Network Categories

- LAN (Local Area Network)
- MAN (Metropolitan Area Network)
- WAN (Wide Area Network)
- WLAN (Wireless Local Aria Network)

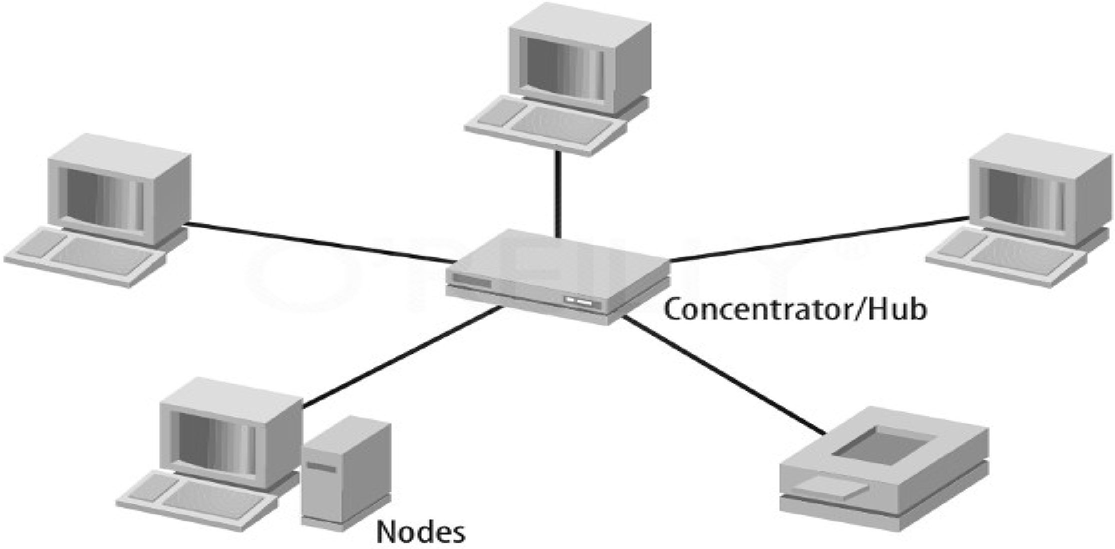
LAN: - A Local Area Network (LAN) is a high-speed communications system designed to link computers and other data processing devices together within a small geographic area, such as a workgroup, department, or building. Several LANs can also be interconnected within a campus of buildings to extend connectivity (also called a Wide Area Network or WAN). This allows users to electronically share vital computing resources, such as expensive hardware

(e.g. printers and CD-ROM drives), application programs, and information.

Local Area Networks implement shared access technology. This means that all of the devices attached to the LAN share a single communications medium, usually a coaxial, twisted-pair, or fiber-optic cable. A physical connection to the network is made by putting a network interface card (NIC) inside the computer and connecting it to the network cable. Once the physical connection is in place, the network software manages communications between stations on the network.

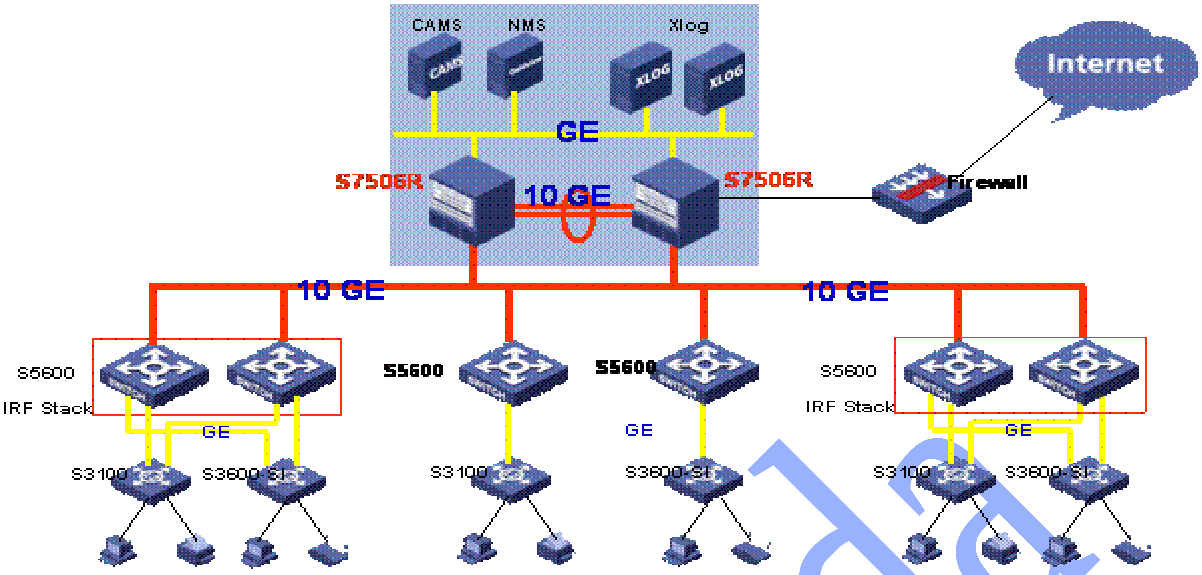
To send messages to and from computers, the network software puts the message information in a packet. (If the message to be sent is too big to fit into one packet, it will be sent in a series of packets.) In addition to the message data, the packet contains a header and a trailer that carry special information to the destination. One piece of information in the header is the address of the destination.
The NIC transmits the packet onto the LAN as a stream of data represented by changes in electrical signals. As it travels along the shared cable, each NIC checks its destination address to determine if the packet is addressed to it. When the packet arrives at the proper address, the NIC copies it and gives its data to the computer. Since each individual packet is small, it takes very little time to travel to the ends of the cable. After a packet carrying one message passes along the cable, another station can send its packet. In this

