Sun Ray™ Server Software 3 Administrator's Guide

for the Linux Operating System

Sun Microsystems, Inc.
www.sun.com

Part No. 817-6811-10
November 2004, Revision A

Submit comments about this document at: `http://www.sun.com/hwdocs/feedback`

Contents

Figures

Tables

Preface

The *Sun Ray Server Software 3 Administrator's Guide for the Linux Operating System* provides instructions for setting up, administering, monitoring, and troubleshooting a system of Sun Ray™ Desktop Units (DTUs) and their server or servers. It is written for system administrators who are already familiar with the Sun Ray™ computing paradigm and have substantial networking knowledge. This guide may also be useful for those interested in customizing Sun Ray systems.

Before You Read This Book

This guide assumes that you have installed the Sun Ray Server Software on your server from the Sun Ray Server Software 3 CD or the Electronic Software Download (ESD) and that you have added the required patches.

How This Book Is Organized

Chapter 1 gives an overview of the Sun Ray system.

Chapter 2 describes the command-line interface.

Chapter 3 describes the Administration Tool.

Chapter 4 describes peripheral devices for Sun Ray DTUs.

Chapter 6 gives a brief description of traffic encryption between Sun Ray clients and servers and server-to-client authentication.

Chapter 6 provides details on installation and configuration of the Gnome Display Manager.

Chapter 8 discusses network requirements, including LAN, VLAN, and dedicated interconnect options, switch requirements, and other network topology issues.

Chapter 9 describes how to implement multihead and XINERAMA features on a Sun Ray system.

Chapter 11 discusses failover groups.

Appendix A addresses user issues and concerns.

Appendix B provides troubleshooting information, including error messages from the Authentication Manager.

Appendix C contains a listing of Sun Ray parameter symbol values defined in the DHCP table and a brief discussion of encapsulated options.

This manual also contains a glossary and an index.

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. This document does, however, contain information about specific Sun Ray system commands.

Typographic Conventions

Typeface	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	Read Chapter 6 in the *User's Guide*. These are called *class* options. You *must* be superuser to do this.
	Command-line variable; replace with a real name or value	To delete a file, type `rm` *filename*.

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

Application	Title	Part Number
Installation	*Sun Ray Server Software 3 Installation and Configuration Guide for the Linux Operating System*	817-6810-10
Release Notes	*Sun Ray Server Software 3 Re;ease Notes for the Linux Operating System*	817-6813-10

Accessing Sun Documentation

You can view, print, or purchase a broad selection of Sun documentation, including localized versions, at:

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

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can email your comments to Sun at:

`docfeedback@sun.com`

Please include the part number (817-6811-10) of your document in the subject line of your email.

CHAPTER 1

Sun Ray System Overview

Although thin client computing has been discussed and attempted for many years, Sun Ray is the first implementation to offer both workstation-like user functionality and sufficient speed and reliability to be suitable for mission-critical applications. The latest generation of Sun Ray Server Software now supports many USB peripheral devices, LAN and low-bandwidth WAN deployment. Originally developed on Sun's Solaris™ Operating System, Sun Ray Server Software is now also supported on three Linux variants: Red Hat Enterprise Linux Advanced Server 3, SuSE Linux Enterprise Server 8, and Sun Java™ Desktop System 2.

Computing Model

The Sun Ray system employs a network-dependent model in which all computing is performed on a server, with input and output data passed back and forth between the Sun Ray server and the Sun Ray Desktop Units (DTUs). Nearly any Sun server with sufficient capacity can be configured as a Sun Ray server so long as it runs a supported version of the Solaris operating system or one of the supported flavors of Linux.

Various models of Sun Ray DTU are available, differing primarily with respect to size and type of screen; however, all Sun Ray DTUs also include a smart card reader, a keyboard, and a mouse. Sun Ray DTUs have no local disks, operating systems, or applications; they are therefore considered *stateless*. This is what makes them true, or "ultra" thin clients, and it is what makes them inexpensive to maintain as well as extremely secure, both from an intellectual property perspective and for government work. Although USB devices are supported, the ability to use them is administered centrally so that sites with security requirements can easily remove the sort of risk imposed by PCs and other fat clients that allow the theft of data in case a physical device is stolen.

Because effective client-server network traffic often relies on the rapid movement of large numbers of packets, an optimal Sun Ray implementation requires a well-designed network. Most large implementations include at least one *failover group* to ensure uninterrupted service whenever a server goes off-line.

Once a failover group is set up, Sun Ray Server Software provides automatic load balancing to optimize performance by spreading the computing load among the servers in the group. If a server is taken out of service, the Group Manager on each remaining server tries to distribute that server's sessions evenly among the remaining servers. The load balancing algorithm takes into account each server's load and capacity (number and speed of its CPUs) so that larger or less heavily loaded servers host more sessions. These concepts are addressed in Chapter 11 and in the *Sun Ray Server Software 3 Installation and Configuration Guide*.

User sessions—groups of services controlled by the Session Manager and associated with a user through an authentication token—reside on a server and are directed to a Sun Ray DTU. Because Sun Ray DTUs are stateless, a user session can be redirected to any Sun Ray DTU on the appropriate network or subnetwork when a user logs in or inserts a smart card.

While the session continues to reside on a server, it appears to follow the user to the new DTU. This functionality, called *session mobility*, is the key architectural feature that enables *hot desking*—the ability of users to access their sessions from any DTU on their network. In early versions of Sun Ray Server Software, mobile sessions were possible only with smart cards. It is now possible to enable hot desking with or without smart cards.

The Sun Ray System

The Sun Ray system consists of Sun Ray DTUs, servers, server software, and the physical networks that connect them.

Sun Ray DTU

The Sun Ray desktop unit (DTU) delivers and may exceed the full functionality of a workstation or a multimedia PC. The key features include:

- 24-bit, 2-D accelerated graphics up to 1920 x 1200 resolution at 72 Hz (640 x 480 at 60 Hz is the lowest resolution)
- Multichannel audio input and output capabilities
- Smart card reader
- USB ports that support hot-pluggable peripherals
- EnergyStar™ compliance

- No fan, switch, or disk
- Very low power consumption

The DTU acts as a frame buffer on the client side of the network. Applications run on the server and render their output to a *virtual frame buffer*. Sun Ray server software formats and sends the rendered output to the appropriate DTU, where the output is interpreted and displayed.

From the point of view of network servers, Sun Ray DTUs are identical except for their Ethernet MAC addresses. If a DTU ever fails, it can easily be replaced.

IP addresses are leased to each Sun Ray DTU when it is connected and can be reused when the DTU is disconnected. IP address leasing is managed by the Dynamic Host Configuration Protocol (DHCP). In cases where they already exist on a network that will support Sun Ray DTUs, separate DHCP servers may be useful for tasks such as assigning IP addresses and network parameters to the DTUs. The use of separate DHCP servers is not required. These questions are discussed in Chapter 7 and Appendix C.

Multihead Displays

Sun Ray Server Software supports the use of multiple displays connected to a single keyboard and pointer. This functionality is important for users who need extra screen real estate, for instance, to monitor many applications or systems simultaneously or to accommodate a single application, such as a large spreadsheet, across multiple screens. To use multiple screens, the administrator sets up multihead groups, consisting of two or more DTUs, for those users who need them. Administration of multihead groups is explained in Chapter 9.

Firmware Module

A small firmware module in each Sun Ray DTU can be updated from the server. The firmware module checks the hardware with a power–on self test (POST) and initializes the DTU. The Sun Ray DTU contacts the server to authenticate the user, and it also handles low-level input and output, such as keyboard, mouse, and display information. If there is a problem with the DTU, the module displays an on–screen display (OSD) icon to make it easier to diagnose. OSD icons are described in Appendix B.

Sun Ray Server Software

Sun Ray server software allows the administrator to configure network connections, select an authentication protocol, administer users, define desktop properties, monitor the system, and troubleshoot a wide variety of administration problems.

Sun Ray server software includes:

- User authentication and access control
- Encryption between the Sun Ray server and DTUs
- System administration tools
- Session management
- Device management, including application-level USB access
- Virtual device drivers for audio and serial, parallel, and mass storage USB devices

Sun Ray server software enables direct access to all Linux X11 applications. Third-party applications running on the Sun Ray server can provide access to Microsoft Windows NT applications and a variety of legacy (mainframe) applications.

Authentication Manager

The Authentication Manager implements the chosen policies for identifying and authenticating users on Sun Ray DTUs. The Authentication Manager uses pluggable components called *modules* to implement various site-selectable authentication *policies*.

The Authentication Manager also verifies user identities and implements site access policies. The Authentication Manager is not visible to the user.

The interaction between the Authentication Manager and the DTU works as follows:

1. A user accesses a DTU.
2. The DTU sends the user's token information to the Authentication Manager and requests access. If a smart card is presented to the DTU, the smart card's type and ID are the token. If not, the DTU's Ethernet address is sent.
3. If the Authentication Manager runs through the entire list of modules and no module takes responsibility for the request, the user is denied.
4. If the user is accepted, the Authentication Manager starts an X Windows session for the user, which takes the user to the login screen. Solaris implementations use the `dtlogin` screen; Linux implementations use GDM.

Normally, the Sun Ray DTU looks for the `AuthSrvr` DHCP option and contacts that address. If that field has not been supplied, or if the server does not respond, the DTU sends a broadcast request for any authentication manager on its subnet.

As an alternative, the administrator can supply a list of servers. If the authentication list is specified, only addresses on the list are checked. The Authentication Manager addresses are tried in order until a connection is made.

The site administrator can construct a combination of the different modules and their options to implement a policy tailored to the site's needs.

The modules are:

- StartSession

  Any type of token is accepted. Users are automatically passed through to the login window. This module is designed primarily for implementations in which Sun Ray DTUs replace workstations or PCs.

- Registered

  The token is accepted *only* if the token has been registered in the Sun Ray administration database *and* the token is enabled. If the token does not meet these conditions, it is rejected. If accepted, the user is passed through to the login window. This module is designed for sites that want to restrict access to only certain users or DTUs.

  Users can be registered in two ways, reflecting two possible policy decisions for the administrator:

  - Central Registration

    The administrator assigns smart cards and/or DTUs to authorized users and registers users' tokens in the Sun Ray administration database.

  - Self-Registration

    Users register themselves in the Sun Ray administration database. If this mode is enabled and the Authentication Manager is presented with an unregistered token, the user is prompted with a registration window. In this case, the user provides the same information a site administrator would request.

  If self-registration is enabled, users can still be registered centrally. If a token has been registered but disabled, the user cannot re-register the token; the user must contact the site administrator to re-enable the token.

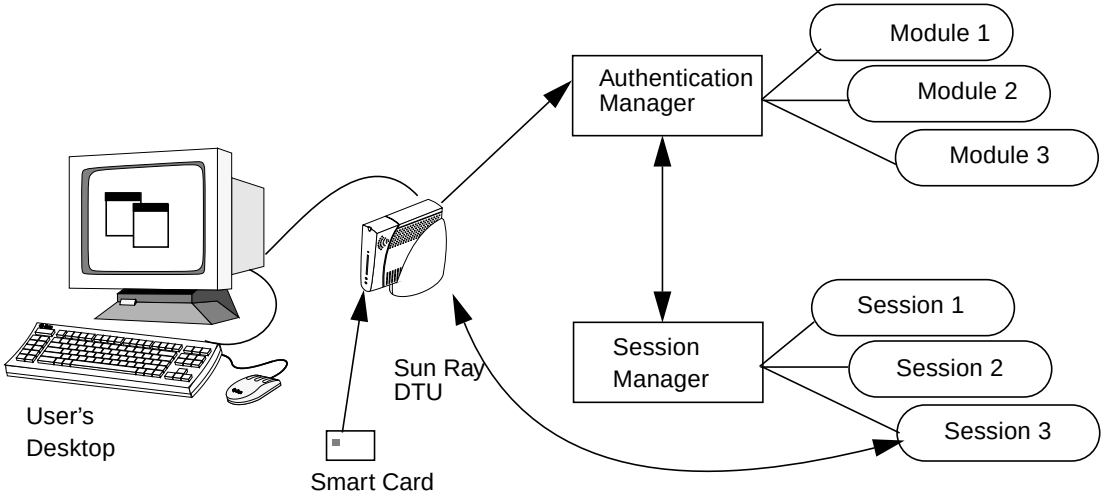


FIGURE 1-1 Authentication and Session Manager Interaction

Sessions and Services

A *session* consists of a group of services controlled by the Session Manager.

The session is associated with a user through an authentication token. A *service* is any application that can connect directly to the Sun Ray DTU. This can include audio, video, X servers, and device control of the DTU. For example, `dtmail` is not a service because it is accessed through an X server.

Session Manager

The Session Manager interacts with the Authentication Manager and directs services to the user. The Session Manager is used at start up for services, for managing screen real estate, and as a rendezvous point for the Authentication Manager.

The Session Manager keeps track of sessions and services by mapping services to sessions and binding and unbinding related services to or from a specific DTU. The Session Manager takes authentication only from authorized Authentication Managers listed in the `/etc/opt/SUNWut/auth.permit` file.

The steps below describe how the process starts and ends:

1. After a user's token is authenticated, the Authentication Manager determines whether a session exists for that token. If a session does not exist, the Authentication Manager asks the Session Manager to create a session and then

starts the appropriate service(s) for the session according to the policy decisions taken by the administrator. Creating a session usually involves starting an `Xserver` process for the session.

2. When services are started, they explicitly join the session by contacting the Session Manager.
3. The Authentication Manager informs the Session Manager that the session associated with the token is to be connected to a specific Sun Ray DTU. The Session Manager then informs each service in the session that it should connect directly to the DTU.
4. The Authentication Manager determines that the session associated with a token should be disconnected from an DTU. The Authentication Manager notifies the Session Manager which, in turn, notifies all the services in the session to disconnect.
5. The Session Manager mediates control of the screen real estate between competing services in a session and notifies the services of changes in screen real estate allocation.

Caution – It is important to keep the session ID private. If the user's session ID is revealed, unauthorized applications can connect directly to the DTU. The `xprop(1)` command can reveal an end user's secret session ID. Also, careless use of the `xhost(1)` command (for example, typing `xhost +`) can allow an intruder to use `xprop` to capture a user's session ID. This action can expose the user's screen images and keyboard input to anyone interested.

Tip – Use `xhost username@system` to enable only those people you specify to access the display and the user's DTU.

The Session Manager is consulted only if the state of the session changes or if other services are added. When a user's token is no longer mapped to an DTU (for example, when a card is removed), the Session Manager disconnects the services from the DTU, but the services remain active on the server. For example, programs attached to the X server continue to run although their output is not visible. The Session Manager daemon must continue running all the time.

Note – To verify that the Session Manager daemon is running, use the `ps` command and look for `utsessiond`.

If the Authentication Manager quits, the Session Manager disconnects all the sessions it authorized and tells them that they have to be re-authenticated. The services are disconnected but still active. If the Session Manager is disrupted, it restarts automatically. Each service contacts the Session Manager to request reattachment to a particular session.

CLI and Admin GUI

Sun Ray Server Software has both a command-line interface (CLI) and a graphical user interface for administrative functions. The CLI is the recommended interface for enabling assistive technologies; the Sun Ray Administration Tool (Admin GUI) is provided for convenience.

Data Store

Sun Ray Server Software 3 provides a private data store service, the Sun Ray Data Store (SRDS). The SRDS provides group-wide access to SRSS administration data.

Network Components

In addition to the servers, server software, DTUs, smart cards, and peripheral devices, such as local printers, the Sun Ray system needs a well-designed network, configured in one of several possible ways, including:

- Dedicated interconnect
- VLAN (Virtual Local Area Network)
- LAN (Local Area Network), with or without network routers
- Low-bandwidth[1] WAN (Wide Area Network)

Various types of network configuration are discussed in depth in Chapter 7.

Sun Ray Interconnect Fabric

Early Sun Ray implementations relied on dedicated interconnects, using physically dedicated Ethernet networks or logically dedicated networks. Sun Rays can now be deployed on existing Local Area Network (LAN) infrastructure, eliminating the requirement for a dedicated interconnect.

1. Bandwidth less than 2 Mbps.

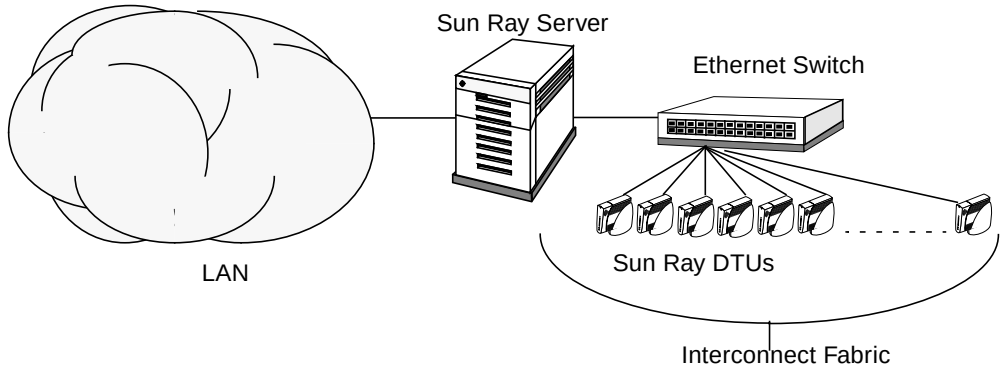


FIGURE 1-2 Sun Ray System with a Dedicated Interconnect Fabric

The Sun Ray interconnect fabric is based on 10/100BASE-T Ethernet technology, using layer-2 or layer-3 switches and Category 5 wiring. Each Sun Ray DTU is attached to the interconnect fabric through its built-in 10/100BASE-T interface.

The following sections illustrate some conservative methods of providing good desktop performance to Sun Ray users at a low cost. Many other network scenarios are possible.

VLAN Implementation

VLANs logically partition a single physical interconnect into two or more broadcast domains. VLANs are commonly configured to implement virtual subnets in a shared physical interconnect. However, because VLANs must share backplane and link bandwidth, they are not true dedicated interconnects.

Implementing a Sun Ray interconnect through VLANs creates a logically dedicated connection, but can also mean sharing physical resources with uncontrolled, non-Sun Ray traffic. These resources could be the limited backplane bandwidth within a switch or on a link that carries multiple VLANs between switches (see FIGURE 1-3). If these resources are consumed by other devices, significant amounts of Sun Ray DTU traffic might be dropped and the results seen as horizontal bands or blocks on the user's display.

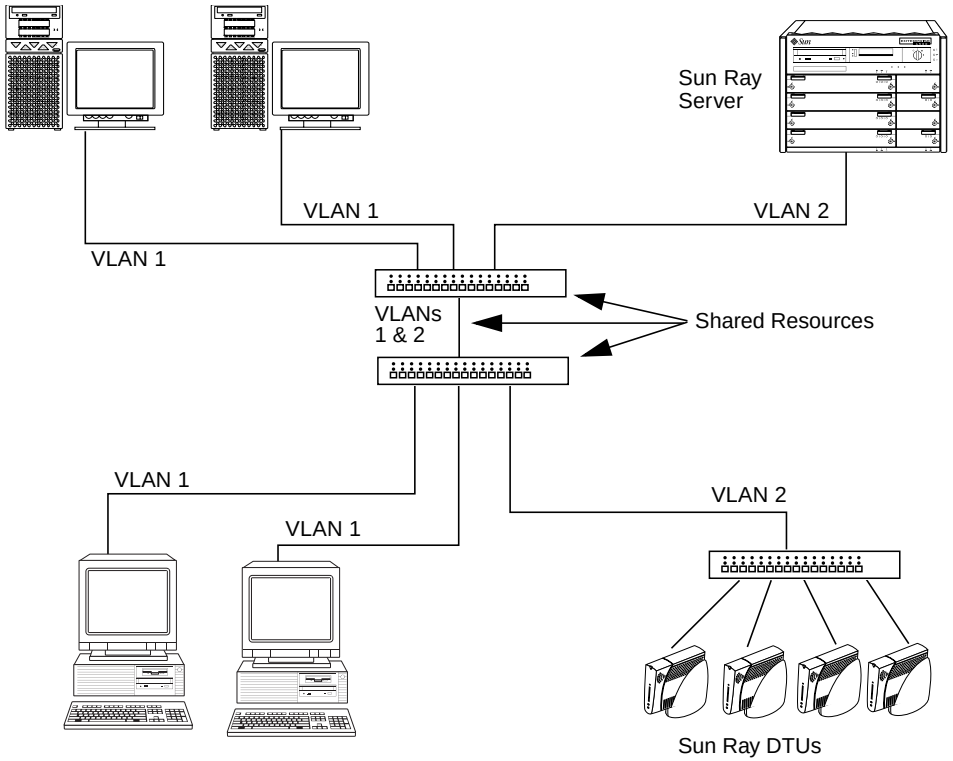


FIGURE 1-3 Example of Shared Physical Resources in Multiple VLANs Configuration

Since switch manufacturers configure their products differently, please refer to the documentation provided with your switch and refer all questions relating to setting up or configuring VLANs to your switch manufacturer.

Implementing the interconnect with a physically dedicated and isolated set of Ethernet switches was recommended because it is easy and reliable. For instance:

- Only layer 2 switches are required.
- The only switch configuration required is to enable fast boot times.
- No ongoing switch configuration and management is required.
- Issues of bandwidth and poor topology are greatly reduced.

LAN Implementation

With Sun Rays deployed on a LAN, users can exercise session mobility across a much larger "domain"—a huge convenience. For basic instructions on configuring different types of networks for Sun Ray implementation, see "Basic Network

Topology" on page 30 of the *Sun Ray Server Software 3 Installation and Configuration Guide*. For a more detailed discussion of network taxonomy and configuration, see "Deployment on Shared Networks" on page 109.

Physical Connections

The physical connection between the Sun Ray server and Sun Ray clients relies on standard switched Ethernet technology.

To boost the power of the interconnect and shield Sun Ray DTU 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 type of switch can be used in the interconnect. They can be managed or unmanaged; however, some managed switches may require basic configuration to be used on a Sun Ray network.

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 the server, thus increasing the number of supportable clients. The distance between the server and the switch can also be extended using gigabit fiber-optic cabling.

The interconnect may be completely dedicated and private, or a VLAN, or it may be part of the corporate LAN. For private interconnects, the Sun Ray server uses at least two network interfaces: one for the corporate LAN, the other for the Sun Ray interconnect.

Even in a LAN deployment, two server network interfaces are recommended: one to connect to the general LAN and one to connect the server to back-end services, such as file servers, compute grids, and large databases.

Deployment Examples

There is no physical or logical limit to the ways that a Sun Ray system can be configured. The following sections offer some typical examples.

Small Deployments

For smaller deployments, such as those with between five and 50 Sun Ray DTUs, the Sun Ray server uses a single 100BASE-T card to connect to a 100BASE-T switch. This switch, in turn, connects to the Sun Ray DTUs. With five or fewer DTUs, a wireless interconnect works acceptably at 10 Mbytes.

For example, in FIGURE 1-2 a Sun Enterprise™ server with a Sun card 10/100BASE-T card and a 24-port 10/100BASE-T switch can easily support 23 users performing standard desktop activities.

Medium to Large Deployments

For larger departments with groups consisting of hundreds or thousands of Sun Ray DTUs, the Sun Ray server uses a gigabit Ethernet card to connect to large 10/100BASE-T switches. Especially with the low-bandwidth enhancements to SRSS, there is no performance need to have more than one gigabit link from the server to the Sun Ray DTU's network.

A 100-user departmental system, for example, consisting of a Sun Enterprise server, one gigabit Ethernet card, and two large (48-port and 80-port) 10/100BASE-T switches delivers services to the 100 Sun Ray DTUs (see FIGURE 1-4).

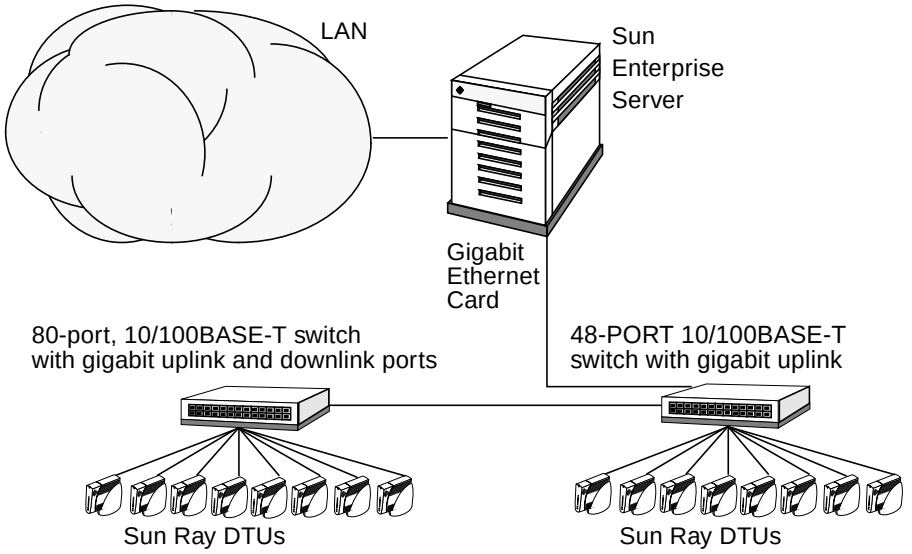


FIGURE 1-4 Small Deployment Scenario

Failover Group Scenario

Sun Ray servers can be bound together to create failover groups. A failover group, comprising two or more servers, provides users with a higher level of availability in case one servers become unavailable due to a network or system failure.

When a server in a failover group goes down, whether for maintenance, a power outage, or any other reason, each Sun Ray DTU connected to it reconnects to another server in the failover group. The DTU connects to a previously existing session for the current token, if there is one, on another server; if there is no existing session, the DTU connects to a server selected by the load balancing algorithm. This server presents a login screen to the user, who must log in again to create a new session. The session on the failed server is lost. Failover groups are discussed in Chapter 11 as well as in the *Sun Ray Server Software 3 Installation and Configuration Guide*.

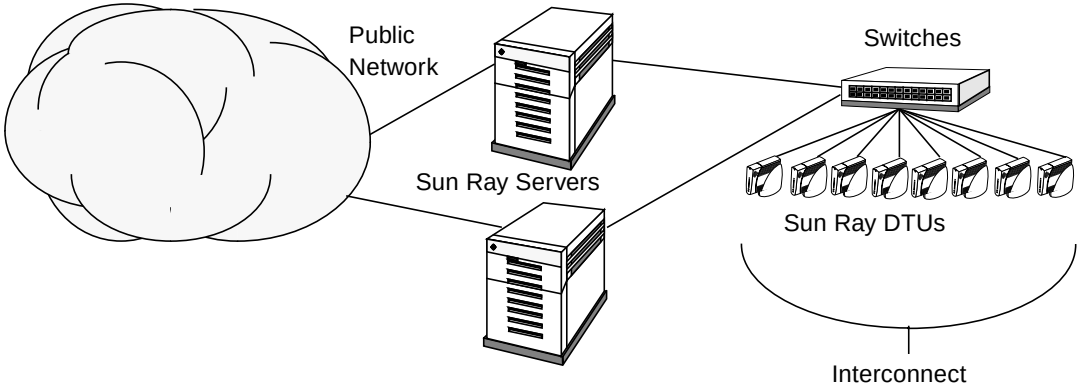


FIGURE 1-5 Simple Failover Group

Security Considerations

Using switched network gear for the last link to the DTUs makes it hard for a malicious PC user or network snooper at one of the network ports to obtain unauthorized information. Because switches send packets only to the proper output port, a snooper plugged into another port receives no unauthorized data. If the server and wiring closet are secure, the last step is switched, and the DTU is plugged directly into the wall jack, then it is very difficult to intercept communications between the server and the DTU. SRSS encryption features also help to protect sensitive data by providing the options to encode keyboard input and display traffic.

CHAPTER 2

Command-Line Interface

The Command-Line Interface (CLI) is the recommended interface for enabling assistive technologies.

This chapter contains the following information:

Supported Commands

Commands that can be executed from the command line are listed in TABLE 2-1, and a few of the most important commands are documented in this chapter. For further information on executing these commands, see the man page for the command in question.

To view any of the specific commands for the Sun Ray system, type:

```
% man -M  /opt/SUNWut/man command
```

or type:

```
% setenv MANPATH=/opt/SUNWut/man
% man command
```

TABLE 2-1 Supported Commands

Command	Definition
`utaction`	The `utaction` program provides a way to execute commands when a Sun Ray DTU session is connected or disconnected.
`utadm`	The `utadm` command manages the private network, shared network, and DHCP (Dynamic Host Configuration Protocol) configuration for the Sun Ray interconnect.
`utcapture`	The `utcapture` command connects to the Authentication Manager and monitors packets sent and packets dropped between the Sun Ray server and the Sun Ray DTUs.
`utcard`	The `utcard` command allows configuration of different types of smart cards in the Sun Ray administration database
`utconfig`	The `utconfig` command performs the initial configuration of the Sun Ray server and supporting administration framework software.
`utcrypto`	The `utcrypto` command is a utility for security configuration.
`utdesktop`	The `utdesktop` command allows the user to manage Sun Ray DTUs connected to the Sun Ray server that the command is run on.
`utdetach`	The `utdetach` command disconnects the current non-smart card mobile session or authenticated smart card session from its respective Sun Ray DTU. The session is not destroyed but put into a detached state. The session can be accessed if the same user token (user name) is presented to the Sun Ray server.
`utdssync`	The `utdssync` command converts the port number for the Sun Ray Data Store service to the new default port on servers in a failover group, then forces all servers in the group to restart Sun Ray services.
`uteject`	The `uteject` command is used to eject media from a removable storage media device.
`utfwadm`	The `utfwadm` command manages firmware versions on the Sun Ray DTUs.
`utfwload`	The `utfwload` command is used primarily to force the download of new firmware to a DTU running older firmware than its server.

TABLE 2-1 Supported Commands *(Continued)*

Command	Definition
`utfwsync`	The `utfwsync` command refreshes the firmware level on the Sun Ray DTUs to what is available on the Sun Ray servers in a failover group. It then forces all the Sun Ray DTUs within the group to restart.
`utgroupsig`	The `utgroupsig` command sets the failover group signature for a group of Sun Ray servers. The `utgroupsig` command also sets the Sun Data Store `rootpw` used by Sun Ray to a value based on the group signature. Although `utgroupsig` sets the `rootpw` in the `utdsd.conf` file, it does *not* set the admin password, which is a separate entity, in the Admin database.
`utgstatus`	The `utgstatus` command allows the user to view the failover status information for the local server or for the named server. The information that the command displays is specific to that server at the time the command is run.
`utinstall`	The `utinstall` utility installs, upgrades, and removes Sun Ray Server Software. All software required to support the Sun Ray server is installed, including the administration framework, and any patches required by the framework.
`utmhadm`	The `utmhadm` command provides a way to administer Sun Ray server multihead terminal groups. The information that `utmhadm` displays and that is editable is stored in the Sun Ray administration database.
`utmhconfig`	The `utmhconfig` tool allows an administrator to list, add, or delete multiheaded groups easily.
`utmhscreen`	The `utmhscreen` tool draws a window displaying the current session on each screen, with the current screen highlighted for easy identification. This tool is automatically launched for users during the X server startup process (session creation).
`utpolicy`	The `utpolicy` command sets and reports the policy configuration of the Sun Ray Authentication Manager, `utauthd`(1M). This command's `-i` and `-t` options were deprecated as of the 2.0 release. Please continue to use the `utpolicy` command for policy changes, but use the `utrestart` command instead of `utpolicy -i`, and use `utreader` instead of `utpolicy -t`.
`utpreserve`	The `utpreserve` command saves existing Sun Ray Server Software configuration data to the `/var/tmp/SUNWut.upgrade` directory.
`utpw`	The `utpw` command changes the Sun Ray administrator password (also known as the UT admin password) used by the Web-based and command-line administration applications.
`utquery`	The `utquery` command collects DHCP information from the Sun Ray DTUs.
`utrcmd`	The `utrcmd` program provides a way to run Sun Ray administrative commands remotely. The `utrcmd` program contacts the `in.utrcmdd` daemon on the remote *hostname* and executes the specified *command* with the specified arguments, *args* (if any).
`utreader`	The `utreader` command is used to add, remove, and configure token readers.
`utreplica`	The `utreplica` command configures the Sun Ray Data Store server to enable replication of administered data from a designated primary server to each secondary server in a failover group. The `-z` option is useful for updating the port number.
`utresadm`	The `utresadm` command allows an administrator to control the resolution and refresh rate of the video monitor signal (persistent monitor settings) produced by the Sun Ray unit.

TABLE 2-1 Supported Commands *(Continued)*

Command	Definition
`utresdef`	The `utresdef` command lists the monitor resolutions and refresh rates that can be applied to Sun Ray units through the `utresadm` command.
`utrestart`	The `utrestart` command is used to start Sun Ray services.
`utselect`	The `utselect` command presents the output of `utswitch -l` in a window and allows mouse-based selection of a Sun Ray server to which the Sun Ray DTU in use is reconnected.
`utsession`	The `utsession` command lists and manages Sun Ray sessions on the local Sun Ray server.
`utset`	Use `utset` to view and change Sun Ray DTU settings.
`utsettings`	The `utsettings` command opens a Sun Ray Settings dialog box that allows the user to view or change audio, visual, and tactile settings for the Sun Ray DTU.
`utswitch`	The `utswitch` command allows switching a Sun Ray DTU among Sun Ray servers in a failover group. It can also list the existing sessions for the current token.
`utsvc`	The `utsvc` script restarts the Sun Ray Server Software and, due to its location in `/etc/init.d`, is executed upon startup of the actual server. Use `utrestart` instead of `utsvc`.
`utusbadm`	The utusbadm command is used to enable or disable access to USB devices.
`utuser`	The `utuser` command allows the administrator to manage Sun Ray users registered on the Sun Ray server that this command is run on. It also provides information on the currently inserted token (smart card) for a specified DTU that is configured as a token reader.
`utwall`	The `utwall` utility sends a message or an audio file to users having an Xsun (X server unique to Sun Ray) process. The messages can be sent in email and displayed in a pop-up window.
`utwho`	The `utwho` script assembles information about display number, token, logged-in user, etc., in a compact format.
`utxconfig`	The `utxconfig` program provides X server configuration parameters for users of Sun Ray DTU sessions.

▼ To Stop Sun Ray Services

- **Type:**

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

▼ To Start Sun Ray Services

- **Type:**

```
# /opt/SUNWut/sbin/utrestart
```

This procedure starts Sun Ray services without clearing existing sessions.

