Sun Ray™ Enterprise Server Software 1.1 Advanced Administrator's Guide

THE NETWORK IS THE COMPUTER™

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303-4900 USA
650 960-1300 Fax 650 969-9131

Part No. 806-4181-10
April 2000, Revision A

Send comments about this document to: `docfeedback@sun.com`

Please
Recycle

Contents

Preface

The *Sun Ray Enterprise Server Software 1.1 Advanced Administrator's Guide* extends the information provided in the *Sun Ray Enterprise Server Software 1.1 Administrator's Guide* so that power users can customize their servers.

This guide is intended for system administrators who are already familiar with the Sun Ray™ computing paradigm and have substantial networking knowledge.

Before You Read This Book

Read the *Sun Ray Enterprise Server Software 1.1 Installation Guide, the Sun Ray Enterprise Server Software 1.1 Administrator's Guide,* and the *Sun Ray Enterprise Server Software 1.1 Product Notes.*

This guide assumes that you have installed the Sun Ray server software on your server from the Sun Ray Enterprise Server Software 1.1 CD and that you have added the required patches.

How This Book Is Organized

Chapter 1 describes the requirements of switches to be used on the Sun Ray interconnect and describes how to configure switches for specific scenarios.

Chapter 2 describes the new failover option, wherein two or more Sun Ray servers may "back-up" each other so that in the event of a Sun Ray server failure, a reserve Sun Ray server is available.

Chapter 3 describes customizing the Sun Ray enterprise server software and alternate window managers.

Chapter 4 describes the use of Citrix ICA Client for Solaris, Citrix MetaFrame, and WindowsNT.

Using UNIX Commands

This document does not contain information on basic UNIX® commands and procedures, such as shutting down the system, booting the system, or configuring devices.

For this information, see the AnswerBook2™ online documentation for the Solaris™ 2.6 or 7 operating environment or `http://docs.sun.com` (see “Sun Documentation on the Web” on page viii).

This document does contain information about unique Sun Ray system commands.

Typographic Conventions

TABLE P-1 Typographic Conventions

Typeface or Symbol	Meaning	Examples
`AaBbCc123`	The names of commands, files, and directories; on-screen computer output.	Edit your `.login` file. Use `ls -a` to list all files. `% You have mail.`
`AaBbCc123`	What you type, when contrasted with on-screen computer output.	`%` **`su`** `Password:`
AaBbCc123	Book titles, new words or terms, words to be emphasized. Command-line variable; replace with a real name or value.	Read Chapter 6 in the *User's Guide.* These are called *class* options. You *must* be `root` to do this. To delete a file, type `rm` *filename.*

Shell Prompts

TABLE P-2 Shell Prompts

Shell	Prompt
C shell	*machine_name*%
C shell superuser	*machine_name*#
Bourne shell and Korn shell	$
Bourne shell and Korn shell superuser	#

Related Documentation

TABLE P-3 Related Documentation

Application	Title	Part Number
Installation	*Sun Ray Enterprise Server Software 1.1 Installation Guide (English)*	805-7916-11
Administration	*Sun Ray Enterprise Server Software 1.1 Administration Guide (English)*	805-7915-11
Product Notes	*Sun Ray Enterprise Server Software 1.1 Product Notes (English)*	805-7918-12

Sun Welcomes Your Comments

Sun™ is interested in improving its documentation and welcomes your comments and suggestions. Email your comments to:

`docfeedback@sun.com`

Please include the part number of your document in the subject line of your email.

Sun Documentation on the Web

The `docs.sun.com`SM web site enables you to access Sun technical documentation on the Web. You can browse the `docs.sun.com` archive or search for a specific book title or subject at:

`http://docs.sun.com`

CHAPTER 1

Switches on the Sun Ray Interconnect

On the Sun Ray™ interconnect, the optimal way to handle network traffic is through switch technology, which supports multiple transmissions simultaneously and increases available bandwidth. Network administrators must verify the configuration of each network device and that its configuration matches its performance.

This chapter describes the requirements of switches to be used on the Sun Ray interconnect and describes how to configure switches for specific scenarios.

Sun Ray System Computing Model

The Sun Ray enterprise system employs a highly network-dependent computing model where all actual computing is done at a server and display data is passed back and forth, instant by instant, between the Sun Ray enterprise server and the Sun Ray 1 enterprise appliances. Traffic in this environment (which is isolated from the LAN) can be heavy, and any network bottlenecks are immediately reflected at the users' desktops. Thus a powerful, well-designed interconnect between server and appliances is essential for providing high quality of service to users.

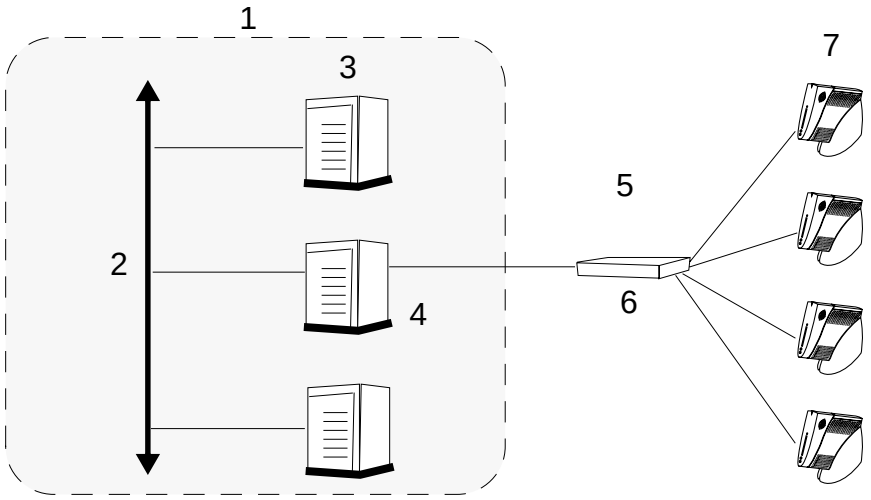

FIGURE 1-1 The Sun Ray Enterprise System and the LAN

Legend:

1. Managed environment
2. Local area network (LAN)—existing connection to intranet or Internet
3. Servers
4. Sun Ray server—executes applications
5. Dedicated interconnect—using Hot Desk protocol
6. Switch
7. Sun Ray 1 enterprise appliances

To boost the power of the interconnect and shield Sun Ray 1 appliance users from the network interaction taking place at every display update, 100 Mbps switches are preferred.

There are two basic types of 100 Mbps switches:

- Low-capacity switches—These switches have 10/100 Mbps interfaces for each port.
- High-capacity switches—These switches have 10/100 Mbps interfaces for each terminal port, but one or more gigabit interfaces to attach to the server.

Either of these switches can be used in the interconnect. They may be managed or unmanaged. However, managed switches usually require some basic configuration to use on a Sun Ray network. For details, refer to the Sun™ I/O Technologies web page at:

```
http://www.sun.com/sunray1
```

Server-to-switch bandwidth should be scaled based on end-user multiplexing needs so that the server-to-switch link does not become overly saturated. Gigabit uplink ports on the switch provide high-bandwidth connections from server, thus increasing the number of supportable clients.

To ensure high-speed transmission of the Hot Desk protocol, the interconnect must be completely dedicated and private (that is, not part of the corporate LAN). To this end, the Sun Ray server uses at least two network interfaces: one for the enterprise LAN, the other for the Sun Ray interconnect. With its own dedicated interface, the interconnect is isolated from other LAN activity and is, therefore, private.

Category 5 cables are required on the Sun Ray interconnect. It is important to make sure that your twisted pair wiring meets the CAT 5 standards.

It is also important to plan for a 100BASE-T, full-duplex network. Half-duplex services, or 10 Mbps, reduce the supported number of Sun Ray 1 enterprise appliances and degrade the quality of service on the interconnect.

Note – You can extend the distance between your Sun Ray server and switch by using gigabit fiber-optic cabling.

Quality of Service

In the Sun Ray enterprise system, the interconnect between the enterprise appliances and the service providers is a private communications channel. The application-specific protocol depends on a reasonable level of assurance that a defined Quality of Service (QOS) level is provided. This level of assurance is directly related to the following elements:

- Switch latency and buffering
- Available bandwidth

Switch Technical Requirements

Although the Sun Ray enterprise system leverages commodity network equipment, not any switch can be used in the interconnect. The interaction between the Sun Ray 1 enterprise appliance, the server, and the switch must meet the following qualifications.

TABLE 1-1 Switching Features Required on the Sun Ray Interconnect

Switch Feature	Requirement	Notes
Auto-negotiation	Enabled	All network equipment must auto-negotiate flawlessly with a Sun Ray 1 enterprise appliance. Sun Ray 1 appliances have no state and therefore have no means to configure link parameters. If there are any auto-negotiation problems, the switches cannot be used.
Buffering	High-capacity	Do not use *cut through* switches. Use *store and forward* switches.
Support for full-duplex connections	Enabled	Switches should support full-duplex connections to the Sun Ray 1 enterprise appliance and to the server. Half-duplex connections reduce the appliance number and performance on the interconnect.
Latency	Low	Switches add latency, or delay, to network traffic. Latency must be low to ensure quality of service to appliance users.
Link-up time	Minimum	The link-up time of certain switches includes a dead time during which all packets from an active link are ignored. This affects appliance startup.
Multicasting	Enabled	The Authentication Manager uses multicasting to enable communication between Sun Ray servers over their Sun Ray network interfaces in a failover environment. If the Sun Ray network switches do not support multicast addressing, the switches falsely determine that the Sun Ray interfaces have timed out. Consequently, manual redirection fails, and other Sun Ray servers are not displayed in the `utselect` or `utswitch` utilities.
Spanning tree	Disabled	Spanning tree policies default to very conservative values that affect appliance startup.

