an IP Address and Netmask for the Network and DSCP

- Command operation

1. Use the `shownetwork`**(8) command to display network interface information.**

```
<Example 1> Display information on all network interfaces of XSCF.
XSCF> shownetwork -a

<Example 2> Display information on network interfaces of LAN#1 in the
XSCF Unit #0 (XSCFU#0).
XSCF> shownetwork xscf#0-lan#1
xscf#0-lan#1
          Link encap:Ethernet  HWaddr 00:0A:48:09:C9:0E
           inet addr:192.168.10.11  Bcast: 192.168.10.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:54424 errors:0 dropped:0 overruns:0 frame:0
          TX packets:14369 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:20241827 (19.3 MiB)  TX bytes:2089769 (1.9 MiB)
          Base address:0xe000

<Example 3> Display the ISN information on network interfaces of XSCFU#0
XSCF> shownetwork xscf#0-if
xscf#0-if Link encap:Ethernet  HWaddr 00:0A:48:09:C9:1E
            inet addr:192.168.10.128  Bcast:192.168.10.255  Mask: 255.255.255.0
           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
           RX packets:54424 errors:0 dropped:0 overruns:0 frame:0
           TX packets:14369 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:0 (0.0 B)  TX bytes:17010 (16.6 KiB)
           Base address:0xe000

<Example 4> Display the takeover IP address information of the XSCF-LAN#0
XSCF> shownetwork lan#0
lan#0    Link encap:Ethernet  HWaddr 00:00:00:12:34:56
         inet addr:192.168.1.10   Bcast:192.168.1.255   Mask:255.255.255.0
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         Base address:0xe000
```

2. **Use the** `showdscp`**(8) command to display DSCP information.**

```
<Example> Display DSCP information.
XSCF> showdscp

DSCP Configuration:

Network: 192.168.244.0
Netmask: 255.255.255.0

Location      Address
----------   ---------
XSCF         192.168.244.1
Domain #00   192.168.244.2
Domain #01   192.168.244.3
Domain #02   192.168.244.4
Domain #03   192.168.244.5
```

3. **Use the** `setnetwork`**(8) command to specify network interface information.**

```
<Example 1> Specify IP address 192.168.1.10 and netmask
255.255.255.0 for XSCF-LAN#0 in the XSCFU#0 to enable it.
XSCF> setnetwork xscf#0-lan#0 -m 255.255.255.0 192.168.1.10

<Example 2> Specify IP address 192.168.12.10 for the ISN in the
XSCFU#0 to enable it.
XSCF> setnetwork xscf#0-if 192.168.12.10

<Example 3> Specify IP address 192.168.11.10 and netmask
255.255.255.0 for the takeover IP address in the XSCF-LAN#0.
XSCF> setnetwork lan#0 -m 255.255.255.0 192.168.11.10

<Example 4> Disable XSCF-LAN#1 in the XSCFU#0.
XSCF> setnetwork xscf#0-lan#1 -c down

<Example 5> Remove the configured IP address and netmask of XSCF-
LAN#1 in the XSCFU#0.
XSCF> setnetwork -r xscf#0-lan#1
```

Note – The setting values like as IP address, netmask, enabling (up) or disabling (down) the network interface by `setnetwork`(8), `sethostname`(8), `setroute`(8), and `setnameserver`(8) commands are applied by performing the `applynetwork`(8) and the `rebootxscf`(8) commands.

---

4. **Use the `setdscp`(8) command (see Note) to specify network interface information.**

```
< Example 1> Specify the entire DSCP network IP address 192.168.2.0
and netmask 255.255.255.0.
XSCF> setdscp -i 192.168.2.0 -m 255.255.255.0

<Example 2> Specify IP address 192.168.2.1 for the XSCF.
XSCF> setdscp -s -i 192.168.2.1

<Example 3>  Specify the IP address of 192.168.2.2 to domain ID 1.
XSCF> setdscp -d 1 -i 192.168.2.2

<Example 4> Setting DSCP addresses using Interactive mode.
XSCF> setdscp
DSCP network  [192.168.244.0  ] > 192.168.2.0

DSCP netmask  [255.255.255.0  ] > 255.255.255.0

XSCF address  [192.168.2.1  ] > 192.168.2.1
Domain #00 address  [192.168.2.2  ] > 192.168.2.2
:
Commit these changes to the database? [y|n]:y
```

It is necessary to configure DSCP to enable it for the domains. For details about the Domain Configuration, see Section 2.2.13, “Domain Configuration” on page 2-146.

Setting DSCP addresses can only be done when affected domains are not running. Use of the `-i` and `-m` options to set all DSCP addresses can only be done when no domains are running. Setting the XSCF address can only be done when no domains are running, since this would affect the XSCF's communication to running domains. Setting individual domain addresses can be done only if the specified domain is not running. When you changed the DSCP address, you must reset XSCF by using the `rebootxscf`(8) command before domain start up, in order to maintain the consistency between XSCF and the domain. After XSCF resetting, the domain restart is required.

You can specify a network address for use by all of the DSCP links using the -i and -m options. In this mode of operation, the IP addresses used by the XSCF and each domain-specific DSCP link are automatically selected from within the range of addresses indicated by the network address.

If you set a netmask using the `-m` option, this netmask value shows the mask value in the XSCF network. A netmask value when you display the DSCP network on the domain is not the netmask value in the XSCF network. The netmask value for the domain DSCP address, which is displayed on the domain by using `ifconfig`(1M), is a value set according to the setting of the network on the domain side.

This is because the DSCP communication protocol, PPP (Point to Point Protocol), does not notify the netmask value specified by the -m option to the domain side, and also because the ifconfig(1M) displays the netmask value corresponding to the class of IP address in the DSCP interface.

Note – All DSCP addresses must be in the same network subnet.

Specifying a Host Name for XSCF

- Command operation

1. **Use the** showhostname**(8) command to display host names.**

```
XSCF> showhostname -a
xscf#0: scf-hostname0.company.com
xscf#1: scf-hostname1.company.com
```

2. **Use the** sethostname**(8) command to specify a host name.**

```
<Example 1> Specify the host name scf0-hostname for XSCFU#0.
XSCF> sethostname xscf#0 scf0-hostname

<Example 2> Specify the domain name com for XSCFU#0.
XSCF> sethostname -d company.com
```

Configuring XSCF Routing

In a redundant XSCF unit configuration, the following are examples of data when routing is done in each subnet.

<Example>

```
XSCF Unit 0             XSCF Unit 1
xscf#0-lan#0 [192.168.1.10] xscf#1-lan#0 [192.168.1.20]
+-------------------------------+
XSCF-LAN#0              XSCF-LAN#0

XSCF Unit 0             XSCF Unit 1
xscf#0-lan#1 [10.12.108.10] xscf#1-lan#1 [10.12.108.20]
+-------------------------------+
XSCF-LAN#1              XSCF-LAN#1

Destination     Gateway         Netmask         Interface
[192.168.1.0]   -               [255.255.255.0] xscf#0-lan#0
[default]       [192.168.1.1]   [0.0.0.0]       xscf#0-lan#0

[192.168.1.0]   -               [255.255.255.0] xscf#1-lan#0
[default]       [192.168.1.1]   [0.0.0.0]       xscf#1-lan#0

[10.12.108.0]   -               [255.255.255.0] xscf#0-lan#1
[default]       [10.12.108.1]   [0.0.0.0]       xscf#0-lan#1

[10.12.108.0]   -               [255.255.255.0] xscf#1-lan#1
[default]       [10.12.108.1]   [0.0.0.0]       xscf#1-lan#1
```

Note – The method of determining the routing for an XSCF interface depends on the network environment at the installation site. The network environment for system operation must have a suitable configuration.

Note – You cannot set the routing to the takeover IP address.

- Command operation

1. Use the `showroute`**(8) command to display the routing environment.**

```
XSCF> showroute -a
Destination    Gateway         Netmask         Flags Interface
10.12.108.0    *               255.255.255.0   U     xscf#0-lan#0
default        10.12.108.1     0.0.0.0         UG    xscf#0-lan#0
:
```

2. **Use the `setroute`(8) command to specify the routing environment for a network interface.**

```
<Example 1> Add routing with Destination 192.168.1.0 and Netmask
255.255.255.0 to XSCF-LAN#0 in the XSCFU#0.
XSCF> setroute -c add -n 192.168.1.0 -m 255.255.255.0 xscf#0-lan#0

<Example 2> Add routing with the default network for Destination
and Gateway 10.12.108.1 to XSCF-LAN#1 in the XSCFU#0.
XSCF> setroute -c add -n 0.0.0.0 -g 10.12.108.1 xscf#0-lan#1

<Example 3> Delete routing with destination 192.168.1.0 and netmask
255.255.255.0 to XSCF-LAN#0 in the XSCFU#0.
XSCF> setroute -c del -n 192.168.1.0 -m 255.255.255.0 xscf#0-lan#0
```

Making XSCF DNS Settings

- Command operation

1. **Use the `shownameserver`(8) command to display the name server and the search path. If multiple name servers and search paths are added, they are displayed on separate lines.**

```
<Example 1> Confirm that three name servers and one search path are
added.
XSCF> shownameserver
nameserver 10.0.0.2
nameserver 172.16.0.2
nameserver 192.168.0.2
search     company1.com

<Example 2> Confirm that no name server and no search path is added.
XSCF> shownameserver
---
```

2. **Use the** `setnameserver`**(8) command to specify the name server and the search path.**

```
<Example 1> Add the three IP addresses 10.0.0.2, 172.16.0.2, and
192.168.0.2 as name servers.
XSCF> setnameserver 10.0.0.2 172.16.0.2 192.168.0.2

<Example 2> Delete all available name servers.
XSCF> setnameserver -c del -a

<Example 3> Deletes the two DNS servers that is repeated three
times.
XSCF> shownameserver
nameserver 10.24.1.2
nameserver 10.24.1.2
nameserver 10.24.1.2
XSCF> setnameserver -c del 10.24.1.2 10.24.1.2
XSCF> shownameserver
nameserver 10.24.1.2

<Example 4> Add the one domain name "company1.com" as search path.
XSCF> setnameserver -c addsearch company1.com

<Example 5> Delete all available search paths.
XSCF> setnameserver -c delsearch -a
```

Note – If you set the search path, you must also specify the name server.

Configuring IP Packet Filtering Rules for XSCF Network

- Command operation

1. Use the `showpacketfilters`**(8) command to display the IP packet filtering rules for XSCF-LANs.**

```
<Example 1> Display the IP packet filtering rules settings for XSCF
network.
XSCF> showpacketfilters -a
-i xscf#0-lan#0 -j ACCEPT
-i xscf#0-lan#1 -j ACCEPT
-s 173.16.0.0/255.255.0.0 -j ACCEPT
-s 205.168.148.100/255.255.255.255 -j ACCEPT

<Example 2> Display status of current IP packet filtering rules.
XSCF> showpacketfilters -l
pkts bytes target     prot in           source
  124  102K ACCEPT     all  xscf#0-lan#0 0.0.0.0/0.0.0.0
    0     0 ACCEPT     all  xscf#0-lan#1 0.0.0.0/0.0.0.0
    0     0 ACCEPT     all  *            173.16.0.0/255.255.0.0
    0     0 ACCEPT     all  *            205.168.148.100

<Example 3> Display that IP packet filtering rule is not set.
XSCF> showpacketfilters -a
XSCF>
```

2. Use the `setpacketfilters`**(8) command to set the IP packet filtering rules. name server and the search path. The IP packet filtering rules are applied in the order in which they are defined.**

```
<Example 1> Permit the IP address 192.168.100.0/255.255.255.0 to
go through.
XSCF> setpacketfilters -y -c add -i xscf#0-lan#0 -s
192.168.100.0/255.255.255.0
-s 192.168.100.0/255.255.255.0 -i xscf#0-lan#0 -j ACCEPT
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y

<Example 2> Communication to xscf#0-lan#0 exclusively
accepts those IP packets sent from the 192.168.100.0/255.255.255.0
network.
XSCF> showpacketfilters -a
-s 192.168.100.0/255.255.255.0 -i xscf#0-lan#0 -j ACCEPT
XSCF>
XSCF> setpacketfilters -y -c add -i xscf#0-lan#0 -j DROP
-s 192.168.100.0/255.255.255.0 -i xscf#0-lan#0 -j ACCEPT
-i xscf#0-lan#0 -j DROP
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
XSCF>
XSCF> showpacketfilters -a
-s 192.168.100.0/255.255.255.0 -i xscf#0-lan#0 -j ACCEPT
-i xscf#0-lan#0 -j DROP

<Example 3> Deletes the IP packet drop setting which has been set
in the IP address 10.10.10.10.
XSCF> showpacketfilters -a
-s 172.16.0.0/255.255.0.0 -i xscf#0-lan#0 -j DROP
-s 10.10.10.10 -j DROP
XSCF>
XSCF> setpacketfilters -y -c del -s 10.10.10.10 -j DROP
-s 172.16.0.0/255.255.0.0 -i xscf#0-lan#0 -j DROP
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
XSCF>
XSCF> showpacketfilters -a
-s 172.16.0.0/255.255.0.0 -i xscf#0-lan#0 -j DROP

<Example 4> Clears all IP packet filtering rules which have been
set.
XSCF> setpacketfilters -c clear
-s 172.16.0.0/255.255.0.0 -i xscf#0-lan#0 -j DROP
(none)
NOTE: applied IP packet filtering rules.
Continue? [y|n] :y
```

Note – You can set the IP filtering rules to the input packets, not to the output packets.

Applying the XSCF Network Settings

- Command operation

1. **After performing the** `setnetwork`**(8),** `sethostname`**(8),** `setroute`**(8), and** `setnameserver`**(8) commands, apply these Network settings.**

2. **Perform the** `applynetwork`**(8) command on the XSCF Shell. When performing the command, the network settings are displayed and you can confirm whether the settings should be applied.**

```
XSCF> applynetwork
The following network settings will be applied:
  xscf#0 hostname  :scf0-hostname
  DNS domain name  :company.com
  nameserver       :10.0.0.2
  nameserver       :172.16.0.2
  nameserver       :192.168.0.2
  search           :company1.com

  interface        :xscf#0-lan#0
  status           :up
  IP address       :192.168.1.10
  netmask          :255.255.255.0
  route            :-n 192.168.1.0 -m 255.255.255.0 -g 192.168.1.1

  interface        :xscf#0-lan#1
  status           :down
  IP address       :
  netmask          :
  route            :

Continue? [y|n] :y
```

Note – When the XSCF Unit is in redundant configuration, ISN addresses must be in the same network subnet.

3. **Use the** `rebootxscf`**(8) command to reset the XSCF and to complete the settings.**

```
XSCF> rebootxscf
The XSCF will be reset. Continue? [y|n] :y
```

- At this time, the window session is disconnected, so please reconnect to the XSCF by using the new network interface and log in again.

4. **Display the Network Configuration by using the** `shownetwork`**(8),** `showhostname`**(8),** `showroute`**(8) and** `shownameserver`**(8) commands again and check the new network information.**

5. **Use the** `nslookup`**(8) command to check the host name information.**

```
<Example> Specify the host name information scf0-hostname.
XSCF> nslookup scf0-hostname
Server:         server.example.com
Address:        192.168.1.3

Name:           scf0-hostname.company.com
Address:        192.168.10.10
```

Confirm XSCF Network Connection Status

- Command operation

1. **Use the** `shownetwork`**(8) command to display the network status.**

```
XSCF> shownetwork -i
Active Internet connections (without servers)
Proto Recv-Q Send-Q Local Address          Foreign Address        State
tcp        0      0 xx.xx.xx.xx:telnet     xxxx:1617              ESTABLISHE
D
```

2. **Use the** `ping`**(8) command to confirm the response to network devices.**

```
<Example> Send packet to the host name scf0-hostname three times.
XSCF> ping -c 3 scf0-hostname
PING scf0-hostname (XX.XX.XX.XX): 56 data bytes
64 bytes from XX.XX.XX.XX: icmp_seq=0 ttl=64 time=0.1 ms
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=64 time=0.1 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=64 time=0.1 ms

--- scf0-hostname ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.1/0.1 ms
```

3. **Use the `traceroute`(8) command to confirm the network path to network devices.**

```
<Example> Display the network path to the host server.example.com.
XSCF> traceroute server.example.com
traceroute to server.example.com (XX.XX.XX.XX), 30 hops max, 40 byte packets
 1  XX.XX.XX.1 (XX.XX.XX.1)  1.792 ms  1.673 ms  1.549 ms
 2  XX.XX.XX.2 (XX.XX.XX.2)  2.235 ms  2.249 ms  2.367 ms
 3  XX.XX.XX.3 (XX.XX.XX.3)  2.199 ms  2.228 ms  2.361 ms
 4  XX.XX.XX.4 (XX.XX.XX.4)  2.516 ms  2.229 ms  2.357 ms
 5  XX.XX.XX.5 (XX.XX.XX.5)  2.546 ms  2.347 ms  2.272 ms
 6  server.example.com (XX.XX.XX.XX)  2.172 ms  2.313 ms  2.36 ms
```

Note – The confirming functions of the XSCF network by `ping`(8) and `traceroute`(8) commands are supported only on M3000/M4000/M5000/M8000/M9000 servers that run certain versions of XCP firmware (beginning with XCP 1080).

2.2.2 User Account Administration

User account administration is used to specify XSCF local user accounts, passwords, and user privileges and the password policy.

To manage user accounts, you can either configure the XSCF local accounts or you can configure the user accounts to authenticate against a remote user database, such as LDAP, Active Directory, or LDAP/SSL. For details of setting LDAP, Active Directory, and LDAP/SSL, see Section 2.2.3, "LDAP Administration" on page 2-44, Section 2.2.4, "Active Directory Administration" on page 2-49., and Section 2.2.5, "LDAP/SSL Administration" on page 2-71.

TABLE 2-3 lists a term used in user account administration.

TABLE 2-3 User Account Administration Term

Term	Description
UID	ID that is assigned automatically to a user account. Also, the UID can be specified. The ID values start from 100 and end at 60000.
Lockout function	After multiple failures of login tried with a certain user account, this function locks out the subsequent login trials with that user account for a certain period of time. You can use this function at logging in by SSH, telnet on XSCF Shell and XSCF Web.

TABLE 2-4 lists setting items and the corresponding shell commands.

TABLE 2-4 User Account Administration

Item	Description	Shell Command	Remarks
Display user account management information	Displays user account management information.	`showuser`	The item displayed is Never, which means unlimited.
Add/delete user account	Adds or deletes a user account.	`adduser` `deleteuser`	The maximum length of a user account is 31 characters.
Password	Sets a user account password. • Specify whether to use a specific number of days or specific date for the account validity period. Or specify no expiration. Specify the following for the password: (Note) • Maximum number of days in the password validity period (up to 999999999 days) • Minimum number of days in the password validity period (minimum 0 days) • Password expiration warning date (seven days in advance by default) • Number of days in which the account remains unlocked after expiration of the password (minimum 0 days, or no limit)	`password`	
Change user privilege	Assigns a user privilege to a user.	`setprivileges`	Multiple user privileges can be assigned to one user.
Enable/ disable user account	Enables or disables a user account.	`enableuser` `disableuser`	
Display password policy	Displays a password policy.	`showpassword-policy`	

TABLE 2-4 User Account Administration *(Continued)*

Item	Description	Shell Command	Remarks
Password policy	Sets a password policy as described below. • Minimum number of days that must elapse before the password can be changed (Mindays) • Maximum number of days that the password is valid (Maxdays) • Number of days preceding password expiration, for the first warning (Warn) • Number of days in which the account remains unlocked after password expiration (Inactive) • Number of days a new account will be valid before expiring and becoming disabled. (Expiry) • Maximum number of retries of password entry (Retry) • Maximum number of characters that must be different in a new password.(Difok) • Minimum password length (Minlen) • Number of maximum credit to the minimum password length by digits contained in a password (Dcredit) • Number of maximum credit to the minimum password length by uppercase letters contained in a password (Ucredit) • Number of maximum credit to the minimum password length by lowercase letters contained in a password (Lcredit) • Number of maximum credit to the minimum password length by symbols contained in a password (Ocredit) • Maximum numbers of passwords in the password history (Remember)	`setpassword-policy`	• Once an account is locked after password expiration, its user must contact the system administrator in order to use the system again. • A password must consist of at least six characters. • Inactive is -1, which means unlimited. • Expiry is 0, which means unlimited. (Note 1) • The number of credit is the number of reduced character from the current minimum password length. When the credit of each character is combined, a shorter password than the current minimum password length can be accepted.
Display lockout setting	Displays lockout settings.	`showloginlockout`	

TABLE 2-4 User Account Administration *(Continued)*

Item	Description	Shell Command	Remarks
Enable/disable lockout function	Enables or disables the lockout function. To disable the lockout, specify 0 minutes for lockout period. To enable lockout, specify a period other than 0 minutes.	`setloginlockout`	• The lockout is disabled by default. • After three sequential login failures, it locks out the user login for a specified period of time. • Range of the lockout period is 0 to 1440 minutes. (Note 2)

Note – (1) If the password policy is set, then the password policy is applied to the users added after that. When you change the password for another user by using the user operand, they system password policy is not enforced. When changing another user's password, be sure to choose a password that conforms with the system password policy.

Note – (2) After the login authentication failure, XSCF locks out the user login for a period of time that specified in the last account lockout setting. On the M8000/M9000 servers, the account lockout function is enabled in both active/standby XSCF. When the user login locked out, a message will be saved in the audit log. The `setloginlockout -s 0` will disable the account lockout. When the account lockout is disabled, a user can attempt to login, and fail, an unlimited number of times. If a user needs to access their locked account before the lockout time is complete they must get an administrator to disable the account lockout to allow them to login and then re-enable the lockout by setting a lockout time. For more information, see the `setloginlockout`(8) and `showloginlockout`(8) man pages.

Note – The ability to specify and view the lockout period is supported in XCP1080 and later.

Adding or Deleting a User Account and Specifying a Password

- Command operation

1. **Use the** `showuser`**(8) command to display all of the user account information. (See the description of the password policy in TABLE 2-4.)**

```
XSCF> showuser -l
User Name:          user001
UID:                101
Status:             Enabled
Minimum:            0
Maximum:            99999
Warning:            7
Inactive:           -1
Last Change:        Jul 11, 2006
Password Expires:   Never
Password Inactive:  Never
Account Expires:    Never
Privileges:         platadm
```

2. **Use the** `adduser`**(8) command to add a user account.**

```
<Example 1> Specify a user account name.
XSCF> adduser jsmith

<Example 2> Specify a UID for a user account.
XSCF> adduser -u 359 jsmith
```

If the XSCF is configured to use LDAP, Active Directory, or LDAP/SSL for user account data, the user name and UID (if specified) must not already be in use locally or in LDAP, Active Directory, or LDAP/SSL.

Note – You cannot use the following user account names, as they are reserved for system use: root, bin, daemon, adm, operator, nobody, sshd, rpc, rpcuser, ldap, apache, ntp, admin, default, or proxyuser.

---

3. **Use the** `password`**(8) command to specify a password.**

```
<Example 1> Specify a password.
XSCF> password jsmith
Changing password for platadm
(current) XSCF password: xxxxxx
New XSCF password: xxxxxx
BAD PASSWORD: is too similar to the old one
New XSCF password: xxxxxx
BAD PASSWORD: it is too simplistic/systematic
New XSCF password: xxx
BAD PASSWORD: it’s WAY too short
New XSCF password: xxxxxx
Retype new XSCF password: xxxxxx
XSCF>

<Example 2> Specify 60 days for the validity period, and also
specify that a validity expiration warning be issued 15 days in
advance.
XSCF> password -M 60 -w 15 jsmith
```

Specifying a User Privilege

- Command operation

1. **Use the** `showuser`**(8) command to display user account settings.**

```
XSCF> showuser -a
User Name:         jsmith
Status:            Enabled
Minimum:           0
Maximum:           99999
Warning:           7
Inactive:          -1
Last Change:       Aug 22, 2005
Password Expires:  Never
Password Inactive: Never
Account Expires:   Never
```

2. **Use the** `setprivileges`**(8) command to assign a user privilege to a user account.**

```
<Example> Specify useradm and auditadm for a user account.
XSCF> setprivileges jsmith useradm auditadm
```

3. **Use the** showuser**(8) command to confirm the privilege.**

```
XSCF> showuser -p
User Name:          jsmith
Privileges:         useradm
                    auditadm
```

Enabling or Disabling a User Account

- Command operation

1. **Use the** showuser**(8) command to display user account settings.**

```
XSCF> showuser -a
```

2. **Use the** enableuser**(8) command to enable a user account.**

```
<Example> Enable a user account.
XSCF> enableuser jsmith
```

Specifying a Password Policy

- Command operation

1. **Use the** showpasswordpolicy**(8) command to display password policy settings.**

```
XSCF> showpasswordpolicy
Mindays:  0
Maxdays:  90
Warn:     7
Inactive: -1
Expiry:   0
Retry:    5
Difok:    1
Minlen:   8
Dcredit:  0
Ucredit:  0
Lcredit:  0
Ocredit:  0
Remember: 4
```

2. **Use the** `setpasswordpolicy`**(8) command to specify a password policy.**

```
<Example> Specify 3 for the retry count, an eight-character
password containing at least two digits, 60 days for the expiration
period, and 15 days for the advance notice of expiration.
XSCF> setpasswordpolicy -y 3 -m 8 -d 2 -u 0 -l 0 -o 0 -M 60 -w 15
```

3. **Use the** `showpasswordpolicy`**(8) command to confirm the settings.**

```
XSCF> showpasswordpolicy
Mindays:  0
Maxdays:  60
Warn:     15
Inactive: -1
Expiry:   0
Retry:    3
Difok:    1
Minlen:   8
Dcredit:  2
Ucredit:  0
Lcredit:  0
Ocredit:  0
Remember: 3
```

Enabling or Disabling the Lockout Function

- Command operation

1. **Use the** `showloginlockout`**(8) command to display lockout settings.**

```
XSCF> showloginlockout
```

2. **Use the** `setloginlockout`**(8) command to set lockout function.**

```
<Example 1> Enable the lockout function to specify 20 minutes for
the lockout period.
XSCF> setloginlockout -s 20
<Example 2> Disable the lockout function
XSCF> setloginlockout -s 0
```

The lockout period becomes effective at the next login. When you specifies 0 minutes, if someone login successfully by a user account at the next time, the lockout function will be disabled.

2.2.3 LDAP Administration

LDAP administration is used to specify items relating to LDAP clients. The LDAP server, bind ID, password, baseDN and so on are set. In the LDAP server, the XSCF user information is managed.

Note – This section does not cover LDAP configuration and administration. An administrator who is familiar with LDAP should perform the LDAP design. For details on adding user information to an account on an LDAP server, see the *Administration Guide*.

TABLE 2-5 lists terms used in LDAP Administration.

TABLE 2-5 LDAP Administration Terms

Term	Description
LDAP	Abbreviation for Lightweight Directory Access Protocol. LDAP is a protocol used to access directory databases in TCP/IP networks.
baseDN	Abbreviation for base Distinguished name. Under LDAP, directory information is in a hierarchical structure. To perform a search, specify the subtree to be searched in the hierarchical structure. To do so, specify the identification name (DN) of the top of the target subtree. This DN is referred to as the search base (basedDN).
Certificate chain	List of certificates including a user certificate and certification authority certificate. OpenSSL and TLS certificates must be downloaded in advance.
TLS	Abbreviation for Transport Layer Security. This is a protocol for encrypting information for transmission via the Internet.

TABLE 2-6 lists setting items and the corresponding shell commands:

TABLE 2-6 LDAP Administration

Item	Description	Shell command	Remarks
Display the use of LDAP	Displays the use of an LDAP server for authentication and privilege lookup.	`showlookup`	
Enable/ disable the use of LDAP	Enables or disables the use of an LDAP server for authentication and privilege lookup.	`setlookup`	If this specifies that authentication data and user privilege data be placed together on an LDAP server, the system first searches the local area, and it searches the LDAP server only if the target data is not found locally.
Display client	Displays LDAP client setting information.	`showldap`	
Bind ID	Bind an ID for a connection to (bind: authenticate) an LDAP server.	`setldap`	Bind ID maximum length is 128 characters.
password	Sets a password used to bind an LDAP server.	`setldap`	A password can consist of 8 to 16 characters.
Search base	Sets an LDAP tree search base (baseDN).	`setldap`	• If this item is omitted, the command searches the tree, beginning from the top. • Search base maximum length is 128 characters.
Certificate chain	Imports the certificate chain of an LDAP server. Import a certificate chain as follows: • Import a secure copy (scp) from a remote file.	`setldap`	• The certificate chain must be in PEM format. (Note 1) • A password may need to be entered to import an scp from a remote file.
LDAP server/port	Specify the IP addresses and port numbers of the primary and secondary LDAP servers. Specify IP addresses or host names for the addresses. (e.g. `ldap://foobar.east,` `ldaps://10.8.31.14:636`)	`setldap`	The default LDAP port number is 636 for ldaps, 389 for ldap when the port number is not specified.
Timeout	Sets the maximum time (seconds) allowed for an LDAP search.	`setldap`	
LDAP test	Tests the connection to an LDAP server.	`setldap`	

Note – PEM: Abbreviation for Privacy Enhanced Mail. Mail to be sent is encrypted for increased privacy.

Enabling or Disabling the LDAP Server

- Command operation

1. **Use the** `showlookup`**(8) command to display the lookup method of authentication and user privileges.**

```
XSCF> showlookup
Privileges lookup: Local only
Authentication lookup: Local and LDAP
```

2. **Use the** `setlookup`**(8) command to enable or disable the LDAP server.**

```
<Example> Enable the use of LDAP server for both user
authentication and user privilege.
XSCF> setlookup -a ldap
XSCF> setlookup -p ldap
```

3. **Use the** `showlookup`**(8) command to confirm the lookup method.**

```
XSCF> showlookup
Privileges lookup: Local and LDAP
Authentication lookup: Local and LDAP
```

Specifying an LDAP Server, Port Number, Bind ID, Bind Password, Search Base (BaseDN) and Search Time (Timeout Period)

- Command operation

1. **Use the** `showldap`**(8) command to display LDAP client settings.**

```
XSCF> showldap
Bind Name:               Not set
Base Distinguished Name: Not set
LDAP Search Timeout:     0
Bind Password:           Not set
LDAP Servers:            Not set
CERTS:                   None
```

2. **Use the** setldap**(8) command to configure an LDAP client.**

```
<Example 1> Specify bind ID and search base (baseDN).
XSCF> setldap -b "cn=Directory Manager" -B "ou=People,dc=users,dc=
apl,dc=com,o=isp"

<Example 2> Specify bind password.
XSCF> setldap -p
Password:xxxxxxxx

<Example 3> Specify the primary and secondary LDAP servers and port
numbers.
XSCF> setldap -s ldap://onibamboo:389,ldaps://company2.com:636

<Example 4> Specify the timeout period for LDAP search.
XSCF> setldap -T 60
```

3. **Use the** showldap**(8) command to confirm the setting.**

```
XSCF> showldap
Bind Name:                 cn=Directory Manager
Base Distinguished Name: ou=People,dc=users,dc=apl,dc=com,o=isp
LDAP Search Timeout:       60
Bind Password:             Set
LDAP Servers:              ldap://onibamboo:389 ldaps://company2.com:636
CERTS:                     None
```

Installing the Certificate Chain of an LDAP Server

- Command operation

1. **Use the** showldap**(8) command to display the LDAP setting.**

```
XSCF> showldap
Bind Name:                 cn=Directory Manager
Base Distinguished Name: ou=People,dc=users,dc=apl,dc=com,o=isp
LDAP Search Timeout:       60
Bind Password:             Set
LDAP Servers:              ldap://onibamboo:389 ldaps://company2.com:636
CERTS:                     None
```

2. **Use the** setldap**(8) command to import the certificate chain.**

```
XSCF> setldap -c hhhh@example.com:Cert.pem
```

3. **Use the** `showldap`**(8) command to confirm that you have imported the certificate chain.**

```
XSCF> showldap
Bind Name:                cn=Directory Manager
Base Distinguished Name: ou=People,dc=users,dc=apl,dc=com,o=isp
LDAP Search Timeout:      60
Bind Password:            Set
LDAP Servers:             ldap://onibamboo:389 ldaps://company2.com:636
CERTS:                    Exists
```

Testing a Connection to an LDAP Server

- Command operation

1. **Use the** `setldap`**(8) command to perform the test.**

```
XSCF> setldap -t sysadmin
onibamboo:389      PASSED
```

2. **Log in as the user created in the LDAP server. Confirm the registration using the user's password.**

```
login: sysadmin
Password:xxxxxxxx
```

3. **Use the** `showuser`**(8) command to confirm whether the displayed privilege is the same as the one created in the LDAP server.**

```
XSCF> showuser
User Name:         sysadmin (nonlocal)
UID:               110
Privileges:        platadm
```

2.2.4 Active Directory Administration

Active Directory administration is used to specify items relating to Active Directory clients. The Active Directory server, loading of server certificate, group name, privileges, user domain, log, DNS locator query, and so on are set. In the Active Directory server, the XSCF user information is managed.

Note – This section does not cover Active Directory configuration and administration. An administrator who is familiar with Active Directory should perform the Active Directory design.

TABLE 2-7 lists terms used in Active Directory Administration.

TABLE 2-7 Active Directory Administration Terms

Term	Description
Active Directory	Active Directory is a distributed directory service from Microsoft Corporation. Like an LDAP directory service, it is used to authenticate users.
User domain	User domain is the authentication domain used to authenticate a user.
DNS locator query	The query is used to query DNS server to determine the Active Directory server to use for user authentication.

Active Directory provides both authentication of user credentials and authorization of the user access level to networked resources. Active Directory uses authentication to verify the identity of users before they can access system resources, and to grant specific access privileges to users in order to control their rights to access networked resources.

User privileges are either configured on XSCF or learned from a server based on each user's group membership in a network domain. A user can belong to more than one group. User domain is the authentication domain used to authenticate a user. Active Directory authenticates users in the order in which the users' domains are configured.

Once authenticated, user privileges can be determined in the following ways:

- In the simplest case, user’s privileges are determined directly through the Active Directory configuration on the XSCF. There is a defaultrole parameter for Active Directory. If this parameter is configured or set, all users authenticated via Active Directory are assigned privileges set in this parameter. Setting up users in an Active Directory server requires only a password with no regard to group membership.

- If the defaultrole parameter is not configured or set, user privileges are learned from the Active Directory server based on the user's group membership. On XSCF, the group parameter must be configured with the corresponding group name from the Active Directory server. Each group has privileges associated with it which are configured on the XSCF. A user's group membership is used to determine the user's privileges once authenticated.

TABLE 2-8 lists setting items and the corresponding shell commands:

TABLE 2-8 Active Directory Administration

Item	Description	Shell command	Remarks
Display the status of Active Directory	Displays the current setting of Active Directory, such as enabled/disabled, DNS locator mode, and so on.	`showad`	
Enable/ disable the use of Active Directory	Enables or disables the use of an Active Directory server for managing authentication and privilege.	`setad`	Active Directory is disabled by default.
Display Active Directory server	Display the primary and up to five alternate Active Directory servers.	`showad`	A port number of "0" indicates that the default port for Active Directory is used.
Active Directory server/port	Sets an IP address or a port number of the primary and up to five alternate Active Directory servers. Specify IP addresses or host names for the addresses. If you specify a host name for an Active Directory server, the server name must be resolvable by DNS server.	`setad`	When the port number is not specified, the default port is used.
Enable/ disable DNS locator mode	Enables or disables the DNS locator mode.	`setad`	DNS locator mode is disabled by default.
Display DNS locator query	Display up to five DNS locator query.	`showad`	
DNS locator query	Configures the DNS locator query. The DNS locator query is used to query DNS server to determine the Active Directory server to use for user authentication.	`setad`	DNS and DNS locator mode must be enabled for DNS locator queries to work.

TABLE 2-8 Active Directory Administration *(Continued)*

Item	Description	Shell command	Remarks
Enable/ disable expanded search mode	Enables or disables the expanded search mode. The expanded search mode is only enabled when to address specific customer environment where user's account is not UserPrincipalName (UPN) format.	`setad`	The expanded search mode is disabled by default.
Enable/ disable strictcertmode	Enables or disables the strictcertmode. If strictcertmode is enabled, the server's certificate must have already been uploaded to the server so that the certificate signatures can be validated when the server certificate is presented.	`setad`	The strictcertmode is disabled by default.
Display server certificate	Displays the following • Certificate information for the primary and up to five alternate Active Directory servers. • The full certificate	`showad`	
Load/Delete certificate	Loads or deletes the certificate of primary and up to five alternate Active Directory servers.	`setad`	The strictcertmode must be in the disabled state for a certificate to be removed.
Display userdomain	Displays the userdomain.	`showad`	
Userdomain	Configures up to five userdomains. Userdomain can take the form of UPN like <USERNAME>@domainname or the form of Distinguished Name (DN) like "uid=<USERNAME>,ou= OrganizationUnit, dc= DomainName".	`setad`	If a user domain is specified directory by UPN form at the login prompt such as "login: ima.admin@dc01.example.com", that user domain is used for this login attempt.
Display defaultrole	Displays the defaultrole setting.	`showad`	
Defaultrole	All users authenticated via LDAP/SSL are assigned privileges set in this parameter.	`setad`	
Display group	Displays configuration of administrator group, operator group, or custom group.	`setad`	
Administrator group	Assigns group name for up to five specified administrator groups. The administrator group has platadm, useradm, and auditadm privileges and you cannot change that.	`setad`	

TABLE 2-8 Active Directory Administration *(Continued)*

Item	Description	Shell command	Remarks
Operator group	Assigns group name for up to five specified operator groups. The operator group has platop and auditop privileges and you cannot change that.	`setad`	
Custom group	Assigns group name and privileges for up to five groups.	`setad`	
Timeout	Configures transaction timeout, in seconds. seconds can be 1 to 20.	`setad`	The default is 4. If the specified timeout is too brief for the configuration, the login process or retrieval of user privilege settings could fail.
Enable/Disable log	Enables or Disables logging of Active Directory authentication and authorization diagnostic messages.	`setad`	This log is cleared on XSCF reset.
Display log	Displays Active Directory authentication and authorization diagnostic messages	`showad`	
Clear log	Clears log file of Active Directory authentication and authorization diagnostic messages.	`setad`	
Default	Resets Active Directory settings to factory default.	`setad`	

Before Active Directory settings

Note the following before settings:

- Active Directory is supported in XCP1091 or later.
- The useradm privilege is required for the Active Directory settings.
- If the XSCF is configured to use LDAP, Active Directory, or LDAP/SSL for user account data, the user name and UID (if specified) must not already be in use locally or in LDAP, Active Directory, or LDAP/SSL.
- To use host name for Active Directory server, DNS settings need to be configured properly before setting Active Directory.
- To support Active Directory, a new system account named proxyuser is added. Verify that no user account of that name already exists. If one does, use the deleteuser(8) command to remove it, then reset XSCF before using the Active Directory feature.

- While Active Directory is enabled, when you attempt to login to XSCF via the telnet, you might fail to login due to timeout of the query to secondary alternated server or later.
- If the specified timeout is too brief for the configuration, the login process or retrieval of user privilege settings could fail. In such case, specify larger value for the timeout and then try again.
- If you are an Active Directory user, you cannot upload a user public key. When you set the user public key to XSCF before XCP1100, delete the user public key. The Active Directory users can access to XSCF via SSH by using the password authentication and can login to XSCF.

Enabling or Disabling the Active Directory Server

- Command operation

1. **Use the `showad`(8) command to display the use of Active Directory server.**

```
XSCF> showad
dnslocatormode: disabled
expsearchmode: disabled
state: disabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

2. **Use the `setad`(8) command to enable or disable the use of Active Directory server.**

```
<Example1> Enable the use of Active Directory server.
XSCF> setad enable

<Example2> Disable the use of Active Directory server.
XSCF> setad disable
```

3. **Use the `showad`(8) command to confirm the use of Active Directory server.**

```
XSCF> showad
dnslocatormode: disabled
expsearchmode: disabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

Specifying an Active Directory Server and Port Number

- Command operation

1. **Use the** `showad`**(8) command to display Active Directory server settings.**

```
XSCF> showad server
Primary Server
    address: (none)
    port: 0

XSCF> showad server -i
Alternate Server  1
    address: (none)
    port: 0
Alternate Server  2
    address: (none)
    port: 0
Alternate Server  3
    address: (none)
    port: 0
Alternate Server  4
    address: (none)
    port: 0
Alternate Server  5
    address: (none)
    port: 0
```

2. **Use the** `setad`**(8) command to configure Active Directory servers.**

```
<Example 1> Specify the primary server and port number.
XSCF> setad server 10.24.159.150:8080

<Example 2> Specify the alternative server.
XSCF> setad server -i 1 10.24.159.151
```

3. **Use the** `showad`**(8) command to confirm the Active Directory server setting.**

```
XSCF> showad server
Primary Server
    address: 10.24.159.150
    port: 8080

XSCF> showad server -i
Alternate Server  1
    address: 10.24.159.151
    port: 0
Alternate Server  2
    address: (none)
    port: 0
Alternate Server  3
    address: (none)
    port: 0
Alternate Server  4
    address: (none)
    port: 0
Alternate Server  5
    address: (none)
    port: 0
```

Enabling or Disabling the DNS locator Mode

- Command operation

1. **Use the** `showad`**(8) command to display the DNS locator mode status.**

```
XSCF> showad
dnslocatormode: disabled
expsearchmode: disabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

2. **Use the** `setad`**(8) command to enable or disable the DNS locator mode.**

```
<Example1> Enable the DNS locator mode.
XSCF> setad dnslocatormode enable

<Example2> Disable the DNS locator mode.
XSCF> setad dnslocatormode disable
```

3. **Use the** `showad`**(8) command to confirm the DNS locator mode status.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: disabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

Configuring the DNS locator Query

- Command operation

1. **Use the** `showad`**(8) command to display the configuration of the DNS locator query.**

```
XSCF> showad dnslocatorquery -i 1
service 1: (none)

XSCF> showad dnslocatorquery -i 2
service 2: (none)
```

2. **Use the** `setad`**(8) command to configure the DNS locator query.**

```
XSCF> setad dnslocatorquery -i 1 '_ldap._tcp.gc._msdcs..'
```

3. **Use the** `showad`**(8) command to confirm the DNS locator query.**

```
XSCF> showad dnslocatorquery -i 1
service 1: _ldap._tcp.gc._msdcs..
```

DNS and DNS locator mode must be enabled for DNS locator queries to work.

Enabling or Disabling the Expanded Search Mode

- Command operation

1. Use the `showad`**(8) command to display the expanded search mode status.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: disabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

2. Use the `setad`**(8) command to enable or disable the expanded search mode.**

```
<Example1> Enable the expanded search mode.
XSCF> setad expsearchmode enable

<Example2> Disable the expanded search mode.
XSCF> setad expsearchmode disable
```

3. Use the `showad`**(8) command to confirm the expanded search mode status.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

Enabling or Disabling the Strictcert Mode

- Command operation

1. Use the `showad`**(8) command to display the strictcert mode status.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

2. **Use the `setad`(8) command to enable or disable the strictcertmode.**

```
<Example1> Enable the strictcertmode.
XSCF> setad strictcertmode enable

<Example2> Disable the strictcertmode.
XSCF> setad strictcertmode disable
```

3. **Use the `showad`(8) command to confirm the strictcertmode status.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 4
logdetail: none
```

If strictcertmode is enabled, the server's certificate must have already been uploaded to the XSCF.

Loading or Deleting the Server Certificate

- Command operation

1. Use the `showad`**(8) command to display the server certificate information.**

```
XSCF> showad cert

Primary Server:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)

XSCF> showad cert -i

Alternate Server 1:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)

Alternate Server 2:
...

Alternate Server 5:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)
```

2. **Use the `setad`(8) command to load the server certificate to the XSCF.**

```
<Example1> Loads a server certificate for the primary server using
a username and password
XSCF> setad loadcert -u yoshi http://domain_2/UID_2333/testcert
Warning: About to load certificate for Primary Server.
Continue? [y|n]: y
Password:

<Example2> Copy and paste the server certificate in the window to
load the certificate for alternative server 1 on the console.
Please press Enter and press the "Ctrl" and "D" keys. Then the
loading is completed.
XSCF> setad loadcert console
Warning: About to load certificate for Alternate Server 1:
Continue? [y|n]: y
Please enter the certificate:

-----BEGIN CERTIFICATE-----
MIIETjCCAzagAwIBAgIBADANBgkqhkiG9w0BAQQFADB8MQswCQYDVQQGEwJVUzET
MBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJU2FuIERpZWdvMRkwFwYDVQQK
ExBTdW4gTWljcm9zeXN0ZW1zMRUwEwYDVQQLEwxTeXN0ZW0gR3JvdXAxEjAQBgNV
...
-----END CERTIFICATE-----
<Press "Ctrl" and "D" keys>
```

3. **Use the** `showad`**(8) command to confirm that the server certificate is loaded.**

```
XSCF> showad cert

Primary Server:
certstatus = certificate present
issuer = DC = local, DC = xscf, CN = apl
serial number = 55:1f:ff:c4:73:f7:5a:b9:4e:16:3c:fc:e5:66:5e:5a
subject = DC = local, DC = xscf, CN = apl
valid from = Mar  9 11:46:21 2010 GMT
valid until = Mar  9 11:46:21 2015 GMT
version = 3 (0x02)

XSCF> showad cert -i 1

Alternate Server 1:
certstatus = certificate present
issuer = DC = local, DC = aplle, CN = aplle.local
serial number = 0b:1d:43:39:ee:4b:38:ab:46:47:de:0a:b4:a9:ea:04
subject = DC = local, DC = aplle, CN = aplle.local
valid from = Aug 25 02:38:15 2009 GMT
valid until = Aug 25 02:44:48 2014 GMT
version = 3 (0x02)
```

4. **Use the** `setad`**(8) command to delete the server certificate.**

```
XSCF> setad rmcert
Warning: About to delete certificate for Primary Server.
Continue? [y|n]: y
```

5. **Use the** `showad`**(8) command to confirm that the server certificate is deleted.**

```
XSCF> showad cert

Primary Server:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)
```

The strictcertmode must be in the disabled state for a certificate to be removed.

Setting a user domain

- Command operation

1. Use the `showad`**(8) command to display user domains.**

```
XSCF> showad userdomain
domain 1: (none)
domain 2: (none)
domain 3: (none)
domain 4: (none)
domain 5: (none)
```

2. Use the `setad`**(8) command to set the user domain.**

```
<Example1> Set the user domain 1.
XSCF> setad userdomain -i 1 ‘@davidc.example.aCompany.com’

<Example2> Set the user domain 2.
XSCF> setad userdomain -i 2 ‘CN=<USERNAME>,CN=Users,DC=davidc,DC=
example,DC=aCompany,DC=com’
```

3. Use the `showad`**(8) command to confirm the user domain.**

```
XSCF> showad userdomain
domain 1: <USERNAME>@davidc.example.aCompany.com
domain 2: CN=<USERNAME>,CN=Users,DC=davidc,DC=example,DC=
aCompany,DC=com
domain 3: (none)
domain 4: (none)
domain 5: (none)
```

If a user domain is specified at the login prompt, for example, “login:ima.admin@dc01.example.com”, that user domain is used for this login attempt.

Setting default roles

- Command operation

1. Use the `showad`**(8) command to display default roles.**

```
XSCF> showad defaultrole
Default role: (none)
```

2. **Use the** `setad`**(8) command to set default roles.**

```
XSCF> setad defaultrole platadm platop
```

3. **Use the** `showad`**(8) command to confirm the default roles.**

```
XSCF> showad defaultrole
Default role: platadm platop
```

Setting Group name and privileges

- Command operation

1. Use the `showad`**(8) command to display the group name.**

```
<Example1> Displays configuration for administrator group.
XSCF> showad group administrator
Administrator Group 1
    name: (none)
Administrator Group 2
    name: (none)
Administrator Group 3
    name: (none)
Administrator Group 4
    name: (none)
Administrator Group 5
    name: (none)

<Example2> Displays configuration for operator group.
XSCF> showad group operator
Operator Group 1
    name: (none)
Operator Group 2
    name: (none)
Operator Group 3
    name: (none)
Operator Group 4
    name: (none)
Operator Group 5
    name: (none)

<Example3> Displays configuration for custom group.
XSCF> showad group operator
Custom Group 1
    name: (none)
    roles: (none)
Custom Group 2
    name: (none)
    roles: (none)
Custom Group 3
    name: (none)
    roles: (none)
Custom Group 4
    name: (none)
    roles: (none)
Custom Group 5
    name: (none)
    roles: (none)
```

2. **Use the** `setad`**(8) command to set group name and privileges.**

```
<Example1> Sets administrator group 1.
XSCF> setad group administrator -i 1 name CN=SpSuperAdmin,OU=
Groups,DC=davidc,DC=example,DC=aCompany,DC=com

<Example2> Sets operator group 1.
XSCF> setad group operator -i 1 name CN=OpGroup1,OU=SCFTEST,DC=
aplle,DC=local

<Example3> Sets custom group 1.
XSCF> setad group custom -i 1 name CN=CtmGroup1,OU=SCFTEST,DC=
aplle,DC=local

<Example4> Sets privileges for custom group 1.
XSCF> setad group custom -i 1 roles platadm,platop
```

3. **Use the `showad(8)` command to confirm the group name and privileges.**

```
<Example1> Confirm administrator group.
XSCF> showad group administrator
Administrator Group 1
    name: CN=<USERNAME>,CN=SpSuperAdmin,OU=Groups,DC=davidc,DC=
example,DC=aCompany,DC=com
Administrator Group 2
    name: (none)
Administrator Group 3
    name: (none)
Administrator Group 4
    name: (none)
Administrator Group 5
    name: (none)

<Example2> Confirm operator group.
XSCF> showad group operator
Operator Group 1
    name: CN=OpGroup1,OU=SCFTEST,DC=aplle,DC=local
Operator Group 2
    name: (none)
Operator Group 3
    name: (none)
Operator Group 4
    name: (none)
Operator Group 5
    name: (none)

<Example3> Confirm custom group.
XSCF> showad group custom
Custom Group 1
    name: CN=CtmGroup1,OU=SCFTEST,DC=aplle,DC=local
    roles: platadm platop
Custom Group 2
    name: (none)
    roles: (none)
Custom Group 3
    name: (none)
    roles: (none)
Custom Group 4
    name: (none)
    roles: (none)
Custom Group 5
    name: (none)
    roles: (none)
```

The administrator group has platadm, useradm, and auditadm privileges and you cannot change that. Also the operator group has platop and auditop privileges and you cannot change that.

Setting timeout

- Command operation

1. **Use the** `showad`**(8) command to display timeout period.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 4
logdetail: none
```

2. **Use the** `setad`**(8) command to set the transaction timeout.**

```
<Example> The timeout priod is set to 10 sec.
XSCF> setad timeout 10
```

3. **Use the** `showad`**(8) command to confirm the timeout.**

```
XSCF> showad defaultrole
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: none
```

Enabling or Disabling the Logging of Active Directory Authentication and Authorization Diagnostic Messages

- Command operation

1. Use the `showad`**(8) command to display the log detail level.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: none
```

2. Use the `setad`**(8) command to set the log detail level.**

```
<Example1> Enable the log and trace is set for detail level.
XSCF> setad logdetail trace

<Example2> Disable the log.
XSCF> setad logdetail none
```

3. Use the `showad`**(8) command to confirm the log detail level.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: trace
```

Display the Diagnostic Messages and Clear the Log File

- Command operation

1. Use the `showad`**(8) command to display the log detail level.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: trace
```

2. **Use the** `showad`**(8) command to display the diagnostic messages.**

```
<Example> Displays diagnostic messages in real time.
XSCF> showad log -f
Mon Nov 16 14:47:53 2009 (ActDir): module loaded, OPL
Mon Nov 16 14:47:53 2009 (ActDir): --error-- authentication status:
auth-ERROR
Mon Nov 16 14:48:18 2009 (ActDir): module loaded, OPL
...
```

3. **Use the** `setad`**(8) command to clear the log file of diagnostic messages.**

```
XSCF> setad log clear
Warning: About to clear log file.
Continue? [y|n]: y
```

Change the Active Directory Settings Back to the Default

- Command operation

1. **Use the** `showad`**(8) command to display the Active Directory settings.**

```
XSCF> showad
dnslocatormode: enabled
expsearchmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: trace
```

2. **Use the** `setad`**(8) command to change the Active Directory setting back to the default.**

```
XSCF> setad default -y
Warning: About to reset settings to default.
Continue? [y|n]: y
```

3. **Use the** `showad`**(8) command to confirm the default settings.**

```
XSCF> showad
dnslocatormode: disabled
expsearchmode: disabled
state: disabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

2.2.5 LDAP/SSL Administration

LDAP/SSL administration is used to specify items relating to LDAP/SSL clients. The LDAP/SSL server, loading of server certificate, group name, privileges, user domain, log, and so on are set. In the LDAP/SSL server, the XSCF user information is managed.

Note – This section does not cover LDAP/SSL configuration and administration. An administrator who is familiar with LDAP/SSL should perform the LDAP/SSL design.

TABLE 2-9 lists terms used in LDAP/SSL Administration.

TABLE 2-9 LDAP/SSL Administration Terms

Term	Description
LDAP/SSL	LDAP/SSL is a distributed directory service like Active Directory. LDAP/SSL offers enhanced security to LDAP users by way of Secure Socket Layer (SSL) technology. Like an LDAP directory service, it is used to authenticate users.

LDAP/SSL provides both authentication of user credentials and authorization of the user access level to networked resources. LDAP/SSL uses authentication to verify the identity of users before they can access system resources, and to grant specific access privileges to users in order to control their rights to access networked resources.

User privileges are either configured on XSCF or learned from a server based on each user's group membership in a network domain. A user can belong to more than one group. User domain is the authentication domain used to authenticate a user. LDAP/SSL authenticates users in the order in which the users' domains are configured.

Once authenticated, user privileges can be determined in the following ways:

In the simplest case, user's privileges are determined directly through the LDAP/SSL configuration on the XSCF. There is a defaultrole parameter for LDAP/SSL. If this parameter is configured or set, all users authenticated via LDAP/SSL are assigned privileges set in this parameter. Setting up users in an LDAP/SSL server requires only a password with no regard to group membership.

If the defaultrole parameter is not configured or set, user privileges are learned from the LDAP/SSL server based on the user's group membership. On XSCF, the group parameter must be configured with the corresponding group name from the

LDAP/SSL server. Each group has privileges associated with it which are configured on the XSCF. A user's group membership is used to determine the user's privileges once authenticated.

TABLE 2-10 lists setting items and the corresponding shell commands:

TABLE 2-10 LDAP/SSL Administration

Item	Description	Shell command	Remarks
Display the status of LDAP/SSL	Displays the current setting of LDAP/SSL, such as enabled/disabled, usermapmode, and so on.	`showldapssl`	
Enable/ disable the use of LDAP/SSL	Enables or disables the use of an LDAP/SSL server for managing authentication and privilege.	`setldapssl`	LDAP/SSL is disabled by default.
Display LDAP/SSL server	Display the primary and up to five alternate LDAP/SSL servers.	`showldapssl`	A port number of "0" indicates that the default port for LDAP/SSL is used.
LDAP/SSL server/port	Sets an IP address or a port number of the primary and up to five alternate LDAP/SSL servers. Specify IP addresses or host names for the addresses. If you specify a host name for an LDAP/SSL server, the server name must be resolvable by DNS server.	`setldapssl`	When the port number is not specified, the default port is used.
Enable/ disable usermapmode	Enables or disables the usermapmode. When enabled, user attributes specified with the usermap operand, rather than userdomain, are used for user authentication.	`setldapssl`	The usermapmode is disabled by default.
Display usermap	Display the settings of usermap.	`showldapssl`	
Usermap	Configures the usermap. The usermap is used for user authentication.	`setldapssl`	The usermapmode must be enabled for using usermap.
Enable/ disable strictcertmode	Enables or disables the strictcertmode. If strictcertmode is enabled, the server's certificate must have already been uploaded to the server so that the certificate signatures can be validated when the server certificate is presented.	`setldapssl`	The strictcertmode is disabled by default.
Display server certificate	Displays the following • Certificate information for the primary and up to five alternate LDAP/SSL servers. • The full certificate	`showldapssl`	

TABLE 2-10 LDAP/SSL Administration *(Continued)*

Item	Description	Shell command	Remarks
Load/Delete certificate	Loads or deletes the certificate of primary and up to five alternate LDAP/SSL servers.	`setldapssl`	The strictcertmode must be in the disabled state for a certificate to be removed.
Display userdomain	Displays the userdomain.	`showldapssl`	
Userdomain	Configures up to five userdomains. Userdomain can take the form of Distinguished Name (DN).	`setldapssl`	
Display defaultrole	Displays the defaultrole setting.	`showldapssl`	
Defaultrole	All users authenticated via LDAP/SSL are assigned privileges set in this parameter.	`setldapssl`	
Display group	Displays configuration of administrator group, operator group, or custom group.	`setldapssl`	
Administrator group	Assigns group name for up to five specified administrator groups. The administrator group has platadm, useradm, and auditadm privileges and you cannot change that.	`setldapssl`	
Operator group	Assigns group name for up to five specified operator groups. The operator group has platop and auditop privileges and you cannot change that.	`setldapssl`	
Custom group	Assigns group name and privileges for up to five groups.	`setldapssl`	
Timeout	Configures transaction timeout, in seconds. Seconds can be 1 to 20.	`setldapssl`	The default is 4. If the specified timeout is too brief for the configuration, the login process or retrieval of user privilege settings could fail.
Enable/Disable log	Enables or Disables logging of LDAP/SSL authentication and authorization diagnostic messages.	`setldapssl`	This log is cleared on XSCF reset.
Display log	Displays LDAP/SSL authentication and authorization diagnostic messages	`showldapssl`	
Clear log	Clears log file of LDAP/SSL authentication and authorization diagnostic messages.	`setldapssl`	
Default	Resets LDAP/SSL settings to factory default.	`setldapssl`	

Before LDAP/SSL settings

Note the following before settings:

- LDAP/SSL is supported in XCP1091 or later.
- The useradm privilege is required for the LDAP/SSL settings.
- If the XSCF is configured to use LDAP, Active Directory, or LDAP/SSL for user account data, the user name and UID (if specified) must not already be in use locally or in LDAP, Active Directory, or LDAP/SSL.
- To use host name for LDAP/SSL server, DNS settings need to be configured properly before setting LDAP/SSL.
- To support LDAP/SSL, a new system account named proxyuser is added. Verify that no user account of that name already exists. If one does, use the deleteuser(8) command to remove it, then reset XSCF before using the LDAP/SSL feature.
- If the specified timeout is too brief for the configuration, the login process or retrieval of user privilege settings could fail. In such case, specify larger value for the timeout and try again.
- If you are an LDAP/SSL user, you cannot upload a user public key. When you set the user public key to XSCF before XCP1100, delete the user public key. The LDAP/SSL users can access to XSCF via SSH by using the password authentication and can login to XSCF.

Enabling or Disabling the LDAP/SSL Server

- Command operation

1. **Use the** `showldapssl`**(8) command to display the use of LDAP/SSL server.**

```
XSCF> showldapssl
usermapmode: disabled
state: disabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

2. **Use the** `setldapssl`**(8) command to enable or disable the use of LDAP/SSL server.**

```
<Example1> Enable the use of LDAP/SSL server.
XSCF> setldapssl enable

<Example2> Disable the use of LDAP/SSL server.
XSCF> setldapssl disable
```

3. **Use the** `showldapssl`**(8) command to confirm the use of LDAP/SSL server.**

```
XSCF> showldapssl
usermapmode: disabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

Specifying an LDAP/SSL Server and Port Number

- Command operation

1. **Use the** `showldapssl`**(8) command to display LDAP/SSL server settings.**

```
XSCF> showldapssl server
Primary Server
    address: (none)
    port: 0

XSCF> showldapssl server -i
Alternate Server  1
    address: (none)
    port: 0
Alternate Server  2
    address: (none)
    port: 0
Alternate Server  3
    address: (none)
    port: 0
Alternate Server  4
    address: (none)
    port: 0
Alternate Server  5
    address: (none)
    port: 0
```

2. **Use the** `setldapssl`**(8) command to configure LDAP/SSL servers.**

```
<Example 1> Specify the primary server and port number.
XSCF> setldapssl server 10.18.76.230:4041

<Example 2> Specify the alternative server.
XSCF> setldapssl server -i 1 10.18.76.231
```

3. **Use the** `showldapssl`**(8) command to confirm the LDAP/SSL server setting.**

```
XSCF> showldapssl server
Primary Server
    address: 10.18.76.230
    port: 4041

XSCF> showldapssl server -i
Alternate Server  1
    address: 10.18.76.231
    port: 0
Alternate Server  2
    address: (none)
    port: 0
Alternate Server  3
    address: (none)
    port: 0
Alternate Server  4
    address: (none)
    port: 0
Alternate Server  5
    address: (none)
    port: 0
```

Enabling or Disabling the Usermapmode

- Command operation

1. **Use the** `showldapssl`**(8) command to display the usermapmode status.**

```
XSCF> showldapssl
usermapmode: disabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

2. **Use the** `setldapssl`**(8) command to enable or disable the usermapmode.**

```
<Example1> Enable the usermapmode.
XSCF> setldapssl usermapmode enable

<Example2> Disable the usermapmode.
XSCF> setldapssl usermapmode disable
```

3. **Use the** `showldapssl`**(8) command to confirm the usermapmode status.**

```
XSCF> showldapssl
usermapmode: enabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

Configuring or Clearing the Usermap

- Command operation

1. **Use the** `showldapssl`**(8) command to display the configuration of the usermap.**

```
XSCF> showldapssl usermap
attributeInfo: (none)
binddn: (none)
bindpw: (none)
searchbase: (none)
```

2. **Use the** `setldapssl`**(8) command to configure the usermap.**

```
<Example1> Configures the attribute information.
XSCF> setldapssl usermap attributeInfo '(&(objectclass=
person)(uid=))'

<Example2> Configures the bind distinguished name.
XSCF> setldapssl usermap binddn CN=SuperAdmin,DC=aCompany,DC=com

<Example3> Configures the bind password.
XSCF> setldapssl usermap bindpw b.e9s#n

<Example4> Configures the search base.
XSCF> setldapssl usermap searchbase OU=yoshi,DC=aCompany,DC=com
```

3. **Use the** `showldapssl`**(8) command to confirm the usermap.**

```
XSCF> showldapssl usermap
attributeInfo: (&(objectclass=person)(uid=))
binddn: CN=SuperAdmin,DC=aCompany,DC=com
bindpw: Set
searchbase: OU=yoshi,DC=aCompany,DC=com
```

4. **Use the** `setldapssl`**(8) command to clear the usermap.**

```
<Example1> Clears the attribute information.
XSCF> setldapssl usermap attributeInfo

<Example2> Clears the bind distinguished name.
XSCF> setldapssl usermap binddn

<Example3> Clears the bind password.
XSCF> setldapssl usermap bindpw

<Example4> Clears the search base.
XSCF> setldapssl usermap searchbase
```

5. **Use the** `showldapssl`**(8) command to confirm that the usermap is cleared.**

```
XSCF> showldapssl usermap
attributeInfo: (none)
binddn: (none)
bindpw: (none)
searchbase: (none)
```

The usermapmode must be enabled for using usermap.

Enabling or Disabling the Strictcert Mode

- Command operation

1. **Use the** `showldapssl`**(8) command to display the strictcert mode status.**

```
XSCF> showldapssl
usermapmode: enabled
state: enabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

2. **Use the** `setldapssl`**(8) command to enable or disable the strictcertmode.**

```
<Example1> Enable the strictcertmode.
XSCF> setldapssl strictcertmode enable

<Example2> Disable the strictcertmode.
XSCF> setldapssl strictcertmode disable
```

3. **Use the `showldapssl`(8) command to confirm the strictcertmode status.**

```
XSCF> showldapssl
usermapmode: enabled
state: enabled
strictcertmode: enabled
timeout: 4
logdetail: none
```

If strictcertmode is enabled, the server's certificate must have already been uploaded to the XSCF.

