Network Interface Cards
The network interface card (NIC), or network card, is a device installed on the system that is responsible for sending and receiving data onto the network. The network card is responsible for preparing data from the system to be transported on the wire by converting the outbound data from a parallel format (due to bus width of the bus architecture that the card is sitting in) to electrical signals that will travel along the network media. On the receiving end, the network card is responsible for receiving the electrical signal and converting it to data that is understood by the system.

The network card also is known as a network adapter; it can be installed in the system after the system has been purchased, or the system comes with a network card built in. A system that comes with a network card built in is said to have an integrated network card—meaning the card is integrated into the system similar to a laptop.

Network cards that are installed on the computer as an add-on can be installed into the system by inserting the card into the expansion bus of the system (usually PCI, but in the past it was ISA) or by plugging in a USB device. There are a number of different types of expansion slots in the system.

When installing a network card, you will need to make sure that you get the correct type of card for the particular type of expansion slot.

For example, a PCI card is placed in a PCI slot and will not fit into an ISA or AGP slot. The following is a list of popular expansion bus architectures
.

- **ISA** Industry Standard Architecture (ISA) is an old bus architecture that runs at 8 MHz and supports 8- or 16-bit cards.
- **MCA** Microchannel Architecture (MCA) was built by IBM and has a 32-bit architecture that runs at 10 MHz.
- **VESA** Video Electronics Standards Association (VESA, also known as VESA local bus, or VLB) at the time ran at the system speed (which was around 33 MHz); it has a 32-bit architecture.
- **EISA** Extended Industry Standard Architecture (EISA) is the upgrade to ISA that supports 32-bit cards running at 8 MHz.
- **PCI** Peripheral Component Interconnect (PCI) is the popular bus architecture today for adding cards to the system. PCI runs at 33 MHz and has a 32-bit or 64-bit bus architecture. Most network cards today are PCI.
- **AGP** Advanced Graphics Port (AGP) is the new graphics standard that runs at 66 MHz and is used by video cards.
- **PCMCIA** Personal Computer Memory Card Industry Association (PCMCIA) is the bus architecture used in laptop computers. PCMCIA has a 16-bit architecture that runs at 33 MHz.

Transceivers
A transceiver is that portion of the network interface that actually transmits and receives electrical signals across the transmission media. When the signal is traveling along the length of the wire, the transceiver picks the signal up and verifies that the data is destined for the local system. If the data is destined for the local system, the data is passed up to the system for processing; if it is not, it is discarded. There are two types of transceivers: onboard and external.

Onboard Transceivers
Onboard transceivers are built onto the network interface card. With these transceivers, the media connector is built right on the back of the NIC. Common examples of this type include RJ-45 receptacles for twisted-pair cable and BNC connectors for thinnet coaxial cable.

External Transceivers
With an external transceiver, the actual media connection is made external to the network card using a small device that attaches to the NIC via an extension cable. These connections use an attachment unit interface (AUI) connector, also called a Digital-Intel-Xerox (DIX) connector, on the back of the network card. The

AUI connector is a female 15-pin D-connector (shown in Figure 3-4) that looks very much like a joystick port and typically is used to connect a workstation to thicknet cabling. The types of transceivers and media that can be served by a NIC determine the appropriate connector. Each media type has a typical connector type or connection method.

Thicknet Coax

Thicknet, or standard Ethernet coax, uses a connection method that typically involves an external transceiver connected to the adapter's AUI port. This external transceiver has a connection called a vampire tap that attaches to the media by drilling a hole in the cable using a special drilling jig that controls the depth of the hole. This jig prevents the drill from drilling through and severing the center conductor. The vampire tap consists of a pin that is inserted into the hole drilled in the cable and a clamp that holds the tap onto the cable. One of the challenges of this type of connection is to position the tap so that it contacts the center conductor without shorting to the shield surrounding it. These difficulties, as well as the cost and size of thicknet cable, have rendered it largely obsolete, although it occasionally could be found in existing installations.

Thinnet Coax

Thinnet coax can be attached directly to a network adapter if an onboard transceiver is used. In this case, a connector called a barrel connector (BNC) on the network card attaches to a T-connector. The T-connector has a female fitting that attaches to the card, as well as two additional male fittings that attach to cable segments or a terminator. Each end of a thinnet Ethernet segment must be terminated, so the last node on each end could have a terminator attached to the side of the T-connector opposite the inbound cable. All other nodes use T-connectors with cable segments attached to both sides, just like holiday tree lights. A thinnet segment cannot be attached directly to the BNC connector on the network adapter; it must use a T-connector.

