Planning for Network Deployment in Oracle® Solaris 11.3

Part No: E54821
April 2019

ORACLE

Planning for Network Deployment in Oracle Solaris 11.3

Part No: E54821

Référence: E54821

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` ou le site `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si vous êtes malentendant.

Contents

Using This Documentation

- **Overview** – Includes basic topics and tasks to assist you in planning for deploying IPv4 and IPv6 networks.
- **Audience** – System administrators.
- **Required knowledge** – Basic understanding of network administration concepts and practices.

Product Documentation Library

Documentation and resources for this product and related products are available at http://www.oracle.com/pls/topic/lookup?ctx=E53394-01.

Feedback

Provide feedback about this documentation at http://www.oracle.com/goto/docfeedback.

♦ ♦ ♦ CHAPTER 1

Planning For Network Deployment

This chapter describes the different considerations when planning for the deployment of a TCP/IP network. The planning tasks that are described can assist you in deploying your network in an organized and cost-effective manner. Note that the details of planning the network are outside the scope of this book. Only general directions are provided. This book also assumes that you are familiar with basic networking concepts and terminology.

For an overview of network administration in this release, see Chapter 1, "About Network Administration in Oracle Solaris" in *Configuring and Managing Network Components in Oracle Solaris 11.3*.

For information about administering an existing TCP/IP network, see Chapter 1, "Administering TCP/IP Networks" in *Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle Solaris 11.3*.

For a high-level overview of the networking strategies that you can implement in the Oracle Solaris release, see Chapter 1, "Summary of Oracle Solaris Network Administration" in *Strategies for Network Administration in Oracle Solaris 11.3*.

This chapter contains the following topics:

Determining the Network Hardware

The number of systems that you expect to support affects how you configure your network. Your organization might require a small network of several dozen standalone physical systems that are located on one floor of a single building. Or, you might need to set up a network with more than 1,000 systems in several buildings. This setup can require you to further divide your network into subdivisions that are called *subnets*.

Note - For a description of the example IP addresses used in this guide, see the `IP address` entry in *Glossary of Networking Terms*.

Some of the planning decisions that you must make about hardware include the following:

- Network topology, the layout, and connections of the network hardware
- Type and number of systems your network can support, including the virtual systems that might be required on your server
- Network devices to be installed in these systems
- Type of network media to use, such as Ethernet, and so on
- Use of bridges, routers, and firewalls to extend the network media or connect the local network to external networks

  For information about how bridges work, see "Overview of Bridged Networks" in *Managing Network Datalinks in Oracle Solaris 11.3*.

  For a description of how routers function, see "Planning for Routers on Your Network" on page 14.

  For information about firewalls, see Chapter 5, "Configuring the Packet Filter Firewall" in *Securing the Network in Oracle Solaris 11.3* and Chapter 6, "IP Filter Firewall in Oracle Solaris" in *Securing the Network in Oracle Solaris 11.3*.

Network Topology Description

Network topology describes how networks fit together. Routers are the entities that connect networks to each other. A router is any machine that has two or more network interfaces and implements IP forwarding. However, the system cannot function as a router until properly configured, as described in Chapter 2, "Configuring a System as a Router" in *Configuring an Oracle Solaris 11.3 System as a Router or a Load Balancer*.

Routers connect two or more networks to form larger internetworks. You must configure the routers to pass packets between two adjacent networks. The routers also should be able to pass

packets to networks that lie beyond the adjacent networks by forwarding them to other routers that are connected to adjacent networks.

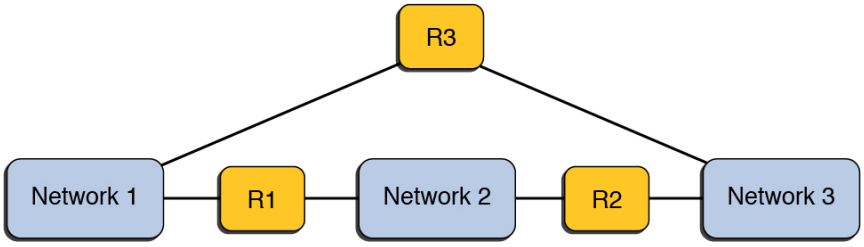
The following figure shows 3 networks connected by 2 routers.

FIGURE 1 Basic Network Topology

In addition to joining networks into internetworks, routers route packets between networks that are based on the addresses of the destination network. As internetworks grow more complex, each router must make more and more decisions about the packet destinations.

The following figure shows a more complex case. Router R3 directly connects networks 1 and 3. The redundancy improves reliability. If network 2 goes down, router R3 still provides a route between networks 1 and 3. You can interconnect many networks. However, the networks must use the same network protocols.

