

System Service Processor Administration

Objectives

Upon completion of this module, you should be able to do the following:

- Explain the functions of the System Service Processor (SSP)
- Describe how the SSP interacts with the system
- Describe security considerations relevant to the Sun Enterprise™10000 server
- Plan the network for a Sun Enterprise10000 server and its SSP
- Completely install the SSP software
- Accomplish a manual failover from the main SSP to the spare SSP
- Configure automatic failover of the main SSP to the spare SSP
- Perform control board switch-over

This module presents details about the SSP. It covers the software used on the SSP to communicate with the Sun Enterprise10000 server. In this module, you learn how to perform common administrative tasks associated with the SSP.

Relevance

Present the following questions to stimulate the students and get them thinking about the issues and topics presented in this module. While they are not expected to know the answers to these questions, the answers should be of interest to them and motivate them to learn the material presented in this module.



Discussion – The following answers to these questions are relevant to understanding the content of this module:

- What kind of hardware configuration is required for the SSP?
- What special software needs to be installed on the SSP?
- What post-installation configuration is required on the SSP?
- Why is there a need for a spare SSP?

Additional Resources



Additional resources – The following resources and reference materials can provide additional details on the topics discussed in this module:

- Sun Microsystems, Inc., November 2001, *Sun Enterprise™ 10000 SSP 3.5 User's Guide*, Part Number 806-7613-05.
- Sun Microsystems, Inc., October 2001, *Sun Enterprise™ 10000 SSP 3.5 Installation Guide and Release Notes*, Part Number 806-7615-05.
- Sun Microsystems, Inc., *Sun Enterprise™ 10000 System Hardware Installation and De-Installation Guide*, Part Number 805-4651-10.
- The man pages for the commands, daemons, and files.

Be sure to tell the students that these documents are available at <http://docs.sun.com>.

The System Service Processor

The System Service Processor (SSP) enables you to control and monitor the Sun Enterprise 10000 server. The SSP is as much an integral part of the Sun Enterprise 10000 server as any of the system boards, fans, or control boards. An SSP is included as part of the Sun Enterprise 10000 server.

SSPs, as supplied by Sun, are available in the following configurations:

- SPARC Ultra™ 5 workstation with one 360 MHz CPU module, 128 Mbyte memory, 8.4 Gbyte internal disk, 32X CD-ROM, Quad Fast Ethernet (QFE) PCI Card, and 19 inch color monitor up to SSP version 3.4
- Two Sun Netra™ T1 AC200 servers, each with one 500 MHz CPU, 2 Mbyte ecache, 256 Mbyte memory, two 18 Gbyte internal drives, one QFE PCI card, and one CD-ROM drive, two 4mm 20 Gbyte tape drives, cables, and a rackmount kit. The entire package is mounted inside the Sun Enterprise 10000 server enclosure. Supported beginning with SSP version 3.3.
- Sun Enterprise™ 250 server with one 400 MHz CPU module, 256 Mbyte memory, two 9.1-GByte internal disks, 32X CD-ROM, 4mm DDS3 tape, and QFE PCI card.

Sun Netra T1 AC200 is not configurable when using Dual Power Configuration or more than 12 Unipack internal boot disks.

Pre-Release – Read Only

SSP Functions

The SSP enables you to do the following:

- Boot domains
- Perform automatic emergency shutdown in an orderly fashion
- Create domains
- Dynamically reconfigure a domain interactively
- Dynamically reconfigure a domain automatically
- Monitor and display the temperature and voltage levels of one or more system boards or domains
- Control fan operations
- Monitor and control power to the components within a system
- Execute diagnostic programs in a domain such as power-on self-test (POST)
- Set up automatic failover thresholds for disk and virtual memory

In addition, the SSP environment is capable of the following:

- Provides console access to the domains on the system
- Warns you of potential problems, such as high temperatures or malfunctioning power supplies
- Notifies you when a software error or failure has occurred
- Automatically reboots a domain after a system software failure
- Keeps logs of the interactions between the SSP and the domains
- Provides support for Inter-Domain Networking (IDN)

Network Planning

Before you can install your system, you need to know what your network should look like. There are a large number of Sun Enterprise 10000 server components that require network addresses. The following is a list of these components:

- The primary and spare SSP
- One or two control boards
- Up to sixteen domains

Some of these require multiple addresses. The SSP can have as many as four subnets, and the domains at least two.

There are several different configurations that work, but all have a common factor: The control boards and corresponding SSPs must exist on separate physical networks from other machines. The reasons for this are both security and performance related and are discussed later in this module.



Caution – Always isolate the control boards on their own network.

Network Considerations

The basic choices that you have to make for the network configuration are as follows:

- Should the domain-to-SSP interfaces be on a private or public network?
- Should a spare SSP be configured?

After these issues are decided, you can begin to assign host names and Internet Protocol (IP) addresses and configure the network for the system.

SSP-to-Sun Enterprise 10000 Connectivity

Communication between an SSP and the system requires a private Ethernet network for the control boards. In addition to the private network, best practices require a private network for the domains and support public networks.

Figure 3-1 shows a recommended layout for the Sun Enterprise 10000 server. Each control board, domain, and SSP network interface must have a unique host name and IP address that are subnetted appropriately.

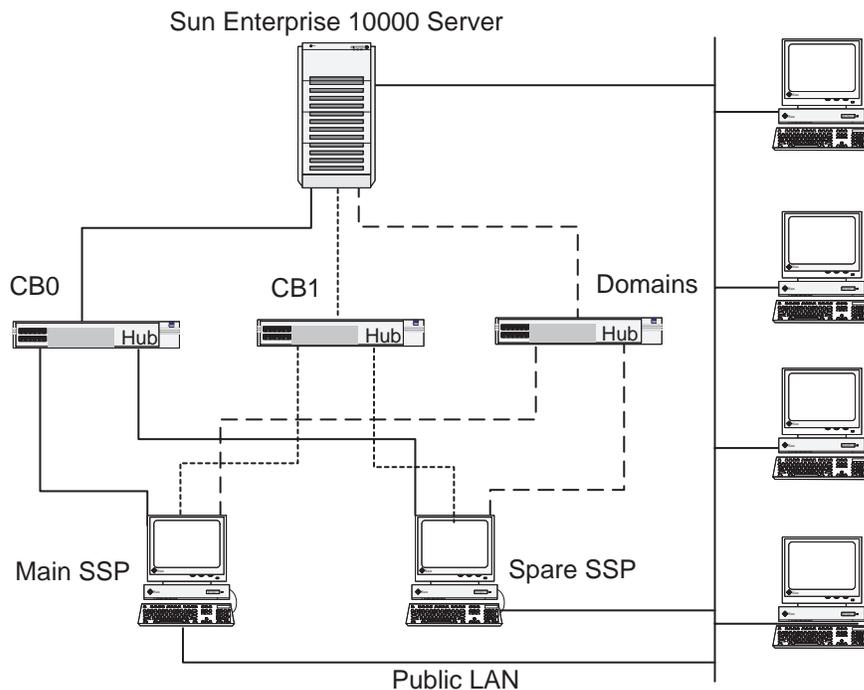


Figure 3-1 SSP-to-Sun Enterprise 10000 Server Connectivity

Private Control Board Network

The private control board network connects the SSP to the control boards.

The control board supports communication between the SSP and Sun Enterprise 10000 server components. This includes communication for support subsystems such as power and cooling.

Private Domain Network

The private domain network connects the SSPs directly to the domains. Each domain has its own connection to the private domain network hub.

Connecting the SSP directly to the domains, through an Ethernet connection, provides system administrators with a more efficient path for administrating the Solaris Operating Environment and user applications running on the domains. This path is not used when the Solaris Operating Environment is down.

Point out to the students that the communication between the control board and the JTAG hardware takes place at 300 baud.

Public Network

The public network connects the Sun Enterprise 10000 server to client sites for access by users. The public domain network must be on a physically separate network from the control boards. Remember to create the `/etc/notrouter` file on the SSP to prevent the SSP from routing domain traffic.

Pre-Release – Read Only

Control Board Network Considerations

The control board network can be configured in two different ways, as is shown in Figure 3-2.

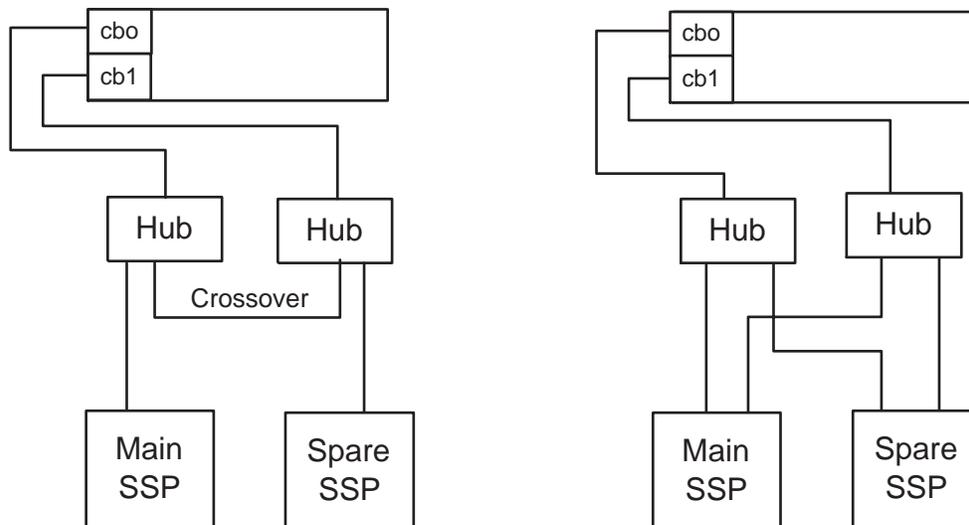


Figure 3-2 Control Board Considerations

SSP Single Network Interface

In an SSP single interface environment, both control boards are on a single subnet. This requires one network interface on each SSP. In order to eliminate a single point of failure, dual hubs should be used connected with a crossover cable.

SSP Dual Network Interface

In an SSP dual interface environment, each control board is on a separate subnet. This requires two network interfaces on each SSP. This network configuration is required for *automatic failover* of the SSP.

Note – While the single network interface configuration is supported, the dual network interface is strongly recommended.



The instructor should point out that for SSP version 3.4 (or later) automated failover to be enabled, **ONLY** the dual subnet configuration can be used.

