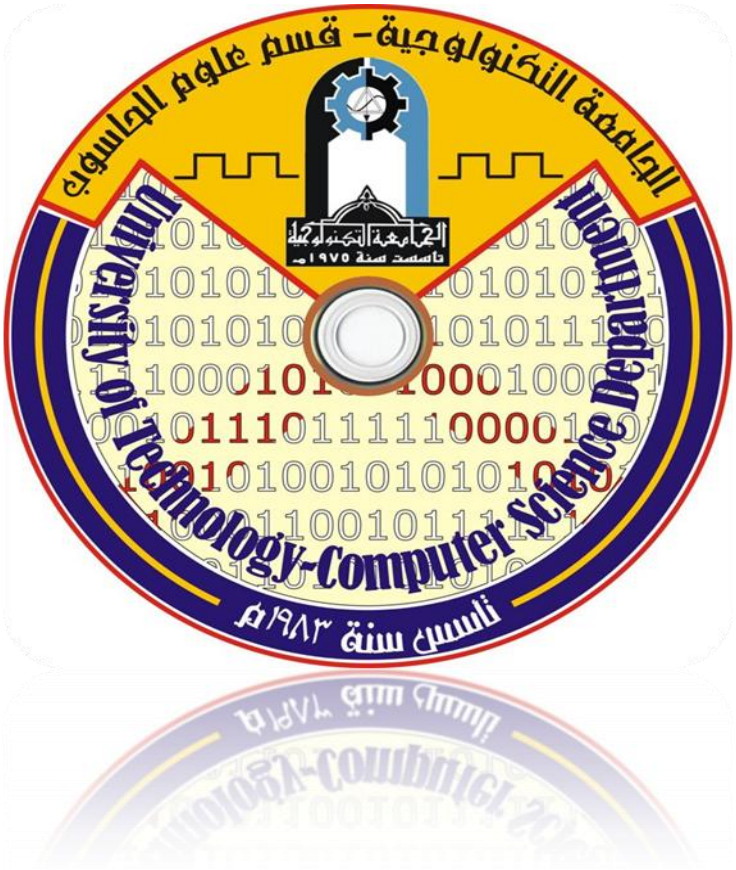


3rd class

Computer Network

شبكات الحاسبة

برمجيات - نظم المعلومات

استاذة المادة: م. إخلاص خلف

1.Introduction to Computer Networks:

Computer networks are defined as:

"Interconnected collection of autonomous computers. Two computers are said to be interconnected if they are able to exchange information."

Or: a network is simply a collection of intercommunicating computers and peripherals possibly having access to remote hosts and other computer networks. A network consists of a set of computers: hosts, connected via a communication subnet, the word 'host' refers to an individual computer connected to the computer, which can communicate with other hosts via the network.

2. Uses of Computer Network:

Many organizations have a substantial number of computers in the operation, often located far apart. For example, a company with many factories may have a computer at each location to keep track of inventories, monitor productivity, and do the local payroll. Computer Networks are used for

a. **Resource Sharing:** The goal is to make all programs, equipment, and especially data available to anyone on the network without regard to the physical location of the resource and the user.
b. **High Reliability:** By Having alternative sources of supply. For example, all files could be replicated on two or three machines, so if one of them is unavailable (due to a hardware failure), the other copies could be used. In addition, the presence of multiple CPUs mean that if one goes down, the others may be able to take it over its work.
c. **Saving Money:** Small Computers have a much better price/performance ratio than large ones. Mainframes are roughly a factor of ten faster than personal computers, but they cost a thousand times more. This imbalance has caused many system designers to build systems consisting of personal computers one per user, with data kept on one or more shares file server machines.
d. **Scalability:** is the ability to increase system performance gradually as the workload grows just by adding more processors.
e. **Computer network delivering services to private individuals at home, like:** (access to remote information, Person –To-Person communication, Interactive entertainment).

3.Network Architecture:

The network architecture specifies how information processing resources are interconnected, and documents the standards for protocols (for network access and communication), topology (design of how devices are connected together), and wiring (physical medium or wireless assignments). It consists of:

1. Network Hardware.
2. Network Software.

3.1 Network Hardware:

Networking hardware includes all computers, peripherals, interface cards and other equipment needed to perform data processing and communications within the network.

1. **Transmission Technology**

   There are two types of transmission technology which are:

   a. Broadcast network.
   b. Point-to-Point network.

   A. Broadcast network: These types of networks have a single communication channel that is shared by all the computers on the network. Short messages called packets are sent by machines and are received by all the others. An address field within the packet specifies for whom it is intended. A machine checks the address field, if the packet is intended for itself, it processes the packet. If the packet is intended for some other machine, it is just ignored. For example, consider someone standing at the end of a corridor with many rooms and shouting " Watson, come here. I want you". Many people will hear that but only Watson responds. The others jut ignore it. Some broadcast systems also support transmission to a subset of the machines.

   B. Point-to-Point: Consists of many connections between individual pairs of machines. To go from source to the destination, packets on this type of network may have to first visit one or more intermediate machines.

   Geographically small localized networks use broadcasting, whereas larger networks usually are Point-to-Point.

2. **Scale**: Networks can be classified by their physical size

Inter-processor distance	Processor Location	Example
0.1 m	Circuit Board	Data flow machine

1 m	System	Multi Computer
10 m	Room	LAN
100 m	Building	
1 Km	Campus	
10 Km	City	WAN
100 Km	Country	
1000 Km	Continent	
10000 Km	Planet	Internet

4. Network Topology:

Topology of a network refers to the configuration of cables, computers, and other peripherals, topology should not be confused with logical topology which is the method used to pass information between workstations (computers). The main types of topologies are:

a. **Star Topology:** Star topology consist of a central node to which all other nodes are connected.
b. **Bus Topology:** Bus topology was the basis for most of the original LAN networks. Ideally suited for use with coaxial cable, the bus topology is a single length of transmission medium with nodes connected to it.
c. **Ring Topology:** Ring topology uses lengths of transmission media to connect the nodes, each node is attached to its neighbor. The transmission signal moves around the ring in one direction and is repeated, instead of just passed, as it moves from node to node. When a station transmits a data message, the transmission is picked up by the next station on the ring, examined, then retransmitted to the downstream neighbor. This process is continued until the transmitted signal is returned to the host that started the transmission, which then removes the data from the network.
d. **Tree Topology:** A tree topology combines the characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable. Tree topologies allow for the expansion of an existing network.

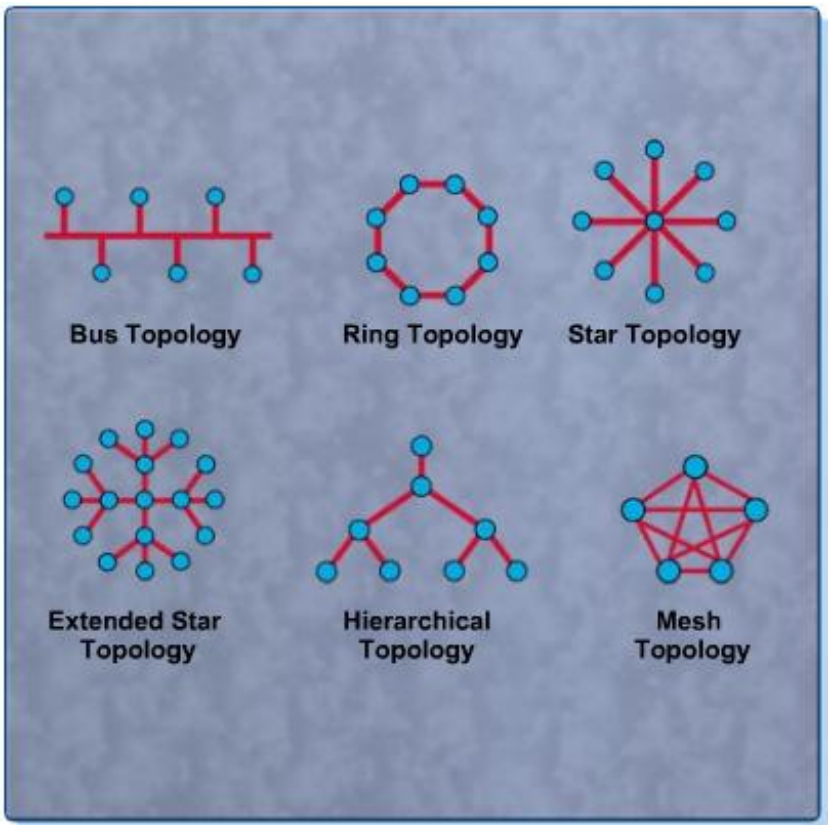


Figure – Network Topologies

5. Network Components:

Network components are used to connect devices on different networks, to create and connect multiple networks or subnets. The components include:

NIC: (Network Interface Card) is used to enable a network device, such as a computer or other network equipment, to connect to a network.

Repeater: A repeater is an inexpensive solution that is at the OSI physical layer and enables a network to reach users in distant portions of a building. A repeater connects two or more cable segments and retransmits any incoming signal to all other segments.

HUB: A hub is a central network device that connects network nodes such as workstation and servers in a star topology. A hub may also be referred to as a concentrator, which is a device that can have multiple inputs and outputs all active at one time.

Bridge: A bridge is a network device that sends information between two LANs.

Router: Routers are devices that direct traffic between hosts.

BRouter: A BRouter is a network device that acts as a bridge in one circumstance and as a router in another. A BRouter is used on networks that operate with several different protocols.

GATEWAY: The term gateway is used in many contexts, but in general it refers to a software or hardware interface that enables two different types of networked systems or software to communicate.

Transmission Media

The purpose of the physical layer, is to transport a raw bit stream from one machine to another. Various physical media can be used for the actual transmission. Each one has is own bandwidth, delay, cost, and ease of installation and maintenance. Media are roughly grouped into guided media such as copper wire and fiber optics and unguided media such as radio and laser through the air.

1. Magnetic Media: one of the most common ways to transport data from one computer to another is to write them onto magnetic tape or floppy disks, physically transport the tape or disks to the destination machine, and read them back in again. Although the bandwidth characteristics of magnetic tape are excellent, the delay characteristics are poor, transmission time is measured in minutes or hours, not milliseconds.

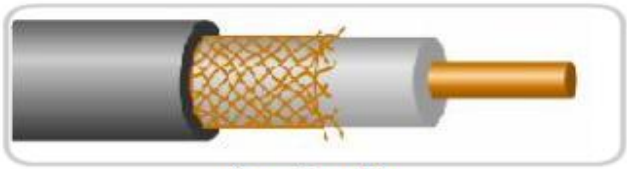
2. Twisted Pair: The oldest and still most common transmission medium is twisted pair. A twisted pair consists of two insulated copper wires, typically 1mm thick. The wires are twisted together in a helical form, just like a DNA molecule. The purpose of twisting the wires is to reduce electrical interference from similar pairs close by.

The most common application of the twisted pair is the telephone system. Twisted pairs can run several kilometers without amplification, but for longer distances, repeaters are needed.

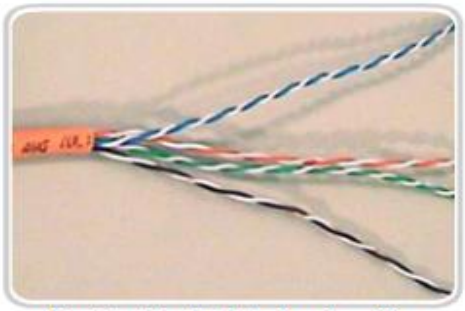
Twisted pairs can be used for either analog or digital transmission. The bandwidth depends on the thickness of the wire and the distance traveled. Twisted pair cabling comes in several varieties, two of which are important for computer networks. **Category_3** twisted consist of two insulated wires gently twisted together. Four such pairs are typically grouped together in a plastic sheath for protection and to keep the eight wires together.