way, many devices can share the same LAN medium. Each LAN has its own unique topology, or geometric arrangement



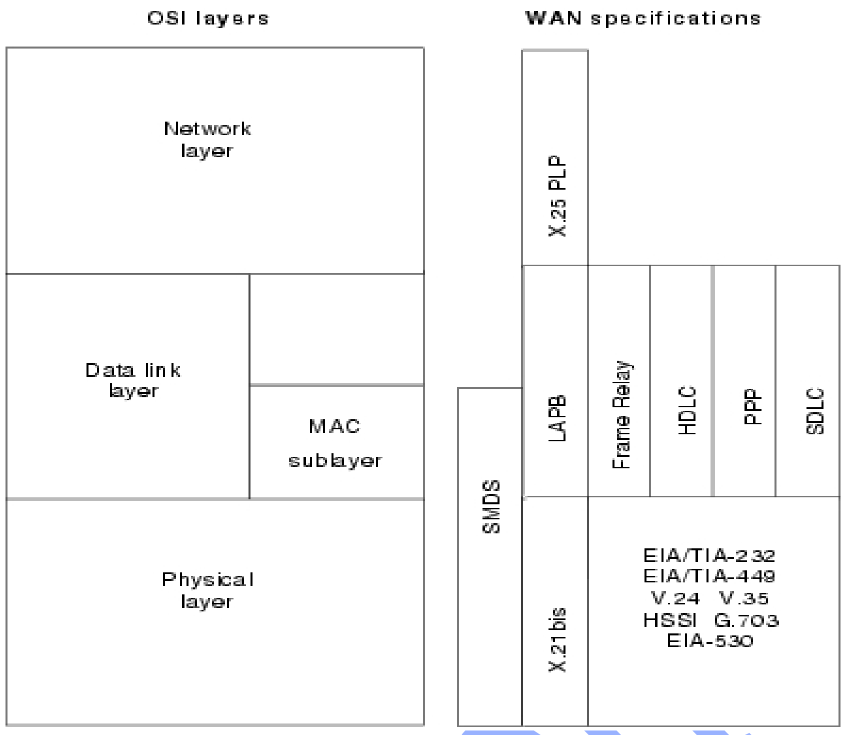
<u>MAN:</u> - A metropolitan area network (MAN) is a network that interconnects users with computer resources in a geographic area or region larger than that covered by even a large local area network (LAN) but smaller than the area covered by a wide area network (WAN). The term is applied to the interconnection of networks in a city into a single larger network (which may then also offer efficient connection to a wide area network). It is also used to mean the interconnection of several local area networks by bridging them with backbone lines. The latter usage is also sometimes referred to as a campus network.

Examples of metropolitan area networks of various sizes can be found in the metropolitan areas of London, England; Lodz, Poland; and Geneva, Switzerland. Large universities also sometimes use the term to describe their networks. A recent trend is the installation of wireless MANs.



WAN: **-** A WAN is a data communications network that covers a relatively broad geographic area and that often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer. Figure 3-1 illustrates the relationship between the common WAN technologies and the OSI model.