FIGURE 2 A Network Topology That Provides an Additional Path Between Networks



Routers are discussed in more detail in “Planning for Routers on Your Network” on page 14.

Using Subnets on Your Network

The use of subnets is connected with the need for administrative subdivisions to address issues of size and control. The more hosts and servers that you have on a network, the more complex your management task. By creating administrative divisions and using subnets, managing complex networks becomes easier.

The decision about setting up administrative subdivisions for your network is determined by the following factors:

- **Size of the network**

  Subnets are also useful even in a relatively small network whose subdivisions are located across an extensive geographical area.
- **Common needs shared by groups of users**

  For example, you might have a network that is confined to a single building and supports a relatively small number of systems. These machines are divided among a number of subnetworks. Each subnetwork supports groups of users with different needs. In this example, you might use an administrative subdivision for each subnet.
- **Security**

  You might want to segregate your mission critical servers, desktop systems, and Internet facing web servers into separate subnets where you can establish firewalls between them.

IPv4 Autonomous System Topology

Sites with multiple routers and networks typically administer their network topology as a single routing domain or an *autonomous system* (AS). Figure 3, “Autonomous System With Multiple IPv4 Routers,” on page 14 shows an AS that is divided into three local networks: `203.0.113.0`, `198.51.100.0`, and `192.0.2.0`.

The network is comprised of the following types of systems:

- Routers

  Router use routing protocols to manage how network packets are directed or routed from their source to their destinations within the local network or to external networks. For information about the routing protocols that are supported in Oracle Solaris and instructions on configuring a system as a router, see “Routing Protocols: Introduction” in *Configuring an Oracle Solaris 11.3 System as a Router or a Load Balancer*.

  Types of routers include the following:

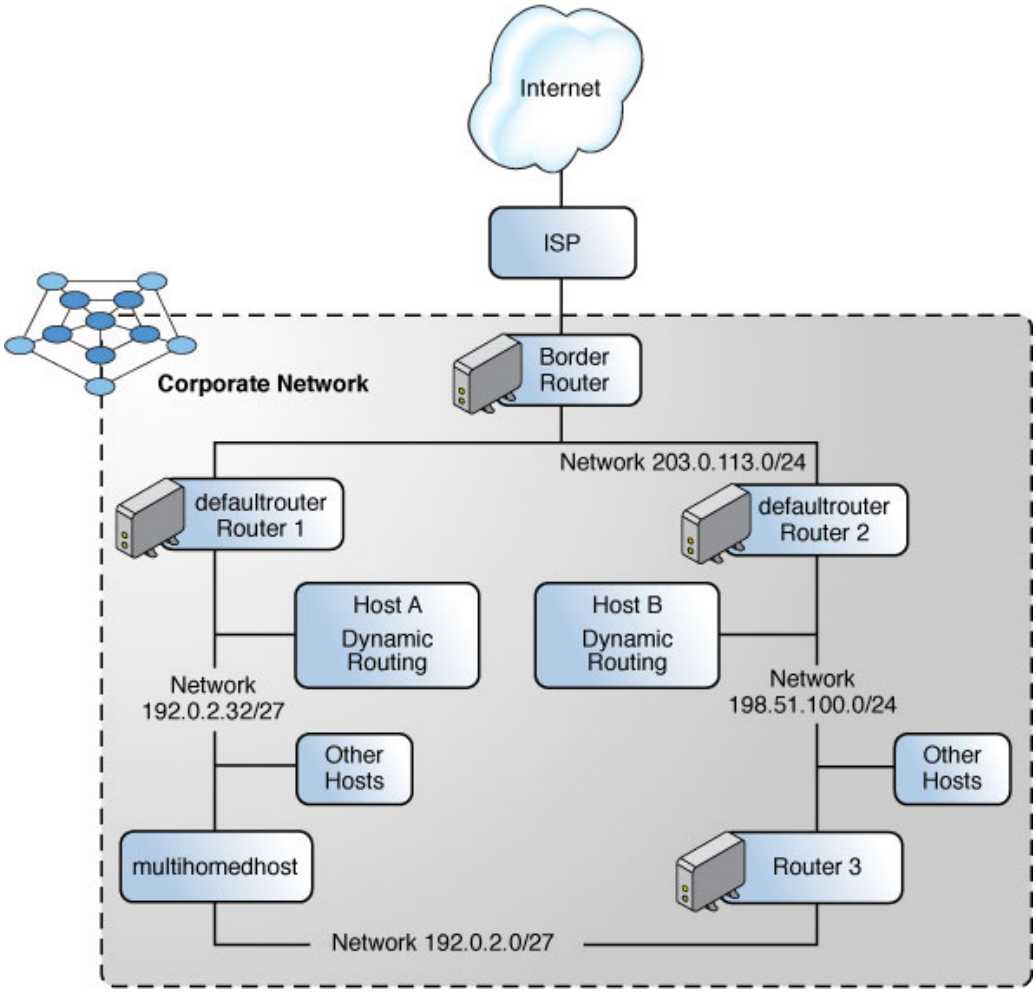
  - Border routers – Connect the local network, such as `203.0.113.0`, externally to a service provider.