Category 5 twisted pairs are similar to category 3 pairs, but with more twists per centimeter and Teflon insulation, which results in less crosstalk and a better quality of signal over longer distances, making them more suitable for high-speed computer communication. Both of these wiring types are often referred to as **UTP** (**U**nshielded **T**wisted **P**air).

Copper Media



Coaxial cable



Unshielded twisted-pair cable

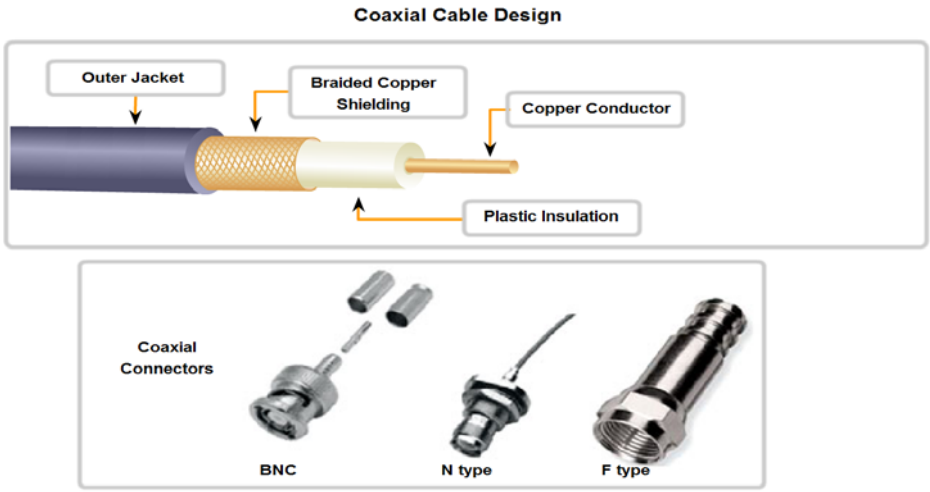
RJ-45 connections

3. Baseband Coaxial Cable: Another common transmission medium is the coaxial cable (known as coax), it has better shielding than twisted pair, so it can span longer distances at higher speeds. Two kinds of coaxial cables are widely used:

a. One kind, 50-ohm cable is commonly used for digital transmission.

b. The other kind, 75-ohm cable is commonly used for analog transmission.

A coaxial cable consists of a stiff copper wire as the core, surrounded by an insulating material. Insulating material is encased by a cylindrical conductor, often as a closely woven braided mesh. The outer conductor is covered in a protective plastic sheath. A cutaway view of a coaxial cable is shown in the figure below.



The construction and shielding of the coaxial cable give it a good combination of high bandwidth and excellent noise immunity. The bandwidth possible depends on the cable length. Coax is still widely used for cable television and some local area networks.

Broadband Coaxial Cable: The other kind of coaxial cable systems uses analog transmission on standard cable television cabling. It is called broadband. The term "broadband cable" in the computer networking world means any cable network using analog transmission.

To transmit digital signals on an analog network, each interface must contain electronics to convert the outgoing bit stream to an analog signal, and the incoming analog signal to a bit stream.

The difference between baseband and broadband is that broadband systems typically cover a large area and therefore need analog amplifiers to strengthen the signal periodically. These amplifiers can only transmit signals in one direction, so a computer outputting a packet will not be able to reach computers "upstream" from it if an amplifier lies between them. To get around this problem two types of broadband systems have been developed: **dual cable** and **single cable** systems.

Dual cable systems have two identical cables running in parallel, next to each other. To transmit data, a computer output the data onto cable 1, which runs to a device called the head-end at the root of the cable tree. The head end then transfers the signal to cable 2 for transmission back down the tree. All computers will transmit on cable 1 and receive on cable 2.

The other scheme single cable systems allocates different frequency bands for inbound and outbound communications on a single cable. The low-frequency band for id used communication from the computers to the

head-end, which then shifts signal to the high-frequency band and rebroadcasts it.

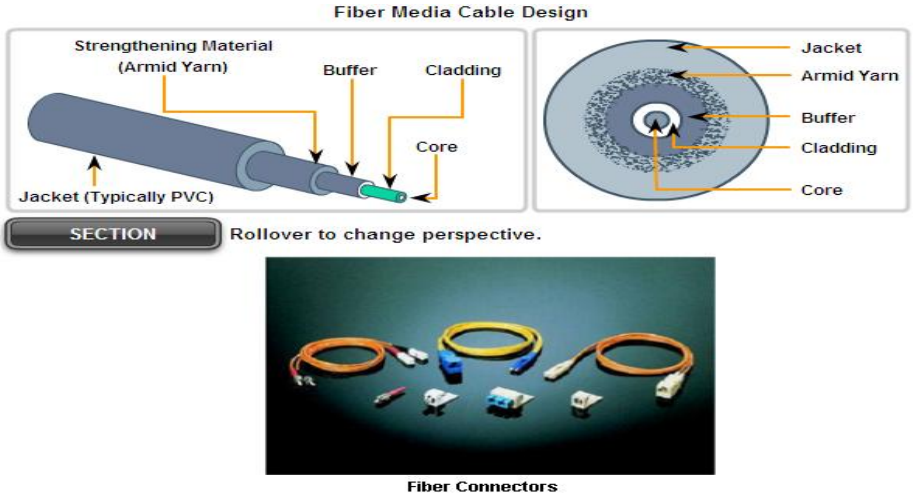
Fiber Optics: Optical transmission system has three components:

1. The light source.
2. The transmission medium.
3. The detector.

A pulse of light indicates a 1-bit and the absence of light indicates a zero bit. The transmission medium is an ultra-thin fiber of glass. The detector generates an electrical pulse when light falls on it.

By attaching a light source to one end of an optical fiber and a detector on the other, we have a unidirectional data transmission system that accepts an electrical signal, converts and transmits it by light pulses, and then reconverts the output to an electrical signal at the receiving end.

Fiber Cables: Fiber optic cables are similar to coaxial without the braid. The figure shows a single fiber viewed from the side. At the center is the glass core through which the light propagates, the core is 50 microns in diameter, about the thickness of a human hair.



Fiber Connectors

The core is surrounded by a glass cladding with a lower index of refraction than the core, to keep all light in the core. Next comes a thin plastic jacket to protect the cladding. Fibers are typically grouped together in bundles.

Fibers can be connected in three different ways:

First, they can terminate in connectors and be plugged into fiber sockets. Connectors lose about 10 to 20 percent of the light, but they make it easy to reconfigure systems.

Second, two pieces of fiber can be fused (melted) to form a solid connection. A fusion splice is almost as good as a single drawn fiber, but even here, a small amount of attenuation occurs.

Two kinds of light sources can be used to do the signaling
1. LEDs (Light Emitting Diodes)
2. Semiconductor lasers.
They have different properties, as shown in the table

Item	LED	Semiconductor
Data rate	Low	High
Mode	MultiMode	MultiMode or Single Mode
Distance	Short	Long
LifeTime	Long Life	Short Life
Temperature Sensitivity	Minor	Substantial
Cost	Low Cost	Expensive

Comparison of Fiber Optics and Copper Wire:

Fiber has many advantages, to start with, it can handle much higher bandwidths than copper. Its use is in high-end networks. Due to the low attenuation, repeaters are needed only about every 30 km on long lines, versus about 5 km for copper, a substantial cost saving. Fiber also has the advantage of not being affected by power surges, electromagnetic interference or power failures. Nor is it affected by corrosive chemicals in the air, making it ideal for harsh factory environments.
Telephone companies like fiber for a different reason:
1. It is thin and lightweight. Many existing cable ducts are completely full, so there is no room to add new cables. Removing all the copper and replacing it by fibers empties up the ducts.
2. Fibers do not leak and are quite difficult to tap, this gives them excellent security against potential writetappers.

On the other side, fiber is an unfamiliar technology requiring skills most engineers do not have since optical transmission is inherently unidirectional. Two way communication requires two fibers. Fiber interfaces cost more than electrical interfaces.

Wireless Transmission:

People who need to be on-line all the time need mobile service, and for these mobile users twisted pair, coaxial, and fiber optic are of no use. They need to get to their data from their laptops and notebooks without being

tethered to the terrestrial communication infrastructure. For these users wireless communication is the answer.

Some people even believe that the future holds only two kinds of communication: fiber and wireless. All fixed (i.e., non mobile) computers, telephone, faxes, so on will be fiber, and all mobile ones will use wireless.

1. Radio Transmission:

Radio waves are easy to generate, can travel long distances, and penetrate buildings easily so they are widely used for communication, both indoors and outdoors. Radio waves also are omni directional, meaning that they travel in all directions from the source, so that the transmitter and receiver do not have to be carefully aligned physically.

The properties of radio waves are frequency dependent. At low frequencies, radio waves pass through obstacles well, they are also absorbed by rain. At all frequencies, radio waves are subject to interference from motors and other electrical equipment. The waves that reach the ionosphere, a layer of charged particles circling the at a height of 100 to 500 km, are refracted by it and sent back to earth.

2. Microwave Transmission:

Microwaves travel in a straight line. If the towers are too far apart the earth will get in the way. Unlike radio waves at lower frequencies microwaves do not pass through buildings well. In addition, even though the beam may be well focused at the transmitter, there is still some divergence in space which is weather and frequency dependent.

Microwave communication is so widely used for long distance telephone, cellular telephones, television distribution and other uses.

It has several significant advantages over fiber. The main one is that when transmitting the signal for log distances we only need to place a tower every 50Km, to retransmit the signal, instead of placing the fiber optic along the way. Microwave is relatively inexpensive.

3. Infrared and Milimeter waves:

Unguided infrared and millimeter waves are widely used for short range communication. The remote controls used in televisions, VCRs, and stereos all use infrared communication, they are relatively directional, cheap and easy to build, but have a major drawback they do not pass through solid objects.

In general, as we go from long wave radio toward visible light, the waves behave, more and more like light and less like radio, security of

infrared systems against eavesdropping is better than that of radio systems precisely. Infrared communication cannot be used outdoors because the sun shines as brighter in the infrared as in the visible spectrum.

4. Lightwave transmission:

Unguided optical signaling has been in use for centuries, this scheme offers

1. very high bandwidth.
2. very low cost.
3. It is also relatively easy to install.

A disadvantage is that laser beams cannot penetrate rain or thick fog, but they normally work well on sunny days. Heat from the sun during the daytime causes convection currents to rise up from the roof of the building, this turbulent air, diverts the beam and make it dance around the detector.

Network Types

1. Local Area Network (LAN):

LANs are privately owned networks within a single building or campus of up to a few kilometers in size. They are widely used to connect personal computers and workstations in company offices and factories to share resources (e.g., printers) and exchange information. LANs are distinguished from other networks by three characteristics:

1. **Their size**: LANs are restricted in size, which means that the worst case transmission time is bounded and known in advance. Knowing this make it possible to use certain kinds of designs that would not otherwise be possible. It also simplifies network management.

2. Their Transmission Technology: LANs often use a transmission technology consisting of a single cable to which all the machines are attached. LANs

1. Run at speed of 10 to 100 Mbps.
2. Make very few errors.
3. Have low delay (tens of microseconds).

The new LAN operate at higher speed, up to hundred of megabits/sec.

3. Their topology: Various topologies are possible for broadcast LAN which are bus and ring.

2. Metropolitan Area Network (MAN):

Is basically a bigger version of a LAN and normally uses similar technology it might cover a group of nearby corporate offices or a city and might be either private or public. A MAN might be related to the local cable television network.

A MAN just has one or two cables. And the main reason for even distinguishing MAN as a special category is called DQDB (Distributed Queue Dual Bus). DQBD consists of two unidirectional buses (cables) to which all the computers are connected. Each bus has a head-end, a device that initiates transmission activity. Traffic that is destined for a computer to the right of the sender uses the upper bus. Traffic to the left uses the lower one.

3. Wide Area Network (WAN):

A WAN spans a large geographical area, often a country or continent. It contains a collection of machines intended for running user programs. We will refer to these machines by hosts. The hosts are connected by a communication subnet, the job of the subnet is to carry messages from host to host, just as the telephone system carries words from speaker to listener. Transmission lines (also called circuits, channels, or trunks) move bits between machines.