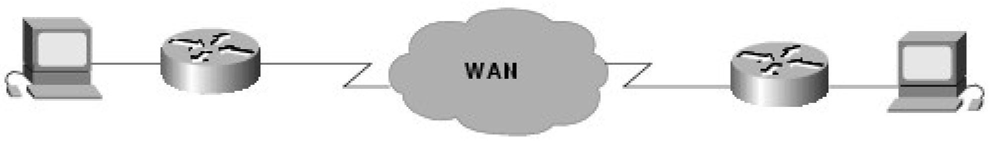
WAN Technologies Operate at the Lowest Levels of the OSI Model



Point-to-Point Links

A point-to-point link provides a single, pre-established WAN communications path from the customer premises through a carrier network, such as a telephone company, to a remote network. Point-to-point lines are usually leased from a carrier and thus are often called leased lines. For a point-to-point line, the carrier allocates pairs of wire and facility hardware to your line only. These circuits are generally priced based on bandwidth required and distance between the two connected points. Point-to-point links are generally more expensive than shared services such as Frame Relay. Figure 3-2 illustrates a typical point-to-point link through a WAN.

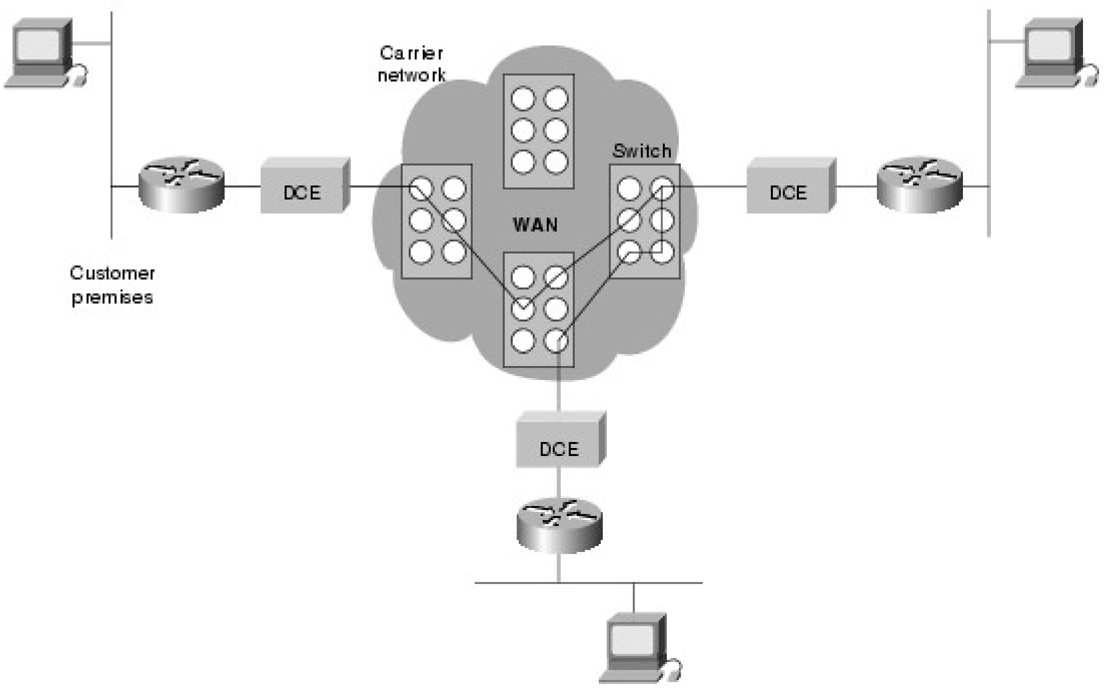
A Typical Point-to-Point Link Operates Through a WAN to a Remote Network



Circuit Switching

Switched circuits allow data connections that can be initiated when needed and terminated when communication is complete. This works much like a normal telephone line works for voice communication. Integrated Services Digital Network (ISDN) is a good example of circuit switching. When a router has data for a remote site, the switched circuit is initiated with the circuit number of the remote network. In the case of ISDN circuits, the device actually places a call to the telephone number of the remote ISDN circuit. When the
two networks are connected and authenticated, they can transfer data. When the data transmission is complete, the call can be terminated. Figure 3-3 illustrates an example of this type of circuit.

A Circuit-Switched WAN Undergoes a Process Similar to That Used for a Telephone Call