Sample hosts File

The following is a sample `/etc/inet/hosts` file that shows all the SSP and domain addresses:

```
# Control boards
10.1.0.200    jefferson          # CB 0
10.2.0.200    madison            # CB 1
# Main SSP interfaces
10.1.0.201    franklin-c0        # CB 0 dedicated interface
10.2.0.201    franklin-cl        # CB 1 dedicated interface
10.3.0.201    franklin-d         # Private domain interface
12.1.1.230    franklin franklin.sun.com # Outside interface
# Spare SSP interfaces
10.1.0.202    hamilton-c0
# CB 0 dedicated interface
10.2.0.202    hamilton-cl        # CB 1 dedicated interface
10.3.0.202    hamilton-d         # Private domain interface
12.1.1.231    hamilton hamilton.sun.com # Outside interface
# Floating IP for domains to talk to
10.3.0.1     live-ssp           # Private domain interface VIP
# Private domain interfaces to the SSP
10.3.0.203    washington-ssp
10.3.0.204    adams-ssp
10.3.0.205    lincoln-ssp
10.3.0.206    jackson-ssp
10.3.0.207    grant-ssp
10.3.0.208    kennedy-ssp
10.3.0.209    johnson-ssp
# Domain interfaces to the outside world
12.1.1.232    washington
12.1.1.233    adams
12.1.1.234    lincoln
12.1.1.235    jackson
12.1.1.236    grant
12.1.1.237    kennedy
12.1.1.238    johnson
```



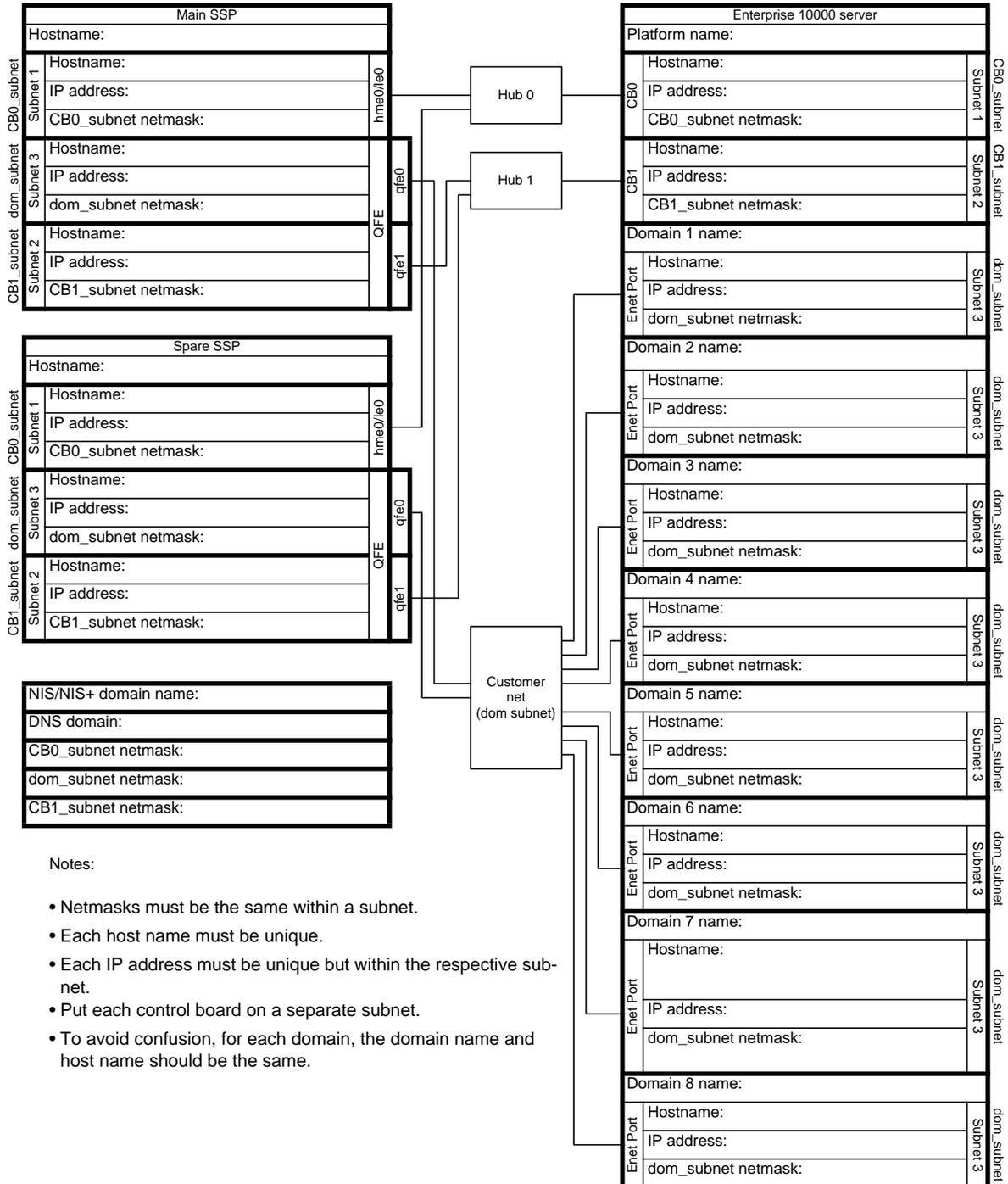
In this configuration, `/etc/notrouter` is created so that the SSP does not route traffic from outside to the domain private interfaces.

Note – The netmask for the 10.0.0.0 network would be 255.255.0.0 in the above example.

Pre-Release – Read Only

Planning Worksheet

Figure 3-3 provides a worksheet that shows the network configuration for your environment.



Notes:

- Netmasks must be the same within a subnet.
- Each host name must be unique.
- Each IP address must be unique but within the respective subnet.
- Put each control board on a separate subnet.
- To avoid confusion, for each domain, the domain name and host name should be the same.

Figure 3-3 Sun Enterprise 10000 Server Planning Worksheet

At this point, provide the students with the classroom network setup they are to use in lab.

Pre-Release – Read Only

SSP Security Considerations

The network connecting the SSPs to the control boards should be accessible *only* by the SSPs and control boards.

Initial communication between the SSP and the Sun Enterprise 10000 server puts a Reverse Address Resolution (RARP) Ethernet packet on each control board network destined to the Ethernet address of the SSP.

If other systems are allowed physical access to this network, Denial of Service (DOS) attacks would be possible.

Decrease exposure by doing the following:

- Limiting physical access to the SSP
- Limiting physical access to the SSP and control board network
- Not connecting any other devices to the SSP and control board network

Pre-Release – Read Only

SSP-to-Control Board Communications

At startup, the main SSP sends a `cb_reset`, causing the control boards to reboot. See Figure 3-4.

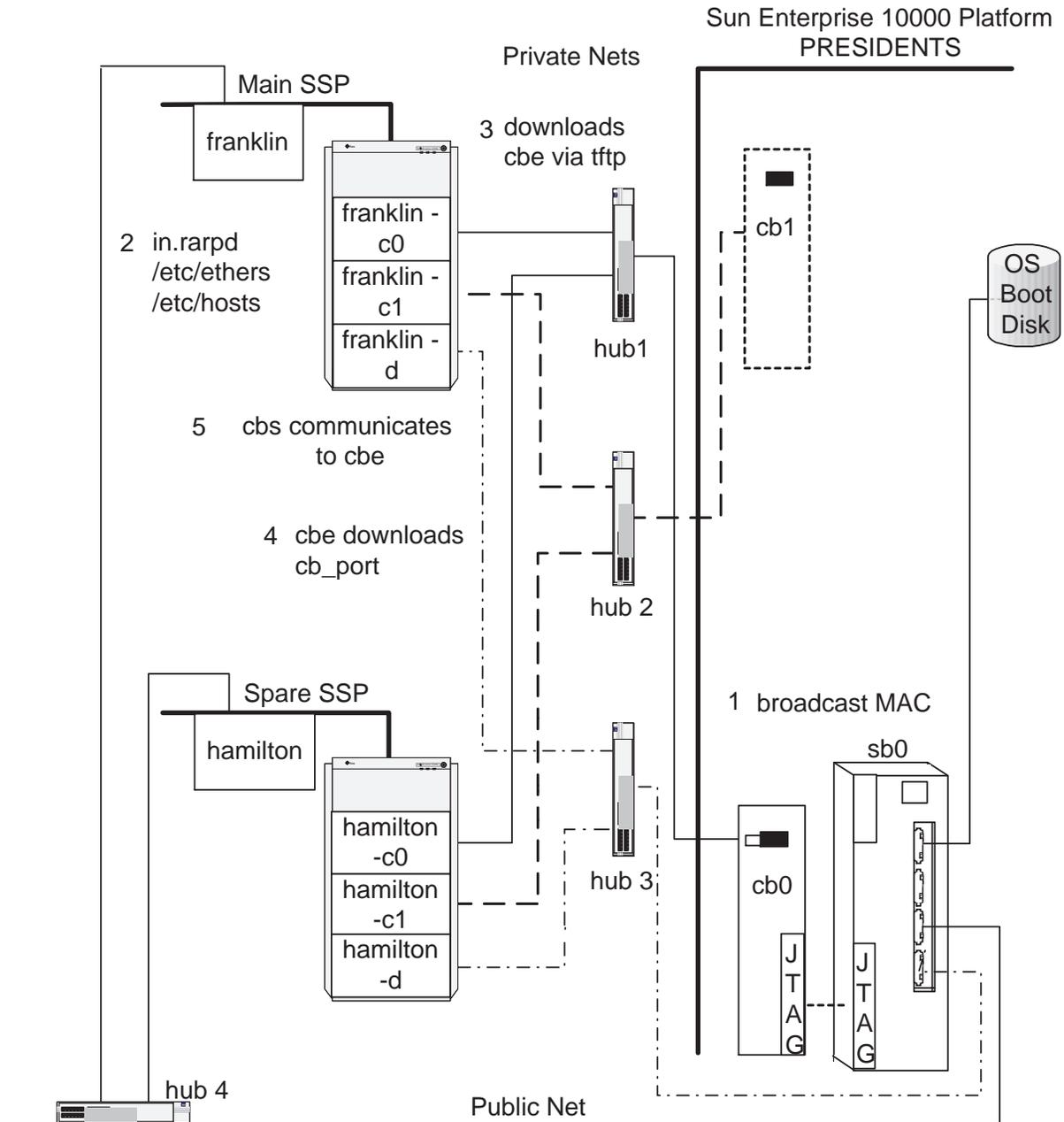


Figure 3-4 The SSP and Sun Enterprise 10000 Server Interaction

1. After resetting, each control board uses its initialization program in the control board flash PROM to send out an RARP request.

Pre-Release – Read Only

2. The `in.rarpd` daemon on the main SSP responds with the IP address of the control board using the `/etc/ethers` and `/etc/hosts` files.
3. The control board downloads the Control Board Executive (`cbe`) daemon using `tftp`. The file name, which is the control board's IP address in hexadecimal format, is located in the `/tftpboot` directory.

CB Name	CB IP Address	CBE File Name	cb_port File Name
madison	10.2.0.200	0A0200C8	0A0200C8.cb_port
jefferson	10.1.0.200	0A0100C8	0A0100C8.cb_port

4. The `cbe` daemon downloads the appropriate `cb_port` file, which defines the input and output ports that it should use for communication. The `cbe` daemon monitors environmental (temp, power, and fans) using the Joint Test Action Group (JTAG) controller.
5. The `cbe` daemon waits to be contacted by the Control Board Server (`cbs`) daemon running on the SSP. Communication is now established between the Sun Enterprise 10000 server and the SSP. At this point, the fans spin down to nominal speed.

The domains can now be initialized through the `bringup` process. See "The Domain `bringup` Process" on page 7-5.