The switching elements are specialized computers used to connect two or more transmission lines.

Wireless Network

Mobile con1puters, such as notebook computers and personal digital assistants (PADs). Are the fastest-growing segment of the computer industry. Many of the owners of these computers have desktop machines on LANs and WANs back at the office and want to be connected to their home base even when away from home. Since having a wired connection is impossible in cars and airplanes, there is a lot of interest in wireless network. Wireless networks have many uses which are:

1. A Common one is the portable office. People on the road often want to use their portable electronic equipment to send and receive telephone calls, fax, and electronic mail, read remote files, and so on, and do this from anywhere on land, sea, or air.
2. Another use is for rescue workers at disaster site (fires, floods, earthquakes, etc.) where the telephone system has been destroyed.

Wireless LANs are easy to install they also have some disadvantages are:

1. They have capacity of 1 - 2 Mbps, which IS much slower than Wired LANs.
2. The error rates are often much higher.
3. The transmission from different computers can interfere with one another.

Internetwork (Internet):

Many networks exist in the world, often with different hardware and software. People connected to one network often want to communicate with people attached to a different one. This desire requires connecting together different, and frequently incompatible networks, sometimes by using machines called gateways to make the connection and provide the necessary

translation, both in terms of hardware and software. A collection of interconnection networks is called an internetwork or just Internet.

A common form of internet is a collection of LANs connected by WAN. In fact, if we were to replace the label "subnet" by " WAN", nothing else in the figure would have change .the only real distinction between a .subnet and a WAN in this case is whether or not hosts are present. If the system with in the closed curve contains only routers, it is a subnet. If it contains both routers and hosts with their own users, it is a WAN.

Protocol Hierarchies

To reduce their design complexity, most networks are organized as a series of **layers or levels,** each one built upon the one below it. The number of layers, the name of each layer, the contents of each layer, and the function of each layer differ from network to network. In all networks, the purpose of each layer is to offer certain services to the higher layers.

Layer n on one machine carries on a conversation with layers on another machine. The rules and conventions used in this conversation are collectively known as, the **layer n protocol** .Basically, a protocol is an agreement between the communicating parties on how communication is to proceed. Violating the protocol will make communication more difficult, if not impossible.

The entities comprising the corresponding layers on different machines are called **peers.** In reality, no data are directly transferred from layer n on one machine to layer n on another machine. Instead, each- layer passes- data and control information to the layer immediately below it, until the lowest layer is reached.

Between each pair of adjacent layers there is an **Interface.** The interface defines which primitive operations and services the lower layer offers to the upper.

A set of layers and protocols are called **network architecture.** The specification of an architecture must contain enough information to allow an implementer to write the program or build the Hardware for each layer so that it will correctly obey the appropriate protocol.

Neither the details of the implementation nor the specification of the interfaces are part of the architecture because these are hidden away inside the machines and not visible from the outside.

It is not even necessary that the interfaces on all machines in a

network be the same, provided that each machine can correctly use all the protocols.

A list of protocols used by a certain system, one protocol peer layer is called a **protocol stack.** Note that each protocol is completely independent of the other ones as long as the interfaces are not changed.

how to provide communication to the top layer of the five-layer network:

1. Message, **M,** is produced by an application process running **layer 5** and given to **layer 4** for transmission.
2. L**ayer 4** puts a header in front of the message to identify the message and parses the result to **layer** 3.
3. The header includes control information, such as sequence numbers, to allow **layer 4** on the destination machine to deliver messages in the right order if the lower layers do not maintain sequence. In some layers, headers also contain size, times, and other control fields.
4. There is-no limit to the size of messages transmitted in the **layer 4** protocol, but there is nearly always a limit imposed by the **layer 3** protocol. Consequently **layer 3** must break up the incoming messages into smaller units, packets, adding a layer header to each packet.
5. L**ayer2** adds not only a header to each piece, but also a trailer, and gives the resulting unit to **layer 1** for physical transmission.
6. At the receiving machine the message moves upward, from layer to layer, with headers being stripped off as it progresses. None of the headers for **layers below n** are passed up to **layer n.**

Design Issues For The Layers:

1. Every layer needs a mechanism for identifying senders and receivers. Since a network, normally has many computers, some of which have multiple processes, a means is needed for a process on one machine to specify with whom it wants to talk.
2. Rules for data transfer: In some systems, data only travel in one direction **(simplex communication).** In others they can travel in either direction, but not simultaneously **(half-duplex communication).** In others they travel in both directions at once **(full-duplex communication).**

3. Error control is an important issue because physical communication circuits are not perfect. The receiver must have some way to telling the sender which messages have been correctly received and which have not.
4. Not all communication channels preserve the order of messages sent on them. The solution is to number the pieces.
5. How to keep a fast sender from swamping a slow receiver, with data Some of them involve some kind of feedback from the receiver to the sender, either directly or indirectly, about the receiver's current situation.
6. The inability of all processes to accept arbitrarily long messages. This property leads to mechanisms for disassembling, transmitting, and then reassembling messages.

The Relationship of Services to Protocols

Services and protocols are distinct concepts, although they are frequently confused. This distinction is:

A **service** is a set of primitives (operations) that a layer provides to the layer above it. The service defines what operations the layer is prepared to perform on behalf of its users, but it says nothing at all about how these operations are implemented. A service relates to an interface between two layers, with the lower layer being the service provider and the upper layer being the service user.

A **Protocol** is a set of rules governing the format and meaning of the frames, packets, or messages that are exchanged by the peer entities within a layer. Entities use protocols in order to implement their service definitions. They are free to change their protocols at will, provided they do not change the service visible to their users. In this way, the service and the protocols are completely decoupled.

Reference Model

We have discussed layered networks; it is time to look at some examples. In the next two sections we will discuss two important network architectures, the OSI reference model and the TCP/IP reference model.

1. The OSI Reference model

The OSI model is shown in the coming Figure This model is based on a proposal developed by the International Standards Organization (ISO) as a

first step toward international standardization of the protocols used in the various layers.

The model is called the ISO OSI (Open system Interconnection Reference Model because it deals with connecting open systems - that is, systems : open for communication with other systems. we will usually just call it the OSI model for short. The OSI model has seven layers. The principles that were applied to arrive at the seven layers are as follows:

1. Each layer should perform a well defined function.
2. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
3. The layer boundaries should be chosen to minimize the information flow across the interfaces.
4. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity, and small enough that the architecture does not become unwieldy.

The Physical Layer:

The physical layer is concerned with transmitting raw bits over a communication channel. The design issues have to do with making sure that when one side sends a 1 bit, it is received by the other side as a 1 bit, not as a 0 bit. Typical questions here are how many volts should be used to represent a 1 and how many for a 0, how many microseconds a bit lasts, whether transmission may proceed simultaneously in both directions, how the initial connection is established and how it is torn down when both sides are finished, and how many pins the network connector has and what each pin is used for. The design issues here largely deal with mechanical, electrical, and procedural interfaces, and the physical transmission medium, which lies below the physical layer.

The Data Link Layer:

The main task of the data link layer is to take a raw transmission facility and transform it into a line that appears free of undetected transmission errors to the network layer. The sender break the input data up into data frames (typically a few hundred or a few thousand bytes), transmit the frames sequentially, and process the acknowledgement frames sent back by the receiver.

It is up to the data link layer to create and recognize frame boundaries. This can be accomplished by attaching special bit patterns to the beginning and end of the frame. A noise burst on the line can destroy a frame completely. **In** this case, the data link layer software on the source

machine can retransmit the frame. Multiple transmissions of the same frame introduce the possibility of duplicate frames. A duplicate frame could be sent if the acknowledgement frame from the receiver back to the sender were lost.

The data link layer may coffer several different service classes to the network layer, each of a different quality and with a different price. Another issue that arises in the data link layer is how to keep a fast transmitter from drowning a slow receiver in data. If the line can be used to transmit data in both directions, this introduces a new complication that the data link layer software must deal with. The problem is that the acknowledgement frames for A to B traffic compete for the use of the line with data frames for the B to A traffic.

The Network Layer

The network layer is concerned with controlling the operation of the subnet. A key design issue is determining how packets are routed from source to destination. Routes can be based on:

1. Static tables that are "wired into" the network and rarely.
2. They can also be determined at the start of each conversation.
3. Finally, they can be highly dynamic.

If too many packets are present in the subnet at the same time, they will get in each other's way forming bottlenecks. The control of such congestion also belongs to the network layer.

When a packet has to travel from one network to another to get to its destination many problems can arise:

1. The addressing used by the second network may be different from the first one.
2. The second one may not accept the packet at all because it is too large.
3. The protocols may differ, and so on. It is up to the network laver to overcome all these problems to allow heterogeneous networks to-be interconnected.

The Transport Layer

The basic function of the transport layer is to accept data from the session layer, split it up into smaller units if need be, pass these to the network layer, and ensure that the pieces all arrive correctly at the other end.

The transport layer creates a distinct network connection for each

transport connection required by the session layer. If the transport connection requires a high throughput, however, the transport layer might create multiple network connections, dividing the data among the network connections to improve throughput. Creating or maintaining a network connection is expensive. The transport layer also determines what type of service to provide the session layer, and ultimately, the users of the network.

The most popular type of transport connection is an error-free point-to-point channel that delivers messages or bytes in the order in which they were sent.

The Session Layer

The session layer allows users on different machines to establish sessions between them. A session allows ordinary data transport, as does the transport layer, but it also provides enhanced services-useful in some applications. A session might be used to allow a user to log into a remote timesharing system or to transfer a file between two machines. One of the services of the session layer is to manage dialogue control. Sessions can allow traffic to go in both directions at the same time, or in only one direction at a time.

The Presentation Layer

The presentation layer is concerned with the syntax and semantics of the information transmitted. Most user programs do not exchange random binary bit strings. They exchange things such as people's names, dates, amounts of money, and Invoices. These items are represented as character strings, integers, floating-point numbers, and data structures composed of several simpler items. Different computers have different codes for representing character strings (e.g., ASCII and Unicode), integers (e.g., one's complement and two's complement), and so on.

In order to make it possible for computers with different representations to communicate, the data structures to be exchanged can be defined in an abstract way along; with a standard encoding to be used "on the wire." The presentation layer manages these abstract data structures and converts from the representation used inside the computer to the network standard representation and back.

The Application Layer

The application layer contains a variety of protocols that are commonly needed. For example, there are hundreds of incompatible terminal types in the world. each with different screen layouts, escape sequences for inserting

and deleting text, moving the cursor, etc.

One way to solve this problem is to define an abstract network virtual terminal that editors and other programs can be written to deal with. To handle each terminal type, a piece of software must be written to map the functions of the network virtual terminal onto the real terminal. For example, when the editor moves the virtual terminal's cursor to the upper left-hand comer of the screen, this software must issue the proper command sequence to the real terminal to get its cursor there too. All the virtual, terminal software is in the application layer. Another application layer function is file transfer. Different file systems have different file naming conventions, different ways of representing text lines, and so on.

Data Transmission in the OSI Model

The figure shows an example of how data can be transmitted using the OSI model. The sending process has some data it wants to send to the receiving process it gives the data to the application layer, which then attaches the application header to the front of it and gives the resulting item to the presentation layer.

The presentation layer may transform this item in various ways and possibly add a header to the front, giving the result to the, session layer. This process is repeated until the data reach the physical layer.

The TCP/IP Reference Model

Let us now turn from the OSI model to the reference model used in the grandparent of all computer networks, the ARPANET, and its successor, the worldwide Internet. This architecture later became known as the ***TCP/IP*** Reference Model.

The Application Layer:

The TCP/IP model does not have session or presentation layers. No need for them was perceived, so they were not included. On top of the transport layer is the application layer. It contains all the higher-level protocols. The early ones include virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP). The virtual terminal protocol allows a user on one machine to log into a distant machine and work there. The file transfer protocol provides a way to move data efficiently from one machine to another.

