
Essentials of Broadband Technology

Executive Summary

With a commitment to provide the easiest to use and most economical of networking products, Linksys has created this white paper to provide an overview of the fundamentals of broadband networking. In addition, the Network Everywhere NC100 Fast Ethernet 10/100 Network Card, NP10T Ethernet 10BaseT PC Card, Model BEFRSR41 EtherFast Cable/DSL Router, and the USB100TX EtherFast 10/100 USB Network Adapter are all profiled in this white paper to illustrate the breadth of networking products accessible from Linksys. While Linksys has over 160 different networking products, the purpose of this white paper is to provide insights into the specific products mentioned, in addition to providing a primer on broadband technologies.

Networking Technologies Overview

Since Ethernet was first developed during the 1970s, it has quickly become the basis for the Internet, local-area networks (LANs), and enterprise-wide networks spanning an entire geographic area, called wide-area networks or WANs. These networks have in turn led to the growth of the Internet as a global exchange capable of handling communication and commerce on a 24/7 basis. Clearly, the growth of the Internet is directly attributable to the continued price/performance gains occurring today in network connectivity products from manufacturers such as Linksys. Committed to bringing the most proven networking technologies to market at the best possible price/performance is the hallmark of companies who will be able to capitalize on the high growth the networking marketplace provides.

Ethernet and specifically broadband technologies work through the use of a standard referred to as the Carrier Sense Multiple Access/Collision Detection (CSMA/CD) approach to arbitrating control of a network. In this standard, each workstation on the network waits until there are no packets being sent across the network, and then sends an initial data stream to another system on the network. This approach is called Collision Detection because a collision of packets or data streams can occur on the network when two or more workstations sense an opening on the network and begin to send. The network detects this “collision” of data and each system on the network waits a predetermined length of time to resend. Each of the network connections waits a random length of time before re-submitting a new data stream in order to alleviate repeated collisions.

A network that experiences a collision rate of 30% is still operable and the performance is still acceptable for a majority of applications. When the collision rate reaches 50 – 60%, however, performance begins lagging and applications, even file and printer sharing, become sluggish. With increasingly complex applications and the need for Internet access, more and more networks are facing capacity limitations. Increasing the performance and capacity of networks, as well as efficiently managing the bandwidth provided is driving the adoption of network products to unprecedented levels.

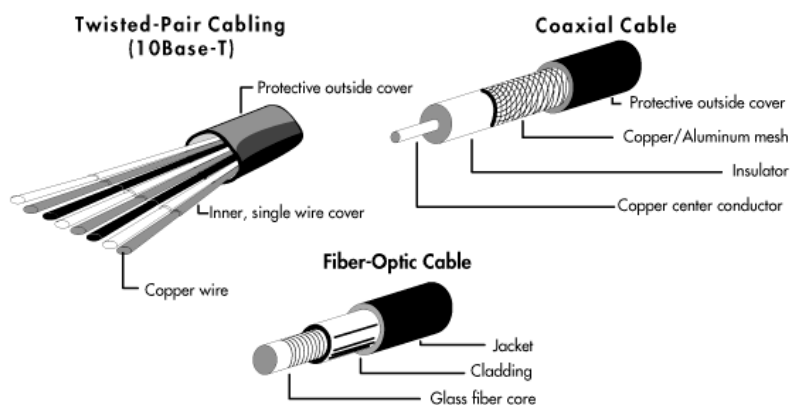
The majority of companies today who have networks use Ethernet or its equivalent, which has a bandwidth of 10 megabits per second (Mbps). With the continued growth of the Internet, coupled with the fact that the majority of network traffic is now graphically-intensive, the need for a faster and more robust bandwidth standard has become quickly apparent. Fast Ethernet works just like Ethernet, including the standardized use of the CSMA/CD for arbitrating control of the network, with the exception that Fast Ethernet operates at 100 Mbps, or 10 times the speed of Ethernet. Linksys is one of the leading companies that provides network interface cards (sometimes called NICs) that can support both 10 and 100 Mbps, even switching between the two speeds when necessary. The ubiquity of 10 Mbps Ethernet connections today serves as a strong foundation for companies to adopt 100 Mbps speeds in their networks. As organizations focus on communicating their uniqueness through graphically-intensive websites, the necessity of a 100 Mbps-based network throughout an organization becomes a given. Just as the benchmark for disk drives is larger capacity, speed is the benchmark for network connectivity products, specifically NICs.

Fundamentals of Network Transmission Media

Data elements in a data stream are generated as electrical signals, either as electromagnetic waves (analog signaling) or as a sequence of voltage pulses (digital signaling). To be sent from one location to another, a signal must travel along a physical path. The physical path that is used to carry a signal between a signal transmitter and a signal receiver is called the *transmission media*.

There are two types of transmission media: guided media and unguided media. Guided media are manufactured so that signals will be confined to a narrow path and include twisted-pair wiring, similar to common telephone wiring; coaxial cable, similar to that used for cable TV; and optical fiber cable. Each of these media offers varying degrees of speed, distance, and reliability. Figure 1 provides a comparison of the various types of cabling used in networking.

Figure 1: Common guided transmission media



When planning a computer network, many designers choose a combination of media, based on the physical circumstances involved and the reliability and data-handling performance required of the network. The objective is to keep costs to a minimum yet provide all parts of the network with the required reliability and performance.

For example, if you needed to build a network consisting of two subnetworks located in separate buildings several miles apart, you might use two or more transmission media. If you did not require the same level of performance on both subnetworks, you might use a different type of wire or cable as the transmission medium on each.

To connect the two subnetworks across town, you might use a T1 or T3 connection. T1 and T3 are dedicated lines (special telephone lines) that support high-speed communications. They can be leased from private companies that specialize in providing communication services. Alternatively, you might use an example of the second medium, Earth's atmosphere, which is unguided, and connect the subnetworks through a microwave link and ensure a reliable connection, unaffected even by rain and fog.

Network Devices and their role on a Network

Once the network transmission media is defined, devices need to be selected for sending and receiving the signals throughout the network. These network connectivity products are designed to propagate a particular type of signal across a particular type of transmission medium. Transmitting and receiving devices used in computer networks include network adapters, repeaters, wiring concentrators, hubs, switches, as well as infrared, microwave, and other radio-band transmitters and receivers.

