Server Grouping for the Sun Ray™ 1 Enterprise Appliance

Technical White Paper

Sun Proprietary: Internal Use Only

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

Please
Recycle

Contents

Introduction 1

The Sun Ray™ enterprise system is Sun Microsystems Inc.'s newest solution for the low-cost enterprise desktop. Based on a fundamentally new architecture that Sun calls the *Sun Ray Hot Desk architecture*, the Sun Ray enterprise system provides a very low cost, zero-administration desktop appliance for the enterprise workgroup environments. Sun's Hot Desk technology and the Sun Ray 1 enterprise appliance are compelling in their ability to deliver responsive, high performance computing to end users while providing the economic benefits of shared computing resources and centralized administration.

The Sun Ray enterprise system leverages the shared resources and the inherent reliability, availability, and scalability of Sun™ servers to deliver server-class computing performance to the desktop with economics unmatched by general-purpose computing platforms. However, even the most reliable servers can become inaccessible to users on occasion, due to planned or unplanned events. This document describes new features in the second release of the Sun Ray enterprise server software that enable multiple servers to share user session management tasks, and to provide user authentication failover if a server becomes unavailable.

Sun Ray Hot Desk Architecture

The Sun Ray Hot Desk architecture is a computing model, initially targeted at the workgroup, where all user state is centralized on a server and linked, by a dedicated interconnect, to a simple zero administration appliance on the desktop.

Today’s Sun Ray Hot Desk architecture implementation is composed of:

- The Sun Ray 1 enterprise appliance
- The Sun Ray enterprise server software
- Hot Desk technology

This model delivers a wide array of computational services to a local community of users, through a new partitioning of system functionality. The Hot Desk architecture enables use of a true, low-cost appliance on the desktop. At the same time it delivers the full power and performance of a server to the desktop, through centralization and the sharing of resources.

The Sun Ray Hot Desk architecture retains many of the desirable features of previous approaches without their drawbacks. It significantly reduces acquisition costs, administration, and desktop maintenance compared to thin-client computing, but without the resource limitations -- all services and resources reside centrally on one or more servers, so functionality is not limited by capacity on the desktop. It also provides the centralization, control, and sharing of resources that characterizes mainframe computing, while providing users a level of performance and access to applications and resources that go far beyond what most other desktop systems can provide.

The Sun Ray Hot Desk technology underlies the Sun Ray Hot Desk architecture. “Hot Desk” or “hot desking” refers to the ability of the user to access their sessions instantly from any Hot Desk enabled appliance in the workgroup. “Hot desking” is enabled by the “Sun Ray Hot Desk technology.”

The key elements of the Sun Ray Hot Desk technology are:

- A fast and efficient interface used to communicate between the Sun Ray enterprise server and any Sun Ray 1 enterprise appliance
- Smart card technology
- Server software which instantly maps users’ sessions to appliances

The initial release of the Sun Ray enterprise system supported only Sun Ray 1 enterprise appliances in a workgroup configuration, defined as a set of Sun Ray 1 enterprise appliances connected to a single Sun Ray enterprise server. With the Sun Ray 1 enterprise appliance’s unique smart-card interface, users can access their user environment from any Sun Ray 1 enterprise appliance within the workgroup. If a Sun Ray 1 enterprise appliance failure occurs, a replacement can simply be plugged in, or the user can move to another Sun Ray 1 enterprise appliance and continue working with no loss of data.

However, in the initial(1.0) software release, the Sun Ray enterprise server represents a potential single point of failure. Although Sun servers are inherently highly reliable and available, if the Sun Ray server becomes unavailable for any reason, all connected Sun Ray 1 appliance users lose access to their sessions.

To mitigate this possibility, and to enable the construction of larger Sun Ray workgroups, the second release of the Sun Ray enterprise server software provides support for multiple Sun Ray enterprise servers to manage a set of connected Sun Ray 1 enterprise appliances. This set of servers can be configured as a “failover group” that provides for automatic user re-authentication on another Sun Ray server if one server in the failover group becomes unavailable. The enhanced software capability also provides static load distribution, so that whenever a new user session is initiated, the session can be placed on any one of the servers in the group based on the availability of server resources.