Note – The control board resets in the event of a power cycle.



The `cbs` and `cbe` Daemons

The Control Board Server (`cbs`) daemon runs on the SSP to provide the communication interface to the Sun Enterprise 10000 server. Whenever a client program running on the SSP (such as `hostview`) needs to access the Sun Enterprise 10000 server, the communication is handled by the `cbs` daemon. The `cbs` daemon communicates directly with the Control Board Executive (`cbe`) daemon running on the active control board. The `cbs` daemon converts client requests to the Control Board Management Protocol (CBMP), which is understood by the `cbe` daemon.

The `cbs` daemon sends commands over the Transmission Control Protocol/Internet Protocol (TCP/IP) to the `cbe` daemon running on the control board. The `cbe` daemon monitors and controls the Sun Enterprise 10000 server hardware through JTAG, under the direction of various SSP applications. Normal domain network traffic, such as File Transfer Protocol (FTP), is handled through the normal TCP/IP interfaces, not by the `cbs` daemon.

The `cbs` daemon uses the `cb_config` file to determine which control board it is to communicate with as the primary board. The `cbs` daemon connects to primary control board, and makes it the system master control board.

To make the other control board the primary, the `cb_config` file must be updated.

The `cb_reset` Command

The `cb_reset` command resets and reboots control boards. It is used by the main SSP at boot time to cause all control boards to re-initialize, and it can also be used to reset individual control boards if they have stopped responding. The `cb_reset` command does not affect active domains.

```
hamilton:presidents% cb_reset madison
Resetting host madison...
madison is ready...
```

The `cb_reset` command's behavior is determined by the `cb_config` file located in the `$SSPVAR/.ssp_private` directory. This file identifies the names of the systems that are managed by the SSP and contains the names of both the primary and spare control boards.



Note – Although the files and commands are set up to allow a single set of SSPs to manage multiple Sun Enterprise 10000 servers, this is not currently supported.

The `cb_prom` Command

The `cb_prom` command maintains the flash PROM on the control boards. The `SUNWsspfp` package includes an updated PROM image. The following commands show examples of using `cb_prom`:

- Querying flash version

```
franklin:presidents% cb_prom -r -h madison
Checking PROM revision... 3.47
```

- Saving flash version

```
franklin:presidents% cb_prom -d madison.prom.image -h madison
Dumping PROM... complete.
```

- Updating flash version

```
franklin:presidents% cb_prom -p flash_boot.ima -h madison
Programming PROM.... complete.
```



Caution – Do *not* interrupt the flash PROM programming process. It can take several minutes to complete.

Network Console

The network console feature, shown in Figure 3-5, provides system administrators with a remote connection from the SSP to a domain over a TCP/IP network.

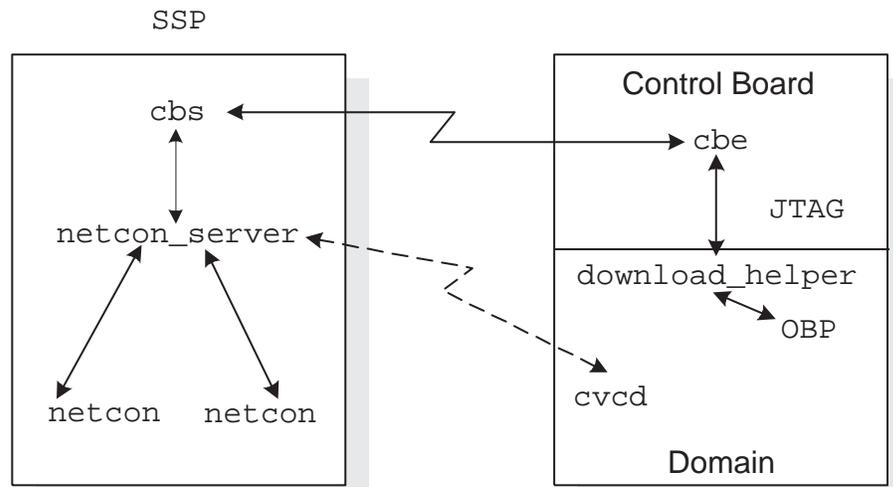


Figure 3-5 Network Console

Two programs are provided for this purpose:

- `netcon`
- `netcontool`



Note – The `netcontool` program is a GUI for the `netcon` program. For the purposes of this discussion, `netcon` functionality is explained. Details on `netcontool` usage are provided in Module 6, “Boot Devices.”

The `netcon` Program

The `netcon` program creates a remote connection to the domain host console program, making the SSP window in which the program is executed a console window for the domain specified by the `SUNW_HOSTNAME` variable.

The `netcon` program can use either the standard network interface or the JTAG interface for domain console window communication. Table 3-1 describes important `netcon` directives.

Table 3-1 Important `netcon` Directives

Directive	Description
<code>~#</code>	Sends break
<code>~.</code>	Performs a disconnect

Multiple people can run simultaneous `netcon` sessions; however, only one of those sessions has the ability to accept input.

The `netcon_server` Program

The `netcon_server` program manages communications between the SSP console window and the specified boot processor of the corresponding domain specified by `SUNW_HOSTNAME` environment variable. There is one instance of `netcon_server` for each domain.

When the domain is up, `netcon_server` acts as a relay between the domain console window and the `cvcd` daemon running on the domain side. When the domain is down, `netcon_server` is a relay between the domain console windows and OBP.

The `cvcd` Daemon

The `cvcd` daemon, which gets its name from the Cray Virtual Console Daemon, is a server process that resides on a Sun Enterprise 10000 server domain. The `cvcd` daemon accepts connections from the `netcon_server` using the private domain network to create a network console window on that SSP. The network console window is able to read data from, and send data to, the domain. This process takes place by way of the SSP `netcon` command.

In order for `cvcd` to communicate with the `netcon_server`, the `/etc/ssphostname` file in the domain must be configured correctly with the virtual IP address assigned for failover capability.

Failover

Communication failover, available starting with release SSP 3.4, requires a logical IP address to be assigned the active private domain network interface on the SSP. The `/etc/ssphostname` in the domain contains either this logical IP address or a name resolved through `/etc/hosts`. When a failover occurs the logical IP address is terminated on the original SSP and restarted on the backup SSP.

The SSP Environment

This section describes the different components that exist in the SSP Environment

SSP Accounts

The SSP requires the following two accounts:

- The `root` account

The `root` account is used to manage the SSP itself and is created when the Solaris Operating Environment is installed.

- The `ssp` account

The `ssp` account is created when the SSP software is installed and is used to control the Sun Enterprise 10000 server and its domains. The install process also installs the `.cshrc` and `.login` files. The account assumes that it is running the C shell; do not modify this default. The default password for the `ssp` account is `ssp`.

Logging in to the SSP

After the software is installed, you can log in to the SSP as user `ssp`. The initial password for this account can be `ssp`, but if it is not, simply log in as `root` and set the password.

```
franklin/# passwd ssp
New password: ssp123
Re-enter new password: ssp123
passwd (SYSTEM): passwd successfully changed for ssp
```

Whenever you log in or open a new terminal window, you are prompted to enter a value for the `SUNW_HOSTNAME` variable.

Enter the name of the domain you want to work with. If you are not sure what domain you want to work with, just enter the name of the system. For example, `presidents`.

```
franklin:/# su - ssp
Sun Microsystems Inc. SunOS 5.8 Generic February 2000
Please enter SUNW_HOSTNAME: presidents
franklin:presidents%
```

Pre-Release – Read Only

The SSP Environment Variables

A number of environment variables are set for the `ssp` account on the SSP. These variables are as follows:

- `$SUNW_HOSTNAME`

No default; it must be set to the name of the domain or system being controlled. The value can be changed by using the `domain_switch` command.

- `$SSPETC`

This variable has the value `/etc/opt/SUNWssp`. This directory contains the SSP startup scripts.

- `$SSPVAR`

This variable has the value `/var/opt/SUNWssp`. This directory contains:

- System and domain configuration files
- Log files
- Scan data files
- Daemon lock files
- The `.ssp_private` directory, which contains `$SUNW_HOSTNAME` configuration files. The contents of this directory must be consistent between the main and spare SSPs.

- `$SSPLOGGER`

This variable has the value `/var/opt/SUNWssp/adm`. This directory contains Sun Enterprise 10000 server log files. Each domain has its own sub-directory here containing domain-specific log files.

- `$SSPOPT`

This variable has the value of `/opt/SUNWssp`:

- The `$SSPOPT/bin` directory contains SSP executables.
- The `$SSPOPT/man` directory is the base directory for the man pages for the SSP software.

The SSP File Structure

The SSP file structure provides the supporting configuration files for the Sun Enterprise 10000 server. See Figure 3-6.

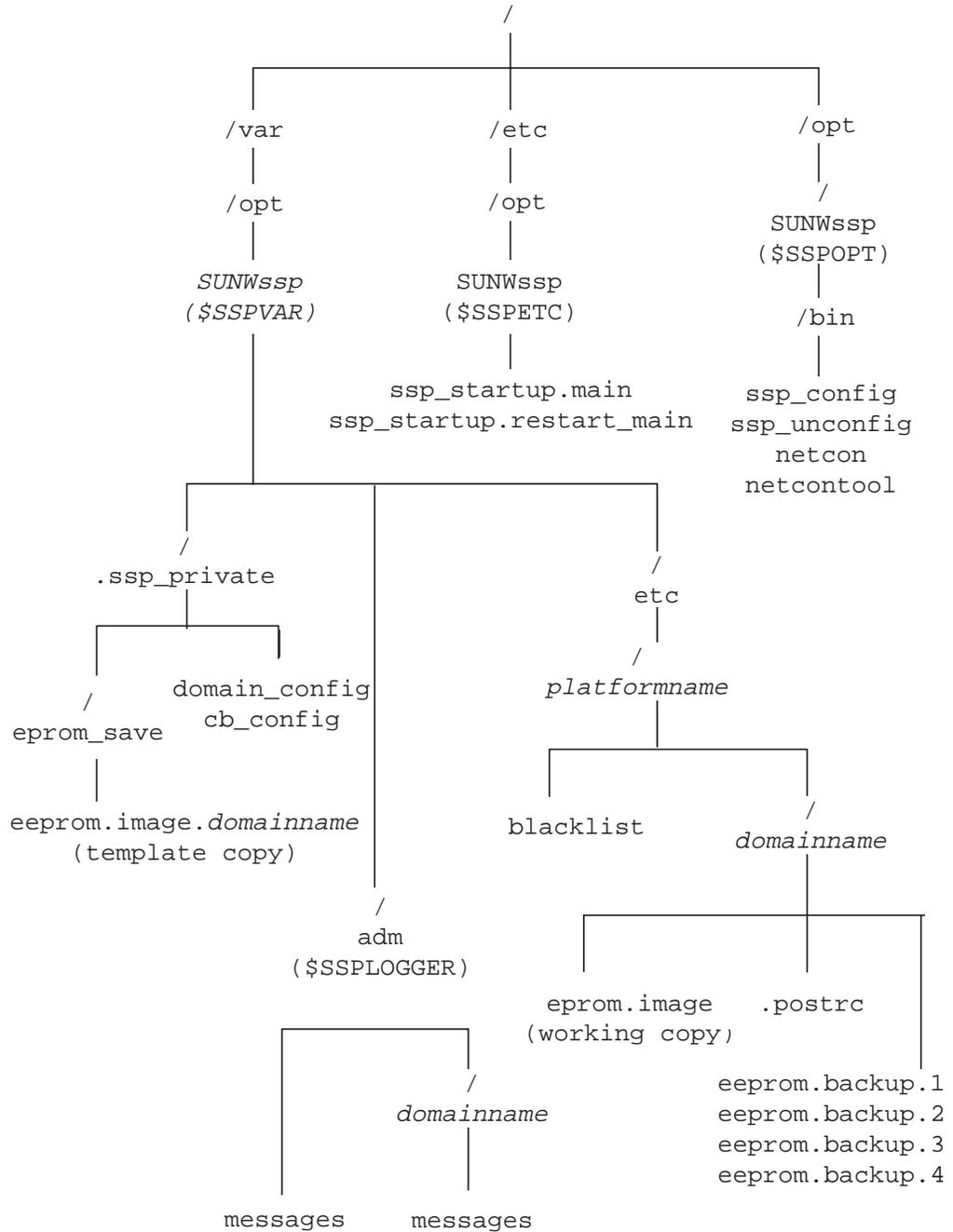


Figure 3-6 SSP File System Structure

Pre-Release – Read Only

The SSP Boot Process

Figure 3-7 shows an outline of the boot process and the daemons that are started.

