



Sun Ray Server Software 1.3 Advanced Administrator's Guide

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303-4900 U.S.A.
650-960-1300

Part No. 806-7713-10
July 2001, [Revision 01](#)

[Send comments about this document to: docfeedback@sun.com](mailto:docfeedback@sun.com)

Copyright 2001 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, CA 94303-4900 U.S.A. All rights reserved.

This product or document is distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, AnswerBook2, docs.sun.com, Sun Ray, UltraSPARC, and Solaris are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

Netscape and Netscape Navigator are trademarks or registered trademarks of Netscape Communications Corporation in the United States and other countries.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

Federal Acquisitions: Commercial Software—Government Users Subject to Standard License Terms and Conditions.

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

Copyright 2001 Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, CA 94303-4900 Etats-Unis. Tous droits réservés.

Ce produit ou document est distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a. Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, AnswerBook2, docs.sun.com, Sun Ray, UltraSPARC, et Solaris sont des marques de fabrique ou des marques déposées, ou marques de service, de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

Netscape et Netscape Navigator est une marque de Netscape Communications Corporation aux Etats-Unis et dans d'autres pays.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.



Contents

Preface	ix
Before You Read This Book	ix
How This Book Is Organized	ix
Using UNIX Commands	x
Typographic Conventions	xi
Shell Prompts	xi
Related Documentation	xii
Accessing Sun Documentation Online	xii
Ordering Sun Documentation	xii
Sun Welcomes Your Comments	xiii
1. Connecting Sun Ray Clients to the Sun Ray Server	15
Sun Ray System Computing Model	15
Switch Technical Requirements	18
Constraints	18
Auto-Negotiation	19
Turn-On Time	19
Bandwidth Limitation and Packet Loss	20
Switching Scenarios	21

Stringing Switches Together	21
Using Additional Network Interface Cards	23
Replacing Hubs With Switches	24
2. VLANs and the Sun Ray	25
Introduction	25
What is a VLAN?	26
Implementing Sun Ray Appliances on VLANs	26
Recommendations for VLAN Implementations	27
Using the <code>utcapture</code> Tool	30
Description	30
Usage	31
Starting <code>utcapture</code>	32
3. Monitoring the Sun Ray System	33
Sun Management Center Software Features	33
Software Requirements	35
Installing the Software	36
▼ To Install the Sun Ray Server Software After Installing the Sun Management Center Software	37
▼ To Install Sun Management Center Software After Installing Sun Ray Server Software	38
▼ To Install the Package on Separate Servers	38
Additional Sun Management Center Modules	39
Setting Up the Monitoring Environment	39
▼ To Set Up the Monitoring Environment	40
▼ To Create an Object	40
Troubleshooting	41
Case 1	41
▼ To Load the Sun Ray Module	41

Case 2	42
▼ To Activate the Sun Ray Module	42
Setting Alarms	43
▼ To Set an Alarm	43
▼ To Start Monitoring	46
Setting Monitoring Guidelines	49
Sun Ray System Panel	49
▼ To Display the Sun Ray System Panel	49
▼ To Refresh the Sun Ray System Panel	50
▼ To Set Alarms	50
Sun Ray Services Panel	51
Failover Group Panel	52
Interconnect Panel	53
▼ To Set an Alarm for Running Out of Addresses	53
Desktops Panel	54
▼ To Add an Appliance to Be Monitored	54
▼ To Delete an Appliance to Exclude Monitoring	54
Using Other Monitoring Programs	56
Removing the SUNWutesa Package	57
▼ To Remove the SUNWutesa Package	58
4. Controlled Access Mode	59
Controlled Access Mode Functionality	59
Enabling Controlled Access Mode	60
▼ To Enable Controlled Access Mode	60
▼ To Configure CAM Settings	61
Building the Controlled Access Mode Environment	63
▼ To Add a New Application	64

- ▼ To Edit an Available Application 64
- ▼ To Make an Application Available to Users 65
- ▼ To Make an Application Not Available to Users 66
- ▼ To Remove an Application 66

Advanced Application Setup 67

Enabling Prototypes 67

- ▼ To Enable Prototypes 67

Using Wrapper Scripts to Customize Controlled Access Mode Applications 68

- ▼ To Launch an Application Using a Wrapper Script 68

Security and the Controlled Access Mode Environment 69

Failover 69

Localization 69

- ▼ To Change the Locale for the Controlled Access Mode Sessions Without Changing the System Locale 70

5. Multihead Feature on Sun Ray Appliances 71

Multihead Groups 72

Multihead Screen Display 73

Display Resolution 73

Multihead Administration Tool 74

- ▼ To Turn On Multihead Policy From the Command Line 74
- ▼ To Turn On Multihead Policy Using the Administration Tool 75
- ▼ To Create a New Multihead Group 75

XINERAMA 78

Session Groups 78

Authentication Manager 79

6. Failover 81

Failover Group Overview	82
Setting Up IP Addressing	83
Setting Up Server and Client Addresses	83
Server Addresses	84
Configuring DHCP	85
Coexistence of the Sun Ray Server With Other DHCP Servers	85
Administering Other Clients	86
▼ To Set Up IP Addressing on Multiple Servers Each With One Sun Ray Interface	86
Group Manager	89
Redirection	90
utselect	90
▼ To Redirect to a Different Server	90
utswitch	91
▼ To Manually Redirect an Appliance	91
▼ To List Available Hosts	91
▼ To Select a Different Server	92
Group Manager Configuration	92
▼ To Restart the Authentication Manager	92
Load Balancing	93
▼ To Turn Off the Load Balancing Feature	93
Setting Up a Failover Group	93
Primary Server	94
▼ To Specify a Primary Server	94
Secondary Server	94
▼ To Specify Each Secondary Server	95
Removing Replication Configuration	95
▼ To Remove the Replication Configuration	95

Viewing the Administration Status	95
▼ To Show Current Administration Configuration	95
Recovery Issues and Procedures	96
Primary Server Recovery	96
▼ To Rebuild the Primary Server Administration Data Store	96
▼ To Replace the Primary Server with a Secondary Server	97
▼ To Replace a Primary Server	98
Secondary Server Recovery	98
Setting Up a Group Signature	99
▼ To Change the Group Manager Signature File	99
Taking Servers Offline	100
▼ To Take a Server Offline	100
▼ To Bring a Server Online	100
▼ To Install the Controlled Browser	101
▼ To Remove the Controlled Browser	102
▼ To Setup the Controlled Browser in Control Access Mode Administration	104
▼ To Print from the Browser	106
▼ To Configure the Printer Location	108
▼ To Add Macromedia Flash Player Plug-in	112
▼ To Add Adobe Acrobat Reader Plug-in and Application	112
▼ To Add RealPlayer Plug-in and Application	115
Glossary	117

Preface

The *Sun Ray Server Software 1.3 Advanced Administrator's Guide* is intended for system administrators who are already familiar with the Sun Ray™ computing paradigm and have substantial networking knowledge. This guide is also useful for those interested in customizing their 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 1.3 CD or the Electronic Software Download (ESD) and that you have added the required patches.

In order to fully use the information in this document, you must have thorough knowledge of the topics discussed in these books:

- *Sun Ray Server Software 1.3 Readme*
- *Sun Ray Server Software 1.3 Installation Guide*
- *Sun Ray Server Software 1.3 Administrator's Guide*

How This Book Is Organized

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

Chapter 2 describes the VLAN option and how to determine packet loss on a Sun Ray system.

Chapter 3 describes how to monitor the Sun Ray system using Sun™ Management Center software.

Chapter 4 describes customizing the Sun Ray server software for controlled access mode.

Chapter 5 describes how to implement multihead and XINERAMA on a Sun Ray system.

Chapter 6 describes the failover option.

This manual also contains a glossary.

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.

See one or more of the following for this information:

- AnswerBook2™ online documentation for the Solaris™ operating environment
- Other software documentation that you received with your system

Typographic Conventions

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

Shell Prompts

Shell	Prompt
C shell	<i>machine_name%</i>
C shell superuser	<i>machine_name#</i>
Bourne shell and Korn shell	\$
Bourne shell and Korn shell superuser	#

Related Documentation

Application	Title	Part Number
Installation	<i>Sun Ray Server Software 1.3 Installation Guide</i>	806-7711-10
Software	<i>Sun Ray Server Software 1.3 Administrator's Guide</i> <i>Sun Ray Server Software 1.3 Readme</i>	806-7712-10

Accessing Sun Documentation Online

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

<http://docs.sun.com>

For Sun Ray specific documentation:

<http://www.sun.com/sunray>

Ordering Sun Documentation

Fatbrain.com, an Internet professional bookstore, stocks select product documentation from Sun Microsystems, Inc.

For a list of documents and how to order them, visit the Sun Documentation Center on Fatbrain.com at:

<http://www.fatbrain.com/documentation/sun>

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 (806-7713-10) of this document in the subject line of your email.

Connecting Sun Ray Clients to the Sun Ray Server

This chapter describes the infrastructure required to connect Sun Ray™ clients to the Sun Ray server.

Topics include:

- “Sun Ray System Computing Model” on page 15
- “Switch Technical Requirements” on page 18
- “Switching Scenarios” on page 21

Sun Ray System Computing Model

The Sun Ray system employs a highly network-dependent computing model where all actual computing is done at a server and display data is passed back and forth between the Sun Ray server and the Sun Ray appliances. Traffic in this environment (which is isolated from the LAN) is bursty in nature. Network bottlenecks might be visible at the users’ desktops. A well-designed interconnect between server and appliances is essential for providing high quality of service to users.

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

Implementing the interconnect with a physically dedicated and isolated set of Ethernet switches is the recommended customer deployment due to the following advantages:

- 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.

The alternative deployment approach is to use VLAN technology to maintain a logically dedicated interconnect but to use shared physical networking equipment (see FIGURE 1-1). The `utcapture` program is supplied as part of the Sun Ray server software package to report packet loss as seen by the Sun Ray clients. This can be used to assess network adequacy for the support of Sun Ray clients.

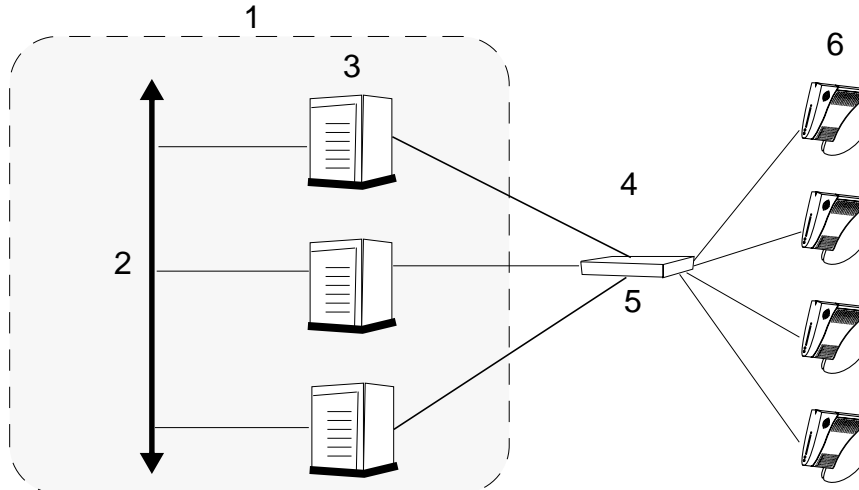


FIGURE 1-1 The Sun Ray System in a dedicated interconnect configuration

Legend:

1. Managed environment
2. Local area network (LAN)—Existing connection to intranet or Internet
3. Sun Ray servers—Execute applications
4. Dedicated interconnect—While VLAN is supported, the dedicated interconnect is the recommended environment for Sun Ray appliances
5. Switch
6. Sun Ray appliances

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

There are two basic types of 100 Mbps switches:

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

Either of these switches can be used in the interconnect. They might be managed or unmanaged. However, some managed switches might require some basic configuration to use 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.

Due to the nature of the Sun Ray design and architecture, the interconnect must be completely dedicated and private, or a VLAN; that is, not part of the corporate LAN. (The dedicated interconnect is the recommended environment for Sun Ray appliances. VLAN is supported. Carefully review the VLAN chapter before implementing Sun Ray appliances on VLAN.) To this end, the Sun Ray server uses at least two network interfaces: one for the corporate LAN, the other for the Sun Ray interconnect.

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

While 10 Mbps services are supported, the preferred configuration is a 100BASE-T, full-duplex network to maximize interconnect quality of service and the number of Sun Ray appliances supported.

Switch Technical Requirements

The Sun Ray system leverages commodity network equipment, and relies on layer 2 or layer 3 switching support. The interaction between the Sun Ray appliance, the server, and the switch must meet the following qualifications (see TABLE 1-1 and TABLE 1-2):

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

Switch Feature	Requirement	Notes
Auto-negotiation	Enabled	Sun Ray appliances have no state and therefore have no means to configure link parameters. If there are any auto-negotiation problems, the switches cannot be used.
Support for full-duplex connections	Enabled	Switches should support full-duplex connections to the Sun Ray appliance and to the server.
Latency	Low	Switches add latency, or delay, to network traffic. Latency must be low to ensure quality of service to appliance users.

TABLE 1-2 Multicasting Considerations

Switch Feature	Requirement	Notes
Multicasting	Enabled	The Authentication Manager uses multicasting (the default) to enable communication between Sun Ray servers over their Sun Ray network interfaces in a failover environment. If the Sun Ray network switches do not support multicast addressing, you must set <code>enableMulticast</code> to <code>false</code> in the <code>auth.props</code> file on all the servers.

Constraints

Sun Ray appliances are designed to work well with any standard Ethernet switch and rely on layer 2 or layer 3 switching support.

In the rare case that a switch does not work satisfactorily within the Sun Ray environment, the problem can be traced back to one of the following issues:

- “Auto-Negotiation” on page 19
- “Turn-On Time” on page 19
- “Bandwidth Limitation and Packet Loss” on page 20

Auto-Negotiation

The Sun Ray appliances contain no internal state, and so they cannot be configured for a specific Ethernet interface setting. The appliances rely on auto-negotiation. To obtain the highest speed and duplex setting, the switch port connected to a Sun Ray appliance should be set to auto-negotiate. If you configure a switch with a specific port setting of 100 Mbps or 10 Mbps, auto-negotiation is disabled on that port. This action forces the Sun Ray appliance to rely on auto-sensing. As a result, the Sun Ray appliance assumes the interface is half-duplex because it cannot reliably detect whether an interface is half- or full-duplex. With a small number of switching products, there exists an auto-negotiation compatibility issue, from complete failure to operating at a negotiated speed/duplex setting of less than 100 Mbps full-duplex. Using switches that fully conform to the IEEE 802.3u auto-negotiation specifications can minimize this compatibility issue.

You can test a switch by connecting the Sun Ray appliance to the switch and observing the results of the auto-negotiation by pressing the three audio keys simultaneously. Extensive testing with more clients gives a greater degree of confidence.

Note – You cannot hard code the speed or duplex rate on the Sun Ray appliances.

Note – All switch ports connected to Sun Ray appliances should be configured to auto-negotiate.

Turn-On Time

The Sun Ray appliances are designed to power on and be fully operational in a very short time—typically less than 10 seconds.

Some switches have initial configurations that can cause this turn-on time to be considerably longer, often taking 30 seconds or longer to achieve a full working state. Longer turn-on times typically are due to the configuration of the Ethernet switch that implements capabilities not needed in the Sun Ray appliance environment. The most common of these capabilities is enabling Spanning Tree protocol, which is designed to detect and compensate for loops in the network. In

the Sun Ray environment, the Spanning Tree protocol should be disabled or deferred for ports connected directly to the Sun Ray appliances. Some manufacturers support a feature that immediately puts a port into the Spanning Tree forwarding mode. This feature is an acceptable alternative to disabling the Spanning Tree protocol on the port.

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

Bandwidth Limitation and Packet Loss

The Sun Ray appliance depends on low latency—low packet loss delivery of the information used to create the screen image. Packet loss can assume two visible forms: as horizontal bands or as larger rectangular holes that fill in a random order. The latter form occurs when low-throughput conditions are detected, which is usually due to packet loss. This data loss is transitory and not critical. The lost information is redisplayed quickly. Additionally, the loss of information is noticed by the server, which slows down transmissions to compensate. This causes the screen output to display more slowly.

These behaviors can be caused by a misconfigured switch, an oversubscribed switch, or an incorrectly configured interconnect. If a switch is not capable of transferring data at the maximum rate on all interfaces simultaneously, it is oversubscribed. This is not a problem in a normal LAN environment because most networks are underused, and dropped packets are recovered by higher-level protocols requesting retransmission of the information. In a seriously oversubscribed environment, the performance of the Sun Ray appliance can be impacted to such a degree that it becomes unsatisfactory.

Recently manufactured switches are designed such that they are not capable of being oversubscribed—that is, there should never be any packets dropped with these switches. If you have older switches installed, the internal bandwidth might be quite low. In this situation, there can be significant oversubscription and the possibility of packet loss during high peak bandwidth usage. With these switches, carefully review the manufacturer's specifications on switching backplane or backplane bandwidth.

Another possible cause of packet loss might be a misconfigured speed and/or duplex setting for the Sun Ray server. If there is an auto-negotiation problem between the Sun Ray server and the switch (for example, the server does not auto-negotiate a full-duplex connection with the switch), both the server and the switch might have to be set manually to operate at full duplex 100 Mbps or 1 Gbps.

For more information, refer to the following SunSolveSM Infodocs:

- Infodoc 18262 (How do I troubleshoot 100 Mbyte Fast Ethernet 802.3 auto-negotiation problems?)
- Infodoc 16144 (How to force the HME card to work at 100 Mbyte full-duplex?)
- Infodoc 23041 (ge QSR)

The SunSolve OnlineSM service is a Web site where patches (software updates) and support documents are readily available. The SunSolve Online service can be accessed at the following URL:

<http://sunsolve.Ebay.Sun.COM/>

Switching Scenarios

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

Stringing Switches Together

Cascading switches using 100 Mbps links (FIGURE 1-2) can reduce overall performance of the interconnect. Cascading switches using gigabit links (FIGURE 1-3) are preferred.