Refer to the web page at `http://www.sun.com/sunray1` for detailed descriptions on how to configure switches to meet these requirements.

Constraints

The Sun Ray 1 enterprise appliance is designed to work well with any standard Ethernet switch and relies solely on Level 2 switching support.

In the rare case that a switch did not test satisfactorily within the Sun Ray 1 enterprise appliance environment, it could be traced back to one of the following issues:

Auto-Negotiation

Note – All switches used in the interconnect should be configured to *Auto-Negotiate* instead of *Hard Coded Direct Connect*.

Note – You cannot hard code the speed / duplex rate on the Sun Ray 1 enterprise appliances.

The Sun Ray 1 enterprise appliance contains no internal state, and so it cannot be configured for a specific Ethernet interface setting. The appliance relies on auto-negotiation. With a small number of switching products, there have been mismatches in the results of auto-negotiation, from complete failure to operate to negotiation of operation at less than 100 Mbps full-duplex. You can test a switch by connecting the Sun Ray 1 enterprise appliance to the switch and observing the results of the connection. Extensive testing with more clients gives a greater degree of confidence.

To prevent negotiation problems for a fast connection, configure both sides of a connection to auto-negotiate. This requirement is described in the IEEE 802.3z (Gigabit system) auto-negotiation specification.

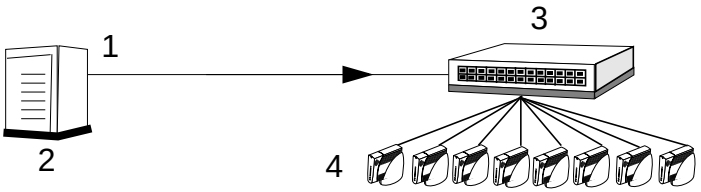

FIGURE 1-2 Problematic Switches and Auto-Configuration

Legend:

1. 10/100 Mbps NIC (network interface card) with port configured for auto-negotiation
2. Sun Ray enterprise server
3. End node configured for 100 Mbps/full-duplex or 10 Mbps/full-duplex (not auto-negotiation)
4. Sun Ray 1 enterprise appliances

For example, if a switch is configured to auto-negotiate and the attached end node is configured to 100 Mbps/full-duplex, the 802.3z specification requires that the switch not allow the 100 Mbps/full link to be established.

In FIGURE 1-2, after failing to auto-negotiate, the switch correctly senses the 100 Mbps speed. Since the end node was configured for a specific speed and duplex state, it does not auto-negotiate; consequently, the downstream switch chooses the communication mode specified by 802.3u (the specification for the 100-Mbps system) standard, which is half-duplex.

This connection works reasonably well at low levels of traffic. However, at higher levels (many end users accessing the internet) the full-duplex device (in this case the downstream switch) experiences reduced bandwidth. The configuration of each network device must be verified, and its configuration should match its performance.

Turn-On Time

The Sun Ray 1 enterprise appliance is designed to turn on and be fully operational in a very short time—typically less than 10 seconds.

Some switches have initial configurations that cause this turn-on time to be considerably longer, often taking as long as 30 seconds to achieve full working state. Turn-on times typically are longer because the Ethernet switch is configured to implement capabilities not needed in the Sun Ray 1 enterprise appliance environment. The most common of these capabilities is enabling Spanning Tree

protocols, which are designed to detect and compensate for loops in the connection between switches. Disable or defer Spanning Tree protocols for Sun Ray 1 enterprise appliance operation.

If Spanning Tree is disabled and the turn-on time is still excessive, contact the switch manufacturer to determine if there are other options that might be interfering with the Sun Ray 1 enterprise appliance. Some switches might have features designed into the switch that cannot be changed; if this is the case, then it may not be possible to reduce the turn-on time.

Bandwidth Limitation and Packet Loss

The Sun Ray 1 enterprise appliance depends on low latency, low packet loss delivery of the information used to create the screen image. Packet losses are visible to the user as horizontal bands in the display, where display update information has been lost. Additionally, the loss of information is noticed by the server, which slows down transmissions to compensate. This causes windows on the screen to display more slowly. These problems are temporary and not critical. The dropped information is redisplayed quickly.

If this behavior occurs frequently, the cause for dropping packets may be either a misconfigured switch or an oversubscribed switch. If a switch is not capable of transferring data at the maximum rate on all interfaces simultaneously, it is oversubscribed. This is not a problem in a normal LAN environment because most networks are underused, and dropped packets are recovered by higher level protocols requesting retransmission of the information. In a seriously oversubscribed environment, the Sun Ray 1 enterprise appliance performance may become unsatisfactory.

Recently manufactured switches cannot be oversubscribed; that is, there should never be any packets dropped with these switches. If you have older switches installed, primarily in mainframe configurations, the bandwidth may be quite low. In this situation, there may be significant oversubscription and the possibility of packet loss during high peak bandwidth usage. With these switches, carefully review the manufacturer’s specifications on switching backplane or backplane bandwidth for further information on bandwidth limitation and packet loss.

Example Topologies

The following figures illustrate topologies for two different sizes of the Sun Ray interconnect.

- In the Medium Interconnect Example, a Sun Enterprise™ 450 server supports 48 Sun Ray 1 appliances through two 24-port switches.
- In the Large Interconnect Example, a Sun Enterprise 4500 supports 204 Sun Ray 1 appliances through two 48-port switches and three 36-port switches.

Details on server resources and wiring are shown in the figures.

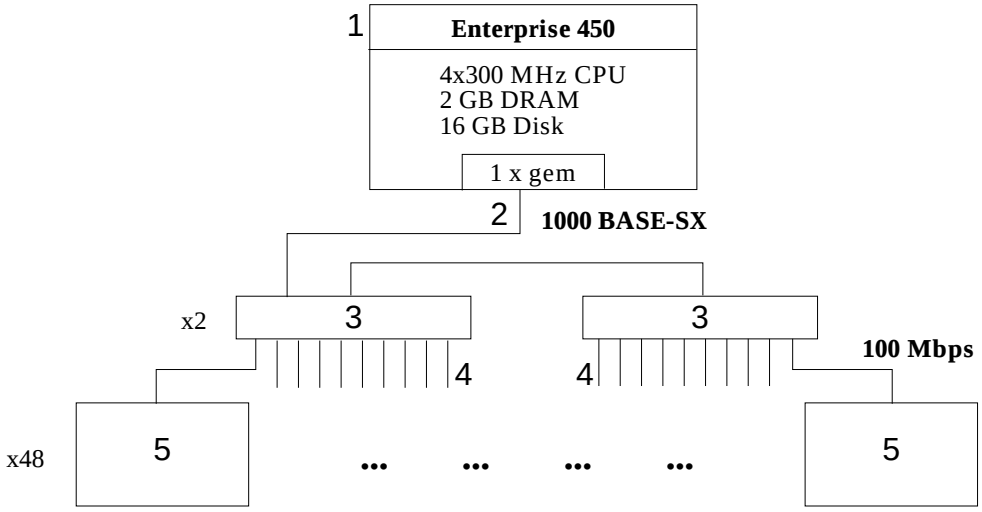

FIGURE 1-3 Medium Interconnect Example

Legend:

1. Sun Enterprise 450 server — configured as follows:
   - Four 300 MHz UltraSPARC™ processors
   - 2 Gigabytes DRAM
   - 16 Gigabytes disk space
   - One GEM network interface card
2. Cabling to provide 1000 BASE-SX
3. 24-port switch with 1000 BASE-SX ports
4. Cabling to provide 100 Mbps bandwidth
5. Sun Ray 1 enterprise appliances

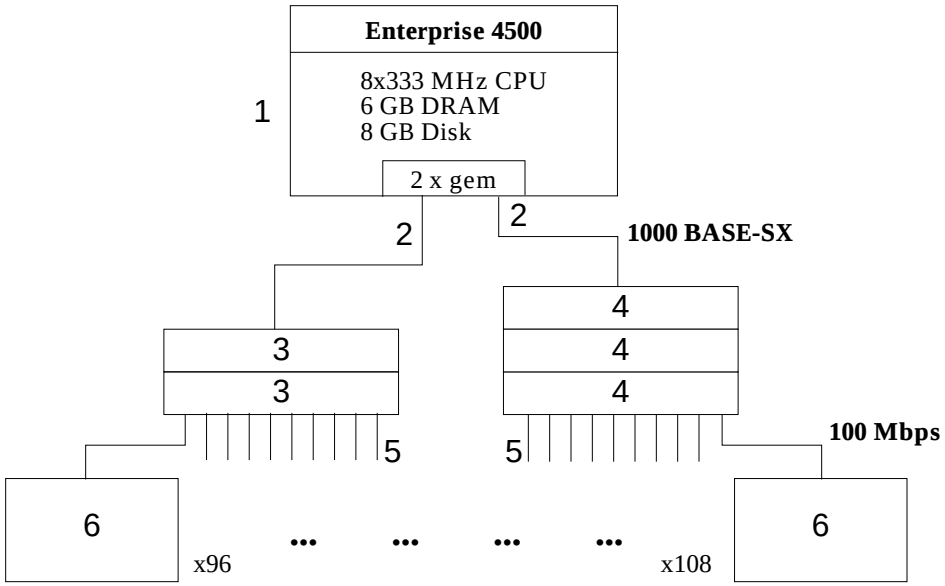

FIGURE 1-4 Large Interconnect Example

Legend:

1. Sun Enterprise 4500 server — configured as follows:
   - Eight 333 MHz UltraSPARC processors
   - 6 Gigabytes DRAM
   - 8 Gigabytes disk space
   - Two GEM network interface cards
2. Cabling to provide 1000 BASE-SX
3. 48-port switch with 1000 BASE-SX ports
4. 36-port switch with 1000 BASE-SX ports
5. Cabling to provide 100 Mbps bandwidth
6. Sun Ray 1 enterprise appliances

Switching Scenarios

When planning the development of the interconnect, take into account both required and available bandwidth. Bottlenecks are more likely to develop in the components connected to the LAN than within the interconnect itself. Carefully select a compatible switch. In workgroup computing, meet the continuously rising demand for bandwidth by using switches and hubs carefully.