    - Default routers – Manage packet routing in the local network, which itself can include several local networks. For example, in Figure 3, “Autonomous System With Multiple IPv4 Routers,” on page 14, Router 1 serves as the default router for `192.0.2.0`. Contemporaneously, Router 1 is also connected to the `203.0.113.0` internal network. Router 2's interfaces connect to the `203.0.113.0` and `198.51.100.0` internal networks.
    - Packet-forwarding routers – Forward packets between internal networks but do not run routing protocols. In Figure 3, “Autonomous System With Multiple IPv4 Routers,” on page 14, Router 3 is a packet-forwarding router with connections to the `198.51.100.0` and `192.0.2.0` networks.
- Client systems
    - Multihomed systems or systems that have multiple NICs. In Oracle Solaris, these systems by default can forward packets to other systems in the same network segment.
    - Single-interfaced systems rely on the local routers for both packet forwarding and receiving configuration information.

For task-related information, see Chapter 3, “Configuring and Administering IP Interfaces and Addresses in Oracle Solaris” in *Configuring and Managing Network Components in Oracle Solaris 11.3*.

Use the following figure as a reference when configuring additional network components.

FIGURE 3 Autonomous System With Multiple IPv4 Routers



Planning for Routers on Your Network

Recall that in TCP/IP, two types of entities exist on a network: hosts and routers. All networks must have hosts, while not all networks require routers. The physical topology of the network

determines if you need routers. The following network topology and routing concepts are important when deciding whether to add another network to your existing network environment.

For complete details and tasks for router configuration on IPv4 and IPv6 networks, see Chapter 2, “Configuring a System as a Router” in *Configuring an Oracle Solaris 11.3 System as a Router or a Load Balancer*.

How Routers Transfer Packets

Routers transfer packets in the following manner:

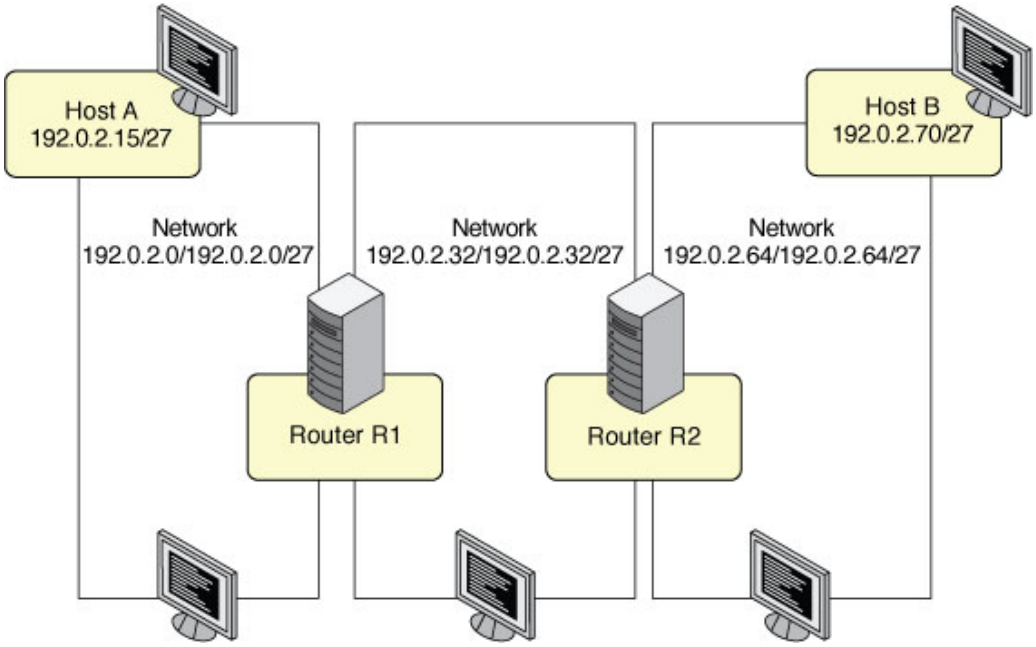
- All nodes on an IP network maintain routing information in routing tables. These tables contain information about how to reach systems that are attached to both local and remote networks. The routing tables are generated from local configuration information and from routing protocol messages that is exchanged with neighboring systems.
- When a system initially sends a packet, it looks up the packet's destination address in its routing table to determine if the destination is on the local network. If yes, the packet goes directly to the host with that IP address. If not, the packet goes to a router on the local network.
- When a router receives a packet, the router checks its routing table to determine if the destination address is for a system on one of its attached networks or if the message must be forwarded through another router. It then sends the message to the next system in the path to the destination.
- This process is repeated on each router that receives the message until the message reaches the destination system.