Or

- **Type:**

```
# /opt/SUNWut/sbin/utrestart -c
```

This procedure starts Sun Ray services and clears existing sessions.

Session Redirection

In addition to automatic redirection after a user's token has been authenticated, whether via smart card token or direct login, the `utselect` graphical user interface (GUI) or the `utswitch` command can be used to redirect the session to a different server.

▼ To Redirect to a Different Server

- **From a shell window on the DTU, type:**

```
% /opt/SUNWut/bin/utselect
```

The selections in the window are sorted in order of the most current to least current active sessions for the token ID.

In FIGURE 2-1, the Server column lists the servers accessible from the DTU. The Session column reports the `DISPLAY` variable X session number on the server if one exists. In the Status column, Up indicates that the server is available. The first server in the list is highlighted by default. Select a server from the list or enter the name of a server in the Enter server: field. If a server without an existing session is selected, a new session is created on that server.

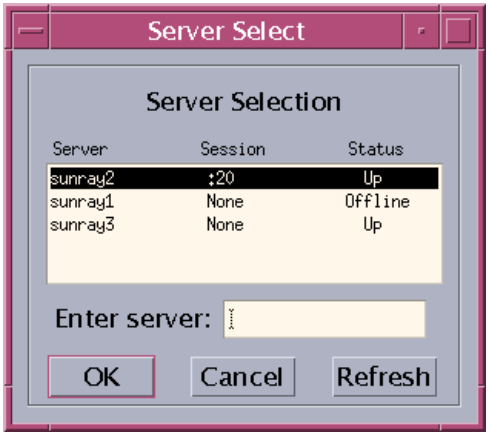


FIGURE 2-1 The Server Selection (`utselect`) GUI

The OK button commits the selection of the highlighted or manually entered server. The Cancel button dismisses the GUI without making any changes to the session. The Refresh button reloads the window with the most current information.

Note – If only one server in the failover group is up, it is displayed in the `utselect` GUI. However, if `selectAtLogin` is set to *true* in the `/etc/opt/SUNWut/auth.props` file, the GUI is not displayed because there appears to be only one server in the failover group.

▼ To Redirect a DTU Manually

- **From a shell window on the DTU, type:**

```
% /opt/SUNWut/bin/utswitch -h host [ -k token]
```

where *host* is the host name or IP address of the Sun Ray server to which the selected DTU is redirected, and *token* is the user's token ID.

▼ To List Available Hosts

- **From a shell window, type:**

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

Hosts available from the Sun Ray DTU are listed.

▼ To Select a Server with the Latest Session

- **In a shell window, type:**

```
% /opt/SUNWut/bin/utswitch -t
```

The DTU is redirected to the server with the latest session connect time.

Changing Policies

When a policy is set with `utpolicy`, the group policy is set automatically, so all that is needed at that point is to reset or restart services.

Tip – Use the `utrestart -c` command instead of rebooting the server.

TABLE 2-2 `utrestart` Commands

Command/Option	Result
`/opt/SUNWut/sbin/utrestart`	Use this option if a minor policy change was made, such as adding a dedicated token reader. With such minor changes, it is not necessary to terminate existing sessions.
`/opt/SUNWut/sbin/utrestart -c`	Use this option if a significant policy change has been made, such as enabling or disabling access to mass storage devices. All existing sessions are terminated.

Enabling and Disabling USB Devices

All USB device access is enabled by default. To disable USB devices, the administrator must explicitly use the provided command line tool or GUI.

This configuration affects all servers in a group and all DTUs connected to that group. The devices' access can only be updated by a privileged administrator.

▼ To Enable All USB Devices

The following commands enable or disable access to USB devices. Before any change can take effect, you must restart Sun Ray services with a cold restart, which terminates all Sun Ray sessions.

- **Use the utusbadm command with the -e option:**

```
# /opt/SUNWut/sbin/utusbadm -e
```

▼ To Disable All USB Device Access

- **Use the `utusbadm` command with the `-d` option:**

```
# /opt/SUNWut/sbin/utusbadm -d
```

▼ To Perform a Cold Restart

- **Use the `utrestart` command with the `-c` option:**

```
# /opt/SUNWut/sbin/utrestart -c
```

▼ To Determine the Current State of Devices

To determine whether or not USB devices are currently enabled:

- **Use the `utusbadm` command:**

```
# /opt/SUNWut/sbin/utusbadm
```

This displays the ENABLED or DISABLED state of the devices.

Configuring Interfaces on the Sun Ray Interconnect Fabric

Use the `utadm` command to manage the Sun Ray interconnect fabric.

Note – If the IP addresses and DHCP configuration data are not set up properly when the interfaces are configured, then the failover feature will not work as expected. In particular, configuring the Sun Ray server's interconnect IP address as a duplicate of any other server's interconnect IP address may cause the Sun Ray Authentication Manager to generate "Out of Memory" errors.

Note – If you make manual changes to your DHCP configuration, you will have to make them again whenever you run `utadm` or `utfwadm`.

Tip – If you issue a `<CTRL>C` signal while performing `utadm` configuration, `utadm` may not function correctly the next time it is invoked. To correct this condition, type: **`dhtadm -R`**.

▼ To Add an Interface

- **Type:**

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

This command configures the network interface *interface_name* as a Sun Ray interconnect. Specify a subnet address or use the default address, which is selected from reserved private subnet numbers between 192.168.128.0 and 192.168.254.0.

Note – If you choose to specify your own subnet, make sure it is not already in use.

After an interconnect is selected, appropriate entries are made in the `hosts`, `networks`, and `netmasks` files. (These files are created if they do not exist.) The interface is activated.

Any valid network interface can be used. For example:

```
hme[0-9], qfe[0-3]
```

▼ To Delete an Interface

- **Type:**

```
# /opt/SUNWut/sbin/utadm -d interface_name
```

This command deletes the entries that were made in the `hosts`, `networks`, and `netmasks` files and deactivates the interface as a Sun Ray interconnect.

▼ To Print the Sun Ray Private Interconnect Configuration

- **Type:**

```
# /opt/SUNWut/sbin/utadm -p
```

For each interface, this command displays the hostname, network, netmask, and number of IP addresses assigned to Sun Ray units by DHCP.

▼ To Add a LAN Subnet

- **Type:**

```
# /opt/SUNWut/sbin/utadm -A subnet_number
```

▼ To Delete a LAN Subnet

- **Type:**

```
# /opt/SUNWut/sbin/utadm -D subnet_number
```

▼ To Print Public LAN Subnets

- **Type:**

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

▼ To Remove All Interfaces and Subnets

Use the `utadm -r` command to prepare for removal of the Sun Ray Server Software.

- **Type:**

```
# /opt/SUNWut/sbin/utadm -r
```

This command removes all of the entries and structures relating to all of the Sun Ray interfaces and subnets.

Managing Firmware Versions

Use the `utfwadm` command to keep the firmware version in the PROM on Sun Ray DTUs synchronized with that on the server.

Note – If the DHCP *version* variable is defined, then when a new DTU is plugged in, its firmware is changed to the firmware version on the server.

Note – If you make manual changes to your DHCP configuration, you will have to make them again whenever you run `utadm` or `utfwadm`.

▼ To Update All the DTUs on an Interface

- **Type:**

```
# /opt/SUNWut/sbin/utfwadm -A -a -n interface
```

Tip – To force a firmware upgrade, power-cycle the DTUs.

▼ To Update a DTU Using the Ethernet (MAC) Address

- **Type:**

```
# /opt/SUNWut/sbin/utfwadm -A -e MAC_address -n interface
```

Restarting the Sun Ray Data Store

If you restart the Sun Ray Data Store daemon (`utdsd`), you must also restart the Sun Ray Authentication Manager. The Sun Ray Data Store (SRDS) daemon may need to be restarted if you change one of its configuration parameters. The following procedure shows the correct order of the steps to take if you need to restart SRDS.

▼ To Restart Sun Ray Data Store

1. **Stop the Sun Ray services:**

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

2. **Stop the Sun Ray Data Store daemon:**

```
# /etc/init.d/utds stop
```

3. **Restart the Sun Ray services:**

```
# /opt/SUNWut/sbin/utrestart
```

Smart Card Configuration Files

Tip – Use the Administration Tool or the `utcard` command to add additional smart card vendor configuration files.

Smart card configuration files are available from a variety of sources, including Sun. For more ample information on smart cards, see the latest version of the *Solaris Smart Card Administration Guide*.

▼ To Load a Configuration File Into the Directory

- **Copy the vendor configuration file containing the vendor tags to the following location:**

```
# cp vendor.cfg /etc/opt/SUNWut/smartcard
```

The additional vendor cards are displayed under the Available column in the Add page in the Administration Tool.

Configuring and Using Token Readers

Some manufacturers print the smart card ID on the card itself, but many do not. Since all the administrative functions refer to this token ID, Sun Ray Server Software provides a way to designate one or more specific DTUs as dedicated token readers. Site administrators can use these dedicated DTUs to administer Sun Ray users. When you enable an authentication policy with registered users, be sure to specify smart card IDs.

In the example configuration in FIGURE 2-2, the second DTU acts as a token reader.

Note – The token reader is not used for normal Sun Ray services, so it does not need a keyboard, mouse, or monitor.

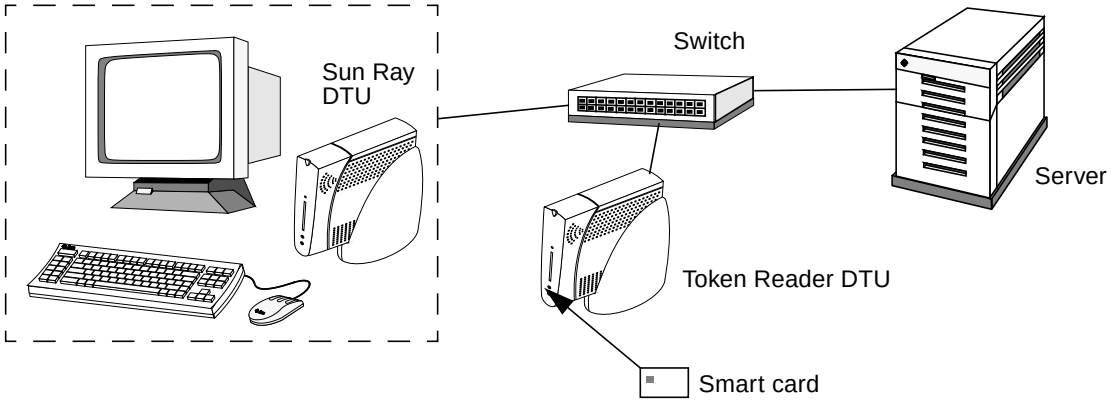


FIGURE 2-2 Using a Token Reader to Register Smart Cards

▼ To Configure a Token Reader

The `utreader` command specifies a DTU for registering smart cards. When a DTU is configured as a token reader, inserting or removing a smart card does not cause session mobility to occur; instead, any session connected to the DTU remains connected to that DTU over a card movement event.

Token reader mode is useful when you want to determine the raw token ID of a smart card.For example, to configure the DTU with MAC address 0800204c121c as a token reader, issue the following `utreader` command:

```
# /opt/SUNWut/sbin/utreader -a 0800204c121c
```

To re-enable the DTU with MAC address 0800204c121c to recognize card movement events and perform session mobility based on the smart card inserted into the DTU:

```
# /opt/SUNWut/sbin/utreader -d 0800204c121c
```

To unconfigure all token readers on this server:

```
# /opt/SUNWut/sbin/utreader -c
```

▼ To Get a Token ID From a Token Reader

- **Type the following command:**

```
# /opt/SUNWut/sbin/utuser -r Token Reader
```

where *Token Reader* is the MAC address of the DTU containing the token (smart card) whose ID you want to read. Insert the token into the DTU and run the utuser command. This command queries the DTU for the token's ID and, if successful, displays it. For example:

```
# /opt/SUNWut/sbin/utuser -r 08002086e18f
Insert token into token reader '08002086e18f' and press return.
Read token ID 'mondex.9998007668077709'
```

Using the `utcapture` Tool

The `utcapture` tool connects to the Authentication Manager and collects data about the packets sent and packets dropped between the Sun Ray server and the DTU. The data in TABLE 2-3 is then displayed on the screen in the following format:

TABLE 2-3 Data Elements Displayed

Data Element	Description
`TERMINALID`	The MAC address of the DTU
`TIMESTAMP`	The time the loss occurred in year-month-day-hour-minute-second format. Example: 20021229112512
`TOTAL PACKET`	Total number of packets sent from server to DTU
`TOTAL LOSS`	Total number of packets reported as lost by DTU
`BYTES SENT`	Total number of bytes sent from server to DTU
`PERCENT LOSS`	Percentage of packets lost between the current and previous polling interval
`LATENCY`	Time in milliseconds for a round trip from DTU to server.

Tip – If Sun Ray DTU traffic loss is more than .1%, allocate higher priority to the VLAN that carries Sun Ray DTU traffic. For more information on how to change the priority, please refer to the manufacturer's documentation for your switch.

The following `utcapture` options are supported:

TABLE 2-4 `utcapture` Options

Option	Definition
`-h`	Help for using the command.
`-r`	Dump output to `stdout` in raw format. By default, data is dumped when there is a packet loss. With this option, the data is always dumped to `stdout`
`-s server`	Name of server on which the Authentication Manager is running. By default, it is the same host that is running `utcapture`.
`-i filename`	Process raw data from a file specified by filename and dump to `stdout` only the data for those DTUs that had packet loss.
desktopID	Collects the data for the specified DTUs only. DTUs are specified on the command line by their desktop IDs separated by a space. By default, data for all currently active desktops is collected.

▼ To Start `utcapture`

From a command line, enter one of the following commands

```
% /opt/SUNWut/sbin/utcapture -h
```

This command lists the help commands for the `utcapture` tool

```
% /opt/SUNWut/sbin/utcapture
```

This command captures data every 15 seconds from the Authentication Manager running on the local host and then writes it to `stdout` if there is any change in packet loss for a DTU

```
% /opt/SUNWut/sbin/utcapture -r > raw.out
```

This command captures data every 15 seconds from the Authentication Manager that is running on the local host and then writes it to `stdout.`

```
% /opt/SUNWut/sbin/utcapture -s sunray_server5118.eng \
080020a893cb 080020b34231
```

This command captures data every 15 seconds from the Authentication Manager running on `server5118.eng` and then writes the output to `stdout` if there is any change in packet loss for the DTU with ID `080020a893cb` or `080020b34231`.

```
% /opt/SUNWut/sbin/utcapture -i raw-out.txt
```

This command processes the raw data from the input file `raw-out.txt` and then writes to `stdout` only the data for those DTUs that had packet loss.

CHAPTER 3

Administration Tool

The Sun Ray Administration Tool (Admin GUI) enables administration of Sun Ray users and DTUs; however, the Command-Line Interface (CLI), documented in Chapter 2, is the recommended interface for enabling assistive technologies.

This chapter is divided into the following sections:

Note – This chapter describes a standalone server. Servers in failover groups are discussed in Chapter 11.

Administration Data

Sun Ray administration data comes from two sources:

- An internal database

  The internal database keeps persistent administration data and grants read access to all internal database clients; however, it allows changes only by those internal database clients that connect as the privileged `utadmin` user.

- The Authentication Manager

  The authentication manager is queried as needed for dynamic data.

Tip – Although Sun Ray administration data is accessible through standard database interfaces and applications, to avoid operational errors, do not modify data except with the Administration Tool.

Logging In

The Administration Tool allows you to administer Sun Ray users and DTUs from a web browser.

▼ To Log Into the Administration Tool

1. **Log in to your Sun Ray server's console or any DTU attached to it.**
2. **Start a browser.**
3. **Type the following URL:**

```
http://hostname:1660
```

Tip – If you chose a different port number when you configured the Sun Ray supporting software, substitute that number for "1660" in the URL above.

If you get a message denying access, make sure that:

- You are running a browser on the Sun Ray server or one of its DTUs.
- The browser is not using a different machine as an HTTP proxy server (to proxy the connection to the HTTP server (web server).

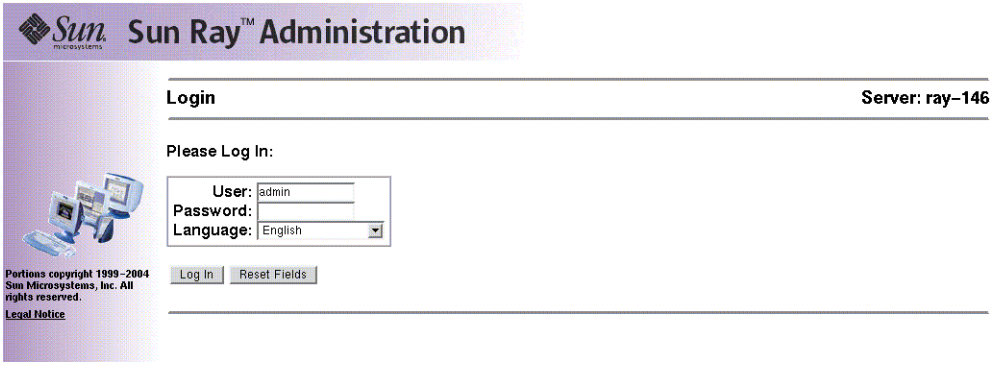


FIGURE 3-1 Login Window

4. **Enter the administrator user name `admin` and the administration password you specified when you configured the Sun Ray Server Software.**

Note – Only `admin` can be entered in the User text box.

5. **Click the Log In button.**

The Summary Status window is displayed.

Use the navigation bar on the left to navigate through the Administration Tool.

Note – If the session is inactive for 30 minutes, you must log in again.

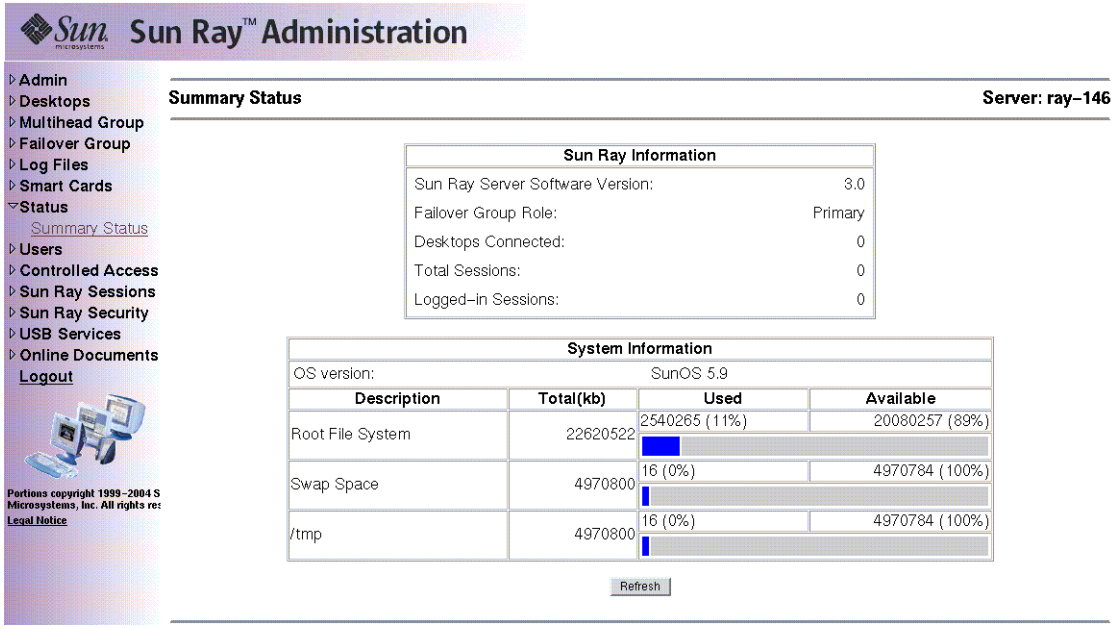


FIGURE 3-2 Summary Status Window

▼ To Change the Administrator's Password

The password allows you to use the Administration Tool to access and change Sun Ray administration data.

1. **In the navigation menu, click the arrow to the left of Admin to view the options.**
2. **Click the Password link.**

   The Change Admin Password window is displayed.

Note – In failover groups, all servers must use the same password for the admin account.

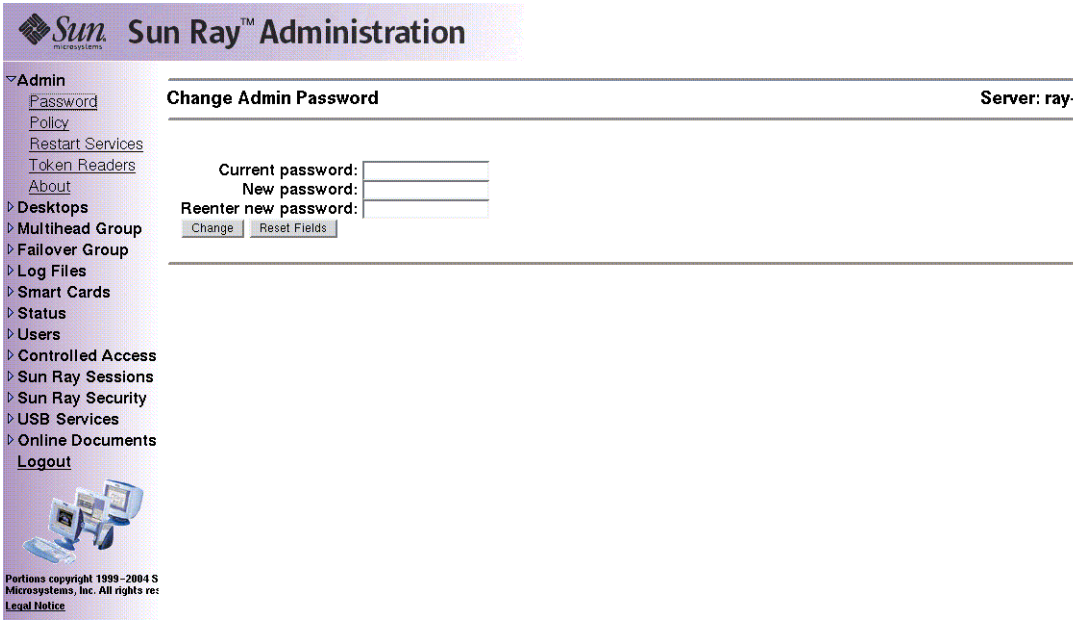


FIGURE 3-3 Change Admin Password Window

3. **Enter your current password.**
4. **Enter a new password.**
5. **Re-enter the new password.**

Tip – If you make a mistake, click the Reset Fields button to clear the fields and start again.

---

6. **Click the Change button.**

   The new password takes effect and the internal database hierarchy is updated.

Changing Policies

Set the same policies on all the Sun Ray servers in a given failover group. If all the servers are configured to use the same policies and a failover occurs, all policies remain consistent.

Changes to local policies affect only the current Sun Ray server; changes to group policies affect all Sun Ray servers in the same group.

▼ To Change the Policy

1. **Select the arrow to the left of Admin in the navigation bar to expand the menu.**
2. **Click the Policy link.**

   The Change Policy window is displayed.

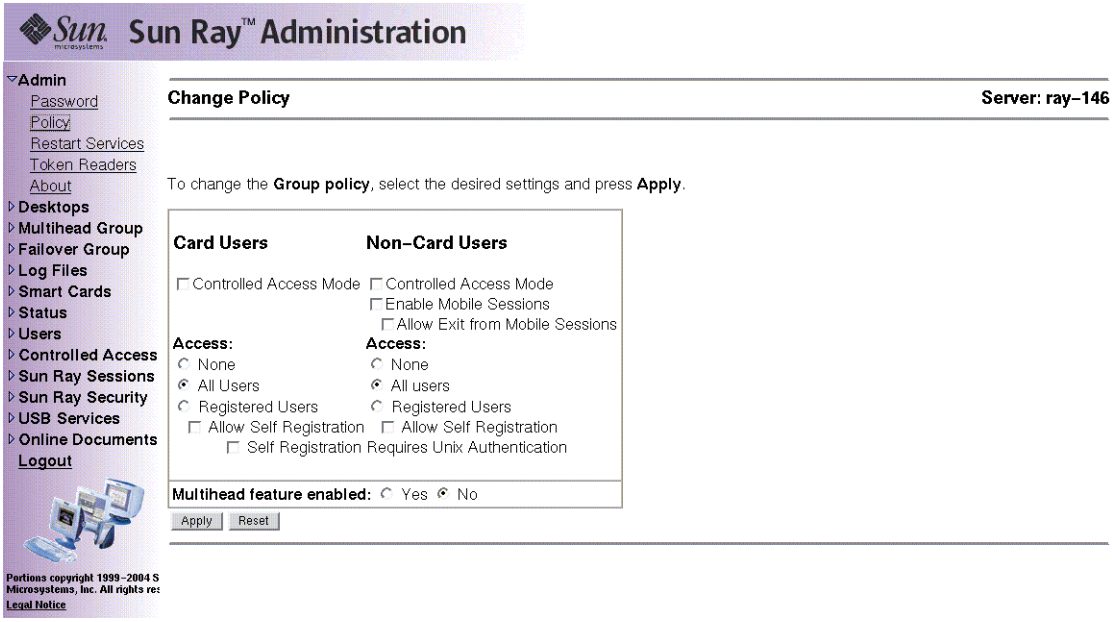


FIGURE 3-4 Change Policy Window

3. **Under Card Users, select either None, All Users, or Registered Users.**
4. **Under Non-Card Users, select either None, All Users, or Registered Users.**

   Registered users are those you have registered. Allow Self Registration enables users to self-register when they insert their cards. All Users encompasses all types of users.
5. **Select Self Registration Requires Authentication, if applicable.**
6. **To enable multihead, click the Yes radio button next to Multihead feature enabled.**
7. **Notify users to log off to avoid losing their sessions.**

8. **Restart services.**

   When changing the Mulihead feature, you have the *option* of resetting Sun Ray services. All other changes *require* you to restart Sun Ray services.

Restarting Sun Ray Services

▼ To Preserve Sessions Upon Restart

1. **From the expanded navigation menu under Admin, click the Restart Services link.**

   The Sun Ray Services window is displayed.

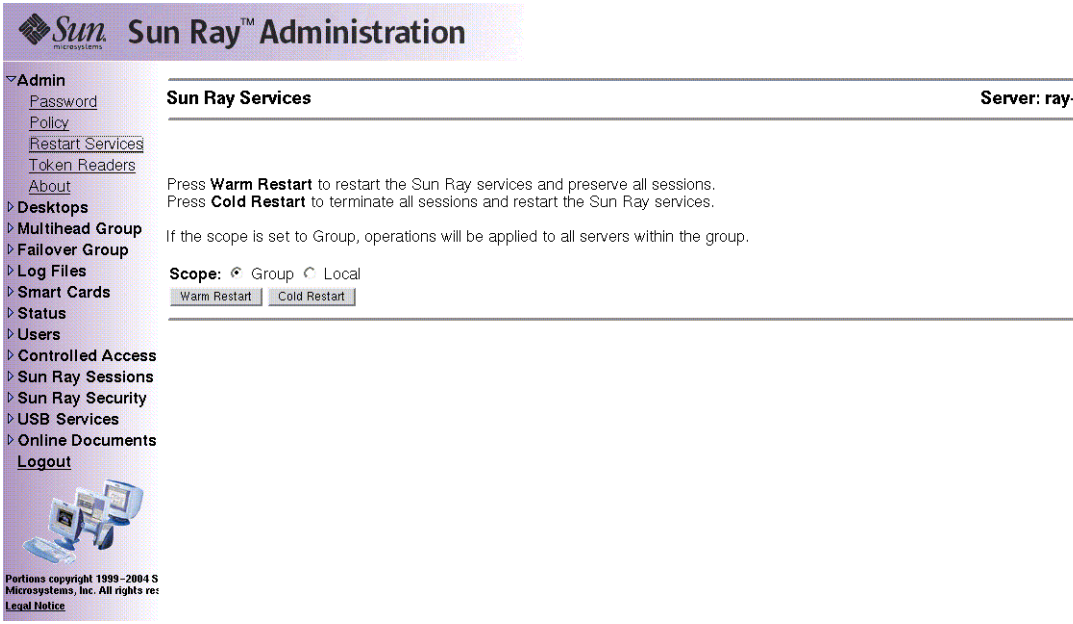


FIGURE 3-5 Sun Ray Services Window

2. **Click Warm Restart.**

   Sun Ray services are reset, and the sessions are preserved.

Note – Warm Restart provides the same functionality as the Reset button in earlier versions of Sun Ray Server Software.

▼ To Terminate Sessions Upon Restart

- **Click Cold Restart.**

  All sessions are immediately terminated, and Sun Ray services are restarted.

Note – In a failover group, you must initiate these functions from the primary server in the group.

Token Readers

You can use the Administration Tool to create token readers and locate Sun Ray DTUs designated as token readers. Sun Ray DTUs configured as token readers do not support hot desking. They display the token reader icon instead of a login dialog box.

Creating a Token Reader

A token reader is a Sun Ray DTU that reads a smart card and returns the card's ID. A valid ID allows you to add a user.

▼ To Create a Token Reader

1. **Click the arrow in front of Desktops to expand the navigation menu.**
2. **Click the View Current link.**

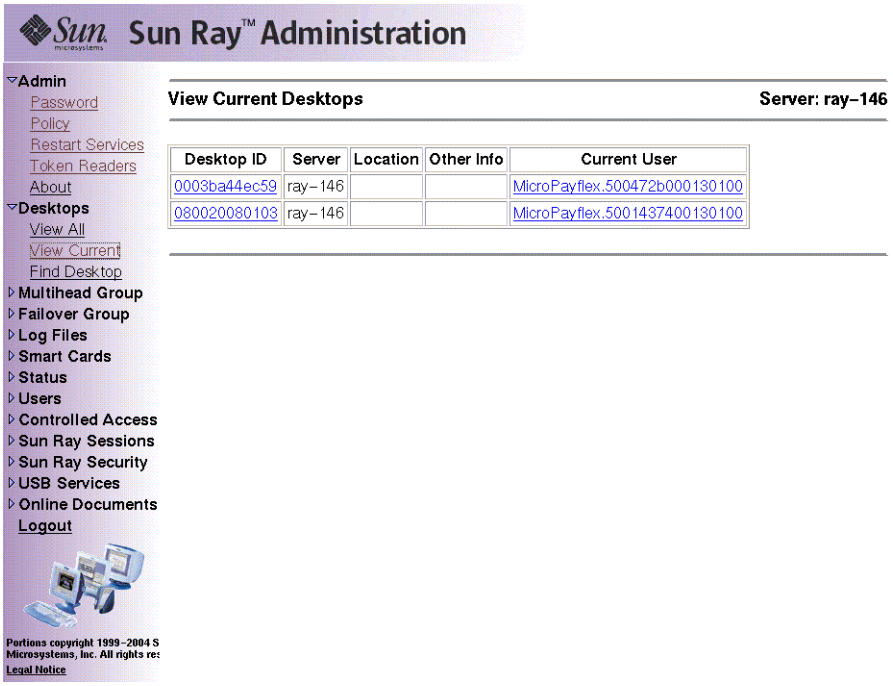


FIGURE 3-6 View Current Desktops Window

3. **Select the desktop of the DTU you want to use as a token reader.**

   The Current Properties window is displayed.

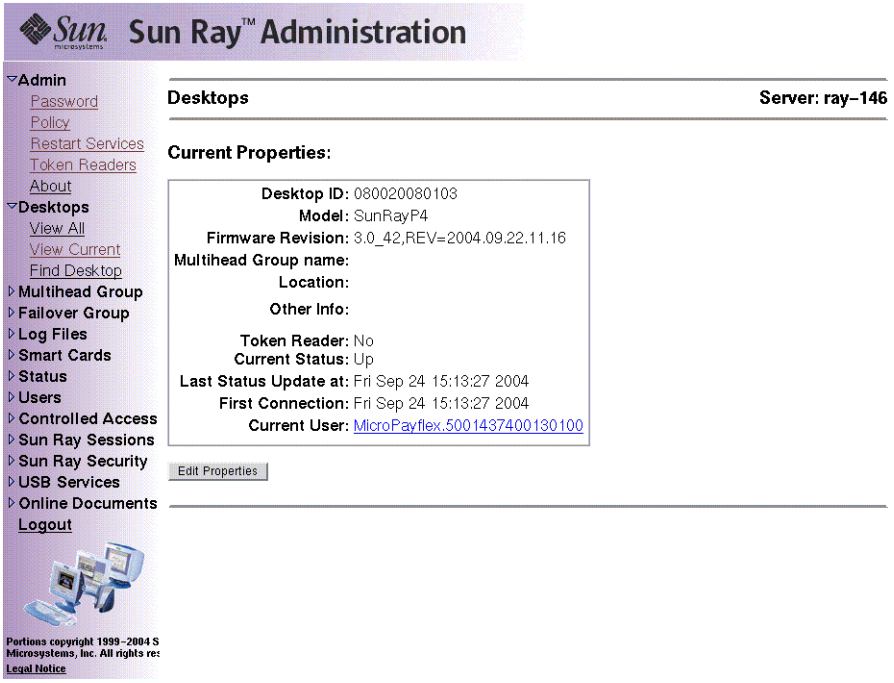


FIGURE 3-7 Current Properties Window

4. **Click the Edit Properties button.**

   The Edit Desktop Properties window is displayed.