Sun Ray™ Enterprise Server Software Failover and Load Distribution Features 2

In the initial release of the Sun Ray™ enterprise system, the Sun Ray enterprise server could represent a single point of failure; if the server became unavailable for any reason, all attached Sun Ray 1 enterprise appliances users would lose access to their sessions. Because there is no local state on the Sun Ray 1 enterprise appliance, these users could not do any work at all until server access is restored.

The new features in the Sun Ray enterprise server software, version 1.1, enable multiple Sun Ray enterprise servers to function as a failover group. A static load distribution feature allows new sessions to be initiated on any one of the servers in the group, based on server capacity and resource availability. This allows more effective usage and sharing of server resources. In addition, if one server fails, all users currently running sessions on that server will automatically be re-authenticated on one of the other servers in the group, and a new session can be started for each user.

This section discusses the new Sun Ray enterprise server software features for user authentication failover and load distribution. It also provides a very brief overview of the Sun Ray 1 enterprise appliance, the interconnect fabric, and the Sun Ray enterprise server. For a more detailed discussion of these elements of the Sun Ray enterprise system, refer to the *Sun Ray 1 Enterprise Appliance Overview and Technical Brief*, and the white paper *Deploying the Sun Ray Hot Desk Architecture*.

Sun Ray 1 Enterprise System

The components in the Sun Ray enterprise system are:

- Sun Ray 1 enterprise appliances
- One or more SPARC™ servers running the Solaris™ 2.6 or Solaris 7 Operating Environment.
- The Sun Ray enterprise server software, which provides user authentication, user session management, static load distribution and failover group management;
- A dedicated interconnect between one or more Sun Ray enterprise servers and the Sun Ray 1 enterprise appliance

Sun Ray 1 Enterprise Appliance

The Sun Ray 1 enterprise appliance is a stateless, zero administration "plug-and-work" device that is centrally managed by, and draws its computing resources from, a server running the Sun Ray enterprise server software. With no operating system or client software on the desktop appliance, application client processes and other services run unchanged on the server. Input and output between the user and the server is carried over a simple, high-speed, dedicated interconnect, to the attached Sun Ray 1 enterprise appliance.

The Sun Ray enterprise server appliance does contain a small amount of code in firmware that manages the client side of the authentication process as well as managing the distribution of input and output to and from the proper physical I/O hardware (monitor, keyboard, audio etc.).

Sun Ray Enterprise Server Software

The Sun Ray enterprise server software runs on a Sun server, and hosts the user sessions run by Sun Ray 1 enterprise appliance users.

The main components of the Sun Ray enterprise server software are:

- Authentication Manager — Recognizes and validates Sun Ray 1 enterprise appliance users
- Group Manager — Keeps track of failover group membership, facilitates server selection and redirection, performs static load distribution of sessions

- Session Manager — Maps a user session on a server to a physical Sun Ray 1 enterprise appliance and binds/unbinds related services to and from the specific Sun Ray 1 enterprise appliance
- Administration Tool — Provides user management and usage monitoring
- Sun Ray 1 enterprise appliance firmware download — Determines whether the firmware in the Sun Ray 1 enterprise appliance matches the version of the Sun Ray enterprise server software, and updates the firmware if necessary. This happens automatically as part of the authentication process.

Interconnect

A dedicated, high-speed, unmanaged interconnection for communication between the Sun Ray enterprise server and Sun Ray 1 enterprise appliances. Based on high-speed Ethernet technology, the Sun Ray enterprise system leverages commodity network components and standard protocols.

In a Sun Ray server failover group, every Sun Ray 1 enterprise appliance must have a path through the interconnect fabric to every Sun Ray enterprise server in the failover group. This is further described in the discussion of the Failover Group later in this paper.

Sun Ray Enterprise Server

A Sun Ray enterprise server is any supported SPARC server running the Solaris Operating Environment (release 2.6 or 7) and the Sun Ray enterprise server software. Each Sun Ray enterprise server runs the Sun Ray enterprise server software, that manages connections to the Sun Ray 1 enterprise appliances and performs enterprise appliance-specific administration functions, in addition to hosting user client sessions.

