Sun Ray Server Software 4.2 Installation and Configuration Guide (Solaris)

April 2011

Sun Ray Server Software 4.2 Installation and Configuration Guide (Solaris)

Sun Ray Server Software 4.2 Installation and Configuration Guide (Solaris)

Table of Contents

Contents

Modules

Contents

Product Requirements for Solaris (All Topics)

Sun Ray Software 5.1 System Requirements

This page provides the product requirements for the Sun Ray Software 5.1 release, which includes SRSS 4.2 and SRWC 2.3.

Sun Ray Software Operating System Requirements

The following table provides the supported Sun Ray Software operating systems for the SRSS 4.2 and SRWC 2.3 releases.

Platform	Releases
Solaris	• Solaris 10 5/09 or later on SPARC and x86 platforms • Solaris 10 5/09 or later on SPARC and x86 platforms with Solaris Trusted Extensions
Linux	• Oracle Linux 5.4, 5.5 (32-bit and 64-bit) • SuSE Linux Enterprise Server (SLES) 10 with Service Pack 2 (32-bit and 64-bit)

Note
Oracle products certified on Oracle Linux are also certified and supported on Red Hat Enterprise Linux due to implicit compatibility between both distributions. Oracle does not run any additional testing on Red Hat Enterprise Linux products.

Note
SuSE Linux Enterprise Server (SLES) will not be supported after the Sun Ray Software 5.1.x releases.

For additional operating system requirements, see Additional Software Requirements.

SRWC 2.3 Feature Support

The following Windows platforms are supported with SRWC:

- Windows XP Professional with Service Pack 2 (64-bit)
- Windows XP Professional with Service Pack 3 (32-bit)
- Windows Server 2003 R2 Enterprise Edition with Service Pack 2 (32-bit and 64-bit)
- Windows 7 Enterprise (32-bit and 64-bit)
- Windows Server 2008 R2 Enterprise (64-bit)

The following table provides the support matrix for the major SRWC features. Some OS platforms require an SRWC component to be installed for specific feature support. For detailed information, see How to Install the Sun Ray Connector Windows Components.

	Windows XP SP2 (64-bit)	Windows XP SP3 (32-bit)	Windows Server 2003 R2 (32-bit/64-bit)	Windows 7 (32-bit/64-bit)	Windows Server 2008 R2 (64-bit)
Adobe Flash Acceleration (1)	✓	✓	✓	✓	✓
Video Acceleration (2)	✓	✓	✓	✓	✓
USB Redirection (3)	✓	✓	✓	✓	✓
Audio Input (4)	✓	✓	✓	✓	✓
Enhanced Network Security	✓	✓	✓	✓	✓
Session Directory/Session Broker	N/A	N/A	✓	N/A	✓

(1) For Windows XP and Windows Server 2003 R2, support is provided by the Adobe Flash acceleration SRWC component.
(2) For Windows XP and Windows Server 2003 R2, support is provided by the multimedia redirection SRWC component. For Windows 7 and Windows Server 2008 R2, support is provided for Windows Media Video (wmv) playback.
(3) For all OS platforms, support is provided by the USB redirection SRWC component.
(4) For Windows XP and Windows Server 2003 R2, support is provided by the audio input SRWC component.

Licensing

The Sun Ray Software can be licensed as follows:

- Per Named User Plus - is defined as an individual authorized by the customer to use the programs which are installed on a single server or multiple servers, regardless of whether the individual is actively using the programs at any given time.
- Per Sun Ray Device - is defined as any licensed software or hardware device, whether from Oracle or a 3rd party, that accesses a Sun Ray Server environment using the ALP (Appliance Link Protocol), an Oracle Virtual Desktop Infrastructure server environment using ALP or RDP (Remote Desktop Protocol), or an Oracle Secure Global desktop environment using the AIP (Adaptive Internet Protocol).

Connecting to a Sun Ray Software environment via a Sun Ray client or the Oracle Virtual Desktop Access client without an appropriate software license is prohibited.

SRS 5 System Requirements

This page provides the product requirements for the SRS 5 release, which includes SRSS 4.2 and SRWC 2.2.

Sun Ray Server Operating System Requirements

The following table provides the supported Sun Ray server operating systems for the SRSS 4.2 and SRWC 2.2 releases.

Platform	Releases
Solaris	• Solaris 10 5/09 or later on SPARC and x86 platforms • Solaris 10 5/09 or later on SPARC and x86 platforms with Solaris Trusted Extensions
Linux	• Oracle Linux 5.4 and 5.5 (32-bit and 64-bit) • SuSE Linux Enterprise Server (SLES) 10 with Service Pack 2 (32-bit and 64-bit) • Red Hat Enterprise Linux 5 Update 3 server (32-bit and 64-bit)

For additional operating system requirements, see Additional Software Requirements.

SRWC 2.2 System Requirements for Components

The following table provides a software support matrix for all the components of SRWC.

Note
Windows 7 and Windows 2008 R2 support requires the SRWC 2.2 patch, version -02 or greater.

	Windows XP SP 2 (64-bit)	Windows XP SP 3 (32-bit)	Windows 2003 R2 SP2 (32-bit/64-bit)	Windows Vista SP 2 (32-bit/64-bit)	Windows 2008 SP 2 (32-bit/64-bit)	Windows 7 (32-bit/64-bit)	Windows 2008 R2 (64-bit)
Windows Remote Desktop Connection Support	✓	✓	✓	✓	✓	✓	✓
SRWC Component							
Multimedia Redirection • Supported only with Windows Media Player 10 and 11	✓	✓	✓				
Adobe Flash Acceleration • Supported only with Internet Explorer version 7 and 8, 32-bit • Adobe Flash 9 content with all Adobe Flash Players from versions 9 and 10	✓	✓	✓				

USB Redirection • Supported only with Sun Ray server running Solaris 10 5/09 or later • Supported only in Full Screen Windows Kiosk Mode	✓	✓					
Audio Input	✓	✓	✓				
Session Directory/Session Broker			✓		✓		✓
32-bit Color				✓	✓	✓	✓
	Windows XP SP 2 (64-bit)	Windows XP SP 3 (32-bit)	Windows 2003 R2 SP2 (32-bit/64-bit)	Windows Vista SP 2 (32-bit/64-bit)	Windows 2008 SP 2 (32-bit/64-bit)	Windows 7 (32-bit/64-bit)	Windows 2008 R2 (64-bit)

> Note
> Multimedia redirection, Adobe Flash acceleration, and USB redirection require additional software to be installed on the Windows server. For detailed information, see How to Install the Sun Ray Connector Windows Components.

Licensing

The Sun Ray Software can be licensed as follows:

- Per Named User Plus - is defined as an individual authorized by the customer to use the programs which are installed on a single server or multiple servers, regardless of whether the individual is actively using the programs at any given time.
- Per Sun Ray Device - is defined as any licensed software or hardware device, whether from Oracle or a 3rd party, that accesses a Sun Ray Server environment using the ALP (Appliance Link Protocol), an Oracle Virtual Desktop Infrastructure server environment using ALP or RDP (Remote Desktop Protocol), or an Oracle Secure Global desktop environment using the AIP (Adaptive Internet Protocol).

Connecting to a Sun Ray Software environment via a Sun Ray client or the Oracle Virtual Desktop Access client without an appropriate software license is prohibited.

Disk Space Requirements (Solaris)

The standard installation of Sun Ray Server Software requires at least 95 MB of disk space.

The following table lists the disk space requirements for specific directories.

Product	Default Installation Path	Requirements

Sun Ray core software	`/`
	`/opt`
	`/var/adm/log`
	`/var/tmp`
	`/var/opt/SUNWut`
		1 Mbyte
		20 Mbytes
		1 Mbyte
		5 Mbytes
		Allow enough disk space for the log files.

Sun Ray Data Store	`/opt/SUNWut/srds`
	`/etc/opt`
	`/var/opt/SUNWut/srds`
		4 Mbytes in `/opt`
		0.1 Mbytes in `/etc`
		Allow enough disk space for the data store and log files. For 1,000 entries, allocate roughly 1.5 Mbytes of disk space, 64 Mbytes of RAM, and 128 Mbytes of swap space.

> Note
> The suggested server configuration includes approximately 50-100 MB of swap space per user.

Additional Software Requirements

Solaris Operating System

> Note
> OpenSSL is generally installed by default on the supported operating systems. Please confirm that OpenSSL is installed before proceeding.

- The “Entire Distribution” software cluster is required and must be installed.
- The latest Recommended Patch Cluster (RPC) must be installed prior to the SRSS installation.
- The Common Desktop Environment (CDE) might not be available in a future Solaris release. Users should migrate to the Java Desktop System. CDE will not be supported on future versions of SRS when CDE is officially removed from the Solaris release.

Linux Operating Systems

> Note
> OpenSSL is generally installed by default on the supported operating systems. Please confirm that OpenSSL is installed before proceeding.

> Note
> On all versions of Linux, the following services must be disabled during the post-installation setup:
>
> - Firewall
> - SELinux

Oracle Linux 5.4 and 5.5

All packages are required and must be installed. In addition to the default RPMs selected, add the following items:

- Software Development Tools
- glib-1.2.10-20.el5.i386.rpm (32-bit RPM on both 32-bit and 64-bit OS)
- dhcp-3.0.5-23.el5 (Servers/Network Servers)
- openldap-2.3.43-12.el5 (Servers/Network Servers)
- openldap-clients-2.3.43-12.el5 (Base System/System Tools)
- tftp-server-0.49-2.0.1 (Servers/Legacy Network Servers)
- libXp-1.0.0-8.1.el5.i386.rpm (32-bit RPM on both 32-bit and 64-bit OS)
- libXpm-3.5.5-3 (32-bit RPM on both 32-bit and 64-bit OS)
- openmotif22-2.2.3-18.i386.rpm (32-bit RPM on both 32-bit and 64-bit OS)
- openssl-0.9.8e-12.el5_4.6.i386.rpm (32-bit RPM on both 32-bit and 64-bit OS for SRWC)
- compat-libstdc++-33-3.2.3-61.i386.rpm (32-bit RPM on both 32-bit and 64-bit OS for SRWC)
- libusb-devel-0.1.12-5.1.i386.rpm (32-bit RPM for 32-bit OS for libusb)
- cdparanoia-libs-alpha9.8-27.2.i386.rpm (32-bit RPM on 64-bit OS for Media Player)

SuSE Linux Enterprise Server (SLES) 10 Service Pack 2

All packages are required and must be installed. In addition to the default RPMs selected, add the following items:

- C/C++ Development Tools
- DHCP & DNS Server
- LDAP
- tftp

Red Hat Enterprise Linux (RHEL) 5 Update 3

All packages are required and must be installed. In addition to the default RPMs selected, add the following items:

- Software Development Tools
- glib-1.2.10-20.el5 (32-bit RPM on 32-bit and 64-bit OS)
- dhcp-3.0.5-3.el5 (Servers/Network Servers)
- openldap-2.3.27-8 (Servers/Network Servers)
- openldap-clients-2.3.27-8 (Base System/System Tools)
- tftp-server-0.42-3.1 (Servers/Legacy Network Server)
- libXp-1.0.0-8.i386.rpm (32-bit RPM on 32-bit and 64-bit OS)
- openmotif22-2.2.3-18.i386.rpm (32-bit RPM on 32-bit and 64-bit OS)
- openssl-0.9.8b-8.3.el5_0.2.i386.rpm (32-bit RPM on 32-bit and 64-bit OS)
- compat-libstdc++-33-3.2.3-61 (32-bit RPM on 32-bit and 64-bit OS)
- libusb-devel-0.1.12-5.1.i386 (32-bit RPM for 32-bit OS for libusb)

> Caution
> The Red Hat installation script asks whether to start a graphical console. Be sure to answer "Yes", otherwise Sun Ray startup scripts and X initialization scripts may fail to run.

Java Runtime Environment (JRE)

SRSS 4.2 requires a 32-bit implementation of a Java(TM) 2 Platform, Standard Edition JRE(TM) of at least 1.6. The latest Java release is available at http://www.oracle.com/technetwork/java/javase/downloads.

To check what JRE version is installed on your system, use the following command:

```
java -version
```

JRE version 1.6 is also bundled on the SRSS product CD for Solaris systems in the `Supplemental` directory.

> Note
> A 64-bit JRE is not suitable for use with SRSS. The 32-bit JRE is required, even when the platform is capable of supporting a 64-bit JRE.

SunMC Requirements (Solaris)

To use SunMC, the administrator must install the correct version of the SunMC software. See Installing SunMC (All Topics).

Sun Ray Admin GUI Web Server Requirements

The Sun Ray Administration Tool (Admin GUI) requires that a Web server be installed and running on each Sun Ray server. The Admin GUI must be hosted in a web container that supports the JavaServlet 2.4 and JavaServer Pages 2.0 specification. The Apache Tomcat 5.5 Web container implements these standards and runs on any operating system that has a Java Runtime Environment (JRE).

The `utconfig` script prompts for the location of an Apache Tomcat HTTP Server and asks whether it should be configured automatically.

- To configure the server automatically, supply the path and answer Yes.
- To configure the HTTP server later by using the `utconfig -w` command, answer No.

An Apache Tomcat 5.5 archive is included in the Sun Ray Server Software 4.2 image under `Supplemental/Apache_Tomcat`. The most recent version of Tomcat 5.5 can be downloaded from http://tomcat.apache.org.

The Sun Ray configuration script uses port 1660 for the Sun Ray Administration Tool (Admin GUI) by default. If this port is unavailable, you can configure a new port while running the `utconfig` script.

See How to Install Apache Tomcat for details.

Web Browser Requirements

The Sun Ray Administration Tool (Admin GUI) requires a web browser such as Firefox or Mozilla.

- The latest version of the Firefox browser is available at http://www.mozilla.com/en-US/firefox/all.html
- The latest version of the Mozilla browser is available at http://www.mozilla.org/download.html

> Note
> There are known issues using Firefox 4 and Google Chrome 10 with the Admin GUI. These specific browser versions should not be used.

Sun Ray Data Store Port Requirements

When you configure a new Sun Ray server in a failover environment that uses SRSS 4.2 only, service port 7012 is used by default.

If you already have an LDAP (Lightweight Data Access Protocol) server configured on the Sun Ray server, it can coexist with Sun Ray Data Store. However, it must not use port 7012, which is reserved for use by the Sun Ray Data Store.

If you configure a new Sun Ray server in a mixed failover group, you must make sure that the primary server is running SRSS 4.2.

If the secondary server is running SRSS 4.2, no special care is required. The `utreplica` utility automatically synchronizes with the port number on the primary.

> Note
> Although configuring mixed failover groups consisting of servers running various versions of Sun Ray Server Software is possible, this practice is discouraged. For more information, see Managing Failover Groups (All Topics).

How to Install Apache Tomcat

If Tomcat 5.5 is already installed on your system, you can omit the steps below and specify the path, if necessary, during configuration. For more information, see Configuring a Sun Ray Server.

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

   ```
   % su -
   ```

2. Change to the `Apache_Tomcat` directory. For example:

   ```
   # cd /cdrom/cdrom0/Supplemental/Apache_Tomcat
   ```

3. Extract the Tomcat archive into a suitable directory, such as `/opt`.

   ### For Solaris

   The Tomcat archive uses GNU tar extensions and must be untarred with a GNU-compatible version of the `tar` command, such as `gtar`.

```
# /usr/sfw/bin/gtar -xvz -C /opt -f apache-tomcat-5.5.20.tar.gz
```

For Linux

```
# tar -xvz -C /opt -f apache-tomcat-5.5.20.tar.gz
```

4. (Optional) Create a symbolic link to the installation to make future Tomcat updates easier.

```
# ln -s /opt/apache-tomcat-5.5.20 /opt/apache-tomcat
```

Contents

Installing on Solaris (All Topics)

START HERE to Install SRSS (Solaris)

> Note
> Sun Ray Software 5.1 includes a new SRSS 4.2 installer that simplifies the product release upgrade and patch updates. The new SRSS 4.2 installer automatically upgrades prior releases of SRSS with new feature updates and the latest patches. The new SRSS 4.2 installer automatically applies the latest patches to existing SRSS 4.2 installations.

The following task map provides information about how to install SRSS 4.2 on a Sun Ray Server.

Step	Details
1. Make sure the target server meets the product requirements.	Product Requirements for Solaris (All Topics)
2. If needed, upgrade the Solaris OS on the target server.	How to Upgrade the Solaris OS
3. Install SRSS on the target server.	How to Install SRSS (Solaris)
4. Configure the installed Sun Ray server.	Task Map - Configuring a Newly Installed Sun Ray Server

How to Check the Current Solaris OS Version on a Server

Check the operating system version by typing the following command:

```
% cat /etc/release
```

This command displays the current operating system release on the Sun Ray server, for example:

```
                        Solaris 10 5/09 s10x_u7wos_08 X86
           Copyright 2009 Sun Microsystems, Inc.  All Rights Reserved.
                        Use is subject to license terms.
                             Assembled 30 March 2009
```

If you need a newer version, contact your Sun Microsystems representative to purchase the latest version of the Solaris software.

How to Upgrade the Solaris OS

1. Obtain the Solaris 10 5/09 installation image.
2. Follow the instructions in the Solaris 10 5/09 Installation Guide: Basic Installations.

For additional operating system requirements, see Additional Software Requirements.

How to Install SRSS (Solaris)

Before You Begin

Be aware of the following information before beginning the installation.

- The `utinstall` script asks about installing the available locale support for the Admin GUI. If you choose to install additional Admin GUI locale support after the installation, you can always use the `pkgadd` command to install the Admin GUI locale packages provided on the installation image:

  ```
  <image_mount_point>/srss_4.2/Sun_Ray_Core_Services_4.2/Solaris_10+/sparc/Packages
  <image_mount_point>/srss_4.2/Sun_Ray_Core_Services_4.2/Solaris_10+/i386/Packages
  ```

- Make sure the system has the required JRE version installed.
- The `utinstall` script requests that you reboot the Sun Ray server. In the past, this step was optional; however, it is now required.
- The `utinstall` script for SRSS 4.2 does not automatically add Sun Ray information to the `crontab`, `syslog`, PAM, and SunMC services as earlier versions did. Instead, it adds them upon the first reboot after installation or upgrade.