Refer to Chapter 2, “Configuring a System as a Router” in *Configuring an Oracle Solaris 11.3 System as a Router or a Load Balancer*.

Sample Network Topology

The following figure shows a network topology with three networks that are connected by two routers.

FIGURE 4 A Network Topology With Three Interconnected Networks



Router R1 connects networks `192.0.2.0/27` and `192.0.2.32/27`. Router R2 connects networks `192.0.2.32/27` and `192.0.2.64/27`.

If Host A on network `192.0.2.0/27` sends a message to Host B on network `192.0.2.32/27`, the following events occur:

1. Host A examines its routing tables for the path to `192.0.2.70/27`. The local network address range does not cover this address, but there is a previously learned default route through router R1 that covers the address. Therefore, Host A sends the packet to Router R1.
2. Router R1 examines its routing tables. No local network's address range covers the destination address, but there is a known route to network `192.0.2.64/27` through Router R2 that covers the address, Router R1 sends the packet to Router R2.
3. Router R2 is connected directly to network `192.0.2.64/27`. The routing table lookup reveals that `192.0.2.70/27` is on the attached network. Router R2 sends the packet directly to Host B.

Obtaining IP Addresses for Your Network

When you plan your network addressing scheme, consider the following factors:

- Type of IP address that you want to use: IPv4 or IPv6
- Number of potential systems on your network
- Number of systems that are multihomed, or routers, which require multiple network interface cards (NICs), each with individual IP addresses
- Whether to use private addresses on your network
- Whether to have a DHCP server that manages pools of IP addresses

For an introduction to IP addresses, refer to available articles about the topic online such as the following resources:

- https://en.wikipedia.org/wiki/IP_address
- http://tools.ietf.org/html/rfc791
- http://tools.ietf.org/html/rfc4632
- http://tools.ietf.org/html/rfc4291

To obtain IP addresses, register with any Internet Service Provider, or through IANA's Internet Registries. See IANA's IP Address Service page (http://www.iana.org/ipaddress/ip-addresses.htm).

Using Naming Entities on Your Network

The TCP/IP protocols locate a system on a network by using its IP address. However, a host name enables you to identify systems more easily than IP addresses.

From a TCP/IP perspective, a network is a set of named entities. A host is an entity with a name. A router is an entity with a name. The network is an entity with a name. A group or department in which the network is installed can also be given a name, as can a division, a region, or a company. In theory, the hierarchy of names that can be used to identify a network has virtually no limit.

Domain Names

Many networks organize their hosts and routers into a hierarchy of administrative domains. If you are using the Network Information Service (NIS) or the Domain Name System (DNS)

naming service, you must select a domain name for your organization that is unique worldwide. To ensure that your domain name is unique, you should register the domain name with *InterNIC*. A unique domain name is required if you plan to allow other sites on the Internet to locate your systems through DNS.

A domain name that is located under another domain is often referred to as a sub-domain. The domain name structure is hierarchical. A new domain typically is located under an existing, related domain. For example, the domain name for a subsidiary company can be located below the domain of the parent company. If the domain name has no other relationship, an organization can place its domain name directly under one of the existing top-level domains such as `.com`, `.org`, `.edu`, `.gov`, and so forth.

Selecting a Naming Service and Directory Service

In Oracle Solaris you can select from three types of naming services: local files, NIS, and DNS. Naming services maintain critical information about the machines on a network, such as the host names, IP addresses, and so forth. You can also use the LDAP directory service in addition to or instead of a naming service. LDAP is a secure network protocol that is used to access directory servers for distributed naming and other directory services. This standard based protocol supports a hierarchical database structure. The same protocol can be used to provide naming services in both UNIX and multi-platform environments. For an introduction to naming services in Oracle Solaris, refer to Chapter 1, “About Naming and Directory Services” in *Working With Oracle Solaris 11.3 Directory and Naming Services: DNS and NIS*.

The configuration of the network databases is critical. Therefore, you need to decide which naming or directory service to use as part of the network planning process. Moreover, the decision to use naming services also affects whether you organize your network into an administrative domain.