Stringing Switches Together

A cascading switch utilizes the connection of twisted pair hubs by running twisted pair cable from one switch to another within the interconnect fabric. You can also cascade or string several switches together via CAT 5 cable. Unfortunately, this technique can reduce the overall performance of the interconnect.

Rather than cascade switches (FIGURE 1-5), it is recommended that you connect them using 1-Gigabit fiber-optic cable. The best approach is to connect multiple switches via a Gigabit core (FIGURE 1-6). Another preferred approach is to daisy chain the switches (FIGURE 1-7). See the figures below.

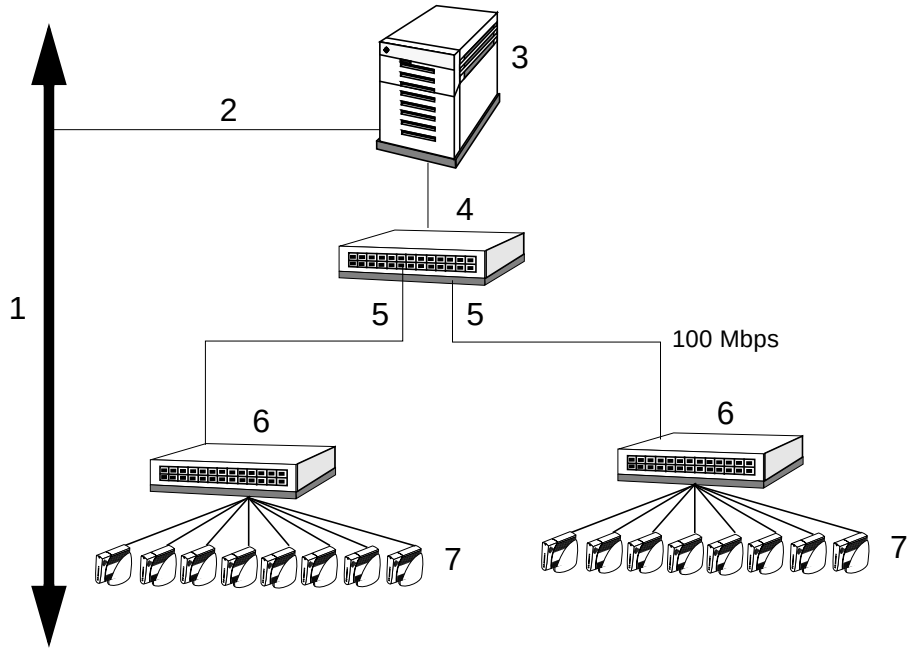

FIGURE 1-5 Cascading Switches

Legend:

1. Local area network (LAN)
2. Category 5 cable
3. Sun Ray enterprise server
4. Gigabit switch
5. Cabling to provide 100 Mbps bandwidth
6. Switches
7. Sun Ray 1 enterprise appliances

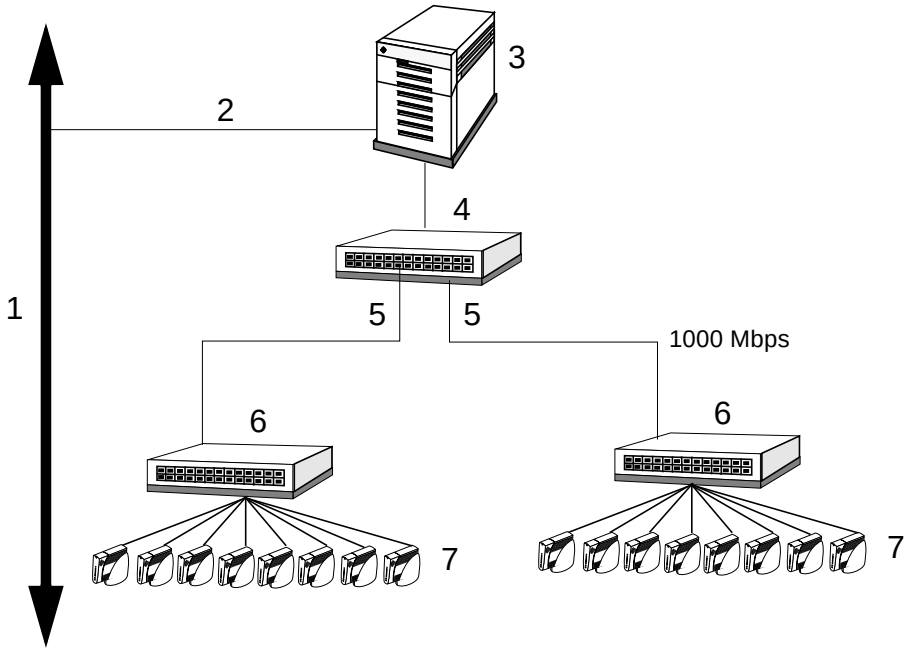

FIGURE 1-6 Cascading Gigabit Switches—Preferred

Legend:

1. Local area network (LAN)
2. Category 5 cable
3. Sun Ray enterprise server
4. Gigabit core switch
5. Cabling to provide gigabit (1000 Mbps) bandwidth
6. Gigabit switches
7. Sun Ray 1 enterprise appliances

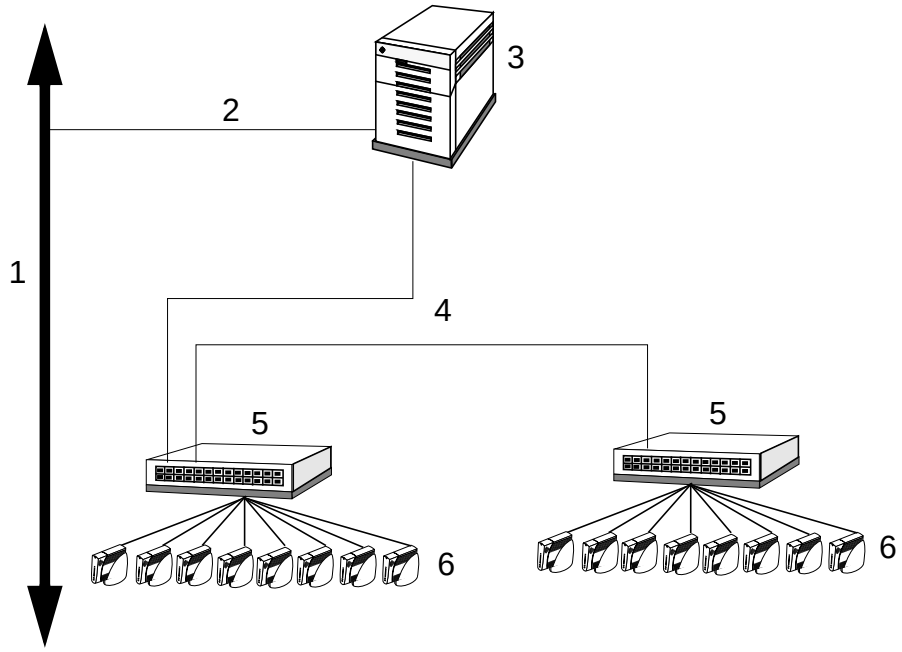

FIGURE 1-7 Daisy-Chained Switches—Preferred

Legend:

1. Local area network (LAN)
2. Category 5 cable
3. Sun Ray enterprise server
4. Cabling to provide gigabit bandwidth
5. Daisy-chained gigabit switches
6. Sun Ray 1 enterprise appliances

Using Additional Network Interface Cards

Additional network interface cards (NICs) can increase the size of the interconnect. Additional cards increase bandwidth and support more users or features.