The Transport Layer:

The layer above the internet layer in the TCP/IP model is called the transport layer. It is designed to allow peer entities on the source and destination hosts to carryon a conversation, the same as in the OSI transport layer. Two end-to-end protocols have been defined here. The first one, **TCP (Transmission Control Protocol)** is a reliable connection-oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet.

The second protocol in this layer, **UDP (User Datagram Protocol),** is an unreliable, connectionless protocol. It is also widely used for one-shot .client-server type request-reply queries and applications in which prompt delivery is more important than accurate delivery.

The Internet Layer:

This layer, called the internet layer, its job is to permit hosts to inject packets into any network and have them travel independently to the destination, (potentially on a different network). They may even arrive in a different order than they were sent. A person can drop a sequence of international Letters into a mail box in one country and most of them will be delivered to the correct address in the destination country.

The internet layer defines an official packet format and protocol called **IP** (Internet Protocol). The job of the internet layer is to deliver **IP** packets where they are supposed to go. Packet routing is clearly the major issue here, as is avoiding congestion. For these reasons, it is reasonable to say that the *TCP/IP* internet layer is very similar in functionality to the OSI network layer.

The Host-To-Network Layer:

The TCP/IP reference model does not really say much about what happens here, except to point out that the host has to connect to the network using some protocol so it can send **IP** packets over it. This protocol is not defined and varies from host to host and network to network.

A Comparison of the OSI and TCP Reference Models:

The OSI and TCP/IP reference models have much similarity which are:

1. Both are based on the concept of a stack of independent protocols.
2. Also the Functionality of the layers is roughly similar. For example, in both models the layers up through and Including the Transport layer are there to provide an end-to-end network-independent transport

service to processes wishing to communicate.

And the Differences are:

1. Three concepts are central to the OSI model:
    A. Services.
    B. Interfaces.
    C. Protocols .

    OSI model make the distinction between these three concepts explicit. Each layer performs some services for the layer above it. The TCP/IP model did not originally clearly distinguished between services, interfaces, and protocols.
2. As a consequence, the protocols in me OSI model are better hidden than TCP/IP model.
3. OSI reference model was devised before the protocols were invented. This ordering means that the model was not biased toward one. With the TCP/IP the reverse was true: the protocols came first, and the model was really just a description of the existing protocols. There was no problem with the protocols fitting the model. They fit perfectly.
4. Another difference is in the area of connectionless versus connection-oriented communication. The OSI model supports both connectionless and connection-oriented communication in the network layer, but only connection-oriented communication in the transport layer. The TCP/IP model has only one mode in the network layer (connectionless) but supports both modes in the transport layer.
5. TCP/IP has four layers where OSI have seven layers.

The Network Layer

The Network layer, or OSI Layer 3, provides services to exchange the individual pieces of data over the network between identified end devices. To accomplish this end-to-end transport, Layer 3 uses four basic processes:

1. Addressing: First, the Network layer must provide a mechanism for addressing the end devices. In an IPv4 network, when this address is added to a device, the device is then referred to as a host.
2. Encapsulation : addition of source address and destination addresses.

3. Routing : Intermediary devices that connect the networks are called routers. The role of the router is to select paths for and direct packets toward their destination. This process is known as routing.
4. Decapsulation: The removal of source address and destination addresses.

Network Layer Protocols

1. Internet Protocol version 4 (IPv4).
2. Internet Protocol version 6 (IPv6).
3. Novell Internetwork Packet Exchange (IPX).
4. AppleTalk.
5. Connectionless Network Service (CLNS/DECNet).

The Network layer services implemented by the TCP/IP protocol suite are the Internet Protocol (IP) Version 4 of IP (IPv4) is currently the most widely-used version of IP. It is the only Layer 3 protocol that is used to carry user data over the Internet.

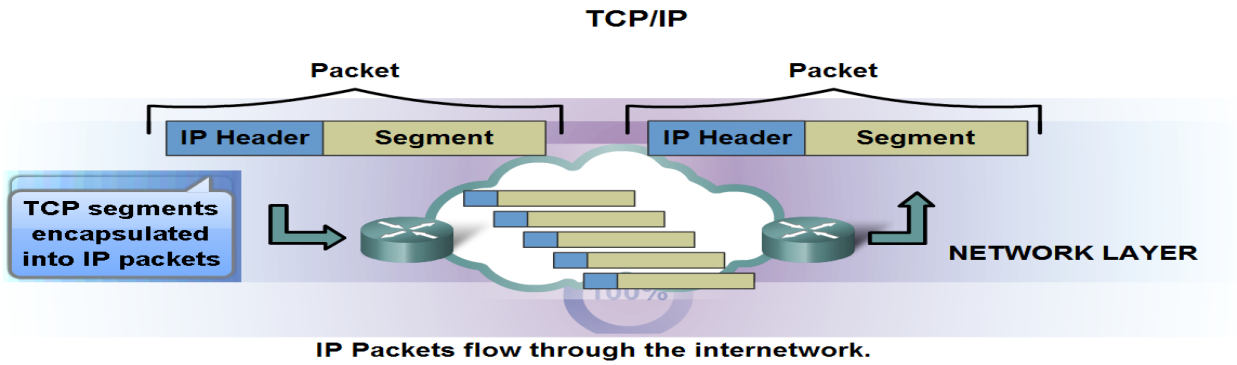
IP version 6 (IPv6) is developed and being implemented in some areas. IPv6 will operate alongside IPv4 and may replace it in the future. The services provided by IP, as well as the packet header structure and contents, are specified by either IPv4 protocol or IPv6 protocol.

The Internet Protocol was designed as a protocol with low overhead. It provides only the functions that are necessary to deliver a packet from a source to a destination over an interconnected system of networks. The protocol was not designed to track and manage the flow of packets.

Layer 3 uses connectionless communication that is sending a letter to someone without notifying the recipient in advance. Connectionless data communications works on the same principle. IP packets are sent without notifying the end host that they are coming.

Connection-oriented protocols, such as TCP, require that control data be exchanged to establish the connection as well as additional fields in the PDU header. Because IP is connectionless, it requires no initial exchange of control information to establish an end-to-end connection before packets are forwarded, nor does it require additional fields in the PDU header to maintain this connection. This process greatly reduces the overhead of IP.

Connectionless packet delivery may, however, result in packets arriving at the destination out of sequence. If out-of-order or missing packets create problems for the application using the data, then upper layer services will have to resolve these issues.



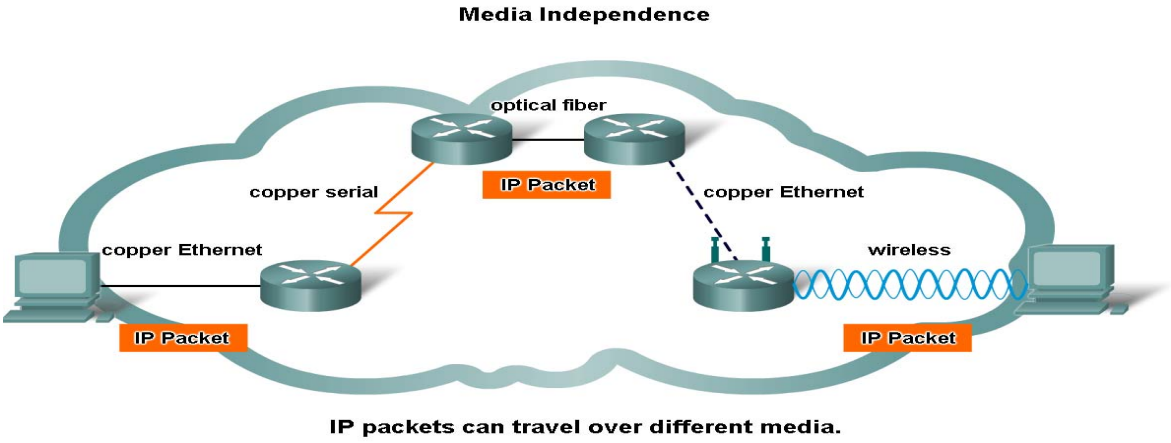
IP Packets flow through the internetwork.

- Connectionless - No connection is established before sending data packets.
- Best Effort (unreliable) - No overhead is used to guarantee packet delivery.
- Media Independent - Operates independently of the medium carrying the data.

The IP protocol does not burden the IP service with providing reliability. Compared to a reliable protocol, the IP header is smaller. Transporting these smaller headers requires less overhead. Less overhead means less delay in delivery. This characteristic is desirable for a Layer 3 protocol. The mission of Layer 3 is to transport the packets between the hosts while placing as little burden on the network as possible. IP is often referred to as an unreliable protocol. Unreliable means simply that IP does not have the capability to manage, and recover from, undelivered or corrupt packets. The header of an IP packet does not include fields required for reliable data delivery. There are no acknowledgments of packet delivery. There is no error control for data. Nor is there any form of packet tracking; therefore, there is no possibility for packet retransmissions.

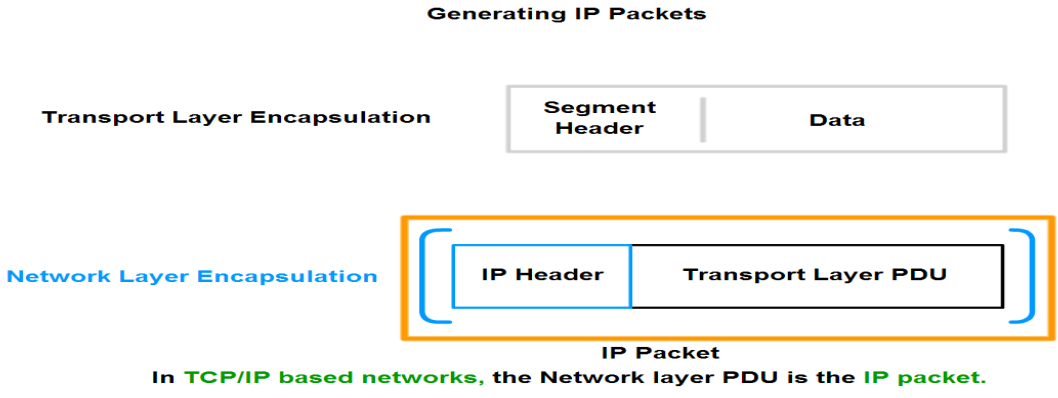
The Network layer is also not burdened with the characteristics of the media on which packets will be transported. IPv4 and IPv6 operate independently of the media that carry the data at lower layers of the protocol stack. Part of the control communication between the Data Link layer and the Network layer is the establishment of a maximum size for the packet. This characteristic is referred to as the Maximum Transmission Unit (MTU). The Data Link layer passes the MTU upward to the Network layer. The Network layer then determines how large to create the packets. In some cases, an intermediary device - usually a

router - will need to split up a packet when forwarding it from one media to a media with a smaller MTU. This process is called fragmenting the packet or fragmentation.



The process of encapsulating data by layer enables the services at the different layers to develop and scale without affecting other layers. This means that transport layer segments can be readily packaged by existing Network layer protocols, such as IPv4 and IPv6 or by any new protocol that might be developed in the future.

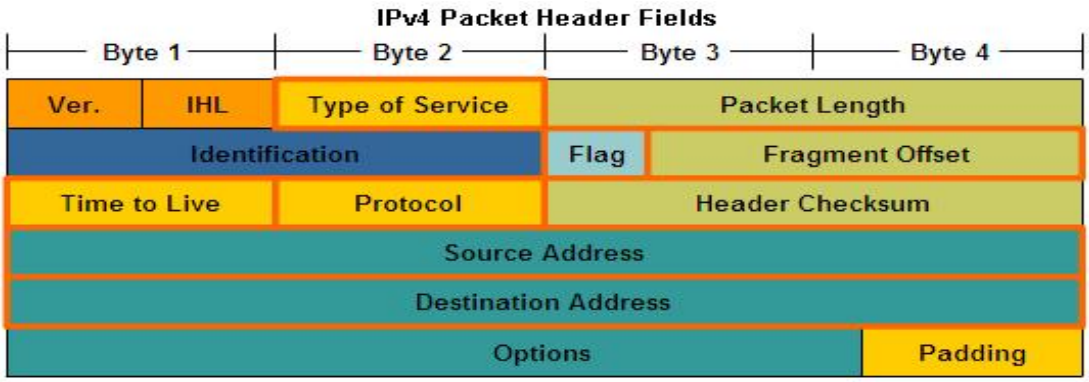
Routers can implement these different Network layer protocols to operate concurrently over a network to and from the same or different hosts. The routing performed by these intermediary devices only considers the contents of the packet header that encapsulates the segment. In all cases, the data portion of the packet - that is, the encapsulated Transport layer PDU - remains unchanged during the Network layer processes.