For a naming or directory service, you can select from the following:

- NIS or DNS – The NIS and DNS naming services maintain network databases on several servers on the network. See *Working With Oracle Solaris 11.3 Directory and Naming Services: DNS and NIS* for a description of these naming services and information about how to configure the databases. In addition, the guide explains the *namespace* and *administrative domain* concepts in more detail.
- LDAP – You can also use the LDAP directory service in addition to or instead of a naming service. LDAP is a secure network protocol that is used to access directory servers for distributed naming and other directory services.
- Local files – If you do not implement NIS, DNS, or LDAP, the network uses *local files* to provide the naming service. The term “local files” refers to the series of files in the `/etc` directory that the network databases use. The procedures in this book assume you are using local files for your naming service, unless otherwise indicated.

Note - If you decide to use local files as the naming service for your network, you can set up another naming service at a later date.

Administering Host Names

Plan a naming scheme for the systems that will comprise the network. Each machine on the network should have a TCP/IP host name that corresponds to the IP address on its primary network interface. The host name must be unique within the system's sub-domain. Just like physical machines, virtual systems should also have a unique IP address and host name.

A system can have the following:

- Multiple host names that map to the system's IP address. For example, `systema.example.com` can also be known as `www.example.com`.
- The same host name for both IPv4 and an IPv6 addresses.
- A new IP address and an old deprecated IP address that are configured with the same host name for a period of time to support network renumbering.
- Multiple network interfaces on different subnets, each with a unique IP address and host name.

When planning your network, make a list of IP addresses and their associated host names for easy access during the setup process. The list can help you verify that all of your host names are unique.

Note - The primary interface's TCP/IP host name is a distinct entity from the *system host name* that you set with the `hostname` command. Although not required by Oracle Solaris, the same name is normally used for both. Some network applications depend on this convention. See the `hostname(1)` man page for more information.

♦ ♦ ♦ CHAPTER 2

Planning for Using IPv6 Addresses

This chapter supplements Chapter 1, "Planning For Network Deployment" by describing additional considerations when using IPv6 addresses on your network. If you do plan to use IPv6 addresses in addition to IPv4 addresses, ensure that your current ISP supports both address types.

For an introduction to IPv6 concepts, refer to Internet Protocol, Version 6 (IPv6) Specification (`http://www.ietf.org/rfc/rfc2460.txt`).

For IPv6 configuration tasks, see "Configuring IPv6 Interfaces" in *Configuring and Managing Network Components in Oracle Solaris 11.3*.

For information about troubleshooting IPv6 networks, see "Troubleshooting Issues With IPv6 Deployment" in *Troubleshooting Network Administration Issues in Oracle Solaris 11.3*.

This chapter contains the following topics:

IPv6 Planning Tasks

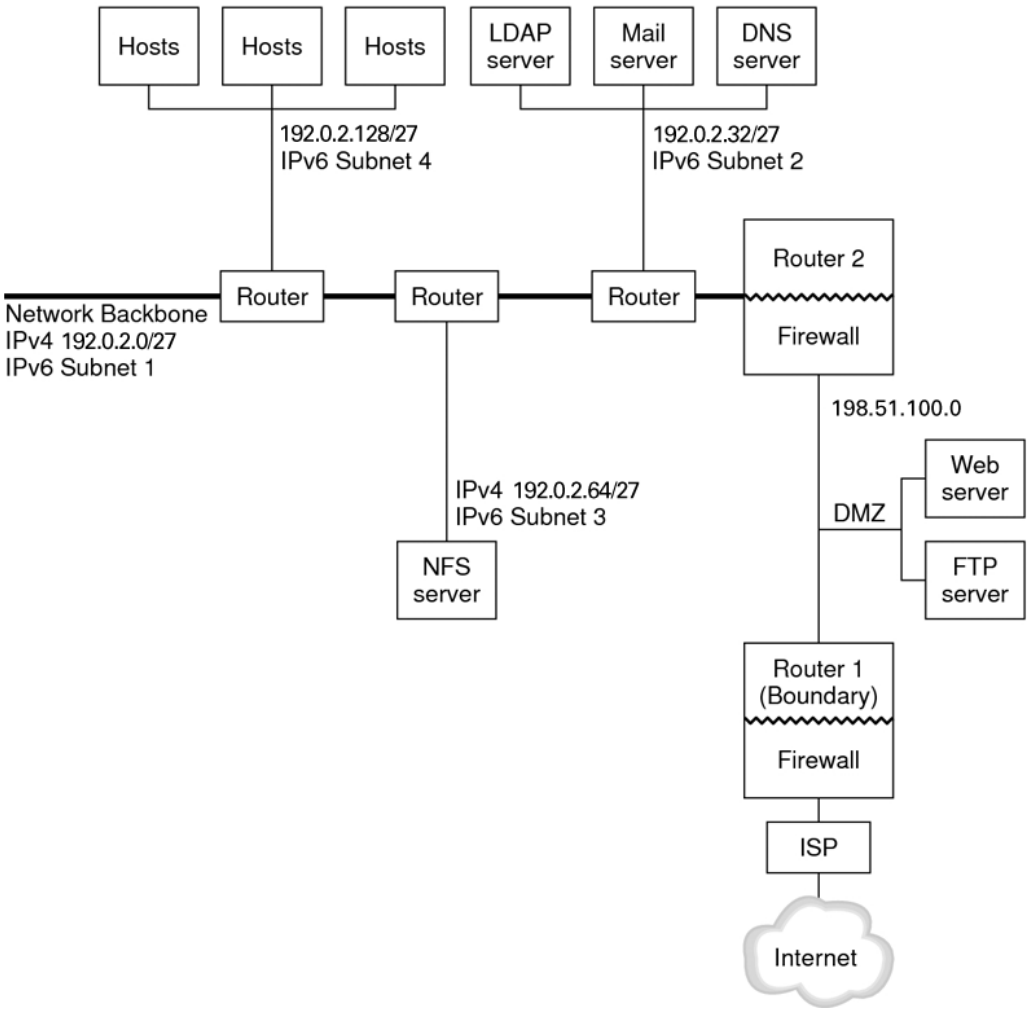
The following table describes different considerations when planning to implement IPv6 on your network. If you are migrating from an existing IPv4 network to an IPv6 network, see "Migrating From an IPv4 Network to an IPv6 Network" in *Configuring and Managing Network Components in Oracle Solaris 11.3* for additional instructions.