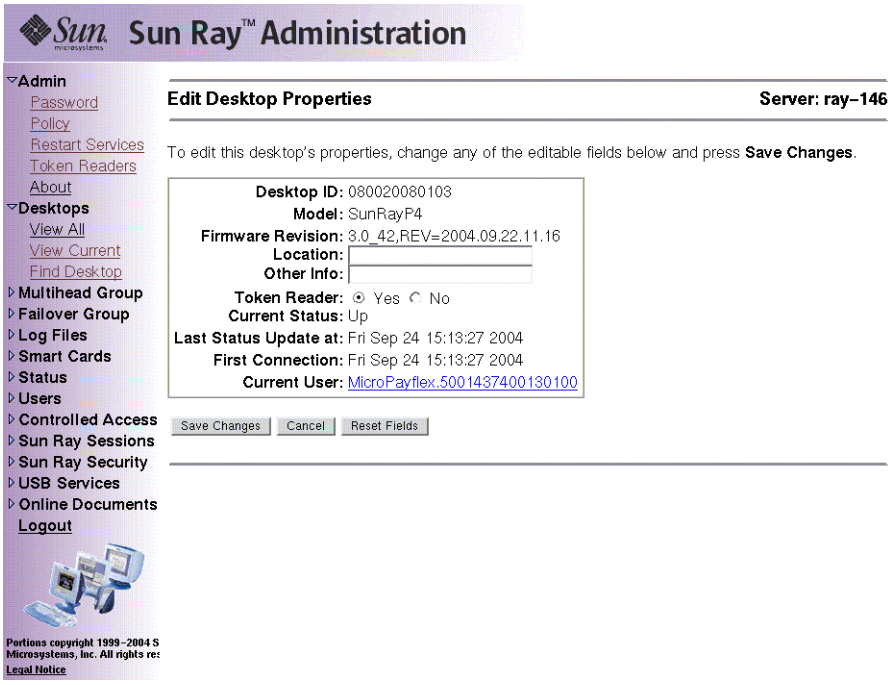


FIGURE 3-8 Edit Desktop Properties Window

5. **Next to Token Reader, select the Yes radio button.**
6. **Click the Save Changes button.**

   The DTU you have selected is now set up to read smart cards.
7. **Restart Sun Ray services.**

   The DTU is now a token reader.

▼ To Locate Token Readers

- **From the expanded navigation menu under Admin, click the Token Readers link.**

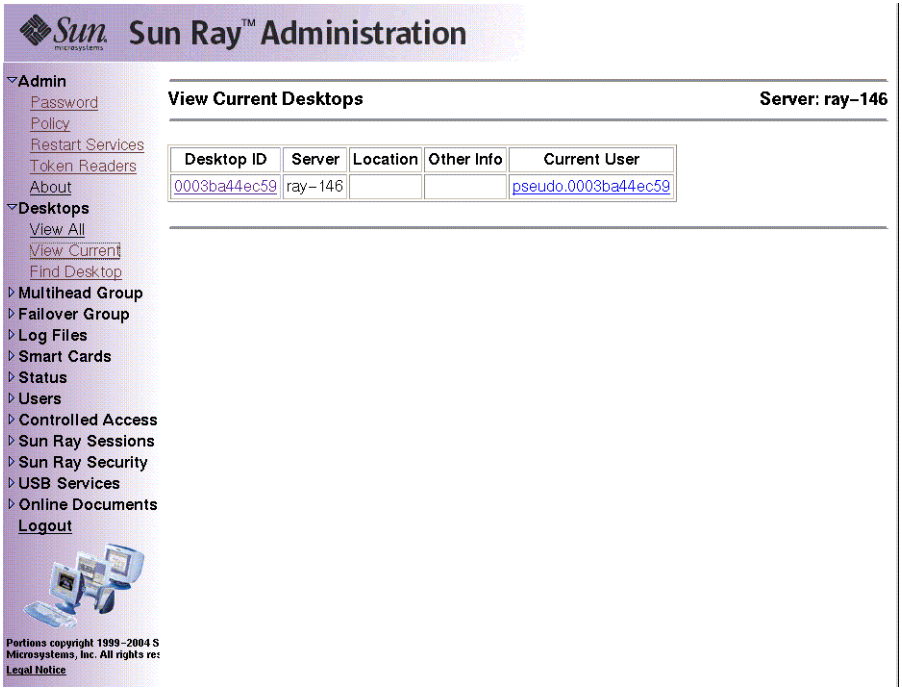


FIGURE 3-9 Token Readers Window

▼ To Get Information on a Token Reader

- **Click the Desktop ID link in the Token Readers window.**

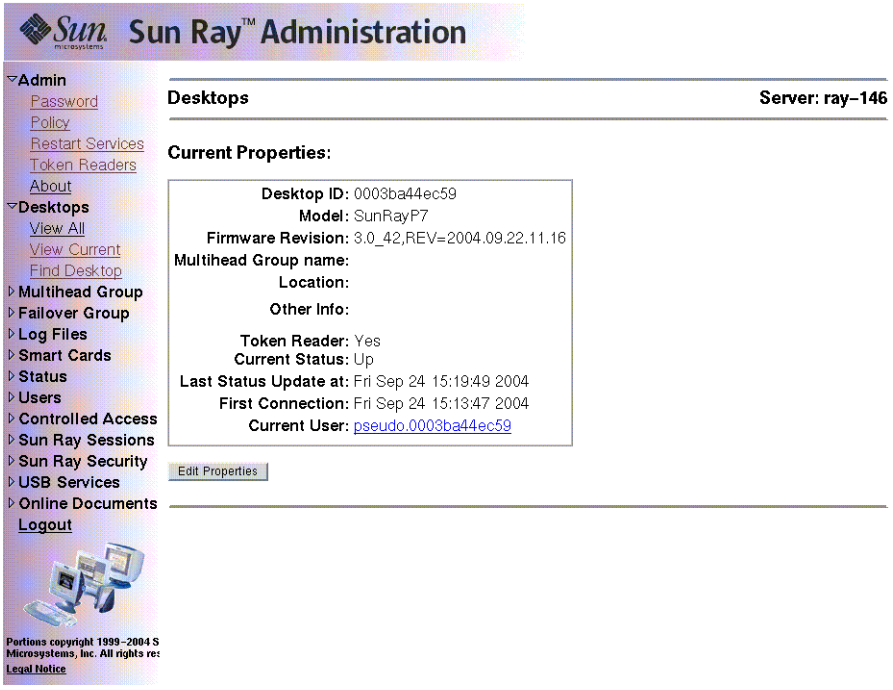


FIGURE 3-10 Current Properties of a Token Reader

Managing Desktops

▼ To List All Desktops

1. **In the navigation menu, click the directional arrow to the left of Desktops to view the options.**
2. **To view all desktops, click View All.**

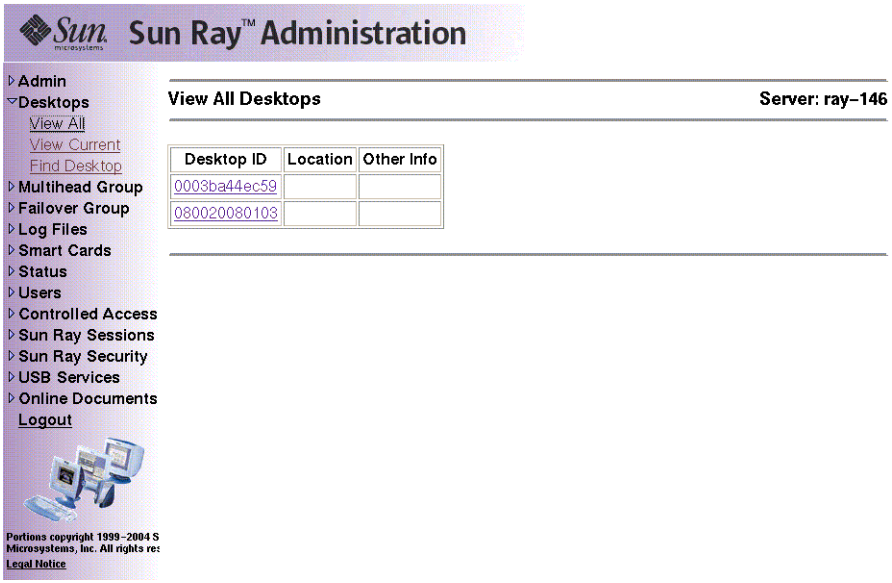


FIGURE 3-11 View All Desktops Window

▼ To Display a Desktop's Current Properties

- **Click a Desktop ID link.**

  The Desktops Current Properties window is displayed (see FIGURE 3-7).

▼ To List Currently Connected Desktops

1. **In the navigation menu, click the directional arrow to the left of Desktops to view the options.**

2. **Click View Current.**

   The View Current Desktops window is displayed (see FIGURE 3-6). This window lists the desktops that are currently connected to this Sun Ray server and communicating with the Authentication Manager or with any other Sun Ray server in the same failover group.

▼ To View the Properties of the Current User

- **From either the View Current User window or the Desktops Current Properties window, click the link for Current User.**

  The Properties window for the Current User is displayed.

▼ To Search for Desktops

1. **In the navigation menu, click the directional arrow to the left of Desktops to view the options.**
2. **Click Find desktop.**

   The Find Desktop window is displayed.

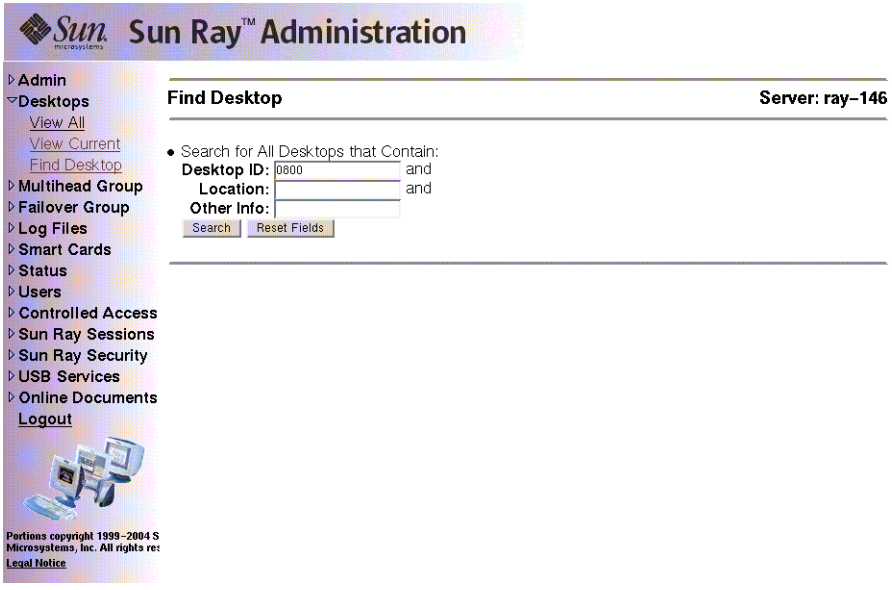


FIGURE 3-12 Find Desktop Window

3. **From the Find Desktop page, enter data into the Desktop ID, Location, and Other Info fields.**

4. **Click the Search button.**

   The Find Desktop window is redisplayed with all matches in the administration database.

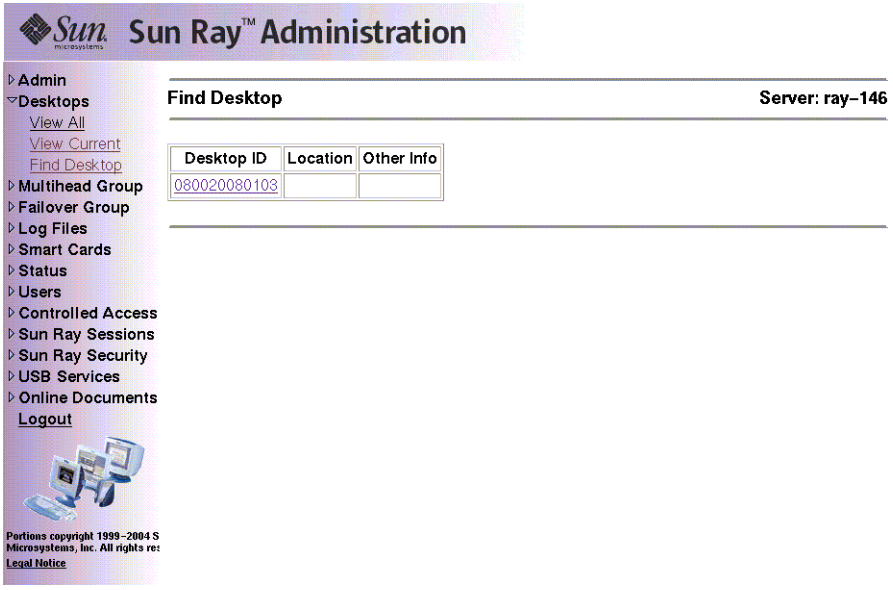


FIGURE 3-13 Find Desktop Search Results Window

▼ To Edit a Single Desktop's Properties

1. **To display the Desktop Properties page for the desktop you want to edit, click the Desktop ID.**

   The Desktops Current Properties window is displayed (see FIGURE 3-7).

2. **Click the Edit Properties button.**

   The Edit Desktop Properties window is displayed (see FIGURE 3-8).

3. **Change the data in the text boxes as appropriate.**

4. **Click the Save Changes button to save the changes to the administration database.**

Sun Ray DTU Settings

Sun Ray Settings is an interactive GUI that allows the user to view and change the settings for the Sun Ray DTU that the user is currently logged into.

The Sun Ray Settings GUI contacts the Session Manager to determine which DTU is currently being used and connects to that unit to get the current values. The GUI maintains a connection to the Session Manager so that the Session Manager can notify the GUI if the user moves to another DTU by removing the smart card and inserting it into another DTU.

▼ To Change the Sun Ray Settings

1. **Press the hot key (by default Shift-Props).**

   The Sun Ray Settings window is displayed.

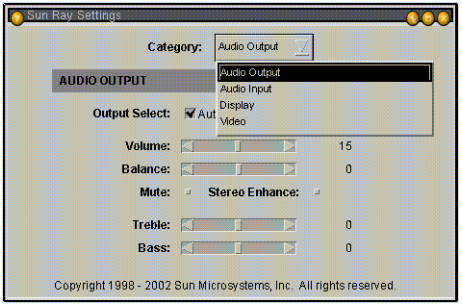


FIGURE 3-14 Settings Screen

2. **Use the Category pull-down menu to access Audio Output, Audio Input, Display, and Video settings.**

3. **To change a setting, move the appropriate scroll bar, checkbox, or pull-down menu.**

   The DTU is updated immediately.

   The only exception is the "Resolution/Refresh Rate" setting, which prompts the user with confirmation dialog boxes before and after the change is made on the DTU.

4. **Press the hot key to close the window.**

Note – Only one instance per session of Sun Ray Settings runs in hot key mode.

Managing Multihead Groups

The multihead feature allows users to control separate applications on multiple Sun Ray screens. Only a single keyboard and pointer device, attached to the primary DTU, are needed. The multihead feature also allows users to display and control a single application, such as a spreadsheet, on multiple screens.

System administrators create multihead groups so that users can access them. A multihead group, consisting of two or more DTUs controlled by one keyboard and mouse, can consist of Sun Ray 1, Sun Ray 100, Sun Ray 150, and Sun Ray 160 DTUs.

For further information on multihead implementations, see Chapter 9.

▼ To View All Multihead Groups

1. **From the navigation menu, select the arrow to the left of Multihead Group to expand the menu.**
2. **Click the View All link.**

   The Multihead Groups window is displayed.

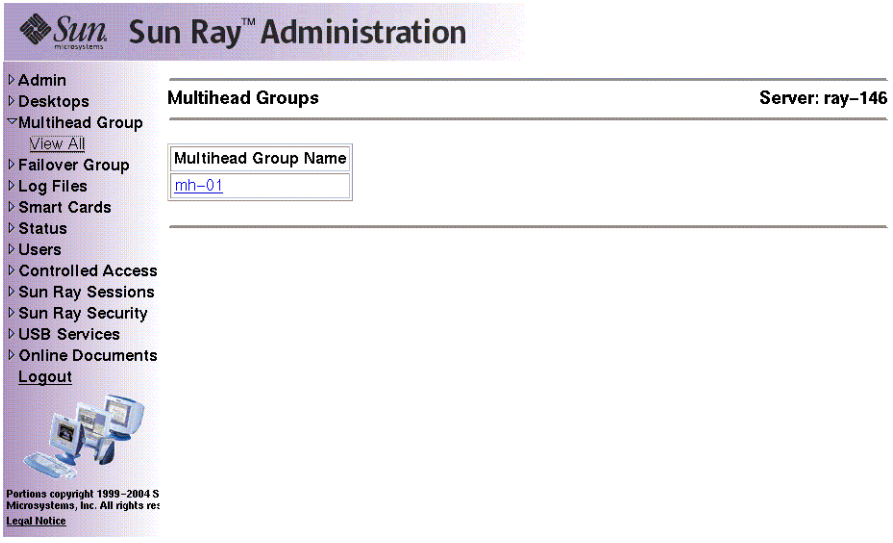


FIGURE 3-15 The Multihead Groups Window

3. **To view the properties for this group, click the Multihead Group Name link.**
   The Multihead Group Properties window is displayed.

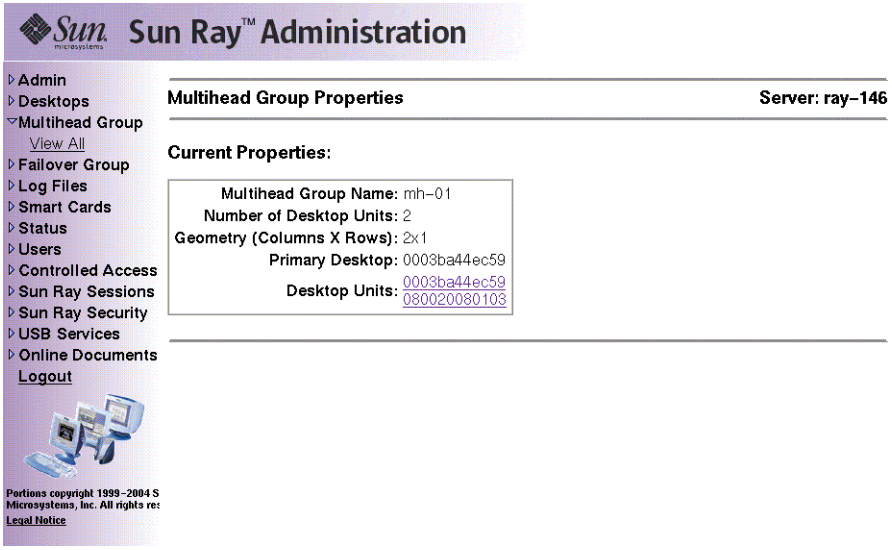


FIGURE 3-16 The Multihead Group Properties Window

4. **To display the Desktops Current Properties for the DTUs that are part of this group, click the Desktop Units links.**

   The Desktops Current Properties window for the link selected is displayed.

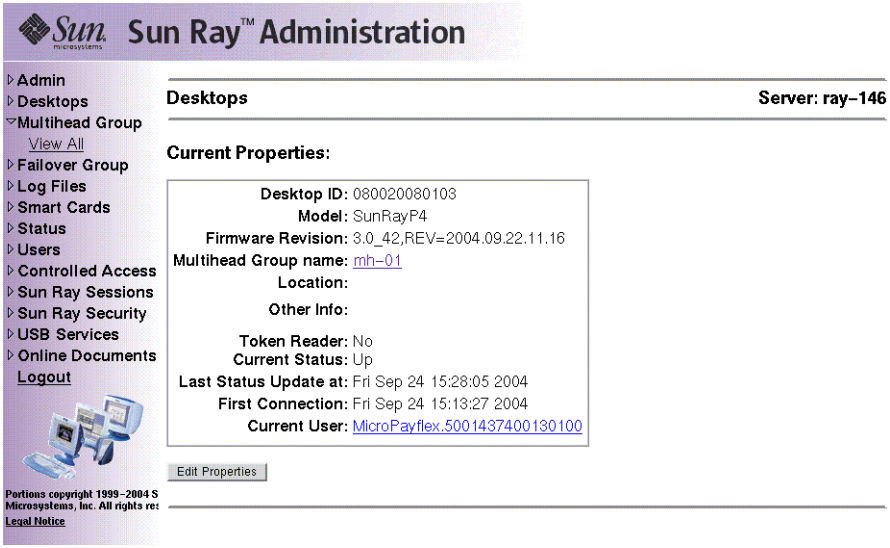


FIGURE 3-17 Desktops Current Properties Window

The Multihead Group name is displayed as a property of this desktop.

Managing USB Services

All USB device access is enabled by default. To disable USB devices, the administrator must explicitly use the GUI, as shown in this section, or the `utusbadm` command, which is described under “Enabling and Disabling USB Devices” on page 22.

Use the following procedure to change the state of USB device access:

▼ To Enable or Disable USB Device Access

1. **From the navigation menu, select the arrow to the left of the USB Services in the navigation bar to expand the menu.**
2. **Click on USB Services in the menu to display the USB Service window.**

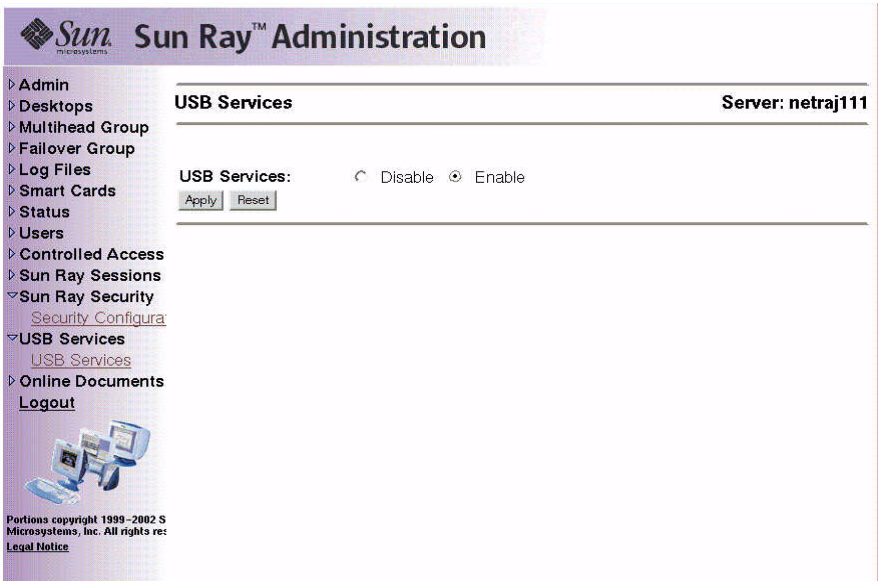


FIGURE 3-18 USB Services Window

3. **Toggle the Disable or Enable radio button.**
4. **Click Apply to make the relevant change.**

   SunRay services must be restarted before these changes can take effect.

Examining Log Files

Significant activity concerning files retrieved from the Sun Ray server is logged and saved. The server stores this information in text files. TABLE 3-1 describes the log files that are maintained.

TABLE 3-1 Log Files

Log File	Path	Description
Administration	`/var/opt/SUNWut/log/admin_log`	Lists operations performed during server administration. This log is updated daily. Archived files are stored on the system for up to one week and are annotated using numeric extensions (for example, from filename `admin_log.0` to `admin_log.5`).
Authentication	`/var/opt/SUNWut/log/auth_log`	Lists events logged from the Authentication Manager. The `auth_log` file is updated (up to a limit of 10) every time the server's authentication policy is changed or started. The archived authentication files are annotated using numeric extensions (for example, from `auth_log.0` to `auth_log.9`).
Automatic Mounting	`/var/opt/SUNWut/log/utmountd.log`	Lists mount messages for mass storage devices. The archived mountd files are annotated using numeric extensions (for example, from `utmountd.log.0` to `utmountd.log.9`).
Mass Storage Devices	`/var/opt/SUNWut/log/utstoraged.log`	Lists mass storage device events. The archived storage files are annotated using numeric extensions (for example, from `utstoraged.log.0` to `utstoraged.log.9`).
Messages	`/var/opt/SUNWut/log/messages`	Lists events from the server's DTUs, including details of registering, inserting, or removing smart cards. This file is updated daily. Archived files are stored on the server for one week annotated with numeric extensions (for example, from `messages.0` to `messages.5`).

▼ To View a Log File

1. **From the navigation menu, select the arrow to the left of Log Files to expand the menu.**
2. **Choose the Log link you want to inspect: Messages, Auth Log, Admin Log, Archived Logs, utmountd.log, or utstoraged.log.**

   The appropriate Log File window is displayed. Use the scroll bar to access data to the right and bottom of the window.

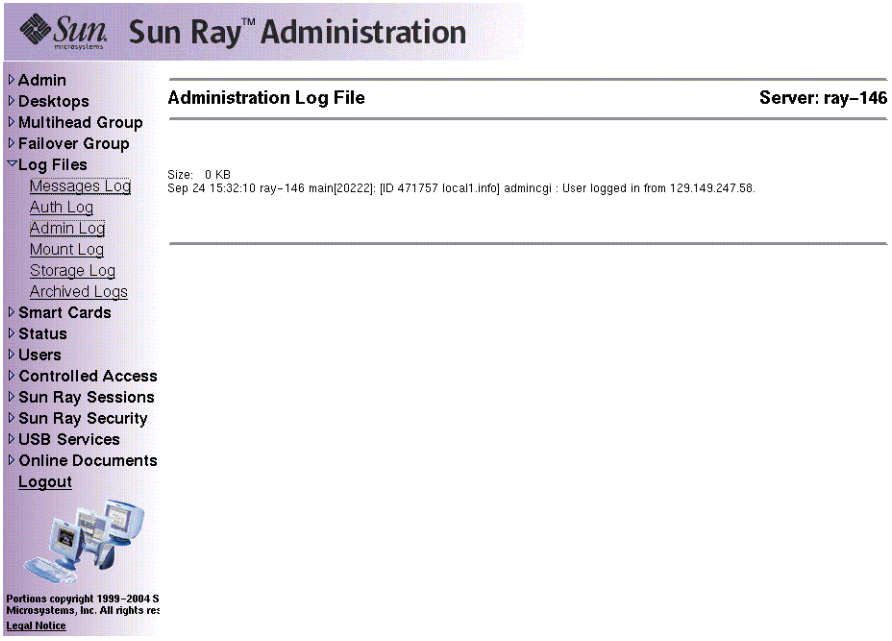


FIGURE 3-19 Administration Log File Window

Managing Smart Cards

The information provided about smart cards is extracted from vendor-supplied configuration files. These configuration files are located in the directory: `/etc/opt/SUNWut/smartcard`. Configuration files must be formatted correctly, and file names must end with a `.cfg` suffix; for example, `acme_card.cfg`.

For certain vendors, the smart card may require additional software to enable the Sun Ray Server Software to probe for it. If required, this optional software must be supplied as Java classes in a Jar file. This file must end with a `.jar` suffix and must have the same pre-suffix filename as the `.cfg` file that contains its configuration information.

▼ To View or List Configured Smart Cards

1. **From the navigation menu, select the arrow to the left of Smart Cards to extend the menu.**
2. **Click the View link.**

   The View Configured Smart Cards window is displayed. Smart cards are listed in probe order, i.e., the order in which they are inspected.

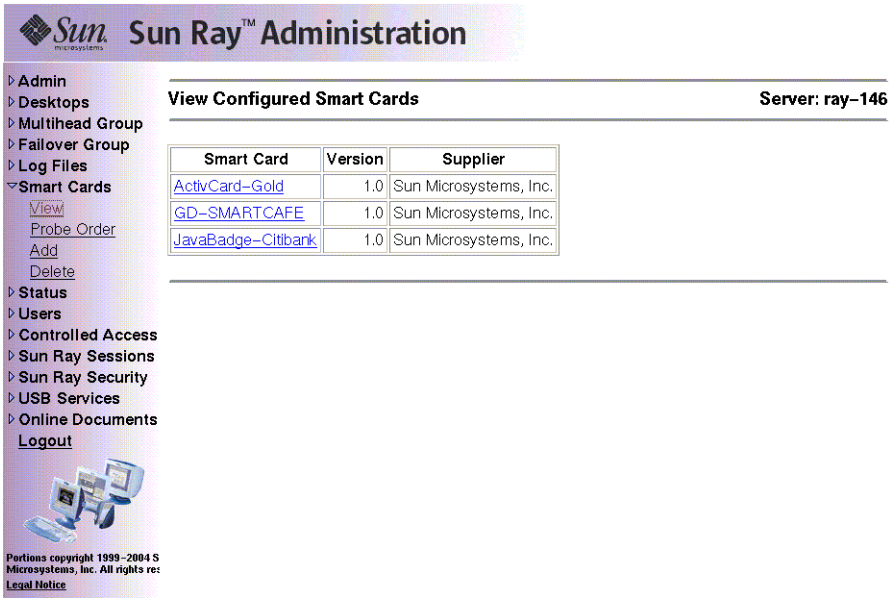


FIGURE 3-20 The View Configured Smart Cards Window

From this window an administrator can see the current list of smart cards as well as the supplier and version number for each card.

3. **From the View Configured Smart Cards window, select the link for the smart card**.
   The main properties for the selected smart card are displayed in FIGURE 3-21.

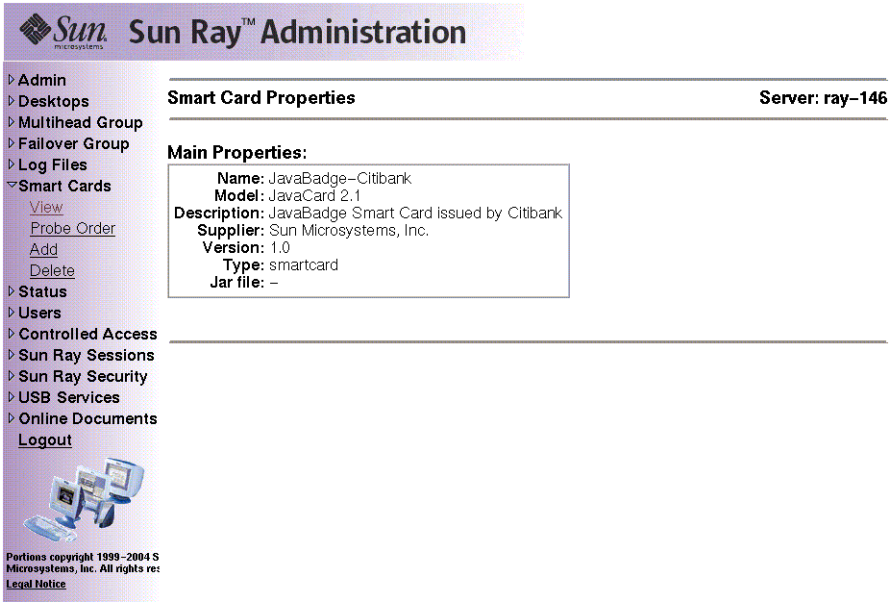


FIGURE 3-21 Smart Card Properties Window

▼ To View The Smart Card Probe Order

- **From the navigation menu under Smart Cards, click the Probe Order link.**

  The Smart Card Probe Order window is displayed.

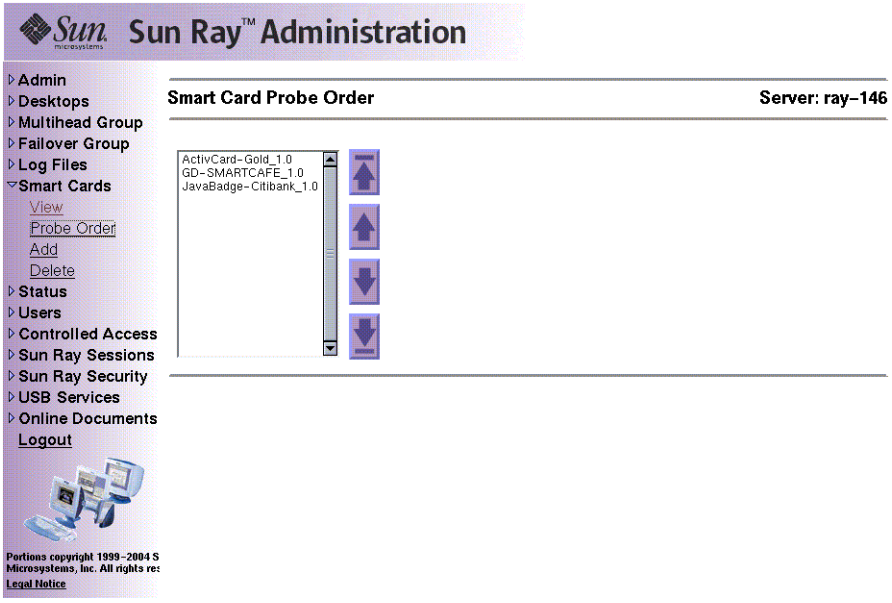


FIGURE 3-22 Smart Card Probe Order Window

Smart cards are probed in the order in which they appear in this list.

Tip – As you add more cards, you can change the order of the cards to move those used most often to the top of the list.

▼ To Change the Smart Card Probe Order

- **Select a smart card and press the appropriate up and down button.**

  Clicking on the first and last buttons (from top to bottom) moves the selected card to either the top or bottom of the list.

▼ To Add a Smart Card

1. **From the expanded navigation menu under Smart Cards click the Add link.**
   The Add Smart Cards to Probe List window is displayed.

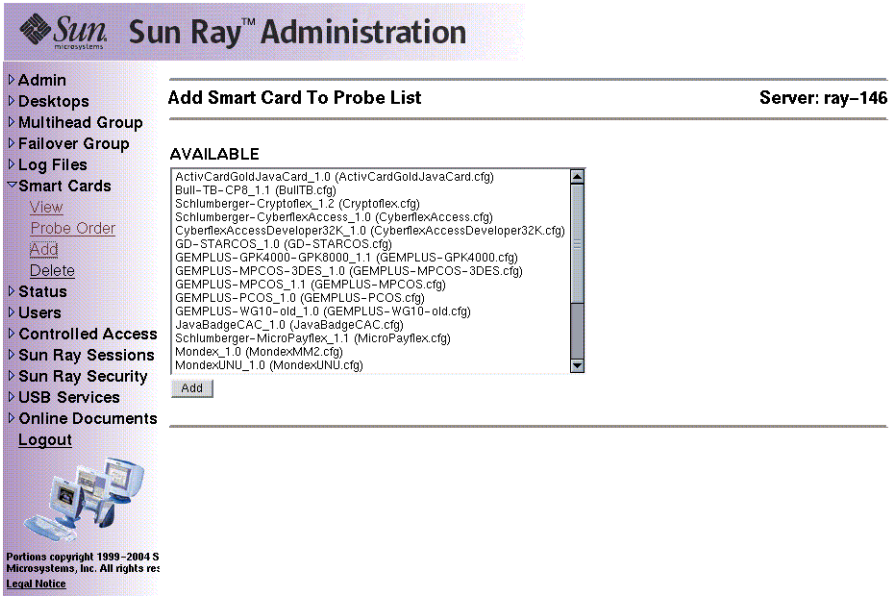


FIGURE 3-23 Add Smart Card to Probe List Window

2. **Select a smart card and click the Add button.**

▼ To Delete a Smart Card

1. **From the expanded navigation menu under Smart Cards, click the Delete link.**
   The Delete Smart Card From Probe List window is displayed.
2. **Select a smart card.**
3. **Click the Delete button.**

Sun Ray System Status

▼ To View the Sun Ray System Status

1. **Click the directional arrow to the left of Status to expand the navigation menu.**
2. **Click the Summary Status link.**
   The Summary Status window is displayed.