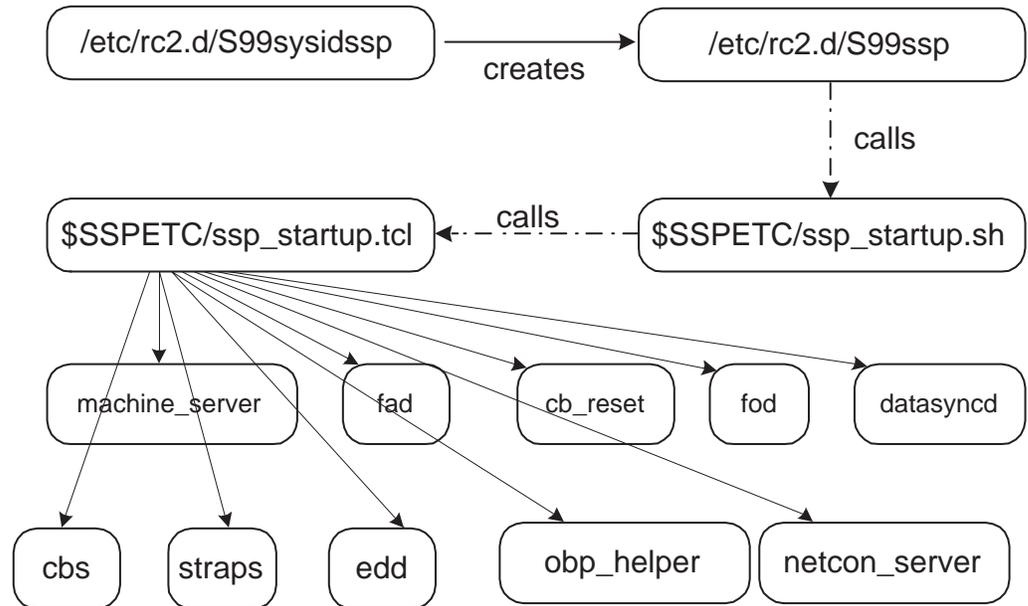


Figure 3-7 The SSP Boot Process

The SSP installation creates a startup script called `/etc/rc2.d/S72sysidssp`, which calls `ssp_config`, as shown in Figure 3-7.

The `ssp_config` Command

The `ssp_config` command performs the following tasks when specific conditions are met:

- It is called only on the first boot after installation
- It prompts the administrator for the configuration information
- It populates the configuration files in `$SSPVAR/.ssp_private`
 - `cb_config`
 - `ssp_resource`
- It creates a new startup script called `/etc/rc2.d/S99ssp`

The /etc/init.d/S99ssp Script

The /etc/init.d/S99ssp script runs `$$SSPETC/sp_startup.sh` in the background.

The /etc/opt/SUNWssp/ssp_startup.sh Script

This script calls the `$$SSPETC/ssp_startup.tcl` script and converts itself into a monitoring program for `syslogd`.

The /etc/opt/SUNWssp/ssp_startup.tcl Script

This script does the following:

- Starts only the daemons that need to run on both the main and the spare SSP that are listed in `$$SSPETC/ssp_startup.remote` directory.
 - `machine_server`
 - `fad`
 - `fod` (This feature is available as of release SSP 3.4.)
- Determines if the SSP should assume the role of main SSP by running `showfailover -r`. (This feature is available as of release SSP 3.4.)
- If the server is the main SSP, then the `$$SSPETC/ssp_startup.tcl` script starts the additional daemons that need to run. These daemons are listed in `$$SSPETC/ssp_startup.main` directory.
 - `datasyncd` (This feature is available in SSP as of release 3.4.)
 - `cbs`
 - `straps`
 - `edd`
 - `obp_helper` (one for each running domain)
 - `netcon_server` (one for each running domain)
 - `cb_reset` (not a daemon)

Point out to the students that the name of the TCL interpreter is "scotty." With a name like that, they might be tempted to beam up or kill off this daemon, with potentially disastrous results.

The SSP Daemons

Table 3-2 summarizes the functions of the SSP daemons. Following the table is a more in depth look at key daemons.

Table 3-2 SSP Daemons and Their Functions

SSP Daemon	Function
cbs	The Control Board Server provides central access to the Sun Enterprise 10000 server control board for client programs running on the SSP.
edd	The Event Detector Daemon uploads event detection scripts to control boards. When one of these scripts detects an event, edd executes a response action script.
netcon_server	This daemon is the connection point for all netcon clients.
snmpd	The Simple Network Management Protocol (SNMP) Proxy Agent Daemon listens to a User Datagram Protocol (UDP) port for incoming requests, and services the objects specified in <code>Ultra-Enterprise-10000.mib</code> .
straps	The SNMP Trap Sink Server listens to the SNMP trap port for incoming trap messages and forwards received messages to all connected clients.
xntpd	The NTP Daemon provides time synchronization services. This service is used to automatically synchronize SSP and domain times.
fad	The File Access Daemon provides file access services to SSP clients that need to monitor, read, and write to the SSP configuration files.
machine_server	This daemon services the TCP port registration requests from netcon_server and ensures that error messages are routed to the proper message file.
obp_helper	During execution, obp_helper provides services to OBP such as nvr _{am} simulation, ID _{prom} simulation, and time of day.
fod	The Fail-Over Daemon monitors SSP to control board communication (starting with SSP 3.4 release).
datasyncd	This daemon keeps files in sync between main and spare SSP. (This feature is available in SSP as of release 3.4.)



Caution – Never run these daemons manually unless directed to do so by the product documentation or a support representative.

The Event Detection Daemon (edd)

If an event detection, on the Sun Enterprise 1000 server, indicates a change of state that warrants an event, an event message is generated and delivered to the `cbs` daemon by the `cbe` daemon as shown in Figure 3-8.

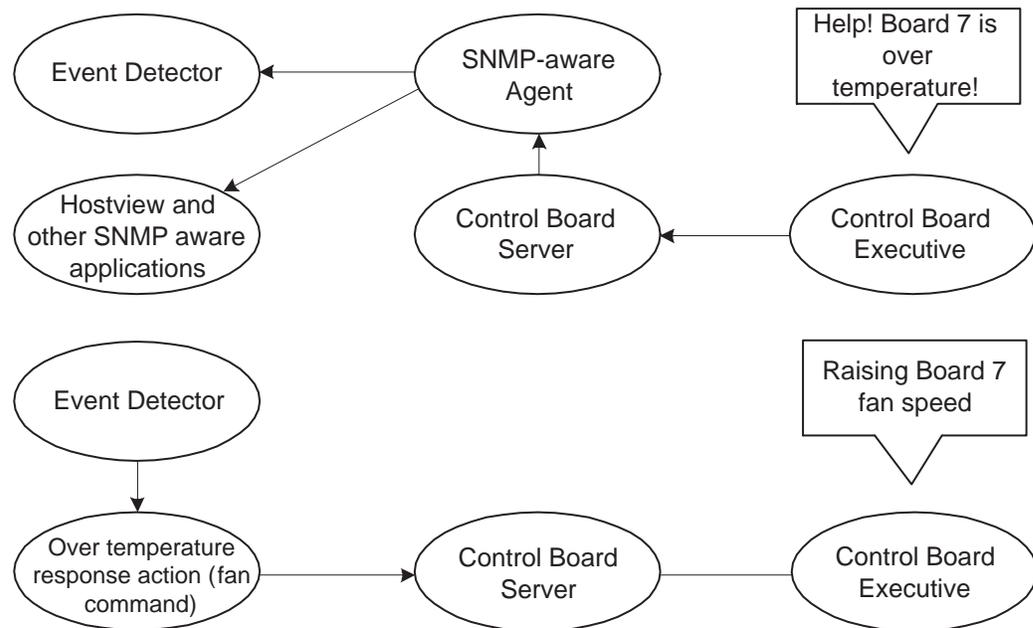


Figure 3-8 The `edd` Daemon Communications

When it receives the event message, the `cbs` daemon delivers the event to the Simple Network Management (SNMP) agent, `snmpd`, which then generates a SNMP trap.

When the `edd` daemon (Event Detector) receives the SNMP trap, it determines whether to initiate a response action. If a response action is required, the `edd` daemon runs the appropriate response action script (as a subprocess).

As an example, in Figure 3-8, the `edd` daemon is shown running a response action script for a high-temperature event. While the response action script is running, additional high-temperature events might be generated by the control board event-monitoring scripts. The `edd` daemon does not respond to those events (generated in response to the original high-temperature condition) until the first response script has finished.

The `edd` daemon uploads event detection scripts to the Sun Enterprise 10000 server control board by using the `cbe` daemon, waits for an event to be generated by the scripts, and then responds to the event by executing a

response action script on the SSP. The event detection scripts poll various conditions within the system including environmental conditions, signature blocks, power supply voltages, performance data, and so forth. Event handling is provided by response action scripts, which are run by the `edd` daemon when an event is received.

The events are transmitted by Simple Network Management Protocol (SNMP) traps. It is the responsibility of the listening application (such as the `edd` daemon or `hostview`) to detect and determine whether to respond to an event.

Warning – Changing `edd` scripts incorrectly can cause physical damage to the Sun Enterprise 10000 server.

The event response configuration files (`edd.erc`) specify how the event detector responds to events. The `edd` daemon obtains many of its initial control parameters from the following configuration files:

- The `$$SSPVAR/etc/platform_name/edd.erc` file provides configuration information for the Sun Enterprise 10000 server.
- The `$$SSPVAR/etc/platform_name/domain_name/edd.ec` file provides configuration information for a particular domain.
- The `$$SSPVAR/etc/platform_name/edd.emc` file lists the events that `edd` monitors.