Twisted-Pair Wiring

The typical connector for a twisted-pair connection is called an RJ-45 connector. The RJ-45 connector looks like an oversized phone connector. The reason for the difference in size is that a phone connector (RJ-11) has a four-wire connector, whereas an RJ-45 connector is an eight-wire connector. An RJ-45 patch cable can be plugged directly into the back of the network adapter. The patch cable usually runs to a wall receptacle, which is wired back to a patch panel and ultimately back to a wiring hub.

Fiber-Optic Cabling

Fiber-optic adapters generally have two connectors, one each for incoming and outgoing fiber cables. The mechanical connectors that join the cable, called ST connectors, are designed to pass light seamlessly across the joined fiber segments. For this reason, these connectors must be made with great precision. Fiber-optic runs generally are made back to a concentrator that performs a hub function.

In many situations, fiber-optic cabling is used to connect high-speed computers and provide a high-speed backbone to which slower LANs are attached. The LANs might connect copper media, such as twisted-pair or coaxial cable, to a set of hubs that are then bridged to the fiber-optic backbone for high-speed data transfer between LANs.

Transceiver Configuration

A number of network cards have multiple types of connectors on the back of the card (called combo cards in this case) to allow you to use different types of cabling to connect the system to the network. The transceiver type that is being used by the network card is typically set to the "auto" setting, which means that the card can sense which transceiver you are using and the card will configure itself to use that transceiver. When troubleshooting to find out why the card is not working, the "auto setting" is the first thing you should change

A setting you may want to configure on your network card is the transmission method of either simplex, half duplex, or full duplex. The three transmission methods are as follows:

- **Simplex** Allows communication in one direction only. You will only be able to send or receive with a simplex device—not both directions. It is either one way or the other.
- **Half duplex** Allows communication in both directions (send and receive), but not at the same time. A network

card set to half duplex will not be able to receive data while sending data. Using the half-duplex setting can slow down communication if your device does support full duplex.

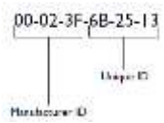
- **Full duplex** Allows communication in both directions at the same time. If a network card supports full duplex, it will be able to receive data when data is being sent because all four pairs of wires are used. If you make sure that a network card that supports full duplex is set to full duplex, you will notice a big difference in throughput if the device is set to half duplex.

Most network cards are set to auto. With this setting, you may want to force the setting to the full-duplex mode to be sure that you are getting full-duplex communication. You can change the communication method through the network card properties in the Device Manager.

MAC Address

Each network card has a unique address that is burned into the card by its nmanufacturer. This unique address, known as a MAC address, is used in the header of the packet for the source and destination addresses of the packet. The MAC address is a 48-bit address displayed in a hexadecimal format that looks similar to 00-90-4B-4C-C1-59 or sometimes 00:90:4B:4C:C1:59.

The MAC address is made up of 12 characters and is in hexadecimal format. The first half of the MAC address is the manufacturer's address, while the last half of the address is the unique address assigned to that network card by the manufacturer. The combination of the manufacturer ID and the unique address ensure that the MAC address is singular. The figure below shows this addressing.



Hubs, MAUs, and Repeaters

Once you have the network card inserted into the computer system or network device, you will next need to connect each of the systems together using devices such as hubs, repeaters, or MAUs.

Hubs

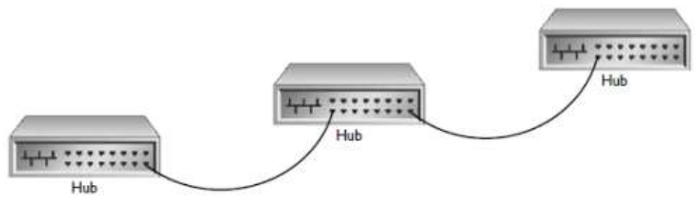
Hubs are one of the most important components of a network because they act as a central point for all network devices to connect to. You can easily remember the layout of a hub if you think of a wheel and picture how the spokes radiate out from the hub of the wheel. In a network, each spoke is a connection, and the hub of the wheel is the hub of the network where all of the cables come together.