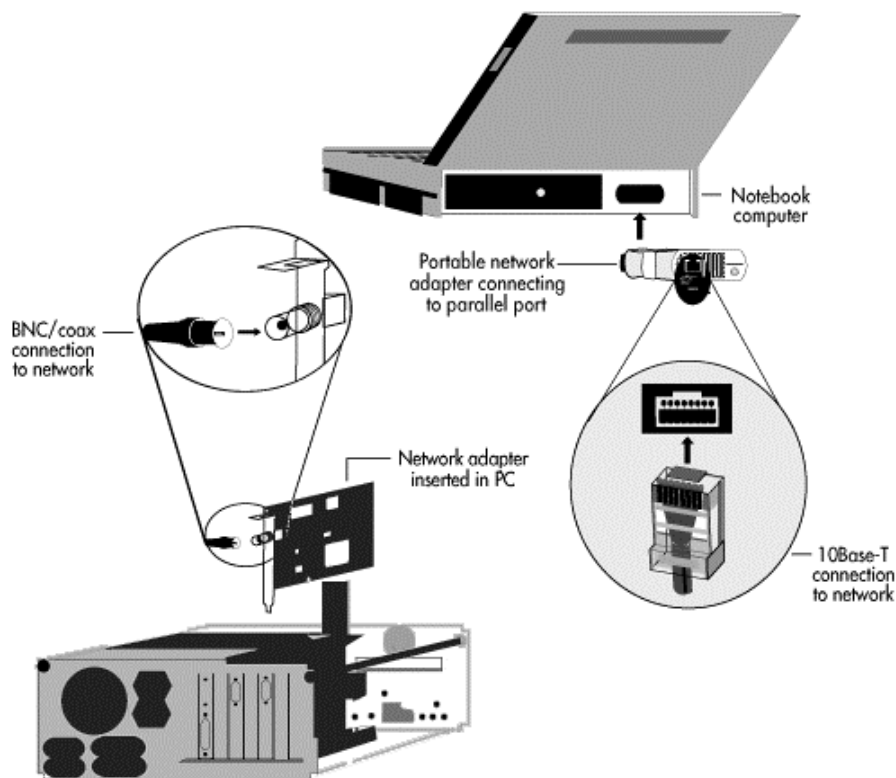
Network Adapters

A network adapter is the hardware installed in computers that enables them to communicate on a network. Network adapters are manufactured in a variety of forms. The most common form is the printed circuit board, which is designed to be installed directly into a standard expansion slot inside a microcomputer. Other network adapters are designed for mobile computing. They are small and lightweight and can be connected to standard connectors on the back of notebook computers so that the computer and network adapter can be easily transported from network to network. Network adapters are now being built into many computers, especially notebook computers.

Network adapters are manufactured for connection to virtually any type of guided medium, including twisted-pair wire, coaxial cable, and fiber-optic cable. They are also manufactured for connection to devices that transmit and receive visible light, infrared light, and radio microwaves, to enable wireless networking across the unguided media of Earth's atmosphere and outer space.

The hardware used to make connections between network adapters and different transmission media depends on the type of medium used. For example, twist-on BNC connectors are commonly used for connection to coaxial cable, while snap-in telephone-type jacks are ordinarily used for connection to twisted-pair wiring. Figure 2 shows two different types of network adapters connected to different computers and media, using different types of connectors.

Figure 2: Network adapters are manufactured in a variety of forms, for virtually every kind of communication medium.



Repeaters

Repeaters are used to increase the distance over which a network signal can be propagated. As a signal travels through a transmission medium, it encounters resistance and gradually becomes weak and distorted. The technical term for this signal weakening is "attenuation." All signals attenuate, and at some point they become too weak and distorted to be reliably received. Repeaters are used to overcome this problem.

A simple, dedicated repeater is a device that receives the network signal and retransmits it at the original transmission strength. Repeaters are placed between other transmitting and receiving devices on the transmission medium, at a point where the signal will not have attenuated too much to be reliably received.

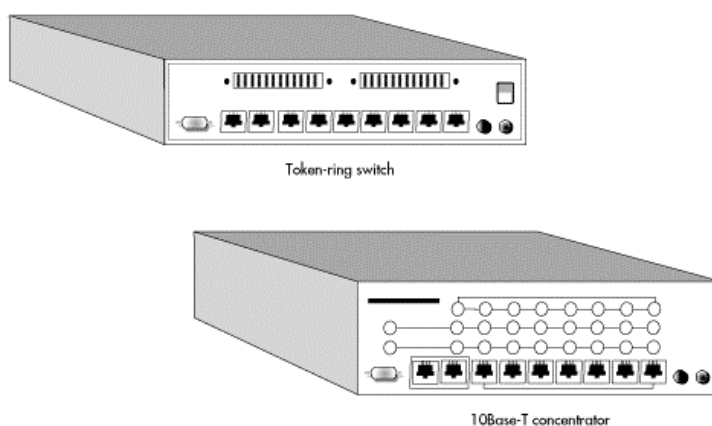
In today's networks, dedicated repeaters are seldom used. Repeating capabilities are built into other, more complex networking devices. For example, virtually all modern network adapters, hubs, and switches incorporate repeating capabilities.

Wiring Concentrators, Hubs, and Switches

Wiring concentrators, hubs, and switches provide a common physical connection point for computing devices. Most hubs and all wiring concentrators and switches have built-in signal repeating capability and thus perform signal repair and retransmission.

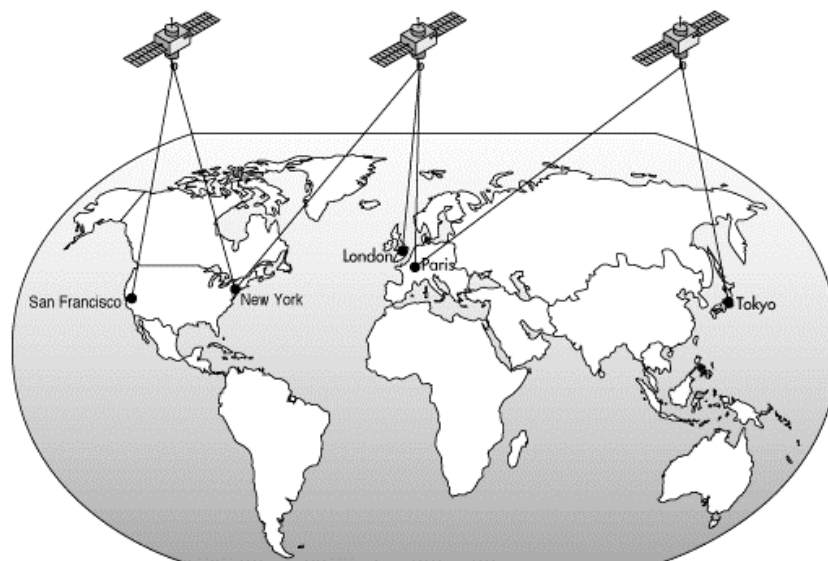
In most cases, hubs, wiring concentrators, and switches are proprietary, standalone hardware. Linksys is one of the leading companies that manufacture such equipment. Occasionally, hub technology consists of hub cards and software that work together in a standard computer. Figure 3 shows two common hardware-based connection devices: a token-ring switch and an Ethernet 10Base-T concentrator.