Loading or Deleting the Server Certificate

- Command operation

1. Use the `showldapssl`**(8) command to display the server certificate information.**

```
XSCF> showldapssl cert

Primary Server:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)

XSCF> showldapssl cert -i

Alternate Server 1:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)

Alternate Server 2:
...

Alternate Server 5:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)
```

2. **Use the `setldapssl`(8) command to load the server certificate to the XSCF.**

```
<Example1> Loads a server certificate for the primary server using
a username and password
XSCF> setldapssl loadcert -u yoshi
http://domain_3/UID_2333/testcert
Warning: About to load certificate for Primary Server.
Continue? [y|n]: y
Password:

<Example2> Copy and paste the server certificate in the window to
load the certificate for alternative server 1 on the console.
Please press Enter and press the "Ctrl" and "D" keys. Then the
loading is completed.
XSCF> setldapssl loadcert console
Warning: About to load certificate for Alternate Server 1:
Continue? [y|n]: y
Please enter the certificate:

-----BEGIN CERTIFICATE-----
MIIETjCCAzagAwIBAgIBADANBgkqhkiG9w0BAQQFADB8MQswCQYDVQQGEwJVUzET
MBEGA1UECBMKQ2FsaWZvcm5pYTESMBAGA1UEBxMJU2FuIERpZWdvMRkwFwYDVQQK
ExBTdW4gTWljcm9zeXN0ZW1zMRUwEwYDVQQLEwxTeXN0ZW0gR3JvdXAxEjAQBgNV
...
-----END CERTIFICATE-----
<Press "Ctrl" and "D" keys>
```

3. **Use the** showldapssl**(8) command to confirm that the server certificate is loaded.**

```
XSCF> showldapssl cert

Primary Server:
certstatus = certificate present
issuer = DC = local, DC = xscf, CN = apl
serial number = 55:1f:ff:c4:73:f7:5a:b9:4e:16:3c:fc:e5:66:5e:5a
subject = DC = local, DC = xscf, CN = apl
valid from = Mar  9 11:46:21 2010 GMT
valid until = Mar  9 11:46:21 2015 GMT
version = 3 (0x02)

XSCF> showldapssl cert -i 1

Alternate Server 1:
certstatus = certificate present
issuer = DC = local, DC = aplle, CN = aplle.local
serial number = 0b:1d:43:39:ee:4b:38:ab:46:47:de:0a:b4:a9:ea:04
subject = DC = local, DC = aplle, CN = aplle.local
valid from = Aug 25 02:38:15 2009 GMT
valid until = Aug 25 02:44:48 2014 GMT
version = 3 (0x02)
```

4. **Use the** setldapssl**(8) command to delete the server certificate.**

```
XSCF> setldapssl rmcert
Warning: About to delete certificate for Primary Server.
Continue? [y|n]: y
```

5. **Use the** showldapssl**(8) command to confirm that the server certificate is deleted.**

```
XSCF> showldapssl cert

Primary Server:
certstatus = certificate not present
issuer = (none)
serial number = (none)
subject = (none)
valid from = (none)
valid until = (none)
version = (none)
```

The strictcertmode must be in the disabled state for a certificate to be removed.

Setting a user domain

- Command operation

1. **Use the** `showldapssl`**(8) command to display user domains.**

```
XSCF> showldapssl userdomain
domain 1: (none)
domain 2: (none)
domain 3: (none)
domain 4: (none)
domain 5: (none)
```

2. **Use the** `setldapssl`**(8) command to set the user domain.**

```
<Example1> Set the user domain 1.
XSCF> setldapssl userdomain -i 1 ‘@davidc.example2.aCompany.com’

<Example2> Set the user domain 2.
XSCF> setldapssl userdomain -i 2 ‘CN=<USERNAME>,CN=Users,DC=
davidc,DC=example2,DC=aCompany,DC=com’
```

3. **Use the** `showldapssl`**(8) command to confirm the user domain.**

```
XSCF> showldapssl userdomain
domain 1: <USERNAME>@davidc.example2.aCompany.com
domain 2: CN=<USERNAME>,CN=Users,DC=davidc,DC=example2,DC=
aCompany,DC=com
domain 3: (none)
domain 4: (none)
domain 5: (none)
```

Setting default roles

- Command operation

1. **Use the** `showldapssl`**(8) command to display default roles.**

```
XSCF> showldapssl defaultrole
Default role: (none)
```

2. **Use the** `setldapssl`**(8) command to set default roles.**

```
XSCF> setldapssl defaultrole platadm platop
```

3. **Use the** `showldapssl`**(8) command to confirm the default roles.**

```
XSCF> showldapssl defaultrole
Default role: platadm platop
```

Setting Group name and privileges

- Command operation

1. **Use the** `showldapssl`**(8) command to display the group name.**

```
<Example1> Displays configuration for administrator group.
XSCF> showldapssl group administrator
Administrator Group 1
    name: (none)
Administrator Group 2
    name: (none)
Administrator Group 3
    name: (none)
Administrator Group 4
    name: (none)
Administrator Group 5
    name: (none)

<Example2> Displays configuration for operator group.
XSCF> showldapssl group operator
Operator Group 1
    name: (none)
Operator Group 2
    name: (none)
Operator Group 3
    name: (none)
Operator Group 4
    name: (none)
Operator Group 5
    name: (none)

<Example3> Displays configuration for custom group.
XSCF> showldapssl group operator
Custom Group 1
    name: (none)
    roles: (none)
Custom Group 2
    name: (none)
    roles: (none)
Custom Group 3
    name: (none)
    roles: (none)
Custom Group 4
    name: (none)
    roles: (none)
Custom Group 5
    name: (none)
    roles: (none)
```

2. **Use the** `setldapssl`**(8) command to set group name and privileges.**

```
<Example1> Sets administrator group 1.
XSCF> setldapssl group administrator -i 1 name CN=SpSuperAdmin,OU=
Groups,DC=davidc,DC=example2,DC=aCompany,DC=com

<Example2> Sets operator group 1.
XSCF> setldapssl group operator -i 1 name CN=OpGroup1,OU=
SCFTEST,DC=aplle2,DC=local

<Example3> Sets custom group 1.
XSCF> setldapssl group custom -i 1 name CN=CtmGroup1,OU=SCFTEST,DC=
aplle2,DC=local

<Example4> Sets privileges for custom group 1.
XSCF> setldapssl group custom -i 1 roles platadm,platop
```

3. **Use the** `showldapssl`**(8) command to confirm the group name and privileges.**

```
<Example1> Confirm administrator group.
XSCF> showldapssl group administrator
Administrator Group 1
    name: CN=<USERNAME>,CN=SpSuperAdmin,OU=Groups,DC=davidc,DC=
example2,DC=aCompany,DC=com
Administrator Group 2
    name: (none)
Administrator Group 3
    name: (none)
Administrator Group 4
    name: (none)
Administrator Group 5
    name: (none)

<Example2> Confirm operator group.
XSCF> showldapssl group operator
Operator Group 1
    name: CN=OpGroup1,OU=SCFTEST,DC=aplle2,DC=local
Operator Group 2
    name: (none)
Operator Group 3
    name: (none)
Operator Group 4
    name: (none)
Operator Group 5
    name: (none)

<Example3> Confirm custom group.
XSCF> showldapssl group custom
Custom Group 1
    name: CN=CtmGroup1,OU=SCFTEST,DC=aplle2,DC=local
    roles: platadm platop
Custom Group 2
    name: (none)
    roles: (none)
Custom Group 3
    name: (none)
    roles: (none)
Custom Group 4
    name: (none)
    roles: (none)
Custom Group 5
    name: (none)
    roles: (none)
```

The administrator group has platadm, useradm, and auditadm privileges and you cannot change that. Also the operator group has platop and auditop privileges and you cannot change that.

Setting timeout

- Command operation

1. Use the `showldapssl`**(8) command to display timeout period.**

```
XSCF> showldapssl
usermapmode: enabled
state: enabled
strictcertmode: enabled
timeout: 4
logdetail: none
```

2. Use the `setldapssl`**(8) command to set the transaction timeout.**

```
<Example> The timeout priod is set to 10 sec.
XSCF> setldapssl timeout 10
```

3. Use the `showldapssl`**(8) command to confirm the timeout.**

```
XSCF> showldapssl defaultrole
usermapmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: none
```

Enabling or Disabling the Logging of LDAP/SSL Authentication and Authorization Diagnostic Messages

- Command operation

1. Use the `showldapssl`**(8) command to display the log detail level.**

```
XSCF> showldapssl
usermapmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: none
```

2. **Use the** `setldapssl`**(8) command to set the log detail level.**

```
<Example1> Enable the log and trace is set for detail level.
XSCF> setldapssl logdetail trace

<Example2> Disable the log.
XSCF> setldapssl logdetail none
```

3. **Use the** `showldapssl`**(8) command to confirm the log detail level.**

```
XSCF> showldapssl
usermapmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: trace
```

Display the Diagnostic Messages and Clear the Log File

- Command operation

1. **Use the** `showldapssl`**(8) command to display the log detail level.**

```
XSCF> showldapssl
usermapmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: trace
```

2. **Use the** `showldapssl`**(8) command to display the diagnostic messages.**

```
<Example> Displays diagnostic messages in real time.
XSCF> showldapssl log -f
Mon Nov 16 14:47:53 2009 (LdapSSL): module loaded, OPL
Mon Nov 16 14:47:53 2009 (LdapSSL): --error-- authentication
status: auth-ERROR
Mon Nov 16 14:48:18 2009 (LdapSSL): module loaded, OPL
...
```

3. **Use the** `setldapssl`**(8) command to clear the log file of diagnostic messages.**

```
XSCF> setldapssl log clear
Warning: About to clear log file.
Continue? [y|n]: y
```

Change the LDAP/SSL Settings Back to the Default

- Command operation

1. **Use the** showldapssl**(8) command to display the LDAP/SSL settings.**

```
XSCF> showldapssl
usermapmode: enabled
state: enabled
strictcertmode: enabled
timeout: 10
logdetail: trace
```

2. **Use the** setldapssl**(8) command to change the LDAP/SSL setting back to the default.**

```
XSCF> setldapssl default -y
Warning: About to reset settings to default.
Continue? [y|n]: y
```

3. **Use the** showldapssl**(8) command to confirm the default settings.**

```
XSCF> showldapssl
usermapmode: disabled
state: disabled
strictcertmode: disabled
timeout: 4
logdetail: none
```

2.2.6 Time Administration

Time administration is used to specify the time and the NTP settings for this system. The server (all domains) uses the XSCF Unit clock as the reference time.

Note – The customer should decide the NTP server operating mode. For details on NTP, see the NTP manuals.

The XSCF Unit can be optionally configured to be an NTP client. If you do not configure the XSCF Unit as an NTP client, the XSCF Unit will run its internal realtime clock (RTC) based on the `setdate`(8) command alone.

Domains can be configured to use a time-of-day management policy on an individual basis, so that each domain can manage its own time-of-day in a different manner. Domain time-of-day policies include:

- If no time or date configuration is done on the Oracle Solaris OS domain (that is, you do not set up the system as an NTP client and you do not use the Oracle Solaris OS `date` command to set the domain's date), the Oracle Solaris OS domain will obtain its initial time-of-day from the XSCF Unit.
- An Oracle Solaris OS domain can be set up as an NTP client with the XSCF Unit being the NTP server. In this case, the XSCF Unit must be set up as an NTP server. In this case, the Oracle Solaris OS domain will obtain its initial time-of-day from the XSCF NTP server, which will then be used to keep the Oracle Solaris domain and the XSCF unit in sync.
- An Oracle Solaris domain can be set up as an NTP client from an external NTP server. In this case, the initial time for Oracle Solaris OS will be obtained from the XSCF Unit. If you connect the domain to an external NTP server, connect a high rank NTP server that supplies the time at the same accuracy for the domain as for XSCF.
- If you use the Oracle Solaris OS `date` command to set the time on an Oracle Solaris OS domain, the time offset between the Oracle Solaris OS domain and the XSCF Unit will be preserved over reboots. Whenever the Oracle Solaris OS domain boots, its initial time-of- day will be the XSCF Unit time adjusted by the time offset created the last time the Oracle Solaris OS `date` command was used on the domain.

TABLE 2-11 lists the settings and the corresponding shell commands.

TABLE 2-11 Setting Time and Date

Item	Description	Shell Command	Remarks
Display time zone	Displays the time zone and Daylight Saving Time information.	`showtimezone`	
Time zone	Sets the time zone and Daylight Saving Time. • Standard time zone • Custom time zone and Daylight Saving Time For the abbreviations of time zone and the name of Daylight Saving Time, specify the alphabets of 3 letters or more. You can specify it in the format which complies with RFC2822.	`settimezone`	The time zone provided by default is pursuant to POSIX standard. The timezone list may be changed each year. The setting time zone list can be referred by specifying "-a" option.
Display system time	Displays the time and date of the XSCF by the local time or the Coordinated Universal Time (UTC).	`showdate`	
Date and time	Sets a date and time to a local time or UTC. The specification format is as follows: • yyyy.mm.dd-HH:MM:SS • mmddHHMMyyyy.SS yyyy: Year, mm: Month, dd: Day of the month, HH: Hour (24-hour system), MM: Minute, SS: Second	`setdate`	The settings can be enabled when all of the domains are powered off. XSCF reset is done after the settings.
Display NTP server settings	Displays NTP server settings	`showntp`	Synchronization is also checked.
NTP server	Configures an NTP server for XSCF network. (In this case, XSCF is an NTP client.) Specify the IP address or host name of an NTP server. You can synchronize with up to three NTP servers.	`setntp`	No default setting has been specified. When an NTP server is registered, the existing setting is deleted and overwriting is performed with the specified NTP server. If you specify a host name for an NTP server, the server name must be resolvable by DNS server.

TABLE 2-11 Setting Time and Date *(Continued)*

Item	Description	Shell Command	Remarks
Prefer	Specifies/cancels "prefer" to an NTP server for XSCF network. If prefer is specified, the NTP server specified first by `setntp` (8) command has priority over the others.	`setntp`	The default is prefer specified.
Stratum value	Specifies a stratum service for XSCF. You can specify an integer from 1 to 15.	`setntp`	The default `stratum` value is 5.
Local clock	Sets the clock address of the XSCF's own local clock. A numeric from 0 to 3 can be specified for the least significant byte of the clock address of the local clock.	`setntp`	The default clock address of the local clock is 127.127.1.0.
Reset time subtraction	Resets the time subtraction between the XSCF and each domain, which is stored in XSCF. As a result, the time of each domain will be set to the same time as the XSCF after startup.	`resetdateoffset`	The settings can be enabled when all of the domains are powered off.
Display time subtraction	Displays the time subtraction between the XSCF and each domain.	`showdateoffset`	

Specifying a Time Zone

- Command operation

1. **Use the** `showtimezone`**(8) command to display the time zone.**

```
XSCF> showtimezone -c tz
America/Chicago
```

2. **Use the** `settimezone`**(8) command to set the system time. The platadm privilege is required.**

```
<Example 1> Display the timezone list.
XSCF> settimezone -c settz -a
Africa/Abidjan
Africa/Accra
:

<Example 2> Set the timezone.
XSCF> settimezone -c settz -s Asia/Tokyo
Asia/Tokyo
```

The set time zone takes effect after executing the command.

3. **Use the** `showtimezone`**(8) command to confirm the setting.**

Specifying a Daylight Saving Time

- Command operation

1. **Use the** `showtimezone`**(8) command to display the time zone.**

```
<Example 1> Display the timezone.
XSCF> showtimezone -c tz
Asia/Tokyo

<Example 2> Displays the Daylight Saving Time information as
follows: the abbreviation of time zone is JST, the offset from GMT
is +9 hours, the name of Daylight Saving Time is JDT, Daylight
Saving Time is 1 hour ahead, and the time period is from the last
Sunday of March 2:00(JST) to the last Sunday of October 2:00(JDT).
XSCF> showtimezone -c dst -m custom
JST-9JDT,M3.5.0,M10.5.0
```

2. **Use the** `settimezone`**(8) command to set the Daylight Saving Time information.**

```
<Example 1> Sets the Daylight Saving Time information as follows:
abbreviation of time zone is JST, the offset from GMT is +9 hours,
the name of Daylight Saving Time is JDT, the offset of Daylight
Saving Time from GMT is +10 hours, and the time period is from the
first Sunday of April 0:00(JST) to the first Sunday of September
0:00(JDT).
XSCF> settimezone -c adddst -b JST -o GMT-9 -d JDT -p GMT-10 -f
M4.1.0/00:00:00 -t M9.1.0/00:00:00
JST-9JDT-10,M4.1.0/00:00:00,M9.1.0/00:00:00

<Example 2> Deletes the Daylight Saving Time information of current
settings.
XSCF> settimezone -c deldst -b JST -o GMT-9
```

   To reflect the Daylight Saving Time information which modified by `-c adddst` or `-c deldst` option, log out and then log in again.

3. **Use the** `showtimezone`**(8) command to confirm the setting.**

Setting the XSCF Time

- Command operation

1. **Use the `showdate`(8) command to display the XSCF time.**

```
<Example 1> Display the current time with local time.
XSCF> showdate
Mon Jan 23 14:53:00 JST 2006

<Example 2> Display the current time with UTC.
XSCF> showdate -u
Mon Jan 23 14:53:00 JST 2006
```

2. **Use the `setdate`(8) command to set the time.**

```
<Example 1> Set the current time to 2006-1-27 16:59:00 of a local
time.
XSCF> setdate -s 012716592006.00
Fri Jan 27 16:59:00 JST 2006
The XSCF will be reset. Continue? [y|n]:y
Fri Jan 27 07:59:00 UTC 2006

<Example 2> Set the current time to 2006-1-27 07:59:00 of UTC.
XSCF> setdate -u -s 012707592006.00
Fri Jan 27 07:59:00 UTC 2006
The XSCF will be reset. Continue? [y|n]:y
Fri Jan 27 07:59:00 UTC 2006
```

Note – After the time settings, XSCF reset is done. At this time, the XSCF session is disconnected. Please reconnect to the XSCF and log in again. Also, when the domains are running and if you use XSCF as an NTP server, please perform a domain reboot or apply the changed time to the domain using the `ntpdate`(1M) command.

Note – When replacing the XSCF unit, be sure to note the time set on the replacement XSCF. If the replacement XSCF time does not match the current time, set it to the current time. For the replacement XSCF unit, execute the `showdate`(8) command to check the time, and reset it using the `setdate`(8) command.

Configuring an NTP Server

- Command operation

1. Use the `showntp`**(8) command to display the NTP server for the XSCF network.**

```
XSCF> showntp -a
server ntp1.example.com prefer
server ntp2.example.com
```

2. Use the `showntp`**(8) command to check synchronization and display the status.**

```
XSCF> showntp -l
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*192.168.0.27   192.168.1.56       2 u   27   64  377   12.929   -2.756   1.993
+192.168.0.57   192.168.1.86       2 u   32   64  377   13.030    2.184  94.421
127.127.1.0     .LOCL.             5 l   44   64  377    0.000    0.000   0.008
```

3. Use the `setntp`**(8) command to add an NTP server.**

```
<Example 1> Add the three IP addresses 192.168.1.2, 130.34.11.111,
and 130.34.11.117 as NTP servers for XSCF.
XSCF> setntp -c add 192.168.1.2 130.34.11.111  130.34.11.117
Please reset the XSCF by rebootxscf to apply the ntp settings.

<Example 2> Add the two host names ntp1.red.com and ntp2.blue.com
as NTP servers for XSCF.
XSCF> setntp -c add ntp1.red.com ntp2.blue.com
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

4. Use the `setntp`**(8) command to delete NTP servers for XSCF network.**

```
<Example> Delete NTP servers for XSCF.
XSCF> setntp -c del 192.168.1.2
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

Note – When you use the `setntp`(8) command with the "`-c add`" or "`-c del`" options, execute the `rebootxscf`(8) command to apply the specified configuration and reset the XSCF.

5. **Use the** `showntp`**(8) command to confirm the NTP server.**

```
XSCF> showntp -a
server ntp1.red.com prefer
server ntp2.blue.com
```

Specifying or Canceling prefer for NTP Server

- Command operation

1. **Use the** `showntp`**(8) command to display the prefer settings.**

```
XSCF> showntp -m
prefer : on
localaddr : 0
```

2. **Use the** `setntp`**(8) command to set the prefer.**

```
<Example 1> Specify prefer for NTP server
XSCF> setntp -m prefer=on
Please reset the XSCF by rebootxscf to apply the ntp settings.

<Example 2> Cancel prefer for NTP server
XSCF> setntp -m prefer=off
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

When you use the `setntp`(8) command to change the prefer, execute the `rebootxscf`(8) command to apply the specified configuration and reset the XSCF.

3. **Use the** `showntp`**(8) command to confirm the prefer settings.**

```
XSCF> showntp -m
prefer : off
localaddr : 0

XSCF> showntp -a
server ntp1.red.com
server ntp2.blue.com
```

Note – The setting of the prefer by `setntp`(8) command is supported only on M3000/M4000/M5000/M8000/M9000 servers that run certain versions of XCP firmware (beginning with XCP 1082).

Changing Stratum Value for XSCF

- Command operation

1. Use the `showntp`**(8) command to display the stratum value for the XSCF network.**

```
XSCF> showntp -s
stratum : 5
```

2. Use the `setntp`**(8) command to change a stratum value.**

```
<Example> Set 7 as stratum value for XSCF network.
XSCF> setntp -c stratum -i 7
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

When you use the `setntp`(8) command to specify the stratum value, execute the `rebootxscf`(8) command to apply the specified configuration and reset the XSCF.

3. Use the `showntp`**(8) command to confirm the stratum value change.**

```
XSCF> showntp -s
stratum : 7
```

Changing a Clock Address of Local Clock for XSCF

- Command operation

1. Use the `showntp`**(8) command to display the clock address of the XSCF's own local clock.**

```
XSCF> showntp -m
prefer : on
localaddr : 0

XSCF> showntp -l
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*192.168.0.27   192.168.1.56      2 u   27   64  377   12.929   -2.756   1.993
+192.168.0.57   192.168.1.86      2 u   32   64  377   13.030    2.184  94.421
127.127.1.0     .LOCL.            5 l   44   64  377    0.000    0.000   0.008
```

2. **Use the `setntp`(8) command to change a clock address of the XSCF's own local clock.**

```
<Example> Set 1 as the least significant byte of the clock address.
XSCF> setntp -m localaddr=1
Please reset the XSCF by rebootxscf to apply the ntp settings.
```

When you use the `setntp`(8) command to specify the `localaddr` value, execute the `rebootxscf`(8) command to apply the specified configuration and reset the XSCF.

3. **Use the `showntp`(8) command to confirm the clock address of the XSCF's own local clock.**

```
XSCF> showntp -m
prefer : on
localaddr : 1

XSCF> showntp -l
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*192.168.0.27   192.168.1.56      2 u   27   64  377   12.929   -2.756   1.993
+192.168.0.57   192.168.1.86      2 u   32   64  377   13.030    2.184  94.421
127.127.1.1     .LOCL.            5 l   44   64  377    0.000    0.000   0.008
```

Note – The setting of the XSCF's own local clock by `setntp`(8) command is supported only on M3000/M4000/M5000/M8000/M9000 servers that run certain versions of XCP firmware (beginning with XCP 1091).

- Notes on the NTP Server Referring to the Local Clock

When the NTP server which XSCF refers to is referring to the server's own system time (local clock), and when the address of "127.127.1.0" is set to that local clock, time synchronization in XSCF might fail.

The address of the XSCF's own local clock is fixed to "127.127.1.0." On the other hand, when the address of the local clock of the NTP server which XSCF refers to is set to "127.127.1.0," the address of the clock source (refid) has the same value as the address of the XSCF's own local clock. An NTP server like this is excluded from the target of XSCF time synchronization.

You can execute the `showntp -l` command to refer to the address of the NTP server's own clock source which is set in XSCF and the address of the XSCF's own local clock.

```
XSCF> showntp -l
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 192.168.1.2     LOCAL(0)         3 u   10 1024  377    0.000    0.000   0.000
*127.127.1.0     .LOCL.           5 l   28   64  377    0.000    0.000   0.008
```

Of the two NTP server outputs, the upper (192.168.1.2) indicates the NTP server which is set by using the `setntp`(8) command. The refid is `LOCAL(0)`, which means that the local clock which has the address of "127.127.1.0" is set to the clock source of this NTP server. On the other hand, the lower indicates the XSCF's own local clock. The address of the XSCF's own local clock is fixed to "127.127.1.0."

Due to this, the NTP server (192.168.1.2) is excluded from the target of XSCF time synchronization; which results in the XSCF synchronizes with its own local clock.

With any of the following measures to avoid the trouble, time can be correctly synchronized with the NTP server which is set by using the `setntp`(8) command.

a. Change the clock source that the NTP server being set in XSCF refers to

Use the `showntp -l` command and check the clock source of the NTP server which is set in XSCF. An NTP server which indicates the refid of `LOCAL(0)` in the output is referring to the local clock which has the address of "127.127.1.0," and you should change it to refer to another clock source.

When you change the clock source of an NTP server, make sure in advance that it has no impact on other NTP clients.

b. Change the address of the local clock of the NTP server

Of the NTP server which XSCF refers to, change the address of the local clock to "127.127.1.1," "127.127.1.2," or "127.127.1.3." Change `/etc/inet/ntp.conf` of Oracle Solaris OS. To enable the change, restart of the NTP daemon is required.

When you change the address of the local clock of an NTP server, make sure in advance that it has no impact on other NTP clients.

c. Change the stratum value of the NTP server

Of the NTP server which XSCF refers to, change the stratum value to "1." An NTP server which has the stratum value of "1" becomes the most significant clock source and has no refid. Therefore, there is no chance that it will have the same address as the XSCF's own local clock.

When you change the stratum value of an NTP server, make sure in advance that it has no impact on other NTP clients.

d. Change the address of the XSCF's own local clock

By using the `setntp -m localaddr=`*`value`* command, change the address of the XSCF's own local clock. In *`value`*, specify the least significant byte of the clock address of the local clock 127.127.1.x for value. A numeric from 0 to 3 can be specified. By specifying either from 1 to 3, the address of an NTP server which is referring to the local clock does not correspond to the address of the XSCF internal local clock anymore, and a server which is referring to the local clock can also be set as the NTP server of XSCF.

Setting the Domain Time to the XSCF Time

- Command operation

1. **Use the** `showdate`**(8) command to display the XSCF time.**

```
XSCF> showdate
Mon Jan 23 14:53:00 JST 2006
```

2. **Use the** `showdateoffset`**(8) command to confirm the difference the XSCF time with each domain time.**

```
XSCF> showdateoffset -a
DID              Domain Date Offset
00               128 sec
01               0 sec
02               -1024 sec
03               -9999999 sec
```

3. **Use the** `poweroff`**(8) command to turn off power to all domains.**

```
XSCF> poweroff -a
DomainIDs to power off:00,01,02,03
Continue? [y|n] :y
00 : Powering off
01 : Powering off
02 : Powering off
03 : Powering off
*Note*
This command only issues the instruction to power-off.
The result of the instruction can be checked by the "showlogs
power".
XSCF>
```

4. **Use the** `resetdateoffset`**(8) command to reset the time subtractions between the domains with the XSCF.**

```
XSCF> resetdateoffset
XSCF>
```

5. **Use the** `poweron`**(8) command to turn on power to all domains.**

```
XSCF> poweron -a
DomainIDs to power on:00,01,02,03
Continue? [y|n] :y
00 :Powering on
01 :Powering on
02 :Powering on
03 :Powering on
*Note*
This command only issues the instruction to power-on.
The result of the instruction can be checked by the "showlogs
power".
XSCF>
```

6. **Use the** `showdateoffset`**(8) command to confirm no difference between the XSCF time and the domain time.**

```
XSCF> showdateoffset -a
DID             Domain Date Offset
00              0 sec
01              0 sec
02              0 sec
03              0 sec
```

7. **Use the Oracle Solaris OS** `date`**(1M) command to display the domain time and use the** `showdate`**(8) command to display the XSCF time. Then confirm that the domain time is the same as the XSCF time.**

2.2.7 SSH/Telnet Administration

The SSH/telnet administration settings are used to specify the SSH and telnet settings required to use the XSCF Shell terminal or domain console with an XSCF-LAN connection. For the server, specify enable/disable for each of SSH and telnet setting, including the SSH access control from domain, the SSH host key, and the automatic timeout period after login. Also, install an SSH user public key to XSCF.

TABLE 2-12 lists terms used in SSH/telnet Administration.

TABLE 2-12 SSH/Telnet Administration Terms

Term	Description
RW console	RW (Read and Write). This is a write-enabled OS console (domain console).
RO console	RO (Read Only). This is a read-only OS console

SSH Client

In this system, you can use the following SSH clients.

- Oracle Solaris Secure Shell
- OpenSSH
- PuTTY
- UTF-8 TeraTerm Pro with TTSSH2

Please refer to each software manual for command usage instructions.

TABLE 2-13 lists setting items and the corresponding shell commands.

TABLE 2-13 SSH/Telnet Administration

Item	Description	Shell command	Remarks
Display SSH setting information	Displays SSH settings. Information on whether SSH is enabled or disabled, SSH access control from domain, the host key, fingerprint, and your user public key is displayed.	`showssh`	The SSH port number is 22. When the user public key is displayed with a user name, the useradm privilege is required.
Enable/ disable SSH	Enables or disables SSH.	`setssh`	The SSH is disabled by default.
SSH access control from domain	Specifies whether or not to permit SSH access from domain via the DSCP.	`setssh`	The SSH access is permitted by default. Specifies "deny", when you don't want to login to XSCF using SSH from domain via the DSCP.

TABLE 2-13 SSH/Telnet Administration *(Continued)*

Item	Description	Shell command	Remarks
Host key	Generates an SSH2 host key (RSA key and DSA key).	`setssh`	When the SSH is enabled first, the host key is generated. The DSA key length is 1024 bits. The RSA key length is 1024 bits by default. Either 2048 or 1024 can be specified for RSA key length.
Display telnet setting information	Displays telnet settings. The displayed telnet settings include information indicating whether telnet is enabled or disabled.	`showtelnet`	The telnet port number is 23.
Enable/ disable telnet	Enables or disables telnet.	`settelnet`	The telnet is disabled by default.
Display timeout	Display the timeout period for automatic logout.	`showautologout`	
timeout	After logging in XSCF, if the system is not used for a certain period, logout is automatically performed. Specify the timeout period (minutes). Note that no time monitoring is performed while the domain console is the current console.	`setautologout`	The default timeout period is 10 minutes. A value ranging from 1 to 255 can be specified for the timeout period.
Install/ Uninstall user public key	Install and uninstall the SSH user public key. One user can install multiple user public keys.	`setssh`	When you install/ uninstall the user public key, the useradm privilege is required.

To enable the SSH, to set the SSH access control from domain, and to disable the telnet, the XSCF reset is required. Please reset the XSCF using by `rebootxscf`(8) command. After the XSCF reset, the XSCF session is disconnected. Please log in again to the XSCF. The SSH or telnet settings are automatically applied to the standby XSCF Unit for a system with a redundant XSCF configuration.

In this system, the RW or RO consoles from multiple domains can be used. Only one RW console can be used for each domain. Use the `console`(8) command to specify either the RW console or RO console as a domain console. For details about consoles, see Chapter 3.

Note – The control function of SSH access from domain by XSCF Shell command is supported only on M3000/M4000/M5000/M8000/M9000 servers that run certain versions of XCP firmware (beginning with XCP 1081).

Note – The XCP 1110 is the first release to support the RSA key of 2048 bit length.

Enabling or Disabling SSH/Telnet

- Command operation

1. **Use the** `showssh`**(8) command to display SSH settings or use the** `showtelnet`**(8) command to display telnet settings.**

```
<Example 1> Display SSH settings
XSCF> showssh
SSH status: enabled
SSH DSCP: accept
RSA key:
:
DSA key:
:

<Example 2> Display telnet settings
XSCF> showtelnet
Telnet status: disabled
```

2. **Use the** `setssh`**(8) command to make the SSH settings or use the** `settelnet`**(8) command to make the telnet settings.**

```
<Example 1> Enable SSH.
XSCF> setssh -c enable
Continue? [y|n] :y
Please reset the XSCF by rebootxscf to apply the ssh settings.

<Example 2> Disable telnet.
XSCF> settelnet -c disable
Please reset the XSCF by rebootxscf to apply the telnet settings.
```

3. **To enable the SSH and to disable the telnet, the XSCF reset is required. Use the** `rebootxscf`**(8) command to reset the XSCF.**

```
XSCF> rebootxscf
The XSCF will be reset. Continue? [y|n] :y
```

- After the XSCF reset, the XSCF session is disconnected. Please log in again to the XSCF.

Permitting or Refusing the SSH Access to XSCF from Domain via DSCP

- Command operation

1. Use the `showssh`**(8) command to display SSH settings.**

```
XSCF> showssh
SSH status: enabled
SSH DSCP: accept
RSA key:
:
DSA key:
:
```

2. Use the `setssh`**(8) command to permit or refuse the SSH access to XSCF from domain via DSCP.**

```
<Example 1> Permit SSH access.
XSCF> setssh -m dscp=accept
Continue? [y|n] :y
Please reset the XSCF by rebootxscf to apply the ssh settings.

<Example 2> Refuse SSH access.
XSCF> setssh -m dscp=deny
Continue? [y|n] :y
Please reset the XSCF by rebootxscf to apply the ssh settings.
```

3. To permit and refuse the SSH access, the XSCF reset is required. Use the `rebootxscf`**(8) command to reset the XSCF.**

```
XSCF> rebootxscf
The XSCF will be reset. Continue? [y|n] :y
```

- After the XSCF reset, the XSCF session is disconnected. Please log in again to the XSCF.

Specifying an SSH Host Key

- Command operation

1. Use the `showssh`**(8) command to display the host key and fingerprint.**

```
XSCF> showssh
SSH status: enabled
SSH DSCP: accept
RSA key:
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAt0IG3wfpQnGr51znS9XtzwHcBBb/UU0LN08Si
lUXE6j+avlxdY7AFqBf1wGxLF+Tx5pTa6HuZ8o8yUBbDZVJAAAAFQCfKPxarV+/5q
zK4A43Qaigkqu/6QAAAIBMLQl22G8pwibESrh5JmOhSxpLz
l3P26ksI8qPr+7BxmjLR0k=
Fingerprint:
1024 e4:35:6a:45:b4:f7:e8:ce:b0:b9:82:80:2e:73:33:c4

DSA key:
ssh-dss
AAAAB3NzaC1kc3MAAACBAJSy4GxD7Tk4fxFvyW1D0NUDqZQPY3PuY2IG7QC4BQ1ke
wDnblB8/JEqI+8pnfbWzmOWU37KHL19OEYNAv6v+WZT6RE
lU5Pyb8F16uq96L8QDMswFlICMZgrn+ilJNStr6r8KDJfwOQMmK0eeDFj2mL40NOv
aLQ83+rRwW6Ny/yF1Rgv6PUpUqRLw4VeRb+uOfmPRpe6/kb4z++lO
htpWI9bay6CK0nrFRok+z54ez7BrDFBQVuNZx9PyEFezJG9ziEYVUag/23LIAiLxx
BmW9pqa/WxC21Ja4RQVN3009kmVwAAAIAON1LR/9Jdd7yyG18
+Ue7eBBJHrCA0pkSzvfzzFFj5XUzQBdabh5p5Rwz+1vriawFIZI9j2uhM/3HQdrvY
SVBEdMjaasF9hB6T/uFwP8yqtJf6Y9GdjBAhWuH8F13pX4BtvK
9IeldqCscnOuu0e2rlUoI6GICMr64FL0YYBSwfbwLIz6PSA/yKQe23dwfkSfcwQZN
q/5pThGPi3tob5Qev2KCK2OyED
MCAOvVlMhqHuPNpX+hE19nPdBFGzQ==
Fingerprint:
1024 9e:39:8e:cb:8a:99:ff:b4:45:12:04:2d:39:d3:28:15
```

2. Use the `setssh`**(8) command to set the host key.**

```
<Example> Update the host key
XSCF> setssh -c genhostkey
Host key create. Continue? [y|n] : y
```

Specifying the Timeout Period of SSH/Telnet

- Command operation

1. **Use the** `showlogout`**(8) command to display the timeout period.**

```
XSCF> showautologout
30min
```

2. **Use the** `setautologout`**(8) command to set the timeout period.**

```
<Example 1> Specify 255 (minutes) for the timeout period.
XSCF> setautologout -s 255
255min
```

The set timeout period becomes effective at the next login.

Installing and Uninstalling an SSH User Public Key

- Command operation

1. **Use the** `showssh`**(8) command to display the user public key.**

```
<Example> The user key is not set.
XSCF> showssh -c pubkey
XSCF>
```

2. **Generate the user private key and the user public key for a created XSCF user account with your client software. See the manual for your client software for procedures to create the user public key and to set the passphrase. We recommend that the passphrase be set.**

3. **Use the** `setssh`**(8) command with option for installing user public key. Then, copy and paste the user public key, which was made in Step 2, on the window display. After pressing the Enter key, press the "Ctrl" and "D" keys to complete the installation.**

```
XSCF> setssh -c addpubkey -u efgh
Please input a public key:
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAzFh95SohrDgpnN7zFCJCVNy+jaZ
PTjNDxcid/QGbihYDCBttI4151Y0Sv85FJwDpSNHNKoVLMYLjtBmUMPbGgGVB61qs
kSv/FeV44hefNCZMiXGItIIpKP0nBK4XJpCFoFbPXNUHDw1rTD9icD5U/wRFGSRRx
FI+Ub5oLRxN8+A8= efgh@example.com
<Press “Ctrl” and “D” keys>
XSCF>
```

4. **Use the** showssh**(8) command to confirm the user public key and its number.**

```
<Example> The user key is set by number 1.
XSCF> showssh -c pubkey
Public key:
1 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAzFh95SohrDgpnN7zFCJCVNy+jaZ
PTjNDxcid/QGbihYDCBttI4151Y0Sv85FJwDpSNHNKoVLMYLjtBmUMPbGgGVB61qs
kSv/FeV44hefNCZMiXGItIIpKP0nBK4XJpCFoFbPXNUHDw1rTD9icD5U/wRFGSRRx
FI+Ub5oLRxN8+A8= efgh@example.com
```

Do the SSH connection by using the user account of XSCF on the client software when you log in the XSCF Shell next time. Confirm that you can log in to the XSCF Shell by authentication with the user key.

5. **When you uninstall the user public key, use the** setssh**(8) command with the number of the user public key.**

```
XSCF> setssh -c delpubkey -s 1
         1 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAzFh95SohrDgpnN7z
FCJCVNy+jaZPTjND/xcidQGbihYDCBttI4151Y0Sv85FJwDpSNHNKoVLMYLjtBmUM
PbGgGVB61qskSv/FeV44hefNCZMiXGItIIpKP0nBK4XJpCFoFbPXNUHDw1rTD9icD
5U/wRFGSRRxFI+Ub5oLRxN8+A8= efgh@example.com
```

6. **Use the** showssh**(8) command to delete the user public key.**

```
XSCF> showssh -c pubkey
XSCF>
```

2.2.8 Https Administration

Use https administration to specify the settings required for operating the web browser window of the XSCF Web over an XSCF-LAN connection. Here, you can specify the enabling/disabling of https and configure https settings. In this system, https is disabled by default. You can use the XSCF Web console securely.

TABLE 2-14 lists a term used in https administration.

TABLE 2-14 https Administration Term

Term	Description
XSCF Web console	The web browser window of the XSCF Web with an XSCF-LAN connection

To use https, please set as follows.

Select Certificate Authority (CA) and Procedures

Please select one of the following in consideration of your system and the environment of a web browser.

- External CA
- CA in intranet
- Self CA

Caution – IMPORTANT - The self CA is constructed in XSCF. You cannot use the XSCF's self CA as an external CA for another system. If no external CA and CA in intranet exists in your system environment, use the self CA. (See Step b)

CA and Procedures

The following are the settings procedures for each type of CA.

a. Using the External CA or CA in Intranet

1. Create a web server private key for the XSCF.
2. Make the Certificate Signing Request (CSR) by the XSCF.
3. Request the issue of the certificate for the CSR to the CA.
4. Import a web server certificate signed by CA to the XSCF.

5. Enable https.

For Step 1 - Step 5 above, specify each option using the `sethttps`**(8)** command. Also, when using the XSCF Web, select the appropriate items for each setting.

- When the XSCF Unit is redundant, the https settings are automatically applied to the standby XSCF Unit.

b. Using the self CA

1. Construct the self CA for the XSCF.

2. Create a web server private key for the XSCF.

3. Make a web server certificate self-signed by the XSCF.

4. Enable https.

When one option of the `sethttps`**(8)** command for the self-authentication is specified, the settings for Step 1 - Step 3 above are automatically completed at a time.

- When the XSCF Unit is redundant, the https settings are automatically applied to the standby XSCF Unit.

TABLE 2-15 lists setting items and the corresponding shell commands.

TABLE 2-15 https Administration

Item	Description	Shell Command	Remarks
Display https setting	Displays the https settings. Information on whether https is enabled or disabled and key states are displayed.	`showhttps`	
Enabling/ disabling	Enables or disables https.	`sethttps`	

TABLE 2-15 https Administration *(Continued)*

Item	Description	Shell Command	Remarks
External authentication	When the external CA and CA in Intranet are used, set the following. • Create a web server private key of XSCF • Make the Certificate Signing Request (CSR) by XSCF and Request the issue of the certificate to CA. • Import a web server certificate to XSCF.	`sethttps`	Specify the following Distinguished Name for making a CSR. • Country (2 letter: Ex.US, JP), Province, Locality, Organization, Organizational unit, Common name (Your name or web server host name), email address of administrator • Each value, except for Country, must consist of up to 64 characters. For details of DN, see the `sethttps`(8) man page, or the *XSCF Reference Manual*.
Self authentication	Automatically, the self CA is constructed in XSCF and the certificate is installed. The following are set. • A self CA is constructed • A private key is made • A web server certificate self-signed is made	`sethttps`	Specify the same DN as the External authentication at making a web server certificate.
Display the certificate	Displays the following: • CSR • Web server certificate	`showhttps`	The certificate expiration of the self-CA is as follows: • Server certificate: 10 year The set value becomes effective, when the certificate will be created next time.

To enable the https, an XSCF reset is required. Please reset the XSCF using by `rebootxscf`**(8)** command. After the XSCF reset, the XSCF session is disconnected. Please log in again to the XSCF. The https settings are automatically applied to the standby XSCF Unit for a system with a redundant XSCF configuration.

When the expiration date of the web server certificate has passed, or you change the web server certificate, configure the https settings again.

Enabling or Disabling Https

- Command operation

1. **Use the** `showhttp`**(8) or the** `showhttps`**(8) command to display https settings.**

```
<Example> Display the https settings.
XSCF> showhttps
HTTPS status: enabled
Server key: installed in Apr 24 12:34:56 JST 2006
CA key: installed in Apr 24 12:00:34 JST 2006
CA cert: installed in Apr 24 12:00:34 JST 2006
CSR:
-----BEGIN CERTIFICATE REQUEST-----
MIIBwjCCASsCAQAwgYExCzAJBgNVBAYTAmpqMQ4wDAYDVQQIEwVzdGF0ZTERMA8G
A1UEBxMIbG9jYWxpdHkxFTATBgNVBAoTDG9yZ2FuaXphdGlvbjEPMA0GA1UECxMG
b3JnYW5pMQ8wDQYDVQQDEwZjb21tb24xFjAUBgkqhkiG9w0BCQEWB2VlLm1haWww
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ5D57X/k42LcipTWBWzv2GrxaVM
5GEyx3bdBW8/7WZhnd3uiZ9+ANlvRAuw/YYy7I/pAD+NQJesBcBjuyj9x+IiJl9F
MrI5fR8pOIywVOdbMPCar09rrU45bVeZhTyi+uQOdWLoX/Dhq0fm2BpYuh9WukT5
pTEg+2dABg8UdHmNAgMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQAux1jH3dyB6Xho
PgBuVIakDzIKEPipK9qQfC57YI43uRBGRubu0AHEcLVue5yTu6G5SxHTCq07tV5g
38UHSg5Kqy9QuWHWMri/hxm0kQ4gBpApjNb6F/B+ngBE3j/thGbEuvJb+0wbycvu
5jrhB/ZV9k8X/MbDOxSx/U5nF+Zuyw==
-----END CERTIFICATE REQUEST-----
```

2. **Use the** `sethttps`**(8) command to make the https settings.**

```
<Example 1> Enable https.
XSCF> sethttps -c enable
Continue? [y|n] : y
Please reset the XSCF by rebootxscf to apply the https settings.

<Example 2> Disable https
XSCF> sethttps -c disable
```

3. **To enable the https, the XSCF reset is required. Use the `rebootxscf`(8) command to reset the XSCF.**

```
XSCF> rebootxscf
The XSCF will be reset. Continue? [y|n] :y
```

- After the XSCF reset, the XSCF session is disconnected. Please log in again to the XSCF.

Importing a Web Server Certificate by Using the External CA or CA in Intranet

- Command operation

1. **Use the `sethttps`(8) command to create a web server private key.**

```
XSCF> sethttps -c genserverkey
Server key already exists. Do you still wish to update? [y|n] :y
Enter passphrase: xxxxxxxx
Verifying - Enter passphrase: xxxxxxxx
```

2. **Use the `sethttps`(8) command to create the CSR specifying the distinguished name (DN). (See the DN description in "External authentication" in TABLE 2-15.)**

```
<Example> Specify the DN (JP, Kanagawa, Kawasaki, Example,
Development, scf-host, abc@example.com)
XSCF> sethttps -c gencsr JP Kanagawa Kawasaki Example Development
scf_host abc@example.com
```

3. **Use the `sethttps`(8) command to display the CSR. Copy the displayed CSR (BEGIN to END) and save it in the text file.**

```
XSCF> showhttps
HTTPS status: disabled
Server key: installed in Jul 11 06:33:25 UTC 2006
CA key: installed in Jul 11 06:33:21 UTC 2006
CA cert: installed in Jul 11 06:33:21 UTC 2006
CSR:
-----BEGIN CERTIFICATE REQUEST-----
MIIByzCCATQCAQAwgYoxCzAJBgNVBAYTAkpQMREwDwYDVQQIEwhLYW5hZ2F3YTER
MA8GA1UEBxMIS2F3YXNha2kxEDAOBgNVBAoTB0ZVSklUU1UxDDAKBgNVBAsTA0VQ
:
uni/n3g2/F5Ftnjg+M4HtfzT6VwEhG01FGP4IImqKg==
-----END CERTIFICATE REQUEST-----
```

4. **Send the copied CSR to the CA and request the web server certificate.**

5. **Perform the** `sethttps`**(8) command with option for import. Then copy and paste the signed web server certificate in the window. Please press Enter and press the "Ctrl" and "D" keys. Then the importing is completed.**

```
XSCF> sethttps -c importca
Please import a certificate:
-----BEGIN CERTIFICATE-----
MIIDdTCCAt6gAwIBAgIBATANBgkqhkiG9w0BAQQFADCBgTELMAkGA1UEBhMCamox:
R+OpXAVQvb2tjIn3kO99dq+begECo4mwknW1t7QI7A1BkcW2/MkOolIRa6iP1ZwgJ
oPmwAbrGyAvGUtdzUoyIH0jl7dRQrVIRA==
-----END CERTIFICATE-----
<Press "Ctrl" and "D" keys>
```

6. **Use the** `sethttps`**(8) command to enable https.**

```
XSCF> sethttps -c enable
Continue? [y/n] :y
Please reset the XSCF by rebootxscf to apply the https settings.
```

7. **Use the** `rebootxscf`**(8) command to reset the XSCF.**

```
XSCF> rebootxscf
The XSCF will be reset. Continue? [y|n] :y
```

- After the XSCF reset, the XSCF session is disconnected. Please log in again to the XSCF.

8. **Access the XSCF Web specifying the https form client. In the window, please check that the security warning dialog is not displayed or confirm whether the certificate is correct.**

Creating a Web Server Certificate by Constructing the Self CA

- Command operation

1. **Use the** `sethttps`**(8) command to create a self-signed web server certificate by specifying the DN.**

```
<Example> Specify the DN (JP, Kanagawa, Kawasaki, Example,
Development, scf-host, abc@example.com)
XSCF> sethttps -c selfsign JP Kanagawa Kawasaki Example Development
scf-host abc@example.com
CA key and CA cert already exist. Do you still wish to update? [y|n]
:y
Enter passphrase: xxxxxxxx
Verifying - Enter passphrase: xxxxxxxx
```

2. **Use the** `showhttps`**(8) command to confirm the generated web server certificate.**

```
XSCF> showhttps
HTTPS status: disabled
Server key: installed in Jul 11 06:33:25 UTC 2006
CA key: installed in Jul 11 06:33:21 UTC 2006
CA cert: installed in Jul 11 06:33:21 UTC 2006
CSR:
-----BEGIN CERTIFICATE REQUEST-----
MIIByzCCATQCAQAwgYoxCzAJBgNVBAYTAkpQMREwDwYDVQQIEwhLYW5hZ2F3YTER
MA8GA1UEBxMIS2F3YXNha2kxEDAOBgNVBAoTB0ZVSklUU1UxDDAKBgNVBAsTA0VQ
:
uni/n3g2/F5Ftnjg+M4HtfzT6VwEhG01FGP4IImqKg==
-----END CERTIFICATE REQUEST-----
```

3. **Use the** `sethttps`**(8) command to enable https.**

```
XSCF> sethttps -c enable
```

4. **Use the** `rebootxscf`**(8) command to reset the XSCF.**

```
XSCF> rebootxscf
The XSCF will be reset. Continue? [y|n] :y
```

- After the XSCF reset, the XSCF session is disconnected. Please log in again to the XSCF.

2.2.9 Audit Administration

Audit administration is used to specify logging of access details, such as which users logged in to XSCF, their login times, and the operations that they executed. In the server, the default access audit setting is enabled. The main audit settings include the access audit enable/disable setting (see TABLE 2-16) and audit trail management method (see TABLE 2-16).

Collecting Audit Data

The server controls the audit module of XSCF firmware to provide an audit trail. When related event information is obtained, the XSCF firmware collects audit information as follows:

1. Audit event data is logged in the form of audit records (see TABLE 2-16).
2. The audit records are stored in order by date in the local audit files of the XSCF firmware (see TABLE 2-16).
3. The audit files are linked and become an audit trail (see TABLE 2-16).
4. Audit records are thus kept as an audit trail so that the user can refer to the Audit trail (see `viewaudit`(8)).

TABLE 2-16 lists terms used in audit administration.

TABLE 2-16 Audit Administration Terms

Term	Description
Audit	Function for auditing system access. It is also called auditing.
Audit event	Security-related system action that can be audited. Multiple audit events can be specified with values or names. (Example: AEV_LOGIN_SSH, LOGIN_SSH, 0, all)
Audit class	Group of audit events related to one another. (Example: Audit events in the login audit class: SSH login, telnet login, https login, logout) Multiple audit classes can be specified. (Example: ACS_AUDIT, AUDIT, 2, all)
Audit record	One audit record is information specifying one audit event. An audit record contains an event, the event time, and other related information. Audit records are stored in audit files.
Audit file	This is also called an audit log file. One audit file (log file) contains multiple audit records.

TABLE 2-16 Audit Administration Terms *(Continued)*

Term	Description
Audit trail	Set of audit files. The user refers to an audit trail to analyze the information contained in it.
Audit policy	Audit settings. The audit policy mainly defines whether auditing is enabled or disabled and the management method when audit trail becomes full.
Audit token	One field in an audit record. An audit token contains an audit event attribute, such as "user" or "privilege".

TABLE 2-17 lists the setting items and the corresponding shell commands.

TABLE 2-17 Audit Administration

Item	Description	Shell Command	Remarks
Display audit setting information	Displays audit settings. Information on whether access audit is enabled or disabled and the Audit policy is displayed.	`showaudit`	
Enable/ disable audit, audit policy	Sets a value for an audit setting. Specify the following types of audit trail administration information: • Enable/disable auditing (Note 1) • Request the log archive (Note 1) • Data deletion Also, specify the audit policy as follows: • Enable or disable auditing for the specified user only or for global policy. (Note 2) • Enable or disable an audit class. • Enable of disable an audit event. • Enable or disable auditing for all users (global policy). • Specify the destination address for the mail sent when usage of the local audit file reaches the threshold. • Specify the write suspend/count applied when an audit trail becomes full. (Note 3) • Specify the local audit file usage threshold (%) that triggers an alarm when reached. (Note 4)	`setaudit`	• Specify values for "User," "Audit Class," and "Audit Event" by delimiting them with the comma in a shell command. • You can use up to 128 characters to specify the mail address. If the receiving address has a restriction, check the settings. • The default write mode when an audit trail becomes full is "count." • The shell command can set a maximum of four warning thresholds delimited by the comma. The default warning threshold is 80 (%).

TABLE 2-17 Audit Administration *(Continued)*

Item	Description	Shell Command	Remarks
Display audit trail	Displays an audit trail. To display an audit trail, select one of the items listed below. Data is displayed in units of audit records. • Records after the specified time • Records before the specified time • Records the specified range of time • Records on a specific date (24 hours of records on that date in local time) • Audit class • Audit event • Audit session ID • User privilege • Return value (success, failure, or none) • User (name or UID) Also, to display an audit trail, specify the following formats: • Line by line printing • Delimiter specified (The default delimiter is the comma.) • Suppressing conversion of UIDs into user names and IP addresses into hostnames • Printing in XML format (Note 5)	`viewaudit`	• To use a delimiter as part of input data, enclose it in quotation marks. Up to three delimiters can be used. • The return values are as follows: Success: 0 Failure: Other then 0 none: No return value ("none" indicates that no audit token has a return value.)

Note – (1) If audit is disabled, writing to the audit trail is stopped, all requests to the log file transfer to the log archive function are also stopped. When audit is enabled, writing restarts. Rebooting the system disables and then enables access auditing. Also, the local audit file of XSCF have the primary and secondary files. The data is kept as is even if you perform archiving unless it exceeds the threshold of audit file. Therefore, the usage of the audit file never becomes 0.

Note – (2) For detail of global policy, see the *Administration Guide*.

Note – (3) If an audit trail becomes full while suspend is specified, XSCF Shell or XSCF Web operation will be locked; you will not be able to complete the operation. Writing any further entries to the audit trail stops until you either clear out some audit trail space, or the until the audit policy is changed to count.

If the audit trail becomes full while count is the specified policy, new audit trail data is discarded, and the number of times that records are dropped is counted.

If you plan to specify suspend, you need to generate in advance a user account that has the `auditadm` privilege specified, and whose audit policy is set to disable.

If an audit trail becomes full when suspend is specified, XSCF will be locked. When this happens, login using the user account that you set up in advance with audit policy set to disable, and clear the audit trail space. Then continue with XSCF operation.

If the audit trail space becomes full when "suspend" is specified, and you *haven't* previously set up in advance a user account with audit policy "disable", you will not be able to clear the audit trail space or perform any other functions. In this case, you must log in as default user from the console, as described in "Setup Summary by the XSCF Shell" on page 2-2. Then clear the audit trail space as default user.

Note – (4) Warnings are displayed as console messages and secure email. The following is an example.

```
WARNING: audit trail is 91% full
```

You can clear space by manually transferring the current audit trail files to remote storage or by deleting them. For details of transferring or deleting, see "Enabling or Disabling Audit, Transferring a Log File, and Deleting Audit Data", the `viewaudit`(8) man page, or the *XSCF Reference Manual*. For audit policy details, see the *Administration Guide*.

Note – (5) For detail of `viewaudit`(8) command, see the *XSCF Reference Manual*.

Enabling or Disabling Audit, Transferring a Log File, and Deleting Audit Data

- Command operation

1. **Use the** `showaudit`**(8) command to display audit settings.**

```
<Example> Display all information on the current audit status in
the system.
XSCF> showaudit all
Auditing:              enabled
Audit space used:      13713 (bytes)
Audit space free:      4180591 (bytes)
Records dropped:       0
Policy on full trail: count
User global policy:    enabled
Mail:
Thresholds:            80% 100%
User policy:
Events:
        AEV_AUDIT_START                   enabled
        AEV_AUDIT_STOP                    enabled
:
```

2. **Use the** `setaudit`**(8) command to configure auditing.**

```
<Example 1> Disable writing to the audit trail and transfer the log
file.
XSCF> setaudit disable

<Example 2> Enable writing to the audit trail.
XSCF> setaudit enable
Turns on writing of the audit records for the audit trail.

< Example 3> Request the log file transfer.
XSCF> setaudit archive

< Example 4> Delete the log data of the audit trail.
XSCF> setaudit delete
```

Specifying the Audit Policy

- Command operation

1. Use the `showaudit`**(8) command to display the audit policy.**

```
XSCF> showaudit all
Auditing:               enabled
Audit space used:       13713 (bytes)
Audit space free:       4180591 (bytes)
Records dropped:        0
Policy on full trail: suspend
User global policy:     enabled
Mail:
Thresholds:             80% 100%
User policy:
Events:
        AEV_AUDIT_START                     enabled
        AEV_AUDIT_STOP                      enabled
:
```

2. Use the `setaudit`**(8) command to set the audit policy.**

```
<Example 1> Specify three users, enable the AUDIT and LOGIN groups
for the Audit class, enable SSH login for the Audit event, and
disable the global policy for the users.
XSCF> setaudit -a yyyyy,uuuuu,nnnnn=enabe -c ACS_AUDIT,ACS_LOGIN=
enable -e AEV_LOGIN_SSH=enable -g disable

<Example 2> Specify the file warning send destination address,
count for the trail-full write mode, and file space warning
threshold.
XSCF> setaudit -m yyyy@example.com -p count -t 50,75,90
```

3. **Use the** `showaudit`**(8) command to confirm the setting.**

```
XSCF> showaudit all
Auditing:             enabled
Audit space used:     13713 (bytes)
Audit space free:     4180591 (bytes)
Records dropped:      0
Policy on full trail: count
User global policy:   enabled
Mail:                 yyyy@example.com
Thresholds:           50% 75% 90%
User policy:
Events:
        AEV_AUDIT_START            enabled
        AEV_AUDIT_STOP             enabled
        AEV_LOGIN_BUI              enabled
        AEV_LOGIN_CONSOLE          enabled
        AEV_LOGIN_SSH              enabled
        AEV_LOGIN_TELNET           enabled
:
```

Displaying the Audit Logs

- Command operation

● **Use the** `viewaudit`**(8) command to display the audit trail.**

```
XSCF> viewaudit
file,1,2006-06-29 13:42:59.128 +09:00,20060629044259.0000000000.localhost
header,20,1,audit - start,localhost.localdomain,2006-06-29 13:42:59.131 +09:00
header,31,1,login - console,localhost.localdomain,2006-06-29 13:45:03.755
+09:00subject,1,default,normal,console
header,60,1,command - showpasswordpolicy,localhost.localdomain,2006-06-29
13:45:33.653 +09:00
subject,1,default,normal,console
command,showpasswordpolicy
platform access,granted
return,0
:
```

For the method of displaying the audit logs, see Appendix B.

2.2.10 Log Archiving Administration

This section explains how to set the log archiving function, which saves the logs retained on an XSCF Unit. The archive host, the archive directory, enable/disable for the log archiving and so on are set.

Note – Logs archived on the log host should be rotated at regular intervals to avoid loss of log information. For example, `logadm(1M)` can be used to configure log rotation on systems that run the Oracle Solaris OS.

TABLE 2-18 lists terms used in log archiving administration.

TABLE 2-18 Log Archiving Administration Terms

Term	Description
Log archiving	Function that saves the log information stored on an XSCF to another host
Archive host	Host to which logs are saved
Archive directory	Directory in the archive host to which logs are saved

TABLE 2-19 lists setting items and the corresponding shell commands.

TABLE 2-19 Log Archiving Administration

Item	Description	Shell Command	Remarks
Display log archiving information	Displays the following log archiving information: • Log archiving settings • Status of a connection to the archive host • Space consumed by archives on the archive host	`showarchiving`	
Enable / Disable log archiving function	Enables or disables the log archiving function.	`setarchiving`	
Archive target	Sets the archive target as follows: • Name or IP address of the archive host • User name used for ssh login to the archive host • Archive directory name	`setarchiving`	To specify the target with the command, specify "user name" + "@host name" + ":directory name."

TABLE 2-19 Log Archiving Administration *(Continued)*

Item	Description	Shell Command	Remarks
Password	Sets a password used for ssh login to the archive host.	`setarchiving`	The password is used for the ssh login.
Host public key	Sets a public key used in server authentication for the archive host. The public key is specified in any of the following ways: • Not specified • Specifying a key by downloading it from the archive host • Using text to specify a public key for the archive host	`setarchiving`	• To specify a public key, use RSA. An MD5 key is displayed for a fingerprint. • If a public key is set but not used for this authentication, the public key is deleted.
Capacity	Sets limits for the space consumed by archives. There are two limits, one for each category of logs: • Audit log • Other logs	`setarchiving`	Specify integer values in units of megabytes for the capacity in order, beginning with the audit log and then other logs (Note 1). The ranges for this setting are as follows (Note 2): • Audit log: 0 or unlimited, 500-50000 • Other logs: 500-50000

Note – For the types of logs that can be saved, see Chapter 8.

Note – When you set neither a defined value nor a value outside the specified range, an error is displayed. In this event, no setting is made and the process is terminated.

Specifying a Host Name, Directory Name, Login User Name and Password for the Target of Log Archiving, and Enabling or Disabling the Log Archiving

- Command operation

1. **Use the** `showarchiving`**(8) command to display log archiving settings.**

```
<Example> No values have been set for the settings
XSCF> showarchiving
*** Archiving Configuration ***
Archiving state ---------- Disabled
Archive host ------------- Not configured
Archive directory -------- Not configured
User name for ssh login -- Not configured
:
```

2. **Use the** `setarchiving`**(8) command to set the log archiving target.**

```
<Example>  Specify a user name, host name, directory, and password
XSCF> setarchiving -t foo@example.com:/var/logs/xx -r
Enter ssh password for foo@example.com: xxxxxx
:
```

3. **Use the** `setarchiving`**(8) command to make an enable or disable selection for the log archiving function.**

```
XSCF> setarchiving enable
```

4. **Use the** `showarchiving`**(8) command to confirm the settings.**

```
XSCF> showarchiving
*** Archiving Configuration ***
Archiving state ---------- Enabled
Archive host ------------- example.com
Archive directory -------- /var/logs/xx
User name for ssh login -- foo
:
```

Specifying the Host Public Key for the Archive Host

- Command operation

1. **Use the** `showarchiving`**(8) command to display the log archiving settings.**

```
XSCF> showarchiving -v
*** Archiving Configuration ***
Archiving state ---------- Enabled
Archive host ------------- example.com
Archive directory -------- /var/logs/this-xscf/xx
User name for ssh login -- foo
Archive host public key -- Server authentication disabled
Archive host fingerprint - Server authentication disabled

*** Connection to Archive Host ***
Latest communication ----- 2005/09/22 22:12:34
:
```

2. **Use the** `setarchiving`**(8) command to set the host public key.**

```
<Example>  Specifying that the host key be downloaded
XSCF> setarchiving -k download
Downloading public host key from example.com
Key fingerprint in md5:
c9:e0:bc:b2:1a:80:29:24:13:d9:f1:13:f5:5c:2c:0f
Accept this public key? [y|n] : y
```

Setting Capacity Limits for the Log Archiving Function

- Command operation

1. **Use the** `showarchiving`**(8) command to display the amount of space used for log archiving.**

```
XSCF> showarchiving -v
*** Archiving Configuration ***
Archiving state ---------- Enabled
Archive host ------------- example.com
Archive directory -------- /var/logs/this-xscf/xx
User name for ssh login -- foo
Archive host public key -- Server authentication disabled
Archive host fingerprint - Server authentication disabled

*** Connection to Archive Host ***
Latest communication ----- 2005/09/22 22:12:34
Connection status -------- OK

                              AUDIT LOGS      OTHER LOGS
                              ----------      ----------
Archive space limit             10000 MB         5000 MB
Archive space used               3010 MB         2252 MB
Total archiving failures             171               2
Unresolved failures                    4               0
```

2. **Use the** `setarchiving`**(8) command to set capacity limits for logs.**

```
<Example>  Specifying capacity limits for the audit log and other
logs
XSCF> setarchiving -l Unlimited,10000
```

3. **Use the** `showarchiving`**(8) command to confirm the settings.**

```
XSCF> showarchiving -v
*** Archiving Configuration ***
Archiving state ---------- Enabled
:
                              AUDIT LOGS      OTHER LOGS
                              ----------      ----------
Archive space limit             10000 MB        10000 MB
Archive space used               3010 MB         2252 MB
Total archiving failures             171               2
Unresolved failures                    4               0
```

Displaying Log Archiving Error Information

- Command operation

● **Use the** `showarchiving`**(8) command to display details of log archiving errors.**

```
<Example 1>  Three errors occurred
XSCF> showarchiving -e
2004/06/17 01:12:12
- Failed to connect to the archive host.
- Output from ssh: "ssh: foo.bar: host not responding"
2004/06/19 22:15:46
- Failed to create a file on the archive host.
- File: /foo/platform/error-details/log.2004-06-19T22:15:48
- Output from scp: "scp: /foo/platform: Permission denied"
2004/06/19 22:15:47
- Command failed on the archive host.
- Command: "/usr/bin/du -sk /foo/bar/error-log"
- Output from command: "/usr/bin/du: Command not found"

<Example 2>  No error occurred
XSCF> showarchiving -e
No archiving errors have occurred
```

2.2.11 SNMP Administration

This section explains how to make different types of protocols settings for SNMP to use the SNMP agent function.