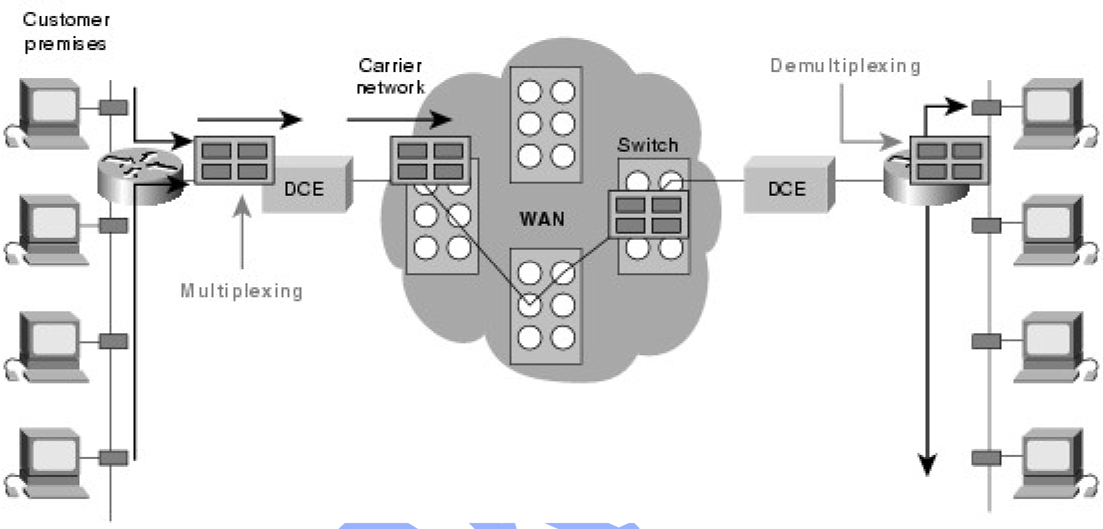
Packet Switching

Packet switching is a WAN technology in which users share common carrier resources. Because this allows the carrier to make more efficient use of its infrastructure, the cost to the customer is generally much better than with point-to-point lines. In a packet switching setup, networks have connections into the carrier's network, and many customers share the carrier's network. The carrier can then create virtual circuits between customers' sites by which packets of data are delivered from one to the other through the network. The section of the carrier's network that is shared is often referred to as a cloud.

Some examples of packet-switching networks include Asynchronous Transfer Mode (ATM), Frame Relay, Switched Multimegabit Data Services (SMDS), and X.25. Figure shows an example packet-switched circuit.

The virtual connections between customer sites are often referred to as a virtual circuit.

Packet Switching Transfers Packets across a Carrier Network



WAN Virtual Circuits

A virtual circuit is a logical circuit created within a shared network between two network devices. Two types of virtual circuits exist: switched virtual circuits (SVCs) and permanent virtual circuits (PVCs).

SVCs are virtual circuits that are dynamically established on demand and terminated when transmission is complete. Communication over an SVC consists of three phases: circuit establishment, data transfer, and circuit termination. The establishment phase involves creating the virtual circuit between the source and destination devices. Data transfer involves transmitting data between the devices over the virtual circuit, and the circuit termination phase involves tearing down the virtual circuit between the source and destination devices. SVCs are used in situations in which data transmission between devices is sporadic, largely because SVCs increase bandwidth used due to the circuit establishment and termination phases, but they decrease the cost associated with constant virtual circuit availability.

PVC is a permanently established virtual circuit that consists of one mode: data transfer. PVCs are used in situations in which data transfer between devices is constant. PVCs decrease the bandwidth use associated with the establishment and termination of virtual circuits, but they increase costs due to constant virtual circuit availability. PVCs are generally configured by the service provider when an order is placed for service.

WAN Dialup Services

Dialup services offer cost-effective methods for connectivity across WANs. Two popular dialup implementations are dial-on-demand routing (DDR) and dial backup.

DDR is a technique whereby a router can dynamically initiate a call on a switched circuit when it needs to send data. In a DDR setup, the router is configured to initiate the call when certain criteria are met, such as a particular type of network traffic needing to be transmitted. When the connection is made, traffic passes over the line. The router configuration specifies an idle timer that tells the router to drop the connection when the circuit has remained idle for a certain period.

Dial backup is another way of configuring DDR. However, in dial backup, the switched circuit is used to provide backup service for another type of circuit, such as point-to-point or packet switching. The router is configured so that when a failure is detected on the primary circuit, the dial backup line is initiated. The dial backup line then supports the WAN connection until the primary circuit is restored. When this occurs, the dial backup connection is terminated.

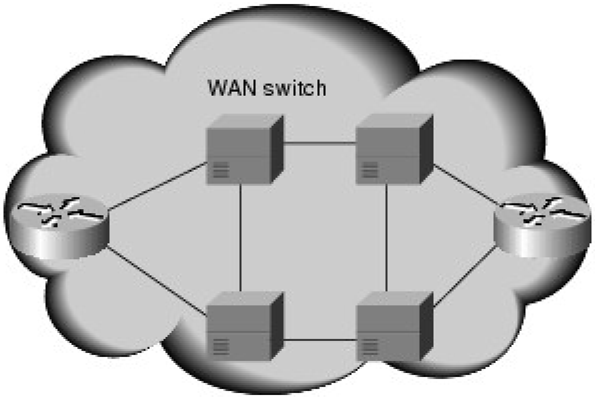
WAN Devices

WANs use numerous types of devices that are specific to WAN environments. WAN switches, access servers, modems, CSU/DSUs, and ISDN terminal adapters are discussed in the following sections. Other devices found in WAN environments that are used in WAN implementations include routers, ATM switches, and multiplexers.