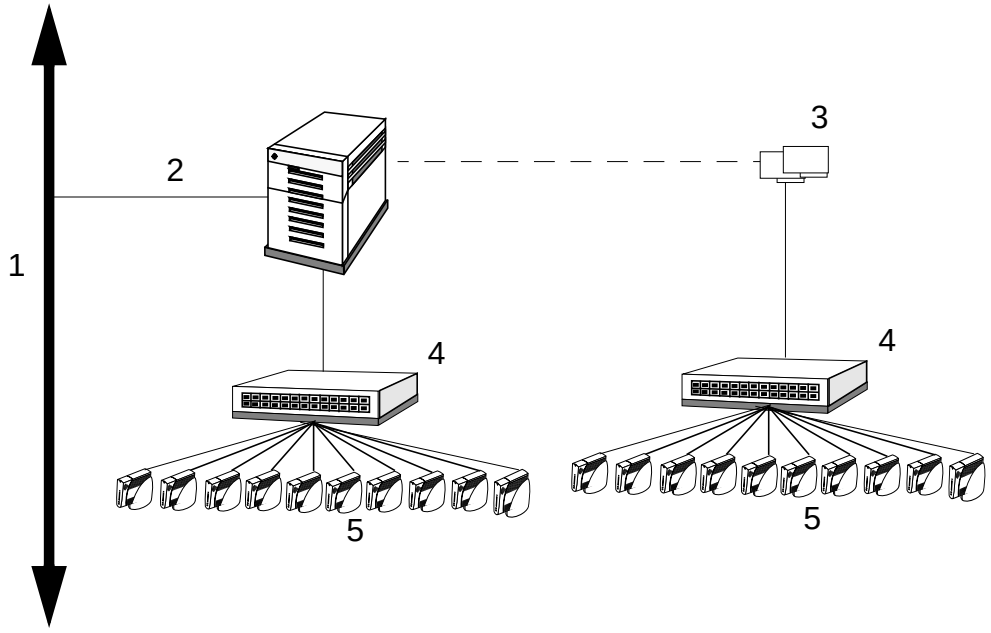

FIGURE 1-8 Additional Network Interface Cards: 10 Users With 1 Card, 20 Users with 2 Cards

Legend:

1. Local area network (LAN)
2. Category 5 cable
3. One or more network interface cards
4. Gigabit switches (10:1 ratio)
5. Sun Ray 1 enterprise appliances

Multiplexing

Multiplexing is the process of transmitting two or more signals over a single channel. This process is sometimes referred to as *muxing*. Since the interconnect fabric is constructed using shared or switched LAN technology, you can assume a moderate degree of statistical multiplexing is present. The Sun Ray 1 enterprise appliance connects to the interconnect via its 100BASE-T interface. The enterprise appliance is capable of displaying approximately 35 Mbps of virtual desktop

protocol. This reflects a multiplexing ratio of 3 to 1 (without any degradation). Using statistical multiplexing ratios as high as 10 to 1 are possible with little chance of packet loss (due to congestion). Ratios of 25 to 1 are a good rule of thumb.

Note – Always assume that moderate amounts of statistical traffic multiplexing exists (10:1 is a very conservative ratio; for example, 100 appliances can be connected via one gigabit link).

Replacing Hubs With Switches

While it is possible to use 100 Mbps hubs on the interconnect, hubs provide *shared* bandwidth rather than *switched* bandwidth. Select a switch over a hub whenever the condition allows. If you plan to distribute video to the Sun Ray 1 clients in the near future, higher-capacity switches (designed to handle the large requirements of high bandwidth) should also be considered.

By replacing existing hubs in your interconnect with switches, switching functions can be provided at the workgroup level. Hubs are half duplex; switches are full duplex. Use hubs only to get fan out (between switches and appliances). Allocate generous bandwidth at the switch when using hubs. Make sure the switch is configured to full bandwidth. Refer to your switch documentation for specific details.

CHAPTER 2

Failover

The single point of failure scenarios discussed in Chapter 1 can be mitigated by instituting a failover group consisting of multiple servers. This chapter describes this failover option, which is new in this release.

This chapter covers these topics:

Failover Overview

The Sun Ray enterprise server software version 1.1 provides clients with a higher level of availability of service when a hosting server becomes unavailable due to a network or machine failure. See FIGURE 2-1.

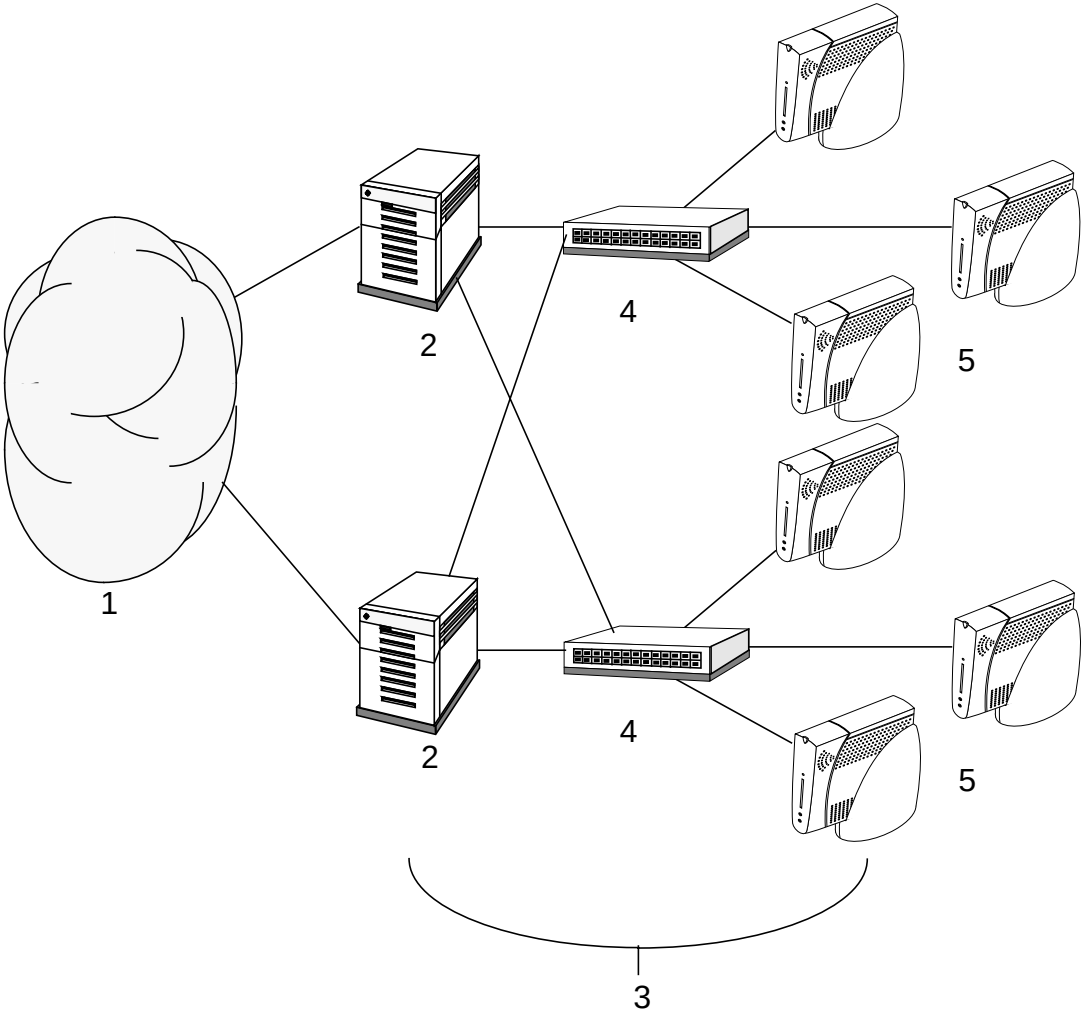

FIGURE 2-1 An Example Sun Ray System with Failover Feature

Legend:

1. Local area network (LAN) — existing connection to intranet or Internet
2. Sun Ray servers — execute X windows servers and X applications
3. Interconnect fabric — private network dedicated to Sun Ray 1 appliances (not part of the LAN)
4. Switches

5. Sun Ray 1 appliances

When a server fails, each Sun Ray 1 appliance that was using that server reconnects to one of the other servers in the failover group. The appliance connects to a previously existing session for that token if there is one on another server. If there is no existing session, the appliance connects to a server selected by a load-distribution algorithm. This server creates a new session and presents a login screen to the user. The user must relogin to create a new session. The state of the session on the failed server is lost.

The principal components needed to implement failover are:

- Multiple, coexisting Dynamic Host Configuration Protocol (DHCP) servers—All servers configured to assign IP addresses to Sun Ray clients have a non-overlapping subset of the available address pool. See FIGURE 2-2.
- Group Manager—A module that monitors the availability (liveness) of the configured servers and facilitates redirection when needed.
- Firmware enhancements to allow redirection of clients if the authenticating server does not own the user's active session.

The Sun Ray interconnect fabric is a *dedicated* and *private* network. Each Sun Ray 1 enterprise appliance must be connected to the interconnect fabric via its built-in network interface. This means that the Sun Ray 1 appliances are attached to a dedicated switch.

Caution – The Sun Ray interconnect fabric is not a corporate LAN. It is not to be shared with the corporate LAN or to be used in place of a corporate LAN. Do not connect Sun Ray 1 enterprise appliances to networks with other devices.

Setting Up IP Addressing

The `utadm` tool guides you in setting up a DHCP server. The default DHCP setup configures each interface for 225 hosts and uses private network addresses for the Sun Ray interconnect fabric. For more information on using the `utadm` command, see the *Sun Ray Enterprise Server Software 1.1 Administrator's Guide* or the man page for `utadm` in `/opt/SUNWut/man`.

Before setting up IP addressing, you must decide on an address scheme. The following examples discuss setting up Class C addresses.

Setting Up Class C Addresses

The loss of a server usually implies the loss of its DHCP service. Therefore, more DHCP addresses must be available from the group of servers than there are Sun Ray appliances. For example, if there are 5 servers and 100 appliances and one of the servers fails, the remaining DHCP servers must have enough addresses so that all the appliances get a working address. In this case, each would need to serve 100/(5-1) = 25 addresses. To deal with the case of the loss of two servers, each DHCP must be given a range of 100/(5-2) = 34 addresses.