A Sun Ray enterprise server also uses the Dynamic Host Configuration Protocol (DHCP) service to assign IP addresses to Sun Ray clients. If the Sun Ray enterprise server is a member of a Sun Ray server failover group, the DHCP server must be configured to coexist with the other DHCP servers on the other member of the failover group.

Sun Ray Server Failover Capability

The new failover capabilities, available in Sun Ray enterprise server software release 1.1, enable multiple Sun Ray enterprise servers to function as a failover group, and provide service redundancy for Sun Ray 1 enterprise appliance users.

This means that the Sun Ray enterprise server is no longer a single point of failure — if a server becomes unavailable, users will automatically be re-authenticated on another server in the failover group, and they will be able to log in again to start another session.

There are some important points to note about the Sun Ray server failover capability:

- Failover occurs at the user authentication level. User sessions do not failover, nor do applications hosted on the Sun Ray server.

  When a server fails, each user whose session was on that server is re-authenticated on another member of the failover group, and is presented with a new session and a new login prompt. The user's new session will restore the user's environment under the normal Solaris Operating Environment/CDE conditions.

  Any applications the user was running within his or her session will need to be restarted. However, applications and data hosted on other servers (application servers, mail and file servers, for example) should be accessible as soon as the user has logged in to his new session. Depending on the application, the user may be able to continue more or less where he left off if he has recently saved his work or if the application regularly creates backup or recovery files. Failover does not provide the same level of state restoration as the user experiences with smart card access to an existing session.

  If the user already has a session running on the new server (not the usual case), the session will resume upon re-authentication. However, this session will resume at the point the user last left it, which will *not* be the same state as the user session running on the unavailable server.

- Applications running on the Sun Ray enterprise server do not fail over under the Sun Ray server failover capability. Applications and data hosted on the unavailable server will be inaccessible from the user's new session until the server is restored. However, applications and data hosted on other servers will be available as soon as the user logs in to the new session. Therefore, it is recommended that critical items be provided by highly available or redundant systems. For example, users' home directories and mail files, as well as corporate databases, should be handled in this way so that users can continue their work after a Sun Ray server failover event.

- Once a new session is begun on a second server, the session will remain on that server until the user logs out. When a user re-inserts his/her smart card, the authentication process connects the user to the most recent session, which will be the one created on the second server. This may result in several sessions for the same user running on different servers.

  The Sun Ray server software does provide a way for a user to explicitly redirect the appliance to a specific server, which may enable the user to re-connect with his original session, once the server is again available, if the session still exists.

Sun Ray Server Load Distribution

The new Sun Ray enterprise server software provides static load distribution for Sun Ray 1 enterprise appliance client sessions. This allows a more efficient usage and sharing of resources among the Sun Ray 1 appliance users.

For example, under the single-server restriction of the Sun Ray 1.0 server software, an organization might have two groups of Sun Ray 1 enterprise appliance users, each with their own server. One group might not use very much of their server's capacity, while the other keeps their server heavily loaded all the time. With the 1.1 software release, some of the user sessions from the second group could be placed on the first group's lightly-used server, thus saving the second group the expense of adding capacity to their server, (as well as providing a failover option for both groups).

Sessions are directed to a server within the server group when a user token is authenticated. The Authentication Manager passes the authenticated token to the Group Manager. The Group Manager determines which server in the failover group should host the user session, based on the CPU and memory capacity, and the current load on the group member servers. For example, a server with 4 CPUs and 2GB of memory will normally be allocated a larger number of sessions than will a server with 2 CPUs and 1 GB of memory.

Once a session has been located on a given server, that session is never automatically relocated, regardless of the load characteristics of the various servers in the group.

Load distribution can be turned on and off independently of the failover capability.

Note – Session relocation happens when a token is accepted — either when a smart card is inserted for which there is currently no running session, or (in the case of a zero-administration policy) through pseudo-token authentication when the Sun Ray 1 enterprise appliance is connected to a functional Sun Ray system. Once the login prompt appears, the session is already running on the server to which it has been assigned. Logout and login have no effect on the session location, unless the user also remove his smart card and leaves it out long enough for the Session Manager to determine that the session should be terminated (15 minutes is the default setting in the Sun Ray 1.1 software).