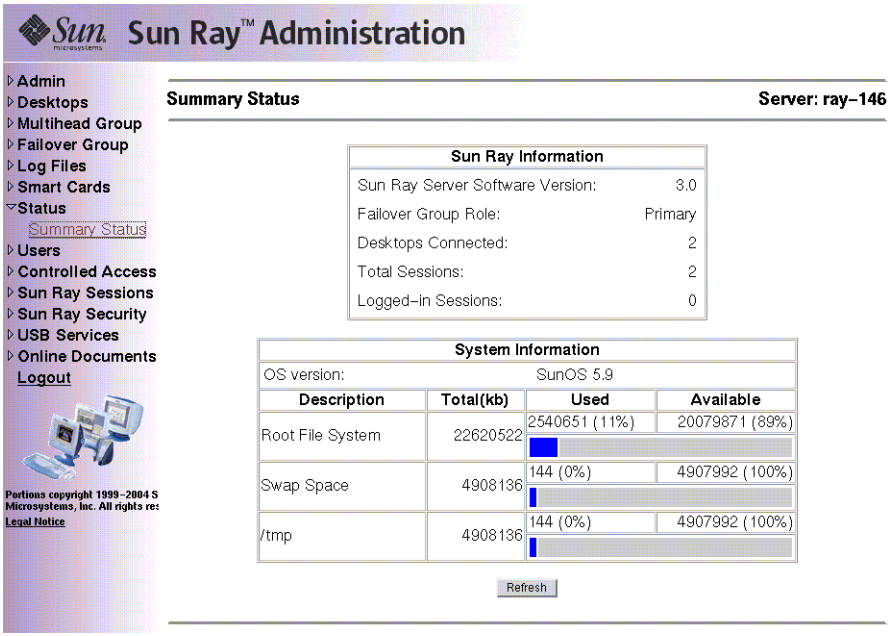


FIGURE 3-24 Summary Status Window

Administering Users

You can specify the following user fields in the Sun Ray administration database:

TABLE 3-2 Key User Fields

Field	Description

Token ID	User's unique token type and ID. For smart cards, this is a manufacturer type and the card's serial ID. For DTUs, this is the type "`pseudo`" and the DTU's Ethernet address. Examples:
	`mondex.9998007668077709`
	`pseudo.080020861234`

Server Name	Name of the Sun Ray server that the user is using.
Server Port	Sun Ray server's communication port. This field should generally be set to `7007`.
User Name	User's name.
Other Info	Any additional information you want to associate with the user (for example, an employee or department number). This field is optional.

▼ To View Users by ID

- **From the expanded Users navigation menu, click the View by ID link.**

  The View Users by ID window is displayed. The list of all the users in the administration database is sorted by the Token ID field. If a user has multiple tokens, they are listed separately.

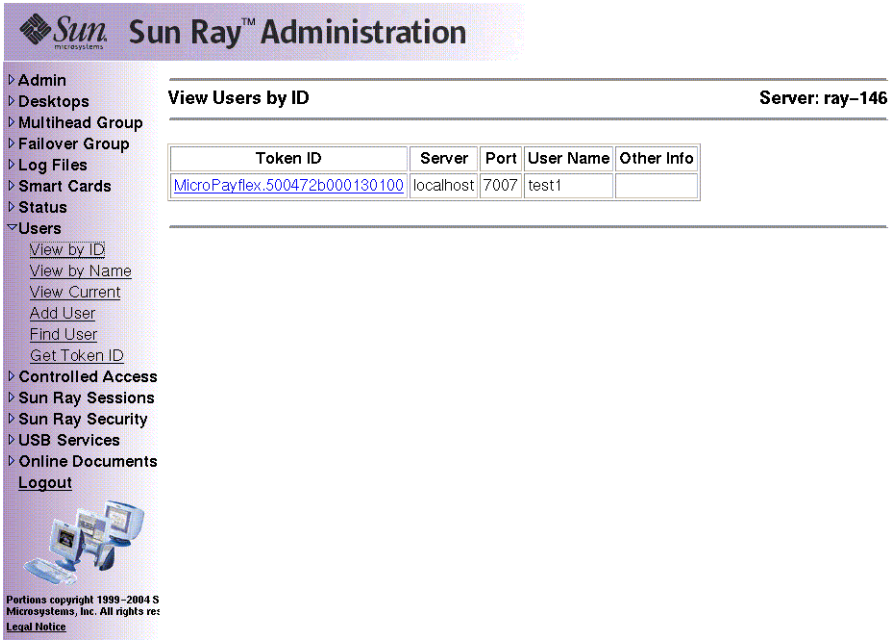


FIGURE 3-25 View Users by ID Window

▼ To View Users by Name

- **From the expanded Users navigation menu, click the View by Name link.**

  The View Users by Name window is displayed, listing all the users in the administration database sorted by the User Name field. If a user has multiple tokens, they are grouped together with the name.

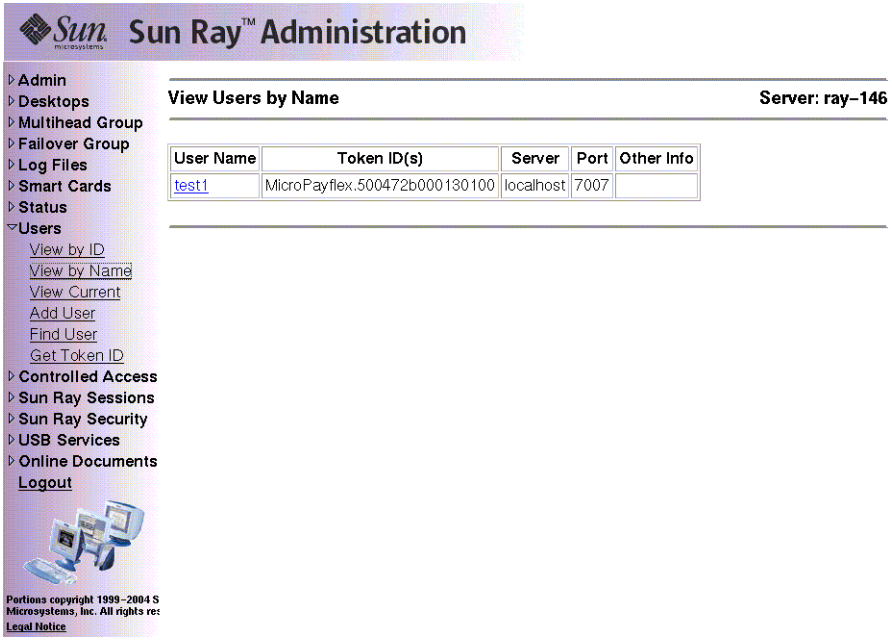


FIGURE 3-26 View Users by Name Window

▼ To Delete a User

Caution – This operation deletes the user and all associated tokens.

1. **From the View by Name window, click the User Name of the user you want to delete.**

   The Current Properties window displays information about the user, host, token, and allows the administrator to edit the user's properties, delete the user, and view the user's session.

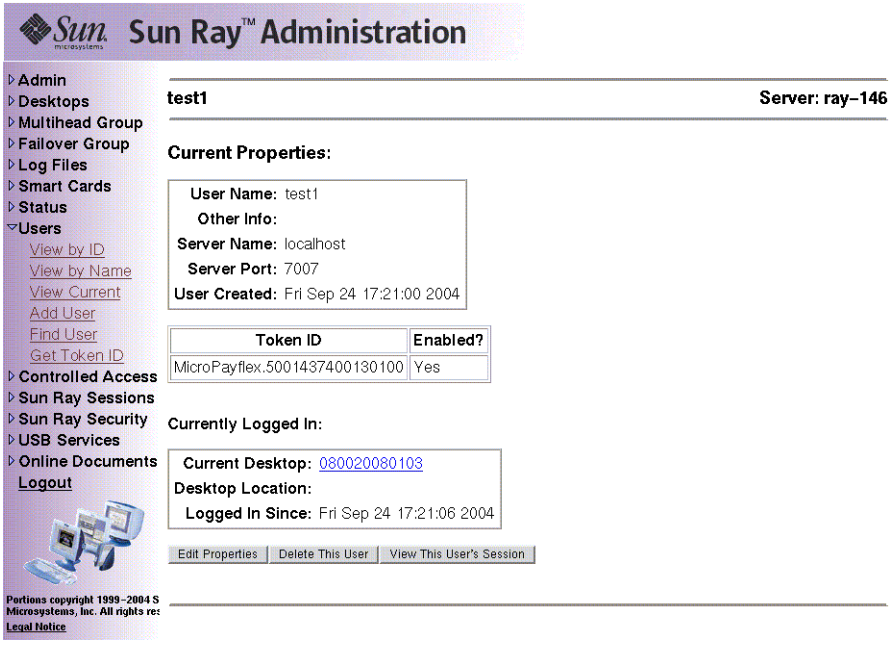


FIGURE 3-27 The Current Properties Window Shows Administrative Options for a User

2. **Press the Delete This User button.**

   The Delete User page is displayed.

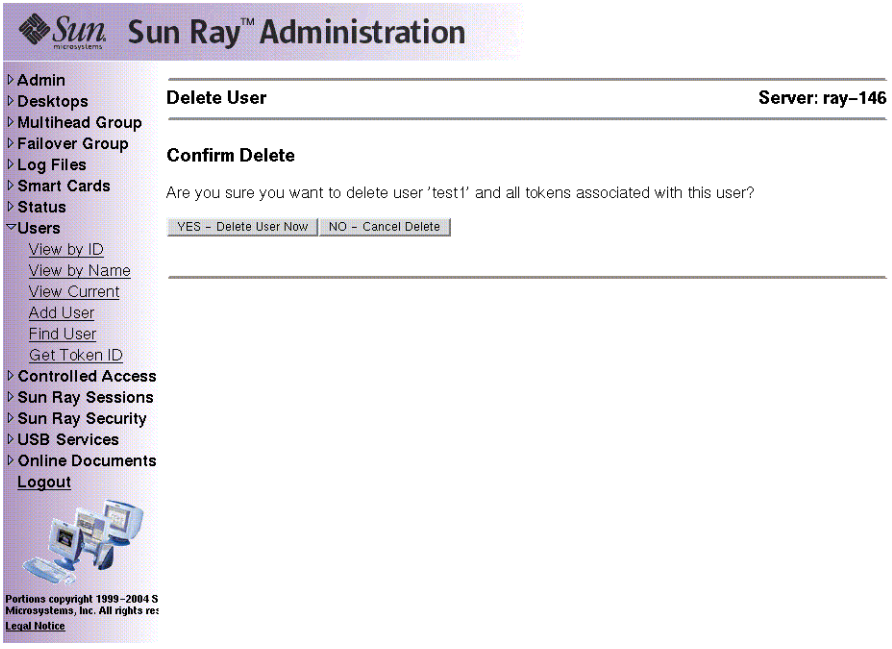


FIGURE 3-28 Delete User Window

3. **To delete the user, press the YES — Delete User Now button.**

   To cancel this delete operation, press the NO — Cancel Delete button. If you press YES, the user and all associated tokens are deleted from the administration database and a confirmation of your delete operation is displayed. If you press NO, you are returned to the Current Properties page.

▼ To View Current Users

- **From the expanded navigation menu under Users, click the View Current link.**

  The View Current Users window is displayed, listing users who currently have active sessions.

Note – The list of users conforms to policies established with `utpolicy`, with which you can enable display of registered users, unregistered users, or both.

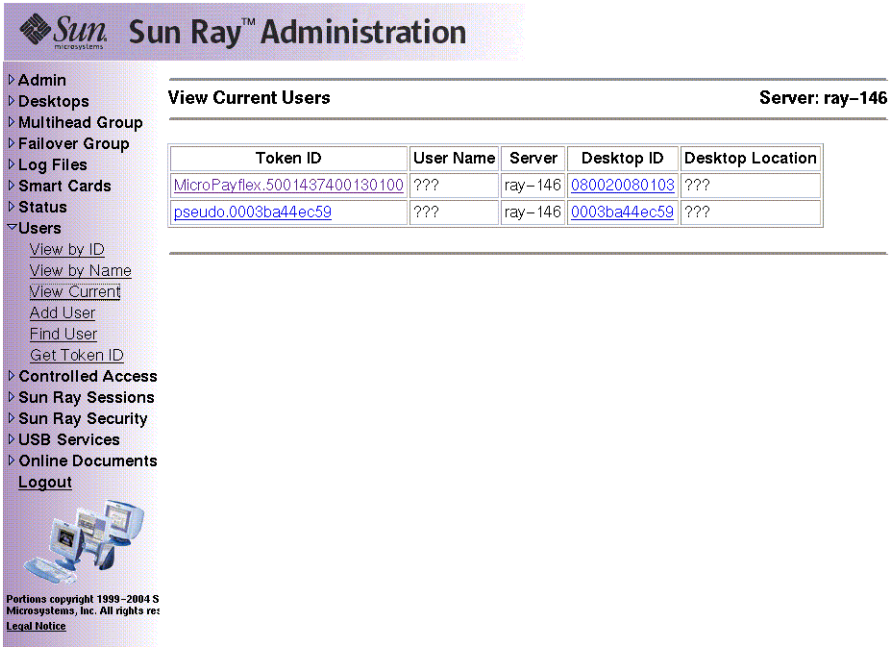


FIGURE 3-29 View Current Users Window

▼ To Display a User's Current Properties

- **Click the Token ID or User Name hyperlink for the user.**

  The Current Properties page for the user is displayed (see FIGURE 3-27). It displays the information about the user contained in the administration database, including the user's current login status.

  The possible states are:

  - Never Logged In
  - Currently Logged In

- Logged Off

For the last two states, the following fields are also displayed:

TABLE 3-3 Login Status Fields

Option	Description
Current Desktop/Last Desktop	Current/last DTU where the user is or was logged in.
Desktop Location	Location of the DTU.
Logged In Since/Logged Off At	Date and time the user logged in or off the DTU.

▼ To Add a User

1. **From the expanded menu under Users, click the Add User link.**

   The Add User window is displayed.

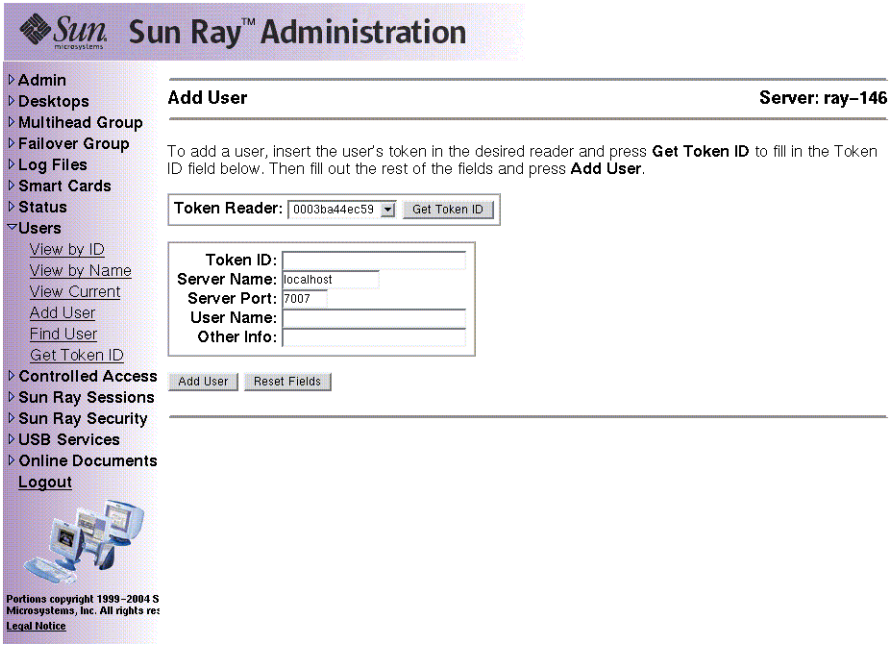


FIGURE 3-30 Add User Window

2. **If you do not know the user's Token ID and have configured a token reader:**

   a. **Insert the user's new card into the selected token reader.**

b. Choose the selected token reader from the pull-down menu of available readers.

c. Press the Get Token ID button.

The application queries the token reader and, if successful, redisplays the form with the Token ID field filled out.

3. **Enter data in the required fields.**

4. **Press the Add User button.**

The user and associated token are created in the administration database.

▼ To View the User's Sessions

- **If the user is currently logged in, you can view the user's session by clicking the View This User's Session button.**

▼ To Edit a User's Properties

1. **From the user's Current Properties page, press the Edit Properties button.**
   The Edit User Properties page is displayed.

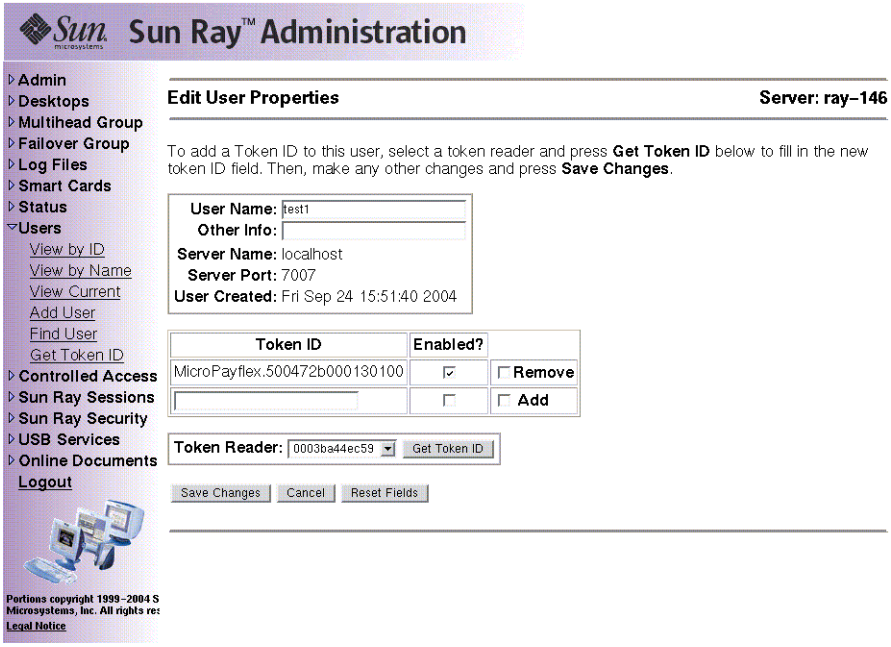


FIGURE 3-31 Edit User Properties Page

2. **Make changes to any of the text boxes.**
   You can also add or remove tokens from a user at the same time.
3. **When finished, press the Save Changes button.**
   The changes are saved to the administration database.

▼ To Add a Token ID to a User's Properties

1. **From the Edit User Properties page, type the new Token ID into the empty Token ID text field.**
2. **If you do not know the new Token ID and have configured a token reader:**
   a. **Insert the user's new card into the selected token reader.**

b. **Choose the selected token reader from the pull-down menu of available readers.**

c. **Press the Get Token ID button.**

   The application queries the token reader and, if successful, redisplays the form with the Token ID text field filled out.

3. **Check the Enabled checkbox next to the new Token ID.**
4. **Check the Add checkbox next to the new Token ID.**

   You can also make any other edits to the user at the same time.

5. **Press the Save Changes button.**

   The changes are then added to the administration database.

▼ To Delete a Token ID From a User's Properties

1. **From the Edit User Properties page, check the Remove checkbox for any token IDs you want to remove.**
2. **Press the Save Changes button.**

   The changes are then added to the administration database.

▼ To Enable or Disable a User's Token

1. **From the Edit User Properties page, check the Enabled checkbox for any token IDs you want to enable.**
2. **Uncheck the Enabled checkbox for any token IDs you want to disable.**
3. **Press the Save Changes button.**

   The changes are saved to the administration database.

▼ To Find a User

1. **From the expanded menu under Users, click the Find link.**
   The Find User window is displayed.

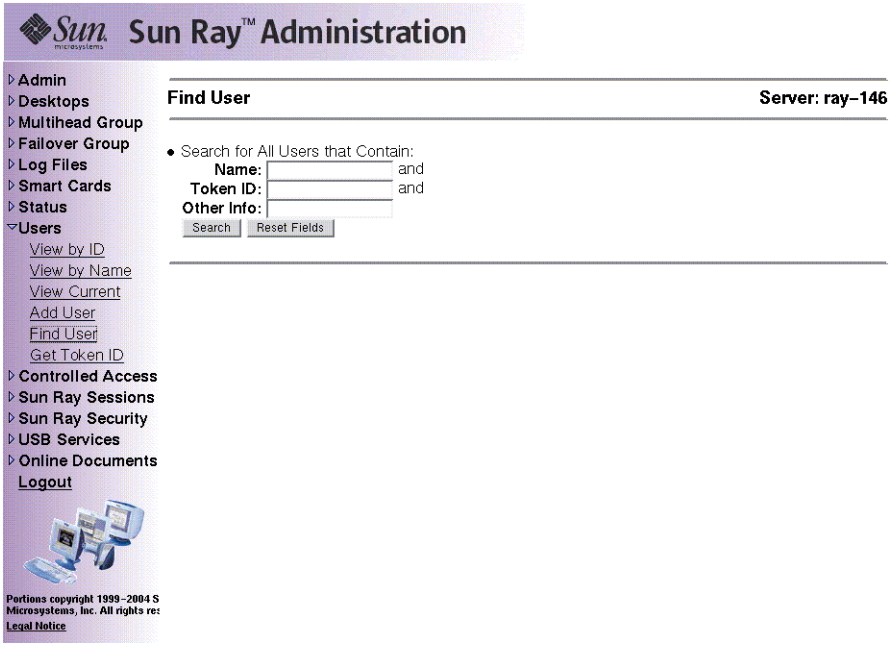


FIGURE 3-32 Find User Window

2. **Enter data in the required fields.**
3. **Press the Search button.**

▼ To Get a Token ID From a Token Reader

1. **From the expanded Users menu, click the Get Token ID link.**

   The Get Token ID window is displayed.

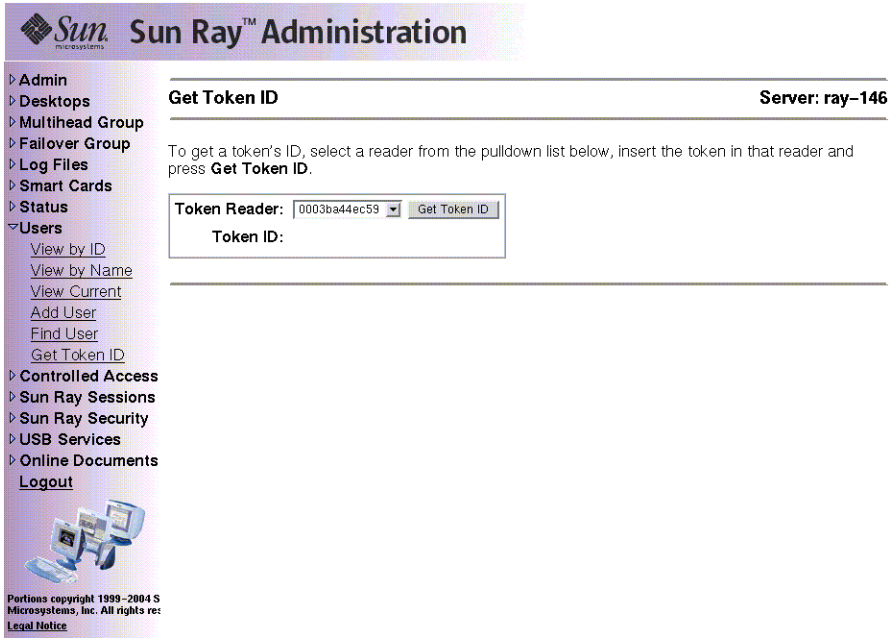


FIGURE 3-33 Get Token ID Window

2. **Insert the new card into the selected token reader.**
3. **Choose the selected token reader from the pull-down menu of available readers.**
4. **Press the Get Token ID button.**

   The application queries the token reader and redisplays the page with the Token ID field filled out.

Managing Sessions

A Sun Ray session is created when the user logs in to a Sun Ray DTU. A Sun Ray session has three possible states, as shown in TABLE 3-4.

TABLE 3-4 Sun Ray Session States

State	Description
Connected/disconnected	A session is currently displayed on a DTU.
Idling	The session is waiting at the Solaris login prompt.
Running/suspended	The session is running unless the startup process and its descendents are stopped.

▼ To Find Sun Ray Sessions

1. **From the navigation menu, click the expansion arrow for Sun Ray Sessions.**
2. **From the expanded navigation menu, click the Find Sun Ray Sessions link.**
3. **In the text fields, enter the User Name, Token ID, or Unix Login Name.**
4. **Click the Search button.**

   If you enter data in error, press the Clear button to clear entered data. The Sun Ray Sessions window is displayed with the Sun Ray search results.

▼ To View Sun Ray Sessions

1. **From the navigation menu, click the expansion arrow for Sun Ray Sessions.**
2. **From the expanded navigation menu, click the View by Server link.**

   Running sessions on the current server are displayed.

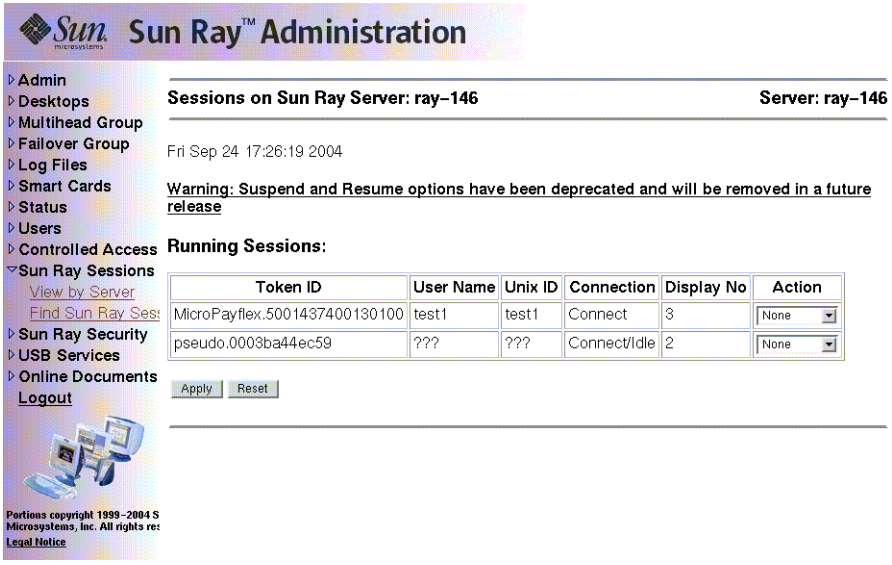


FIGURE 3-34 Sessions on Current Sun Ray Server Window

3. **To change the state of any of the displayed sessions, use the Action pull-down menu button to display your choices.**

   There are three possible actions: None, Terminate, and Suspend.

4. **To apply your changes, click the Apply button.**

CHAPTER 4

Peripherals for Sun Ray DTUs

This chapter contains information about selected USB, parallel, and serial devices and printing from Sun Ray DTUs.

There are two kinds of peripherals: serial and parallel. Serial peripherals enable RS-232-style serial connections to the Sun Ray DTU. Parallel peripherals enable printing and come in two types: adapters and direct USB-connected printers.

Third-party adapters are useful for supporting legacy serial and parallel devices.

Sun Ray Server Software recognizes a parallel printer with an adapter as a USB printer.

Device Nodes and USB Peripherals

Sun Ray Server Software creates a device directory called `IEEE802.`*MACID* in the `/tmp/SUNWut/units` directory. This directory contains the MAC address for each DTU on the interconnect. The `IEEE802.`*MACID* directory for each DTU contains `dev` and `devices` directories. The Sun Ray `dev` directory contains a representation of the logical topology of the `devices` connected to the DTU. The Sun Ray `devices` directory contains a representation of the physical topology of some of the devices connected to the DTU.

Note – Sun Ray Server Software does not create device nodes for every USB device. Some USB device drivers export their device interfaces through other mechanisms than a traditional UNIX device node.

Directories correspond to buses and hubs, and files correspond to ports. Hub directories are named according to the port on the upstream hub into which they are attached.

Device Nodes

In Sun Ray `devices`, device nodes are created for each serial or printer port on an attached USB device. The device nodes are created in the `hub` directory corresponding to the hub to which they are attached. They are named:

manufacturer_name, model_name@upstream_hub_port

If the USB device has multiple identical ports (for example, two serial ports), the name is followed by :*n* where *n* is a numerical index, starting at 1.

The following is a typical device node path:

`/tmp/SUNWut/units/IEEE802.`*MACID*`/devices/usb@1/hub@1/\`
manufacturer_name, model_name`@3:1`

TABLE 4-1 Definitions of Naming Conventions

Term	Definition
physical topology	The *physical topology* is hub@*port*/hub@*port* and so on. The *port* refers to the port on the parent hub into which the device or child hub is plugged.
printer name 1, *terminal name 1*	The printer and terminal name in the Sun Ray `devices` directory is *manufacturer, model@port* with a colon separating the numerical index when the string just described is not unique in the directory.
printer name 2, *terminal name 2*	The printer and terminal name in the Sun Ray `dev` directory is the manufacturer and serial number concatenated with an alphabetic index when the serial number is not unique.

Device Links

Device links are created under the `dev` directory. A link to each serial node is created in `dev/term`, and a link to each parallel node is created in `dev/printers`.

Typical device links are:

```
/tmp/SUNWut/units/IEEE802.080020cf428a/dev/term/manufacturer_name-67a
/tmp/SUNWut/units/IEEE802.080020cf428a/dev/printers/1608b-64
```

manufacturer_name-serial_numberindex

where *index* is an increasing alphabetical character, starting at `a`.

If the manufacturer name is not available, the USB vendor and product ID numbers are used for the name of the device link.

Device Node Ownership

Some device nodes are owned by the user whose session is active on the DTU, while others may be owned by root or by other users that may have had previously active sessions on the DTU. Device permissions, access controls and ownership rules are determined by the class of device. For serial and parallel devices, only the user whose session is active on the DTU or the superuser have permission to use the attached device. If there is no user with an active session, superuser owns the serial and parallel device nodes. This rule may not hold for other classes of USB devices connected to the DTU.

Hot Desking and Device Node Ownership

Note – The following description of the behavior of USB devices when sessions are connected and disconnected from a DTU applies only to USB serial and USB parallel devices. Other device classes may have different semantics regarding ownership and device lease times.

Changing the active session on a DTU changes the ownership of the device nodes to the user associated with the new session. A session change occurs whenever a user:

- Inserts or removes a smart card from a DTU
- Logs into a session
- Detaches from a session using non-smart card mobility

In a failover environment, you can use the `utselect` or `utswitch` command to change a session. A session change causes all devices currently open by a non-root user to be closed after 15 seconds. Any input or output to or from any affected device results in an error. Devices currently opened by the superuser remain unaffected by the session change.

Note – When a session is changed, any input or output in progress on a device node opened by a non-root user is cancelled after 15 seconds. If the original session is restored within 15 seconds, the ownership is not relinquished, and input and output continue uninterrupted.

Attached Printers

Sun Ray Server Software 3 supports PostScript™ printers connected directly to a USB port on the Sun Ray DTU or connected through a USB-to-parallel port adapter. For non-PostScript printer support, refer to "Printers Other Than PostScript Printers" on page 89.

Note – The `lp` subsystem opens the device node as superuser for each print request, so print jobs are not affected by hot desking.

Printer Setup

The following generic instructions may vary slightly from one Linux implementation to another but should provide enough information to enable an administrator to set up basic printing services.

▼ To Set Up a Printer

1. **Log in as superuser on a Sun Ray DTU.**
2. **To determine the MAC address of the DTU, press the three audio option keys to the left of the power key in the upper right corner of the keyboard.**

   The alphanumeric string displayed above the connection icon is the MAC address.

3. **To locate the Sun Ray DTU, type:**

```
# cd /tmp/SUNWut/units/*MAC_address
# pwd
 /tmp/SUNWut/units/IEEE802.MACID/
```

The path to the extended MAC address for your particular Sun Ray DTU is displayed.

4. **Locate the port for the printer by typing:**

```
# cd dev/printers
# pwd
/tmp/SUNWut/units/IEEE802.MACID/dev/printers
#ls
printer-node-name
```

5. **In the directory, locate the printer node.**

6. **Start the Administration Tool by typing:**

```
# admintool &
```

7. **Go to Browse -> Printers -> Edit -> Add -> LocalPrinter.**

8. **Type in:**

   a. **Printer name:** *printername*

   b. **Description (optional)**

   c. **Printer Port**

   Choose Other to enter the printer port path name, using the resulting directory from Step 4.

```
/tmp/SUNWut/units/IEEE802.MACID/dev/printers/printer-node-name
```

Note – Do not use the port name under the `devices` directory.

---

   d. **Click OK.**

e. If you are using a PostScript printer, under Printer Type choose PostScript unless your printer is listed.

Select the printer type according to your printer model. If no option matches, select **other**; then type your printer type or **unknown**.

f. If you are using a PostScript printer, under File Contents choose PostScript and ASCII.

g. Options: Default Printer (optional)

h. Click OK.

Note – Do not click OK more than once. If you do, a failure message is displayed.

---

9. To verify that the printer has been set up correctly, type:

```
# lpstat -d printername
```

Printers Other Than PostScript Printers

Printers that do not use PostScript, such as engineering plotters, are best supported by third-party software. Low-cost inkjet printers require third-party software such as:

- Easy Software's ESP PrintPro, available from `http://www.easysw.com`
- Ghostscript, available from `http://www.ghostscript.com`
- Vividata PShop, available from `http://www.vividata.com`

Check with the vendors for pricing and the precise printer models supported.

Adapters

For a list of verified serial and parallel adapters, see:

`http://www.sun.com/io_technologies/sunray/usb/sunray-usb.html`

■

CHAPTER 6

Encryption and Authentication

SunRay Server Software provides interconnect security. Two main aspects of this feature are:

- Traffic encryption between the SunRay client and server
- SunRay server-to-client authentication

Introduction

In earlier versions of Sun Ray Server Software, data packets on the SunRay interconnect were sent in the clear. This made it easy to “snoop” the traffic and recover vital and private user information, which malicious users might misuse. To avoid this type of attack, SunRay Server Software allows administrators to enable traffic encryption. This feature is optional; the system or network administrator can configure it based on site requirements.

