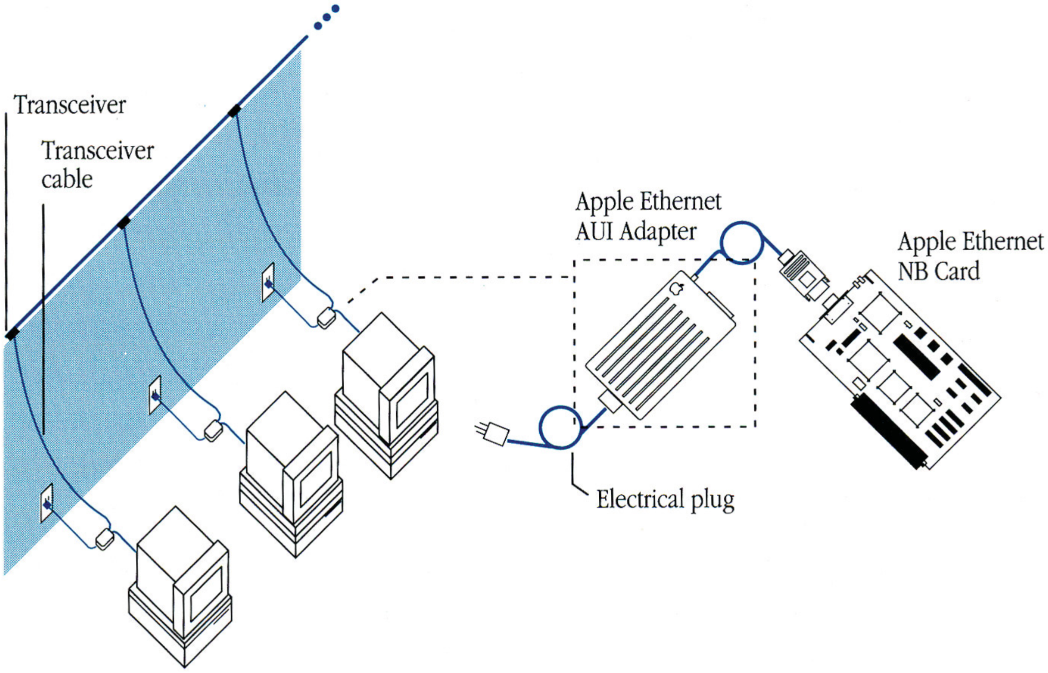
## *Thick coax and other cable systems for Ethernet*

The Apple Ethernet AUI Adapter enables you to connect a device equipped with an Apple Ethernet port to standard Ethernet transceivers for thick coax, fiber-optic, and other Ethernet media types. The AUI Adapter will work with external transceivers from all companies following the 802.3 AUI (Attachment Unit Interface) specification.

***Ethernet cable system for fiber-optic and thick coax***



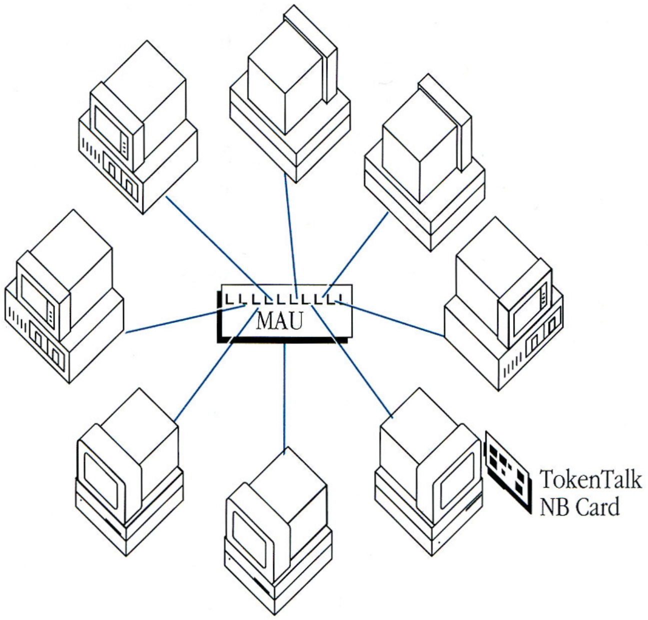
# AppleTalk over Token Ring: TokenTalk

A TokenTalk network transmits AppleTalk protocols over industry-standard (IEEE 802.5) **Token Ring** networks. The growing popularity of Token Ring is the result of its compatibility with standard cabling installations and its role in IBM's Systems Application Architecture (SAA), making it ideal for large business installations.

Providing transmission rates of either 4 megabits per second (Mbps) or 16 Mbps, Token Ring can use either shielded twisted-pair cable or unshielded twisted-pair cable. A single network can connect up to 260 devices.

Each device on a Token Ring network is connected to a MAU that is usually located in a wiring closet. A typical MAU provides eight ports for connecting network devices. As your network grows, you can add MAUs to support more devices.

You need TokenTalk software and a Token Ring interface card for each computer that you want to attach to the network. To connect members of the Macintosh II family of computers to Token Ring networks that operate at 4 Mbps, Apple provides the TokenTalk NB Card. This card connects to IBM Type 1 cable (shielded twisted-pair). Other vendors provide media filters for attaching to IBM Type 3 cable (unshielded twisted-pair). You may also purchase interface cards from other companies that allow you to connect a Macintosh SE or SE/30 to a Token Ring network.



## Conclusion

In this chapter, you've learned about the different network types that are supported by the AppleTalk network system—LocalTalk, Ethernet, and Token Ring. These network types target the needs of varying network environments. The following table enables you to compare the features of these network types. Note that AppleTalk protocols can also operate on other types of networks, such as ARCnet, LANSTAR, and IBM baseband networks. For more information on these additional network types, refer to the sources listed in the Appendix.

**Table 6-1** A comparison of network types

| | **Medium** | **Transmission rate** | **Topology** | **Maximum number of devices** | **Maximum length** | **Ease of installation** |
|---|---|---|---|---|---|---|
| *LocalTalk* | Shielded twisted-pair | 230.4 Kbps | Bus | 32 | 1000 ft. | Easy |
| | Unshielded twisted-pair (phone wire) | 230.4 Kbps | Bus<br>Passive star | 20–40<br>Varies | 2000 ft.<br>4000 ft. (sum of branches) | Easy<br>Requires installer |
| | | | Active star | 254 | 3000 ft./branch | Requires installer |
| | Infrared light | 230.4 Kbps | NA | 128 per transceiver | Transceivers must be within 70-ft. diameter | Easy |
| *Ethernet* | Thick coaxial | 10 Mbps | Bus | 100/segment<br>1024/network | 8250 ft. | Requires installer |
| | Thin coaxial | 10 Mbps | Bus | 40/segment<br>1024/network | 3300 ft. | Easy with Apple Ethernet product |
| | Twisted-pair | 10 Mbps | Star | 1024 | 330 ft. from hub to device | Requires installer |
| | Fiber optic | 10 Mbps | Bus | 1024 | 14,256 ft. | Requires installer |
| *Token Ring* | Shielded twisted-pair | 4 /16 Mbps | Star-wired ring | 260/ring | 990 ft. from MAU to device | Usually requires installer |
| | Unshielded twisted-pair | 4 /16 Mbps | Star-wired ring | 72/ring | 330 ft. from MAU to device | Usually requires installer |

# Extending and connecting networks

When designing your network, you may find that you need to extend a single network or divide the network into two or more connected *subnetworks.* Connection devices such as repeaters, bridges, routers, and gateways (discussed fully in the next section) extend networks or provide the link between individual networks, enabling many users to communicate and share resources with one another.

The following situations commonly call for extending or connecting networks:

- *Enlarging a network that has reached its maximum length or number of devices.* If you've reached the specified device or cable length limits of a network, you may need to extend the network. For example, if you're using LocalTalk cable and need to extend the cable beyond the specified 1000-foot limit, you would need to use a connection device.
- *Linking two or more existing networks in your organization.* It's not unusual for networks to be installed in an organization for different reasons and at different times. The result? Separate networks that don't communicate. Connection devices can link these networks together, allowing users on each network to access network services on the entire internet.
- *Connecting different network types or networks using different protocols.* A common reason for connecting networks is to link different network types, such as LocalTalk and Ethernet, each using different connection methods and transmission media. Or you may need to link your AppleTalk network to a network running an entirely different set of protocols, such as DECnet or TCP/IP.
- *Maintaining a satisfactory level of network performance.* In a high-traffic network, performance can be increased significantly by dividing the network into subnetworks, each with a low demand for the resources of another subnetwork. A logical way to divide an existing network is along natural divisions within the organization. For example, networks are commonly divided by department or by groups that have shared requirements. By partitioning the network into largely self-contained subnetworks, you can minimize the amount of traffic flowing between them and maintain higher levels of performance on each subnetwork.