Steps

1. Download the Sun Ray Software 5.1 Media Pack and make it accessible to the Sun Ray server.
2. Become superuser on the Sun Ray server.
   To avoid installation script errors that can occur if user environment settings are carried forward, use the following command:

   ```
   % su - root
   ```

3. Install Sun Ray Server Software.

   ```
   # ./utinstall
   ```

   The `utinstall` script performs the following steps:

- Displays the text of the Sun Software License Agreement and prompts you to accept its terms and conditions.
- Asks if you want to install a localized Admin GUI.
- Prompts you for the location of the Java Runtime Environment.
- Informs you that it will install the required software products and any necessary patches and waits for approval.
- Installs the Sun Ray Data Store
- Installs the Sun Ray server (Administration software, English man pages, Core software, Configuration, Drivers)
- Installs the Kiosk Mode software

When the script ends, a log file is available at:

```
/var/adm/log/utinstall.<year><month><date><hour>:<minute>:<second>.log
```

The values in the file name reflect a time stamp of when `utinstall` was started. Check this file for notices of installation problems.

4. Reboot the Sun Ray server.

```
# /usr/sbin/reboot
```

This needs to be done before you can run `utadm` or `utconfig`.

For a listing of `utinstall` error messages, see Troubleshooting Installation.

Where to Go Next

Go to Task Map - Configuring a Newly Installed Sun Ray Server for instructions about how to prepare to configure and reboot the Sun Ray server.

How to Remove the Sun Ray Software

The following procedure is not required for installation or upgrade.

To remove Sun Ray Server Software in its entirety, follow this procedure.

Steps

1. Log in as the superuser of the Sun Ray server.
2. Open a shell window and change to the `/opt/SUNWut/sbin` directory.

```
# cd /opt/SUNWut/sbin
```

3. If you are removing Sun Ray Server Software from a server in a failover group:
    a. Disable Sun Ray DTU firmware downloads.

For a Private interconnect	`# ./utfwadm -D -a -n all`
For a LAN configuration	`# ./utfwadm -D -a -N all`

    b. Remove the replication configuration.

```
# ./utreplica -u
```

4. Remove the Sun Ray network interfaces.

   ```
   # ./utadm -r
   ```

5. Unconfigure the Sun Ray software.

   ```
   # ./utconfig -u
   ```

   Answer y to all of the prompts.

6. Uninstall Sun Ray Server Software.

   ```
   # cd /
   # /opt/SUNWut/sbin/utinstall -u
   ```

   Answer y to all of the prompts.

7. Repeat the steps in this procedure for all remaining Sun Ray servers.

Troubleshooting Installation

Installation (utinstall) Error Messages

If during an installation, upgrade, or uninstall the `utinstall` script returns an error, refer to the following table for assistance.

All Installations

Message	Meaning	Resolution
`utinstall: fatal, media-dir is not a valid directory.`	You called the `-d` option, but media-dir is incomplete.	The media-dir directory requires relevant patches and packages for installation. The media-dir directory includes the Sun Ray directory.
`xxxxxx not successfully installed`	Might occur for the installation of any application or patch if relevant packages have not been properly installed.	Verify that he component xxxxxx is present in the installation media directory path and has the correct permissions, then run the `utinstall` script again.
{{A different version x.x of product has been detected. The other-product Software is only compatible with product y.y. You must either upgrade or remove the current product installation before proceeding. Exiting ...}}	Some of the applications provided with Sun Ray Server Software are compatible only with certain versions of other applications.	Compatible and necessary applications are included with Sun Ray Server Software. Remove older versions, then run the `utinstall` script again.
`error, no Sun Ray software packages installed.`	None of the Sun Ray components are installed on this system.	No action is required as the product is not installed.

The following files were not successfully replaced during this upgrade. The saved copies can be found in <directory>	Some files were not properly replaced as part of the upgrade.	Manually copy the listed files from the directory, overwriting the newer files if applicable.
Partition Name Space Required Space Available -------------- -------------- --------------- partition xxx yyy	Not enough disk space was allocated for partition. Repartition the disk and run utinstall again.	

Linux Installations

Message	Meaning	Resolution
The following packages were not successfully removed xxxxxx ...	The packages listed have not been properly removed.	Use the rpm -e command to remove each listed rpm manually, then run utinstall -u again.
Removal of product was not successfully completed. See log file for more details.	Removal of Sun Ray Server Software was incomplete.	Check the log file for the package that started the problem and manually remove it with the rpm -e command, then run utinstall -u again.

Solaris Installations

Message	Meaning	Resolution
Cannot open for read admin-file	The admin_default file is unreadable, or you called the -a option and the admin-file is unreadable.	Verify that the installation administration file exists (admin_default or other) and the permissions are correct.
For SPARC platforms: SunOS release is x.x, valid releases are: 10	You are attempting to install Sun Ray Server Software onto a Solaris software version that does not support SRSS 4.2.	Upgrade to the supported version 10 of the Solaris OS before installing Sun Ray Server Software.
For x86 platforms: SunOS release is x.x, valid releases are: 10	You are not running a valid OS release for this platform.	Upgrade to the supported version 10 of the Solaris OS before installing Sun Ray Server Software.
Please clean up the directory /var/tmp/SUNWut.upgrade before rerunning utinstall.	Other unrelated files were found in the preserve directory.	Remove unrelated files from the directory.
Please remove the existing preserved file <preserved_tarfilename> before rerunning utinstall.	You decided not to restore from the indicated tar file.	Remove the tar file before running utinstall again.
utpreserve: unable to preserve data. Error while creating archive file	The utinstall script failed to preserve existing configuration files.	Either exit and manually preserve these files or just continue.
The following packages were not successfully removed xxxxxx ...	The packages listed have not been properly removed.	Use the pkgrm command to remove each listed package manually, then run utinstall -u again.
Removal of product was not successfully completed. See log file for more details.	Removal of Sun Ray Server Software was incomplete.	Check the log file for the package that started the problem and manually remove it with the pkgrm command, then run utinstall -u again.

Modified System Files (Solaris)

The following files are modified during `utadm`:

- `/etc/inet/hosts`
- `/etc/inet/networks`
- `/etc/inet/netmasks`
- `/etc/inet/dhcpsvc.conf` # including all DHCP-related files
- `/etc/nsswitch.conf`
- `/etc/hostname.`*`intf`*

The following files are modified during Sun Ray service startup:

- `/etc/inet/services`
- `/etc/inet/inetd.conf`

The following files are modified during `utconfig`:

- `/etc/passwd`
- `/etc/shadow`
- `/etc/group`

After installation, the following files are updated upon reboot:

- `/etc/syslog.conf`
- `/etc/pam.conf`

Modified System Files (Linux)

The following files are modified during `utadm`:

- `/etc/dhcpd.conf`
- `/etc/nsswitch.conf`
- `/etc/opt/SUNWut/net/dhcp/SunRay-options`
- `/etc/opt/SUNWut/net/dhcp/SunRay-interface-eth1`
- `/etc/opt/SUNWut/net/hostname.eth1`
- `/etc/opt/SUNWut/net/networks`
- `/etc/opt/SUNWut/net/netmasks`
- `/etc/hosts`

The following files are modified during `utconfig`:

- `/etc/passwd`
- `/etc/shadow`
- `/etc/group`

SRSS also updates the GDM configuration file, `custom.conf`, to make sure it has the following entries, which are removed when SRSS is removed:

```
VTAllocation=false
DynamicXServers=true
```

In addition, display files are created for each Sun Ray DTU in the following directories:

- `PreSession`
- `PostSession`
- `Init`
- `PostLogin`

Contents

Upgrading on Solaris (All Topics)

START HERE to Upgrade SRSS (Solaris)

> Note
> Sun Ray Software 5.1 includes a new SRSS 4.2 installer that simplifies the product release upgrade and patch updates. The new SRSS 4.2 installer automatically upgrades prior releases of SRSS with new feature updates and the latest patches. The new SRSS 4.2 installer automatically applies the latest patches to existing SRSS 4.2 installations.

> Note
> You cannot migrate a Sun Ray server configuration to a hardware platform of a different Instruction Set Architecture. For example, you cannot migrate an existing SPARC-based Sun Ray server configuration to a new x86-based Sun Ray server.

> Note
> Upgrades from SRSS version 4.0 and version 4.1 are supported with SRSS 4.2. See How to Check Installed SRSS Version.

Use the following task map to upgrade an existing Sun Ray server to SRSS 4.2.

Step	Details
1. Confirm that your Sun Ray server meets the product requirements.	Product Requirements for Solaris (All Topics) If the Sun Ray server does not have the required Solaris OS, follow the OS upgrade instructions later in this process.
2. If you are upgrading Sun Ray servers in a failover group, consider ways to reduce downtime.	Planning Upgrades Using Failover Groups
3. Preserve the Sun Ray server data before upgrading.	How to Preserve Sun Ray Software Configuration Data (Solaris) Although the configuration data is automatically preserved during an upgrade, backing up data before an upgrade is always good practice.
4. Inform users about the upgrade.	Before you upgrade Sun Ray Server Software, inform your users of your plans, and have them terminate their sessions. An effect of the upgrade procedure is that all active and suspended sessions are lost.
5. If necessary, upgrade the Solaris OS on the Sun Ray server and apply the necessary patches.	How to Upgrade the Solaris OS
6. Upgrade the SRSS software on the Sun Ray server.	How to Upgrade SRSS (Solaris)
7. Configure the upgraded Sun Ray server.	Task Map - Configuring an Upgraded Sun Ray Server

Planning Upgrades Using Failover Groups

By configuring two or more Sun Ray servers in a failover group, you can reduce interruption of new service availability in the event that one server fails. If you plan to combine existing Sun Ray servers into a failover group, or to upgrade an existing failover group, please consider the following:

- You should always upgrade the secondary servers first before upgrading the primary server. New functionality from the release may not work until all the servers in the failover group are upgraded.
- Before you upgrade a given server, make sure that Sun Ray DTU users terminate their sessions.

> Note
> If upgrading servers in a large configuration at once is not convenient, upgrade one or two servers at a time until the entire configuration is complete.

- For best results in groups of four or more servers, configure the primary server so that it serves only the Sun Ray Data Store. Configure the secondary servers so that they serve users directly in addition to serving the Data Store.
- While upgrading the primary server, secondary servers will not be able to do any updates to the Data Store.
- To take advantage of the new features in this release, do not mix different Sun Ray Server Software versions within a failover group. Failover groups that use more than one software version revert to the functionality of the earliest version.
- Using the Admin GUI to restart or reset Sun Ray services does not work across servers with different Sun Ray releases. For example, even if you use the Admin GUI to restart all the servers in a failover group that are running SRSS 4.2, you should still restart or reset any Sun Ray servers running earlier versions of SRSS manually.
- Turn off all firmware updates until all the servers in a failover group are upgraded. For details, see How to Disable All Firmware Updates.

> Note
> Even if you upgrade one or two servers per week, you must wait until all servers in the group are upgraded before you update their firmware.

- If your configuration is a dedicated private interconnect, disconnect the server from the Sun Ray interconnect.

See About Failover Groups for a more general discussion of failover groups, including diagrams of failover topologies.

How to Check Installed SRSS Version

This procedure is useful to verify your SRSS installation or to determine if an upgrade is supported on your current Sun Ray server.

1. Become superuser on the Sun Ray server.
2. Check the installed SRSS version.
    - Solaris:

      ```
      # pkginfo -x SUNWuta
      ```

    - Linux:

      ```
      # rpm -q SUNWuta
      ```

How to Check the Current Solaris OS Version on a Server

Check the operating system version by typing the following command:

```
% cat /etc/release
```

This command displays the current operating system release on the Sun Ray server, for example:

```
                        Solaris 10 5/09 s10x_u7wos_08 X86
           Copyright 2009 Sun Microsystems, Inc.  All Rights Reserved.
                        Use is subject to license terms.
                             Assembled 30 March 2009
```

If you need a newer version, contact your Sun Microsystems representative to purchase the latest version of the Solaris software.

How to Preserve Sun Ray Software Configuration Data (Solaris)

When you choose an upgrade, the `utinstall` script automatically preserves your existing configuration information. You must preserve your existing configuration before running the `utinstall` script only in the following situations:

- You are upgrading the Solaris OS on an existing Sun Ray server that requires you to reformat the server's disk.
- You are replacing an existing Sun Ray server hardware with a new server. If replacing a Sun Ray server with a new one, the replacement must be the same architecture, for example, a SPARC system must be replaced with another SPARC system.

In both of these cases, you will need to add the `/var/tmp/SUNWut.upgrade/preserve_version.tar.gz` backup file to the newly installed server before you start the `utinstall` program. The `utinstall` program automatically restores the configuration data in the `preserve_version.tar.gz` after it installs the SRSS software.

> Note
> If you are using the Solaris upgrade program to upgrade an existing Sun Ray server running a previous Solaris 10 release to Solaris 10 5/09, you do not need to preserve the configuration data--the upgrade will not overwrite the server's data. However, backing up data before performing an OS upgrade is always good practice.

The `utpreserve` script in the Sun Ray Server Software image directory preserves the following information:

- X user settings
- Sun Ray Data Store
- Authentication Manager configuration files
- `utslaunch` properties
- Failover group information
- Kiosk mode configuration

The `utpreserve` script does not preserve the following information:

- The Sun Ray server's network and DHCP configuration settings (`utadm` configuration information). You must reconfigure those settings after upgrading the Sun Ray Server Software.
- The `/etc/pam.conf` is not saved. You need to back up and restore this file manually.

Before You Begin

Depending on the size of your configuration, this procedure, including the operating system software upgrade, might take anywhere from five minutes to several hours or even more to complete.

> Caution
> Running the `utpreserve` script stops all Sun Ray daemons and services, including the Sun Ray Data Store, causing users to lose all of their sessions, both active and disconnected. Make sure to inform them of your plans.

Steps

If you have already mounted the Sun Ray Server Software 4.2 CD-ROM locally or from a remote server, or if you have extracted the ESD files to an image directory, begin at Step 3.

1. As superuser, open a shell window on the Sun Ray server.
2. Insert the Sun Ray Server Software 4.2 CD-ROM.

If a file manager window opens, close it. It is not necessary for installation.

3. Change to the image directory.
   For example:

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

4. Preserve the Sun Ray configuration:

```
# ./utpreserve
```

   The `utpreserve` script warns that it will stop all Sun Ray services, consequently terminating all user sessions, and asks whether it should continue.
   If you answer `y`, the `utpreserve` script:

   - Stops the Sun Ray services and the Sun Ray Data Store daemon.
   - Lists the files that are saved.
   - Tars and compresses the entire list of files as the `/var/tmp/SUNWut.upgrade/preserve_`*`version`*`.tar.gz` file, where version is the currently installed version of the Sun Ray Server Software.
   - Indicates that a log file is available at `/var/adm/log/utpreserve.`*`year_month_date_hour:minute:second`*`.log`:
     where year, month, and so on are represented by numeric values reflecting the time `utpreserve` was started.

     > Note
     > Check this log file for notices of errors.

   - Recommends that the `/var/tmp/SUNWut.upgrade/preserve_`*`version`*`.tar.gz` file be moved to a safe location before the operating system software upgrade.
5. Use NFS, FTP, or other means to copy the `/var/tmp/SUNWut.upgrade/preserve_`*`version`*`.tar.gz` file to a safe location on another server.
6. Make a tape backup of the Sun Ray server's file systems.
7. If necessary, make a backup of the modified `/etc/pam.conf` file.

> Caution
> If you have modified the `/etc/pam.conf` in a previous version of Sun Ray Server Software, your changes might be lost when SRSS is upgraded. To avoid losing your modifications, be sure to save a copy before performing the update, then use the saved copy to restore your earlier modifications.

How to Upgrade the Solaris OS

1. Obtain the Solaris 10 5/09 installation image.
2. Follow the instructions in the Solaris 10 5/09 Installation Guide: Basic Installations.

For additional operating system requirements, see Additional Software Requirements.

How to Upgrade SRSS (Solaris)

This procedure describes how to upgrade SRSS on an existing Sun Ray server running the Solaris OS.

Before You Begin

Before you begin the upgrade, note the following information:

- Make sure you have performed all the necessary steps outlined in START HERE to Upgrade SRSS (Solaris).
- The SRSS installation script automatically installs whatever locales were previously installed.
- Make sure the Sun Ray server has the required JRE version installed.
- The `utinstall` script requests that you reboot the Sun Ray server. In the past, this step was optional; however, it is now required.

- The `utinstall` script for SRSS 4.2 does not automatically add Sun Ray information to the `crontab`, `syslog`, PAM, and SunMC services as earlier versions did. Instead, it adds them on the first reboot after installation or upgrade.

Steps

1. Download the Sun Ray Software 5.1 Media Pack and make it accessible to the Sun Ray server.
2. Become superuser on the Sun Ray server.
   To avoid installation script errors that can occur if user environment settings are carried forward, use the following command:

   ```
   % su - root
   ```

3. If needed, use NFS, FTP, or other means to return the `/var/tmp/SUNWut.upgrade/preserve_`*`version`*`.tar.gz` file to the Sun Ray server.
   This step is needed only if you had to reformat the existing Sun Ray server's hard drive or replaced the current Sun Ray server with a new server. See How to Preserve Sun Ray Software Configuration Data (Solaris) for details.
4. Upgrade the Sun Ray Server Software.