The ARCFOUR encryption algorithm, selected for its speed and relatively low CPU overhead, supports a higher level of security between Sun Ray services and SunRay desktop units. In the 2.0 release, only the X server traffic was encrypted.

Encryption alone does not provide complete security. It is still possible, if not necessarily easy, to spoof a SunRay server or a SunRay client and pose as either. This leads to the man-in-the- middle attack, in which an impostor claims to be the SunRay server for the clients and pretends to be client for the server. It then goes about intercepting all messages and having access to all secure data.

Client and server authentication can resolve this type of attack. This release offers server-side authentication only, through the pre-configured public-private key pairs in Sun Ray Server Software and firmware. The Digital Signature Algorithm (DSA) is used to verify that clients are communicating with a valid Sun Ray server. This

authentication scheme is not completely foolproof, but it mitigates trivial man-in-the-middle attacks and makes it harder for attackers to spoof Sun Ray Server Software.

Security Configuration

When configuring the security for a Sun Ray system, you should evaluate the security requirements. You may choose:

- to enable encryption for upstream traffic only
- to enable encryption for downstream traffic only
- to enable bidirectional encryption
- to enable server authentication (client authentication is not currently available)

Additionally, you must decide whether to enable hard security mode. To configure your site, you can use the `utcrypto` command or the Sun Ray Administration Tool (Admin GUI).

Security Mode

Hard security mode ensures that every session is secure. If security requirements cannot be met, the session is refused. Soft security mode ensures that every client that requests a session gets one; if security requirements cannot be met, the session is granted but not secure.

For example, in hard security mode, if any SunRay DTU that does not support security features (for instance, because of old firmware) connects to a Sun Ray server, the server denies the session.

In soft security mode, given the above situation, the SunRay server grants the DTU a non-secure session. It is now up to the user to decide whether to continue using a non-secure session.

For more information, please see the man page for `utcrypto` or "Administration Tool" on page 33.

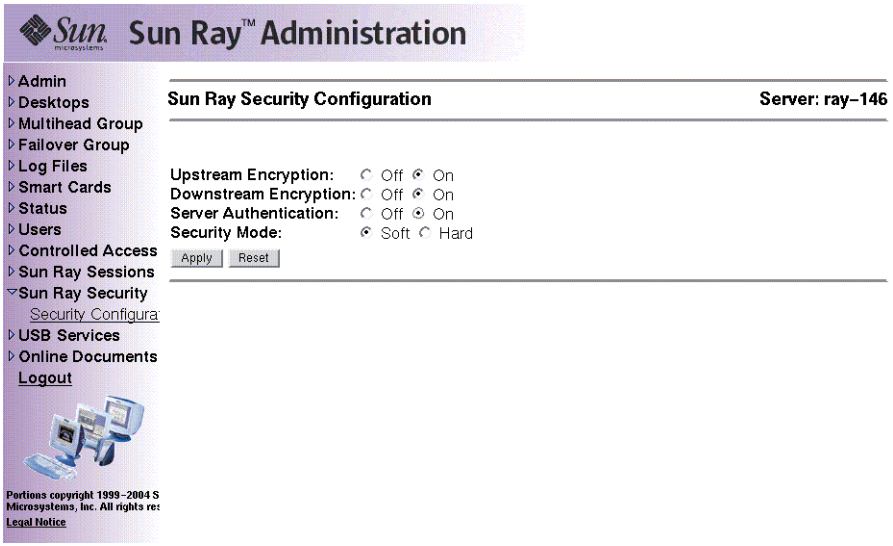


FIGURE 6-1 Sun Ray Security Configuration Window

Session Security

Use the `utsession` command to display session status. Its output has been modified to included security status for a session. The State column in `utsession -p` output now displays the encrypted/authenticated state of the session by using *E* for encrypted and *A* for authenticated session types. This information is not displayed for any session in the disconnected state.

In a multihead environment, there may be a case where the primary and the secondary servers have different firmware. For instance, if the secondary has version 1.3 or earlier firmware, it cannot support any of the security features. In this case, the lowest security setting is displayed. In other words, if the secondary server is configured with 1.3 firmware and the primary server with 2.0 or version 3 firmware, and encryption and authentication are configured, neither an *E* or an *A* is displayed.

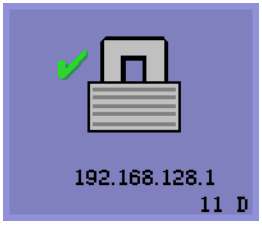
```
# utsession -p
Token ID Registered NameUnix IDDisp State
Payflex.0000074500000202 ??? ??? 2IEA
Micropayflex.0000035400045450?????3D
```

Security Status

Once a connection has been successfully established between a client and a server, the user can determine whether the connection is secure at any time by pressing the three volume keys together (currently used to determine MAC address of the terminal).

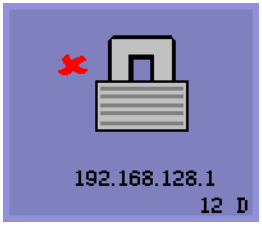
One of the following icons is also displayed when a Sun Ray DTU connects to a session. Each icon displays information about connection security status.

There are several variations on the security icon:



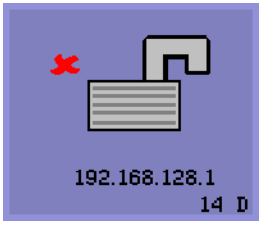
Locked Authenticated

The server is authenticated to the client and the data link is encrypted.



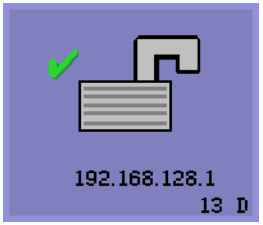
Locked Not Authenticated

The server is not authenticated to the client and the data link is encrypted.



Unlocked Not Authenticated

The server is not authenticated to the client and the data link is not encrypted.



Unlocked Authenticated

The server is authenticated to the client but the data link is not encrypted.

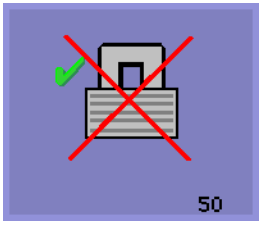
Session Connection Failures

The following icons are displayed when there might be a security breach.

Session Refused

Definition: The client is refusing to connect to a server because it is unable to verify the validity of the Sun Ray server.

This error can occur only if an unknown Sun Ray server intercepts the messages and tries to emulate a valid Sun Ray server. *This is a session security breach*.



Session Refused

Definition: The server is refusing to grant a session to the client because the client is unable to fulfill the server's security requirements.

Actions to take:

- Check the client's firmware version. This error may occur with firmware versions earlier than 2.0 if the server is configured for hard security mode.
- Upgrade the firmware to version 2.0 or later, preferably to SRSS 3. As an alternative, confirm whether your site requires hard security mode. If not, the session can be enabled with soft security mode.

CHAPTER 6

Gnome Display Manager

The Gnome Display Manager (GDM) is responsible for logging users into your system and starting their sessions (an X11 server plus applications). It is typically used to manage the console on a system that is configured with a graphics device, but it may be used to manage other displays attached to a system as well.

Unfortunately the version of GDM that is supplied with your system is not able to work in a SunRay environment. Therefore, the SunRay server software includes a GDM that has been enhanced with the ability to manage SunRay devices. This enhanced GDM is otherwise identical to the GDM it replaces, and can still be used to manage the console and/or other displays.

Installation

During the SRSS installation process, you will be asked whether the installation script should remove the existing GDM from your system. You must answer “yes” to this question in order to continue with the SRSS installation. SRSS will then remove the old GDM from your system and install the SunRay-enhanced version. If you answer “no”, the SRSS install process will be aborted.

Since the existing GDM will be removed during SRSS install, it is recommended that you *not* use a GDM-controlled display to do the install. Use a telnet session into the server, or a virtual terminal.

Uninstallation

If you need to remove the SRSS software, you will be asked whether the SunRay-enhanced GDM should remain on your system. If you answer “no”, be advised that you may have to install the original GDM RPM if you want non-SunRay displays, such as the console, to be managed.

Configuration

SunRay's GDM is based on version 2.4.4.7. If you have already upgraded your system to a newer version of GDM, the SunRay version may not have all the features you expect.

SunRay installation will remove the current GDM from your system, including its configuration file, `/etc/X11/gdm/gdm.conf` (or `/etc/gnome2/gdm/gdm.conf` on Suse systems)

Therefore, if you have modified to your `gdm.conf` configuration, backup the file before installing SRSS. You may wish to reapply your changes to the `gdm.conf` that SRSS installs.

Tip – Do not simply put your old `gdm.conf` in place of the SRSS-installed one, SunRay will not work correctly.

The default configuration for GDM is to manage `DISPLAY 0` (zero) on the console. If you do not wish to start an X11 server on the console, edit `/etc/X11/gdm/gdm.conf` and remove `DISPLAY 0` from the servers section.

Gnome Display Manager Privileges

Many Linux systems come configured with liberal administrative privileges for non-root users. You most likely do *not* want these privileges offered to users who login using a SunRay. Please review the man pages for `pam_console`, `console.perms`, and `console.apps`. It is also a good idea to edit the `/etc/security/console.perms` file to remove display numbers from the definition of *console*. If a definition exists for *xconsole*, it should be removed entirely.

For example, a line that reads:

```
<console>=tty[0-9][0-9]* vc/[0-9][0-9]* :[0-9].[0-9] :[0-9]
```

should instead read:

```
<console>=tty[0-9][0-9]* vc/[0-9][0-9]*
```

And a line such as:

```
<xconsole>=:[0-9].[0-9] :[0-9]
```

should be removed altogether.

CHAPTER 7

Deployment on Shared Networks

This chapter describes the process of deploying DTUs on shared network segments. It covers the following topics:

When first introduced, Sun Ray DTUs could be deployed only on dedicated, directly-connected interconnect subnets. Although dedicated interconnects provide reliable service and are easy to configure, they require the full-time commitment of networking equipment, cabling, and host interfaces. This constraint has been removed from SRSS 2.0 and 3, allowing network administrators to deploy Sun Ray DTUs nearly anywhere on an enterprise intranet. The most important advantages of intranet deployment are:

- Sun Ray can be deployed on any existing network infrastructure that meets Sun Ray Quality of Service (QoS) requirements.
- Sun Ray DTUs can be deployed at a greater distance from their Sun Ray server.

Sun Ray DTU Initialization Requirements

Because Sun Ray DTUs are stateless, they rely entirely on network services to provide the configuration data they need to complete their initialization.

- Each DTU must first acquire basic network parameters, such as a valid IP address, on the network to which it is connected.
- The DTU can also be supplied with additional configuration information to support advanced product features, such as the ability to update the DTU firmware and to report exception conditions to a syslog service.

- The DTU must locate and contact a Sun Ray server that can offer desktop services to the Sun Ray user.

The Sun Ray DTU uses the Dynamic Host Configuration Protocol (DHCP) to obtain this information.[1]

DHCP Basics

The DTU is a DHCP client that solicits configuration information by broadcasting DHCP packets on the network. The requested information is supplied by one or more DHCP servers in response to the client's solicitations. DHCP service may be provided by a DHCP server process executing on a Sun Ray server, by DHCP server processes executing on other systems, or by some combination of the two. Any conforming implementation of a DHCP service can be used to satisfy the DHCP requirements of the DTU. Sun's Solaris DHCP service is one such implementation. Third-party implementations executing on non-Sun platforms can also be configured to deliver information to Sun Ray DTUs.

The DHCP protocol defines a number of *standard options* that can be used to inform the client of a variety of common network capabilities. DHCP also allows for a number of *vendor-specific options*, which carry information that is meaningful only to individual products.

The Sun Ray DTU depends on a small number of standard options to establish its basic network parameters. It depends on several standard and vendor-specific options to provide the additional information that constitutes a complete DTU configuration. If these additional configuration parameters are not supplied, the DTU cannot perform certain activities, the most important of which is the downloading of new DTU firmware. TABLE 7-2 lists the vendor-specific options.

Note – If an administrator chooses not to make this additional configuration information available to the Sun Ray DTUs, a procedure must be established to deliver firmware updates to them. One solution would be a small, dedicated interconnect on one Sun Ray server. Then, the administrator can transfer the DTUs one-by-one when new firmware becomes available on the server, for instance, through a patch or Sun Ray product upgrade.

The location of the Sun Ray server is usually conveyed to the DTU through one of a pair of DHCP vendor-specific options, *AuthSrvr* and *AltAuth*.[2]

1. DHCP is an Internet Engineering Task Force (IETF) protocol described in Requests for Comments (RFC) *RFC 2131* and *RFC 2132*.

2. See Table 7-2 on page 130.

If the DTU does not receive this information, it uses a broadcast-based discovery mechanism to find a Sun Ray server on its subnet. The DTU firmware now goes one step further. If the broadcast-based discovery mechanism fails, the DTU interprets the DHCP standard option (option 49) of the *X Window Display Manager* as a list of Sun Ray server addresses where it attempts to contact Sun Ray services. This can simplify the DHCP configuration of LAN-deployed Sun Rays by removing the need for a DHCP vendor option to carry this information (see TABLE 7-1).

TABLE 7-1 DHCP Service Parameters Available

Parameters	Sun Ray Server DHCP Service	External DHCP service with vendor-specific options	External DHCP service without vendor-specific options	No DHCP service
Basic network parameters	Yes	Yes	Yes	No
Additional parameters (for firmware download, etc.)	Yes	Yes	No	No
Sun Ray server location	Yes	Yes	Yes, through broadcast discovery or the *X Display Manager* standard option	Yes, through broadcast discovery

DHCP Parameter Discovery

DHCP enables two stages of parameter discovery. The initial `DHCPDISCOVER` stage discovers basic network parameters. This stage may be followed by a `DHCPINFORM`, which finds additional information that was not provided during `DHCPDISCOVER`.

All Sun Ray DTUs must have access to at least one DHCP service, which provides network parameters in response to a `DHCPDISCOVER` request from the DTU. DTUs containing firmware delivered with Sun Ray Server Software 2.0 or later can exploit the `DHCPINFORM` feature. They enable full configuration of the DTU, even when an external DHCP service that is not capable of providing complete configuration data provides the network parameters of the DTU.

DTUs that contain pre-2.0 firmware require all of their configuration information in the initial `DHCPDISCOVER` phase. They do not attempt a `DHCPINFORM` step. If the deployment strategy requires a two-step DHCP interaction, such DTUs must be upgraded with Sun Ray Server Software firmware version 2.0 or later before being deployed on a shared subnet.

DHCP Relay Agent

The DTU sends DHCP requests as broadcast packets that propagate only on the local LAN segment or subnet. If the DTU resides on the same subnet as the DHCP server, the DHCP server can see the broadcast packet and respond with the information the DTU needs. If the DTU resides on a different subnet than the DHCP server, the DTU must depend on a local DHCP Relay Agent to collect the broadcast packet and forward it to the DHCP server. Depending on the physical network topology and DHCP server strategy, the administrator may need to configure a DHCP Relay Agent on each subnetwork to which Sun Ray clients are connected. Many IP routers provide DHCP Relay Agent capability. If a deployment plan requires the use of a DHCP Relay Agent, and the administrator decides to activate this capability on a router, the appropriate instructions can be found in the router documentation, usually under the heading of "DHCP Relay" or "`BOOTP` forwarding."[3]

In certain cases, an existing enterprise DHCP service provides the DTU with its IP address while a Sun Ray server provides it with firmware version details and Sun Ray server location. If a deployment plan calls for DHCP parameters to be provided to the DTU by multiple servers, and none of those servers is connected to the subnet where the DTU resides, the DHCP Relay Agent should be configured so that the DTUs subnet can deliver broadcasts to all the DHCP servers. For example, in routers controlled by a Cisco IOS Executive, the `ip helper-address` command activates a DHCP Relay Agent. Specifying multiple arguments to the `ip helper-address` command enables relaying to multiple DHCP servers.

Network Topology Options

There are three basic topology options for Sun Ray deployment. DTUs can be deployed on:

- a directly-connected dedicated interconnect.
- a directly-connected shared subnet.
- a remote shared subnet.

A Sun Ray server can support any combination of these topologies, which are shown in FIGURE 7-1.

3. DHCP is derived from an earlier protocol called BOOTP. Some documentation uses these names interchangeably.

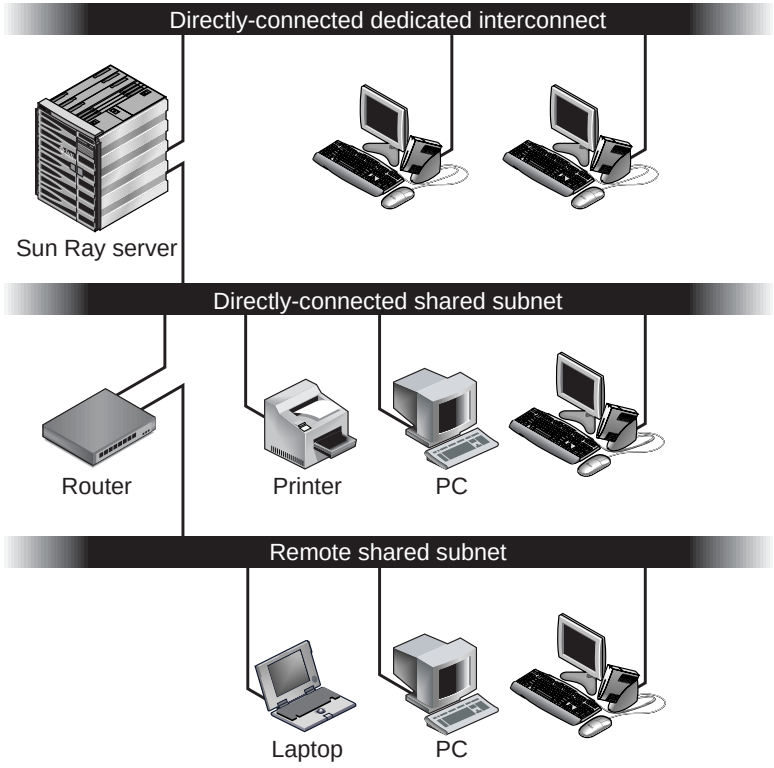


FIGURE 7-1 Network Topologies for Sun Ray DTU Deployment

Note – Sun Ray traffic on shared networks is potentially more exposed to an eavesdropper than traffic on a dedicated Sun Ray interconnect. Modern switched network infrastructures are far less susceptible to snooping activity than earlier shared technologies, but to obtain additional security the administrator may choose to activate Sun Ray's encryption and authentication features. These capabilities are discussed in "Encryption and Authentication" on page 103.

Directly-Connected Dedicated Interconnect

The *directly-connected dedicated interconnect*—often referred to simply as an interconnect—places DTUs on subnets that are:

- directly connected to the Sun Ray server (that is, the server has a network interface connected to the subnet).
- devoted entirely to carrying Sun Ray traffic. Prior to the release of Sun Ray Server Software 2.0, this was the only officially supported Sun Ray topology.

The Sun Ray server, which guarantees the delivery of the full set of DTU configuration parameters, is always used to provide DHCP service for a dedicated interconnect.

Directly-Connected Shared Subnet

Sun Ray Server Software now supports DTUs on a *directly-connected shared subnet*, in which:

- the Sun Ray server has a network interface connected to the subnet.
- the subnet may carry a mix of Sun Ray and non-Sun Ray traffic.
- the subnet is generally accessible to the enterprise intranet.

On a directly-connected shared subnet, DHCP service can be provided by the Sun Ray server, or some external server, or both. Since the Sun Ray server can see broadcast DHCP traffic from the DTU, it can participate in DTU initialization without requiring a DHCP Relay Agent.

Remote Shared Subnet

Sun Ray Server Software now also supports DTUs on a *remote shared subnet*. On a remote shared subnet:

- a Sun Ray server does not have a network interface connected to the subnet.
- the subnet can carry a mix of Sun Ray and non-Sun Ray traffic.
- all traffic between the server and the DTU flows through at least one router.
- the subnet is generally accessible to the enterprise intranet.

On a remote shared subnet, DHCP service can be provided by the Sun Ray server, by some external server, or by both. For DHCP service on the Sun Ray server to participate in DTU initialization, a DHCP Relay Agent must be configured on the remote subnet, where it collects DHCP broadcast traffic and forwards it to the Sun Ray server.

Network Configuration Tasks

The addition of directly-connected and remote shared subnet support allows DTUs to be deployed virtually anywhere on the enterprise intranet, subject only to the provision of DHCP service and a sufficient quality of service between the DTU and the Sun Ray server.

The following sections explain how to configure a network to support these deployment scenarios:

- a directly-connected dedicated interconnect
- a directly-connected shared subnet
- a remote shared subnet

FIGURE 7-2 shows the overall topology and configuration tasks.[4]

Preparing for Deployment

Before deploying a DTU onto any subnet, the administrator must answer three questions:

1. From which DHCP server will DTUs on this subnet get their basic IP networking parameters?
2. From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?
3. How will DTUs on this subnet locate their Sun Ray server?

The answers to these questions determine what configuration steps will let DTUs placed on this subnet initialize themselves and offer Sun Ray sessions to users.

The following sections present examples of DTU deployment on the directly-connected dedicated interconnect A, the directly-connected shared subnet B, and the remote shared subnets C and D shown in FIGURE 7-2.

4. The /24 suffix in IP addresses indicates the use of Classless Inter Domain Routing (CIDR) notation, which is documented in IETF RFCs 1517, 1518, and 1519

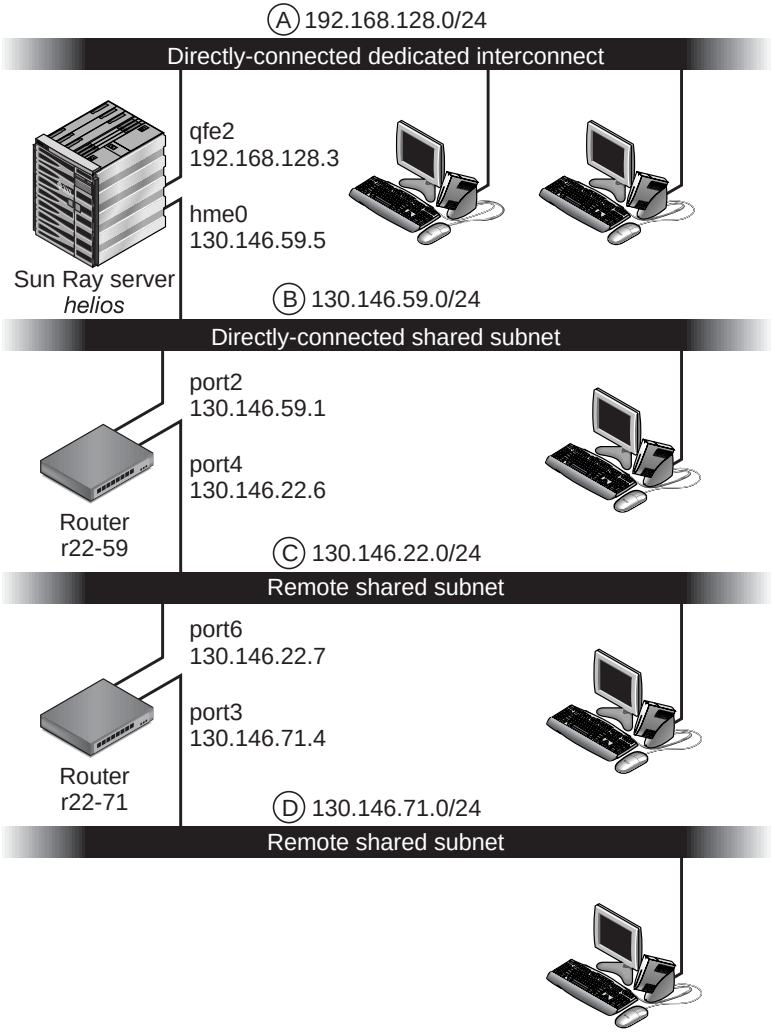


FIGURE 7-2 Sun Ray Network Topology

Deployment on a Directly-Connected Dedicated Interconnect

Subnet A in FIGURE 7-2 is a directly-connected dedicated interconnect. Its subnet will use IP addresses in the range `192.168.128.0/24`. The Sun Ray server named *helios* is attached to the interconnect through its `qfe2` network interface, which will be assigned the IP address `192.168.128.3`.

In an interconnect scenario, the DHCP service on the Sun Ray server always provides both basic networking parameters and additional configuration parameters to the DTU. The answers to the three pre-deployment questions are:

1. From which DHCP server will DTUs on this subnet get their basic IP networking parameters?

   On a directly-connected dedicated interconnect, basic networking parameters are always supplied by the DHCP service on the Sun Ray server.

2. From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?

   On a directly-connected dedicated interconnect, additional configuration parameters are always supplied by the DHCP service on the Sun Ray server.

3. How will DTUs on this subnet locate their Sun Ray server?

   On a directly-connected dedicated interconnect, the DTU is always notified of the location of the Sun Ray server through an additional configuration parameter supplied in Step 2.

Directly-Connected Dedicated Interconnect: Example

This is an example of DHCP service for the directly-connected dedicated interconnect A shown in FIGURE 7-2.

1. Configure the Sun Ray server to provide both basic and additional parameters to the interconnect.

Use the `utadm -a` *ifname* command to configure DHCP service for DTUs on an interconnect. In this example, the interconnect is attached through interface `qfe2`, so the appropriate command is:

```
# /opt/SUNWut/sbin/utadm -a qfe2
### Configuring /etc/nsswitch.conf
### Configuring Service information for Sun Ray
### Disabling Routing
### configuring qfe2 interface at subnet 192.168.128.0
 Selected values for interface "qfe2"
   host address:         192.168.128.1
   net mask:             255.255.255.0
   net address:          192.168.128.0
   host name:            helios-qfe2
   net name:             SunRay-qfe2
   first unit address:   192.168.128.16
   last unit address:    192.168.128.240
   auth server:          192.168.128.1
   firmware server:      192.168.128.1
   router:               192.168.128.1
   alternate servers:
```

```
 Accept as is? ([Y]/N): n
 new host address: [192.168.128.1] 192.168.128.3
 new netmask: [255.255.255.0]
 new host name: [helios-qfe2]
 Do you want to offer IP addresses for this interface? ([Y]/N):
 new first Sun Ray address: [192.168.128.16]
 number of Sun Ray addresses to allocate: [239]
 new auth server: [192.168.128.3]
 new firmware server: [192.168.128.3]
 new router: [192.168.128.3]
Specify alternate server list? (Y/[N]):
 Selected values for interface "qfe2"
  host address:           192.168.128.3
  net mask:               255.255.255.0
  net address:            192.168.128.0
  host name:              helios-qfe2
  net name:               SunRay-qfe2
  first unit address:     192.168.128.16
  last unit address:      192.168.128.254
  auth server:            192.168.128.3
  firmware server: 1      192.168.128.3
  router:                 192.168.128.3
  alternate servers:
 Accept as is? ([Y]/N):
### successfully set up "/etc/hostname.qfe2" file
### successfully set up "/etc/inet/hosts" file
### successfully set up "/etc/inet/netmasks" file
### successfully set up "/etc/inet/networks" file
### finished install of "qfe2" interface
### Building network tables - this will take a few minutes
### Configuring firmware version for Sun Ray
        All the units served by "helios" on the 192.168.128.0
        network interface, running firmware other than version
        "2.0_37.b,REV=2002.12.19.07.46" will be upgraded at their
        next power-on.
### Configuring Sun Ray Logging Functions
DHCP is not currently running, should I start it? ([Y]/N):
### started DHCP daemon
#
```

In this example, the default values initially suggested by utadm were not appropriate. (Specifically, the suggested value for the server's IP address on the interconnect was not the desired value.) The administrator replied **n** to the first `Accept as is?` prompt and was given the opportunity to provide alternative values for the various parameters.

2. **Restart Sun Ray services on the Sun Ray server.**

   Once the `utadm` command has completed, issue a `utrestart` command to fully activate Sun Ray services on the newly-defined interconnect:

```
# /opt/SUNWut/sbin/utrestart
Resetting servers... messages will be logged to /var/opt/SUNWut/log/messages.
```

Deployment on a Directly-Connected Shared Subnet

Subnet B in FIGURE 7-2 is a directly-connected shared subnet that uses IP addresses in the range `130.146.59.0/24`. The Sun Ray server *helios* is attached to the interconnect through its `hme0` network interface, which has been assigned the IP address `130.146.59.5`. The answers to the three pre-deployment questions are:

1. From which DHCP server will DTUs on this subnet get their basic IP networking parameters?

   In a shared subnet scenario, you must choose whether a DHCP service on the Sun Ray server or some external DHCP service will provide the DTU with basic network parameters. If the enterprise already has a DHCP infrastructure that covers this subnet, it probably supplies basic network parameters. If no such infrastructure exists, configure the Sun Ray server to provide basic network parameters.

2. From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?

   The administrator must choose whether to supply additional configuration parameters to the DTU and, if so, whether to use a DHCP service on the Sun Ray server or some external DHCP service for this purpose. On a directly connected shared subnet, it is possible to deploy DTUs without providing additional parameters at all, but since this deprives the DTU of a number of features, including the ability to download new firmware, it is generally undesirable.

   Administrators of an already established DHCP infrastructure may be unable or unwilling to reconfigure that infrastructure to provide additional Sun Ray configuration parameters, so it is usually more convenient to have the Sun Ray server provide these parameters. Even when the established infrastructure is capable of delivering the additional parameters, it may be desirable to have the Sun Ray server provide them. This enables SRSS commands to be used to manage the values of the additional configuration parameters when those values need to be changed in response to software upgrades or patch installations on the Sun Ray server. For instance, a patch that delivers new DTU firmware could automatically update the firmware version string that is delivered to the DTU. However, if the firmware version parameter is supplied by some external DHCP

service, an administrator must manually edit the firmware version parameter string in the external DHCP configuration rules to reflect the new firmware version delivered by the patch. This activity is time-consuming and error-prone, as well as unnecessary.

3. How will DTUs on this subnet locate their Sun Ray server?

   Use one of the optional additional configuration parameters to report the location of the Sun Ray server to the DTU. If additional configuration parameters are not supplied to the DTU at all, the DTU has no indication of the location of any Sun Ray server. In these circumstances, the DTU attempts to discover the location of a Sun Ray server by using a broadcast-based mechanism. However, the DTUs broadcast packets propagate only on the local subnet, so, in the case of a remote subnet, the broadcast cannot reach the Sun Ray server, and contact cannot be established.

The following examples illustrate two configurations of the directly connected shared subnet. In the first example, the Sun Ray server delivers both basic networking parameters and additional parameters. In the second example, an external DHCP service supplies basic networking parameters, and no additional parameters are provided to the DTU, which must establish contact with the Sun Ray server through its local subnet broadcast discovery mechanism.

The most likely case, where an external DHCP service provides basic networking parameter and the Sun Ray server provides additional parameters, is illustrated by an example in "Deployment on a Remote Subnet."

Directly-Connected Shared Subnet: Example 1

In this example, the answers to the three pre-deployment questions are:

1. From which DHCP server will DTUs on this subnet get their basic IP networking parameters?

   From the Sun Ray server.

2. From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?

   From the Sun Ray server.

3. How will DTUs on this subnet locate their Sun Ray server?

   The DTUs will be informed of the location of the Sun Ray server through an additional configuration parameter delivered in Step 2.

1. **Configure the Sun Ray server to provide both basic and additional parameters to the shared subnet.**

   DHCP service for DTUs on a shared subnet is configured through the `utadm -A` *subnet* command. In this example, the shared subnet has network number `130.146.59.0`, so the appropriate command is `utadm -A 130.146.59.0`:

```
# /opt/SUNWut/sbin/utadm -A 130.146.59.0
  Selected values for subnetwork "130.146.59.0"
    net mask:                   255.255.255.0
    no IP addresses offered
    auth server:                130.146.59.5
    firmware server:            130.146.59.5
    router:                     130.146.59.1
    alternate servers:
  Accept as is? ([Y]/N): n
  netmask: 255.255.255.0 (cannot be changed - system defined netmask)
  Do you want to offer IP addresses for this subnet?  (Y/[N]): y
  new first Sun Ray address: [130.146.59.4]  130.146.59.200
  number of Sun Ray addresses to allocate: [55] 20
  new auth server:           [130.146.59.5]
  new firmware server:       [130.146.59.5]
  new router:                [130.146.59.1]
Specify alternate server list? (Y/[N]):
  Selected values for subnetwork "130.146.59.0"
    net mask:                130.146.59.0
    first unit address:      130.146.59.200
    last unit address:       130.146.59.219
    auth server:             130.146.59.5
    firmware server:         130.146.59.5
    router:                  130.146.59.1
    alternate servers:
 Accept as is? ([Y]/N):
### Building network tables - this will take a few minutes
### Configuring firmware version for Sun Ray
    All the units served by "helios" on the 130.146.59.0
    network interface, running firmware other than version
    "2.0_37.b,REV=2002.12.19.07.46" will be upgraded at
    their next power-on.
### Configuring Sun Ray Logging Functions
### stopped DHCP daemon
### started DHCP daemon
#
```

   The default values initially suggested by utadm were not appropriate. Specifically, this server would not have offered any IP addresses on the `130.146.59.0` subnet because utadm assumes that basic networking parameters, including IP addresses,

are provided by some external DHCP service when the DTU is located on a shared subnet. In this example, however, the Sun Ray server is required to provide IP addresses, so the administrator replied **n** to the first `Accept as is?` prompt and was given the opportunity to provide alternative values for the various parameters. Twenty IP addresses, starting at `130.146.59.200`, were made available for allocation to DHCP clients on this subnet.

2. **Restart Sun Ray services on the Sun Ray server.**

   Once the `utadm` command has completed, issue a `utrestart` command to fully activate Sun Ray services on the shared subnet:

```
# /opt/SUNWut/sbin/utrestart
Resetting servers... messages will be logged to /var/opt/SUNWut/log/messages.
```

Directly-Connected Shared Subnet: Example 2

In this example, the answers to the three pre-deployment questions are:

1. From which DHCP server will DTUs on this subnet get their basic IP networking parameters?

   From an external DHCP service.

2. From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?

   The DTUs will not be supplied with additional parameters.

3. How will DTUs on this subnet locate their Sun Ray server?

   By using the local subnet broadcast discovery mechanism.