- *Isolating a single group generating high traffic.* When one group of users generates a large amount of network traffic, performance may decline on the entire network. For example, several users performing frequent, high-volume printing and file sharing can cause network congestion for all other users on the same network.

  When designing your network layout, you can plan for such high-traffic groups ahead of time by isolating these users in a network of their own. If your network is already in place, you can use the same traffic-isolation technique, dividing one large network into two smaller networks.
- *Accommodating different user requirements.* If users' needs for network resources vary greatly, you may want to consider creating two networks linked by a connection device. In this way, the special interests of each group may be better satisfied.
- *Restricting access to sensitive information.* You may decide that sensitive or important information—such as product development plans or personnel files—can be better safeguarded and supervised by placing the information in a separate network. Even though users in other networks can access devices on the "secure" network, you can set up certain servers that have restricted access.
- *Creating zones for efficient network organization.* **Zones** are logical divisions within an internet that enable an administrator to balance the number of network services presented to users. See "Dividing Your Internet Into Zones" later in this chapter for a discussion of zones.

## Which connection device do you need?

Four kinds of devices are used to extend or connect networks:

- repeaters
- bridges
- routers
- gateways

The device you choose depends on what kind of connection services you need, as described in the following sections.

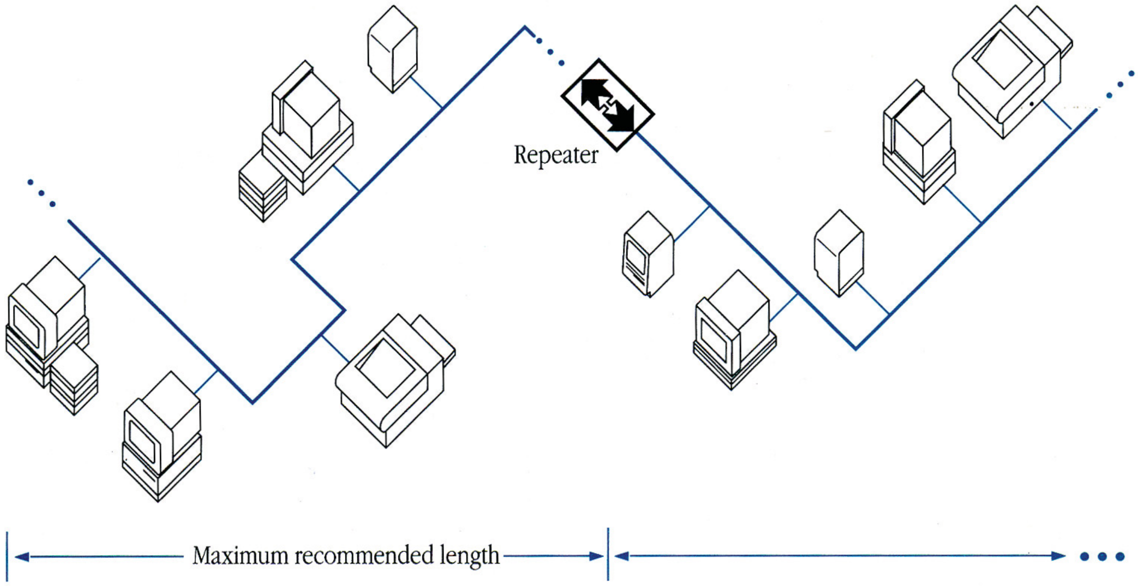
## Repeaters

A **repeater** is a piece of hardware about the size of a modem. It is commonly used to add another length of cable to a network, extending the cable beyond its recommended maximum length. As a transmission signal travels through the network cable, the signal becomes weakened. The repeater amplifies and retransmits this signal, effectively enabling it to travel beyond the normal limitations of the cable.

A repeater can be very helpful if, for example, you have a few users on a LocalTalk network whose offices are isolated from the rest of their group, requiring a total cable length greater than the 1000 feet allowed by LocalTalk. The repeater enables you to connect those users to the network rather than creating another, separate, network.

You can also use a repeater to add devices to a network cable; however, there are two important points to keep in mind. One, repeaters *do not isolate traffic.* When you add a repeater to your network, the result is one larger network. The traffic that results from adding more devices can quickly degrade performance on the entire network. Two, be aware of the recommended device limitations of each network type. It would be unwise, for example, to use a repeater to go well beyond the 32-device limitation of LocalTalk (using the LocalTalk cable system), since performance would rapidly suffer. However, if you're using Ethernet, which can accommodate a large number of devices, a repeater may be a good choice for adding more devices.

***Repeaters*** *enable a cable to be extended beyond its recommended length.*



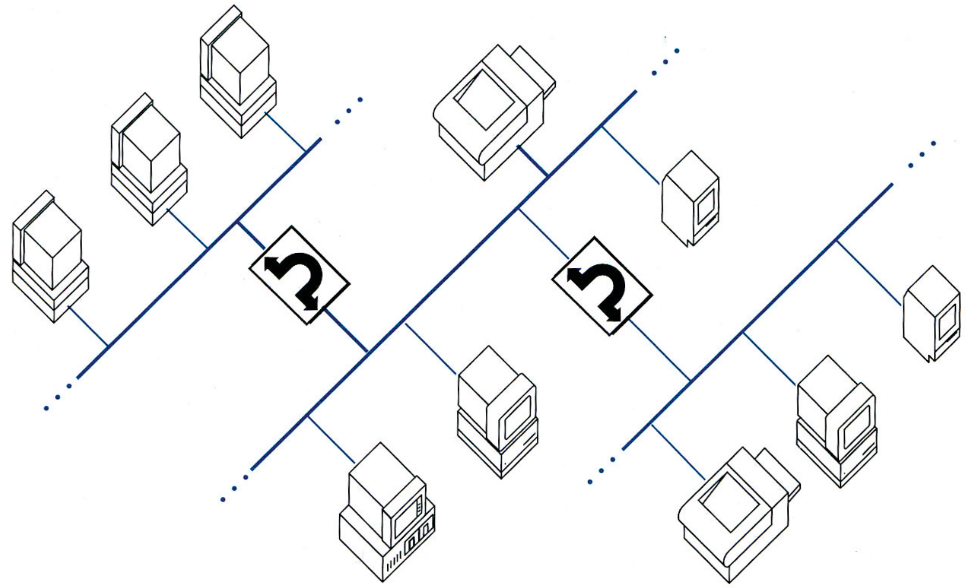
## Bridges

A **bridge** can be used to join two networks of the same network type (such as two Ethernet networks or two Token Ring networks). The networks can use different types of media, such as fiber-optic or coaxial cable. Note that there are currently no bridges available to connect LocalTalk networks; routers are used instead (see the next section for a discussion of routers).

Unlike a repeater, which simply retransmits all data onto the connected cable segment, bridges can interpret data addresses. This means that bridges can *isolate* traffic on each network, sending only those packets across the bridge specifically destined for the other network. (Note that bridges do not typically isolate **broadcast traffic,** which results from such activities as using the Chooser.)

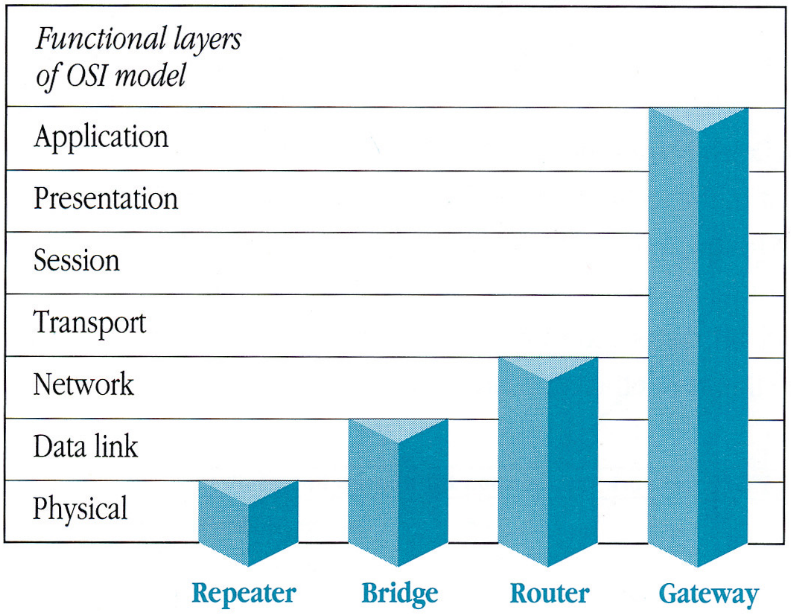
Bridges can be dedicated, self-contained devices or computers running appropriate bridging software. Because the networks connected by a bridge are not identified by network numbers or zone names (unlike routers), installing and administering a bridge is usually quite easy. Bridges provide administrators with information about network activity levels and error statistics, which are helpful in monitoring the network.