   ```
   # ./utinstall
   ```

   The `utinstall` script performs the following steps:

   - Displays the text of the Sun Software License Agreement and prompts you to accept its terms and conditions.
   - Checks to see which required software products are already installed.
   - Displays a message about what it has found.
   - Might indicate that an encryption change is about to happen. Answer y (yes).
   - Asks whether you want to install a localized Admin GUI.
   - Informs you that it will install, upgrade, or migrate the required software products and any necessary patches and waits for approval.
   - Preserves the current SRSS configuration data in the `/var/tmp/SUNWut.upgrade/preserve_`*`version`*`.tar.gz` file.
   - Removes all previous Sun Ray software
   - Installs the Sun Ray Data Store
   - Installs the Sun Ray server (Administration software, English man pages, Core software, Configuration, Drivers)
   - Installs the Kiosk Mode software
   - Restores the SRSS configuation data from the `/var/tmp/SUNWut.upgrade/preserve_`*`version`*`.tar.gz` file.
   - Provides a notice that the system must be rebooted.

5. When prompted, reboot the Sun Ray server.

Check the log file. Many installation problems are reported in this file that are frequently overlooked. A time-stamped log file indicating when the install was started is available at:

```
/var/adm/log/utinstall.<year>_<month>_<date>_<hour>:<minute>:<second>.log
```

For a listing of `utinstall` error messages, see Troubleshooting Installation.

Where to Go Next

Go to Task Map - Configuring an Upgraded Sun Ray Server for instructions how to prepare to configure and reboot the Sun Ray server.

Contents

Configuring a Sun Ray Server (All Topics)

Task Map - Configuring a Newly Installed Sun Ray Server

The following steps describe how to configure a Sun Ray server after a new installation of the Sun Ray Server Software.

Step	Description
1. Determine your network topology.	Sun Ray servers can be deployed on dedicated private networks and on shared networks. Sun Ray Server Software deployments on shared networks, whether routed or non-routed shared networks (LANs), offer many benefits to users, especially hotdesking. Shared networks can be configured with or without separate DHCP servers or bootp forwarding. If you are not sure about any aspect of your network configuration, consult your IT staff. For more information, see Configuring Sun Ray System Networks.
2. Fill in the Configuration Worksheet.	Configuration Worksheets
3. Configure the Sun Ray server on the network.	• On a Private Network (no LAN) • On a Shared Network (LAN) Using Existing DHCP Server • On a Shared Network (LAN) and Configuring the Sun Ray Server as a DHCP Server
4. Configure the Sun Ray Server Software.	How to Configure the Sun Ray Server Software
5. For failover groups, configure the hierarchy of the Sun Ray servers in the failover group.	Task Map - Managing Failover Groups
6. Synchronize the Sun Ray DTU firmware.	How to Synchronize the Sun Ray DTU Firmware
7. After configuration, reboot the Sun Ray server.	How to Reboot a Sun Ray Server

Repeat this sequence for each Sun Ray server in a failover group.

Note
When the host name or IP address of a Sun Ray server is changed, the interfaces should also be configured, especially if the Sun Ray server is used for DHCP services.

Task Map - Configuring an Upgraded Sun Ray Server

The following steps describe how to configure a Sun Ray server after an upgrade of the Sun Ray Server Software. These steps assume that the upgrade has used the `utpreserve` script.

Step	Description
1. Have your configuration Worksheet Ready.	If you filled out the worksheet before the upgrade, you can use the information to help you with network configuration. See Configuration Worksheets.
2. Configure the Sun Ray server on the network.	• On a Private Network (no LAN) • On a Shared Network (LAN) Using Existing DHCP Server • On a Shared Network (LAN) and Configuring the Sun Ray Server as a DHCP Server
3. Synchronize the Sun Ray DTU firmware.	How to Synchronize the Sun Ray DTU Firmware
4. Reconfigure the Sun Ray Server	You must reconfigure the Sun Ray using the `utconfig -w` command to update the location of the Tomcat installation. See Admin GUI Upgrade (CR 6572246).
5. After configuration, reboot the Sun Ray server.	How to Reboot a Sun Ray Server

Task Map - Additional Sun Ray Server Configuration

Task	Description
How to Check and Fix Corrupted Configuration Files (Solaris)	Explains how to fix the Xsun server that is not starting properly.
How to Synchronize Primary and Secondary Sun Ray Servers	Explains how to synchronize Sun Ray servers in a Failover Group to sync time stamps for error messages.
How to Unconfigure a Sun Ray Server	Explains how to unconfigure SRSS on a Sun Ray server.
How to Disconnect a Sun Ray Server From the Interconnect	Explains how to disconnect a Sun Ray server from the interconnect.
How to Convert and Synchronize the Sun Ray Data Store Port (Solaris)	Explains how to convert the old Sun Directory Service to the Sun Ray Data Store, and how to re-enable the previous SunDS service.

Configuration Worksheets

Fill out these worksheets so that the information is readily available during the actual configuration process.

- Values that are provided in italics are only examples and should not be used.
- Values provided in normal font are defaults and can be used.
- Superscripted numbers $^{(\#)}$ refer to footnotes at the end of each section.

Note
The blank rows in the worksheets are provided for you to add additional information about your environment if you choose to print the worksheets.

Sun Ray Server Dedicated Interconnect Configuration Worksheet

Aspect or Variable	Default Value, Example, or (Other)	Your Primary Server Value	Your Secondary Server Value
Configuring the Sun Ray interconnect interface using **`utadm`**	(Provide the start time)		
Interface name	hme1_ (Solaris), _eth1 (Linux)		
• Host address [(1)]	192.168.128.1		
• Net mask	255.255.255.0		
• Net address	192.168.128.0		
• Host name [(1)]	hostname-interface-name		
If the Sun Ray server is used for IP address allocation:			
• First Sun Ray DTU address	192.168.128.16		
• Number of Sun Ray DTU addresses [(2)]	X		
Firmware server [(3)]	192.168.128.1		
Router [(3)]	192.168.128.1		
Specify additional server list? (optional)	(yes or no)		
• If yes, filename	filename		
• Or, Server IP address	192.168.128.2		
Configuring Sun Ray Server Software using utconfig	(Provide the start time)		
Admin password	adminpass		
Configure Admin GUI? If yes, then:			
• Sun Ray admin server port number	1660		
• Enable remote administration? (optional)	(yes or no)		
• Enable secure connection? (optional)	(yes or no)		
Configure Kiosk Mode? (optional)	(yes or no)		

• If yes, User prefix	utku		
• Group name	utkiosk		
• User ID range start	150000		
• Number of users [4]	25		
Configure failover group? (optional)	(yes or no)		
• If yes, Failover group signature [5]	signature1		

[1] These values are different for each Sun Ray server, even if that server is part of a failover group.

[2] These values must be unique among the servers in a failover group. The following guidelines can help you determine what addresses to allocate for each Sun Ray server:

- X = (Number of DTUs/(Number of servers - 1)) - 1
- First unit address for primary server= 192.168.128.16
- Last unit address for all servers = X + first unit address. If last unit address is greater than 240, reduce to 240.
    - First unit address for secondary servers = 1 + last unit address of previous server. If first unit address is greater than 239, configure for a class B network. Example: 120 DTUs, 4 servers. X= 39

[3] These values are the same as the interface host address by default.

[4] The value entered for the number of users is the greater of:

- The total number of Sun Ray DTUs
- The total number of disconnected and active sessions

[5] This signature^ must be the same for every Sun Ray server in a failover group. The signature requires at least one numeric character.

Sun Ray Server LAN Configuration Worksheet

If you are configuring a Sun Ray server on a LAN, use the following worksheet.

Aspect or Variable	Default Value, Example, or (Other)	Your Primary Server Value	Your Secondary Server Value
Configuring the Sun Ray interconnect interface using **`utadm`**	(Provide the start time)		
• Subnetwork	192.168.128.0		

- Host address [6]	192.168.128.1		
- Net mask	255.255.255.0		
- Net address	192.168.128.0		
- Host name [6]	hostname-interface-name		
If the Sun Ray server is used for IP address allocation:			
- First Sun Ray DTU address [7]	192.168.128.16		
- Number of Sun Ray DTU addresses [7]	X		
- Firmware server [8]	192.168.128.1		
- Router [8]	192.168.128.1		
Specify additional server list? (optional)	(yes or no)		
- If yes, filename	filename		
- Or, Server IP address	192.168.128.2		

[6] These values are different for each Sun Ray server, even if that server is part of a failover group.

[7] These values must be unique among the servers in a failover group. The following guidelines can help you determine what addresses to allocate for each Sun Ray server:

- X = (Number of DTUs/(Number of servers - 1)) - 1
- First unit address for primary server= 192.168.128.16
- Last unit address for all servers = X + first unit address. If last unit address is greater than 240, reduce to 240.
    - First unit address for secondary servers = 1 + last unit address of previous server. If first unit address is greater than 239, configure for a class B network. Example: 120 DTUs, 4 servers. X= 39

[8] These values are the same as the interface host address by default.

Sun Ray Server Failover Group Worksheet

If you are configuring for a failover group, fill in this portion of the worksheet:

Aspect or Variable	Default Value, Example, or (Other)	Your Primary Server Value	Your Secondary Server Value
Configuring the Sun Ray server hierarchy using **`utreplica`** (required for failover groups)	(Provide the start time)		
Primary Sun Ray server host name [9]	primary-server		
Secondary Sun Ray server host name [9]	secondary-server		

[9] These values are different for each Sun Ray server, even if that server is part of a failover group.

First and Last Unit Address in a Failover Group

Server	First Unit Address	Last Unit Address
Primary	192.168.128.16	192.168.128.55
Secondary	192.168.128.56	192.168.128.95
	192.168.128.96	192.168.128.135
Secondary	192.168.128.136	192.168.128.175
Secondary		

Note
If you forget the address range, use `utadm -l` to list the addresses you specified or `utadm -p` to print them.

How to Configure a Sun Ray Server as a Private Interconnect

This procedure shows how to configure a Sun Ray server as a private interconnect, where the DTU display network is directly connected to the Sun Ray server.

1. Log in as the superuser of the Sun Ray server, either locally or remotely.
2. Change to the following directory:

```
# cd /opt/SUNWut/sbin
```

Note
Make sure that the `/etc/hosts` file contains the IP address of the system host name.

3. Configure the Sun Ray interconnect interface:

```
# ./utadm -a <interface-name>
```

where `<interface-name>` is the name of the interface to the Sun Ray interconnect, for example: `hme1`, `qfe0`, or `ge0` (Solaris) or `eth1` (Linux).

The `utadm` script begins configuring DHCP for the Sun Ray interconnect, restarts the DHCP daemon, and configures the interface. The script then lists the default values and asks whether they are acceptable.

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

4. Evaluate the default values:
   - If you are satisfied with the default values, and the server is not part of a failover group, answer y.
   - Otherwise, answer n and accept whatever default values are shown by pressing Return, or provide the correct values from the worksheet.

     The `utadm` script prompts for the following:
   - New host address (192.168.128.1)
   - New netmask (255.255.255.0)
   - New host name (hostname-interface-name)
   - Offer IP addresses for this interface? ([Y]/N)
   - New first Sun Ray DTU address (92.168.128.16)
   - Total number of Sun Ray DTU address (X)
   - New authorization server address (192.168.128.1)
   - New firmware server address (192.168.128.1)
   - New router address (192.168.128.1)
   - An additional server list.
     If you answer yes, it requests either a file name (filename) or a Server IP Address (192.168.128.2).

5. The `utadm` script again lists the configuration values and asks whether they are acceptable.
   - If not, answer n and revise the answers provided in Step 4.
   - If the values are correct, answer y. The following Sun Ray files are configured:
     For Solaris:

     ```
     /etc/hostname.<interface-name>
     /etc/inet/hosts
     /etc/inet/netmasks
     /etc/inet/networks
     ```

     For Linux:

     ```
     /etc/opt/SUNWut/net/dhcp/SunRay-options
     /etc/opt/SUNWut/net/dhcp/SunRay-interface-eth1
     /etc/opt/SUNWut/net/hostname.eth1
     /etc/hosts
     /etc/opt/SUNWut/net/netmasks
     /etc/opt/SUNWut/net/networks
     /etc/dhcpd.conf
     ```

     The `utadm` script configures the Sun Ray DTU firmware versions and restarts the DHCP daemon.

6. Repeat this procedure for each of the secondary servers in your failover group.

Next Steps

Go to How to Configure the Sun Ray Server Software.

How to Configure a Sun Ray Server on a LAN (and DHCP Server Setup)

This procedure shows how to configure a Sun Ray server as a shared interconnect where DTUs are connected to a network (LAN) that is shared with other workstations or servers. This procedure also sets up the Sun Ray Server as a DHCP server.

Before You Begin

- If your network does not have a separate DHCP server, configure the Sun Ray server using IP addresses supplied by the Sun Ray server.
- If your network has a separate DHCP server, configure the Sun Ray server using IP addresses supplied by the DHCP server.

Steps

1. Log in as the superuser of the Sun Ray server.
2. Change to the following directory:

   ```
   # cd /opt/SUNWut/sbin
   ```

3. Configure the Sun Ray LAN subnet:

   ```
   # ./utadm -A <subnet#>
   ```

   where `<subnet#>` is the identifying number of the subnet, such as 192.168.128.0.
   The `utadm` script begins configuring DHCP for the Sun Ray interconnect, restarts the DHCP daemon, and configures the interface. The script then lists the default values and asks whether they are acceptable.

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

4. Evaluate the default values.
   - If you are satisfied with the default values and the server is not part of a failover group, answer y.
   - Otherwise, answer n and accept whatever default values are shown by pressing Return or provide the correct values from the worksheet.

     The `utadm` script prompts for the following:
   - New netmask (255.255.255.0)
   - New first Sun Ray DTU address (192.168.128.16)
   - Total number of Sun Ray DTU addresses
   - New authorization server address (192.168.128.1)
   - New firmware server address (192.168.128.10)
   - New router address (192.168.128.1)
   - An additional server list.
     If you answer yes, it requests either a file name (filename) or a server IP address (192.168.128.2)
5. The `utadm` script again lists the configuration values and asks whether they are acceptable.
   - If not, answer n and revise the answers you provided in Step 4.
   - If the values are correct, answer y. The `utadm` script configures the Sun Ray DTU firmware versions and restarts the DHCP daemon.
6. Repeat this procedure for each of the secondary servers in your failover group.
7. If a router is between the Sun Ray server and the DTUs, configure bootp forwarding in the routers.

Next Steps

Go to How to Configure the Sun Ray Server Software.

How to Configure a Sun Ray Server on a LAN (Using Existing DHCP Server)

If you plan to use an existing DHCP server to provide Sun Ray parameters, use this procedure to enable or disable the LAN connection on the Sun Ray server. If you need the Sun Ray server to provide DHCP services, see How to Configure a Sun Ray Server on a LAN (and DHCP Server Setup).

1. Log in as the superuser of the Sun Ray server, either locally or remotely.
2. Enable the Sun Ray LAN connection.

   ```
   # /opt/SUNWut/sbin/utadm -L on
   ```

3. Restart services as prompted.

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

   If you plan to configure the Sun Ray Server Software, you can wait to restart services until after you configure the software.

4. Verify the current setting for the Sun Ray LAN connection.

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

> Note
> When the LAN connection is turned off on a Sun Ray server, Sun Ray DTUs on the LAN cannot attach to the server. To turn off the Sun Ray server LAN connection, use the `utadm -L off` command and restart services.

Next Steps

Go to How to Configure the Sun Ray Server Software.

How to Configure the Sun Ray Server Software

1. If you have not already done so, log in as the superuser of the Sun Ray server.
2. Change to the following directory:

   ```
   # cd /opt/SUNWut/sbin
   ```

3. Configure Sun Ray Server Software.

   ```
   # ./utconfig
   ```

4. Accept the default `utconfig` values shown by pressing Return or provide the correct values from the worksheet. The `utconfig` script prompts for the following information:

- Whether the script should continue (press Return)
- Sun Ray administration password (adminpass)
- Sun Ray administration password again
  Note that all servers in a failover group must use the same administration password.
- To configure the Sun Ray Web Administration (Admin GUI), (press Return)
- Path to the Apache Tomcat installation directory (/opt/apache-tomcat)
- Web server port number (1660)
- Whether to enable secure connections (y/n)
- If Yes, type HTTPS port number (1661)
- To supply a user name for the Tomcat process (utwww)
- Whether you want to enable remote administration (y/n)
- Whether you want to configure Kiosk Mode (y/n).
  If yes, it requests:
  - User prefix (utku)
  - Group (utkiosk)
  - User ID range start (150000)
  - Number of users (25)
- Whether you want to configure for a failover group
- Whether the script should continue (press Return)

The `utconfig` script begins configuring Sun Ray Server Software.

- If you responded that this is a failover group, the script requests the signature (signature1)
- The signature again

The Sun Ray Data Store is restarted.

> Note
> The `utconfig script` states that you must restart the authentication manager. You can restart the authentication manger by rebooting the Sun Ray server or by restarting the Sun Ray services through the `/opt/SUNWut/sbin/utrestart -c` command.

The `utconfig` script ends, indicating a log file is available.
Solaris OS location:

```
/var/adm/log/utconfig.<year>_<month>_<date>_<hour>:<minute>:<second>.log
```

Linux OS location:

```
/var/log/SUNWut/utconfig.<year>_<month>_<date>_<hour>:<minute>:<second>.log
```

where the date and time information is represented by numeric values reflecting the time that `utconfig` was started.

5. Repeat this procedure for each secondary server if in a failover group.

Next Steps

Do one of the following:

- If you have a failover group, see Task Map - Managing Failover Groups.
- Otherwise, go to How to Synchronize the Sun Ray DTU Firmware.

Task Map - Managing Failover Groups

For more information about failover groups, see About Failover Groups.