There are currently only two ways to start a session on a different server from the one initially designated by the Group Manager.

- The first method is to use the *utselect* command. This command brings up a small window that allows the user to select a server on which to create a new session. This is the most reliable method if the user wants to run his session on a particular server. Once the new session is running, the user must run utselect again, return to the original server, and log out of the old session. He is then automatically returned to the new session. If the user wants continue working where he left off in the first session, he will need to save his work because the old session state will not migrate. The utselect command is documented in the *Sun Ray 1 Enterprise Server Software 1.1 Advance Administrator's Guide*.
- The second method is to log out and remove the smart card from the Sun Ray 1 enterprise appliance, leaving it out for at least 15 minutes. After this time, the session manager determines that the session is no longer needed, and terminates it. Logging out by itself does not end a session, it just returns the session to the login state. After 15 minutes, the user can re-insert his smart card, and the relocation process will take place. However, there is no guarantee that the Group Manager will not again select the same server where the previous session was running.

Load Distribution with a Zero-Administration Policy

The Sun Ray enterprise server software provides a zero-administration authentication policy for organizations that do not want to use smart cards, and do not need session mobility. When this policy is in place, sessions are tied to physical Sun Ray 1 enterprise appliances by using the appliance's "pseudo-token" for authentication.

When a Sun Ray 1 appliance is plugged into a functional Sun Ray interconnect with a running server, the appliance pseudo-token is used to authenticate the device. At this point the Group Manager software determines where to locate the new session. Once the login screen is presented, the session is already running and the server location decision has already been made.

As in the discussion above, the user can use the utselect command to start a session on a different server. Since there isn't a smart card involved, the only other way to force a new session is to unplug the Sun Ray 1 appliance from the interconnect, wait at least 15 minutes, and plug it in again. The utselect command is definitely the preferable method.

The Failover Group

A failover group is a set of Sun Ray enterprise servers, all running the Sun Ray enterprise server release 1.1 or higher software, and all having access to all the Sun Ray client devices connected to the private interconnect.

The failover group can include a heterogeneous group of Sun servers (for example a mixture of Ultra Enterprise™ 250s and 450s servers) running either the Solaris 2.6 or Solaris 7 Operating Environment. However, the servers must all run the same version of the Sun Ray enterprise server software (version 1.1 or higher).

All the servers in the failover group should be accessible from all the Sun Ray clients over the interconnect. Figure 1 shows several server and interconnect configurations that meet this requirement.