In this example, the Sun Ray server does not participate in DTU initialization at all. Why, then, are configuration steps required on the Sun Ray server? The Sun Ray server responds by default only to DTUs located on directly connected dedicated interconnects. It responds to DTUs on shared subnets only if the `utadm -L on` command has been executed. Running the `utadm -A` *subnet* command to activate DHCP on the Sun Ray server for a shared subnet, as in this example, implicitly executes `utadm -L on`. If `utadm -A` *subnet* has not been run, the administrator must run `utadm -L on` manually to allow the server to offer sessions to DTUs on the shared subnet.

1. **Configure the external DHCP service.**

   Determining how to configure the external DHCP infrastructure to provide basic networking parameters to the DTUs on this subnet is beyond the scope of this document. Bear in mind:

- If the external DHCP service does not have its own direct connection to this subnet, the administrator must configure a DHCP Relay Agent to deliver DHCP traffic on this subnet to the external DHCP service. The most likely location for such a Relay Agent would be on a router in this subnet, in this case the router named `r22-59` in FIGURE 7-2. For a brief introduction to this topic refer to "DHCP Relay Agent" on page 112.
- An existing external DHCP service may need to have its IP address allocation for this subnet increased in order to support the new DTUs. (This applies whenever additional DHCP clients are placed on a subnet.) It might also be desirable to reduce the lease time of addresses on this subnet so that addresses become eligible for reuse quickly.

2. **Configure the Sun Ray server to accept DTU connections from shared subnets.**
   Run `utadm -L on`:

```
# /opt/SUNWut/sbin/utadm -L on
### Turning on Sun Ray LAN connection
NOTE: utrestart must be run before LAN connections will be allowed
```

3. **Restart Sun Ray services on the Sun Ray server.**
   Once the `utadm` command has completed, issue a `utrestart` command to fully activate Sun Ray services on the shared subnet::

```
# /opt/SUNWut/sbin/utrestart
Resetting servers... messages will be logged to /var/opt/SUNWut/log/messages.
```

Deployment on a Remote Subnet

Subnets C and D in FIGURE 7-2 are remote shared subnets.

Subnet C uses IP addresses in the range `130.146.22.0/24`. Subnet D uses IP addresses in the range `130.146.71.0/24`. The Sun Ray server named *helios* has no direct attachment to either of these subnets; it is this characteristic that defines them as remote. The answers to the three pre-deployment questions are:

1. From which DHCP server will DTUs on this subnet get their basic IP networking parameters?

   In a shared subnet scenario, the administrator must choose whether a DHCP service on the Sun Ray server or some external DHCP service will provide the DTU with basic network parameters.

If the enterprise already has a DHCP infrastructure that covers this subnet, it probably supplies basic network parameters. If no such infrastructure exists, configure the Sun Ray server to provide basic network parameters.

2. From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?

   The administrator must choose whether additional configuration parameters will be supplied to the DTU, and if so whether they will be supplied by a DHCP service on the Sun Ray server or by some external DHCP service.

   Administrators of an established DHCP infrastructure may be unable or unwilling to reconfigure it to provide additional Sun Ray configuration parameters, so it is usually more convenient to have the Sun Ray server provide them.

   Even when the established infrastructure is capable of delivering the additional parameters, it may be desirable to have the Sun Ray server provide them. This enables you to use Sun Ray Server Software commands to manage the values of the additional configuration parameters, when those values need to be changed in response to software upgrades or patch installations on the Sun Ray server. For instance, a patch that delivers new DTU firmware could automatically update the firmware version string delivered to the DTU. However, if the firmware version parameter is supplied by some external DHCP service, an administrator must manually edit the firmware version parameter string in the external DHCP configuration rules to reflect the new firmware version delivered by the patch. This kind of activity is time-consuming and error-prone as well as unnecessary.

3. How will DTUs on this subnet locate their Sun Ray server?

   Use one of the optional additional configuration parameters to report the location of the Sun Ray server to the DTU. If additional configuration parameters are not supplied to the DTU at all, the DTU cannot locate a Sun Ray server, so it tries to discover the location of a Sun Ray server by using a broadcast-based mechanism. However, the DTUs broadcast packets propagate only on the local subnet; they cannot reach a Sun Ray server located on a remote subnet, and cannot establish contact.

The next two examples illustrate representative remote shared subnet configurations. In the first example, an external DHCP service provides basic networking parameters, and the Sun Ray server provides additional parameters. This is by far the most likely configuration for a Sun Ray deployment in an enterprise that has an established DHCP infrastructure.

In the second example, basic networking parameters and a bare minimum of additional parameters—just enough to enable the DTU to contact a Sun Ray server—are supplied by an external DHCP. In this case, it is the DHCP service in a Cisco router. This scenario is less than ideal.

No firmware parameters are delivered to the DTU, so it cannot download new firmware. The administrator must make some other arrangement to provide the DTU with new firmware, for instance, by rotating it off this subnet periodically onto an interconnect or onto some other shared subnet where a full set of additional configuration parameters is offered.

Note – For examples of shared subnet deployments in which both basic networking parameters and additional parameters are delivered by the Sun Ray server and basic networking parameters are supplied by an external DHCP service (with no additional DTU parameters provided), see Directly-Connected Shared Subnet.

Remote Shared Subnet: Example 1

In this example, in which DTUs are deployed on subnet C in FIGURE 7-2, the answers to the three pre-deployment questions are:

1. From which DHCP server will DTUs on this subnet get their basic IP networking parameters?

   From an external DHCP service.

2. From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?

   From the Sun Ray server.

3. How will DTUs on this subnet locate their Sun Ray server?

   The DTUs will be informed of the location of the Sun Ray server through an additional configuration parameter delivered in Step 2.

   Use the `utadm -A` *subnet* command as follows to configure DHCP service for DTUs on a shared subnet.

1. Configure the External DHCP Service.

Determining how to configure the external DHCP infrastructure to provide basic networking parameters to the DTUs on this subnet is beyond the scope of this document. Bear in mind:

- If the external DHCP service does not have its own direct connection to this subnet, the administrator must configure a DHCP Relay Agent to deliver DHCP traffic on this subnet to the external DHCP service. The most likely location for such a Relay Agent would be on a router in this subnet, in this case the router named `r22-59` in FIGURE 7-2. For a brief introduction to this topic refer to DHCP Relay Agent.

- An existing external DHCP service may need to have its IP address allocation increased for this subnet to support the new DTUs. (This applies whenever additional DHCP clients are placed on a subnet.) It might also be desirable to reduce the lease time of addresses on this subnet so that addresses become eligible for re-use quickly.

2. **Arrange to Deliver DHCP Traffic to the Sun Ray Server.**

   Because the Sun Ray server does not have its own direct connection to this subnet, the administrator must configure a DHCP Relay Agent to deliver the subnet's DHCP traffic to the Sun Ray server. The most likely location for such a Relay Agent would be on a router in this subnet, in this case the router named `r22-59` in FIGURE 7-2. For a brief introduction to this topic refer to DHCP Relay Agent.

   If `r22-59` is running the Cisco IOS, the `ip helper-address command` can be used to activate its DHCP Relay Agent to relay DHCP broadcasts from its 10/100 Ethernet port number 4 to the Sun Ray server at `130.146.59.5`.

```
r22-59> interface fastethernet 4
r22-59> ip helper-address 130.146.59.5
r22-59>
```

   If the external DHCP service also lacks a connection to this subnet, configure a DHCP Relay Agent to forward requests from the DTU to:

   - The external DHCP service (so that the DTU can obtain basic networking parameters)
   - The DHCP service on the Sun Ray server (so that the DTU can obtain additional parameters)

   The Cisco IOS `ip helper-address` command accepts multiple relay destination addresses, so if, for instance, the external DHCP service could be contacted at `130.146.59.2` on subnet B in FIGURE 7-2, the appropriate sequence would be:

```
r22-59> interface fastethernet 4
r22-59> ip helper-address 130.146.59.2 130.146.59.5
r22-59>
```

Note – Details of the IOS interaction vary according to the specific release of IOS, the model of the router, and the hardware installed in the router.

---

3. **Configure the Sun Ray server to provide additional parameters to the shared subnet.**

   Use the `utadm -A` *subnet* command to configure DHCP service for DTUs on a shared subnet. In this example, the shared subnet has network number `130.146.22.0`, so the appropriate command is `utadm -A 130.146.22.0`.

```
# /opt/SUNWut/sbin/utadm -A 130.146.22.0
  Selected values for subnetwork "130.146.22.0"
    net mask:              255.255.255.0
    no IP addresses offered
    auth server:           130.146.59.5
    firmware server:       130.146.59.5
    router:                130.146.22.1
    alternate servers:
Accept as is? ([Y]/N): n
new netmask:[255.255.255.0]
Do you want to offer IP addresses for this subnet? (Y/[N]):
new auth server:[130.146.59.5]
new firmware server:[130.146.59.5]
new router: [130.146.22.1] 130.146.22.6
Specify alternate server list? (Y/[N]):
Selected values for subnetwork "130.146.59.0"
    net mask:              255.255.255.0
    no IP addresses offered
    auth server:           130.146.59.5
    firmware server:       130.146.59.5
    router:                130.146.22.6
    alternate servers:
Accept as is? ([Y]/N):
### Building network tables - this will take a few minutes
### Configuring firmware version for Sun Ray
All the units served by "helios" on the 130.146.22.0
network interface, running firmware other than version
"2.0_37.b,REV=2002.12.19.07.46" will be upgraded at their
next power-on.
### Configuring Sun Ray Logging Functions
### stopped DHCP daemon
### started DHCP daemon
#
```

In this example, the default values initially suggested by `utadm` were not appropriate. Specifically, the default router address to be used by DTUs on this subnet was not correct because `utadm` guesses that the address of the default router for any shared subnet will have a host part equal to 1. This was a *great* guess for the directly-connected subnet B in FIGURE 7-2, but it is not correct for subnet C.

The appropriate router address for DTUs on this subnet is `130.146.22.6` (port 4 of router `r22-59`), so the administrator replied **`n`** to the first `Accept as is?` prompt and was given the opportunity to provide alternative values for the various parameters.

4. **Restart Sun Ray services on the Sun Ray server.**

   Once the `utadm` command has completed, issue a `utrestart` command to fully activate Sun Ray services on the shared subnet:

```
# /opt/SUNWut/sbin/utrestart
Resetting servers... messages will be logged to /var/opt/SUNWut/log/messages.
```

Remote Shared Subnet: Example 2

In this example, deploying DTUs on subnet D in FIGURE 7-2, the answers to the three pre-deployment questions are:

1. From which DHCP server will DTUs on this subnet get their basic IP networking parameters?

   From an external DHCP service.

2. From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?

   The DTUs will not be supplied with the additional parameters required to support firmware download or to activate other advanced DTU features.

3. How will DTUs on this subnet locate their Sun Ray server?

   The external DHCP service will supply a single additional parameter to inform the DTU of the location of a Sun Ray server.

In this example, the Sun Ray server does not participate in DTU initialization at all. Why, then, are configuration steps required on the Sun Ray server? The Sun Ray server responds by default only to DTUs located on directly connected dedicated interconnects. It responds to DTUs on shared subnets only if the `utadm -L on` command has been executed. Running the `utadm -A` *subnet* command to activate DHCP on the Sun Ray server for a shared subnet, as in this example, implicitly executes `utadm -L on`. If `utadm -A` *subnet* has not been run, the administrator must run `utadm -L on` manually to allow the server to offer sessions to DTUs on the shared subnet.

1. **Configure the External DHCP Service.**

   Determining how to configure the external DHCP infrastructure to provide basic networking parameters to the DTUs on this subnet is beyond the scope of this document. However, for this example, assume that DHCP service is provided by

Cisco IOS-based router `r22-71` in FIGURE 7-2, attached to the `130.146.71.0` subnet through its 10/100 Ethernet port 3. This router can be configured to provide basic networking parameters and the location of a Sun Ray server as follows:

```
r22-71> interface fastethernet 3
r22-71> ip dhcp excluded-address 130.146.71.1 130.146.71.15
r22-71> ip dhcp pool CLIENT
r22-71/dhcp> import all
r22-71/dhcp> network 130.146.71.0 255.255.255.0
r22-71/dhcp> default-router 130.146.71.4
r22-71/dhcp> option 49 ip 130.146.59.5
r22-71/dhcp> lease 0 2
r22-71/dhcp> ^Z
r22-71>
```

Note – Details of the IOS interaction vary according to the specific release of IOS, the model of router and the hardware installed in the router.

DHCP option 49, the standard option of the *X Window Display Manager*, identifies `130.146.59.5` as the address of a Sun Ray server. In the absence of `AltAuth` and `Auth-Srvr` vendor-specific options, the DTU tries to find a Sun Ray server by broadcasting on the local subnet. If the broadcasts evoke no response, the DTU uses the address supplied in t option of the *X Window Display Manager*—provided that the DTU contains firmware at Sun Ray Server Software 2.0 patch level 114880-01 or later.

Note – This is an unorthodox use of the option of the *X Window Display Manager*, but in a remote subnet deployment where vendor-specific options can not be delivered, it may be the only way of putting a DTU in touch with a server.

---

2. **Configure the Sun Ray server to accept DTU connections from shared subnets by running** `utadm -L on`**.**

```
# /opt/SUNWut/sbin/utadm -L on
### Turning on Sun Ray LAN connection
NOTE: utrestart must be run before LAN connections will be allowed
#
```

3. **Restart Sun Ray services on the Sun Ray server.**

   Once the utadm command has completed, issue a `utrestart` command to fully activate Sun Ray services on the shared subnet:

```
# /opt/SUNWut/sbin/utrestart
Resetting servers... messages will be logged to
/var/opt/SUNWut/log/
messages.
#
```

TABLE 7-2 lists the vendor-specific DHCP options that Sun Ray defines and uses.

TABLE 7-2 Vendor-specific DHCP Options

Parameter Name	Client Class	Option Code	Data Type	Optional/ Mandatory	Granularity	Max Count	Comments
AltAuth	SUNW.NewT.SUNW	35	IP	Optional	1	0	List of Sun Ray server IP addresses
AuthSrvr	SUNW.NewT.SUNW	21	IP	Mandatory	1	1	Single Sun Ray server IP addresses
AuthPort	SUNW.NewT.SUNW	22	NUMBER	Optional	2	1	Sun Ray server port
NewTVer	SUNW.NewT.SUNW	23	ASCII	Optional	1	0	Desired firmware version
FWSrvr	SUNW.NewT.SUNW	31	IP	Optional	1	1	Firmware TFTP server IP address
BarrierLevel	SUNW.NewT.SUNW	36	NUMBER	Mandatory	4	1	Firmware Download: barrier level
LogHost	SUNW.NewT.SUNW	24	IP	Optional	1	1	Syslog server IP address
LogKern	SUNW.NewT.SUNW	25	NUMBER	Optional	1	1	Log level for kernel
LogNet	SUNW.NewT.SUNW	26	NUMBER	Optional	1	1	Log level for network
LogUSB	SUNW.NewT.SUNW	27	NUMBER	Optional	1	1	Log level for USB
LogVid	SUNW.NewT.SUNW	28	NUMBER	Optional	1	1	Log level for video
LogAppl	SUNW.NewT.SUNW	28	NUMBER	Optional	1	1	Sun Rat server interface name
Intf	SUNW.NewT.SUN	29	ASCII	Optional	1	0	Sun Ray server interface name
NewTBW		30	NUMBER	Optional	4	1	Bandwidth cap
NewTDispIndx	SUNW.NewT.SUNW	32	NUMBER	Optional	4	1	Obsolete. Do not use.
NewTFlags	SUNW.NewT.SUNW	34	NUMBER	Optional	4	1	Obsolete. Do not use.

The DTU can perform its basic functions even if none of these options are delivered during initialization, but some advanced DTU features do not become active unless certain options are delivered to the DTU. In particular:

- `AltAuth` and `AuthSrvr` indicate the IP addresses of Sun Ray servers. Addresses in the `AltAuth` list are tried in order until a connection is established. Current firmware ignores `AuthSrvr` if `AltAuth` is provided, but it is good practice always to specify `AuthSrvr` for the benefit of old (pre Sun Ray Server Software 1.3) firmware, which does not understand the `AltAuth` option. If neither of these

options is supplied, the DTU tries to locate a Sun Ray server by sending broadcasts on the local subnet. If the DTU contains firmware at Sun Ray Server Software 2.0 patch level 114880-01 or later, it resorts to trying to contact a Sun Ray server at the address supplied in the option of the `X Window Display Manager` if that option has been provided.

- `NewTVer` and `FWSrvr` must both be provided in order for the DTU to attempt a firmware download. `NewTVer` contains the name of the firmware version that the DTU should use. If this name does not match the name of the firmware version that the DTU is actually running, the DTU tries to download the desired firmware from a TFTP server at the address given by `FWSrvr`.
- `LogHost` must be specified in order for the DTU to report messages through the syslog protocol. Reporting thresholds for major DTU subsystems are controlled by the `LogKern, LogNet, LogUSB, LogVid`, and `LogAppl` options.

Note – The message formats, contents, and thresholds are intended for use only by service personnel and are not documented intentionally.

The DHCP Client Class name for all Sun Ray vendor-specific options is `SUNW.NewT.SUNW`. The DTU cites this name in DHCP requests so that the server can respond with the appropriate set of vendor-specific options. This mechanism guarantees that the DTU is not given vendor options defined for some other type of equipment and that other equipment is not given options that are meaningful only to the DTU.

Network Performance Requirements

This section describes the minimal network infrastructure needed to support a Sun Ray implementation.

Packet Loss

Before version 2.0, Sun Ray Server Software was intolerant of packet losses, so it was recommended that packet loss not exceed 0.1 percent over any extended period. However, because this is often an impractical requirement in local area (LAN) and wide area (WAN) network Sun Ray deployments, the Sun Ray Server Software has been made much more robust in the face of packet loss. The first version of this improved software was released with the first 2.0 patch, with additional improvements in releases supporting low-bandwidth WAN Sun Ray deployments.

In earlier versions, the server tried to avoid packet loss by severely limiting its use of available bandwidth whenever it encountered packet loss. Because random losses are inevitable in a non-dedicated LAN or WAN network environment, this approach put unnecessary limits on performance.

Sun Ray Server Software has always had the capability to detect and recover quickly from such losses, so avoiding them was a matter of policy more than necessity. The new software is less timid and avoids operating at bandwidth levels that create packet losses. Instead, it tries to send data at the highest possible rate that it can without incurring large losses. By design, it sometimes sends data at a rate that is too great for the capacity of the connection between the server and the client, and thus discovers what that capacity is. With very high demand, sustained packet losses of up to 10 percent may sometimes be seen, but the software continues to operate and update the contents of the screen correctly nevertheless.

Latency

Network latency between any Sun Ray client and its server is an important determinant of the quality of the user experience. The lower the latency, the better; latencies under 50 milliseconds for round trip delay are preferred. However, like familiar network protocols such as TCP, the Sun Ray DTU does tolerate higher latencies, but with degraded performance. Latencies up to 150 milliseconds provide usable, if somewhat sluggish, performance.

Out-of-Order Packets

DTUs that contain Sun Ray Server Software 2.0 firmware or later can tolerate small occurrences of out-of-order packet delivery, such as might be experienced on an Internet or wide-area intranet connection. Current Sun Ray firmware maintains a reordering queue that restores the correct order to packets when they are received out of order. In releases prior to Sun Ray Server Software 2.0, out-of-order packets were simply discarded.

Troubleshooting Tools

`utcapture`

The `utcapture` utility connects to the Sun Ray Authentication Manager and reports packet loss statistics and round-trip latency timings for each DTU connected to this server. See the `utcapture` man page to learn more about this command.

`utquery`

The `utquery` command interrogates a DTU and displays the DTUs initialization parameters along with the IP addresses of the DHCP services that supplied those parameters. It can be helpful in determining whether a DTU was able to obtain the parameters that were expected in a particular deployment and in determining specific DHCP servers that contributed to the DTUs initialization. See the `utquery` man page to learn more about this command.

OSD Icons

Sun Ray DTU on-screen display (OSD) icons contain information that can help the administrator understand and debug network configuration problems. The amount of information encoded into the icons has been significantly expanded in the firmware delivered with Sun Ray Server Software. The icon structure and progression are described in detail in Appendix .

CHAPTER 9

Multihead Administration

The multihead feature on Sun Ray™ DTUs enables users to control separate applications on multiple screens, or *heads*, using a single keyboard and pointer device attached to the primary DTU. Users can also display and control a single application, such as a spreadsheet, on multiple screens. System administrators create multihead groups that may be accessed by users. A multihead group, consisting of between two and 16 DTUs controlled by one keyboard and mouse, may be composed of Sun Ray 1, Sun Ray 100, and Sun Ray 150 DTUs. Each DTU presents an X screen of the multihead X display.

Note – For the multihead feature to function properly:
1. You must be in administered mode; therefore, you must run `utconfig` before you run `utmhconfig` and `utmhadm.`
2. You must enable the multihead policy using either `utpolicy` or the Admin GUI.
3. Always run `utmhconfig` from a Sun Ray DTU.

By default, when the user logs into a multihead group, the user gets a multihead session using the number of screens available in that group. The resolution for the group is automatically set to the largest supported resolution of the primary DTU, which is the DTU that controls the other DTUs in the group and to which all peripherals are attached. Auto-size can be turned off and the Xserver size can be changed using the `utxconfig` command. Because auto-size affects X display dimensions as well as the initial multihead session group geometry, the user might experience panning or black-band effects.

The user can explicitly choose not to use multiple screens for a session by executing the `utxconfig -m off` command. The user can also choose a particular number of screens in a particular geometry by executing (in the following order):

- the `utxconfig -s off` command to disable autosize
- the `utxconfig -R` *geometry* command to have it take effect

When the user moves the mouse pointer past the edge between two screens, it moves from one screen to the next. The geometry of the multihead group determines which screen is displayed.

Multihead Groups

A multihead group is comprised of a set of associated Sun Ray DTUs controlled by a primary DTU to which a keyboard and pointer device, such as a mouse, are connected. This group, which can contain a maximum of 16 DTUs, is connected to a single session.

Unless XINERAMA is enabled (see "XINERAMA" on page 159 for more details), sessions will have a separate CDE toolbar (with separate workspaces) per screen. A window cannot be moved between screens.

The primary DTU hosts the input devices, such as a keyboard and a pointer device, and the USB devices associated with the session. The remaining DTUs, called the secondaries, provide the additional displays. All peripherals are attached to the primary DTU, and the group is controlled from the primary DTU.

Multihead groups can be created easily by using a smart card to identify the terminals with the `utmhconfig` GUI utility.

Tip – For best results, run `utmhconfig` only from a DTU.

However, if you disconnect the secondary DTUs without deleting the multihead group to which they belong, the screens are not displayed on the single primary DTU. The primary DTU is still part of the multihead group, and the mouse seems to get lost when it goes to the disconnected secondary DTU. To recover from this situation, you can either reconnect the missing DTU or delete the multihead group using the `utmhconfig` or `utmhadm` command, or you can delete the multihead group, replace the missing DTU, and create a new multihead group that incorporates the replacement DTU.

Multihead Screen Display

When the multihead feature is used, a small window indicating the current session on each screen is displayed with the current screen highlighted for easy identification. This window is automatically displayed for users during session creation. For example, the display in "XINERAMA" on page 159 indicates that the user is on the second screen of a three-screen display.

FIGURE 9-1 The Multihead Screen Display

Display Resolution

To avoid panning, all the monitors in a workgroup must support the same resolution.

The auto-size feature sets the user's X server display dimensions automatically to match the preferred resolution supported by the primary DTU when the session is created. This resolution will be the optimum resolution for the multihead group. This feature can be turned off and on using the `utxconfig` command. The default geometry, which is the number of rows and columns in the multihead group, and the screen order are also automatically set when a session is created. This feature can be turned off and on using the `utxconfig` command.

If auto-size is on when you create a session on a 2x1 multihead group, the result is a 2x1 session. If auto-size is turned off, the size of the session is whatever you designate. For instance, if auto-size is off and the geometry is set to 3x1, then even if you log in to a 2x1 multihead group (or even a non-multihead, 1x1 terminal), you will get a 3x1 session with screen flipping. This might be useful if you know you are going to hot desk to a 3x1 multihead group in the future and want to take full advantage of it when you get there.

Note – If the resolutions of the monitors differ, you may have problems with unwanted on-screen movement called *panning*, or large *black bands* around the visible screen area.

Multihead Administration Tool

The administration tool for the multihead feature displays the current multihead groups and enables you to create new groups.

▼ To Turn On Multihead Policy From the Command Line

- **On the command-line interface, type:**

```
# /opt/SUNWut/sbin/utpolicy -a -m -g your_policy_flags
# /opt/SUNWut/sbin/utrestart
```

This enables the multihead policy for the failover group and restarts Sun Ray Server Software with the new policy on the local server without disrupting existing sessions.

Tip – Issue the `utrestart` command on every server in the failover group.

▼ To Turn On Multihead Policy Using the Administration Tool

1. **Bring up the Administration Tool by typing the following URL into your browser's location field:**

```
http://hostname:1660
```

2. **Select Admin from the navigation menu on the left side of the tool.**
3. **Select Policy.**
4. **Next to Multihead feature enabled, click the Yes radio button.**
5. **Click the Apply button.**
6. **Under Admin in the lefthand menu, select Reset Services.**
7. **Click the Restart button.**

   This sets the multihead policy for all servers and restarts Sun Ray Server Software on all servers.

▼ To Create a New Multihead Group

1. **On the command-line interface, type:**

```
# /opt/SUNWut/sbin/utmhconfig
```

2. **On the initial screen, click Create New Group.**

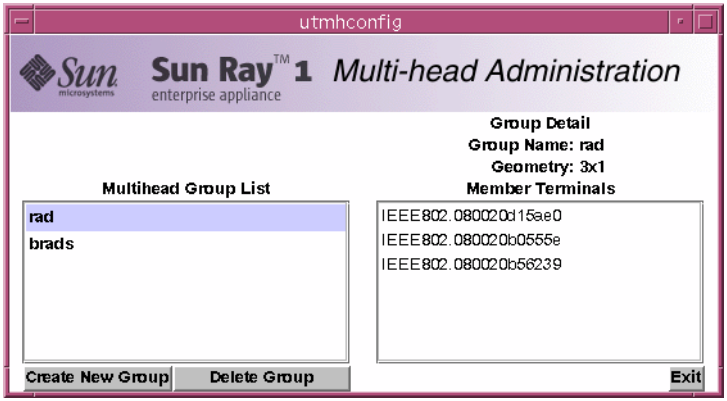


FIGURE 9-2 Multihead Group List With Group Detail

The Create New Multiheaded Group pop-up dialog box is displayed. The number of rows and the number of columns you enter are displayed as the group geometry when the group has been created.

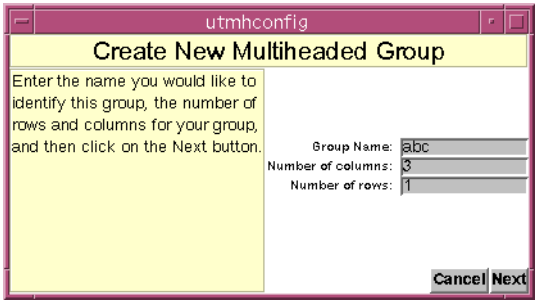


FIGURE 9-3 Create New Multiheaded Group Pop-up Dialog Box

3. **Enter the information for the group.**

   Enter a name for the group and the number of rows and columns.

4. **Click the Next button.**

   A third screen is displayed.

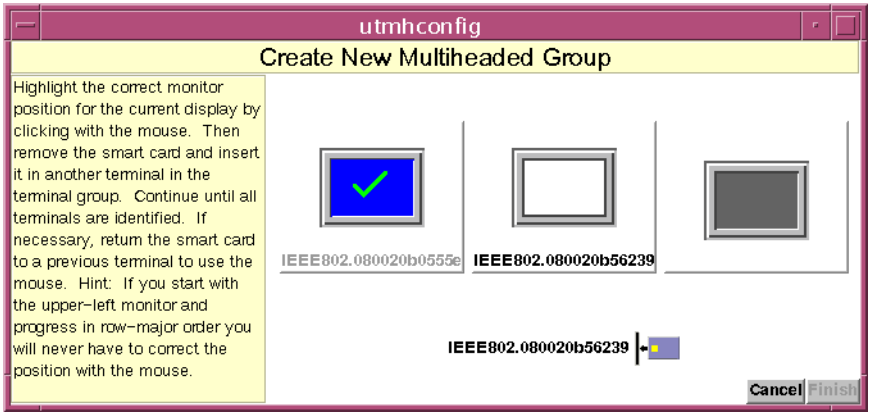


FIGURE 9-4 Setup Display for the New Multihead Group

5. **Select the DTUs within the multihead group and insert a smart card in each Sun Ray DTU in turn to establish the order of the group.**

   The Finish button, which was previously grayed out, is now active.

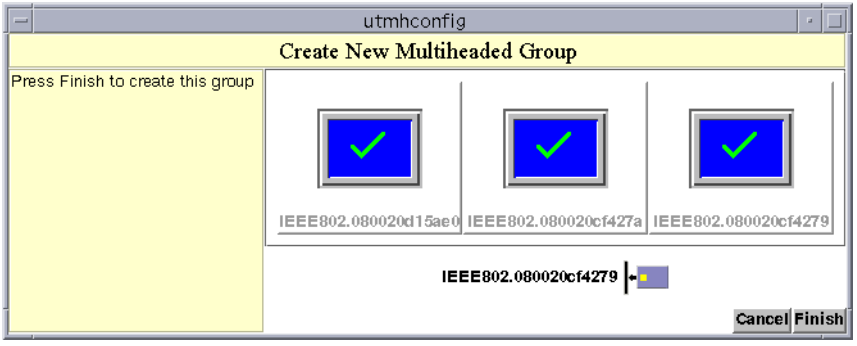


FIGURE 9-5 Completed Multihead Group List With Active Finish Button

6. **Click the Finish button.**
7. **Exit the session or disconnect by removing your card.**

XINERAMA

The XINERAMA extension to X11creates one single large screen displayed across several monitors. With XINERAMA only one toolbar is displayed, and a window can be moved smoothly from one part of the screen to the next.

A single CDE toolbar (and set of workspaces) manages the configured monitors. A window can span monitors, since they are still within the same screen. This includes the CDE toolbar itself.

Tip – Because XINERAMA consumes a lot of CPU, memory and network bandwidth, please set the `shmsys:shminfo_shmmax` parameter in the `/etc/system` file to at least *LARGEST_NUMBER_OF_HEADS * width * height * 4* for reasonable performance.

Users enable or disable XINERAMA as part of their X preferences. The `utxconfig` command handles this on an individual token basis. The user must log off for this to take effect.

The XINERAMA feature is enabled using the following command:

```
% /opt/SUNWut/bin/utxconfig -x on
```

The XINERAMA feature is disabled using the following command:

```
% /opt/SUNWut/bin/utxconfig -x off
```

To enable as default for a single system or failover group, as superuser, type the following command:

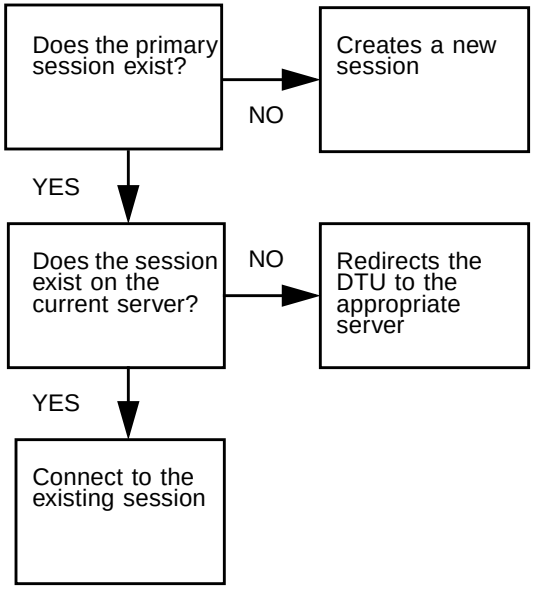
```
% utxconfig -a -x on
```

Session Groups

If you hot desk from a multihead group to a DTU that is not part of a multihead group—that is, a DTU with a single head—all the screens created in the original multihead group can be viewed on the single screen or head by panning to each screen in turn. This is called *screen flipping*.

Authentication Manager

The TerminalGroup policy module extends the Authentication Manager to support multihead groups. When a DTU connects to the Authentication Manager or a new smart card is inserted, the TerminalGroup module queries its database to determine whether the DTU is part of a multihead group and, if so, whether the DTU is a primary or secondary DTU of that group. If it is not identified as part of a multihead group, the DTU is treated normally.



This flow chart asks the following questions:

FIGURE 9-6 Authentication Manager Flowchart for the Primary DTU

If the DTU is determined to be part of a multihead group and it is the multihead group's primary DTU, a normal session placement occurs. If a session does not exist on the current server, but there is a preexisting session for the DTU or smart card on another server in the failover group, the primary DTU will be redirected to that server. If there is no session on any server, the request for a session is directed to the least-loaded server and a session is created there.

If a DTU is determined to be part of a multihead group and it is a multihead group secondary DTU, the TerminalGroup module determines if the multihead- group primary DTU is locally attached to a session. If it is, it tells the Session Manager to allow the secondary DTU to also attach to that session. If the primary DTU is not attached locally, the TerminalGroup module determines if the primary DTU is attached to another server in the failover group (if any), and if it is, it redirects the secondary DTU to that server.

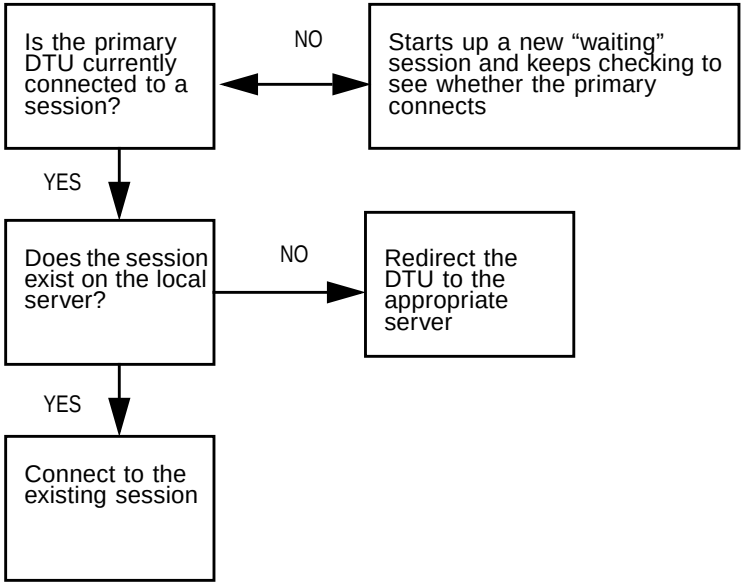


FIGURE 9-7 Authentication Manager Flowchart for the Secondary DTU

If the primary DTU is determined to not be attached to any server in the failover group at that moment, a "waiting for primary" icon is displayed on the DTU, and further activity is blocked on that DTU until the primary is discovered. The secondary DTU is redirected to the server to which the primary is attached.