The IP V4 Packet Header

- IP Destination Addresss field : contains a 32-bit binary value that represents the packet destination Network layer host address.
- The IP Source Address field : contains a 32-bit binary value that represents the packet source Network layer host address.
- The Time-to-Live (TTL) : is an 8-bit binary value that indicates the remaining "life" of the packet. The TTL value is decreased by at least one each time the packet is processed by a router (that is, each hop). When the value becomes zero, the router discards or drops the packet and it is removed from the network data flow. This mechanism prevents routing loop.
- Protocol : This 8-bit binary value indicates the data payload type that the packet is carrying. The Protocol field enables the Network layer to pass the data to the appropriate upper-layer protocol. Example values are: 01 ICMP, 06 TCP, 17 UDP.
- The Type-of-Service field: contains an 8-bit binary value that is used to determine the priority of each packet. This value enables a Quality-of-Service (QoS) mechanism to be applied to high priority packets, such as those carrying telephony voice data.
- Fragment Offset : As mentioned earlier, a router may have to fragment a packet when forwarding it from one medium to another medium that has a smaller MTU. When fragmentation occurs, the IPv4 packet uses the Fragment Offset field and the MF flag in the IP header to reconstruct the packet when it arrives at the destination host. The fragment offset field identifies the order in which to place the packet fragment in the reconstruction.
- The More Fragments (MF) flag : is a single bit in the Flag field used with the Fragment Offset for the fragmentation and reconstruction of packets. The More Fragments flag bit is set, it means that it is not the last fragment of a packet. When a receiving host sees a packet arrive with the MF = 1, it examines the Fragment Offset to see where this fragment is to be placed in the reconstructed packet. When a receiving host receives a frame with the MF = 0 and a non-zero value in the Fragment offset, it places that fragment as the last part of the reconstructed packet. An unfragmented packet has all zero fragmentation information (MF = 0, fragment offset =0).
- The Don't Fragment (DF) flag is : a single bit in the Flag field that indicates that fragmentation of the packet is not allowed. If the Don't Fragment flag bit is set, then fragmentation of this packet is NOT permitted. If a router needs to fragment a packet to allow it to be

passed downward to the Data Link layer but the DF bit is set to 1, then the router will discard this packet.



- Version - Contains the IP version number (4)
- Header Length (IHL) - Specifies the size of the packet header.
- Packet Length - This field gives the entire packet size, including header and data, in bytes.
- Identification - This field is primarily used for uniquely identifying fragments of an original IP packet
- Header Checksum - The checksum field is used for error checking the packet header.
- Options - There is provision for additional fields in the IPv4 header to provide other services but these are rarely used.

Separating Hosts into Common Groups

Rather than having all hosts everywhere connected to one vast global network, it is more practical and manageable to group hosts into specific networks. The large network was separated into smaller networks that were interconnected. These smaller networks are often called subnetworks or subnets.

Similarly, as our networks grow, they may become too large to manage as a single network. At that point, we need to divide our network. When we plan the division of the network, we need to group together those hosts with common factors into the same network.

- Grouping Hosts Geographically - We can group network hosts together geographically. Grouping hosts at the same location - such as each building on a campus or each floor of a multi-level building - into separate networks can improve network management and operation.

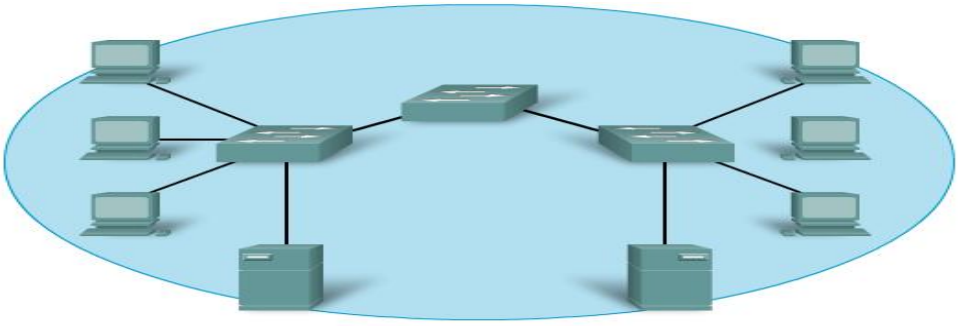
- Grouping Hosts for Specific Purposes - Users who have similar tasks typically use common software, common tools, and have common traffic patterns. We can often reduce the traffic required by the use of specific software and tools by placing the resources to support them in the network with the users.
- Grouping Hosts for Ownership - Using an organizational (company, department) basis for creating networks assists in controlling access to the devices and data as well as the administration of the networks. Dividing hosts into separate networks provides a boundary for security enforcement and management of each network.

Large numbers of hosts connected to a single network can produce volumes of data traffic that may stretch, if not overwhelm, network resources such as bandwidth and routing capability.

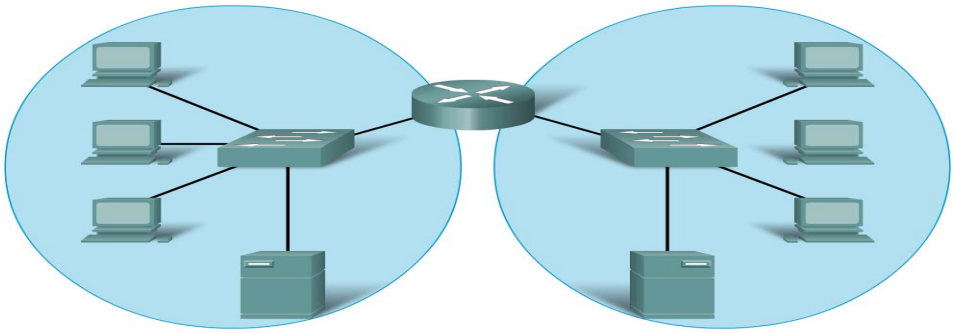
Dividing large networks so that hosts who need to communicate are grouped together reduces the traffic across the internetworks. In addition to the actual data communications between hosts, network management and control traffic (overhead) also increases with the number of hosts. A significant contributor to this overhead can be network broadcasts.

A broadcast is a message sent from one host to all other hosts on the network. Typically, a host initiates a broadcast when information about another unknown host is required. Broadcasts are a necessary and useful tool used by protocols to enable data communication on networks. However, large numbers of hosts generate large numbers of broadcasts that consume network bandwidth. And because every other host has to process the broadcast packet it receives, the other productive functions that a host is performing are also interrupted or degraded.

Broadcasts are contained within a network. In this context, a network is also known as a broadcast domain.



All devices in this network are connected in one broadcast domain when the switch is set to the factory default settings. Since switches forward broadcasts by default, broadcasts are processed by all devices in this network.

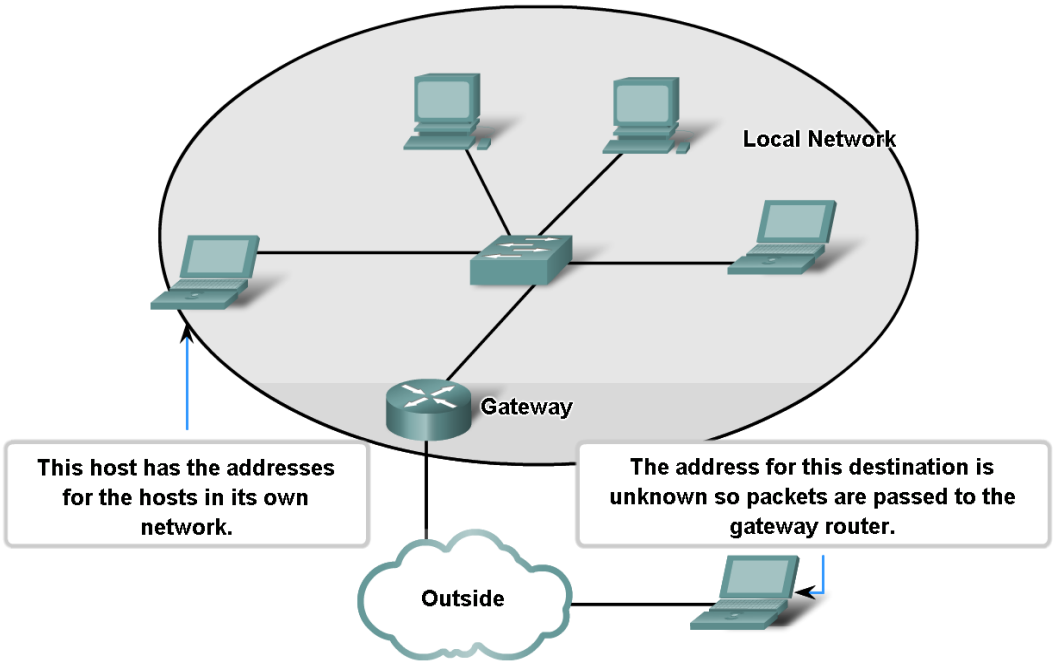


Replacing the middle switch with a router creates 2 IP subnets, hence, 2 distinct broadcast domains. All devices are connected but local broadcasts are contained.

Dividing networks based on ownership means that access to and from resources outside each network can be prohibited, allowed, or monitored.

Security between networks is implemented in an intermediary device (a router or firewall appliance) at the perimeter of the network. The firewall function performed by this device permits only known, trusted data to access the network.

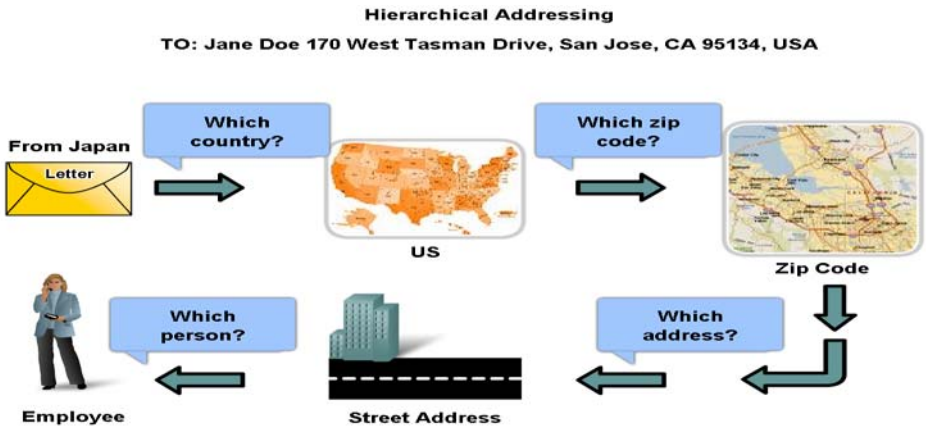
Dividing large networks so that hosts who need to communicate are grouped together reduces the unnecessary overhead of all hosts needing to know all addresses. For all other destinations, the hosts only need to know the address of an intermediary device, to which they send packets for all other destinations addresses. This intermediary device is called a gateway. The gateway is a router on a network that serves as an exit from that network.



Hosts do not know how to deliver data to devices in a remote network - this is the role of the gateway.