WAN Switch

A WAN switch is a multiport internetworking device used in carrier networks. These devices typically switch such traffic as Frame Relay, X.25, and SMDS, and operate at the data link layer of the OSI reference model. Figure 3-5 illustrates two routers at remote ends of a WAN that are connected by WAN switches.

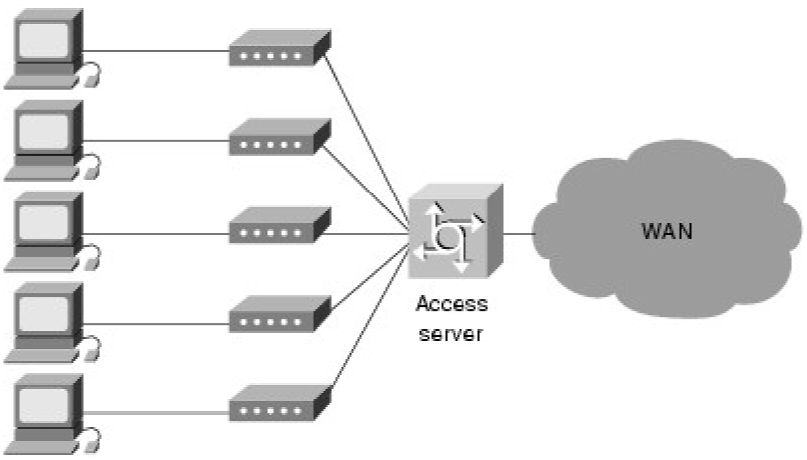
Two Routers at Remote Ends of a WAN Can Be Connected by WAN Switches



Access Server

An access server acts as a concentration point for dial-in and dial-out connections. Illustrates an access server concentrating dial-out connections into a WAN.

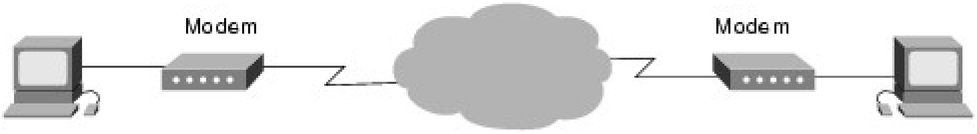
An Access Server Concentrates Dial-Out Connections into a WAN



Modem

A modem is a device that interprets digital and analog signals, enabling data to be transmitted over voice-grade telephone lines. At the source, digital signals are converted to a form suitable for transmission over analog communication facilities. At the destination, these analog signals are returned to their digital form. Figure 3-7 illustrates a simple modem-to-modem connection through a WAN.

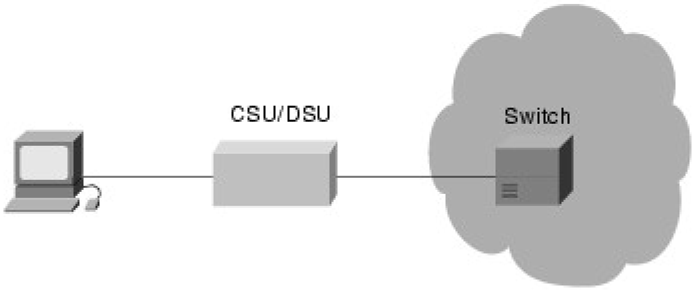
A Modem Connection through a WAN Handles Analog and Digital Signals



CSU/DSU

A channel service unit/digital service unit (CSU/DSU) is a digital-interface device used to connect a router to a digital circuit like a T1. The CSU/DSU also provides signal timing for communication between these devices. Figure 3-8 illustrates the placement of the CSU/DSU in a WAN implementation.

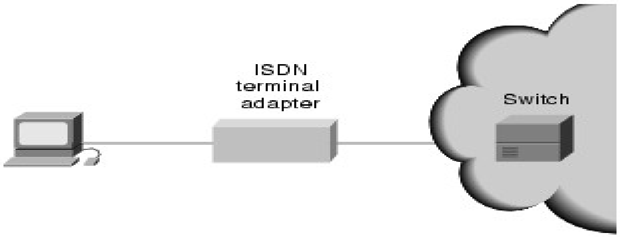
The CSU/DSU Stands between the Switch and the Terminal



ISDN Terminal Adapter

An ISDN terminal adapter is a device used to connect ISDN Basic Rate Interface (BRI) connections to other interfaces, such as EIA/TIA-232 on a router. A terminal adapter is essentially an ISDN modem, although it is called a terminal adapter because it does not actually convert analog to digital signals. Figure 3-9 illustrates the placement of the terminal adapter in an ISDN environment.