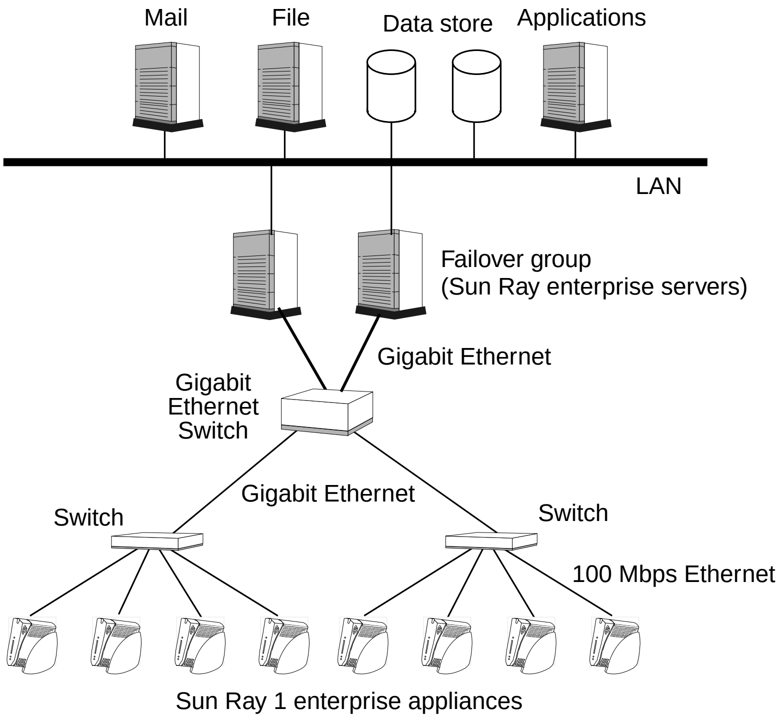

Figure 1 Example configuration for Sun Ray enterprise system with failover group

The decision as to how to deploy the Sun Ray enterprise servers and appliances will depend on the existing network infrastructure, technology, and the redundancy required at the server NIC point of failure. This is discussed further in the next section.

The Group Manager

The Group Manager is a distributed process — one copy runs on each Sun Ray enterprise server in a failover group. The Group Manager keeps track of the group membership and network topology, facilitates server selection and redirection, and performs static load distribution of sessions, if that capability is enabled.

The Group Managers keep each other informed by broadcasting a “keep-alive” message that contains information on that Group Manager hostname and address, network interface information, CPU and memory capacity, and the number of sessions it has running.

Each Group Manager takes the information and constructs a global state map. It uses this information to determine how to handle a user token once it has been authenticated.

When a token is presented for authentication, it may be handled by the Authentication Manager on any of the servers in the failover group. Once the token has been authenticated, it is passed to the Group Manager on that server. The Group Manager first queries the other Sun Ray servers to find out if a session already exists for the token. If so, it passes the token to the server that has the most recent session associated with the token. If no session exists, then the Group Manager uses the capacity, load and session information about the other servers to determine whether (and where) to redirect the session. Once this determination is made, the token is sent to the new server, which re-authenticates the token and passes it to the Session Manager which creates the new session.

If a server fails to send a keep-alive message within a specified time, the assumption is that the server is unavailable, and the other Group Managers remove that server’s information from the global map. Meanwhile, when the Sun Ray appliances connected to the unavailable server detect the loss of access, they will re-request authentication. The request will be picked up by one of the remaining servers, and the user will be re-authenticated, and a session started on a different server.

Trusted Servers

Finally, the failover group can be configured as a “trusted group,” implemented through the Group Manager. The trusted relationship is based on the contents of a signature file that must be identical at all members of the trusted group.

Trusted and untrusted servers cannot be mixed in a failover group. If the trusted group capability is used, then the Group Manager will not redirect a session to any server that is not a member of the trusted group.

Implementing the Sun Ray Server Failover and Load Distribution Capabilities 3

This section provides a brief overview of the requirements for implementing failover and load distribution in the Sun Ray enterprise system environment. Detailed and exact instructions for implementing these features can be found in the *Sun Ray Enterprise Server Software Advance Administrator's Guide*.

Sun Ray Server Configuration Requirements in a Failover Environment

There is no theoretical limit to the number of servers in a Sun Ray server failover group. The servers can be any of the Sun servers supported as a Sun Ray enterprise server. This includes the Sun Enterprise™ 10000 server, where each domain can function as a member of a failover group. The number of servers and Sun Ray 1 enterprise appliances in a failover group will be limited in practice by the capacity of the interconnect, as all servers must be accessible by all clients.

The rules for server capacity configuration in a Sun Ray server failover environment are basically the same as for an individual Sun Ray enterprise server, based on the expected number of active users and the characteristics of the applications they will run.

However, the expected number of users needs to be calculated differently. Each server in a failover group must be configured not only to handle the expected number of users under normal conditions, but it must also be able to handle users redirected to it when another server becomes unavailable.

If the failover group consists of just two servers, then each server must be able to handle *all* the expected active users in the workgroup under failover conditions, with some reasonable level of performance. If a failover group contains more than two servers, then each server in the group must be able to handle its own expected load plus a portion of the load normally hosted the largest capacity server in the failover group.

For example, if servers A, B, and C are members of a failover group, and servers A and B have similar capacity while server C is a larger capacity server, then servers A and B should each have the capacity to handle all their own sessions plus at least half of server C’s sessions.