Figure 3: Token-ring switch and Ethernet 10Base-T concentrator



Microwave Transmitters

Microwave transmitters and receivers, especially satellite systems, are commonly used to transmit network signals over great distances. A microwave transmitter uses the atmosphere or outer space as the transmission medium to send the signal to a microwave receiver. The microwave receiver either relays the signal to another microwave transmitter, which sends it to another microwave receiver, or the receiving station translates the signal to some other form, such as digital impulses, and sends it along on some other suitable medium. Figure 4 shows a satellite microwave link.

Figure 4: Satellite microwave link

Modems

Modems convert digital (computer) signals to analog (audio) signals, and vice versa, by modulating and demodulating a carrier frequency. The most common modems transmit and receive data across ordinary voice-grade telephone lines.

A transmitting modem converts (modulates) the encoded data signal to an audible signal and transmits it. A modem connected at the other end of the line listens to the audible signal and converts it back into a digital signal (demodulates it) for the computer on the receiving end of the communication link. Modems are commonly used for inexpensive, intermittent communications between geographically isolated computers and a main network.

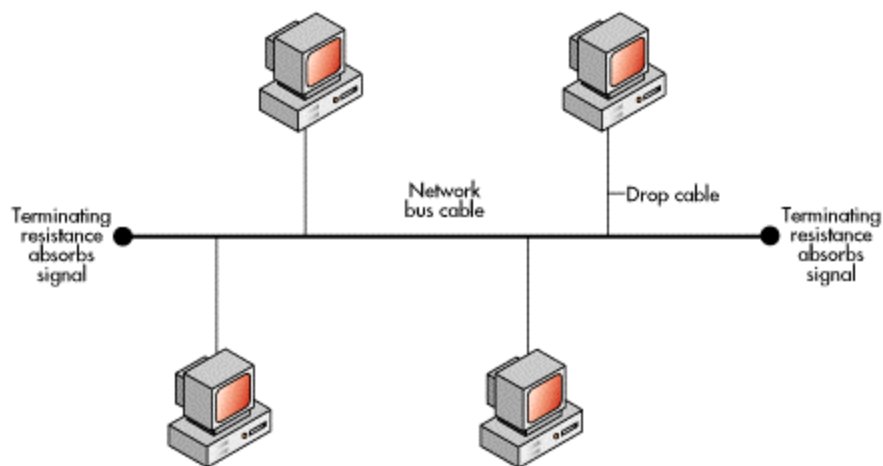
Connecting Network Devices

With the network media defined and the network devices used for connecting workstations throughout a network identified, the next step is the development of a network topology. There are three logical topologies or the electronic schemes used to connect network devices. Physical topology is the physical layout of the guided transmission media. The most common physical topologies are the Bus, the Star, and the Star-Wired Ring.

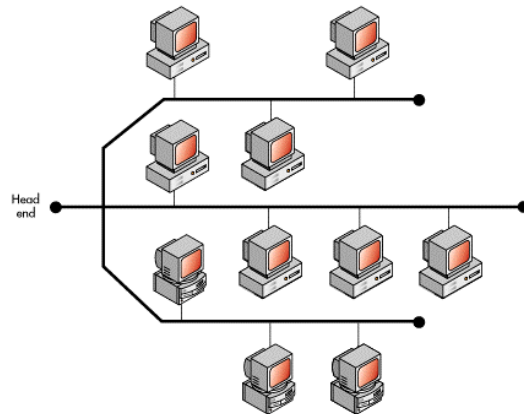
Physical Bus

The simplest form of a physical bus topology consists of a trunk (main) cable with only two end points. When the trunk cable is installed, it is run from area to area and device to device—close enough to each device so that all devices can be connected to it with short drop cables and T-connectors. The signal generated at any point along the bus is sent along the trunk and is eventually absorbed by the terminator. This simple "one wire, two ends" physical bus topology is illustrated in Figure 5.

Figure 5: Physical bus topology



A more complex form of the physical bus topology is the distributed bus (also called the tree topology). In the distributed bus, the trunk cable starts at what is called a "root," or "head end," and branches at various points along the way. (Thus, unlike the simple bus topology described above, this variation uses a trunk cable with more than two end points.) Where the trunk cable branches, the division is made by means of a simple connector. The signal is thus "distributed" throughout the network. The distributed bus topology is illustrated in Figure 6.

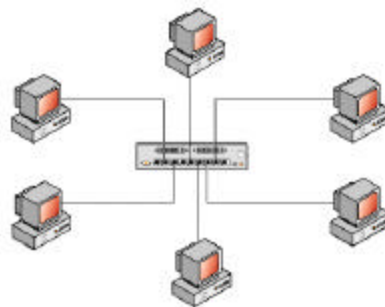
Figure 6: Distributed bus topology

Physical Star

The simplest form of the physical star topology consists of multiple cables—one for each network device—attached to a single, central connection device. For example, 10Base-T Ethernet networks are based on a physical star topology—each network device is attached to a 10Base-T hub by means of twisted-pair cable.

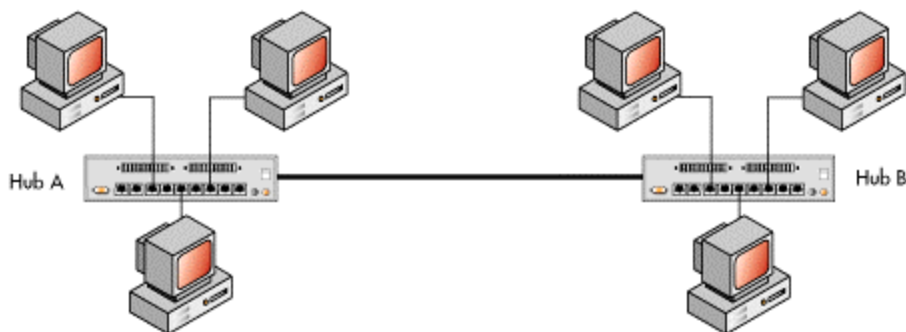
In a real-life implementation of even a simple physical star topology, the actual layout of the transmission media need not form a recognizable star pattern; the only required physical characteristic is that each network device be connected by its own cable to the central connection point.