These calculations represent the minimum number of addresses required per server. Since clients can get addresses from different servers each time they reboot, more addresses may be required even though only one of these addresses is in use at any given time. Since these unused addresses are not released until 24 hours after they are allocated, supply enough addresses so that a single DHCP server can service all of the clients. For example, with 2 servers and 100 clients, each server would have 100 IP addresses, which fits into a single class C network.

Note – For larger address ranges, use class B addresses since class C addresses support only 256 addresses in a single subnet.

Server Addresses

In the following example (see FIGURE 2-2), the server addresses are 192.168.128.1, 192.168.128.2, and 192.168.128.3.

Client Addresses

For client addresses in the following example, on the first server choose an address range for clients that won't overlap the addresses for the other servers; for example, 192.168.128.16 to 90.

On the second server, choose an address range for clients that won't overlap the addresses for the servers *and* the first client range; for example, 192.168.128.91 to 165.

On the third server, choose an address range for clients that won't overlap the addresses for the servers or the first and second client ranges; for example, 192.168.128.166 to 240.

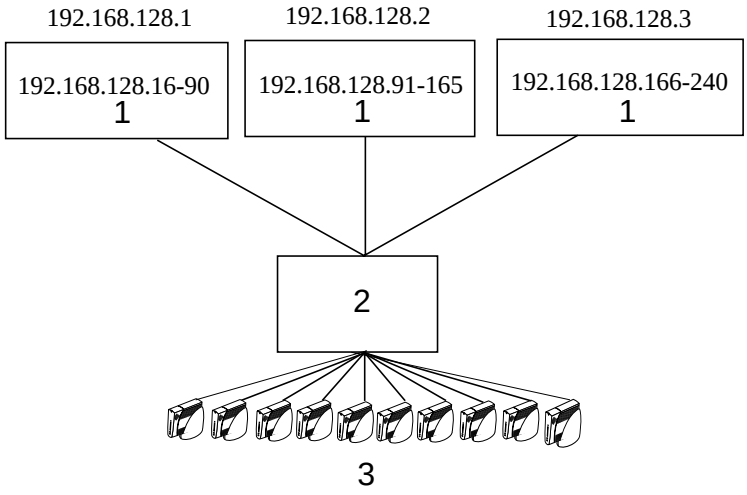

FIGURE 2-2 Client Address Ranges and Failover Scenario on Multiple DHCP Servers

Legend:

1. Sun Ray DHCP servers, including server and client IP addresses
2. Switching network
3. Sun Ray 1 appliances

When the user logs onto a Sun Ray, the appliance sends a DHCP broadcast request to all possible servers on the network interface. One or more responds with an IP address allocated from its non-overlapping range of addresses. The appliance accepts the first IP address that it receives and configures itself to send and receive at that address. The accepted DHCP response also contains information about the IP address and port number of the Authentication Manager on the server that sent the response. The appliance then attempts to establish a TCP connection to the Authentication Manager on that server. If it is unable to connect, it goes through another simple broadcast protocol similar to DHCP in which it asks Authentication Managers on the servers to identify themselves. The appliance then attempts to connect to the servers that responded in the order the responses were received.

Once a TCP connection to the Authentication Manager on a server has been established, the appliance presents its token to the Authentication Manager. The token is either a pseudo-token representing the individual appliance (its unique Ethernet address) or a smart card. Each token can be bound to an X windows session on each of the servers and possibly have a session on more than one server. However, a token can only be connected to one session at a time; that is, one server at a time. Therefore, to switch among existing sessions, the appliance must be redirected from one server to another.

For example, a smart card is inserted in a Sun Ray appliance. The appliance is connected to one of the servers and is running a session bound to the pseudo-token for that appliance. First, the Authentication Manager on the server disconnects the appliance from the pseudo-token session. Then it looks for the appropriate server for the newly inserted smart card token by sending a query to all of the other Authentication Managers on the same subnet that the appliance is on and asks for information about existing sessions for the token. The other Authentication Managers respond, indicating whether there is a session for the token and the last time the token was connected to the session. The requesting Authentication Manager selects the server with the latest connection time and redirects the appliance to that server. Each time the user inserts the smart card, the user is connected to the same session. If no session is found for the token, the requesting Authentication Manager selects the server with the lightest load and redirects the appliance to that server. The new server creates a new session for the token.

The Authentication Manager allows both implicit (smart card) and explicit switching. For explicit switching, see “Group Manager” on page 25.

Configuring DHCP

In a large IP network, a Dynamic Host Configuration Protocol (DHCP) server houses the IP addresses and other configuration information for individual computers on that network.

Coexistence of the Sun Ray DHCP Server With Other DHCP Servers

When you introduce a Sun Ray enterprise system into an existing corporate network, you must isolate Sun Ray DHCP services from other DHCP services on the network. Under no circumstances should a non-Sun Ray DHCP server reside on the same subnet as the Sun Ray interconnect. The Sun Ray interconnect is not intended to be shared with any other network traffic.

The Sun Ray DHCP server can coexist with DHCP servers on other subnets, provided you isolate it from other DHCP traffic by verifying that all routers on the network are configured not to relay DHCP requests. (This is the default behavior for most routers.)

Administering Other Clients

The Sun Ray interconnect is intended to be private. No other clients should reside on the interconnect itself. However, if the Sun Ray server has multiple interfaces (one of which is the Sun Ray interconnect), the Sun Ray DHCP server should be able to manage both the Sun Ray interconnect and the other interfaces without cross-interference.

Strictly speaking, DHCP requests from the Sun Ray 1 enterprise appliances could be resolved by a another DHCP server. However, because the interconnect is intended to be completely private, this situation should not arise. The `utadm` utility configures the Sun Ray DHCP server specifically to administer Sun Ray 1 appliances. Any other DHCP server would be cumbersome to configure.

▼ To Set Up IP Addressing on Multiple Servers Each With One Sun Ray Interface

1. **On each server, type:**

```
# /opt/SUNWut/sbin/utadm -a <interface_name>
```

where *-a* is add and <*interface_name*> is the name of the Sun Ray network interface to be configured; for example, `hme[0-9], qfe[0-9], or gem[0-9]`. The following table lists the options available for this command.

TABLE 2-1 Available Options

Option	Definition
-c	Create a framework for the Sun Ray interconnect
-r	Remove all Sun Ray interconnects
-a <*interface_name*>	Add <*interface_name*> as Sun Ray interconnect
-d <*interface_name*>	Delete <*interface_name*> as Sun Ray interconnect
-p	Print current configuration

Note – You must be logged on as root to run this command.

The `utadm` script configures the interface (for example, `hme1`) at the subnet (in this example, 128). The script displays default values, such as the following:

```
Selected values for interface "hme1"
    host address:       192.168.128.1
    net mask:           255.255.255.0
    net address:        192.168.128.0
    host name:          ray-231-128
    net name:           SunRay-128
    first unit address: 192.168.128.16
    last unit address:  192.168.128.240
    firmware server:    192.168.128.1
```

2. **When you are asked to accept the default values, type**:

```
 Accept as is? ([Y]/N): n
```

3. **Change the server IP address by typing the new address, in this case 192.168.128.2.**

```
new host address: [192.168.128.1] 192.168.128.2
```

4. **Accept the default values for netmask, host name, and net name.**

```
new netmask: [255.255.255.0]
new host name: [ray-231-128]
new net name: [SunRay-128]
```

5. **Change the client ranges for the interconnect by typing the new addresses.**

```
new first Sun Ray address: [192.168.128.16] 192.168.128.91
new last Sun Ray address: [192.168.128.240] 192.168.128.165
```

6. **Accept the default firmware server value.**

```
new firmware server: [192.168.128.2]
```

The selected values for interface `hme1` are displayed.

```
host address:       192.168.128.2
net mask:           255.255.255.0
net address:        192.168.128.0
host name:          ray-231-128
net name:           SunRay-128
first unit address: 192.168.128.91
last unit address:  192.168.128.165
firmware server:    192.168.128.2
```

7. **If these are correct, accept the new values.**

```
Accept as is? ([Y]/N): y
```

8. **Reboot the server and power cycle the appliances.**

Group Manager

Every server has a group manager module that monitors availability, facilitates redirection, and is coupled with the Authentication Manager. For more information on the Authentication Manager, see Chapter 1 in the *Sun Ray Enterprise Server Software 1.1 Administrator's Guide*.

In setting policies, the Authentication Manager, using the selected authentication modules, decides what tokens are valid and which users have access.

Warning – The same policy should exist on every linked server or undesirable results may occur. For information on policies, refer to the *Sun Ray Enterprise Server Software 1.1 Administrator's Guide*.

The group managers each create individual maps of the topology of the failover group by exchanging `keepalive` messages among themselves. Each group manager periodically sends a broadcast or multicast `keepalive` message to a well-known UDP port (typically 7009) on all of its configured network interfaces. The

`keepalive` message contains enough information for each server to construct a list of servers and the common subnets that each server can access. In addition, the group manager remembers the last time that a `keepalive` message was received from each server on each interface.

The `keepalive` messages contain the following information about the server:

- Server's hostname
- Server's primary IP address
- Elapsed time since it was booted
- IP information for every interface it can be reached on
- Machine information (number and speed of CPUs, configured RAM, and so on)
- Load information (CPU / memory utilization, number of sessions, and so on)

Note – The last two entries are used to facilitate load distribution. See "Load Distribution" on page 32.

The information maintained by the group manager is used primarily to perform server selection when a token is presented. The server and subnet information is used to determine the list of servers a given appliance can connect to, and these are the ones queried about sessions belonging to the token. Servers whose last `keepalive` messages on the appliance's network were received after the timer expires are deleted from the list since either the network connection or the server is probably down.