TABLE 2-20 lists the terms used in SNMP administration.

TABLE 2-20 SNMP Administration Terms

Term	Description
SNMP	Abbreviation for Simple Network Management Protocol. This query, command, and response protocol is used to test and change configuration parameters of LANs and WANs that are connected to bridges, routers, switches, or other devices via networks. Currently, SNMPv1, SNMPv2c, and SNMPv3 are available. SNMPv3 has added encryption and authentication functions, in comparison with SNMPv1 and SNMPv2c.
MIB	Abbreviation for Management Information Base. This is the information database used to manage the SNMP agent function, which responds with MIB information to requests from the SNMP manager.
USM	Abbreviation for User-based Security Model. This user-based security model is defined by SNMPv3.

TABLE 2-20 SNMP Administration Terms *(Continued)*

Term	Description
VACM	Abbreviation for View-based Access Control Model. This view-based access control model is defined by SNMPv3.
Group	Users belonging to a VACM model. The group is defined in the access privilege of every user in the group.
OID	Abbreviation for Object Identifier. This is an object identification number. a numerical address for an object in the MIB definition file, expressed with integers using a dot as the delimiter.
View (MIB View)	Method of referring to the MIB definition file. A view is a subtree of the MIB, which is defined with OIDs and OID masks. An MIB access control view can be provided to a group.

TABLE 2-21 lists settings and the corresponding shell commands.

TABLE 2-21 SNMP Administration

Item	Description	Shell Command	Remarks
Display SNMP setting information	Displays the SNMP agent setting information and status.	`showsnmp`	
System management information	Makes the following settings as management information that is common to the v1,v2c,v3 agent protocol: • Installation location of the agent system • Mail address of the administrator • Description of the agent system • Port number of the agent (listening port number)	`setsnmp`	• The default agent port number is 161. The default values of other port numbers are to be defined. • You can use up to 128 characters to specify the mail address. If the receiving address has a restriction, check the settings.
Enable/Disable Agent	Enables/disables SNMP agent. You can specify the name of the MIB module as follows. • SP-MIB (XSCF extension MIB) • FM-MIB (Fault Management MIB) • ALL (All the MIB modules in this list) When you do not specify the name of the MIB module, it activates the SNMP agent with support for all MIB modules or stops the SNMP agent.	`setsnmp`	• The default is disabled. • FM-MIB is the fault management MIB, which has a format compatible with the Oracle Solaris OS. The FM-MIB is provided for users who are familiar with the Oracle Solaris OS.

TABLE 2-21 SNMP Administration *(Continued)*

Item	Description	Shell Command	Remarks
SNMPv1/ SNMPv2c communication	Enables/disables SNMPv1 and SNMPv2c communication.	`setsnmp`	The community string used to enable SNMPv1/SNMPv2c is Read-Only.
SNMPv3 trap	Makes the following SNMPv3 trap settings: • User name (Note 1) • Authentication password (Note 1) • Encryption password (Note 1) • Engine ID of local agent or request of an acknowledgement from the receiving host. • Port number of the trap destination • Host name of the trap destination	`setsnmp`	• Must start with 0x, but also consist of an even number of hexadecimal digits. • One of the following two authentication algorithms is selected: MD5, Secure Hash Algorithm (SHA) • The default values of the trap destination host are to be defined. • The default port number of the trap destination is 162.
SNMPv1/ SNMPv2c Trap	Makes the following SNMPv1 and SNMPv2c trap settings: • Trap type setting • Community string • Port number of the trap destination • Host name of the trap destination	`setsnmp`	• One of the following three trap types is selected: v1, v2, inform (Note 2) • The default port number of the trap destination is 162.
Disable SNMPv3 trap	Disables trap sending to the target host, with the following specified: • User name • Trap destination host	`setsnmp`	
Disable SNMPv1/ SNMPv2c trap	Disables trap sending to the target host, with the following specified: • Defined protocol type (v1/v2c) • Trap destination host	`setsnmp`	
Initialize SNMP configration	Stops the SNMP agent and change the SNMP configration set by `setsnmp`(8) to the default.	`setsnmp`	
Display USM management information	Displays the USM management information for the SNMP agent	`showsnmpusm`	

TABLE 2-21 SNMP Administration *(Continued)*

Item	Description	Shell Command	Remarks
USM management information	Sets USM management information for the following for the SNMP agent: • Specifying a user authentication algorithm • Sets authentication/encryption passwords for users • Changing authentication/encryption -passwords for users • Copying a user • Deleting a user	`setsnmpusm`	• SNMPv3 settings. • Specify the password over 8 characters.
Display VACM management information	Displays VACM management information for the SNMP agent	`showsnmpvacm`	
VACM management information	Sets VACM management information for the following for the SNMP agent: Making access control group and access control view (MIB view) settings for a user • Adds a user account to an access control group • Deleting a user from an access control group • Creating an MIB access control view • Deleting an MIB access control view • Providing an MIB access control view to a group • Deleting a group from all MIB access control views	`setsnmpvacm`	• SNMPv3 settings. • Any access control view that is provided to a group is a Read-Only view.

Note – (1) A user name, authentication password, and encryption password that are common to both the sending and receiving sides are set for an SNMPv3 user.

Note – (2) If inform is specified, InformRequest is sent using the SNMPv2c agent.

Setting the SNMP Agent's System Management Information and Enabling/Disabling the SNMP Agent

- Command operation

1. Use the `showsnmp`**(8) command to display the SNMP settings.**

```
<Example>  Display of the status when no management information has
been set
XSCF> showsnmp
Agent Status:       Disabled
Agent port:         161
System Location:    Unknown
System Contact:     Unknown
System Description: Unknown
:
```

2. Use the `setsnmp`**(8) command to make the SNMP settings.**

```
<Example>  Specifying the installation location of the system, system
description, and mail address of the administrator
XSCF> setsnmp -l MainTower21F -c foo@example.com -d DataBaseServer
```

3. Use the `setsnmp`**(8) command to enable the SNMP agent.**

```
<Example 1>  Enabling the agent.
XSCF> setsnmp enable

<Example 2>  Disabling the agent.
XSCF> setsnmp disable
```

4. Confirm the SNMP settings.

```
XSCF> showsnmp
Agent Status:       Enabled
Agent port:         161
System Location:    MainTower21F
System Contact:     foo@example.com
System Description: DataBaseServer
:
```

Setting SNMPv3 Trap

- Command operation

1. **Use the** `showsnmp`**(8) command to display SNMP settings.**

```
<Example>  Display of the status when settings have been made for
SNMPv1 and SNMPv2c
XSCF> showsnmp
Agent Status:       Enabled
Agent Port:         161
System Location:    MainTower21F
System Contact:     foo@example.com
System Description: DataBaseServer

Trap Hosts:
Hostname  Port  Type  Community String  Username  Auth Protocol
--------  ----  ----  ----------------  --------  --------------
host1     162   v1    public            n/a       n/a
host2     1162  v2    public            n/a       n/a

SNMP V1/V2c:
Status: Enabled
Community String: public
```

2. **Use the** `setsnmp`**(8) command to make SNMPv3 trap settings.**

```
<Example>  Specify a user name, an engine ID, an authentication
algorithm, authentication and encryption passwords, and the host
name or IP address of the trap destination
XSCF> setsnmp addv3traphost -u yyyyy -n 0x### -r SHA host3
Authentication Password: *****
Encryption Password: xxxxxxxx
```

3. **Confirm the SNMPv3 trap settings.**

```
XSCF> showsnmp
Agent Status:       Enabled
Agent Port:         161
System Location:    MainTower21F
System Contact:     musha@jp.fujitsu.com
System Description: DataBaseServer

Trap Hosts:

Hostname   Port  Type  Community String  Username  Auth Protocol
--------   ----  ----  ----------------  --------  -------------
host3       162    v3               n/a     yyyyy            SHA
host1        62    v1            public       n/a            n/a
host2      1162    v2            public       n/a            n/a

SNMP V1/V2c:
Status: Enabled
Community String: public

Enabled MIB Modules:

SP MIB
FM MIB
```

Disabling Traps to the Target Host of SNMPv3

- Command operation

1. **Use the** `showsnmp`**(8) command to display SNMP settings.**

```
XSCF> showsnmp
```

2. **Use the** `setsnmp`**(8) command to disable the trap destination host of the SNMPv3 target.**

```
XSCF> setsnmp remv3traphost -u yyyyy host3
```

3. **Use the** `showsnmp`**(8) command to confirm that the trap destination host has been disabled.**

```
XSCF> showsnmp
```

Enabling/Disabling the SNMPv1 and SNMPv2c Communication

- Command operation

1. **Use the** `showsnmp`**(8) command to display SNMP settings.**

```
XSCF> showsnmp
```

2. **Use the** `setsnmp`**(8) command to enable the SNMPv2c agent.**

```
<Example 1> Enable SNMPv1 and SNMPv2c
XSCF> setsnmp enablev1v2c public

<Example 2> Disable SNMPv1 and SNMPv2c
XSCF> setsnmp disablev1v2c
```

3. **Use the** `setsnmp`**(8) command to enable the SNMP agent.**

```
XSCF> setsnmp enable
```

4. **Use the** `setsnmp`**(8) command to confirm enabling/disabling of the SNMP.**

```
XSCF> showsnmp
```

Setting the SNMPv1 and SNMPv2c Trap

- Command operation

1. **Use the** `showsnmp`**(8) command to display the SNMP settings.**

```
XSCF> showsnmp
```

2. **Use the** `setsnmp`**(8) command to set the SNMPv1 or SNMPv2c trap.**

```
<Example 1>  Specifying the type for SNMPv2c.
XSCF> setsnmp addtraphost -t v2 -s public host2

<Example 2> Specifying the type for SNMPv1.
XSCF> setsnmp addtraphost -t v1 -s public host1
```

3. **Confirm the SNMPv1 and SNMPv2c trap settings.**

```
XSCF> showsnmp
```

Disabling Traps to the Target Host of SNMPv1/SNMPv2c

- Command operation

1. **Use the `showsnmp`(8) command to display SNMP settings.**

```
XSCF> showsnmp
```

2. **Use the `setsnmp`(8) command to disable the trap destination host of the SNMPv1 or SNMPv2c target.**

```
<Example> Disables trap host for SNMPv2c type.
XSCF> setsnmp remtraphost -t v2 host2
```

3. **Use the `showsnmp`(8) command to confirm the disabling of the target the trap destination host.**

```
XSCF> showsnmp
```

Initializing the SNMP Setting to the Default Value

- Command operation

1. **Use the `showsnmp`(8) command to display SNMP settings.**

```
XSCF> showsnmp
```

2. **Use the `setsnmp`(8) command to change the SNMP settings back to the default. At this time, the SNMP agent becomes disabled.**

```
XSCF> setsnmp default
```

3. **Use the `showsnmp`(8) command to confirm that the SNMP setting returned to the default.**

```
XSCF> showsnmp
```

4. **Set the SNMP again and enable the SNMP agent.**

```
XSCF> setsnmp enable
```

5. **Confirm the SNMP settings.**

```
XSCF> showsnmp
```

Note – When you changed the SNMP settings back to the default, if the Sun Management Center (Sun MC) is being used, the SNMP agent information for Sun MC is also cleared. To set the SNMP agent information for Sun MC again, execute the `setsunmc`(8) command with the `-s` option. For details about the command, see the *XSCF Reference Manual* or the man page.

Specifying a User Authentication Algorithm, Creating or Changing an Authentication/Encryption Password, Copy a User, or Delete a User, All of Which is USM Management Information

- Command operation

1. **Use the** `showsnmpusm`**(8) command to display USM management information.**

```
XSCF> showsnmpusm

Username              Auth Protocol
--------------        ------------------
yyyyy                 MD5
user2                 MD5
```

2. **Use the** `setsnmpusm`**(8) command to set USM management information.**

```
<Example 1>  Create an authentication algorithm, authentication
password, and encryption password for a new user.
XSCF> setsnmpusm create -a SHA yyyyy
Authentication Password: xxxxxxxx
Encryption Password: xxxxxxxx

<Example 2>  Change only an authentication password.
(If no password is entered, entry of a password is requested.)
XSCF> setsnmpusm passwd -c auth -o ***** -n xxxxxxxx  yyyyy

<Example 3>  Copy an existing user to add a new user.
XSCF> setsnmpusm clone -u yyyyy newuser

<Example 4> Delete a user
XSCF> setsnmpusm delete yyyyy
```

3. **Use the** showsnmpusm**(8) command to display USM management information.**

```
XSCF> showsnmpusm

Username           Auth Protocol
--------------     ------------------
yyyyy              SHA
user2              MD5
```

Creating a User Account in an Access Control Group, Deleting a User Account From an Access Control Group, Creating and Deleting MIB Access Control Views, Providing an MIB Access Control View to a Group, and Deleting a Group From All MIB Access Control Views, All of Which is VACM Management Information

- Command operation

1. **Use the** showsnmpvacm**(8) command to display VACM management information.**

```
XSCF> showsnmpvacm
Groups:
Groupname         Username
---------------   -------------------
xxxxx             user1, user2
Views
View              Subtree              Mask              Type
---------------   -------------------  ---------------   --------
all_view          .1                   ff                include
Access
View Group
---------------   -------------------
all_view          xxxxx
```

2. **Use the** setsnmpvacm**(8) command to set VACM management information.**

```
<Example 1>  Add a user to an access control group xxxxx.
XSCF> setsnmpvacm creategroup -u yyyyy xxxxx

<Example 2>  Delete a user from an access control group xxxxx.
XSCF> setsnmpvacm deletegroup -u yyyyy xxxxx

<Example 3>  Create an MIB access control view without conditions.
XSCF> setsnmpvacm createview -s .1 all_view

<Example 4>  Create an MIB access control view by using an OID mask.
XSCF> setsnmpvacm createview -s .1.3.6.1.2.1 -m fe excl_view

<Example 5>  Delete an MIB access control view.
XSCF> setsnmpvacm deleteview -s .1.3.6.1.2.1 excl_view

<Example 6>  Provide an MIB access control view to a group.
XSCF> setsnmpvacm createaccess -r all_view xxxxx

<Example 7>  Delete a group from all MIB access control views.
XSCF> setsnmpvacm deleteaccess group1
```

3. **Use the** showsnmpvacm**(8) command to confirm the settings.**

```
XSCF> showsnmpvacm
```

2.2.12 Mail Administration

The mail report function is used to send an email to the system administrator when the fault has occurred in the system. This section explains how to set up the XSCF mail report function.

Note – You should set up the mail configuration so the designated users (platadm, system administrators, and so on) can receive immediate notification of faults that occur on the platform or domain.

TABLE 2-22 lists the settings and the corresponding shell commands.

TABLE 2-22 Mail Administration

Item	Description	Shell Command	Remarks
Display SMTP server settings	Displays SMTP server setting information.	`showsmtp`	
SMTP server	Sets the host name or IP address of the SMTP server.	`setsmtp`	No default value has been set. Only one SMTP server can be specified. If you specify a host name for an SMTP server, the server name must be resolvable by DNS server.
Authentication server	If you enable the Authentication, at the same time, select the POP authentication or the SMTP authentication. When you enable the authentication, specify the host name or IP address of the authentication server, user ID, and password.	`setsmtp`	Default is disable authentication.
Port number	Sets the port number of the SMTP server.	`setsmtp`	The default port number of the SMTP server is 25.
Reply address	Sets the mail address to be specified in the From: header of a mail message.	`setsmtp`	To send an error mail when there is a problem in the path to the recipient address from the mail server, the mail address is specified.
Display mail settings	Displays mail report function setting information.	`showemailreport`	
Enable/ Disable	Enables or disables the mail report function.	`setemailreport`	The default setting is "Disable."
Recipient address	Sets the recipient address for a mail message to be sent to the system administrator.	`setemailreport`	• Multiple addresses can be specified to up to 255 characters, by using a comma as the delimiter. • Include one @ mark per address. (Ex. name1@domain1, name2@domain2, name3@domain3, ...)

Specifying the Host Name, Port Number, and Reply Address of the SMTP Server

- Command operation

1. Use the `showsmtp`**(8) command to display SMTP server setting information.**

```
XSCF> showsmtp
Mail Server:
Port: 25
Authentication Mechanism: none
Reply address:
```

2. Use the `setsmtp`**(8) command to set SMTP server setting information.**

```
<Example 1> Specifying a host name, port number, reply address and
SMTP authentication
XSCF> setsmtp -s mailserver=192.1.4.5 -s port=25 -s replyaddress=
yyyy@example.com -s auth=smtp-auth -s usr=usr001 -s password=
xxxxxxxx

<Example 2> Specifying a host name, port number, reply address and
POP authentication
XSCF> setsmtp
Mail Server [192.1.4.2]: 192.1.4.5
Port[25]:
Authentication Mechanism [none]:pop
        POP Server [192.1.4.2]:
        User Name []: usr001
        Password []: xxxxxxxx
Reply Address [yyyy@example.com]:
```

3. Check the SMTP server setting information.

```
XSCF> showsmtp
Mail Server: 192.1.4.5
Port: 25
Authentication Mechanism : pop
             User Name: usr001
             Password: ********
Reply Address: yyyy@example.com
```

Enabling or Disabling the Mail Report Function and Specifying the Recipient Address Used for Notification

- Command operation

1. **Set the SMTP server as described in Specifying the Host Name, Port Number, and Reply Address of the SMTP Server. Use the** `showemailreport`**(8) command to display mail report setting information.**

```
XSCF> showemailreport
E-Mail Reporting: disabled
```

2. **Use the** `setemailreport`**(8) command to set mail report information.**

```
<Example>  Enabling the mail report function and specifying a reply
addresses
XSCF> setemailreport
Enable E-Mail Reporting? [no]: yes
E-mail Recipient Address []: xxxxx@example.com
Do you want to send a test mail now [no]?: yes
... Sending test mail to 'xxxxx@example.com'
```

3. **Use the** `showemailreport`**(8) command to confirm mail report setting information.**

```
XSCF> showemailreport
E-Mail Reporting: enabled
Recipient Address: xxxxx@example.com
```

4. **Confirm the test mail by checking if an email with the subject "Test Mail" was received.**

2.2.13 Domain Configuration

Domain Configuration logically assigns (by partitioning) multiple system boards (XSBs) mounted in the server to domains. One PSB can be logically divided into 1 (Not divided) or 4 units. It cannot be divided into 2 or 3. (There are two PSBs in the maximum M4000/M5000 server configuration.)You can assign each of the divided system boards to any of the configured domains. In the M3000 server, however, the system board cannot be configured. The system board has been configured to 1 unit (Not divided) by default.

For details on whether to divide a PSB into 1 (Not divided) or 4 units, see Section 2.2.14, “System Board Configuration” on page 2-175.

In the M3000 server, you cannot perform the operations such as setting the domain configuration, or adding or deleting the system board. Domain has been configured by default and cannot be changed. However, you can set the configuration policy and display the domain information.

For an overview of the domain and the system board, see the *Overview Guide* for your server. Also, for an overview of the components, see the *Service Manual* for your server.

TABLE 2-23 lists terms used in Domain Configuration.

TABLE 2-23 Domain Configuration Terms

Term	Description
Domain	When hardware resources in the server are logically divided into one or more units, each set of divided resources can be used as one system, which is called a domain. An Oracle Solaris OS can operate in each domain.
PSB	The PSB is made up of physical components, and can include 1 CMU (CPU/Memory Board unit) and 1 IOU (I/O unit) or just 1 CMU. In the M4000/M5000 servers, the CMU is mounted on the MBU. A PSB can also be used as to describe a physical unit for addition/deletion/exchange of hardware. The PSB can be used in one of two methods, one complete unit (undivided status) or divided into four subunits. However, in the M3000 server, the PSB can be used in one complete unit (undivided status) only. **Note -** On the M4000/M5000 servers, 1 PSB is 1 CMU. In an M4000 server, a PSB makes up the entire MBU. In an M5000 server, there are two PSBs on the single Motherboard unit (one PSB contains CPUs 0 to 3 and the other PSB contains CPUs 4 to 7). In the M3000 server, a PSB makes up the entire MBU. There is only one PSB, which contains CPU, I/O, and memory. The PSB cannot be divided into four subunits.
XSB	The XSB is made of physical components. In the XSB, the PSB can be either one complete unit (undivided status) or divided into four subunits. The XSB is a unit used for domain construction and identification, and can be also used as a logical unit.
LSB	A logical unit name assigned to an XSB. Each domain has its own set of LSB assignments. LSB numbers are used to control how resources such as kernel memory get allocated within domains.
System board	The hardware resources of a PSB or an XSB. A system board is used to describe the hardware resources for operations such as domain construction and use. In this manual, the system board refers to the XSB.
Uni-XSB	One of the division types for a PSB to be configured. Uni-XSB is a name for when a PSB is logically only one unit (undivided status). It is a default value setting for the division type for a PSB. The division type can be changed by using the XSCF command, `setupfru`(8). Uni-XSB may be used to describe a PSB division type or status.
Quad-XSB (Note 3)	One of the division types for a PSB to be configured. Quad-XSB is a name for when a PSB is logically divided into four parts. The division type can be changed by using the XSCF command, `setupfru`(8). Quad-XSB may be used to describe a PSB division type or status.
Hardware resource	Hardware components contained on a system board that configures a domain.

TABLE 2-23 Domain Configuration Terms *(Continued)*

Term	Description
Domain Configuration	Divides hardware resources in this system into independent software-based units. Partitioning is performed with XSCF as follows: 1. XSBs are defined with each consisting of a CMU or MBU and an I/O unit divided by software. (In M4000/M5000 servers, there will be I/O on only half of the XSBs.) 2. Each XSB is handled as an LSB so that it can configure a domain and be assigned a number (LSB number). Furthermore, XSCF can define LSB resources in detail. 3. The domain operates with the LSB resources and the LSB number.
Domain ID (DID)	ID assigned to a domain.
Domain Component List (DCL)	This is a list of domain configuration information. The DCL represents the hardware resource information that is set for each domain and each LSB belonging to a domain. It can be specified and displayed by `setdcl`(8) and `showdcl`(8), respectively.
Memory mirror mode	In this mode, a PSB has two memory units, one mirroring the other. Saving the same data in the separate memory units improves data security.
DIMM (Memory)	Memory modules on a system board. For details on DIMMs, see the *Service Manual* for your server.
Configuration policy (Note 2)	If an error is detected in a domain in an initial hardware diagnosis, the range of logical resources to be removed can be specified. The policy determines whether to remove system boards or separate resources. On M3000 servers, the `setdcl`(8) command can only be used to set configuration policy.
Omit-I/O option (Note 2)	System board (XSB) configuration that prevents a specific domain from logically using I/O units on a system board. The DR function (Note 1) is enabled with fewer hardware resources. (A PCI and LAN driver are prevented from being incorporated into the domain of an LSB.)
Omit-memory option (Note 2)	System board (XSB) configuration that prevents a specific domain from logically using memory on a system board.
Floating board (Note 2)	A floating board is designated to be moved easily to another domain. In operation with a kernel and important I/O on the system board in a domain, and to facilitate the DR operation of the system board, it is necessary to define the system board so that can be deleted or moved easily. This definition is called a floating board option. A system board that lowered priority of the kernel memory loading by enabling the floating board option is called a floating board.

TABLE 2-23 Domain Configuration Terms *(Continued)*

Term	Description
XSB status	The power status and the diagnostic, assignment, and integration conditions of a system board belonging to a domain are displayed for each XSB. The progress of changes in conditions can be found by switching the domain configuration. The XSB status information can be referred to with `showdcl`(8) and `showboards`(8). For details on the XSB status, see TABLE 2-27.
Fault code	Indicating that an error occurred in an XSB. For details on the fault codes, see TABLE 2-27.
System board pool (SP)	The state of system board that does not belong to any domain. A system board that is the system board pool state can be added to a domain where a CPU or memory has a high load. When the added system board becomes unnecessary, the system board can be returned to the system board pool state.

Note – (1) DR*:* Abbreviation for Dynamic Reconfiguration. This function dynamically adds a system board to a domain or deletes it from a domain. For details on DR, see the *Dynamic Reconfiguration User's Guide*.

Note – (2) Specified or displayed by the DCL. When the system board uses kernel or I/O, for details of the DR operation and notation, see the *Dynamic Reconfiguration User's Guide*.

Note – (3) Although a CMU with two CPUMs can be configured into Quad-XSB mode on an M8000/M9000 server, be aware of the following points:

- Only an XSB with at least one valid CPUM and memory can be configured into a domain.
- Memory within an XSB that does not have a CPUM becomes unavailable. The result is loss of access to half the installed memory on the CMU.
- You can add DIMMs to a CMU, but you cannot reconfigure memory resident on a CMU to the valid XSBs to prevent that memory from becoming unavailable.
- The server generates a "configuration error" message for those XSBs that do not have a CPUM and memory.

For details of components such as CPU/Memory Board unit, I/O unit, and Motherboard unit, see the *Service Manual* for your server.

TABLE 2-24 lists the number of domains and XSBs for each system.

TABLE 2-24 Number of Domains and XSBs for Each System

System		Range of Domain ID	Maximum Number of XSBs	Memory Mirror (Note)
Entry-level systems	The system containing 1 CPU chip. (M3000 server)	0	1	Not available
Midrange systems	The system containing up to 4 CPU chips. (M4000 server)	0 - 1	4 (1 x 4)	Enabled for both Uni-XSBs and Quad-XSBs
	The system containing up to 8 CPU chips. (M5000 server)	0 - 3	8 (2 x 4)	
High-end systems	The system containing up to 32 CPU chips. (M9000)	0 - 23	32 (8 x 4)	Uni-XSBs only Enabled
	The system containing up to 16 CPU chips. (M8000)	0 - 15	16 (4 x 4)	
High-end system with expansion cabinet	The system containing up to 64 CPU chips. (M9000)	0 - 23	64 (16 x 4)	

Note – Enabling Memory Mirror would require twice the amount of memory of a domain used for operation. If the system board is a Quad-XSB in the M8000/M9000 servers, Memory Mirror cannot be used.

TABLE 2-25 lists the PSB, XSB, and LSB numbers to be assigned.

The PSB number is same as the CPU/Memory Board unit or I/O unit slot number.

If a PSB has one XSB number, the Uni-XSB configuration is assumed; and if it has four XSB numbers, the Quad-XSB configuration is assumed.

TABLE 2-25 PSB, XSB, and LSB Numbers to be Assigned (Decimal)

PSB Number (Note)	XSB Number (Uni-XSB) (Note)	XSB Number (Quad-XSB) (Note)	LSB Number
00	00-0	00-0, 00-1, 00-2, 00-3	Independent values, 00 to 15, can be arbitrarily specified in a domain.
01	01-0	01-0, 01-1, 01-2, 01-3	
02	02-0	02-0, 02-1, 02-2, 02-3	
:	:	:	
15	15-0	15-0, 15-1, 15-2, 15-3	

TABLE 2-26 lists DCL information. The DCL has descriptors that each specify one item of LSB information. Up to 16 items of LSB information (on the DCL) can be set for one domain. These items can be displayed and specified by `showdcl`(8), and `setdcl`(8). For details on DCL terms, see TABLE 2-23.

TABLE 2-26 DCL Information

DCL Item	Setting Details and Notes
Domain ID	Local domain number.
LSB number	LSB number.
XSB number	XSB number assigned to an LSB. The same XSB number cannot be assigned to another LSB in the same domain.
no-mem (Omit-memory option)	True : Memory cannot be used. False : Memory can be used (default).
no-io (Omit-I/O option)	True : Does not add I/O. False : Adds I/O (default).

TABLE 2-26 DCL Information *(Continued)*

DCL Item	Setting Details and Notes
Floating Board	True : Selects a Floating Board. False : Does not select a Floating Board (default).
Configuration policy	FRU : Removal in units of Field Replaceable Unit (FRU) components. (Default) XSB : Removal in XSB units System : Hardware is degraded in units of domains or the relevant domain is stopped without degradation. In the M3000 server, you can set the configuration policy only.
Domain status	Display domain status as follows. Powered Off: Power off state. Initialization Phase: State that POST is proceeding or initializing is started by OpenBoot PROM. OpenBoot Executing Completed: State that initializing is completed by OpenBoot PROM Booting/OpenBoot PROM prompt: The Oracle Solaris OS is booting. Or due to the domain shutdown or reset, the system is in the OpenBoot PROM running state, or is suspended in the OpenBoot PROM (`ok` prompt) state. Running: State that Oracle Solaris OS is running. Shutdown Started: State that the power off is started. Panic State: State that panic is occurred and reset is not started.

One domain can use up to 16 LSBs. The user can define the different XSB in each LSB by using XSCF. Also, multiple domains can assign LSBs to the same XSB. If multiple domains assign them to the same XSB, however, the domains not using that XSB are in a state (Unconfigured) that does not allow them to use the XSB until the domain using it (Assigned or Configured) releases it.

Caution – IMPORTANT - If the XSB associated with the specified LSB has been configured in the domain configuration, the information that is set for the LSB cannot be changed. Also, if the specified domain is running, the value of configuration policy cannot be changed. To change the value, first turn off power to the domain.

TABLE 2-27 lists the XSB status information. This information can be displayed by the `showboards`(8) command.

TABLE 2-27 XSB Status Information

Item	Explanation
XSB number	XSB number.
DID	Domain ID.
LSB	LSB number that is used for domain.
assignment (Assignment)	Status of pre-arranged registration in a domain unavailable: ..... The XSB is in the system board pool (not assigned to a domain) and its status is one of the following: not-yet diagnosed, under diagnosis, or diagnosis error. All XSBs that are not mounted are also shown as Unavailable. available: ..... XSB is in the system board pool and its diagnosis has completed normally. assigned: ..... XSB assigned to the domain.
power (Pwr)	Indicates the XSB power status. n: ..... XSB power off state y: ..... XSB power on state
connectivity (Conn)	Indicates the state of a hardware connection to a domain. n: ..... System board pool state The XSB has been deleted from the domain by hardware. (This includes a domain shutdown.) y: ..... XSB connected by hardware to the domain. (The XSB is active in the domain or ready to be added to the Oracle Solaris OS.)
configuration (Conf)	Status of a logical connection to a domain. n: ..... Not added to the domain (Oracle Solaris OS). y: ..... Active and added to the domain (Oracle Solaris OS).
test (Test)	Indicates the diagnosis status. (Note) Unmount: ..... XSB not yet mounted or defined. Unknown: ..... Diagnosis not yet performed. Testing: ..... Diagnosis in progress. Passed: ..... Diagnosis completed normally. Failed: ..... A diagnosis error was detected and XSB continuous operation is not possible.

TABLE 2-27 XSB Status Information *(Continued)*

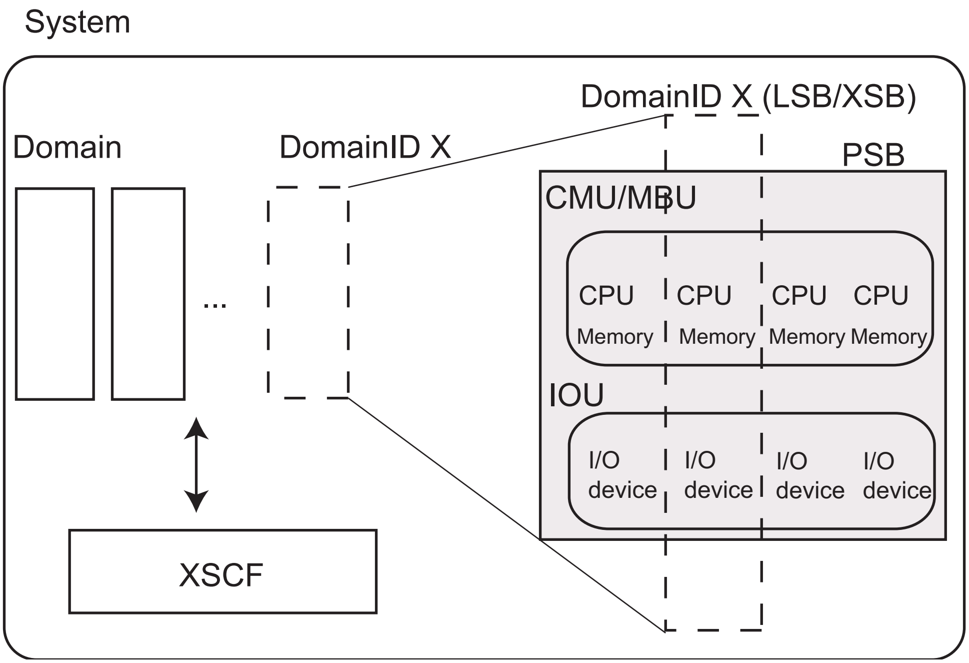
Item	Explanation
fault_code (Fault)	Indicates that state of a degradation in the XSB. Normal: ..... Normal. Degraded: ..... A component is to be removed. Faulted: ..... Error found in initial diagnosis.
Reservation (R)	Displays the reservation status of XSB. If * mark is displayed in the XSB, DR processing is reserved. When the domain is rebooted, the XSB is incorporated into or disconnected from the domain, and the domain configuration is changed.
COD (COD)	Displays the COD status of XSB. n: ..... There is no components of COD. y: ..... There is a component of COD.

Note – The result of the initial diagnosis by `testsb`(8) command is displayed in specified PSB. Also you can use the `showboards`(8) command to check diagnosis results such as the 'Test' or 'Fault' status. For details about the command, see the *XSCF Reference Manual*. In the M3000 server, the `testsb`(8) command is not available, so confirm the diagnosis result by executing the `poweron`(8) command. For details on XSB status transitions during system board installation, removal, and replacement in the server, see the *Dynamic Reconfiguration User's Guide*.

Domain Hardware and Software Configurations

FIGURE 2-2 lists the hardware resources that configure a domain. XSCF manages the hardware configuration of each domain in the server. The CPU and the memory (DIMM) are installed in a CMU or MBU. The domain uses CPU, memory, and I/O device logically divided as one system board.

FIGURE 2-2 Domain Component Hardware (In Midrange and High-End Servers)



Note – In the entry-level server, the number of domains is one, and the domain fully uses the resources in the PSB

Note – FIGURE 2-3 is an XSCF-domain correlation diagram. XSCF enables domain configuration control and DR function control by using DSCP interface and SCF interface for XSCF-domain modules (control program) communication.

FIGURE 2-3 XSCF-Domain Correlation Diagram

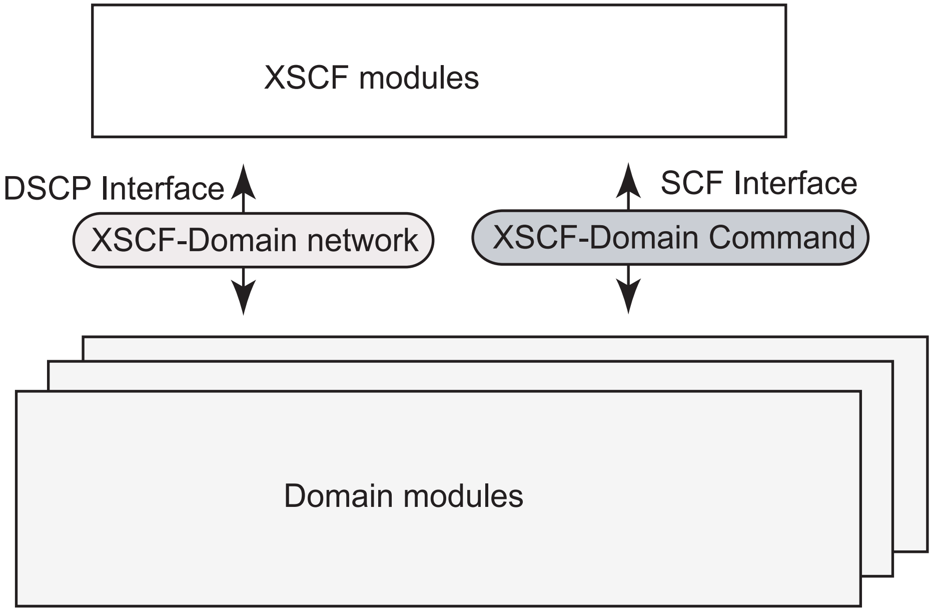


FIGURE 2-4 and FIGURE 2-5 show XSB hardware configuration diagrams in the midrange servers. The number of hardware resources depends on whether the PSB type is a Uni-XSB or Quad-XSB. FIGURE 2-4 and FIGURE 2-5 are examples when two CMUs are mounted on the MBU.

FIGURE 2-4 XSB Configuration Diagram (Uni-XSB) (In the Midrange Servers)

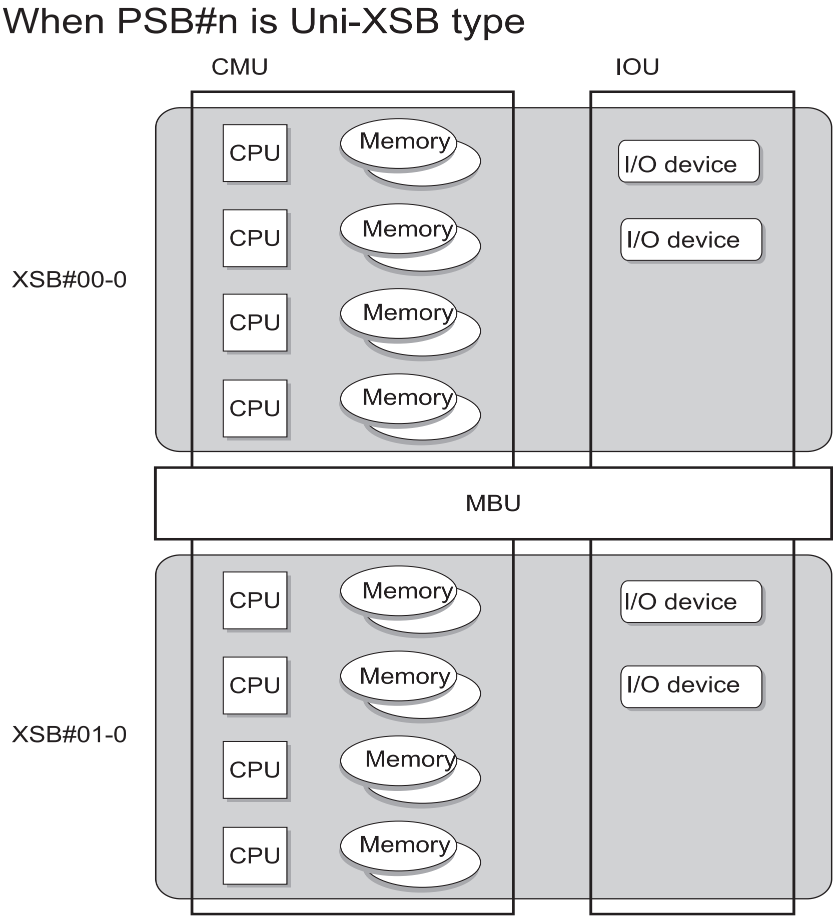


FIGURE 2-5 XSB Configuration Diagram (Quad-XSB) (In the Midrange Servers)

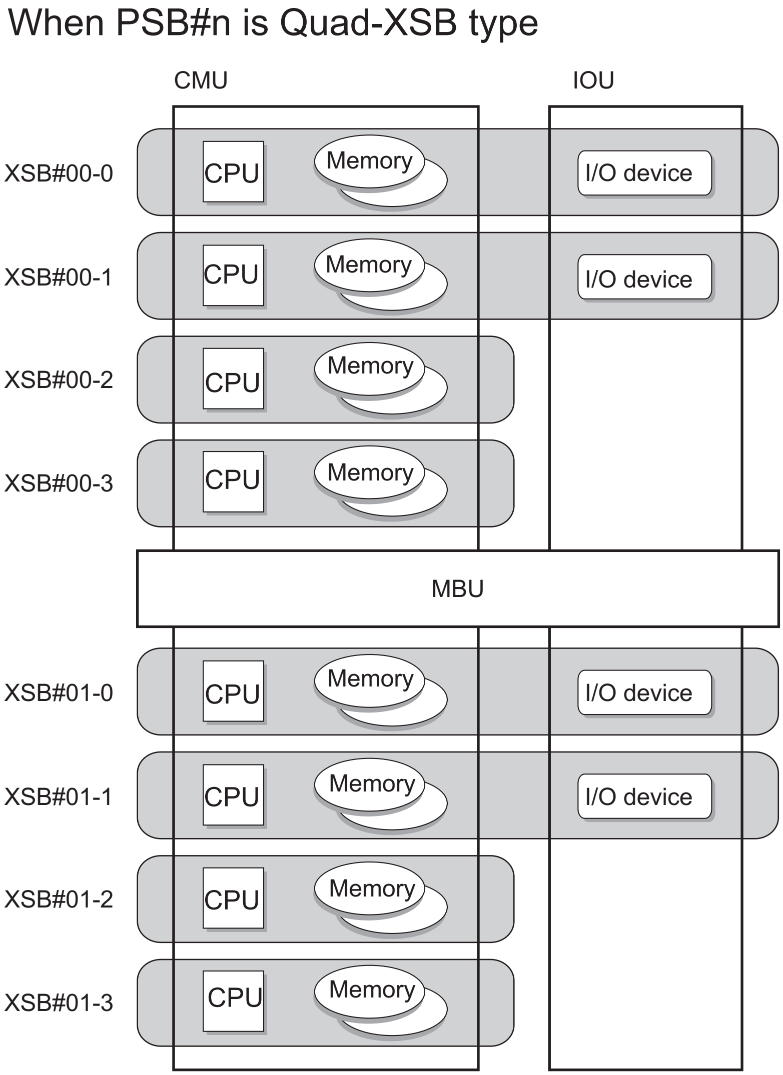


FIGURE 2-6 and FIGURE 2-7 show XSB hardware configuration diagrams in the high-end servers. The number of hardware resources depends on whether the PSB type is a Uni-XSB or Quad-XSB.

FIGURE 2-6 shows Uni- XSB hardware configuration diagrams in high-end servers.

FIGURE 2-6 XSB Configuration Diagram (Uni-XSB) (In the High-End Servers)

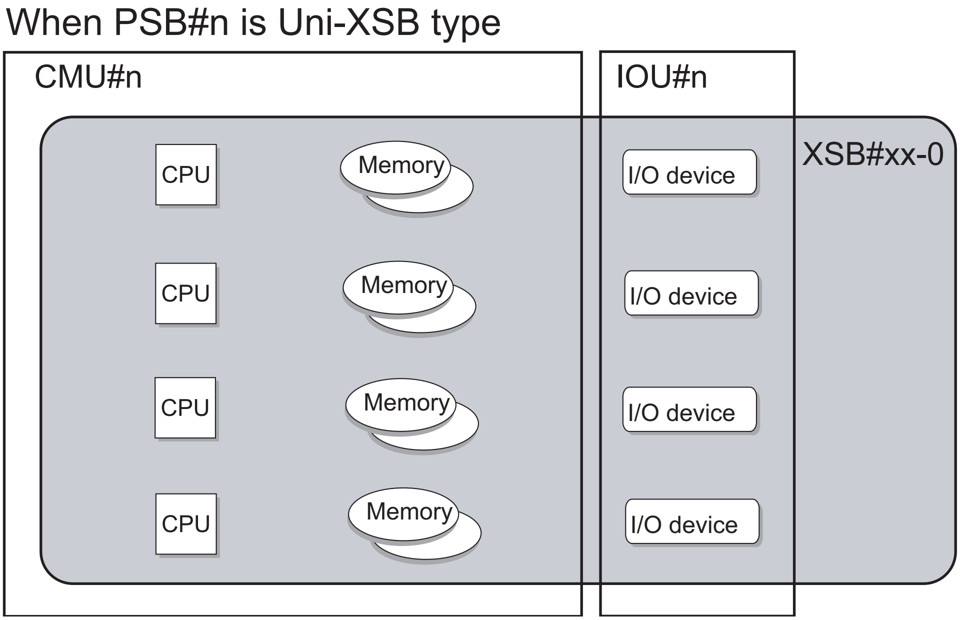


FIGURE 2-7 shows Quad-XSB hardware configuration diagrams in high-end servers.

FIGURE 2-7 XSB Configuration Diagram (Quad-XSB) (In the High-End Servers)

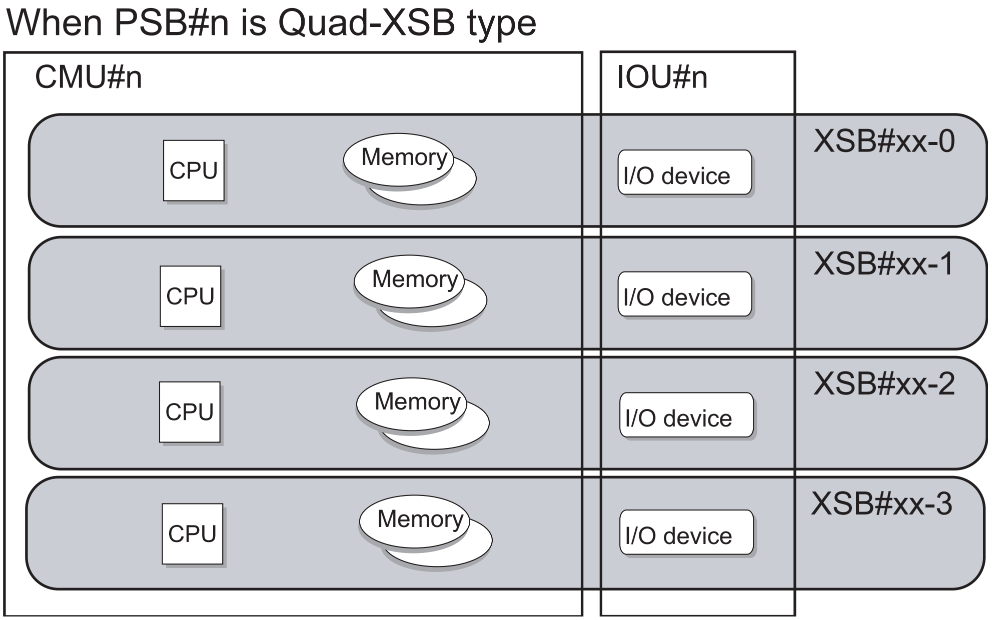
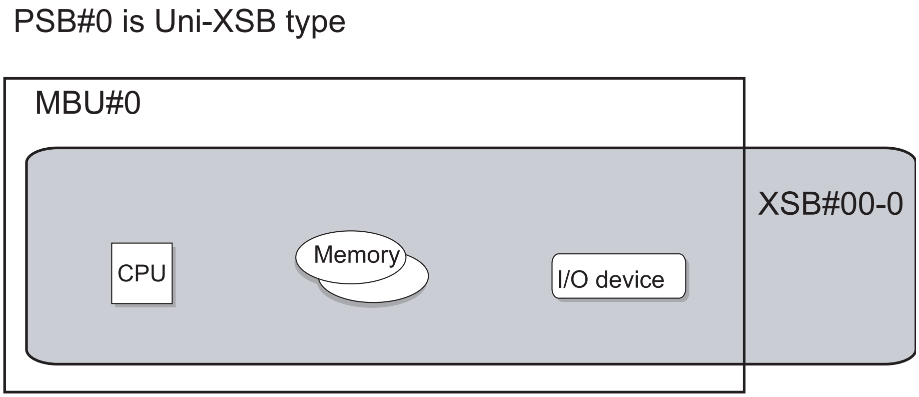


FIGURE 2-8 shows Uni-XSB hardware configuration diagrams in an entry-level server. The PSB type is fixed to Uni-XSB. In the entry-level server, the number of domains is one, and the domain fully uses the resources in the PSB

FIGURE 2-8 XSB Configuration Diagram (Uni-XSB) (In the Entry-Level Server)



Domain Configuration Procedure and Reference Sources

The steps from making domain configuration settings to activating a domain are shown below. Each step contains a reference to where you can find additional information.

In the M3000 server, Step 2 and Step 4 are not required. Perform Step 1, Step 3 and Step 5, only if you change the domain configuration policy.

1. **Log in to XSCF.**

2. **Make memory mirror mode and Uni/Quad-XSB settings for each PSB. (Note) (See** `showfru`**(8),** `setupfru`**(8), and** Section 2.2.14, "System Board Configuration" on page 2-175.**)**

3. **Create the DCL information corresponding to a domain, LSB, and XSB. (See** `showdcl`**(8),** `setdcl`**(8).)**

4. **Assign an XSB to the domain, according to the created DCL information. (See** `addboard`**(8),** `showboard`**(8).)**

5. **Turn on the power to the domain.**

Note – Make these settings only to change the number of XSB divisions and the mirror mode.

Note – For the procedure for installing, removing, or replacing a system board in the server, see the *Service Manual* for your server. Also, for details on using the DR function, see the *Dynamic Reconfiguration User's Guide*.

Note – For an overview of configuring domains, including an extensive example, refer to the *Administration Guide*.

TABLE 2-28 lists setting items and the corresponding shell commands.

TABLE 2-28 Domain Configuration

Item	Description	Shell command	Remarks
Display XSB status	Displays the XSB status for the specified domain or all domains. For XSB status information, see TABLE 2-27.	`showboards`	
Display domain status	Displays one of the following items for the current domain status: For details of domain status, see TABLE 2-26.	`showdomainstatus` `showdcl`	
Display resource use state	Displays the use status of devices and resources on an XSB.	`showdevices`	
Display DCL information	Displays the DCL information for a system board in the specified domain.	`showdcl`	
DCL	Sets DCL information. Specify configuration for LSB of specified domain. For details of configuration information, see TABLE 2-26.	`setdcl`	"Omit-memory", "Omit-I/O", and "Floating board" are false by default.
Add to domain	Adds or assigns an XSB to a domain, according to DCL information. Specify the following: • Domain ID and number of the added XSB • assign Specify one of the following integration states when the domain is running (the DR function): • configure (configure into Oracle Solaris OS) • assign • reserve (assign (reserve))	`addboard`	If the XSB is placed in the assign state, a reboot of the assigned domain or the `addboard`(8) command with "configure" specified would configure the board into a running Oracle Solaris OS domain (the DR function).

TABLE 2-28 Domain Configuration *(Continued)*

Item	Description	Shell command	Remarks
Delete from domain	Deletes an XSB from a domain. Specify the following: • Number of the deleted XSB • unassign Specify one of the following states after deletion when the domain is running (the DR operation): • disconnect (deletion (assigned state)) • unassign (complete deletion (pool state)) • reserve (reserve deletion)	`deleteboard`	• The XSB is placed in the assigned state when "disconnect" is performed. At this state, a reboot of the domain or the `addboard`(8) command would add the XSB again. • If the XSB is placed in the reserve (reserve deletion) state, turning off power to the domain places it in the pool state. (These are the DR functions.)
Move to domain	Moves an XSB from its current domain to another domain. After the XSB is deleted from its domain, the function adds or assigns it to the other domain. Specify the following: • Domain ID and XSB number of the move destination • assign Specify one of the following movement/integration states when the domain is running (the DR function): • configure (configure into Oracle Solaris OS) • assign (assign the XSB to the move destination (reserve)) • reserve (reserve movement)	`moveboard`	• If the XSB is placed in the assign state, a reboot or the `addboard`(8) command with "configure" specified at the domain of the move destination would add the XSB. • If the XSB is placed in the reserve (reserve movement) state, turning off power to the domain places it in the pool state. Turning on power to the move destination adds the XSB. (These are the DR functions; see Note.)

Note – For details on using DR functions, see the *Dynamic Reconfiguration User's Guide.*

Displaying the XSB Status

By referring to the XSB status of a domain, the user obtains information about an XSB, such as whether its has been assigned and whether it has been recognized by the Oracle Solaris OS. Such information also includes the current process and state of the XSB and whether it was added or deleted successfully. The procedure for displaying status information is shown below.

To display the domain partitioning status, see Section 2.2.14, "System Board Configuration" on page 2-175. In the M3000 server, only the following number is displayed, domain ID is 00, XSB is 00-0, and LSB is 00.

- Command operation

● **Use the** `showboards`**(8) command to display XSB status information.**

```
<Example 1> Display all XSB status information.
XSCF> showboards -va
XSB  R DID(LSB) Assignment  Pwr  Conn Conf Test    Fault    COD
---- - -------- ----------- ---- ---- ---- ------- -------- ----
00-0   00(00)   Assigned    y    y    y    Passed  Normal   n
00-1   00(01)   Assigned    y    y    y    Passed  Normal   n
00-2   02(02)   Assigned    y    y    n    Passed  Normal   n
00-3   03(03)   Assigned    y    y    n    Passed  Normal   n
01-0   01(01)   Assigned    y    y    y    Passed  Normal   n
01-1   01(02)   Assigned    y    y    y    Passed  Normal   n
01-2   02(06)   Assigned    y    y    n    Passed  Normal   n
01-3   03(07)   Assigned    y    y    n    Passed  Normal   n

<Example 2> Display detailed information about XSB#00-0.
XSCF> showboards -v 00-0
XSB  R DID(LSB) Assignment  Pwr  Conn Conf Test    Fault    COD
---- - -------- ----------- ---- ---- ---- ------- -------- ----
00-0   00(00)   Assigned    y    y    y    Passed  Normal   n

<Example 3> Display XSB information about pooled XSBs and domain ID 0.
XSCF> showboards -c sp -d 0
XSB  DID(LSB) Assignment  Pwr  Conn Conf Test    Fault
---- -------- ----------- ---- ---- ---- ------- --------
00-0 SP       Assigned    n    n    n    Passed  Normal
```

Displaying or Specifying DCL Information

- Command operation

1. Use the `showdcl`**(8) command to display DCL information.**

```
<Example> Display DCL information on domain ID 2.
XSCF> showdcl -v -d 2
DID   LSB   XSB   Status   No-Mem   No-IO   Float     Cfg-policy
02                Powered Off                         System
      00    00-0           False    False    False
      01      -
:
      15      -
```

2. Use the `setdcl`**(8) command to specify DCL information.**

```
<Example 1> In domain ID 2, specify XSB#01-0 for an LSB#07, system
for the configuration policy, false for Omit-memory option, false
for Omit-I/O option,  and false for floating board.
XSCF> setdcl -d 2 -a 7=1-0
XSCF> setdcl -d 2 -s policy=system
XSCF> setdcl -d 2 -s no-mem=false 7
XSCF> setdcl -d 2 -s no-io=false 7
XSCF> setdcl -d 2 -s float=false 7

<Example 2> In domain ID 2, specify XSB#00-0 for an LSB#00, XSB#00-1
for an LSB#01, XSB#01-1 for an LSB#08, XSB#01-2 for an LSB#09,
XSB#01-3 for an LSB#10.
XSCF>  setdcl -d 2 -a 0=0-0 1=0-1 8=1-1 9=1-2 10=1-3

<Example 3> Delete the data defined for LSB#01 in domain ID 2.
XSCF> setdcl -d 2 -r 1
```

3. **Use the** `showdcl`**(8) command to display DCL information.**

```
XSCF> showdcl -va
DID   LSB   XSB   System   No-Mem   No-IO    Float    Cfg-policy
02                Powered Off                         System
      00    00-0           False    False    False
      01    -
      02    -
      03    -
      04    -
      05    -
      06    -
      07    01-0           False    False    False
      08    01-1           False    False    False
      09    01-2           False    False    False
      10    01-3           False    False    False
      11    -
      12    -
      13    -
      14    -
      15    -
```

Assigning or Configuring a System Board to a Domain

- Command operation

1. **After the DCL information, use the** `showfru`**(8),** `showdcl`**(8) commands to display XSB status information.**

```
XSCF> showfru -a sb
Device  Location    XSB Mode            Memory Mirror Mode
sb      00          Uni                 no
sb      01          Quad                no
XSCF>
XSCF> showdcl -va
DID   LSB   XSB   System   No-Mem   No-IO    Float    Cfg-policy
02                Powered Off                         System
      00    00-0           False    False    False
      01    -
      02    -
      03    -
      04    -
      05    -
      06    -
      07    01-0           False    False    False
      08    01-1           False    False    False
      09    01-2           False    False    False
      10    01-3           False    False    False
      11    -
      12    -
      13    -
      14    -
      15    -
```

2. **Use the** `showboards`**(8) command to display XSB status information.**

```
<Example> Display detailed information about XSBs.
XSCF> showboards -va
XSB  R DID(LSB) Assignment  Pwr  Conn Conf Test    Fault    COD
---- - -------- ----------- ---- ---- ---- ------- -------- ----
00-0   SP       Available   n    n    n    Passed  Normal   n
01-0   SP       Available   n    n    n    Passed  Normal   n
01-1   SP       Available   n    n    n    Passed  Normal   n
01-2   SP       Available   n    n    n    Passed  Normal   n
01-3   SP       Available   n    n    n    Passed  Normal   n
```

3. **Use the** `addboard`**(8) command to add an XSB and use the** `showboards`**(8) command to confirm the XSB status.**

```
<Example> Assign XSB#00-0, XSB#01-0, XSB#01-1, XSB#01-2, XSB#01-3 to domain ID 2.
XSCF> addboard -c assign -d 2 00-0 01-0 01-1 01-2 01-3
XSB#00-0 will be assigned to DomainID 2. Continue?[y|n] :y
XSB#01-0 will be assigned to DomainID 2. Continue?[y|n] :y
XSB#01-1 will be assigned to DomainID 2. Continue?[y|n] :y
XSB#01-2 will be assigned to DomainID 2. Continue?[y|n] :y
XSB#01-3 will be assigned to DomainID 2. Continue?[y|n] :y
XSCF>
XSCF> showboards -va
XSB  R DID(LSB) Assignment  Pwr  Conn Conf Test    Fault    COD
---- - -------- ----------- ---- ---- ---- ------- -------- ----
00-0   02(00)   Assigned    n    n    n    Passed  Normal   n
01-0   02(07)   Assigned    n    n    n    Passed  Normal   n
01-1   02(08)   Assigned    n    n    n    Passed  Normal   n
01-2   02(09)   Assigned    n    n    n    Passed  Normal   n
01-3   02(10)   Assigned    n    n    n    Passed  Normal   n
```

4. **Use the** `poweron`**(8) command to start up domain ID 2.**

```
XSCF> poweron -d 2
DomainIDs to power on:02
Continue? [y|n] :y
02 :Powering on

*Note*
 This command only issues the instruction to power-on.
 The result of the instruction can be checked by the "showlogs
power".
```

5. **Use the** `console`**(8) command to connect a domain console. Check the configuration by using** `prtdiag`**(1M).**

```
<Example> Connect the OS console of domain ID 2.
XSCF> console -d 2

Console contents may be logged.
Connect to DomainID 2?[y|n] :y
:
exit from console.
```

To switch from the domain console to the XSCF Shell, press the Enter, “#” (default escape character), and “.” (period) keys.

6. **Use the** `showboards`**(8) command to confirm the XSB status. (See TABLE 2-27.)**

```
XSCF> showboards -va
XSB  R DID(LSB) Assignment  Pwr  Conn Conf Test    Fault    COD
---- - -------- ----------- ---- ---- ---- ------- -------- ----
00-0   02(00)   Assigned    y    y    y    Passed  Normal   n
01-0   02(07)   Assigned    y    y    y    Passed  Normal   n
01-1   02(08)   Assigned    y    y    y    Passed  Normal   n
01-2   02(09)   Assigned    y    y    y    Passed  Normal   n
01-3   02(10)   Assigned    y    y    y    Passed  Normal   n
```

7. **Use the** `showdomainstatus`**(8) command to confirm the domain ID 2 status. (See TABLE 2-26.)**

```
XSCF> showdomainstatus -a
DID        Domain Status
00         -
01         -
02         Running
03         -
```

Note – When adding the system board to the domain using DR functions that operate the XSB without stopping the domain, see the *Dynamic Reconfiguration User's Guide*.

Deleting a System Board From a Domain

- Command operation

1. Use the `showdevices`**(8) command to display the usage of XSB resources.**

```
<Example> Display usage of XSB resources of domain ID 2.
XSCF> showdevices -d 2

CPU:
----
DID XSB  id  state    speed  ecache
02  01-0 0   on-line   2376       0
02  01-0 1   on-line   2376       0
02  01-0 2   on-line   2376       0
02  01-0 3   on-line   2376       0
02  01-1 488 on-line   2376       0
02  01-1 489 on-line   2376       0
02  01-1 490 on-line   2376       0
02  01-1 491 on-line   2376       0
02  01-2 40  on-line   2376       0
02  01-2 41  on-line   2376       0
02  01-2 42  on-line   2376       0
02  01-2 43  on-line   2376       0
02  01-3 50  on-line   2376       0
02  01-3 51  on-line   2376       0
02  01-3 52  on-line   2376       0
02  01-3 53  on-line   2376       0

Memory:
-------
          board   perm    base                domain  target deleted remaining
DID XSB   mem MB  mem MB  address             mem MB  XSB    mem MB  mem MB
02  01-0    8192    2048  0x000003c000000000   32768
02  01-1    8192       0  0x0000020000000000   32768
02  01-2    8192       0  0x000001c000000000   32768
02  01-3    8192       0  0x0000018000000000   32768

IO Devices:
----------
DID XSB       device  resouce                usage
02  01-0      sd0     /dev/dsk/c0t0d0s0      mounted filesystem "/"
02  01-0      sd0     /dev/dsk/c0t0d0s1      swap area
02  01-0      sd0     /dev/dsk/c0t0d0s1      dump device (swap)
```

2. **Use the** `showboards`**(8) command to display XSB status information.**

```
XSCF> showboards -va
XSB  R DID(LSB) Assignment  Pwr  Conn Conf Test    Fault    COD
---- - -------- ----------- ---- ---- ---- ------- -------- ----
00-0   02(00)   Assigned    y    y    y    Passed  Normal   n
01-0   02(07)   Assigned    y    y    y    Passed  Normal   n
01-1   02(08)   Assigned    y    y    y    Passed  Normal   n
01-2   02(09)   Assigned    y    y    y    Passed  Normal   n
01-3   02(10)   Assigned    y    y    y    Passed  Normal   n
```

3. **Use the** `poweroff`**(8) command to power off domain ID 2.**

```
XSCF> poweroff -d 2
DomainIDs to power off:02
Continue? [y|n] :y
02 :Powering off
*Note*
 This command only issues the instruction to power-off.
 The result of the instruction can be checked by the
 "showlogs power".
```

4. **Use the** `showboards`**(8) command to display XSB status information.**

```
XSCF> showboards -va
XSB  R DID(LSB) Assignment  Pwr  Conn Conf Test    Fault    COD
---- - -------- ----------- ---- ---- ---- ------- -------- ----
00-0   02(00)   Assigned    n    n    n    Passed  Normal   n
01-0   02(07)   Assigned    n    n    n    Passed  Normal   n
01-1   02(08)   Assigned    n    n    n    Passed  Normal   n
01-2   02(09)   Assigned    n    n    n    Passed  Normal   n
01-3   02(10)   Assigned    n    n    n    Passed  Normal   n
```

5. **Use the** `deleteboard`**(8) command to delete an XSB.**

```
<Example> Delete XSBs and make XSBs pool state.
XSCF> deleteboard -c unassign 1-1
XSB#01-1 will be unassigned from domain immediately. Continue?[y|n]
:y
XSCF>
```

Note – When you delete the system board, please confirm the domain status, the system board status, the device usage status on the system board, and also the processes usage that are bound to the CPU or are accessing I/O devices. Then confirm whether you should be able to delete the system board. Remember that CPU/Memory Board unit resources also define the I/O resources, so deleting one resource will affect the other. For details about operating the XSB while the Oracle Solaris OS is running, and for details about DR messages, see the *Dynamic Reconfiguration User's Guide*.