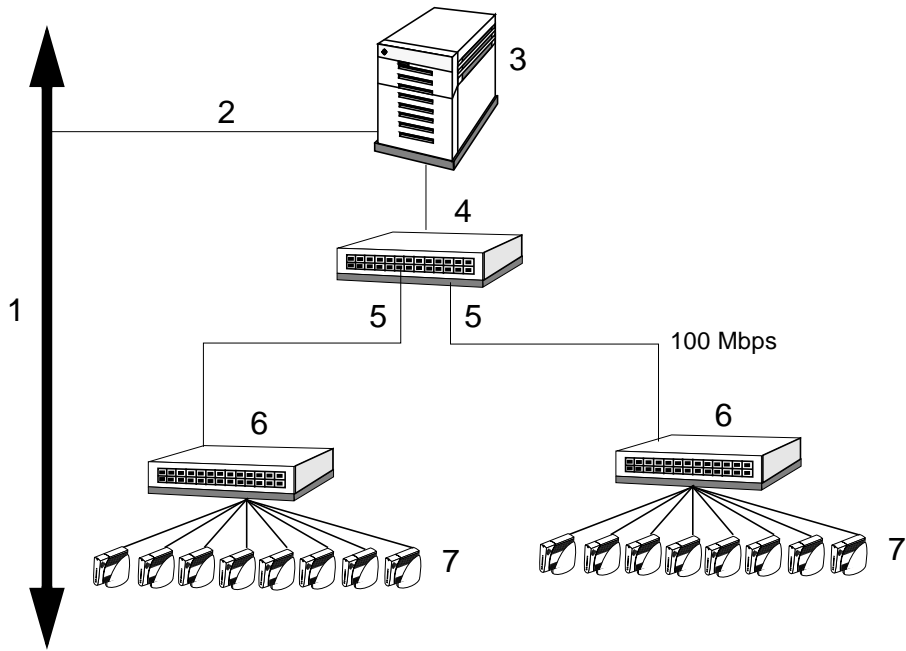


FIGURE 1-2 Cascading Switches Using 100 Mbps Links

Legend:

1. Local area network (LAN)
2. Category 5 cabling for 100 Mbps
3. Sun Ray server
4. Switch with gigabit connections to the Sun Ray server and 100 Mbps connection to the downstream switches
5. Category 5 cabling for 100 Mbps
6. Switches
7. Sun Ray appliances

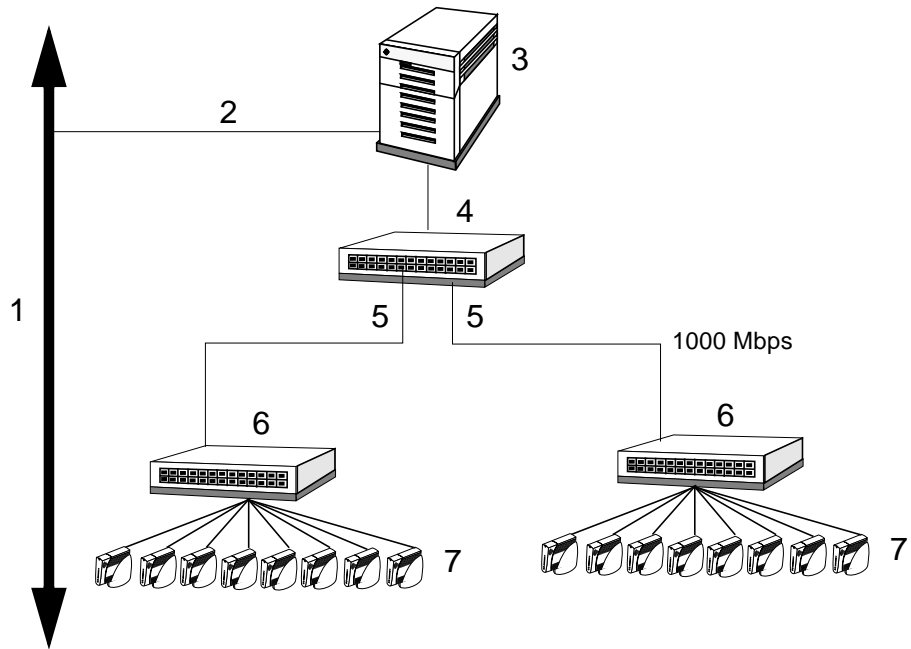


FIGURE 1-3 Cascading Switches Using Gigabit Links—Preferred

Legend:

1. Local area network (LAN)
2. Category 5 cabling for 100 Mbps
3. Sun Ray server
4. Gigabit core switch
5. Fiber-optic cabling for 1000 Mbps
6. Switches with gigabit connection to the core switch
7. Sun Ray appliances

Using Additional Network Interface Cards

Installing an additional network interface card (NIC) can increase the size of the interconnect and support more users (see FIGURE 1-4).

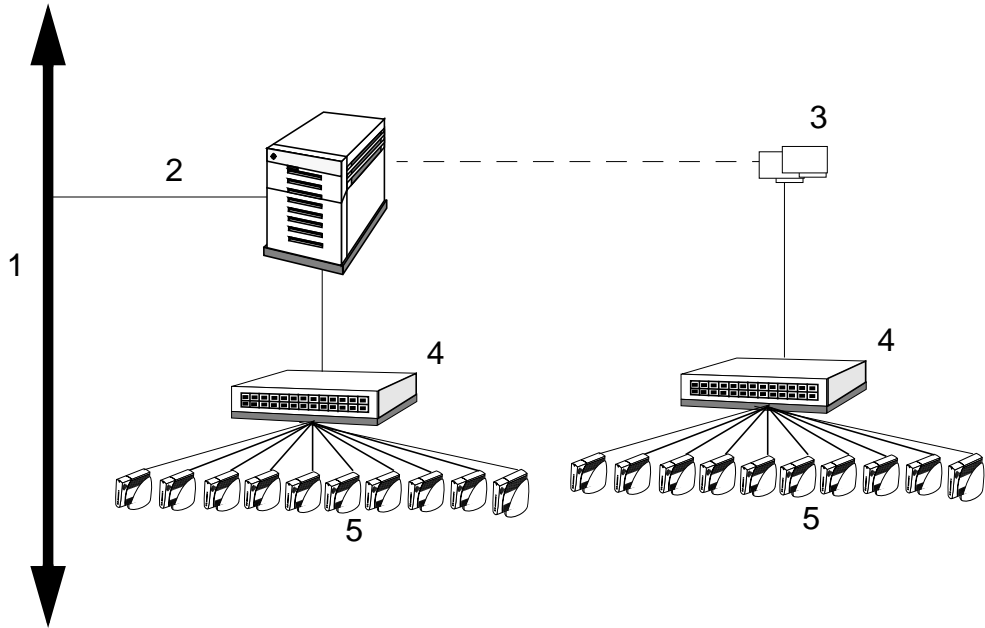


FIGURE 1-4 Additional Network Interface Cards

Legend:

1. Local area network (LAN)
2. Category 5 cabling for 100 Mbps
3. One or more network interface cards installed on the Sun Ray server
4. Switches with gigabit connection to the Sun Ray server
5. Sun Ray appliances

Replacing Hubs With Switches

Hubs provide *shared* bandwidth rather than *switched* bandwidth. Hubs should not be used in a Sun Ray interconnect.

VLANs and the Sun Ray

This chapter includes information on the operation of Sun Ray appliances on a Virtual Local Area Network (VLAN) and how to address VLAN switching issues encountered within the Sun Ray environment.

Topics include:

- “Introduction” on page 25
- “What is a VLAN?” on page 26
- “Implementing Sun Ray Appliances on VLANs” on page 26
- “Using the `utcapture` Tool” on page 30

Introduction

Sun Ray server software 1.3 includes a packet loss reporting tool, `utcapture`. The `utcapture` tool will report the rate of packet loss experienced at the Sun Ray appliances. You can then make the adjustments necessary to correct the problem on the interconnect. The `utcapture` tool reports packet loss but is not intended to be a network troubleshooting tool.

This chapter does not provide the instructions for setting up or configuring your VLAN, as this information is provided by the manufacturer of your particular switch. All adjustments made to your VLAN are also based on the instructions provided by your switch manufacturer. Please refer to the documentation from your switch manufacturer for information regarding the operation of your hardware.

What is a VLAN?

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. Because VLANs must share backplane and link bandwidth, they are not true dedicated interconnects. Traffic outside the VLAN could adversely affect the bandwidth available for Sun Ray appliance traffic, which, in the worse case, could result in horizontal bands or blocks on the screen and reduced painting rates.

Implementing Sun Ray Appliances on VLANs

The Sun Ray appliance works well with any standard Ethernet switch and works with layer 2 or layer 3 switching support. The switches are used as an input-output connection where the network behavior is potentially visible to the end user.

There is no configuration required or possible on the Sun Ray appliance. Both layer 2 and layer 3 switches are appropriate for this purpose. In a heterogeneous switching environment, all switches in the VLAN network should be compliant with the IEEE 802.1Q requirements and implement the IEEE 802.3ac frame extensions to prevent Ethernet frames larger than the current IEEE 802.3 maximum of 1518 bytes from being discarded.

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

The recommended environment for the Sun Ray appliances is a dedicated interconnect. In a dedicated interconnect, all of the traffic is Sun Ray traffic, which is controlled and limited by the Sun Ray servers. This reduces the potential for oversubscribing switches and links, since the server compensates for traffic loss.

Implementing a Sun Ray interconnect through VLANs creates a logical dedicated connection, but can also mean sharing physical resources with uncontrolled traffic that is not Sun Ray appliance traffic. These resources could be a limited backplane bandwidth within a switch or on a link between switches that carries multiple VLANs (see FIGURE 2-1). If these resources are consumed by other devices, significant amounts of Sun Ray appliance traffic might be dropped and the results seen as horizontal bands or blocks on the user's display.

Note – Sun Ray deployments using VLAN technology are only supported when the packet loss to the client is less than 0.1% as reported by the `utcapture` tool.

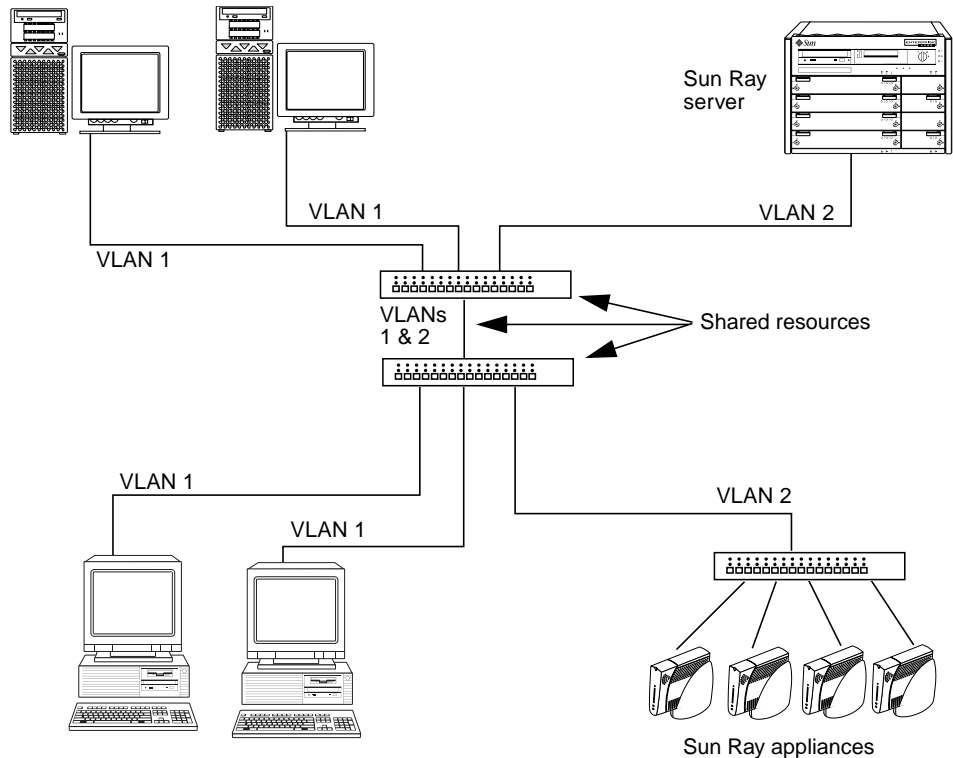


FIGURE 2-1 Example of Shared Physical Resources in Multiple VLANs Configuration

Recommendations for VLAN Implementations

- **Design in Sufficient Bandwidth**—Be sure to design in sufficient bandwidth for the switches to avoid oversubscription and packet loss. Most modern switches are not capable of being oversubscribed. With older switches, review the specifications on *switching fabric* or *backplane bandwidth*.
- **Assign VLANs on Port Basis**—VLAN membership is determined by assigning a VLAN ID to a group of ports. A port can be a member of only one port-based VLAN unless IEEE 802.1Q tagging is applied to the port; 802.1Q tagging adds four additional bytes to the Ethernet packet. The first two bytes identify the packet as having an 802.1Q tag while the last two bytes contain the packet

priority information (if used) and the VLAN ID. With tagging, the device that receives the tagged packet can then determine to which VLAN the packet belongs.

FIGURE 2-2 shows an example of when to tag the ports in a Sun Ray interconnect. The ports connecting the Sun Ray appliances and the Sun Ray appliance servers are untagged because they are in only one port-based VLAN. The ports on the link between the two switches are tagged because they are in multiple port-based VLANs (VLANs 1 and 2). The link carries information from multiple VLANs, and it is the tag information that dictates to which VLAN the packet belongs.

- **Allocate Higher Priority to the Sun Ray Appliance VLAN**—If there is a significant amount of Sun Ray appliance traffic loss either within switches or at interconnect links, the VLAN carrying Sun Ray traffic should be given higher priority than all other VLANs to minimize loss. Manufacturers have different options for choosing and implementing priorities. Refer to your switch documentation for details.
- **Increase Available Bandwidth in Case of Bottleneck**—If interconnect links become significant bottlenecks and cause the loss of Sun Ray appliance traffic, the bandwidth of the links should be increased either by connecting a higher-bandwidth link or by aggregating individual links together (see FIGURE 2-3). If you choose to employ port aggregation, you should not select a round-robin approach. This could result in out-of-order Sun Ray packets that are treated as dropped packets.

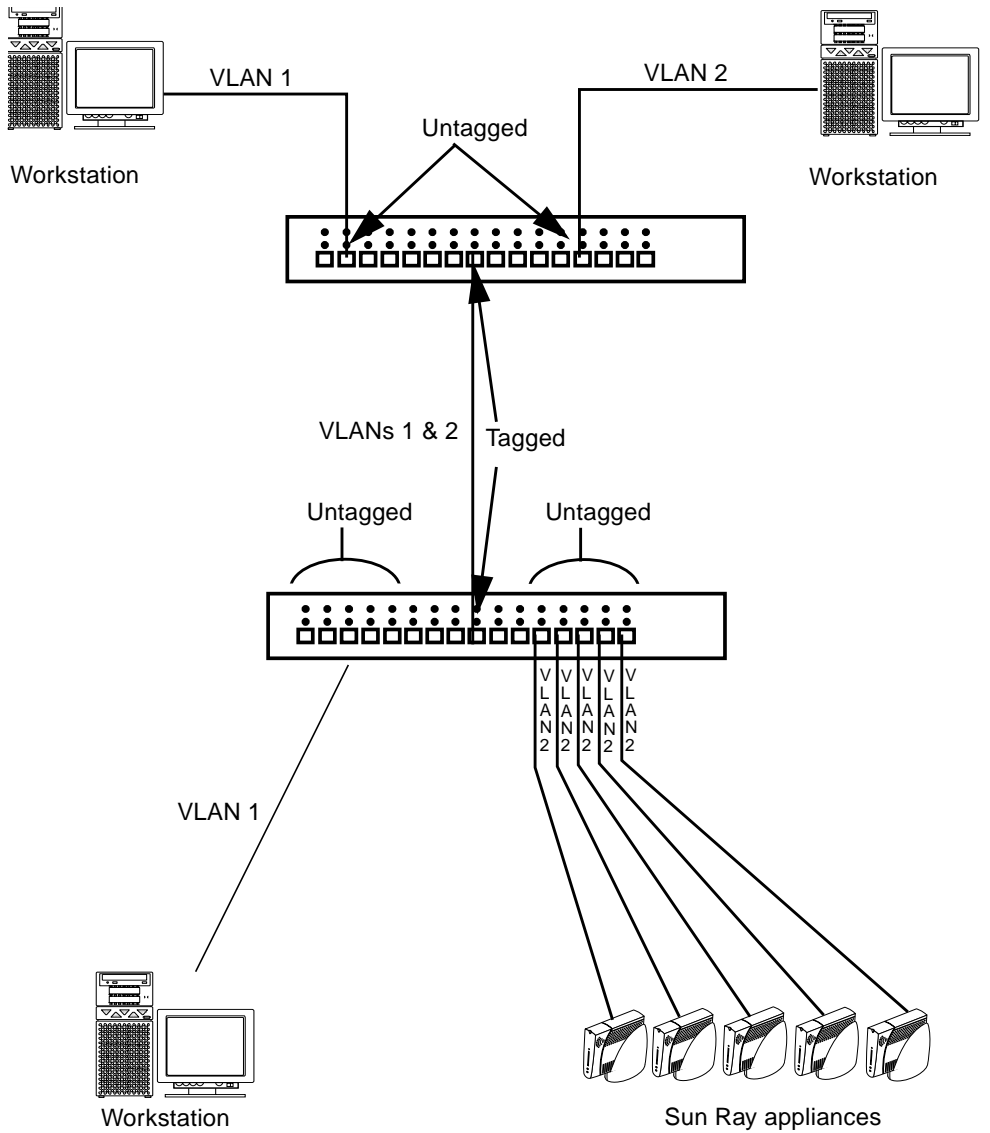


FIGURE 2-2 Tagged and Untagged Ports in Port-Based VLANs

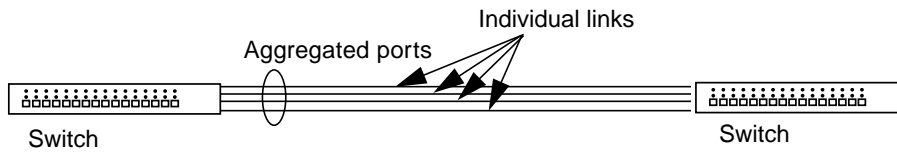


FIGURE 2-3 Aggregating Individual Links

Note – For details on specific switches, refer to the switch manufacturer’s technical documentation.

Using the `utcapture` Tool

Description

The `utcapture` tool is used to report packet loss information experienced by Sun Ray appliances. 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 appliance. This data in TABLE 2-1 is then displayed on the screen in the following format:

TABLE 2-1 Data Elements Displayed

Data Element	Description
TERMINALID	The MAC address of the appliance
TIMESTAMP	The time the loss occurred in year-month-day-hour-minute-second format. Example: 20010329112512
TOTAL PACKET	Total number of packets sent from server to appliance

TABLE 2-1 Data Elements Displayed

Data Element	Description
TOTAL LOSS	Total number of packets reported as lost by appliance
BYTES SENT	Total number of bytes sent from server to appliance
PERCENT LOSS	Percentage of packets lost between the current and previous polling interval

If there is more than .01% of Sun Ray appliance traffic loss, follow the recommendations as outlined in “Recommendations for VLAN Implementations” on page 27 and make appropriate modifications to your network to improve performance.