The level of performance provided when additional users are redirected during a failover incident, is a matter of individual organizational policy. Organizations may choose to make a trade-off between performance under failover conditions versus the expense of creating the extra capacity required. However, note that once sessions are redirected to a server under failover conditions, they are not automatically redirected back when the unavailable server revives. Thus, unless users explicitly re-establish their sessions back on the original server, or users regularly log off (and remove their smart cards) to end their session, the load on the second server may stay high indefinitely.

Server Software Requirements

There are several requirements regarding the software on the Sun Ray enterprise servers that support failover and load distribution. These are:

- Each Sun Ray server in a server group must be running the same version of the Sun Ray Enterprise Server software, including patches.
- All servers in the group must use the same configurations (i.e. Authentication Manager and Session Manager configuration, including authentication policies etc.)
- Either all servers in the group must be “trusted hosts” or none of them can be trusted hosts.
- Servers within the group can run either the Solaris 2.6 or Solaris 7 Operating Environment — the OS environment can be heterogeneous.

DHCP Configuration

The Sun Ray Hot Desk technology uses DHCP to assign client addresses to the Sun Ray 1 enterprise appliances when they are authenticated. In a failover environment, multiple Sun Ray servers should run a DHCP service, with the following considerations:

- Multiple servers should provide the DHCP service to avoid a single point of failure, but DHCP does not need to run on every Sun Ray server in the group.
- Each DHCP server must be configured to use a non-overlapping subset of the available client addresses.
- Each address range must contain enough addresses to accommodate all clients that are attached to the interconnect. This is because whenever a desktop appliance is authenticated on a particular server, DHCP assigns an IP address for that session, but IP addresses do not get reallocated right away when a session terminates. Thus, it is theoretically possible to have an IP address on every server for every user—at least temporarily.
- Class C is the default address range, but class B can be used for larger address ranges.

As an example, consider the situation with 80 Sun Ray 1 enterprise appliances connected to three Sun Ray enterprise servers, each running a DHCP service, and using class C addressing. In this case, the address ranges for the three servers would be:

	Server A	**Server B**	**Server C**
Server IP address	192.168.128.1	192.168.128.2	192.168.128.3
First address in range	192.168.128.6	192.168.128.86	192.168.128.166
last address in range	192.168.128.85	192.168.128.165	192.168.128.245

Table 1 Class C address ranges for DHCP for three servers

Primary and Secondary Administration

In a multi-server environment, if the Sun Ray enterprise system is configured to use an authentication policy *other than* zero-administration, then the failover group must also be configured as an administered group. This means that the LDAP must be configured to enable replication of the Sun Ray administration data (registered token information, users, smart cards etc.) across the group. The administration group is composed of a primary administration server and one or more secondary administration servers. If the primary administration server fails, a secondary server can assume the administration data and tasks for the Sun Ray system.

If the Sun Ray enterprise system uses a zero-administration policy, then no administration is necessary, and an administration group is not needed. Note that all servers in a Sun Ray server failover group must use the same set of administration policies.

The new Sun Ray enterprise server software 1.1 provides a set of commands that enable the configuration of an administration group.

Interconnect Configuration Requirements

The requirements for the interconnection fabric in a Sun Ray failover environment are basically the same as in a single-server environment.

- It is recommended that all switches have multicast enabled (this is the default assumption made by the Sun Ray enterprise server software). However, it is possible to configure the software so that this is not necessary.
- All servers in the failover group should have access to (and be accessible by) all the Sun Ray 1 enterprise appliances connected to the interconnect.

Beyond these few conditions, the failover environment supports the same interconnect topologies that are supported in a single-server Sun Ray environment.

Bandwidth Considerations

In many ways the bandwidth considerations are similar to the considerations in a single-server scenario. However, bandwidth projections need to provide for the demands under load distribution and failover scenarios, where additional user sessions may be communicating on routes they would not use in a single-server scenario. Again, there are trade-offs that can be made in terms of the level of performance supported under failover conditions versus the costs of providing the extra capacity to help ensure that performance.

The figures below illustrate possible server and interconnection topologies, with a brief discussion of the issues surrounding each.