The Terminal Adapter Connects the ISDN Terminal Adapter to Other Interfaces



Difference between a LAN, a MAN, and a WAN

A **LAN** (local area network) is a group of computers and network devices connected together, usually within the same building. By definition, the connections must be high speed and relatively inexpensive (e.g., token ring or Ethernet). Most Indiana University Bloomington departments are on LANs. For more information on LANs, see what is a LAN (local area network)?

A **MAN** (metropolitan area network) is a larger network that usually spans several buildings in the same city or town. The IUB network is an example of a MAN.

A **WAN** (wide area network), in comparison to a MAN, is not restricted to a geographical location, although it might be confined within the bounds of a state or country. A WAN connects several LANs, and may be limited to an enterprise (a corporation or an organization) or accessible to the public. The technology is high speed and relatively expensive. The Internet is an example of a worldwide public WAN.

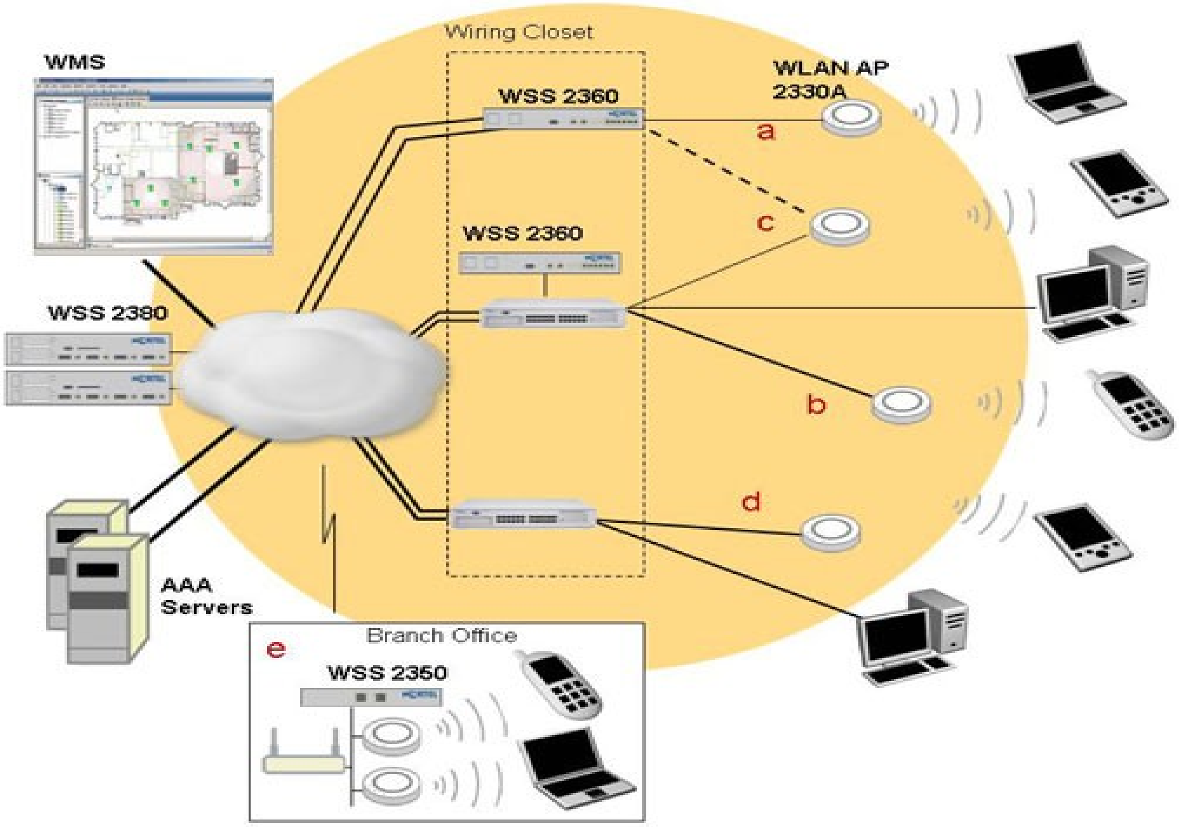
CICNet: - CICNet was founded in 1988 by the Committee on Institutional Cooperation, the academic sister organization of the Big Ten Athletic Conference. From its central hub in Chicago, CICNet connected the networks of the Big Ten schools, as well as numerous other organizations in the Midwest. In 1997, CICNet was acquired by the Internet Access Group, which at the time was another Midwestern Internet service provider (ISP) and was later acquired by Verio.