Initial Configuration

Step	Description	Task
1	Set up server addresses and client addresses, and how to configure DHCP.	Set Up IP Addressing How to Set Up IP Addressing on Multiple Servers, Each with One Sun Ray Interface
2	Use the `utreplica` command to designate a primary server, advise the server of its administration primary status, and designate the host names of all the secondary servers.	How to Configure a Primary Server
3	Use the `utreplica` command to advise each secondary server of its secondary status and the host name of the primary server for the group.	How to Add a Secondary Server
4	Synchronize secondary servers with their primary server to make troubleshooting easier. Use `crontab` to schedule this command to execute periodically.	How to Synchronize Primary and Secondary Sun Ray Servers
5	Change the group manager signature.	How to Change the Group Manager Signature

Related Tasks

Task	Description
How to Take a Server Offline and Online	Explains how to take servers offline to make maintenance easier.
How to Show the Current SRDS Replication Configuration	Explains how to display the current SRDS configuration.
How to Remove the Replication Configuration	Explains how to remove the replication configuration.
How to View Network (Failover Group) Status	Explains how to view failover group status.
Recovery Issues and Procedures	Explains how to recover primary and secondary servers if they fail.

How to Synchronize the Sun Ray DTU Firmware

You must perform this task on a stand-alone Sun Ray server or the last Sun Ray server configured in a failover group. It takes the current firmware available on the Sun Ray server and upgrades all the firmware on the Sun Ray DTUs.

1. Log in as the superuser of the Sun Ray server.
2. Change to the following directory:

```
# cd /opt/SUNWut/sbin
```

3. Synchronize the Sun Ray DTU firmware.

```
# ./utfwsync
```

The Sun Ray DTUs reboot themselves and load the new firmware.

How to Reboot a Sun Ray Server

If you perform a configuration procedure on a Sun Ray server, you must reboot the Sun Ray server to have the change take effect.

1. If you have not already done so, log in as the superuser of the Sun Ray server.
2. Reboot the Sun Ray server.

```
# /usr/sbin/reboot
```

How to Check and Fix Corrupted Configuration Files (Solaris)

If the `dtlogin` daemon cannot start the `Xsun` server properly, the following configuration files might be corrupted:

- `/etc/dt/config/Xservers`
- `/etc/dt/config/Xconfig`

The following procedure explains how to correct this problem

Note
This procedure shows output from a simplified example. Your output may have tens of lines between the BEGIN SUNRAY CONFIGURATION and END SUNRAY CONFIGURATION comments.

Steps

1. As a user of the Sun Ray server, open a shell window and compare the `/usr/dt/config/Xservers` and `/etc/dt/config/Xservers` files.

```
% diff /usr/dt/config/Xservers /etc/dt/config/Xservers
```

   This command compares a known good file with the suspect file. The output should be similar to the following example.

```
106a107,130
> # BEGIN SUNRAY CONFIGURATION
> :3 SunRay local@none /etc/opt/SUNWut/basedir/lib/utxsun :3 -nobanner
    .
    .
> :18 SunRay local@none /etc/opt/SUNWut/basedir/lib/utxsun :18 -nobanner
> # END SUNRAY CONFIGURATION
```

   The first line of output contains 106a107,130. The 106 means that the two files are identical to the 106th line of the files. The a107,130 means that the information on lines 107 through 130 of the second file would have to be added to the first file to make it the same as the second file.
   If your output shows the first three digits to be a number less than 100, the `/etc/dt/config/Xservers` file is corrupt.

2. Compare the `/usr/dt/config/Xconfig` and `/etc/dt/config/Xconfig` files.

```
% diff /usr/dt/config/Xconfig /etc/dt/config/Xconfig
```

   The output should be similar to the following example.

```
156a157,180
> # BEGIN SUNRAY CONFIGURATION
> Dtlogin.*_8.environment: SUN_SUNRAY_TOKEN=ZeroAdmin.m1.at88sc1608.6d0400aa
    .
    .
> Dtlogin.*_9.environment: SUN_SUNRAY_TOKEN=ZeroAdmin.m1.at88sc1608.a10100aa
> # END SUNRAY CONFIGURATION
```

   If your output shows the first three digits to be a number less than 154, the `/etc/dt/config/Xconfig` file is corrupt.

3. If either file is corrupted, continue this procedure to replace the configuration files.
4. As superuser, open a shell window and stop the Sun Ray server.

   ⚠ Caution
   Replacing the `Xservers` file requires shutting down all Sun Ray DTU services. Remember to inform users of the outage.

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

5. Replace the `Xservers` and `Xconfig` files as appropriate.

   ```
   # /bin/cp -p /usr/dt/config/Xservers /etc/dt/config/Xservers
   # /bin/cp -p /usr/dt/config/Xconfig /etc/dt/config/Xconfig
   ```

   Note
   For headless servers, comment out or remove the `:0` entry from the `Xservers` file.

6. Re-initialize the authentication policy.

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

   The extra lines within the previous `Xservers` and `Xconfig` files are automatically rebuilt.

How to Synchronize Primary and Secondary Sun Ray Servers

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

The Network Time Protocol (NTP) is the recommended protocol to synchronize primary and secondary servers. With NTP, you can synchronize to an absolute time source and it provides additional synchronization capabilities. In some deployments, the simpler TIME protocol configured through the `rdate` command may be sufficient.

For detailed information about configuring NTP on Solaris servers, see Solaris 10 System Administration Guide: Network Services.

Note
Both the NTP and TIME protocols are disabled by default on Solaris servers.

How to Unconfigure a Sun Ray Server

1. Log in as superuser on the Sun Ray server.
2. Remove the replication configuration.

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

3. Unconfigure Sun Ray Server Software.

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

4. Answer y to all the prompts.

How to Disconnect a Sun Ray Server From the Interconnect

Caution
This procedure disconnects users from their sessions on the Sun Ray server. Make sure your users terminate their sessions before you continue.

1. Log in as superuser on the Sun Ray server.
2. Disconnect the Sun Ray server from the Sun Ray interconnect.

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

Note
(Solaris Only) If you press `Ctrl+C` while performing `utadm` configuration, the Admin GUI may not function correctly the next time you invoke it. To correct this condition, type `dhtadm -R`.

How to Convert and Synchronize the Sun Ray Data Store Port (Solaris)

In place of the old Sun Directory Service (SunDS) used in Sun Ray Server Software versions 1.0 through 1.3, a private data store service, the Sun Ray Data Store (SRDS), has been provided starting with version 2.0.

SRDS uses service port 7012 to avoid conflict with the standard LDAP port number, 389. When you upgrade a server to at least version SRSS 2.0, the LDAP port remains in use until all the servers in the failover group have been upgraded and converted. Port conversion is required only if you plan to continue to run SunDS on the recently upgraded SRSS server.

Note
Even though you have upgraded a server, you cannot run the Sun Ray Data Store until you also convert the port number. Perform this task on stand-alone Sun Ray servers or on the primary server in a failover group after all the servers in the group have been upgraded.

1. Log in as the superuser of the primary Sun Ray server.
2. Change to the following directory.

```
# cd /opt/SUNWut/sbin
```

3. Convert and synchronize the Sun Ray Data Store service port number on all the servers in a failover group:

```
# ./utdssync
```

This step restarts the Sun Ray Data Store on all the servers.

Contents

Configuring Sun Ray System Networks (All Topics)

About Sun Ray System Networks

Network administrators can deploy Sun Ray DTUs nearly anywhere on an enterprise intranet. The most important advantages of intranet deployment are:

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

Basic Network Topology

Before configuring a Sun Ray server on a network, you should understand what your basic network configuration looks like. The three basic topology options for Sun Ray deployment are the following:

- Dedicated Private Non-Routed Sun Ray Network - A directly connected dedicated interconnect
- Shared Network With Non-Routed Sun Ray DTUs - A directly connected shared subnet
- Shared Routed Network - A remote shared subnet

The following sections describe, in simplified form, the most common types. If you have any doubt as to which network model most nearly approximates your site, consult your IT staff.

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

Routerless VPN Capability

Sun Ray Server Software and the most recent firmware provide a VPN solution for remote users that does not require a separate VPN router. The IPsec capability in the Sun Ray firmware enables the Sun Ray DTU to act as a stand-alone VPN device. The most commonly used encryption, authentication, and key exchange mechanisms are supported, along with Cisco extensions that enable a Sun Ray DTU to interoperate with Cisco gateways that support the Cisco EzVPN protocol.

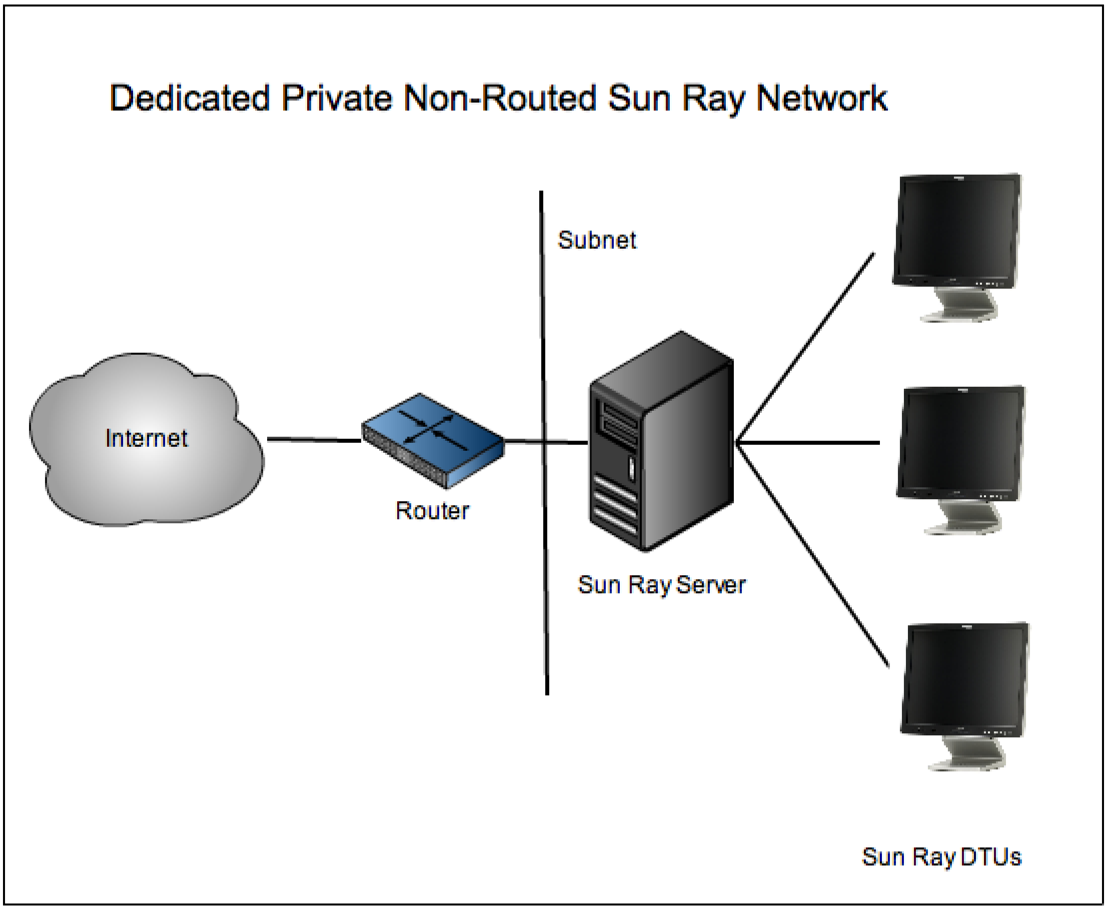
Although digital certificates are not supported, the security model is identical to that of the Cisco software VPN client. Using a common group name and key for the initial IKE phase one authentication exchange, the DTU authenticates the user individually with the Cisco Xauth protocol, either by presenting a fixed user name and password stored in flash memory or by requiring the entry of a user name and one-time password generated by a token card.

Dedicated Private Non-Routed Sun Ray Network

The directly connected dedicated interconnect (often referred to as an interconnect) places DTUs on subnets that meet the following criteria:

- Directly connected to the Sun Ray server, that is, the server has a network interface connected to the subnet.
- Devoted entirely to carrying Sun Ray traffic.

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



Shared Network With Non-Routed Sun Ray DTUs

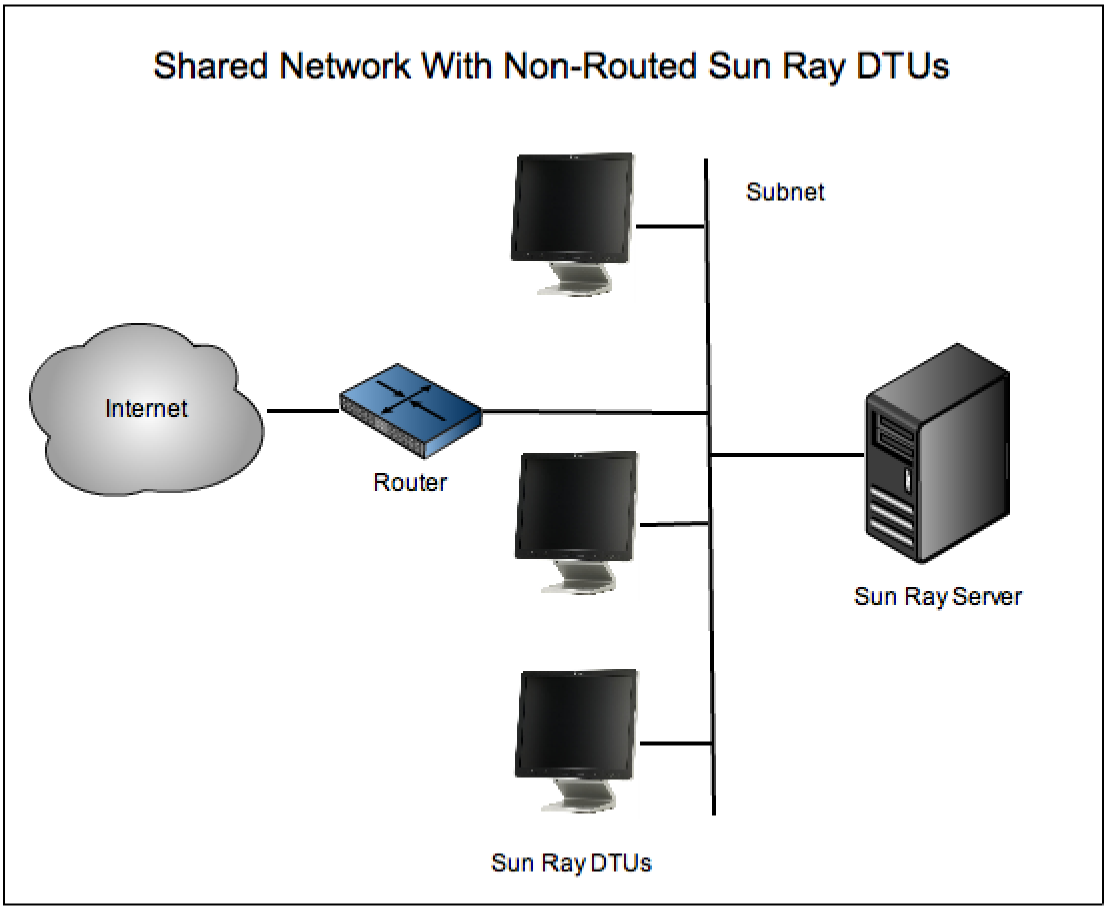
In contrast to private network configurations, shared network configurations with existing DHCP servers may require bootp forwarding in order to function properly with existing network infrastructure.

Sun Ray Server Software supports DTUs on a directly connected shared subnet that meet the following criteria:

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

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

Many newer configurations resemble the following diagram, which shows a shared network with non-routed Sun Ray DTUs.



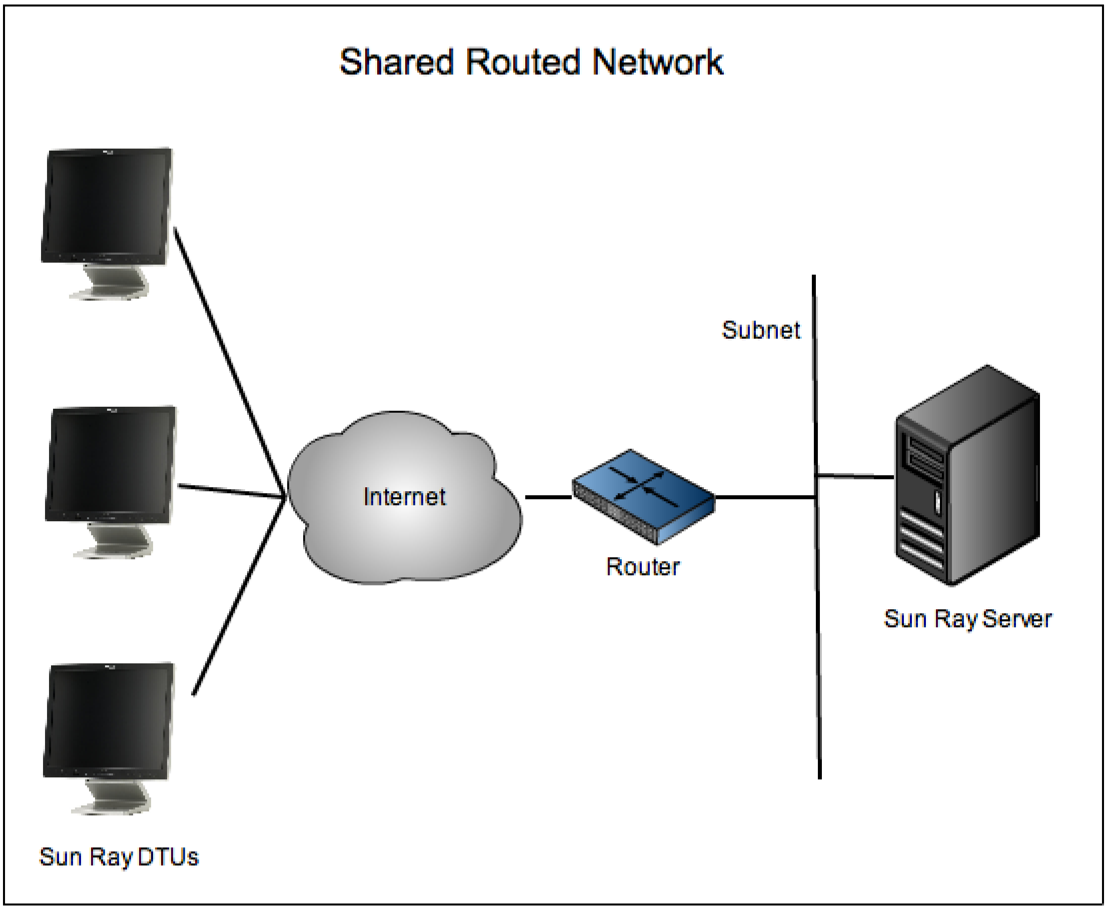
Shared Routed Network

Sun Ray Server Software also supports DTUs on a remote shared subnet that meet the following criteria:

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

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

A shared routed network is shown below.