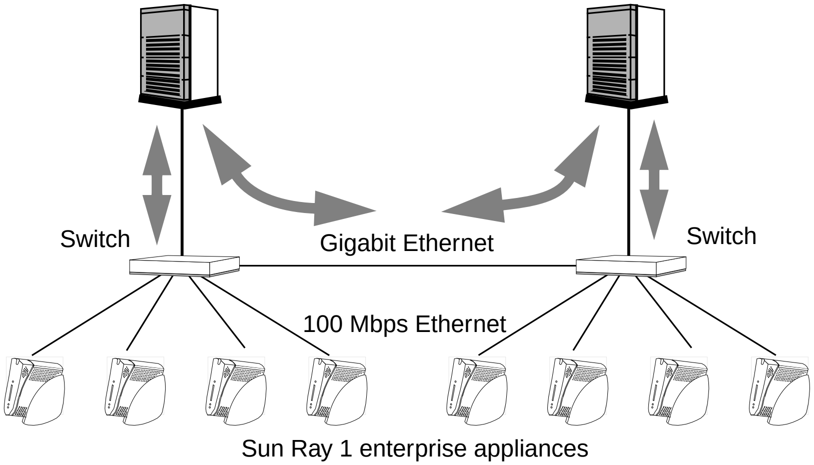

Figure 2 Two Sun Ray 1 appliance workgroups interconnected through a switch-to-switch link.

The scenario in Figure 2 is perhaps the simplest way of providing load distribution and failover — it basically involves connecting two separate Sun Ray enterprise system workgroups through their switches. When load distribution is in effect, traffic could be moving in both directions across the inter-switch connection, as shown in the figure.

The potential drawback is that in the case of a server failure, one switch must be capable of handling all the traffic from the other switch, in addition to the traffic from its own users. Thus, it may not be sufficient to simply interconnect to existing Sun Ray workgroups, since their switches may not have the capacity to handle the additional load. In this scenario, upgrading the workgroup switches would be a possibility.

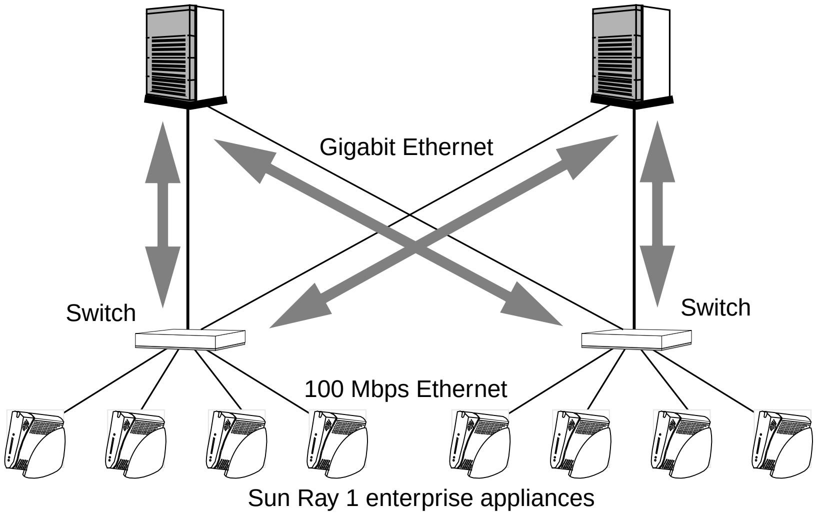

Figure 3 Scenario with two NICs in each server, providing paths to each switch

The scenario in Figure 3 shows another way to interconnect two separate workgroups. In this case, instead of interconnecting the switches, a second NIC is added to each server and is cross-connected to the other switch. In this scenario, the load on the switches does not increase, but there is additional expense reflected in the second NIC card in each server.