The simplest form of the physical star topology is illustrated in Figure 7.

Figure 7: Physical star topology

A more complex form of the physical star topology is the distributed star. In this topology, there are multiple central connection points, which are all connected to form a string of stars. This topology is illustrated in Figure 8.

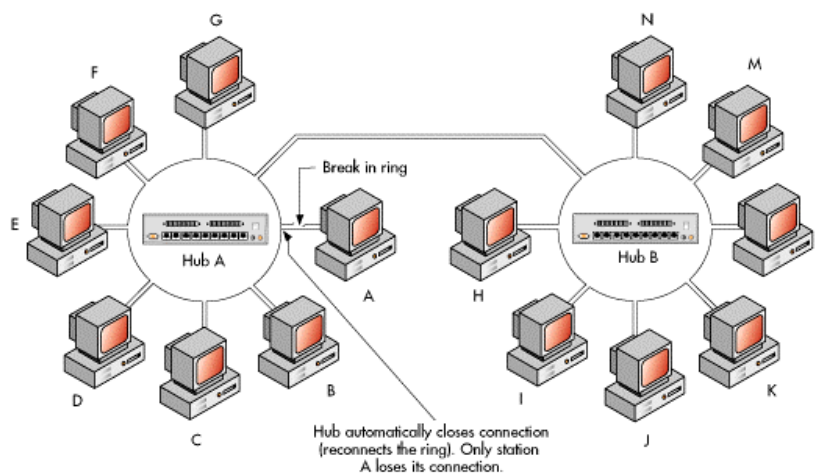
Figure 8: Distributed star topology



Physical Star-Wired Ring

In the star-wired ring physical topology, individual devices are connected to a central hub, as they are in a star or distributed star network. However, within each hub the physical connections form a ring. Where multiple hubs are used, the ring in each hub is opened, leaving two ends. Each open end is connected to an open end in some other hub (each to a different hub) so that the entire network cable forms one physical ring. This physical topology, which is used in IBM's Token-Ring network, is illustrated in Figure 9.

Figure 9: Physical star-wired ring topology



In the star-wired ring physical topology, the hubs are "intelligent." If the physical ring is somehow broken, each hub is able to close the physical circuit at any point in its internal ring so that the ring is restored. Refer to details shown in Figure 9, hub A, to see how this works.

Currently, the star topology and its derivatives are most preferred by network designers and installers because using these topologies makes it simple to add network devices anywhere. In most cases, you can simply install one new cable between the central connection point and the desired location of the new network device, without moving or adding to a trunk cable or making the network unavailable for use by other stations.

Fundamentals of Internetworking

As a business grows, it might need to split its network. Alternatively, a business might need to connect two separate networks so that users on each can use resources on either. When a network is split (or when two networks with different addresses are connected), this results in an internetwork. An internetwork has subnetworks (network segments) that have different network addresses. Even a modest-sized business often has several subnetworks operating, each serving a specific portion of the organization.

The most common reason for segmenting a network is to preserve network performance. On even the fastest and most efficient network, if the network has too many users (devices that need to transmit), the transmission media can become so busy that devices have to wait an unacceptable time to transmit. When this happens, users begin to notice delays when they try to save or open files or perform other operations.

When a network is segmented, each subnetwork is given its own network address. This results in two separate transmission media segments, which can be used simultaneously. Each of the two segments will have only half the users of the original network. Thus, network performance is doubled (on some networks, performance can more than double because on an overloaded network, the overhead required to manage transmission collisions takes a much larger percentage of bandwidth than on a modestly busy network).

Networks are also segmented to enhance data security and to minimize the effect of equipment failure on any part of the network.

Internetworking includes everything from connecting two small workgroup networks, each with perhaps two or three workstations, to connecting thousands of computers—from notebook computers to mainframes—on tens to hundreds of individual segments in a worldwide organization.

Internetworking Devices: Bridges and Routers

Bridges and routers are the devices used to interconnect subnetworks. They can be either hardware or software based. Software-based routers and bridges can be part of a server's operating system or can at least run in the server with the operating system. Hardware-based bridges and routers can also be installed on standard computers to create dedicated, standalone devices.

To understand internetworking, it is not essential that you understand all the technical differences between a bridge and router. In fact, without some study, this can be a confusing area. For example, if you read about multiprotocol Routers, you will find that these routers also perform what is called source-route bridging.

However, without a basic understanding of bridging and routing technology, you will find it difficult to understand the capabilities of some products and the reasons such capabilities are useful or important. Keep in mind that bridges and routers have one important thing in common: They both allow the transfer of data packets (frames) between subnetworks with different network addresses.

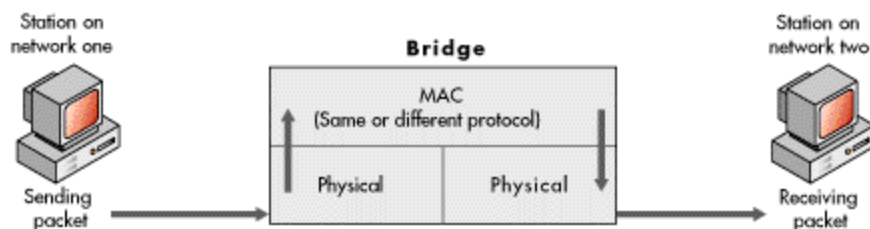
Bridges

A bridge operates at the data-link layer (layer two) of the OSI model. A bridge acts as an address filter; it relays data between subnetworks (with different addresses) based on information contained at the media access control level.

Simple bridges are used to connect networks that use the same physical-layer protocol and the same MAC and logical link protocols (OSI layers one and two). Simple bridges are not capable of translating between different protocols.

Other types of bridges, such as translational bridges, can connect networks that use different layer-one and MAC-level protocols; they are capable of translating, then relaying, frames. After a physical connection is made (at OSI layer one), a bridge receives all frames from each of the subnetworks it connects and checks the network address of each received frame. The network address is contained in the MAC header. When a bridge receives a frame from one subnetwork that is addressed to a workstation on another subnetwork, it passes the frame to the intended subnetwork.

Figure 10: Internetworking through a bridge



Spanning Trees and Source-Route Bridging

There are two terms connected with bridging that will be useful to understand: spanning trees and source-route bridging.