Hierarchical Addressing

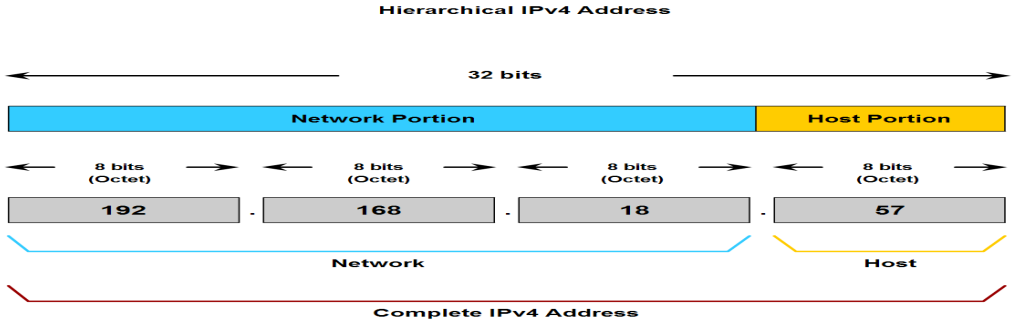
Hierarchical Network layer addresses work in much the same way as a postal system. Layer 3 addresses supply the network portion of the address. Routers forward packets between networks by referring only to the part of the Network layer address that is required to direct the packet toward the destination network. By the time the packet arrives at the destination host network, the whole destination address of the host will have been used to deliver the packet.



At each step of delivery, the post office need only examine the next hierarchical level.

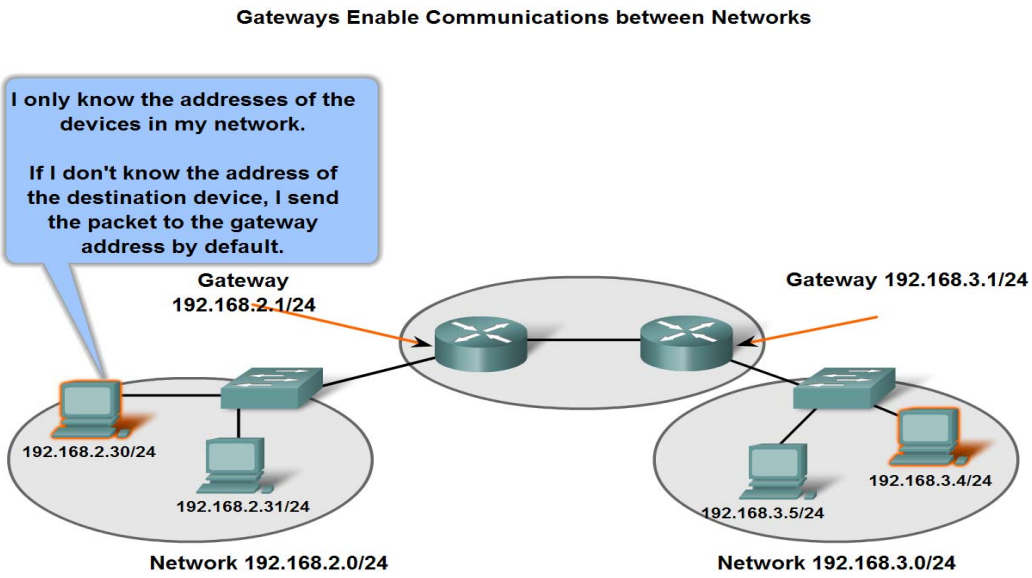
The logical 32-bit IPv4 address is hierarchical and is made up of two parts. The first part identifies the network and the second part identifies a host on that network. Both parts are required for a complete IP address. For convenience IPv4 addresses are divided in four groups of eight bits (octets). Each octet is converted to its decimal value and the complete address written as the four decimal values separated by a dot (period).

This is hierarchical addressing because the network portion indicates the network on which each unique host address is located. Routers only need to know how to reach each network, rather than needing to know the location of each individual host. With IPv4 hierarchical addressing, the network portion of the address for all hosts in a network is the same.

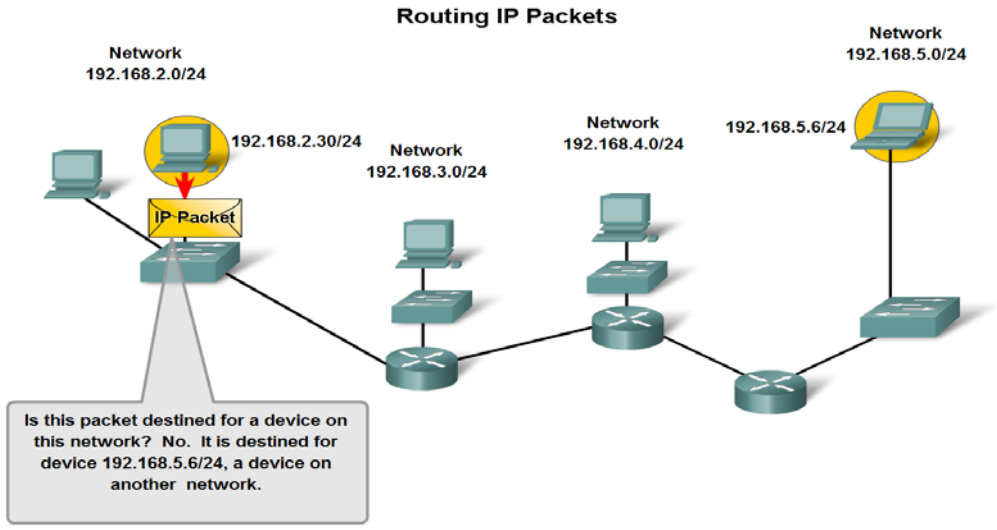


The number of bits of an address used as the network portion is called the prefix length. For example if a network uses 24 bits to express the network portion of an address the prefix is said to be /24. In the devices in an IPv4 network, a separate 32-bit number called a subnet mask indicates the prefix.

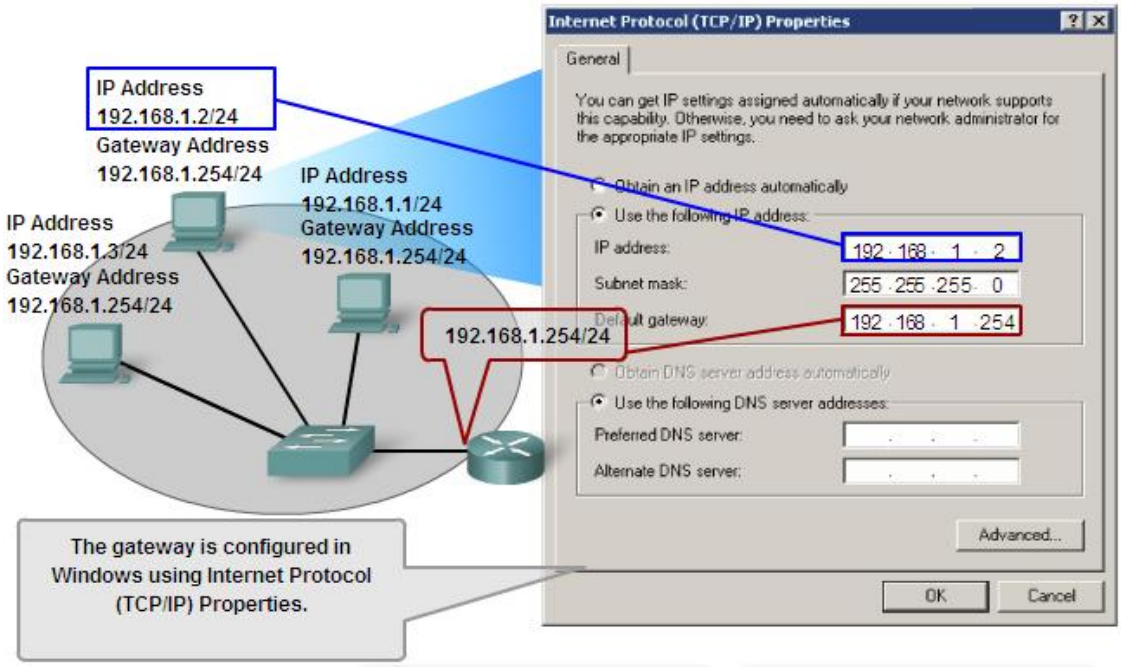
When a host needs to communicate with another network, an intermediary device, or router, acts as a gateway to the other network. As a part of its configuration, a host has a default gateway address defined. To communicate with a device on another network, a host uses the address of this gateway, or default gateway, to forward a packet outside the local network. The router also needs a route that defines where to forward the packet next. This is called the next-hop address. If a route is available to the router, the router will forward the packet to the next-hop router that offers a path to the destination network.



As you know, the role of the Network layer is to transfer data from the host that originates the data to the host that uses it. During encapsulation at the source host, an IP packet is constructed Layer 3 to transport the Layer 4 PDU. If the destination host is in the same network as the source host, the packet is delivered between the two hosts on the local media without the need for a router. However, if the destination host and source host are not in the same network, the packet may be carrying a Transport layer PDU across many networks and through many routers. As it does, the information contained within is not altered by any routers when forwarding decisions are made.

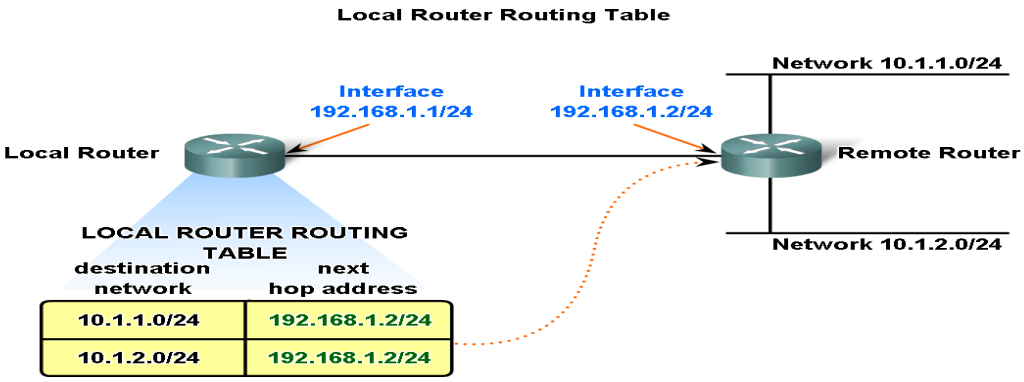


The gateway, also known as the default gateway, is needed to send a packet out of the local network. If the network portion of the destination address of the packet is different from the network of the originating host, the packet has to be routed outside the original network. To do this, the packet is sent to the gateway. This gateway is a router interface connected to the local network. The gateway interface has a Network layer address that matches the network address of the hosts. The hosts are configured to recognize that address as the gateway.



No packet can be forwarded without a route. A host must either forward a packet to the host on the local network or to the gateway. A router makes a forwarding decision for each packet that arrives at the gateway interface. This forwarding process is referred to as routing. To forward a packet to a destination network, the router requires a route to that network. If a route to a destination network does not exist, the packet cannot be forwarded.

The destination network may be a number of routers or hops away from the gateway. The route to that network would only indicate the next-hop router to which the packet is to be forwarded, not the final router. The routing process uses a route to map the destination network address to the next hop and then forwards the packet to this next-hop address.



Like end devices, routers also add routes for the connected networks to their routing table. When a router interface is configured with an IP address and subnet mask, the interface becomes part of that network. The routing table now includes that network as a directly connected network. All other routes, however, must be configured or acquired via a routing protocol. To forward a packet the router must know where to send it. This information is available as routes in a routing table.

The routing table stores information about connected and remote networks. Connected networks are directly attached to one of the router interfaces. These interfaces are the gateways for the hosts on different local networks. Remote networks are networks that are not directly connected to the router.

The router matches the destination address in the packet header with the destination network of a route in the routing table and forwards the packet to the next-hop router specified by that route. If there are two or more possible routes to the same destination, the router decides which route is the best.

If a route representing the destination network is not on the routing table, the packet will be dropped (that is, not forwarded). The router may also use a default route to forward the packet. The default route is used when the destination network is not represented by any other route in the routing table.