Redirection

In addition to automatic redirection at authentication time, manual redirection can be accomplished using the `utselect` graphical user interface (GUI) or `utswitch` from the command-line interface.

Note – The `utselect` graphical user interface (GUI) is the preferred method to use for server selection. The `utswitch` command is to be used as a backup method.

`utselect`

For the user, the server select GUI (see FIGURE 2-3) provides an easy and preferred method for server selection.

▼ To Redirect to a Different Server

- **Type**

```
# /opt/SUNWut/bin/utselect
```

The selections in the window are sorted in order of the last connection time with the latest first.

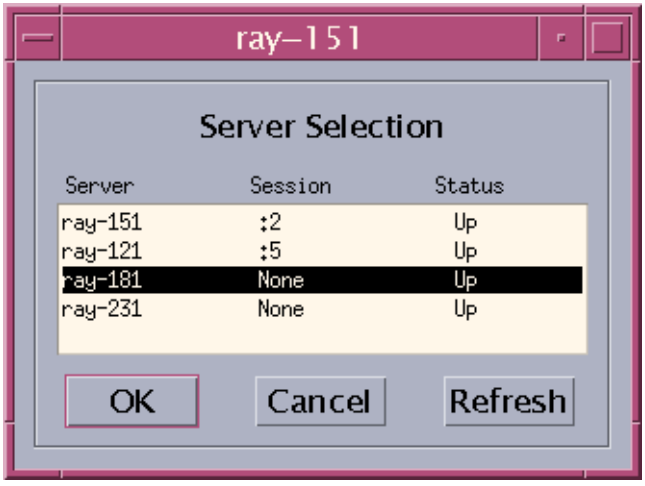

FIGURE 2-3 The Server Select Graphical User Interface

In the above illustration, the Server column lists the servers accessible from the appliance being used. The Session column reports the X session number on the server if one exists or None if there is no session. In the Status column, Up indicates that the server is available. The third server is highlighted by default to facilitate switching between servers. In FIGURE 2-3 server “ray-181” is highlighted. Since None appears under Session, a new session will be started.

The Refresh button reloads the window, which is not dynamic, with the most current information. The OK button changes to the highlighted server.

See the man page for `utselect` in `/opt/SUNWut/man`.

utswitch

The `utswitch` command provides the command line interface to redirection.

▼ To Manually Redirect an Appliance

- **Type:**

```
# /opt/SUNWut/bin/utswitch -h host [ -k token] [ -s sid ]
```

Where *host* is a host name or IP address to which the selected appliance is redirected. In the normal case, the optional arguments are not specified, and the selected appliance is the one on which the command is entered. If *-k token* is given, then the selected appliance is the one connected to the token's session on the current server. Similarly, if *-s SID* is given, the selected appliance is the one connected to the session with session ID *SID* on the current server. In both cases, an appliance may not be connected to the specified session; in which case, the command does nothing.

▼ To List Available Hosts

- **To list hosts that are available from the given Sun Ray unit, type:**

```
# /opt/SUNWut/bin/utswitch -l
```

▼ To Select a Different Current Server

This variant of the command, not normally invoked directly by the user, runs the server selection protocol that is executed when a token is presented to a server. When a user logs out from the current session, this command is executed so that the timestamp of the session the user is logging out from will be artificially modified backward in time. If there are existing sessions on other servers associated with the token, the user will be redirected to whatever existing session has the latest connect time. The *-k token* and *-s sid* options are used to identify the selected appliance in the same way as they are in the *-h* version of the command.

- **To redirect the selected appliance to the server with the latest session connect time, type:**

```
# /opt/SUNWut/bin/utswitch -t [ -k token] [ -s sid ]
```

See the man page for `utswitch` in `/opt/SUNWut/man`.

Group Manager Configuration

The Authentication Manager has a configuration file that contains parameters used by the group manager at runtime. The file is `/etc/opt/SUNWut/auth.props`. By default, the parameters are commented out. To change the default parameter values, remove the hash mark (#) in front of the parameter and set the parameter to the desired value. For example:

```
# gmDebug
# flag to turn on group manager debugging
  gmDebug = 2
```

The following parameters, discussed below, are configurable by the administrator though, in most cases, the defaults can be left unchanged:

- gmport
- gmKeepAliveInterval
- enableGroupManager
- enableLoadBalancing
- enableMulticast
- multicastTTL
- gmSignatureFile
- gmDebug

Excerpt from the `auth.props` file:

```
# Group Manager Port
# The group manager uses this port to send and receive keepalive/
# discovery messages from other auth managers.
# gmport = 7011
```

The group manager port only needs to be changed if another process is already using the same port number. Every host used in the failover scheme must use the same group manager port.

Excerpt from the `auth.props` file:

```
# Group Manager keep alive interval
# The group manager uses this as the time in seconds between
# broadcast keepalive messages
# gmKeepAliveInterval = 20
```

The keepalive interval may be changed to make the group managers communicate with each other more or less often. Although it is not essential, the gmKeepAliveInterval value should be identical on every server.

Excerpt from the auth.props file:

```
# enableGroupManager
# flag to turn on the group manager function
# enableGroupManager = true
```

This flag must always be on in a multiple server configuration. It may be turned off (that is, set to false) if only one server is used. However, if a second server is added to the group, the group manager must then be enabled and the Authentication Manager restarted before the additional server is recognized.

Excerpt from the auth.props file:

```
# enableLoadBalancing
# flag to turn on group manager load balancing
# enableLoadBalancing = true
```

The group manager attempts to distribute the session load evenly among the available servers. This capability does result in authenticating servers sometimes redirecting a Sun Ray appliance to a different server even when there is no existing session for the token, which results in an increased use of bandwidth resources.

The additional resource use should be negligible; however, this feature may be turned off (that is, set to false) if desired.

Excerpt from the auth.props file:

```
# Enable Multicast
# Flag to enable/disable use of multicast in group manager
# If disabled, group manager will use broadcast
# enableMulticast = true
```

Note – Some switches have multicast capability disabled by default although it can usually be turned on. If you do not want to use multicast in the Sun Ray interconnect, set this parameter to "false."

Excerpt from the `auth.props` file:

```
# Multicast Time-to-Live
# Time-to-live parameter for forwarding multicast packets
# If set above one, keepalive messages can pass through routers
# multicastTTL = 1
```

Note – This feature is only needed in sophisticated Sun Ray network configurations which contain routers.

Excerpt from the `auth.props` file:

```
# gmSignatureFile - Group Manager Signature File
# The group manager can "sign" messages to other group managers
# based on the contents of a signature file. Other group managers
# with the same signature file contents are "trusted". To be
# usable, the file must be owned by 'root' and must not be readable,
# writable, or executable by anyone else; it must contain at least
# 8 bytes, at least two of which are letters and at least one which
# is a non-letter.
# gmSignatureFile = /etc/opt/SUNWut/gmSignature
```

The `gmSignatureFile` property controls the location of the group manager signature file. The group manager signature file is used to create a trusted group of Sun Ray servers. See "Setting Up an Administered Group" on page 32.

Excerpt from the `auth.props` file:

```
# gmDebug
# flag to turn on group manager debugging
# gmDebug = 0
```

By default, the group manager does not output any debugging information. However, if problems occur where additional debugging information is desired, the `gmDebug` parameter can be raised to a positive value. The higher the value, the more information that is printed. Output is written to the file `/var/opt/SUNWut/log/auth_log`.

▼ To Restart the Authentication Manager

If any parameter is modified while the Authentication Manager is running, the change will not take effect until the `authd` is restarted.

- **To restart the Authentication Manager, type:**

```
# /etc/init.d/utsvc restart
```

Load Distribution

At the time of a server failure, the Group Manager on each remaining server attempts to distribute the failed server's sessions evenly among the remaining available servers. This method takes into account each server's capacity (number and speed of its CPUs) and load so that larger or less heavily loaded servers host more sessions. When the Group Manager receives a token from a Sun Ray and finds that no server owns an existing session for that token, it redirects the Sun Ray to the server in the group with the lightest load. If a different server is the least loaded, the Sun Ray is instructed to reauthenticate on that server. Thus, in some instances, a Sun Ray appears to authenticate twice, once on the server that answered its DHCP request and a second time on a server that was less loaded than the first.

▼ To Turn Off the Load Distribution Feature

- **In the** `auth.props` **file set:**

```
enableLoadBalancing = false
```

Setting Up an Administered Group

An administered group is one in which there are two or more group servers which utilize a policy other than Zero Admin. In such a group you must configure Lightweight Directory Access Protocol (LDAP) to enable replication of the administered data across the group. Such a group is composed of a primary server and one or more secondary servers. If the primary server fails, the secondary servers assume the administration data of the primary server, such as users, smart cards, and so on.

With the Zero Admin policy, it is possible to have a grouping of systems without having to administer them; that is, without running `utconfig` on each system.

The `utreplica` commands are only required for an administered system; that is, a system that has had the `utconfig` command run on it. The `utconfig` command sets up the LDAP server for a single system initially.

Note – This procedure may only be performed *after* running `utconfig` on each individual server.

Note – The value entered for `@(ROOTPW)` must be the same value used on all the secondary servers at `utconfig` time. See the Configuration Worksheet in Chapter 3, *Configuring the Software*, in the *Sun Ray Enterprise Server Software 1.1 Administrator's Guide*.

The LDAP server stores registered token information on stable storage. In a multiple host group, the distributed LDAP server uses a master-slave setup.