***Bridges** are used to connect networks together. Devices see the previously separate networks as one single, larger network.*



### *Connection devices and the OSI model*

Connection devices perform network functions that involve different layers in the hierarchical OSI model. In this hierarchy, as you may recall from Chapter 2, each layer represents a separate level of network function. Network connection devices perform functions that may involve one or more of these layers. For example, repeaters—very simple hardware devices—make use of the protocols in just the physical layer, whereas gateways—sophisticated translators between different protocol architectures—use the greatest range of networking protocols.



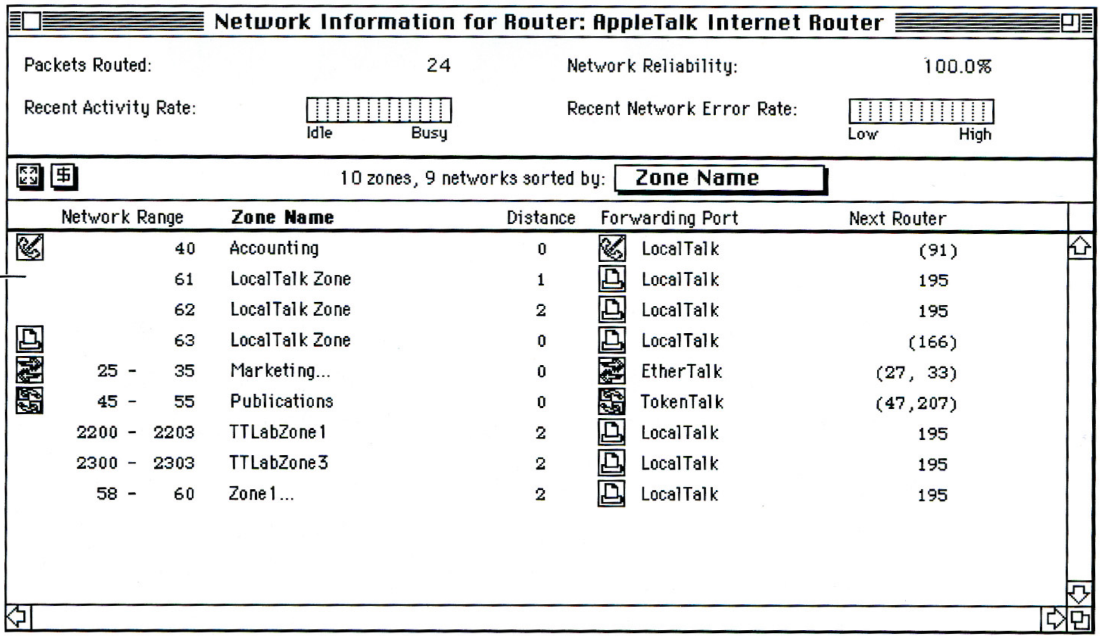
## Routers

**Routers** can connect networks of the same network type (such as two LocalTalk networks) or of different network types (such as an Ethernet network and a Token Ring network). Routers enable the connected networks to retain separate identities with their own unique network numbers, and they can selectively route data along the most efficient path possible. This ensures faster traffic flow and can automatically provide for detours if a connection is broken along the path.

Routers are often used to isolate areas of high traffic from lower-traffic areas for optimum network performance. They also enable you to partition an internet into zones, which make it easier for users to locate and access network services. In addition, routers (like bridges) provide administrators with information about network activity levels and error statistics, which are helpful in monitoring the network.

Routers can be hardware- or software-based. A hardware-based router is a dedicated box whose only function is routing. It is generally a self-contained device, without a monitor or keyboard, designed to be used only as a router. A software-based router operates on a general-purpose computer such as a Macintosh. It can be used as either a dedicated or nondedicated router, depending on the level of performance your network requires. A dedicated router is a computer which, when running routing software, is used for no other purpose. A nondedicated router operates on a computer that can be used concurrently for other network services as well. If your router is sending large amounts of traffic to other networks or if you need the highest possible performance from your router, a dedicated router is the better choice.

Each router on an internet maintains a **routing table** (shown in the following figure) that lists all networks and routers in the internet. The routing table enables routers to determine the most efficient route for each packet of data.



Routing table information

Network Information for Router: AppleTalk Internet Router

Packets Routed: 24

Network Reliability: 100.0%

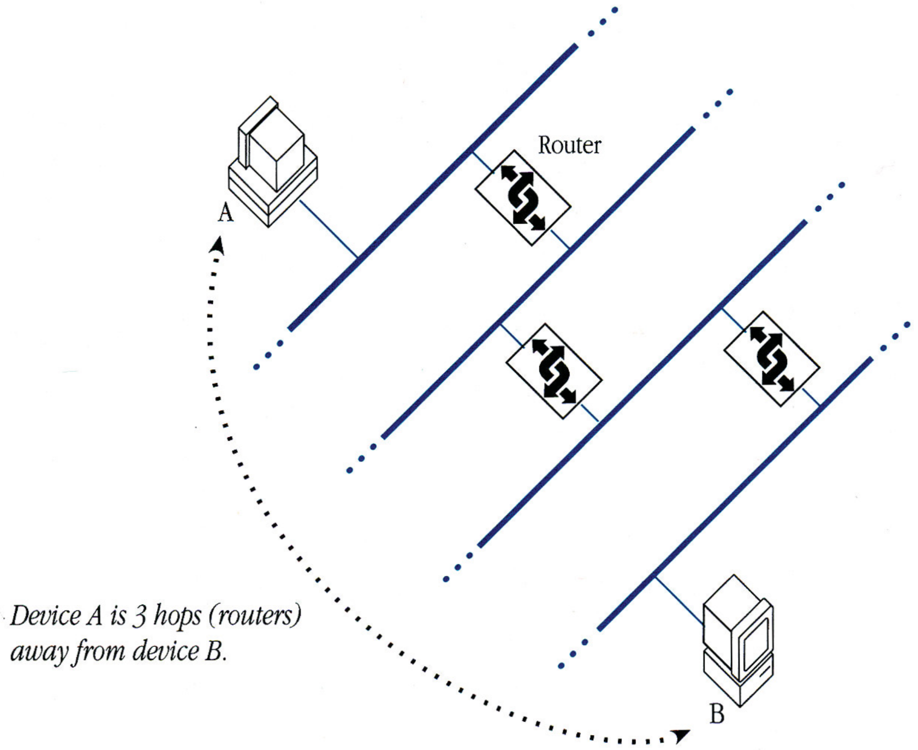
Recent Activity Rate: Idle Busy

Recent Network Error Rate: Low High

10 zones, 9 networks sorted by: Zone Name

| Network Range | Zone Name | Distance | Forwarding Port | Next Router |
|---|---|---|---|---|
| 40 | Accounting | 0 | LocalTalk | (91) |
| 61 | LocalTalk Zone | 1 | LocalTalk | 195 |
| 62 | LocalTalk Zone | 2 | LocalTalk | 195 |
| 63 | LocalTalk Zone | 0 | LocalTalk | (166) |
| 25 - 35 | Marketing... | 0 | EtherTalk | (27, 33) |
| 45 - 55 | Publications | 0 | TokenTalk | (47,207) |
| 2200 - 2203 | TTLabZone1 | 2 | LocalTalk | 195 |
| 2300 - 2303 | TTLabZone3 | 2 | LocalTalk | 195 |
| 58 - 60 | Zone1... | 2 | LocalTalk | 195 |

The routing table serves as a logical map of the internet. It lists the network number (or network range) for each network, associated zone names, the address of the next router in the path to a given destination network, and the distance to other networks, measured in **hops.** A hop is a unit count between networks on an internet, and means "one router away." Each router uses this routing table to determine where (and whether) to forward a data packet.