Usage

The `utcapture` options listed in TABLE 2-2 are supported.

TABLE 2-2 `utcapture` Options

Option	Definition
<code>-h</code>	Help for using the command.
<code>-r</code>	Dump output to <code>stdout</code> in raw format. By default, data is dumped only when there is a packet loss. With this option, the data will always be dumped to <code>stdout</code>
<code>-s server</code>	Name of server on which the Authentication Manager is running. By default, it is the same host that is running <code>utcapture</code> .
<code>-i filename</code>	Process raw data from a file specified by <code>filename</code> and dump to <code>stdout</code> only the data for those appliances that had packet loss.

The following optional argument is supported:

`desktopID`—Collects the data for the specified appliances only. Appliances are specified on the command line by their desktop IDs separated by a space. By default, data for all currently active desktops is collected.

Starting utcapture

From a command line, enter one of the following commands

```
% utcapture -h
```

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

```
% 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 an appliance

```
% 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`

```
% 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 appliance with ID `080020a893cb` or `080020b34231`.

```
% 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 appliances that had packet loss.

Monitoring the Sun Ray System

This chapter describes how to use the Sun Management Center software to monitor the Sun Ray System.

Topics include:

- “Sun Management Center Software Features” on page 33
- “Software Requirements” on page 35
- “Installing the Software” on page 36
- “Setting Up the Monitoring Environment” on page 39
- “Setting Monitoring Guidelines” on page 49
- “Using Other Monitoring Programs” on page 56
- “Removing the SUNWutesa Package” on page 57

Sun Management Center Software Features

The Sun™ Management Center software monitors managed objects in the Sun Ray system. A *managed object* is any object that can be monitored. Sun Ray nodes contain many managed objects. The Create Topology Object dialog box enables you to create a Sun Ray node. If the Sun Ray package is installed when you create a Sun Ray node, the following managed objects are created by default:

- Sun Ray system
- Sun Ray services
- Failover group
- Interconnect
- Desktops

Each managed object is monitored separately and has independent alarm settings.

For example, in a failover configuration, the group and any part of the group can be monitored—each server and its load, each interconnect, and each appliance. Sun Management Center software also monitors Sun Ray server software daemons that:

- Authenticate users
- Start sessions
- Manage peripheral devices
- Handle DHCP services

After you set an alarm, the Sun Management Center software notifies you when your specified parameter value has been reached. One of these parameters might be how many appliances are on a server. This enables you to monitor possible overload scenarios. Other alarms can be set to notify you when a server, interconnect, or appliance goes down or when a daemon is not running.

The three Sun Management Center components (TABLE 3-1) can be installed on three separate machines.

TABLE 3-1 Three Components of Sun Management Center Software

Component	Function
Console	Enables you to set and view alarms and to request system information. Requests can be automated or on demand.
Server	Processes requests and passes them on to the appropriate agent. The agent returns the requested information to the server, which then forwards it to the console.
Agents	Monitor the system. Agents return the requested information to the server. These agents, based on SNMP (Simple Network Management Protocol), monitor the status of the <i>managed object</i> (server, interface, or appliance).

The Sun Ray system monitoring feature consists of one package. This package, `SUNWutesa`, is installed as part of the Sun Ray server software 1.3. If the Sun Management Center monitoring server is not a Sun Ray server, this package also needs to be added to the Sun Management Center monitoring server. The package contains the localized messages and icons displayed on the Sun Management Center console, a module of Sun Management Center for Sun Ray, and the Sun Ray Management Information Base (MIB). This feature interfaces with the Sun Management Center software using SNMP. For information on additional monitoring programs that interact with Sun Management Center software, see “Using Other Monitoring Programs” on page 56.

Software Requirements

The Sun Ray system monitoring feature has the following software requirements:

- Sun Management Center 2.1.1 or 3.0 software
- Sun Ray server software 1.3

For sizing requirements for the Sun Management Center software, see the *Configuration and Deployment Guide* on

<http://www.sun.com/sunmanagementcenter/docs/index.html> or see the *Sun Ray Server Software 1.3 Installation Guide*.

The Sun Ray module adds the following requirements (TABLE 3-2 and TABLE 3-3) when added to either the Sun Management Center server or agent component:

TABLE 3-2 Additional Requirements for the Server

Component	Size
RAM	8 KB
/opt/SUNWut	602 KB
/opt/SUNWsymon	12 KB

TABLE 3-3 Additional Requirements for the Agent

Component	Size
RAM	1 MB
Swap	1 MB
/opt/SUNWut	602 KB
/opt/SUNWsymon	12 KB
/var/opt/SUNWsymon	0.5 KB

The Sun Ray module adds the following requirements (TABLE 3-4) to the Sun Management Center server and agent components:

TABLE 3-4 Additional Requirements to the Server and Agent Components

Component	Size
RAM	1008 KB
Swap	1 MB
/opt/SUNWut	602 KB
/opt/SUNWsymon	12 KB
/var/opt/SUNWsymon	.5 KB

Note – The Sun Management Center server component has very high resource requirements. It is strongly recommended that you do not install the complete Sun Management Center software on a Sun Ray server, especially if the Sun Ray server is configured for failover.

Installing the Software

The Sun Ray server software includes one package, `SUNWutesa`, for interfacing with Sun Management Center software. If the Sun Ray server software and Sun Management Center software are to run on the same server, different procedures are used, depending on the order in which the software is installed. If the Sun Ray server software and Sun Management Center server component are on separate servers, then this package must be installed on both servers.

Various installation scenarios follow:

- The Sun Ray server software and the Sun Management Center software are on the same server:
 - To install the Sun Ray server software after installing the Sun Management Center software
 - To install the Sun Management Center software after installing the Sun Ray server software

- The Sun Ray server software and the Sun Management Center software are on separate servers:
 - To install the package on separate servers

If you are doing a clean installation of Sun Management Center software and the Sun Ray server software on the same server, it is easier to install Sun Management Center software first.

When you install Sun Management Center software, you are given the option of installing any of the three components on the selected server. If you want to add only the agent to a Sun Ray server, just choose to add the agent component.

After the appropriate hardware configuration product is installed on the server, you can choose to run the setup now or later. When you run the setup, you are prompted for a host name of Sun Management Center server, a seed to generate security keys, a base URL for the console, and if there is a conflict, a different port for the agent. Complete the setup.

Note – To monitor all the servers in a failover group, each server must be running the Sun Ray server software 1.3 and one server must run the Sun Management Center agent component.

▼ To Install the Sun Ray Server Software After Installing the Sun Management Center Software

1. Start the Sun Management Center software:

```
# /opt/SUNWsymon/sbin/es-start -c
```

Check to see if the Sun Management Center works. If not, reinstall the Sun Management Center software. Use the *Sun Management Center 3.0 Software Installation Guide* and the *Sun Management Center 3.0 Software User's Guide* to install the Sun Management Center software.

2. Use the standard Sun Ray installation script to add the Sun Ray module:

```
# utinstall
```

The standard Sun Ray install script automatically stops the Sun Management Center software, adds the Sun Ray module, and restarts the Sun Management Center software.

▼ To Install Sun Management Center Software After Installing Sun Ray Server Software

1. Use the standard Sun Ray installation script:

```
# utinstall
```

The `SUNWutesa` package is installed automatically on the server when `utinstall` installs the Sun Ray server software.

2. Follow the installation instructions found in the *Sun Management Center 3.0 Software Installation Guide* to install the Sun Management Center software.
3. Type the following to enable Sun Ray monitoring:

```
# utsunmc
```

4. Start the Sun Management Center software:

```
# /opt/SUNWsymon/sbin/es-start -c
```

Check to see if Sun Management Center works. If not, reinstall the Sun Management Center software.

▼ To Install the Package on Separate Servers

1. Verify that the Sun Management Center agent package, `SUNWesagt`, is installed on the Sun Ray server:

```
# pkginfo -l SUNWesagt
```

2. Perform a standard installation of the Sun Ray server software:

```
# utinstall
```

Note – The Sun Management Center agents can be installed after the Sun Ray server software install. However, the Sun Ray module must then be enabled by typing `utsunmc`.

Note – The `pkgadd` process stops and restarts the Sun Management Center software.

3. Install the Sun Ray interface package on the Sun Management Center server:

```
# pkgadd -d <mount point>/Sun_Ray_Server_Software_1.3/Solaris_2.6+/Product
SUNWutesa
```

Additional Sun Management Center Modules

There are other useful Sun Management Center modules available to monitor processes and help tune your Sun Ray system. For example, the Health Monitor module monitors resources on the Sun Ray server so you know when to add memory, swap space, or additional CPUs. The Sun Management Center Process Monitoring module helps identify runaway processes and limit multimedia applications.

Setting Up the Monitoring Environment

After installing the Sun Management Center software, you need to set up your monitoring environment. This section contains the following information:

- “Troubleshooting” on page 41
- “Setting Alarms” on page 43

A default administrative domain is automatically created for you based on the Sun Management Center server component. You need to set a home administrative domain. This domain is displayed whenever the console is started.

Next, create the hierarchy of the system you want to monitor. This can be done manually by adding nodes to the administrative domain or by using the Discovery Manager.

▼ To Set Up the Monitoring Environment

1. **After installing the Sun Management Center software, start the console on the server that has the console component installed:**

```
# /opt/SUNWsymon/sbin/es-start -c
```

The login screen is displayed.

2. **Enter your user name and password.**

Specify the Sun Management Center server.

3. **Click Login.**

Two windows are displayed—the Sun Management Center window and the Set Home Domain window.

4. **In the Set Home Domain window, highlight the appropriate domain and click Go To.**

The panels in the Sun Management Center window are populated.

5. **Click Close to dismiss the Set Home Domain window.**

▼ To Create an Object

1. **Expand the Sun Management Center Domains list.**

2. **Select the domain you plan to add an object to.**

The selected domain is displayed.

3. **Select Edit -> Create an Object.**

The Create Topology Object pop-up window is displayed.

4. **On the Node page, enter a Node Label and Description. Then enter the Hostname (server name), IP Address, and Port for the Sun Ray server.**

The port entered here must be the same port you configured (entered) during the installation of the Sun Management Center.

Troubleshooting

Usually, if all the software is installed, the agent for Sun Ray monitoring starts automatically. This section describes two cases where that has not happened.

Case 1

If the Sun Ray server has the Sun Management Center agent component installed, but the Detail window shows no Sun Ray object for the Sun Ray server node, load the Sun Ray module:

▼ To Load the Sun Ray Module

1. Click the Modules tab.

Note where the Sun Ray module is listed (if it is not listed, see Case 2). For the module to be loaded, it should be listed in Modules with Load Status (see FIGURE 3-1). In addition, it should be loaded and enabled.

2. If the Sun Ray module is listed in Available Modules (see FIGURE 3-1), highlight it and then click the Load button.

This loads the module and moves it to the Modules with Load Status list.

3. If the Sun Ray module is disabled, highlight it and then click the Enable button.

This enables the module.

4. Return to the Detail window.

The Detail window shows a Sun Ray object for the Sun Ray server node.

Info Browser Alarms **Modules** View Log Applications Hardware

Modules with Load Status:

Module Name	Loaded	Scheduled	Enabled
Agent Statistics	Yes	No	Yes
Config Reader (Ultra Work...	Yes	No	Yes
Kemel Reader (Simple)	Yes	No	Yes
MIB-II System (Simple)	Yes	No	Yes
Sun Ray	Yes	No	Yes

Unload
Load Now
Edit...
Enable
Disable
Rules...
Load...

Available Modules:

Module Name	Multi-instance
Data Logging Registry	No
MIB-II Proxy Monitoring	Yes

FIGURE 3-1 Module Panel

Case 2

If, after clicking the Modules tab on the Details window of the Sun Ray server node, the Sun Ray module is not listed, activate the Sun Ray module:

▼ To Activate the Sun Ray Module

1. Register the module by typing:

```
# opt SUNWut/sbin/utsummc
```

This command adds the module to the Sun Management Center and starts the agent.

2. If you receive the following message, perform steps 3 and 4.

```
Starting the SunMC agent...

NOTICE:          SunMC agent failed to start.
                  To start it manually run the command
                  /opt/SUNWsymon/sbin/es-start -a
```

3. Check to see if the agent is running:

```
# ps -ef |grep agent
```

If the Sun Management Center agent is running, wait a minute and check the Detail window again.

4. If the agent is not running, type:

```
# /opt/SUNWsymon/sbin/es-start -a
```

This procedure starts the agent.

Setting Alarms

Alarms are used to notify you when errors occur or your performance needs to be tuned. Alarms are triggered (tripped) if:

- A server goes down.
- An interconnect is no longer working.
- An appliance is down or is displaying a green newt cursor.

These alarms are set by default and you can change them. A tuning alarm could be based on the number of active sessions on each server in a failover group to determine if one of the servers is overloaded. You set the thresholds that trigger this type of alarm.

▼ To Set an Alarm

- 1. After creating an object, bring up the Details window of the object (see FIGURE 3-2).**

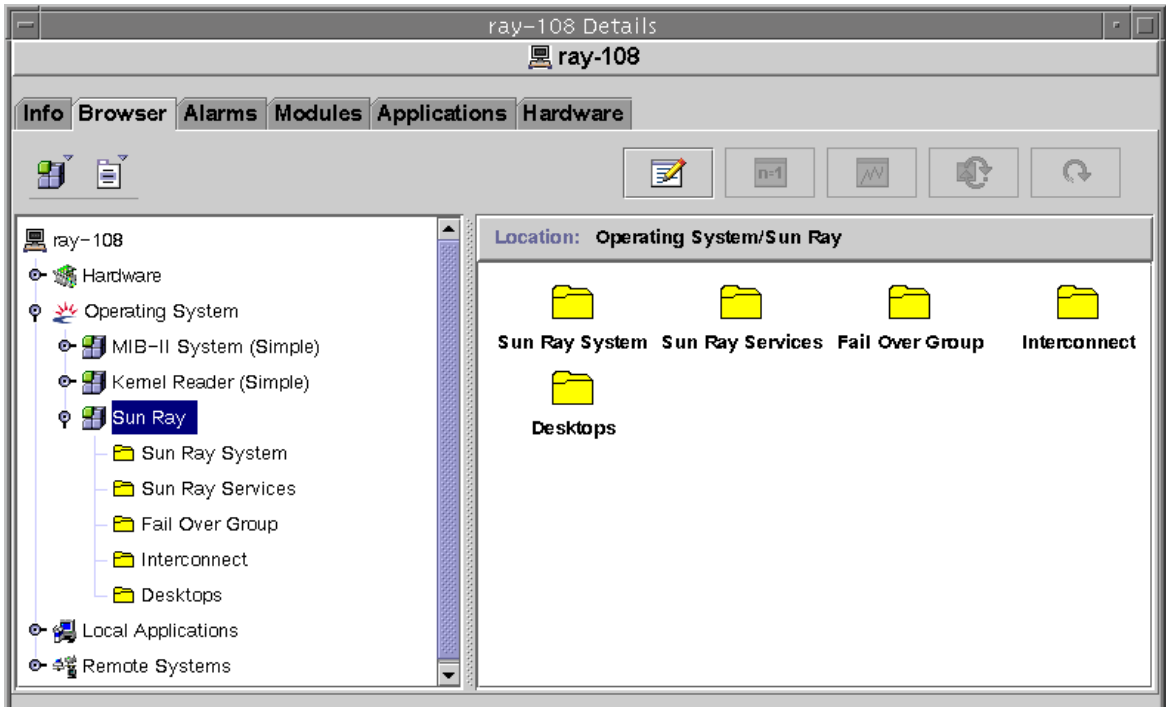


FIGURE 3-2 Sun Management Center Details Window

2. Double-click, for example, Failover Group in the left panel.
3. Right-click the value portion (Status) of the table row (see FIGURE 3-3).

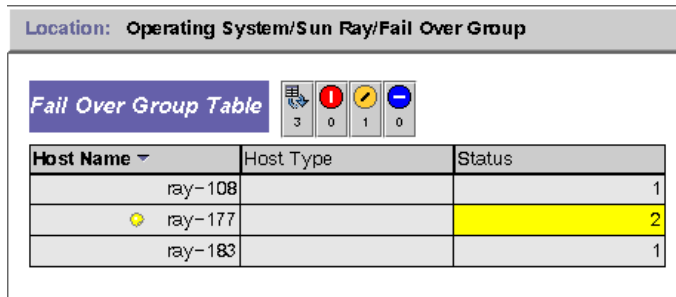


FIGURE 3-3 Example Using the Failover Group Panel

A pop-up menu is displayed.

4. Select Attribute Editor.

The Attribute Editor window for that table entry is displayed.

5. Select the Alarms tab.

See FIGURE 3-4.

The possible alarm values are:

- Critical Threshold (>)
- Alert Threshold (>)
- Caution Threshold (>)
- Critical Threshold (<)
- Alert Threshold (<)
- Caution Threshold (<)

6. Supply an appropriate number for the type of alarm that you choose to monitor.

In this example, the Alert Threshold alarm is set at greater than 1 to notify you when that server in the failover group is down.

7. Click the Apply button to save the value of the alarm and continue setting other values in the Attribute Editor

8. Click the OK button, which saves the value of the alarm and closes the window.

As soon as you set an alarm it takes effect.

9. Select the Actions tab and enter an action to perform.

Here you can also specify an action such as sending email or running a script for each alarm.

10. Select the Refresh tab to set the number of seconds between pollings.

The default value is 300 seconds (5 minutes).

