Chapter 2

Planning a Network

This chapter contains common-sense approaches to planning the physical and logical aspects of your network environment. The information contained in this chapter should be read before you set up a new network or integrate into an existing network.

This chapter contains the following sections:

Planning the Physical Network

Planning the physical network requires that you first answer the question, "What network media and topology configuration would best suit the needs of my users?" A review of the MAC (Medium Access Control) level and application-level performance information about the products you are considering will help you determine the appropriate choice of media for your environment. In your review, consider the size (number of stations) of your network. Your network size will influence the media type and topology you choose for your network. If your network requires different types of media, determine whether you have the correct equipment for integrating the various media types.

The subsections that follow will help you answer this list of planning questions:

- What will my physical network look like?
- Do I have a map of my network?
- Will I need a repeater, bridge, router, or gateway?
- Will this network configuration meet my users' needs?
- Where are my performance bottlenecks? Can I reduce or avoid them?

Repeaters, Bridges, Routers, and Gateways

Your choice of media and the number of stations, networks, and protocols in your network may require the use of a repeater, bridge, router, or gateway. This section suggests the type of device required for certain network functions.

*repeate*r
: A device that regenerates and amplifies electrical signals. Its purpose is to extend the physical length of a network.

bridge
: A device that decodes MAC-layer frames transmitted between different hardware and media. Its purpose is to resolve network media differences; it allows a network to be composed of various media types (Ethernet, fiber, serial, and so on). It can also be used to segment similar media types.

router
: A device that decodes and passes network-layer packets between different networks. Its purpose is to provide the physical and logical route from one network to another.

gateway
: A device that translates protocols from one station to another. Its purpose is to allow stations with different networking protocols to communicate successfully.

Note: The terms *router* and *gateway* are sometimes used interchangeably. Be sure you know the function of the device you are considering, as the term may be technically inaccurate.

Note that each device may not be limited to a single function. For example, a gateway may also perform router functions if it is configured as a router. Table 2-1 summarizes the characteristics of each network device.

Table 2-1 Network Device Characteristics

Device Name	Media	Protocol	LAN	Purpose
repeater	same	same	same	extends physical length of the network
bridge	different/same	different/same	same/different	bridge network media differences
router	same/different	same	different	provides physical and logical route between networks
gateway	same/different	different	same/different	communication between stations with different networking protocols

Performance Planning

You can circumvent some performance bottlenecks with appropriate planning. These bottlenecks might occur as a result of your choice of media, topology, number of network devices, controller boards, or network design.

Choice of media

Be sure the capacity of the medium you have selected is adequate for the network size and data transmission type (large or small volumes of data, sporadic or steady traffic). For example, Ethernet has a range of capacities depending on the specific type of Ethernet cable used (10base5, 10base2, or 10baseT). Media type is also a factor in data degradation. For example, 10baseT is unshielded twisted pair and is more sensitive to environmental conditions than 10base5. This should be a consideration if you are planning a network for a manufacturing environment that produces a high degree of electrostatic discharge.

Number of devices

Network devices can cause degradation to the network performance. Use repeaters only when necessary. Each additional devices introduces additional resistance onto the network.

Choice of controller

Choose the most efficient controller for your media. For example, Silicon Graphics supplies a standard Ethernet controller. An optional Efast™ card handles more of the protocol processing in hardware and frees the station's CPU for other processing.

Design of network

Think about the design of your network before you begin setting it up. If possible, put departments that interact heavily on the same network to decrease router traffic. Use dedicated routers to handle heavy traffic between networks.

Wide Area Networks

In addition to the many options available for constructing local area networks, there are several different ways of connecting local area networks into wide area networks. These systems can be used to tie together local area networks at different locations, to allow users working at scattered locations to access a network, and to connect your network to the outside world. Figure 2-1 shows how different kinds of wide-area connections might fit into a large heterogeneous network.

Two of the available systems, Serial Line Internet Protocol (SLIP) and Point-to-Point Protocol (PPP), provide a way of transferring Internet Protocol (IP) packets over a serial telephone line; this means that SLIP and PPP users can access network resources much as it they were on the local area network. PPP can also be used with Integrated Services Digital Network (ISDN). ISDN uses a high-speed digital telephone line to achieve higher throughput than a modem connection.

Another system, UNIX to UNIX Copy Program (UUCP) is an older system, primarily designed for transferring information (such as network news and electronic mail) in batch mode over serial lines.