For more information on LDAP, see the documentation for SunDS.

Primary Server

The layered administration of the group takes place in the primary server in the group. Using the `utreplica` command, designate a primary server, advise it of its Administration Primary status, and inform it of the hostnames of all the secondary servers in the group.

Note – You must configure the primary server before any of the secondary servers.

Note – Each failover server in the interconnect fabric must have a unique hostname.

▼ To Specify a Primary Server

- **Type**:

```
# /opt/SUNWut/sbin/utreplica -p secondary_admin_pw \
secondary_server [secondary_server ...]
```

Where *secondary_admin_pw* is the value for `@(UTPASSWD)` entered when `utconfig` was run on each secondary server and *secondary_server [secondary_server ...]* is a list of the hostnames the secondary servers in the group.

Note – To include an additional secondary server to an already configured primary server, repeat the command including the additional secondary server in the new complete list of secondary servers.

Replication Setup

The secondary servers in the group hold a replicated version of the primary server administration data. Use the `utreplica` command to advise each secondary server of its secondary status and also the *hostname* of the primary server for the group.

▼ To Specify Each Secondary Server

- **Type:**

```
# /opt/SUNWut/sbin/utreplica -s primary_admin_pw <primary_server>
```

Where *primary_admin_pw* is the value for `@(UTPASSWD)` entered when `utconfig` was run on the primary server and <*primary_server*> is the hostname of the primary server.

Removing Replication Configuration

▼ To Remove the Replication Configuration

- **Type:**

```
# /opt/SUNWut/sbin/utreplica -u
```

This leaves the server as a standalone server from an administration perspective.

Note – This command must not be run without also reconfiguring/unconfiguring the other servers involved in the failover group.

Other Scenarios

Other scenarios include unconfiguring a primary/secondary pair and a primary with multiple secondary servers.

Primary/Secondary Pair

In the case of a primary/secondary pair, the replication context is eliminated. In this instance, both servers must be unconfigured.

Note – Unconfigure the primary server first.

Primary/Multiple Secondaries—Unconfiguring a Secondary

In this instance, first reconfigure the primary to replicate to all the secondaries except the one marked for removal. Then unconfigure that secondary.

Primary/Multiple Secondaries—Unconfiguring the Primary

Do not unconfigure the primary unless your intent is to reconfigure one of the secondaries as a primary, such as in a recovery scenario. In this case, all servers must be unconfigured and reconfigured.

Viewing the Administration Status

▼ To Show Current Administration Configuration

- **Type the command**:

```
# /opt/SUNWut/sbin/utreplica -l
```

The result indicates whether the server is Standalone, Primary (with the slave hostnames), or Secondary (with the Primary hostname).

Recovery Issues and Procedures

If one of the members of a group of services fails, the surviving group members should only operate from the administration data as it existed prior to the failure.

The recovery procedure required depends on the severity of the failure and whether a primary or secondary server has failed.

Note – When the primary server has failed, it is not possible to make administration changes to the system as all changes must be successful on the primary server for replication to work.

Secondary Server Recovery

Where a secondary server has failed, administration of the group may continue. A log of updates will be maintained that is applied automatically to the secondary server when it is recovered. If the secondary server needs to be reinstalled, repeat the steps outlined in the set up as though it were being initially configured. See the *Sun Ray Enterprise Server Software 1.1 Installation Guide*.

Primary Server Recovery

There are several strategies for recovering the primary server.

▼ To Rebuild the Primary Server Administration Data Store

1. **On one of the secondary servers, capture the current data store in a file called store:**

```
# /opt/SUNWconn/sbin/ldmcat /var/opt/SUNWconn/ldap/dbm.ut \
/id2entry.dbb > /tmp/store
```

   This provides an LDIF format file of the current database.

2. **FTP this file to `/tmp` on the newly installed primary server.**

   See the *Sun Ray Enterprise Server Software 1.1 Installation Guide*.

3. **Configure the primary server and type the following at the end of Step 4 in the installation procedure:**

```
# /opt/SUNWconn/sbin/ldif2ldbm -c -n 2 -j 10 -i /store
```

This populates the primary server and synchronizes its data with the secondary server.

4. **Stop and start the servers:**

```
# /etc/init.d/dsserv stop
# /etc/init.d/dsserv start
```

5. **Confirm that the data store is repopulated:**

```
# /opt/SUNWut/sbin/utuser -l
```

6. **Continue the remaining steps of primary server configuration.**

Setting Up a Trusted Group

A group of servers form a trusted group when the servers have identical contents in their group manager signature files. The group manager signature file is conventionally placed in:

```
/etc/opt/SUNWut/gmSignature
```

However, the location can be changed by changing the `gmSignatureFile` property in the `auth.props` file. See “Group Manager Configuration” on page 29.

To form a fully functional trusted group, the signature file must:

- be owned by root and must not be readable, writable, or executable by anyone else
- contain at least 8 bytes, at least two of which are letters and at least one which is a non-letter

---

Note – For additional security, use long passwords.

▼ To Create the Group Manager Signature File

1. **Type:**

```
# utgroupsig
```

You will be prompted for the signature.

2. **Enter it twice identically for acceptance.**

Note – It is important that the signature be entered via this command now and not be created in any other way since the command also ensures that LDAP replication occurs properly.

In that case in which all the Sun Ray servers are in the same group, any functions which depend on the database are unavailable. For example, the registration and the Administration application would be unavailable in the Zero Admin mode.

CHAPTER 3

Customizing the Window Manager

This chapter provides notes on customizing the window manager used by the Sun Ray clients. The benefits of changing or stripping down window managers include reduced training for new users and a more supportable installation.

Topics include:

Window Manager Functionality

A window manager provides the user with the graphical icons and controls needed to organize applications on the desktop. The types of handles and the degree of control afforded by the window manager determine the look and feel of the desktop.

For example, the window manager controls:

- The appearance of window frame components
- The behavior of windows, including their stacking order and focus behavior
- Key bindings and button bindings
- The appearance of minimized windows
- Desktop and window menus

It is possible to run applications without a window manager, and this mode may be desirable for certain single-function applications. However, if an application launches multiple windows, a window manager is needed to maintain a clear workspace. Otherwise, every time a new window is launched it displaces the current window.

The Solaris™ Common Desktop Environment (CDE) is the default windowing environment used by the Sun Ray desktops. Solaris CDE includes not only a window manager—`dtwm` (desktop window manager)—but also a login manager, a session manager, and applications such as a mail tool and calendar.

The following sections provide notes on modifying the CDE environment for your Sun Ray users: customizing CDE, stripping down CDE for kiosk mode, or replacing CDE's `dtwm` with a different window manager.

Customizing CDE

Details for customizing CDE are provided in the *Solaris CDE Advanced User's and System Administrator's Guide*, which is in the Solaris 7 User Collection available at:

```
http://docs.sun.com
```

CDE provides two basic levels of configuration: system-level and user-specific. System-level configurations apply to one Solaris system, whereas user-specific configurations apply to one user account. In general, CDE customizations for the Sun Ray enterprise should be made at the system level (on the Sun Ray enterprise server), as these changes are automatically applied to all Sun Ray users when they log into the server via a Sun Ray 1 appliance. However, user-level changes are appropriate if you want to customize the desktop for individual users.

The following is an example procedure you would use if your Sun Ray users required only two or three applications and you wanted to remove all other application icons from the CDE Front Panel.

▼ To Remove an Icon From the Front Panel

1. **Create a front panel configuration file (`.fp` file):**
   - For the Sun Ray enterprise server:

     `/etc/dt/appconfig/types/language/`*`name`*`.fp`
   - For a specific user:

     HomeDirectory`/.dt/types/`*`name`*`.fp`

2. **Copy the definition of the control you want to delete into the new file.**

   If the control is built-in, its definition is in `/usr/dt/appconfig/types/language/dtwm.fp`.

   You do not need to copy the entire definition. However, the portion you copy must include the fields `CONTAINER_NAME` and `CONTAINER_TYPE`.

3. **Add the Delete field to the definition:**

   ```
   DELETE    True
   ```

   For example, the following control definition placed in the file `TrashCan.fp` removes the Trash Can control from the front panel.

```
CONTROL Trash
       {
        CONTAINER_NAME  Top
        CONTAINER_TYPE  BOX
        DELETE          True
       }
```

4. **Save the configuration file.**

   The change is applied when each user restarts the window manager or logs out and logs in.

   In the figure below, all icons have been removed from the default CDE front panel except the following:

   - StarOffice™
   - Default web browser
   - Screen lock
   - Exit
   - Workspace switches

Legend:

1. Staroffice icon
2. Default web browser icon

Kiosk Mode

The central administration model of the Sun Ray enterprise makes it well-suited to kiosk deployments. For example, one type of kiosk would be a public computer terminal that might run a single, interactive application or browser to provide users with site-specific information, such as city maps or airline schedules.

Kiosk mode is characterized by the lack of a login manager and session manager. The master application is also the session manager for the system. When the user exits the master application, a new session is started immediately.

This can be implemented using features and paragraph scripting with CDE. If you are unfamiliar with how to do this, please see your system provider about obtaining examples or assistance.

Alternate Window Managers

CDE's window manager, `dtwm`, can be replaced by an alternate window manager to change the look and feel of the Sun Ray desktop.

In addition, dozens of window managers exist in the public domain for Solaris and Linux environments. Theoretically, any of them will work in the Sun Ray enterprise. You can find information on many of them on the web or in trade magazines.