11. Select the History tab to view information about the log file that records monitored values.

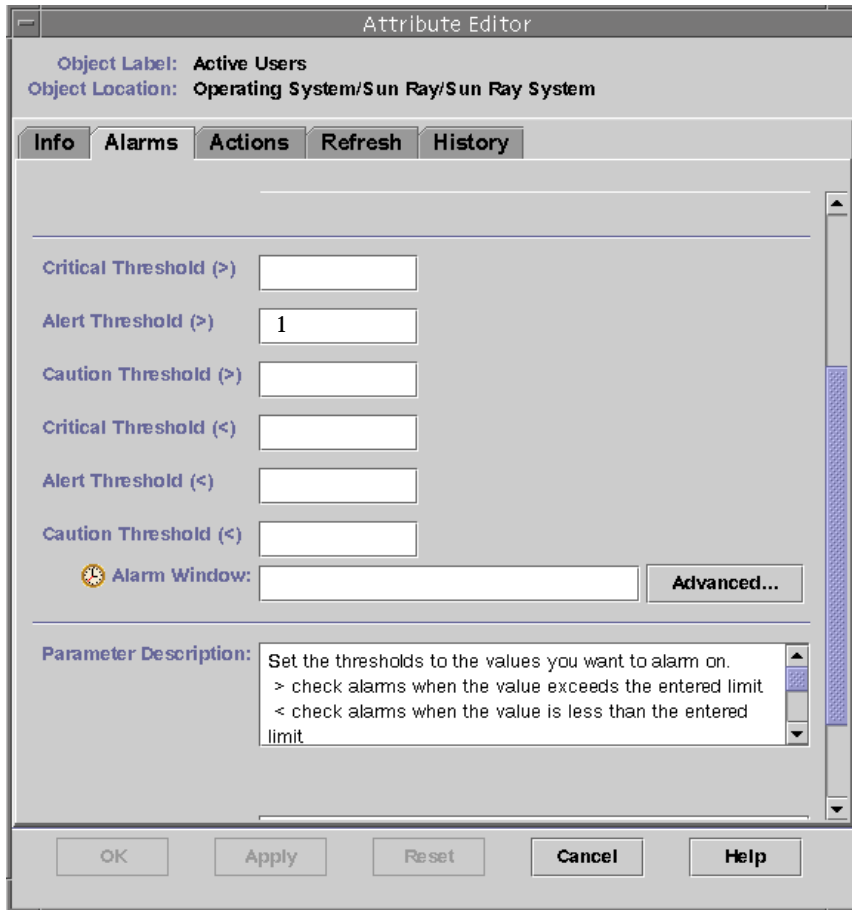


FIGURE 3-4 Alarm Window

If an alarm is tripped, a critical alarm displays as red, an alert alarm displays as yellow, and a caution displays as blue. See FIGURE 3-5 for an example of an alert alarm.

▼ To Start Monitoring

1. Start the Sun Management Center software:

```
# /opt/SUNWsymon/sbin/es-start -c
```

A window for the Default domain is displayed.

2. Highlight the appropriate domain and click Go To.

3. When the console GUI is displayed, close the Domain window by clicking Close.
4. Double-click the server in either panel.
The server Details window is displayed.
5. Expand the hierarchy in the left or right panel until it displays the level you want.

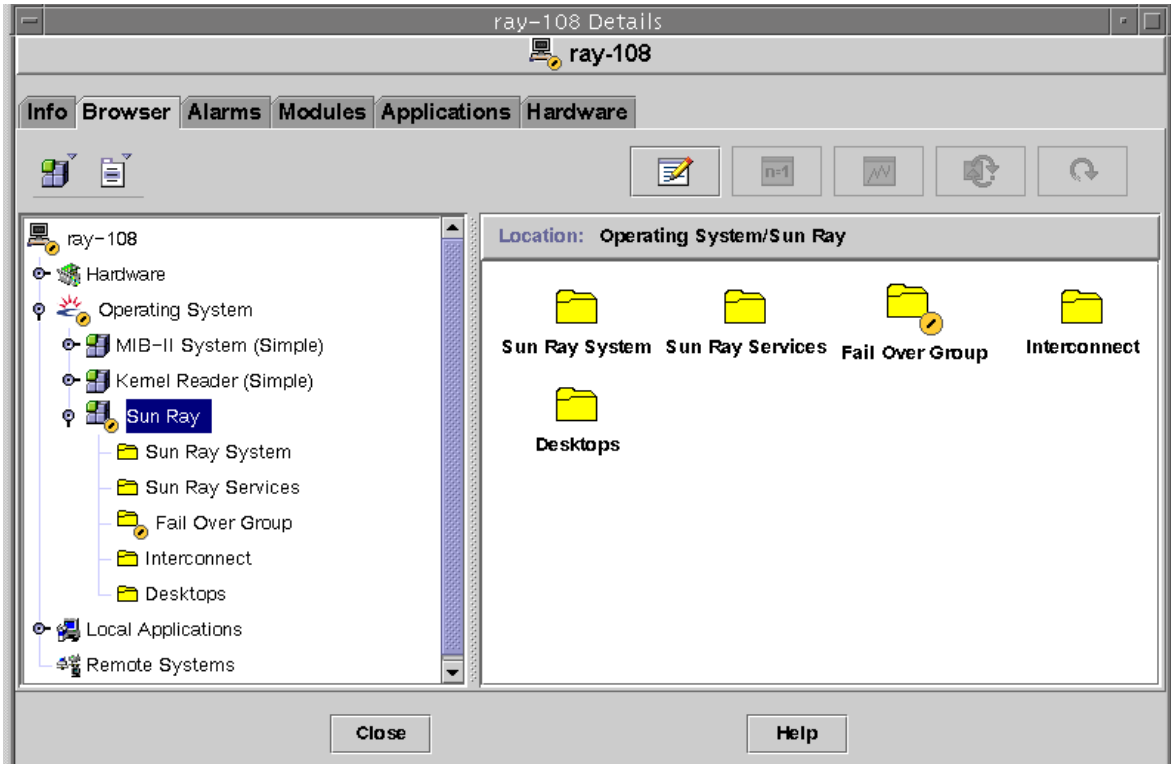


FIGURE 3-5 Details Window With Alarms

This console Details window (see FIGURE 3-5) shows the hierarchical details of your system. You can immediately see if any alarms have been tripped. An alarm's area and type appear in the left panel as a colored circle with a bar. The Alert alarm also shows up on the title bar by the server node name and at the Operating System, Sun Ray, and Failover Group levels. Double-clicking the area where an alarm icon is present updates the right panel with the detailed information. If you position the mouse pointer over one of the colored circles in either panel, a pop-up window is displayed detailing the alarm information.

If you click the Alarms tab in the Details window, a window is displayed that lists a summary of all the current alarms. When you stop the Sun Ray services (daemons), the alarms display as shown in FIGURE 3-6.

The screenshot shows a window titled "Alarm Summary Window" with a toolbar at the top containing icons for refresh, search, and print. Below the toolbar, it displays "Last Refresh: Apr 05 16:56:01". The window shows "Current Page: 1" and navigation buttons. Below that, it states "Total Alarms for Object: 12". The main content is a table with the following data:

Severity	Start time	State	Action	Message
Blue	Apr 04 14:05:27	Yellow	Green	Sun Ray utsessiond Instances < 2
Blue	Apr 04 14:05:27	Yellow	Green	Sun Ray utdevmgrd Instances < 2
Blue	Apr 04 14:05:27	Yellow	Green	Sun Ray utseriald Instances < 2
Red	Apr 04 14:05:27	Yellow	Green	Sun Ray Up Time (1/100ths sec.) Session Manager down
Blue	Apr 04 14:05:27	Yellow	Green	Sun Ray utparalleld Instances < 2
Yellow	Apr 04 14:05:26	Yellow	Green	Sun Ray utauthd Status > 1
Yellow	Apr 04 14:05:26	Yellow	Green	Sun Ray utsessiond Status > 1
Yellow	Apr 04 14:05:26	Yellow	Green	Sun Ray utdevmgrd Status > 1
Yellow	Apr 04 14:05:26	Yellow	Green	Sun Ray utseriald Status > 1
Yellow	Apr 04 14:05:26	Yellow	Green	Sun Ray utparalleld Status > 1
Yellow	Apr 04 14:05:26	Yellow	Green	Sun Ray in?2edhcpd Status > 1
Yellow	Apr 04 14:05:26	Yellow	Green	Sun Ray rpc?2ebootparamd Status > 1

FIGURE 3-6 Alarm Summary Window

At the top of the right panel (see FIGURE 3-7), a list details the total number of alarms set for the area, and the number of critical alarms (red), alert alarms (yellow), and caution alarms (blue) that are tripped. More specific details are displayed in a table in the right panel. Some of the cells in the table, when a mouse-over event occurs, display a pop-up window giving the current status and when it last changed. This window is called a *Tool Tip window*, and shows the type of alarm, its value, and when it occurred or when the last alarm was cleared. The Tool Tip time can also be the last time the agent was restarted.

For example, on the Sun Ray System panel, a Tool Tip for Up Time (1/100ths sec.) would be:

Clear. Up Time (1/100th sec.) OK Status changed Mar. 6, 15:23:55.

This tip states that the server was restarted and the alarm cleared on March 6 at 15:23:55. Similar information is provided for Active Sessions, Total Sessions, Active Desktops, and Active Users.

Setting Monitoring Guidelines

There are five managed objects that you can monitor:

- Sun Ray System—Describes the Sun Ray server and load information
- Sun Ray Services—Describes the Sun Ray daemons on a Sun Ray server
- Failover Group—Lists all the servers in the group
- Interconnect—Lists all the interfaces on a Sun Ray server
- Desktops—Lists all monitored appliances (desktops) and appliances that have exceptions that are connected to a Sun Ray server

Sun Ray System Panel

The Sun Ray System panel displays an overview of your Sun Ray system. From this window you can set specific alarms to monitor the server and its load.

▼ To Display the Sun Ray System Panel

- Double-click the Sun Ray System icon in the left panel.

The Operating System/Sun Ray/Sun Ray System panel is populated. See FIGURE 3-7.

The screenshot shows a management console interface. On the left is a tree view of system components. The 'Sun Ray System' folder is selected and highlighted in blue. The right pane displays the 'Sun Ray System' panel, which includes a title bar with the location 'Operating System/Sun Ray/Sun Ray System', a status bar with the title 'Sun Ray System' and four status icons (a list icon, a red circle with a white exclamation mark, a yellow circle with a white checkmark, and a blue circle with a white minus sign), and a table of properties.

Property	Value
Host Name	ray-108
Contact Name	System Admin
Up Time (1/100ths sec.)	59098900
Version	1.3_01.a,REV=2001.02.06.17.35
Install Date	Feb 16 2001 15:37
Patch Information	
Active Sessions	0
Total Sessions	0
Active Desktops	0
Active Users	0
Policy	-a -g -z both

FIGURE 3-7 Sun Ray System Panel

▼ To Refresh the Sun Ray System Panel

- **Click the refresh button (circular arrow in the upper right corner).**

The entire system panel is refreshed (see TABLE 3-5).

The Up Time, session, appliance (desktop), and user information is refreshed periodically based on the number of seconds you set in the Attribute Editor. However, the console is updated only every five minutes unless an alarm occurs. The number of seconds set in the Attribute Editor only changes how soon an alarm is triggered.

Note – It is not recommended to set the seconds to less than 60 since the load interferes with the Sun Ray server performance.

In this panel, you set alarms to monitor the status of the server; how many sessions, users, or appliances are active; and how many total sessions exist.

▼ To Set Alarms

1. **Click the Value cell of the Property you want to set an alarm for with the right mouse button.**
2. **Select Attribute Editor.**
3. **Click the Alarms tab.**
4. **Enter a value for each threshold you want to monitor.**
5. **Click OK.**

TABLE 3-5 Properties on the Sun Ray System Panel

Property	Value
Host Name	Name of server that was queried. This information is obtained when Sun Ray System is selected or on refresh.
Contact Name	This information is obtained when Sun Ray System is selected or on refresh.
Up Time (1/100ths sec.)	Number of 1/100th seconds since the last of all the daemons critical to the Sun Ray server was started. A value of 0 means the server is down and an alarm is tripped. The default refresh rate is 300 seconds.
Version	List of version, build, and date of build of the Sun Ray server software. This information is obtained when Sun Ray System is selected or on refresh.

TABLE 3-5 Properties on the Sun Ray System Panel *(Continued)*

Property	Value
Install Date	Date the Sun Ray server software was installed. This information is obtained when Sun Ray System is selected or on refresh.
Patch Information	List of Sun-Ray-specific patches. This information is obtained when Sun Ray System is selected or on refresh.
Active Sessions	Number of sessions based on logged-in sessions with a smart card plugged in, plus sessions for appliances logged in without smart cards. Set an alarm here to watch for overloading of this server. The default refresh rate is 300 seconds.
Total Sessions	Number of active and suspended sessions. The default refresh rate is 300 seconds.
Active Desktops	Number of connected appliances. The default refresh rate is 300 seconds.
Active Users	Number of currently active users. When pseudo tokens are allowed (this is a policy setting), this number includes appliances at the login prompt. The default refresh rate is 300 seconds.
Policy	The policy that has been set (see <i>Sun Ray Server Software 1.3 Administrator's Guide</i> for details). This information is obtained when Sun Ray System is selected or on refresh.

Sun Ray Services Panel

The Sun Ray Services panel displays the status of the Sun Ray daemons. If, for example, `utauthd` is not running, all of the user sessions are disconnected.

On the Sun Ray Services panel (see FIGURE 3-8), default alarm values are set for the status of each daemon and the number of instances. You can reset them if you want to do so.

Location: Operating System/Sun Ray/Sun Ray Services

Services Table

Daemon	Status	Started Time	Last Changed	Instances	Description
dsservd	1	982367108	982367108	1	LDAP daemon
httpd	1	982367024	982367024	1	Web Admin dae...
in.dhcpd	1	982366873	982366873	1	DHCP daemon
utauthd	1	982367119	982367119	1	Auth Manager
utdevmgrd	1	982367118	982367118	2	Device Manager
utparallelid	1	982367118	982367118	2	Parallel Device ...
utserialid	1	982367118	982367118	2	Serial Device d...
utsessiond	1	982367118	982367118	2	Session Manager

FIGURE 3-8 Sun Ray Services (daemons) Panel

The Status values are: 1, the daemon is running; 2, the daemon is down. The reason that some of the daemons have two instances is that they have two functions: one to listen and one to interact.

Failover Group Panel

The Failover Group panel displays the topography of your failover group (see FIGURE 3-9). The panel lists the primary and secondary servers and their status. The active monitoring server is listed first.

Location: Operating System/Sun Ray/Fail Over Group

Fail Over Group Table

Host Name	Host Type	Status
ray-108	secondary	1
ray-177	secondary	2
ray-183	primary	1






FIGURE 3-9 Failover Group Panel

If the Status is 1, the server is running. If the Status is 2, the server is down and there is one Alert (yellow) alarm.






Interconnect Panel

The Interconnect panel lists all the network interfaces usable by the Sun Ray server (see FIGURE 3-10).

Location: **Operating System/Sun Ray/Interconnect**

DHCP Table     

Network Name	Available Addresses
SunRay-hme1	73

Interface Table     

Entry Name	Status	Address	Netmask	Last Packet Seen (1/100ths sec)	Lan Type
hme0	1	192.9.116.108	255.255.255.0	1700	LAN
hme1	1	192.168.128.1	255.255.255.0	1700	

FIGURE 3-10 Interconnect Panel

If the Status is 1, the interface is up. If the Status is 2, the interface is down.

The DHCP Table lists the interfaces that are used for the Sun Ray interconnect. Available Addresses lists the number of addresses available for new end users. The alarms that are set here let the system administrator know when the Sun Ray server is running out of addresses to give to users.

The Interface Table lists all the interfaces on the Sun Ray server. The Address is the IP address for the interface. You entered this address as the Net Mask when you first configured your system.

▼ To Set an Alarm for Running Out of Addresses

1. Click the Available Addresses cell in the DHCP Table using the right mouse button.
2. Select Attribute Editor.
3. Click the Alarms tab.
4. Enter the number of addresses left when an alarm should be tripped.
5. Click OK.

Desktops Panel

The Desktops panel is where you can select individual appliances to monitor (see FIGURE 3-11). The possible values for the status of the appliances are: 1, running; 2, down; and 3, displaying the green newt cursor (see *Sun Ray Server Software 1.3 Administrator's Guide* for details). The default polling time is 300 seconds (5 minutes).

Appliances can be added and deleted from the Monitored Desktops list.

In a failover group, you can monitor any desktop from any server.

▼ To Add an Appliance to Be Monitored

1. **Click Name using the right mouse button.**

A pop-up window is displayed.

2. **Click Add Row.**

A pop-up window is displayed.

3. **In the Add Row window, enter the MAC address of the appliance you want to monitor in the Name field.**

4. **Click OK.**

▼ To Delete an Appliance to Exclude Monitoring

1. **Using the right mouse button, click the cell containing the MAC address.**

A pop-up window is displayed.

2. **Click Delete Row.**

A pop-up window is displayed.

3. **Confirm the deletion by clicking Yes on the pop-up window.**

Sample results of polling the Desktops are provided below.

:

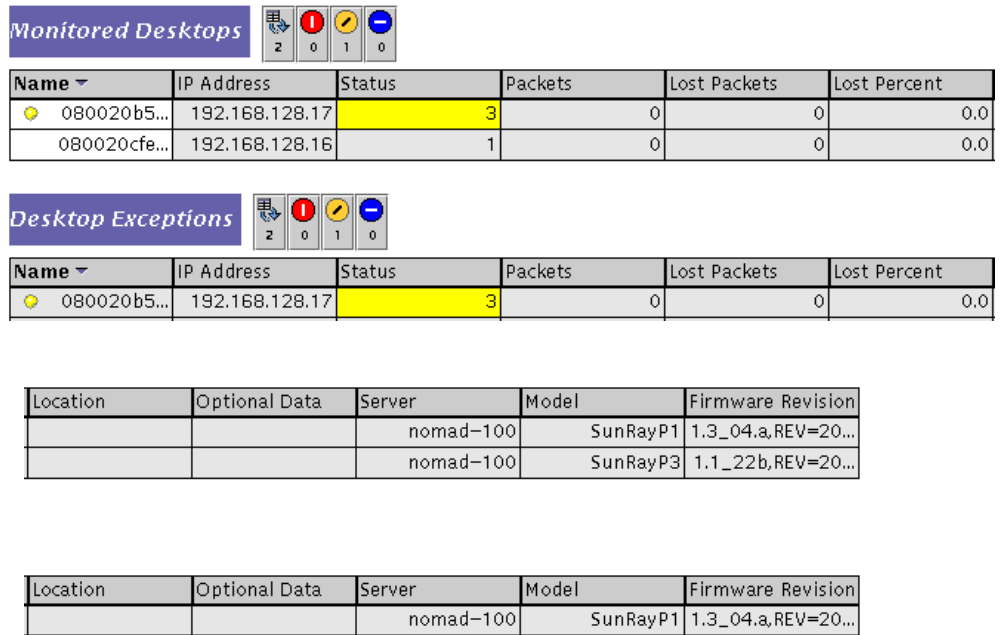


FIGURE 3-11 Desktops Panel

TABLE 3-6 describes the information in each column:

TABLE 3-6 Desktop Information

Property	Value
Name	Ethernet or MAC address of the appliance
IP Address	Assigned DHCP address of the appliance
Status	1 running, 2 down, and 3 displaying the green newt cursor
Packets	Number of packets received by the appliance
Lost Packets	Number of packets the appliance reported lost
Lost Percent	Percentage of packets lost
Location	Optional field; information supplied by system administrator
Optional Data	Optional field; information supplied by system administrator

TABLE 3-6 Desktop Information *(Continued)*

Property	Value
Server	Server that owns the appliance
Model	The type of appliance: SunrayP1 (Sun Ray 1), SunrayP2 (Sun Ray 100), or SunrayP3 (Sun Ray 150)
Firmware Revision	List of version, build, and build date

Using Other Monitoring Programs

System administrators using HP OpenView™VPO, Tivoli TMS, or CA Unicenter can also monitor Sun Ray servers. An interoperability interface exists between each of these packages and the Sun Management Center software. These interfaces translate Sun Management Center alarms appropriately so that you are notified when problems arise. These interfaces also enable you to view the server status. Hewlett-Packard provides the interface needed between HP OpenView™VPO and Sun Management Center. Sun provides the interface needed between Sun Management Center and Tivoli TMS or CA Unicenter (see FIGURE 3-12).