Network Performance Requirements

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

Packet Loss

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

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

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

Latency

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

Out-of-Order Packets

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

Encapsulated Options

For each parameter name, there is a vendor ID, an option code, an option type, and an indication as to whether the parameter is mandatory.

Vendor-specific options are delivered through encapsulated options in DHCP. Encapsulated options are somewhat more complicated, as illustrated in the following DHCPINFORM response, or DHCPACK, which shows the taxonomy of the bytes in the vendor-specific information portion.

```
2b 4a 17 1d 32 2e 30   .......: .+J..2.0
0140  5f 31 39 2e 63 2c 52 45  56 3d 32 30 30 32 2e 30   _19.c,RE V=2002.0
0150  39 2e 30 36 2e 31 35 2e  35 34 21 04 68 6d 65 30   9.06.15. 54!.hme0
0160  1f 04 81 92 3a 88 15 04  81 92 3a 88 1d 01 06 1c   ....:... ..:.....
0170  01 06 1b 01 06 1a 01 06  19 01 06 18 04 81 92 3a   ........ .......:
0180  88 16 02 1b 61
```

Note
In this description, hexadecimal values are preceded by 0x and followed by their decimal value, after an = sign, as in `0x2b=43`.

- The first byte is the option code.
- The next byte represents the encapsulated option length, that is, the number of bytes that make up the option value.
- The next one or more bytes make up the multi-byte option value.

The option value is followed by another encapsulated option code, and so on.

The example begins with `0x2b=43`, the DHCP option for vendor-specific information. It has a length of `0x4a=74` bytes, which is the total number of bytes that follow. These bytes contain the encapsulated vendor options.

The remainder of the example represents the value of the vendor-specific information options. The first byte contains the first encapsulated option, whose value is `0x17=23`, and the `NewTVer` option, whose value type is ASCII. The next byte is `0x1d=29`, which is the length of the `NewTVer` string. These options are followed by 29 bytes that represent the string itself.

The ASCII interpretation at the right of the DHCPACK, is `2.0_19.c,REV=2002.09.06.15.54`. This is the end of the first encapsulated option. The next byte is the beginning of the next option, Intf, represented by `0x21=33`. The next byte, the length, is `0x04=4`, and the next four bytes are the ASCII value `hme0`. That's the end of the second encapsulated option.

The next byte is `0x1f=31`, which represents the FWSrvr parameter, whose function is to indicate the IP address of the firmware TFTP server. The next byte is the length, 4, which is always be true for an IP address. The hexadecimal value is `0x81 0x92 0x3a 0x88`, which corresponds to the IP address `129.146.58.136`.

Ports and Protocols

The following tables summarize Sun Ray system port and protocol usage. For SRWC specific port and protocol requirements, see the SRWC Ports and Protocols page.

The range of dynamic/UDP ports on the server is constrained to the range defined by the `utservices-low` and `utservices-high` UDP service definitions, whose default values in `/etc/services` are 40000 and 42000 respectively.

- Dynamic/TCP ports on the client are in the range 32768-65535.
- Dynamic/UDP ports on the client are in the range 4096-65535.
- ALP rendering traffic (ALP-RENDER) always uses a UDP port number greater than 32767 at the client.

Sun Ray Client-to-Server Ports and Protocols

In the following table, a double-headed arrow in the Flow column indicates the direction of the initial packet. In most cases, the client (a Sun Ray DTU or Sun Desktop Access Client) initiates the interaction.

Client Port	Flow	Protocol	Flow	Server Port	Peer	Importance	Comments
66/UDP (BOOTPC/ DHCPC)	--broadcast->> --unicast->>	DHCP	<-broadcast-- <-unicast--	67/UDP (BOOTPS/DHCPS)	DHCP Service	Mandatory	Network and configuration parameter discovery
Dynamic/ UDP	--unicast->>	TFTP	<-unicast--	69/UDP (TFTP)	TFTP Service	Recommended	Firmware download (Configuration parameter download)
Dynamic/ UDP	--unicast->>	DNS	<-unicast--	53/UDP (domain)	DNS Service	Optional	For server name lookups
514/ UDP (syslog)	--unicast->>	Syslog	(none)	514/UDP (syslog)	Syslog Service	Optional	Event reporting
Dynamic/ UDP	--broadcast->>	ALP-DISCOVERY	<-unicast--	7009/UDP (utauthd-gm)	Sun Ray Server	Optional	On-subnet Sun Ray server discovery
Dynamic/ TCP	--unicast->>	ALP-AUTH	<-unicast--	7009/TCP (utauthd)	Sun Ray Server	Mandatory	Presence, control, status
Dynamic/ UDP with port number >= 32768	--unicast-> or --unicast->> when NAT is in use	ALP-RENDER	<<-unicast-- or <-unicast-- when NAT is in use	Dynamic/UDP constrained by utservices-low and utservices-high	Sun Ray Server	Mandatory	On-screen drawing, user input, audio
5498/UDP	--unicast->>	ALP-AUDIO-IN		Dynamic/UDP constrained by utservices-low and utservices-high	Sun Ray Server	Optional	Inbound audio
Dynamic/ TCP	-unicast->>	ALP-DEVMGR	<-unicast--	7011/TCP (utdevmgr)	Sun Ray Server	Optional	Device management
7777/ TCP	--unicast->	ALP-DEVDATA	<<-unicast--	Dynamic/TCP	Sun Ray Server	Optional	Device data transfer
7013/ UDP (utquery)	--unicast->	ALP-QUERY	<<-unicast-- <<-broadcast--	Dynamic/UDP	Any	Optional	utquery support

ℹ Due to CR 6985550, the keyboard may become unresponsive to input. To work around this issue, allow ICMP messages to flow from the Sun Ray server to the client.

Sun Ray Server-to-Server Protocols

Sun Ray Server Port	Protocol	Port	Peer	Notes
	<<-ARP->>		All on subnet	IP-to-MAC mapping

Transient	--SYSLOG/UDP unicast->>	514 (SYSLOG)	Syslog Server	Status reporting, if required
7009 (UTAUTHD)	<<-UTAUTHD-GM/UDP->> broadcast or multicast	7009 (UTAUTHD)	Sun Ray Server	Group discovery, if required
7011 (UTDEVMGRD)	<<-UTDEVMGRD/TCP->>	7011 (UTDEVMGR)	SR Group Member	Device control and status
7008 (UTRCMD)	<<-UTDEVMGRD/TCP->	Privileged	SR Group Member	Remote execution
	<<-ICMP ECHO->		Any	Admin: presence (a bug)
7010 (UTAUTH-CB)	<<-UTAUTH-CB/TCP->	Transient	Any	Admin: control and status
7012 (UTDS)	<<-UTDS/TCP->	Transient	Any	Data store, if required. If you are using the obsolete SunDS port of 389, you should switch to 7012. If you need to convert from SunDS, refer to How to Convert and Synchronize the Sun Ray Data Store Port (Solaris) .
7007 (UTSESSIOND)	<<-UTSESSION/TCP->	Transient	Any	Session members
7011 (UTDEVMGR)	<<-UTDEVMGR/TCP->	Transient	Any	Device clients
1660 (HTTP)	<<-HTTP/TCP->	Transient	Localhost	Web GUI, if configured
1661 (HTTPS)	<<-HTTPS/TCP->	Transient	Localhost	Web GUI, if configured
7007 (UTSESSIOND)	<<-UTSESSION/TCP->	Privileged	Localhost	Session management

Network Configuration Examples

By supporting various network configurations, the Sun Ray system enables DTUs to be deployed virtually anywhere on the enterprise intranet, subject only to the provision of DHCP service and a sufficient quality of service between the DTU and the Sun Ray server.

Preparing for Deployment

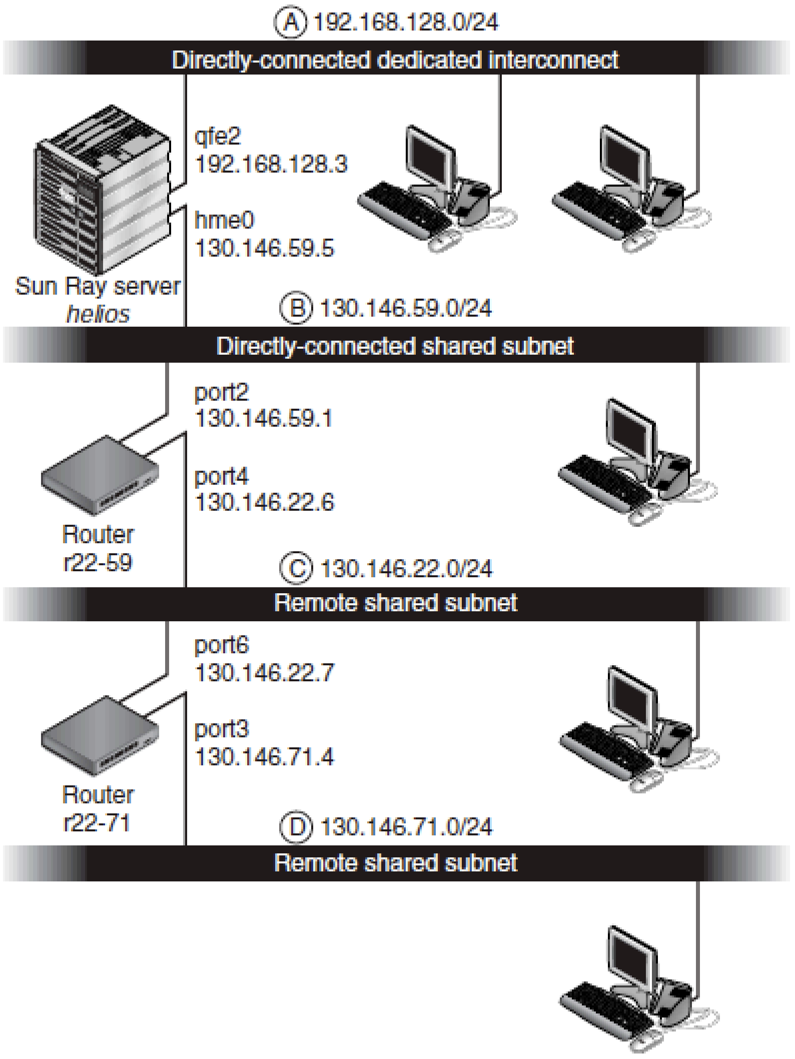
Before deploying a DTU onto any subnet, the administrator must answer three questions:

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

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

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

Sun Ray Network Topology



Deployment on a Directly Connected Dedicated Interconnect

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

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

- From which DHCP server will DTUs on this subnet get their basic IP networking parameters?
  On a directly connected dedicated interconnect, basic networking parameters are always supplied by the DHCP service on the Sun Ray server.
- From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?
  On a directly connected dedicated interconnect, additional configuration parameters are always supplied by the DHCP service on the Sun Ray server.
- How will DTUs on this subnet locate their Sun Ray server?
  On a directly connected dedicated interconnect, the DTU is always notified of the location of the Sun Ray server through an additional configuration parameter supplied when Sun Ray services are restarted.

Directly Connected Dedicated Interconnect: Example

This example shows the DHCP service for the directly connected dedicated interconnect A shown in Sun Ray Network Topology.

1. Configure the Sun Ray server to provide both basic and additional parameters to the interconnect.
   Use the `utadm -a <ifname>` command to configure DHCP service for DTUs on an interconnect. In this example, the interconnect is attached through interface `qfe2`:

```
# /opt/SUNWut/sbin/utadm -a qfe2
### Configuring /etc/nsswitch.conf
### Configuring Service information for Sun Ray
### Disabling Routing
### configuring qfe2 interface at subnet 192.168.128.0
 Selected values for interface "qfe2"
   host address:         192.168.128.1
   net mask:             255.255.255.0
   net address:          192.168.128.0
   host name:            helios-qfe2
   net name:             SunRay-qfe2
   first unit address:   192.168.128.16
   last unit address:    192.168.128.240
   auth server list:          192.168.128.1
   firmware server:      192.168.128.1
   router:               192.168.128.1
 Accept as is? ([Y]/N): n
 new host address: [192.168.128.1] 192.168.128.3
 new netmask: [255.255.255.0]
 new host name: [helios-qfe2]
 Do you want to offer IP addresses for this interface? ([Y]/N):
 new first Sun Ray address: [192.168.128.16]
 number of Sun Ray addresses to allocate: [239]
 new auth server list: [192.168.128.3]
To read auth server list from file, enter file name:
Auth server IP address (enter <CR> to end list):
If no server in the auth server list responds, should an auth server be located
by broadcasting on the network? ([Y]/N):
 new firmware server: [192.168.128.3]
 new router: [192.168.128.3]
 Selected values for interface "qfe2"
  host address:           192.168.128.3
  net mask:               255.255.255.0
  net address:            192.168.128.0
  host name:              helios-qfe2
  net name:               SunRay-qfe2
  first unit address:     192.168.128.16
  last unit address:      192.168.128.254
  auth server list:       192.168.128.3
  firmware server: 1      192.168.128.3
  router:                 192.168.128.3
 Accept as is? ([Y]/N):
### successfully set up "/etc/hostname.qfe2" file
### successfully set up "/etc/inet/hosts" file
### successfully set up "/etc/inet/netmasks" file
### successfully set up "/etc/inet/networks" file
### finished install of "qfe2" interface
### Building network tables - this will take a few minutes
### Configuring firmware version for Sun Ray
        All the units served by "helios" on the 192.168.128.0
        network interface, running firmware other than version
        "2.0_37.b,REV=2002.12.19.07.46" will be upgraded at their
        next power-on.
### Configuring Sun Ray Logging Functions
DHCP is not currently running, should I start it? ([Y]/N):
### started DHCP daemon
#
```

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

2. Restart Sun Ray services on the Sun Ray server by issuing the `utrestart` command to fully activate Sun Ray services on the newly defined interconnect.

```
# /opt/SUNWut/sbin/utrestart
A warm restart has been initiated... messages will be logged to
/var/opt/SUNWut/log/messages.
```

Deployment on a Directly Connected Shared Subnet

Subnet B in Sun Ray Network Topology is a directly connected shared subnet that uses IP addresses in the range `130.146.59.0/24`. The Sun Ray server `helios` is attached to the interconnect through its `hme0` network interface, which has been assigned the IP address `130.146.59.5`. The answers to the three predeployment questions are as follows:

- From which DHCP server will DTUs on this subnet get their basic IP networking parameters?
  In a shared subnet scenario, you must choose whether a DHCP service on the Sun Ray server or some external DHCP service will provide the DTU with basic network parameters. If the enterprise already has a DHCP infrastructure that covers this subnet, it probably supplies basic network parameters. If no such infrastructure exists, configure the Sun Ray server to provide basic network parameters.
- From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?
  The administrator must choose whether to supply additional configuration parameters to the DTU and, if so, whether to use a DHCP service on the Sun Ray server or some external DHCP service for this purpose. On a directly connected shared subnet, it is possible to deploy DTUs without providing additional parameters at all, but this configuration is not desirable because it deprives the DTU of a number of features, including the ability to download new firmware.

  Administrators of an already established DHCP infrastructure might be unable or unwilling to reconfigure that infrastructure to provide additional Sun Ray configuration parameters, so having the Sun Ray server provide these parameters is usually more convenient. This setup can be desirable even when the established infrastructure is capable of delivering the additional parameters. This setup enables SRSS commands to be used to manage the values of the additional configuration parameters when those values need to be changed in response to software upgrades or patch installations on the Sun Ray server.

  For instance, a patch that delivers new DTU firmware could automatically update the firmware version string that is delivered to the DTU. However, if the firmware version parameter is supplied by some external DHCP service, an administrator must manually edit the firmware version parameter string in the external DHCP configuration rules to reflect the new firmware version delivered by the patch. This activity is time-consuming and error-prone, as well as unnecessary.
- How will DTUs on this subnet locate their Sun Ray server?
  Use one of the optional additional configuration parameters to report the location of the Sun Ray server to the DTU. If additional configuration parameters are not supplied to the DTU at all, the DTU has no indication of the location of any Sun Ray server. In these circumstances, the DTU attempts to discover the location of a Sun Ray server by using a broadcast-based mechanism. However, the DTUs broadcast packets propagate only on the local subnet so, in the case of a remote subnet, the broadcast cannot reach the Sun Ray server, and contact cannot be established.

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

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

Directly Connected Shared Subnet: Example 1

In this example, the answers to the three predeployment questions are as follows:

- From which DHCP server will DTUs on this subnet get their basic IP networking parameters?
  From the Sun Ray server.
- From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?
  From the Sun Ray server.
- How will DTUs on this subnet locate their Sun Ray server?
  The DTUs will be informed of the location of the Sun Ray server through an additional configuration parameter delivered when Sun Ray services are restarted.

1. Configure the Sun Ray server to provide both basic and additional parameters to the shared subnet.
   DHCP service for DTUs on a shared subnet is configured through the `utadm -A <submet>` command. In this example, the shared subnet has network number `130.146.59.0`, so the appropriate command is `utadm -A 130.146.59.0`.