The `edd_cmd` Command

You can use the `edd_cmd` command to turn on and off `edd` processing. The `edd_cmd -x stop` command stops `edd` processing, and the `edd_cmd -x start` command restarts it.

Warning – Be careful turning off `edd` processing. When `edd` processing is off, the SSP is not able to respond to most requests for service from the Sun Enterprise 10000 server, such as power or over-temperature events, which could cause physical damage to server components.



The SNMP Daemon (snmpd)

The `snmpd` daemon is the Sun Enterprise 10000 server's SNMP server proxy agent. It supports the SNMP Version 1 `set`, `get`, and `getnext` requests. It generates SNMP traps for the events detected by the `cbe` running the `edd` rules in the control board.

Since there is no software running on the Sun Enterprise 10000 server itself, SNMP management is done from the SSP on behalf of the system. The SSP and domains still support their own individual SNMP agents if configured to do so.

The `snmpd` daemon sends its traps to the SNMP trap sink server daemon (`straps`) on the SSP, and to possibly other hosts and applications listening for Sun Enterprise 10000 server SNMP events. See Figure 3-9.

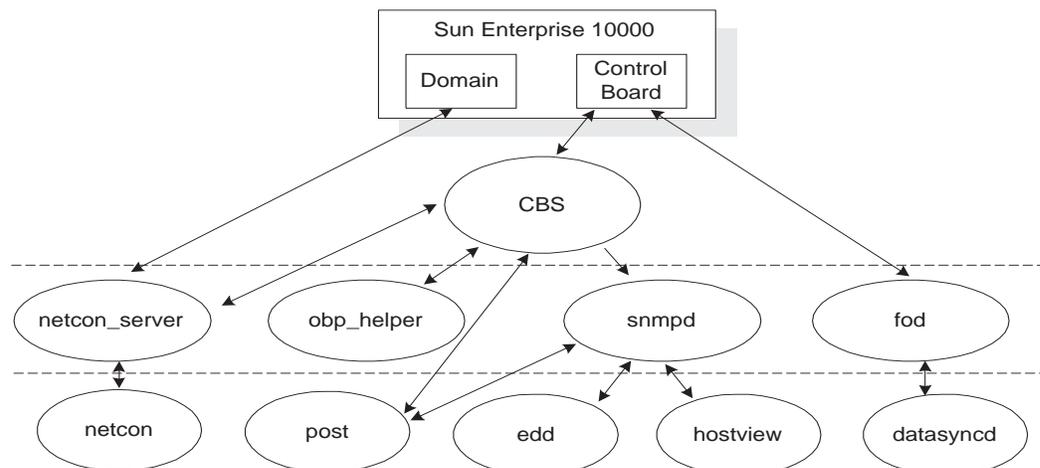


Figure 3-9 SNMP Daemon

To see how the Sun Enterprise 10000 server responds to SNMP events, you can display the SNMPD files located in the `$$SSPETC/snmpd` directory.

The SNMPD files are as follows:

- Configuration file
`$$SSPETC/snmp/agt/Ultra-Enterprise-10000.snmpd.cnf`
- MIB (Management Information Block) definition file (static data)
`$$SSPETC/snmp/Ultra-Enterprise-10000.mib`
- MIB data file (dynamic data)

`$SSPETC/snmp/Ultra-Enterprise-10000.dat`



Warning – Changing the SNMP responses incorrectly can cause physical damage to the Sun Enterprise 10000 server by interfering with `edd` event processing.

SNMP Trap Sink Server (`straps`) Daemon

The `straps` daemon monitors the SNMP trap port. When an SNMP trap is received, it forwards the trap to all connected clients without modification.

These clients include the following:

- `hostview`
- `edd`
- Customer-supplied SNMP managers

Have the students refer back to Figure 3-3 on page 3-10 to review the event flow.

Daemon Communication Paths

Figure 3-10 pictorially represents the relationships between the SSP daemons and the Sun Enterprise 10000 server.

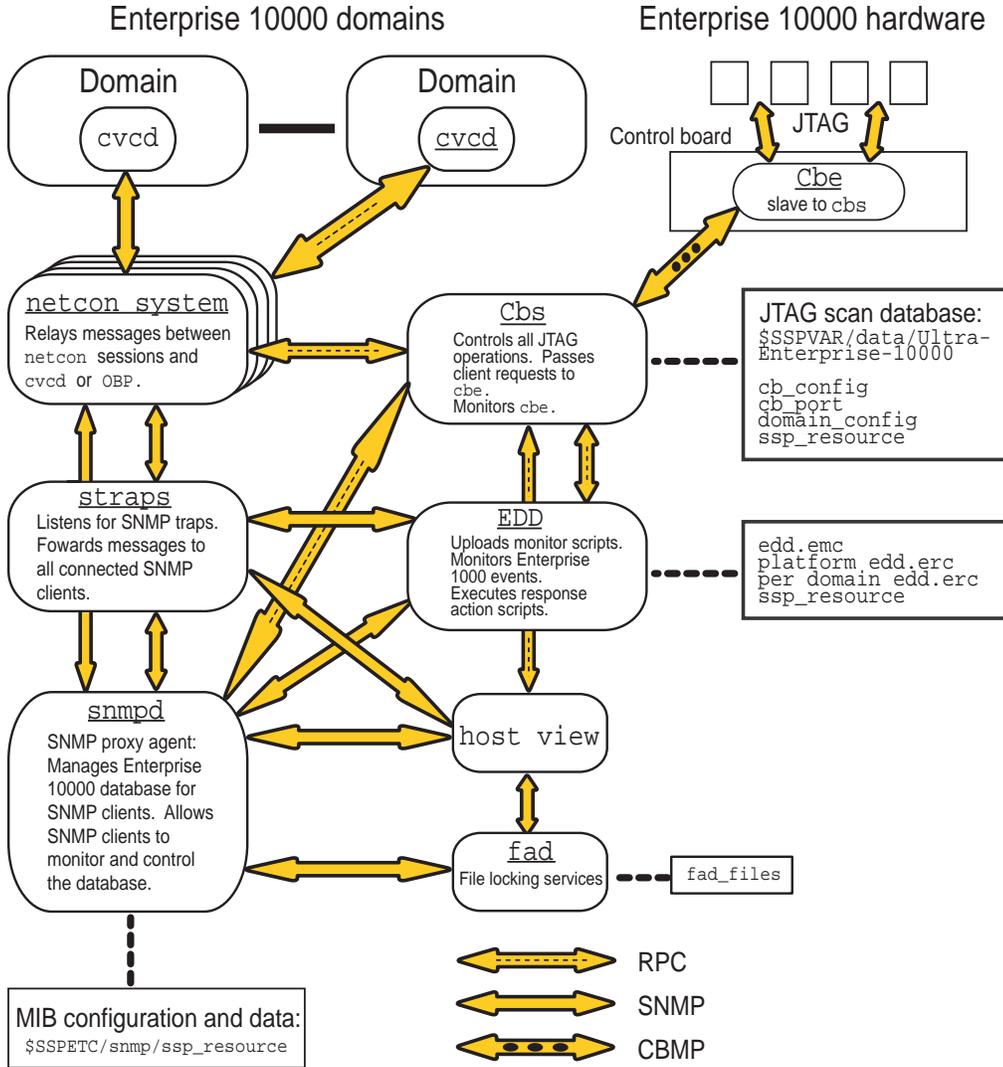


Figure 3-10 The SSP and Sun Enterprise 10000 Server Interaction

Pre-Release – Read Only

The Failover Daemons

Version 3.4 and onwards of the SSP software adds the following two daemons:

- The `datasyncd` daemon that periodically copies the critical data files from the main SSP to the spare SSP without need for a manual backup and restore process.
- The `fod` daemon that monitors communication between the SSPs and the control boards and initiates automated takeover of the main SSP role if the main SSP fails.

The Data Synchronization Daemon (`datasyncd`)

The `datasyncd` command provides synchronization of data files between the main SSP and the Spare SSP. It performs the following:

- Runs only on the main SSP.
- Checks files for changes hourly (or immediately if it is told to by the `setdatasync` command). User defined files can be checked at any interval.
- Reads the following two input files:
 - `$SSPVAR/.ssp_private/fad_files` – the list of critical system and domain state files maintained by the SSP.
 - `$SSPVAR/.ssp_private/user_file_list` – a user maintainable list of files which synchronizes with the spare SSP.
- Transfers any changed files listed in the files above to the spare.

Note – The `datasyncd` command does not operate if the SSP failover status is not “Active.”

- Uses `rshell` as the mechanism for transferring the files.

Note – The SSP installation creates a `~ssp/.rhosts` file with the host names of the opposite SSP’s control board interface names in it.



Synchronizing Files

The following command results in the `~/ssp/notes.txt` file being propagated to the spare SSP. The file is then checked for changes every three minutes.

```
hamilton:presidents% setdatasync -i 3 schedule  
/export/home/ssp/notes.txt
```

To verify synchronization, use the following command:

```
hamilton:presidents% showdatasync -l  
TIME PROPAGATED      INTERVAL  FILE  
Jul 18 07:30:08           3  /export/home/ssp/notes.txt
```



Note – Because `datasyncd` runs as the SSP user, the files to be transferred *must* be readable and writable by the SSP user, and the directory where the file is written *must* be writable by the SSP user.

The Failover Daemon (`fod`)

The `fod` process runs on both the main and the spare SSP and communicates with the other SSP and the control boards using the Failover Protocol (FOP). Figure 3-11 demonstrates the functionality of the `fod` process.

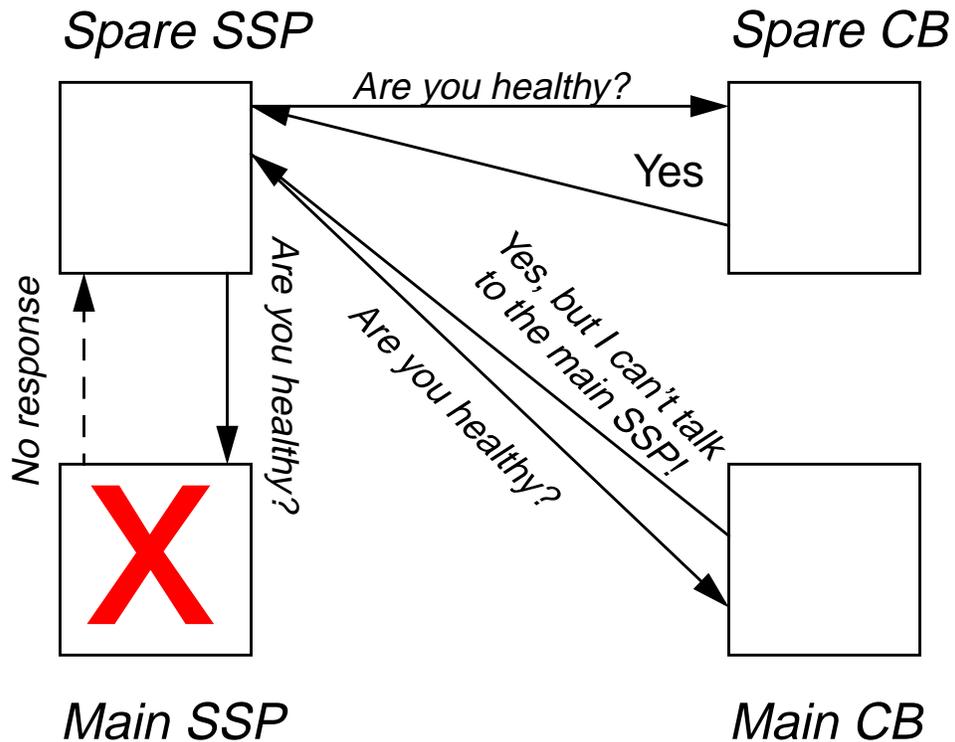


Figure 3-11 The `fod` Daemon

When it first starts, `fod` attempts to discover whether this SSP is the main SSP or the spare SSP. To do this, it attempts a connection to the other SSP to inquire about whether it thinks it is the main or spare SSP. If this connection fails, it tries to contact the control board to determine the role it should take.