Higher-performance network connections can be made using specialized hardware. These connections are usually over dedicated lines, leased from a telephone company, or over the telephone company's packet-switched network.

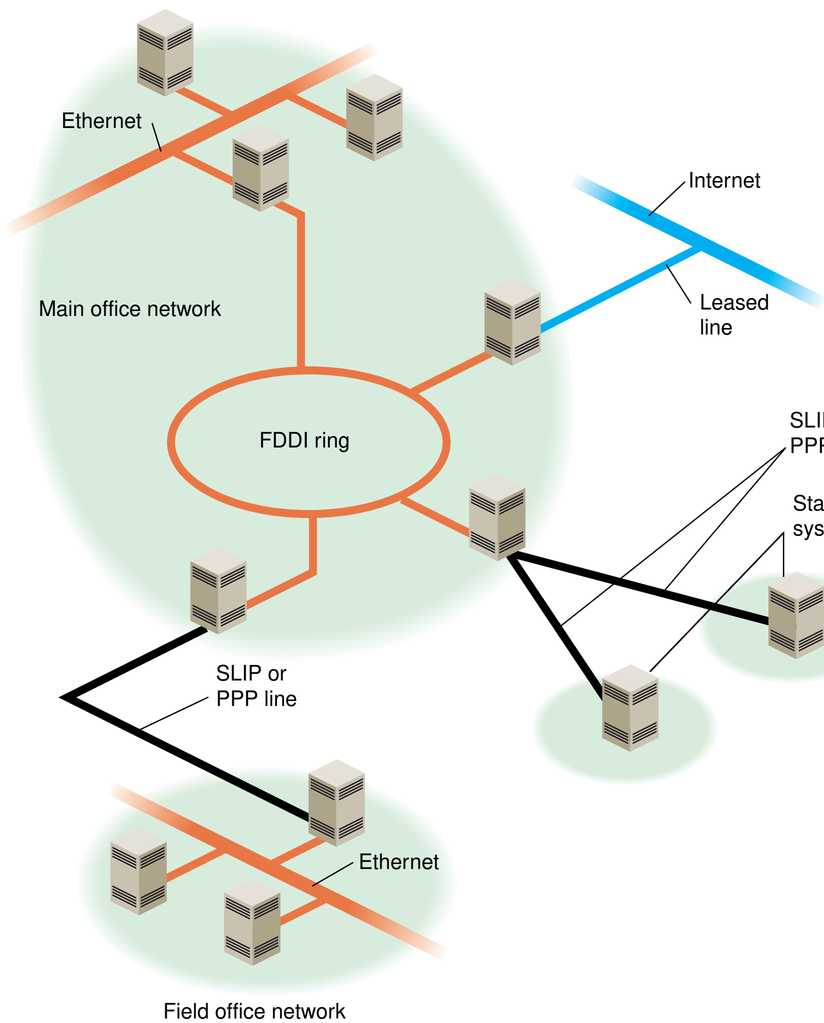

Figure 2-1 Heterogeneous Network With Wide-Area Connections

Serial Line Internet Protocol (SLIP)

SLIP provides simultaneous operation of multiple processes on a serial cable or telephone line. It allows network users the freedom to use TCP/IP based applications over a serial cable or modem connection.

You might consider setting up a SLIP network when cost and distance are large factors in your network planning.

Point to Point Protocol (PPP)

The Point to Point Protocol is similar in nature to SLIP. PPP provides a network connection as if your system were connected to the remote host by a LAN connection. Multiple processes and TCP/IP based applications are supported.

UNIX to UNIX Copy Program (UUCP)

UUCP, also called the Basic Networking Utilities, is a set of utilities that lets stations using a version of the UNIX operating system (such as IRIX) communicate with each other over serial lines. The utilities provided range from those used to copy files between computers to those used for remote login and command execution.

You may consider setting up UUCP for long-haul communications using modems and telephone lines. It is usually used to distribute electronic mail and network news.

Integrated Services Digital Network (ISDN)

ISDN is a system that connects systems using high-speed digital telephone lines. ISDN can achieve throughput up to 128 Kb per second, several times faster than normal modem connections. However, ISDN service can be expensive, and is not available in all areas. See the *ISDN User's Guide* for more information on ISDN.