CHAPTER 11

Failover Groups

Sun Ray servers configured in a failover group provide users with a high level of availability when one of those servers becomes unavailable because of a network or system failure. This chapter describes how to configure failover groups

This chapter covers these topics:

Failover Group Overview

A failover group consists of two or more Sun Ray servers grouped together to provide highly-available and scalable Sun Ray service for a population of Sun Ray DTUs. Releases earlier than 2.0 supported DTUs available to the servers only on a common, dedicated interconnect. Beginning with the 2.0 release, this capability was expanded to allow access across the LAN to either local or remote Sun Ray devices. However, there is still a requirement for the servers in a failover group to be able to reach one another, using multicast or broadcast, over at least one shared subnet. Servers in a group authenticate (or "trust") one another using a common group signature. The group signature is a key used to sign messages sent between servers in the group; it must be configured to be identical on each server.

Failover groups that use more than one version of Sun Ray Server Software will be unable to use all the features provided in the 2.0 and 3 releases. On the other hand, the failover group can be a heterogeneous group of Sun servers.

When a dedicated interconnect is used, all servers in the failover group should have access to, and be accessible by, all the Sun Ray DTUs on a given sub-net. The failover environment supports the same interconnect topologies that are supported by a single-server Sun Ray environment. However, switches should be multicast-enabled.

FIGURE 11-1 illustrates a typical Sun Ray failover group. For an example of a redundant failover group, see FIGURE 11-2.

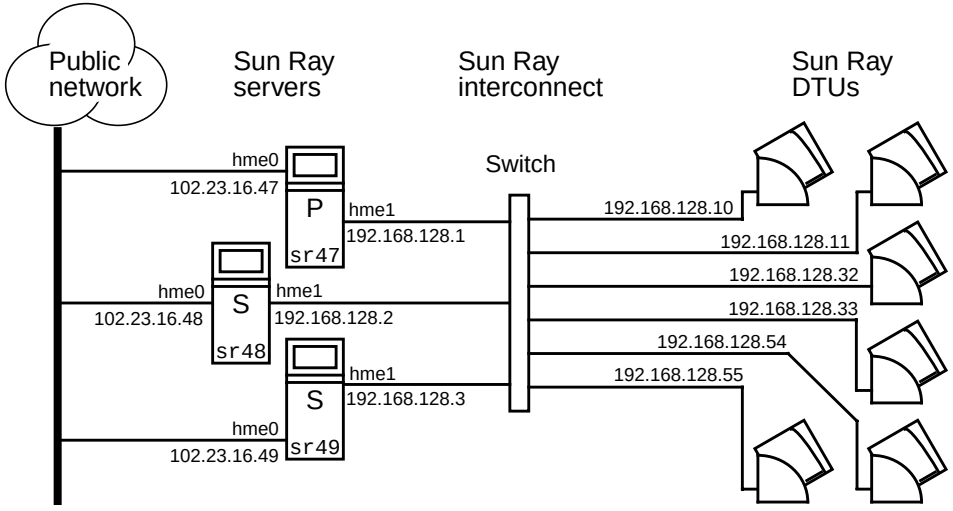


FIGURE 11-1 Simple Failover Group

When a server in a failover group fails for any reason, each Sun Ray DTU connected to that server reconnects to another server in the same failover group. The failover occurs at the user authentication level; the DTU connects to a previously existing session for the user's token. If there is no existing session, the DTU connects to a server selected by the load-balancing algorithm. This server then presents a login screen to the user and 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:

- Group Manager—A module that monitors the availability (liveness) of the Sun Ray servers and facilitates redirection when needed.
- Multiple, coexisting Dynamic Host Configuration Protocol (DHCP) servers—All DHCP servers configured to assign IP addresses to Sun Ray DTUs have a non-overlapping subset of the available address pool.

Note – The failover feature cannot work properly if the IP addresses and DHCP configuration data are not set up properly when the interfaces are configured. In particular, if the Sun Ray server's interconnect IP address is a duplicate of any other server's interconnect IP address, the Sun Ray Authentication Manager throws "Out of Memory" errors.

The redundant failover group illustrated in FIGURE 11-2 can provide maximum resources to a few Sun Ray DTUs. The server `sr47` is the primary Sun Ray server and `sr48` is the secondary Sun Ray server; other secondary servers (`sr49`, `sr50...` are not shown.

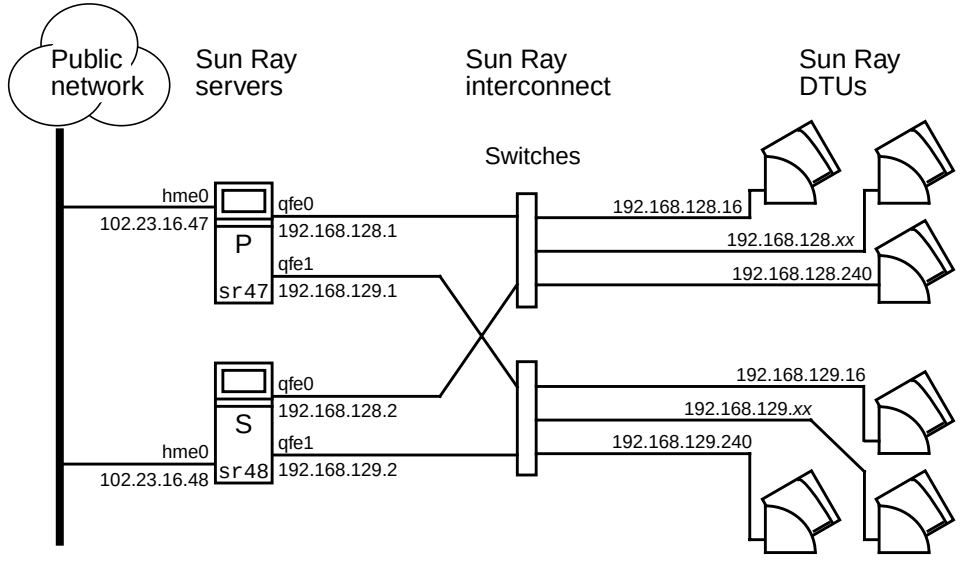


FIGURE 11-2 Redundant Failover Group

Setting Up IP Addressing

The `utadm` command assists 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. For more information on using the `utadm` command, see the man page for `utadm`.

Before setting up IP addressing, you must decide upon an addressing scheme. The following examples discuss setting up class C and class B addresses.

Setting Up Server and Client Addresses

The loss of a server usually implies the loss of its DHCP service and its allocation of IP addresses. Therefore, more DHCP addresses must be available from the address pool than there are Sun Ray DTUs. Consider the situation of 5 servers and 100 DTUs. If one of the servers fails, the remaining DHCP servers must have enough available addresses so that all "orphaned" DTUs get a new working address.

TABLE 11-1 describes how to configure five servers for 100 DTUs, accommodating the failure of two servers (class C) or four servers (class B).

TABLE 11-1 Configuring Five Servers for 100 DTUs

	Class C (2 Servers Fail)		Class B (4 Servers Fail)	
Servers	Interface Address	DTU Address Range	Interface Address	DTU Address Range
`serverA`	192.168.128.1	192.168.128.16 to 192.168.128.49	192.168.128.1	192.168.128.16 to 192.168.128.116
`serverB`	192.168.128.2	192.168.128.50 to 192.168.128.83	192.168.129.1	192.168.129.16 to 192.168.129.116
`serverC`	192.168.128.3	192.168.128.84 to 192.168.128.117	192.168.130.1	192.168.130.16 to 192.168.130.116
`serverD`	192.168.128.4	192.168.128.118 to 192.168.128.151	192.168.131.1	192.168.131.16 to 192.168.131.116
`serverE`	192.168.128.5	192.168.128.152 to 192.168.128.185	192.168.132.1	192.168.132.16 to 192.168.132.116

The formula for address allocation is: address range (AR) = number of DTUs/(total servers - failed servers). For example, in the case of the loss of two servers, each DHCP server must be given a range of 100/(5-2) = 34 addresses.

Ideally, each server would have an address for each DTU. This would require a class B network. Consider these conditions:

- If AR multiplied by the total number of servers is *less than or equal to* 225, configure for a class C network
- If AR multiplied by the total number of servers is *greater than* 225, configure for a class B network

---

Tip – If all available DHCP addresses are allocated, it is possible for a Sun Ray DTU to request an address yet not find one available, perhaps because another unit has been allocated IP addresses by multiple servers. To prevent this condition, give each DHCP server enough addresses to serve the all the DTUs in a failover group.

Server Addresses

Server IP addresses assigned for the Sun Ray interconnect should all be unique. Use the `utadm` tool to assign them.

When the Sun Ray DTU boots, it sends a DHCP broadcast request to all possible servers on the network interface. One (or more) server responds with an IP address allocated from its range of addresses. The DTU 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 numbers of the Authentication Managers on the server that sent the response.

The DTU then attempts to establish a TCP connection to an Authentication Manager on that server. If it is unable to connect, it uses a protocol similar to DHCP in which it uses a broadcast message to ask the Authentication Managers to identify themselves. The DTU then attempts to connect to the Authentication Managers that responded in the order in which the responses were received.

Note – For the broadcast feature enabled, the broadcast address (255.255.255.255) must be the last one in the list. Any addresses after the broadcast address are ignored. If the local server is not in the list, Sun Ray DTUs cannot attempt to contact it.

Once a TCP connection to an Authentication Manager has been established, the DTU presents its token. The token is either a pseudo-token representing the individual DTU (its unique Ethernet address) or a smart card. The Session Manager then starts an X window/X server session and binds the token to that session.

The Authentication Manager then sends a query to all of the other Authentication Managers on the same subnet 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 DTU to that server. If no session is found for the token, the requesting Authentication Manager selects the server with the lightest load and redirects the token to that server. A new session is created for the token.

The Authentication Manager enables both implicit (smart card) and explicit switching. For explicit switching, see "Group Manager" on page 186.

Configuring DHCP

In a large IP network, a DHCP server distributes the IP addresses and other configuration information for interfaces on that network.

Coexistence of the Sun Ray Server With Other DHCP Servers

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 the Sun Ray DHCP server from other DHCP traffic. Verify that all routers on the network are configured not to relay DHCP requests. This is the default behavior for most routers.

Caution – If the IP addresses and DHCP configuration data are not set up correctly when the interfaces are configured, the failover feature cannot work properly. In particular, configuring the Sun Ray server's interconnect IP address as a duplicate of any other server's interconnect IP address may cause the Sun Ray Authentication Manager to throw "Out of Memory" errors.

Administering Other Clients

The Sun Ray interconnect is intended to be private. No devices other than switches and Sun Ray DTUs should reside on the interconnect. 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.

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

1. **Log in to the Sun Ray server as superuser and, open a shell window. Type:**

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

where <*interface_name*> is the name of the Sun Ray network interface to be configured; for example, `hme[0-9]`, `qfe[0-9]`, or `ge[0-9]`. You must be logged on as superuser 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:          serverB-hme1
    net name:           SunRay-hme1
    first unit address: 192.168.128.16
    last unit address:  192.168.128.240
    firmware server:    192.168.128.1
    router:             192.168.128.1
    alternate servers:
```

The default values are the same for each server in a failover group. Certain values must be changed to be unique to each server.

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

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

3. **Change the second server's IP address to a unique value, 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: [serverB-hme1]
```

5. **Change the DTU address ranges for the interconnect to unique values. For example:**

```
Do you want to offer IP addresses for this interface? [Y/N]:
new first Sun Ray address: [192.168.128.16] 192.168.128.50
number of Sun Ray addresses to allocate: [205] 34
```

6. **Accept the default firmware server and router values:**

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

The `utadm` script asks if you want to specify an alternate server list:

```
Specify alternate server list?  (Y/[N]): n
```

These servers are specified by a file containing a space-delimited list of server IP addresses or by manually entering the server IP addresses.

Note – Under most conditions, an alternate server list is not required.

The newly selected values for interface `hme1` are displayed:

```
Selected values for interface "hme1"
    host address:       192.168.128.2
    net mask:           255.255.255.0
    net address:        192.168.128.0
    host name:          serverB-hme1
    net name:           SunRay-hme1
    first unit address: 192.168.128.50
    last unit address:  192.168.128.83
    firmware server:    192.168.128.2
    router:             192.168.128.2
    alternate servers:
```

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

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

8. **Stop and restart the server and power cycle the DTUs to download the firmware.**

TABLE 11-2 lists the options available for the `utadm` command. For additional information, see the `utadm` man page.

TABLE 11-2 Available Options

Option	Definition
-c	Create a framework for the Sun Ray interconnect.
-r	Remove all Sun Ray interconnects.
-A <*subnetwork*>	Configure the subnetwork specified as a Sun Ray sub-network. This option only configures the DHCP service to allocate IP address and/or to provide Sun Ray parameters to Sun ray clients. It also will automatically turn on support for LAN connections from a shared subnetwork.
-a <*interface_name*>	Add <*interface_name*> as Sun Ray interconnect.
-D <*subnetwork*>	Delete the subnetwork specified form the list of configured Sun Ray subnetworks.
-d <*interface_name*>	Delete <*interface_name*> as Sun Ray interconnect.
-l	Print the current configuration for all the Sun Ray subnetworks, including remote subnetworks.
-p	Print the current configuration.

TABLE 11-2 Available Options *(Continued)*

Option	Definition
-f	Take a server offline
-n	Bring a server online
-x	Print the current configuration in a machine-readable format

Group Manager

Every server has a group manager module that monitors availability and facilitates redirection. It is coupled with the Authentication Manager.

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

Warning – The same policy must exist on every server in the failover group or undesirable results might occur.

Each Group Manager creates maps of the failover group topology by exchanging `keepalive` messages among themselves. These `keepalive` messages are sent to a well-known UDP port (typically 7009) to all of the configured network interfaces. The `keepalive` message contains enough information for each Sun Ray 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` message contains the following information about the server:

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

Note – The last two items are used to facilitate load distribution. See "Load Balancing" on page 188.

The information maintained by the Group Manager is used primarily for server selection when a token is presented. The server and subnet information is used to determine the servers to which a given DTU can connect. These servers are queried about sessions belonging to the token. Servers whose last `keepalive` message is older than the timeout are deleted from the list, since either the network connection or the server is probably down.

Redirection

In addition to automatic redirection at authentication, you can use the `utselect` graphical user interface (GUI) or `utswitch` command for manual redirection.

Note – The `utselect` GUI is the preferred method to use for server selection. For more information, see the `utselect` man page.

Group Manager Configuration

The Authentication Manager configuration file, `/etc/opt/SUNWut/auth.props`, contains properties used by the Group Manager at runtime. The properties are:

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

These properties have default values that are rarely changed. Only very knowledgeable Sun support personnel should direct customers to change these values to help tune or debug their systems. If any properties are changed, they must be changed for all servers in the failover group, since the `auth.props` file must be the same on all servers in a failover group.

▼ To Restart the Authentication Manager

Property changes do not take effect until the Authentication Manager is restarted.

- **As superuser, open a shell window and type:**

```
# /opt/SUNWut/sbin/utrestart
```

The Authentication Manager is restarted.

Load Balancing

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 servers. The load balancing algorithm 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 DTU and finds that no server owns an existing session for that token, it redirects the Sun Ray DTU to the server in the group with the lightest load. It is possible that a Sun Ray DTU appears to connect 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 Balancing Feature

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

```
enableLoadBalancing = false
```

Setting Up a Failover Group

A failover group is one in which two or more Sun Ray servers use a common policy and share services. It is composed of a primary server and one or more secondary servers. For such a group, you must configure Sun Ray Data Store to enable replication of the Sun Ray administration data across the group.

The `utconfig` command sets up the internal database for a single system initially, and enables the Sun Ray servers for failover. The `utreplica` command then configures the Sun Ray servers as a failover group.

Log files for Sun Ray servers contain time-stamped error messages which are difficult to interpret if the time is out of sync. To make troubleshooting easier, all secondary servers should periodically synchronize with their primary server.

Tip – Use `rdate <primary-host>`, preferably with `crontab`, to synchronize secondary servers with their primary server.

Primary Server

Layered administration of the group takes place on the primary server. The `utreplica` command designates a primary server, advises the server of its Administration Primary status, and tells it the host names of all the secondary servers.

Tip – Configure the primary server before you configure the secondary servers.

▼ To Specify a Primary Server

- **As a superuser, open a shell window on the primary server and type:**

```
# /opt/SUNWut/sbin/utreplica -p secondary-server1 [secondary-server2 ...]
```

where *secondary_server1 [secondary_server2...]* is a space-separated list of unique host names of the secondary servers.

Secondary Server

The secondary servers in the group store a replicated version of the primary server's administration data. Use the `utreplica` command to advise each secondary server of its secondary status and also the host name of the primary server for the group.

▼ To Specify Each Secondary Server

- **As superuser, open a shell window on the secondary server and type:**

```
# /opt/SUNWut/sbin/utreplica -s primary-server
```

where *primary-server* is the hostname of the primary server.

▼ To Add Additional Secondary Servers

To include an additional secondary server in an already configured failover group:

1. **On the primary server, rerun `utreplica -p -a` with a list of secondary servers.**

```
# /opt/SUNWut/sbin/utreplica -p -a secondary-server1, secondary-server2,...
```

2. **Run `utreplica -s` *primary-server* on the new secondary server.**

```
# /opt/SUNWut/sbin/utreplica -s primary-server
```

Removing Replication Configuration

▼ To Remove the Replication Configuration

- **As superuser, open a shell window and type:**

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

This removes the replication configuration.

Viewing the Administration Status

▼ To Show Current Administration Configuration

- **As superuser, open a shell window and type:**

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

The result indicates whether the server is standalone, primary (with the secondary host names), or secondary (with the Primary host name).

Viewing Failover Group Status

A failover group is a set of Sun Ray servers all running the same release of Sun Ray Server Software and all having access to all the Sun Ray DTUs on the interconnect.

▼ To View Failover Group Status

1. **From the navigation menu in the Admin GUI, select the arrow to the left of Failover Group to expand the menu.**

2. **Click the Status link.**

   The Failover Group Status window is displayed.

   The Failover Group Status window describes the health and current state of multiple Sun Ray servers within your failover group. This window also describes the health of any Sun Ray servers that have responded to a Sun Ray broadcast.

   The Failover Group Status window provides information on group membership and network connectivity. The servers are listed by name in the first column. Failover Group Status only displays public networks and Sun Ray interconnect fabrics.

   In FIGURE 11-3 the information provided is from the point of view of the server in the upper left hand of the table. In this example the server is nomad-100.

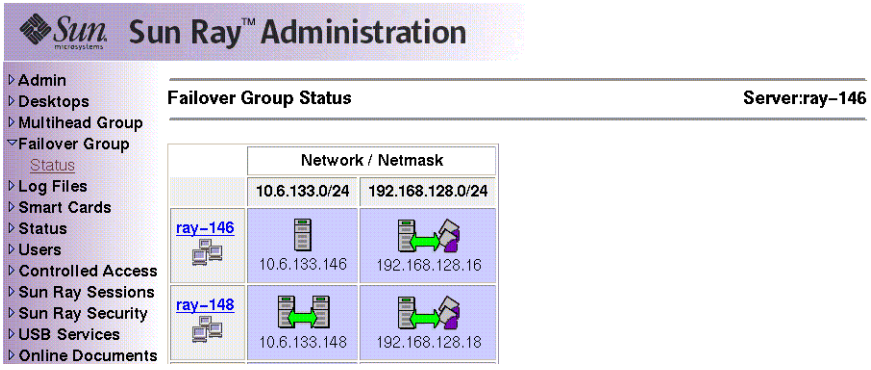


FIGURE 11-3 Failover Group Status Table

Note – Sun Ray server broadcasts do not traverse over routers or servers other than Sun Ray servers.

Sun Ray Failover Group Status Icons

These icons depict current failover group status:

TABLE 11-3 Failover Group Status Icons

Icons	Description
	Information is displayed from the perspective of the system performing the failover status.
	A failover group is established and functioning properly. The trusted hosts are members of this failover group because they share the same group signature.
	A Sun Ray interconnect fabric is established and functioning properly.
	This Sun Ray interconnect fabric is unreachable from the server performing the failover group status. This may indicate a failure in the interconnect fabric between Sun Ray servers if they are supposed to be on the same interconnect. In the past, this host was reachable but is no longer from the point of view of the system performing failover status.
	The servers are unreachable. This network is unreachable from the server performing the Failover Group Status. This could be an alert situation. Over a public network the conditions could be normal, except for the Sun Ray broadcast information, which cannot traverse over routers.
	Servers that appear in the same group use this icon. The signature files, `/etc/opt/SUNWut/gmSignature`, on those two machines are identical. This icon identifies systems as trusted hosts. Failover occurs for any Sun Ray DTUs connected between these systems. The `utgroupsig` utility is used to set the `gmSignature` file.

Recovery Issues and Procedures

If one of the servers of a failover group fails, the remaining group members operate from the administration data that existed prior to the failure.

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

Note – When the primary server fails, you cannot make administrative changes to the system. For replication to work, all changes must be successful on the primary server.

Primary Server Recovery

There are several strategies for recovering the primary server. The following procedure is performed on the same server which was the primary after making it fully operational.

▼ To Rebuild the Primary Server Administration Data Store

Use this procedure to rebuild the primary server administration data store from a secondary server. This procedure uses the same hostname for the replacement server.

1. **On one of the secondary servers, capture the current data store to a file called** `/tmp/store`**:**

```
# /opt/SUNWut/srds/lib/utldbmcat \
/var/opt/SUNWut/srds/dbm.ut/id2entry.dbb > /tmp/store
```

   This provides an LDIF format file of the current database.

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

3. **Follow the directions in the *Sun Ray Server Software 3 Installation and Configuration Guide* to install Sun Ray Server Software.**

4. **After running** `utinstall`**, configure the server as a primary server for the group. Make sure that you use the same admin password and group signature.**

```
# utconfig
      :
# utreplica -p <secondary-server1> <secondary-server2> ...
```

5. **Shut down the Sun Ray services, including the data store:**

```
# /etc/init.d/utsvc stop
# /etc/init.d/utds stop
```

6. **Restore the data:**

```
# /opt/SUNWut/srds/lib/utldif2ldbm -c -j 10 -i /tmp/store
```

This populates the primary server and synchronizes its data with the secondary server. The replacement server is now ready for operation as the primary server.

7. **Restart Sun Ray services:**

```
# utrestart -c
```

8. **(Optional) Confirm that the data store is repopulated:**

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

9. **(Optional) Perform any additional configuration procedures.**

▼ To Replace the Primary Server with a Secondary Server

Note – This procedure is also known as promoting a secondary server to primary.

1. **Choose a server in the existing failover group to be promoted and configure it as the primary server:**

```
# utreplica -u
# utreplica -p <secondary-server1> <secondary-server2> ...
```

2. **Reconfigure each of the remaining secondary servers in the failover group to use the new primary server.:**

```
# utreplica -u
# utreplica -s <new-primary-server>
```

This resynchronizes the secondary server with the new primary server.

Note – This process may take some time to complete, depending on the size of the datastore. Since Sun Ray services will be offline during this procedure, you may want to schedule your secondary servers' downtime accordingly. Be sure to perform this procedure on each secondary server in the failover group.

Secondary Server Recovery

Where a secondary server has failed, administration of the group can continue. A log of updates is maintained and applied automatically to the secondary server when it has recovered. If the secondary server needs to be reinstalled, repeat the steps described in the *Sun Ray Server Software 3 Installation and Configuration Guide.*

Setting Up a Group Signature

The `utconfig` command asks for a group signature if you chose to configure for failover. The signature, which is stored in the `/etc/opt/SUNWut/gmSignature` file, must be the same on all servers in the group.

The location can be changed in the `gmSignatureFile` property of the `auth.props` file.

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

- be owned by root with only root permissions
- contain at least eight characters, in which at least two are letters and at least one is not

Tip – For slightly better security, use long passwords.

▼ To Change the Group Manager Signature File

1. **As superuser of the Sun Ray server, open a shell window and type:**

```
# /opt/SUNWut/sbin/utgroupsig
```

   You are prompted for the signature.

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

3. **For each Sun Ray server in the group, repeat the steps, starting at step 1.**

Note – It is important to use the `utgroupsig` command, rather than any other method, to enter the signature. `utgroupsig` also ensures that internal database replication occurs properly.

Taking Servers Offline

Being able to take servers offline makes maintenance easier. In an offline state, no new sessions are created. However, old sessions continue to exist and can be reactivated unless Sun Ray Server Software is affected.

▼ To Take a Server Offline

- **At the command-line interface, type:**

```
# /opt/SUNWut/sbin/utadm -f
```

▼ To Bring a Server Online

- **At the command-line interface, type:**

```
# /opt/SUNWut/sbin/utadm -n
```

APPENDIX **A**

User Settings and Concerns

Supported Devices and Libraries

Sun Ray Server Software supports a wide variety of end-user devices, including end-user peripherals that can be connected to a Sun Ray DTU's serial, parallel, or USB ports; however, because of the growing number of USB devices available, it has not been possible to test all of them on Sun Ray DTUs.

Managing Monitor Settings

Sun Ray users can modify their screen resolution settings by invoking `utsettings`. Any resolution selections they make within a session remain effective whenever the session is displayed on that particular DTU. The selection is not lost if the unit goes into power-save mode or is power-cycled.

Settings selected through `utsettings` apply *only* to the DTU where `utsettings` is run; a user moving to another DTU does not bring the new timing along as part of the session. However, the selected timing is retained and used again if a user hot desks back to the original DTU.

If the session is associated with a personal mobile token (a smartcard or an NSCM credential), then `utsettings` offers to make the selected timing permanent. If a user accepts that offer, then the timing is retained and reused on that user's subsequent personal mobile token sessions on the same DTU.

In addition, the administrator may use the `utresadm` command to:

- Arrange for a particular monitor timing to be used whenever a specific token is presented on a specific DTU.
- Arrange for a particular monitor timing to be used on a specific DTU, regardless of the token that is presented at the DTU.
- Arrange for a particular monitor timing to be used on all DTU's regardless of the token that is presented at the DTU.

Any conflict among settings is resolved in favor of the most tightly-specified configuration rule. That is, a configuration record for a specific token at a specific DTU takes precedence over a record for *any token* at that specific DTU, and a configuration record for *any token* at a specific DTU takes precedence over a record for *any token* at a*ny DTU*.

Configuring Hot Key Preferences

Hot keyscan be configured for various Sun Ray utilities. The scope for these hot keys can be:

- System-wide default setting
- User default setting
- System-wide mandatory setting

To support these levels of customization, the utilities look for the properties files in TABLE A-1, in the following order, at startup:

TABLE A-1 Sun Ray Settings Properties Files

File	Defaults	Description
`/etc/opt/SUNWut/utslaunch_defaults.properties`	System-wide	This file contains helpful default properties. Any properties specified here override any defaults built into the application itself.
`$HOME/.utslaunch.properties`	User	This file contains the user's preferred values, which override any application or site-wide defaults.
`/etc/opt/SUNWut/utslaunch_mandatory.properties`	System-wide mandatory	This file contains site-wide mandatory settings that cannot be overridden by the user. These properties override any application, site-wide, or user defaults.

If your policy is for all DTUs to use a standard hot key, use the system-wide mandatory defaults file to specify this standard key. This prevents users from specifying their own hot key preferences.

The format of the hot key entry in these properties files is:

```
<utility_name>.hotkey=value
```

where <*utility_name*> is the name of the utility, such as `utsettings` or `utdetach`, and *value* is a valid X keysym name preceded by one or more of the supported modifiers (`Ctrl`, `Shift`, `Alt`, `Meta`) in any order. Values are shown in TABLE A-2.

TABLE A-2 Specific Hot Key Values

Example Value	Notes
`Shift+Props`	This brings up the Settings GUI.
`Ctrl+Alt+Backspace` twice	This kills a session.
`Ctrl+Alt+Del` twice	This kills the process that has taken control of the X server.
`Shift+Pause`	This detaches a non-smart card mobility session.
`Mute+Softer+Louder`	This displays the DTU's MAC address.
`Ctrl+Power` Key	This cycles power.

Users can configure both `Shift+Props` and `Shift+Pause`.

Setting Hot Key Values

▼ To Change the Hot Key for the Settings GUI

If you do not want to use the Sun Props key as your default hot key, use the system-wide defaults file to specify a function key. Users can still specify their preferences in the user defaults file.

Use this procedure to modify the settings GUI for all users on a server.

1. **As superuser, open the `/etc/opt/SUNWut/utslaunch_defaults.properties` file in a text editor.**

Tip – If you want to make the change mandatory, change the value in the `/etc/opt/SUNWut/utslaunch_mandatory.properties` file.

---

2. **Locate the original hot key entry for the `utdetach` utility and place a # in front of that statement.**

   The # comments out the first hot key property.

```
# utdetach.hotkey=Shift Pause
```

3. **Type in the new hot key property after the first statement. For example,**

```
utsettings.hotkey=Shift F8
```

4. **Save the `utslaunch_defaults.properties` file.**

   The new hot key takes effect when the next user logs in. The next user to log in uses the new hot key to display the Sun Ray Settings screen. Users who were logged in before you changed the hot key continue to use the old value.

▼ To Change the Hot Key Used to Detach NSCM Sessions

Note – This resembles the procedure for changing the hot key for the settings GUI except for Step 3.

---

1. **As superuser, open the `/etc/opt/SUNWut/utslaunch_defaults.properties` file in a text editor.**
2. **Locate the original hot key entry for the utsettings utility and place a # in front of it to comment it out.**

```
# utsettings.hotkey=Shift SunProps
```

3. **Type in the new hot key property after the first statement. For example,**

```
utdetach.hotkey=Alt F9
```

▼ To Change the Hot Key Setting for a Single User

1. **In your home directory, create the `.utslaunch.properties` file.**

2. **Add a line to the `.utslaunch.properties` file with the value for the hot key. For example:**

```
utsettings.hotkey=Shift F8
```

3. **Save the `.utslaunch.properties` file.**
4. **Log out and log back in to enable the new hot key.**

Note – You can modify other hot keys in a similar fashion.

Power Cycling a Sun Ray DTU

▼ To Power Cycle a Sun Ray DTU

disconnect then reconnect the power cord.

▼ To Perform a Soft Reset

use the key sequence `Ctrl`-Power (the Power key at the right side of the top row of the Sun Type 6 keyboard has crescent moon icon).

▼ To Kill a User's Session

Use the key sequence `Ctrl-Alt-Bksp-Bksp`.

This kills the Xserver process, alerting the current session's parent process to start another session.

APPENDIX **B**

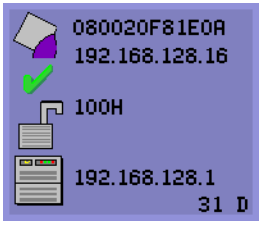
Troubleshooting and Tuning Tips

This appendix contains the following sections:

Understanding OSD

Sun Ray Server Software on-screen displays (OSD) to help administrators and others identify problems visually. The most important information about the Sun Ray DTU and its current state is displayed on the screen.

OSD Icon Topography



The OSD icons display:

- Ethernet address
- Currently assigned IP address of the DTU
- Link status of the currently connected Sun Ray server
- Authentication Server IP address
- Icon code and DHCP state

To help you locate problems, the OSD icons display a numeric icon code followed by an alphabetic DHCP state code. You can look up the meaning of the numeric OSD message codes in TABLE B-1 and the alphabetic DHCP state codes in TABLE B-2. Encryption and authentication information is also displayed when appropriate.

Note – Sun Ray DTUs can function in a private interconnect or in a simple LAN environment with only an IP address, but additional basic parameters and Sun Ray-specific vendor options are needed for more complex LAN operations, such as when a DTU is located several hops away from the Sun Ray Server's subnet.

OSD icon messages and codes are summarized in the following tables:

TABLE B-1 Icon Messages

Icon Code	Meaning
1	Sun Ray unit is starting up and is waiting for ethernet link
2	Sun Ray unit is downloading new firmware
3	Sun Ray unit is storing new firmware in its flash memory
4	Either the download or storage of new firmware has failed
5	There is no session to connect with the Sun Ray
6	The server is denying access to the Sun Ray
7	Local pin entry to the smart card has failed
8	In local smartcard pin entry mode
9	There is an over current condition on the USB bus, i.e., the total number of devices draws too much current. Consider using a powered hub.
11	Server is authenticated by the Sun Ray and the graphic/keyboard network connection is encrypted
12	The Sun Ray cannot authenticate the server but the graphic/keyboard network connection is still being encrypted
13	Server authenticated to the Sun Ray; network connection between Sun Ray and server not encrypted
14	Server not authenticated to the Sun Ray; graphic/keyboard network connection is not encrypted
15	The Sun Ray is refusing to talk to the server due to the server's refusal or inability to authenticate or encrypt the network connection
16	The Sun Ray USB bus is temporarily busy servicing a high-speed device, and the keyboard or mouse may not be responsive to user input.
21	The Sun Ray unit is booting up and is waiting on DHCP IP address and parameter assignment.
22	The Sun Ray unit is booting up and is now waiting for the initial connection to a Sun Ray server.
23	The connection between the Sun Ray and the network is down. Check the network drop cable and (if the network drop cable is okay) the network switch.
24	The Sun Ray has disconnected from the previous server.
25	The Sun Ray is being redirected to a new server.
26	The Sun Ray has connected to the server and is waiting for graphics traffic (this is the GNC state).