The Role of Hubs in Networking

The hub, also known as a concentrator, is responsible for allowing all systems a central point of connection, so that when a computer sends a piece of data to another computer, the electrical signal leaves the network card of the sending system and reaches the hub, and the hub sends the signal to all ports on the hub so that all systems can check to see whether the data is destined for them.

Cascading Hubs

If you wanted to connect three 24-port hubs together, you would need to uplink from port 24 on the first hub to any port on the second hub (I usually uplink to the first port on the second hub), then use port 24 on the second hub to uplink to the first port on the third hub, as shown in the figure.



A hub sends the signal to all ports on the hub. This means that, if you have a 24-port hub linked to another 24-port hub and a workstation sends data to another

workstation, the data will be sent to all 48 ports on the network. This leads to a lot of unneeded traffic and contention across the entire network that will slow network performance. A solution would be to use a switch.

Passive Hubs
The function of a passive hub is simply to receive data from one port of the hub and send it out to the other ports. For example, an eight-port hub receives data from port 3 and then resends that data to ports 1, 2, 4, 5, 6, 7, and 8.

A passive hub contains no power source or electrical components, there is no signal processing (such as when the hub receives the electrical signal), and there is no regenerating of the signal to ensure that it is readable at the destination. A passive hub simply attaches the ports internally and enables communication to flow through the network. Regeneration of the signal is a function of an active hub.

Active Hubs
An active hub provides the same functionality as a passive hub with an additional feature. Active hubs rebuild (regenerate) the data before sending it to all of the destination ports on the hub. Using active hubs, you can increase the length of your network, because although the signal weakens with distance, when the active hub receives the signal, it rebuilds the data, allowing it once more to go a greater distance. It is important to remember that UTP cabling can be run a maximum of 100 meters. With an active hub, you can run this type of cable 100 meters on each side of the hub. An active hub has a power source and built-in repeaters to boost the signal. Extra electronics built into an active hub allow for signal regeneration.

Hybrid Hubs
A hybrid hub is a hub that can use many different types of cables in addition to UTP cabling. A hybrid hub usually is cabled using thinnet or thicknet Ethernet along with popular cable types such as twisted-pair cabling. A few years ago, hybrid hubs were fairly popular. UTP seems to be the popular cable type today, so you may not see the thinnet or thicknet connector on the hub as well.

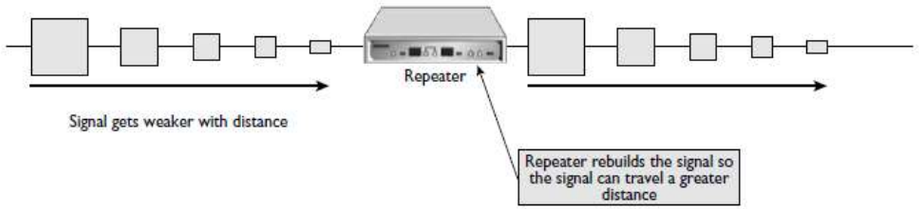
Multistation Access Units

A multistation access unit (MAU) is a device to which multiple workstations are connected in order to communicate on a Token Ring network. A MAU is a hub-type device for Token Ring networks with some features that make it a little bit different from a hub—for example, a MAU regenerates the signal when it reaches the MAU. Because Token Ring networks use token passing instead of CSMA/CD, there is no chance for collisions on a Token Ring network. The first difference you will notice with MAUs over hubs is that a MAU does not have collision indicators on it because you can't have collisions on a Token Ring network. The figure below shows a picture of a MAU; notice that there are no collision indicators on the device.

Another major difference with a MAU is that MAUs don't actually use an uplink port. With Token Ring, there is a logical ring within the MAU, and when you connect to another MAU, you must complete a full ring structure again. Therefore, you will notice on the Token Ring MAU that it has a ring-in port and a ring-out port. When you wish to connect two MAUs together, you must ring out of the first MAU and, with that cable, ring in to the second MAU. Then you must ring out of the second MAU and ring in to the first MAU.