High Performance Wide Area Networks

If you need higher performance than you can get using SLIP or PPP over a modem link or ISDN, there are several choices available to you. The choices include Frame Relay networking and leased line service, from 56K (56 Kb per second) to T1 (1.5 Mb per second) and T3 (up to 45 Mb per second). If you require this kind of service, you'll have to shop around, comparing the prices and services offered by local Internet service providers.

Internet Protocol Addresses

Each system on your network needs a unique Internet Protocol (IP) address for each of its network interfaces. The Internet Network Information Center (InterNIC) is responsible for assigning the network portion of an Internet address for each site. For example, if Company A applies for an Internet address, the InterNIC provides the network portion of the Internet address for the entire Company A site. A centralized organization within Company A is responsible for assigning and managing the station ID portion of the Internet address.

Internet addresses are maintained on each station or in a centralized network database such as NIS or BIND. See "Name-to-Address Mapping" on page 24 for a comparison of the different database types. Each station that wishes to communicate must have a valid Internet address registered in the appropriate database. The standard hosts name-address database on IRIX stations is the */etc/hosts* file.

The subsections that follow will help you answer this list of planning questions:

- How do I obtain a valid Internet address for my site?
- How do I obtain a domain name assigned for my site?
- Do I understand the purpose of the */etc/hosts* file?
- Do I have valid Internet addresses ready for all required stations?

Format of Internet Protocol (IP) addresses

An IP address is a 32-bit number that network software uses to identify a system on a network. For the sake of human readability, these addresses are usually represented as four one-byte integers, separated by dots (for example, 150.166.248.17). Every system on an IP network must have its own unique IP address for the network to function properly. Systems with more than one network interface must have a unique IP address for each interface.

Note: Unlike a system's Ethernet address, a system's IP address is determined by the network and network system administrators.

Conceptually, each 32-bit IP address is a pair of numbers where one number represents the network and the other the system itself. There are four classes of addresses in use (A through D). The class of address is determined by the first bits of the address:

- Class A addresses begin with 0 and have 7 bits for the network number and 24 bits for the host number.
- Class B addresses begin with 10 and have 14 bits for the network number and 16 bits for the host number.
- Class C addresses begin with 110 and have 21 bits for the network number and 8 bits for the host number.
- Class D addresses begin with 1110 and are special "multicast" addresses for use within a network site.

In all cases, host numbers 0 and 255 are reserved, and may not be used for actual systems.

Figure 2-2 shows the format of the different classes of Internet addresses.

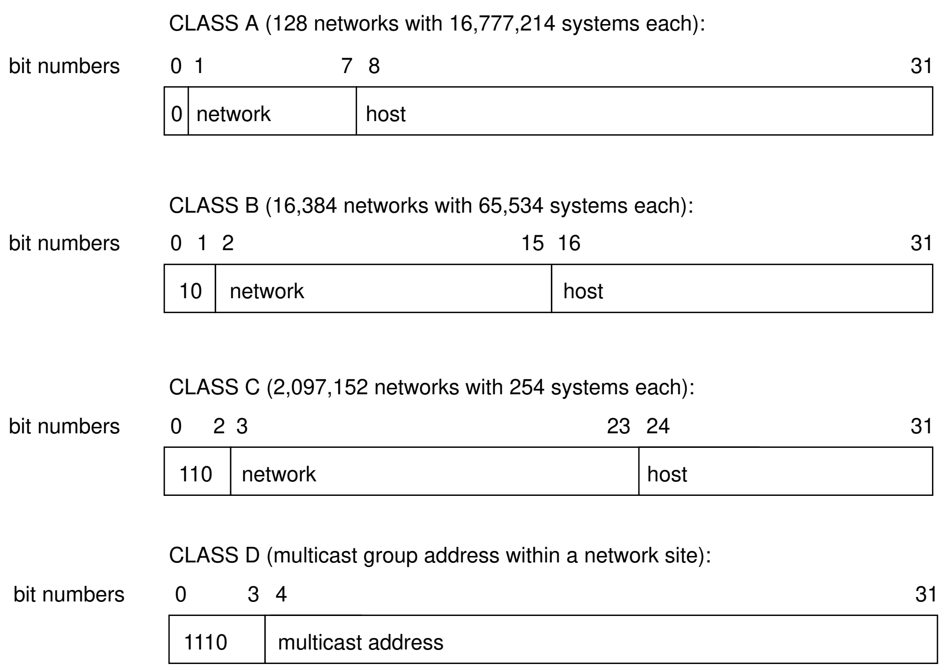

Figure 2-2 The Format of Internet Protocol (IP) Addresses

To simplify Internet addressing, dotted decimal notation is used to break the 32-bit number into four decimal numbers separated by dots.