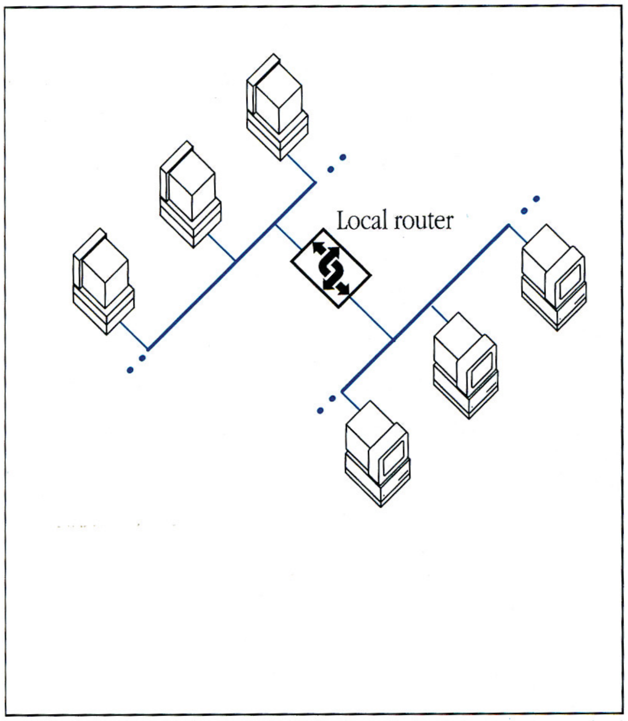


Routers can be used in the following ways.

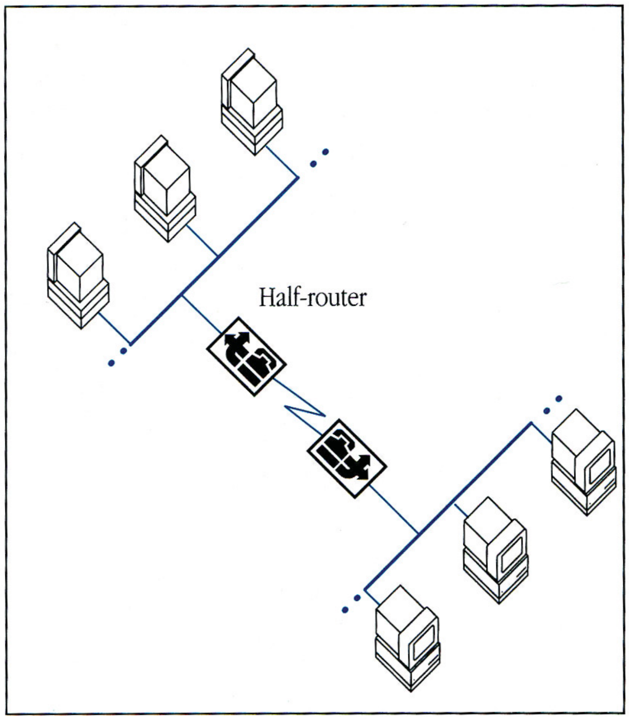
- *To connect local networks:* A **local router** is used to connect two or more networks in close proximity.
- *To connect remote networks:* A **half-router** (or *remote router*) is used to connect two or more remote networks over a long-distance telecommunications link. Each network is connected to a router, which in turn is connected to a modem.
- *To connect networks to a backbone:* A **backbone router** can be either a local router or a half-router. The router is used to connect networks through a backbone network, allowing you to link networks in a nonserial manner. This configuration minimizes the number of hops between networks (a network is no more than two hops from another network) and thereby improves performance. (See "When to Use a Backbone" later in this chapter for more information on backbone networks.)

*A* ***router*** *maintains a logical map of networks in an internet and can route data along the most efficient path.*

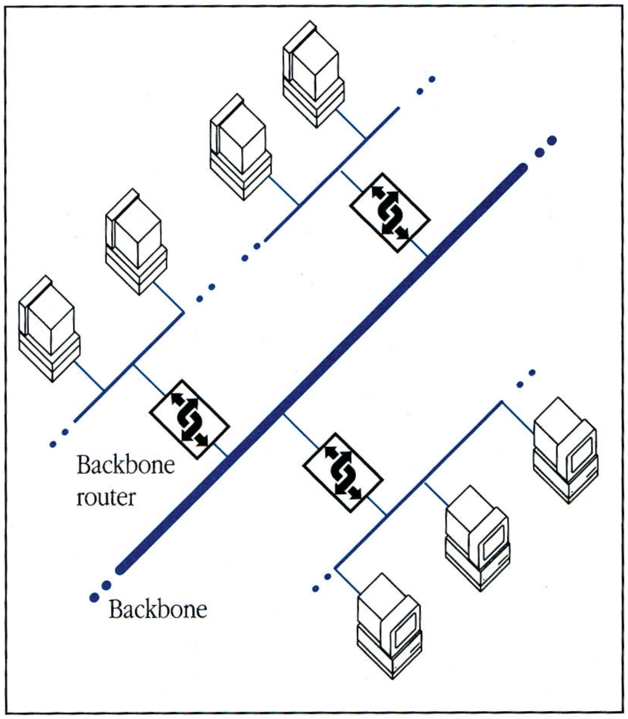
*Local networks*



*Remote networks*



*Networks connected to a backbone*

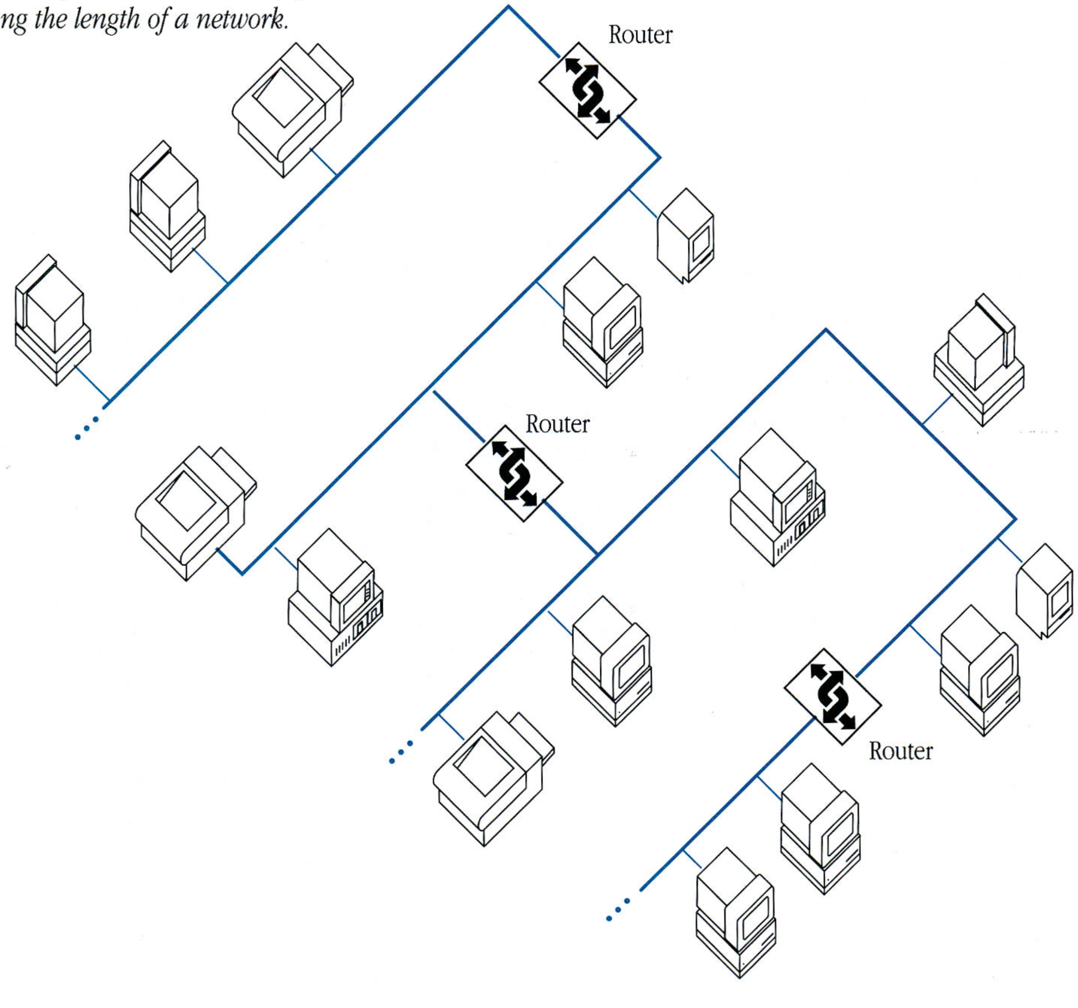


Because routers are inherently more intelligent than bridges, they do require more administration time. When you set up a router, you must identify each connected network with a *network number* or *network range* (see "Assigning Network Numbers and Ranges" later in this chapter), and you also need to specify zone names. Routers generate more overhead traffic than bridges since they are continually updating the routing tables of all routers in the internet.