Repeaters
One of the pitfalls of networking environments is that the electrical signal that is traveling the wire is weakened over distance as a result of outside interference. Eventually, if two systems are too far from one another, the signal is so weak that by the time it reaches the other side it is unreadable. This is where repeaters come in. If your network layout exceeds the normal specifications of the cable, you can use repeaters to allow the signal to travel the distance by placing the repeaters at different points in the network. For example, if you are using thinnet cabling, you know that thinnet is limited to 185 m. But what if you want to connect two systems together that are 235 m apart? You would place a repeater somewhere before the 185 m mark so that the repeater will regenerate or rebuild the signal, allowing it to travel the extra

difference. The figure below shows a signal that is weakened over distance but is regenerated through the use of a repeater.



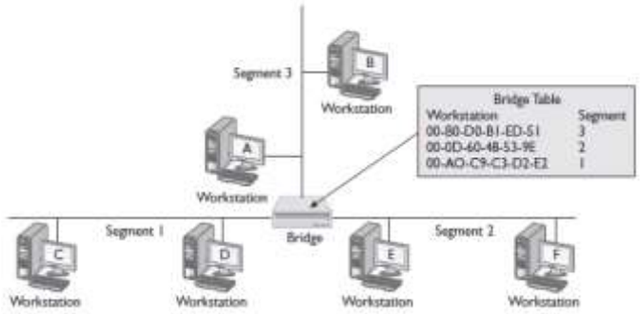
Bridges and Switches

Layer-2 devices are a little smarter than layer-1 devices in the sense that they actually can make decisions about where the electrical signal needs to go. Remember that a hub, which is a layer-1 device, would forward the signal to all ports on the hub, which will lead to traffic problems as you start adding hubs to the topology.

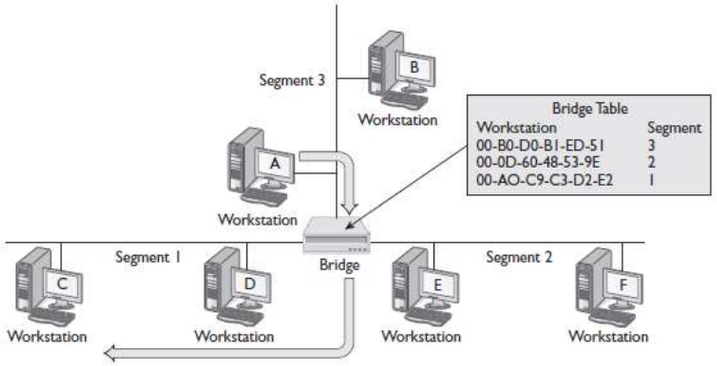
By filtering network traffic, we are conserving precious bandwidth on the network, which will have a huge impact on the overall performance of the network.

Bridges

A bridge is a network connectivity device that is used to break the network down into multiple network segments. A bridge runs at layer 2, the data link layer, and is used to filter traffic by only forwarding traffic to the destination network segment. The figure below shows an example of a bridged network.



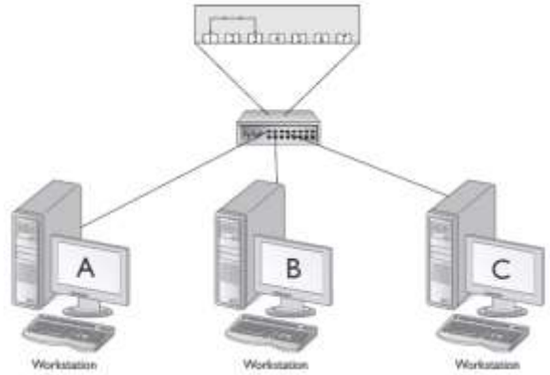
Let's look at an example of how a bridge filters network traffic. Assume that you have just completed connecting the bridge to the network segments shown in
The figure above. When Workstation A sends data to Workstation F, the data will go out the network card of Workstation A and will travel the full length of segment 3 in both directions. The signal will reach the bridge, and the bridge will look at the destination MAC address of the packet. Once the bridge looks at the destination MAC address, it will compare that MAC address with the MAC addresses in its bridging table. The bridging table is a table in memory that lists all known MAC addresses and which network segment that MAC address lives on. This table is critical to the bridge's filtering features. Since this is the first piece of data sent on the network, the MAC address for Workstation F is not in the bridging table, so the bridge will need to forward the data to both segment 1 and segment 2. It will not forward the information to network segment 3 because that is where the data came from, and if Workstation F existed on that network, it would already have the data. When the bridge received the initial data from Workstation A, it recorded the MAC address of Workstation A and the network segment that Workstation A resides on in the bridging table. This way if anyone sends data to Workstation A, the bridge will have an entry for Workstation A in the bridging table, and the bridge will forward the data only to network segment 3 and not to the other segments. Also note that when Workstation F replies to Workstation A, the data will need to pass through the bridge, so the bridge will know what network segment Workstation F resides on and will record that MAC address in the bridging table. Over time, the bridging table will be filled with MAC addresses and their associated network segments. In our example, after the bridging table has been constructed, if Workstation A sends data to Workstation C, the data will reach the bridge and the bridge will forward the data only to network segment 1. This prevents network segment 2 from being congested with the traffic (shown in the figure below).