TABLE B-1 Icon Messages

Icon Code	Meaning
27	The Sun Ray is broadcasting to locate a Sun Ray server since either it was not provided with Sun Ray specific DHCP parameters or all of the specified servers are not responding.
	Icon numbers 31 through 34 are the network status display brought up by the user pressing all three audio keys.
31	The network link is up, the server is authenticated, and graphics/keyboard network connections is are encrypted.
32	The network link is up, the server is not authenticated, and graphics/keyboard network connections are encrypted.
33	The network link is up, the server is authenticated and graphics/keyboard are encrypted.
34	The network link is up, the server is not authenticated and graphics/keyboard are not encrypted.
50	The server is refusing to talk to the Sun Ray due to the Sun Ray's refusal or inability to authenticate or encrypt the network connection

TABLE B-2 DCHP State Codes

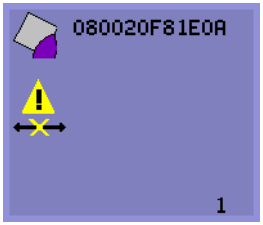
DCHP State Code	State Meaning
A	DCHP only provided IP address with no additional parameters
B	DCHP provided IP address, subnet mask, and router, but Sun Ray vendor-specific parameters are missing.
C	DHCP provided IP address and Sun Ray vendor-specific parameters, but subnet mask and router are missing.
D	DHCP provided all expected parameters.

TABLE B-3 Power LED

DTU Hardware State	Action to Take
Off	Check to see if the DTU is plugged in. Replace the DTU.
Amber	Hardware fault. Replace the DTU.
Blinking	PROM is corrupted. Check that firmware downloads are properly configured and enabled. Then power cycle the DTU.
Card reader LED remains on even when smart card is removed	Card reader hardware problem. Replace the DTU.

Sun Ray Desktop Unit Startup

The first display a user should see is OSD 1: Waiting for the Interconnect.



Definition: The DTU has passed the power-on self test but has not detected an Ethernet signal yet. This icon is displayed as part of the normal startup phase and is usually displayed for only a few seconds.

▼ Actions to take if this icon stays on for more than 10 seconds:

1. **Check that the Ethernet cable is correctly plugged in to the back of the DTU and the other end is plugged in to the correct hub, switch, or network outlet.**

   A link light on the switch or hub indicates that the connection is alive.

2. **If the DTU is connected through a hub or a switch, make sure that the hub or switch is powered on and configured correctly.**

   After the Sun Ray desktop unit has verified its network connection, the user should see the DHCP Pending display.

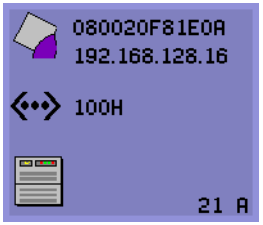
Definition: The DTU has detected the Ethernet carrier but has not yet received its initial parameters or IP address from DHCP. This icon is displayed as part of the normal startup phase and is usually displayed for only a few seconds.

▼ Actions to take if this icon stays on for more than 10 seconds:

1. **Make sure that the DHCP server is configured correctly, is up and running, and has not run out of IP addresses to assign to clients.**

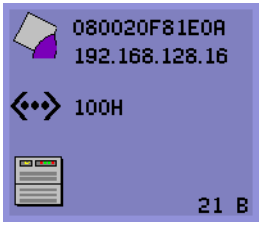
2. **Verify that your DHCP server is configured properly for network parameters.**

   At this point, depending on whether you have configured your Sun Ray servers to run on a LAN or a dedicated interconnect, one of the following icons may display:



Startup Wait for DHCP Information

After the DHCP server has allocated an IP address, the icon is updated with the unit's IP address; if the response is inadequate, the Sun Ray issues a `DHCP inform` request to attempt to obtain the Sun Ray vendor-specific parameters. The Sun Ray continues all the way through booting with just a DHCP supplied IP address but usually functions better with some additional parameters.



Code 21 A indicates that the DTU got an IP address and is waiting for a `DHCP inform` response to other parameters.

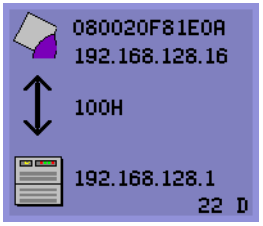
Code 21 B indicates that the DTU got an IP address and IP router and is waiting for Sun Ray vendor-specific options from `DHCP inform`.

Note – If you see a 21 A or 21 B with a DTU IP address in a LAN deployment, the Sun Ray DTU is trying to use `DHCP_INFORM` to get Sun Ray-specific parameters.

▼ Actions to take:

1. **For LAN configurations with other (non-Sun Ray) DHCP services but no `bootp` proxy agent, verify the DHCP server and the Sun Ray vendor tags.**
2. **For routed configurations, verify that the `bootp` proxy agent is configured correctly in the Sun Ray DTU's subnet and that it points to one of the Sun Ray servers in the failover group.**
3. **For non-routed private interconnect configurations, the Sun Ray server also performs the functions of a DHCP server. Verify that it is configured properly for DHCP services.**

When DHCP has finished, the Sun Ray DTU tries to connect to a Sun Ray server and the authentication manager that is running on that server.



Waiting to Connect to Authentication Manager

Definition: The DTU has received its initial parameters from DHCP but has not yet connected to the Sun Ray Authentication Manager. This icon is displayed as part of the normal startup phase and is usually displayed for only a few seconds.

▼ Actions to take if the icon displays for more than a few seconds or if the DTU continues to reset after the icon is displayed:

1. **Make sure that the Sun Ray services, including the Authentication Manager, are up and running on the Sun Ray server.**

   In a LAN configuration or other routed environment:

2. **Make sure that the authentication manager can be reached from the IP address assigned to the DTU.**

3. **Verify that the routing information the DTU receives is correct.**

4. **Run `utquery` for the DTU's IP address.**

   The `utquery` command displays the parameters a Sun Ray DTU has received. If `utquery` fails to display an *AuthSrvr* parameter, the DHCP server for Sun Ray parameters may not be reachable or may not be configured properly. Confirm that the *DHCPServer* and *INFORMServer* values are appropriate. If not, look at your `bootp` relay configurations and DHCP server configurations for network and Sun Ray parameters. For details of these parameters, see the `utquery` man page.

Note – To Restart DHCP, type the following as superuser:

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

▼ To Identify a Hung Session

- **As superuser, type:**

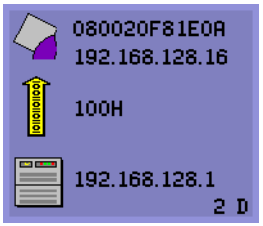
```
# /opt/SUNWut/sbin/utdesktop -l -w
```

▼ To Kill a Hung Session

- **As superuser, type:**

```
# /opt/SUNWut/sbin/utsession -k -t token
```

Firmware Download



Downloading PROM Software

Definition: The DTU is currently downloading new flash PROM software from the Sun Ray server.

▼ Actions to take:

1. **Wait until the download is complete.**

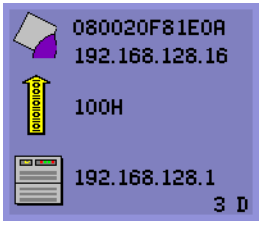
   Downloading and saving the new PROM software usually takes less than a minute. If you interrupt the download, the DTU has to download new PROM software the next time it reboots.

   If the firmware download fails, the following syslog message indicates that the barrier level has been set to prevent Sun Ray DTUs with SRSS 3 firmware from automatically downloading an earlier version of the firmware:

   ```
   Firmware upgrade/downgrade not allowed! Barrier is 300 Firmware level is 0
   ```

2. **Check `/var/opt/SUNWut/log/messages` to confirm that your configuration is set up properly.**

Note – For LAN configurations, the minimum barrier level is 200.



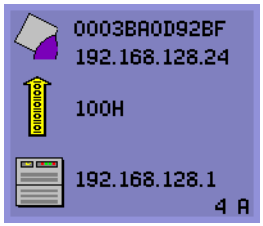
Saving PROM Software

Definition: The DTU has just downloaded new PROM software from the Sun Ray server and is saving it to the DTU's PROM.

▼ Actions to take:

- **Wait until the download is done.**

  Downloading and saving the new PROM software usually takes less than a minute. If you interrupt the download, the DTU has to download new PROM software the next time it reboots.



Firmware Download Failed

Definition: The DTU has failed to download new firmware.

▼ Actions to take:

1. **Check the messages file `/var/opt/SUNWut/log/messages` to verify the version number.**
2. **Correct, if necessary, with `utadm -l`.**

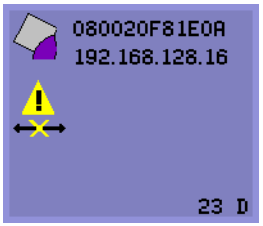
Bus Busy

Sun Ray USB Bus Busy

Definition: The Sun Ray USB bus is temporarily busy servicing a high-speed device, and the keyboard or mouse may not be responsive to user input.

This icon typically appears only during an unusually long print job and disappears when the job is done. This is an informational OSD; there is no particular action to take unless it is necessary to kill the print job.

No Ethernet



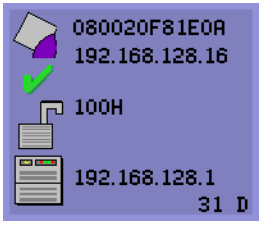
No Ethernet Connection

Definition: The DTU has an Ethernet address and an IP address but has lost the Ethernet signal. This icon is displayed only after the DTU successfully boots and receives an IP address, but then loses its Ethernet signal.

▼ Actions to take:

1. **Check that the Ethernet cable is correctly plugged in to the back of the DTU and the other end is plugged into the correct switch or network outlet.**
2. **If the DTU is connected through a hub or switch, make sure that the hub or switch is on and configured correctly.**

Ethernet Address



Definition: This OSD, shows the Ethernet address, the currently assigned IP address, the currently connected server, the encryption status, and the DHCP state. To display it, press the three audio volume keys simultaneously.

Tip – To get the same effect on non-Sun keyboard, disconnect and reconnect the Ethernet wire.

Link speed is also indicated (for example, 10F, 10H,100F, 100H). F stands for full duplex, and H stands for half duplex. 10 stands for 10 Mbps, and 100 for 100 Mbps.

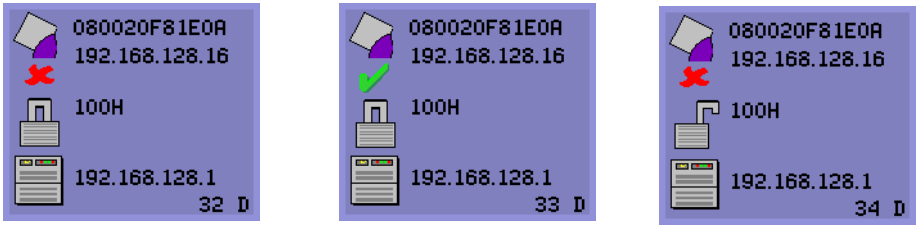
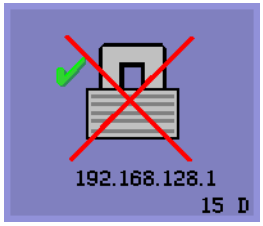


FIGURE B-1 Ethernet Address OSD with Different Encryption and Authentication States

Session Connection Failures

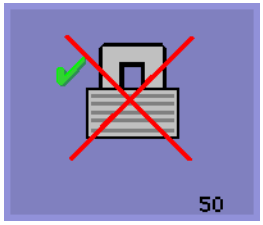
The following icons are displayed when there might be a security breach.



Session Refused

Definition: The client is refusing to connect to a server because it is unable to verify the validity of the Sun Ray server.

This error can occur only if an unknown Sun Ray server intercepts the messages and tries to emulate a valid Sun Ray server. This is a session security breach.



Session Refused

Definition: The server is refusing to grant a session to the client because the client is unable to fulfill the server's security requirements.

▼ Actions to take:

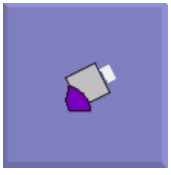
1. **Check the client's firmware version.**

   This error may occur with firmware versions earlier than 2.0 if the server is configured for hard security mode.

2. **Upgrade the firmware.**

   As an alternative, confirm whether your site requires hard security mode. If not, the session can be enabled with soft security mode.

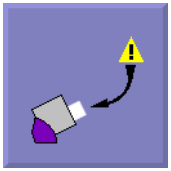
Token Reader Icon



Card Reader Icon

When a site policy disallows pseudo sessions, DTUs configured as token readers display the Card Reader icon instead of the Login Dialog box card.

Card Read Error OSD



Card Read Error

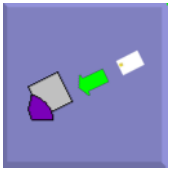
Definition: The Card Read Error OSD icon appears whenever the firmware is unable to read the card due to one of the following causes:

- The DTU is running old firmware.
- The card contacts are dirty, the contacts on the card reader are dirty, or the card is not properly inserted.
- The card is malfunctioning.
- The card is of a type that the firmware is not configured to read.
- There is an error in the configuration for reading this type of card.

▼ Actions to take:

1. **Upgrade the firmware.**
2. **Replace the card.**

Prompt for Card Insertion OSD



Prompt for Card Insertion

Definition: If the current authentication policy allows access only by card, this OSD icon appears and prompts the user to insert a card.

Access Denied OSD

Access Denied

Definition: The Access Denied OSD icon appears when the current authentication policy denies access to the presented token. Specifically, this icon is displayed if a disabled card has been inserted into an DTU.

The Sun Ray administration model has seven user session types:

- Default—Normal user login
- Register—User self-registration

- Kiosk—Anonymous user operation
- Insert card—User smart card required
- Card error—Unrecognized user smart card type
- No entry—User's smart card token is blocked
- Session Refused—The server refuses to grant a session to a client that does not meet the server's security requirements

The first three session types have normal login processes. When there is a problem, the administrator should examine:

- Sun Ray Server configuration files

Caution – Sun Ray Server Software modifies certain system configuration files. In most cases, these changes are identified with SRSS-specific comments. Please do not change these modifications.

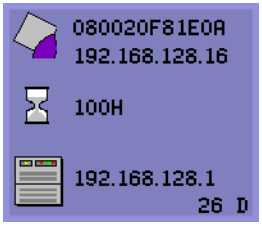
- Any locally modified X server startup files
- `dt`login status

Although the last four session types display icons on the Sun Ray DTU, they do not have login processes at all. The icons indicate that the user must take steps before a successful login is possible. If the user immediately removes and reinserts the smart card, the icon disappears, but the Wait for Session OSD remains.

These last four session types and their OSDs should not cause alarm. The user can:

- Insert a recognized smart card in the correct orientation
- Ask the Sun Ray administrator to grant access
- Ask the Sun Ray administrator to download the correct firmware

Wait for Session OSD



Wait for Session

This OSD represents the transition state for the Sun Ray DTU. If it is displayed for an extended period, there is probably no X Window server running.

Note – The current wait icon is a white "X" cursor. In earlier releases, the wait icon was displayed as a green newt cursor.

Wait Icon Cursor for Default Session Type

This section applies to a normal `dtlogin` session.

The `Xsun` server is indirectly started by the `dtlogin` daemon. In the process of starting the `Xsun` server, the `dtlogin` daemon reads two configuration files:

- `/etc/dt/config/Xservers`
- `/etc/dt/config/Xconfig`

If, after several retries, the `Xsun` process does not start, the `dtlogin` daemon just gives up. The problem can usually be traced back to an older version of the `dtlogin` daemon or the configuration files for the `dtlogin` daemon.

Patches

For the latest information regarding Sun Ray Server Software patches, check:

`http://www.sun.com/products/sunray/patches.html`

Authentication Manager Errors

Authentication Manager errors can be found in the following error logs:

- Installation logs:
  - `/var/adm/log`
  - `/var/opt/SUNWut/log`
- General log files:
  - `/var/opt/SUNWut/srds/log`
  - `/var/opt/SUNWut/srds/replog`

The general format of the log messages is:

```
timestamp   thread_name    message_class     message
```

For example:

```
May  7 15:01:57 e47c utauthd: [ID 293833 user.info] Worker3
NOTICE: SESSION_OK pseudo.080020f8a5ee
```

Message components are defined as follows:

- `timestamp` format:

  year.month.day hours:minutes:seconds

- `thread_name`

  There are several different types of threads. The most common thread handles DTU authentication, access control, and session monitoring. These threads are named "worker" plus number. The Worker# thread names are reused when a connection terminates. Other threads are:

  - SessionManager#—Communicate with `utsessiond` on behalf of a Worker# thread.
  - AdminJobQ—Used in the implementation to wrap a library that would not otherwise be thread-safe.
  - CallBack#—Communicate with applications such as `utload`.
  - WatchID—Used to poll data/terminals from connections
  - Terminator—Cleans up terminal sessions
  - Group Manager—Main group manager thread

- `message_class`

  Messages with the same thread name are related. The exception occurs when a Worker# thread disconnects a DTU and then purges the connection information from memory. After a Worker# DESTROY message, the next use of that Worker# thread name has no relation to previous uses of the thread name (in other words, the thread names are reused).

  - `CLIENT_ERROR`—Indicates unexpected behavior from a DTU. These messages can be generated during normal operation if a DTU is rebooted.
  - `CONFIG_ERROR`—Indicates a system configuration error. The Authentication Manager generally exits after one of these errors is detected.
  - `NOTICE`—Logs normal events.
  - `UNEXPECTED`—Logs events or conditions that were not anticipated for normal operation but are generally not fatal. Some of these errors should be brought to the attention of the Sun Ray product development team.
  - `DEBUG`—Only occurs if explicitly enabled. Beneficial to developers. Debug messages can reveal session IDs, which must be kept secret to ensure proper security.

TABLE B-4 Error Message Examples

Error class	Message	Description
CLIENT_ERROR	...Exception ... : cannot send keepAliveInf	Error encountered while attempting to send a keep-alive message to a DTU.
	...keepAlive timeout	A DTU has failed to respond within the allotted time. The session is being disconnected.
	duplicate key:	DTU does not properly implement the authentication protocol.
	invalid key:	DTU does not properly implement the authentication protocol.
CONFIG_ERROR	attempt to instantiate CallBack 2nd time.	Program error.
	AuthModule.load	Problem encountered while loading configuration module.
	Cannot find module	Program or installation error.
NOTICE	“discarding response: “ + param	No controlling application is present to receive DTU response.
	”NOT_CLAIMED PARAMETERS: “ + param	A token was not claimed by any authentication module.
	...authentication module(s) loaded.	Notification that authentication modules have loaded.
	...DISCONNECT ...	Normal notification of disconnection.
UNEXPECTED	“CallBack: malformed command”	Bad syntax from a user application such as `utload` or `utidle`.
	.../ ... read/0:” + ie	Possible program error.
	.../ ... read/1: ... Exception ...	Error encountered while reading messages from the DTU.
	.../... protocolError: ...	Various protocol violations are reported with this message. This is also a way for `utauthd` to force the DTU to reset.

Audio

Each time a user logs in to a Sun Ray DTU, a script automatically assigns the `$AUDIODEV` environment variable to that session. One `utaudio(1)`real-time process is assigned to each session. Refer to the `audio(7i)`man page for more information.

Audio Device Emulation

The emulated audio device follows the user session during hot desking. The device name appears in the `$AUDIODEV` environment variable but is transparently interpreted by audio programs for Sun systems. Device nodes are created in the `/tmp/SUNWut/dev/utaudio` directory. The directory tree is completely recreated at boot time.

Caution – Do not remove the `/tmp/SUNWut/dev/utaudio` directory. Deleting this directory prevents existing users with `utaudio` sessions from using their audio pseudo device nodes.

If your application uses `/dev/audio`, the Sun Ray server software reroutes the audio signal appropriately.

Audio Malfunction

If audio features are malfunctioning:

1. **To confirm whether audio is working, run the following command on the DTU:**

```
% cat /usr/demo/SOUND/sounds/whistle.au >/$AUDIODEV
```

2. **Bring up** `utsettings`**:**

```
% utsettings
```

3. **Verify that audio output is selected properly, e.g., for headphones or speakers.**
4. **Check the volume level.**
5. **Verify that Mute is not selected.**

Some applications are hard-coded to use `/dev/audio` for output. Sun Ray System Software provides a redirection library that you can use to correct this behavior.

▼ To Activate the Redirection Library

1. **Set the environment variable `LD_PRELOAD` to `libc_ut.so` in the shell or wrapper from which you started the audio player:**

```
# setenv LD_PRELOAD libc_ut.so
```

2. **Restart the application.**

Performance Tuning

Some applications, such as intensive 3-D visual simulations, may run very slowly on Sun Ray. Other applications, such as pseudo-stereo viewers using double-buffering, or high-frequency dynamic color table flips on 8-bit visuals, do not produce the expected visual result.

General Configuration

You can usually improve performance by configuring `/etc/system` shared memory segment parameters. The exact settings depend on application demands and the number of Sun Ray users, but a convenient starting point is:

```
set shmsys:shminfo_shmmax = 0x2000000
set shmsys:shminfo_shmmni = 0x1000
set shmsys:shminfo_shmseg = 0x100
```

Due to the nature of the Xinerama (single virtual X display) mode of multihead, the system shared memory requirements may be even higher. To get reasonable performance, the `shmsys:shminfo_shmmax` parameter must be at least:

```
LARGEST_NUMBER_OF_HEADS * width * height * 4
```

Applications

Placing the user's interactive applications, such as Netscape or StarOffice, or PC interoperability tools, such as Citrix or Tarantella, on the Sun Ray server usually helps performance by reducing network load. The applications benefit from faster transport of commands to the Sun Ray's X server.

Applications that can be configured to use shared memory instead of DGA or openGL usually perform better on Sun Ray when they used shared memory.

Sluggish Performance

Sluggish Sun Ray server performance or excessive disk swapping is an indication that the Sun Ray server is under-provisioned. Under these circumstances, there is not enough virtual memory available to start an X Window server instance for a user's session.

The solution in this situation is to add more memory or increase the size of the swap partition. In other situations, network load or packet loss may be too high. In very rare cases, network cables or switch equipment may be defective.

1. **To determine whether there is excessive swapping, use `vmstat 5`.**

```
# vmstat 5
```

   If there is excessive swapping, the system may be undersized or overutilized.

2. **Verify that network connections are 100F.**
3. **Use utcapture to assess network latency and packet loss.**

   As latency and packet loss increase, performance suffers.

Monitor Display Resolution Defaults to 640 x 480

First, eliminate the most obvious possible causes:

- An older monitor
- A bad cable
- Monitor was off when the Sun Ray DTU was started

If the Sun Ray DTU is unable to read DDC data from the monitor, then it defaults to 640 x 480 pixels.

To correct this condition:

1. **Replace the cable**
2. **Restart the Sun Ray DTU after powering the monitor on**
3. **Replace the monitor**
4. **Use the `utresadm` to set persistent display setting to override the default.**

Old Icons (Hourglass with Dashes Underneath) Appear on Display

If the old icons appear on the display, either the DTU's firmware has not been upgraded or it is failing.

1. **Upgrade the firmware from to SRSS 3.**
2. **Follow the procedure to upgrade the firmware. See the** *Sun Ray Software 3 Installation and Configuration Guide***.**

   You may need to use a dedicated private network.

Port Currently Owned by Another Application

If this message displays, use the following procedure to correct it:

1. **Download the latest Java Communications API (javax.comm API version 2.0.2 and above)**
2. **Make sure that the supported USB-Serial Adapter is used.**

   The supported USB devices list is available at

   `http://www.sun.com/io_technologies/sunray/usb/`
3. **Click the Change Synchronization Settings icon and select the appropriate port (to which the Palm cradle should be connected), then click OK.**
4. **If the ports are not correctly shown in the Serial Port drop down menu, close the application and hot plug the device.**
5. **Start the application again.**

Design Tips

- Avoid drawing into off-screen memory and then copying large areas to the screen. This technique produces slow Sun Ray performance.
- `GXcopy` mode is usually the fastest drawing mode.
- To display large images, use shared memory pixmaps, if possible.
- Opaque stipple patterns are faster than transparent stipples.
- Opaque (image) text is faster then other text.

APPENDIX **C**

Sun Ray and Network Parameter Delivery (DHCP)

Sun Ray relies on DHCP to obtain network parameters and Sun Ray parameters. Network parameters include IP address, subnet mask, and router.

Sun Ray parameters enable Sun Ray devices to function normally in a Sun Ray environment.For Sun Ray DTUs to be able to discover the Sun Ray server on the network, they need to have at least the `AuthSrvr` parameter delivered through DHCP.

For a more comprehensive treatment of DHCP, see the *Dynamic Host Configuration Protocol RFC* at `http://www.ietf.org/rfc/rfc2131.txt?number=2131`.

For details on *DHCP Options and BOOTP Vendor Extensions*, see `http://www.ietf.org/rfc/rfc2132.txt?number=2132`

TABLE C-1 lists the Sun Ray parameter symbol values defined in the DHCP table. The remainder of this appendix describes the encapsulated options.

TABLE C-1 Sun Ray Parameter Symbol Values (as defined in the DHCP table)

Parameter Name	Vendor ID	Code	Type		Mandatory/ Optional	Comments
NewTFlags	Vendor=SUNW.NewT.SUNW,	34,	NUMBER,	4,1	Optional	
Intf	Vendor=SUNW.NewT.SUNW,	33,	ASCII,	1,0	Optional	Interface used for Sun Ray service
NewTDispIndx	Vendor=SUNW.NewT.SUNW,	32,	NUMBER,	4,1	Optional	
FWSrvr	Vendor=SUNW.NewT.SUNW,	31,	IP,	1,1	Optional	Firmware server IP address (needed for firmware upgrade)
LogAppl	Vendor=SUNW.NewT.SUNW,	29,	NUMBER,	1,1	Optional	Log level for application
LogVid	Vendor=SUNW.NewT.SUNW,	28,	NUMBER,	1,1	Optional	Log level for video
LogUSB	Vendor=SUNW.NewT.SUNW,	27,	NUMBER,	1,1	Optional	Log level for USB
LogNet	Vendor=SUNW.NewT.SUNW,	26,	NUMBER,	1,1	Optional	Log level for network
LogKern	Vendor=SUNW.NewT.SUNW,	25,	NUMBER,	1,1	Optional	Log level for kernel
LogHost	Vendor=SUNW.NewT.SUNW,	24,	IP,	1,1	Optional	Log level for host
NewTBW	Vendor=SUNW.NewT.SUNW,	30,	NUMBER,	4,1	Optional	Limits bandwidth available for the Sun Ray
NewTVer	Vendor=SUNW.NewT.SUNW,	23,	ASCII,	1,0	Optional	Specifies which firmware version to upgrade to.
AuthPort	Vendor=SUNW.NewT.SUNW,	22,	NUMBER,	2,1	Optional	Sun Ray server port to connect to
AltAuth	Vendor=SUNW.NewT.SUNW,	35,	IP,	1,0	Optional	Alternate set of Sun Ray server IP addresses
AuthSrvr	Vendor=SUNW.NewT.SUNW,	21,	IP,	1,1	Mandatory	Sun Ray server IP address to connect to
BarrierLevel	Vendor=SUNW.NewT.SUNW,	36,	NUMBER,	4,1	Optional	Barrier level for firmware download

Sun Ray parameters are encapsulated vendor-specific options; that is, the value for the standard DHCP vendor-specific information is an encapsulated set of options that only the vendor equipment—the Sun Ray server, in this case—knows how to interpret.

Encapsulated Options

For each parameter name, there is a vendor ID, an option code, an option type, and an indication as to whether the parameter is mandatory.

Encapsulated options are somewhat more complicated, as illustrated in the following DHCPINFORM response, or DHCPACK, which shows the taxonomy of the bytes in the vendor-specific information portion.

```
                                                2b 4a 17 1d 32 2e 30   .......:
.+J..2.0
0140  5f 31 39 2e 63 2c 52 45  56 3d 32 30 30 32 2e 30   _19.c,RE V=2002.0
0150  39 2e 30 36 2e 31 35 2e  35 34 21 04 68 6d 65 30   9.06.15. 54!.hme0
0160  1f 04 81 92 3a 88 15 04  81 92 3a 88 1d 01 06 1c   ....:... ..:.....
0170  01 06 1b 01 06 1a 01 06  19 01 06 18 04 81 92 3a   ........ .......:
0180  88 16 02 1b 61
```

Note – In this description, hexadecimal values are preceded by `0x` and followed by their decimal value, after an = sign, as in `0x2b=43`.

- The first byte is the option code.
- The next byte represents the encapsulated option length, that is, the number of bytes that make up the option value.
- The next one or more bytes make up the multi-byte option value.
  The option value is followed by another encapsulated option code, and so on.

The example begins with `0x2b=43`, the DHCP option for vendor-specific information. It has a length of `0x4a=74` bytes, which is the total number of bytes that follow. These bytes contain the encapsulated vendor options.

The remainder of the example represents the value of the vendor-specific information options. The first byte contains the first encapsulated option, whose value is `0x17=23`, and the `NewTVer` option, whose value type is `ASCII`. The next byte is `0x1d=29`, which is the length of the `NewTVer` string. These options are followed by 29 bytes that represent the string itself.

The ASCII interpretation at the right of the DHCPACK, is `2.0_19.c,REV=2002.09.06.15.54`. This is the end of the first encapsulated option. The next byte is the beginning of the next option, `Intf`, represented by `0x21=33`. The next byte, the length, is `0x04=4`, and the next four bytes are the ASCII value `hme0`. That's the end of the second encapsulated option.

The next byte is `0x1f=31`, which represents the `FWSrvr` parameter, whose function is to indicate the IP address of the firmware TFTP server. The next byte is the length, 4, which is always be true for an IP address. The hexadecimal value is `0x81 0x92 0x3a 0x88`, which corresponds to the IP address `129.146.58.136`.

Glossary

B

backplane bandwidth Sometimes also referred to as switch fabric. A switch's backplane is the pipe through which data flows from an input port to an output port. Backplane bandwidth usually refers to the aggregate bandwidth available amongst all ports within a switch.

barrier mechanism To prevent clients from downloading firmware that is older than the firmware they already have, the administrator can set a barrier mechanism. The barrier mechanism symbol `BarrierLevel` is defined by default in the DHCP table of Sun Ray servers running version 2.0 or later of Sun Ray Server Software.

bpp Bits per pixel.

C

CAM Controlled access mode, also known as *kiosk mode*.

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.

cut-through switches The switch begins forwarding the incoming frame onto the outbound port as soon as it reads the MAC address, while it continues receiving the remainder of the frame.

D

DHCP Dynamic Host Configuration Protocol, which is a means of distributing IP addresses and initial parameters to the DTUs.

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.

E

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.

Ethernet switch A unit that redirects packets from input ports to output ports. It can be a component of the Sun Ray interconnect fabric.

F

failover The process of transferring processes from a failed server to a functional server.

filling station When a client's firmware is downgraded to an earlier version because it connects to a server running the earlier version, it needs to be connected to a filling station so that it can download newer firmware. For this purpose, a filling station can be any private network configured for Sun Ray services or any shared network in which the Sun Ray DHCP server is the only DHCP server.

firmware barrier See *barrier mechanism*.

FTP File Transfer Protocol. The name of the Internet protocol and the program used to transfer files between hosts.

G

GEM Gigabit Ethernet.

H

head Colloquial term for a screen, or display, or monitor, especially in a context where more than one is used in conjunction with the same keyboard and mouse, as in “multihead” feature.

hot desking The ability for a user to remove a smart card, insert it into any other DTU within a server group, and have the user’s session “follow” the user, thus allowing the user to have instantaneous access to the user’s windowing environment and current applications from multiple DTUs.

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 DTU.

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 DTUs are hot-pluggable.

I

interconnect fabric All the cabling and switches that connect a Sun Ray server’s network interface cards to the Sun Ray DTUs.

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

Internet 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 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 DTU IP addresses are leased.

K

kiosk mode Same as *CAM*.

L

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

layer 2 The data link layer. In the OSI (Open Standards Interconnection) model, there are a total of seven layers. Layer 2 is concerned with procedures and protocols for operating the communication lines between networks as well as clients and servers. Layer 2 also has the ability to detect and correct message errors.

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.

M

MAC address Media Access Control. A MAC address is a 48-bit number programmed into each local area network interface card (NIC) at the time of manufacture. LAN packets contain destination and source MAC names and can be used by bridges to filter, process, and forward packets. `8:0:20:9e:51:cf` is an example of a MAC address. See also Ethernet address.

mobility For the purposes of the Sun Ray Server Software, the property of a session that allows it to follow a user from one DTU to another within a server group. On the Sun Ray system, mobility requires the use of a smart card or other identifying mechanism.

modules Authentication modules are used to implement various site-selectable authentication policies.

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

multihead See *head*.

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

N

namespace A set of names in which a specified ID must be unique.

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

network address The IP address used to specify a network.

network interface An access point to a computer system on a network. Each interface is associated with a physical device. However, a physical device can have multiple network interfaces.

network interface card NIC. The hardware that links a workstation or server to a network device.

network latency The time delay associated with moving information through a network. Interactive applications such as voice, video displays and multimedia applications are sensitive to these delays.

network mask A number used by software to separate the local subnet address from the rest of a given Internet protocol address. An example of a network mask for a class C network is 255.255.255.0.

network protocol stack A network suite of protocols, organized in a hierarchy of layers called a stack. TCP/IP is an example of a Sun Ray protocol stack.

NIC Network interface card.

non-smart card mobility A mobile session on a Sun Ray DTU that does not rely on a smart card.

O

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

P

patch A collection of files and directories that replace or update existing files and directories that prevent proper execution of the software on a computer system. The patch software is derived from a specified package format and can only be installed if the package it fixes is already present.

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

port (1) A location for passing data in and out of a computer system. (2) The abstraction used by Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host.

power cycling Using the power cord to restart a DTU.

S

screen flipping The ability to pan to individual screens on a DTU with a single head that were originally created by a multihead group.

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

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

session A group of services associated with a single user.

session mobility The ability for a session to "follow" a user's login ID or a token embedded on a smart card.

smart card A plastic card containing a microprocessor capable of making calculations.

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).

store-and-forward switches The switch reads and stores the entire incoming frame in a buffer, checks it for errors, reads and looks up the MAC addresses, and then forwards the complete good frame out onto the outbound port.

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

T

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.

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

timeout value The maximum allowed time interval between communications from a DTU to the Authentication Manager.

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 DTU's built-in type (pseudo) and ID (the unit's Ethernet address) are supplied as the token.

U

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.

USB Universal serial bus.

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.

V

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

VLAN Virtual local area network.

W

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

X

X server A process which controls a bitmap display device in an X window system. It performs operations on request from client applications.

Index

C

D

R

S

T

U

V

W

X