Task	Description	For Instructions
Prepare your hardware to support IPv6.	Ensure that your hardware can be upgraded to IPv6.	“Ensuring Hardware Support for IPv6” on page 24
Ensure that your applications are IPv6 ready.	Verify that your applications can run in an IPv6 environment.	“Configuring Network Services to Support IPv6” on page 26
Design a plan for tunnel usage.	Determine which routers should run tunnels to other subnets or external networks.	“Planning for Tunnel Use on the Network” on page 28
Plan how to secure your networks and develop an IPv6 security policy.	For security purposes, you need an addressing plan for the Demilitarized Zone (DMZ) and its entities before you configure IPv6. Decide how you would implement security, such as using IP Filter, IP security architecture (IPsec), Internet Key Exchange (IKE), and other security features of this release.	“Security Considerations for an IPv6 Implementation” on page 29 *Securing the Network in Oracle Solaris 11.3*
Create an addressing plan for systems on the network.	Your plan for addressing servers, routers, and hosts should be in place before IPv6 configuration. This step includes obtaining a site prefix for your network as well as planning IPv6 subnets, if needed.	“Preparing an IPv6 Addressing Plan” on page 25

IPv6 Network Topology Overview

Typically, IPv6 is used in a mixed network topology that also uses IPv4, such as shown in the following figure. The following figure is used as reference in the description of IPv6 configuration tasks that are described in this chapter.

FIGURE 5 IPv6 Network Topology Scenario



The enterprise network scenario depicted in the figure consists of five subnets with existing IPv4 addresses. The links of the network correspond directly to the administrative subnets. The four internal networks are shown with RFC 1918-style private IPv4 addresses, which is a common solution for the lack of IPv4 addresses.

These internal networks use the following address scheme:

- Subnet 1 is the internal network backbone `192.0.2.0/27`
- Subnet 2 is the internal network `192.0.2.32/27`, with LDAP, `sendmail`, and DNS servers
- Subnet 3 is the internal network `192.0.2.64/27`, with the NFS servers of the enterprise
- Subnet 4 is the internal network `192.0.2.128/27`, which contains hosts for the employees of the enterprise

The external, public network `198.51.100` functions as the corporation's DMZ. This network contains web servers, anonymous FTP servers, and other resources that the enterprise offers to the outside world. Router 2 runs a firewall and separates public network `198.51.100` from the internal backbone. On the other end of the DMZ, Router 1 runs a firewall and serves as the boundary server of the enterprise.

In Figure 5, “IPv6 Network Topology Scenario,” on page 23, the public DMZ has the RFC 1918 private address `198.51.100`. In the real world, the public DMZ must have a registered IPv4 address. Most IPv4 sites use a combination of public addresses and RFC 1918 private addresses. However, when you introduce IPv6, the concept of public addresses and private addresses changes. Because IPv6 has a much larger address space, you use public IPv6 addresses on both private networks and public networks.