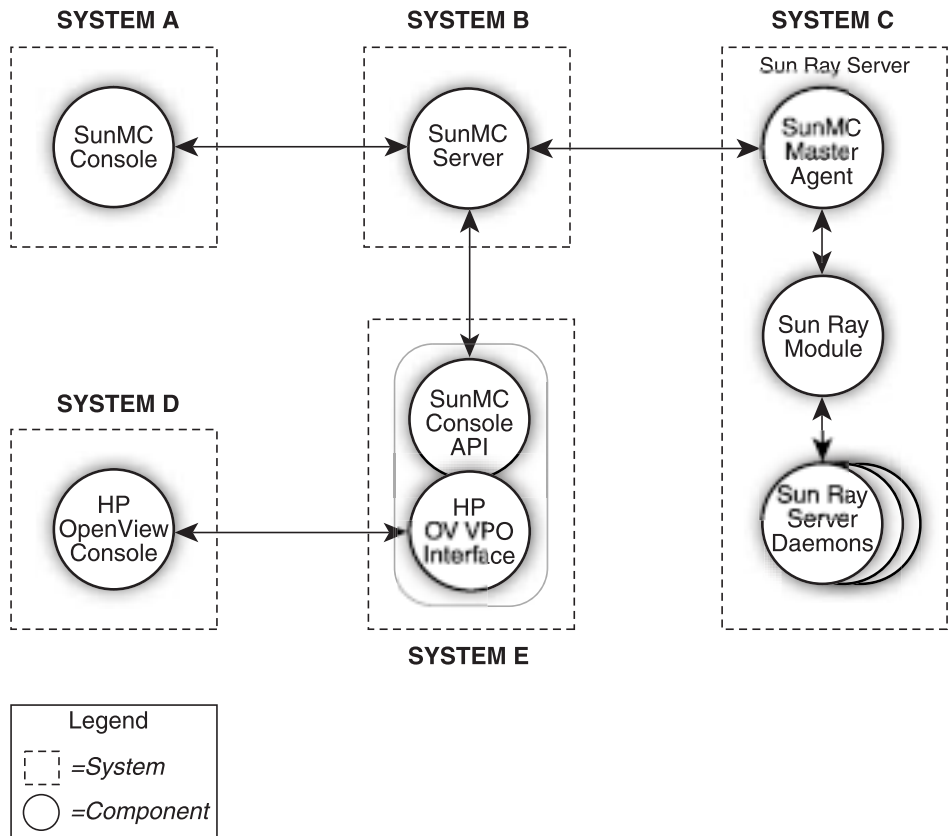


FIGURE 3-12 Example of Interoperability

Note – In the example, System B, System C, and System E must be SPARC Solaris systems.

Removing the SUNWutesa Package

The `SUNWutesa` package is installed automatically when `utinstall` installs the Sun Ray server software.

▼ To Remove the SUNWutesa Package

- To unregister the module on the Sun Ray server, type:

```
# utsunmc -u
```

- To remove the package on the SunMC server, type:

```
# pkgrm SUNWutesa
```

Controlled Access Mode

This chapter describes the new feature Controlled Access Mode (CAM) as well as how to deploy, install, and configure your system to allow controlled, simplified access to anonymous users without compromising the Sun Ray server's security.

Topics include:

- “Controlled Access Mode Functionality” on page 59
- “Enabling Controlled Access Mode” on page 60
- “Building the Controlled Access Mode Environment” on page 63
- “Advanced Application Setup” on page 67
- “Security and the Controlled Access Mode Environment” on page 69
- “Failover” on page 69
- “Localization” on page 69

Controlled Access Mode Functionality

The Sun Ray system is well-suited to host a CAM application, such as public terminals in an airport. In CAM, a user accesses only specified applications. The user does not need to pass security to log in or use a smart card.

Enabling Controlled Access Mode

The CAM feature is administered through the Sun Ray Administration Tool.

CAM is a policy decision affecting system-level operations (see the *Sun Ray Server Software 1.3 Administrator's Guide* for details). Use of this mode requires additional configuration steps and selections made using the Administration Tool. You turn the Controlled Access Mode on and off in the Change Policy section of the Admin function of the Administration Tool. The CAM Policy option can be enabled for all users: smart card, non-smart card, or both.

The Sun Ray policy turns the Controlled Access Mode on and off. When Controlled Access Mode is turned on, `kiosk.start` uses scripts to choose temporary users and home directories and then uses the `kiosk.conf` file to configure and populate the user's environment, and launch enabled applications. When a session terminates, `kiosk.start` cleans up all the files and entries related to the session, then recreates the environment for a new user.

Note – Configure CAM on the primary server in a failover environment using `utconfig`.

▼ To Enable Controlled Access Mode

1. **Start the Administration Tool.**
2. **Select the arrow to the left of Admin to expand the navigation menu.**
3. **Click the Policy link.**
4. **For smart card users, select the Controlled Access Mode check box in the Card Users column.**
5. **For non-smart card users, select the Controlled Access Mode check box in the Non-Card Users column.**

All smart card users get a Controlled Access Mode session. See FIGURE 4-1.



FIGURE 4-1 Change Policy Window

6. Click the **Apply** button.
7. Select the **Reset Services** menu.
8. Under **Scope**, click the **Local** or **Group** radio button, depending on the failover scenario.

▼ To Configure CAM Settings

1. Click the arrow to the left of **Controlled Access Mode** in the navigation menu.
2. Click the **Settings** link.

This panel is where the action parameters are set for the Controlled Access Mode (see FIGURE 4-1). The values define how a session is managed.

3. Click the **Submit Changes** button to store the action parameters in the `/var/opt/SUNWut/kiosk.conf` file, which is the **Controlled Access Mode configuration file**.

The Controlled Access Mode Configuration panel is displayed. The default settings for each controlled access mode session can be edited from this panel (see FIGURE 4-2). The Card Session Action option determines if card sessions remain resident after a card is removed. If you choose the option to kill the session (the default), the Timeout text box value determines how long to wait before killing the session.

Controlled Access Mode Configuration Server: nomad-100

Card Session Action: Suspend session upon removal of card
 Kill session upon removal of card

Timeout (seconds):

Maximum CPU Time (seconds):

Maximum VM (KB):

Maximum File Size (512 Byte Blocks):

FIGURE 4-2 Controlled Access Mode Configuration Panel

The default values in the maximum CPU, VM, and File Size text boxes are set using the `ulimit` command. These limits contain the CAM user processes.

4. Click the **Confirm** link in the navigation menu to save the changes.
5. Click the arrow to the left of **Admin** to expand the navigation menu.
6. Click the **Reset Services** link.
7. Select the **Local** or **Group** radio button, depending on the failover scenario.

Building the Controlled Access Mode Environment

If CAM is simply enabled, `dtsession` is launched by default and provides the basic Controlled Access Mode function. Additional applications need to be added to the user's session to extend this basic functionality. Possible applications include:

- Browser (You can use the demonstration version of the Controlled Browser on the Sun Ray 1.3 CD-ROM. See Appendix A.)
- Clock
- Calculator
- Custom application

Note – You must complete your additions and edits in the Add/Edit Apps section (see FIGURE 4-3) and your selections in the Select Applications section before clicking the Confirm link.

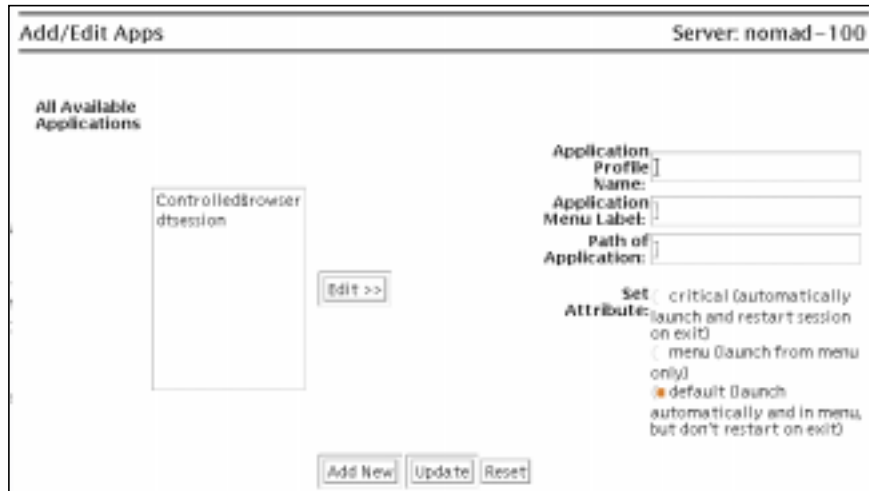


FIGURE 4-3 Add/Edit Apps Panel

▼ To Add a New Application

1. **Click the Add/Edit Applications link from the Controlled Access Mode menu.**

The Add/Edit Apps window is displayed.

2. **Enter a profile name, a menu label, and a path to the application.**

In the Path of Application text field:

- List the full path with command-line options or
- Point to a script that you want to run at session start up (see “Advanced Application Setup” on page 67)

3. **Set the application behavior by clicking one of the radio buttons.**

4. **Click the Add New button.**

The new application is added to the Available Applications list.

5. **Click the Confirm link.**

The confirm panel is displayed.

6. **Click the Confirm Configuration button.**

The Confirm link sends `kiosk.conf` information to the internal Sun Ray database which is then replicated to the failover group. After defining a user's session by writing the `kiosk.conf` file, failover services must be restarted to propagate the configuration to all the servers in a failover group.

▼ To Edit an Available Application

1. **Click the Add/Edit Applications link from the Controlled Access Mode menu.**

The Add/Edit Apps window is displayed.

2. **Highlight the application in the All Available Applications list that you want to change and click the Edit button.**

The fields on the right are populated.

3. **Make the changes and click the Update button.**

The application information is updated.

4. **Click the Confirm link.**

The confirm panel is displayed.

5. **Click the Confirm Configuration button.**

Note – You cannot edit `dtsession`.

6. If the application is enabled, click the **Reset Services** link in the **Admin** menu.
7. Click the **Restart** button.
8. To enable the newly added application, go to the **Select Applications** panel and add the application to the **Applications to Launch** list.

All applications must be accessible to all servers in the failover group. Add new applications to all servers in a failover group. See FIGURE 4-4.

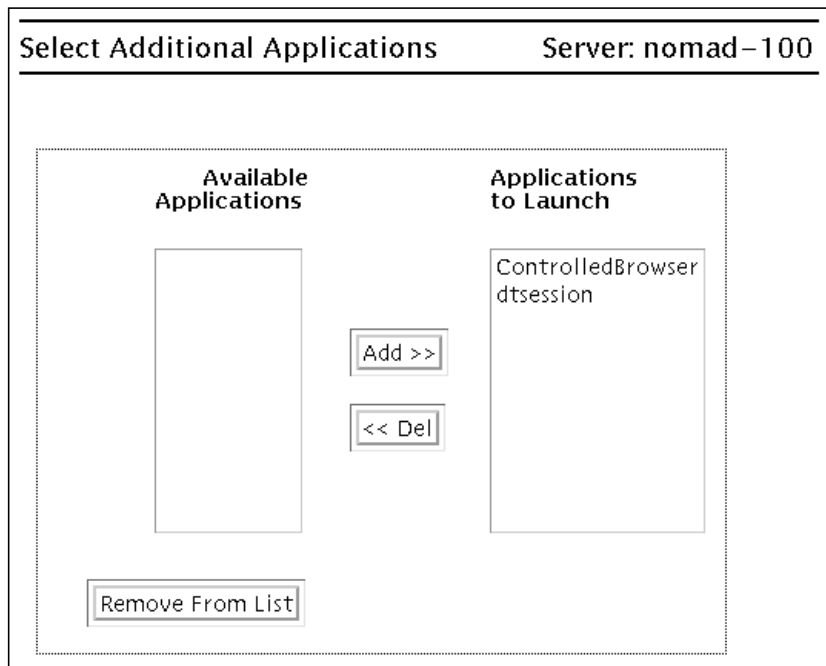


FIGURE 4-4 Additional Applications Configuration Panel

▼ To Make an Application Available to Users

1. Choose **Select Applications** from the **Controlled Access Mode** menu.

This panel lists the other applications that are available for the user's sessions. In FIGURE 4-4, there are default applications and two possible additional applications you can make available to the user.

2. **In the Available Applications column, highlight the application that you plan to add.**
3. **Click the Add button to add it to the Applications to Launch column.**
4. **Click the Confirm link.**
The confirm panel is displayed.
5. **Click the Confirm Configuration button.**
6. **Under the Admin menu, click the Reset Services link.**
7. **Click the Restart button.**

▼ To Make an Application Not Available to Users

1. **From the Controlled Access Mode menu, click the Select Applications link.**
2. **In the Applications to Launch list, highlight the application that you want to make unavailable.**
For more detail, see FIGURE 4-4.
3. **Click the Del button.**
This moves the application back to the Available Applications list.
4. **Click the Confirm link.**
The confirm panel is displayed.
5. **Click the Confirm Configuration button.**
6. **Under the Admin menu, click the Reset Services link.**
7. **Click the Restart button.**

▼ To Remove an Application

1. **From the Controlled Access Mode menu, click the Select Applications link.**
2. **In the Available Applications list, highlight the application that you want to remove.**
For more detail, see FIGURE 4-4.
3. **Click the Remove From List button.**
This completely removes the application.

4. Click the Confirm link.

The confirm panel is displayed.

5. Click the Confirm Configuration button.

If, for example, you want to change a default application to be a critical application, you must edit the application and change the attribute to critical.

Advanced Application Setup

To customize the CAM user's environment further, you can use prototypes or wrapper scripts to enhance application behavior.

Enabling Prototypes

Prototypes enhance application behavior by providing files in the user's home directory specific to that application.

Note – The name of the prototype directory must match the name given in the Application Profile Name field of the Administration Tool when you add new applications.

▼ To Enable Prototypes

- 1. Create a directory with the same name as the application profile name provided in the Add/Edit Applications section of the Administration Tool:**

```
/var/opt/SUNWut/kiosk/prototypes/application_profile_name
```

- 2. Populate the new prototype directory with files specific to that application:**

```
files/directories to be copied into the user's home directory
```

If the application is enabled, everything below the prototype directory is copied recursively to each user's home directory at runtime by the Controlled Access Mode startup scripts. For example, at runtime, there is a `dtsession` prototype directory that matches the application profile name, `dtsession`.

- The application name is `dtsession`.
- The prototype directory is
`/var/opt/SUNWut/kiosk/prototypes/dtsession`.
- The prototype directories and files are
`/var/opt/SUNWut/kiosk/prototypes/dtsession/.dt`
- The files and directories at the `.dt` level are copied to the user's home directory
(`/HOME/user1/.dt`) at runtime.

Using Wrapper Scripts to Customize Controlled Access Mode Applications

If an application requires specific environment variables to be set or if you need to launch the application instead of simply providing the path to the application with options, you can use a wrapper script.

▼ To Launch an Application Using a Wrapper Script

1. **When you add the application using the Administration Tool, provide the path to the wrapper script instead of a path to the executable:**

```
/opt/SUNWut/kiosk/bin/dtsession
```

This example wrapper script customizes the right-click menu button to reflect application labels for menu or default-attributed applications. The script then launches `dtsession`.

2. **Alternatively, put the wrapper script in the directory where the Controlled Access Mode program checks for wrapper scripts:**

```
/opt/SUNWut/kiosk/wrappers
```

In this case, the wrapper scripts must have the same name as the Application Profile Name that is entered in the Add/Edit Applications tab. Refer to an example of a wrapper script, `ControlledBrowser`, which is installed when `cbinstall` is executed. The `cbinstall` script is found in the Supplemental directory on the CD-ROM in the `/opt/SUNWut/kiosk/wrappers` directory.

Security and the Controlled Access Mode Environment

Since Controlled Access Mode bypasses a login mechanism, you must consider the security of the applications added to the user environment. Many custom applications provide built-in security while other applications do not and, therefore, are not suitable for Controlled Access Mode.

For example, adding an application, such as `xterm`, provides users with access to a command-line interface from a Controlled Access Mode session. This would not be desirable in a public environment and is not advised. However, using a custom application for a call center would be an ideal situation. See Appendix A for an example of an application modified for Controlled Access Mode.

Failover

In a failover environment, the administrative settings in the `kiosk.conf` file are copied to the failover servers. You must be sure that all application paths added to the Controlled Access Mode sessions are copied across the servers in the failover group. For example, if the Netscape application is added to the sessions with the executable path, `/usr/local/exe/netscape`, make sure that the path to the binary is available to all servers in the failover group.

Note – Applications must be installed in the same location and set up the same way on each server in the failover group.

Localization

Controlled Access Mode sessions use their server's default locale.

▼ To Change the Locale for the Controlled Access Mode Sessions Without Changing the System Locale

- Add the following line to the end of the `/etc/default/init` file:

```
LANG=new-locale
```

The new locale is used by the Controlled Access Mode sessions.

Note – Adding this line changes the locale for all users on this server.

Multihead Feature on Sun Ray Appliances

The multihead feature on Sun Ray™ appliances enables users to control separate applications on multiple screens using a single keyboard and pointer device attached to the primary appliance. 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 2 and 16 appliances controlled by one keyboard and mouse, may be composed of Sun Ray 1, Sun Ray 100, and Sun Ray 150 appliances. Each appliance presents an X screen of the multihead X display.

Note – For multihead to function properly, you must be in administered mode; therefore, you must run `utconfig` before you run `utmhconfig` and `utmhadm`.

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 appliance, which is the appliance that controls the other appliances 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 appliances controlled by a primary appliance to which a keyboard and pointer device, such as a mouse, are connected. See FIGURE 5-1. This group, which can contain a maximum of 16 appliances, is connected to a single session.