### *Where to place a router*

Each internet is, in some ways, unique. The connected networks can differ in size, layout, and type. As long as a router is properly connected, there are no absolute rules that govern its placement in the internet. You can place a router at any point along the length of a network. It isn't necessary to connect networks end-to-end with a router between each network. The figure below shows examples of possible router locations.

*You can place a router at any point along the length of a network.*

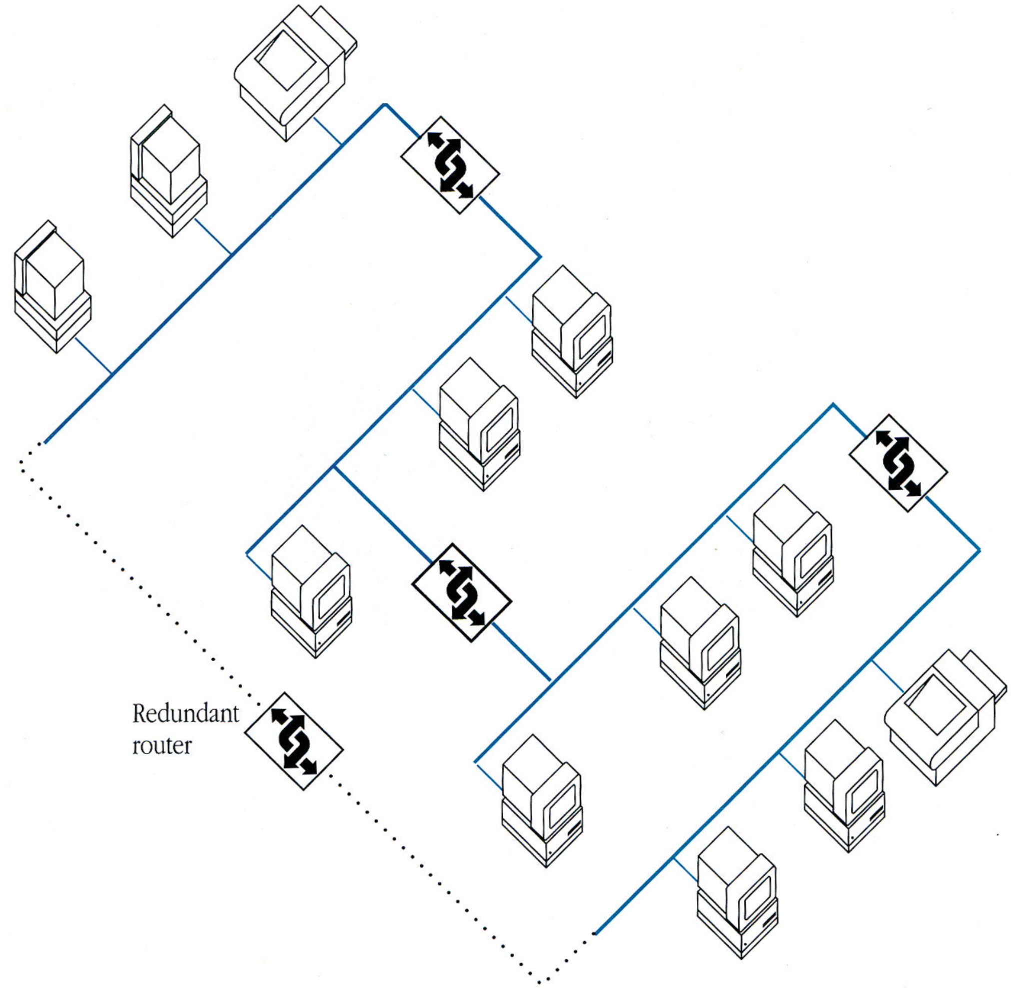


### *Creating redundant routes*

Where possible, try to create duplicate routes to each individual network in an internet. Using this technique, called **redundant routing,** you can prevent networks from getting cut off from the rest of the internet if a break occurs on one of their access routes.

In the figure below, a router has been added to the internet, resulting in redundant connections between networks. The additional router provides an alternate access route between any two networks, thereby improving network reliability; it also reduces the number of hops between some of the networks.

Be aware that if you create redundant routes with the same number of hops, troubleshooting can be more difficult, because it may be hard to figure out which path the packets are following.



### *Dividing your internet into zones*

During router setup, you can arrange devices into logical groupings called **zones** that *conceptually* partition the internet. There are two main reasons to create zones: to make it easier for users to locate devices, and to facilitate the creation of departmental workgroups that may reside on different physical networks.

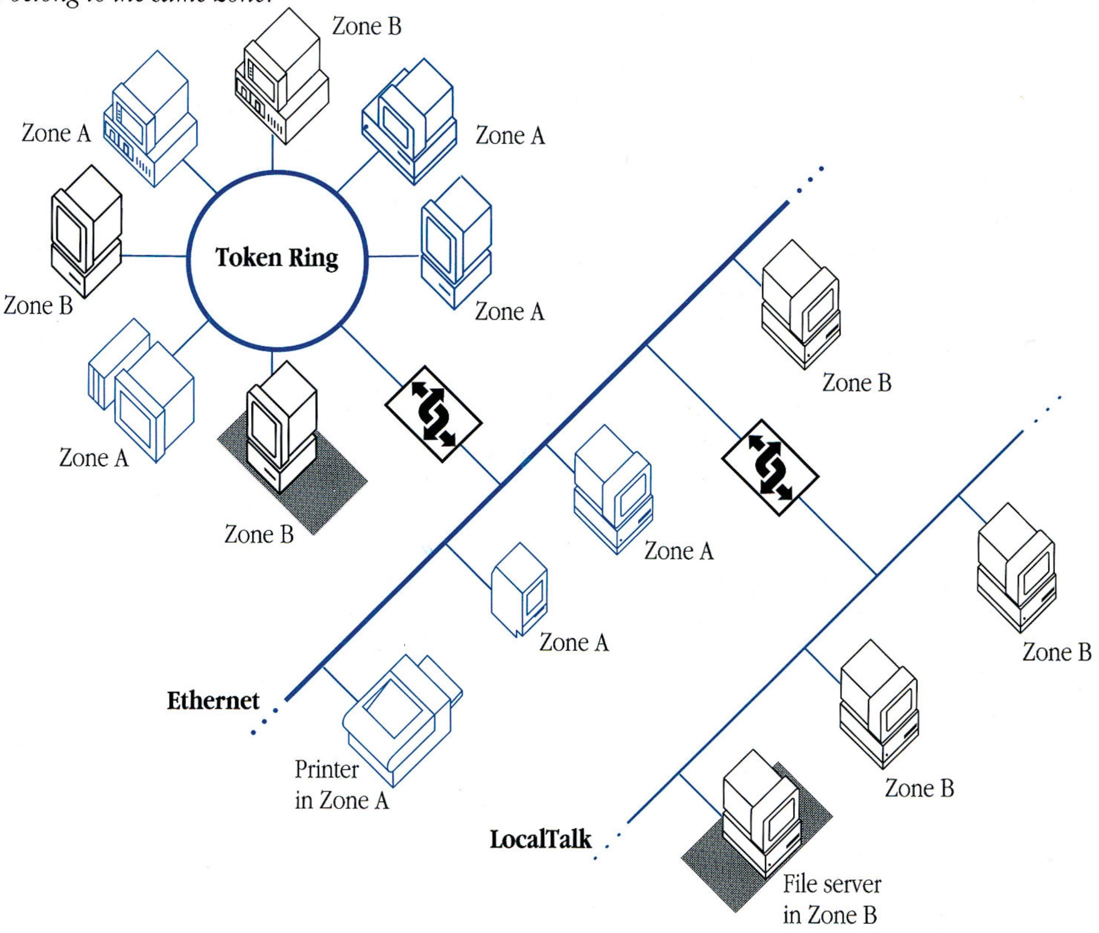
Internets can contain many hundreds of shared resources, such as printers and file servers. If users had to sort through a list of all these devices, the process would be overwhelmingly long and cumbersome. Dividing the internet into zones is a much preferred alternative, enabling users to view the devices within a single zone rather than those on the entire internet.