For example, the IP address 128.74.41.123 in binary is:

```
10000000| 01001010| 00101001| 01111011
```

or

```
128 | 74 | 41 | 123
```

Class A, B and C IP addresses in dot notation conform to the following specifications:

`Class A -- 001.`*hhh.hhh.hhh* `through 126.`*hhh.hhh.hhh*

`Class B -- 128.001.`*hhh.hhh* `through 191.254.`*hhh.hhh*

`Class C -- 192.000.001.`*hhh* `through 223.255.254.`*hhh*

Note: *hhh* is the local system and the leading numbers are the network.

Networks are usually identified by *network numbers*—IP addresses in which the host portion is not specified. For example, 150.166 represents a Class B network, and 192.26.80 represents a Class C network.

If your network will be connected to the Internet, then you must obtain a unique network number, as described in "Obtaining a Network Number" on page 15. All the systems on your network must have IP addresses allocated from your network.

If you are adding a machine to an existing network, its IP address must be allocated from that network.

Obtaining a Network Number

You should obtain an Internet network number before you begin setting up your network.The allocation of network numbers is managed by a set of organizations called Network Information Centers (NICs). If your network is going to be isolated, and will never be attached to the Internet, you can theoretically use any addresses you like. However, if your network is ever going to be attached to the Internet, you should obtain a valid network number. Before you request the network number, you should determine the current needs of your organization (how many systems do you currently have that should be on the network?) and expected growth over the next five years.

There are several ways to obtain a network number. In many cases the best option, if you are connecting to the Internet through an Internet service provider, is to have the service provider assign you a portion of the address space they have been allocated by the local NIC.

The InterNIC recommends that you request a network number from your network service provider. If they cannot supply one, contact your provider's provider. As a last resort, contact your Network Information Center. See "Contacting Your Local Network Information Center" on page 19.

NIC Required Information

To request an Internet network address, you will typically need to supply the following information to the local NIC:

- Your administrative point of contact (POC). The administrative POC is the person responsible for answering administrative and policy questions about the network. You need to know his/her name, title, mailing address, and phone number.
- Your technical point of contact (POC). The technical POC is responsible for the technical support of the network. You need to know his/her name, title, mailing address, and phone number.
- Organization name and postal address.
- Your network name (up to 12 characters).
- Your network's geographic location and organization name.
- The name and location of the network document plan.
- Gateway information (connectivity, hardware, software, address).
- The approximate size of your network (number of hosts and subnets), initially and within one year.
- Type of network (research, educational, government non-defense, commercial).

If you already have one or more network numbers assigned to your organization, the NIC ,may require you to provide information on how these are being used, as evidence that you really need a new network number.

If you request 16 or more Class C network numbers, the InterNIC requires you to provide information on network topology, and if you request 256 or more Class C network numbers or a Class B network number, the InterNIC requires you to provide a diagram of the proposed network.

Domain Names

If you're planning on putting your site on the Internet or exchanging e-mail with sites on the Internet, you should register a domain name with your local NIC. A domain name uniquely identifies your organization. For example, Silicon Graphics has the domain name "sgi.com."

The Internet uses Domain Name Service (DNS) to map domain names to IP addresses. Therefore, even if you don't use DNS internally, you must provide DNS name servers on the Internet in order to connect your network to the Internet. You should have at least two name servers, a primary and a secondary server. For robustness, the secondary server should not be connected to the Internet through the same gateway as the primary server. Since many organizations are not big enough to have multiple gateways to the Internet, a common solution is to make a reciprocal arrangement with another organization to provide secondary name service for each other.

If you are connecting to the Internet through an Internet service provider, they may be able to provide name service for your organization, or help you locate someone to provide secondary name service if you are able to provide a primary name server.

Obtaining a Domain Name

As with network numbers, the registration of domain names is administered by the Network Information Centers. In some cases, there is a fee associated with holding a domain name. For example, the InterNIC currently charges a fee of $100 for the first two years, and $50 a year thereafter for domains under its jurisdiction.

You can register your domain name through your local NIC. See "Contacting Your Local Network Information Center" on page 19 for contact information. When you register a domain, you should also register a *reverse domain*, also known as an *IN-ADDR* domain. The reverse domain provides a mapping from IP addresses to domain names.