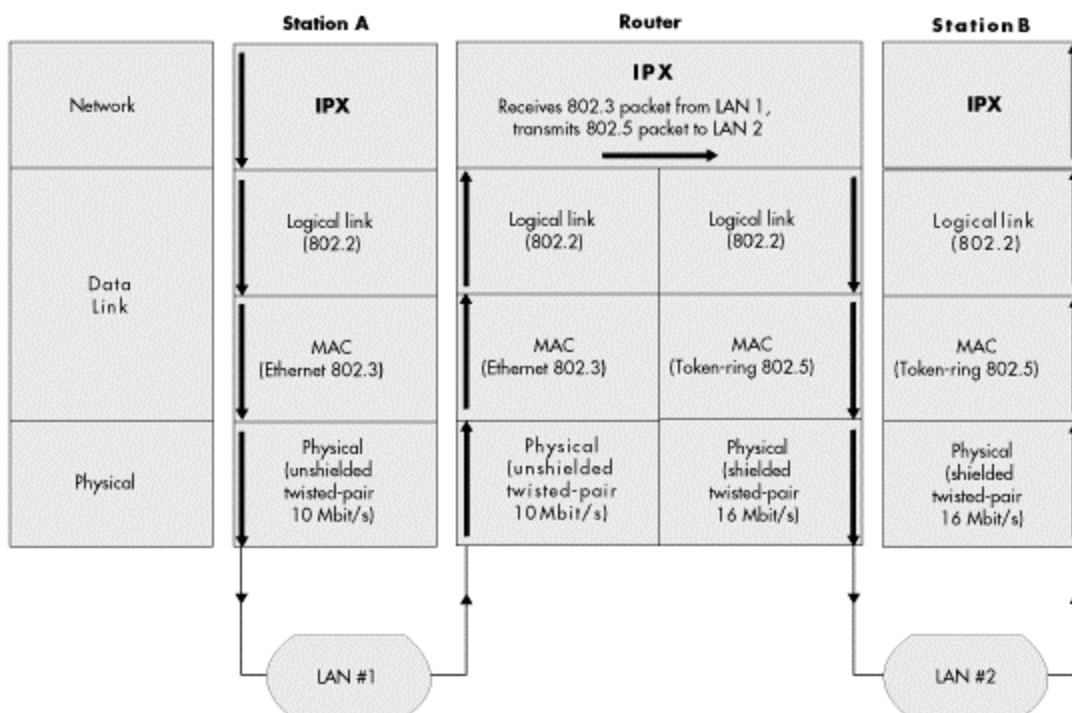
Spanning trees prevent problems resulting from the interconnection of multiple networks by means of parallel transmission paths. In various bridging circumstances, it is possible to have multiple transmission routes between computers on different networks. If multiple transmission routes exist, unless there is an efficient method for specifying only one route, it is possible to have an endless duplication and expansion of routing errors that will saturate the network with useless transmissions, quickly disabling it. Spanning trees are the method used to specify one, and only one, transmission route.

Source-route bridging is a means of determining the path used to transfer data from one workstation to another. Workstations that use source routing participate in route discovery and specify the route to be used for each transmitted packet. Source-route bridges merely carry out the routing instructions placed into each data packet when the packet is assembled by the sending workstation—hence the name "source routing." In discussions of bridging and routing, do not be confused by the term "source routing." Though it includes the term "routing," it is a part of bridging technology. Source-route bridging is important because it is a bridge-routing method used on IBM Token-Ring networks.

Routers

Routers function at the network layer of the OSI model (one layer above bridges). To communicate, routers must use the same network-layer protocol. And, of course, the sending and receiving workstations on different networks must either share identical protocols at all OSI layers above layer three, or there must be necessary protocol translation at these layers. Like some bridges, routers can allow the transfer of data between networks that use different protocols at OSI layers one and two (the physical layer and the data-link layer, which includes sublayers for media access control and logical link control). Routers can receive, reformat, and retransmit data packets assembled by different layer-one and layer-two protocols. Different routers are built to manage different protocol sets. Figure 11 illustrates how a router transfers data packets.

Figure 11: Internetworking through a router

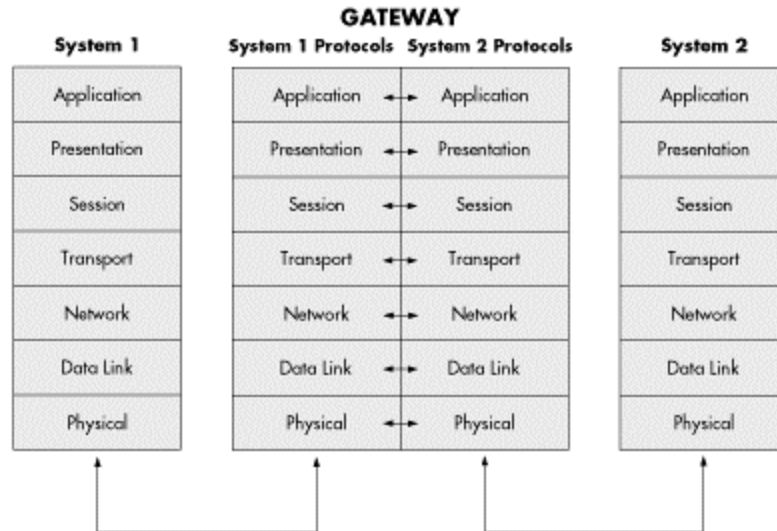


Gateways

In contrast to bridges and routers, which function at only one layer of the OSI model, a gateway translates protocols at more than one OSI layer. Therefore, a gateway is used to interconnect computer systems that have different architectures and that therefore use different communication protocols at several OSI layers.

A gateway may connect dissimilar systems on the same network or on different networks (thus, using a gateway does not necessarily involve internetworking). For example, a gateway might translate protocols at several different OSI layers to allow transparent communications between IPX-based systems and systems based on TCP/IP, System Network Architecture (SNA), or AppleTalk. Figure 12 illustrates how a gateway is used to translate protocols to enable communications between two heterogeneous systems.

Figure 12: Gateways provide protocol translation between dissimilar systems at more than one OSI layer.



A gateway may consist of hardware, software, or a combination of the two, and it may provide translation at all or at only some of the different OSI layers, depending on the types of systems it connects.

Exploring the NC100 Faster Ethernet 10/100 Network Card

Fast Ethernet is a relatively new standard of networking built specifically for speed-intensive network applications such as video-conferencing, multimedia development, imaging, and complex databases. Capable of sending and receiving data at 100 megabits-per-second over 4 wires in half duplex mode, and 200Mbps in full duplex, Fast Ethernet technology is 10 times faster than traditional 10BaseT networks. Figure 13 shows the NC100 and packaging from Linksys.