Zones also enable administrators to group users into a single zone regardless of where they are physically located. A group of users assigned to the same zone can efficiently locate the network resources in that zone. This is convenient in situations where members of a department or workgroup reside in different physical areas. This also lets administrators change zone groupings without having to change any physical connections.

If you do set up users so that they are in the same zone, but reside on different networks, be aware that this may cause areas of high traffic on the internet. For example, in the following diagram, if a user in Zone B on the Token Ring network needs to access the file server in Zone B on the LocalTalk network, this will cause traffic on both the intervening Ethernet network and the LocalTalk network. Especially in large internets, you should consider grouping all the users on one network into a single zone to isolate traffic within that network.

Zones have no physical boundaries or size limits. A zone can include one device, several devices, or all of the devices on the entire internet.

*Users connected to different physical networks can belong to the same zone.*



## *Zone names and zone lists*

When you set up a router, you can associate one or more **zone names** with each network connected to the router. The name identifies the zone to users through the Chooser and is used in various router displays. It's a good idea to keep zone names short and simple and to make them meaningful to users. A common method is to use departmental names or locations, such as Personnel, Engineering, or Finance East and Finance West.

A single LocalTalk network can be associated with only *one* zone name; all of the devices on that network belong to this one zone. A single Ethernet or Token Ring network can have *multiple* zone names, which means that the devices on the network can belong to different zones. These multiple zone names are referred to as a **network zone list,** which contains one or more zone names available to nodes on that network. During router setup, you specify the default zone for each device. You (or any other user) can change the zone to which a device belongs through the Network control panel (or the Control Panel if you're using Macintosh system software earlier than version 7.0).

If only one zone is defined for the entire internet (or if no zones are defined), *all* network services in the internet are presented in each Macintosh user's Chooser window, and *no* zone name is displayed.

### *Assigning network numbers and ranges*

When you use a router to connect networks, you need to identify each network by assigning it a unique number or range of numbers. (As with zone name assignments, this is done during router setup.) LocalTalk networks are always identified by a single network number. Ethernet and Token Ring networks are identified by a **network range.** The network number or range must be unique in the internet. No two networks can have the same number and no two network ranges can overlap or have any network numbers in common.

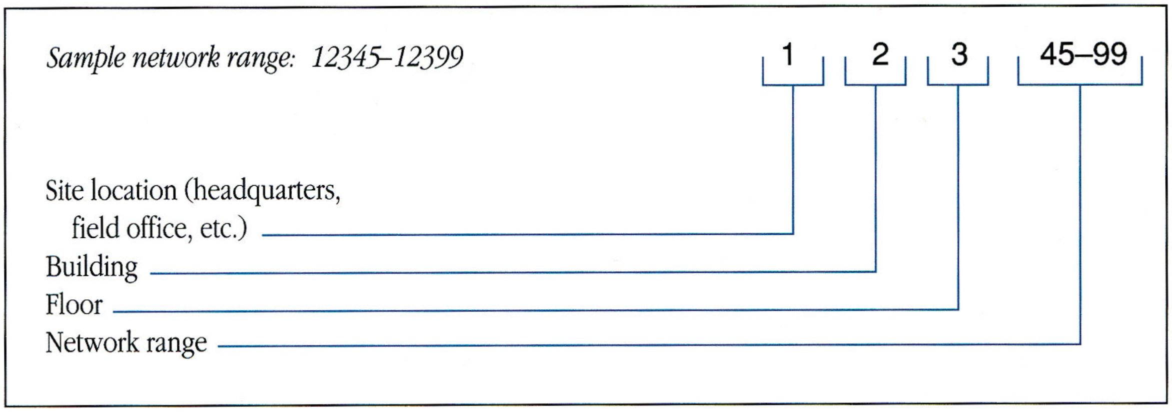
The network range is a series of contiguous network numbers, such as 1–10. Each number in a network range is a network identifier that can be associated with up to 254 devices. The size of the network range determines the maximum number of AppleTalk devices on the physical network. For example, a network having the range 1–10 could contain up to 10 x 254 devices, or 2,540 devices. If an Ethernet or Token Ring network is never expected to require more than 254 devices, you can assign a range that contains a single number, such as 100–100.

When assigning a network range, be sure the size of the range allows for ample network growth. For example, in a network containing 500 devices, the range 1–2 would accommodate current needs (2 x 254 devices = 508), but would only allow 8 additional node addresses for future growth. Exceeding this level of growth would require you to shut down the router and assign a new, larger network range, disrupting network services to users.

The recommended guideline in choosing a network range is to allow capacity for at least twice the current number of nodes (more, if rapid growth is anticipated). Since an AppleTalk internet supports up to 65,279 network addresses, or over 16 million possible node addresses (65,279 x 254 nodes), it's possible to assign oversized network ranges and still have sufficient addresses for a *very* large internet. For further flexibility in your internet setup, when assigning network ranges, allow wide margins between the ranges you select. For example, if you assign a range of 100–110 to a network, you may want to start the next range with network number 120 rather than network number 111. If your internet has relatively few networks, margins between network ranges can be very large.

◆ **Note** Network ranges are part of the extended addressing capabilities of **AppleTalk Phase 2.** To learn more about the capabilities of AppleTalk Phase 2, refer to *Inside AppleTalk* (second edition), the *AppleTalk Phase 2 Introduction and Upgrade Guide,* and *The Advantages of AppleTalk Phase 2.* See the Appendix for information on how to obtain these publications. ◆

Although there are no rules for numbering networks, it's useful to observe a consistent network numbering scheme—especially in large and fast-growing internets. One such scheme involves assigning a location code or department code to the digits in a network number. The following figure illustrates how a network numbering system can help to identify networks in an orderly way.


*Sample network range: 12345–12399*
1
2
3
45–99
Site location (headquarters, field office, etc.)
Building
Floor
Network range

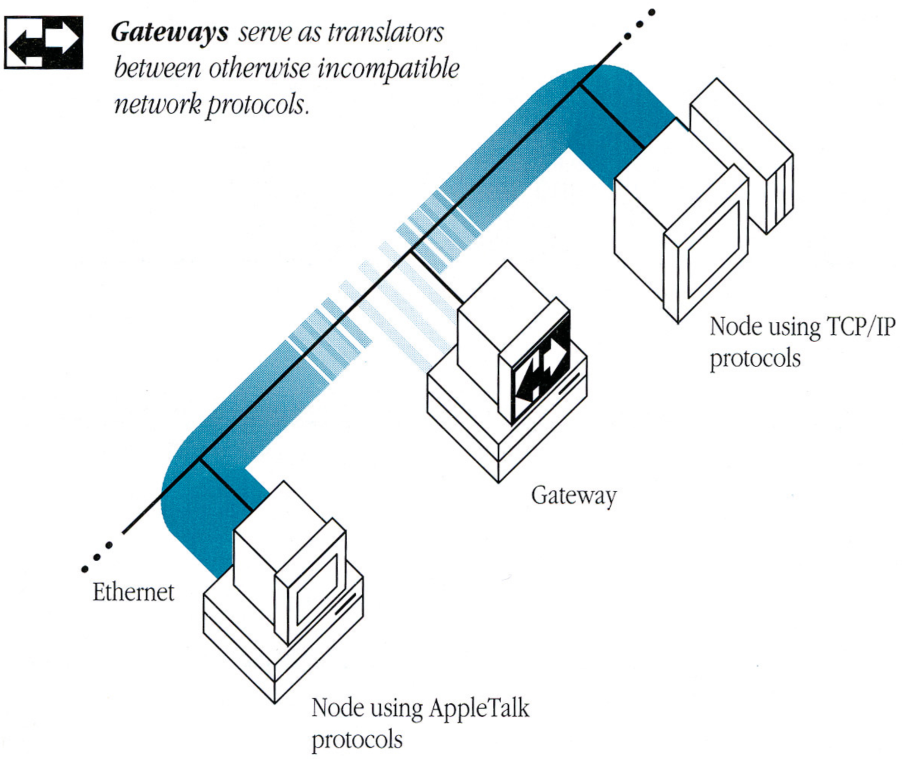
A network numbering system serves several purposes:

- It facilitates the assignment of network numbers when new networks are created.
- It identifies each network in a way that is meaningful to you. For instance, you can look at a routing table and immediately associate the network numbers with their physical locations (such as "building 2, third floor").
- It avoids potential network numbering conflicts that can arise with duplicate numbers.