6. **Use the** `showboards`**(8) command to confirm that the XSB has been deleted from the domain.**

```
XSCF> showboards -va
XSB  R DID(LSB) Assignment  Pwr  Conn Conf Test    Fault    COD
---- - -------- ----------- ---- ---- ---- ------- -------- ----
00-0   02(00)   Assigned    n    n    n    Passed  Normal   n
01-0   02(07)   Assigned    n    n    n    Passed  Normal   n
01-1   SP       Available   n    n    n    Passed  Normal   n
01-2   02(09)   Assigned    n    n    n    Passed  Normal   n
01-3   02(10)   Assigned    n    n    n    Passed  Normal   n
```

Moving a System Board From One Domain to Another

- Command operation

1. **Use the** `showdcl`**(8) command to display DCL information.**

```
XSCF> showdcl -a
DID   LSB   XSB   Status
02                Powered Off
      00    00-0
      07    01-0
      08    01-1
      09    01-2
      10    01-3
```

2. **Use the** `setdcl`**(8) command to define the LSB of a new domain.**

```
<Example> In domain ID 1, specify XSB#01-0 for an LSB#00,  XSB#01-1
for an LSB#01,  XSB#01-2 for an LSB#02,  XSB#01-3 for an LSB#03.
XSCF> setdcl -d 1 -a 0=1-0 1=1-1 2=1-2 3=1-3
```

3. **Use the** `showdcl`**(8) command to confirm the DCL information.**

```
XSCF> showdcl -a
DID   LSB   XSB   Status
01                Powered Off
      00    00-0
      01    01-1
      02    01-2
      03    01-3
------------------------------------------
02                Powered Off
      00    00-0
      07    01-0
      08    01-1
      09    01-2
      10    01-3
```

4. **Use the** `showboards`**(8) command to display XSB status information.**

```
XSCF> showboards -va
XSB  R DID(LSB) Assignment  Pwr  Conn Conf Test    Fault    COD
---- - -------- ----------- ---- ---- ---- ------- -------- ----
00-0   02(00)   Assigned    n    n    n    Passed  Normal   n
01-0   02(07)   Assigned    n    n    n    Passed  Normal   n
01-1   SP       Available   n    n    n    Passed  Normal   n
01-2   02(09)   Assigned    n    n    n    Passed  Normal   n
01-3   02(10)   Assigned    n    n    n    Passed  Normal   n
```

5. **Use the** `moveboard`**(8) command to move an XSB.**

```
<Example> Delete XSBs and make XSB assignment to new domain.
XSCF> moveboard -c assign -d 1 1-0
XSB#01-0 will be assigned to DomainID 1 immediately. Continue?[y|n]
:y
XSCF>
```

6. **Use the** `showboards`**(8) command to display the XSB status again.**

```
XSCF> showboards -va
XSB  R DID(LSB) Assignment  Pwr  Conn Conf Test    Fault    COD
---- - -------- ----------- ---- ---- ---- ------- -------- ----
00-0   02(00)   Assigned    n    n    n    Passed  Normal   n
01-0   01(00)   Assigned    n    n    n    Passed  Normal   n
01-1   SP       Available   n    n    n    Passed  Normal   n
01-2   02(09)   Assigned    n    n    n    Passed  Normal   n
01-3   02(10)   Assigned    n    n    n    Passed  Normal   n
```

7. **Use the** `poweron`**(8) command to start up all domains.**

```
XSCF> poweron -a
DomainIDs to power on:01,02
Continue? [y|n] :y
01 :Powering on
02 :Powering on
*Note*
 This command only issues the instruction to power-on.
 The result of the instruction can be checked by the
 "showlogs power".
```

8. **Use the** `showboards`**(8) command to confirm that the XSB has been added to domain ID 1.**

```
XSCF> showboards -va
XSB  R DID(LSB) Assignment  Pwr  Conn Conf Test    Fault    COD
---- - -------- ----------- ---- ---- ---- ------- -------- ----
00-0   02(00)   Assigned    y    y    y    Passed  Normal   n
01-0   01(00)   Assigned    y    y    y    Passed  Normal   n
01-1   SP       Available   y    n    n    Passed  Normal   n
01-2   02(09)   Assigned    y    y    y    Passed  Normal   n
01-3   02(10)   Assigned    y    y    y    Passed  Normal   n
```

Note – When moving the system board to the domain by using the DR function that operates the XSB without stopping the domain, see the *Dynamic Reconfiguration User's Guide*.

2.2.14 System Board Configuration

System board configuration settings are used to specify XSB division information for a PSB and configure the memory mirror mode.

System board configuration is a function which is available on the M4000/M5000/M8000/M9000 servers. In the M3000 server, the system board has been configured by default and you cannot change the settings. However, you can refer to the system board information

Before dividing a PSB into XSBs or changing the memory mirror mode, make sure that the PSB is not assigned to any domain (system board pool state; unassign).

TABLE 2-29 lists a term used in system board configuration.

TABLE 2-29 System Board Configuration Term

Term	Description
Memory mirror mode	In this mode, a PSB has two memory units, one mirroring the other. Saving the same data in the separate memory units improves data security.

TABLE 2-30 lists the settings and the corresponding shell commands.

TABLE 2-30 System Board Configuration

Item	Description	Shell Command	Remarks
Display XSB division/ memory mirror mode information	Displays information on dividing a PSB into XSBs and memory mirror mode information.	`showfru`	
XSB division	Sets one of the following PSB type: • Divide as one unit (not divided) (Uni-XSB). • Divide as four units (Quad-XSB).	`setupfru`	
Memory mirror mode	Enables or disables the memory mirroring. • Enable (mirroring). • Disable (mirroring).		Mirroring is disabled by default. (Note 1)
Add device	The device, such as a system board, is added.	`addfru`	(Note 2)

TABLE 2-30 System Board Configuration *(Continued)*

Item	Description	Shell Command	Remarks
Delete device	The device, such as a system board, is deleted.	`deletefru`	(Note 2)
Replace device	The device, such as a system board, is replaced.	`replacefru`	(Note 2)
Diagnosis	Diagnose the system board. The specified system board must be unconfigured from the domain or the domain in which the system board is configured must be powered off.	`testsb`	

Note – (1) Memory mirroring requires twice the amount of memory domain used for operation. If the PSB is a Quad-XSB type in M8000/M9000 servers, memory mirroring cannot be used. In M4000/M5000 servers, memory mirroring can be used regardless of whether the system board is a Uni-XSB or Quad-XSB.

Note – (2) The add/delete/replace operations are done by field engineers (FEs). If a command is performed, the maintenance guidance is displayed. FEs will use the device check, select, add, and delete operations in the guidance window. For information about how to handle and operate these devices, see the *Service Manual* for your server and any manual written for FEs.

Dividing a PSB Into XSBs

- Command operation

1. **Use the** `showfru`**(8) command to display information on dividing a PSB into XSBs.**

```
XSCF> showfru -a sb
Device  Location    XSB Mode        Memory Mirror Mode
sb      00          Uni             No
sb      01          Uni             No
sb      02          Uni             No
```

2. **Use the** `setupfru`**(8) command to divide a PSB into XSBs.**

```
<Example> Specify PSB#00 for a Quad-XSB.
XSCF> setupfru -x 4 sb 00
```

3. **Use the** `showfru`**(8) command to display information on dividing a PSB into XSBs.**

```
XSCF> showfru -a sb
Device  Location    XSB Mode        Memory Mirror Mode
sb      00          Quad            No
sb      01          Uni             No
sb      02          Uni             No
```

Setting the Memory Mirror Mode for a PSB

- Command operation

1. **Use the** `showfru`**(8) command to display PSB memory mirror mode information.**

```
XSCF> showfru -a sb
Device  Location    XSB Mode        Memory Mirror Mode
sb      00          Quad            No
sb      01          Uni             No
sb      02          Uni             No
```

2. **Use the** `setupfru`**(8) command to enable memory mirror mode on a PSB.**

```
<Example> Enable Memory Mirror mode on PSB#00.
XSCF> setupfru -m y sb 00
```

3. **Use the** `showfru`**(8) command to confirm the setting of memory mirror mode.**

```
XSCF> showfru -a sb
Device  Location    XSB Mode        Memory Mirror Mode
sb      00          Quad            Yes
sb      01          Uni             No
sb      02          Uni             No
```

4. **Use the `testsb`(8) command to check the PSB, then check the results by using the `showboards`(8) command.**

```
XSCF> testsb 0
Initial diagnosis is about to start. Continue? [y|n] : y
Initial diagnosis is executing.
Initial diagnosis has completed.
XSB  Test    Fault
---- ------- --------
00-0 Passed  Normal
00-1 Passed  Normal
00-2 Passed  Normal
00-3 Passed  Normal
XSCF> showboards -va
XSB  R DID(LSB) Assignment  Pwr  Conn Conf Test     Fault    COD
---- - -------- ----------- ---- ---- ---- -------  -------- ----
00-0   SP       Unavailable n    n    n    Passed   Normal   n
00-1   SP       Unavailable n    n    n    Passed   Normal   n
00-2   SP       Unavailable n    n    n    Passed   Normal   n
00-3   SP       Unavailable n    n    n    Passed   Normal   n
01-0   SP       Unavailable n    n    n    Unknown  Normal   n
02-0   SP       Unavailable n    n    n    Unknown  Normal   n
```

2.2.15 Domain Mode Configuration

Domain mode configuration is used to specify the initial hardware diagnostic level, enables or disables break signal suppression, enables or disables host watchdog, enables or disables automatic boot and CPU operational mode for the specified domain.

You may want to suppress some functions for a domain during system operation or maintenance. For example, during system maintenance, you may not want to use automatic boot (enable automatic boot suppression), suppress a break signal from the console (enable break signal suppression), or suppress a panic during a Host watchdog reset.

In the M3000 server, CPU operational mode cannot be configured.

TABLE 2-31 lists terms used in domain mode configuration.

TABLE 2-31 Domain Mode Configuration Terms

Term	Description
Initial hardware diagnostic level	Sets a POST diagnostic level. The following levels can be set: • Maximum • Standard • None
Host watchdog	Based on communication between XSCF and a domain, the host watchdog function checks whether the domain is alive (heart beat or alive check). XSCF periodically monitors the operational status of Oracle Solaris OS, to detect the Oracle Solaris OS hang-up. When detected the Oracle Solaris OS hang-up, XSCF generates an Oracle Solaris OS panic on the relevant domain. To enable or disable host watchdog, set the configuration file of scfd driver (scfd.conf) that installed in the Oracle Solaris OS of the relevant domain. By enabling host watchdog (Alive Check function), XSCF monitors the relevant domain.
Automatic boot	The automatic boot function automatically boots the Oracle Solaris OS, such as to start a domain and sets the `auto-boot?` OpenBoot PROM variable to either true or false. If the automatic boot function is suppressed, it stops at an `ok` prompt, so that the user can start the Oracle Solaris OS in single-user mode in an Oracle Solaris OS installation, for example.
Break signal	"Break" means to forcibly interrupt data sending and restore the initial state. The signal used for this purpose is called a break signal. When a break signal is sent from a domain console, XSCF receives the signal and stops the domain at an ok prompt.
Mode switch	Switches on the operator panel. The mode switch has the following two modes: • Locked: Normal operation mode • Service: Maintenance mode.
CPU operational mode	Operational mode for CPU hardware that Oracle Solaris OS uses. The CPU operational mode includes the following two types: • SPARC64 VII enhanced mode Operates using the enhanced functions of the SPARC64 VII+ and SPARC64 VII processors. This mode is set to domains that consist only of SPARC64 VII+ and SPARC64 VII processors and when the CPU operational mode is determined automatically by Oracle Solaris OS. • SPARC64 VI compatible mode All the mounted CPUs operate with the functions equivalent to the SPARC64 VI processor. This mode can be set for a domain of any CPU configuration.

Note – When the mode switch on the operator panel is set to Service, the automatic boot and host watchdog functions are suppressed and the break signal is received, regardless of the domain mode settings.

TABLE 2-32 lists setting items and the corresponding shell commands.

TABLE 2-32 Domain Mode Configuration

Item	Description	Shell command	Remarks
Display domain mode setting information	Displays domain host ID, ethernet address (mac address), and domain mode setting information on the specified domain.	`showdomainmode`	
Initial diagnostic level (diag)	Sets the initial hardware diagnostic level for the specified domain or all domains. The following diagnostic levels are available: • Maximum (max) • Standard (min) • None (none)	`setdomainmode`	The default level is standard. If you set this with domain power on, an error will occur.
Host watchdog / Break signal suppression (secure)	Enables (on) or disables (off) host watchdog and break signal suppression for the specified domain or all domains. If Disable is specified, host watchdog is not performed and break signals are received for the domain(s).		The host watchdog is enabled and the break signal suppression is enabled by default. To apply the setting to the domain, restart the domain.
Automatic boot (autoboot)	Enables (on) or disable (off) automatic boot for the specified domain or all domains. If the function is disabled, automatic boot is not performed for the domain(s).		The function is enabled by default. To apply the setting to the domain, restart the domain.
CPU Mode (cpumode)	Specifies the setting method of the CPU operational mode for CPUs mounted in the domain. The following CPU operational mode settings are available: • auto: Automatically determines the operational mode of the CPU at domain startup. Depending on the CPU configuration in the domain, Oracle Solaris OS automatically determines, and sets, the appropriate mode, either SPARC64 VII enhanced mode or SPARC64 VI compatible mode. • compatible: Oracle Solaris OS operates in SPARC64 VI compatible mode.		The default setting is auto. If you set this with domain power on, an error will occur.

Note – The display for domain ethernet address (mac address) by the showdomainmode(8) command is supported only on M3000/M4000/M5000/M8000/M9000 servers that run certain versions of XCP firmware (beginning with XCP 1082).

The Status of the Mode Switch on Oracle Solaris OS

When you execute the prtdiag(1M) command on Oracle Solaris OS, either "LOCK" or "UNLOCK" is displayed in the output as the status of the mode switch of the operator panel. The output varies depending on the combination of the value of the secure variable, which is set on each domain by using the setdomainmode(8) command and the key position of the mode switch on the operator panel.

TABLE 2-33 shows the status of the mode switch displayed in the prtdiag (1M) command output which depends on the value of secure variable and the key position of the mode switch on the operator panel.

TABLE 2-33 Value of Secure Variable and Status of Mode Switch

Value of secure variable set by setdomainmode**(8)**	**Key position of mode switch**	**Status of mode switch in the** prtdig**(1M) output**
on	Service	UNLOCK
off		UNLOCK
on	Locked	LOCK
off		UNLOCK

For details of the setdomainmode(8) command, see the XSCF Reference Manual. For details of the prtdiag(1M) command, see the Oracle Solaris OS documentation.

SPARC64 VII+, SPARC64 VII, and SPARC64 VI Processors and CPU Operational Modes

The M4000/M5000/M8000/M9000 support system boards that contain SPARC64 VII+, SPARC64 VII, and SPARC64 VI processors, or a mix of these processor types. The M3000 servers support only SPARC64 VII+ or SPARC64 VII processors.

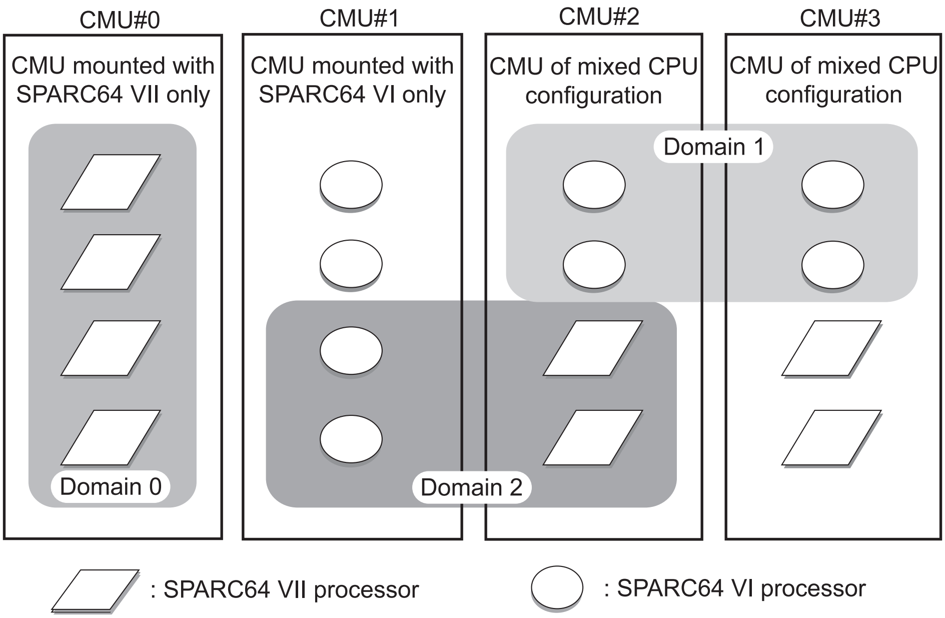
This section applies only to M4000/M5000/M8000/M9000 servers that run or will run SPARC64 VII+ or SPARC64 VII processors. On the M3000 server, only SPARC64 VII+ or SPARC64 VII processor is mounted and Oracle Solaris OS operates in SPARC64 VII enhanced mode.

Note – Supported firmware releases and Oracle Solaris releases vary based on processor type. For details, see the Product Notes that apply to the XCP release running on your server and the latest version of the Product Notes (no earlier than XCP version 1100).

The first firmware to support the newer M3000 server is the XCP 1080 firmware. For specific information about minimum OS requirements, see the Product Notes for your server.

FIGURE 2-9 shows an example of a mixed configuration of SPARC64 VI and SPARC64 VII processors.

FIGURE 2-9 CPUs on CPU/Memory Board Unit (CMU) and Domain Configuration Example


CMU#0
CMU#1
CMU#2
CMU#3
CMU mounted with SPARC64 VII only
CMU mounted with SPARC64 VI only
CMU of mixed CPU configuration
CMU of mixed CPU configuration
Domain 1
Domain 0
Domain 2
: SPARC64 VII processor
: SPARC64 VI processor

Different types of processors can be mounted on a single CMU, as shown in CMU#2 and CMU#3 in FIGURE 2-9. And a single domain can be configured with different types of processors, as shown in Domain 2 in FIGURE 2-9.

A domain runs in one of the following CPU operational modes:

- SPARC64 VI Compatible Mode (for M4000/M5000/M8000/M9000 servers only)

  All processors in the domain behave like and are treated by the Oracle Solaris OS as SPARC64 VI processors. The extended capabilities of SPARC64 VII+ and SPARC64 VII processors are not available in this mode. Domains 1 and 2 in FIGURE 2-9 correspond to this mode.

- SPARC64 VII Enhanced Mode (for M3000/M4000/M5000/M8000/M9000 servers)

  All boards in the domain must contain only SPARC64 VII+ or SPARC64 VII processors. In this mode, the server utilizes the extended capabilities of these processors. Domain 0 in FIGURE 2-9 corresponds to this mode.

To check the CPU operational mode, execute the `prtdiag`(1M) command on the Oracle Solaris OS. If the domain is in SPARC64 VII Enhanced Mode, the output will display `SPARC64-VII` on the `System Processor Mode` line. If the domain is in SPARC64 VI Compatible Mode, nothing is displayed on that line.

By default, the Oracle Solaris OS automatically sets a domain's CPU operational mode each time the domain is booted based on the types of processors it contains. It does this when the `cpumode` variable – which can be viewed or changed by using the `setdomainmode`(8) command – is set to `auto`.

You can override the above process by using the `setdomainmode`(8) command to change the `cpumode` from `auto` to `compatible`, which forces the Oracle Solaris OS to set the CPU operational mode to SPARC64 VI Compatible Mode on reboot. To do so, power off the domain, execute the `setdomainmode`(8) command to change the `cpumode` setting from `auto` to `compatible`, then reboot the domain.

TABLE 2-34 shows CPU configuration for domain at DR operations and the CPU operational mode. The system board (XSB) which can be added by DR is decided by the CPU operational mode currently set to the domain, which is as follows:

TABLE 2-34 CPU configuration for domain at DR operations and the CPU operational mode

Domain CPU configuration	Value of CPU Mode	Current CPU operational mode	CPU configuration of a system board which can be added by DR operation
SPARC64 VII+/VII	`auto`	SPARC64 VII enhanced mode	SPARC64 VII+/VII
SPARC64 VII+/VII	`compatible`	SPARC64 VI compatible mode	Any CPU configuration
SPARC64 VII+/VII and SPARC64 VI	`auto` or `compatible`	SPARC64 VI compatible mode	Any CPU configuration
SPARC64 VI	`auto` or `compatible`	SPARC64 VI compatible mode	Any CPU configuration

For details of the CPU operational mode and the DR operation, see the *Dynamic Reconfiguration User's Guide*.

DR operations work normally on M4000/M5000/M8000/M9000 server domains running in SPARC64 VI Compatible Mode. You can use DR to add, delete or move boards with any of the processor types, which are all treated as if they are SPARC64 VI processors. The M3000 servers do not support DR operations.

DR also operates normally on domains running in SPARC64 VII Enhanced Mode, with one exception: You cannot use DR to add or move into the domain a system board that contains any SPARC64 VI processors. To add a SPARC64 VI processor you must power off the domain, change it to SPARC64 VI Compatible Mode, then reboot the domain.

In an exception to the above rule, you can use the DR `addboard`(8) command with its `-c reserve` or `-c assign` option to reserve or register a board with one or more SPARC64 VI processors in a domain running in SPARC64 VII Enhanced Mode. The next time the domain is powered off then rebooted, it comes up running in SPARC64 VI Compatible Mode and can accept the reserved or registered board.

Note – Change the `cpumode` from `auto` to `compatible` for any domain that has or is expected to have SPARC64 VI processors. If you leave the domain in `auto` mode and all the SPARC64 VI processors later fail, the Oracle Solaris OS will see only the SPARC64 VII+ and SPARC64 VII processors – because the failed SPARC64 VI processors will have been degraded –and it will reboot the domain in SPARC64 VII Enhanced Mode. You will be able to use DR to delete the bad SPARC64 VI boards so you can remove them. But you will not be able to use DR to add replacement or repaired SPARC64 VI boards until you change the domain from SPARC64 VII Enhanced Mode to SPARC64 VI Compatible mode, which requires a reboot.

Setting `cpumode` to `compatible` in advance enables you to avoid possible failure of a later DR add operation and one or more reboots.

Changing the Initial Hardware Diagnostic Level

- Command operation

1. Use the `showdomainmode`**(8) command to display the initial hardware diagnostic level.**

```
<Example> Display the initial hardware diagnostic levels of domain
ID 0.
XSCF> showdomainmode -d 0 -v
Host-ID                :0f010f10
Diagnostic Level       :min
Secure Mode            :off
Autoboot               :on
CPU Mode               :auto
Ethernet Address       :00:0b:5d:e2:01:0c
```

Note – The `-v` option and the display for ethernet address is supported in XCP1082 or later.

---

2. **Use the** `setdomainmode`**(8) command to change the initial hardware diagnostic level.**

```
<Example> Specify the maximum initial hardware diagnostic level for domain ID 0.
XSCF> setdomainmode -d 0 -m diag=max
Diagnostic Level    :min      -> max
Secure Mode         :off      -> -
Autoboot            :on       -> -
CPU Mode            :auto     -> -
The specified modes will be changed.
Continue? [y|n]:y
configured.
Diagnostic Level    :max
Secure Mode         :off (host watchdog: unavailable  Break-signal:receive)
Autoboot            :on (autoboot:on)
CPU Mode            :auto
```

3. **Use the** `showdomainmode`**(8) command to confirm the initial hardware diagnostic level.**

```
<Example> Display the initial hardware diagnostic levels of domain
ID 0.
XSCF> showdomainmode -d 0
Host-ID             :0f010f10
Diagnostic Level    :max
Secure Mode         :off
Autoboot            :on
CPU Mode            :auto
```

Enabling or Disabling the Host Watchdog Function and the Break Signal Suppression

- Command operation

1. **Use the** `showdomainmode`**(8) command to display the host watchdog and break signal suppression setting.**

```
<Example> Display the setting for domain ID 0.
XSCF> showdomainmode -d 0
Host-ID             :0f010f10
Diagnostic Level    :max
Secure Mode         :off
Autoboot            :on
CPU Mode            :auto
```

2. **Use the** setdomainmode**(8) command to specify host watchdog and break signal suppression.**

```
<Example> Enable Host watchdog and Break signal suppression for domain ID 0.
XSCF> setdomainmode -d 0 -m secure=on
Diagnostic Level    :max     -> -
Secure Mode         :off     -> on
Autoboot            :on      -> -
CPU Mode            :auto    -> -
The specified modes will be changed.
Continue? [y|n]:y
configured.
Diagnostic Level    :max
Secure Mode         :on (host watchdog: available  Break-signal:non-receive)
Autoboot            :on (autoboot:on)
CPU Mode            :auto
```

3. **Use the** showdomainmode**(8) command to confirm the secure mode is on. Also, to apply the setting to the domain, restart the domain.**

Enabling or Disabling the Automatic Boot Function

- Command operation

1. **Use the** showdomainmode**(8) command to specify automatic boot.**

```
XSCF> showdomainmode -d 0
Host-ID                 :0f010f10
Diagnostic Level        :max
Secure Mode             :on
Autoboot                :on
CPU Mode                :auto
```

2. **Use the** `setdomainmode`**(8) command to disable automatic boot.**

```
<Example> Disable automatic boot for domain ID 0.
XSCF> setdomainmode -d 0 -m autoboot=off
Diagnostic Level    :max        -> -
Secure Mode         :on         -> -
Autoboot            :on         -> off
CPU Mode            :auto       -> -
The specified modes will be changed.
Continue? [y|n]:y
configured.
Diagnostic Level    :max
Secure Mode         :on (host watchdog: available  Break-signal:non-receive)
Autoboot            :off (autoboot:off)
CPU Mode            :auto
```

3. **Use the** `showdomainmode`**(8) command to confirm that autoboot is off. Also, to apply the setting to the domain, restart the domain.**

Specifying the CPU Operational Mode

Note – In the M3000 server, CPU operational mode cannot be configured.

- Command operation

1. **Power off the domain.**

2. **Use the** `showdomainmode`**(8) command to specify the CPU operational mode.**

```
XSCF> showdomainmode -d 0
Host-ID                :0f010f10
Diagnostic Level       :max
Secure Mode            :on
Autoboot               :on
CPU Mode               :auto
```

3. **Use the** `setdomainmode`**(8) command to set the CPU operational mode.**

```
<Example> Specify SPARC64 VI compatible mode for CPU operational mode of domain
ID 0.
XSCF> setdomainmode -d 0 -m cpumode=compatible
Diagnostic Level    :max        -> -
Secure Mode         :on         -> -
Autoboot            :on         -> -
CPU Mode            :auto       -> compatible
The specified modes will be changed.
Continue? [y|n]:y
configured.
Diagnostic Level    :max
Secure Mode         :on (host watchdog: available  Break-signal:non-receive)
Autoboot            :on (autoboot:on)
CPU Mode            :compatible
```

4. **Use the** `showdomainmode`**(8) command to confirm that the CPU Mode is compatible.**

Note – Restart the domain to apply the settings to the domain. You may set the initial diagnostic level, enable or disable the host watchdog function, break signal, automatic boot, and CPU operational mode.

2.2.16 Locale Administration

Locale administration is used to set the XSCF Shell default locale.

TABLE 2-35 lists setting items and the corresponding shell commands.

TABLE 2-35 Locale Administration

Item	Description	Shell Command	Remarks
Display locale	Displays the locale of XSCF Shell.	`showlocale`	
Locale	Specify the following a default locale: • English • Japanese (UTF8)	`setlocale`	

Setting Locale

- Command operation

1. **Use the** `showlocale`**(8) command to check the current locale information.**

```
<Example 1> Japanese locale
XSCF> showlocale
ja_JP.UTF-8

<Example 2> English locale
XSCF> showlocale
C
```

2. **Use the** `setlocale`**(8) command to set a locale.**

```
<Example 1> Specify a Japanese locale
XSCF> setlocale -s ja_JP.UTF-8

<Example 2> Specify a English locale
XSCF> setlocale -s C
```

The locale setting becomes effective at the next login.

2.2.17 Altitude Administration

This section explains the altitude settings. The server changes the system monitoring due to the altitude of the server. Therefore, the operator must set the altitude during the initial system setting. This setting is done by FEs.

With the altitude setting, the fan speed level varies by the environmental temperature. To display the fan speed level for each environmental temperature, execute the `showenvironment`(8) command. For the fan speed level corresponding to the altitude and the environmental temperature, see Section 4.1.1, "Displaying System Information" on page 4-2.

TABLE 2-36 lists setting items and the corresponding shell commands.

TABLE 2-36 Altitude Administration

Item	Description	Shell Command	Remarks
Display settings	Display the altitude settings for the server.	`showaltitude`	
Altitude	Specify the location altitude of the server: A set unit is specified in increments of 100 meters. The setting of less than 100 meters is rounded up.	`setaltitude`	A negative altitude cannot be set.

Setting Altitude

- Command operation

1. **Use the `showaltitude`(8) command to check the current altitude settings.**

```
XSCF> showaltitude
1000m
```

2. **Use the `setaltitude`(8) command to set the altitude settings.**

```
<Example 1> Specify an altitude of 1000 meters
XSCF> setaltitude -s altitude=1000
1000m

<Example 2> Specify an altitude of 200 meters
XSCF> setaltitude -s altitude=200
200m
```

Note – To apply the specified configuration, execute the `rebootxscf`(8) command and reset XSCF.

2.2.18 DVD Drive/Tape Drive Unit Administration

DVD drive/tape drive unit configuration is used to specify a DVD drive unit and tape drive unit by specifying a PCI card port that can connect to the DVD/tape drive.

Note – A DVD drive unit and tape drive unit needs to be specified only for M8000/M9000 servers. In an M3000/M4000 server, the MBU#0 on a MBU_A has the DVD drive unit. In an M5000 server, the MBU#0 on a MBU_B has the DVD drive unit.

TABLE 2-37 lists terms used in DVD drive/tape drive unit administration.

TABLE 2-37 DVD Drive/Tape Drive Unit Administration Terms

Term	Description
DVD drive unit	DVD: digital video disk drive unit. A basic cabinet and an expansion cabinet contain one DVD drive unit respectively, which is accessed through I/O unit card A (IOUA) mounted in an I/O unit. The DVD drive unit is connected to a specified I/O unit and is used to a single domain that use the I/O unit. In the M8000/M9000 servers, the DVD drive unit can be assigned to the specified IOUA port. In the M3000/M4000/M5000 servers, the DVD drive is assigned to a specific system board, but the port cannot be specified.
Tape drive unit	A basic cabinet and an expansion cabinet contain one tape drive unit respectively, which is accessed through IOU card A (IOUA) mounted in an I/O unit. The tape drive unit is connected to a specified I/O unit and is assigned to a single domain that uses the I/O unit. In the M8000/M9000 servers, the tape drive unit can be assigned to the specified IOUA port. In the M3000/M4000/M5000 servers, the tape drive unit is assigned to a specific system board, but the port cannot be specified.

Note – The DVD drive/tape drive unit cannot be used to back up XSCF information.

TABLE 2-38 lists the settings and the corresponding shell commands.

TABLE 2-38 DVD Drive/Tape Drive Unit Configuration

Item	Description	Shell Command	Remarks
Display DVD drive/tape drive unit setting information	Displays the DVD drive/tape drive unit setting information for an IOUA port.	`cfgdevice`	
DVD drive/tape drive unit	Sets the target IOUA port for connecting or disconnecting DVD drive and tape drive units. (Note) Specify the following: • Connect/disconnect • IOUA port number (I/O unit number - IOUA number) I/O unit number: 0-7; basic cabinet 8-15; expansion cabinet	`cfgdevice`	In the system with expansion cabinet, the IOUA port number is specified one per cabinet.

Note – After the drive units are used for a domain (even if domain configuration is changed and CPU/Memory Board unit or the I/O unit is replaced) the settings of the IOUA port number are valid.

Changing the DVD Drive/Tape Drive Unit Settings

- Command operation

1. **Use the** `cfgdevice`**(8) command to display DVD drive/tape drive unit settings.**

```
<Example> Display DVD drive/tape drive unit setting information.
XSCF> cfgdevice -l
Current connection for DVD/DAT:
      Main chassis:      port 0-2
      Expansion chassis: port 8-0
Expander status
Port No. IOU/SAS-status SAS-status
------------------------------------------------------
0-0      enable up      enable up
0-2      disable down     enable up
0-4      disable down     enable up
0-6      disable down     enable up
1-0      disable down     enable up
1-2      disable down     enable up
1-4      disable down     enable up
1-6      disable down     enable up
2-0      disable down     enable up
```

2. **Use the** `cfgdevice`**(8) command to change the DVD drive/tape drive unit settings.**

```
<Example 1> Specify the IOUA port number 0-0 for connecting.
XSCF> cfgdevice -c attach -p 0-0
Are you sure you want to attach the device [y|n] :y
Completed.( Reservation )

<Example 2> Specify the IOUA port number 0-0 for disconnection.
XSCF> cfgdevice -c detach -p 0-0
Are you sure you want to detach the device [y|n] :y
Completed.
```

3. **Use the** `cfgdevice`**(8) command to display DVD drive/tape drive unit settings. Confirm the enabling/disabling the specified IOUA number.**

2.3 Save and Restore XSCF Configuration Information

To save/restore the XSCF configuration information, execute the `dumpconfig`(8) and the `restoreconfig`(8) command in the XSCF Shell. When the command is executed with some options, all XSCF configuration information is saved at the specified location and is restored from the specified location.

Note – The saving and restoring functions of the XSCF configuration by XSCF Shell command are supported only on M3000/M4000/M5000/M8000/M9000 servers that run certain versions of XCP firmware (beginning with XCP 1080). For specific information about these minimum firmware requirements, see the latest version of the Product Notes (no earlier than the XCP 1080 edition) for your server.

The XSCF configuration information can be saved in the device and can be restored using one of the following two methods.

- The configuration information can be saved and restored when a USB device has been connected to the USB connector mounted on the XSCF Unit front panel of the M4000/M5000/M8000/M9000 servers or rear panel of the M3000 server.
- The configuration data is transmitted through the network with an encryption protocol.

Saving and Restoring Notes

- The USB device should only be formatted using the FAT32 file system. Please ask authorized service personnel about the USB capacity and the handling of USB devices.
- You can restore the configuration information only to a system of the same model as where the information was saved. For instance, the configuration information saved in the M4000 server can be restored only to another M4000 server. The consistency of a current system configuration file and a restored file are checked when data is restored. When it is consistent with the configuration files, such as version, system name, the data can be restored. In addition, the version of configuration files doesn't depend on XCP version. Even if the XCP versions is the same when data is saved and restored, the versions of each configuration file might be different.
- In the M8000/M9000 server, the configuration information can be saved from either an Active or Standby XSCF Unit. However, restoring can be done only to an Active XSCF Unit.

- The dumpconfig(8) command can encrypt saved data by specifying an option. You can safely restore the encrypted data by performing the restoreconfig(8) command, then input the specified key when saving.
- The head of the saved configuration file contains the following identification data. The identification data can be referred to in the text.
  - User comments
  - Data version
  - Presence of encryption
  - Saved time
  - System name
  - Serial number
  - XCP version
- In the network configuration, restore the data by specifying an option.
- Power off all domains when you restore the configuration information. Moreover, after completing the command, turn the input power supply of the server off, then on.

For details of configuration file and encryption, see the man page or the *XSCF Reference Manual*.

The following is the procedure for saving configuration information.

Saving the Configuration Information by Connecting the USB Device for Exclusive Use to the Panel of the XSCF Unit

- Command operation

1. **Connect a USB device to the USB connector mounted on the XSCF Unit panel.**

2. **Perform the** dumpconfig**(8) command and specify the local USB device on the XSCF Unit for the output file (see Note).**

```
XSCF> dumpconfig file:///media/usb_msd/backup-file.txt
```

3. **When the data transfer is complete, disconnect a USB device from the USB connector.**

4. **Confirm the identification data in the head of the saved configuration file.**

Note – For details on using the dumpconfig(8) command, including how to enable encryption, see the man page or the *XSCF Reference Manual*.

Saving the Configuration Information to a Specified Target Directory Over a Network

- Command operation

1. **Perform the** `dumpconfig`**(8) command specifying the target directory.**

```
XSCF> dumpconfig ftp://server/backup/backup-sca-ff2-16.txt
:
```

2. **When the data transfer is complete, confirm the identification data in the head of the saved configuration file.**

Note – For detail of `dumpconfig`(8) command, including how to enable encryption, see the man page or the *XSCF Reference Manual*.

The form of the saved configuration file is as follows.

File name :	User specification
File format :	Text-encoded in base64 encoding

The following is the procedure for restoring configuration information.

Restoring the Configuration Information by Connecting the USB Device for Exclusive Use to the Panel of the XSCF Unit

---

Note – To view XSCF messages in the following procedure, connect a serial connection terminal to the XSCF Unit.

- Command operation

1. **Power off all domains.**

2. **Connect a USB device containing the saved configuration file to the USB connector mounted on the XSCF Unit panel.**

3. **Perform the `restoreconfig`(8) command and specify the local USB device on the XSCF Unit for the input file.**

```
XSCF> restoreconfig file:///media/usb_msd/backup-file.txt
Configuration backup created on Tue Jul 19 17:04:48 2011
 :
*** You will need to power-cycle the entire system after this
operation is completed
*** Do you want to restore this configuration to your system? [y|n]:
```

4. **The message includes the identification data. Verify that the correct desired configuration file was selected and answer yes to continue.**

5. **The XSCF will be reset. After about 10 minutes, the data is restored and the XSCF halts. When the restoration is complete, disconnect the USB device from the USB connector.**

Note – If a serial terminal is connected to the XSCF Unit, you should see the message, "XSCF BOOT STOP (recover by NFB-OFF/ON)".

---

6. **Turn the input power supply of the server off, then on.**

Note – For more about encrypted data, see the man page or the *XSCF Reference Manual* of the `restoreconfig`(8) command.

Restoring the Configuration Information from a Specified Target Directory Over a Network

---

Note – To view XSCF messages in the following procedure, connect a serial connection terminal to the XSCF Unit.

- Command operation

1. **Power off all domains.**

2. **Perform the `restoreconfig`(8) command specifying the target directory.**

```
XSCF> restoreconfig ftp://server/backup/backup-sca-ff2-16.txt
Configuration backup created on Tue Jul 19 17:04:48 2011
 :
*** You will need to power-cycle the entire system after this
operation is completed
*** Do you want to restore this configuration to your system? [y|n]:
```

3. **The message includes the identification data. Verify that the correct desired configuration file was selected and answer yes to continue.**

4. **The XSCF will be reset. After about 10 minutes, the data is restored and the XSCF halts.**

Note – If a serial terminal is connected to the XSCF Unit, you should see the message, "XSCF BOOT STOP (recover by NFB-OFF/ON)".

---

5. **Turn the input power supply of the server off, then on.**

Note – For more about encrypted data, see the man page or the *XSCF Reference Manual* of the `restoreconfig`(8) command.

CHAPTER 3

Connecting to the XSCF and the Server

This chapter describes how to connect consoles and terminals to XSCF in order to use the software, and how to connect to the server.

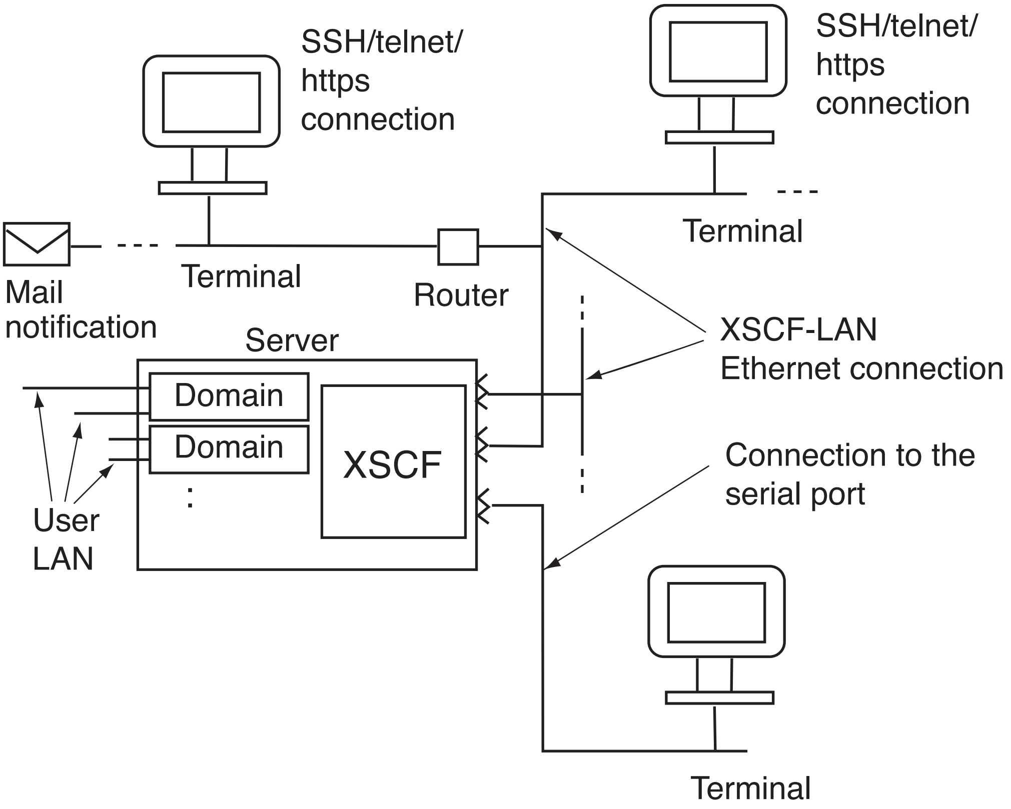
3.1 Connect Terminals to the XSCF

XSCF monitors and controls the server. You can use a terminal to interface with XSCF by connecting to the LAN or serial port of the XSCF Unit. This section describes the modes for connecting terminals and the methods of establishing a connection to XSCF from a remote console. For the initial settings for connection to XSCF, see Chapter 2.

3.1.1 Terminal Operating Modes for Connection to XSCF

The FIGURE 3-1 shows the terminal operating modes for connecting to XSCF.

FIGURE 3-1 Operating Modes for Connection to XSCF (In Midrange Servers)


SSH/telnet/ https connection
SSH/telnet/ https connection
Terminal
Mail notification
Terminal
Router
Server
XSCF-LAN Ethernet connection
Domain
Domain
XSCF
Connection to the serial port
User LAN
Terminal

Note – In a system that has one XSCF Unit (M3000/M4000/M5000 servers), the number of XSCF-LAN ports is two, and the number of serial ports is one. In systems with two XSCF Units (M8000/M9000 servers), the number of actual XSCF-LAN and serial ports is twice that of the system with one XSCF Unit.

3.1.2 Port and Terminal Types Connected to the XSCF

As shown in FIGURE 3-1, two types of ports, serial and Ethernet, can be used for connecting to the XSCF and the XSCF terminal.

Serial

The XSCF Shell and domain console (OS console) can be used while a terminal is connected to a serial port.

Ethernet

The XSCF Shell and domain console can be used with SSH or telnet at a terminal using an Ethernet (referred to as XSCF-LAN, in this document) connection. Also, the XSCF Web can be used, with the appropriate browser settings. Other functions which rely on XSCF-LAN (Ethernet) connectivity are the mail notification function, the SNMP function, the log archiving function, the remote maintenance service function, time synchronization with an external NTP server, and user authentication with an LDAP server.

Connect cables to the appropriate connectors, log in to XSCF from the XSCF terminal, and then perform the `console`(8) command. After that, you can use the domain console (see Note below). You can return to the XSCF Shell console by pressing the "#" (default escape character) and "." (period) keys while holding down the Enter key. The XSCF functions do not vary according to the port type.

Note that the XSCF Web cannot be used on PCs and workstations that are connected via serial port.

Note – The function used to switch from the XSCF Shell to the domain console by a command is called the XSCF console redirection function. In the server, each system board is serially and directly connected to the XSCF Unit (multipath configuration). When the user performs the `console`(8) command, XSCF automatically selects a path to the valid domain.

TABLE 3-1 lists the types of terminals connected to each port shown in FIGURE 3-1 and corresponding port numbers.

TABLE 3-1 Types of Terminals Connected With XSCF

Port	Terminal Type	Port Number, Cable
XSCF-LAN port (2 ports per XSCF Unit) [10/100 Mbps]	XSCF Shell terminal • You can use the XSCF Shell with SSH or telnet connection. • Either of the two XSCF-LAN ports can be used concurrently by more than one user. (Note 1) • Switching to the domain console is enabled by the console(8) command. For details on changing these default keys, see the description on the console(8) command. • After login, if the XSCF Shell is not used for a certain period, the user is forcibly logged out. For details on setting XSCF session timeout, see the description on the setautologout(8) command. • To return to the shell window from the domain console, press the "#" (default escape character) and "." (period) while holding down the Enter key. For details on changing these default keys, see the description on the console(8) command.	SSH: 22 telnet: 23 A LAN cable is required.
	Domain console (RW console) (Note 2) • OS console enabled for input and output. The RW console is enabled by specifying a write-enabled console in the console(8) command from the shell terminal. • In one domain, only one user (one connection) at a time can use the RW console. • When you return to XSCF Shell console without logging out from the domain, the return causes automatically logging out from the domain. At this time, a background program is forced to quit. To avoid the background program force-quit, return to XSCF Shell console with logging out from the domain. • For detailed instructions on setting the session timeout value for domain console, see the Oracle Solaris OS manual.	
	Domain console (RO console) • OS console used for display only. The RO console is enabled by specifying a reference-only console in the console(8) command from the shell terminal.	
	XSCF Web • The XSCF Web can be used by specifying a URL in a browser.	https: 443 A LAN cable is required.

TABLE 3-1 Types of Terminals Connected With XSCF *(Continued)*

Port	Terminal Type	Port Number, Cable
Serial port (One per XSCF Unit)	XSCF Shell terminal • The XSCF Shell can be used immediately following connection to a serial port. • As with that of the XSCF-LAN port, a screen transition to the domain console is possible. • As with that of the XSCF-LAN port, after login, if the XSCF Shell is not used for a certain period, the user is forcibly logged out. Domain console (RW console) • This console is similar to that of the XSCF-LAN port. Domain console (RO console) • This console is similar to that of the XSCF-LAN port.	A RS-232C serial crosscable is required. If only a LAN cable is available, a 9-pin conversion cable is required on the PC side.

Note – A maximum of 20 users can be connected to the XSCF at the same time in the M3000/M4000/M5000 servers. If 20 users are already connected to the XSCF, access from the 21st (20 +1) user attempting to establish a connection is denied. In the M8000/M9000 servers, there is a maximum of 100 users.

Note – In one domain, only one user can use the RW console. While one user is using the RW console, another user cannot start another RW console in the same domain. A maximum of 20 consoles can be connected to RW console and RO console at the same time on the M3000/M4000/M5000 servers.
(Ex. M4000/M5000 servers; domain ID 0 <RW x 1, RO x 17>, domain ID 1 <RW x 1,RO x 1>).
In the M8000/M9000 servers, max is 100 consoles.

3.1.3 About the XSCF-LAN/the DSCP Link Port Number and the Function and the Firewall

TABLE 3-2 lists the port numbers used for the XSCF-LAN ports and XSCF functions. To defend from attacks against XSCF and prevent unauthorized access to XSCF, a firewall must be installed for connections to external networks. When the firewall has been installed, each XSCF-LAN port must be permitted to pass packets as necessary.

TABLE 3-2 XSCF-LAN Port Numbers and Connection Directions for Functions

Port Number / Protocol	Function	Connection Direction
22/TCP	XSCF Shell (SSH)	External network -> XSCF
22/TCP	Log archiving, firmware update and data collector (snapshot)	XSCF -> External network
23/TCP	XSCF Shell (telnet)	External network -> XSCF
25/TCP	Mail notification and remote maintenance service	XSCF -> external network
53/TCP 53/UDP	DNS	XSCF -> external network
110/TCP	Authentication with a POP server	XSCF -> external network
123/UDP	Time synchronization using NTP (when an external server is used)	XSCF -> external network
161/UDP	SNMP function	External network -> XSCF
162/UDP	SNMP Trap function	XSCF -> External network
636/TCP	Authentication with an LDAP server	XSCF -> external network
443/TCP	XSCF Web (https)	External network -> XSCF

TABLE 3-3 lists the port numbers used for the DSCP Link and the functions. When you want to strengthen security of domain side, the following each port must be permitted to pass packets as necessary.

TABLE 3-3 DSCP Link Port Numbers and Connection Directions for Functions

Port Number / Protocol	Function	Connection Direction
12/TCP	FMA event translation	XSCF -> Domain
22/TCP	SSH	Domain -> XSCF
24/TCP	FMA event translation	XSCF -> Domain
665/TCP	DR control	XSCF -> Domain
123/UDP	Time synchronization	Domain -> XSCF

3.1.4 Connecting to XSCF via the Serial Port

The following is the procedure for connecting to a terminal to XSCF via the serial port.

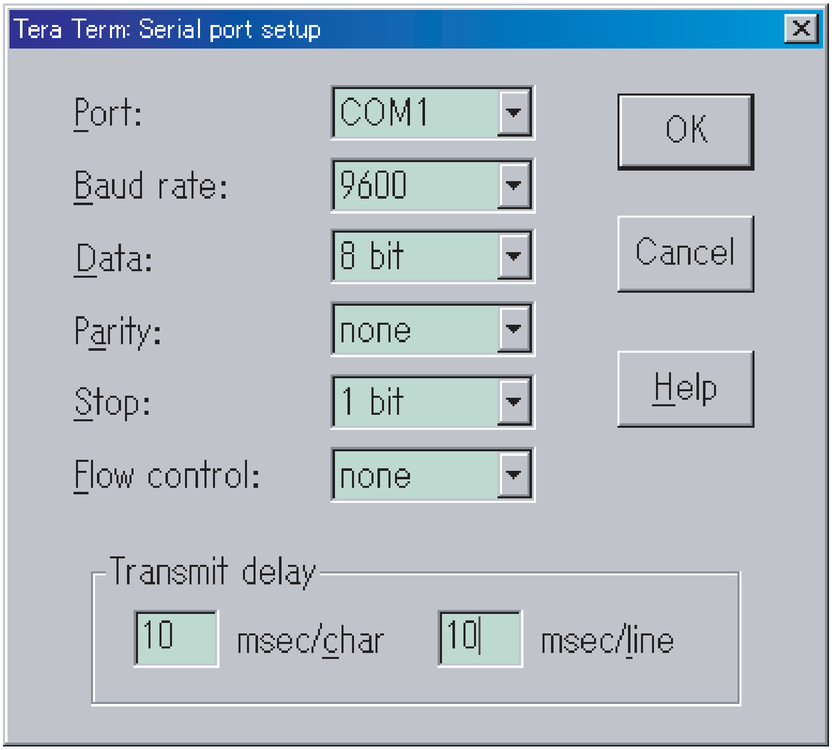
1. **Confirm that a serial cable is inserted into the serial connector on the front of the XSCF Unit, and confirm that the PC and workstation to be used are correctly connected.**

2. **Check whether the following are set on the terminal software.**

```
Baud rate: 9600 bps, Data length: 8 bit, No parity, STOP bit: 1 bit,
No flow control, Delay: Except for 0
```

FIGURE 3-2 shows an example with settings.

FIGURE 3-2 Example of Terminal Software Settings



Tera Term: Serial port setup

Port: COM1

Baud rate: 9600

Data: 8 bit

Parity: none

Stop: 1 bit

Flow control: none

Transmit delay

10 msec/char 10 msec/line

Note – Please increase the delay, when you cannot connect.

---

3. **On the PC or workstation to be used, use one of the following procedures:**

- Connecting the XSCF Shell terminal

   a. **Establish a connection via the serial port to use the XSCF Shell terminal.**

   b. **Enter a user account and password to login to the XSCF Shell.**

   c. **Confirm that the XSCF Shell prompt (XSCF>) is displayed.**

   d. **The XSCF Shell can now be used.**

- Connecting the domain console (OS console)

   a. **If the domain is powered off, use the** `poweron`**(8) command for the domain on the XSCF Shell terminal and turn it on to start the Oracle Solaris OS.**

   b. **Follow** Step a **to** Step c **in the above "**Connecting the XSCF Shell terminal**."**

   c. **Perform the** `console`**(8) command.**

   d. **Confirm the change into the specified domain console.**

3.1.5 Connecting to XSCF Using SSH via the LAN Port

The procedure described below assumes that SSH is enabled in the SSH/telnet settings of XSCF, as described in Chapter 2. For details on cable connections between the server and a LAN and the connection between a PC and workstation, see the *Installation Guide* for your server.

The following is the procedure for connecting to XSCF using SSH via the XSCF-LAN port.

1. **Confirm that a LAN cable is inserted into the XSCF-LAN port connector on the front of the XSCF Unit, or confirm that the PC and workstation to be used are correctly connected.**

2. **On the PC or workstation to be used, use one of the following procedures:**

   - Connecting the XSCF Shell terminal

   a. **To establish an SSH connection, start an SSH client and specify the IP address of XSCF. In the systems with redundant XSCF Units, specify the IP address of active XSCF.**

   b. **Enter a user account and password to login to the XSCF Shell.**

   c. **Confirm that the XSCF Shell prompt (XSCF>) is displayed.**

   The XSCF Shell can now be used.

Note – To start up the SSH client, see your SSH manual. For details on login, see Chapter 5.

- Connecting the domain console (OS console)

a. **If the domain is powered off, use the `poweron`(8) command for the domain on the XSCF Shell terminal and turn it on to start the Oracle Solaris OS.**

b. **Follow Step a to Step c in the above "Connecting the XSCF Shell terminal."**

c. **Perform the `console`(8) command.**

d. **Confirm the change into the specified domain console.**

Note – In this system, you can use SSH to access from domain to XSCF via DSCP. And you can use the `setssh`(8) command to disable the SSH access from domain to XSCF. For details on the SSH access control via DSCP, see Section 2.2.7, "SSH/Telnet Administration" on page 2-104.

3.1.6 Connecting to XSCF Using Telnet via the LAN Port

The procedure described below assumes that telnet is enabled in the SSH/telnet settings of XSCF, as described in Chapter 2. For details on cable connections between the server and a LAN and the connection between a PC and workstation, see the *Installation Guide* for your server.

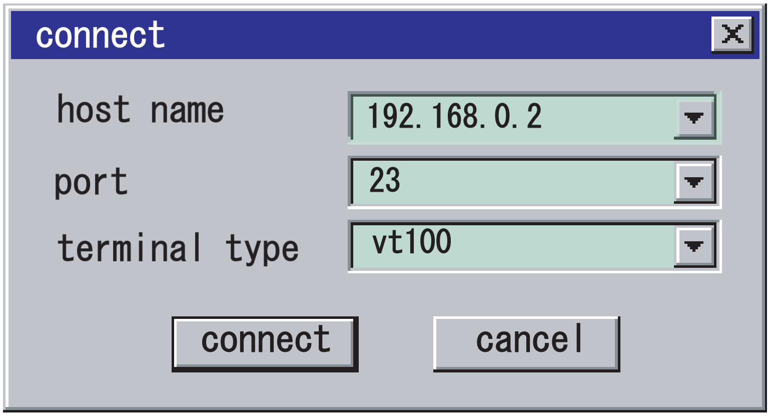
The following is the procedure for connecting to a terminal using telnet via the XSCF-LAN port.

1. **Confirm that the LAN cable is inserted into the XSCF-LAN port connector on the front of the XSCF Unit, or confirm that the PC and workstation to be used are correctly connected.**

2. **On the PC or workstation to be used, use one of the following procedures:**

   - Connecting the XSCF Shell terminal

FIGURE 3-3 Example of Starting the Terminal Emulator



host name: 192.168.0.2

port: 23

terminal type: vt100

a. **To establish a telnet connection, activate the terminal emulator and specify the IP address of XSCF and port number 23. In the systems with redundant XSCF Units, specify the IP address of active XSCF.**

b. **Enter a user account and password to login to the XSCF Shell.**

c. **Confirm that the XSCF Shell prompt (XSCF>) is displayed.**

d. **The XSCF Shell can now be used.**

- Connecting the domain console (OS console)

a. **If the domain is powered off, use the `poweron`(8) command for the domain on the XSCF Shell terminal and turn it on to start the Oracle Solaris OS.**

b. **Follow Step a to Step c in the above "Connecting the XSCF Shell terminal."**

c. **Perform the `console`(8) command.**

d. **Confirm the change into the specified domain console.**

3.1.7 Switching Between the XSCF Shell and the Domain Console

With a PC or workstation connected to an XSCF-LAN port or the serial port, the XSCF Shell and domain console can be operated through one window exclusively. The following is the switching procedure:

1. **Perform the `console`(8) command on the XSCF Shell terminal screen to select the domain console.**

```
XSCF> console -d 0
```

Note – One RW console can be connected in one domain. If a user with platadm or domainadm user privilege forcibly connects a RW console, the currently connected RW console is disconnected.

---

2. **To switch from the domain console to the XSCF Shell, press the "#" (default escape character) and "." (period) keys while holding down the Enter key.**

3. **Confirm that the XSCF Shell prompt (XSCF>) is displayed in the terminal.**

4. **To set a escape character different from the default value, perform the `console`(8) command with specifying the option. It is enabled only at the current session.**

```
<Example> Change the escape character to |.
XSCF> console -d 0 -s "|"

Console contents may be logged.
Connect to DomainID 0?[y|n] :y
```

Note – For details on types of the escape character, see the man page or the *XSCF Reference Manual*.

3.2 Types of XSCF Connections

This section provides some examples of XSCF connection.

3.2.1 Connecting XSCF via the XSCF-LAN Port Or the Serial Port

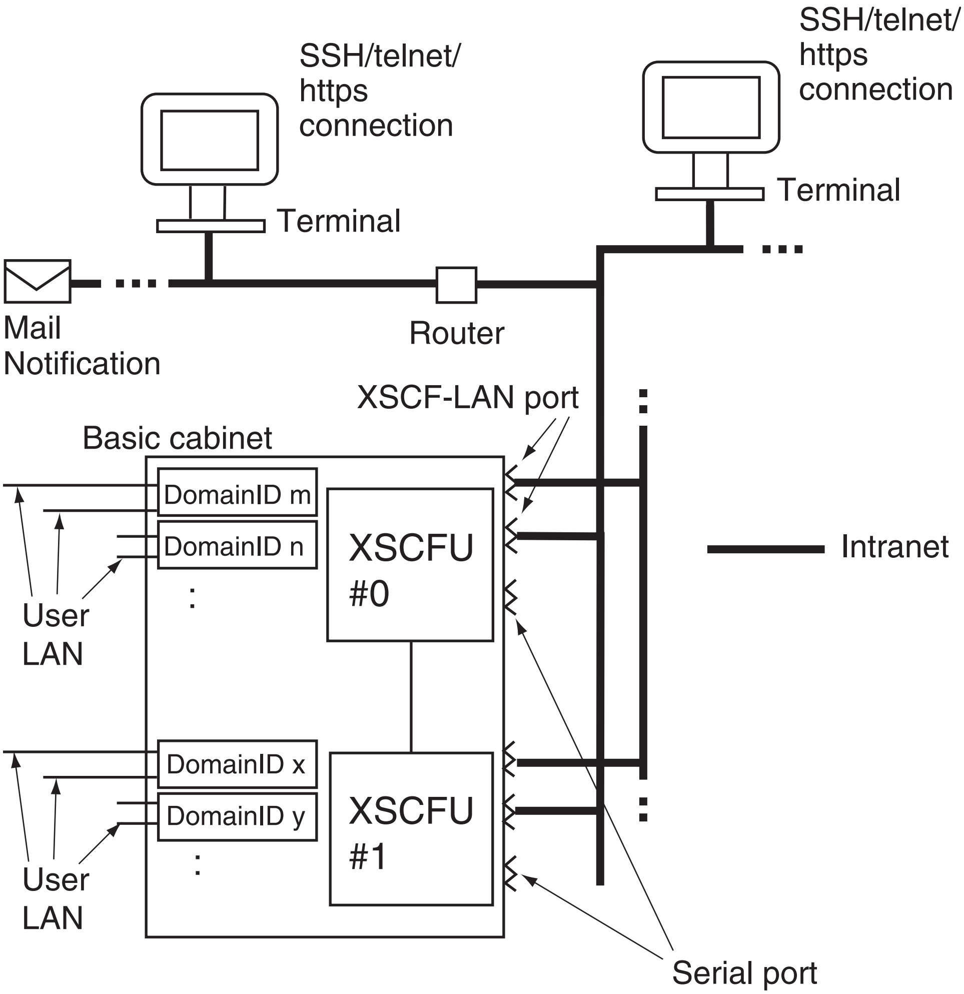
XSCF Connection via an XSCF-LAN Port (Recommended)

Establish an XSCF connection via a XSCF-LAN port. The Ethernet connection used for XSCF connection is shown in FIGURE 3-1. The XSCF connection to the LAN utilizes the functions listed below. For the summary of these functions, see Chapter 1.

- XSCF Shell
- XSCF Web
- SNMP agent function
- Mail notification function
- Time synchronization with an external NTP server
- Authentication function using an LDAP server
- Log archiving function

FIGURE 3-4 shows the intranet connection.

FIGURE 3-4 Intranet Connection (In a High-End Server)

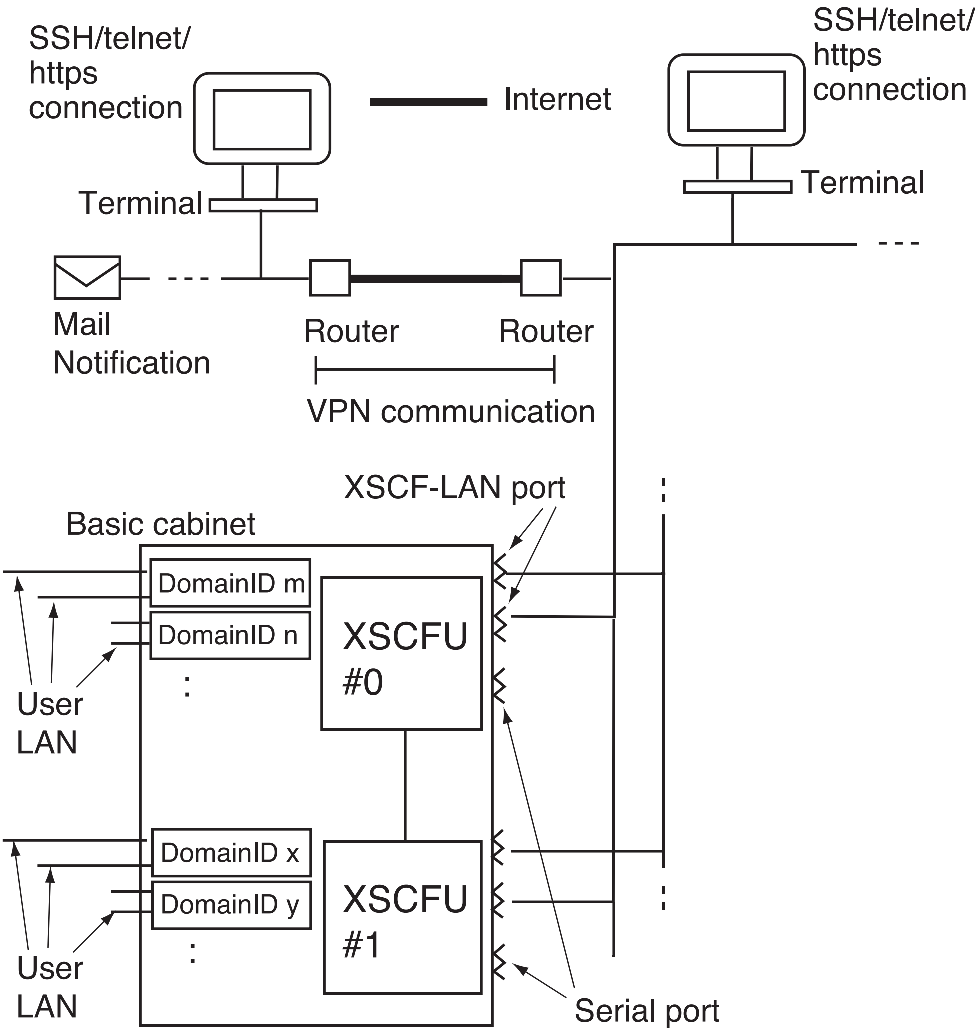


When you use the XSCF Shell, you can have high security by using SSH not telnet.

The XSCF Web uses SSL to provide authentication security.

FIGURE 3-5 shows the connection via an external network.

FIGURE 3-5 Connection of External Internet Using VPN Communication (In High-End Server)



For security reasons, using Virtual Private Network (VPN) as the external network is strongly recommended.

XSCF Connection via a Serial Port

Establish an XSCF connection via a serial port. Connect the serial port as shown in FIGURE 3-1. An XSCF connection via the serial port has the following functions and advantages:

- XSCF Shell
- Advantageous when connection to the LAN is not desirable for reasons of security
- Displaying the initial diagnostic message at the XSCF connection

XSCF Connection via XSCF-LAN and Serial Ports

Establish the XSCF connection via XSCF-LAN and serial ports. This type of connection is also shown in FIGURE 3-1. The XSCF connection via both ports has the following advantage in addition to those for the connection via the XSCF-LAN port.

- A user who connected with the serial port can safely use the XSCF Shell.

3.2.2 XSCF-LAN and Serial Connection Purposes

The XSCF Unit has one serial port and two XSCF-LAN ports with 10/100 Mbps interfaces. This section describes examples of using the XSCF-LAN ports and the serial port.

Caution – IMPORTANT - The IP address of XSCF-LAN#0 and IP address of XSCF-LAN#1 must be specified in different subnet addresses.