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

The default values initially suggested by `utadm` were not appropriate. Specifically, this server would not have offered any IP addresses on the `130.146.59.0` subnet because `utadm` assumes that basic networking parameters, including IP addresses, are provided by some external DHCP service when the DTU is located on a shared subnet. In this example, however, the Sun Ray server is required to provide IP addresses, so the administrator replied n to the first "Accept as is?" prompt and was given the opportunity to provide alternative values for the various parameters. Twenty IP addresses, starting at `130.146.59.200`, were made available for allocation to DHCP clients on this subnet.

2. Restart Sun Ray services on the Sun Ray server by issuing the `utrestart` command to fully activate Sun Ray services on the shared subnet.

```
# /opt/SUNWut/sbin/utrestart
A warm restart has been initiated... messages will be logged to
/var/opt/SUNWut/log/messages.
```

Directly Connected Shared Subnet: Example 2

In this example, the answers to the three predeployment questions are as follows:

- From which DHCP server will DTUs on this subnet get their basic IP networking parameters?
  From an external DHCP service.
- From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?
  The DTUs will not be supplied with additional parameters.
- How will DTUs on this subnet locate their Sun Ray server?
  By using the local subnet broadcast discovery mechanism.

In this example, the Sun Ray server does not participate in DTU initialization at all. Configuration steps are still required on the

Sun Ray server because it responds by default only to DTUs located on directly connected dedicated interconnects. It responds to DTUs on shared subnets only if the `utadm -L` on command has been executed. Running the `utadm -A <subnet>` command to activate DHCP on the Sun Ray server for a shared subnet, as in this example, implicitly executes `utadm -L` on. If `utadm -A <subnet>` has not been run, the administrator must run `utadm -L` on manually to enable the server to offer sessions to DTUs on the shared subnet.

1. Configure the external DHCP service.
   Determining how to configure the external DHCP infrastructure to provide basic networking parameters to the DTUs on this subnet is beyond the scope of this document. Note the following guidelines:
   - If the external DHCP service does not have its own direct connection to this subnet, the administrator must configure a DHCP Relay Agent to deliver DHCP traffic on this subnet to the external DHCP service. The most likely location for such a Relay Agent would be on a router in this subnet, in this case, the router named `r22-59` in Sun Ray Network Topology. For a brief introduction to this topic, refer to Sun Ray DTU Initialization Requirements Using DHCP.
   - An existing external DHCP service might need to have its IP address allocation for this subnet increased in order to support the new DTUs. This requirement applies whenever additional DHCP clients are placed on a subnet. You might also want to reduce the lease time of addresses on this subnet so that addresses become eligible for reuse quickly.
2. Configure the Sun Ray server to accept DTU connections from shared subnets by running the following command:

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

3. Restart Sun Ray services on the Sun Ray server by issuing the `utrestart` command to fully activate Sun Ray services on the shared subnet.

```
# /opt/SUNWut/sbin/utrestart
A warm restart has been initiated... messages will be logged to
/var/opt/SUNWut/log/messages.
```

Deployment on a Remote Subnet

Subnets C and D in Sun Ray Network Topology are remote shared subnets.

Subnet C uses IP addresses in the range `130.146.22.0/24`. Subnet D uses IP addresses in the range 130.146.71.0/24. The Sun Ray server named `helios` has no direct attachment to either of these subnets. This characteristic defines them as remote. The answers to the three predeployment questions are as follows:

- From which DHCP server will DTUs on this subnet get their basic IP networking parameters?
  In a shared subnet scenario, the administrator must choose whether a DHCP service on the Sun Ray server or some external DHCP service will provide the DTU with basic network parameters.
  If the enterprise already has a DHCP infrastructure that covers this subnet, it probably supplies basic network parameters. If no such infrastructure exists, configure the Sun Ray server to provide basic network parameters.
- From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?
  The administrator must choose whether additional configuration parameters will be supplied to the DTU, and, if so, whether they will be supplied by a DHCP service on the Sun Ray server or by some external DHCP service.

  Administrators of an established DHCP infrastructure might be unable or unwilling to reconfigure it to provide additional Sun Ray configuration parameters, so having the Sun Ray server provide them is usually more convenient. This setup can be desirable even when the established infrastructure is capable of delivering the additional parameters. This setup enables you to use Sun Ray Server Software commands to manage the values of the additional configuration parameters, when those values need to be changed in response to software upgrades or patch installations on the Sun Ray server.

  For instance, a patch that delivers new DTU firmware could automatically update the firmware version string delivered to the DTU. However, if the firmware version parameter is supplied by some external DHCP service, an administrator must manually edit the firmware version parameter string in the external DHCP configuration rules to reflect the new firmware version delivered by the patch. This kind of activity is time-consuming and error-prone as well as unnecessary.
- How will DTUs on this subnet locate their Sun Ray server?
  Use one of the optional additional configuration parameters to report the location of the Sun Ray server to the DTU. If additional configuration parameters are not supplied to the DTU at all, the DTU cannot locate a Sun Ray server, so it tries

to discover the location of a Sun Ray server by using a broadcast-based mechanism. However, the DTUs broadcast packets propagate only on the local subnet so they cannot reach a Sun Ray server located on a remote subnet, and cannot establish contact.

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

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

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

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

Remote Shared Subnet: Example 1

In this example, in which DTUs are deployed on subnet C in Sun Ray Network Topology, the answers to the three predeployment questions are as follows:

- From which DHCP server will DTUs on this subnet get their basic IP networking parameters?
  From an external DHCP service.
- From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?
  From the Sun Ray server.
- How will DTUs on this subnet locate their Sun Ray server?
  The DTUs will be informed of the location of the Sun Ray server through an additional configuration parameter delivered once Sun Ray services are restarted. Use the `utadm -A` subnet command as follows to configure DHCP service for DTUs on a shared subnet.

1. Configure the external DHCP service.
   Determining how to configure the external DHCP infrastructure to provide basic networking parameters to the DTUs on this subnet is beyond the scope of this document. Note the following guidelines:
   - If the external DHCP service does not have its own direct connection to this subnet, the administrator must configure a DHCP Relay Agent to deliver DHCP traffic on this subnet to the external DHCP service. The most likely location for such a Relay Agent would be on a router in this subnet, in this case, the router named `r22-59` in Sun Ray Network Topology. For a brief introduction to this topic refer to Sun Ray DTU Initialization Requirements Using DHCP.
   - An existing external DHCP service might need to have its IP address allocation increased for this subnet to support the new DTUs. This requirement applies whenever additional DHCP clients are placed on a subnet. You might also want to reduce the lease time of addresses on this subnet so that addresses become eligible for re-use quickly.
2. Arrange to deliver DHCP traffic to the Sun Ray server.
   Because the Sun Ray server does not have its own direct connection to this subnet, the administrator must configure a DHCP Relay Agent to deliver the subnet's DHCP traffic to the Sun Ray server. The most likely location for such a Relay Agent would be on a router in this subnet, in this case, the router named `r22-59` in Sun Ray Network Topology. For a brief introduction to this topic, refer to Sun Ray DTU Initialization Requirements Using DHCP.
   - If `r22-59` is running the Cisco IOS, the `ip helper-address` command can be used to activate its DHCP Relay Agent to relay DHCP broadcasts from its 10/100 Ethernet port number 4 to the Sun Ray server at `130.146.59.5`.

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

- If the external DHCP service also lacks a connection to this subnet, configure a DHCP Relay Agent to forward requests from the DTU to the following services:
    - The external DHCP service so that the DTU can obtain basic networking parameters
    - The DHCP service on the Sun Ray server so that the DTU can obtain additional parameters

      The Cisco IOS `ip helper-address` command accepts multiple relay destination addresses, so if, for example, the external DHCP service could be contacted at `130.146.59.2` on subnet B in Sun Ray Network Topology, the appropriate sequence would be:

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

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

3. Configure the Sun Ray server to provide additional parameters to the shared subnet.
   Use the `utadm -A` subnet command to configure DHCP service for DTUs on a shared subnet. In this example, the shared subnet has network number `130.146.22.0`, so the appropriate command is `utadm -A 130.146.22.0`.

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

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

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

4. Restart Sun Ray services on the Sun Ray server by issuing the `utrestart` command to fully activate Sun Ray services on

the shared subnet.

```
# /opt/SUNWut/sbin/utrestart
A warm restart has been initiated... messages will be logged to
/var/opt/SUNWut/log/messages.
```

Remote Shared Subnet: Example 2

In this example, deploying DTUs on subnet D in Sun Ray Network Topology, the answers to the three predeployment questions are as follows:

- From which DHCP server will DTUs on this subnet get their basic IP networking parameters?
  From an external DHCP service.
- From which DHCP server will DTUs on this subnet get additional configuration parameters to support features such as firmware download?
  The DTUs will not be supplied with the additional parameters required to support firmware download or to activate other advanced DTU features.
- How will DTUs on this subnet locate their Sun Ray server?
  The external DHCP service will supply a single additional parameter to inform the DTU of the location of a Sun Ray server.
  In this example, the Sun Ray server does not participate in DTU initialization at all. Configuration steps are still required on the Sun Ray server because it responds by default only to DTUs located on directly connected dedicated interconnects. It responds to DTUs on shared subnets only if the `utadm -L on` command has been executed. Running the `utadm -A subnet` command to activate DHCP on the Sun Ray server for a shared subnet, as in this example, implicitly executes `utadm -L on`. If `utadm -A subnet` has not been run, the administrator must run `utadm -L on` manually to enable the server to offer sessions to DTUs on the shared subnet.

1. Configure the external DHCP service.
   Determining how to configure the external DHCP infrastructure to provide basic networking parameters to the DTUs on this subnet is beyond the scope of this document. However, for this example, assume that DHCP service is provided by Cisco IOS-based router `r22-71` in Sun Ray Network Topology, attached to the `130.146.71.0` subnet through its 10/100 Ethernet port 3. This router can be configured to provide basic networking parameters and the location of a Sun Ray server as follows:

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

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

   DHCP option 49, the standard option of the X Window Display Manager, identifies `130.146.59.5` as the address of a Sun Ray server. In the absence of `AltAuth` and `Auth-Srvr` vendor-specific options, the DTU tries to find a Sun Ray server by broadcasting on the local subnet. If the broadcasts evoke no response, the DTU uses the address supplied in `t` option of the X Window Display Manager.

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

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

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

3. Restart Sun Ray services on the Sun Ray server by issuing the `utrestart` command to fully activate Sun Ray services on the shared subnet.

```
# /opt/SUNWut/sbin/utrestart
A warm restart has been initiated... messages will be logged to
/var/opt/SUNWut/log/messages.
```

The following table below lists the vendor-specific DHCP options that Sun Ray defines and uses.

Vendor-specific DHCP Options

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

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

- `AltAuth` and `AuthSrvr` indicate the IP addresses of Sun Ray servers. Addresses in the `AltAuth` list are tried in order until a connection is established. Current firmware ignores `AuthSrvr` if `AltAuth` is provided, but always specify `AuthSrvr` for the benefit of old (pre Sun Ray Server Software 1.3) firmware, which cannot handle the `AltAuth` option. If neither of these options is supplied, the DTU tries to locate a Sun Ray server by sending broadcasts on the local subnet. The DTU tries to contact a Sun Ray server at the address supplied in the option of the X Window Display Manager if that option has been provided.

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

> Note
> Because the message formats, contents, and thresholds are intended for use only by service personnel, they are not documented here.

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

Sun Ray Client Boot Process

This process flow shows how a Sun Ray client obtains its basic network parameters, firmware server, and Sun Ray server.

> Note
> The GUI firmware is required to locally configure the Sun Ray parameters using the Pop-up GUI. Locally configured parameter values override network values with the exception of MTU, which is always the minimum of the values seen.

Sun Ray Client Boot Process

1) Power unit on.

2) Read local configuration, if present.

a) netType = STATIC IP OR DHCP OR Auto-config (IPv6)
b) If netType is STATIC IP, use locally configured values for

- IP Address
- Net mask
- Broadcast address
- Router
- MTU

3) Bring up the network interface.

a) If any networking values missing, then perform DHCP.
b) If AuthSrvr value is not defined, then perform DHCP_INFORM request.
c) Merge any local values, DHCP vendor options, and DHCP_INFORM values (local values override DHCP except MTU, which is minimum of values seen).
d) If XDispMgr was given by DHCP AND no AltAuth vendor option was found, then set AltAuth to XDispMgr (option 49) values.

4) Read Configuration Parameter file (model.parms file) on firmware server.

4.1) Try the to find firmware servers that contain .parms file, in order:

a) Locally configured value
b) DHCP vendor option (FWSrvr)
c) Option 66 (TftpSrvr) IP Address or DNS name
d) DNS lookup of "sunray-config-servers" (if mapped to multiple addresses, choose one randomly)

4.2) Download the .parms file.

a) Search for SunRayPx.MAC.parms.
b) Search for SunRayPx.parms.

4.3) Parse the .parms file.

- parms.version = firmware version
- parms.revision = max supported hardware revision
- parms.barrier = barrier value of server firmware
- parms.BarrierLevel = barrier override value
- parms.servers = server list
- parms.select = inorder | random

4.4) If .parms file was successfully parsed OR firmware server was obtained by locally configured value , then go to Step 5.

> Note
> If a locally configured firmware server is unreachable or the correct configuration parameter file does not exist, the Sun Ray client will not attempt any of the other methods in Step 4.1 to locate configuration parameter files. This setup prevents the unintentional loading of a different firmware version than is provided by the locally designated firmware server.

4.5) If no .parms file found AND not at end of firmware server list, then go to Step 4.1 and pick next firmware server on the list.

4.6) If no firmware servers left to try, then set following values:

- parms.version = DHCP vendor option NewTVer (set to NULL string if none provided by DHCP)
- parms.BarrierLevel = DHCP BarrierLevel (set to current_barrier if none provided by DHCP)
- set parms.revision to current_revision
- set parms.barrier to current_barrier
- set parms.select = inorder

5) Determine if there is new firmware to load.

If:

- parms.version is not equal to the current firmware version
- AND parms.version is not equal to "NONE"
- AND parms.revision is >= to current hardware revision
- AND either parms.barrier is >= to parms.BarrierLevel or parms.barrier is >= current firmware's barrier level

Then:

a) Download firmware.
b) Write firmware to flash.
c) Reboot.

Else:

No firmware is loaded.

6) Determine a Sun Ray server to connect to.

6.1) If AlthAuth/AuthSrvr/parms.servers are all empty, then set server_list to "sunray-servers". Otherwise set server_list to parms.servers.

6.2) If untried server_list addresses are left, then:

a) Select a name either randomly or in order, according to parms.select.

b) Translate the name to a list of IP addresses (either DNS lookup, or IP address notation).

c) Select an IP address from the list, either randomly or inorder according to parms.select.

d) Set that broadcast address was seen.

e) Go to Step 6.8.

6.3) If there are untried AltAuth addresses, then:

a) Select one randomly or in order.

b) Set that broadcast address was seen.

c) Go to Step 6.8.

6.4) If AuthSrvr is defined, then:

a) Set address to try to AuthSrvr.

b) Go to Step 6.8.

6.5) If broadcast address was seen, then perform broadcast protocol.

6.6) If broadcast response received, then:

a) Set selected address to responder.

b) Go to Step 6.8.

6.7) Timeout in 30 seconds and reboot.

6.8) Try to connect to selected address.

6.9) If connection fails, then go to step 6.2.

7) Sun Ray is connected.

How to Set DTU Configuration Parameters (Pop-up GUI)

Sun Ray Server Software provides optional functionality, called the Pop-up Graphical User Interface (Pop-up GUI), which enables the entry of configuration parameters for a Sun Ray DTU from the attached keyboard. Most of these configuration parameters are stored in the DTU's flash memory. Certain control key combinations are used to invoke this new facility, which provides a tree of menus that can be navigated to set and examine configuration values.

Access Control

To accommodate customers with differing requirements with respect to flexibility and security, two versions of the DTU software are provided.

- The default version of Sun Ray DTU firmware is installed at `/opt/SUNWut/lib/firmware`. This firmware does not enable the Pop-up GUI.
- The Pop-up GUI-enabled version of the firmware is installed at `/opt/SUNWut/lib/firmware_gui`. To make the Pop-up GUI available, the administrator must run `utfwadm -f` to install the firmware.

Features and Usage

The Pop-up GUI enables several features that require the ability to set and store configuration information on the Sun Ray DTU itself, including:

- Non-DHCP network configuration for standalone operation, when configuring local DHCP operation is impossible
- Local configuration of Sun Ray specific parameters, such as server list, firmware server, MTU, and bandwidth limits
- DNS servers and domain name for DNS bootstrapping

- IPsec configuration
- Wireless network configuration, which is used in Tadpole laptops

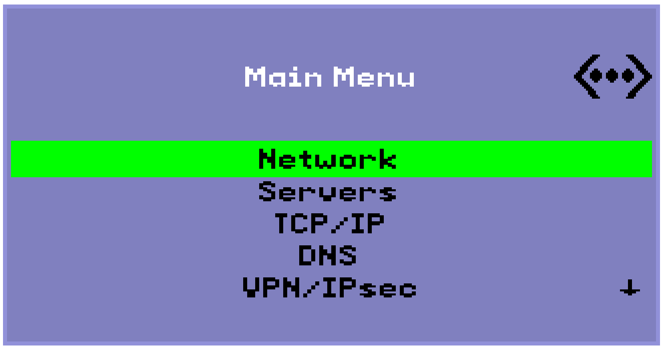
To protect the use of stored authentication information, the VPN configuration includes a PIN entry. This feature enables two-factor authentication for Sun Ray at Home VPN deployments.