Keep track of your network numbers and ranges by recording them in a logbook, in an electronic spreadsheet, or on your network map.

## Gateways

The fourth kind of connection device—a **gateway**—is a combination of hardware and software that connects an AppleTalk network with a network using non-AppleTalk protocols, such as TCP/IP or DECnet. Gateways serve as translators between these otherwise incompatible network protocols. A gateway is not necessarily used to make a network larger; its primary purpose is to overcome differences between connected networks. The gateway interprets network-related information in a data transmission, such as addressing and routing instructions, then translates this information into the format of the protocols running on the connected network.



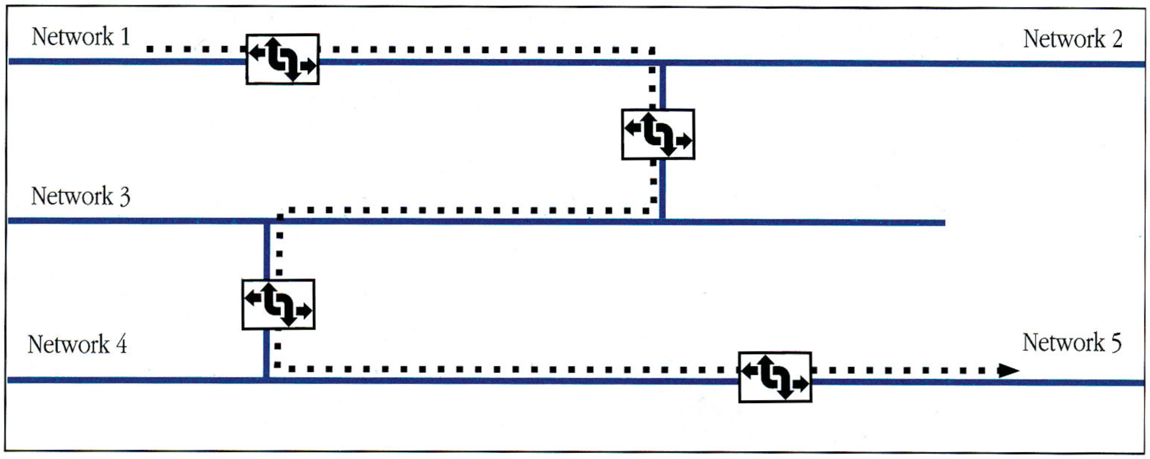
***Gateways*** *serve as translators between otherwise incompatible network protocols.*

# When to use a backbone

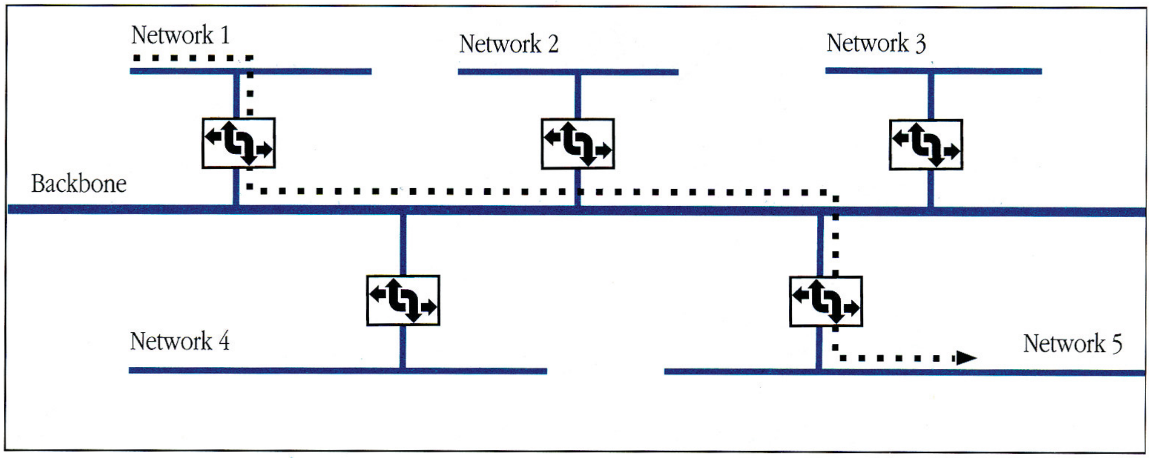
If you are planning an internet, you'll find that a **backbone network** is a very useful part of an efficient network layout. The primary function of a backbone is to transport information between other (often slower-speed) networks. A backbone is like a superhighway. It alleviates cross-network traffic congestion, providing each connected network with a more direct route to every other network in the internet. With a well-planned backbone network, data can be sent through a minimal number of routers to reach the destination network.

It's especially useful to create a backbone network to connect many separate networks or to connect networks that aren't physically contiguous. A backbone is often used to connect networks on different floors of a building or in different buildings. In addition, you can connect network devices directly to a backbone, permitting faster access to heavily used devices such as file servers.

***Example A:*** *without a backbone*



***Example B:*** *with a backbone*



In the preceding figure, Example A shows five networks connected serially by routers, with no backbone. To get from Network 1 to Network 5, a packet would need to travel four hops and would have to contend with network traffic on three intervening networks—which may themselves be slower networks. In contrast, in Example B, the same transmission would need to travel only two hops, with the backbone network in between. (Network performance can be further enhanced if the backbone is a high-speed network such as Ethernet, as discussed in the next section.)

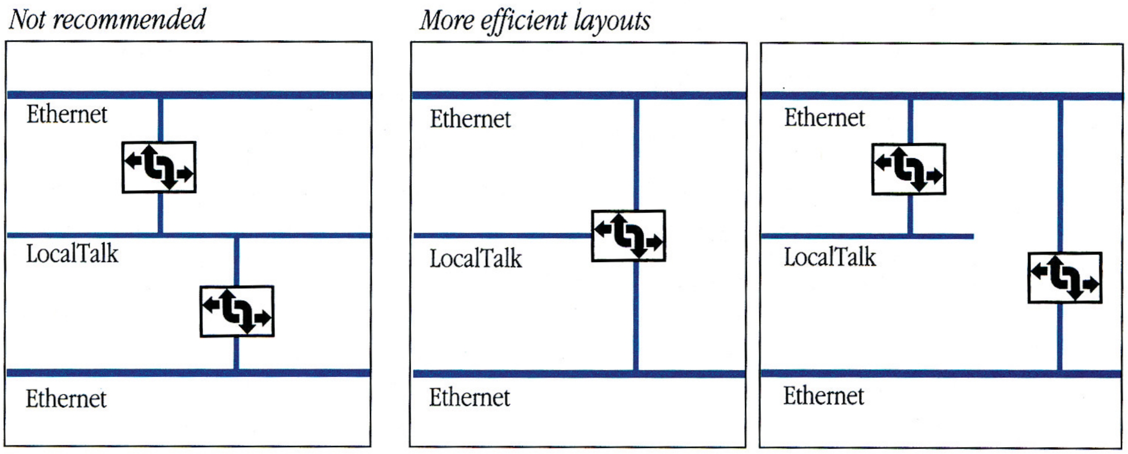
## Selecting the backbone network type

Any network type that can be connected to a router can be set up as a backbone. However, since the object of a backbone is to enhance performance—and since the backbone may be used as a thoroughfare for many connected networks—it's desirable for the backbone network to transmit data at a fast rate.

For example, any type of network can provide the efficiency of fewer hops between networks, but an Ethernet or Token Ring backbone also provides a high transmission speed. The backbone network type you select should take into account the usage level and performance needs of your own internet.

## Connecting networks of different speeds

Since you can combine different network types in an internet, you need to consider *where* it would be most advantageous to place higher-speed networks in the layout of your internet. When possible, use faster networks in a busy route between other networks, as illustrated in the following figure.



*Not recommended*

*More efficient layouts*

When connecting networks of different speeds, consider that most lower-cost routers (including the AppleTalk Internet Router) do not distinguish the *speed* of a network when selecting the most direct route to a destination. Instead, these routers select the route with the least number of *hops*. If you have a lower-cost router, wherever redundant routes exist, try to place fewer hops in the faster network so that this is the path selected. You may want to consider eliminating redundant routes in which the number of hop counts will cause the router to select the slower-speed route.