Using Two LAN Ports and Making the LAN Redundant

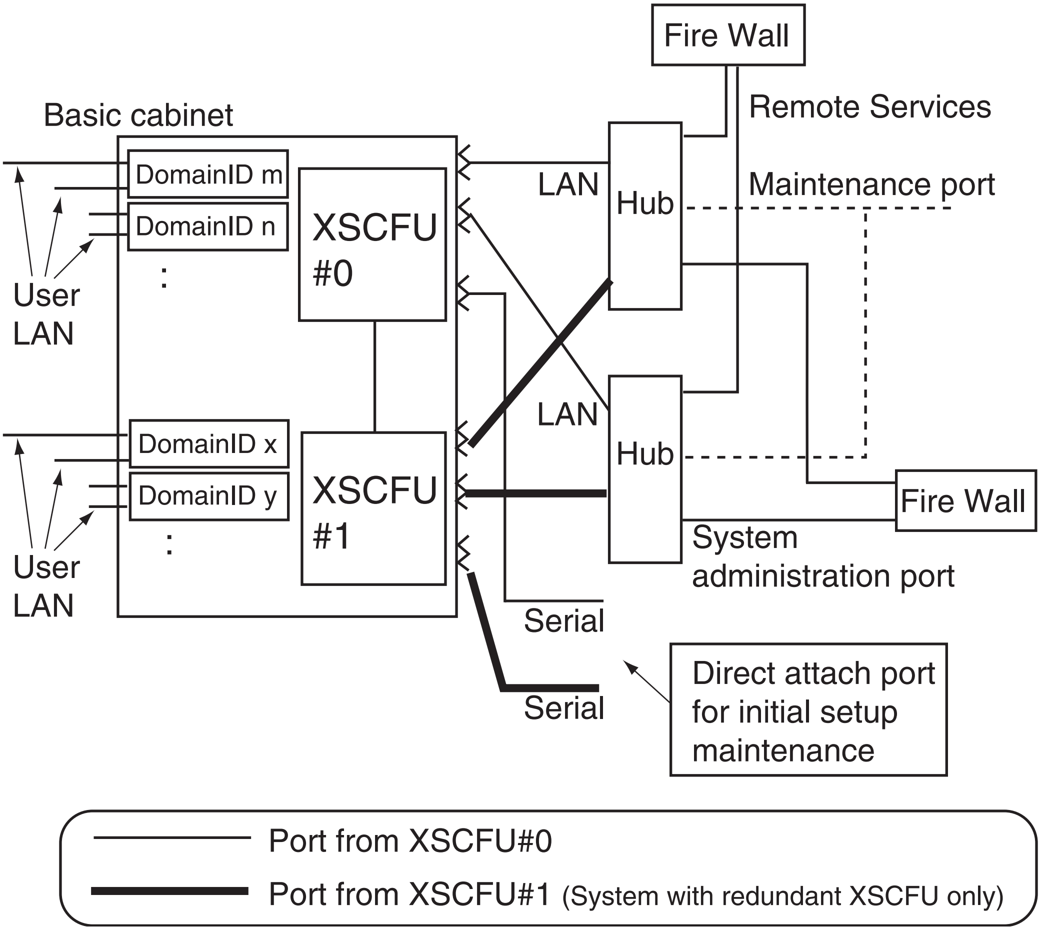
FIGURE 3-6 shows an example of a configuration where the two XSCF-LAN ports of one XSCF Unit are used for the same purpose. This configuration makes the XSCF-LAN redundant. The purpose is as follows:

- The two LANs, which are redundantly configured, are used for the system administrator
- The two LANs, which are redundantly configured, are used for the remote maintenance service.
- FE uses either of the two LANs or a maintenance terminal that is serially and directly connected.

In the example of the configuration shown in FIGURE 3-6, if errors occur in either of the two LAN ports and its switch hub, its LAN is replaced by the other LAN. Moreover, if an error occurs in the switch hub, the other LAN can be relied on for notification.

If an error occurs in the active XSCF Unit in the systems with two XSCF Units, XSCF generates a failover, then the LAN of the other XSCF Unit can be used.

FIGURE 3-6 Example of LAN Port Connections Made Redundant

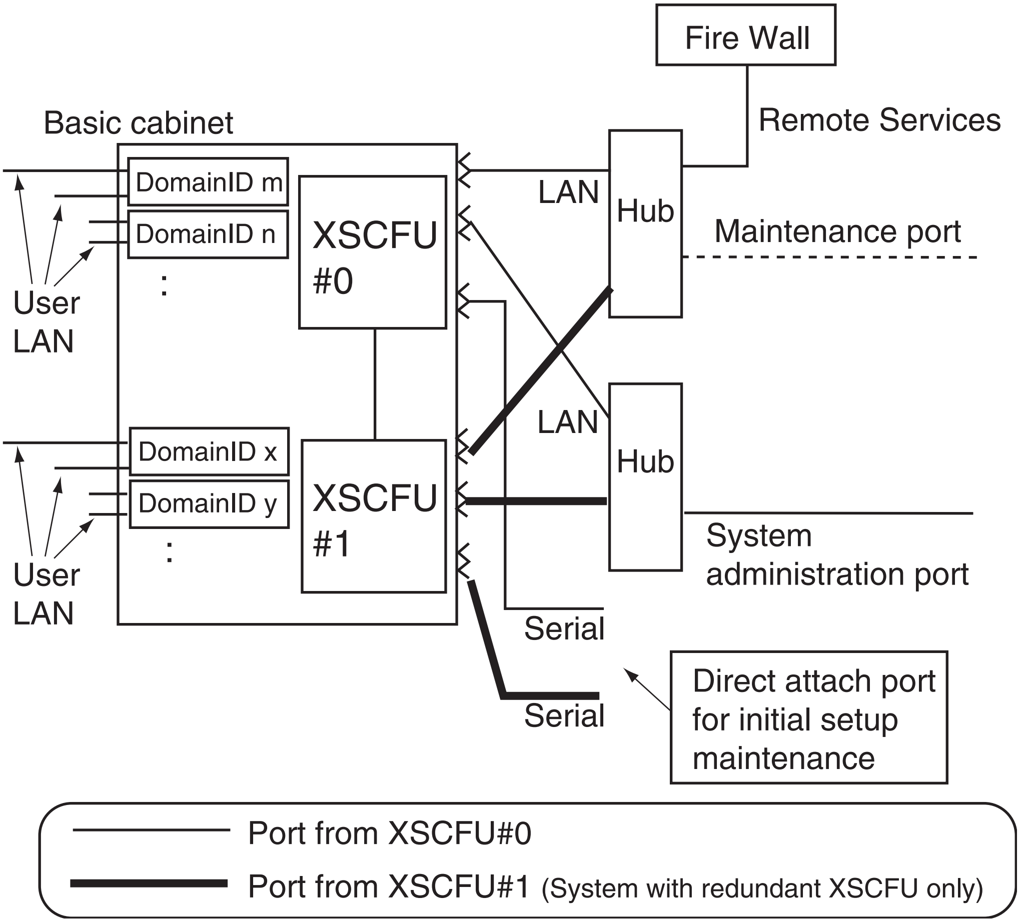


Using Two LAN Ports Selectively for Management and Maintenance

FIGURE 3-7 shows an example of a configuration where the two XSCF-LANs of one XSCF Unit are used selectively for the system administrators and the FE. This configuration does not make the XSCF-LAN redundant. The purpose is as follows:

- One LAN is used for the system administrator.
- The other LAN is used for the remote maintenance service only or by the FE.

FIGURE 3-7 Example of LAN Port Connections Not Made Redundant



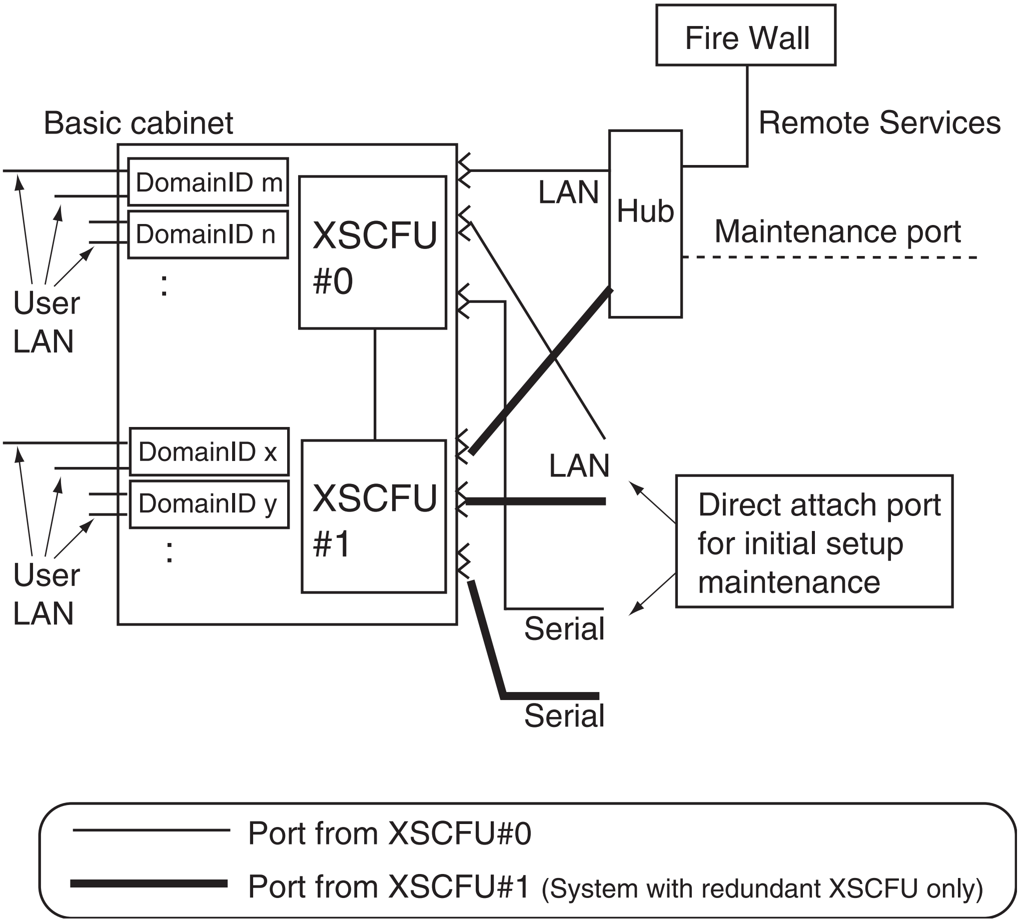
Using a Single LAN Port for Management and Remote Maintenance

FIGURE 3-8 shows an example where one XSCF-LAN port of an XSCF Unit is used as follows:

- The XSCF-LAN port is used by the system administrator.
- The same XSCF-LAN port is used for the remote maintenance service.

An FE uses either the other XSCF-LAN port with the other LAN or a maintenance terminal that is serially and directly connected.

FIGURE 3-8 Example of a Connection With One LAN Port



CHAPTER 4

Operation of the Server

This chapter mainly describes operation of the server hardware.

4.1 Display Server Hardware Environment

This section describes methods for checking the configuration and status of the server hardware during system configuration or operation.

To display the configuration and status of a server, use the XSCF Shell.

Commands Used to Display Information

Execute the following commands individually, as appropriate. For details of these commands, see Chapter 5.

- `showhardconf`
- `version`
- `showdate`
- `showenvironment`
- `showstatus`
- `cfgdevice`

4.1.1 Displaying System Information

- Command operation

1. **Use the `showhardconf(8)` command to check the mode switch status.**

```
XSCF> showhardconf
SPARC Enterprise xxxx;
     + Serial:PP20605005; Operator_Panel_Switch:Locked;
     + Power_Supply_System:Single; SCF-ID:XSCF#0;
     + System_Power:On; System_Phase:Cabinet Power On;
     Domain#0 Domain_Status:Powered Off;

     MBU_B Status:Normal; Ver:0101h; Serial:7867000282  ;
:
```

2. **Use the `showdate(8)` command to display the system time.**

```
XSCF> showdate
Thu Jul 6 14:48:01 UTC 2006
```

3. **Use the `version(8)` command to display the XCP comprehensive firmware version, XSCF version, and OpenBoot PROM version.**

```
XSCF> version -c xcp -v
XSCF#0 (Active)
XCP0 (Current): 1082
OpenBoot PROM : 02.09.0000
XSCF          : 01.08.0005
XCP1 (Reserve): 1082
OpenBoot PROM : 02.09.0000
XSCF          : 01.08.0005
XSCF#1 (Standby )
XCP0 (Current): 1082
OpenBoot PROM : 02.09.0000
XSCF          : 01.08.0005
XCP1 (Reserve): 1082
OpenBoot PROM : 02.09.0000
XSCF          : 01.08.0005
OpenBoot PROM BACKUP
#0: 02.08.0000
#1: 02.09.0000
```

(This screenshot is provided as an example.)

4. **Use the** `showstatus`**(8) command to display information on degraded components in the system.**

```
XSCF> showstatus
*   BP_A Status:Degraded;
*       DDC_A#0 Status:Faulted;
*   PSU#0 Status:Faulted;
```

(This screenshot is provided as an example.)

5. **Use the** `showenvironment`**(8) command to display the ambient temperature, humidity, and voltage of the system.**

```
XSCF> showenvironment
Temperature:30.70C
Humidity:90.00%
XSCF> showenvironment temp
Temperature:30.70C
CMU#0:43.00C
    CPUM#0-CHIP#0:65.00C
    CPUM#1-CHIP#0:61.20C
    CPUM#2-CHIP#0:64.80C
    CPUM#3-CHIP#0:63.60C
CMU#1:45.50C
:
XSCF>  showenvironment volt
MBU_B
    1.0V Power Supply Group:1.000V
    1.8V Power Supply Group:1.910V
    CPUM#0-CHIP#0
        1.0V Power Supply Group:1.050V
:
```

(This screenshot is provided as an example.)

Note – The humidity information is only displayed in M8000/M9000 servers.

Environmental Temperature and Fan Speed Level

With the altitude setting, the fan speed level varies by the environmental temperature. To display the fan speed for each environmental temperature, execute the `showenvironment`(8) command. Fan speed level indicates Low speed, Middle speed, or High speed.

The M8000/M9000 servers do not indicate Middle speed. The M3000 server indicates multi levels. In case errors detected in the fan, Full or High speed will be indicated.

TABLE 4-1, TABLE 4-2 and TABLE 4-3 list the fan speed level indicated by using the `showenvironment`(8) command, which corresponding to the altitude configured and the environmental temperature.

TABLE 4-1 Fan speed levels corresponding to altitude and environmental temperature (Entry-Level system)

Fan speed levels	Environmental temperatures by altitude			
	500 m or less	501-1000 m	1001-1500 m	1501-3000 m
Low speed (level-1)	20°C or less	18°C or less	16°C or less	14°C or less
Low speed (level-2)	19-22°C	17-20°C	15-18°C	13-16°C
Low speed (level-3)	21-24°C	19-22°C	17-20°C	15-18°C
Low speed (level-4)	23-26°C	21-24°C	19-22°C	17-20°C
Middle speed (level-5)	25-28°C	23-26°C	21-24°C	19-22°C
Middle speed (level-6)	27-30°C	25-28°C	23-26°C	21-24°C
High speed (level-7)	29-32°C	27-30°C	25-28°C	23-26°C
High speed (level-8)	31-34°C	29-32°C	27-30°C	25-28°C
High speed (level-9)	More than 33°C	More than 31°C	More than 29°C	More than 27°C

TABLE 4-2 Fan speed levels corresponding to altitude and environmental temperature (Midrange system)

Fan speed levels	Environmental temperatures by altitude			
	500 m or less	501-1000 m	1001-1500 m	1501-3000 m
Low speed	25°C or less	23°C or less	21°C or less	19°C or less
Middle speed	23-30°C	21-28°C	19-26°C	17-24°C
High speed	More than 28°C	More than 26°C	More than 24°C	More than 22°C

TABLE 4-3 Fan speed levels corresponding to altitude and environmental temperature (High-end system)

Fan speed levels	Environmental temperatures by altitude			
	500 m or less	501-1000 m	1001-1500 m	1501-3000 m
Low speed	27°C or less	25°C or less	23°C or less	21°C or less
High speed (level-9)	More than 24°C	More than 22°C	More than 20°C	More than 18°C

For the altitude setting, see Section 2.2.17, "Altitude Administration" on page 2-191

Power consumption and Exhaust air

To display power consumption and exhaust air of a server, use the power consumption monitoring function and the airflow indicator. Power consumption monitoring function and airflow indicator make it possible to routinely confirm the amount of power consumed on and airflow emitted while the server is up and running.

Note – The power consumption monitoring function is supported only on M3000 server that run certain versions of XCP firmware as below. The M4000/M5000/M8000/M9000 servers do not support the power consumption monitoring function.
- M3000 server; XCP 1081 or later
The airflow indicator is supported only on M3000/M4000/M5000/M8000/M9000 servers that run certain versions of XCP firmware as below.
- M3000 server; XCP 1082 or later
- M4000/M5000 servers; XCP1100 or later
- M8000/M9000 servers; XCP1090 or later

For specific information about these minimum software and firmware requirements, see the latest version of the Product Notes (no earlier than the XCP 1081 edition) for your server.

To display the power consumption, use the `showenvironment power` command. The results displays the maximum (`Permitted AC power consumption`) and actual (`Actual AC power consumption`) power consumption values. When the power type is DC [direct-current] power supply, "... DC power ..." is displayed. To display the amount of exhaust air, use the `showenvironment air` command. You can also obtain the data of power consumption and exhaust air using the SNMP agent function.

The following is the showenvironment examples on M3000 server:

```
XSCF> showenvironment air
Air Flow:63CMH

XSCF> showenvironment power
Permitted AC power consumption:470W
Actual AC power consumption:450W
```

Note – Power consumption and airflow values are for reference only. These values vary depending on factors such as system load.

The `showenvironment power` and `showenvironment air` commands do not include the information of External I/O Expansion Unit and peripheral I/O device. Also, the M4000/M5000/M8000/M9000 servers do not indicate power consumption by `showenvironment` command. For a power consumption value of the M4000/M5000/M8000/M9000 servers, see the *SPARC Enterprise M4000/M5000 Servers Site Planning Guide* or the *SPARC Enterprise M8000/M9000 Servers Site Planning Guide*.

For details of the `showenvironment`(8) command, see the *XSCF Reference Manual* and man page. For the installation of server, see the *Site Planning Guide* for your server.

Note – To obtain the data of exhaust air using the SNMP agent function, install the latest XSCF extension MIB definition file to the SNMP manager. For details on obtaining the XSCF extension MIB definition file, see the Product Notes for your server or download site for firmware.

Note – The amount of power consumption and exhaust air may not be indicated correctly in the MIB information, in the `showenvironment power`, `showenvironment air` commands output, and on the XSCF Web in the following cases; and you should wait for one minute and check the value again.
- During the server powering on or powering off, or for a while after the power-on or power-off complete
- During the active replacement of power supply unit, or for a while after the active replacement complete

---

4.1.2 Display Server Configuration/Status Information

- Command operation

● **Use the `showhardconf`(8) command to check the status of a device.**

```
XSCF> showhardconf
SPARC Enterprise xxxx;
     + Serial:PP20605005; Operator_Panel_Switch:Locked;
     + Power_Supply_System:Single; SCF-ID:XSCF#0;
     + System_Power:On; System_Phase:Cabinet Power On;
     Domain#0 Domain_Status:Powered Off;

     MBU_B Status:Normal; Ver:0101h; Serial:7867000282 ;
:
```

The status information of each device is as below.

- CPU/Memory board unit / Motherboard unit information

  Unit number, status, version, serial number, FRU number, memory capacity, and type.

  In the M3000 server, the displayed information is CPU status, CPU operating frequency, CPU type, number of CPU cores, and number of CPU strands.

- CPU module information

  Unit number, status, version, serial number, FRU number, CPU operating frequency, CPU type, number of CPU cores, and number of CPU strands.

- Memory information

  Unit number, status, version, serial number, FRU number, and information on each memory slot. In the M3000/M8000/M9000 servers, there is information on each memory slot.

  The displayed information on each memory slot includes the unit number, status, code, type and memory capacity.

  Note that the type field indicates the size and rank of the DIMM using a two-character code, as follows:

  i. Type 1A = 1 GB, 1 rank

  ii. Type 2A = 2 GB, 1 rank

  iii. Type 2B = 2 GB, 2 rank

  iv. Type 4A = 4 GB, 1 rank

  v. Type 4B = 4 GB, 2 rank

  vi. Type 8B = 8 GB, 2 rank

- DDC information

  Unit number, status

- I/O unit information

  Unit number, status, version, serial number, FRU number, type, and information on each PCI and DDC.

  The displayed information on each PCI includes the unit number, name property, card type, serial number, type, and FRU number.

  The displayed information on each DDC includes the unit number and status. In the M3000 server, there is information on each PCI slot.

- External I/O Expansion Unit (IOBOX) information

  Unit number, serial number and information on each I/O boat and power supply unit in an I/O expansion unit (see Note).

The displayed information on each I/O boat includes the unit number, serial number, and link information.

The displayed link information includes the version, serial number, and type.

The displayed information on each power supply unit includes the unit number and serial number.

- XSCF Unit information

  Unit number, status, version, serial number, and FRU number

- Crossbar Unit (XBU) information

  Unit number, status,version, serial number, and FRU number

- Backplane (BP) information

  Unit number, status, version, serial number, FRU number and each DDC information

  The displayed information on each DDC includes the unit number version, serial number, and FRU number.

- Clock unit information

  Unit number, status, version, serial number, and FRU number

- Operator panel information

  Unit number, status, version, serial number and FRU number

- Power supply unit information

  Unit number, status, serial number, FRU number, power status, power type, and voltage
  Note that the power type field indicates "AC", which is AC power supply or "DC", which is DC power supply.

- Fan backplane information

  Unit number, status, version, serial number, and FRU number

- Fan unit information.

  Unit number, status, serial number

Note – The configuration information might change based on model configuration in M3000/M4000/M5000/M8000/M9000 servers.

Note – The External I/O Expansion Unit may be referred to as IOBOX in example program output and the text in this manual.

Note – 8GB DIMM is supported in XCP1081 or later.
"Type" in the CPU/Memory board unit information is supported in XCP1090 or later on M8000/M9000 servers.
"Type" in the Motherboard unit information is supported in XCP1100 or later on M4000/M5000 servers.
"Type" in the I/O unit information is supported in XCP1100 or later on M4000/M5000/M8000/M9000 servers.
The "Type" information for the CPU/Memory board unit, Motherboard unit, and I/O unit may be identified by a letter or number, such as "Type:A" or "Type:1". A larger letter or number indicates that a newer version of hardware is installed.
The power type in the Power supply unit information is supported in XCP1091 or later on M3000 server.

4.2 Display Domain Information

This section describes methods for checking the configuration and status of a domain.

Note – For details on domain management, configuration and each command, see Chapter 2, the *XSCF Reference Manual*, or the *Administration Guide*.

Commands Used to Display Domain Information

Execute the following commands individually, as appropriate. For details of commands, see Chapter 5.

- `showdcl`
- `showboards`
- `showdomainstatus`
- `version`

4.2.1 Domain Information

- Command operation

1. **Use the** `showdcl`**(8) command to check the domain ID, LSB number, configuration policy, No memory state (true/false), No IO state (true/false), floating board state, and degradation information.**

```
<Example 1> In the SPARC Enterprise M4000/M5000/M8000/M9000 servers
XSCF> showdcl -va
DID   LSB   XSB   Status    No-Mem  No-IO  Float    Cfg-policy
00                Running                           FRU
      00    00-0             False  False  False
      01    -
      02    -
      03    -
      04    01-0             False  True   False
      05    -
:
      15    -
<Example 2> In the M3000 servers
XSCF> showdcl -va
DID   LSB   XSB   Status    No-Mem  No-IO  Float    Cfg-policy
00                Running                           FRU
      00    00-0             False  False  False
```

2. **Use the** `showdomainstatus`**(8) command to check the domain status.**

```
XSCF> showdomainstatus -a
DID         Domain Status
00          Running
01          -
02          Powered Off
03          Panic State
04          Shutdown Started
05          Booting/OpenBoot PROM prompt
06          Initialization Phase
07          OpenBoot Execution Completed
```

3. **Use the** showboards**(8) command to check the XSB number, domain ID, LSB number, and XSB status.**

```
XSCF> showboards -a
XSB  DID(LSB) Assignment  Pwr  Conn Conf Test    Fault
---- -------- ----------- ---- ---- ---- ------- --------
00-0 00(00)   Assigned    y    y    y    Passed  Normal
00-1 00(01)   Assigned    y    y    y    Passed  Normal
00-2 SP       Available   y    n    n    Passed  Normal
00-3 02(00)   Unavailable y    n    n    Unknown Normal
```

4. **Use the** version**(8) command to check the OpenBoot PROM version of a domain.**

```
XSCF> version -c cmu
DomainID  0: 02.09.0000
DomainID  1: 02.09.0000
:
DomainID  3: 02.09.0000
```

4.3 Adding or Removing Domains

The system can adopt a domain configuration by combining multiple system boards in a server. Each domain can operate independently.

To configure domains for a server, use the XSCF Web console or the XSCF Shell commands.

Note – In the M3000 server, the domain configuration policy can be changed by using the `setdcl`(8) command. However, other domain configurations cannot be changed.

Commands Used to Setup or Display Information

Execute the following commands individually, as appropriate. For details of these commands, see Chapter 5.

- `setdcl`
- `setupfru`
- `addboard`

- `deleteboard`
- `moveboard`

For details on adding or changing a domain, see Chapter 2 of the *XSCF Reference Manual* or the *Administration Guide*.

For details on using the DR function to change the domain configuration, see the *Dynamic Reconfiguration User's Guide*.

4.4 Server and Domain Power Operations

This section describes power operations for servers and domains, and it explains how to display the power status of a server or domain.

To perform the power operations, use the XSCF Shell commands.

Commands Used for the Operations or Status Display

Execute the following commands individually, as appropriate. For details of these commands, see Chapter 5.

- `poweron`
- `poweroff`
- `reset`
- `sendbreak`
- `setpowerupdelay`
- `showpowerupdelay`
- `setshutdowndelay`
- `showshutdowndelay`
- `setdualpowerfeed`
- `showdualpowerfeed`

With the power operations, the following can be performed:

- System power on
- System power off
- Domain power on
- Domain power off
- Sending a Domain Panic Request (Solaris OS dump request)

- Domain reset
- Sending break signal to a domain
- Air-conditioning wait time administration
- Warm-up time administration
- Dual power feed

4.4.1 System Power On

- Command operation

1. **Use the** `showlogs power` **command to check the status of system power off.**

   The System Power Off status means one of the following.

   - The input power supply has been turned on, and the `poweron`(8) command is not yet executed or the POWER switch of the operator panel is not yet pressed; that is, all domains have not yet been powered on.
   - The `poweroff`(8) command has been executed or the POWER switch of the operator panel has been pressed, to power off all domains; and "System Power Off" is displayed in the showlogs power command execution result.

```
XSCF> showlogs power
Feb 26 13:52:19 JST 2010    SCF Reset        Power on -- Service
Or
Feb 26 13:52:19 JST 2010    System Power Off Operator -- Service
```

2. **Use the** `poweron`**(8) command to turn on power to all domains.**

```
XSCF> poweron -a
DomainIDs to power on:00,01,02,03
Continue? [y|n] :y
00 :Not powering on: The power supply has already been turned on.
01 :Powering on
02 :Powering on
03 :Powering on

*Note*
 This command only issues the instruction to power-on.
 The result of the instruction can be checked by the
 "showlogs power".
```

Note – Only the domains that are able to be powered on are displayed.

---

3. **Use the** `showlogs power` **command to check the system power on.**

```
XSCF> showlogs power
Feb 26 14:12:19 JST 2010    System Power On Operator    --   Service
```

Note – Use the showdomainstatus(8) command to check the power status of the domain.

4.4.2 System Power Off

- Command operation

1. **Use the** `showlogs power` **command to check the power status of the system.**

```
XSCF> showlogs power
Feb 26 14:12:19 JST 2010    System Power On  Operator    --   Service
```

2. **Use the** `showdomainstatus`**(8) command to check the power status of the system.**

```
XSCF> showdomainstatus -a
DID          Domain Status
00           Running
01           Running
02           Running
03           Running
```

3. **Use the** `poweroff`**(8) command to turn off power to all domains.**

```
XSCF> poweroff -a
DomainIDs to power off:00,01,02,03
Continue? [y|n] :y
00 : Powering off
01 : Powering off
02 : Powering off
03 : Powering off

*Note*
 This command only issues the instruction to power-off.
 The result of the instruction can be checked by the
 "showlogs power".
```

Note – Only the domains that are able to be powered off are displayed.

Note – If the poweroff(8) command is performed, and the shutdown has completed, then the domain is powered off.

4. **Use the** showlogs power **command to check the system power off.**

```
XSCF> showlogs power
Feb 26 14:22:19 JST 2010   System Power Off Operator    --   Service
```

4.4.3 Domain Power On

- Command operation

1. **Use the** showdomainstatus**(8) command to check the power status of all domains.**

```
XSCF> showdomainstatus -a
DID         Domain Status
00          Powered Off
01          Running
02          Powered Off
03          Powered Off
```

2. **Use the** poweron**(8) command to turn on power to the specified domain.**

```
<Example 1>  Turn on power to the specified domain.
XSCF> poweron -d 0
DomainIDs to power on:00
Continue? [y|n] :y
00 :Powering on

*Note*
 This command only issues the instruction to power-on.
 The result of the instruction can be checked by the
 "showlogs power".

<Example 2>  Cancel domain power on in progress.
XSCF> poweron -d 0
DomainIDs to power on:00
Continue? [y|n] :n
XSCF>
```

4.4.4 Domain Power Off

- Command operation

1. **Use the** `showdomainstatus`**(8) command to check the power status of all domains.**

```
XSCF> showdomainstatus -a
DID         Domain Status
00          Running
01          Running
02          Running
03          Powered Off
```

2. **Use the** `poweroff`**(8) command to turn off power to the specified domain.**

```
<Example 1>  Turn off power to the specified domain.
XSCF> poweroff -d 1
DomainIDs to power off:01
Continue? [y|n] :y
01 : Powering off

*Note*
 This command only issues the instruction to power-off.
 The result of the instruction can be checked by the
 "showlogs power".

<Example 2>  Cancel domain power off in progress.
XSCF> poweroff -d 1
DomainIDs to power off:01
Continue? [y|n] :n

<Example 3>  Forcibly turn off power to a domain.
XSCF> poweroff -f -d 1
DomainIDs to power off:01
The -f option will cause domains to be immediately reset.
Continue? [y|n] :y
01 :Powering off

*Note*
 This command only issues the instruction to power-off.
 The result of the instruction can be checked by the
 "showlogs power".
```

Note – If the `poweroff`(8) command is performed, and the shutdown has completed, then the domain is powered off.

Caution – IMPORTANT - See the following paragraphs for important information about the domain power-off procedure.

- When Oracle Solaris OS of the domain is being booted, the power cannot be turned off. After Oracle Solaris OS booting is completed, execute the `poweroff`(8) command again.
- When Oracle Solaris OS of the domain is running in single user mode, the power cannot be turned off using the `poweroff`(8) command. Execute the `shutdown`(1M) command on the domain.

Note that when Oracle Solaris OS of the domain is running, domain power-off (`shutdown -i5`, or equivalent) is required.

Also, even if a system abnormality (like a fan or temperature abnormality) is detected while the Oracle Solaris OS is being booted, or the system is running in single user mode, there may be cases where the power cannot be turned off. (An Oracle Solaris OS shutdown is not executed.) In such cases, immediately perform the procedure above.

4.4.5 Sending a Domain Panic Request

- Command operation

1. **Use the `showdomainstatus`(8) command to check the power status of the domain to which a panic instruction is to be issued.**

```
XSCF> showdomainstatus -a
DID         Domain Status
00          Running
01          Running
02          Running
03          Running
```

2. **Use the `reset`(8) command to issue a panic instruction to the specified domain.**

```
<Example>  Issue a panic instruction to the specified domain.
XSCF> reset -d 0 panic
DomainID to panic:00
Continue? [y|n] :y
00 :Panicked

*Note*
 This command only issues the instruction to reset.
 The result of the instruction can be checked by the
 "showlogs power".
```

4.4.6 Domain Reset

- Command operation

1. **Use the** `showdomainstatus`**(8) command to check the power status of the domain.**

```
XSCF> showdomainstatus -a
DID         Domain Status
00          Running
01          Running
02          Running
03          Running
```

2. **Use the** `reset`**(8) command to issue a reset instruction to the specified domain.**

```
<Example 1>  Issue a domain ID 0 reset instruction.
XSCF> reset -d 0 por
DomainID to reset:00
Continue? [y|n] :y
00 :Reset

*Note*
 This command only issues the instruction to reset.
 The result of the instruction can be checked by the
 "showlogs power".

<Example 2>  Issue an XIR reset instruction.
XSCF> reset -d 0 xir
DomainID to reset:00
Continue? [y|n] :y
00 :Reset

*Note*
 This command only issues the instruction to reset.
 The result of the instruction can be checked by the
 "showlogs power".
```

3. **Use the showdomainstatus(8) command to check the power status of the domain specified to be reset.**

```
XSCF> showdomainstatus -a
DID         Domain Status
00          Booting/OpenBoot PROM prompt
01          Running
02          Running
03          Running
```

Note – When the mode switch on the operator panel is set to "Service" or auto boot is disabled by the setdomainmode(8) command, automatic boot of the Oracle Solaris OS after the reset instruction is suppressed.

Note – Since the reset(8) command forcibly resets the system, this command may cause a failure in a hard disk drive or other components. Use this command only for the purpose of recovery, such as if the Oracle Solaris OS hangs, and for other limited purposes.

4.4.7 Sending a Break Signal to a Domain

- Command operation

1. **Use the showdomainstatus(8) command to confirm the domain status.**

```
XSCF> showdomainstatus -a
DID         Domain Status
00          Running
01          Running
02          Running
03          Running
```

2. **Use the sendbreak(8) command to send a Break signal to the specified domain.**

```
XSCF> sendbreak -d 0
Send break signal to DomainID 0?[y|n] :y
```

3. **Confirm ok prompt on the specified domain console.**

Note – To send the break signal to the domain, the domain mode setting is required. When the mode switch on the operator panel is set to Service, the automatic boot and host watchdog functions are suppressed and the break signal is received, regardless of the domain mode settings. For details of the domain mode settings, see Section 2.2.15, "Domain Mode Configuration" on page 2-178.

4.4.8 Air-Conditioning Wait Time Administration

The air-conditioning wait time is intended to prevent the server from performing power-on processing until the room temperature environment is prepared by air-conditioning facilities. Once the air-conditioning wait time is set, the server will start power-on processing after its power is turned on and the set air-conditioning time elapses.

- Command operation

1. **Use the** `showpowerupdelay`**(8) command to display the air-conditioning wait time (wait time).**

```
XSCF> showpowerupdelay
warmup time : 10 minute(s)
wait time   : 20 minute(s)
```

2. **Use the** `setpowerupdelay`**(8) command to set the air-conditioning wait time. Set the air-conditioning wait time from 0 to 255 (min). The default is "0 min."**

```
<Example>  The air-conditioning wait time is set to 15 min.
XSCF> setpowerupdelay -c wait -s 15
```

3. **Use the** `showpowerupdelay`**(8) command to confirm the setting. Also, to apply the setting, turning on the server power supply.**

```
XSCF> showpowerupdelay
warmup time : 10 minute(s)
wait time   : 15 minute(s)
```

4. **Confirm whether the setting time is valid when turning on the server power supply the next time, by checking the time from when you perform the power on till when the power supply unit is actually turned on.**

4.4.9 Warm-Up Time Administration

The warm-up time is intended to prevent the power supply unit and the fan from running until the power supply environments of peripheral units are prepared after the server starts the power-on processing. Once the warm-up time is set, the OpenBoot PROM will start after the server power supply is turned on, the power-on processing starts, and the set warm-up time elapses.

Note – The fan in an M3000/M4000/M5000 server is driven at low speed as the server starts the power-on process.

- Command operation

1. **Use the `showpowerupdelay`(8) command to display the warm-up time (`warmup time`).**

```
XSCF> showpowerupdelay
warmup time : 10 minute(s)
wait time   : 20 minute(s)
```

2. **Use the `setpowerupdelay`(8) command to set the warm-up time. Set the warm-up time from 0 to 255 (min). The default is "0 min."**

```
<Example>  The warm-up time is set to 5 min.
XSCF> setpowerupdelay -c warmup -s 5
```

3. **Use the `showpowerupdelay`(8) command to confirm the setting. Also, to apply the setting, turning on the server power supply.**

```
XSCF> showpowerupdelay
warmup time : 5 minute(s)
wait time   : 20 minute(s)
```

4. **When turning on the server power supply the next time, please confirm that it takes more time than usually by checking the amount of time it takes from the power on until the time when the first Power On Self Test (POST) start message is displayed.**

Note – Once the air-conditioning time is set, the warm-up time will be valid after the power is turned on and the air-conditioning time elapses. The air-conditioning time and the warm-up time are also valid when the power is turned on at the power recovery after the power failure.

Caution – IMPORTANT - When the power is turned on from the operator panel, the air-conditioning time and warm-up time that you set are ignored. If you have set these times and wish to observe them at startup, perform the poweron(8) command.

4.4.10 Shutdown Wait Time Administration

The shutdown wait time administration is a setting to delay the shutdown start by specifying the shutdown start time when a power failure has occurred in the system with the UPS.

- Command operation

1. **Use the** showshutdowndelay**(8) command to display the shutdown wait time.**

```
XSCF> showshutdowndelay
UPS shutdown wait time : 500 second(s)
```

2. **Use the** setshutdowndelay**(8) command to set the shutdown wait time. Set the shutdown wait time from 0 to 9999 (sec). The default is "10 sec."**

```
<Example>  The shutdown wait time is set to 600 sec.
XSCF> setshutdowndelay -s 600
```

4.4.11 Dual Power Feed Administration

The dual power feed is a type of power feed for high-reliability systems that contain dual lines to the power supply. If one line stops, the other line does not stop and enables the system to continue operation. This capability can be enabled or disabled using an XSCF Shell command. This setting is done by FEs.

Note – The ability to enable and disable the dual power feed or display its current status is available on M3000/M4000/M5000 servers only. However, the dual power feed mode cannot be used with 100V power on M4000/M5000 servers. When the optional power cabinet for dual power feed is connected on M8000/M9000 servers, it automatically configures the dual power feed mode. For details about the setting the dual power feed, see the *Installation Guide* for your server.

- Command operation

1. **Use the** `showdualpowerfeed`**(8) command to display the current setting status of the dual power feed.**

```
XSCF> showdualpowerfeed
Dual power feed is disabled.
```

2. **Use the** `setdualpowerfeed`**(8) command to enable or disable the dual power feed of this system.**

```
<Example 1>  Enabling the dual power feed.
XSCF> setdualpowerfeed -s enable
disable -> enable
NOTE: Dual power feed will be enabled the next time the platform
is powered on.

<Example 2> Disabling the dual power feed.
XSCF> setdualpowerfeed -s disable
enable -> disable
NOTE: Dual power feed will be disabled the next time the platform
is powered on.
```

3. **Confirm the new setting, and if it is correct, turn off the input power and then turn on to apply the specified configuration. When you enabled the dual power feed mode, you can apply the configuration by executing the** `rebootxscf`**(8) command.**

```
XSCF> showdualpowerfeed
disable -> enable
NOTE: Dual power feed will be enabled the next time the platform
is powered on.
```

4. **Confirm whether the setting is valid after turning off/on the input power.**

```
XSCF> showdualpowerfeed
Dual power feed is enabled.
```

4.5 Identifying the Location of the System

When more than one same type of system is installed in the same area, it may be difficult to locate the target system. You can easily find target machine, even when it does not have any faulty components, by using the XSCF Shell `showlocator`(8) command and looking for the blinking the CHECK LED on the operator panel.

- Command operation

1. **Use the `showlocator`(8) command to display the current status of the CHECK LED.**

```
XSCF> showlocator
Locator LED status: Off
```

2. **Use the `showlocator`(8) command to blink or reset the CHECK LED.**

```
<Example 1> Blink the CHECK LED.
XSCF> setlocator blink

<Example 2> Reset the CHECK LED.
XSCF> setlocator reset
```

3. **Use the `showlocator`(8) command to display the state of the CHECK LED.**

```
XSCF> showlocator
Locator LED status: Blinking
```

4.6 Managing Fault Degradation

4.6.1 Displaying the Degraded Component

The status of a faulty or degraded component, or a part of such component, can be displayed by using the following methods:

- Command operation

- **Use the `showstatus`(8) command to display the unit status. An asterisk (*) is attached to a unit in abnormal status.**

```
<Example 1>  The memory board and memory on the motherboard unit
(MBU) are degraded due to failure.
XSCF> showstatus
    MBU_B Status:Normal;
*       MEMB#1 Status:Deconfigured;
*           MEM#3B Status:Deconfigured;

<Example 2>  The CPU is degraded due to the effect of the crossbar
unit (XBU) being degraded.
XSCF> showstatus
    MBU_B Status:Normal;
*       CPUM#1-CHIP#1 Status:Deconfigured;
*   XBU_B#0 Status:Degraded;

<Example 3>  No degraded component is found.
XSCF> showstatus
No failures found in System Initialization.
```

The meaning of each component status is as follows:

Faulted — The component is faulty and not operating.

Degraded — The component is operating. However, either an error has been detected or the component is faulty. As a result, the component might be operating with reduced functionality or performance.

Deconfigured — As a result of another component's faulted or degraded status, the component is not operating. (The component itself is not faulted or degraded.)

Maintenance — The corresponding component is under maintenance. A `deletefru`(8), `replacefru`(8), and `addfru`(8) operation is currently underway.

Normal — The component is operating normally.

4.6.2 Clearing the Fault/Degradation Information

The information on a faulty or degraded component is cleared when the component is replaced. For a component replacement, please contact a field engineer.

4.7 Changing the Time

The time of the server is based on the XSCF time. Time can be displayed or set to local time or UTC. For details on displaying or setting the system time, see Chapter 2.

4.8 Switching the XSCF Unit

In some cases, such as when an error occurs in the LAN route of the XSCF Unit on the active side in a system in which the XSCF Unit is redundantly configured, it may be necessary to switch the active side over to the standby side.

The procedure for switching the XSCF Unit status from standby to active is as follows:

- Command operation

1. **Log in the XSCF Unit on the standby side.**
2. **Use the `switchscf`(8) command to switch the XSCF Unit from standby status to active status.**

Note – If possible, confirm that the ACTIVE LED states changes on the front panels of both XSCF Units. Execute the `switchscf`(8) command only on one side (active side or standby side) of the XSCF Units to automatically switch active/standby status of the other XSCF Unit.

For specifying an option in the `switchscf`(8) command, see the *XSCF Reference Manual*.

Processing Continued at XSCF Reset or Failover

In case an XSCF reset or failover was generated while the following processes are executing, the process will be continued:

- Domain power-on process
- Domain power-off process
- DR function

Caution – IMPORTANT - An XSCF reset or failover might prevet the above setting operation from completing. If a reset or failover occurs during the operation, log in to the active XSCF to determine if the operation succeeded. If not, try it again. For details on DR, see the *Dynamic Reconfiguration User's Guide*.

4.9 Displaying State of an External I/O Expansion Unit and Administration

This section describes the management overview of an External I/O expansion unit connected to the server, components in the External I/O Expansion Unit such as I/O boards, link cards, and power supply units (PSUs), and downlink cards mounted in PCI slots in the server, and cards that contain Energy Storage Modules (ESM) and are attached to the host system.

Note – For the hardware configuration of an External I/O Expansion Unit, see the *External I/O Expansion Unit Installation and Service Manual* or the *Service Manual* for your server. For details and examples of use of commands, see the *XSCF Reference Manual* and the `ioxadm`(8) man page.

TABLE 4-4 lists terms used in External I/O Expansion Unit administration.

TABLE 4-4 External I/O Expansion Unit Administration Terms

Term	Description
Host path	Device path. A device name and device number are used to represent the layer location of a component in the component layer structure. (Example: IOU#1-PCIE#4)
Downlink card path	A downlink card that is mounted in a PCI slot in an I/O unit of the server and connected to an External I/O Expansion Unit. An External I/O Expansion Unit is connected to one or two downlink cards. A downlink card path represents the layer location indicating which downlink card is connected to the External I/O Expansion Unit in the layer structure. (Example: IOU#1-PCIE#2)

TABLE 4-5 lists setting items and the corresponding shell commands.

TABLE 4-5 External I/O Expansion Unit Administration

Item	Description	Shell Command	Remarks
Display list	Displays a list of External I/O Expansion Units and cards in the host slot is identified by the host_path to the card. The following is displayed: • Set External I/O Expansion Unit numbers and downlink card paths • External I/O Expansion Units, I/O boards, link cards (Note 1), downlink cards, power supply unit types, firmware versions, serial numbers, part numbers, and states	`ioxadm`	External I/O Expansion Unit numbers are set in two ways: specifying last four digits of serial numbers such as `iox@nnnn`, and specifying instance numbers such as ioxn.
Display environment information	Displays the status of the environment of the specified External I/O Expansion Unit or downlink card as sensor measurement values. Also displays the environmentals of a FRU in an I/O Expansion Unit or a card in a host slot. The following is displayed: • Current (A) • Voltage (V) • Fan speed (RPM) • Temperature (C) • LED state • SWITCH	`ioxadm`	Also, the preciseness is displayed together with the sensor measurement values.

TABLE 4-5 External I/O Expansion Unit Administration *(Continued)*

Item	Description	Shell Command	Remarks
Display/set locator LED (Note 2)	Displays and sets the locator LED state for individual components in the specified External I/O Expansion Unit. Each locator LED is in one of the following states: • Blinking • Lit • Off Any of the following locator LED states can be set: • Enabled (on) • Disabled (off)	`ioxadm`	Only one locator LED can be enabled or disabled at a time in an External I/O Expansion Unit.
Power on/off	Turns on or off power to the specified I/O board or power supply unit. Note: To forcibly disconnect an IO board belonging to a domain, use the `-f` option.	`ioxadm`	Even after the power switch is set to off, LEDs and fans continue operating as long as they are supplied with power.
Display/set runtime of card with ESM	Displays and clears runtime of the card with ESM.	`ioxadm`	

Note – (1) Also called uplink cards. They are mounted on I/O boards.

Note – (2) A locator LED that indicates a location. The names of locator LEDs depend on the corresponding components. For the External I/O Expansion Unit and LED types and the descriptions of components contained in an External I/O Expansion Unit, see the *External I/O Expansion Unit Installation and Service Manual* for your server.

Displaying a List of External I/O Expansion Units, I/O Boards, Link Cards, and Power Supply Units or Displaying Their Environment Information

- Command operation

● **Use the** `ioxadm`**(8) command to display a list of External I/O Expansion Units and downlink card paths and to display information for each component.**

```
<Example 1>  Display a list of External I/O Expansion Units and
downlink cards
XSCF> ioxadm list
IOX             Link 0          Link 1
IOX@5309        IOU#2-PCI#2     IOU#3-PCI#1
IOX@A3B5        -               IOU#1-PCI#1
-               -               IOU#2-PCI#1

<Example 2>  Display a list of External I/O Expansion Units, I/O
ports, link cards, and power supply units
XSCF> ioxadm -v list IOU#1-PCI#1
Location        Type        FW Ver    Serial Num   Part Num     State
IOX@A3B5        IOX         1.4       CP0001       5016937-01   On
IOX@A3B5/PS0    A195        -         PS0001       3001701-02   On
:
<Example 3> Display a card using host_path in verbose mode with
headers suppressed
XSCF> ioxadm -p -v list IOU#1-PCI#2
IOU#1-PCI#2       F20  -   000004      5111500-01   On

<Example 4>  Display environment information based on sensor
measurements
XSCF> ioxadm env -te IOX@A3B5
Location        Sensor         Value         Res  Units
IOX@A3B5/PS0    T_AMBIENT     28.000       1.000      C
IOX@A3B5/PS0    V_ISHARE       0.632       0.040      V
IOX@A3B5/PS0    I_DC           2.316       0.289      A
IOX@A3B5/PS0    S_FAN_SET   4500.000     300.000    RPM
:
```

Displaying and Setting the Locator LED State of Each Specified Component in an External I/O Expansion Unit

- Command operation

● **Use the** `ioxadm`**(8) command to display or set the locator LED state of the specified component.**

```
<Example 1>  Display the locator LED states of an External I/O
Expansion Unit and components.
XSCF> ioxadm locator iox@12B4
Location        Sensor  Value   Res     Units
IOX@12B4        LOCATE  Fast    -       LED
IOX@12B4/PS0    SERVICE Fast    -       LED

<Example 2>  Set the locator LED state of PSU0 to on.
XSCF> ioxadm locator on iox@12B4/ps0
Location        Sensor  Value   Res     Units
IOX@12B4        LOCATE  Fast    -       LED
IOX@12B4/PS0    SERVICE On      -       LED
```

Turning On or Off Power to an I/O Board or Power Supply Unit

- Command operation

● **Use the** `ioxadm`**(8) command to display, turn on or off power to the specified component.**

```
<Example 1>  Display the PSU states of an External I/O Expansion Unit and
components.
XSCF> ioxadm -v list IOX@12B4
Location               Type       FW Ver    Serial Num   Part Num    State
IOX@12B4                IOX       1.0       XCX033       5016937-03  On
IOX@12B4/PS0           A195       -         T01056       3001701-03  On
IOX@12B4/PS1           A195       -         T01074       3001701-03  On
IOX@12B4/IOB0          PCIX       -         XX00A3       5016938-04  On
IOX@12B4/IOB0/LINK     OP         1.3       XF00X8       5017040-03  On

<Example 2>  Turn off power to I/O board 0.
XSCF> ioxadm poweroff iox@12B4/iob0

<Example 3>  Turn on power to I/O board 0 again.
XSCF> ioxadm poweron iox@12B4/iob0
```

Displaying and Clearing the Card with ESM

- Command operation

● **Use the** `ioxadm`**(8) command to display and clear runtime of the card with ESM.**

```
<Example 1>  Display runtime of card with ESM using verbose output.
XSCF> ioxadm -v lifetime IOU#0-PCI#1
NAC           Total Time On   (% of life)  Warning Time   Fault Time
IOU#0-PCI#1   1052370          100         1041120        1051200

<Example 2> Clear runtime of card with ESM, show runtime is cleared.
XSCF> ioxadm lifetime -z IOU#0-PCI#1
XSCF> ioxadm lifetime IOU#0-PCI#1
NAC           Total Time On   (% of life)
IOU#0-PCI#1   0                0
```

4.10 Restore Factory Settings of the Server or XSCF Unit

To restore the server or the XSCF Unit to the factory settings, execute the `restoredefaults`(8) command on the XSCF Unit.

Caution – IMPORTANT - User information and error logs are cleared from the XSCF Unit.

The restoredefaults(8) command can initialize the server (Operator panel and the XSCF Unit) or the XSCF Unit.

When the command is executed on the active XSCF of the M8000/M9000 server, both the active and standby XSCF or the server (the operator panel and both XSCF Units) are initialized. However, when the command is executed on the standby XSCF of the M8000/M9000 server, only the standby XSCF is initialized. The server or the active XSCF cannot be initialized from the standby XSCF.

- Command operation

To execute this command:

1. **Connect to the XSCF over a serial connection.**

2. **Log in the XSCF Unit.**

3. **Use the `restoredefaults`(8) command to initialize the server (operator panel and XSCF Unit) or the XSCF Unit.**

For specifying an option in the `restoredefaults`(8) command, see the *XSCF Reference Manual*.

Note – For this command support information, see the Product Notes for your server.

CHAPTER 5

Overview of the XSCF Shell

This chapter describes how to use the XSCF Shell. The chapter also describes how to use commands and log in with an XSCF user account. It also explains command errors.

5.1 Overview of the XSCF Command Shell

Performing certain XSCF commands on the XSCF Shell terminal can display the server status so that control and configuration information related to system operation can be viewed.

The XSCF commands are effectively used by users who have created user accounts for the XSCF Shell terminal but cannot use the XSCF Web.

The following XSCF commands can be used from the XSCF Shell prompt (XSCF>) displayed after login to XSCF.

There are nine user privilege types as described below. For details on setting the user privilege, see Chapter 2. For details on the operations available with each user privilege level, see Chapter 1 or the *Administration Guide*.

- domainop: The user can refer to all status information in a domain.
- domainmgr: The user can perform domain power operations.
- domainadm: The user has domain administrator privilege and can perform every type of domain operation.
- platop: The user can refer to all status information in the entire system.
- platadm: The user has system administrator privilege and can use almost all XSCF Shell commands
- useradm: The user can manage user accounts.

- auditop: The user can refer to the audit method of the XSCF and the audit records.
- auditadm: The user can control the audit to the XSCF.
- fieldeng: The user can perform the commands for FEs.

TABLE 5-1 outlines the XSCF Shell commands. For details on each command and user privileges, see the man page or the *XSCF Reference Manual*.

TABLE 5-1 XSCF Commands

Command	Description
`adduser`	Creates an XSCF user account.
`deleteuser`	Deletes an XSCF user account.
`disableuser`	Disables an XSCF user account
`enableuser`	Enables an XSCF user account.
`showuser`	Displays XSCF user account information. Alternatively, it displays the user's own user account information.
`password`	Changes an XSCF user account password. Alternatively, it changes the user's own XSCF user account password.
`setpasswordpolicy`	Configures the XSCF password policy.
`showpasswordpolicy`	Displays the XSCF password policy.
`setprivileges`	Assigns user privileges.
`setloginlockout`	Configures the lockout of user accounts.
`showloginlockout`	Displays the lockout setting of user accounts.
`setnetwork`	Configures the XSCF network.
`shownetwork`	Displays the XSCF network settings and XSCF-LAN network status.
`setroute`	Configures the XSCF-LAN route.
`showroute`	Displays XSCF-LAN route settings.
`sethostname`	Specifies the XSCF-LAN host name and domain name.
`showhostname`	Displays the XSCF-LAN host name and domain name.
`setnameserver`	Sets the XSCF name servers (DNS servers) and the search paths.
`shownameserver`	Displays the XSCF name servers and the search paths.
`applynetwork`	Applies the network settings.
`setdscp`	Configures DSCP.
`showdscp`	Displays the DSCP settings.
`nslookup`	Checks for the name resolution of a host name.

TABLE 5-1 XSCF Commands *(Continued)*

Command	Description
`ping`	Checks the response for a host.
`traceroute`	Displays the network path to the host by list.
`setpacketfilters`	Sets the IP packet filtering rules to be used in the XSCF network.
`showpacketfilters`	Displays the IP packet filtering rules that are set in the XSCF network.
`settimezone`	Specifies the time zone.
`showtimezone`	Displays the time zone setting.
`setdate`	Sets the XSCF time.
`showdate`	Displays the XSCF time.
`setntp`	Configures the NTP server.
`showntp`	Displays the NTP server setting.
`resetdateoffset`	Resets the time subtraction between the XSCF and the domain.
`showdateoffset`	Displays the time subtraction between the XSCF and the domain.
`setssh`	Configures SSH. Generates RSA and DSA keys for SSH2 host authentication.
`showssh`	Displays the SSH settings and fingerprint.
`settelnet`	Configures telnet.
`showtelnet`	Displays the telnet settings.
`setautologout`	Sets the session timeout time of the XSCF Shell.
`showautologout`	Displays the session timeout time of the XSCF Shell.
`setsmtp`	Configures the SMTP server.
`showsmtp`	Displays the SMTP server settings.
`setemailreport`	Configures mail notification.
`showemailreport`	Displays the mail notification settings.
`setlookup`	Enables or disables the use of an LDAP server for authentication and user privilege lookup.
`showlookup`	Displays information about whether an LDAP server is used for authentication and user privilege lookup.
`setldap`	Configures LDAP client settings.
`showldap`	Displays LDAP client settings.
`setad`	Configures Active Directory client settings.
`showad`	Displays Active Directory client settings.
`setldapssl`	Configures LDAP/SSL client settings.

TABLE 5-1 XSCF Commands *(Continued)*

Command	Description
`showldapssl`	Displays LDAP/SSL client settings.
`sethttps`	Configures the https settings.
`showhttps`	Displays the https settings.
`setupplatform`	• Sets up platform-specific settings. Note: In the platform-specific settings, the following items can be optionally configured. Each item is the same as the setting of Chapter 2. • User Account settings • XSCF Network Settings • Internal DSCP Network • Domain Name Service • Network Time Protocol • SSH • HTTPS Server • Email Reports
`setarchiving`	Configures the log archiving function of XSCF.
`showarchiving`	Displays the settings of the log archiving function of XSCF.
`setaudit`	Configures the auditing of XSCF.
`showaudit`	Displays the settings of the audit of XSCF.
`viewaudit`	Displays the audit records (Audit trail) of XSCF.
`setsnmp`	Configures the SNMP Agent.
`showsnmp`	Displays the SNMP Agent settings.
`setsnmpusm`	Configures the USM management information for the SNMP agent.
`showsnmpusm`	Displays the USM management information for the SNMP agent.
`setsnmpvacm`	Configures the VACM management information for the SNMP agent.
`showsnmpvacm`	Displays the VACM management information for the SNMP agent.
`setsunmc`	Start or stop the Sun Management Center agent and make changes to its configuration.
`showsunmc`	Show setup information and status of Sun Management Center agent.
`setdcl`	Specifies the domain configuration information (DCL).
`showdcl`	Displays the domain configuration information.
`showboards`	Displays the component information and the COD information about a system board.
`showdevices`	Displays the domain information specified for a system board.
`showdomainstatus`	Displays the domain status.

TABLE 5-1 XSCF Commands *(Continued)*

Command	Description
setupfru	Specifies the number of XSB partitions of the system board and sets the memory mirror mode.
showfru	Displays the specified number of XSB partitions of the system board and the memory mirror mode that is set.
testsb	Diagnoses the system board.
addboard	Adds a system board to a domain.
deleteboard	Deletes a system board from a domain. Alternatively, it reserves a delete to the system board. If the deletion is reserved, the deletion is done after Oracle Solaris OS reboot.
moveboard	Moves a system board to another domain. Alternatively, it reserves a move to the system board. If the movement is reserved, the deletion is done after Oracle Solaris OS reboot of source domain, and the assignment to the new domain is done.
replacefru	Replaces a CPU/Memory Board unit, I/O unit, fan unit, PSU, or XSCF Unit in work performed according to the applicable guide.
addfru	Installs a CPU/Memory Board unit, I/O unit, fan unit, or PSU in work performed according to the applicable guide.
deletefru	Removes a CPU/Memory Board unit or I/O unit in work performed according to the applicable guide.
setdomainmode	Sets a hardware initial diagnostic level (No, standard, maximum). Enables or disables break signal sending, host watchdog, automatic boot, and sets CPU operation mode.
showdomainmode	Displays the domain host ID, the hardware initial diagnostic level, information of enabled or disabled status on break signal sending, Host watchdog, automatic boot, and displays CPU operation mode, ethernet address (mac address).
sendbreak	Sends a break signal to the server.
showresult	Displays the exit status of the most recently executed command.
setlocale	Sets locale.
showlocale	Displays locale.
setaltitude	Sets altitude.
showaltitude	Displays altitude.
cfgdevice	Sets the connection destination of the DVD drive unit and tape drive unit. Displays the setting status information.
console	Connects to a domain console.
showconsolepath	Displays the operating status of the main console.

TABLE 5-1 XSCF Commands *(Continued)*

Command	Description
showenvironment	Displays the temperature, humidity, voltage, fan rotation speed, power consumption, and exhaust airflow.
showstatus	Lists degraded components.
showhardconf	Displays all components mounted in the server.
poweron	Turns on power to all domains or the specified domain.
poweroff	Turns off power to all domains or the specified domain.
reset	Resets the specified domain. Note: The following three reset modes are available: por: Domain system reset request: Domain panic instruction xir: Domain CPU reset
setpowerupdelay	Sets the warm-up time and the air-conditioning wait time.
showpowerupdelay	Displays the warm-up time and the air-conditioning wait time settings.
setshutdowndelay	Sets the UPS shutdown delay time at power failure.
showshutdowndelay	Displays the UPS shutdown delay time at power failure.
setdualpowerfeed	Sets the dual power feed.
showdualpowerfeed	Displays the dual power feed.
setlocator	Enables or disables the CHECK LED blinking.
showlocator	Displays the LED status.
switchscf	Switches the XSCF Unit state (Active/Standby).
ioxadm	Configures the External I/O Expansion Unit (IOBOX). Displays the External I/O Expansion Unit settings.
clockboard	Sets/Displays the number of clock unit (CLKU) used when the next platform is powered on.
setdomparam	Rewrites the OpenBoot PROM environment variable that is compulsory.
getflashimage	Gets the firmware update program.
flashupdate	Updates the firmware program.
version	Displays the comprehensive firmware (XCP) version. Displays the XSCF firmware version. Displays the OpenBoot PROM firmware version.
prtfru	Displays the FRU-ROM data.
dumpconfig	Saves XSCF configuration information to the specified destination.
restoreconfig	Restores XSCF configuration information from the specified destination.

TABLE 5-1 XSCF Commands *(Continued)*

Command	Description
`restoredefaults`	Initializes the server or XSCF Unit to the factory shipping state.
`snapshot`	Saves log information to the specified destination.
`showmonitorlog`	Displays the XSCF monitoring messages on console in real time.
`showlogs`	Displays an error log, power log, event log, console log, panic log, IPL log, temperature/humidity log, and monitor message log.
`fmadm`	Monitors or controls the Fault Management Diagnosis Engines (FMDE).
`fmdump`	Dumps the fault event log containing FM diagnosis results.
`fmstat`	Displays the FMDE status.
`unlockmaintenance`	Forcibly release the locked status of the XSCF.
`rebootxscf`	Resets the XSCF.
`who`	Displays users who login to the XSCF.
`man`	Displays the man page of the specified command. You can see the list of commands by executing `man intro`.
`exit`	Ends the XSCF Shell.

Note – In the M3000/M4000/M5000/M8000/M9000 servers, some of the commands are not available, depending on the model in use. For the support information of each command, see the man page or the *XSCF Reference Manual*.

5.2 Login to XSCF Shell

This section describes how to log in to XSCF. The user can log in to XSCF from an XSCF-LAN port using either SSH or telnet, or from the serial port.

5.2.1 Before Logging In

Note the following before attempting to log in:

- For details on how to create, add, and delete user accounts, see Chapter 2.

- After login, if the shell has not been accessed for a certain period, XSCF automatically terminates the shell. The default timeout period is 10 minutes. The timeout period can be specified. For details on specifying the timeout period, see Chapter 2.
- In one domain, only one user can use the RW console (write-enabled console). While one user is using the RW console, another user cannot start another RW console in the same domain. For details on console connection, see Chapter 3.
- When a login fails, see Appendix D.

Note – In this manual, the window of the XSCF Shell terminal is called the XSCF console.

5.2.2 Operation From a Terminal Connected to the Serial Port

This section describes how to log in from a terminal connected to the serial port.

1. **After the terminal is connected to the serial port, press the Enter key on the terminal.**

2. **Enter a user account and password when prompted by XSCF.**

3. **Enter XSCF commands at the shell prompt (XSCF>) that is displayed after login to XSCF.**

The following is a login example:

```
login: jsmith
Password: xxxxxxxx
XSCF>
```

5.2.3 Operation for Connecting Via the XSCF-LAN (SSH)

This section describes how to log in to XSCF through an XSCF-LAN (SSH) connection.

1. **Before logging in using SSH, check that the fingerprint is pre-stored. If you did not save the fingerprint, please connect to the serial port and use `showssh`(8) to make a memo of the fingerprint of the host public key.**

2. **From an SSH client, specify the IP address or host name of XSCF and the port number, if necessary (default port number 22), and use SSH connection via XSCF-LAN.**

3. **Enter a user account and password when prompted by XSCF.**

4. **The fingerprint of the host public key may be displayed with a request to confirm its authenticity. If it is authentic, enter "yes" as the response, since the XSCF is correct with confirming the fingerprint.**

5. **Enter XSCF commands at the shell prompt (XSCF>) that is displayed after log in to XSCF.**

Note – To set the password for an XSCF user account, use the `password`(8) command. The `shownetwork`(8) command can be used to display XSCF-LAN setting information and the current network connection status.

The following is a login example:

```
[foo@phar foo]% ssh june@192.168.0.2
The authenticity of host '192.168.0.2 (192.168.0.2)' can't be established.
RSA key fingerprint is 03:4b:b4:b2:3d:4d:0c:24:03:ca:f1:63:f2:a7:f3:35.
Are you sure you want to continue connecting ? [yes|no] : yes
Warning: Permanently added '192.168.0.2' (RSA) to the list of known hosts.
foo@phar's password:xxxxxx
XSCF>
```

When the SSH connection is done using a user key, install the user public key in XSCF in advance. See Chapter 2 for instructions on how to install the user public key.

The following example shows a login using a user public key:

```
[client]# ssh nana@192.168.1.12
Enter passphrase for key '/home/nana/.ssh/id_rsa': xxxxxxx
Warning: No xauth data; using fake authentication data for X11
forwarding.
Last login: Mon Sep 1 10:19:37 2006 from client
XSCF>
```

5.2.4 Operation For Connecting Via the XSCF-LAN (Telnet)

This section describes how to log in to XSCF via an XSCF-LAN (telnet) connection.