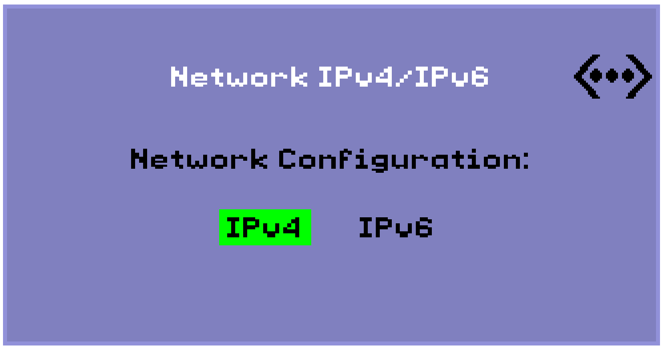
How to Start the DTU Pop-Up GUI

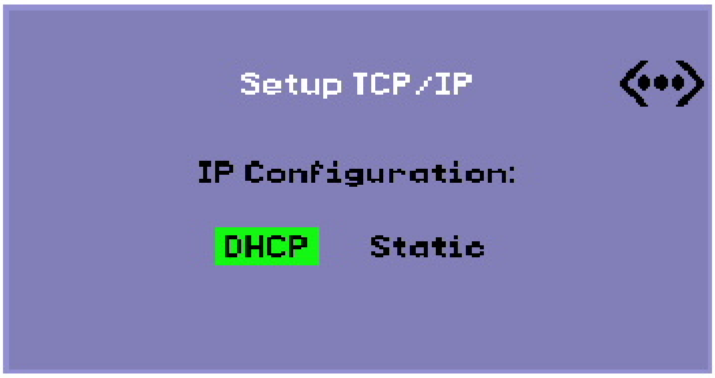
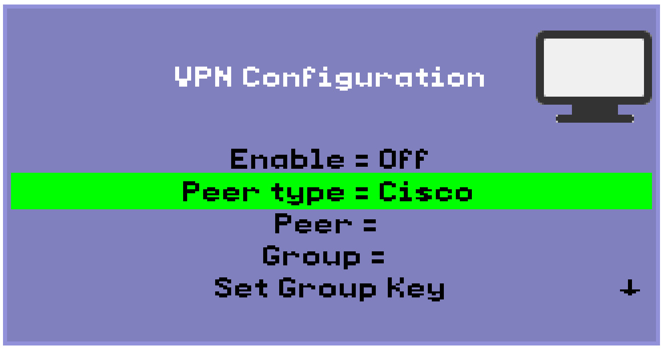
- If you are using a Sun keyboard, you can press one of the following key combinations:
  - `Stop+S`
  - `Stop+M`
- If you are using a non-Sun keyboard, you can press one of the following key combinations:
  - `Ctrl+Pause+S`
  - `Ctrl+Pause+M`

The arrow at the lower right corner indicates that the menu can be scrolled with the Up and Down arrow keys.

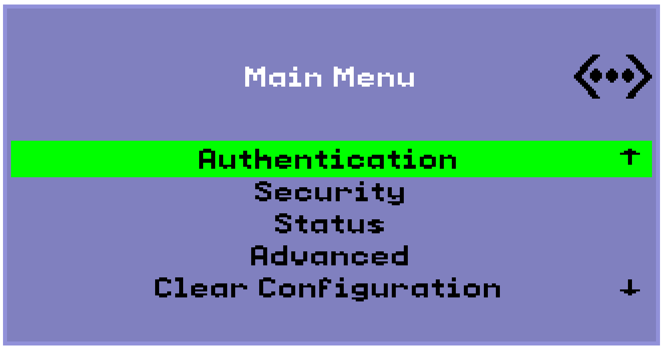
Pop-up GUI Main Menu (Part I)



Main Menu Item	Description
Network	
Servers	• Server list - A list of comma-separated server names or IP addresses • Firmware server - Name or IP address of firmware/config server • Log host - IP address of syslog host

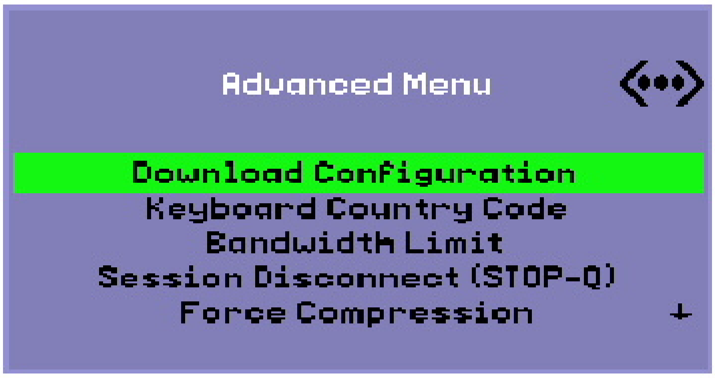
TCP/IP	 Setup TCP/IP IP Configuration: DHCP Static • DHCP - MTU • Static - IP address, netmask, router, broadcast address, MTU
DNS	• Domain name - One only • DNS server list - List of IP addresses
VPN/IPsec	 VPN Configuration Enable = Off Peer type = Cisco Peer = Group = Set Group Key Cisco EzVPN authentication model • Enable - On/Off • Peer type - Cisco or Netscreen (Juniper Networks) • Peer - Gateway peer (name or IP address) • Group - Group name • Set Group Key • Username - Xauth user name (if static) • Set Password - Xauth password (if static) • Set PIN - If the PIN has been set, the user is prompted for it before a locally stored Xauth user name and password are used. • Advanced • DH Group - Diffie-Hellman group • PFS Group • IKE Lifetime - IKE Phase 1 lifetime • IPsec Lifetime • Dead Peer Detection • Session timeout - Idle timeout, after which VPN connection is dropped

Pop-up GUI Main Menu (Part II)



Main Menu Item	Description
Authentication	For HTTP authentication - Enable/Disable switch - Port number
Security	Set password (lock configuration under password control)
Status	Version (equivalent to STOP-V)
Advanced	- Download Configuration - Keyboard Country Code - Bandwidth Limit (in bits per second) - Session Disconnect (STOP-Q) - Force Compression - Lossless Compression - Disallow `utload` - Force Full Duplex - Enable Fast Download - Video (set blanking timeout) - Video Input Disable
Clear Configuration	Equivalent to STOP-C.

Pop-up GUI Advanced Menu (Part I)

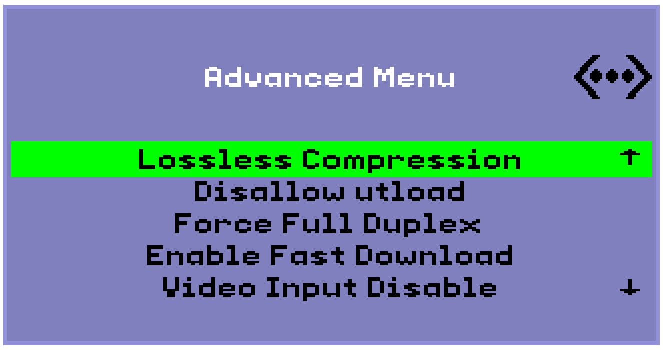


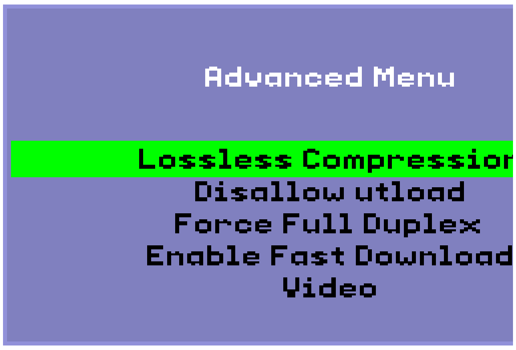
Main Menu Item	Description

Download Configuration	Prompts for a server name and file name of a file to be downloaded from the server, in the form server: filename. The default server is the TFTP server value if defined, and the default file name is `config.`MAC, where MAC is the unit's MAC address in upper-case hexadecimal. This field can be overwritten when selected. Pressing Return causes the corresponding file to be read and the configuration values parsed and set. For configuration values, see Pop-up GUI Menu Configuration Values. On success, the user is prompted to save the values. Otherwise, the previous menu is displayed. No other error indications are given. Some of the menus have an `Exit` entry, but the Escape key always invokes one level higher than the current menu. Escape at the top level prompts for any changes to be saved or discarded. If changes have been written to the flash memory, the Escape key resets the DTU.
Keyboard Country Code	A keyboard country code (keyboard map) that is applied to a keyboard that returns a country code of 0, for use with non-U.S. USB keyboards that do not report a country code. Here are the valid keyboard country code values: • 1 Arabic • 2 Belgian • 3 Canada_Bi • 4 French-Canadian • 5 Czech • 6 Denmark • 7 Finnish • 8 France • 9 Germany • 10 Greek • 12 Hungarian • 14 Italy • 15 Japan • 16 Korea • 17 Latin-American • 18 Netherland • 19 Norway • 21 Polish • 22 Portugal • 23 Russia • 24 Slovakian • 25 Spain • 26 Sweden • 27 Switzerland • 28 Switzerland_Ge • 30 Taiwan • 31 TurkeyQ • 32 UK-English • 33 US-English • 35 TurkeyF
Bandwidth Limit	The maximum amount of network bandwidth in bits per second that a given client will use.
Session Disconnect	Enables or disables the ability to terminate a session by pressing STOP-Q. This feature is useful when you want to terminate a VPN connection and leave the Sun Ray in an inactive state. Pressing the Escape key after the session has terminated reboots the Sun Ray DTU.
Force Compression	Sets a tag sent from the Sun Ray DTU to the Xserver telling it to enable compression regardless of available bandwidth.

Pop-up GUI Advanced Menu (Part II)

Sun Ray 270 (Video Input Disable) | Sun Ray 2, 2FS, 270, and later models





Main Menu Item	Description
Lossless Compression	Disables the use of lossy compression for image data.
Disallow utload	Disables the ability to explicitly force a firmware load into a DTU. In this way, firmware can be tightly controlled using `.parms` files or DHCP parameters.
Force Full Duplex	Allows the DTU to operate correctly when the network port that it is connected to does not auto-negotiate. In that case, the auto-negotiation results in the Sun Ray running at half duplex, which significantly impacts network performance. This setting allows the Sun Ray to operate with better performance in this situation.
Enable Fast Download	If set, the DTU uses the maximum TFTP transfer size if the TFTP server supports it. Over a high latency connection, this setting typically doubles the speed of firmware downloads. There are no disadvantages to enabling fast downloads on low latency LANs. This parameter is disabled by default and the transfer size is set at 512-byte packets. It is disabled by default for backwards compatibility with TFTP servers that might not support the more advanced protocol. If this parameter were on by default and a firmware download were to fail, there would be no way to recover.
Video	• Blanking Timeout - The time until the screen is put to sleep, in minutes. (specify zero to disable). • OSD Quiet Display - If set, disables most of the OSD icons except when error conditions are detected.
Video Input Disable	Sun Ray 270 only. If set, turns off the input selector on the front of a Sun Ray 270 and locks the monitor so that it displays only the Sun Ray output. This feature prevents users from connecting a PC to the VGA video input connector on a Sun Ray 270 and using it as a monitor.

How to Load DTU Configuration Data Remotely

To help avoid error-prone manual entry of configuration data for deployments where preconfiguration is required, you can use the Pop-up GUI to download a configuration to a Sun Ray DTU from a file on a server via TFTP, as indicated in Pop-up GUI Advanced Menu (Part I).

The following keywords correspond to configuration values that can be set from the Pop-up GUI menus. To group items that are logically related, some of the keywords take the form family.field.

Pop-up GUI Menu Configuration Values

VPN/IPsec Submenu	Comment
vpn.enabled	Enable toggle
vpn.peer	Remote gateway name/IP address
vpn.group	VPN group
vpn.key	VPN key
vpn.user	Xauth user

vpn.passwd	Xauth password
vpn.pin	PIN lock for use of user/passwd
vpn.dhgroup	Diffie-Hellman group to use
vpn.lifetime	Lifetime of IKE connection
vpn.killtime	Idle timeout value to drop VPN connection.
DNS Submenu	
dns.domain	Domain name
dns.servers	Server list (comma-separated IP addresses)
Servers Submenu	
servers	Sun Ray server
tftpserver	TFTP server
loghost	Syslog host
Security Submenu	
password	Set administrator password
TCP/IP Submenu	
ip.ip	Static IP
ip.mask	Static netmask
ip.bcast	Static broadcast address
ip.router	Static router
ip.mtu	MTU
ip.type	Type of network ("DHCP" | "Static")
Advanced Submenu	
kbcountry	Keyboard country code
bandwidth	Bandwidth limit in bits per second.
stopqon	Enable (1) or Disable (0) STOP-Q for disconnect
compress	Force compression on when 1
lossless	Force use of lossless compression when 1
utloadoff	Disallow use of utload to force firmware download when 1
fastload	Force maximum TFTP transfer rate when 1.
videoindisable	Disable input selector of Sun Ray 270 when 1.

The format of the file is a set of key=value lines, each terminated by a newline character, which are parsed and the corresponding configuration items set (see the sample file below). No whitespace is permitted. Key values are case-sensitive and should be always lower case, as listed above. Setting a keyword to have a null value results in the configuration value being cleared in the local configuration.

Sample VPN Configuration File

```
vpn.enabled=1
vpn.peer=vpn-gateway.sun.com
vpn.group=homesunray
vpn.key=abcabcabc
vpn.user=johndoe
vpn.passwd=xyzxyzxyxzy
dns.domain=sun.com
tftpserver=config-server.sun.com
servers=sunray3,sunray4,sunray2
```

Configuring Interfaces on the Sun Ray Interconnect Fabric

Use the `utadm` command to manage the Sun Ray interconnect fabric. Note the following infomration:

- If the IP addresses and DHCP configuration data are not set up properly when the interfaces are configured, then the failover feature will not work as expected. In particular, configuring the Sun Ray server's interconnect IP address as a duplicate of any other server's interconnect IP address may cause the Sun Ray Authentication Manager to generate "Out of Memory" errors.
- If you make manual changes to your DHCP configuration, you will have to make them again whenever you run `utadm` or `utfwadm`.
- If you press `CTRL-C` while performing utadm configuration, `utadm` might not function correctly the next time it is invoked. To correct this condition, type `dhtadm -R`.

How to Configure a Private Sun Ray Network

- To add an interface, type:

```
# utadm -a <interface_name>
```

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

> Note
> If you choose to specify your own subnet, make sure the address is not already in use.

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

Any valid Solaris network interface can be used. For example:

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

How to Configure a Second Private Sun Ray Network

- To add another interface, use the `utadm` command.

```
# utadm -a <hme1>
```

How to Delete an Interface

```
# utadm -d <interface_name>
```

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

How to Print the Sun Ray Private Interconnect Configuration

```
# utadm -p
```

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

> Note
> Sun Ray servers require static IP addresses; therefore, they cannot be DHCP clients.

How to Add a LAN Subnet

```
# utadm -A <subnet_number>
```

How to Delete a LAN Subnet

```
# utadm -D <subnet_number>
```

How to List the Current Network Configuration

```
# utadm -l
```

`utadm -l` lists all the currently configured networks.

How to Remove All Interfaces and Subnets

Use the `utadm -r` command to remove all entries and structures relating to Sun Ray interfaces and subnets.

```
# utadm -r
```

Contents

Configuring SRSS on Solaris Trusted Extensions (All Topics)

Task Map: Configuring SRSS on Solaris Trusted Extensions

For the latest Solaris Trusted Extensions information, see http://docs.sun.com/app/docs/coll/175.9?l=en.

Perform the following procedures as root from ADMIN_LOW (global zone).

Step	Details
1. Configure a Dedicated Sun Ray Interconnect for Trusted Extensions.	How to Configure a Dedicated Sun Ray Interconnect for Trusted Extensions
2. Configure shared multilevel ports (MLP) for Sun Ray Services.	How to Configure Shared Multilevel Ports (MLP) for Sun Ray Services
3. Increase the number of X server ports.	How to Increase the Number of X Server Ports
4. Reboot the Sun Ray server.	How to Reboot a Sun Ray Server

How to Configure a Dedicated Sun Ray Interconnect for Trusted Extensions

Use the Solaris Management Console (SMC) Security Templates to assign the `cipso` template to the Sun Ray server. Assign all other Sun Ray devices on the network an `admin_low` label. The `admin_low` template is assigned to the range of IP addresses you are planning to use in the `utadm` command.

The `/etc/security/tsol/tnrhdb` file should contain the following entries when you finish:

```
192.168.128.1:cipso
192.168.128.0:admin_low
```

1. Start the Solaris Management Console (SMC).

```
# smc &
```

2. Make the following selections:
   a. In the SMC, select Management Tools->Select hostname:Scope=Files, Policy=TSOL.
   b. Select System Configuration->Computers and Networks->Security Templates->cipso.
   c. From the menu bar, choose Action->Properties->Hosts Assigned to Template.
   d. Select Host and type the IP Address of the Sun Ray interconnect
   (for example, 192.168.128.1).
   e. Click Add and then OK.
   f. Select System Configuration->Computers and Networks->Security Families->admin_low.
   g. From the menu bar, choose Action->Properties->Hosts Assigned to Template.
   h. Select Wildcard.
   i. Type the IP Address of the Sun Ray Interconnect Network (192.168.128.0).
   j. Click Add and then OK.
3. Assign all Sun Ray servers in the failover group a `cipso` label.
   a. Select System Configuration->Computers and Networks->Security Families->cipso.
   b. From the menu bar, choose Action->Properties->Hosts Assigned to Template.
   c. Select Host and type the IP Address of the other Sun Ray server.
   d. Click Add and then OK.

How to Configure Shared Multilevel Ports (MLP) for Sun Ray Services

A shared multilevel port has to be added to the global zone for Sun Ray services in order to have access from a labeled zone.

1. Start the Solaris Management Console (SMC).

```

# smc &
```

2. Go to Management Tools.
3. Select hostname:Scope=Files, Policy=TSOL.
4. Select System Configuration->Computers and Networks->Trusted Network Zones->global.
5. From the menu bar, choose Action->Properties.