Switches

Switches, also known as switching hubs, have become an increasingly important part of our networking today, because when working with hubs, a hub sends the data to all ports on the hub. If you have a large network structure, this means that you have probably linked a few hubs together, and when data is sent from one system to another, all computers see the traffic. This leads to a lot of network traffic, which eventually slows network performance.

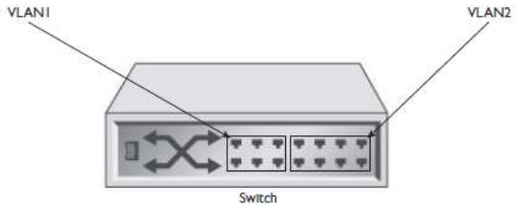
When you use a switch instead of a hub, the switch acts as a filtering device by associating the MAC address of the system connected to the switch with the port on the switch that the system is connected to. For example, in the figure below, Computer A transmits a packet to Computer C. The packet enters the switch from port 1 and then travels a direct route to port 3, because the switch uses the destination MAC address of the packet and knows that the MAC address is of the device connected into port 3. From port 3, the packet is transmitted to Computer C. During this process, Computer B is unaware of the traffic between Computers A and C, because there is a direct path within the switch and no shared bandwidth.



Understanding VLANs

Virtual LANs (VLANs) are a feature of special switches, known as managed switches, which allow the administrator to group ports on a switch to a “virtual LAN.” When a port is configured for a particular VLAN, it is unable to communicate with systems that are not on that VLAN without the use of a routing device such as a router. This is similar to the fact that, if we had two physical networks, a machine cannot send data from one network to the other without the use of a router.

The purpose of a VLAN is to cut down on broadcast traffic through the use of what are known as broadcast domains. A VLAN acts as a broadcast domain. Normally, if we had a 24-port hub or switch and a computer wanted to send data to all systems, it would “broadcast” the data out onto the network. A broadcast will hit every port on that switch or hub. With a VLAN supported switch, you can create VLANs that act as “broadcast” domains. This means that if Workstation A is on VLAN1, which is made up of ports 1 through
12 on the 24-port switch, when Workstation A sends broadcast traffic (traffic intended for all systems), it will be sent only to ports 1 through 12 because the virtual LAN is acting as a boundary for traffic. The benefit of this is that you are now able to minimize traffic within or across switches, which increases network throughput. The figure below shows a switch that is divided into two different VLANs.



Ports on a switch associated with VLANs

How you implement your VLAN depends on what type of switch you have. There are a number of different types of switches:

- **Layer-1 switch** A layer-1 switch implements what is known as port switching. Port switching means that the network administrator associates the ports on the switch as being members of a particular VLAN. With port switching, you need to ensure that you are satisfied with the fact that if you move a computer from one port to another, the system may become a member of a different VLAN, because the port is the member of the VLAN, not the network card connected to it. Layer-1 switches do offer benefits; they are great for increasing security and isolation. They also allow an administrator to move a system to a new VLAN by reconfiguring the port for the new VLAN. The benefit is that there is no need to move the system physically.
- **Layer-2 switch** A layer-2 switch doesn't associate the port with the VLAN, but the MAC addresses of systems are associated with the VLAN. The network administrator is responsible for listing all the MAC addresses for each VLAN on the switch. When a packet is sent by a system and reaches the switch, the switch tags the packet as being a member of the VLAN, and it will be sent only to other systems in the VLAN. The benefit of layer-2 switches is that, because the MAC address is associated with the VLAN, it doesn't matter what port the system is plugged into. This is a great feature for laptop users who typically roam around on the network—they will always be a member of the same VLAN unless the switch is reconfigured.
- **Layer-3 Switch** A layer-3 switch bases membership to a VLAN on the subnet ID of the layer-3 address of a packet. With layer-3 switches, the workstations do not actually belong to the VLAN, but the packets that are being sent do belong, because they have the source address information which contains the network ID in them.