1. **Enter the IP address or host name of XSCF and port number 23, and use telnet via XSCF-LAN.**
2. **Enter a user account and password from the XSCF console.**
3. **Enter XSCF commands at the shell prompt (XSCF>) that is displayed after you login to XSCF.**
4. **The following is a login example:**

```
login:jsmith
Password:xxxxxxxx
XSCF>
```

5.3 View Server Status and Control Commands

This section describes the typical XSCF Shell commands that can be used to display the server status, operate the server, and control the server. For details on the commands, see the man page or the *XSCF Reference Manual*. For XSCF setup commands, see Chapter 2.

- showenvironment
- showlocator/setlocator
- showconsolepath
- fmadm / fmdump / fmstat
- showdomainstatus
- reset / poweron / poweroff
- sendbreak

showenvironment

The `showenvironment`(8) command displays the values of all sensors in the server. By finding out the intake temperature, humidity, voltage, and fan rotation speed in the server, the system administrator can check for errors in the system environment.

In addition, by knowing the power consumption and volume of air exhausted from the server, the plant administrator can identify the specific areas in the installation site where the energy consumption can be reduced.

showlocator/setlocator

These commands display status information indicated by the LEDs on devices and the operator panel of the server. Finding out information on device errors is helpful in component degradation and replacement. Also, the system administrator can use the commands to identify the target device among many devices.

showconsolepath

The `showconsolepath`(8) command displays the operating status of the domain console. By finding out the users of domain consoles, the system administrator can notify the users before a user performs a server operation or server control.

fmadm / fmdump / fmstat

The server has an architecture that performs fault management (FMA) for CPUs, memory, and the I/O system during Oracle Solaris OS operation. The system administrator can use the `fmadm`(8) command to display configuration and status information about individual FMA modules that detect faults, perform fault diagnoses, and resolve faults. The command can also list faulty and degraded resources. The `fmstat`(8) command displays the processing time and number of events for each FMA module. The `fmdump`(8) command displays detailed fault information so that system administrator can determine faulty resources.

showdomainstatus

The `showdomainstatus`(8) command displays the current operating status of a domain. The system administrator can find out the status of each domain from its power on time to its operation start time.

reset / poweron / poweroff

There are three types of resets: the system reset, the panic instruction, and the CPU reset. To reset a domain, the system administrator can perform the `reset`(8) command with one of these three types specified. Performing the `poweron`(8) or `poweroff`(8) command can turn power on or off to a constructed domain in the system configuration.

sendbreak

The system administrator can use the `sendbreak`(8) command to send a break signal to the Oracle Solaris OS.

5.4 Server Configuration Information Commands

This section describes the typical XSCF Shell commands used to display configuration information on components in the server, such as the number of CPUs and memory capacity, the XSCF network configuration, the time, and degradation information.

- showhardconf
- shownetwork / showhostname / showroute / shownameserver / showdscp
- showntp / showdate
- showstatus

showhardconf

The showhardconf(8) command lists all the components mounted in the server and their status information. A problem component is indicated by a mark (*). The system administrator can check the component configurations and the numbers of different types of components.

shownetwork / showhostname / showroute / shownameserver / showdscp

The shownetwork(8) command displays the IP addresses, masks, and network connection information for the XSCF-LAN and ISN installed in the XSCF Unit. Also, the shownetwork(8) command displays the XSCF network connection status. By finding out the amount of data sent or received through a particular interface, the system administrator can check the LAN connection status and the management network load. The showhostname(8) command displays the current host name for the XSCF unit. The showroute(8) command displays routing environment such as destination IP addresses. The shownameserver(8) displays the DNS server. The system administrator can view the interface information required for the XSCF network. The showdscp(8) command displays the IP addresses assigned for DSCP usage. The showpacketfilters(8) command displays the IP packet filtering rules that are set in the XSCF network.

showntp / showdate

The showntp(8) command displays the NTP server configured with the server and the XSCF's own local clock informations. The showdate(8) command displays the system standard time (XSCF time). The system administrator can use the showdate(8) command to determine the reference time used in the server.

showstatus

The system administrator can use the showstatus(8) command to list degraded components.

5.5 Domain Control and Maintenance Commands

This section describes the typical XSCF Shell commands that manage resource assignment to domains and resource removal from domains, install devices, remove devices, replace devices, and enable or disable functions.

- showdevices / cfgdevice
- console
- showdcl / setdcl
- showfru / setupfru
- addfru / deletefru / replacefru
- showboards / addboard / deleteboard / moveboard
- showdomainmode / setdomainmode

showdevices / cfgdevice

The cfgdevice(8) command displays the domain to which a DVD drive unit or tape drive unit is assigned. Also, the cfgdevice(8) command can be used only on M8000/M9000 servers. The showdevices(8) command displays the operating status of resources installed on a system board (XSB). The system administrator can use this command to determine the devices to be assigned to a domain and check whether the DR function can be used to connect or disconnect an XSB.

console

The `console`(8) command establishes a connection to the domain console. This command supports both interactive and read-only connections.

showdcl / setdcl

The `showdcl`(8) command displays the domain configuration information (DCL) specified for individual domains or LSBs that compose a domain, and the `setdcl`(8) command specifies the configuration. The system administrator refers to and specifies DCL when adding an XSB to a domain.

showfru / setupfru

The `showfru`(8) command displays the locations of devices, such as system boards, mounted in the server and resource partition information, and the `setupfru`(8) command specifies these locations and this information. The system administrator can use the commands for effective use of resources.

addfru / deletefru / replacefru

The `addfru`(8) command is used to select a device, such as a CPU/Memory Board unit, I/O unit, fan unit, or PSU, to add it to the server, and the `deletefru`(8) and `replacefru`(8) commands are used to select and remove or replace, respectively, such a device mounted in the server. Each type of operation can be performed interactively with menus.

showboards / addboard / deleteboard / moveboard

The `showboards`(8) command displays status information about a system board (XSB). The system administrator can use the command to find out whether a system board has been configured to a domain or unconfigured from it, and to find out whether this operation was successful. The `addboard`(8) command adds a system board to the domain, the `deleteboard`(8) command removes a system board, and the `moveboard`(8) command moves a system board.

Note – In the M3000 server, the domain configuration cannot be changed.

showdomainmode / setdomainmode

In a certain domain, the user may want to suppress the break signal or panic with host watchdog or disable the automatic boot function. The system administrator can use the `showdomainmode`(8) command to display the related function settings and the `setdomainmode`(8) command to suppress or disable one of these functions for a domain. Also, the `showdomainmode`(8) command displays a domain host ID and ethernet address (mac address).

5.6 View and Archive the XSCF Logs

This section describes the XSCF commands that fetch and display server operation logs, console logs, temperature histories, and error logs from XSCF log files which also configure the information for archiving XSCF logs to a host.

For details on error logs, see Appendix B.

- showlogs
- showarchiving / setarchiving

showlogs

The `showlogs`(8) command displays error logs, power logs, event logs, console logs, panic logs, IPL logs, and temperature/humidity logs. The system administrator can use the command to check the operating status of the server and the cause of any error in the system.

showarchiving / setarchiving

The `showarchiving`(8) and `setarchiving`(8) commands display and specify, respectively, the information required for saving XSCF log information to servers. The system administrator can use these commands to set up automatic, secure archiving of logs to a specified archive host.

5.7 User Management and Security Commands

This section describes the typical XSCF commands for user management and security management.

- showuser / adduser / deleteuser / enableuser / disableuser
- password / setprivileges / showpasswordpolicy / setpasswordpolicy
- showlookup / setlookup / showldap / setldap / showad / setad / showldapssl / setldapssl
- showaudit / setaudit / viewaudit
- showloginlockout / setloginlockout
- showssh / setssh

showuser / adduser / deleteuser / enableuser / disableuser

The `showuser`(8) command can be used to list XSCF user accounts or display information about a particular user account. The `adduser`(8) and `deleteuser`(8) commands add and delete user accounts. The `enableuser`(8) and `disableuser`(8) commands enable and disable, respectively, user accounts.

password / setprivileges / showpasswordpolicy / setpasswordpolicy

The `password`(8) and `setprivileges`(8) commands set passwords and user privileges, respectively, for user accounts. The `showpasswordpolicy`(8) and `setpasswordpolicy`(8) commands display and specify the validity of passwords and other password policy information.

showlookup / setlookup / showldap / setldap / showad / setad / showldapssl / setldapssl

The `showlookup`(8) and `setlookup`(8) commands display and specify information on whether an LDAP server should be used for looking up the authentication and the user privilege. The `showldap`(8) and `setldap`(8) commands display and specify LDAP client settings, which are used when retrieving data from an LDAP server. The `showad`(8) and `setad`(8) commands display and specify Active Directory client settings, which are used when retrieving user informations from an Active Directory server. The showldapssl(8) and setldapssl(8) commands display and specify LDAP/SSL client settings, which are used when retrieving user informations from an LDAP/SSL server.

showaudit / setaudit / viewaudit

The showaudit(8) and setaudit(8) commands display and specify information such as which events can be subject for auditing. The system administrator can use the viewaudit(8) command to display audit records (audit trail).

showloginlockout / setloginlockout

The showloginlockout(8) and setloginlockout(8) commands display and specify information on whether to refuse a user login for a certain period of time after multiple attempts to log in to that user account failed.

showssh / setssh

The showssh(8) and setssh(8) commands can be used to display and specify the information on whether or not to enable the SSH access when a user logs in to XSCF. These commands can be used in generating the host key, registering/deleting the user public key, setting the timeout period of XSCF Shell, and setting whether or not to permit the SSH access from domain to XSCF via DSCP.

5.8 Use the XSCF Other Commands

The following XSCF Shell commands end the XSCF Shell and display version information. (Note)

- exit
- version

Note – The server provides many other commands. For details on these commands, see the man page or the *XSCF Reference Manual*.

exit

The exit(1) command ends the XSCF Shell.

version

The version(8) command displays the comprehensive firmware version (XCP version, see Note) of the XSCF firmware and POST/OpenBoot PROM firmware. The system administrator can display version information when upgrading firmware.

Note – XCP: XSCF Control Package that includes the programs which control the hardware components making up a computer system.

5.9 View XSCF Shell Error Messages

TABLE 5-2 lists the typical messages from each XSCF Shell command.

TABLE 5-2 Error Messages of XSCF Shell Commands

Message	Meaning
Invalid parameter.	An abnormal parameter error has occurred.
Operation failed.	Abnormal end.
Permission denied.	An execution authority error has occurred.
Operation not supported on this system.	Unsupported function.
Operation interrupted.	Processing interruption from user.
The current configuration does not support this operation.	Abnormal configuration.
A hardware error occurred. Please check the error log for details.	A hardware error has occurred.
An internal error has occurred. Please contact your system administrator.	An XSCF internal error has occurred.

Note – The error message depends on the command. Therefore, you will occasionally see more messages.

CHAPTER 6

XSCF Mail Function

This chapter describes the XSCF mail function.

6.1 Overview of XSCF Mail Function

The mail report function, used by XSCF firmware to send messages to the administrator, has the following features:

- Notification by email of faults in system components monitored by the XSCF

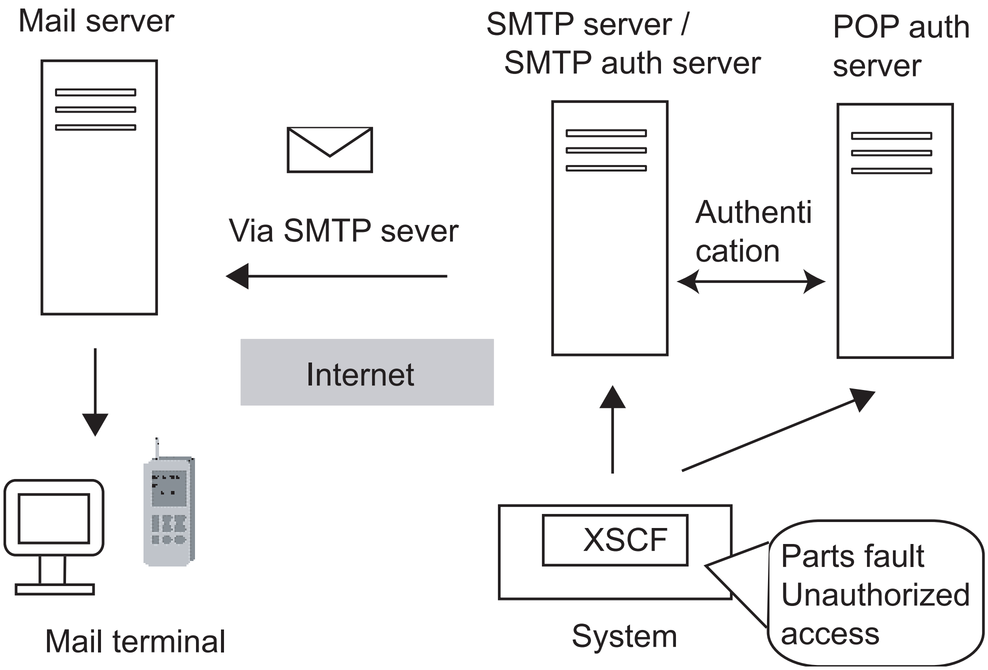
Even if a system failure or a serious error that disables reboot occurs, an email message is guaranteed to be sent.

- POP authentication facility and SMTP authentication at email sendings are possible

To prevent illegal Mail Sending, POP Authentication (POP before SMTP) or SMTP Authentication (SMTP-AUTH) can be done before mail sending is accepted with a SMTP server.

FIGURE 6-1 outlines the XSCF mail function.

FIGURE 6-1 XSCF Mail Function



XSCF Email Notification Path

The email notification path is described below. The setting for notification is made with the XSCF Shell.

- Sending an email message through the SMTP server

The host name or IP address of the SMTP server must be set.

- Sending an email with POP authentication or SMTP authentication

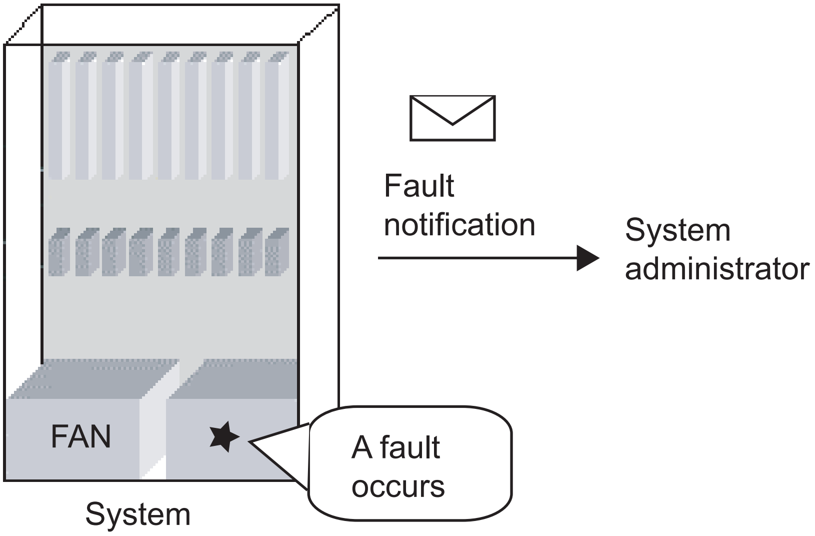
It is necessary to specify whether to do the authentication. And the POP authentication or the SMTP authentication must be selected. Then, ID and password for the authentication is required.

Parts Fault Notification

XSCF monitors components (such as CPU modules, fan units, CPU/Memory Board unit) in the server. XSCF can notify the system administrator by email of any fault that occurs in these devices.

FIGURE 6-2 shows mail being sent for parts fault notification to the system administrator.

FIGURE 6-2 XSCF Fault Notification



6.2 Setting Up the Mail Function

This section explains how to set up the XSCF mail function.

The workflow is as described below. Perform each step for setup with the XSCF Shell command line. For details on setup, see Chapter 2.

1. **Log in to XSCF.**
2. **Make the following settings for the XSCF mail function:**

   Host name or IP address of the SMTP server—(See `setsmtp`(8))

   Select POP authentication or SMTP authentication—(See `setsmtp`(8))

Reply address (from specification)—(See setsmtp(8))

Recipient address for mail for the system administrator—(See setemailreport(8))

3. **Enable the XSCF mail function. (See** setemailreport**(8))**

4. **Send test mail.**

   Test mail is automatically sent when the work for these mail settings is completed. If the email message sent as test mail is confirmed to have been received by the system administrator, it means that the correct settings have been made. If the email massage is not received, error mail is sent to the reply mail address (From:) or a record is made in an error log. In this event, identify the cause of the error, correct it, and start from step 1 again.

   Once the test is completed normally, the mail report function is enabled. Use the showemailreport(8) command to check whether the test is completed.

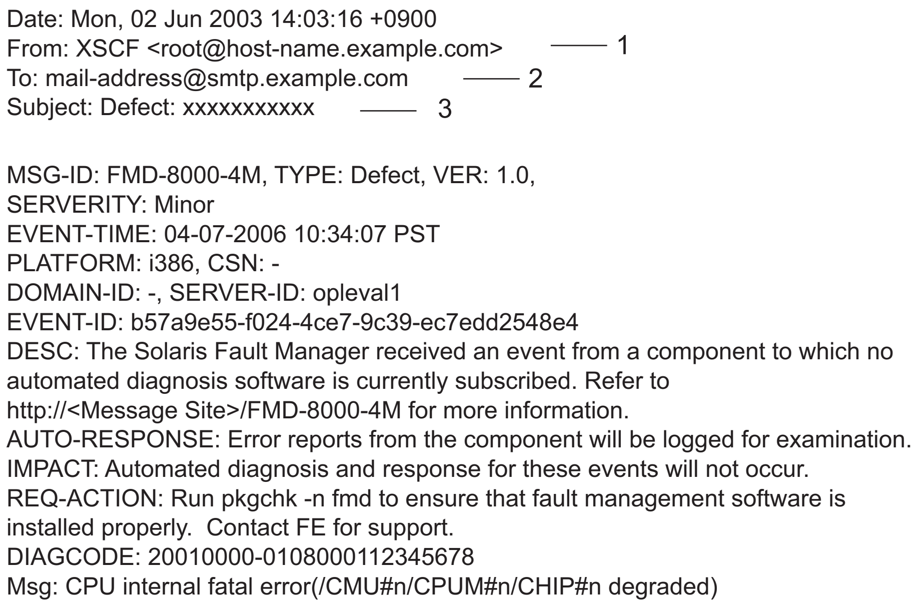
   For details on making settings for the SMTP server and name server, see Chapter 2.

6.3 Contents of Parts Fault Notification

This section explains the contents of the email messages sent for parts faults that occur.

FIGURE 6-3 shows the contents of mail sent for a parts fault that occurred.

FIGURE 6-3 Mail Sent for an XSCF Parts Fault That Occurred



```
Date: Mon, 02 Jun 2003 14:03:16 +0900
From: XSCF <root@host-name.example.com>
To: mail-address@smtp.example.com
Subject: Defect: xxxxxxxxxxx

MSG-ID: FMD-8000-4M, TYPE: Defect, VER: 1.0,
SERVERITY: Minor
EVENT-TIME: 04-07-2006 10:34:07 PST
PLATFORM: i386, CSN: -
DOMAIN-ID: -, SERVER-ID: opleval1
EVENT-ID: b57a9e55-f024-4ce7-9c39-ec7edd2548e4
DESC: The Solaris Fault Manager received an event from a component to which no
automated diagnosis software is currently subscribed. Refer to
http://<Message Site>/FMD-8000-4M for more information.
AUTO-RESPONSE: Error reports from the component will be logged for examination.
IMPACT: Automated diagnosis and response for these events will not occur.
REQ-ACTION: Run pkgchk -n fmd to ensure that fault management software is
installed properly.  Contact FE for support.
DIAGCODE: 20010000-0108000112345678
Msg: CPU internal fatal error(/CMU#n/CPUM#n/CHIP#n degraded)
```

1. Reply address set with Mail Administration

2. Recipient address set with Mail Administration

3. Mail title

Note – The contents may be changed as a result of a function improvement without notice. For details on the settings, see Chapter 2.

The following items are displayed in the mail example of FIGURE 6-3 (No.1 to 3 in the figure are excluded):

- MSG-ID: Message ID. Use the message ID for accessing the specified URL to acquire detailed information on this problem. For the specified URL, see the Web site information about messages described in the Product Notes for your server. For the message ID, the following information can be confirmed at the Web site:
  - Message type (Type)
  - Fault level (Severity)
  - Outline of fault (Description)
  - Machine operation after failure (Automated Response)
  - Influence (Impact)
  - Action to be taken (Action)
  - Detailed information (Details)
- TYPE, SEVERITY, DESC, AUTO-RESPONSE, IMPACT, and REQ-ACTION, these are the same items that the web site information in MSG-ID corresponds.
- VER: Version
- EVENT-TIME: Time of fault occurrence (indicated in local time)
- FLATFORM: Target architecture
- CSN: Chassis serial number
- DOMAIN-ID: Domain ID
- SERVER-ID: ID of this system
- EVENT-ID: Number used to uniquely identify the problem in an arbitrary system set
- DIAGCODE: Field engineers and authorized service personnel use this code for troubleshooting. The user is requested to inform the field engineer and authorized service personnel of this code, which is useful in resolving problems at an early stage.
- Msg: Message to show summary of problem

6.4 Test Mail

After XSCF mail function settings are made, a test mail can be sent to verify the settings. The send time of the test mail (the local time is displayed) and the information about the mail sender are displayed. Also, the "`Test Mail:`" characters are included in the subject of the test mail.

CHAPTER 7

XSCF SNMP Agent Function

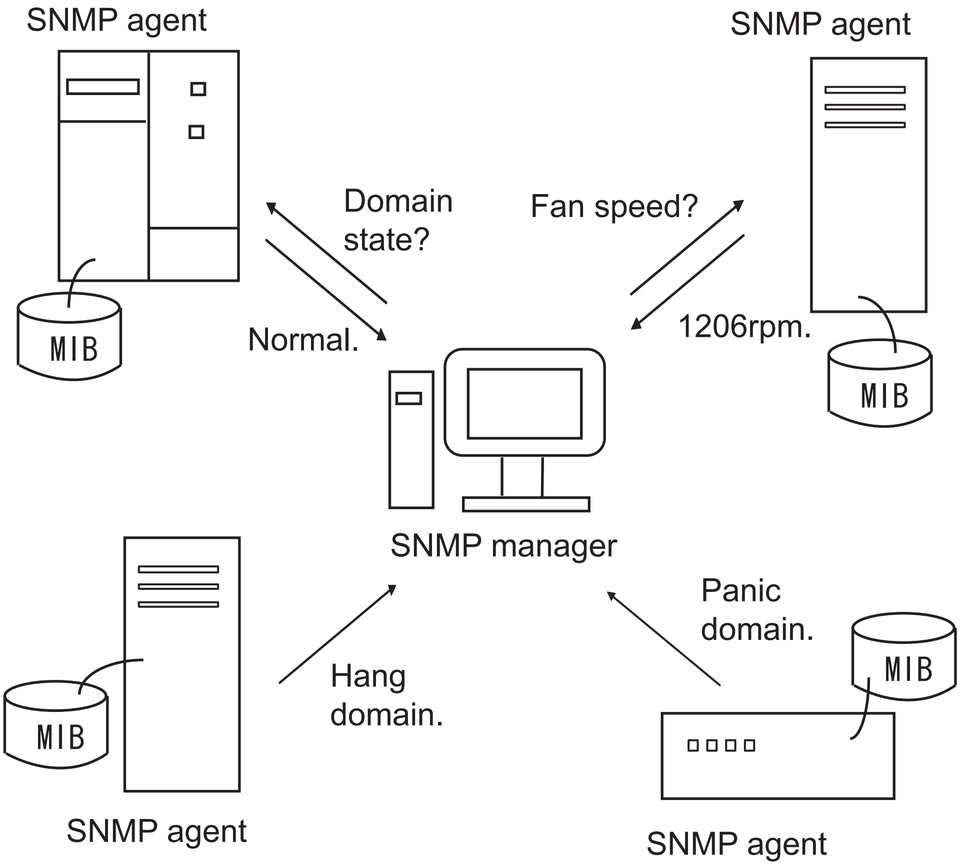
This chapter explains the XSCF SNMP agent function.

7.1 Overview of the XSCF SNMP Agent

XSCF supports the Simple Network Management Protocol (SNMP) agent function.

FIGURE 7-1 shows an example of a network management environment using SNMP.

FIGURE 7-1 Example of a Network Management Environment



SNMP

SNMP is a protocol for managing networks. The SNMP manager consolidates management of the operating conditions of terminals and network problems. The SNMP agent responds with management information from the Management Information Base (MIB) to requests from the manager. Also, a function called Trap can be used by the SNMP agent to exchange special information in asynchronous communication with the manager.

Note – The SNMP agent uses the 161 port and the 162 port for trap by default.

7.2 MIB Definition File

The SNMP agent responds with management information from the MIB information to requests from the manager.

Standard MIB

XSCF supports MIB-II (supports SNMPv2c and SNMPv3) and MIB-I (supports SNMPv1), which are Internet standards, to manage mainly the following information:

- Basic XSCF-LAN information (such as, administrator name)
- XSCF-LAN communication processing information
- XSCF SNMP agent behavior information

For a list from the standard MIB information supported by XSCF, see Appendix C.

Extended MIB

Other than the standard MIB, two extended MIBs are supported by this system as follows:

- The XSCF extension MIB, which has been extended for the XSCF SNMP agent.
- The Fault Management MIB, which has a format compatible with the Oracle Solaris OS.

They are used to manage the following information:

- Basic system information such as, serial number
- Different types of system status information (such as, operating status of a higher-level Oracle Solaris OS)
- Information on parts faults in the system

The following shows data as an example of MIB management information.

```
scfMachineType          OBJECT-TYPE
     SYNTAX                    DisplayString
     ACCESS                    read-only
     STATUS                    mandatory
     DESCRIPTION         "System model name and model type name."
     ::= { scfInfo 1 }

scfNumberOfCpu          OBJECT-TYPE
     SYNTAX                    INTEGER
     ACCESS                    read-only
     STATUS                    mandatory
     DESCRIPTION          "Number of CPUs"
     ::= { scfInfo 2 }

scfSysSerial            OBJECT-TYPE
     SYNTAX                    DisplayString
     ACCESS                    read-only
     STATUS                    mandatory
     DESCRIPTION          "System serial number"
     ::= { scfInfo 3 }
```

Note – This MIB data is provided as an example.

For a list from the extended MIB information supported by XSCF, see Appendix C.

Note – The contents of the MIB definition file are defined using the notations of the ASN1 standard.

The XSCF extension MIB definition file defines the administration information for the SNMP manager to monitor the M3000/M4000/M5000/M8000/M9000 servers. To perform server monitoring, install the XSCF extension MIB definition file to the SNMP manager. For the method of installation, see the manuals of the SNMP manager in use. For details on obtaining the XSCF extension MIB definition file and the Fault Management MIB definition file, see the Product Notes for your server or download site for firmware.

7.3 About Trap

When an event occurs, the SNMP agent function notifies the SNMP manager of the event. This function is called a Trap (see FIGURE 7-2). The XSCF Trap covers the following events:

1. XSCF failover
2. Additions, removals, and replacements of a component such as a system board
3. Part fault occurrences in the system, or replacement of a faulty component in the system and system recovery (see note)
4. Divided mode change of a system board
5. Hung domain or panicked domain
6. Configures an XSB into a domain or unassigns an XSB from domain
7. Additions and removals of an External I/O expansion unit (I/O box)
8. External I/O expansion unit LED state change
9. External I/O expansion unit temperature faults
10. XSCF SNMP agent function startup (Standard trap)
11. Occurrence of unauthorized access to the XSCF SNMP agent (Standard trap)
12. Cold start trap generated at changing in composition of managed object for when the SNMP agent starts up (Standard trap)

Note – In case 3 above, the target components are those whose fault location and part number can be identified from among the system components monitored by the XSCF. Even if the component cannot be identified, a Trap is issued during the XSCF event notification.

Note – For trap types, see the MIB definition file. For details on obtaining the XSCF extension MIB definition file and the Fault Management MIB definition file, see the Product Notes for your server or download site for firmware.

The following shows an example of the SNMP-trap when a part fault has occurred in the system.

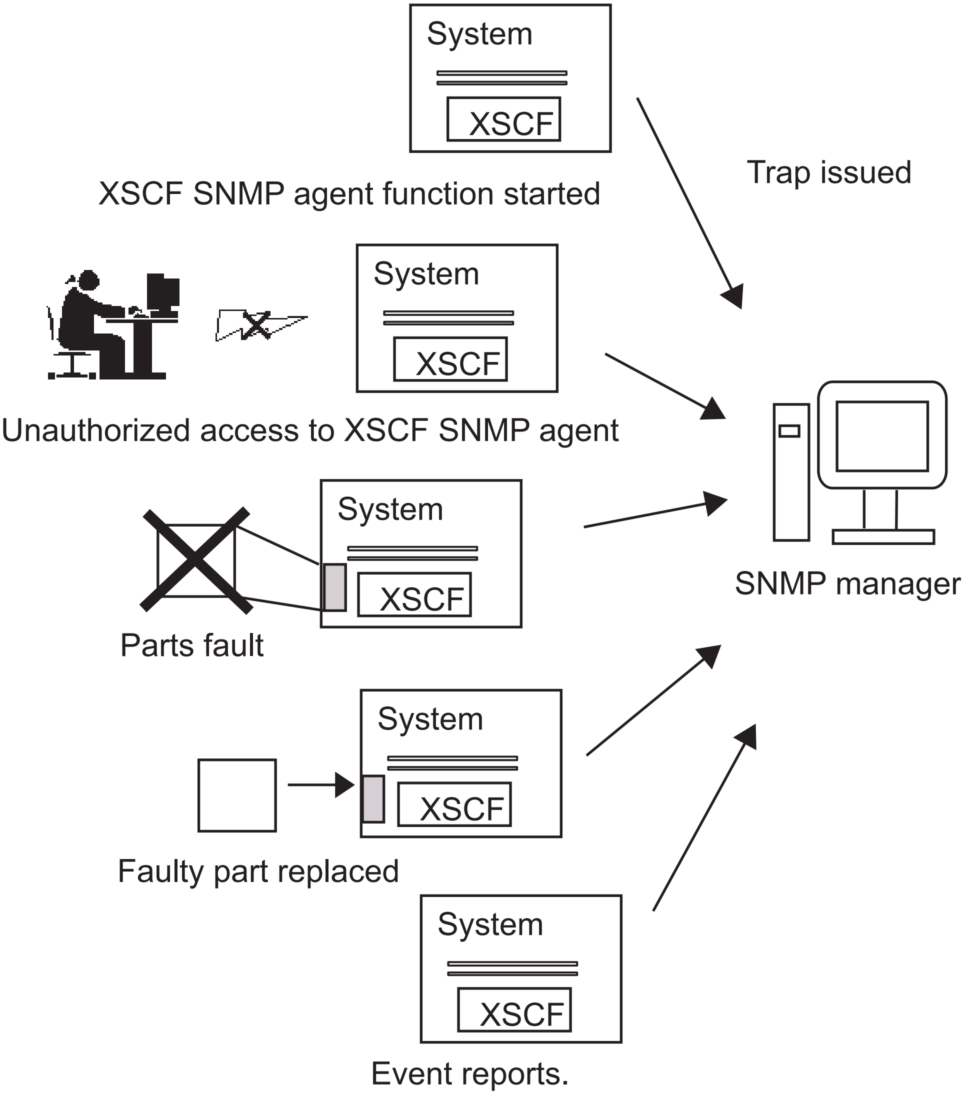
```
TRAP agent:10.123.223.18 community:- generic:6
enterprise:enterprises.42.2.195.1.7 specific:1 timestamp:754201501
varbind:(enterprises.42.2.195.1.1.1.2.36.51.101.49.52.53.52.53.50.45.54.53.52.
57.45.52.97.55.101.45.57.97.99.52.45.49.100.55.52.98.101.49.57.53.98.56.52 [2
36 0] 3e145452-6549-4a7e-9ac4-
1d74be195b84)(enterprises.42.2.195.1.1.1.3.36.51.101.49.52.53.52.53.50.45.54.5
3.52.57.45.52.97.55.101.45.57.97.99.52.45.49.100.55.52.98.101.49.57.53.98.56.5
2 [2 11 0] FMD-8000-
11)(enterprises.42.2.195.1.1.1.4.36.51.101.49.52.53.52.53.50.45.54.53.52.57.45
.52.97.55.101.45.57.97.99.52.45.49.100.55.52.98.101.49.57.53.98.56.52 [2 54 0]
http://xxxx.com/sparcenterprise/msg/FMD-8000-11)
```

In the example above, the following items are displayed:

- agent-address: The IP address of the XSCF which sent trap. (TRAP agent)
- community: Community string. (community)
- generic-trap-type: Standard Trap number. (generic)
- enterprise ID: The object ID which identifies equipment classification. (enterprise)
- specific-trap-type: Extension Trap number. (specific)
- time-stamp: Time of sending trap on the basis of a XSCF SNMP agent starting. [The unit is 10ms.] (timestamp)
- variable-bindings: Provides additional information about the trap. The UUID, MSG-ID, and message site might be included. For details about the UUID, MSG-ID, and message site, see Appendix B. (varbind)

FIGURE 7-2 is a conceptual diagram of issuance of a Trap.

FIGURE 7-2 Trap Issuance



7.4 Setting Up the XSCF SNMP Agent Function

This section explains how to set up the XSCF SNMP agent function.

The workflow is as described below. Perform each setup step with the `setsnmp`(8) command of the XSCF Shell. For details on setup, see Chapter 2.

Starting Transmission

- Step 1:

For setting items common to the agent protocols of SNMPv1, SNMPv2c, and SNMPv3, specify the management information listed below.

The following setting items are reflected in the MIB information:

  - Installation location of the agent system
  - Mail address of the administrator
  - Description of the agent system
  - Port number of the agent (listening port number)

- Step 2:

Specify the following management information for SNMPv3, SNMPv1, and SNMPv2c:

[SNMPv3 management information settings]

  - User name (Note)
  - Authentication password (Note)
  - Encryption password (Note)
  - Authentication algorithm
  - Port number of the trap destination
  - Host name of the trap destination

Note – A user name, authentication password, and encryption password that are common to both the sending and receiving sides must be set for SNMPv3.

[SNMPv1 and SNMPv2c management information settings]

  - Defined Trap type (specify v1, v2c, or inform <v2c in your response>)

- Community name
- Port number of the trap destination
- Host name of the trap destination

- Step 3:

Enable the XSCF SNMP agent function. Enable one or both of the following, according to the user environment:

- SNMPv1 and SNMPv2c
- SNMPv3

Note – All MIB information except the setting items in step 2 is initialized when the XSCF SNMP agent function is enabled.

Caution – IMPORTANT - Since SNMPv1 and SNMPv2c do not provide a capability to encrypt communication data, neither are secure enough. In SNMPv3, more secure transmission can be achieved through authentication and encryption settings on both the agent and manager sides. The server uses SNMPv3 as the default SNMP agent.

Suspending or Disabling Transmission

[Disabling the XSCF SNMP agent function]

Disable one or both of the following, according to the user environment:

- SNMPv1 and SNMPv2c
- SNMPv3

[Disabling sending to the target trap destination host for SNMPv3]

Specify the following to disable sending:

- User name
- Trap destination host

[Disabling sending to the target trap destination host for SNMPv1, SNMPv2c]

Specify the following to disable sending:

- Defined protocol type (v1/v2c)
- Trap destination host

Performing User Management (USM Management) and Management of the Access Control Views of the MIB Definition File (VACM Management)

- Step 1:

Set, change, and delete user management information by performing the following operations individually:

  - Specifying a user authentication algorithm
  - Setting authentication/encryption passwords for users
  - Changing authentication/encryption passwords for users
  - Copying a user
  - Deleting a user

- Step 2:

Add user accounts in and delete users from access control groups and provide access control views (MIB views) by performing the following operations individually:

  - Adding a user account to an access control group
  - Deleting a user from an access control group
  - Creating an MIB access control view
  - Deleting an MIB access control view
  - Providing an MIB access control view to a group
  - Deleting a group from all MIB access control views

Note – Perform USM management and VASM management for SNMPv3.

CHAPTER **8**

Upgrade of XSCF Firmware and Maintenance

This chapter explains how to update the firmware and how to collect log data.

8.1 Update the XSCF Firmware

This section explains firmware update functions and how to update the firmware. The firmware update work is performed by the system administrator or a field engineer.

8.1.1 Firmware Update Overview

The firmware programs listed below are updated by the firmware update.

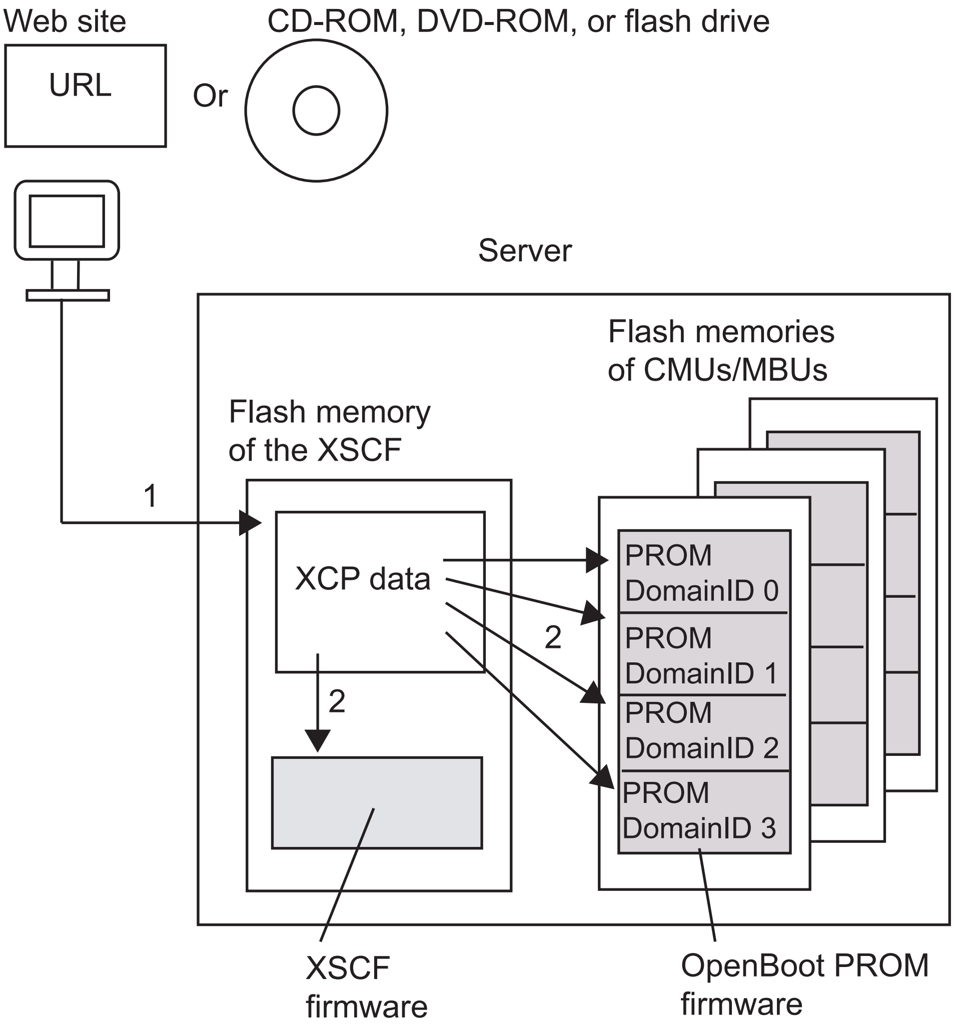
- POST and OpenBoot PROM firmwares (hereafter collectively called the OpenBoot PROM firmware)
- XSCF firmware

When updating the firmware, the new XCP firmware (see Note) is obtained from a web site (or from external media such as a CD-ROM disk) and downloaded to an arbitrary folder on a personal computer or workstation connected to the server. The firmware update sequence is: 1) XCP import in the system and 2) update.

Note – XCP: Abbreviation for the XSCF Control Package. XCP contains the control programs that configure a computing system. The XSCF firmware and the OpenBoot PROM firmware are included in the XCP file. The firmware update functions provided by XSCF are used to manage XCP.

FIGURE 8-1 is a conceptual diagram of the firmware update.

FIGURE 8-1 Conceptual Diagram of the Firmware Update



1. XCP import
2. Update (includes application of the XSCF firmware)

Note – The OpenBoot PROM firmware is applied by a domain reboot. In the M3000 server, this function updates the OpenBoot PROM firmware which is in the flash memory of the single MBU. And the number of domains to be updated is one.

User Interfaces

The following function is used for the firmware update:

- Firmware update using XSCF Web in a browser
  - XCP Import: Imports firmware to this system.
  - XCP Update: Updates the firmware to flash memory, applies the XSCF firmware, and the OpenBoot PROM firmware.
  - Version: Displays the firmware version.

Using the XSCF Web console, the user can easily update firmware from a browser. Also, regular maintenance and emergency firmware updates are supported. For the method of starting XSCF Web, see Chapter 9.

- Firmware update using the XSCF Shell

Use the following commands to update the firmware:

  - `getflashimage`(8) command: Imports firmware to this system.
  - `flashupdate`(8) command: Downloads the firmware to flash memory and applies the XSCF firmware.
  - `poweron`(8) command and `reset`(8) command: Applies the OpenBoot PROM firmware.
  - `version`(8) command: Displays the firmware version.

Note – For details on these four commands, see the man pages or the *XSCF Reference Manual*.

8.1.2 Firmware Update Conditions and Environment

User Privileges

The firmware update can be performed with either of the following two user privileges:

- platadm

- fieldeng

Firmware Update Environment

The following environment is required for the firmware to update properly:

- The update is performed from a browser connected to the XSCF-LAN.
- The update is performed after the domain console is switched to the XSCF Shell console.
- The update is performed with the maintenance terminal connected to the XSCF serial port or XSCF-LAN port.

8.1.3 Method of Delivering Firmware

Delivering the XCP Files

The XCP files are stored at the locations and in the format described below. After obtaining the XCP files, you can import XCP regardless of whether the operating system is running or stopped.

- At a web site
- Format: Compressed tar file (`tar.gz)` or Windows executable (`exe)`

Note – To obtain the URL of the Web site, see the description of the firmware download in the Product Notes for your server.

Note – When the operation is done by Service or Field Engineers (SEs/FEs), a CD-ROM, DVD-ROM, or flash drive may be used.

8.1.4 Method of Checking the Firmware Version

The firmware version for this system is called the XCP version. Higher version numbers represent newer firmware. Before updating the firmware, be sure to check the XCP version in the current system. The following example shows a command that displays the XCP version:

```
XSCF> version -c xcp
XSCF#0 (Active)
XCP0 (Current) : 1080
XCP1 (Reserve) : 1080
XSCF#1 (Standby)
XCP0 (Current) : 1080
XCP1 (Reserve) : 1080
```

The XCP version number appears as xyyz by four digits, where:

- x = Major firmware release number
- yy = Minor release number
- z = Micro release number

Note – Because micro release numbers may be updated more often than the documentation, the micro release number may appear in documents as a variable. An example might be XCP 108*x*.

The XSCF and OpenBoot PROM firmwares have different firmware version numbers. You can use the `version`(8) command or XSCF Web to display the XCP version for the system or the version of a firmware program.

In the flash memory of firmware, there are two bank fields: the current bank and the reserve bank. The firmware update is controlled by using these two banks. In the current bank, there is a firmware that the system is using now. The reserve bank is used to do the firmware update safely.

Note – To obtain the latest XCP information, see the Product Notes that apply to the firmware on your server, and those that apply to the latest firmware release.

8.1.5 Three Steps of the Firmware Update

The firmware update for the server has three steps (XCP import, update, application) as explained below.

1. **XCP import**

   Storing the obtained XCP data in this system is called "XCP import." The system administrator or a field engineer obtains the XCP data files from the network or external media (CD-ROM, DVD-ROM, or flash drive), then he or she imports the data file using an XSCF console from a client (personal computer or workstation) connected to the server.

   Simply importing XCP does not update the firmware that is running. Also, the XCP file is imported only by the versions number of one generation.

2. **Update**

   Writing the XSCF and OpenBoot PROM firmware programs that were imported in step 1 to flash memory in this system is called "update." Performing the download writes the XSCF firmware to the flash memory of the XSCF Unit, resets the XSCF, applies the XSCF firmware, and completes the firmware update. The OpenBoot PROM firmware is written to the flash memory on the system board. The OpenBoot PROM firmware is applied during a reboot.

Caution – IMPORTANT – Even if this system is divided into domains, the update is performed to newly write the OpenBoot PROM firmware to the flash memory on the XSB of every domain. However, unlike the XSCF firmware, just the download of this firmware does not update the OpenBoot PROM firmware that is running. To complete updating the OpenBoot PROM firmware in the target domain, the domain must be rebooted.

---

3. **Application**

   Making the firmware written to flash memory in this system actually usable is called "application."

Note – The number of domains that can be updated (application) is one or more. To apply the OpenBoot PROM firmware in the target domain, be sure to reboot the domain for firmware application.

Note – The update of the pool system board is completed at the following timing.
- Using DR functions, when you configure the board into a domain, the board is automatically matched to the version of target domain. After rebooting the target domain, the board is updated to new firmware version.
- If the board is assigned into a domain, after rebooting the target domain and the board is configured into the Oracle Solaris OS, then the board is updated to new firmware version.

8.1.6 Features of XSCF Firmware Update

The firmware update that is managed by XSCF has the following features:

- New firmware for a domain can be updated without stopping the domain. To update the OpenBoot PROM firmware, however, the target domain must be rebooted so that the firmware can be applied.
- When a component is replaced, the firmware is automatically updated. However, when a component is replaced in the state of input power off (The cold replacement), the firmware is not updated automatically.
- Even in a system consisting of multiple domains, firmware in a domain can be updated to the latest firmware without affecting the other domains.
- Even if an error occurs during the update operation, the firmware generation management mechanism (which retains spare firmware) can prevent firmware data destruction.

8.1.7 Firmware Update Types and Timing

The firmware update includes two types: operator's update and automatic update (automatic matching of versions). In the M3000 server, automatic update is not available, so the operator’s update is needed.

TABLE 8-1 describes the firmware update types and update times.

TABLE 8-1 Firmware Update Types and Timing

Type	Description	Conditions	Update Time
Operator's update (XCP update)	Imports XCP and updates the XSCF firmware and OpenBoot PROM firmware on the XSBs belonging to all domains (including pooled domains). This is also referred to as "XCP update."	The system power is off (input power is on and all domains are stopped), or power to the domains is on. Note: The update is completed at the time of a reboot for application in all domains.	XCP update time
Automatic update (Automatic matching of versions) Note: In the M3000 server, automatic update is not available.	• When a CPU/Memory Board unit (Note 1) is added or replaced, or the XSCF Unit is replaced, the firmware version of each replacement component is automatically matched to the version of the replaced component. (Note 2) However, when a component is replaced in the state of input power off (The cold replacement), the firmware is not updated automatically. • When the DR function is used to add, move, or replace a system board (XSB), the firmware version is automatically matched to the firmware version in the domain that uses the system board.	The system power is off (input power is on and all domains are stopped), or power to the domains is on. • In the system with redundant XSCF Units, If you replace an XSCF Unit by using the maintenance guidance, the firmware version of the replacement XSCF Unit is matched to the firmware version of the replaced XSCF Unit. • In CPU/Memory Board unit addition or replacement, the target domain need not be rebooted for application of the OpenBoot PROM firmware. However, when the domain is powered off, the number of versions is matched by the startup of the domain.	• Time of CPU/Memory Board unit addition or replacement. Or time of replacement of an XSCF Unit that is configured redundantly • Time of addition, move, or replacement of a system board by the DR function

Note – (1) Corresponds to a Motherboard unit in the M4000/M5000 servers. (The same is true for the description below.) Also, turn off the input power before replacing the Motherboard unit.

Note – (2) The replacement of the XSCF Unit and the version matching is performed by FEs. When both XSCF Units are replaced in the systems with redundant XSCF Units (the M8000/M9000 servers), or when in the M4000/M5000 servers, or when a Motherboard unit is replaced (an XSCF Unit is replaced) in the M3000 server, the firmware version cannot be automatically set to match the version of the replaced unit. Perform the operator's update for the XCP version.

8.1.8 Firmware Update for Redundant XSCF Units

In a system with redundant XSCF Units, you have only to connect to the XSCF Unit on the active side and update the firmware. The firmware upgrade is performed first on the XSCF Unit on the standby side and then on the active side automatically. Due to resetting the XSCF and switching the networks of the XSCF Units on the active and standby sides, the network is disconnected at this time. Therefore, the user must log in again. For details, see Section 8.1.10, “Firmware Update Procedure” on page 8-11

In a system with redundant XSCF Units, if the system is operating with only the active XSCF Unit, such as because of a failure, the update of all firmware is suppressed.

8.1.9 Ensuring Proper Operation After a Firmware Update

Supported Hardware

When an improvement is made to the hardware such as Motherboard unit, CPU/Memory Board unit, CPU module or XSCF Unit, the firmware update must be performed by using the XCP data which supporting the new hardware function.

See the latest version of the Product Notes for your server, for specific information about minimum softwares and firmware requirements, when new hardware is supported.

Note – If data for an older version of XCP is used for the firmware update of a system that is running, system operation cannot be guaranteed.

Making Versions Agree With Each Other

XSCF automatically sets firmware versions to match each other as follows:

- When power to a domain is turned on, the versions on the system boards in the domain are automatically set to match each other.
- When a system board is moved to a domain by the DR function, the version on the board is automatically matched to the version in the destination domain.
- When a maintenance component is replaced or added, the version is automatically matched to the version of the firmware currently running.

8.1.10 Firmware Update Procedure

TABLE 8-2 outlines the firmware update tasks. Detailed descriptions are provided at the link destinations of each task item.

Note – Depending on the XCP version and system configuration, firmware update procedures and requirements might be slightly different. For information about specific firmware update procedures and requirements, refer to the *Product Note* about your server.

TABLE 8-2 Firmware Update Tasks

Firmware Update Task Item	Outline	Task time
Updating XCP From the Network	Obtain the XCP files from the appropriate web site, and use XSCF to import XCP. Use XSCF Web or the XSCF Shell for the firmware update. Reboot the system for application to all domains. Note: If the system has redundant XSCF Units, the XSCF Units are switched while the update is in progress.	• In the system with a XSCF Unit; About 45 minutes • In the system with redundant XSCF Units; About 120 minutes (Excludes the time for component replacement work)
Updating XCP From External Media (When the XCP file is copied onto external media such as a CD-ROM.)	Imports XCP from the CD-ROM disk by using XSCF. Use the XSCF Web or the XSCF Shell for the firmware update. The rest of the task is the same as updating XCP from the network.	• In the system with a XSCF Unit; About 45 minutes • In the system with redundant XSCF Units; About 120 minutes (Excludes the time for component replacement work)
Confirming That the OpenBoot PROM Firmware is Updated When a CMU/MBU Is Added or Replaced	The firmware update is automatically performed. Confirm the version of the OpenBoot PROM firmware in the update target domain. This function is available when you are using the M4000/M5000/M8000/M9000 servers. In the M3000 server, when a Motherboard unit is replaced, the operator must match the number of the firmware versions.	About 5 minutes (Excludes the time for component replacement work)

TABLE 8-2 Firmware Update Tasks *(Continued)*

Firmware Update Task Item	Outline	Task time
Confirming That the XSCF Firmware is Updated When an XSCF Unit Is Replaced (There Are Redundant XSCF Units)	The firmware update is automatically performed by using the maintenance guidance for FE. Confirm the version of the updated XCP. This function is available when you are using M8000/M9000 servers. **Note:** When a component is replaced in the state of main line switch off (the cold replacement), the firmware is not updated automatically. The operator must match the number of the versions.	About 5 minutes (Excludes the time for component replacement work)
Confirming That the XSCF Firmware Is Updated When the XSCF Unit Is Replaced (in a System With a Single XSCF Unit or Both Replacement in a System With Redundant XSCF Units)	The firmware is not updated automatically. The operator must match the number of the firmware versions. This function is available when you are using M4000/M5000/M8000/M9000 servers.	• In the system with a XSCF Unit; about 20 minutes • In the system with redundant XSCF Units; about 40 minutes (Excludes the time for component replacement work)
Confirming That the XSCF Firmware Is Updated When the MBU Is Replaced (in the M3000 server)	The firmware is not updated automatically. The operator must match the number of OpenBoot PROM and XSCF firmware versions. This function is available when you are using M3000 servers.	About 20 minutes (Excludes the time for component replacement work)

Updating XCP From the Network

- File preparation:

1. **Download the XCP files from the web site to an arbitrary folder on a personal computer or workstation connected to the server.**

   In the web site, there will be the XCP file (the firmware program (`tar.gz`)), the MIB definition file, and a document concerning the XCP. There are three types of firmware program files (`tar.gz`) as described below:

   - The firmware program for M3000 servers (the file name begins with `IKXCP`).
   - The firmware program for M4000/M5000 servers (the file name begins with FFXCP).
   - The firmware program for M8000/M9000 servers (the file name begins with `DCXCP`).

   When you import the firmware (the XCP importing), choose the appropriate firmware program for your system.

2. **Confirm the XCP version.**

   To confirm the XCP version, see the figure of a four-digit number that exists in the firmware program (`tar.gz`) file name. The latest XCP information is released on a web site. To obtain the URL of the web site, see the description of the firmware download in the Product Notes for your server.

- Command operation

1. **Log in to XSCF Shell.**

2. **Import XCP.**

   a. **Use the** `getflashimage`**(8) command to confirm the list of the firmware program files (**`tar.gz`**) that are still on the system.**

```
XSCF> getflashimage -l
Existing versions:
        Version                Size  Date
        FFXCP1080.tar.gz   51298982  Thu Jan 15 20:09:09 JST 2009
```

   b. **Use the** `getflashimage`**(8) command to specify the firmware program (**`tar.gz`**) file and import XCP to the system.**
   (The update is not performed at this point.)

```
<Example> Login a remote ftp server specifying the user name and
host name that requires authentication password, then, import the
new 1082 version firmware program (tar.gz).

XSCF> getflashimage -u yyyyy ftp://imgserver/img/FFXCP1082.tar.gz
Existing versions:
        Version                Size  Date
        FFXCP1080.tar.gz   51298982  Thu Jan 15 20:09:09 JST 2009
Warning: About to delete old versions.
Continue? [y|n]: y
Removing FFXCP1080.tar.gz.
Password: [not echoed]
  0MB received
  1MB received
  2MB received
  ...
  40MB received
Download successful: 41470 Kbytes in 46 secs (940.250 Kbytes/sec)
MD5: 683fb5240e4937948dd6ad83b4a99669
```

c. **If complete message, "Download successful: ..." and "MD5: ..." are displayed, the XCP import has ended. Use the `getflashimage`(8) command with `-l` option to confirm the imported version.**

Note – After importing, if "Error: File is invalid or corrupt" message is displayed, it means the XCP file that imported is not a correct file. There is a possibility of either obtaining an illegal XCP file or that the XCP file was falsified by unauthorized access after the customer downloaded the XCP file.

---

3. **Perform the firmware update.**

   The XSCF firmware is downloaded and applied, and the OpenBoot PROM firmware is downloaded.

   a. **Use the `version`(8) command to display the current firmware version.**

```
XSCF> version -c xcp -v
XSCF#0 (Active)
XCP0 (Current): 1080
OpenBoot PROM : 02.07.0000
XSCF          : 01.08.0001
XCP1 (Reserve): 1010
OpenBoot PROM : 02.07.0000
XSCF          : 01.08.0001
OpenBoot PROM BACKUP
#0: 02.03.0000
#1: 02.07.0000
```

   b. **Use the `flashupdate`(8) command to confirm whether to be able to update the new firmware version. If the "XCP update is possible with domains up" message is displayed, you can update the firmware**

```
XSCF> flashupdate -c check -m xcp -s 1082
```

Note – If the XCP firmware version is 1050 or before, and if the "XCP update enabled during system powered on state" message is displayed, you can update the firmware.

Note – If the "XCP update requires all domains to be rebooted (Previous OpenBoot PROM update has not been completed)" message is displayed, you cannot update the firmware because previous OpenBoot PROM firmware update has not been completed. Perform the firmware update again after rebooting all domains.

c. **Use the** `flashupdate`**(8) command to update the firmware.**
In the system with redundant XSCF Units, before updating the firmware, perform the `showhardconf`**(8) command and check the Status of the XSCF Unit 0/1, which is Active or Standby.**

```
<Example> Update XCP from an early version, 1080, to the newer 1082 version.
XSCF> flashupdate -c update -m xcp -s 1082
The XSCF will be reset. Continue? [y|n] :y
XCP update is started (XCP version=1082:last version=1080)
OpenBoot PROM update is started (OpenBoot PROM version=02090000)
OpenBoot PROM update has been completed (OpenBoot PROM version=02090000)
XSCF update is started (XSCFU=0,bank=1,XCP version=1082:last version=1080)
XSCF download is started (XSCFU=0,bank=1,XCP version=1082:last
version=1080, Firmware Element ID=00:version=01080001:last version=01080000)
XSCF download has been completed (XSCFU=0,bank=1,XCP version=1082:last
version=1080, Firmware Element ID=00:version=01080001:last version=01080000)
...
XSCF download is started (XSCFU=0,bank=1,XCP version=1082:last
version=1080, Firmware Element ID=07:version=01080004:last version=01080000)
XSCF download has been completed (XSCFU=0,bank=1,XCP version=1082:last
version=1080, Firmware Element ID=07:version=01080004:last version=01080000)
XSCF update has been completed (XSCFU=0,bank=1,XCP version=1082:last
version=1080)
XCP update is started (XCP version=1082:last version=1080)
OpenBoot PROM update is started (OpenBoot PROM version=02090000)
OpenBoot PROM update has been completed (OpenBoot PROM version=02090000)
XSCF update is started (XSCFU=0,bank=0,XCP version=1082:last version=1080)
XSCF download is started (XSCFU=0,bank=0,XCP version=1082:last
version=1080, Firmware Element ID=00:version=01080001:last version=01080000)
XSCF download has been completed (XSCFU=0,bank=0,XCP version=1082:last
version=1080, Firmware Element ID=00:version=01080001:last version=01080000)
...
XSCF download is started (XSCFU=0,bank=0,XCP version=1082:last
version=1080, Firmware Element ID=07:version=01080004:last version=01080000)
XSCF download has been completed (XSCFU=0,bank=0,XCP version=1082:last
version=1080, Firmware Element ID=07:version=01080004:last version=01080000)
XSCF update has been completed (XSCFU=0,bank=0,XCP version=1082:last
version=1080)
XSCF is rebooting to update the reserve bank
```

Note – The display might be different according to XCP version and system configuration.

At this time, the XSCF will reset and the XSCF session will disconnect, so please connect the XSCF again. Only the application of the XSCF firmware is completed.

Note – The work described below applies to a system with redundant XSCF Units.

i) Before updating the firmware, perform the `showhardconf`(8) command and check the Status of the XSCF Unit 0/1, which is Active or Standby.

ii) Perform the firmware update in order, beginning with the standby side and then the active side automatically. After the update on the standby side is completed, the active and standby sides are switched. At this time, the XSCF reset is done and the XSCF session is disconnected.

iii) Re-connect the XSCF and log in again.

iv) XSCF firmware update is completed.

v) When the firmware update completes, the active and the standby states of the XSCF unit have become the opposite of original state. For instance, if the firmware update is executed on XSCFU#0, when completing the command, XSCFU#1 would become the active side. To switch the XSCF, execute the `switchscf` (8) command. To confirm the switching between XSCFs, execute the `showhardconf` (8) command and check the Status of the XSCF Unit 0/1, which is Active or Standby.
<Example>
XSCF> switchscf -t Standby
The XSCF unit switch between the Active and Standby states. Continue? [y|n] :y

d. **To confirm that the XSCF firmware update has finished, use the `showlogs`(8) command with the monitor option. Confirm no abnormality is found during the update. If the "XCP update has been completed" message is displayed in each XSCF Unit, the firmware update has completed.**

```
XSCF> showlogs monitor
:
Jun 20 07:25:48 FF1-1-0 monitor_msg: SCF:XCP update has been
completed (XCP version=1082)
```

4. **To complete the update of the OpenBoot PROM firmware, restart the domain.**

5. **Confirm that the version of the system firmware that is running is that of the firmware applied at the XSCF Shell command line by using the `version(8)` command.**

- Web browser operation

For information about using the XSCF Web, see Chapter 9.

1. **Start the XSCF Web.**

```
https://manual.host /(Specify the host name or IP address of XSCF)
```

2. **The login window of the XSCF Web console is displayed. Please enter an XSCF user account and password.**

3. **Select [Utility]-[Firmware Update] to display the menu.**

4. **Import XCP.**

   a. **Display the XCP import window.**

   b. **Following instructions in the window, specify the firmware program (`tar.gz`) file and import XCP to the system.**
   (The update is not performed at this point.)

5. **If complete message is displayed, the XCP importing has ended. Perform the firmware update.**

   The XSCF firmware is downloaded and applied, and the OpenBoot PROM firmware is downloaded.

   a. **Display the XCP update window. (The version of the imported XCP firmware and the version of the firmware currently running has already displayed in the screen.)**

   b. **Make a selection for the firmware version check. Confirm whether or not it is possible to update to the new firmware version.**

   c. **Make a selection for the firmware update. Following instructions in the window, update the firmware.**
   At this time, the XSCF will reset and the XSCF session will disconnect, so please connect the XSCF again. Only the application of the XSCF firmware is completed.

Note – In a system with redundant XSCF Units:

i) Perform the firmware update in order, beginning with the standby side and then the active side automatically. After the update on the standby side is completed, the active and standby sides are switched. At this time, the XSCF reset is done and the XSCF session is disconnected.

ii) Re-connect the XSCF and log in again.

iii) XSCF firmware update is completed.

iv) To switch the XSCF, select [Utility]-[Switch Over].

d. **Refer to the Monitor message log to confirm that the XSCF firmware update has finished.**

6. **To complete the update of the OpenBoot PROM firmware, restart the domain.**

7. **Confirm that the version of the system firmware that is running is that of the firmware applied from the XSCF Web console.**

Updating XCP From External Media

1. **Insert the external media with the XCP file into the drive. Insert the external media into a drive connected to the network that XSCF has access to. If necessary, copy the XCP file to an arbitrary folder.**

2. **Confirm the XCP version in the XCP file (tar.gz) of external media. The latest XCP information is released on external media or a web site. To obtain the URL of the web site, see the description of the firmware download in the Product Notes for your server.**

3. **Perform the same steps in** Updating XCP From the Network**.**

Confirming That the OpenBoot PROM Firmware is Updated When a CMU/MBU Is Added or Replaced

Note – This function is not available when you are using the M3000 server. When a MBU is replaced, you must match the number of the firmware versions. See Confirming That the XSCF Firmware Is Updated When the MBU Is Replaced (in the M3000 server)

1. **After a CMU/MBU addition or replacement task and an allocation to a domain have completed, turn on power to the domain. The update of the OpenBoot PROM firmware is automatically performed at this time (automatic matching of versions).**

2. **Confirm that the firmware version of the target domain agrees with the version of the XSB firmware allocated to the added or replacement CMU/MBU.**

- Command operation

   a. **Execute the** `version`**(8) command, and confirm it.**

```
XSCF> version -c cmu
DomainID  0: 02.09.0000
DomainID  1: 02.09.0000
        :
DomainID  3: 02.09.0000
```

- Web browser operation

   a. **Display the "Firmware Update" menu.**

   b. **Display the OpenBoot PROM firmware version, and confirm it.**

Confirming That the XSCF Firmware is Updated When an XSCF Unit Is Replaced (There Are Redundant XSCF Units)

a. Operation in State of the Input Power On

1. **After doing an XSCF Unit replacement task by using the maintenance guidance for FEs, the version of the XSCF firmware is automatically set to match the appropriate firmware.**

2. **Confirm the firmware version of replaced XSCF Unit.**

Note – When a component is replaced in the state of input power off (a cold replacement), the firmware is not updated automatically. The operator must match the number of versions.

---

b. Operation in State of the Input Power Off

The procedures below explain the firmware update when the replacement of one XSCF Unit is done. When you replace both XSCF Units, see "Confirming That the XSCF Firmware Is Updated When the XSCF Unit Is Replaced (in a System With a Single XSCF Unit or Both Replacement in a System With Redundant XSCF Units)".