▼ To Specify an Alternate Window Manager

The alternate window manager should be installed on the Sun Ray enterprise server.

1. **Create or open the alternate window manager configuration file:**
   - For the Sun Ray enterprise server:

     `/etc/dt/config/language/sys.resources`
   - For a specific user:

     HomeDirectory`/.Xdefaults`

2. **Specify the full path name and options for the alternate window manager with the `Dtsession*wmStartupCommand` resource.**

   For instructions on setting options for the window manager, see "Administering Application Resources, Fonts, and Colors" in the *Solaris CDE Advanced User's and System Administrator's Guide,* which is in the Solaris 7 User Collection available at:

   `http://docs.sun.com`.

3. **Save your changes.**

   The changes are applied when each user logs out and logs in.

Note – Not all window managers handle 24-bit color or drag-and-drop proficiently. You may also experience problems with fonts, localized fonts, and cut/copy/paste key functionality.

CHAPTER 4

Citrix and Windows NT

Citrix software is one way a Sun Ray user can access Microsoft Windows NT applications.

Microsoft Windows NT on Sun Ray System—Guidelines

To run NT sessions on the Sun Ray 1 appliance, you need:

- An NT server (x86 platform) or other appropriate hardware
- Citrix ICA Client for Solaris, or Java available at the Citrix website `http://www.citrix.com`
- Microsoft Windows NT Terminal Server (may be purchased from Microsoft or a software reseller)
- Citrix MetaFrame™ (may be purchased from Citrix or software reseller)

NT Terminal Server

For this connectivity, a Windows NT Terminal server is installed on a x86-based machine and configured to join the network using TCP/IP.

For instructions on how to install Microsoft Windows NT Terminal Server, please refer to the documentation included with the software. You must decide in advance whether to configure the machine as a stand-alone server or domain controller and whether to use NTFS or FAT partitions. Please consult your NT administrator regarding these issues.

Citrix MetaFrame

Install the Citrix MetaFrame software on the x86-based machine after installing the Windows NT Terminal Server. It is a straightforward installation procedure. For more detailed installation instructions, please refer to the documentation shipped with the software.

As the final step of the MetaFrame installation, the installation wizard asks you to remap the drive letters to other letters; for example, C:, D:, and so on, to X:, Y:, and so on. Choose “No” to leave the current settings or change the drive letters to X, Y, and Z. The Sun Ray 1 appliance has no local drive letters that could create conflicts.

ICA Client

You can download the latest ICA client from the Citrix website at `http://www.citrix.com`. Extract the package on your Solaris server and then run the install script. It is straightforward and requires little configuration. You are prompted to type in the path of the directory where you want the ICA client installed. Once the client is installed, a file named `wfcmgr` is created on the Solaris server.

To access NT, simply run the `wfcmgr` binary file on the Solaris server and specify a connection with the details of your Windows Terminal server. Double-clicking on this connection displays the Windows NT logon screen.

The `wfcmgr` binary can be run from the Sun Ray server console or from any Sun Ray 1 appliance that is connected to the Sun Ray server.

User Accounts on NT

All Sun Ray users must have accounts created for them within the NT domain to be able to access the Windows NT environment. Windows NT does not authenticate with Solaris servers. For information on how to create user accounts within NT, please refer to the Windows NT documentation. It is possible to disable the login screen or simply have everyone login automatically with a specific account (consider all the security implications before doing this). Please refer to Microsoft documentation or any third-party Windows NT administrator’s documentation for more details.

Unix Settings

Make the following changes only in case of problems:

- Make sure `xhosting` is enabled on your Solaris server if it has been disabled.
- Sometimes a Sun Ray 1 appliance's monitor does not display the NT session. Ask the user to type:

```
% echo $DISPLAY
```

to get the session number (##), then type:

```
% setenv $DISPLAY servername:##.0
```

to set the display. For example:

```
% setenv $DISPLAY yoyodata:91.0
```

- Sometimes 8-bit color needs to be turned on by using the `utxconfig -p on` command.

Note – For information on determining 8-bit status, see Chapter 1 of the *Sun Ray Enterprise Server Software 1.1 Administrator's Guide*.

On Sun Ray with one 24-bit TrueColor visual enabled, the ICA client is the first and default visual. If you turn on the PseudoColor visual, use `utxconfig` to make the ICA Client the default.

- If you are using the Solaris version of the ICA Client, make the following adjustments to the Sun Ray settings:

```
# utxconfig -p off
# utxconfig -p default
```

Note – This adjustment is not necessary if you are running the Java version of the ICA Client.

Glossary

bps	Bits per second.
category 5	The most common type of wiring used in LANs. It is approved for both voice and data (at up to 100Mhz). Also called cat 5.
client-server	A common way to describe network services and the user processes (programs) of those services.
DHCP	Dynamic Host Configuration Protocol. DHCP is a means of distributing IP addresses and initial parameters to the appliances.
domain	A set of one or more system boards that acts as a separate system capable of booting the OS and running independently of any other board.
Ethernet switch	A unit that redirects packets from input ports to output ports. Can be a component of the Sun Ray interconnect fabric.
Ethernet	Physical and link-level communications mechanism defined by the IEEE 802.3 family of standards.
Ethernet address	The unique hardware address assigned to a computer system or interface board when it is manufactured. See MAC address.
fan out	Connections that radiate out from a hub or switch.
FTP	File Transfer Protocol. The name of the Internet protocol and the program used to transfer files between hosts.
GEM	Gigabit Ethernet.
hot key	A pre-defined key that causes something to appear on your screen. A hot key is used to bring up the Settings screen on the Sun Ray enterprise appliance.
hot-pluggable	A property of a hardware component that can be inserted into or removed from a system that is powered on. USB devices connected to Sun Ray appliances are hot-pluggable.
Interconnect fabric	All the cabling, switches, or hubs that connect Sun Ray server's network interface cards to the Sun Ray appliances.

internet A collection of networks interconnected by a set of routers that enable them to function as a single, large virtual network.

Internet (Note the capital "I") The largest internet in the world consisting of large national backbone nets (such as MILNET, NSFNET, and CREN) and a myriad of regional and local campus networks all over the world. It is a global collection of networks connecting a wide range of computers using a common protocol to communicate and share services.

intranet Any network that provides similar services within an organization to those provided by the Internet outside it but which is not necessarily connected to the Internet.

IP address A unique number that identifies each host or other hardware system on a network. An IP address is composed of four integers separated by periods. Each decimal integer must be in the range 0-255 (for example, 129.144.0.0).

IP address lease The assignment of an IP address to a computer system for a specified length of time, rather than permanently. IP address leasing is managed by the Dynamic Host Configuration Protocol (DHCP). Sun Ray appliance IP addresses are leased.

LAN Local area network. A group of computer systems in close proximity that can communicate with one another via some connecting hardware and software.

LDAP Lightweight directory access protocol.

local host The CPU or computer on which a software application is running.

local server From the client's perspective, the most immediate server in the LAN.

login The process of gaining access to a computer system.

login name The name by which the computer system knows the user.

multicasting The process of enabling communication between Sun Ray servers over their Sun Ray network interfaces in a failover environment.

multiplexing The process of transmitting multiple channels across one communications circuit.

network Technically, the hardware connecting various computer systems enabling them to communicate. Informally, the systems so connected.

NIC Network interface card.

OSD On-screen display. The Sun Ray appliance uses small OSD icons to alert the user of potential start-up problems.

policies Authentication Manager, using the selected authentication modules, decides what tokens are valid and which users have access.

server A computer system that supplies computing services or resources to one or more clients.

service For the purposes of the Sun Ray software, any application that can directly connect to the Sun Ray appliance. It can include audio, video, X servers, access to other machines, and device control of the appliance.

session A group of services associated with a single user.

spanning tree The spanning tree protocol is an intelligent algorithm that allows bridges to map a redundant topology and eliminates packet looping in Local Area Networks (LAN).

subnet A working scheme that divides a single logical network into smaller physical networks to simplify routing.

token In the Sun Ray system, a token must be presented by the user. It is required by the Authentication Manager to consider allowing a user to access the system. It consists of a type and an ID. If the user inserted a smart card, the smart card's type and ID are used as the token. If the user is not using a smart card, the enterprise appliance's built-in type (pseudo) and ID (the unit's Ethernet address) are supplied as the token.

thin client Thin clients remotely access some resources of a computer server, such as compute power and large memory capacity. The Sun Ray appliances rely on the server for all computing power and storage.

time-out value The maximum allowed time interval between communications from an appliance to the Authentication Manager.

TCP-IP Transmission Control Protocol/Internet Protocol (TCP/IP) is a networking protocol that provides communication across interconnected networks, between computers with diverse hardware architectures and operating systems.

URL Uniform Resource Locator. A standard for writing a textual reference to an arbitrary piece of data in the World Wide Web (WWW). The syntax of a URL is `protocol://host/localinfo` where `protocol` specifies a protocol to use to fetch the object (like HTTP or FTP), `host` specifies the Internet name of the host on which to find it, and `localinfo` is a string (often a file name) passed to the protocol handler on the remote host.

user name The name a computer system uses to identify a particular user. Under UNIX this is a text string of up to eight characters composed of letters (a-z and A-Z), digits (0-9), hyphens (-), and underscores (_) (for example, jpmorgan). The first character must be a letter.

virtual frame buffer A region of memory on the Sun Ray server that contains the current state of a user's display.

work group A collection of associated users who exist in near proximity to one another. A set of Sun Ray appliances that are connected to a Sun Ray server provides computing services to a work group.

Index

V

W