The routing table contains the information that a router uses in its packet forwarding decisions. For the routing decisions, the routing table needs to represent the most accurate state of network pathways that the router can access. Out-of-date routing information means that packets may not be forwarded to the most appropriate next-hop, causing delays or packet loss. This route information can be manually configured on the router or learned dynamically from other routers in the same internetwork. After the

interfaces of a router are configured and operational, the network associated with each interface is installed in the routing table as a directly connected route.

Types of Network Addresses in a IPv4 Network

- Network address - The address by which we refer to the network.
- Broadcast address - A special address used to send data to all hosts in the network.
- Host addresses - The addresses assigned to the end devices in the network.

Network Prefixes

The prefix length is the number of bits in the address that gives us the network portion. For example, in 172.16.4.0 /24, the /24 is the prefix length - it tells us that the first 24 bits are the network address. This leaves the remaining 8 bits, the last octet, as the host portion.

Exercise

Given address/prefix of **183.26.103.215 /30**

For each row, enter the values ...

Type of Address	Enter LAST octet in binary	Enter LAST octet in decimal	Enter full address in decimal
Network			
Broadcast			
First Usable Host Address			
Last Usable Host Address			

In an IPv4 network, the hosts can communicate one of three different ways:

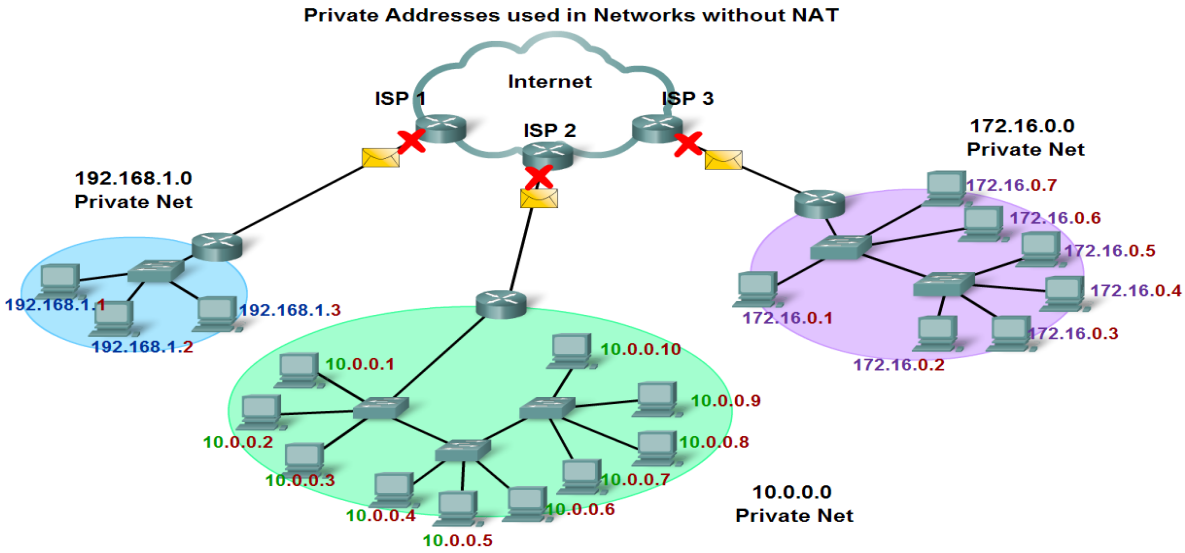
- Unicast - the process of sending a packet from one host to an individual host.
- Broadcast - the process of sending a packet from one host to all hosts in the network.
- Multicast - the process of sending a packet from one host to a selected group of hosts

There are two types of broadcasts: directed broadcast and limited broadcast.

- Directed Broadcast - A directed broadcast is sent to all hosts on a specific network. This type of broadcast is useful for sending a broadcast to all hosts on a non-local network. For example, for a host outside of the network to communicate with the hosts within the 172.16.4.0 /24 network, the destination address of the packet would be 172.16.4.255.
- The limited broadcast is used for communication that is limited to the hosts on the local network. These packets use a destination IPv4 address 255.255.255.255. Routers do not forward this broadcast.

There are two types of addresses which are public and private addresses
The private address blocks are:

- 10.0.0.0 to 10.255.255.255 (10.0.0.0 /8)
- 172.16.0.0 to 172.31.255.255 (172.16.0.0 /12)
- 192.168.0.0 to 192.168.255.255 (192.168.0.0 /16)



IP addresses are classified into three classes but there are limits to the Class-based System : Not all organizations' requirements fit well into one of these three classes.

Classful allocation of address space often wasted many addresses, which exhausted the availability of IPv4 addresses.

Classless Addressing is the system that we currently use and is referred to as classless addressing. With the classless system, address blocks

appropriate to the number of hosts are assigned to companies or organizations without regard to the unicast class.

IP Address Classes

Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

** All zeros (0) and all ones (1) are invalid hosts addresses.

There are certain addresses that cannot be assigned to hosts for various reasons. There are also special addresses that can be assigned to hosts but with restrictions on how those hosts can interact within the network.

- Network and Broadcast Addresses - As explained earlier, within each network the first and last addresses cannot be assigned to hosts. These are the network address and the broadcast address, respectively.
- Loopback - One such reserved address is the IPv4 loopback address 127.0.0.1. The loopback is a special address that hosts use to direct traffic to themselves. The loopback address creates a shortcut method for TCP/IP applications and services that run on the same device to communicate with one another. By using the loopback address instead of the assigned IPv4 host address, two services on the same host can bypass the lower layers of the TCP/IP stack. You can also ping the loopback address to test the configuration of TCP/IP on the local host.
- Although only the single 127.0.0.1 address is used, addresses 127.0.0.0 to 127.255.255.255 are reserved. Any address within this block will loop back within the local host. No address within this block should ever appear on any network.
- Link-Local Addresses - IPv4 addresses in the address block 169.254.0.0 to 169.254.255.255 (169.254.0.0 /16) are designated as link-local addresses. These addresses can be automatically assigned to

the local host by the operating system in environments where no IP configuration is available. These might be used in a small peer-to-peer network or for a host that could not automatically obtain an address from a Dynamic Host Configuration Protocol (DHCP) server.

- TEST-NET Addresses - The address block 192.0.2.0 to 192.0.2.255 (192.0.2.0 /24) is set aside for teaching and learning purposes. These addresses can be used in documentation and network examples. Unlike the experimental addresses, network devices will accept these addresses in their configurations. Addresses within this block should not appear on the Internet.

Assigning Addresses

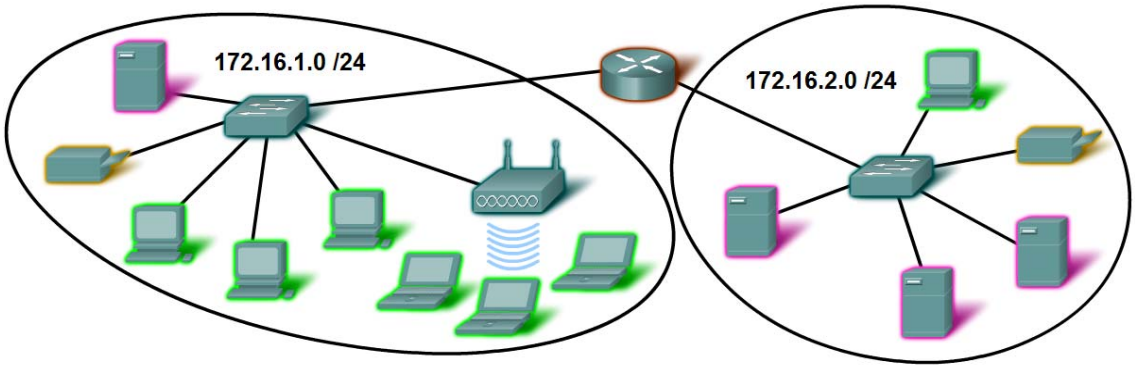
The allocation of addresses inside the networks should be planned and documented for the purpose of:

- Preventing duplication of addresses
- Providing and controlling access – (For example, if a server has a random address assigned).
- Monitoring Security and Performance.

Addresses that should be assigned to devices inside the network

Devices IP Address Ranges

Use	First Address	Last Address	Summary Address
Network Address	172.16.x.0	.....	172.16.x.0 /25
User hosts (DHCP pool)	172.16.x.1	172.16.x.127	
Servers	172.16.x.128	172.16.x.191	172.16.x.128 /26
Peripherals	172.16.x.192	172.16.x.223	172.16.x.192 /27
Networking devices	172.16.x.224	172.16.x.253	172.16.x.224 /27
Router (gateway)	172.16.x.254	.....	
Broadcast	172.16.x.255	.....	



The Internet Assigned Numbers Authority (IANA)

A company or organization that wishes to have network hosts accessible from the Internet must have a block of public addresses assigned. The use of these public addresses is regulated and the company or organization must have a block of addresses allocated to it. This is true for IPv4, IPv6, and multicast addresses. The IANA is the master holder of the IP addresses. The IP multicast addresses and the IPv6 addresses are obtained directly from IANA.

The Internet Service Providers (ISPs)

To get access to the services of the Internet, we have to connect our data network to the Internet using an Internet Service Provider (ISP). ISPs have their own set of internal data networks to manage Internet connectivity and to provide related services. Among the other services that an ISP generally provides to its customers are DNS services, e-mail services, and a website. Depending on the level of service required and available, customers use different tiers of an ISP.

There are three levels for the ISPs

- Level one - These ISPs are large national or international ISPs that are directly connected to the Internet backbone. The customers of level 1 ISPs are either lower-tiered ISPs or large companies and organizations. Because they are at the top of Internet connectivity, they engineer highly reliable connections and services. Among the technologies used to support this reliability are multiple connections to the Internet backbone.
- Level two - Level 2 ISPs acquire their Internet service from level 1 ISPs and give their service to level 3 ISPs
- Level 3 - Level 3 ISPs purchase their Internet service from level 2 ISPs. The focus of these ISPs is the retail and home markets in a specific locale.

The anding Process

Use the subnet mask and ANDing process to extract the network address from the IP address.

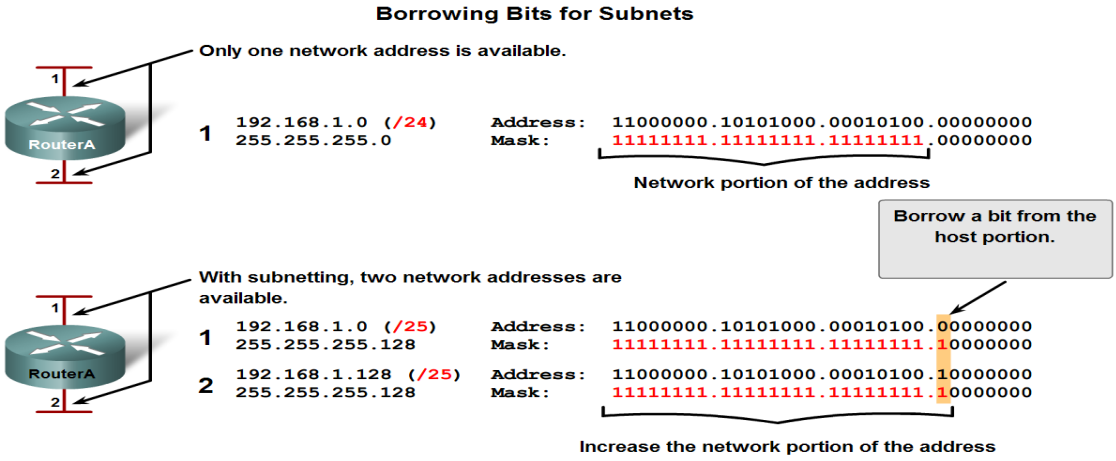
Applying the Subnet Mask

A device with address 192.0.0.1 belongs to network 192.0.0.0

	High order bits Prefix /16		Low order bits	
	192 .	0 .	0 .	1
Host	11000000	00000000	00000000	00000001
Subnet	255 11111111	255 11111111	0 00000000	0 00000000
Network	11000000	00000000	00000000	00000000

Subnetting

With IPv4 hierarchical addressing, the network portion of the address for all hosts in a network is the same. To divide a network, the network portion of the address is extended to use bits from the host portion of the address. These borrowed host bits are then used as network bits to represent the different subnetworks within the range of the original network.