Figure 13: The Linksys NC100



Built to run with the fastest network applications, the Fast Ethernet 10/100 Network Card is a high performance network adapter for desktop computers with 32-bit PCI expansion slots. Boasting an incredible maximum data throughput of 200 megabits per second in full duplex mode (100Mbps in half duplex), the Fast Ethernet is ready to run with both 10BaseT and 100BaseTX networks right out of the box – the card's 10/100 auto-sensing port automatically detects your network's maximum speed and adjusts itself accordingly.

Here are the specifics on the NC100:

System:	PCI 2.1 (or higher) compliant PC
Standards:	IEEE 802.3, IEEE 802.3u, PCI 2.1 or higher
Protocol:	CSMA/CD
Port:	One Auto-sensing RJ-45 10/100 Port
Speed: (Mbps)	Full Duplex 200/20 (Aggregate) Half Duplex 100/10
Cabling Type:	Category 3 (10BaseT) Category 5 (100BaseTX) included
Topology:	Star
LED Status Lights:	Link/Activity (Link/Act), 100Mbps (100)
Environmental	
Dimensions:	5" x 2.3" x 0.75" (127 x 58 x 19 mm)
Unit Weight:	2 oz.
Power:	2W Maximum
Certifications:	FCC Class B, CE Mark Commercial
Operating Temperature:	0°C - 50°C (32°F - 122°F)
Storage Temperature:	-20°C - 70°C (-4°F - 158°F)

Operating Humidity: 10% - 85% Non-Condensing
Storage Humidity: 5% - 90% Non-Condensing

Driver Downloads: www.networkeverywhere.com/downloads.html

Exploring the NP10T Ethernet 10BaseT PC Card

The Network Everywhere Ethernet 10BaseT PC Card is a 10Mbps network adapter for notebook computers with 16 or 32-bit PCMCIA expansion slots. Ready to run right out of the box at home, in the office, or on the road, the 10BaseT PC Card offers is compatible with Windows 98, 95 and NT 4.0, and Windows2000. Figure 14 shows the NP10T Ethernet 10BaseT PC Card.

Figure 14: Linksys NP10T Ethernet 10BaseT PC Card



Product Features

Standard:	IEEE 802.3 PCMCIA Type II 16-Bit
Speed:	10Mbps
Port:	1 RJ-45 on detachable coupler
LED Indicators:	Link, Activity Indicator
Bus Type:	PCMCIA Type II 16-Bit
Certification:	FCC Class B, CE Mark
Cabling:	Category 3 or 5 UTP or STP
Dimensions:	3.6" x 2.2" x 0.3"
Weight:	2.2 oz

Product Benefits

- Connects to any 10Mbps Network
- 10BaseT Cable Port on Detachable Coupler
- Works in Virtually Any PCMCIA Type II slot
- Easy Installation and Setup
- Low Power Consumption - Autosleep Mode
- Hot Swappable
- Compatible with Virtually All Notebooks
- 16KB Buffer for Fast File and Transfers
- Works With Most Major NOS
- Compatible with Windows 98, 95 and NT
- NE2000 Compatible
- Easy-to-Read Status Lights on the Coupler
- Free Technical Support
- 5-Year Limited Warranty

Driver Downloads: www.networkeverywhere.com/downloads.html

Exploring the Linksys BEFRS41 Router

The EtherFast Cable/DSL Router is the perfect option to connect a small group of PCs to a high-speed Broadband Internet connection or to an Ethernet backbone. Configurable as a DHCP server, the EtherFast Cable/DSL Router acts as the only externally recognized Internet device on your local area network (LAN). The Router serves as an Internet firewall, protecting your network from being accessed by outside users. All incoming data packets are monitored and filtered. The router can also be configured to block internal users' access to the Internet.

Features

- DMZ Host option provides two-way communication between one PC and your Internet services.
- Connects to a Broadband modem or to an Ethernet backbone.
- Equipped with a 4-port 10/100 Switch (BEFSR41 only).
- Connects all of your PCs to the Internet with only one purchased IP address.
- Creates a firewall to protect your PCs from outside intruders.
- Configurable through any networked PC's web browser using Netscape or Internet Explorer 4.0 or higher.
- Supports IPsec Pass-Thru which is remotely administered through your internet connection.
- The switch dramatically speeds up your gaming and multimedia connections.
- Can simultaneously act as both a DHCP Server on the LAN and a DHCP Client on the WAN.
- Compatible with virtually all standard Internet applications.
- Administrators can block specific interior users' Internet access.

Connecting to the Linksys BEFSRU41

The rear panel of the Router is where all of the Router's connections are made.



WAN The WAN (Wide Area Network) Port is where you will connect your cable or DSL modem.

Uplink The Uplink Port is where you can expand your network by connecting to another switch or hub. The Uplink Port is shared with Port 1. Uplinking to another Router, switch or a hub is done by simply running a cable from the Uplink Port to the other device. If the Uplink port is being used, Port 1 will not work.

Ports 1-4 These four LAN (Local Area Network) ports are where you will connect networked devices, such as PCs, print servers, remote hard drives, and anything else you want to put on your network. If Port 1 is being used, the Uplink Port will not work.

Power The Power Port is where you will connect the included AC Power adapter.

Status Indicators on the Linksys BEFSRU41



The LAN Indicators

Power Green. The Power LED illuminates when the Router is powered on.

Link/Act Green. The Link/Act LED serves two purposes. If the LED is continuously illuminated, the Router is successfully connected to a device through the corresponding port (1, 2, 3 or 4). If the LED is flickering, the Router is actively sending or receiving data over that port.

Full/Col Green. The Full/Col LED also serves two purposes. If this LED is continuously illuminated, the connection made through the corresponding port is successfully running in Full Duplex mode. If the LED is flickering, the connection is experiencing collisions. Infrequent collisions are normal. If this LED is flickering too often, there may be a problem with your connection. Check the Troubleshooting section on page 30 if you think there is a problem.

100 or 10/100 Orange. The 100 LED illuminates when a successful 100Mbps connection is made through the corresponding port.

The WAN Indicators

Link Green. The Link LED illuminates when a successful connection is made between the Router and your Broadband device or network.

Act Green. The Act LED flickers when the Router is sending or receiving data over the broadband port.