The Oracle Solaris dual protocol stack supports concurrent IPv4 and IPv6 operations. You can successfully run IPv4–related operations during and after deploying IPv6 on your network. When you deploy IPv6 on an operating network that is already using IPv4, ensure that you do not disrupt ongoing operations.

Ensuring Hardware Support for IPv6

Check the manufacturers' documentation for IPv6 readiness regarding the following classes of hardware:

- Routers
- Firewalls
- Servers
- Switches

Note - All of the procedures in the this book assume that your equipment, particularly routers, can be upgraded to IPv6. However, some router models cannot be upgraded to IPv6. For more information and a workaround, refer to “Cannot Upgrade IPv4 Router to IPv6” in *Troubleshooting Network Administration Issues in Oracle Solaris 11.3*.

Preparing an IPv6 Addressing Plan

A major part of transitioning from IPv4 to IPv6 includes developing an addressing plan, which involves the following preparations:

- "Obtaining a Site Prefix" on page 25
- "Creating the IPv6 Numbering Scheme" on page 25

For actual migration tasks, see "Migrating From an IPv4 Network to an IPv6 Network" in *Configuring and Managing Network Components in Oracle Solaris 11.3*.

Obtaining a Site Prefix

Before you configure IPv6, you must obtain a site prefix. The site prefix is used to derive IPv6 addresses for all the nodes in your IPv6 implementation.

Any ISP that supports IPv6 can provide your organization with a 48-bit IPv6 site prefix. If your current ISP only supports IPv4, you can use another ISP for IPv6 support while retaining your current ISP for IPv4 support. In such an instance, you can use one of several workarounds. For more information, see "Current ISP Does Not Support IPv6" in *Troubleshooting Network Administration Issues in Oracle Solaris 11.3*.

If your organization is an ISP, then you obtain site prefixes for your customers from the appropriate Internet registry. For more information, see the Internet Assigned Numbers Authority (IANA) (`http://www.iana.org`).

Creating the IPv6 Numbering Scheme

Unless your proposed IPv6 network is entirely new, use your existing IPv4 topology as the basis for the IPv6 numbering scheme.

For most hosts, stateless autoconfiguration of IPv6 addresses for their interfaces is an appropriate, time saving strategy. When the host receives the site prefix from the nearest router, Neighbor Discovery automatically generates IPv6 addresses for each interface on the host.

Servers need to have stable IPv6 addresses. If you do not manually configure a server's IPv6 addresses, a new IPv6 address is autoconfigured whenever a NIC card is replaced on the server.

Keep the following tips in mind when you create addresses for servers:

- Give servers meaningful and stable interface IDs. One strategy is to use a sequential numbering scheme for interface IDs. For example, the internal interface of the LDAP server

in Figure 5, “IPv6 Network Topology Scenario,” on page 23 might become `2001:db8:3c4d:2::2`.

- Alternatively, if you do not regularly renumber your IPv4 network, consider using the existing IPv4 addresses of the routers and servers as their interface IDs. In Figure 5, “IPv6 Network Topology Scenario,” on page 23, suppose Router 1's interface to the DMZ has the IPv4 address `192.0.2.0/27`, then you can convert the IPv4 address to hexadecimal, and use the result as the interface ID. The new interface ID would be `::C000:0200`

  Only use this approach if you own the registered IPv4 address, rather than having obtained the address from an ISP. If you use an IPv4 address that was provided to you by an ISP, you create a dependency that would create problems if you change ISPs.

Due to the limited number of IPv4 addresses that are available, in the past, a network designer had to consider where to use global, registered addresses and private, RFC 1918 addresses. However, the notion of global and private IPv4 addresses does not apply to IPv6 addresses. You can use *global unicast addresses*, which include the site prefix, on all links of the network, including the public DMZ.

For your IPv6 subnets, begin your numbering scheme by mapping your existing IPv4 subnets into equivalent IPv6 subnets. You can use various online tools to convert IPv4 subnets to their equivalent IPv6 designations.

Configuring Network Services to Support IPv6

The following typical IPv4 network services are also IPv6 ready:

- DNS
- HTTP (supported release of Apache or Orion)
- LDAP
- NFS
- `sendmail`

The IMAP mail service is for IPv4 only.

Nodes that are configured for IPv6 can run IPv4 services. When you turn on IPv6, not all services accept IPv6 connections. Services that have been ported to IPv6 will accept a connection. Services that have not been ported to IPv6 continue to work with the IPv4 portion of the protocol stack.

Some issues can arise after you upgrade services to IPv6. For details, see “Problems Encountered When Upgrading Services to Support IPv6” in *Troubleshooting Network Administration Issues in Oracle Solaris 11.3*.