The `fod` daemon requires a logical IP address for the main SSP. This obviates the need to change the `/etc/ssphostname` file on all the domains when the SSP fails over.

In the example shown in Figure 3-11 on page 3-32, the spare `fd` is unable to talk to the main SSP, yet it is able to talk to the main control board. In this case, the spare `fd` initiates an automated SSP failover. Table 3-3 shows the action `fd` takes based on detected failures.

Table 3-3 The Action `fd` Takes Based on Detected Failure

Failure Point	Failover SSP	Disable SSP Failover	Control Board Failover	Disable Control Board Failover
Main SSP to domains	Yes			
Spare SSP to domains		Yes		
Main SSP	Yes			
Spare SSP		Yes		
Main SSP to spare hub		Yes		Yes
Spare SSP to main hub		Yes		
Main SSP to main hub	Yes			
Spare SSP to spare hub		Yes		
Main hub			Yes	
Spare hub		Yes		Yes
Primary Control Board to main hub			Yes	
Spare Control Board to spare hub				yes
Primary Control Board			Yes	
Spare Control Board				Yes

The instructor should spend some time here running through a couple of scenarios from the following table. For example, if the `fd`s decide that the spare hub has died because they can contact each other on the control board 0 interface, but not on the control board 1 interface, then it makes sense to disable the control board failover, but why do the `fd`s decide to disable SSP failover too?

Table 3-3 was taken from the “SSP Internals” chapter of the *Sun Enterprise 10000 SSP 3.5 User’s Guide*.



Note – Once a failover occurs, the failover state is marked “Failed.” In order to fail back to the original SSP or control board, you must re-enable the failover state.

Dual Control Board Handling

A system should be configured with dual control boards to minimize downtime in the event of a control board failure.

As discussed earlier, if connectivity to the main control board is lost (because of a network problem or a hub failure), `nod` automatically causes failover to the other control board.

The primary control board essentially serves the following two purposes:

- It provides the JTAG interface
- It provides a system clock

There are two types of failover that can occur depending on the prevailing conditions at the time. The following are examples of these failover types:

- Partial failover – Only the JTAG interface is moved to the spare control board. The primary control board continues to provide the system clock and running domains are not affected.
- Complete failover – Both the JTAG function and the system clock function are moved to the spare control board.

When a control board failure occurs, and there are no domains running, a complete failover is initiated.



Note – In a complete failover situation, any running domains fail. Complete failover cannot be performed without rebooting all running domains, because the control board is providing the high-frequency system clocks for all boards in the system.

The inactive control board can be hot swapped.

Using the showfailover and setfailover Commands

To display the fod daemon current status, use the `showfailover` command. It can run only on the main SSP.

Failover Status

The following command displays the failover status:

```
hamilton:presidents% showfailover
Failover State:
  SSP Failover: Active
  CB Failover: Active
Failover Connection Map:
  Main SSP to Spare SSP thru Main Hub:    GOOD
  Main SSP to Spare SSP thru Spare Hub:   GOOD
  Main SSP to Primary Control Board:      GOOD
  Main SSP to Spare Control Board:        GOOD
  Spare SSP to Main SSP thru Main Hub:    GOOD
  Spare SSP to Main SSP thru Spare Hub:   GOOD
  Spare SSP to Primary Control Board:     GOOD
  Spare SSP to Spare Control Board:       GOOD
SSP/CB Host Information
  Main SSP:                               hamilton
  Spare SSP:                              franklin
  Primary Control Board (JTAG source):     jefferson
  Spare Control Board:                    madison
  System Clock source:                    jefferson
```

If an SSP failover has already happened, the SSP failover is automatically set to “Failed,” as shown by using the following command:

```
franklin:presidents% showfailover |grep "SSP Failover"
  SSP Failover: Failed
```

Forcing a Manual Failover of the SSP

To failover the SSP, the failover capability must be enabled. Perform the following:

1. Run the following command on the main SSP:

```
hamilton:presidents% setfailover force
```



Note – If the `setfailover force` command says “the failover has already occurred,” then this means that failover is currently disabled. Simply enable failover with `setfailover on` and retry the `force` command.

On the main SSP, the `setfailover force` command does the following:

- Causes `datasyncd` to synchronize all the critical files to the spare SSP
- Relinquishes the floating IP address
- Switches the SSP to “spare” mode
- Sends a TERM signal to `datasyncd`, `cbs`, `snmpd`, `edd`, and any `netcon_server` and `obp_helper` processes
- Renames `/tftpboot` to the `/tftpboot.spare`
- Shuts down `in.rarpd`
- Restarts `fod`
- Comments-out the `tftp` entry in `/etc/inetd.conf` and restarts `inetd`
- Advises the spare SSP to become the main SSP
- Issues a `cb_reset` to reboot the control boards

On the spare SSP, failover does the following:

- Adopts the floating IP address
- Renames the `/tftpboot.spare` directory to the `/tftpboot` directory
- Starts the `in.rarpd` daemon
- Uncomment the `tftp` entry in `/etc/inetd.conf` and restarts the `inetd` daemon

- Advises `ssp_startup.sh` to start up the main ssp daemons

Re-enabling the Failover Capability

To re-enable the failover capability, execute the following:

```
franklin:presidents% setfailover on  
Failover enable request sent.  
Please use the showfailover (1M) command to verify that failover has been  
successfully enabled.  
If FAILED connections are detected, then failover will be re-disabled.
```

Disabling Failover

To disable failover capability, execute the following:

```
hamilton:presidents% setfailover off
```

Switching the Active Control Board

To switch the active control board, perform the following steps:

1. Shut down all domains.
2. Power off all system components except the control boards.

```
hamilton:presidents% power -off -all
```

3. Power on all system components.

```
hamilton:presidents% power -on -all
```

4. Switch to the spare control board.

```
hamilton:presidents% setfailover -t cb force
```



Note – If the domains were not shut down and the power was not cycled on the system boards, then *only* the JTAG interface is switched to the spare control board.

5. Use the `showfailover` command to verify that both the JTAG and the system clock source have changed:

```
franklin:presidents% showfailover
Failover State:
  SSP Failover: Active
  CB Failover: Active
Failover Connection Map:
  Main SSP to Spare SSP thru Main Hub:    GOOD
  Main SSP to Spare SSP thru Spare Hub:   GOOD
  Main SSP to Primary Control Board:      GOOD
  Main SSP to Spare Control Board:        GOOD
  Spare SSP to Main SSP thru Main Hub:    GOOD
  Spare SSP to Main SSP thru Spare Hub:   GOOD
  Spare SSP to Primary Control Board:     GOOD
  Spare SSP to Spare Control Board:       GOOD
SSP/CB Host Information
  Main SSP:                               franklin
  Spare SSP:                              hamilton
  Primary Control Board (JTAG source):    jefferson
  Spare Control Board:                   madison
  System Clock source:                   jefferson
```

You can also look at the `hostview` GUI to determine which control board is the clock source (marked with the “C”), and which control board is the JTAG source (marked with a “J”).

After you are sure that both the JTAG source and the clock source have been relocated to the other control board, you can use `bringup` to start up all the domains.

Other Causes of Automatic Failover

Obviously, a catastrophic failure of the main SSP can trigger a failover; however, there are two other situations that can occur that also cause an SSP failover. These other situations include the following:

- Insufficient virtual memory for the SSP to operate
- Insufficient disk space for the SSP to operate

Virtual Memory and Disk Space Threshold

Use the `setfailover` command to display the current memory threshold:

```
hamilton:presidents% setfailover -m  
Current virtual memory threshold (in KByte): 1000
```

Use the `setfailover` command to display the current disk threshold:

```
hamilton:presidents% setfailover -d  
Current disk space threshold (in KByte): 1
```

The limits in the examples above are far too low to be reasonable.

Setting the Virtual Memory and Disk Space Thresholds

Use the `setfailover` command as follows to set the required thresholds for virtual memory and disk space:

```
hamilton:presidents% setfailover -m 10000  
hamilton:presidents% setfailover -d 2000
```

Installing the SSP Software

The SSP software comes installed on the SSP system when it is delivered. However, there are several reasons why you might need to re-install the software. These reasons are as follows:

- A disk or hardware failure occurred on the SSP.
- A new version of the SSP software is required to support:
 - A new OS version on a domain
 - New hardware (faster processors, for example)
- You want to move to a dual-SSP configuration.

Preparing to Install the SSP Software

Several steps must be completed before proceeding with the installation. These steps are as follows:

1. Update the name service `hosts` registry—Network Information Service (NIS or NIS+), `/etc/hosts`, or Domain Name Service (DNS)—to include the host names and IP addresses of the control boards.
2. Update the name service `ethers` registry (NIS, NIS+, `/etc/ethers`) to include the host names and Ethernet addresses of your control boards.

With NIS or NIS+, it might be useful to have the Sun Enterprise 10000 server control board information in the `/etc/hosts` and `/etc/ethers` files in the event that the NIS or NIS+ server goes down. You cannot control the Sun Enterprise 10000 server without the control board connections.

3. Ensure that `/etc/nsswitch.conf` is properly configured.

If the SSP is using NIS or NIS+, you *must* edit the `/etc/nsswitch.conf` file on the SSP to force it to use its local `/etc/ethers`, `/etc/bootparams`, `/etc/services`, and `/etc/netmasks` files before the NIS or NIS+ files.

Correct entries should appear as follows (for NIS):

```
ethers:      files nis
netmasks:   files nis
bootparams: files nis
services:   files nis
```

4. Use `touch` to create the `/etc/notrouter` file.

The SSP Packages

There are 12 packages that need to be installed, as shown in Table 3-4.