To create the VLANs, the network administrator will need to run the configuration utility on the VLAN-supported switch. Also note that with a layer-1 switch, if a system needs to be moved from VLAN1 to VLAN2, there is no need to move systems around; you simply need to configure the port that the system is connected to from one VLAN to the other on the switch.

Switch Features

Most enterprise-capable switches have a number of features that make the switch attractive for large organizations. The following is a listing of popular features incorporated into big-name switches such as those from Cisco and Juniper Networks.

Spanning Tree Protocol (STP) The Spanning Tree Protocol (STP) runs at layer 2 and is designed to prevent loops on a network that could occur if you connect a number of switches together. For example, a loop is created if you connect Switch1 to Switch2 and then turn around and connect Switch2 back to Switch1 using a different cable and ports on the switches.

Having a loop on the network could cause the network to go down and creates instability in the switches. To prevent this, STP was designed. STP is a protocol that looks at all of the ports used to create a loop and then places one of those ports in a blocking state so that no data traffic can pass through the port. Once the port is in a blocking state, the loop is broken and the network becomes more stable.

The fact that the port is in a blocking state instead of being disabled means that if one of the other links go down, then the port is transitioned into a forwarding state automatically. When a port is in a forwarding state, it is allowed to send and receive data on the port.

Trunking Trunking is a feature on Cisco switches that allows you to connect the switches together and then assign one of the ports as a trunk port. The trunk port is the port that is used to carry VLAN traffic to the other switch. VLANs are allowed to contain ports as members that are from multiple switches. If data is destined for all systems in the VLAN, the VLAN identification information is added to the data packet and then the switch sends the packet out the trunk port. When another switch

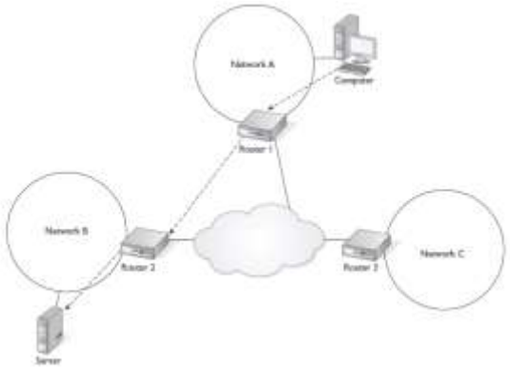
receives the packet, it checks the VLAN identification information and then sends the data to all of its ports that are a member of that particular VLAN.

ISL and 802.1Q When a switch assigns the VLAN identification information to a packet, this is known as tagging. Two popular protocols for tagging are the Inter-Switch Link (ISL) and the IEEE 802.1Q protocol.
ISL is the Cisco proprietary protocol for tagging packets and associating them with a particular VLAN on older switches, while 802.1Q is the IEEE standard for VLAN trunking. Newer Cisco and Juniper Networks switches use 802.1Q as the tagging method.

Port Mirroring Port mirroring, also known as port monitoring, is a feature that allows the switch to send a copy of data that reaches certain ports to the mirrored, or monitored, port. Port monitoring allows an administrator to plug his/her workstation into the port that the copy of the data is being sent to, and monitor the network traffic. Port mirroring is an important feature of a switch because by default the switch filters traffic by only sending the data to the port that the destination system resides on. The switch's filtering feature will prevent the monitoring of traffic, and as a result the administrator will have to enable port mirroring (monitoring) and specify the port that receives the copy of data.
Port Authentication Port authentication is another important feature of the switch that allows the administrator to associate the MAC address of the system that will connect to the port. The administrator can also specify that if a system with a different MAC address connects to the port, the port is to be automatically disabled.
Port authentication will help increase the security of the network by allowing only authorized systems to connect to the network—a critical feature of any switch!
Content Switch A content switch is a special switch that is designed for optimizing data delivery to clients by incorporating features to improve performance such as data caching or load balancing features on the switch. Here is an example of how the switch can load-balance traffic: if you connect two servers into the switch, the switch creates a virtual server using a virtual IP, and when a request comes in to the virtual IP, the switch then forwards the request to one of the servers connected to the switch. The result is that the load is balanced across both servers and performance is increased.