- Command operation

1. **Turn on power to the server after completing XSCF Unit replacement task.**

2. **If the replacement unit and the replaced unit have different versions, a message is displayed such as the following.**

```
XCP version of Panel EEPROM and XSCF FMEM mismatched,

        Panel EEPROM=1080, XSCF FMEM=1090
```

3. **Confirm the firmware version by using the** `version`**(8) command. If you find an unmatched version of the replaced XSCF Unit, make the replaced XSCF unit version match the current system version using the** `flashupdate`**(8) command.**

```
XSCF> version -c xscf
XSCF#0 (Active )
01.08.0001(Reserve) 01.08.0001(Current)
XSCF#1 (Standby)
01.08.0001(Current) 01.08.0001(Reserve)
```

```
XSCF> flashupdate -c sync
```

4. **Confirm the firmware version again.**

Note – The sync option is only used at the active XSCF Unit. When the firmware on the standby site is applied, the XSCF reset of the standby site is done. Then even if the XSCF session is disconnected, the active XSCF Unit has no impact on.

- Web browser operation

1. **Repeat** Step 1 **and** Step 2 **of the** Command operation**. Then login to the XSCF on the XSCF Web.**

2. **Display the firmware update menu.**

3. **Display the XSCF firmware version, and confirm it.**

4. **If you find an unmatched version of the replaced XSCF Unit, select the XCP sync. In the window, match the version of the current firmware.**

5. **Display the XCP version and XSCF firmware version, and confirm them.**

Confirming That the XSCF Firmware Is Updated When the XSCF Unit Is Replaced (in a System With a Single XSCF Unit or Both Replacement in a System With Redundant XSCF Units)

1. **Turn on power to the server after completing the XSCF Unit replacement task.**

2. **If the replacement unit and the replaced unit have different versions, a message is displayed such as the following. In this case, the firmware is not updated automatically. The operator must perform a update to match the number of the firmware versions.**

```
XCP version of Panel EEPROM and XSCF FMEM mismatched,

        Panel EEPROM=1080, XSCF FMEM=1090
```

3. **When you update, follow the procedure in** Updating XCP From External Media **or** Updating XCP From the Network **to update XCP, and confirm the version.**

Confirming That the XSCF Firmware Is Updated When the MBU Is Replaced (in the M3000 server)

1. **Turn on power to the server after completing the Motherboard unit replacement task.**

2. **If the replacement unit and the replaced unit have different versions, a message is displayed such as the following. In this case, the firmware is not updated automatically. The operator must match the number of the firmware versions.**

```
XCP version of Panel EEPROM and XSCF FMEM mismatched,

        Panel EEPROM=1080, XSCF FMEM=1090
```

3. **When you update, follow the procedure in** Updating XCP From External Media **or** Updating XCP From the Network **to update XCP, and confirm the version.**

8.1.11 If an Error Occurs During XSCF Firmware Update

If the system hangs or any of the messages shown below is output during the firmware update, the XSCF Unit on the faulty side cannot be used and is treated as a faulty component.

Try the firmware update again when an error occurs while updating the XSCF firmware. The second attempt may succeed where the first failed.

- Case where the XSCF Unit is redundantly configured (on M8000/M9000 servers)

Error involving a failed write or reset operation on the standby or active side

- Case where there is one XSCF Unit (on M3000/M4000/M5000 servers)

Error involved a failed write or reset operation

8.1.12 Frequently Asked Questions

Q: Is there any problem in executing reboot twice when applying the OpenBoot PROM firmware?

> There is no problem.

Q: In cases with redundant XSCF Units, why are the XSCF Units on the active and standby sides switched while the update is in progress?

> XSCF on the active side has control for updating firmware on the XSCF Unit on the standby side. When the firmware update of the standby side is completed, the standby side that has new firmware is switched to the active side. Then, the firmware on the standby XSCF Unit (formerly the active XSCF Unit) is updated in turn.

Q: Can the update of the OpenBoot PROM firmware be applied to all domains at one time?

> Yes, it can. By specifying all domains in the `poweron`(8) command, the new firmware can be applied simultaneously to all the domains.

8.2 Collecting XSCF Logs

Log information for the XSCF firmware is used for investigating hardware or firmware faults. XSCF log information can be viewed by the system administrator, domain administrators, and FEs.

8.2.1 Log Types and Reference Commands

You can view XSCF log information from the XSCF console after logging in to XSCF. When the log archiving function is enabled, logs are stored on the archive host (see Section 8.2.2, "Method of Collecting the Log Information" on page 8-27). The logs include the following types:

- Logs containing fault information
- Other logs

Logs Containing Fault Information

If a failure occurs in the system, the system and XSCF collects some fault information logs. TABLE 8-3 lists the types of logs that are collected, descriptions, and reference methods. For details on commands, see the *XSCF Reference Manual* and the man page.

TABLE 8-3 Logs Containing Fault Information

Type	Description	Size (Entry Size)	Output/Display Destination (Standard Storage Period) Archiving	Reference Method
Fault management log (FM log)	Log for error events, notifications and faults occurred in server. The display form of the log is interchangeable *on the* Oracle Solaris OS.	About 200 generations (Variable-length)	Domain, XSCF (Amount for about 1 month) Archived (Note)	• `fmdump`(8) • `fmdump`(1M)
XSCF error log	Log for error events, notifications and faults occurred in server. Log information is the same as the FM log. The display form of the log is peculiar to the platform.	About 200 generations (Variable-length)	Domain, XSCF (Amount for about 1 month) Archived	• `showlogs`(8) • XSCF Web
System log	Log for recording output Oracle Solaris OS messages. If a failure occurs, an outline of the failure is output.		Domain	Oracle Solaris OS commands are used to refer to the logs.
Monitor message log	Log for recording messages, from the XSCF firmware, reporting abnormalities	512KB, About 10000 lines	XSCF	• `showlogs`(8) • XSCF Web

---

Note – Archived: Indicates log entries are replicated (backed up) on the archive host, if log archiving is enabled. The logs displayed by the Oracle Solaris OS commands are not archived.

Other Logs

TABLE 8-4 outlines other logs collected for XSCF log information.

TABLE 8-4 Other Logs

Type	Description	Size (Entry Size)	Standard Storage Period Archiving	Reference Method
Power log	Log for recording power events of the main unit	1920 generations (M8000/M9000 servers) 720 generations (M3000/M4000/ M5000 servers) (x16B)	About 1 month Archived	• showlogs(8) • XSCF Web
Event log	Log for recording system operations, operator panel operations, and events reported to the operating system	4096 generations (x48B)	About 1 month Archived	• showlogs(8) • XSCF Web
Console log	Log that is recorded as a console message log if the XSCF console is specified as the output destination of the Oracle Solaris OS console. When the input power is turned off, the log is clear.	512KB /domain, About 10000 lines/domain	Amount for about 1 week Archived	• showlogs(8) • XSCF Web
Panic log	Console log for a panic occurrence	64KB (About 1200 lines)	Amount for 1 time Archived	• showlogs(8) • XSCF Web
IPL log	Log for the period from power on to completion of Oracle Solaris OS startup	32KB/domain, About 600 lines/domain	Amount for 1 time Archived	• showlogs(8) • XSCF Web
Audit log	Log for XSCF audits	4MB	About 1 month Archived	• viewaudit(8) • XSCF Web
Active Directory log	Log for Active Directory authentication and authorization diagnostic messages	250KB (About 3000 lines)	Not Archived	• showad(8) • XSCF Web

TABLE 8-4 Other Logs *(Continued)*

Type	Description	Size (Entry Size)	Standard Storage Period Archiving	Reference Method
LDAP/SSL log	Log for LDAP/SSL authentication and authorization diagnostic messages	250KB (About 3000 lines)	Not Archived	• showldapssl(8) • XSCF Web
Temperature and humidity history log	Log containing a history of the temperature and humidity of the main unit environment The humidity history is displayed only in the high-end server.	16384 generations (x16B) (Every 10 minutes)	About 6 months Archived	• showlogs(8) • XSCF Web
COD activation log	Log for COD hardware activation permits additions and deletions.	1024 generations (x32KB)	Archived	• showcodactivationhistory(8) • XSCF Web

---

Note – The table is read in the same way as TABLE 8-3. For examples of logs, see Appendix B.

Note – When the log becomes full, the log data is overwritten, beginning with the oldest log.

8.2.2 Method of Collecting the Log Information

The field engineers and authorized service personnel collect the log information. Also, the system administrator might collect the log information.

To download the log information, execute the snapshot(8) command with some options in the XSCF Shell. When the command is executed, all XSCF log information is saved at the specified location.

Note – The download information by using the snapshot(8) command does not include log archives. The archived logs are stored on the archive host. The log archives can be accessed by logging in to the archive host.

The log can be saved in the device using one of the following two methods.

- The configuration information can be saved and restored when a USB device has been connected to the USB connector mounted on the XSCF Unit front panel of the M4000/M5000/M8000/M9000 servers or on the rear panel of the M3000 server.
- The log data is transmitted through the network with an encryption protocol.

Note – The USB device should only be formatted using the FAT32 file system. Please ask authorized service personnel about the USB capacity and the handling of USB devices.

Note – The `snapshot`(8) command can encrypt collected data by specifying an option. If you collect the data, be sure to ask the authorized service personnel to collect only the log file, the encryption information, and the method of sending the log file.

The following is the procedure for saving logs.

Saving the Logs by Connecting the USB Device for Exclusive Use to the Front Panel of the XSCF Unit

- Web browser operation

1. **Select the snapshot (Note) menu for saves of the logs menu and display the saving operation page.**
2. **Connect a USB device to the USB connector mounted on the XSCF Unit panel.**
3. **In the window, select the USB device on the XSCF Unit panel.**
4. **Set the encryption password used for encrypting the output log file.**
5. **Execute the data transfer. When the data transfer is complete, please contact authorized service personnel.**

Note – The snapshot menu may be displayed as "Data Collector".

- Command operation

1. **Connect a USB device to the USB connector mounted on the XSCF Unit panel.**
2. **Perform the** `snapshot`**(8) command and specify the local USB device on the XSCF Unit for the output file (see Note).**

```
XSCF> snapshot -d usb0
```

3. **When the data transfer is complete, please contact authorized service personnel.**

Note – For details on using the `snapshot(8)` command, including how to enable encryption, see the man page or the *XSCF Reference Manual*.

Saving the Logs to a Specified Target Directory Over a Network

- Web browser operation

1. **Select the snapshot menu for saving the log menu and display the saving operation page.**
2. **In the window, select the download button and specify the target directory.**

3. **Execute the data transfer. When the data transfer is complete, please contact authorized service personnel.**

   - Command operation

1. **Perform the** `snapshot`**(8) command using a public key, specifying the target directory, and specifying the encryption password for the output file.**

```
XSCF> snapshot -t joe@jupiter.west:/home/joe/logs/x
:
```

2. **When the data transfer is complete, please contact authorized service personnel.**

Note – For detail of `snapshot`(8) command, including how to enable encryption, see the man page or the *XSCF Reference Manual*.

Caution – IMPORTANT - When the XSCF Unit is the redundant configuration, log in to the standby side and collect the log in the same way.

The form of the collected log file is as follows.

File name : The file name is generated automatically at XSCF IP address and the log taking out time. So, the log file cannot be generated in the file name of the user specification.

File format : zip

CHAPTER 9

How to Use the XSCF Web

This chapter describes how to use the XSCF Web.

9.1 Overview of the XSCF Web

The XSCF Web uses https and the SSL/TLS protocols for connection to the server connected to a user network and for web-based support of server status display, server operation control, and configuration information display.

When a configured user establishes a connection with a web browser to the XSCF Web from a client terminal and logs in with an XSCF user account, either a tree index of available pages or another such page is displayed. Select the target page, such as the device status page. For details on creating the user account, see Chapter 2.

TABLE 9-1 outlines each page.

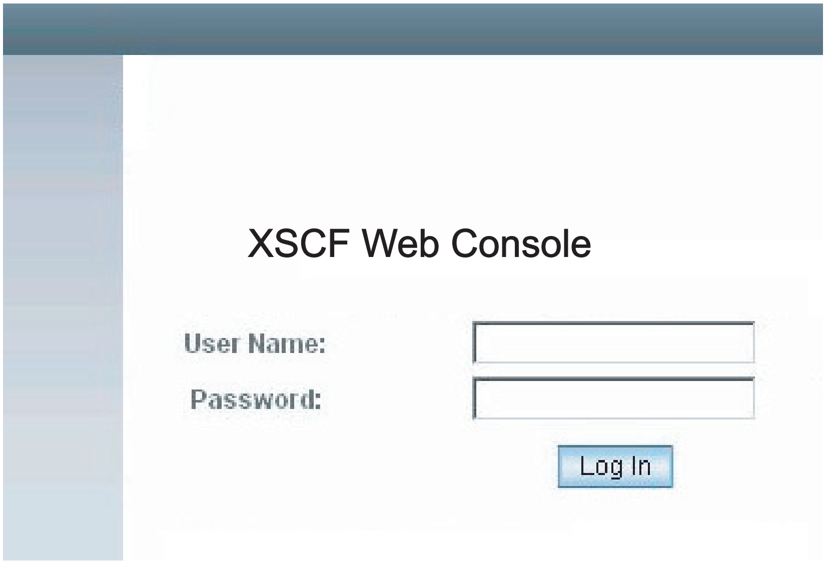
TABLE 9-1 XSCF Web Pages

Basic Page	Description
Login page	XSCF Web console login page. Log in with an XSCF user account from the login page.
Masthead frame	The page on the upper part of the screen. The masthead frame displays the user account name specified at login, the connected host name, and so on. When you log out from the masthead frame, you are returned to the login page.
Menu frame (Tree frame)	In the page displayed by default after login, there is a frame of the tree navigator to select each page. There are the following three kinds of tree navigators. - Menu; The menu of various settings, operations, and state displays that are displayed in the tree. - Physical; Physical components of the server are displayed in the tree - Logical; Logical components of each domain are displayed in the tree
Main page	A generic name of the detailed page located at the right of the screen. When you select an item from the menu in the tree frame, the target page is displayed here.
Event frame (Monitor message frame)	A page that displays the monitoring message located under the screen. Frame displaying the entire system events. As for the monitor message frame, the content of the display is regularly refreshed. An initial value at refreshing intervals is 60 seconds. You can change the interval value on the same frame.
Status display	Page displaying the status of the entire system and the domain status. The page display includes the External I/O expansion Unit status.
System/domain operation	Page for operations for the entire system and individual domains. When a setting item is selected by the menu, a target page is displayed. The pages include pages for power operations, domain configuration management, and DR operations.
XSCF settings	Pages for making XSCF operation settings. When a setting item is selected by the tree frame menu, a target page is displayed.
Utility pages	Pages such as firmware update, remote maintenance service, XSCF reset, and XSCF switch (M8000/M9000 servers only).
Log display	Page displaying logs. Error logs, power logs, event logs, console logs, and other logs are displayed.
Standby side page (M8000/M9000 servers only)	Page is displayed when you login to standby Unit. This page is included for XSCF switch and log collection.

The following figures show examples of these pages in a web browser.

FIGURE 9-1 shows an example of the Login page.

FIGURE 9-1 Example of the Login Page



XSCF Web Console

FIGURE 9-2 shows an example of the Tree frame.

FIGURE 9-2 Example of the Tree Frame

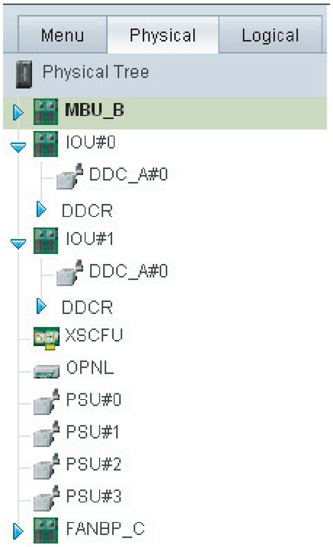
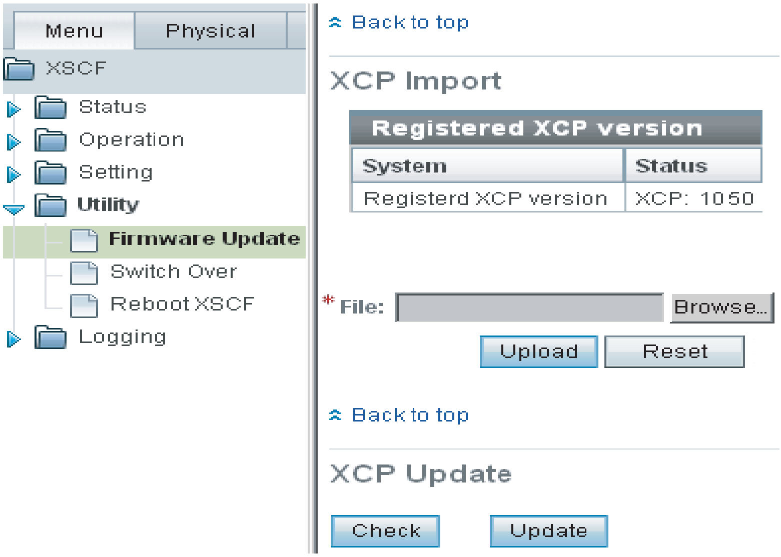


FIGURE 9-3 shows an example of the Tree frame and main page.

FIGURE 9-3 Example of the Tree Frame and Main Page



Registered XCP version

System	Status
Registerd XCP version	XCP: 1050

Note – Screen layouts and displays are provided as image examples, and they may be changed to improve functionality. The screen displays shown may also depend on the model and other conditions.

9.2 Start the XSCF Web

This section describes how to start the XSCF Web console with the XSCF Web. To use the XSCF Web, log in via an XSCF-LAN port. This connection cannot be established from a serial port.

Note – The browser window for the XSCF Web is called the XSCF Web console.

9.2.1 Prerequisites

Some settings are disabled in the initial settings of the XSCF Web. To use this function, advance configuration is required as follows:

- Create an XSCF user account.
- Enable https at the https setting to use the XSCF Web.
- Register the web server certificate at the https setting.
- Specify mail notification (recommended for failure notification).

For details on the settings, see Chapter 2.

9.2.2 Supported Browsers

TABLE 9-2 lists the web browsers supported by the XSCF Web. To use functions in any of the following web browsers, enable the appropriate settings.

TABLE 9-2 Supported Browsers

Browser	Version
Microsoft Internet Explorer	6.0 and later
Firefox (Oracle Solaris 10)	2.0 and later
Firefox (Oracle Solaris 11)	6.0 and later

The first firmware to support the newer entry-level server is the XCP 1080 firmware. For specific information about minimum OS and firmware requirements, see the latest version of the Product Notes (no earlier than the XCP 1080 edition) for your server.

9.2.3 Functions to be Enabled on the Browser

The following functions are necessary for the browser.

1. Secure Socket Layer Protocol (SSL) Ver. 3,
   Transport Layer Security (TLS) Ver. 1

2. JavaScript enabled

3. Cookies enabled for session management

9.2.4 Specifying the URL

When specifying the URL, specify the IP address configured with XSCF or the XSCF host name as the root directory.

Example: URL `https://192.168.111.111/` (Note: The IP address of XSCF is input by number)

Alternatively, `https://`*XSCF-host-name*`/` (Note: Not the host name of a domain)

Note – At the beginning of communication, the browser may request confirmation of a certificate. In such cases, check the contents, and accept the certificate.

9.3 Logging In and Out of the XSCF Web

This section describes how to connect the XSCF Web console.

9.3.1 Logging in to XSCF

The XSCF Web pages are connected by login from the top page. When login is successful, the default page is displayed. In the default page, the tree frame to select each page and one page are displayed.

If Authentication Fails

If login fails, a message indicating that login failed is displayed. Further, event and audit logs are collected.

9.3.2 Access Status Monitoring

The XSCF Web monitors the accounts of XSCF users logged in to XSCF. After successful login to XSCF, if no access is made for a certain period, an authentication timeout occurs and the XSCF Web logs out the user. If the XSCF Web is accessed after the authentication timeout, a dialog box indicating the timeout is displayed and then the top page is displayed. To use the XSCF Web again, log in to XSCF again.

The authentication timeout setting can be changed. The authentication timeout is 10 minutes by default. The monitoring interval ranges from 1 to 255 minutes. You can set the monitoring interval ranges at the [Menu]-[Settings]-[Autologout] page.

9.3.3 Logging Out From XSCF

To exit the XSCF Web, log out by selecting "logout" in the page on XSCF Web console.

9.4 XSCF Web Pages

This section describes the configuration of pages available with the XSCF Web console.

Menu and page configuration are described below.

• Menu tree + XSCF + Status - System Status - Domain Status - Device Status + Operation + Domain Operation - Domain Power - Domain Mode Configuration + Domain Configuration - System Board Configuration - Domain Configuration + Settings + Network - Current - Reserve - Time - SSH/Telnet - LDAP - LDAP/SSL - Active Directory - User Manager - Audit - SMTP - Email Reporting - SNMP - SNMP Security - Log Archives - Capacity on Demand - Sun MC - Autologout	When you select an item on the menu, the target page is displayed on the main page. Pages, which are the system/domain state display, the system/domain operation, the XSCF configuration, firmware update, and log display, are provided. Also, the page for switching XSCF is included on the M8000/M9000 servers only. For information about the function of the target page, see TABLE 9-3 or later.

(Continued)

```
 + Utility
  - Firmware Update
  - Switch Over
  - Reboot XSCF
 + Logs
  - Error Log
  - Power Log
  - Event Log
  - Console Log
  - Panic Log
  - Environment Log
  - IPL Message Log
  - Monitor Message Log
  - Audit Log
  - Active Directory Log
  - LDAP/SSL Log
  - Snapshot (or Data Collector)
  - COD Activation History
```

• Physical tree + Physical components in the server	When you select each component, the component information and the state are displayed in the main page.

• Logical tree + Logical components that belong to each domain	When you select each component, the logical component and the state that belongs to each domain is displayed.

Note – Menu items may be changed to improve functionality. The menu displays shown below may also depend on the model and other conditions.

Page configuration is described below. Each function provides the same results as those of the corresponding XSCF Shell command. For details on the functions, see Chapter 2 and Chapter 5.

Displaying System Status

TABLE 9-3 lists the functions for displaying the status of the entire system. Select [Status]-[System Status] in the Menu tree.

TABLE 9-3 System Status Display

Function	**Remarks**
Mode switch display	Displays the mode switch status of the operator panel. This function is equivalent to the `showhardconf`(8) command.
System time display	This function is equivalent to the `showdate`(8) command.
Failure component display	This function is equivalent to the `showstatus`(8) command.
Displaying temperature and humidity information	This function is equivalent to the `showenvironment`(8) command. The humidity is displayed for the M8000/M9000 servers.
Displaying air flow information	This function is equivalent to the `showenvironment`(8) command.
Displaying temperature, voltage, power consumption, and fan information	Displays the exhaust temperature, voltage value, and fan speed of each component. Also, displays the power consumption of server. The power consumption is displayed for the M3000 server. This function is equivalent to the `showenvironment`(8) command.

TABLE 9-4 lists the functions for displaying the status of a domain. Select [Status]-[Domain Status] in the Menu tree.

TABLE 9-4 Domain Status Display

Function	Remarks
Domain configuration information display	Displays the XSB number corresponding to each LSB number of each domain in the form of a table. **Note -** In the M3000 server, this function does not display the table of the corresponding XSB and LSB, but displays the detail information which is displayed with the domain status display function and the XSB information display function.
Domain status display	Configuration policy and domain power status are displayed. This function is equivalent to the `showdcl`(8) command.
XSB information display	XSB status is displayed. This function is equivalent to the `showdcl`(8), `showboards`(8), and `showstatus`(8) commands.

TABLE 9-5 lists the function for displaying the status of CPU, memory, and I/O devices in each XSB. Select [Status]-[Device Status] in the Menu tree.

TABLE 9-5 Device Status Display

Function	Remarks
CPU status display	Displays the CPU status corresponding to a specified XSB number or Domain ID. This function is equivalent to the `showdevices`(8) command.
Memory information display	Displays the memory information corresponding to a specified XSB number or Domain ID. This function is equivalent to the `showdevices`(8) command.
I/O device information display	Displays the I/O device information corresponding to a specified XSB number or Domain ID. This function is equivalent to the `showdevices`(8) command.

Note – In the M3000 server, this function displays the device information corresponding to Domain ID 0 and XSB 00-0.

System and Domain Operation

TABLE 9-6 lists the function used for the system as a whole and individual domains. Select [Operation]-[Domain Operation]-[Domain Power] in the Menu tree.

TABLE 9-6 System and Domain Operation

Function	Remarks
System power on/off	Specifies the system power on/off. This function is equivalent to the `poweron`(8) / `poweroff`(8) commands.
Domain power-on/off	Specifies the domain power on/off. This function is equivalent to the `poweron`(8) / `poweroff`(8) commands.
Reset	System reset, XIR reset and panic for the domain are performed. This function is equivalent to the `reset`(8) command.
Send break	Specifies the send break. This function is equivalent to the `sendbreak`(8) command.

Note – In the M3000 server, the number of the target domain is one. Domain ID is fixed to 00.

TABLE 9-7 lists the functions used for specifying each domain mode. Select [Operation]-[Domain Operation]-[Domain Mode Configuration] in the Menu tree.

TABLE 9-7 Domain Mode Configuration

Function	Remarks
Domain mode configuration/display	Sets a hardware initial diagnostic level. Suppresses the send break, Host watchdog, and automatic boot functions. Also, displays the host ID, the domain mode status, and domain ethernet address (mac address). This function is equivalent to the `setdomainmode`(8) and `showdomainmode`(8) commands. On the XSCF Web, you cannot display/configure the CPU operational mode. Use the `showdomainmode`(8) and `setdomainmode`(8) commands.

TABLE 9-8 lists the functions used for System board configuration. Select [Operation]-[Domain Configuration]-[System Board Configuration] in the Menu tree.

TABLE 9-8 System Board Configuration

Function	Remarks
System board configuration information display	Displays the XSB division information, the XSB number, and the memory mirror information for each PSB in the form of table. **Note -** The M3000 server does not display the system board configuration, but displays the detail information in the system board detail display.
System board detail display	Displays the PSB and the XSB on the PSB detail information. This function is equivalent to the `showfru`(8), `showhardconf`(8), and `showboards`(8) commands.
XSB division / memory mirroring configuration	Divides a PSB into XSBs and sets the memory mirror mode. This function is equivalent to the `setupfru`(8) command. Note - In the M3000 server, this function is not available.

TABLE 9-9 lists the functions for the domain configuration. Select [Operation]-[Domain Configuration]-[Domain Configuration] in the Menu tree.

TABLE 9-9 Domain Configuration

Function	**Remarks**
Domain configuration information display (DCL)	Displays the DCL information for a system board in the specified domain, and sets the configuration policy for the domain. These functions are equivalent to the `showdcl`(8)and `setdcl`(8) commands. In the M3000 server, the information for domain ID 0 is displayed and only the configuration policy can be set.
Configure the DCL information	Sets the DCL information. Specify configuration for the LSB of a specified domain. This function is equivalent to the `setdcl`(8) command. For detail of configuration information, see TABLE 2-26. In the M3000 server, this function is not available.
XSB addition, deletion, and movement	Specifies the XSB configuration modification to the domain as below. • Assign or configure a system board to a domain • Delete a system board from a domain • Move a system board form one domain to another These functions are equivalent to the `addboard`(8), `deleteboard`(8), `and moveboard`(8) commands. Please operate as well as the procedure in Section 2.2.13, "Domain Configuration" on page 2-146. When you use the DR function, also run the procedure in the *Dynamic Reconfiguration User's Guide.* In the M3000 server, this function is not available.

Setting System

TABLE 9-10 lists the functions for the network configuration of XSCF. Select [Settings]-[Network]-[Current] or [Settings]-[Network]-[Reserve] in the Menu tree. You can make the network configuration from both [Current] and [Reserve] menus. The [Current] menu displays the XSCF network information which is running on the server, and the [Reserve] menu can be used to confirm the data you configured. Click the [Apply] and [Reboot] buttons on the [Reserve] menu to apply the setting values of network configuration.

TABLE 9-10 Network Configuration *(1 of 2)*

Menu	Function	Remarks
Current	XSCF network information and status display, and XSCF network configuration	Displays the XSCF network information and status which is running on the server. This function is equivalent to the `shownetwork`(8) and `showhostname`(8) commands. Also, this function sets each host name, domain name, IP address, netmask, and enabling/disabling of the XSCF network interface. This function is equivalent to the `setnetwork`(8) and `sethostname`(8) commands. You can confirm the settings from the [Reserve] menu.
	Route display and configuration	Displays the current routing, and configures the routing. This function is equivalent to the `showroute`(8) and `setroute`(8) commands. You can confirm the settings from the [Reserve] menu.
	DNS display and configuration	Displays the current name server and search path, and configures the name server and the search path. This function is equivalent to the `shownameserver`(8) and `setnameserver`(8) commands. You can confirm the settings from the [Reserve] menu.

TABLE 9-10 Network Configuration *(2 of 2)*

Menu	Function	Remarks
Reserve	XSCF network configuration information display and configuration	Displays the XSCF network configuration information. This function is equivalent to the `applynetwork`(8) command. Also, this function sets each host name, domain name, IP address, netmask, and enabling/disabling of the XSCF network interface. This function is equivalent to the `setnetwork`(8) and `sethostname`(8) commands.
	Route configuration information display and configuration	Displays the route configuration information. This function is equivalent to the `applynetwork`(8) command. Also, this function configures the routing. This function is equivalent to the `setroute`(8) command.
	DNS configuration information display and configuration	Displays the name server and the search path configuration information. This function is equivalent to the `applynetwork`(8) command. Also, this function configures the name server and the search path. This function is equivalent to the `setnameserver`(8) command.
	Apply network settings	Displays and applies the network settings. This function is equivalent to the `applynetwork`(8) command. After saving the settings, to complete the settings, XSCF reset is required. This function is equivalent to the `rebootxscf`(8) command.

Note – The [Current] and [Reserve] menus are supported in XCP1090 or later.

Note – The DSCP link address cannot be set and displayed through the XSCF Web. Set and display the address by using the `setdscp`(8) and `showdscp`(8) commands.

Note – The IP packet filtering rules cannot be set and displayed through the XSCF Web. Set and display the filtering rules by using the `setpacketfilters`(8) and `showpacketfilters`(8) commands.

TABLE 9-11 lists the functions for setting the XSCF time. Select [Settings]-[Time] in the Menu tree.

TABLE 9-11 Time Settings

Function	Remarks
System time display and setting	Displays and sets the current system time. This function is equivalent to the applynetwork(8) and rebootxscf(8) commands. After setting, the XSCF is reset
NTP server display and configuration	Displays and sets the NTP server used on the XSCF network, the preferred server, the stratum value, and the XSCF's own local clock. These function are equivalent to the showntp(8) and setntp(8) commands. Reset XSCF to complete the settings.

TABLE 9-12 lists the functions for setting the SSH/telnet. Select [Settings]-[SSH/Telnet] in the Menu tree.

TABLE 9-12 SSH/telnet Settings

Function	Remarks
SSH Enabling and disabling	Displays and sets the enabling/disabling the SSH. These function are equivalent to the showssh(8) and setssh(8) commands. After enabling SSH, the XSCF reset is required.
Access control from domain to the SSH	Specifies whether or not to permit access from domain to the SSH via the DSCP. These function are equivalent to the showssh(8) and setssh(8) commands. After setting the SSH access control, the XSCF reset is required.
telnet Enabling and disabling	Displays and sets the enabling/disabling of telnet. These function are equivalent to the showtelnet(8) and settelnet(8) commands. After disabling telnet, XSCF reset is required.

Note – The host key generation, the user public key registration/deletion, and the timeout period setting for XSCF Shell are not supported by XSCF Web. Set these functions by using XSCF Shell.

TABLE 9-13 lists the functions for configuring LDAP. Select [Settings]-[LDAP] in the Menu tree.

TABLE 9-13 LDAP Configuration

Function	Remarks
LDAP server display and registration	Displays and configures the LDAP server when XSCF is as an LDAP client. This function is equivalent to the `showldap`(8) and `setldap`(8) commands.
Certificate display and importation	Displays and import an LDAP server certificate. This function is equivalent to the `showldap`(8) and `setldap`(8) commands.

Note – In the setting of the LDAP server, on XSCF Web, you can enter up to 128 characters. To set 129 characters or more, use XSCF Shell.

TABLE 9-14 lists the functions for configuring LDAP/SSL. Select [Settings]-[LDAP/SSL] in the Menu tree.

TABLE 9-14 LDAP/SSL Configuration

Function	Remarks
LDAP/SSL server display and configuration	When XSCF is as an LDAP/SSL client, enable and disable the LDAP/SSL. Displays and configures an LDAP/SSL server, modes, timeout piriod, log, default settings, and so on. This function is equivalent to the `showldapssl`(8) and `setldapssl`(8) commands.
User map display and configuration	Displays and configures a user map. This function is equivalent to the `showldapssl`(8) and `setldapssl`(8) commands.
Certificate display and configuration	Displays, loads, and removes an LDAP/SSL server certificate. This function is equivalent to the `showldapssl`(8) and `setldapssl`(8) commands.
Defaultrole display and configuration	Displays and configures privileges for all users authenticated via LDAP/SSL. This function is equivalent to the `showldapssl`(8) and `setldapssl`(8) commands.
Alternative servers display and configuration	Displays and configures up to five alternate LDAP/SSL servers. This function is equivalent to the `showldapssl`(8) and `setldapssl`(8) commands.
Groups display and configuration	Displays and configures administrator groups, operator groups, and custom groups. This function is equivalent to the `showldapssl`(8) and `setldapssl`(8) commands.
Userdomain display and configuration	Displays and configures up to five user domains. This function is equivalent to the `showldapssl`(8) and `setldapssl`(8) commands.

TABLE 9-15 lists the functions for configuring Active Directory. Select [Settings]-[Active Directory] in the Menu tree.

TABLE 9-15 Active Directory Configuration

Function	Remarks
Active Directory server display and configuration	When XSCF is as an Active Directory client, enable and disable the Active Directory. Displays and configures an Active Directory server, modes, timeout piriod, log, default settings, and so on. This function is equivalent to the showad(8) and setad(8) commands.
Certificate display and configuration	Displays, loads, and removes an Active Directory server certificate. This function is equivalent to the showad(8) and setad(8) commands.
Defaultrole display and configuration	Displays and configures privileges for all users authenticated via Active Directory. This function is equivalent to the showad(8) and setad(8) commands.
Alternative servers display and configuration	Displays and configures up to five alternate Active Directory servers. This function is equivalent to the showad(8) and setad(8) commands.
Groups display and configuration	Displays and configures administrator groups, operator groups, and custom groups. This function is equivalent to the showad(8) and setad(8) commands.
Userdomain display and configuration	Displays and configures up to five user domains. This function is equivalent to the showad(8) and setad(8) commands.
DNS locator query display and configuration	Displays and configures up to five DNS locator query. This function is equivalent to the showad(8) and setad(8) commands.

TABLE 9-16 lists the functions for configuring XSCF user management. Select [Settings]-[User Manager] in the Menu tree.

TABLE 9-16 User Management Configuration

Function	Remarks
User accounts list display	Displays user accounts information and the state being registered now. The useradm privilege is required. This function is equivalent to the `showuser`(8) command.
User accounts addition and deletion	Adds and deletes a user account. The useradm privilege is required. These functions are equivalent to the `adduser`(8) and `deleteuser`(8) commands.
Enabling/disabling user accounts	Enable and disable a user account. The useradm privilege is required. These functions are equivalent to the `enableuser`(8) and `disableuser`(8) commands.
User accounts information display and change	Displays a user account information and changes the password, privilege, password policy. The useradm privilege is required. These function are equivalent to the `password`(8), `setprivileges`(8), and `setpasswordpolicy`(8) commands.
Your own account information display and password change	Displays information of your own account without the useradm privilege and changes the password. These functions are equivalent to the `showuser`(8) and `password`(8) commands.
Password policy display and setting	Display the current system password policy. And set the password policy that will be applied now. These function are equivalent to the `showpasswordpolicy`(8) and `setpasswordpolicy`(8) commands.
Privileges for remote user account settings	Change the privilege for a user account that is defined in an LDAP repository. This function is equivalent to the `setprivileges`(8) command.

Note – The login lockout function is not supported by XSCF Web. Set the function by using `setloginlockout`(8) and `showloginlockout`(8) commands.

TABLE 9-17 lists the functions for configuring XSCF audit. Select [Settings]-[Audit] in the Menu tree.

TABLE 9-17 Audit Configuration

Function	Remarks
Audit enabling and disabling	Enable and disable the auditing. This function is equivalent to the `setaudit`(8) command.
Request the archive and data deletion	Request the log archive for the audit trail. Also delete the audit trail in the secondary partition. This function is equivalent to the `setaudit`(8) command.
Audit policy display and setting	Display and specify the policy, such as when an audit trail becomes full, the local audit file usage threshold (%) that triggers an alarm when reached, the destination address for that alarm. This function is equivalent to the `setaudit`(8) command.
Audit event/class display and setting	Display the audit events and the audit classes. Also, Enable and disable the audit events and the audit classes. This function is equivalent to the `setaudit`(8) command.

TABLE 9-18 lists the functions for configuring XSCF mail. This page provides the SMTP server settings. Select [Settings]-[SMTP] in the Menu tree.

TABLE 9-18 Mail Configuration (SMTP)

Function	Remarks
SMTP server display and configuration	Displays SMTP server setting information. Sets the host name and the port number of the SMTP server. These functions are equivalent to the `showamtp`(8) and `setsmtp`(8) commands.
Authentication server display and configuration	When you enable the Authentication, displays and specifies the authentication mechanism and authentication server. These functions are equivalent to the `showsmtp`(8) and `setsmtp`(8) commands.
Reply address server display and setting	Displays and specifies the recipient address for error mail. These functions are equivalent to the `showsmtp`(8) and `setsmtp`(8) commands.

TABLE 9-19 lists the functions for configuring XSCF mail. This page provides the email report settings. Select [Settings]-[Email Reporting] in the Menu tree.

TABLE 9-19 Mail Configuration (Email Reporting)

Function	Remarks
Mail notification function display and configuration	Displays and sets the mail report function. Enables or disables the mail report function, and displays and specifies the recipient address to be sent to the system administrator. These functions are equivalent to the `showemailreport`(8) and `setemailreport`(8) commands.

TABLE 9-20 lists the functions for configuring SNMP for XSCF. This page provides the SNMPv1v2c and SNMPv3 settings. Select [Settings]-[SNMP] in the Menu tree.

TABLE 9-20 SNMP Configuration

Function	Remarks
Agent display and configuration	Enables and disables the SNMPv1v2c or SNMPv3 agent, sets the system management information, and selects the MIB module. This functions is equivalent to the `showsnmp`(8) and `setsnmp`(8) commands.
Notification destination server display and setting	Displays and sets the trap host for SNMPv1v2c or SNMPv3. This functions is equivalent to the `showsnmp`(8) and `setsnmp`(8) commands

TABLE 9-21 lists the functions for configuring security access for SNMPv3. Select [Settings]-[SNMP Security] in the Menu tree.

TABLE 9-21 SNMP Configuration (Security Access)

Function	Remarks
USM management information display and setting	Displays and sets the USM management information for SNMPv3. This function is equivalent to the `showsnmpusm`(8) and `setsnmpusm`(8) commands. For details of the USM management, see TABLE 2-21.
VACM management information display and setting	Displays and sets the VACM management information for SNMPv3. This functions is equivalent to the `showsnmpvacm`(8) and `setsnmpvacm`(8) commands. For detail of VACM management information, see TABLE 2-21.

TABLE 9-22 lists the functions for configuring Log archiving for XSCF. Select [Setting]-[Log Archives] in the Menu tree.

TABLE 9-22 Log Archiving Configuration

Function	Remarks
Log archiving display and configuration	Displays and sets the archiving host to save the XSCF log information, enabling and disabling log archiving, and the log capacity limits. These functions are equivalent to the `showlogarchiving`(8) and `setlogarchiving`(8) commands.
Host public key setting	Sets a public key used in server authentication for the archive host. This function is equivalent to the `setlogarchiving`(8) command.

Select [Setting]-[Capacity on Demand] in the Menu tree for configuring COD. The following functions are supported.

- COD resource use status display and headroom configuration
- COD management information for each domain's display and setting
- COD hardware activation permit (COD permit) information display, and COD hardware activation key (COD key) addition and deletion

For COD settings and command information, see the *COD User's Guide* and the *XSCF Reference Manual*.

Note – In the M3000 server, this function is not available.

TABLE 9-23 lists the functions for configuring Sun Management Center agent. Select [Setting]-[Sun MC] in the Menu tree.

TABLE 9-23 Sun Management Center Agent Configuration

Function	Remarks
Sun Management Center Agent Configuration	Displays setup information and status of Sun Management Center agent. Start or stop the Sun Management Center agent and make changes to its configuration. These functions are equivalent to the `showsunmc`(8) and `setsunmc`(8) commands.

TABLE 9-24 lists the functions for configuring the authentication timeout period for XSCF Web console. Select [Settings]-[Autologout] in the Menu tree.

TABLE 9-24 Auto Logout Configuration (XSCF Web)

Function	Remarks
Timeout period display and configuration	After logging in XSCF, if the system is not used for a certain period, logout is automatically performed. Displays and specifies the timeout period in minutes. The authentication timeout is 10 minutes by default. The monitoring interval ranges from 1 to 255 minutes.

Utility

The Pages of Utility include remote maintenance service, firmware update, XSCF reset, and XSCF switch (M8000/M9000 servers only).

Note – This document does not provide details on the function of the remote maintenance service. For information of the remote maintenance service, see the Product Notes for your server.

TABLE 9-25 lists the functions for the firmware update. Select [Utility]-[Firmware Update] in the Menu tree.

TABLE 9-25 Firmware Updating

Function	Remarks
XCP version display	Displays the XCP version. This function is equivalent to the `version`(8) command.
XSCF/OpenBoot PROM version display	Displays the XSCF firmware and the OpenBoot PROM firmware versions. This function is equivalent to the `version`(8) command.
XCP importing	Import the XCP file into the server. This function is equivalent to the `getflashimage(8)` command.
Firmware update	Update the firmwares of XCP. This function is equivalent to the `flashupdate`(8) command.
Version matching (M8000/M9000 servers only)	Match the firmware versions of the two XSCF Units. This is done when the XSCF Unit is replaced. This function is equivalent to the `flashupdate`(8) command.

To switch the XSCF, select [Utility]-[Switch Over] in the menu tree. This function is equivalent to the `switchscf`(8) command. This function is available in the M8000/M9000 servers only. On the page which is displayed after you log in to the standby XSCF Unit, you can perform operations such as XSCF switching and log collection.

To reset the XSCF, select [Utility]-[Reboot XSCF] in the menu tree. This function is equivalent to the `rebootxcf`(8) command.

Logs

TABLE 9-26 lists the functions for referring and saving each log. Select [Logs] in the Menu Tree, and select a target log.

TABLE 9-26 Log Collection

Function	Remarks
Error log display	Display the error log. Also, you can search the logs. This function is equivalent to the error option of the showlogs(8) command.
Power log display	Display the power log. Also, you can search the logs. This function is equivalent to the power option of the showlogs(8) command.
Event log display	Display the event log. Also, you can search the logs. This function is equivalent to the event option of the showlogs(8) command.
Console log display	Display the console log. This function is equivalent to the console option of the showlogs(8) command.
Panic log display	Display the panic log. This function is equivalent to the panic option of the showlogs(8) command.
Temperature and humidity history log display (Environment Log)	Display temperature and humidity history log in the server environment. Also, you can search the logs. This function is equivalent to the env option of the showlogs(8) command. The humidity history is displayed only in M8000/M9000 servers.
IPL message log display	Display the IPL message log. This function is equivalent to the ipl option of the showlogs(8) command.
Monitor message log display	Display the monitor message log. This function is equivalent to the monitor option of the showlogs(8) command.
Audit log display	Display the audit log. This function is equivalent to the viewaudit(8) command.
Active Directory log display	Display the Active Directory log. This function is equivalent to the log option of the showad(8) command.

TABLE 9-26 Log Collection *(Continued)*

Function	Remarks
LDAP/SSL log display	Display the LDAP/SSL log. This function is equivalent to the `log` option of the `showldapssl`(8) command.
Snapshot (or Data Collector)	Collects the log. This function is equivalent to the `snapshot`(8) command.
COD log display	Display the COD log. This function is equivalent to the `showcodactivationhistory`(8) command.

Component Information

To refer to the information and status of physical components in the server, select the target component in the Physical tree. When you select a component, the component information and the state are displayed in the main page. This information is equivalent to the `showhardconf`(8) command.

To refer to the information and status of logical components that belong to each domain, select the target component in the Logical tree. When you select a component, the logical component information and the state are displayed in the main page. This information is equivalent to the `showboards`(8) and `showhardconf`(8) commands.

In addition, the state of each component on the Physical tree and the Logical tree can be updated by pushing the REFRESH button of the XSCF Web Console. If there is a component with an abnormal status, a mark is added to the component on the tree. Select the component so marked, and confirm its details.

Note – Screen layouts and configurations may be changed to improve functionality.

9.5 XSCF Web Error Messages

TABLE 9-27 lists the typical messages category from the XSCF Web. Moreover, in each category, detailed messages are displayed.

Also, the message from XSCF Web is almost the same as the error message of the XSCF Shell command. For typical messages from the XSCF Shell command, see Chapter 5.

TABLE 9-27 Error Messages of XSCF Web

Message	Meaning
Authentication Failed	Login failed.
XSCF ERROR	XSCF abnormally ended.

Note – The error message depends on the XSCF Web item. Therefore, you will occasionally see more messages.

APPENDIX **A**

Warning and Information Messages

This appendix explains the XSCF fault and informational messages output during the operation with the console, mail, or SNMP function of the server.

A.1 Message Types

- syslog message

The Oracle Solaris OS outputs this message to the domain console. For instructions on how to reference syslog messages, see the Oracle Solaris OS documentation.

- FMA message

The FMA message describes the results of a diagnosis automatically generated for hardware or software faults by the server's Fault Management Architecture (FMA) fault management facility. When this message is output to the domain console, the user can identify the portion corresponding to the notified fault in the server. The FMA message is retained as log information (in a fault log or error log). The Oracle Solaris `fmdump`(1M) command or the `fmdump`(8), or `showlogs`(8) command of the XSCF Shell can be used to display the message contents for more detailed investigation. The user can also confirm the contents by using the specified URL based on the MSG-ID displayed on the console.

- IPL message

This message is output during the system startup. The IPL message is output to the domain console and retained as log information (in an IPL log) in the XSCF. The IPL log retains the information corresponding to the last single system startup for each domain. The `showlogs`(8) command of the XSCF Shell can be used to display the IPL log.

- Panic message

This message is output in case of panic. The panic message is output to the domain console and retained as log information in the XSCF. The panic log retains the information corresponding to the last single panic event that occurred. The `showlogs`(8) command of XSCF can be used to display the panic log.

- Console message

The console message is a general term used to describe syslog messages, FMA messages, panic messages, IPL messages, and other messages output by POST, OpenBoot PROM, and the Oracle Solaris OS. The console messages are output to each domain console and are retained as log information (in a console log) in the XSCF. The `showlogs`(8) command of the XSCF Shell can be used to display the console log.

Note – Console messages are overwritten, beginning with the oldest message. Even when the wraparound feature causes a console message to be overwritten, the system startup message is retained in the IPL log, and in case of panic, the log is retained in the panic log.
When the XSCF unit is redundant, the console messages retained in the XSCF Unit on the active side are not copied to the standby side. Accordingly, after the XSCF Unit is switched, the console messages on the previously active side cannot be referenced.

- Monitoring message

The XSCF firmware outputs this message to notify the server fault or status. The monitoring message is output by using the `showmonitorlog`(8) command, and retained as log information (in a monitor message log or XSCF error log) in the XSCF. The `showlogs`(8) command of the XSCF Shell can be used to display the monitoring message and XSCF error log for more detailed investigation. Authorized service personnel use the DIAGCODE output in the message to acquire detailed information.

Note – Monitoring messages are overwritten, beginning with the oldest message. When the XSCF Unit is redundant, monitoring messages output by the XSCF Unit on the active side are also managed on the standby side. Even after the XSCF Unit is switched, the monitoring messages on the previously active side can be referenced.

- Other notice message

In addition to the messages above, there is a notification message displayed on the domain console when power off or reset processing is performed normally or an event occurs.

A.2 Messages in Each Function

This section explains each Oracle Solaris OS and XSCF function by which the user can recognize status notification or fault information in the server, including messages.

Recognizing Status Notification or Fault Information by a Message on the Domain Console

1. **The user recognizes status notification or fault information in a console message such as a syslog message and FMA message output to the domain console. The following shows an example of the FMA message on the domain console.**

```
<Example>  FMA Message
SUNW-MSG-ID: SUN4U-800J-C0, TYPE: Fault, VER: 1, SEVERITY: Critical
EVENT-TIME: Wed Jun 28 17:45:36 PDT 2006
PLATFORM: SUNW,SPARC-Enterprise, CSN: -, HOSTNAME: dc102
SOURCE: eft, REV: 1.5
EVENT-ID: 24fe9f8c-f302-4128-c5b8-b38a4083769f
DESC: The number of errors associated with this CHIP has exceeded acceptable
levels. Refer to http://sun.com/msg/SUN4U-800J-C0 for more information.
  Refer to SUN4U-800J-C0 for more information.
AUTO-RESPONSE: An attempt will be made to remove the affected CHIP from
service.

IMPACT: The system will not be functioning at the same performance level with
the CHIP removal.

REC-ACTION: Schedule a repair procedure to replace the affected CHIP. Use
fmdump -v -u to identify the smallest CPU/Strand ID of the affected CORE on
this CHIP.
```

Note – The message format may change in future releases.

2. **Fault information in the FMA message is stored in the log. Therefore, the log file can be referenced on the domain console. Perform an Oracle Solaris OS command such as the syslog reference command or `fmdump`(1M) command on the domain console. For how to identify fault information by using these commands, see the Oracle Solaris OS documentation.**

3. **The contents of notification or fault information can be confirmed by accessing the specified URL according to the message ID (SUNW-MSG-ID) displayed on the domain console. If no message ID (MSG-ID) is found, acquire detailed information from the syslog information.**

4. **To acquire more detailed information, log in to the XSCF and perform the** `fmdump`**(8) or** `showlogs`**(8) command to identify the fault information. For details of these two commands, see** Appendix B**.**

5. **Repair the fault according to processing recommended by the information provided on the specified URL (Note).**

In some cases, the user may recognize the fault by referring to the console messages, panic messages, IPL messages, or monitoring messages stored in the XSCF log. The `showlogs`(8) command of the XSCF Shell with each log option specified can be used to reference this log information.

Note – For up-to-date URL information, see the web site information about the messages listed in the Product Notes for your server.

Recognizing a Fault in a Message Reported by Email

1. **The user recognizes status notification or fault information as the Subject of the email reported by XSCF or in the text of the message. For an example of a mail message, see** Chapter 6**.**

2. **According to the displayed message ID (MSG-ID), the user can access the specified URL to confirm the information. Authorized service personnel can use the DIAGCODE output in the message to acquire detailed information.**

3. **To obtain more detailed information, log in to the XSCF and perform the** `fmdump` **(8) or** `showlogs`**(8) command to identify the fault information.**

4. **Repair the fault according to the processing recommended by the information provided on the specified URL.**

Recognizing Status Notification or Fault Information in an SNMP Trap Message

1. **The user recognizes status notification or fault information in the trap information issued by the SNMP manager from the XSCF. The contents of the report are the same as those of email.**

2. **Perform** Step 2 **to** Step 4 **above in "**Recognizing a Fault in a Message Reported by Email**".**

Recognizing Status Notification or Fault Information in a Monitoring Message on the XSCF Shell Terminal

1. **The user recognizes status notification or fault information in a XSCF monitoring message output by using** `showmonitorlog`**(8) comannd. The following shows an example of the XSCF monitoring message.**

```
Jun 16 12:20:37 JST 2005 FF2-5-0:Alarm:/CMU#0/CPU#0:XSCF:Uncorrectable error
( 80006000-20010000-0108000112345678)
```

   (The example is subject to change without previous notice for functional improvement.)

2. **To obtain more detailed information, specify the error option and perform the** `showlogs`**(8) command to identify fault information.**

3. **In the XSCF error log, confirm the contents of entry corresponding to the fault. (See Appendix B.)**

4. **Specify the error detail option in** `showlogs`**(8) to display the message ID (MSG-ID). The information can be confirmed by accessing the specified URL according to the displayed message ID (MSG-ID). Authorized service personnel use the DIAGCODE (Code) output in the message to acquire more detailed information.**

5. **Repair the fault according to the processing recommended by the information provided on the specified URL.**

APPENDIX **B**

XSCF Log Information

This appendix explains the following XSCF log information that can be referenced using the XSCF Shell showlogs(8) command on the XSCF console.

The log types that can be referenced by the showlogs(8) command are shown below. See TABLE 8-3 for an outline of each log, its size, and generation number.

- XSCF Error Log
- Power Log
- Event Log
- Monitor Message Log
- Temperature and Humidity History Log
- Console Log
- Panic Log
- IPL Log

The logs that can be referenced by the showaudit(8), showad(8), showldapssl(8), and showcodactivationhistory(8), commands are shown below.

- Audit Log
- Active Directory Log
- LDAP/SSL Log
- COD Activation Log

B.1 XSCF Error Log

To reference the log related to a status notification or a fault information that occurred in the server, use these two commands:

- showlogs(8) error option

- `fmdump`(8)

The `showlogs`(8) error option displays fault information in a format specific to the platform. Conversely, the `fmdump` command displays fault information in a format compatible with the Oracle Solaris OS. This latter command is provided for users who are familiar with the Oracle Solaris OS. When the log is referenced by these two commands, there is a difference in display format but little difference in the information. Use these commands in the following cases:

- To check whether a fault occurred if a message is output to the domain console and XSCF console. (See Appendix A.)
- To check whether the information is fault information if it was reported to the previously registered email address.
- To check whether the information is fault information if TRAP occurred in the SNMP manager.

Using the `showlogs`*(8) Command to Confirm a Fault*

1. **Specify the error option on the XSCF Shell and perform the** `showlogs`**(8) command to reference the XSCF error log.**

```
XSCF> showlogs error
Date: Mar 30 15:45:31 JST 2005      Code: 00112233-44556677-8899aabbcceeff00
  Status: Warning                    Occurred: Mar 30 15:45:26.000 JST 2005
  FRU: PSU#1,PSU#2
  Msg: ACFAIL occurred (ACS=3)(FEP type = A1)
Date: Mar 30 17:45:31 JST 2005      Code: 00112233-44556677-8899aabbcceeff00
  Status: Alarm                      Occurred: Mar 30 15:45:26.000 JST 2005
  FRU: PSU#1,PSU#2,*
  Msg: ACFAIL occurred (ACS=3)(FEP type = A1)
```

(The layout of the command example is subject to change without previous notice for functional improvement.)

In the example above, the following items are displayed:

- Time at which each problem was logged (Date). This date is indicated in local time.
- DIAGCODE that the field engineer and authorized service personnel use for troubleshooting (Code). The user is requested to inform the field engineer and authorized service personnel of this Code. This is useful in settling the problem at an early stage.
- Fault level of the component (Status). One of the following items is displayed:

Alarm:	The relevant component failed.
Warning:	Some subcomponents in the relevant component failed or degraded.
Information:	Notification.
Notice:	System state notification.

- Time at which each problem occurred (Occurred). This is indicated in local time.
- Replacement component (FRU) that is probably faulty. A comma (,) separates two suspect components displayed. For additional suspect components, an "*" (asterisk) is displayed after the comma (,). Each component is displayed hierarchically in a component mounting path format. Whether more suspect components are to be displayed depends on the position where the fault was detected.

The following explains cases where "FRU:" is displayed.

(a) "PSU#1, PSU#2" is displayed.

The above indicates the following: PSU#1 and PSU#2 were detected as the first and second suspect components, respectively. It might be necessary to replace the respective components as circumstances require.

(b) "PSU#1, PSU#2,*" is displayed.

The above indicates the following: PSU#1 and PSU#2 were detected as the first and second suspect components, respectively, with other components also detected. It might be necessary to replace the respective components.

(c) "IOU#0/PCI#3" is displayed.

The above indicates the following: IOU#0/PCI#3 was detected as the suspect component, and PCI slot No.3 of I/O unit No.0 is problematic. It might be necessary to replace the device connected to PCI slot No.3 as circumstances require.

(d) "MBU_A/MEMB#0/(MEM#02A)" is displayed.

The above indicates the following: MBU_A/MEMB#0/MEM#02A was detected as the suspect component, and memory slot No.02A of memory board No.0 on the MBU is problematic. It may be necessary to replace memory slot No.02A as circumstances require.

(e) "CMU#0/MEM#02A" is displayed.

The above indicates the following: CMU#0/MEM#02A was detected as the suspect component, and memory slot No.02A of CMU 0 is problematic. It may be necessary to replace memory slot No.02A as circumstances require.

(f) "CMU#0/MEM#02A-02B" is displayed.

The above indicates the following: CMU#0/MEM#02A-02B was detected as the suspect component, and memory slot No.02A and No.02B of CMU 0 are problematic. It may be necessary to replace the memory as pairs in memory slots No.02A and No.02B as circumstances require.

- One-row message to indicate an outline of the problem (Msg).
- Message ID that can be used to access the corresponding description of information at the specified URL site (MSG-ID). (The `-v` option must be specified.)

2. **Use the message ID for accessing the specified URL to acquire detailed information corresponding to this problem. For the specified URL, see the web site information about the messages described in the Product Notes for your server.**

   For the message ID, the following information can be confirmed at the web site.

- Message type (Type)
- Fault level (Severity)
- Outline of fault (Description)
- Machine operation after the fault (Automated response)
- Influence (Impact)
- Action to be taken (Action)
- Detailed information (Details)

3. **Repair the fault according to the recommended processing.**

For details of the `showlogs`(8) command, see the *XSCF Reference Manual* or the man page.Use the `fmdump`(8) command to confirm the XSCF error log in a display format that is compatible with the Oracle Solaris OS.

Using the `fmdump`*(8) Command to Confirm a Fault*

1. **Perform the `fmdump`(8) command on the XSCF Shell and reference the log.**

```
XSCF> fmdump
TIME                   UUID                                  MSG-ID
Dec 28 13:01:27.3919   bf36f0ea-9e47-42b5-fc6f-c0d979c4c8f4  FMD-8000-11
Dec 28 13:01:49.3765   3a186292-3402-40ff-b5ae-810601be337d  FMD-8000-11
Dec 28 13:02:59.4448   58107381-1985-48a4-b56f-91d8a617ad83  FMD-8000-OW
:
```

(The layout of the command example is subject to change without previous notice for functional improvement.)

In the example above, the following items are displayed:

- Time at which the problem was registered in the log (TIME).
- Universal Unique Identifier that can be used to uniquely identify the problem in an optional system set (UUID)
- Message ID (MSG-ID) that can be used to access the corresponding description of information at the specified site

2. **Use the message ID for accessing the specified URL to acquire detailed information corresponding to this problem. For the specified URL, see the web site information about the messages described in the Product Notes for your server. The information that can be referenced for the message ID is the same as that described in the item of `showlogs`(8) error.**

3. **After confirming the problem, repair the fault according to the recommended processing.**

For details of the `fmdump`(8) command, see the *XSCF Reference Manual* or the main page.

B.2 Power Log

When a power operation or resetting is performed in the server or domain, the XSCF firmware collects a power log. This section explains how to reference the power log. See TABLE 8-3 for the size and generation number of a power log.

Using the `showlogs`*(8) Command to Reference Power Logs*

- **Specify the power option on the XSCF Shell and perform the `showlogs`(8) command to reference power logs.**

```
<Example 1>  Power logs are displayed as a list.
XSCF> showlogs power
Date                       Event              Cause          DID  Switch
Mar 30 17:25:31 JST 2005   System Power Off   Pow.Fail/Recov.--   Service
Mar 30 17:35:31 JST 2005   System Power On    Pow.Fail/Recov.--   Locked
Mar 30 17:45:31 JST 2005   Domain Power Off   Operator       00   Locked
Mar 30 17:50:31 JST 2005   Domain Power On    Operator       00   Service

<Example 2>  Power logs are listed in order of the most-to-least recent by
specifying a start time and end time.
XSCF> showlogs power -t Mar3017:302005 -T Mar3017:492005 -r
Date                       Event              Cause          DID  Switch
Mar 30 17:45:31 JST 2005   Domain Power Off   Operator       00   Locked
Mar 30 17:35:31 JST 2005   System Power On    Pow.Fail/Recov.--   Locked
```

(The examples are subject to change without previous notice for functional improvement.)

In the examples above, the following items are displayed:

- Time at which each power log was collected (Date). This is indicated in local time.
- Type of power event that occurred (Event). The following lists each event and its meaning:

Event	Meaning
SCF Reset:	The XSCF was reset.
Domain Power ON:	The domain power supply was turned on.
Domain Power OFF:	The domain power supply was turned off.
System Power ON:	The power supply of the server common section was turned on.
System Power OFF:	The power supply of the server common section was turned off.
XIR:	The XIR was reset.
Domain Reset:	The domain was reset.

Factor by which the power event was instructed (Cause). The causes and their meanings are as follows:

Cause	Meaning
Self Reset:	Self-resetting of the XSCF reset the XSCF.
Power On:	Turning on the input power supply reset the XSCF.
System Reset:	The detection of an error reset the XSCF.

Panel:	Operating a switch on the operator panel caused a power event.
Scheduled:	Setting the TOD timer caused a power event.
RCI:	The I/O device connected to the RCI caused a power event.
Pow.Fail/Recov.:	Power recovery turned on the power supply.
Operator:	An operator's instruction caused a power event.
Pow.Fail/Recov.:	A power interruption cut off the power supply.
SW Request:	An Oracle Solaris OS instruction caused a power event.
Alarm:	The server environment or a hardware fault caused a power event.
Fatal:	Fatal caused a power event.
Panic:	Panic caused a power event.

- Domain ID for power event (DID)
- Mode switch status on the operator panel (Switch). The following lists the switches and their meanings:

Switch status	Meaning
Locked:	The mode switch is locked.
Service:	The mode switch is in service.

B.3 Event Log

When an event occurs in the server, such as when the system status changes, the configuration is changed, the operator panel operated, or an event was sent to the Oracle Solaris OS in the server or domain, the XSCF firmware collects an XSCF event log. The field engineer and authorized service personnel use the XSCF event logs to analyze a fault that occurs, investigate the server operation status, or reference the history of maintenance operation. This section explains how to reference XSCF event logs. See TABLE 8-3 for the size and generation numbers of XSCF event logs.

Using the `showlogs`(8) Command to Reference XSCF Event Logs

● **Specify the event option on the XSCF Shell and perform the `showlogs`(8) command to reference XSCF event logs.**

```
<Example>  XSCF event logs are displayed as a list.
XSCF> showlogs event
Date                       Message
Mar 30 17:45:31 JST 2005   System power on
Mar 30 17:55:31 JST 2005   System power off
```

(The example is subject to change without previous notice for functional improvement.)

In the example above, the following items are displayed:

- Time at which each event log was gathered (Date). This is indicated in local time.
- Event message (Message).

B.4 Using the `showlogs` Command to Display Other Logs

This section explains how to reference the other main logs by using `showlogs`(8) command. For details of each log option of `showlogs`(8), see the *XSCF Reference Manual* or the main page. See TABLE 8-3 for the size and generation number of each log.

B.4.1 Monitor Message Log

Using the `showlogs` *(8) Command to Reference Monitor Message Logs*

An event that occurred in the server is displayed as a monitoring message in real time for the user who logged in the XSCF. The XSCF firmware collects this message in a monitor message log. Specify the monitor option on the XSCF Shell and perform the `showlogs`(8) command to reference the monitor message log. The following items are displayed:

- Time at which the monitoring message was collected (Date). This is indicated in local time.
- Monitoring message (Message).

B.4.2 Temperature and Humidity History Log

Using the `showlogs`*(8) Command to Reference Temperature and Humidity History Logs*

The XSCF firmware collects the environment and temperature and humidity history regarding the server in a temperature and humidity log. The temperature and humidity history log is displayed at ten-minute intervals. Specify the `env` option on the XSCF Shell and perform the `showlogs`(8) command to reference temperature and humidity history logs. The following items are displayed:

- Time at which each thermal log was collected (Date). This is indicated in local time.
- Temperature (Temperature)
- Humidity (Humidity). The humidity is only displayed in the M8000/M9000 servers.
- Power supply status (ON or OFF) of the server (Power).