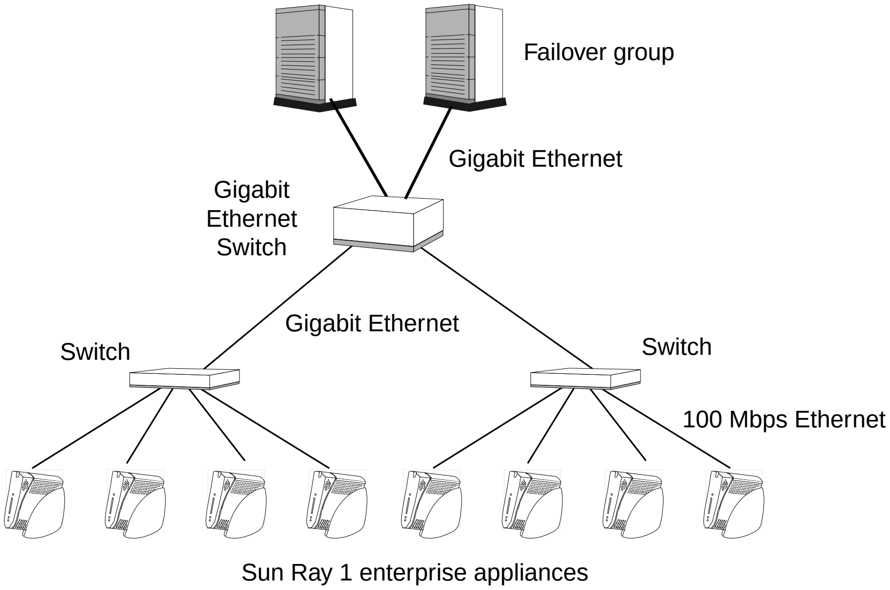

Figure 4 Scenario using a high-capacity gigabit ethernet switch

In this scenario (Figure 4), a gigabit ethernet switch is placed between the individual workgroup switches and the two servers. This scenario adds the expense of the gigabit switch instead of multiple NIC cards or upgraded workgroup switches.

Sun Microsystems Incorporated
901 San Antonio Road
Palo Alto, CA 94303 USA
650 960-1300
FAX 650 969-9131
http://www.sun.com

Sales Offices

Africa (North, West and Central):
+33 1 30674680
Argentina: +54-11-4317-5600
Australia: +61-2-9844-5000
Austria: +43-1-60563-0
Belgium: +32-2-716 79 11
Brazil: +55-11-5181-8988
Canada: +905-477-6745
Chile: +56-2-3724500
Colombia: +571-629-2323
Commonwealth of Independent States:
+7-502-935-8411
Czech Republic: +420-2-33 00 93 11
Denmark: +45 4556 5000
Estonia: +372-6-308-900
Finland: +358-9-525-561
France: +33-01-30-67-50-00
Germany: +49-89-46008-0
Greece: +30-1-6188111
Hungary: +36-1-202-4415
Iceland: +354-563-3010
India: +91-80-5599595
Ireland: +353-1-8055-666
Israel: +972-9-9513465
Italy: +39-039-60551
Japan: +81-3-5717-5000
Kazakhstan: +7-3272-466774
Korea: +822-3469-0114
Latvia: +371-750-3700
Lithuania: +370-729-8468
Luxembourg: +352-49 11 33 1
Malaysia: +603-264-9988
Mexico: +52-5-258-6100
The Netherlands: +31-33-450-1234
New Zealand: +64-4-499-2344
Norway: +47-2202-3900
People's Republic of China:
Beijing: +86-10-6803-5588
Chengdu: +86-28-619-9333
Guangzhou: +86-20-8777-9913
Shanghai: +86-21-6466-1228
Hong Kong: +852-2802-4188
Poland: +48-22-8747800
Portugal: +351-1-412-7710
Russia: +7-502-935-8411
Singapore: +65-438-1888
Slovak Republic: +421-7-522 94 85
South Africa: +2711-805-4305
Spain: +34-91-596-9900
Sweden: +46-8-623-90-00
Switzerland: +41-1-825-7111
Taiwan: +886-2-2514-0567
Thailand: +662-636-1555
Turkey: +90-212-236 3300
United Arab Emirates: +971-4-366-333
United Kingdom: +44-1-276-20444
United States: +1-800-555-9SUN OR +1-650-960-1300
Venezuela: +58-2-905-3800
Worldwide Headquarters:
650-960-1300 or 800-555-9SUN
Internet: www.sun.com

Printed in USA