Until January 1998, CICNet was Indiana University's connection to the national backbone and thus the rest of the Internet. IU's connection to the commodity Internet is now maintained by a connection to a major ISP.

Wireless Technologies

Introduction: - A wireless LAN, or WLAN, is simply a local area network that doesn't rely on wired Ethernet connections. A WLAN can be either an extension to a current wired network or an alternative to it. Use of a WLAN adds flexibility to networking. A WLAN allows users to move around while keeping their computer connected, without having to depend on Ethernet cables.

WLANs try to provide all the features of wired LANs, but without the wires. The only noticeable differences to the end user tend to be in speed (ranging from 1 to 54Mbps, with some manufacturers currently offering proprietary 108Mbps solutions) and security (the wireless access point is shared among everybody nearby, so security issues exist with WLANs that don't exist for wired networks). WLANs can cover areas ranging in size from a small office to a large campus, with neighborhood and city-wide ranges planned for the future. Most commonly, WLANs employ access points that provide access within a radius of 65 to 300 feet. Many companies are developing WLAN technology. The information below was adapted from the Wireless LAN Association web page.



WLAN types

Following are the general types of WLANs:

- **The private home or small business WLAN:** This consists of one or two access points covering around a 100- to 200-foot radius. The equipment is common enough to be found in most office supply or electronics stores, or even some retail stores like Target or Wal-Mart. With few exceptions, hardware in this category subscribes to the 802.11a, b, or g standards (also known as Wi-Fi).

- **The enterprise class WLAN:** This type has a larger number of individual access points covering a wider area. The access points themselves have features not needed for a home or small office, like better security, authentication, remote management, and tools to help integrate with existing networks. Each access point has a larger coverage area than home or small office products, and all are designed to work together to cover a much larger area. Equipment here also adheres to the 802.11a, b, or g standard, and in the future will likely adhere to further security-refining standards such as 802.1x.

- **The Wireless Metropolitan Area Network (WMAN):** The Indiana University wireless network is an example of this. A WMAN covers an area from multiple city blocks up to a city's boundaries. The most common type of WMAN is a collection of individual enterprise class wireless networks that collectively allow users to access all of them. For example, IU's WMAN is a collection of individual buildings' and departments' WLANs taken together as a whole.

  In most places, WMANs usually consist of wireless networks belonging to several businesses or Internet service providers. Take the Kiva Everywhere network as a limited example of this (limited because it's open only to IU users): IU's wireless network (already a WMAN in itself) and Kiva Every where’s network of KSpots together serve as a Bloomington area WMAN for IU users.

  The WMAN is also the point where you start seeing different technologies and standards. Again, the most common WMAN is basically a group of individual access points and WLANs. But different designs, like Angel Technologies' developmental project called the HALO (High Altitude Long Operation) Network would use specially equipped airplanes as airborne wireless access points.

  While you will see the term Metropolitan Area Network (MAN), don't confuse it with a Wireless Metropolitan Area Network (WMAN). Aside from the fact that MANs tend to be wired networks, they usually exist to provide connectivity to local ISPs, or to business and enterprise class LANs. In contrast, a WMAN exists to provide connectivity directly to an end user. In other words, a MAN normally acts as a backbone, while a WMAN acts as the "last mile" connection directly to a user's computer. Exceptions exist, but in broad terms this is true.

- **Wireless WAN (Wide Area Network):** Although a WAN by definition is the exact opposite of a LAN, Wireless WANs (WWANs) deserve brief mention here. Most WANs exist to connect LANs that are not in the same geographical area (for more information, see what is the difference between a LAN, a MAN, and a WAN, and what is a

LAN connection?), and until recently this was also the case for WWANs. But recently, cellular phone companies like Sprint (for Broadband Direct) and AT&T (among others) have begun offering WWAN technology that the end user can access directly. Those WWANs use cellular data technology to cover extremely wide areas. While they are considerably slower than wireless LAN speeds (most advertise between 50 to 144Kbps; compare this to dial-up speeds, which are around 56Kbps), they're still better than the lowest end of DSL speeds (128Kbps), plus they allow far greater mobility than standard 802.11a, b, or g wireless. Since they rely on coverage by the major cellular network providers, coverage areas for wireless Internet access tend to be more or less the same as they are for cell phones. There are many different standards competing at this level (GSM, CDMA, GPRS, 3G, to name a few). Most of them are mobile data standards that previously were used only on cell phones.