B.4.3 Console Log

Using the `showlogs`*(8) Command to Reference Console Logs*

The XSCF firmware collects the domain console messages output through the XSCF in a console log. A console log is collected as one entry for each line feed code. In some cases, console logs may be called console message logs. Specify the console option on the XSCF Shell and perform the `showlogs`(8) command to reference console logs. The following items are displayed:

- Domain ID (DomainID)
- Time at which each console log was collected (Date). This is indicated in local time.
- Console message (Message)

B.4.4 Panic Log

Using the `showlogs`*(8) Command to Reference Panic Logs*

In case of panic, a console message is output to the domain console. This console message is collected by the XSCF firmware in a panic log. In some cases, panic logs may be called panic message logs. Specify the panic option on the XSCF Shell and perform the `showlogs`(8) command to reference panic logs. The following items are displayed:

- Domain ID (DomainID)
- Time at which each panic log was collected (Date). This is indicated in local time.
- Panic message (Message)

B.4.5 IPL Log

Using the `showlogs`*(8) Command to Reference IPL Logs*

After the domain power supply is turned on, console messages are output to the domain console until the running status is set. These console messages are collected by the XSCF firmware in an IPL log. In some cases, IPL logs may be called IPL message logs. Specify the ipl option on the XSCF Shell and perform the `showlogs`(8) command to reference IPL logs. The following items are displayed:

- Domain ID (DomainID)
- Time at which each IPL log was collected (Date). This is indicated in local time.
- IPL message (Message)

B.5 Audit Log

This section explains how to reference the audit logs by using the `viewaudit`(8) command. For details of each log option, audit class, and audit event of `viewaudit`(8), see the *XSCF Reference Manual* or the main page. See TABLE 8-3 for the size and generation number of each log.

Using the `viewaudit`*(8) Command to Confirm the Audit Trail*

- **Perform the** `viewaudit`**(8) command on the XSCF Shell.**

```
<Example> Display all audit records.
XSCF> viewaudit
file,1,2006-04-26 21:37:25.626
+00:00,20060426213725.0000000000.SCF-4-0
header,20,1,audit - start,0.0.0.0,2006-04-26 21:37:25.660 +00:00
header,43,1,authenticate,0.0.0.0,2006-04-26 22:01:28.902 +00:00
authentication,failure,,unknown user,telnet 27652 0.0.197.33
header,37,1,login - telnet,0.0.0.0,2006-04-26 22:02:26.459 +00:00
subject,1,opl,normal,telnet 50466 10.18.108.4
header,78,1,command - setprivileges,0.0.0.0,2006-04-26
22:02:43.246 +00:00
subject,1,opl,normal,telnet 50466 10.18.108.4
command,setprivileges,opl,useradm
platform access,granted
return,0
```

In the example above, By default records are displayed in text format, one token per line, with a comma as the field separator.

The following list displays the Token types and their data (in display order):

- File Token

  Label, version, time, filename

- Header Token

  Label, record byte count, version, event type, machine address, time (event recorded)

- Subject Token

  Label, audit session ID, UID, mode of operation, terminal type, remote IP address, remote port

- Upriv Token

  Label, success/failure

- Udpriv Token

  Label, success/failure, privilege name, domain1, ... , domainN

- Command Token

  Label, command name, argument1, ... , argumentN

- Authentication Token

  Label, authentication result, user name, message, terminal type, remote IP address, remote port

- Return Token

  Label, return value

- Text Token

  Label, text string

Note – Some fields might not be output according to the environment.

The following lists the principal audit events and Tokens:

- Login telnet

  header

  subject

  text

  return

- Login SSH

  As for Login telnet.

- Login BUI

  As for Login telnet.

- Logout

  Header

  Subject

- Audit start

  Header

- Audit stop

  Header

- Shell command

  Header

  Subject

  Command

  Text

  Upriv | Updpriv

  Return

Note – Some Tokens might not be output according to the environment. Also, it might be changed because of the function improvement without notice.

B.6 Active Directory Log

This section explains how to reference the Active Directory logs by using the showad(8) command. For details of each log option of showad(8), see the *XSCF Reference Manual* or the main page. See TABLE 8-3 for the size and generation number of each log.

Using the showad*(8) Command to Confirm the Active Directory Log*

- ● **Perform the** showad**(8) command on the XSCF Shell.**

  When the Active Directory authentication and authorization for users, the diagnostic messages are logged. This log is for use in troubleshooting and is cleared on XSCF reset. Specify the log option on the XSCF Shell and perform the showad(8) command to reference Active Directory logs. The following items are displayed:

- Time at which each Active Directory log was collected.
- Console message

B.7 LDAP/SSL Log

This section explains how to reference the LDAP/SSL logs by using the showldapssl(8) command. For details of each log option of showldapssl(8), see the *XSCF Reference Manual* or the main page. See TABLE 8-3 for the size and generation number of each log.

Using the showldapssl*(8) Command to Confirm the LDAP/SSL Log*

- ● **Perform the** showldapssl**(8) command on the XSCF Shell.**

  When the LDAP/SSL authentication and authorization for users, the diagnostic messages are logged. This log is for use in troubleshooting and is cleared on XSCF reset. Specify the log option on the XSCF Shell and perform the showldapssl(8) command to reference LDAP/SSL logs. The following items are displayed:

- Time at which each LDAP/SSL log was collected.

- Console message

B.8 COD Activation Log

When an addition and a deletion of COD hardware activation permit occurs in the server, the XSCF firmware collects an COD activation log. Specify the log option on the XSCF Shell and perform the `showcodactivationhistory`(8) command to reference COD activation logs. For details of each log option of `showcodactivationhistory`(8), see the *XSCF Reference Manual* or the man page. See TABLE 8-3 for the size and generation number of each log.

APPENDIX **C**

XSCF MIB

This appendix explains the XSCF Management Information Base (MIB), which is supported by the XSCF SNMP agent function.

C.1 MIB Object Identifiers

TABLE C-1 below explains the MIB object identifiers supported by the XSCF.

TABLE C-1 MIB Object Identifiers

internet	OBJECT IDENTIFIER ::=	{ iso org(3) dod(6) 1 }
directory	OBJECT IDENTIFIER ::=	{ internet 1 }
mgmt	OBJECT IDENTIFIER ::=	{ internet 2 }
experimental	OBJECT IDENTIFIER ::=	{ internet 3 }
private	OBJECT IDENTIFIER ::=	{ internet 4 }
mib-2	OBJECT IDENTIFIER ::=	{ mgmt 1 }
system	OBJECT IDENTIFIER ::=	{ mib-2 1 }
interfaces	OBJECT IDENTIFIER ::=	{ mib-2 2 }
at	OBJECT IDENTIFIER ::=	{ mib-2 3 }
ip	OBJECT IDENTIFIER ::=	{ mib-2 4 }
icmp	OBJECT IDENTIFIER ::=	{ mib-2 5 }
tcp	OBJECT IDENTIFIER ::=	{ mib-2 6 }

TABLE C-1 MIB Object Identifiers *(Continued)*

udp	OBJECT IDENTIFIER ::=	{ mib-2 7 }
snmp	OBJECT IDENTIFIER ::=	{ mib-2 11 }
enterprises	OBJECT IDENTIFIER ::=	{ private 1 }
fujitsu	OBJECT IDENTIFIER ::=	{ enterprises 211 }
product	OBJECT IDENTIFIER ::=	{ fujitsu 1 }
solaris	OBJECT IDENTIFIER ::=	{ product 15 }
sparcEnterprise	OBJECT IDENTIFIER ::=	{ solaris 3 }
oplSpMIB	OBJECT IDENTIFIER ::=	{ sparcEnterprise 1 }
scfObjects	OBJECT IDENTIFIER ::=	{ oplSpMIB 1 }
scfInfo	OBJECT IDENTIFIER ::=	{ scfObjects 1 }
scfState	OBJECT IDENTIFIER ::=	{ scfObjects 2 }
scfMonitorInfo	OBJECT IDENTIFIER ::=	{ scfObjects 3 }
scfSystemInfo	OBJECT IDENTIFIER ::=	{ scfObjects 4 }
scfDomainInfo	OBJECT IDENTIFIER ::=	{ scfObjects 5 }
scfXsbInfo	OBJECT IDENTIFIER ::=	{ scfObjects 6 }
scfLsbInfo	OBJECT IDENTIFIER ::=	{ scfObjects 7 }
scfBoardInfo	OBJECT IDENTIFIER ::=	{ scfObjects 8 }
scfCpuInfo	OBJECT IDENTIFIER ::=	{ scfObjects 9 }
scfMemoryInfo	OBJECT IDENTIFIER ::=	{ scfObjects 10 }
scfIoBoxInfo	OBJECT IDENTIFIER ::=	{ scfObjects 11 }
scfComponentInfo	OBJECT IDENTIFIER ::=	{ scfObjects 12 }
scfMIBTraps	OBJECT IDENTIFIER ::=	{ oplSpMIB 2 }
scfMIBTrapPrefix	OBJECT IDENTIFIER ::=	{ scfMIBTraps 0 }
scfMIBTrapData	OBJECT IDENTIFIER ::=	{ scfMIBTraps 1 }
scfMIBConformances	OBJECT IDENTIFIER ::=	{ oplSpMIB 3 }
scfMIBCompliances	OBJECT IDENTIFIER ::=	{ scfMIBConformances 1 }
scfMIBGroups	OBJECT IDENTIFIER ::=	{ scfMIBConformances 2 }

TABLE C-1 MIB Object Identifiers *(Continued)*

scfMIBObjectGroups	OBJECT IDENTIFIER ::=	{ scfMIBGroups 1 }
scfMIBNotifGroups	OBJECT IDENTIFIER ::=	{ scfMIBGroups 2 }

C.2 Standard MIB

The standard MIB supported by the XSCF conforms to the following RFC (Note). For the standard MIB definition file, see the general RFC document.

MIB II	RFC1213
User-based Security Model (USM)	RFC3414
View-based Access Control Model (VACM)	RFC3415
SNMPv2-MIB	RFC3418

Note – RFC: Abbreviation of Request For Comment. Technical document issued by the Internet Engineering Task Force (IETF), which is a body that prescribes technical standards related to the Internet.

C.3 Extended MIB

The information from the XSCF extension MIB provided by the XSCF includes:

- Server information, hardware/firmware version, and server configuration information
- Environment information (temperature, humidity, voltage, and fan speed)
- Domain status and domain configuration information

Note – For details of the Fault Management MIB, see the Oracle Solaris OS documentation.

Note – In the M3000/M4000/M5000/M8000/M9000 servers, information has been added, such as power consumption and exhaust air. If you install a new server, reinstall the XSCF extension MIB definition file to the SNMP manager. For specific information about power consumption and exhaust air, see the latest version of the Product Notes (no earlier than the XCP 1080 edition) for your server.

The list below explains the group summary of the extension MIB supported by the XSCF.

1. scfInfo group

   This group provides general information pertaining to the XSCF.

2. scfState group

   This group provides overall status information known to the XSCF.

3. scfMonitorInfo group

   This group provides environmental information for a variety of components within the system.

4. scfSystemInfo group

   This group provides general System information and LED states.

5. scfDomainInfo group

   This group provides information specific to all Domains known to the XSCF.

6. scfXsbInfo group

   This group provides information specific to all XSBs known to the XSCF.

7. scfLsbInfo group

   This group provides information specific to all LSBs.

8. scfBoardInfo group

   This group provides information pertaining to specific board components within a System.

9. scfCpuInfo group

   This group provides information for all CPU Modules/Cores within the System.

10. scfMemoryInfo group

    This group provides information for all Memory Modules within the System.

11. scfIoBoxInfo group

    This group provides information for the External I/O Expansion Unit (IOBOX) that is attached to the system and the components which make it up.

    The components include I/O boats, Link Cards, and Power Supplies/Fans. For details about these components, see the *Service Manual* for your server.

12. scfComponentInfo group

    This group provides FRU and Status information for every component in the System.

Obtaining the Latest Extension MIB

For details on obtaining the XSCF extension MIB definition file and the Fault Management MIB definition file, see the Product Notes for your server or download site for the XCP firmware.

C.4 Trap

Traps are classified as either a standard Trap or an extension Trap. Standard Trap is provided for each device defined in SNMP as standard. For a description of a standard Trap, see the general document. In this document, the Trap in cases where an event native to this system is recognized is called an extension Trap.

For more information about traps, see Chapter 7.

APPENDIX D

Troubleshooting

This chapter describes problems that can occur during use of the XSCF console or during the operation of the system and provides solutions for them.

D.1 Troubleshooting XSCF and FAQ

This section describes problems that may occur during the use of XSCF and provides solutions for the problems. The section also contains frequently asked questions along with their answers.

Could Not Log in to XSCF

- Check whether you entered the correct user name for login.
- Check whether you entered the correct password.
- Check the number of XSCF users. For information about the number of users, see Chapter 2 and Chapter 3.

Forgot the Login Password for XSCF

- Ask a system administrator who has the platadm or useradm user privilege to reset your password using the `password`(8) command.
- If a system administrator forgets the login password, log in using the "default" account. Then use the `password`(8) command to register again. For details about logging in using the "default" account, see Chapter 2.

Could Not Connect to XSCF Through the Serial Port

- Check the connection between the terminal software and the serial port.
- Check the settings of the terminal software (baud rate is set to 9600 bps, delay is set to 0, etc.). For information about the settings, see "Connecting to XSCF via the serial port" in Chapter 3.

Could Not Connect Using Telnet to XSCF via the XSCF-LAN

- Check the LAN cable connection between the XSCF terminal and the server.
- Check the connection between the terminal software and the telnet port.
- Use the `shownetwork`(8) command to check whether the setting for the XSCF-LAN is enabled.
- Use the `showtelnet`(8) command to check whether the setting for telnet is enabled.
- Check whether the entered IP address and port number match their settings.
- Confirm that the number of connections using telnet/SSH does not exceed its maximum number. For information about the maximum number, see Chapter 2 and Chapter 3.
- If necessary, use the console on the personal computer that is directly connected to XSCF through the serial port to log in to the XSCF Shell, and check the XSCF-LAN settings by using the `shownetwork`(8) command.

Could Not Connect Using SSH to XSCF via the XSCF-LAN

- Check the LAN cable connection between the XSCF terminal and the server.
- Use the `shownetwork`(8) command to check whether the setting for the XSCF-LAN is enabled.
- Use the `showssh`(8) command to check whether the setting for SSH is enabled.
- Check whether the entered IP address and port number match their settings.
- Confirm that the number of connections using telnet/SSH does not exceed limit. For information about the limitation, see Chapter 3.
- If necessary, use the console on the personal computer that is directly connected to XSCF through the serial port to log in to the XSCF Shell, and check the XSCF-LAN settings using the `shownetwork`(8) command.
- Check whether the host key has the correct setting. During XSCF Unit replacement, the host key setting is restored to the preset key setting of XSCF.
- Check whether the client software has the correct settings.

Do Not Know the IP Address of XSCF

- Use the shownetwork(8) command to check the current network configuration. If it has not yet been set, ask the network administrator to check the setting.
- If necessary, use the console on the personal computer that is directly connected to XSCF through the serial port to log in to the XSCF Shell, and check the XSCF-LAN settings using the shownetwork(8) command.

The Console of the XSCF Shell or the Domain Console was Suddenly Disconnected

- Someone may perform the applynetwork(8) and rebootxscf(8) commands after the setnetwork(8), setroute(8), sethostname(8), and setnameserver(8) commands were executed, or the flashupdate(8) command may have been executed. To use the XSCF, establish another connection and log in to the system again.
- Someone may have used the setdate(8) command or the switchscf(8) command. To use the XSCF, establish another connection and log in to the system again.
- If the XSCF Shell is not used during the specified length of time after login, it automatically terminates itself. This forced termination occurs when the specified period has elapsed, only if the time monitoring function is enabled and a length of time is specified for this function in the XSCF settings.
- When the escape character (Example: "#") set by client and "." (period) keys are entered, the Oracle Solaris Secure Shell or SSH client of OpenSSH is disconnected. If the setting of escape character is the same in the Oracle Solaris Secure Shell/SSH client and console(8) command, the terminal is disconnected. So, please change the value of either setting. For more information, see the manual for SSH Client.

Could Not Power On or Off the Server

- In operation with a user privilege other than the platadm or fieldeng privilege, the power on and power off operations for the entire system are not available. For information about user privileges, see the *Administration Guide* or *XSCF Reference Manual*.

Could Not Add an XSCF User

- Check the number of XSCF registration users. For information about the number of registration users, see Chapter 2 and Chapter 3. Otherwise, contact the system administrator.

A Mail Report Was Not Received From XSCF

- XSCF does not necessarily report all events. It sends a mail message for each part fault or authentication failure event. Check for the relevant event in the error log, or use the reference for event logs in Appendix B to check whether this is an event in an event log to be reported.
- Use the `showemailreport`(8) command to check whether the appropriate setting is enabled. If no mail message for this event has been received, check whether an error mail message has been sent to the error mail recipient, or check the log of recorded errors.
- If a cellular phone is used for receiving mail messages, check the phone settings for any set restriction on receiving messages.

Could Not Access the Top Page of the XSCF Web Function

- Use the `showhttps`(8) command to check whether the setting for XSCF is enabled.
- Check whether the entered URL is correct (e.g., whether the “s” in "https" is missing).
- Ask the system administrator to check whether access through the IP address that is set is permitted.
- Check whether the SSL/TSL function setting of the web browser is enabled.

Could Not Display XSCF Web Windows

- If XSCF Web windows are not displayed even after login to the system from the top page of XSCF Web, JavaScript may be disabled in the web browser settings. Enable JavaScript in the browser settings, and retry login.
- If pop-up window display is disabled in the web browser settings, XSCF Web windows cannot be displayed. Check the browser settings.

Forgot the Login Password for the XSCF Web

- Since XSCF Web authentication is the same as XSCF Shell authentication, see the above Forgot the Login Password for XSCF.

Failed in the First Attempt to Access the XSCF Web Function After Login

- Check whether Cookies are accepted in the web browser settings.

Web Pages of the XSCF Web Function are not Displayed Correctly

- Some versions of web browsers do not display the windows correctly. See "Supported browsers" in Chapter 9, and update your browser to the latest version.

Alert Message is Displayed in XSCF Web

- Please confirm the content of the security alert message and stop the use of XSCF Web. Perform the countermeasure to the content of the confirmed warning. When the expiration is over, re-set the https setting of XSCF. For the details of settings, see Section 2.2.8, "Https Administration" on page 2-113 in Chapter 2.

Other Problems

Contact the system administrator. If XSCF log data must be collected, use the XSCF Shell command to collect it. For information about the log collection method, see Section 8.2, "Collecting XSCF Logs" on page 8-24.

Frequently Asked Questions (FAQ)

Q. Is an IP address assigned by default to the LAN port used for the XSCF-LAN?

A. An IP address is not assigned by default. If an IP address were assigned by default, one IP address would be temporarily duplicated during the concurrent setup of multiple units. This may affect the user LAN environment. To prevent this, the XSCF-LAN network function is disabled by default. However, there is a default value for the IP address for the network connecting redundantly configured XSCF Units (ISN). For information about the default value, see Section 2.2.1, "Network Configuration" on page 2-16 in Chapter 2.

Q. If an Oracle Solaris OS hang-up event occurs during Oracle Solaris OS startup after the main unit is powered on, can the main unit power be turned off?

A. If an Oracle Solaris OS hang-up event occurs, the first action is to do the following instead of turning off the main unit power:

1. **First, execute the `reset`(8) command with the panic option from the XSCF Shell.**

2. **After doing Step 1, if the Oracle Solaris OS dump fails, move to the ok prompt by executing "Break", or executing the `reset`(8) command with the xir option from the XSCF Shell. At this point, execute the "`sync`" command.**

3. **After doing Step 2, if the reset operation or the "`sync`" command fails, execute the `reset`(8) command with the "`por`" option from the XSCF Shell, or forcibly turn off power by using any of the following methods:**

Method 1. Press and hold down the POWER switch on the operator panel of the main unit for four seconds.

Method 2. Execute the `poweroff`(8) command from the XSCF Shell.

Q. What kind of processing is executed by XSCF from the time that input power to the main unit is turned on until the Oracle Solaris OS starts?

A. The processing flow before system startup is as follows:

1. The operator turns on input power.
2. XSCF starts.
3. The operator turns on the power to the server.
4. XSCF initializes the hardware.
5. The POST starts and performs an initial diagnosis of hardware.
6. OpenBoot PROM starts.
7. OpenBoot PROM starts the boot process.
8. The Oracle Solaris OS starts.

Q. During normal log in to or log out from XSCF, what kind of messages are displayed on the terminal?

A. The following example shows successful log in to XSCF:

```
login: jsmith
Password: xxxxxxxx
XSCF>
```

The following example shows an unsuccessful log in:

```
login: jsmith
Password: xxxxxxxx
Login incorrect
```

The following example shows a successful log out from XSCF:

```
XSCF> exit
logout
```

The following example shows an unsuccessful log out:

```
XSCF> exit
Not supported in this system.
```

Note – The above examples vary depending on the client software on the terminal.

Q. What is the relationship between the XSCF error log and error information in the MIB file?

A. Error information reflected in the MIB file is the latest log data of XSCF.

D.2 Troubleshooting the Server While XSCF Is Being Used

This section describes how to effectively use XSCF in case the main unit is not responding, which means that a problem or panic occurred in the unit.

Before Contacting Our Authorized Service Personnel

Before contacting our authorized service personnel, first follow the procedure below. This procedure may be helpful not only in solving the problem but also could eliminate the need to make an inquiry.

1. **If the server does not respond, set the Mode switch on the operator panel to Service mode.**
2. **Check the system status by using either of the following methods:**

- When you cannot use the XSCF Shell through SSH/telnet
  - a. **Connect a terminal to the serial port of XSCF.**
  - b. **Enter your user account and password to log in to the XSCF Shell.**
  - c. **Use the XSCF Shell to check error logs.**
- When you can use the XSCF Shell through SSH/telnet or the serial port
  - a. **Use your XSCF user account to log in to XSCF.**
  - b. **Establish a connection through the XSCF-LAN port, and use the XSCF Shell to check error logs and other information. See Appendix B for the corrective action.**
  - c. **Otherwise, check the XSCF event logs and server status by using the XSCF Shell through the serial port.**

Use the following commands to check the events that occurred at the time the problem occurred:

- `showlogs error`
- `showlogs event`
- `showlogs power`
- `showlogs monitor`
- `showlogs console`
- `fmdump`

If you find an error, see Appendix B in this manual for the corrective action.

d. **Check the XSCF console log or panic log for the latest messages. A message may have been output by the Oracle Solaris OS after it detected the problem. In cases involving a panic, use the** `showlogs`**(8) command with the panic option to check the events that occurred at the time the panic occurred. For information about using the command, see the** *XSCF Reference Manual***.**

3. **If you cannot find any problem after checking the above points, restart the system.**

4. **If you find any problem, see** Appendix B **and take measures based on the corrective action that is described, such as using the maintenance guidance of the XSCF Shell command for replacement of the relevant component.**

APPENDIX **E**

Software License Conditions

Some of the software functions explained in this manual are licensed under public licenses (GNU Public License (GPL), GNU Lesser Public License (LGPL), and others). This appendix lists these public licenses and conditions.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.
To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING,REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>
Copyright (C) 19yy <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

GNU LESSER GENERAL PUBLIC LICENSE
Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc. 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
    <one line to give the library's name and a brief idea of what it does.>
     Copyright (C) <year>  <name of author>

     This library is free software; you can redistribute it and/or
     modify it under the terms of the GNU Lesser General Public
     License as published by the Free Software Foundation; either
     version 2.1 of the License, or (at your option) any later version.

     This library is distributed in the hope that it will be useful,
     but WITHOUT ANY WARRANTY; without even the implied warranty of
     MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the GNU
     Lesser General Public License for more details.

     You should have received a copy of the GNU Lesser General Public
     License along with this library; if not, write to the Free Software
     Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-
1301 USA
```

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

```
  Yoyodyne, Inc., hereby disclaims all copyright interest in the  library
`Frob' (a library for tweaking knobs) written by James Random Hacker.

  <signature of Ty Coon>, 1 April 1990
  Ty Coon, President of Vice
```

That's all there is to it!

```
-----
/
* ====================================================================
 * The Apache Software License, Version 1.1
 *
 * Copyright (c) 2000-2003 The Apache Software Foundation.  All rights
 * reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
 * 3. The end-user documentation included with the redistribution,
 *    if any, must include the following acknowledgment:
 *       "This product includes software developed by the
 *        Apache Software Foundation (http://www.apache.org/)."
 *   Alternately, this acknowledgment may appear in the software itself,
 *    if and wherever such third-party acknowledgments normally appear.
 *
 * 4. The names "Apache" and "Apache Software Foundation" must
 *    not be used to endorse or promote products derived from this
 *    software without prior written permission. For written
 *    permission, please contact apache@apache.org.
 *
 * 5. Products derived from this software may not be called "Apache",
 *    nor may "Apache" appear in their name, without prior written
 *    permission of the Apache Software Foundation.
 *
 * THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR
 * IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
 * PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE
 * APACHE SOFTWARE FOUNDATION OR ITS CONTRIBUTORS BE
 * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
 * EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
 * LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER
 * IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
 * OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
 * SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
 *  DAMAGE.
 * ====================================================================
 *
  * This software consists of voluntary contributions made by many
individuals
 * on behalf of the Apache Software Foundation.  For more information on
the
 *  Apache Software Foundation, please see
 * <http://www.apache.org/>.
 *
 * Portions of this software are based upon public domain software
  * originally written at the National Center for Supercomputing
Applications,
 * University of Illinois, Urbana-Champaign.
 */
/*
 * Copyright (c) 1987, 1993, 1994
 *      The Regents of the University of California.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *   documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *      This product includes software developed by the University of
 *      California, Berkeley and its contributors.
 * 4. Neither the name of the University nor the names of its contributors
 *   may be used to endorse or promote products derived from this software
 *    without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND
 * CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED
 * WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
 * WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
 * PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE
 * REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT,
 * INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
 * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
 * PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
 * CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
 * OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
 * SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
 * DAMAGE.
/* Copyright (c) 1996 by Internet Software Consortium.
 *
 * Permission to use, copy, modify, and distribute this software for any
 * purpose with or without fee is hereby granted, provided that the above
  * copyright notice and this permission notice appear in all copies.
  *
 * THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE
 * CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS
 * SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF
 * MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET
 * SOFTWARE
 * CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR
 * CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER
 * RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN
 * ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS
 * ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
 * PERFORMANCE OF THIS SOFTWARE.
 */

!*  This code is based on the UltraSPARC atomics library by Mike Bennett
!*  The Initial Developer of the Original Code is Mike Bennett,
!*  mbennett@netcom.com, Copyright (C) 1999. All Rights Reserved.
!*  This code is based on the sparc architecture Manual version 9
!*  section J.11 (page 333)

 *  Based on libdl (dlfcn.c/dlfcn.h) which is
 *  Copyright (c) 1992,1993,1995,1996,1997,1988
 *  Jens-Uwe Mager, Helios Software GmbH, Hannover, Germany.
 *
 *  Not derived from licensed software.
 *
 *  Permission is granted to freely use, copy, modify, and redistribute
 *  this software, provided that the author is not construed to be liable
 *  for any results of using the software, alterations are clearly marked
 *  as such, and this notice is not modified.

  strnatcmp.c -- Perform 'natural order' comparisons of strings in C.
  Copyright (C) 2000 by Martin Pool <mbp@humbug.org.au>

   This software is provided 'as-is', without any express or implied
warranty.  In no event will the authors be held liable for any damages
arising from the use of this software.

  Permission is granted to anyone to use this software for any purpose,
including commercial applications, and to alter it and redistribute it
freely, subject to the following restrictions:

  1. The origin of this software must not be misrepresented; you must not
claim that you wrote the original software. If you use this software in a
product, an acknowledgment in the product documentation would be
appreciated but is not required.
 2. Altered source versions must be plainly marked as such, and must not
be      misrepresented as being the original software.
    3. This notice may not be removed or altered from any source
distribution.

/*
 * Copyright (c) 2002-2006 Asim Jalis
 *
 * This library is released under the zlib/libpng license as described at
 *
 * http://www.opensource.org/licenses/zlib-license.html
 *
```

```
 * Here is the statement of the license:
 *
  * This software is provided 'as-is', without any express or implied
warranty.
 * In no event will the authors be held liable for any damages arising from
 * the use of this software.
 *
 * Permission is granted to anyone to use this software for any purpose,
 * including commercial applications, and to alter it and redistribute it
 * freely, subject to the following restrictions:
 *
 * 1. The origin of this software must not be misrepresented; you must not
 * claim that you wrote the original software. If you use this software
in a
 * product, an acknowledgment in the product documentation would be
 * appreciated but is not required.
 *
 * 2. Altered source versions must be plainly marked as such, and must not
be
 * misrepresented as being the original software.
 *
  * 3. This notice may not be removed or altered from any source
distribution.
 */

-----
 * This is derived from material copyright RSA Data Security, Inc.
 * Their notice is reproduced below in its entirety.
 *
 * Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights
 * reserved.
 *
 * License to copy and use this software is granted provided that it  is
identified
 * as the "RSA Data Security, Inc. MD4 Message-Digest Algorithm" in all
 * material mentioning or referencing this software or this function.
 *
 * License is also granted to make and use derivative works provided that
such
 * works are identified as "derived from the RSA Data Security, Inc. MD4
 * Message-Digest Algorithm" in all material mentioning or referencing the
 * derived work.
 *
 * RSA Data Security, Inc. makes no representations concerning either the
 * merchantability of this software or the suitability of this software
for any
 * particular purpose. It is provided "as is" without express or implied
warranty
 * of any kind.
 *
 * These notices must be retained in any copies of any part of this
 * documentation and/or software.

/*
 * The apr_md5_encode() routine uses much code obtained from the FreeBSD
 * 3.0 MD5 crypt() function, which is licenced as follows:
 * ---------------------------------------------------------------------
-------
 * "THE BEER-WARE LICENSE" (Revision 42):
 * <phk@login.dknet.dk> wrote this file.  As long as you retain this notice
you
 * can do whatever you want with this stuff. If we meet some day, and you
think
 * this stuff is worth it, you can buy me a beer in return.   Poul-Henning
Kamp
 * ---------------------------------------------------------------------
-------
 */
/*
 * apr_ldap_compat.c: LDAP v2/v3 compatibility things
 *
 * Original code from auth_ldap module for Apache v1.3:
 * Copyright 1998, 1999 Enbridge Pipelines Inc.
 * Copyright 1999-2001 Dave Carrigan
 */

/*
 * Portions Copyright (c) 1992-1996 Regents of the University of Michigan.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms are permitted provided
 * that this notice is preserved and that due credit is given  to the
University of
 * Michigan at Ann Arbor. The name of the University may not be used to
 * endorse or promote products derived from this software without specific
prior
 * written permission. This software is provided ``as is'' without express
or
 * implied warranty.
 */
```

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd
and Clark Cooper

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Copyright (C) 2004 Internet Systems Consortium, Inc. ("ISC")
Copyright (C) 1996-2003 Internet Software Consortium.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

$Id: COPYRIGHT,v 1.6.2.4 2004/03/15 04:44:37 marka Exp $

Portions Copyright (C) 1996-2001 Nominum, Inc.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.
THE SOFTWARE IS PROVIDED "AS IS" AND NOMINUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL NOMINUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

(*
This document is freely plagiarised from the 'Artistic Licence', distributed as part of the Perl v4.0 kit by Larry Wall, which is available from most major archive sites
*)

This documents purpose is to state the conditions under which these Packages (See definition below) viz: "Crack", the Unix Password Cracker, and "CrackLib", the Unix Password Checking library, which are held in copyright by Alec David Edward Muffett, may be copied, such that the copyright holder maintains some semblance of artistic control over the development of the packages, while giving the users of the package the right to use and distribute the Package in a more-or-less customary fashion, plus the right to make reasonable modifications.

So there.

****
***

Definitions:

A "Package" refers to the collection of files distributed by the Copyright Holder, and derivatives of that collection of files created through textual modification, or segments thereof.

"Standard Version" refers to such a Package if it has not been modified, or has been modified in accordance with the wishes of the Copyright Holder.

"Copyright Holder" is whoever is named in the copyright or copyrights for the package.

"You" is you, if you're thinking about copying or distributing this Package.

"Reasonable copying fee" is whatever you can justify on the basis of media cost, duplication charges, time of people involved, and so on. (You will not be required to justify it to the Copyright Holder, but only to the computing community at large as a market that must bear the fee.)

"Freely Available" means that no fee is charged for the item itself, though there may be fees involved in handling the item. It also means that recipients of the item may redistribute it under the same conditions they received it.

1. You may make and give away verbatim copies of the source form of the Standard Version of this Package without restriction, provided that you duplicate all of the original copyright notices and associated disclaimers.

2. You may apply bug fixes, portability fixes and other modifications derived from the Public Domain or from the Copyright Holder. A Package modified in such a way shall still be considered the Standard Version.

3. You may otherwise modify your copy of this Package in any way, provided that you insert a prominent notice in each changed file stating how and when AND WHY you changed that file, and provided that you do at least ONE of the following:

a) place your modifications in the Public Domain or otherwise make them Freely Available, such as by posting said modifications to Usenet or an equivalent medium, or placing the modifications on a major archive site such as uunet.uu.net, or by allowing the Copyright Holder to include your modifications in the Standard Version of the Package.

b) use the modified Package only within your corporation or organization.

c) rename any non-standard executables so the names do not conflict with standard executables, which must also be provided, and provide separate documentation for each non-standard executable that clearly documents how it differs from the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

4. You may distribute the programs of this Package in object code or executable form, provided that you do at least ONE of the following:

a) distribute a Standard Version of the executables and library files, together with instructions (in the manual page or equivalent) on where to get the Standard Version.

b) accompany the distribution with the machine-readable source of the Package with your modifications.

c) accompany any non-standard executables with their corresponding Standard Version executables, giving the non-standard executables non-standard names, and clearly documenting the differences in manual pages (or equivalent), together with instructions on where to get the Standard Version.

d) make other distribution arrangements with the Copyright Holder.

5. You may charge a reasonable copying fee for any distribution of this Package. You may charge any fee you choose for support of this Package. YOU MAY NOT CHARGE A FEE FOR THIS PACKAGE ITSELF. However, you may distribute this Package in aggregate with other (possibly commercial) programs as part of a larger (possibly commercial) software distribution provided that YOU DO NOT ADVERTISE this package as a product of your own.

6. The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission.

7. THIS PACKAGE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE.

The End

```
/* CMU libsasl
 * Tim Martin
 * Rob Earhart
 * Rob Siemborski
 */
/*
 * Copyright (c) 1998-2003 Carnegie Mellon University.  All rights
reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are
met:
 *
 * 1. Redistributions of source code must retain the above copyright
notice, this
 *  list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 * notice, this list of conditions and the following disclaimer in the
 * documentation and/or other materials provided with the distribution.
 *
 * 3. The name "Carnegie Mellon University" must not be used to endorse or
 * promote products derived from this software without prior written
permission.
 * For permission or any other legal details, please contact

 *      Office of Technology Transfer
 *      Carnegie Mellon University
 *      5000 Forbes Avenue
 *      Pittsburgh, PA  15213-3890
 *      (412) 268-4387, fax: (412) 268-7395
 *      tech-transfer@andrew.cmu.edu
 *
 * 4. Redistributions of any form whatsoever must retain the following
 *  acknowledgment:
 *  "This product includes software developed by Computing Services at
 *  Carnegie Mellon University (http://www.cmu.edu/computing/)."
 *
 * CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH
 * REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES
 * OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE
 * MELLON UNIVERSITY BE LIABLE
 * FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR
 * ANY DAMAGES
 * WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS,
 * WHETHER IN
 * AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS
 * ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
 * PERFORMANCE OF THIS SOFTWARE.
 */
```

The Open Software License
v. 1.0

This Open Software License (the "License") applies to any original work of authorship (the "Original Work") whose owner (the "Licensor") has placed the following notice immediately following the copyright notice for the Original Work: "Licensed under the Open Software License version 1.0"

License Terms

1) Grant of Copyright License. Licensor hereby grants You a world-wide, royalty-free, non-exclusive, perpetual, non-sublicenseable license to do the following:

a) to reproduce the Original Work in copies;

b) to prepare derivative works ("Derivative Works") based upon the Original Work;

c) to distribute copies of the Original Work and Derivative Works to the public, with the proviso that copies of Original Work or Derivative Works that You distribute shall be licensed under the Open Software License;

d) to perform the Original Work publicly; and

e) to display the Original Work publicly.

2) Grant of Patent License. Licensor hereby grants You a world-wide, royalty-free, non-exclusive, perpetual, non-sublicenseable license, under patent claims owned or controlled by the Licensor that are embodied in the Original Work as furnished by the Licensor ("Licensed Claims") to make, use, sell and offer for sale the Original Work. Licensor hereby grants You a world-wide, royalty-free, non-exclusive, perpetual, non-sublicenseable license under the Licensed Claims to make, use, sell and offer for sale Derivative Works.

3) Grant of Source Code License. The term "Source Code" means the preferred form of the Original Work for making modifications to it and all available documentation describing how to access and modify the Original Work. Licensor hereby agrees to provide a machine-readable copy of the Source Code of the Original Work along with each copy of the Original Work that Licensor distributes. Licensor reserves the right to satisfy this obligation by placing a machine-readable copy of the Source Code in an information repository reasonably calculated to permit inexpensive and convenient access by You for as long as Licensor continues to distribute the Original Work, and by publishing the address of that information repository in a notice immediately following the copyright notice that applies to the Original Work.

4) Exclusions From License Grant. Nothing in this License shall be deemed to grant any rights to trademarks, copyrights, patents, trade secrets or any other intellectual property of Licensor except as expressly stated herein. No patent license is granted to make, use, sell or offer to sell embodiments of any patent claims other than the Licensed Claims defined in Section 2. No right is granted to the trademarks of Licensor even if such marks are included in the Original Work. Nothing in this License shall be interpreted to prohibit Licensor from licensing under different terms from this License any Original Work that Licensor otherwise would have a right to license.

5) External Deployment. The term "External Deployment" means the use or distribution of the Original Work or Derivative Works in any way such that the Original Work or Derivative Works may be accessed or used by anyone other than You, whether the Original Work or Derivative Works are distributed to those persons, made available as an application intended for use over a computer network, or used to provide services or otherwise deliver content to anyone other than You. As an express condition for the grants of license hereunder, You agree that any External Deployment by You shall be deemed a distribution and shall be licensed to all under the terms of this License, as prescribed in section 1(c) herein.

6) Warranty and Disclaimer of Warranty. LICENSOR WARRANTS THAT THECOPYRIGHT IN AND TO THE ORIGINAL WORK IS OWNED BY THE LICENSOR OR THAT THE ORIGINAL WORK IS DISTRIBUTED BY LICENSOR UNDER A VALID CURRENT LICENSE FROM THE COPYRIGHT OWNER. EXCEPT AS EXPRESSLY STATED IN THE IMMEDIATELY PRECEEDING SENTENCE, THE ORIGINAL WORK IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF NON-INFRINGEMENT AND WARRANTIES THAT THE ORIGINAL WORK IS MERCHANTABLE OR FIT FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY OF THE ORIGINAL WORK IS WITH YOU. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO LICENSE TO ORIGINAL WORK IS GRANTED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

7) Limitation of Liability. UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL THE LICENSOR BE LIABLE TO ANY PERSON FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER ARISING AS A RESULT OF THIS LICENSE OR THE USE OF THE ORIGINAL WORK INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PERSON SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

8) Acceptance and Termination. Nothing else but this License (or another written agreement between Licensor and You) grants You permission to create Derivative Works based upon the Original Work, and any attempt to do so except under the terms of this License (or another written agreement between Licensor and You) is expressly prohibited by U.S. copyright law, the equivalent laws of other countries, and by international treaty. Therefore, by exercising any of the rights granted to You in Sections 1 and 2 herein, You indicate Your acceptance of this License and all of its terms and conditions. This license shall terminate immediately and you may no longer exercise any of the rights granted to You by this License upon Your failure to honor the proviso in Section 1(c) herein.

9) Mutual Termination for Patent Action. This License shall terminate automatically and You may no longer exercise any of the rights granted to You by this License if You file a lawsuit in any court alleging that any OSI Certified open source software that is licensed under any license containing this "Mutual Termination for Patent Action" clause infringes any patent claims that are essential to use that software.

10) Jurisdiction, Venue and Governing Law. You agree that any lawsuit arising under or relating to this License shall be maintained in the courts of the jurisdiction wherein the Licensor resides or in which Licensor conducts its primary business, and under the laws of that jurisdiction excluding its conflict-of-law provisions. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any use of the Original Work outside the scope of this License or after its termination shall be subject to the requirements and penalties of the U.S. Copyright Act, 17 U.S.C. § 101 et seq., the equivalent laws of other countries, and international treaty. This section shall survive the termination of this License.

11) Attorneys Fees. In any action to enforce the terms of this License or seeking damages relating thereto, the prevailing party shall be entitled to recover its costs and expenses, including, without limitation, reasonable attorneys' fees and costs incurred in connection with such action, including any appeal of such action. This section shall survive the termination of this License.

12) Miscellaneous. This License represents the complete agreement concerning the subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable.

13) Definition of "You" in This License. "You" throughout this License, whether in upper or lower case, means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License. For legal entities, "You" includes any entity that controls, is controlled by, or is under common control with you. For purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

This license is Copyright (C) 2002 Lawrence E. Rosen. All rights reserved. Permission is hereby granted to copy and distribute this license without modification. This license may not be modified without the express written permission of its copyright owner.

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd
                               and Clark Cooper
Copyright (c) 2001, 2002, 2003 Expat maintainers.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

```
   Copyright [yyyy] [name of copyright owner]

   Licensed under the Apache License, Version 2.0 (the "License");
  you may not use this file except in compliance with the License.
   You may obtain a copy of the License at
       http://www.apache.org/licenses/LICENSE-2.0
```

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and limitations under the License.

APACHE HTTP SERVER SUBCOMPONENTS:

The Apache HTTP Server includes a number of subcomponents with separate copyright notices and license terms. Your use of the source code for the these subcomponents is subject to the terms and conditions of the following licenses.

For the mod_mime_magic component:

```
/*
 * mod_mime_magic: MIME type lookup via file magic numbers
 * Copyright (c) 1996-1997 Cisco Systems, Inc.
 *
 * This software was submitted by Cisco Systems to the Apache Group in July
 * 1997.  Future revisions and derivatives of this source code must
 * acknowledge Cisco Systems as the original contributor of this module.
 * All other licensing and usage conditions are those of the Apache Group.
 *
 * Some of this code is derived from the free version of the file command
 * originally posted to comp.sources.unix.  Copyright info for that
program is
 * included below as required.
 * ---------------------------------------------------------------------
------
 * - Copyright (c) Ian F. Darwin, 1987. Written by Ian F. Darwin.
 *
 * This software is not subject to any license of the American Telephone
and
 * Telegraph Company or of the Regents of the University of California.
 *
 * Permission is granted to anyone to use this software for any purpose
on any
 * computer system, and to alter it and redistribute it freely, subject
to the
 * following restrictions:
 *
 * 1. The author is not responsible for the consequences of use of this
 * software, no matter how awful, even if they arise from flaws in it.
 *
 * 2. The origin of this software must not be misrepresented, either by
explicit
 * claim or by omission.  Since few users ever read sources, credits must
 * appear in the documentation.
 *
 * 3. Altered versions must be plainly marked as such, and must not be
 * misrepresented as being the original software.  Since few users ever
read
 * sources, credits must appear in the documentation.
 *
 * 4. This notice may not be removed or altered.
 * ---------------------------------------------------------------------
----
 *
 */
```

"macmartinized" polygon code copyright 1992 by Eric Haines, erich@eye.com

```
/**********************************************************************
*
 * NCSA HTTPd Server
 * Software Development Group
 * National Center for Supercomputing Applications
 * University of Illinois at Urbana-Champaign
 * 605 E. Springfield, Champaign, IL 61820
 * httpd@ncsa.uiuc.edu
 *
 * Copyright  (C)  1995, Board of Trustees of the University of Illinois
 *

***********************************************************************
 *
 * md5.c: NCSA HTTPd code which uses the md5c.c RSA Code
 *
 *  Original Code Copyright (C) 1994, Jeff Hostetler, Spyglass, Inc.
 *  Portions of Content-MD5 code Copyright (C) 1993, 1994 by Carnegie
Mellon
 *     University (see Copyright below).
 *  Portions of Content-MD5 code Copyright (C) 1991 Bell Communications
 *     Research, Inc. (Bellcore) (see Copyright below).
 *  Portions extracted from mpack, John G. Myers - jgm+@cmu.edu
 *  Content-MD5 Code contributed by Martin Hamilton (martin@net.lut.ac.uk)
 *
 */

/* these portions extracted from mpack, John G. Myers - jgm+@cmu.edu */
/* (C) Copyright 1993,1994 by Carnegie Mellon University
 * All Rights Reserved.
 *
 * Permission to use, copy, modify, distribute, and sell this software and
its
 * documentation for any purpose is hereby granted without fee, provided
that
 * the above copyright notice appear in all copies and that both that
copyright
 * notice and this permission notice appear in supporting documentation,
and
 * that the name of Carnegie Mellon University not be used in advertising
or
 * publicity pertaining to distribution of the software without specific,
written
 * prior permission.  Carnegie Mellon University makes no representations
 * about the suitability of this software for any purpose.  It is provided
"as is"
 * without express or implied warranty.
 *
 * CARNEGIE MELLON UNIVERSITY DISCLAIMS ALL WARRANTIES WITH
 * REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES
 * OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CARNEGIE
 * MELLON UNIVERSITY BE LIABLE FOR ANY SPECIAL, INDIRECT OR
 * CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER
 * RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN
 * AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS
 * ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR
 * PERFORMANCE OF THIS SOFTWARE.
 */
```

```
/*
 * Copyright (c) 1991 Bell Communications Research, Inc. (Bellcore)
 *
 * Permission to use, copy, modify, and distribute this material for any
purpose
 * and without fee is hereby granted, provided  that the above copyright
notice
 * and this permission notice appear in all copies, and that the name of
 * Bellcore not be used in advertising or publicity pertaining to this
material
  * without the specific, prior written permission of an authorized
representative
 * of Bellcore.  BELLCORE MAKES NO REPRESENTATIONS ABOUT THE
 * ACCURACY OR SUITABILITY OF THIS MATERIAL FOR ANY PURPOSE.
 * IT IS PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED
 * WARRANTIES.
  */

/*
 * This is work is derived from material Copyright RSA Data Security, Inc.
 *
 * The RSA copyright statement and Licence for that original material is
 * included below. This is followed by the Apache copyright statement and
 * licence for the modifications made to that material.
 */

 *
 * This is derived from material copyright RSA Data Security, Inc.
 * Their notice is reproduced below in its entirety.
 *
 * Copyright (C) 1990-2, RSA Data Security, Inc. Created 1990. All rights
 * reserved.
 *
 * RSA Data Security, Inc. makes no representations concerning either the
 * merchantability of this software or the suitability of this software
for any
 * particular purpose. It is provided "as is" without express or implied
warranty
 * of any kind.
 *
 * These notices must be retained in any copies of any part of this
 * documentation and/or software.
 */

#
# install - install a program, script, or datafile
# This comes from X11R5 (mit/util/scripts/install.sh).
#
# Copyright 1991 by the Massachusetts Institute of Technology
#
# Permission to use, copy, modify, distribute, and sell this software and
its
# documentation for any purpose is hereby granted without fee, provided
that
# the above copyright notice appear in all copies and that both that
copyright
# notice and this permission notice appear in supporting documentation,
and
# that the name of M.I.T. not be used in advertising or publicity
pertaining to
# distribution of the software without specific, written prior permission.
M.I.T.
# makes no representations about the suitability of this software for any
# purpose.  It is provided "as is" without express or implied warranty.
#
```

PCRE LICENCE

PCRE is a library of functions to support regular expressions whose syntax and semantics are as close as possible to those of the Perl 5 language.

Written by: Philip Hazel <ph10@cam.ac.uk>

University of Cambridge Computing Service,
Cambridge, England. Phone: +44 1223 334714.

Copyright (c) 1997-2001 University of Cambridge

Permission is granted to anyone to use this software for any purpose on any computer system, and to redistribute it freely, subject to the following restrictions:

1. This software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

2. The origin of this software must not be misrepresented, either by explicit claim or by omission. In practice, this means that if you use PCRE in software which you distribute to others, commercially or otherwise, you must put a sentence like this

 Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England.

   somewhere reasonably visible in your documentation and in any relevant files or online help data or similar. A reference to the ftp site for the source, that is, to

     ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/

   should also be given in the documentation.

3. Altered versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. If PCRE is embedded in any software that is released under the GNU General Purpose Licence (GPL), or Lesser General Purpose Licence (LGPL), then the terms of that licence shall supersede any condition above with which it is incompatible.

The documentation for PCRE, supplied in the "doc" directory, is distributed under the same terms as the software itself.

End PCRE LICENCE

```
/*                            ZeusBench V1.01
                 ===============
```

This program is Copyright (C) Zeus Technology Limited 1996.

This program may be used and copied freely providing this copyright notice is not removed.

This software is provided "as is" and any express or implied waranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall Zeus Technology Ltd. be liable for any direct, indirect, incidental, special, exemplary, or consequential damaged (including, but not limited to, procurement of substitute good or services; loss of use, data, or profits; or business interruption) however caused and on theory of liability. Whether in contract, strict liability or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

     Written by Adam Twiss (adam@zeus.co.uk). March 1996

Thanks to the following people for their input:
  Mike Belshe (mbelshe@netscape.com)
  Michael Campanella (campanella@stevms.enet.dec.com)

*/
Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd
                               and Clark Cooper

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

==

Redistribution and use in source and binary forms of libcap, with or without modification, are permitted provided that the following conditions are met

1. Redistributions of source code must retain any existing copyright notice, and this entire permission notice in its entirety, including the disclaimer of warranties.

2. Redistributions in binary form must reproduce all prior and current copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of any author may not be used to endorse or promote products derived from this software without their specific prior written permission.

ALTERNATIVELY, this product may be distributed under the terms of the GNU General Public License, in which case the provisions of the GNU GPL are required INSTEAD OF the above restrictions. (This clause is necessary due to a potential conflict between the GNU GPL and the restrictions contained in a BSD-style copyright.)

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIEDWARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

This library (libselinux) is public domain software, i.e. not copyrighted.
Warranty Exclusion

You agree that this software is a non-commercially developed program that may contain "bugs" (as that term is used in the industry) and that it may not function as intended. The software is licensed "as is". NSA makes no, and hereby expressly disclaims all, warranties, express, implied, statutory, or otherwise with respect to the software, including noninfringement and the implied warranties of merchantability and fitness for a particular purpose.

Limitation of Liability

In no event will NSA be liable for any damages, including loss of data, lost profits, cost of cover, or other special, incidental, consequential, direct or indirect damages arising from the software or the use thereof, however caused and on any theory of liability. This limitation will apply even if NSA has been advised of the possibility of such damage. You acknowledge that this is a reasonable allocation of risk.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000
Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.
CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2004, Sparta, Inc All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----
Copyright (c) 2004, Cisco, Inc and Information Network
Center of Beijing University of Posts and Telecommunications.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULARPURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

```
-----
**********************************************************************
******
```

```
*
*
* Copyright (c) David L. Mills 1992-2003                              *
*
*
* Permission to use, copy, modify, and distribute this software and   *
* its documentation for any purpose and without fee is hereby         *
* granted, provided that the above copyright notice appears in all   *
* copies and that both the copyright notice and this permission       *
* notice appear in supporting documentation, and that the name    *
* University of Delaware not be used in advertising or publicity       *
*  pertaining  to  distribution  of  the  software  without  specific,
*
* written prior permission. The University of Delaware makes no       *
* representations about the suitability this software for any         *
* purpose. It is provided "as is" without express or implied          *
*                                                             warranty.
*
*
*
**********************************************************************
*******
----
```

The OpenLDAP Public License
Version 2.8, 17 August 2003

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions in source form must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.
Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

```
     * Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland
     *                    All rights reserved
     *
     * As far as I am concerned, the code I have written for this software
     * can be used freely for any purpose.  Any derived versions of this
     * software must be clearly marked as such, and if the derived work is
     * incompatible with the protocol description in the RFC file, it must
be
     * called by a name other than "ssh" or "Secure Shell".

    [Tatu continues]
     *  However, I am not implying to give any licenses to any patents or
     * copyrights held by third parties, and the software includes parts
that
     * are not under my direct control.  As far as I know, all included
       * source code is used in accordance with the relevant license
agreements
     * and can be used freely for any purpose (the GNU license being the
most
     * restrictive); see below for details.
```

[However, none of that term is relevant at this point in time. All of these restrictively licenced software components which he talks about have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library
- IDEA is no longer included, its use is deprecated
- DES is now external, in the OpenSSL library
- GMP is no longer used, and instead we call BN code from OpenSSL
- Zlib is now external, in a library
- The make-ssh-known-hosts script is no longer included
- TSS has been removed
- MD5 is now external, in the OpenSSL library
- RC4 support has been replaced with ARC4 support from OpenSSL
- Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "http://www.cs.hut.fi/crypto".

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The 32-bit CRC implementation in crc32.c is due to Gary S. Brown.
Comments in the file indicate it may be used for any purpose without restrictions:

```
     * COPYRIGHT (C) 1986 Gary S. Brown.  You may use this program, or
     * code or tables extracted from it, as desired without restriction.
```

```
* Cryptographic attack detector for ssh - source code
* Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.
*
* All rights reserved. Redistribution and use in source and binary forms,
with or without modification, are permitted provided that this copyright
notice is retained.
*
* THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR
*  IMPLIED  WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE
* SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING
* FROM THE USE OR MISUSE OF THIS SOFTWARE.
*
* Ariel Futoransky <futo@core-sdi.com>
* <http://www.core-sdi.com>

* Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.
*
* Modification and redistribution in source and binary forms is permitted
* provided that due credit is given to the author and the OpenBSD project
by
* leaving this copyright notice intact.

     * @version 3.0 (December 2000)
     *
     * Optimised ANSI C code for the Rijndael cipher (now AES)
     *
     * @author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>
     * @author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>
     * @author Paulo Barreto <paulo.barreto@terra.com.br>
```

```
     *
     * This code is hereby placed in the public domain.
     *
 * THIS SOFTWARE IS PROVIDED BY THE AUTHORS ''AS IS'' AND ANY
 * EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
 *THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
 * PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE
 * AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
 * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
 *  (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE
 * GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
 * INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
 * WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
 * NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF
 *THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

```
* Copyright (c) 1983, 1990, 1992, 1993, 1995
* The Regents of the University of California.  All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions are
met:
* 1. Redistributions of source code must retain the above copyright
notice, this
* list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. All advertising materials mentioning features or use of this software
*  must display the following acknowledgement:
*  This product includes software developed by the University of
California,
Berkeley and its contributors.
* 4. Neither the name of the University nor the names of its contributors
may
* be used to endorse or promote products derived from this software without
* specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE REGENTS AND
* CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED
*  WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
* WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
*  PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE
* REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT,
* INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL     * DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
*  SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
* INTERRUPTION)  HOWEVER CAUSED AND ON ANY THEORY OF
* LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
* (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE
*  POSSIBILITY OF  SUCH DAMAGE.

* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions are
met:
*  1. Redistributions of source code must retain the above copyright
notice, this
* list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
*  notice, this list of conditions and the following disclaimer in the
*  documentation and/or other materials provided with the distribution.
*
* THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY
* EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
* TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS
* FOR A PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL
* THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT,  INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING,
* BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR
* SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS
* INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF
* LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
* (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT * OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE
* POSSIBILITY OF SUCH DAMAGE.
```

```
/* ====================================================================
 * Copyright (c) 1998-2002 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are
met:
 *
 * 1. Redistributions of source code must retain the above copyright
notice, this
 * list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *  notice, this list of conditions and the following disclaimer in the
 * documentation and/or other materials provided with the distribution.
 *
 * 3. All advertising materials mentioning features or use of this software
must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project for
use
 *   in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used
 * to  endorse or promote products derived from this software without prior
 * written permission. For written permission,
 * please contac openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL" nor
 * may "OpenSSL" appear in their names without prior written permission
of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *  acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS''
 * AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT
 * NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY
 * AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.  IN
 * NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE
 * LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
 * EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
 * LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
 * CONTRACT,  STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
 * OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF
* ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */
/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation
 * written by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
the
 * following conditions are aheared to.  The following conditions apply
to all
 * code found in this distribution, be it the RC4, RSA, lhash, DES, etc.,
code;
 * not just the SSL code.  The SSL documentation included with this
 * distribution is covered by the same copyright terms except that the
holder is
 * Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in the
 * code are not to be removed.  If this package is used in a product, Eric
Young
 * should be given attribution as the author of the parts of the library
used.
 * This can be in the form of a textual message at program startup or in
 *  documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are
met:
 * 1. Redistributions of source code must retain the copyright notice,
this list of
 * conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *  notice, this list of conditions and the following disclaimer in the
 *   documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *   must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *     The word 'cryptographic' can be left out if the rouines from the
library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof)
from
  *  the  apps  directory  (application  code)  you  must  include  an
acknowledgement:
  *       "This  product  includes  software  written  by  Tim  Hudson
(tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY
 * EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED
 * TO, THE  IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS
 * FOR A PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT
 * SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY
 * DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
 * CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
 * PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
 * USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
 * CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE
 * OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
 * SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
 * DAMAGE.
 *
 * The licence and distribution terms for any publically available version
or
 * derivative of this code cannot be changed.  i.e. this code cannot simply
be
 * copied and put under another distribution licence
 *  [including the GNU Public Licence.]
 */
----
```

Redistribution and use in source and binary forms of Linux-PAM, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain any existing copyright notice, and this entire permission notice in its entirety, including the disclaimer of warranties.

2. Redistributions in binary form must reproduce all prior and current copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of any author may not be used to endorse or promote products derived from this software without their specific prior written permission.

ALTERNATIVELY, this product may be distributed under the terms of the GNU General Public License, in which case the provisions of the GNU GPL are required INSTEAD OF the above restrictions. (This clause is necessary due to a potential conflict between the GNU GPL and the restrictions contained in a BSD-style copyright.)

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 1998 Red Hat Software

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE X CONSORTIUM BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of the X Consortium shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from the X Consortium.

```
/*-
 * Copyright (c) 1990 The Regents of the University of California.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are
met:
  * 1. Redistributions of source code must retain the above copyright
notice, this
 * list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *   documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 * This product includes software developed by the University of
 * California, Berkeley and its contributors.
 * 4. Neither the name of the University nor the names of its contributors
may
 *  be used to endorse or promote products derived from this software
 *   without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND
 * CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED
 * WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
 * WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
 * PARTICULAR PURPOSE ARE DISCLAIMED.
* IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR
* CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
* PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF
* USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)  HOWEVER
* CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
* CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
* OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
* SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
* DAMAGE.
 */
```

Copyright (C) 2002 Roaring Penguin Software Inc.

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Roaring Penguin Software Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Roaring Penguin Software Inc..
Roaring Penguin Software Inc. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright (C) 1995,1996,1997,1998 Lars Fenneberg <lf@elemental.net>

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Lars Fenneberg not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Lars Fenneberg.

Lars Fenneberg makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Copyright 1992 Livingston Enterprises, Inc.
Livingston Enterprises, Inc. 6920 Koll Center Parkway Pleasanton, CA 94566

Permission to use, copy, modify, and distribute this software for any purpose and without fee is hereby granted, provided that this copyright and permission notice appear on all copies and supporting documentation, the name of Livingston Enterprises, Inc. not be used in advertising or publicity pertaining to distribution of the program without specific prior permission, and notice be given in supporting documentation that copying and distribution is by permission of Livingston Enterprises, Inc.

Livingston Enterprises, Inc. makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

[C] The Regents of the University of Michigan and Merit Network, Inc. 1992, 1993, 1994, 1995 All Rights Reserved

Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies of the software and derivative works or modified versions thereof, and that both the copyright notice and this permission and disclaimer notice appear in supporting documentation.

THIS SOFTWARE IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE REGENTS OF THE UNIVERSITY OF MICHIGAN AND MERIT NETWORK, INC. DO NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET LICENSEE'S REQUIREMENTS OR THAT OPERATION WILL BE UNINTERRUPTED OR ERROR FREE. The Regents of the University of Michigan and Merit Network, Inc. shall not be liable for any special, indirect, incidental or consequential damages with respect to any claim by Licensee or any third party arising from use of the software.

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991.
All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

```
/************************************************************************
*
* Copyright 1995 by Wietse Venema.  All rights reserved.  Some individual
* files may be covered by other copyrights.
*
* This material was originally written and compiled by Wietse Venema at
* Eindhoven University of Technology, The Netherlands, in 1990, 1991,
* 1992, 1993, 1994 and 1995.
*
* Redistribution and use in source and binary forms are permitted provided
* that this entire copyright notice is duplicated in all such  copies.
*
* This software is provided "as is" and without any expressed or implied
* warranties, including, without limitation, the implied warranties of
* merchantibility and fitness for any particular purpose.
*************************************************************************
/
```

```
/*
 * Copyright (c) 1989 The Regents of the University of California.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are
met:
  * 1. Redistributions of source code must retain the above copyright
notice, this
 * list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *   documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
  *  This product includes software developed by the University of
California,
 *  Berkeley and its contributors.
 * 4. Neither the name of the University nor the names of its contributors
may
 *  be used to endorse or promote products derived from this software
 *  without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND
 * CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED
 * WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
 * WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
 * PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE
 * REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT,
 * INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
 * SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
 * PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER
 * IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
 * NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
 * USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 *from: @(#)telnetd.h       5.3 (Berkeley) 3/1/91
 *$Id: telnetd.h,v 1.2 1999/03/27 07:46:21 dholland Exp $
 */

----
/*
 * Copyright (c) 1989 The Regents of the University of California.
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions are
met:
 * 1. Redistributions of source code must retain the above copyright
notice, this
 * list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *     must display the following acknowledgement:
 * This product includes software developed by the University of
 * California, Berkeley and its contributors.
 * 4. Neither the name of the University nor the names of its contributors
may
 * be used to endorse or promote products derived from this software
 *  without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE REGENTS AND
 * CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED
 * WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
 * WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A
 * PARTICULAR PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE
 * REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT,
 * INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF
 *  SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR
 * PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER
 * IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING
 * NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
 *  USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 */
----
ORIGINAL LICENSE:
This software is

(c) Copyright 1992 by Panagiotis Tsirigotis

The author (Panagiotis Tsirigotis) grants permission to use, copy, and
distribute this software and its documentation for any purpose and without
fee, provided that the above copyright notice extant in files in this
distribution is not removed from files included in any redistribution and
that this copyright notice is also included in any redistribution.
Modifications to this software may be distributed, either by distributing
the modified software or by distributing patches to the original software,
under the following additional terms:

1. The version number will be modified as follows:
      a. The first 3 components of the version number
         (i.e <number>.<number>.<number>) will remain unchanged.
     b. A new component will be appended to the version number to indicate
        the modification level. The form of this component is up to the
         author of the modifications.
2. The author of the modifications will include his/her name by appending
it
   along with the new version number to this file and will be responsible
for
   any wrong behavior of the modified software.

The author makes no representations about the suitability of this software
for any purpose.  It is provided "as is" without any express or implied
warranty.

Modifications:
Version: 2.1.8.7-current
Copyright 1998-2001 by Rob Braun

Sensor Addition
Version: 2.1.8.9pre14a
```

```
Copyright 2001 by Steve Grubb

This is an exerpt from an email I recieved from the original author,
allowing xinetd as maintained by me, to use the higher version numbers:

I appreciate your maintaining the version string guidelines as specified
in the copyright. But I did not mean them to last as long as they did.

So, if you want, you may use any 2.N.* (N >= 3) version string for future
xinetd versions that you release. Note that I am excluding the 2.2.* line;
using that would only create confusion. Naming the next release 2.3.0
would put to rest the confusion about 2.2.1 and 2.1.8.*.

/* zlib.h -- interface of the 'zlib' general purpose compression library
  version 1.2.1, November 17th, 2003

  Copyright (C) 1995-2003 Jean-loup Gailly and Mark Adler

   This software is provided 'as-is', without any express or implied
warranty.  In no event will the authors be held liable for any damages
arising from the use of this software.

  Permission is granted to anyone to use this software for any purpose,
including commercial applications, and to alter it and redistribute it
freely, subject to the following restrictions:

  1. The origin of this software must not be misrepresented; you must not
claim that you wrote the original software. If you use this software in a
product, an acknowledgment in the product documentation would be
appreciated but is not required.
  2. Altered source versions must be plainly marked as such, and must not
be      misrepresented as being the original software.
    3. This notice may not be removed or altered from any source
distribution.

  Jean-loup Gailly        Mark Adler
  jloup@gzip.org          madler@alumni.caltech.edu

  The data format used by the zlib library is described by RFCs (Request
for Comments) 1950 to 1952 in the files
http://www.ietf.org/rfc/rfc1950.txt  (zlib format), rfc1951.txt (deflate
format) and rfc1952.txt (gzip format).
*/
```

Index