Table 3-4 SSP Packages

Package Name	Description
SUNWsspdpf	Data files
SUNWsspdo	Domain utilities
SUNWsspdr	Dynamic reconfiguration utilities
SUNWsspfp	Flash PROM image
SUNWsspfd	Inter-Domain Networking
SUNWsspnm	On-line manual pages
SUNWsspob	Open Boot PROM utilities
SUNWsspoc	Core utilities
SUNWsspoo	POST utilities
SUNWsspr	System Service Processor, (Root)
SUNWsspst	Scan tests
SUNWsspue	User environment

They are included on the Supplemental CD-ROM that is shipped with Solaris 7 and Solaris 8 Operating Environments.

Installation of the packages is order-dependant. Use the installation script called *ssp_install*, as described in “Installing the SSP Software Packages” on page 3-47. Using of this script ensures that the packages are installed correctly. This script is located in the `Tools` directory under the SSP software root.

Installing the SSP Software Packages

The following procedure shows how to install SSP 3.4 software from a CD-ROM.



Note – If you are installing from an NFS mount, the directory from which you are installing the SSP software will be different from that of the CD-ROM. Also, you need to be in multi-user mode.

To install the SSP software packages from the SSP CD-ROM:

1. Insert the SSP CD-ROM into the CD-ROM drive.
2. Change to the `/cdrom/cdrom/Tools` directory.
3. Install the SSP software by typing:

```
# ./ssp_install ../Product
```
4. When prompted about whether to install the `SUNWsspfp` packages, type “y”.
5. After installing the SSP packages, reboot the SSP system.



Note – At this point you are asked to provide configuration information about the SSP. See “Configuring the Control Boards” on page 3-44 for details about configuration.

6. Log in as user `ssp` on the SSP. The initial password is `ssp`.
7. Type the following:

```
franklin% tail -f $SSPLOGGER/messages
```

Wait for the Startup of SSP programs complete message before you continue.



Caution – Whenever you reboot the SSP, it can take a few minutes before you can run any SSP commands. This delay is needed to enable the SSP software initialization process to complete.

Getting Information About Installed SSP Software

SSP package information such as version, revision, size, install date, and status can be obtained by typing the following command:

```
ssp% pkginfo -l SUNWsspue
  PKGINST: SUNWsspue
    NAME: System Service Processor User Environment
  CATEGORY: application,servproc
    ARCH: sparc
  VERSION: 3.4.0,REV=2000.08.20.19.44
  BASEDIR: /
  VENDOR: Sun Microsystems, Inc.
    DESC: System Service Processor User Environment
  PSTAMP: sspbuild.westm20194522
  INSTDATE: Jul 16 2001 21:31
  HOTLINE: Please contact your local service provider
  STATUS: completely installed
  FILES:   32 installed pathnames
          1 shared pathnames
          6 directories
          2 executables
          94 blocks used (approx)
```

Pre-Release – Read Only

Configuring the Control Boards

When the SSP system boots for the first time after you install the SSP software (or for the first time after you receive the system from Sun), the boot process runs the `ssp_config` utility to configure the control boards and the SSP environment. This utility can also be used to reconfigure the SSP environment and the control boards after the initial setup.

The `ssp_config` Command

The `ssp_config` command is used to initially configure or reconfigure the SSP. The command asks you for the following information:

- Sun Enterprise 10000 server name
- Control board 0 host name and IP address
- Control board 1 host name and IP address (if present)
- The name and IP address that “floats” between SSPs (always belonging to the one configured as “main”)
- The speed of the processors in your Sun Enterprise 10000 server
- Whether this is the main or a spare SSP

This information is used to configure the `cb_config` file in the `$SSPVAR/.ssp_private` directory.

Note – If you manually run the `ssp_config` command, reboot the SSPs.



The `ssp_unconfig` Command

Use the `ssp_unconfig` command to unconfigure the SSP. To unconfigure the SSP you first must halt domains, remove their configurations, and then run the `ssp_unconfig` command. This will unconfigure the `cb_config` file.

Responding to the ssp_config Questions

The following is an example of the configuration questions generated during the first reboot cycle.

Do you wish to configure this system as an SSP for an E10000? (y/n) **y**

The system name identifies the entire host machine to the SSP software. The system name occupies a different name space than domain name (host names of bootable systems).

What is the name of the platform this SSP will service? **presidents**

Please enter the floating host name of the main SSP [presidents-ssp-main]: **live-ssp**

main SSP name = live-ssp

main SSP IP address = 192.9.201.131

Is this correct? (y/n) **y**

You must specify what type of processor modules you have installed in your Enterprise-10000 platform. If you have a mixture of processors, select the option corresponding to the lowest processor speed in your configuration. Please select one of the options below.

- 1) 250 MHz processors
- 2) 366 MHz processors
- 3) 400 MHz processors
- 4) 466 MHz processors
- 5) Unlisted (manually enter clock values)

What speed of processors do you have installed? **1**

Your selections are apparently for a 250 MHz processor.

Is this correct? (y/n) **y**

The platform name identifies the entire host machine to the SSP software. The platform name occupies a different name space than domain names (hostnames of bootable systems).

What is the name of the platform this SSP will service [presidents]?

Do you have a control board 0? (y/n) **y**

Please enter the host name of the control board 0 [cb0]: **jefferson**

Do you have a control board 1? (y/n) **y**

Please enter the host name of the control board 1 [cb1]: **madison**

Please identify the primary control board.

Is Control Board 0 [jefferson] the primary? (y/n) **y**

Platform name = presidents

Control Board 0 = jefferson => 10.1.0.200

Control Board 1 = madison => 10.2.0.200

Primary Control Board = jefferson

Is this correct? (y/n) **y**

The Control Board Configuration File

The control board configuration file is named `$$SSPVAR/.ssp_private/cb_config`. It contains only one line.

The format of the line is:

```
platform_name:platform_type:cb0_hostname:status0:cb1_hostname:status1
```

where:

- *platform_name* - The Enterprise 10000 platform name assigned at installation time.
- *platform_type* - Always Ultra-Enterprise-10000.
- *cb0_hostname* - Control board 0 host name, if one is installed.
- *status0* - Indicates if control board 0 is the primary. P indicates primary; anything else or blank indicates alternate.
- *cb1_hostname* - Control board 1 host name, if one is installed.
- *status 1* - Indicates if control board 1 is the primary. P indicates primary; anything else or blank indicates alternate.

For example:

```
presidents:Ultra-Enterprise-10000:jefferson:P:madison:
```

This example shows that there are two control boards installed in the `presidents` platform. They have host names `jefferson` (which is the primary) and `madison`.



Caution - Do not try to change the primary control board designation by editing this file. It is not sufficient, and may cause your domains to fail.

Switching the Primary Control Board

You can change the primary control board by using the `ssp_config cb` command. The `ssp_config` command updates the `$$$SPVAR/.ssp_private/cb_config` file.

1. Run `ssp_config cb` from the SSP, specifying the new control board configuration. Do the following on the main SSP as root:

```
hamilton# /opt/SUNWssp/bin/ssp_config cb
Configuring control boards.
Platform name   = presidents
Control Board 0 = jefferson => 10.1.0.200
Control Board 1 = madison  => 10.2.0.200
Primary Control Board = 0
Is this correct? (y/n): n
Do you have a control board 0? (y/n): y
Please enter the host name of the control board 0 [jefferson]:
Do you have a control board 1? (y/n): y
Please enter the host name of the control board 1 [madison]:
Please identify the primary control board.
Is Control Board 0 [jefferson] the primary? (y/n) n
Is Control Board 1 [madison] the primary? (y/n) y
Platform name   = presidents
Control Board 0 = presidents-cb0 => 10.1.0.200
Control Board 1 = presidents-cb1 => 10.2.0.200
Primary Control Board = 1
Is this correct? (y/n): y
```

2. When you have completed the `ssp_config cb` command, reboot the SSPs.

Saving the SSP Environment

The SSP contains files that are difficult to rebuild if they are damaged or lost, so these files should be backed up regularly, as shown in Figure 3-12.

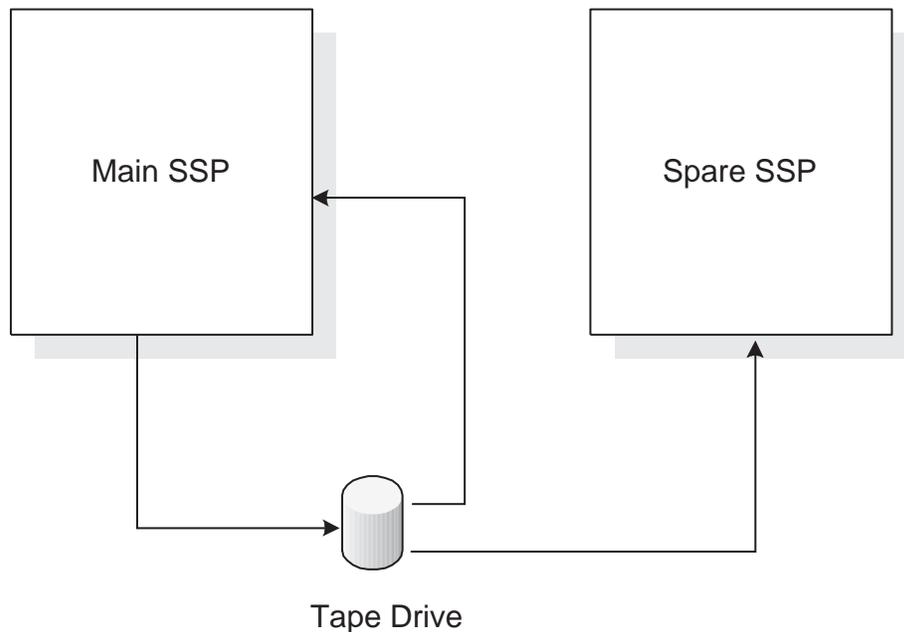


Figure 3-12 Saving the SSP Environment

Remember that much of the Sun Enterprise 10000 server's configuration information is loaded from the SSP.

To back up the SSP files, use the `ssp_backup` command. It:

- Must be run as root
- Takes a single argument: the name of the directory where the backup should be written
- Creates a backup that is a cpio archive named `ssp_ backup.cpio`
- Takes a snapshot of the files containing the current status of the system.

Prior to SSP version 3.4, the SSP backup command was the mechanism for keeping the spare SSP consistent with the state of the main SSP.