Routers and Brouters
One of the most popular network devices along with a switch is a network router. A router is responsible for sending data from one network to another and is a layer-3 device. This section will introduce you to routers and brouters.

Routers
Routers are layer-3 devices and are responsible for routing, or sending data from one network to another. A router will have multiple network interfaces, with each network connecting to a network or a WAN environment.
Routers are typically used to connect the LAN to a WAN environment by having a network interface and a WAN interface connecting to each type of network. The router then passes data from one interface to the other.
Routers work with layer-3 addresses, which are logical addresses assigned to the systems that are used to determine how to reach the destination network. Routers use a routing table stored in memory on the router to determine how to reach a system on a destination network.
The figure below shows three networks connected by routers. In the figure, notice that if a system on
Network A wants to send data to a system on Network B, it must leave Network A by means of Router 1 and then Router 1 will send the data to Router 2. It is the responsibility of Router 2 to send the data to the destination computer.
Routers are a great way to filter network traffic as well, because they act as a broadcast domain. Traffic will not cross the router unless it is actually destined for a system on the remote network. Most router administrators do not allow broadcasts to pass through the router.



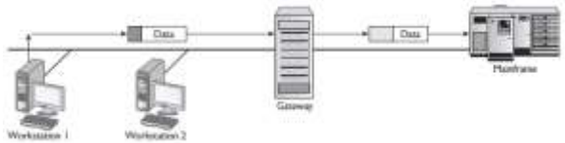
Routers connecting LANs to a WAN

Brouters
A number of network environments use multiple network protocols on the network to support different network applications or services. If you need to route data for one protocol but need the bridging functionality for another protocol, instead of buying both a bridge and a router, you can purchase a brouter. A brouter is the combination of a bridge and a router, and it makes the decision whether it needs to bridge the data or route the data according to the protocol being used. If the protocol is a non-routable protocol such as NetBEUI, the data will be bridged. If the protocol is TCP/IP or IPX/SPX, the routing features of the brouter will be used.

Gateways and Security Devices
Two other types of devices that are found in networking environments are gateways and firewalls. This section discusses gateways and acts as an introduction to security devices such as firewalls and intrusion detection systems.

Gateways
A gateway is responsible for translating information from one format to another and can run at any layer of the OSI model, depending on what information the gateway translates. A typical use of a gateway is to ensure that systems in one environment can access information in another environment. For example, you want to make sure that your PC environment can access information on the company's mainframe.

As shown in the figure below, when the packet reaches the gateway, the gateway strips the packet down and repackages it so that it is understood on the other side of the gateway.
In the figure, notice that the information sent by Workstation 1 has been reformatted after reaching the gateway. Gateways do this by stripping the packet down to just the data and then rebuilding the packet so that it is understood at the destination.



A gateway translates data from one format to another

It is also important to note that when you configure TCP/IP and you configure the "default gateway" setting, you are pointing to the address of the router on the network. It really has nothing to do with an actual "gateway" device.

Firewalls
Firewalls are a networking component responsible for protecting the network from outside intruders. The firewall is designed to block specific types of traffic while allowing certain information to pass through. For example, a firewall that blocks any data that tries to reach the network from the Internet unless it is HTTP traffic. The reason we have allowed HTTP traffic through the firewall is that we would like customers to be able to view the web site. The firewall administrator selectively chooses which traffic can and cannot pass through the firewall.

Intrusion Detection Systems
An intrusion detection system (IDS) is a security device that monitors system or network activity and then notifies the administrator of any suspicious activity. Intrusion detection systems are important devices that will complement other security devices such as firewalls. The IDS is an important device because it will notify you not only of suspicious activity against the firewall, but also of suspicious activity inside the network.
There are two types of intrusion detection systems:

- **Host based -** Host-based intrusion detection systems monitor the local system for suspicious activity. A host-based IDS is typically a piece of software installed on the system and can only monitor activity on the system the IDS was installed on.
- **Network based -** A network-based IDS monitors network traffic for suspicious behavior. A network-based IDS has the capability of monitoring the entire network and comparing that traffic to known malicious traffic patterns. When a match is found an alert can be triggered. Network-based IDSs can be software loaded on a system that monitors network traffic or can be a hardware device.