In many cases, Internet service providers will register your domain for you, for a fee.

Subdomains

Once you have a domain name registered, you're free to establish subdomains of your own. This is particularly useful for large organizations that use the Domain Name

Service (DNS). The use of subdomains with DNS allows some administrative chores to be decentralized.

For example, suppose “salad.com” has branch offices in Gilroy and Paris. These could be established as subdomains, “gilroy.salad.com,” and “paris.salad.com.”

The Internet

Chances are, you will want to connect your system or network to the Internet. Wherever you may be, there is likely an Internet gateway available within your local calling range. The following sections offer some information that should help you get set up and running. Obviously, each situation is somewhat different, and your local service provider will have variations in service and equipment. Some research and experimentation is usually required before everything works smoothly.

Before Connecting to the Internet

Before you sign up for an internet connection, consider what level of service you need. For example, if you are an individual looking for basic e-mail, news, and file transfer capabilities, it probably wouldn't make sense to install a dedicated network cable in your home for economic reasons. A better choice for single-user access might be to subscribe to a network provider who establishes an account for you on their system (one that is currently connected to Internet). Typically, access to their system is through a modem connection.

If you are trying to establish a connection to the Internet for a corporation, you will likely need the bandwidth of a leased line, and all the required hardware that goes with it. You will have to take into consideration the many administrative issues of running a site. These issues include, but are not limited to

- cost analyses/budget
- establishing a domain
- applying for IP addresses
- establishing site policy
- establishing site security

- administration of network services (such as Domain Name Services, NIS, e-mail, and so on)

There are providers of network connectivity that can provide varying levels of service. You must investigate the providers, and decide who provides the level of service you need, at the appropriate cost.

If you choose an individual account on a provider's machine, the service provider deals with most, if not all, of the administrative tasks, and you simply enjoy access to the Internet.

If you would like a broader range of services, most providers will set you up with a dedicated modem and phone line for your exclusive use, or they can provide a network-only service (using SLIP, PPP, or UUCP), either through modems or other network connections.

Connecting your network to the Internet requires a number of steps, including arranging name servers, obtaining a network number, and registering a domain name for your organization. Many Internet service providers are willing to provide these services for a fee.

If you are trying to set up internet access for a company, or corporation, you should research the issues listed above. Based on the information you obtain, formulate a plan for your site based on the needs and expectations of your organization. One of the best sources of information is the Internet itself. You should first obtain an individual account from a local provider. With the individual account, you can gain access to a large amount of information pertaining to establishing a site on the Internet.

Contacting Your Local Network Information Center

Before you connect your site to the Internet, you'll need to contact your local Network Information Center. The assignment of network numbers and domain names is coordinated by the Network Information Centers. There are three main regional Network Information Centers, as shown in Table 2-2.

Table 2-2 Network Information Centers

Region	Organization
Asia/Pacific	Asia Pacific Network Information Center (APNIC)
Europe	Réseaux IP Européens Network Coordination Centre (RIPE NCC)
Americas	Internet Network Information Center (InterNIC)
other areas	InterNIC

Procedures for obtaining IP addresses and registering domain names vary, so contact your local NIC for information.

Internet Network Information Center

The Internet Network Information Center (InterNIC) was formerly the sole Network Information Center. It serves as the primary NIC for most of North and South America, as well as for other regions that do not yet have NICs of their own. InterNIC maintains a large archive of informational documents, which can be accessed using WWW, FTP, or by e-mail to an automated-response mail server. Registration authority for some countries (including Canada and Brazil) is delegated to national NICs. Contact information for the national NICs may be obtained through InterNIC.

Network Solutions
Attn: InterNIC Registration Services
505 Huntmar Park Drive
Herndon, VA 22070
Phone: 1-800-444-4345 or 1-703-742-4777
E-mail: question@internic.net (general inquiries)
E-mail: hostmaster@internic.net (registration services)
WWW: http://www.internic.net/
FTP: ftp.ds.internic.net (complete RFCs, and so on)
FTP: rs.internic.net (registration information)
E-mail server: mailserv@rs.internic.net (send message with subject line “HELP”)

Réseaux IP Européens

Réseaux IP Européens (RIPE) maintains an NIC that provides registration services for European sites. It also maintains a store of informational documents, including the InterNIC's FYI documents, and instructions on how to register a host or network in one of the European domains.