The `ssp_restore` command is used to restore lost files. It:

- Restores the operational environment of the SSP from a backup file created by `ssp_backup`

- Must be run as root
- Takes a single argument: the name of the backup file to restore
- Can be used to do the following:
 - Restore the operational environment to the main SSP
 - Restore the operational environment to the spare SSP
 - Restore the operational environment from one of multiple archives

Backing up and Restoring the SSP

The following is an example of a script that you would use to back up and restore SSP Configuration files:

```
hamilton:/# /opt/SUNWssp/bin/ssp_backup /tmp
hamilton:/# ls -l /tmp/ssp_backup*
-rw-r--r-- 1 root other 8077312 Jul 17 18:39 /tmp/ssp_backup.cpio
```

In order to be restored to a different machine, the backup file must be copied to the other machine using ftp, rcp, tape archive, or some other method.

```
franklin:/# /opt/SUNWssp/bin/ssp_restore /tmp/ssp_backup.cpio
Backing up /home/ssp/.Xdefaults as /home/ssp/.Xdefaults.__upgrade
Backing up /home/ssp/.cshrc as /home/ssp/.cshrc.__upgrade
Backing up /home/ssp/.dtprofile as /home/ssp/.dtprofile.__upgrade
Backing up /home/ssp/.login as /home/ssp/.login.__upgrade
Backing up /home/ssp/.openwin-init as /home/ssp/.openwin-init.__upgrade
Backing up /home/ssp/.openwin-menu as /home/ssp/.openwin-menu.__upgrade
Backing up /home/ssp/.postrc as /home/ssp/.postrc.__upgrade
Backing up /home/ssp/.redxrc as /home/ssp/.redxrc.__upgrade
Backing up /home/ssp/.ssp_env as /home/ssp/.ssp_env.__upgrade
15776 blocks
/tftpboot/C009C95A.cb_port linked to /tftpboot/cb_port
/tftpboot/C009C963.cb_port linked to /tftpboot/cb_port
/tftpboot/C009C963 linked to /tftpboot/C009C95A
/tftpboot/cbe.ima linked to /tftpboot/C009C95A
15776 blocks
Restoring /var/opt/SUNWssp/.ssp_private/fad_files.__upgrade as
/var/opt/SUNWssp/.ssp_private/fad_files
```

If the restore is taking a long time, you can monitor the restore's progress by typing:

```
# tail -f/var/opt/SUNWssp/ssp_restore.out
```



Caution – The `ssp_backup` archive file can be very large (20 Mbytes or larger). You can minimize the size of the backup file by first deleting the SSP log files that are no longer needed from the `/var/opt/SUNWssp/adm` directory. Make sure to always backup the SSP configurations after installing patches. Consider submitting the `ssp_backup` command to the `cron` utility. Any changes to the SSP configuration are automatically backed up.

Network Time Protocol (NTP) Software

The `xntp` software might not need to be installed on a factory SSP, but `xntp` configuration is required.

The NTP daemon (`xntpd`) for Solaris 2.6 Operating Environment, Solaris 7 Operating Environment, or Solaris 8 Operating Environment provides a mechanism for keeping the time settings synchronized between the SSP and the domains, as shown in Figure 3-13.

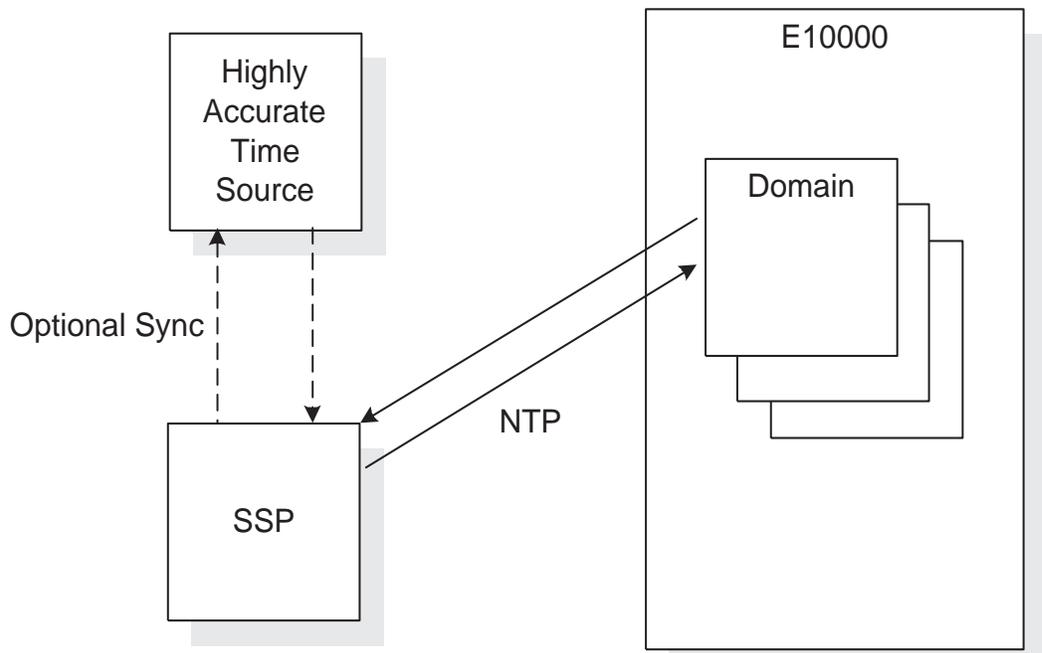


Figure 3-13 Synchronizing Between SSP and the Domains

OBP obtains the time from the SSP when the domain is booted, and the NTP daemon keeps the time synchronized from that point on.

Starting with the release of the Solaris 2.6 Operating Environment, the NTP software comes bundled with the Solaris Installation disks.

Configuring the SSP as an NTP Time Server

The Solaris 7 Operating Environment and Solaris 8 Operating Environment come with two sample configuration files:

- `/etc/inet/ntp.server`
- `/etc/inet/ntp.client`

If you want the SSP to offer a time service, copy the `/etc/inet/ntp.server` file to the default configuration file `/etc/inet/ntp.conf`.

```
franklin# cp ntp.server ntp.conf
```

Edit the `ntp.conf` file by making the following changes:

```
#server 127.127.XType.0 prefer
#fudge 127.127.XType.0 stratum 0
server 127.127.1.0 prefer
fudge 127.127.1.0 stratum 0
```

Then, start the NTP daemon by typing the following:

```
franklin# /etc/init.d/xntpd start
```

This is a minimal config. If the clock on the SSP drifts, then so will the clock on the domains.

If you have NTP available within your network, then you should synchronize the time on the SSPs to your network time service.

Configuring the Domain as an NTP Client

If you want the domain to be a time client, copy the `/etc/inet/ntp.client` file to the default configuration file named `/etc/inet/ntp.conf`.

```
franklin# cp ntp.client ntp.conf
```

Then, start the NTP daemon:

```
franklin# /etc/init.d/xntpd start
```

Exercise: Installing and Configuring the SSP

In this exercise you participate in the installation and configuration of SSP 3.4 or 3.5 user environment packages on your assigned lab workstation.

Preparation

Your instructor shall provide you with the SSP 3.5 software packages and a classroom configuration plan showing detailed information about the network connection between your workstation and the Sun Enterprise 10000 server.

Each student workstation must be pre-configured with the Solaris 2.6 Operating Environment or later and the `xntp` package. The SSP user environment packages must be removed. See lab instructor notes in Module 2, "Architecture Overview."

Provide each student group with the SSP 3.4 or 3.5 user environment packages.

Tasks

In the following exercise, you install and configure the SSP 3.5 software.

Installing the SSP 3.5 User Environment

Answer the following questions:

1. Based on the configuration information gathered in the exercise in "Assess the Main SSP Configuration" on page 2-32, what is the current version of the Solaris Operating Environment installed on your workstation?

2. Does the currently installed Solaris Operating Environment support SSP 3.5?

Perform the following steps to install the SSP 3.5 user environment:

1. Log in to your workstation as superuser.
2. Verify that the `/etc/inet/hosts` file has the classroom network layout requirements provided in the lecture.

3. Verify that each network interface on your workstation meets the classroom network layout requirements.
4. Install the SSP 3.5 user environment from the network.
5. Reboot your SSP system.
6. Log in as user `ssp` on the SSP and monitor the SSP user environment initialization using the `tail` command.



Note – When your SSP reboots, you are asked to provide the configuration information discussed in “Responding to the `ssp_config` Questions” on page 3-45. Provide the configuration information before answering the questions below.

Configuring the SSP User Environment

Answer the following questions:

1. How can the current version of the installed SSP user environment be determined?

2. What configuration information must you have available before configuring the SSP user environment?



Note – Refer to the classroom network layout provided during the lecture, for specific configuration information. You need this information to complete the following steps. If you need assistance, contact your instructor.

Perform the following steps to configure the SSP user environment:

1. When asked, enter the name of the Sun Enterprise 10000 server according to the classroom network layout.
2. Enter the host name of control board 0 according to the classroom network layout.
3. Enter the host name of control board 1 according to the classroom network layout.

4. Configure your workstation as a spare SSP.

Switching to the spare SSP and dual control board handling labs are covered in “The Failover Daemon (fod)” on page 3-32.

Investigate the SSP environment variables, log files, and daemons as follows:

1. Examine the SSP environment variables and locate the log files.
2. Investigate the SSP daemons by looking at their configuration files. You can view:
 - `/etc/init.d/ssp` and `/etc/init.d/sysidssp`
 - The `edd` files in `$SSPVAR/etc/platform_name`
 - The SNMP files in `$SSPETC/snmp`
 - The `ssp` account home directory
 - The `$SSPETC` directory
 - The `$SSPVAR` directory
 - The `$SSPOPT` directory

Exercise Summary



Discussion – Take a few minutes to discuss what experiences, issues, or discoveries you had during the lab exercises.

Manage the discussion here based on the time allowed for this module, which was given in the “About This Course” module. If you find you do not have time to spend on discussion, then just highlight the key concepts students should have learned from the lab exercise.

- **Experiences**

Ask students what their overall experiences with this exercise have been. You might want to go over any trouble spots or especially confusing areas at this time.

- **Interpretations**

Ask students to interpret what they observed during any aspects of this exercise.

- **Conclusions**

Have students articulate any conclusions they reached as a result of this exercise experience.

- **Applications**

Explore with students how they might apply what they learned in this exercise to situations at their workplace.

Exercise Solutions

The solutions to the exercises are as follows:

Installing the SSP 3.5 User Environment

1. Based on the configuration information gathered in the exercise in “Assess the Main SSP Configuration” on page 2-32, what is the current version of the Solaris Operating Environment installed on your workstation?

Solaris 7, Hardware 11/99 or later

2. Will the currently installed Solaris Operating Environment support SSP 3.4?

Yes

Configuring the SSP User Environment

1. How can the current version of the installed SSP user environment be determined?

By running the command `pkginfo -l SUNWsspue`

2. What configuration information must you have available, before configuring the SSP user environment?

Sun Enterprise 10000 platform name

Control board 0 host name and IP address

Control board 1 host name and IP address (if present)

Whether this is the main or a spare SSP

Check Your Progress

Before continuing on to the next module, check that you are able to accomplish or answer the following:

- Explain the functions of the System Service Processor (SSP)
- Describe how the SSP interacts with the system
- Describe security considerations relevant to the Sun Enterprise 10000 server
- Plan the network for a Sun Enterprise 10000 server and its SSP
- Completely install the SSP software
- Accomplish a manual failover from the main SSP to the spare SSP
- Configure automatic failover of the main SSP to the spare SSP
- Perform control board switch-over

Think Beyond

Why is the SSP Solaris Operating Environment software profile edited the way it is?

What would happen if you used the SSP for purposes other than monitoring the Sun Enterprise 10000 server?

Why are the SSP packages order-dependent?

Why might you need to create or re-create `eeprom.image` files?

When would you use `ssp_config` or `ssp_unconfig`?

Pre-Release – Read Only

Pre-Release – Read Only