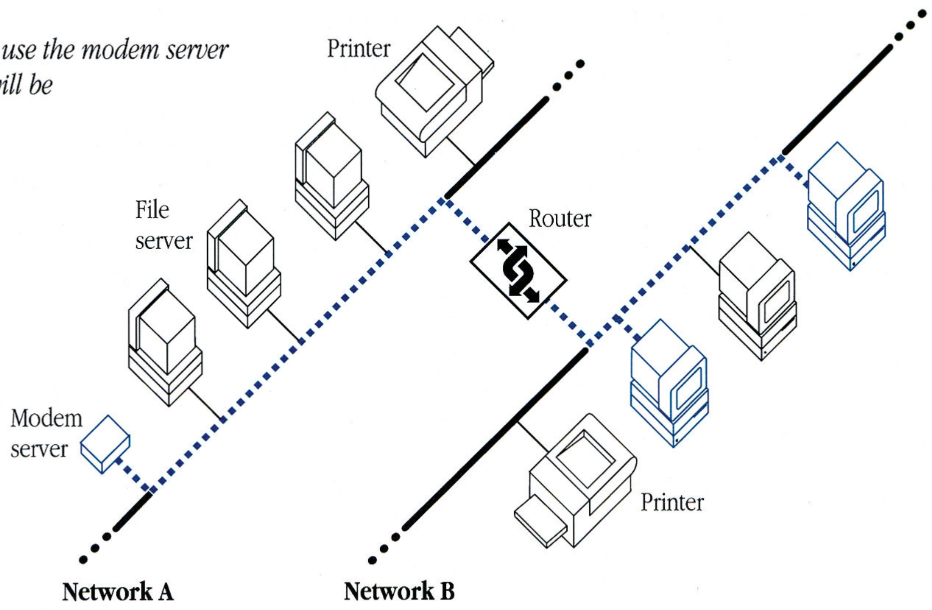
## Where to place shared resources

How do you determine where it would be most efficient to place shared resources? If you have a single network, it doesn't matter where you place printers and servers from a *network performance* standpoint. However, you *will* want to consider factors such as convenience and security. Shared printers should be easily accessible by network users. You may want to place servers close to you for administrative purposes or in an isolated area for security reasons (see Chapter 9 for a discussion of security).

If you have two or more connected networks, there is one basic, common-sense rule about where to place shared resources: always try to place them on the same network as the people most frequently using them. Avoid placing routers or bridges between users and the devices they share. This will cause unnecessary traffic over networks that do not use the devices or that use them infrequently. If your internet includes a backbone network, consider locating devices shared equally by many networks on that backbone. (See the following examples.)

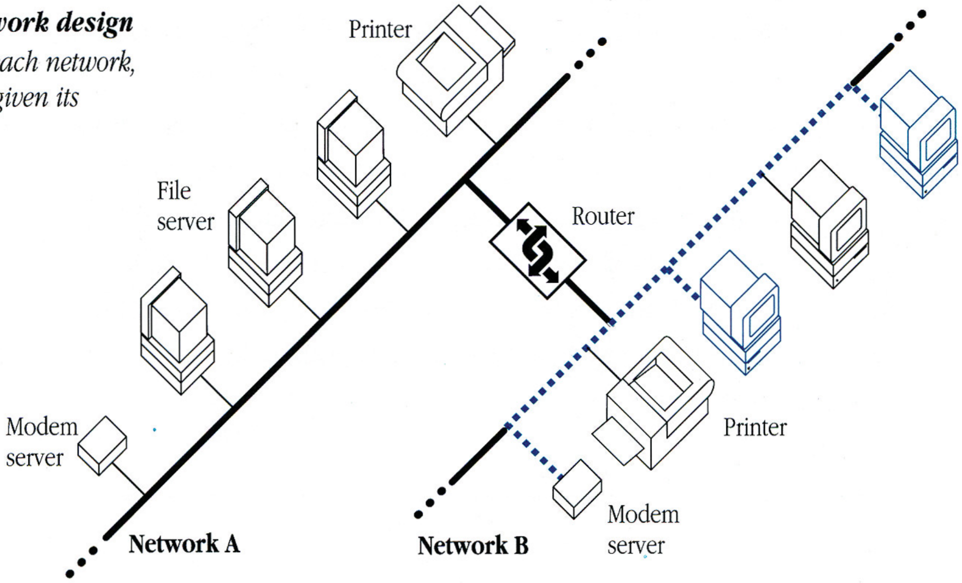
***Poor network design***

*If many users on Network B need to use the modem server on Network A, unnecessary traffic will be generated on Network A.*

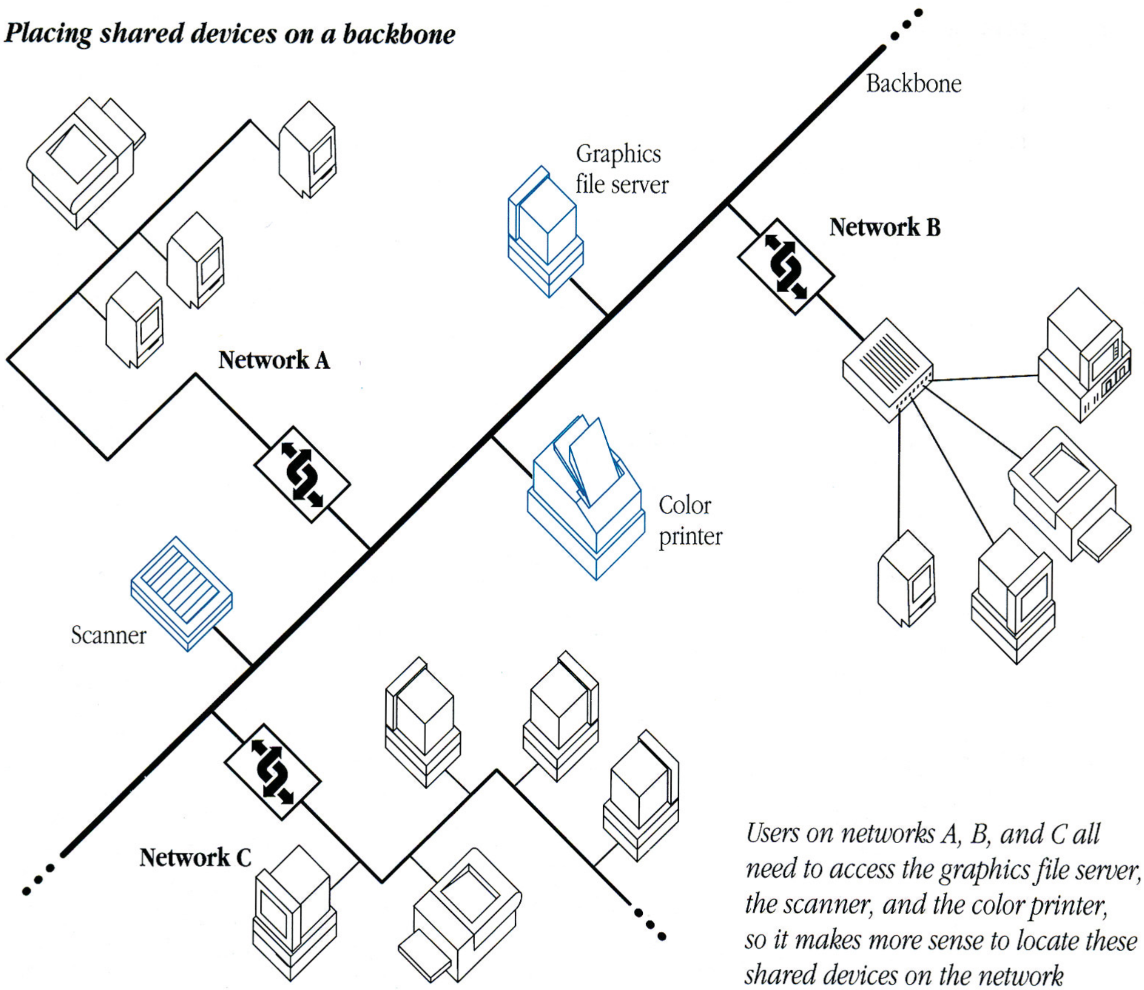


***Recommended network design***

*To isolate traffic on each network, Network B has been given its own modem server.*



***Placing shared devices on a backbone***



*Users on networks A, B, and C all need to access the graphics file server, the scanner, and the color printer, so it makes more sense to locate these shared devices on the network backbone.*