How to Prepare Network Services for IPv6 Support

1. **Update the following network services to support IPv6:**

   - Mail servers
   - NIS servers
   - NFS

   Note - LDAP supports IPv6 without requiring IPv6-specific configuration tasks.

2. **Verify that your firewall hardware is IPv6 ready.**
   Refer to the appropriate firewall-related documentation for instructions.

3. **Verify that other services on your network have been ported to IPv6.**
   For more information, refer to marketing collateral and associated documentation for the software.

4. **If your site deploys the following services, make sure that you have taken the appropriate measures for these services:**

   - **Firewalls** – Consider strengthening the policies that are in place for IPv4 to support IPv6. For more security considerations, see "Security Considerations for an IPv6 Implementation" on page 29.
   - **Mail** – In the mail exchanger record (MX record) for DNS, consider adding the IPv6 address of your mail server.
   - **DNS** – For DNS-specific considerations, see "How to Prepare DNS for IPv6 Support" on page 27.
   - **IPQoS** – Use the same *Diffserv* policies on a host that were used for IPv4.

5. **Audit any network services that are offered by a node prior to converting that node to IPv6.**

How to Prepare DNS for IPv6 Support

Oracle Solaris supports DNS resolution on both the client side and the server side. Use the following procedure to prepare DNS services for IPv6.

For more information that is related to DNS support for IPv6, refer to *Working With Oracle Solaris 11.3 Directory and Naming Services: DNS and NIS*.

1. **Ensure that the DNS server that performs recursive name resolution is dual-stacked (IPv4 and IPv6) or for IPv4 only.**

2. **On the DNS server, populate the DNS database with relevant IPv6 database AAAA records in the forward zone.**

   Note - Servers that run multiple critical services require special attention. Ensure that the network is working properly. Also ensure that all critical services are ported to IPv6. Then, add the server's IPv6 address to the DNS database.

3. **Add the associated PTR records for the AAAA records into the reverse zone.**

4. **Add either IPv4 only data, or both IPv6 and IPv4 data into the NS record that describes zones.**

Planning for Tunnel Use on the Network

The IPv6 implementation supports a number of tunnel configurations to serve as transition mechanisms as your network migrates to a mix of IPv4 and IPv6. Tunnels enable isolated IPv6 networks to communicate. Because most of the Internet runs IPv4, IPv6 packets from your site need to travel across the Internet through tunnels to destination IPv6 networks.

The following are some major scenarios for using tunnels in the IPv6 network topology:

- The ISP from which you purchase IPv6 service allows you to create a tunnel from your site's boundary router to the ISP network. Figure 5, “IPv6 Network Topology Scenario,” on page 23 shows such a tunnel. In this case, you would run a manual IPv6 over IPv4 tunnel.
- You manage a large, distributed network with IPv4 connectivity. To connect the distributed sites that use IPv6, you can run an automatic 6to4 tunnel from the edge router of each subnet.
- Sometimes, a router in your infrastructure cannot be upgraded to IPv6. In this case, you can manually create a tunnel over the IPv4 router, with two IPv6 routers as endpoints.

For procedures for configuring tunnels, refer to Chapter 5, “Administering IP Tunnels” in *Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle Solaris 11.3*. For more information about IP tunnel configuration, refer to “About the IP Tunnel Feature” in *Administering TCP/IP Networks, IPMP, and IP Tunnels in Oracle Solaris 11.3*.

Security Considerations for an IPv6 Implementation

When you introduce IPv6 into an existing network, you must take necessary precautions to ensure that you do not compromise the security of the site.

Be aware of the following security issues as you phase in your IPv6 implementation:

- The same amount of filtering is required for both IPv6 packets and IPv4 packets.
- IPv6 packets are often tunneled through a firewall.

  Therefore, you should implement either of the following scenarios:

  - Have the firewall perform content inspection inside the tunnel.
  - Put an IPv6 firewall with similar rules at the opposite tunnel endpoint.
- Some transition mechanisms that use IPv6 over User Datagram Protocol (UDP), and User Datagram Protocol (UDP) over IPv4 tunnels exist. These mechanisms might prove problematic by short-circuiting the firewall.
- IPv6 nodes are globally reachable from outside the enterprise network. If your security policy prohibits public access, you must establish stricter rules for the firewall. For example, consider configuring a *stateful firewall*.

Refer to the following documents for information about security features that you can use with an IPv6 implementation:

- IPsec enables you to provide cryptographic protection for IPv6 packets. For more information, refer to Chapter 8, “About IP Security Architecture” in *Securing the Network in Oracle Solaris 11.3*.
- IKE and IKEv2 automates keys management for IPsec. For more information, refer to Chapter 10, “About Internet Key Exchange” in *Securing the Network in Oracle Solaris 11.3*.

Index