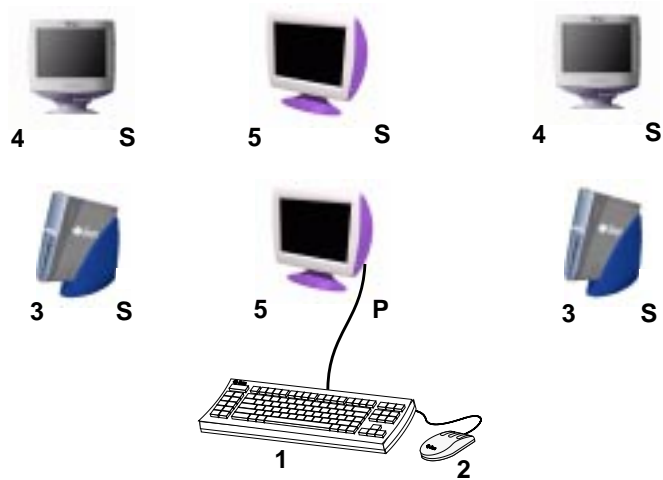


FIGURE 5-1 A Multiheaded Group

Legend:

- 1. Keyboard
- 2. Mouse
- 3. Sun Ray 1 appliance
- 4. Sun Ray 100 appliance
- 5. Sun Ray 150 appliance
- P = Primary appliance
- S = Secondary appliance

Unless XINERAMA is enabled (see “XINERAMA” on page 78 for more details), sessions will have a separate CDE toolbar (with separate workspaces) per screen. A window cannot be moved between screens.

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

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

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

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 FIGURE 5-2 indicates that the user is on the second screen of a three-screen display.



FIGURE 5-2 The Multihead Screen Display

Display Resolution

All the monitors in a workgroup must have the same resolution to avoid panning. However, if the resolution differs among monitors within a workgroup, designate the lowest resolution monitor as the primary monitor and the others as the secondary monitors, since the primary monitor sets the resolution for all secondary monitors.

The auto-size feature sets the user's X server display dimensions automatically to match the preferred resolution supported by the primary appliance 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 movement on your screen 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
# /etc/init.d/utsvc restart
```

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

Note – The `/etc/init.d/utsvc restart` command should be issued 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 the 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.**
See FIGURE 5-3.

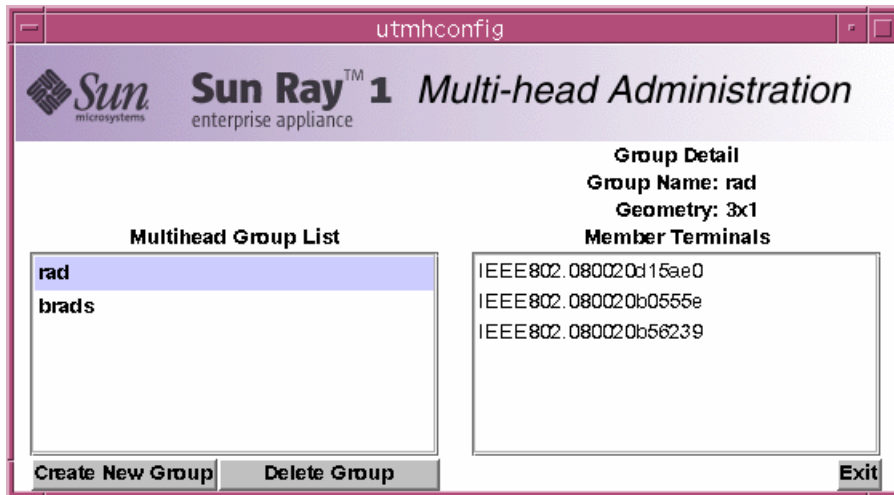


FIGURE 5-3 Multihead Group List With Group Detail

The Create New Multiheaded Group pop-up dialog box is displayed. See FIGURE 5-4. The number of rows and the number of columns you enter are displayed as the group geometry when the group has been created. See FIGURE 5-3.

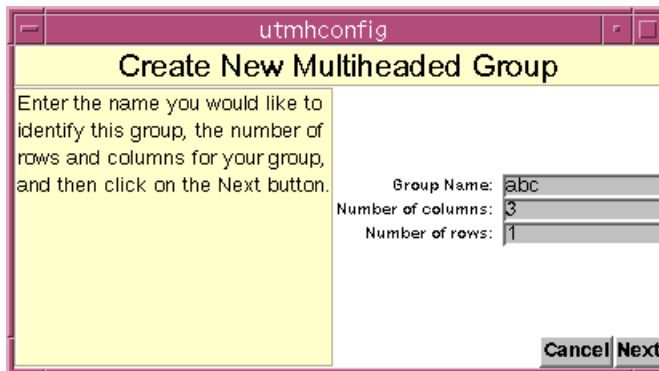


FIGURE 5-4 Create New Multiheaded Group Pop-up Dialog Box

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. See FIGURE 5-5.



FIGURE 5-5 Setup Display for the New Multihead Group

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

The Finish button, which was previously grayed out, is now active. See FIGURE 5-6.

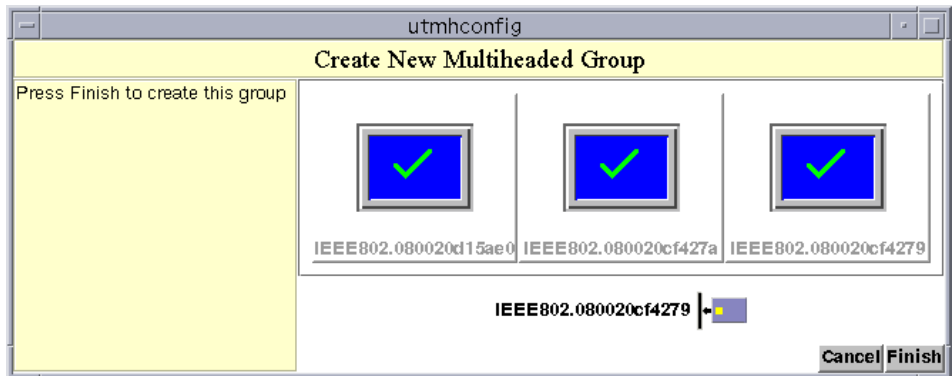


FIGURE 5-6 Completed Multihead Group List With Active Finish Button

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

XINERAMA

The XINERAMA extension to X11 creates 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. XINERAMA is supported in both the Solaris 7 and Solaris 8 operating environments.

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.

Note – XINERAMA consumes more CPU, memory, and network bandwidth.

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 an appliance that is not part of a multihead group—that is, an appliance 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 an appliance connects to the Authentication Manager or a new smart card is inserted, the TerminalGroup module queries its database to determine whether the appliance is part of a multihead group and, if so, whether the appliance is a primary or secondary appliance of that group. If it is not identified as part of a multihead group, the appliance is treated normally.

If the appliance is determined to be part of a multihead group and it is the multihead group's primary appliance, a normal session placement occurs. If a session does not exist on the current server, but there is a preexisting session for the appliance or smart card on another server in the failover group, the primary appliance 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. See FIGURE 5-7.

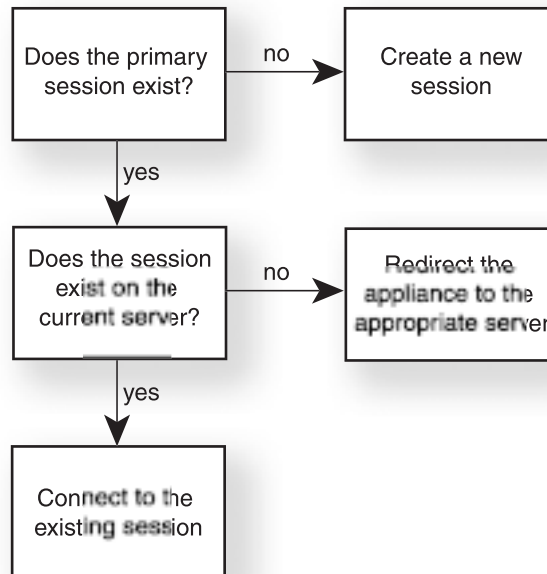


FIGURE 5-7 Authentication Manager Flowchart for the Primary Appliance

If an appliance is determined to be part of a multihead group and it is a multihead group secondary appliance, the TerminalGroup module determines if the multihead group primary appliance is locally attached to a session. If it is, it tells the Session Manager to allow the secondary appliance to also attach to that session. If the primary appliance is not attached locally, the TerminalGroup module determines if the primary appliance is attached to another server in the failover group (if any), and if it is, it redirects the secondary appliance to that server. See FIGURE 5-8.

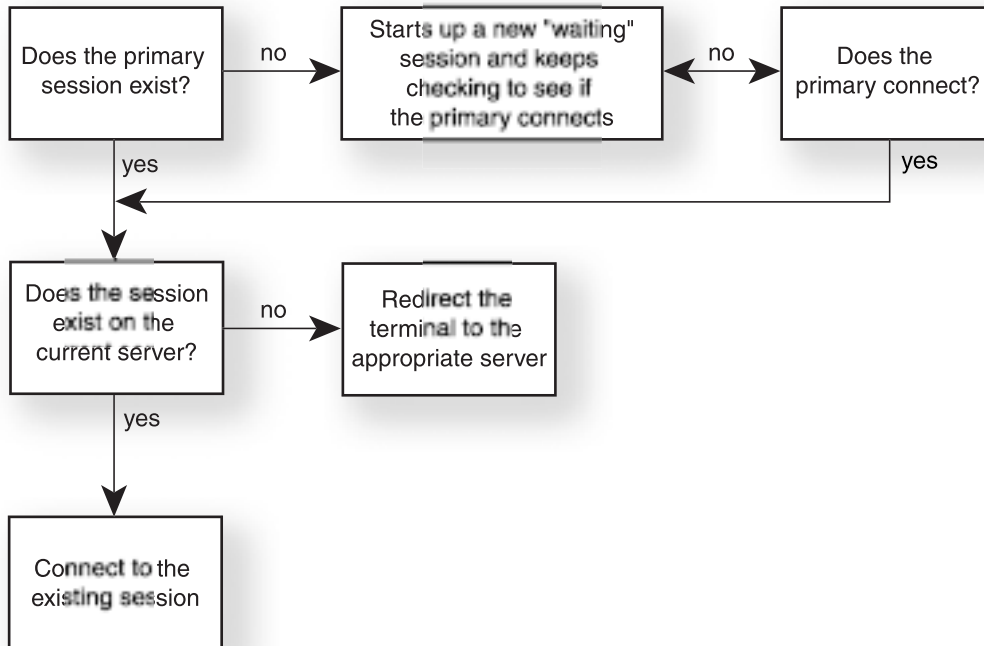


FIGURE 5-8 Flowchart for the Secondary Appliance

If the primary appliance 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 appliance, and further activity is blocked on that appliance until the primary is discovered. The secondary appliance is redirected to the server to which the primary is attached.

Failover

The Sun Ray servers in a failover group provide users with a higher level of availability should one of those servers become unavailable due to a network or system failure. This chapter describes how to configure a failover group.

This chapter covers these topics:

- “Failover Group Overview” on page 82
- “Setting Up IP Addressing” on page 83
- “Group Manager” on page 89
- “Load Balancing” on page 93
- “Setting Up a Failover Group” on page 93
- “Viewing the Administration Status” on page 95
- “Recovery Issues and Procedures” on page 96
- “Setting Up a Group Signature” on page 99
- “Taking Servers Offline” on page 100

Failover Group Overview

A failover group is a set of Sun Ray servers, all running the same release of the Sun Ray server software, and all having access to all the Sun Ray appliances on the interconnect. The Sun Ray servers are configured to trust one another by using the same group signature.

Note – Do not mix releases of Sun Ray server software within a failover group.

The failover group can be a heterogeneous group of Sun servers (for example, a mixture of E250s and E450s) running a mix of Solaris 2.6, Solaris 7, and Solaris 8 operating environments.

All servers in the failover group should have access to and be accessible by all the Sun Ray appliances. 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 6-1 illustrates a typical Sun Ray failover group.

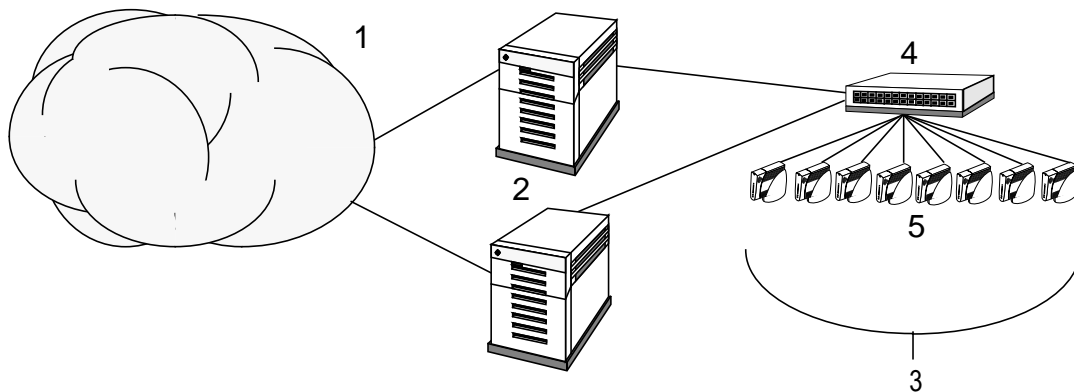


FIGURE 6-1 An Example Sun Ray Failover Group

Legend:

1. Public network—Existing connection to intranet or Internet
2. Sun Ray servers—Provides Sun Ray services
3. Sun Ray Interconnect—Private network or VLAN dedicated to Sun Ray appliances (not part of the public network)

4. Switch

5. Sun Ray appliances

Should a server fail in a failover group, each Sun Ray appliance that was using the server reconnects to another server in the failover group. The failover occurs at the user authentication level whereas the appliance connects to a previously existing session for the user's token. If there is no existing session, the appliance 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:

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

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 *Sun Ray Server Software 1.3 Administrator's Guide* or 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 appliances. Consider the situation of 5 servers and 100 appliances. If one of the servers fails, the remaining DHCP servers must have enough available addresses so that all “orphaned” appliances get a new working address.

The formula for address allocation is: address range (AR) = number of appliances / (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 appliance. 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

TABLE 6-1 describes how to configure five servers for 100 appliances, accommodating the failure of two servers (class C) or four servers (class B).

TABLE 6-1 Configuring 5 Servers for 100 Appliances

Servers	Class C (2 Servers Fail)		Class B (4 Servers Fail)	
	Interface Address	Appliance Address Range	Interface Address	Appliance 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

Server Addresses

Server IP addresses assigned for the Sun Ray interconnect should all be unique. IP addresses are assigned using the `utadm` tool.

When the Sun Ray appliance 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 appliance accepts the first IP address that it receives and configures itself to send and receive at that address.

The accepted DHCP response also contains information about the IP address and port numbers of the Authentication Managers on the server that sent the response.

The appliance 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 asks the Authentication Managers to identify themselves. The appliance then attempts to connect to the Authentication Managers that responded in the order in which the responses were received.

Once a TCP connection to an Authentication Manager has been established, the appliance presents its token. The token is either a pseudo-token representing the individual appliance (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 appliance 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 89.

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

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

The Sun Ray DHCP server can coexist with DHCP servers on other subnets, provided you isolate 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.

Administering Other Clients

The Sun Ray interconnect is intended to be private. No devices other than switches and Sun Ray appliances 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 appliance address ranges for the interconnect to unique values. For example:

```
new first Sun Ray address: [192.168.128.16] 192.168.128.50
new last Sun Ray address: [192.168.128.240] 192.168.128.83
```

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 appliances to download the firmware.

TABLE 6-2 lists the options available for the `utadm` command. For additional information, see the `utadm` man page.

TABLE 6-2 Available Options

Option	Definition
-c	Create a framework for the Sun Ray interconnect
-r	Remove all Sun Ray interconnects
-a <interface_name>	Add <interface_name> as Sun Ray interconnect
-d <interface_name>	Delete <interface_name> as Sun Ray interconnect
-p	Print current configuration
-f	Take a server offline
-n	Bring a server online

Group Manager

Every server has a group manager module that monitors availability, facilitates redirection, and is coupled with the Authentication Manager. For more information on the Authentication Manager, see the *Sun Ray Server Software 1.3 Administrator's Guide*.

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. For information on group policies, refer to the *Sun Ray Server Software 1.3 Administrator's Guide* and the `utglpolicy` man page.

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 93.

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 appliance 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, manual redirection can be accomplished using the `utselect` graphical user interface (GUI) or `utswitch` command.

Note – The `utselect` GUI is the preferred method to use for server selection.

`utselect`

The server select GUI (see FIGURE 6-2) provides an easy and preferred method for server selection.

▼ To Redirect to a Different Server

- From a shell window on the client, type:

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

The selections in the window are sorted in order of the most current.

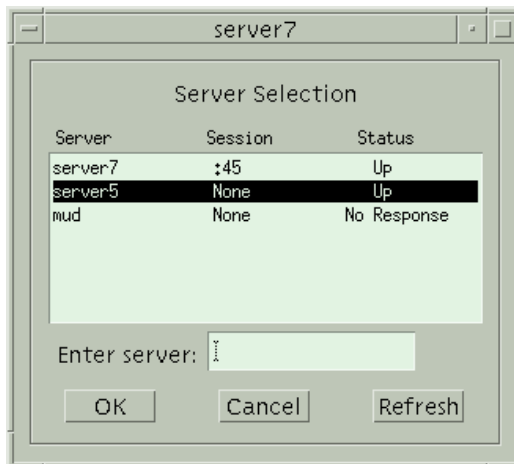


FIGURE 6-2 The Server Selection GUI

In FIGURE 6-2, the Server column lists the servers accessible from the appliance. 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 second server is highlighted by default to facilitate switching between servers. Since no session exists, if `server5` is selected, a new session will be created.

The Refresh button reloads the window with the most current information. The OK button commits your selection of the highlighted server.

Note – If only one server is up in the failover group and all other servers are down, the `utselect` GUI displays only one server. However, if `selectAtLogin` is set to true in the `/etc/opt/SUNWut/auth.props` file, the `utselect` GUI is not displayed because there is only one server in the failover group. If all servers are up, the `utselect` GUI is displayed as usual authentication.

For further information, see the `utselect` man page.

`utswitch`

The `utswitch` command provides redirection from the command line.

▼ To Manually Redirect an Appliance

- From a shell window on the client, type:

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

where `host` is the host name or IP address of the Sun Ray server to which the selected appliance is redirected. In most cases, the optional arguments are not specified, and the appliance is the one on which the command is entered. If `-k token` is provided, then the selected appliance is the one connected to the token's session on the current server. Similarly, if `-s sid` is provided, the appliance is the one connected to the session with session ID `SID` on the current server. In both cases, if an appliance is not connected to the specified session, the command does nothing.

▼ To List Available Hosts

- From a shell window, type:

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

Hosts available from the Sun Ray appliance are listed.

▼ To Select a Different Server

The `-t` option runs the server selection protocol that is executed when a token is presented to a server. If there are existing sessions on other servers associated with the token, the user is redirected to whatever existing session has the latest connect time. The `-k token` and `-s sid` options are used to identify the selected appliance in the same way as they are in the `-h` option of the command.

- In a shell window, type:

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

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

For further information, see the `utswitch` 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:**

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

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 appliance and finds that no server owns an existing session for that token, it redirects the Sun Ray appliance to the server in the group with the lightest load. It is possible that a Sun Ray appliance 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 there are two or more Sun Ray servers that 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 SunDS to enable replication of the Sun Ray administration data across the group.

For information on failover installation, see the *Sun Ray Server Software 1.3 Installation Guide*.

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.

If the Sun Ray server is currently monitored by Sun Management Center, the agent needs to be stopped and restarted. After `utreplica` is run, the following steps need to be performed:

```
# /opt/SUNWsymon/sbin/es-stop -a
# /opt/SUNWsymon/sbin/es-start -a
```

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 informs it of the host names of all the secondary servers.

Note – Configure the primary server before any of 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.

Note – To include an additional secondary server in an already configured failover group, run `utreplica -u` on the primary server. Then on the primary server, rerun `utreplica -p` with a complete list of secondary servers. Run `utreplica -s primary-server` on the new secondary 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

1. 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).

Recovery Issues and Procedures

If one of the servers of a failover group fails, the remaining group members operate from the administration data as it 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 has failed, it is not possible to make administration changes to the system as all changes must be successful on the primary server for replication to work.

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

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

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

This provides an LDIF format file of the current database.

2. **FTP this file to the /tmp directory on the primary server.**
3. **Follow the directions in the *Sun Ray Server Software 1.3 Installation Guide* to install the Sun Ray server software 1.3.**
4. **After running `utinstall`, type the following:**

```
# /opt/SUNWconn/sbin/ldif2ldb -c -n 2 -j 10 -i /tmp/store
```

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

5. Follow the configuration procedures in the *Sun Ray Server Software 1.3 Installation Guide*.

6. Reboot the Sun Ray server:

```
# sync;sync;init 6
```

7. Confirm that the data store is repopulated:

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

8. Perform any additional configuration procedures.

▼ To Replace the Primary Server with a Secondary Server

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

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

This provides an LDIF format file of the current database.

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

3. Type:

```
# /opt/SUNWconn/sbin/ldif2ldb -c -n 2 -j 10 -i /tmp/store
```

4. On all servers, type unconfigure replication:

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

5. Configure the primary and secondary servers.

Refer to “*Configuring the Server Hierarchy*” in the *Sun Ray Server Software 1.3 Installation Guide* or the `utreplica` man page for further information.

▼ To Replace a Primary Server

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

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

This provides an LDIF format file of the current database.

2. Install and configure a Sun Ray server according to the procedures in the *Sun Ray Server Software 1.3 Installation Guide*.
3. Reboot the Sun Ray server:

```
# sync;sync;init 6
```

4. FTP the `/tmp/store` file to the new Sun Ray server.
5. Type:

```
# /opt/SUNWconn/sbin/ldif2ldb -c -n 2 -j 10 -i /tmp/store
```

6. On the secondary servers, unconfigure replication:

```
# utreplica -u
```

7. Configure the primary and secondary servers.

Refer to “Configuring the Server Hierarchy” in the *Sun Ray Server Software 1.3 Installation Guide* or the `utreplica` man page for further information.

Secondary Server Recovery

Where a secondary server has failed, administration of the group can continue. A log of updates are maintained and will be 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 1.3 Installation Guide*.

Setting Up a Group Signature

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

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 8 characters in which at least two are letters and at least one is not

Note – For added 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 that the signature is entered or changed using the `utgroupsig` command and is not created in any other way since the command 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 the 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
```

Controlled Browser

The Controlled Browser is an unsupported product. For your convenience, we have provided a sample implementation of the Netscape Navigator 4.76 browser. This browser is provided in English only and has not been localized.

The objective of this implementation is to provide a browser environment for a publicly accessed Sun Ray appliance with minimal risk of server security compromise. The browser is specially set up to provide for a more controlled and secure browser environment. The Netscape Navigator functions normally with the exception of disabled downloads and a new GUI print interface to the command-line print interface.

This appendix contains the following sections:

- “Controlled Browser Installation” on page 101
- “Controlled Browser Functionality” on page 103
- “Browser Printing” on page 106
- “Adding Plug-ins to the Controlled Browser” on page 108

Controlled Browser Installation

▼ To Install the Controlled Browser

Note – This procedure can take ten minutes to complete.

1. If you have already mounted the Sun Ray server software 1.3 CD-ROM locally or from a remote server or if you extracted the ESD files to an image directory, begin at Step 4.

2. As superuser, open a shell window on the Sun Ray server.

3. Insert the Sun Ray server software 1.3 CD-ROM.

If a file manager window opens, close it. The file manager CD-ROM window is not necessary for this procedure.

4. Change to the image directory by typing:

```
# cd /cdrom/cdrom0
```

5. Change to the controlled browser directory by typing:

```
# cd Supplemental/Controlled_Browser/Solaris_2.6+/Product
```

6. Install the browser by typing:

```
# ./cbinstall
```

The controlled browser is installed and set as a critical application for CAM sessions.

To further configure the browser, refer to the Controlled Browser Functionality in this section.

▼ To Remove the Controlled Browser

The `cbinstall` script also removes the controlled browser.

Note – When you remove the Sun Ray server software, you must first remove the controlled browser if it has been installed. This procedure may take ten minutes to complete.

1. If you have already mounted the Sun Ray server software 1.3 CD-ROM locally or from a remote server or if you extracted the ESD files to an image directory, begin at Step 4.

2. As superuser, open a shell window on the Sun Ray server.

3. Insert the Sun Ray server software 1.3 CD-ROM.

If a file manager window opens, close it. The file manager CD-ROM window is not necessary for this procedure.

4. Change to the image directory by typing:

```
# cd /cdrom/cdrom0
```

5. Change to the controlled browser directory by typing:

```
# cd Supplemental/Controlled_Browser/Solaris_2.6+/Product
```

6. Remove the browser by typing:

```
# ./cbinstall -u
```

The controlled browser is removed.

Controlled Browser Functionality

The browser environment is controlled by taking advantage of the Solaris `chroot` command. This command allows for the execution of the browser to run relative to an alternative root directory. The Sun Ray user runs the browser within the confined environment setup in `/var/opt/SUNWbb/root`, thus avoiding potential access to damaging commands and system files. Since these users are not authenticated, they have limited access to only specified applications confined to the directory tree below the `chroot` directory so as to maintain system security. The `chroot` environment is analogous to a Web server's document root in that users of the environment are confined to the directory tree below the `chroot` directory. The `chroot` environment creates a subdirectory that appears as the `root` directory for a given process or set of processes. The browser and all subprocesses that it may spawn are run in this restricted environment.

Note – This controlled browser does not address general network security, Java applet security, or plug-in security.

▼ To Setup the Controlled Browser in Control Access Mode Administration

1. Start the Administration Tool.
2. Click the arrow to the left of **Controlled Access Mode** to expand the navigation menu.
3. Click the **Controlled Browser** link.

The Controlled Browser Configuration window is displayed.

Sun Ray™ Administration
Controlled Browser Configuration
Server: nomad-100

Set Behavior: critical (automatically launch and restart session on exit)
 menu (launch from menu only)
 default (launch automatically and in menu, but don't restart on exit)

Home Page: []

Browser Window Location (pixels x,y): []

Browser Window Size (pixels width,height): []

Proxy Setting: Manual Proxy Configuration Direct Connection
Will retain default values if "Direct Connection" is selected

HTTP cache: [] port: []

SSL cache: [] port: []

FTP cache: [] port: []

WAIS cache: [] port: []

Gopher cache: [] port: []

Submit Changes

Copyright 2000-2001 Sun Microsystems, Inc. All rights reserved.

FIGURE A-1 Controlled Browser Configuration Window

Note – This menu selection will only appear after Controlled Browser is installed.

4. Set the browser behavior by clicking one of the radio buttons.
 - If you select critical, the session starts with this application. If the session dies, the whole session is regenerated automatically.

- If you select menu, this application is only presented on the menu, which is accessed when the user clicks the right mouse button.
 - If you select default, the session starts with this application but does not restart if it dies. This application is also available on the menu. A user can restart the application by using the menu.
5. In the Home Page text box, type the URL to be accessed when the browser first starts.
 6. In the Browser Window Location text field, displays the screen location in pixels.
 7. The Browser Window Size text field displays the size in pixels.
 8. If a proxy server is being used, click the Manual Proxy Configuration button and set the proxy values for the controlled browser by typing the values in the text boxes.

Proxy Setting:
 Will retain default values if "Direct Connection" is selected

Manual Proxy Configuration (Direct Connection)

HTTP cache: port:

SSL cache: port:

FTP cache: port:

WAIS cache: port:

Gopher cache: port:

FIGURE A-2 Controlled Browser Configuration—Proxy Setting Section

9. Click the Submit Changes button to save your selections in the `kiosk.conf` file.
10. Click the Confirm link in Controlled Access Mode menu.
The confirm panel is displayed.
11. Click the Confirm Configuration button.
The `kiosk.conf` file is updated. If the internal Sun Ray database is up, the configuration file is imported to it.

Browser Printing

This browser implementation has replaced the command-line print interface with a graphical interface.

▼ To Print from the Browser

1. **Select the Print icon on the Netscape menu bar or select File->Print from the pull-down menu.**

The Netscape: Print dialog box is displayed. See FIGURE A-4.

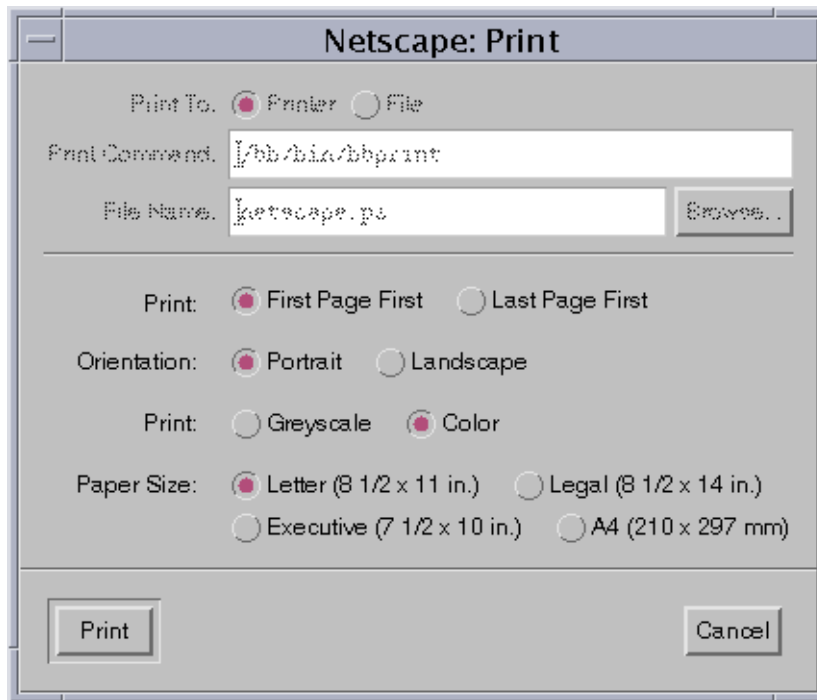


FIGURE A-3 Netscape Print Dialog Box

2. **Press the Print button.**

A new Print dialog box is displayed. See FIGURE A-4.

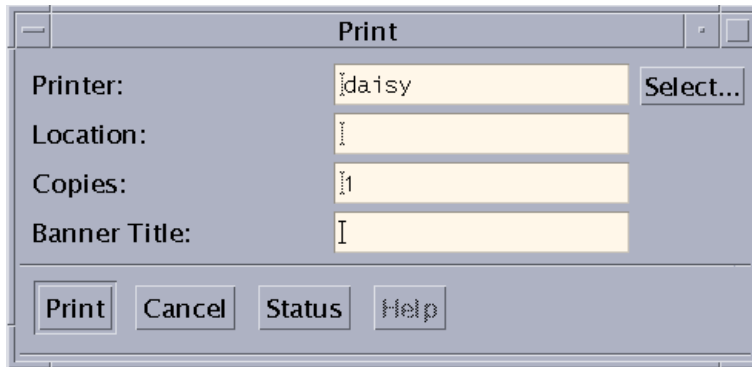


FIGURE A-4 Graphical Printing Interface

3. If there is no printer name in the Printer text box or if you wish to send your print job to a printer other than the one listed in the Printer text box, press the Select button.

The Select Printer dialog box, which contains a list of configured printers for your server, is displayed. See FIGURE A-5.



FIGURE A-5 Select Printer Dialog Box

4. Highlight the desired printer and press the OK button.
5. Once a printer has been selected, press the Status button on the Print dialog box to view the status of the printer.

The Printer Status dialog shows the printer name, the number of jobs queued for this printer, and details of each of the print jobs including print job number, size of file to print, and date stamp for this job. This information helps the user determine if whether to print to a different printer in cases where print queues are too long or individual print jobs on the print queue are too big.

6. Enter the number of print copies required in the Copies text box.
7. If the printer selected is configured to print banners before each print job, enter a banner name in the Banner Title text box.

The Location field cannot be edited and may contain information regarding the location of the selected printer.

8. To print the page, press the Print button or the Cancel button to cancel print operations

▼ To Configure the Printer Location

```
# lpadmin -p printerName -D "<printerLocation>Location information</printerLocation>"
```

Adding Plug-ins to the Controlled Browser

Plug-ins can be added to the Controlled Browser. Since the browser is executed through `chroot` and Controlled Access Mode, extra steps need to be taken to make sure that the plug-ins work properly.

Some plug-ins only need to be installed into the browser's plug-in directory, such as Macromedia Flash Player plug-in. Others require more work to install files into the Control Access Mode user's home directory, add lines to the browser's `mimetypes` file, and setup environment variables needed before the browser is executed.

The restricted runtime environment (`chroot`) has an automated setup mechanism to support dynamic user environment creation. A UNIX user ID is selected dynamically for every new CAM session. The home directory is created and populated with a configured set of files at the start of the session and destroyed upon reset or exit of a session or critical application. How to set up the files to populate the home directory related to plug-ins and their associated helper applications is discussed below.

Set Up Considerations

For plug-ins and helper applications to work properly, the following might be set up:

1. Mime types
2. Environment variables
3. Per user configuration (for example, `$HOME/.xyz` files)

Mime Types

The restricted runtime environment provides an interface to register mime types with the restricted browser. A plug-in usually registers its mime type through the plug-in API, but helper applications use the `.mimetype` and `.mailcap` files.

To register its mime types, a helper application installs a file `helper.mimedef` into the following:

```
/opt/SUNWbb/mime.d/
```

The syntax for this file is as follows:

helper;flags;extensions;mime-type;description

Note – A line is either empty, a comment (line starts with #), or has the above form. Each mime type definition must be a single line. A new line is not allowed in a single mime type definition..

TABLE A-1 Mime Type Definition Syntax

Variable	Definition
<i>helper</i>	<code>bbhelper helperpath args exts</code>
<i>helperpath</i>	helper app to execute for this mime type
<i>args</i>	usually <code>%s</code> or <code>%u</code>
<i>exts</i>	Space-separated list of extensions to match on the URL. If no match, then the first extension is concatenated to the file name. This allows the helper application to guess what content type it deals with. This is because the browser does not provide any hint to the helper on the mime type being handled.

TABLE A-1 Mime Type Definition Syntax (*Continued*)

Variable	Definition
<i>flags</i>	Browser-specific flags such as: x-mozilla-flags=plugin; Usually empty field for helper applications
<i>extensions</i>	exts="ext0 ext1" list of possible extensions for files of this mime type
<i>mime-type</i>	type=mimetype/subtype
<i>description</i>	desc="....."

Environment Variables

To provide environment variables to helper applications or plug-ins, the restricted runtime environment uses files located in `/opt/SUNWbb/appschr.d/`.

These files define variables exported by the controlled browser. A line in these files can either be empty, a comment (start with #), or can have exactly one assignment of the following form:

`VARIABLE=value`

The assignments should be valid bourne shell assignments.

Per User Configuration

Some helper applications need per user configuration data. To allow helper applications to set up a user's home directory, the restricted runtime environment uses files located in `/opt/SUNWbb/apps.d/`.

These files can be bourne or korn shell scripts that are sourced and run with the permissions of the selected user. The following environment variables are available:

TABLE A-2 Environment Variables

Variable	Definition
<i>BBUSER</i>	The user for whom the set up is done.
<i>BBHOME</i>	The user's home directory.

General Requirements and Other Considerations

The following requirements must be met for a plug-in or helper application to run in the restricted runtime environment:

- It must install into a selectable directory location.

The recommended location is as follows:

```
/var/opt/SUNWbb/root/bb/apps/helper-plugin-dir
```

This is the path seen when the browser executes the helper application or plug-in.

- Sometimes the install procedure puts the install path into the installed helper application or plug-in configuration files or scripts.

At run-time it then tries to find components in:

```
/var/opt/SUNWbb/root/bb/apps/helper-plugin-dir
```

which does not exist in the restricted runtime environment. To solve this problem, create the following symbolic link:

```
# cd /var/opt/SUNWbb/root/var/opt/SUNWbb/root
# ln -s /bb bb
```

Tip – For setup and testing purposes, it might be a good idea to temporarily configure `xterm` as an application on the CAM desktop. This aids in the testing and configuration of the plug-ins and their helper applications, many of which use the home directory for configuration files and directories. Remember to remove `xterm` from the CAM desktop before the Sun Ray appliances are ready for use to avoid potential security problems.

Sample Plug-In Setup

Below are steps for setting up some of the more popular browser plug-ins and helper applications for the Solaris operating environment.

Note – The download file names, version numbers, and installation conventions of the plug-ins referenced may change over time. Please note accordingly.