RIPE Network Coordination Centre
Kruislaan 409
NL-1098 SJ Amsterdam
The Netherlands
Phone: +31 20 592 5065
Fax: +31 20 592 5090
E-mail: ncc@ripe.net
WWW: http://www.ripe.net/
FTP: ftp.ripe.net

Asia Pacific Network Information Center

The Asia Pacific Network Information Center (APNIC) coordinates network information for the Asia and Pacific region. Registration authority for some countries is delegated to national NICs. Contact information for the national NICs may be obtained through APNIC.

Asia Pacific Network Information Center
c/o United Nations University
53-70 Jingumae 5-chome
Shibuya-ku, Tokyo 150
Japan
Phone: +81-3-5467-7014
Fax: +81-3-5276-6239
E-mail: info@apnic.net
WWW: http://www.apnic.net/
FTP: archive.apnic.net

Online Information Sources

With an individual account or other access to the Internet, you can get the information you need to provide access to your own site.

Usually, the provider of an individual account will also provide new-user documentation that describes the basics of using the Internet. You can use the World Wide Web (WWW) and the File Transfer Protocol (FTP) to access a wealth of information on many subjects, including Internet connectivity. If you don't know how to use FTP, see "Retrieving Files With Anonymous FTP" on page 23 for a short tutorial. How you access the Web depends on what Web browser you're using. Most Web browsers have online help available.

Network Information Centers

Your local NIC maintains archives of useful information on connecting to the Internet. In addition to information about requesting network numbers and registering domain names, they may have lists of local service providers. Most NICs make this information available by WWW and FTP. See "Contacting Your Local Network Information Center" on page 19 for WWW and FTP addresses for the major NICs.

The InterNIC has produced a series of information bulletins called FYIs. Especially notable is FYI 16, entitled *Connecting to the Internet -—What Connecting Institutions Should Anticipate*. While this is aimed primarily at U.S. educational institutions, it remains one of the better pieces of documentation on establishing a site on the Internet. The FYI documents are available by WWW and FTP from the InterNIC and from RIPE.

The Internet Society

The Internet Society is a non-governmental international organization for global cooperation and coordination of the Internet. They also provide useful online information—in particular, information on finding an Internet service provider, and a list of network service providers around the world. This information is available by WWW. A subset is available by anonymous FTP.

WWW: http://www.isoc.org/
FTP: ftp.isoc.org

Retrieving Files With Anonymous FTP

Anonymous FTP is a conventional way of allowing you to sign onto a computer on the Internet in order to obtain copies of files that are made available to the public. Some sites offer anonymous FTP accounts to distribute software and various kinds of information. If you have never used *ftp*, here is a brief summary on how to use the *ftp* command. To connect to a remote host, specify the hostname on the command line:

```
ftp ftp.ds.internic.net
```

When ftp connects with the remote system, it prompts you for a login name. Use the login name “anonymous”:

```
Connected to ftp.ds.internic.net.
Name (ftp.ds.internic.net:guest): anonymous
331 Guest login ok, send ident as password.
Password:
```

Many systems allow any password and request that the password you choose is your user ID. If this fails, the generic password is usually “guest.”

```
230 Guest login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Once connected and logged in, you can use *ftp*’s *cd* and *ls* commands to look at the files available on the remote system. To obtain a file from the remote system, use the *get* command. The *get* command copies one file from the remote system to your local system. To obtain multiple files from the remote system, use the *mget* command.

```
ftp> cd fyi
250 CWD command successful.
ftp> get fyi6.txt
local: fyi6.txt remote: fyi6.txt
200 PORT command successful.
150 Opening BINARY mode data connection for fyi6.txt (3459 bytes).
226 Transfer complete.
3459 bytes received in 0.46 seconds (7.34 Kbytes/s)
ftp>
```

Name-to-Address Mapping

Because IP addresses are difficult to remember, they are usually associated with names. In the case of a machine with a single IP address, this name *usually* consists of the machine's hostname and domain name. For example, a machine called "fruit" in the domain "salad.com" would usually be referred to as "fruit.salad.com". For clarity, this type of name will be referred to in this section as a *network connection name*.

Because network connection names usually correspond to the machine's hostname, these network connection names are commonly referred to as "hostnames," but this can be misleading. The actual hostname is defined in the */etc/sys_id* file. By default, this hostname is used as the network connection name for the machine's primary network interface, but this behavior is configurable. A machine with multiple network interfaces has multiple network connection names associated with it. By convention, each of these connection names contains the hostname—for example, if the host "fruit" acts as a gateway between two networks in the "salad.com" domain, it might use these names:

```
fruit.salad.com
gate-fruit.salad.com
```

The process of mapping network connection names to IP addresses is commonly called *hostname resolution*. There are several different systems for hostname resolution. Machines can use a local database (the */etc/hosts* database), or they can obtain information from servers on the network, using either the Network Information Service (NIS) or the Domain Name System (DNS). The following sections describe the advantages and drawbacks of the different systems:

- "The /etc/hosts database" on page 24
- "Domain Name System" on page 25
- "Network Information Service (NIS)" on page 25

The /etc/hosts database

The */etc/hosts* database is an ASCII file that you can modify with any text editor. The file contains lines of text that specify IP addresses and network connection names.

For a small network of stations under the same administrative control, maintaining a consistent */etc/hosts* database is straightforward. Establish a master copy on one station and make additions or deletions from its file. Then use *rcp*(1C) or *rdist*(1C) to copy the file to the other stations in the network.

Maintaining consistent versions of */etc/hosts* on every station in a large network is troublesome. NIS and the BIND name server both make maintenance easier by providing a centralized version of the host database.

Domain Name System

The Internet uses the Domain Name System (DNS) to map names to IP addresses. The most common implementation of a DNS name server is called Berkeley Internet Name Domain (BIND). If your network interfaces with the Internet, you must have at least two DNS name servers, a primary and a secondary server. Your Internet service provider may be able to take care of this requirement for you.

BIND is best suited for large networks, or networks connected directly or indirectly to the Internet. BIND provides access to a much larger set of stations than is provided in the */etc/hosts* database. A drawback of BIND is its complicated setup. BIND is described in more detail in Chapter 6, “BIND Name Server”

Network Information Service (NIS)

NIS is a network-based information service and an administrative tool. It allows centralized database administration and a distributed lookup service. NIS supports multiple databases based on regular text files. For example, NIS databases can be generated from the *hosts*, *passwd*, *group*, and *aliases* files on the NIS master.

NIS is best suited for a moderate-sized network (one containing approximately 1000 stations, or a small collection of interconnected networks). NIS is part of the NFS optional software and is detailed in the *NIS Administration Guide*.

Planning to Subnet Local Networks

Subnetting allows you to divide a single network into a set of subnetworks. Subnetworks are useful for many reasons. For example, if you have a satellite office that connects to your main network, it should have its own network number or subnet. If you have a large number of systems to be connected by Ethernet, you may have to use subnets to overcome physical limitations on the number of hosts and length of network cable that can be supported on a single Ethernet network.

Subnetting should be considered when the class limits are unrealistic for your network. For example, a Class B network gives you approximately 64,000 stations per network. This far exceeds the maximum number of stations allowed on most networks. Subnetting allows the local organization to designate some of the host ID bits to form a subnet. Subnetting generates a realistic number of stations per network. All changes are made at the local site by the site administration group and are transparent to off-site stations.

Planning is required for subnetting a network (see “Subnetting a Network” on page 45 for subnetting procedure). Primarily, you must determine how to partition the host part of the 32-bit Internet address. To define local subnetworks, use bits from the host number sequence to extend the network portion of the Internet address. This reinterpretation of IP addresses is done only for local networks. It is not visible to off-site stations.You should have at least a rough idea of the physical layout of the network before you plan your subnets. For example, you might want to have a subnet for each floor of your building. If you have a branch office that’s connected to your main network, you might want to set aside one or more subnets for it. In some cases, you may want to set aside a subnet for SLIP and PPP clients (see “SLIP and PPP Routing and Address Allocation” on page 90).

Sites with a Class A network number have 24 bits of host part with which to work; sites with a Class B network number, 16 bits; and sites with a Class C network number, 8 bits. For example, if your site has a Class B network number, each station on the network has an Internet address that contains 16 bits for the network number and 16 bits for the host number. To define 254 local subnetworks, each possessing at most 254 stations, you can use 8 bits from the host portion of the address. Construct new network numbers by concatenating the original 16-bit network number with the extra 8 bits containing the local subnetwork number.

Figure 2-3 shows what happens to the bit assignments in a Class B Internet address that is subnetted.

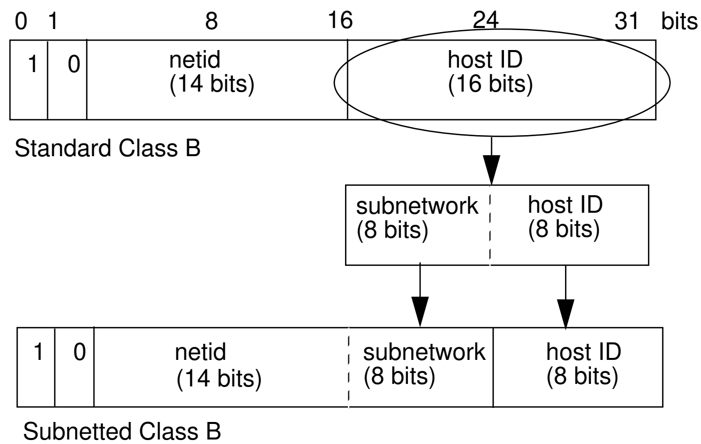

Figure 2-3 Subnetted Class B Address

For example, the Class B Internet address for an entire site as seen from other sites might be 128.50. If subnetting is enabled within the site, the site might be composed of several subnets with network IDs like 128.50.20, 128.50.21, 128.50.22, and so on. A station that resides on the subnet 128.50.21 might have the Internet address 128.50.21.5.

Note: The numbers 0 and 1 are reserved for broadcast addresses. Do not use subnetwork numbers with all 0s or all 1s.

Allocating IP Addresses

Once you have obtained a network number, decided which system to use for hostname resolution, and decided whether you're going to subnet the network, you're ready to allocate IP addresses for individual systems. For most systems, this is as simple as assigning an unused IP address from the correct net or subnet. If you use the syntax of the /etc/hosts file, this will look something like this:

```
150.26.80.1    green.salad.com green
150.26.80.2    tossed.salad.com tossed
150.26.80.3    jello.salad.com jello
```

Note: Host numbers 0 and 255 are reserved, and shouldn't be used.

Systems with more than one network interface may be connected to more than one subnet, and require one address for each connected interface. Each interface should be assigned an address from the subnet that the interface is connected to. For example, if fruit.salad.com acts as a gateway between the 150.26.80 net and the 150.26.42 net, it might have the following entries:

```
150.26.80.19   fruit.salad.com fruit
150.26.42.1    gate-fruit.salad.com gate-fruit
```

Even if you're planning on using NIS or BIND for hostname resolution, you will probably want to put together an */etc/hosts* file. If you install this on your systems as you attach them to the network, you'll be able to communicate while you get NIS or BIND up and running.

You should also establish some policy for allocating IP addresses for new systems once the network is in place. If your organization is large, you might want to delegate this authority to separate organizational units. For example, the branch office with its own subnet should allocate IP addresses as needed from its subnet. If your organization is divided up into subdomains, you might want to assign authority over certain subnets to subdomain administrators.

Planning for Network Security

Securing a network is difficult. If you can discourage potential intruders and quickly isolate or pinpoint successful intruders, you can consider your network secure. You should establish a plan for keeping your network secure before you connect your network to the Internet. For information on network security, see Chapter 5, "Network Security," in IRIX Admin: Backup, Security, and Accounting.

Using Common Network Applications

This guide is written specifically to support the standard network hardware and software—Internet protocols over Ethernet. However, when discussing networking in general, it is difficult to ignore network applications that are not standard, but are common to most network environments. This section presents a brief overview of some of the common network applications that you should consider when planning your network.

Electronic Mail

Electronic mail is a group of programs (*sendmail*) used to send and receive messages to and from users on the same local station or between remote stations. Mail can be sent using UUCP or TCP/IP protocols. IRIX supports both System V (*/bin/mail)* and 4.3BSD (*/usr/sbin/Mail*) mail programs, as well as *MediaMail*, which provides a graphical interface for electronic mail.

Network File System (NFS)

NFS is a network program that can access a remote station's filesystem and attach it and its data to the local station's filesystem. On the local station, the remote filesystem is accessed as if it were local.

NFS should be considered in a network when you want to share files between stations. With NFS, software or data used by a group is put on an NFS server. Authorized NFS clients access the data over the network when needed. This approach ensures consistent information, frees up disk space on client stations, and simplifies the backup procedure. NFS is an optional software product and is described in the *ONC3/NFS Administrator's Guide*.