6. Click Add under Multilevel Ports for Shared IP Addresses.
7. Add 7007 as Port Number, select TCP as Protocol, and click OK.
8. Repeat the previous step for ports 7010 and 7015.
9. Restart network services by running the following command:

```
# svcadm restart svc:/network/tnctl
```

10. Verify that these ports are listed as shared ports by running the following command:

```
 # /usr/sbin/tninfo -m global
```

How to Increase the Number of X Server Ports

The default entry in `/etc/security/tsol/tnzonecfg` makes three displays available (6001-6003). Increase the number of available X server ports per requirements.

1. Start the Solaris Management Console (SMC).

```
# smc &
```

2. Go to Management Tools.
3. Select hostname:Scope=Files, Policy=TSOL option.
4. Select System Configuration->Computers and Networks->Trusted Network Zones->global.
5. From the menu bar, choose Action->Properties.
6. Under Multilevel Ports for Zone's IP Addresses, select 6000-6003/tcp.
7. Click Remove.
8. Choose Add->Enable Specify A Port Range.
9. Type `6000` in Begin Port Range Number and `6050` (for 50 displays) in End Port Range Number.
10. Select TCP as the Protocol.
11. Click OK.

How to Reboot a Sun Ray Server

If you perform a configuration procedure on a Sun Ray server, you must reboot the Sun Ray server to have the change take effect.

1. If you have not already done so, log in as the superuser of the Sun Ray server.
2. Reboot the Sun Ray server.

```
# /usr/sbin/reboot
```

Glossary

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

If you would like to add a term to the list, use the Add Comment link at the bottom of the page to contact us.

A

Term	Description

AAC	Advanced Audio Coding, a "lossy" compression format capable of delivering relatively high quality at relatively low bit rates.
AH	Authentication headers, used as part of an IPSec implementation.
alias token	An alias token enables a card owner to access the same Sun Ray session with more than one physical token. This setup can be useful, for example, when a user needs a duplicate smart card.
ALP	The Sun Appliance Link Protocol, a suite of network protocols that enable communication between Sun Ray servers and DTUs.
AMGH	Automatic Multigroup Hotdesking. See regional hotdesking.
authentication policy	The Authentication Manager, using the selected authentication modules, decides what tokens are valid and which users, as token owners, have access to the system and sessions.
authentication token	Although all tokens are used by the Authentication Manager to grant or deny access to Sun Ray sessions, this term usually refers to a user's smart card token. See token.

B

Term	Description
backplane bandwidth	Sometimes also referred to as switch fabric. A switch's backplane is the pipe through which data flows from an input port to an output port. Backplane bandwidth usually refers to the aggregate bandwidth available amongst all ports within a switch.
barrier mechanism	To prevent clients from downloading firmware that is older than the firmware they already have, the administrator can set a barrier mechanism. The barrier mechanism symbol BarrierLevel is defined by default in the DHCP table of Sun Ray servers running version 2.0 or later of Sun Ray Server Software.
bpp	Bits per pixel.

C

Term	Description
CABAC	Context-adaptive binary arithmetic coding, a "lossless" entropy coding technique used in H.264/MPEG-4 AVC video encoding.
CAM	Controlled Access Mode, also known as Kiosk Mode.
card reader	See token reader.
category 5	The most common type of wiring used in LANs. It is approved for both voice and data (at up to 100 Mhz). Also called cat 5.
client	See Sun Ray client.
client key	An automatically generated public-private key pair that represents a Sun Ray DTU or a Sun Data Access Client. A client key is used to authenticate the device when it connects to a server.
client-server	A common way to describe network services and the user processes (programs) of those services.
codec	A device or program capable of encoding or decoding a digital data stream or signal.
cold restart	Pressing the Cold Restart button terminates all sessions on a given server before restarting Sun Ray services. See restart.
cut-through switches	The switch begins forwarding the incoming frame onto the outbound port as soon as it reads the MAC address while continuing to receive the remainder of the frame.

D

Term	Description
DHCP	Dynamic Host Configuration Protocol, which is a means of distributing IP addresses and initial parameters to the DTUs.
domain	A set of one or more system boards that acts as a separate system capable of booting the OS and running independently of any other board.
DTU	See Sun Ray DTU.

E

Term	Description
ESP	Encapsulating Security Payloads, used as part of IPSec.
Ethernet	Physical and link-level communications mechanism defined by the IEEE 802.3 family of standards.
Ethernet address	The unique hardware address assigned to a computer system or interface board when it is manufactured. See MAC address.
Ethernet switch	A unit that redirects packets from input ports to output ports. It can be a component of the Sun Ray interconnect fabric.

F

Term	Description
failover	The process of transferring processes from a failed server to a functional server.
failover group	Two or more Sun Ray servers configured to provide continuity of service in the event of a network or system failure. Sometimes abbreviated as FOG or HA (for high availability). The term high availability refers to the benefit of this type of configuration; the term failover group refers to the functionality.
filling station	When a DTU's firmware is downgraded to an earlier version because it connects to a server running the earlier version, the DTU needs to be connected to a filling station so that it can download newer firmware. For this purpose, a filling station can be any private network configured for Sun Ray services or any shared network in which the Sun Ray DHCP server is the only DHCP server.
firmware barrier	See barrier mechanism.
FOG	See failover group.
fps	Frames per second.
frame buffer	Video output device that drives the video display. See virtual frame buffer.

G

Term	Description
GEM	Gigabit Ethernet.
group-wide	Across a failover group.

H

Term	Description

H.264	A standard for video compression developed by MPEG and VCEG for a wide range of bit rates and resolutions. Also known as MPEG-4 AVC (Advanced Video Coding) and MPEG-4 Part 10.
HA	High availability. Sun Ray HA groups have traditionally been called failover groups.
head	Colloquial term for a screen, or display, or monitor, especially in a context where more than one is used in conjunction with the same keyboard and mouse, as in "multihead" feature.
high availability	See failover. The term high availability refers to a benefit of this type of configuration; the term failover group refers to the functionality.
hotdesking	The ability for a user to remove a smart card, insert it into any other DTU within a failover group, and have the user's session "follow" the user, thus allowing the user to have instantaneous access to the user's windowing environment and current applications from multiple DTUs.
hot key	A predefined key that causes an activity to occur. For example, a hot key is used to display the Settings screen on the Sun Ray DTU.
hot-pluggable	A property of a hardware component that can be inserted into or removed from a system that is powered on. USB devices connected to Sun Ray DTUs are hot-pluggable.

I

Term	Description
idle session	A session that is running on a Sun Ray server but to which no user (identified by a smart card token or a pseudo-token) is logged in.
IKE	Internet Key Exchange, a component of IPSec.
interconnect fabric	All the cabling and switches that connect a Sun Ray server's network interface cards to the Sun Ray DTUs.
internet	A collection of networks interconnected by a set of routers that enable them to function as a single, large virtual network.
intranet	Any network that provides similar services within an organization to those provided by the Internet but which is not necessarily connected to the Internet.
IP address	A unique number that identifies each host or other hardware system on a network. An IP address is composed of four integers separated by periods. Each decimal integer must be in the range 0-255, for example, 129.144.0.0.
IP address lease	The assignment of an IP address to a computer system for a specified length of time, rather than permanently. IP address leasing is managed by the Dynamic Host Configuration Protocol (DHCP). The IP addresses of Sun Ray DTUs are leased.
IPSec	The Internet Protocol (Security) set of protocols seeks to secure IP communications by encoding data packets through authentication headers (AH) and encapsulating security payloads (ESP) and by providing a key exchange mechanism (IKE).

K

Term	Description
key	A random sequence of bits that is used with cryptographic algorithms for authentication or encryption.
keyboard country code	A number representing a specific USB keyboard map that can be set in the Sun Ray client firmware to provide better Non-US keyboard support. This code is used if the keyboard returns a country code of 0.
key fingerprint	A user-viewable hexadecimal string representing a public key, which is generated by an MD5 hash based on the public key data.

key pair	A pair of related keys used for authentication. Also known as a public-private key pair. The 'private key' is only known by the owner. The 'public key' is published and distributed. It is used to authenticate the owner of the private key.
Kiosk Mode	A facility to run sessions without a UNIX login under an anonymous user account. Kiosk sessions provide a preconfigured, usually restricted, software environment. Kiosk sessions are configured through a Kiosk session type. The term Kiosk Mode was used interchangeably with CAM in earlier versions of SRSS.
Kiosk session	A user session running in Kiosk Mode. Also called Kiosk Mode session.
Kiosk session type	A set of scripts and configuration files, which are described by a Kiosk session descriptor file. A Kiosk session type defines the kind of user session that will run in Kiosk Mode. A session type is sometimes referred to as a session configuration.

L

Term	Description
LAN	Local Area Network. A group of computer systems in close proximity that can communicate with one another through some connecting hardware and software.
layer 2	The data link layer. The OSI (Open Standards Interconnection) model has a total of seven layers. Layer 2 is concerned with procedures and protocols for operating the communication lines between networks as well as clients and servers. Layer 2 also has the ability to detect and correct message errors.
local host	The CPU or computer on which a software application is running.
local server	From the DTU's perspective, the most immediate server in the LAN.

M

Term	Description
MAC address	Media Access Control. A MAC address is a 48-bit number programmed into each local area network interface card (NIC) at the time of manufacture. LAN packets contain destination and source MAC names and can be used by bridges to filter, process, and forward packets. 8:0:20:9e:51:cf is an example of a MAC address. See also Ethernet address
managed object	An object monitored by the Sun Management Center software.
mobile token	If mobile sessions are enabled, a user can log into an existing session from different locations without a smart card, in which case the user name is associated with the session. This type of pseudo-token is called a mobile token.
mobility	For the purposes of the Sun Ray Server Software, the property of a session that allows it to follow a user from one DTU to another within a server group. On the Sun Ray system, mobility requires the use of a smart card or other identifying mechanism.
modules	Authentication modules are used to implement various site-selectable authentication policies.
MPPC	Microsoft Point-to-Point Compression protocol.
MTU	Maximum Transmission Unit, used to specify the number of bytes in the largest packet a network can transmit.
multicasting	The process of enabling communication between Sun Ray servers over their Sun Ray network interfaces in a failover environment.
multihead	See head.
multiplexing	The process of transmitting multiple channels across one communications circuit.

N

Term	Description
namespace	A set of names in which a specified ID must be unique.
NAT	See network address translation.
network	Technically, the hardware connecting various computer systems enabling them to communicate. Informally, the systems so connected.
network address	The IP address used to specify a network.
network address translation	NAT. Network address translation typically involves the mapping of port numbers to allow multiple machines (Sun Ray DTUs in this case, but not Sun Ray servers) to share a single IP address.
network interface	An access point to a computer system on a network. Each interface is associated with a physical device. However, a physical device can have multiple network interfaces.
network interface card	NIC. The hardware that links a workstation or server to a network device.
network latency	The time delay associated with moving information through a network. Interactive applications such as voice, video displays and multimedia applications are sensitive to these delays.
network mask	A number used by software to separate the local subnet address from the rest of a given Internet protocol address. An example of a network mask for a class C network is 255.255.255.0.
network protocol stack	A network suite of protocols organized in a hierarchy of layers called a stack. TCP/IP is an example of a Sun Ray protocol stack.
NIC	Network interface card.
non-smart card mobility	A mobile session on a Sun Ray DTU that does not rely on a smart card. NSCM requires a policy that allows pseudo-tokens.
NSCM	See non-smart card mobility.

O

Term	Description
OSD	On-screen display. The Sun Ray DTU uses OSD icons to alert the user about potential start-up or connectivity problems.

P

Term	Description
PAM	Pluggable Authentication Module. A set of dynamically loadable objects that gives system administrators the flexibility of choosing among available user authentication services.
PAM session	A single PAM handle and runtime state associated with all PAM items, data, and the like.
patch	A collection of files and directories that replaces or updates existing files and directories that prevent proper execution of the software on a computer system. The patch software is derived from a specified package format and can only be installed if the package it fixes is already present.
PCM	Pulse Code Modulation.
policy	See authentication policy.
Pop-up GUI	A mechanism that allows the entry of configuration parameters for a Sun Ray DTU from the attached keyboard.

port	(1) A location for passing data in and out of a computer system. (2) The abstraction used by Internet transport protocols to distinguish among multiple simultaneous connections to a single destination host.
POST	Power-on self test.
power cycling	Using the power cord to restart a DTU.
pseudo-session	A Sun Ray session associated with a pseudo-token rather than a smart card token.
pseudo-token	A user accessing a Sun Ray session without a smart card is identified by the DTU's built-in type and MAC address, known as a pseudo-token. See token.

R

Term	Description
RDP	Microsoft Remote Desktop Protocol.
regional hotdesking	This SRSS feature enables users to access their sessions across wider domains and greater physical distances than was possible in earlier versions of SRSS. Administrators enable this feature by defining how user sessions are mapped to an expanded list of servers in multiple failover groups. Originally known as Automatic Multigroup Hotdesking (AMGH).
restart	Sun Ray services can be restarted either from the `utrestart` command or with the Warm Restart or Cold Restart buttons through the GUI. A cold restart terminates all Sun Ray sessions; a warm restart does not.
RHA	Remote Hotdesk Authentication, a security enhancement that requires SRSS authentication before users can reconnect to an existing session. RHA does not apply to Kiosk sessions, which are designed for anonymous access without authentication. RHA policy can be administered either through a GUI option or with the `utpolicy` command.

S

screen flipping	The ability to pan to individual screens that were originally created by a multihead group on a DTU with a single head.
server	A computer system that supplies computing services or resources to one or more clients.
service	For the purposes of the Sun Ray Server Software, any application that can directly connect to the Sun Ray DTU. It can include audio, video, X servers, access to other machines, and device control of the DTU.
session	A group of services associated with an authentication token. A session may be associated with a token embedded on a smart card. See token.
session mobility	The ability for a session to "follow" a user's login ID or a token embedded on a smart card.
smart card	Generically, a plastic card containing a microprocessor capable of making calculations. Smart cards that can be used to initiate or connect to Sun Ray sessions contain identifiers such as the card type and ID. Smart card tokens may also be registered in the Sun Ray Data Store, either by the Sun Ray administrator or, if the administrator chooses, by the user.
smart card-based authentication	Using a smart card to authenticate a card holder based on credentials supplied by the card and authentication information from the card holder, such as a PIN or biometric data. Requires Solaris middleware.
smart card-based session mobility	Using a smart card to provide a unique token ID and token type that enables SRSS to locate the card holder's session. In some cases, card holders might be required to authenticate themselves using smart card-based authentication.
smart card token	An authentication token contained on a smart card. See token.
SNMP	Simple Network Management Protocol
spanning tree	The spanning tree protocol is an intelligent algorithm that enables 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.
Sun Desktop Access Client	A software application that runs on common client operating systems and provides the ability to connect to a desktop session running on a Sun Ray server. Users can switch between their Sun Ray DTU and any supported Desktop Access Client enabled PC without using smart cards.
Sun Ray client	A hardware or software-based client that obtains a desktop session from a Sun Ray server. Currently, there are two types of clients: Sun Ray DTU and Sun Desktop Access Client.
Sun Ray DTU	Sun Ray desktop units were originally known as Desktop Terminal Units, hence the acronym. They are also referred to as Sun Ray thin clients, Sun Ray ultra-thin clients, and Sun Ray virtual display terminals.
system	The Sun Ray system consists of Sun Ray DTUs, servers, server software, and the physical networks that connect them.

T

thin client	Thin clients remotely access some resources of a computer server such as compute power and large memory capacity. The Sun Ray DTUs rely on the server for all computing power and storage.
tick	The time interval since a specified network event. Early versions of SRSS defined a tick as 1/50th of a second. It is now defined as 1/100th of a second, which is the usual SNMP convention.
timeout value	The maximum allowed time interval between communications from a DTU to the Authentication Manager.
token	The Sun Ray system requires each user to present a token that the Authentication Manager uses to allow or deny access to the system and to sessions. A token consists of a type and an ID. If the user uses a smart card, the smart card's type and ID are used as the token. If the user is not using a smart card, the DTU's built-in type and ID (the unit's Ethernet, or MAC, address) are used instead as a pseudo-token. If mobile sessions are enabled, a user can log into an existing session from different locations without a smart card, in which case the user name is associated with the session. A pseudo-token used for mobile sessions is called a mobile token. Alias tokens can also be created to enable users to access the same session with more than one physical token.
token reader	A Sun Ray DTU that is dedicated to reading smart cards and returning their identifiers, which can be associated with card owners (that is, with users).
trusted server	Servers in the same failover group that "trust" one another through a common group signature.

U

USB	Universal Serial Bus.
user session	A session that is running on a Sun Ray server and to which a user, identified by a smart card token or a pseudo toke, is logged in.

V

VC-1	Informal name of the SMPTE 421M video codec standard, now a supported standard for Blu-ray discs and Windows Media Video 9.
virtual desktop	A virtual machine containing a desktop instance that is executed and managed within the virtual desktop infrastructure, usually a Windows XP or Vista desktop accessed through RDP.
virtual frame buffer	A region of memory on the Sun Ray server that contains the current state of a user's display.
VLAN	Virtual Local Area Network.

VPN	Virtual Private Network.

W

Term	Description
WAN	Wide Area Network.
warm restart	See restart.
WMA	Windows Media Audio data compression file format and codec developed by Microsoft.
work group	A collection of associated users who exist in near proximity to one another. A set of Sun Ray DTUs that are connected to a Sun Ray server provides computing services to a work group.

X

Term	Description
Xnewt	The new default X server for Sun Ray Server Software 4.1 and later on Solaris.
X server	A process that controls a bitmap display device in an X Window System. It performs operations on request from client applications. Sun Ray Server Software contains two X servers: Xsun, which was the default Xserver in previous versions of SRSS, and Xnewt, which is the default Xserver for SRSS 4.1 and later. Xnewt enables the latest multimedia capabilities.

Y

Term	Description
YUV	Simple, lossless mechanism to store images or a sequence of images.

owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.