Diag Red. The Diag LED illuminates when the Router goes through its self-diagnosis mode during boot-up. It will turn off upon successful completion of the diagnosis. If this LED stays on for an abnormally long period of time, refer

BEFSRU41 4-Port Router Specifications

Standards	IEEE 802.3 10BaseT, 802.3u 100BaseTX
Protocol	CSMA/CD
Ports	Four 10/100 RJ45 Switched connectors (LAN) One 10Base-T Ethernet RJ-45 connector for ADSL/Cable Modem
Speed Router	10Mbps, Switch - 10/100Mbps
Cabling Type	10BaseT: UTP/STP Category 3 or 5 100BaseTX: UTP/STP Category 5
Topology	Star
LED Indicators	Power, Link/Activity, Full Duplex/Collision, Speed for LAN. Link, Activity, Diag for WAN

Environmental

Dimensions	142 x 236 x 46 mm (5.6 x 9.3 X 1.8 inches)
Unit Weight	12 oz.
Power Input	External, 5VDC 3A
Certifications	FCC Class B, CE Mark Commercial
Operating Temp.	0°C to 40°C (32°F to 104°F)
Storage Temp.	-20°C to 70°C (-4°F to 158°F)
Operating Humidity	10% to 85% non-condensing
Storage Humidity	5% to 90% non-condensing

Exploring the USB100TX

Now you can connect to any 10, 100, or 10/100Mbps hub or switch without having to open your PC. The EtherFast 10/100 USB Network Adapter from Linksys allows you to instantly connect to a network from a USB-enabled desktop or notebook PC with Windows 98 or Windows 2000.

The Plug-and-Play compatible adapter attaches to any USB-enabled Windows 98 or Windows 2000 PC. Connect a standard network cable into the other end the EtherFast 10/100 USB Network Adapter, install the included network software drivers, and go

The EtherFast 10/100 USB Network Adapter is bus-powered—it draws power from the host PC and requires no external power cords. The 10/100 USB Network Adapter features a maximum of 12Mbps throughput (the maximum throughput supported by USB), easy-to-read LEDs, compact design, a 1-year limited warranty, and free world-class technical support

Features

- One B-type (Female) USB Port For a Standard USB Cable
- One RJ-45 10/100 Port For a Category 3 or 5 Cable
- 32K Memory Buffer
- Powered by the Host PC—No External Power Supply Needed
- Compact Design-Perfect for Use with Notebook PCs
- RJ-45 Network Port Connects to Any 10, 100, or 10/100Mbps Hub or switch
- Easy-to-Read Link and Activity LED Indicators
- Plug-and-Play Compatible with Windows 98 and Windows 2000 for Easy Installation
- Free Technical Support 24 hours a day (North America Only)
- 1-Year Limited Warranty

Specifications

Model Number:	USB100TX
Standards:	IEEE 802.3 IEEE 802.3u, USB v1.0 or higher
Protocol:	CSMA/CD
Ports:	1 USB Type B Port 1 10BaseT/100BaseTX Auto-Sensing RJ-45
Speed:	10Mbps (Ethernet), 100Mbps (Fast Ethernet)
Cabling:	UTP/STP Category 5 (or better)
Topology:	Star
Bus Speed:	12Mbps (Buffered) Universal Serial Bus
LED Status Lights:	Link, TX/RX

Environmental

Dimensions:	3.8" x 2.6" x 1.2" (97 x 66 x 30 mm)
Unit Weight:	5.0 oz. (156 g)
Power:	5v Bus Powered from PC
Certifications:	FCC Class B, CE Mark (Commercial)
Operating Temperature:	32°F to 122°F (0°C to 49°C)
Storage Temperature:	-4°F to 158°F (-20°C to 70°C)
Operating Humidity:	10% to 85% Non-Condensing
Storage Humidity:	5% to 90% Non-Condensing

Learning About USB

USB, which is short for Universal Serial Bus, is a technology designed to make connecting devices to computers easier. Originally developed in 1996 by a group of computer industry leaders that included Compaq, Digital, IBM, Intel, Microsoft, NEC, and Northern Telecom, USB is quickly becoming the first choice for users who want to add peripherals to their computers.

USB is unique because it is Plug-and-Play, which allows a computer to instantly recognize when a device like a keyboard, mouse, or scanner has been connected to it. Once the device has been recognized, it's ready to go. No special setup is required. Similarly, USB supports hot swapping -- the insertion or removal of devices while the computer is turned on. You can swap one device for another without having to power down your system or install any special software -- it really is that easy.

Another unique USB feature is its ability to allow multiple devices to be connected to a computer's single USB port. When used in conjunction with a USB 4-Port Hub, (Linksys Model: USBHUB04), all four ports can operate simultaneously and independent of each other, allowing easy access to an enormous array of different devices at the same time. Hubs and devices can be connected together -- you can connect up to 127 devices to a PC's USB port.

Some of the devices that USB supports include digital cameras and scanners, joysticks, gamepads, virtual reality headgear and gloves, keyboards, hard drives, mice, modems, phones, printers, speakers, and more.

Glossary

Access Point – Linksys' wireless-based device for connecting roaming wireless PC cards directly to the Internet. The Access Point is a device that provides the benefits of roaming and mobility from a stationary Internet connection.

ADSL—Asymmetric DSL. A DSL technology providing asymmetrical bandwidth over a single wire pair. The downstream bandwidth going from the network to the subscriber is typically greater than the upstream bandwidth going from the subscriber to the network.

ATM—Asynchronous Transfer Mode. Under ATM, multiple traffic types (such as voice, video, or data) are conveyed in fixed-length cells (rather than the random-length "packets" moved by technologies such as Ethernet and Fiber Distributed Data Interface [FDDI]). This enables very high speeds, making ATM popular for demanding network backbones. With networking equipment that has recently become available, ATM will also support WAN transmissions. This feature makes ATM valuable for large, dispersed organizations.

Backbone—The part of a network that acts as the primary path for traffic moving between, rather than within, networks.

Bandwidth—The "data-carrying" capacity of a network connection, used as an indication of speed. For example, an Ethernet link is capable of moving 10 million bits of data per second. A Fast Ethernet link can move 100 million bits of data per second—10 times more bandwidth.

Bridge—A device that passes packets between multiple network segments using the same communications protocol. If a packet is destined for a user within the sender's own network

segment, the bridge keeps the packet local. If the packet is bound for another segment, the bridge passes the packet onto the network backbone.

Cable modem—A class of modem that is used for connecting to a cable TV network, which in turn connects directly to the Internet. Cable-modem based connections to the Internet are typically much faster than dial-up modems, yet have the issue of security, as a cable-based network is comparable to a closed network.

Client—A networked PC or terminal that shares "services" with other PCs. These services are stored on or administered by a server.