Data transmitted through mobile phone signals
Wireless Enabled Notebook

WLAN standards

WLAN standards below the metropolitan level are fairly well defined; most people have heard about 802.11b and g Wi-Fi standards. Some upcoming standards like 3G are attempting to increase range and seamless availability. Others like 802.1x, EAP, and 802.11i are attempting to increase security. Currently, the industry emphasis is on extending range or strengthening security rather than trying to increase speed, but that may change in the future.

802.11a, b, and g: The big three standards

The 802.11a, b, and g standards are by far the most common ones for home wireless access points up through large business wireless systems. The differences in the protocols are these:

802.11a

- Shortest range of the big three standards (generally around 60 to 100 feet)
- Broadcasts in the 5GHz frequency
- Supports up to 54Mbps (megabits per second) speed
- Less able to penetrate physical barriers like walls
- Better speed than 802.11b, supports more simultaneous connections, and because it operates in a more regulated frequency, gets less signal interference from other devices, so is considered to be more consistent in terms of maintaining a connection. In certain circumstances, such as areas with major radio interference (e.g., airports, business call centers), 802.11a will outperform and actually outrange 802.11b.

802.11b

- Better range than 802.11a: up to 300 feet in ideal circumstances, and better than 802.11a even in real-world circumstances (Tests by independent reviewers tend to achieve anywhere from 70 to 150 feet.)
- Broadcasts in the 2.4GHz frequency
- Supports up to 11Mbps speed
- Hardware tends to be lower in cost nowadays.
- Better able than 802.11a to penetrate physical barriers, and lower in cost, but cannot support as many simultaneous connections. Also, it operates on the same frequency as many cordless phones and other appliances; therefore, it is more susceptible to interference and other things that degrade its performance, so it's not considered a good

technology for certain applications requiring absolutely reliable connections, such as live video streaming.

802.11g

- Very close to 802.11b in certain aspects; is actually backwards compatible with 802.11b products (but will run only at 802.11b speeds when operating with them)
- Faster speed than 802.11b; supports up to 54Mbps. Some proprietary solutions (Netgear, Linksys) manage to get 108Mbps out of the 802.11g standard by broadcasting on more than one of the eight channels that 802.11b uses.
- Also uses the 2.4GHz frequency
- Slightly shorter range than 802.11b, but still better than 802.11a. Most independent reviews report around 65 to 120 feet in real-world situations.
- Suffers from the same problems, such as interference and absolute reliability, as 802.11b

Security standards

Wireless 802.11 does provide for some basic security, but as it has become more widespread, the basic security has come to be seen as inadequate. Further security standards have been created, some to extend the basic ones, others to replace the basic standard entirely.

- **WEP (Wired Equivalent Privacy):** One of the earliest security schemas, WEP was originally created for 802.11b, but migrated to 802.11a as well. It simply encrypts the data traffic between the wireless access point and the client computer.

  WEP is generally considered insufficient security nowadays. For starters, WEP simply encrypts the traffic; it doesn't actually secure either end of the transmission. Also, the encryption level is 40 bits, which now is considered very weak.

- **WPA (Wi-Fi Protected Access):** WPA was created in response to the flaws discovered in WEP. WPA implements higher security and addresses the flaws in WEP, but is intended to be only an intermediate measure until further 802.11i security measures are developed. When used in PSK (pre-shared key) mode, WPA-PSK is considered safe enough for most home and small business use, and when combined with technologies like RADIUS and VPN, is considered secure enough for all but the most sensitive enterprise applications.

- **802.1x:** This standard is part of a full WPA security standard. WPA consists of a pair of smaller standards that address different aspects of security: TKIP (Temporal Key Integrity Protocol encryption), which is what encrypts the wireless signal, and 802.1x, which handles the authentication of users to the network. Currently, many wireless systems either have you log into individual wireless access points (home systems work like this), or let you onto the wireless network but keep you from getting anywhere without either further authentication or technology being used. (This is how IU's network works; any wireless device can see the wireless signal and get on the wireless network, but until the device is registered for DHCP and a VPN connection is established, you cannot use the connection to access the Internet. VPN is what authenticates you, but you're already on the wireless network at that point). 802.1x makes you authenticate to the wireless network itself, not an individual access point, and not to some other level like VPN. This is more secure, as unauthorized traffic can be denied right at the wireless access point.

- **802.11i:** This is basically the end point of the process that began with WPA-PSK. It combines that standard with the highest level of encryption yet for a wireless connection (called Advanced Encryption Standard [AES]). The encryption level is high enough that additional dedicated chips are needed on the access points and wireless interface cards to handle the encryption. In summary, 802.11i is the "adult", or finished version of WPA-PSK/TKIP/802.1x/AES