Intrusion detection systems can be either active or passive. An active IDS will monitor activity, log any suspicious activity, and then take some form of corrective action. For example, if a system is doing a port scan on the network, the IDS may log the activity but also disconnect the system creating the suspicious action from the network.
A passive intrusion detection system does not take any corrective action when suspicious activity has been identified. The passive IDS will simply identify the activity and then log to file any information needed during an investigation. The passive IDS does not take any corrective action.

Wireless Access Points
Wireless access points (WAPs) are network devices that can be connected to the wired network to allow a wireless client to pass through to get access to the wired network and its resources. A wireless access point also is known as a cell, which is a device that transmits and receives radio frequencies between the PCs and network devices with wireless transmitters connected to them. The wireless access point is connected to a physical cable, which connects the WAP device to the rest of the network. The figure below shows an example of a Linksys home router that is a wireless access point as well. Notice the wireless antennas attached to the access point.

The typical home router is a multifunctional device; it acts as a wireless access point, firewall, switch, and router, all wrapped up in one device.

Modems
There are other forms of networking devices beyond the typical network card; for instance, modems can be used to communicate with other systems across the public switched telephone network (PSTN). They are used to convert digital data from the PC to analog transmission so that the information can be transmitted over the analog phone lines. The modem on the receiving end is designed to convert the analog signal to a digital format readable by the system.

CSU/DSU
A channel service unit/data service unit (CSU/DSU) is either one device or a pair of devices that allows an organization to get a very-high-speed WAN connection from the telephone company, such as a T1 or T3 link. The CSU is used at the business end to get the connection to the WAN, and the DSU may be used at the provider's end to allow the CSU to connect.

ISDN
The Integrated Services Digital Network (ISDN) is a communication standard for sending voice and data over normal telephone lines or digital telephone lines. In order to connect to the ISDN lines, a system will need an ISDN modem, which doesn't really act like a modem because, whereas a modem converts digital data to analog, the ISDN modem carries digital data from one digital system to another, and so it really is acting as a terminal adapter connecting you to the ISDN lines.
There are two popular types of ISDN connections:

- **Basic rate interface (BRI) -** This is a 128 Kbps connection that is made up of two 64 Kbps channels (known as B-channels) and one 16 Kbps control channel (known as a D-channel).
- **Primary rate interface (PRI) -** This is a 1.55 Mbps connection that is made up of twenty-three 64 Kbps channels (B-channels) and one 64 Kbps D-channel for signaling and control information.

Wiring Distribution

Plenum vs. Nonplenum

Plenum refers to the space between the ceiling tiles and the floor located above them. This space is typically used to route power and network cables. It is important to use plenum grade cables in this space because if there is a fire and you are not using plenum grade cables, a toxin is given off that could be carried throughout the building, causing harm to individuals. Plenum-grade cabling uses a low-toxicity material for the jacket of the cable in case of fire.

Patch Panel

Most companies have network jacks located in the walls that allow systems to connect to the network. These jacks have cables connected to them that are then routed a long distance to a patch panel in a server room.

The patch panel then has a patch cable that connects to the front of the patch panel and a port on a switch. When a computer connects to the network jack in the wall, the patch cable is used to map that system to the port on the switch. The concept of the patch panel allows ease of administration and flexibility in moving systems from one switch to another without visiting the workstation. The figure below displays a patch panel.

Cross Connects, MDF, and IDF

When wiring the network you will typically have the outside line coming into the building connect to a panel; this panel is known as the main distribution frame, or MDF. From the MDF you would typically connect to other panels, known as intermediate distribution frames (IDFs), which is what the workstations connect to. This hierarchy of MDF and IDF panels allows greater flexibility when rearranging the network at a later time.

A typical example of how the MDF and IDFs are used is that the MDF would connect to the cable coming from outside the building. Then there may be a separate IDF panel representing each floor in the building, with the workstations on a particular floor connecting to the panel associated with that floor.