Digital Subscriber Line—A digital phone services that provides for voice, video and digital data over existing phone systems at higher speeds than are available in typical dial-up Internet sessions.

DSL modem—A modem that connects a PC to a DSL network, which in turn connects to the Internet.

DSL—digital subscriber line. A public network technology that delivers high bandwidth over conventional copper wiring at limited distances. There are four types of DSL: ADSL, HDSL, SDSL, and VDSL. All are provisioned via modem pairs, with one modem located at a central office and the other at the customer site. Because most DSL technologies do not use the whole bandwidth of the twisted pair, there is room remaining for a voice channel.

Ethernet—A popular LAN technology that uses CSMA/CD (collision detection) to move packets between workstations and runs over a variety of cable types at 10 Mbps. Also called 10BASE-T.

Extranet—A network that provides external users (such as suppliers, independent sales agents, and dealers) access to company documents such as price lists, inventory reports, shipping schedules, and more.

Fast Ethernet—Uses the same transmission method as 10-Mbps Ethernet (collision detection) but operates at 100 Mbps- 10 times faster. Fast Ethernet provides a smooth upgrade path for increasing performance in congested Ethernet networks, because it uses the same cabling, applications, and network management tools. Variations include 100BASE-FX, 100BASE-T4, and 100BASE-TX.

FDDI—Fiber Distributed Data Interface, a LAN technology based on a 100- Mbps token-passing network running over fiber-optic cable. Usually reserved for network backbones in larger organizations.

Frame Relay—Wide-area network service that provides switched ("on-and-off") connections between distant locations.

FTP—File Transfer Protocol, a part of the chief Internet protocol "stack" or group (TCP/IP), used for transferring files from Internet servers to your computer.

Gigabit Ethernet—The latest version of Ethernet. It offers 1000-Mbps (1-gigabit per second [Gbps]) raw bandwidth, that is 100 times faster than the original Ethernet, yet is compatible with existing Ethernets, because it uses the same CSMA/ CD and Media Access Control (MAC) protocols. Gigabit Ethernet competes most directly with ATM and is forcing out FDDI and Token Ring.

Home Phonenumber Networking Alliance (HomePNA)—An organization that works to ensure that all products sold into the home networking marketplace adopt a single, unified phonenumber networking standard. This is specifically done to bring a unified set of interoperable home networking solutions to the marketplace. Linksys is a member of the HomePNA association.

HTML—Hypertext Markup Language, a simple document formatting language used for preparing documents to be viewed by a tool such as a worldwide Web browser.

HTTP—Hypertext Transfer Protocol, a protocol that governs transmission of formatted documents over the Internet.

Hub – A networking device that enables attached devices to receive data streams that are transmitted over a network. This device also makes it possible for devices to share the network bandwidth available on a network.

Hub—A device that interconnects clients and servers, repeating (or amplifying) the signals between them. Hubs act as wiring "concentrators" in networks based on star topologies (rather than bus topologies, in which computers are daisy-chained together).

IDSL—ISDN digital subscriber line, a DSL technology that is basically a naming convention for an ISDN Basic Rate Interface (BRI), both B channels and the D channels permanently bonded for 144 kbps over a single wire pair. ISDN digital subscriber line (IDSL) uses 2B1Q line coding.

Internet—A massive global network, interconnecting tens of thousands of computers and networks worldwide and accessible from any computer with a modem or router connection and the appropriate software.

Intranet—An internal network that takes advantage of some of the same tools popularized on the Internet (browsers for viewing material, HTML for preparing company directories or announcements, and so on).

IP telephony—IP telephony combines different types of communications—such as data, voice, and video—over a single packet cell-based infrastructure. IP telephony extends the value of the network with these nontraditional applications. By combining different types of traffic on a single network connection, small and medium-sized businesses and small branch offices can dramatically reduce the costs of their voice and data networks.

ISDN—Integrated Services Digital Network, a communication protocol offered by telephone companies that permits high-speed connections between computers and the network in dispersed locations.

ISP – An acronym that stands for Internet Service Provider. An ISP is typically a company or organization that provides Internet access for individuals and companies.

LAN—Local Area Network, typically, a network or group of network segments confined to one building or a campus. Compare to WAN.

Local Area Network (LAN) – A series of PCs that have been joined together via cabling so that resources can be shared, including file and print services. LANs are increasingly being found in homes, where sharing of Internet access is one of the most dominant uses of this networking approach.

Megabits per second (Mbps) – Defines the speed at which data is travelling, which are measured in millions of per second. This is a measure of a performance of a device.

Modem—Device that enables a computer to connect to other computers and networks using ordinary phone lines. Modems "modulate" the digital signals of the computer into analog signals for transmission, and then "demodulate" those analog signals back into digital language that the computer on the other end can understand.

Network – Typically a collection of devices that include PCs, printers, and storage devices that are connected together for the purpose of sharing information and resources.

Network Interface Card (NIC) – A device that provides for connecting a PC to a network. NIC cards are also called network adapters, are provide the essential link between a device

and the network. NICs are also found in many peripherals including storage subsystems and printers.

Packet—A block of data with a "header" attached that can indicate what the packet contains and where it is headed. Think of a packet as a "data envelope," with the header acting as an address.

Remote-access server—Device that handles multiple incoming calls from remote users who need access to central network resources. A remote-access server can allow users to dial into a network using a single phone number. The server then finds an open channel and makes a connection without returning a busy signal.

Router—Device that moves data between different network segments and can look into a packet header to determine the best path for the packet to travel. Routers can connect network segments that use different protocols. They also allow all users in a network to share a single connection to the Internet or a WAN.

Server—A computer or even a software program that provides services to clients—such as file storage (file server), programs (application server), printer sharing (print server), fax (fax server) or modem sharing (modem server). See also client.

Switch—A device that improves network performance by segmenting the network and reducing competition for bandwidth. When a switch port receives data packets, it forwards those packets only to the appropriate port for the intended recipient. This further reduces competition for bandwidth between the clients, servers, or workgroups connected to each switch port.

Token Ring—LAN technology in which packets are conveyed between network end stations by a token moving continuously around a closed ring between all the stations. Runs at 4 or 16 Mbps.

VPN—Virtual private network, enables IP traffic to travel securely over a public TCP/IP network by encrypting all traffic from one network to another. A VPN uses "tunneling" to encrypt all information at the IP level

Wide Area Network (WAN) – A public or private networks that provides coverage of a broad geographic area, hence the name “wide” in the description. WANs are typically used for connecting several metro areas as part of a larger network. Universities and larger corporations typically use WANs to connect their geographically dispersed locations.