▼ To Add Macromedia Flash Player Plug-in

1. Create the directory for the plug-in download by typing:

```
# mkdir /var/opt/SUNWbb/root/bb/apps/Flash
```

2. Download the Macromedia Flash Player plug-in for the Solaris operating environment from the Macromedia Web site and save it in the following directory:

```
/var/opt/SUNWbb/root/bb/apps/Flash
```

3. Change directory, uncompress the file, and untar the file by typing:

```
# cd /var/opt/SUNWbb/root/bb/apps/Flash
# /usr/bin/gunzip flash_solaris.tar.gz
# tar xvf flash_solaris.tar
```

4. Copy the resulting files into the Netscape plug-ins directory by typing:

```
# cp libflashplayer.so /var/opt/SUNWbb/root/bb/apps/netscape/plugins
# cp ShockwaveFlash.class /var/opt/SUNWbb/root/bb/apps/netscape/plugins
```

▼ To Add Adobe Acrobat Reader Plug-in and Application

1. Create a temporary directory for the plug-in download by typing:

```
# mkdir /var/opt/SUNWbb/root/bb/apps/temp
```

2. Download the Adobe Acrobat Reader for Solaris from the Adobe Web site and save in the following directory:

```
/var/opt/SUNWbb/root/bb/apps/temp
```


3. Change directory, uncompress the file, untar the file, and install by typing:

```
# cd /var/opt/SUNWbb/root/bb/apps/temp
# /usr/bin/gunzip sunsparc-rs-405.tar.gz
# tar xvf sunsparc-rs-405.tar
# cd SSOLRS.install
# ./INSTALL
```

4. Follow the installation instructions. When prompted for the installation directory, enter:

```
/var/opt/SUNWbb/root/bb/apps/ Acrobat4
```

Note – After installation is complete, you can delete the `temp` directory.

5. Copy the Acrobat Reader plug-in library into the Netscape plug-in directory by typing:

```
# cd /var/opt/SUNWbb/root/bb/apps/Acrobat4/Browsers/sparcsolaris
# cp nppdf.so /var/opt/SUNWbb/root/bb/apps/netscape/plugins
```

6. Create the file `/opt/SUNWbb/mime.d/acrobat.mimedef` containing the following lines:

```
/bb/apps/Acrobat4/bin/acroread %s;exts="pdf";type=application/pdf;desc="Portable Document Format"
/bb/apps/Acrobat4/bin/acroread -iconic %s;exts="fdf";type=application/vnd.fdf;desc="application/vnd.fdf"
```

7. Execute the following script to update the browser's mime information:

```
# /opt/SUNWbb/init.d/bbnsinit
```

- 8. Copy the following executable commands into the `/bin` directory of the `chroot` directory by typing:**

```
# cp -p /usr/bin/basename /var/opt/SUNWbb/root/bin
# cp -p /usr/bin/cat /var/opt/SUNWbb/root/bin
# cp -p /usr/bin/dirname /var/opt/SUNWbb/root/bin
# cp -p /usr/bin/expr /var/opt/SUNWbb/root/bin
# cp -p /usr/bin/uname /var/opt/SUNWbb/root/bin
# cp -p /usr/bin/ksh /var/opt/SUNWbb/root/bin
```

The executable for the helper application `acroread` is a script. In the script, executable commands are used to launch the application. Since this script is launched from the browser running under the `chroot` environment, these executable commands have to be explicitly copied into the `/bin` directory of the `chroot` directory.

- 9. Determine what default files need to be copied into the CAM user's home directory by running the browser and plug-in once to see what files are copied into the users directory.**

In the case of Acrobat Reader, the files `.acrorc` and `.acrosrch` are created. The default files can be created by having the CAM user access a PDF file through the Controlled Browser. Once the Acrobat Reader brings up the PDF file, exit Acrobat Reader. This writes out the `.acrorc` and `.acrosrch` file into the home directory of the CAM user (`/var/opt/SUNWbb/root/home/CAM_user_name`).

- 10. Copy the resulting files into a permanent directory by typing:**

```
# cp .acrorc /opt/SUNWbb/config/acrobat4.acrorc
# cp .acrosrch /opt/SUNWbb/config/acrobat4.acrosrch
# chmod 644 /opt/SUNWbb/config/acrobat4.*
```

- 11. Create the file `/opt/SUNWbb/app.d/acrobat.rc` containing the following lines:**

```
cp /opt/SUNWbb/config/acrobat4.acrorc $BBHOME/.acrorc
chmod 644 $BBHOME/.acrorc
cp /opt/SUNWbb/config/acrobat4.acrosrch $BBHOME/.acrosrch
chmod 644 $BBHOME/.acrosrch
```

- 12. Make `/opt/SUNWbb/app.d/acrobat.rc` executable:**

```
# chmod 755 /opt/SUNWbb/app.d/acrobat.rc
```

▼ To Add RealPlayer Plug-in and Application

1. To create a temporary directory for the plug-in download, type:

```
# mkdir /var/opt/SUNWbb/root/bb/apps/temp
```

2. Download the RealPlayer for the Solaris operating environment from the Real Web site and save it in the following directory:

```
/var/opt/SUNWbb/root/bb/apps/temp
```

3. Change directory, make the binary file executable, and execute by typing:

```
# cd /var/opt/SUNWbb/root/bb/apps/temp
# chmod 755 rp8_solaris27_sparc_cs2.bin
# ./rp8_solaris27_sparc_cs2.bin
```

4. Follow the installation instructions. When you are prompted for the installation directory, enter:

```
# /var/opt/SUNWbb/root/bb/apps/RealPlayer
```

Note – After installation is complete, you can delete the `temp` directory.

5. Copy the RealPlayer plug-in libraries into the Netscape plug-in directory by typing:

```
# cd /var/opt/SUNWbb/root/bb/apps/RealPlayer
# cp raclass.zip /var/opt/SUNWbb/root/bb/apps/netscape/plugins
# cp rpnsp.so /var/opt/SUNWbb/root/bb/apps/netscape/plugins
```

6. Create the file `/opt/SUNWbb/mime.d/realplayer.mimedef` containing the following lines:

```
/bb/apps/RealPlayer/realplay %u;exts="ra,rm,ram";type=audio/x-pn-realaudio;desc="Realaudio"
/bb/apps/RealPlayer/realplay %u;exts="ra,rm,ram";type=audio/vnd.rn-realaudio;desc="Realaudio"
/bb/apps/RealPlayer/realplay %u;exts="smi";type=application/smil;desc="Realaudio"
bbhelper /bb/apps/RealPlayer/realplay %s m3u;exts="m3u";type=audio/x-mpegurl;desc="streaming Mpeg audio"
bbhelper /bb/apps/RealPlayer/realplay %s m3u;exts="m3u";type=audio/mpegurl;desc="streaming Mpeg audio"
```

7. To execute the following script to update the browser's mime information, type:

```
# /opt/SUNWbb/init.d/bbnsinit
```

8. Create the following file `/opt/SUNWbb/appschr.d/realplayerenv.rc` containing the following lines:

```
REALPLAYER_HOME=/bb/apps/RealPlayer
```

9. Determine what default files need to be copied into the CAM user's home directory by running the browser and plug-in once to see what files are copied into the user's directory.

In the case of RealPlayer, the files `.RealNetworks_RealMediaSDK_60`, `.RealNetworks_RealPlayer_60`, and `.RealNetworks_RealShared_00` are created.

The ideal user session should be set up at this point. Default settings, such as transport protocol used, proxy settings, and so on, should be set.

10. Copy the resulting files to a permanent directory by typing:

```
# cp .RealNetworks_RealMediaSDK_60 /opt/SUNWbb/config/realplayer.RealNetworks_RealMediaSDK_60
# cp .RealNetworks_RealPlayer_60 /opt/SUNWbb/config/realplayer.RealNetworks_RealPlayer_60
# cp .RealNetworks_RealShared_00 /opt/SUNWbb/config/realplayer.RealNetworks_RealShared_00
# chmod 644 realplayer.*
```

11. Create the file `/opt/SUNWbb/app.d/realplayer.rc` containing the following lines:

```
cp /opt/SUNWbb/config/realplayer.RealNetworks_RealMediaSDK_60 $BBHOME/.RealNetworks_RealMediaSDK_60
chmod 644 $BBHOME/.RealNetworks_RealMediaSDK_60
cp /opt/SUNWbb/config/realplayer.RealNetworks_RealPlayer_60 $BBHOME/.RealNetworks_RealPlayer_60
chmod 644 $BBHOME/.RealNetworks_RealPlayer_60
cp /opt/SUNWbb/config/realplayer.RealNetworks_RealShared_00 $BBHOME/.RealNetworks_RealShared_00
chmod 644 $BBHOME/.RealNetworks_RealShared_00
```

12. Make `/opt/SUNWbb/app.d/realplayer.rc` executable by typing:

```
# chmod 755 /opt/SUNWbb/app.d/realplayer.rc
```

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.
- bps** Bits per second.

C

- 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. DHCP is a means of distributing IP addresses and initial parameters to the appliances.
- domain** A set of one or more system boards that acts as a separate system capable of booting the OS and running independently of any other board.

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.
- Ethernet switch** A unit that redirects packets from input ports to output ports. Can be a component of the Sun Ray interconnect fabric.

F

- fan out** Connections that radiate out from a hub or switch.
- FTP** File Transfer Protocol. The name of the Internet protocol and the program used to transfer files between hosts.

G

- GEM** Gigabit Ethernet.

H

- hot key** A predefined key that causes something to appear on your screen. A hot key is used to bring up the Settings screen on the Sun Ray appliance.
- hot-pluggable** A property of a hardware component that can be inserted into or removed from a system that is powered on. USB devices connected to Sun Ray appliances are hot-pluggable.

I

- interconnect fabric** All the cabling, switches, or hubs that connect a Sun Ray server's network interface cards to the Sun Ray appliances.
- internet** A collection of networks interconnected by a set of routers that enable them to function as a single, large virtual network.
- Internet** (Note the capital "I.") The largest internet in the world consisting of large national backbone nets (such as MILNET, NSFNET, and CREN) and a myriad of regional and local campus networks all over the world. It is a global collection of networks connecting a wide range of computers using a common protocol to communicate and share services.
- intranet** Any network that provides similar services within an organization to those provided by the Internet outside it but which is not necessarily connected to the Internet.
- IP address** A unique number that identifies each host or other hardware system on a network. An IP address is composed of four integers separated by periods. Each decimal integer must be in the range 0-255 (for example, 129.144.0.0).
- IP address lease** The assignment of an IP address to a computer system for a specified length of time, rather than permanently. IP address leasing is managed by the Dynamic Host Configuration Protocol (DHCP). Sun Ray appliance IP addresses are leased.

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.
- 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

- managed object** An object monitored by the Sun Management Center software.
- multicasting** The process of enabling communication between Sun Ray servers over their Sun Ray network interfaces in a failover environment.
- multiplexing** The process of transmitting multiple channels across one communications circuit.

N

- network** Technically, the hardware connecting various computer systems enabling them to communicate. Informally, the systems so connected.
- NIC** Network interface card.

O

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

P

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

S

screen flipping The ability to pan to individual screens on an appliance 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 appliance. It can include audio, video, X servers, access to other machines, and device control of the appliance.

session A group of services associated with a single user.

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

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 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 appliances rely on the server for all computing power and storage.

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

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 inserts 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 appliance'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.

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.

W

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

Index

NUMERICS

100BASE-T, 17

A

Adding

script, 64

Adding applications

calendar, 65

clock, 65

other, 65

Agent, 35

agent, 34, 37

additional requirements with Sun Ray

module, 35

alarms, 34

Details window, 47

monitoring, 46

setting, 43

Tool Tip window, 48

values, 45

Applet

security, 103

appliance, 30, 72, 83

adding to be monitored, 54

deleting to be excluded, 54

Hot Desking to a multihead group, 78

multihead feature, 71

multihead group, 72

Application

adding, 63

critical, 104

default, 104

menu, 104

Attribute Editor, 50

Authentication Manager

flowchart for secondary appliance, 80

Authentication Manager, 18, 30, 79, 85, 89

configuration file, 92

flowchart for primary appliance, 79

multicasting, 18

restarting, 92

Authentication manager, 89

Automatic restart, 104

auto-negotiation, 18, 19

problem, 20

auto-size feature, 74

B

backplane

bandwidth, 27

switching, 20

backplane bandwidth, 20

bandwidth

increasing if bottlenecks, 28

limitation, 20

limited backplane, 26

shared, 24

switched, 24

Browser

proxy settings, 105

C

Cables

- category 5, 17

Cabling

- fiber-optic, 17

Category 5 cabling, 22, 24

CDE toolbar, 73, 78

command

- utadm, 83, 88
- utcapture, 16, 25
 - data elements, 30
- utconfig, 71, 94, 99
- utmhconfig, 73
- utreplica, 94
- utselect, 90
- utswitch, 91, 92
- utxconfig, 71

console, 34

Critical application, 104

D

daemons

- Sun Ray Service panel, 52

Default application, 105

Desktops panel, 54

DHCP, 83

- configuring for failover, 85

DHCP server, 86

DHCP servers, 83

display resolution

- auto-size feature, 74
- on workgroup monitors, 73

duplex

- full, 18, 19, 20
- half, 19

E

Ethernet switch, 15, 18

F

Failover

- controlled access mode, 69

failover

- address allocation formula, 83

- configuring DHCP, 85

- group, 33, 81

 - primary server, 94

 - removing replication configuration, 95

 - secondary server, 94

- Group Manager module, 83

- group overview, 82

- principle components needed, 83

- server IP addresses, 84

- setting up group, 93

- taking servers offline, 100

failover group

- administration status, 95

- monitoring servers, 37

- recovery procedures, 96

full-duplex, 18, 19

G

Group Manager

- keepalive message, 89

- load balancing, 93

- redirection, 90

- using Authentication Manager properties, 92

Group manager, 89

group manager

- keepalive message, 89

group manager module, 89

group signature

- setting up, 99

H

half-duplex, 19

Hot Desk, 74, 78

hub

- shared bandwidth, 24

I

IEEE 802.3u, 19

Interconnect, 17

- interconnect, 15, 86
 - boost power of, 16
 - dedicated, 16
 - implementing a Sun Ray, 26
 - planning the development of, 21
 - tagging ports in a Sun Ray, 28
- Interconnect panel, 53
- Internal database, 94

K

- keepalive message, 89
- kiosk.conf, 62

L

- LAN, 20, 21, 24
 - example interconnect system, 16
- latency, 18
- layer 2, 18, 26
- layer 2 switch, 15
- layer 3, 18, 26
- load balancing, 93
 - turning off, 93
- low latency, 20

M

- managed object, 33
 - desktops, 54
 - Interconnect panel, 53
 - monitoring, 49
 - Sun Ray system, 49
- Management Information Base, 34
- Menu application, 105
- MIB, 34
- monitoring programs
 - CA Unicenter, 56
 - HP OpenView VPO, 56
 - Tivoli TMS, 56
- monitors
 - display resolution, 73
- multicasting, 18
- multihead

- administration tool, 74
- creating a new group, 75
- group, 72, 79
- Hot Desking to an appliance, 78
- screen display, 73
 - auto-size feature, 74
- turning on policy from command line, 74
- turning on policy with administration tool, 75
- multihead feature, 71

N

- network
 - interface card (NIC), 23
- Network security, 103
- NIC, 23

P

- Packet Loss, 20
- packet loss
 - low, 20
 - utcapture, 30
- panel
 - Desktops, 54
 - Interconnect, 53
 - Sun Ray System, 50
- pkgadd, 39
- Primary server, 93

R

- redirection
 - Group Manager, 90
- Remove replication, 95

S

- screen flipping, 78
- Secondary server, 93
- Server addresses, 84
- Server-to-switch bandwidth, 17
- shared bandwidth, 24

- Simple Network Management Protocol, 34
 - SNMP, 34
 - Spanning, 19
 - Spanning Tree protocol, 19, 20
 - Sun Management Center (Sun MC), 33
 - Sun MC
 - additional modules, 39
 - additional requirements with Sun Ray module, 35
 - components, 34
 - creating an object, 40
 - installing, 37
 - interfacing with SUNWutesa package, 36
 - notifying when parameter reached, 34
 - setting up monitoring environment, 39
 - Sun Ray appliance, 15, 16, 18, 24, 28, 30
 - auto-negotiation, 19
 - implementing on VLANs, 26
 - multihead feature, 71
 - multihead group, 72
 - power on, 19
 - recommended environment, 26
 - shield users, 16
 - testing a switch, 19
 - traffic, 26
 - Sun Ray client, 16
 - Sun Ray daemons, 51
 - Sun Ray interconnect, 86
 - server IP addresses, 84
 - Sun Ray module
 - activating for troubleshooting, 42
 - loading, 41
 - requirements, 35
 - troubleshooting, 41
 - Sun Ray node
 - creating, 33
 - Sun Ray server, 15, 16, 20, 24, 30
 - installing software, 37
 - installing the software, 36
 - monitoring with CA Unicenter, 56
 - monitoring with HP OpenView VPO, 56
 - monitoring with Tivoli TMS, 56
 - network interfaces, 17
 - performing standard software installation, 38
 - software, 25
 - software daemons, 34
 - Sun Ray services, 33
 - Sun Ray Services panel
 - daemons, 52
 - Sun Ray system, 18, 33
 - computing model, 15
 - monitoring feature, 34
 - software requirements, 35
 - Sun Ray System panel
 - displaying, 49
 - refreshing, 50
 - setting alarms, 50
 - SunMC, 33
 - Health Monitor module, 39
 - Process Monitoring, 39
 - SunSolve
 - Infodocs, 21
 - Online service, 21
 - SUNWesagt package
 - to verify installation on Sun Ray, 38
 - SUNWsynom, 40
 - SUNWutesa
 - Sun Ray subagent, 34
 - SUNWutesa package, 36, 38
 - removing, 57
 - Switch
 - high-capacity, 17
 - low-capacity, 17
 - requirements, 18
 - switch
 - basic types of 100 Mbps, 17
 - cascading, 21
 - layer 2, 15
 - misconfigured, 20
 - oversubscribed, 20
 - turn-on time, 19
 - switched bandwidth, 24
 - switching backplane, 20
 - switching fabric, 27
 - switching support
 - layer 2, 18, 26
 - layer 3, 26
 - layer3, 18
- T**
- TCP, 85
 - TerminalGroup policy, 79

- troubleshooting
 - activating the Sun Ray module, 42
 - loading the Sun Ray module, 41
- Turn-on time, 19

U

- Uplink ports, 17
- utadm command, 83
 - available options, 88
- utcapture command, 16, 25
 - data elements, 30
- utconfig command, 71, 94, 99
- utgroupsig, 99
- utmhconfig command, 73
- utreplica command, 94
- utselect command, 90
- utsunmc
 - install, 38
- utswitch command, 91, 92
- utxconfig command, 71

V

- VLAN, 16, 17
 - definition, 26
 - implementing a Sun Ray interconnect, 26
 - multiple configuration, 27
 - multiple port-based, 28
 - network, 26
 - one port-based, 28
 - recommendations for implementation, 27
 - switching issues, 25
 - tagged and untagged ports, 29

X

- XINERAMA, 73, 78