Addressing Scheme: Example of 2 networks

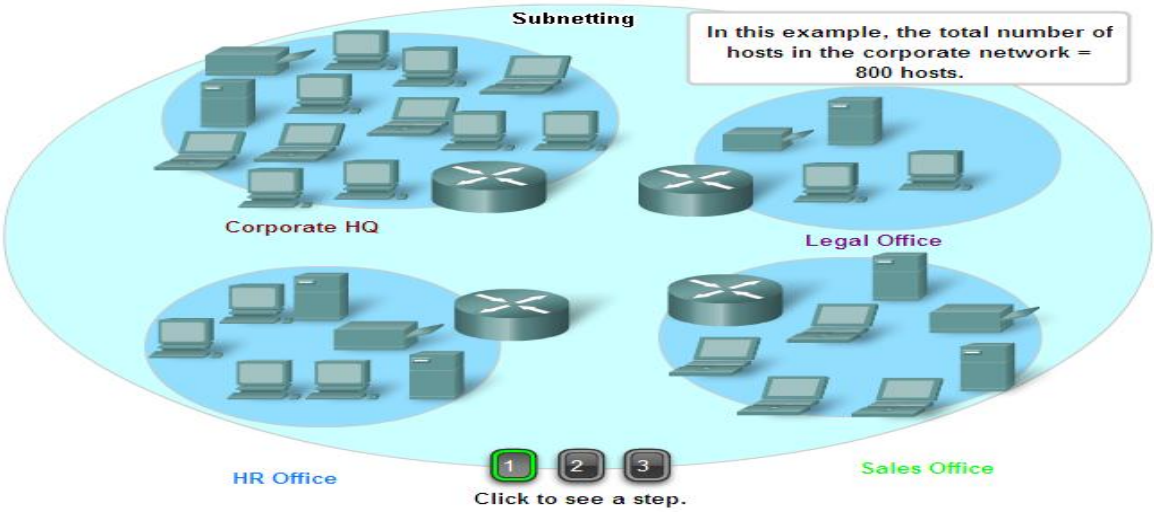
Subnet	Network address	Host range	Broadcast address
0	192.168.1.0/25	192.168.1.1 - 192.168.1.126	192.168.1.127
1	192.168.1.128/25	192.168.1.129 - 192.168.1.254	192.168.1.255

Example

Every network within the internetwork of a corporation or organization is designed to accommodate a finite number of hosts. Some networks, such as point-to-point WAN links, only require a maximum of two hosts. Other networks, such as a user LAN in a large building or department, may need to accommodate hundreds of hosts. Network administrators need to devise the internetwork addressing scheme to accommodate the maximum number of hosts for each network. The number of hosts in each division should allow for growth in the number of hosts.

Determine the Total Number of hosts

First, consider the total number of hosts required by the entire corporate internetwork. We must use a block of addresses that is large enough to accommodate all devices in all the corporate networks. This includes end user devices, servers, intermediate devices, and router interfaces.



Next, consider the number of networks and the size of each required based on common groupings of hosts. We subnet our network to overcome issues with location, size, and control. In designing the addressing, we consider the factors for grouping the hosts that we discussed previously:

- Grouping based on common geographic location
- Grouping hosts used for specific purposes
- Grouping based on ownership

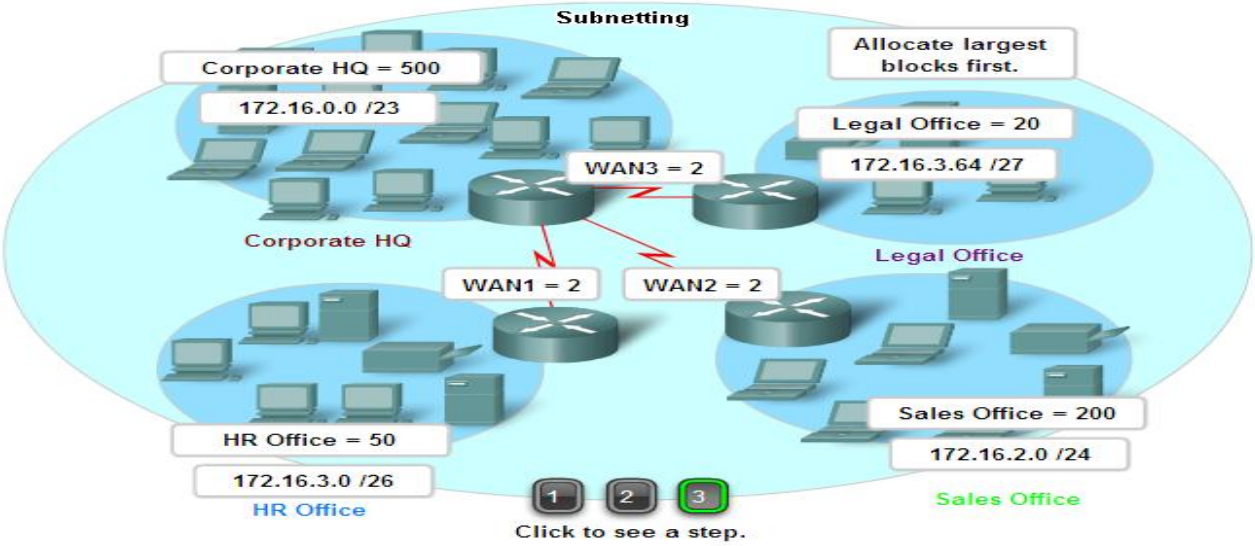
Each WAN link is a network. We create subnets for the WAN that interconnect different geographic locations. When connecting the different locations, we use a router to account for the hardware differences between the LANs and the WAN. Although hosts in a common geographic location typically comprise a single block of addresses, we may need to subnet this block to form additional networks at each location. We need to create subnetworks at the different locations that have hosts for common user needs.

Now that we have a count of the networks and the number of hosts for each network, we need to start allocating addresses from our overall block of addresses. See Step 3 of the figure.

This process begins by allocating network addresses for locations of special networks. We start with the locations that require the most hosts and work down to the point-to-point links. This process ensures that large

enough blocks of addresses are made available to accommodate the hosts and networks for these locations.

When making the divisions and assignment of available subnets, make sure that there are adequately-sized address blocks available for the larger demands. Also, plan carefully to ensure that the address blocks assigned to the subnet do not overlap.



IP v_6

In its early years, the Internet was largely used by universities, high-tech industry. With the explosion of interest in the Internet starting in the mid 1990s, it began to be used by different group of people, especially by people with different requirements producing a billion machines being used. Under these circumstances it became apparent that IP had to evolve and become more flexible. In 1990 the Internet Engineering Task Force (IETF) started work on a new version of IP, one which would never run out of addresses, would solve a variety of other problems, and be more flexible and efficient as well. Its major goals were:

1. Support billions of hosts, even with inefficient address space allocation.
2. Reduce the size of the routing table.
3. Simplify the protocol, to allow routers to process packets faster.
4. Provide better security (authentication and privacy) than current IP.
5. Pay more attention to the type of service, particularly for real-time data.
6. Allow the protocol to evolve in the future.

In general IPv6 is not compatible with IPv4, but it is compatible with other auxiliary protocols, including TCP,UDP, etc. the main features of IPv6 are discussed below:

First, IPv6 has longer addresses than IPv4, they are 16 bytes long, which solves the problem that IPv6 set out to solve: provide an effectively unlimited supplyof Internet addresses.

The second major improvement of IPv6 is the simplification of the header. It contains only seven fields (versus 13 in IPv4). This change allows routers to process packets faster and thus improve throughput and delay.

The third improvement was better support for options. This change was essential with the new header because fields that previously were required are now optional. In addition, the way options are represented is different, making them it simple for routers to skip over options not intended for them. This feature speeds up packet processing time.

The fourth area in which IPv6 represents a big advance is in security. Authentication and privacy are the key features of the new IP.

Finally, more attention has been paid to the quality of service.

The Main IPv6 Header

The **version** field (4-bit) is always 6 for IPv6.

The **Traffic class** field (8-bit) is used to distinguish between packets with different real-time delivery requirements. Experiments are now underway to determine how best it can be used for multimedia delivery

The **Flow label** field (20 bits) is also still experimental but will be used to allow a source and destination to set up a pseudoconnection with particular properties and requirements. For example, a stream of packets from one process on a certain source host to a certain process on a certain destination host might have stringent delay requirements and thus need reserved bandwidth. The flow can be set up in advance and given an identifier.

The **Payload** length field (16 bits) tells how many bytes follow the 40-byte header. The 40 header bytes are no longer counted as part of the length (as they used to be).

The **Next header** field (8 bits) there can be 6 (optional) extension headers. This field tells which of the currently six extension headers, if any, follows this one. If this header is the last IP header, the Next header field tells which transport protocol handler is the last IP header (e.g. TCP, UDP) to pass the packet to.

The **Hop limit** field (8 bits) is used to keep packets from living forever. It is in practice the same as the **time to live** in IPv4.

Next comes the **Source** and **Destination** address fields (16 bytes).

A new notation has been devised for writing 16-byte addresses. They are written as eight groups of four hexadecimal digits with colons between the groups, like this:

8000:0000:0000:0000:0123:4567:89AB:CDEF

Since many addresses will have many zeros inside them, three optimizations have been authorized. First, leading zeros with a group can be omitted, so 0123 can be written as 123, second, one or more groups of 16 zero bits can be replaced by a pair of colons. Thus, the above address now becomes

8000::123:4567:89AB:CDEF

Domain Name System (DNS)

Although programs theoretically could refer to hosts, mailboxes, and other resources by their n.etwork (e.g., IP) address, these addresses are hard for people to remember. consequently, ASCII names were introduced to decouple machine names from machine addresses. Nevertheless, the network itself understands only numerical addresses, so some mechanism is required to convert the ASCII strings to network addresses. To solve these problems DNS was invented.

The DNS Name Space

Conceptually the Internet is divided into over 200 top-level domains, where each domain covers many hosts. Each domain is partitioned into subdomains, and these are further partitioned, and so on. All these domains can be represented by a tree, as shown in the following figure. The leaves of the tree represent domains the have no subdomains. A leaf domain may contain a single host, or it may represent a company and contain thousands of hosts.

The top level domains come in two flavors: generic and countries. The original generic domains were *com* (commercial), *edu* (educational institutions), *gov* (Governmental), *int* (ceratin international orgaqnizations), *mil* (military), net (network providers) and *org* (nonprofit organizations). The country domain include one entry for every country, as defined in ISO 3166. In November 2000, four new general purpose top level domains were approved, *biz* (business), info (information), *name* (people's names), and *pro* (professionals such as doctors and lawyers).in addition to some certain industries. These are *aero* (aerospace industry), *coop* (co-operatives), and *museum* (museums). Other top-level domains will be added in the future.

In general, getting a second level-level domain, such as *name-of-company*.com, is easy. It merely requires going to a registrar for the corresponding top-level domain (*com* in the case) to check if the desired name is available and not somebody else's trademark. If there are no problems, the requester pays a small annual fee and gets the name.

Each domain is named by the path upward from it to the (unnamed) root. The components are separated by periods (dots). Thus the engineering department at Sun Microsystems might be *eng.sun.com*.

Domain names can be either absolute or relative. An absolute domain name always ends with a period (e.g., *eng.sun.com.*), whereas a relative one does not. Relative names have to be interpreted in some context to uniquely determine their true meaning. In both cases, a named domain refers to a specific node in the tree and all the nodes under it. There is no rule against registering under two top level domains (e.g. *sony.com* and *sony.nl*).

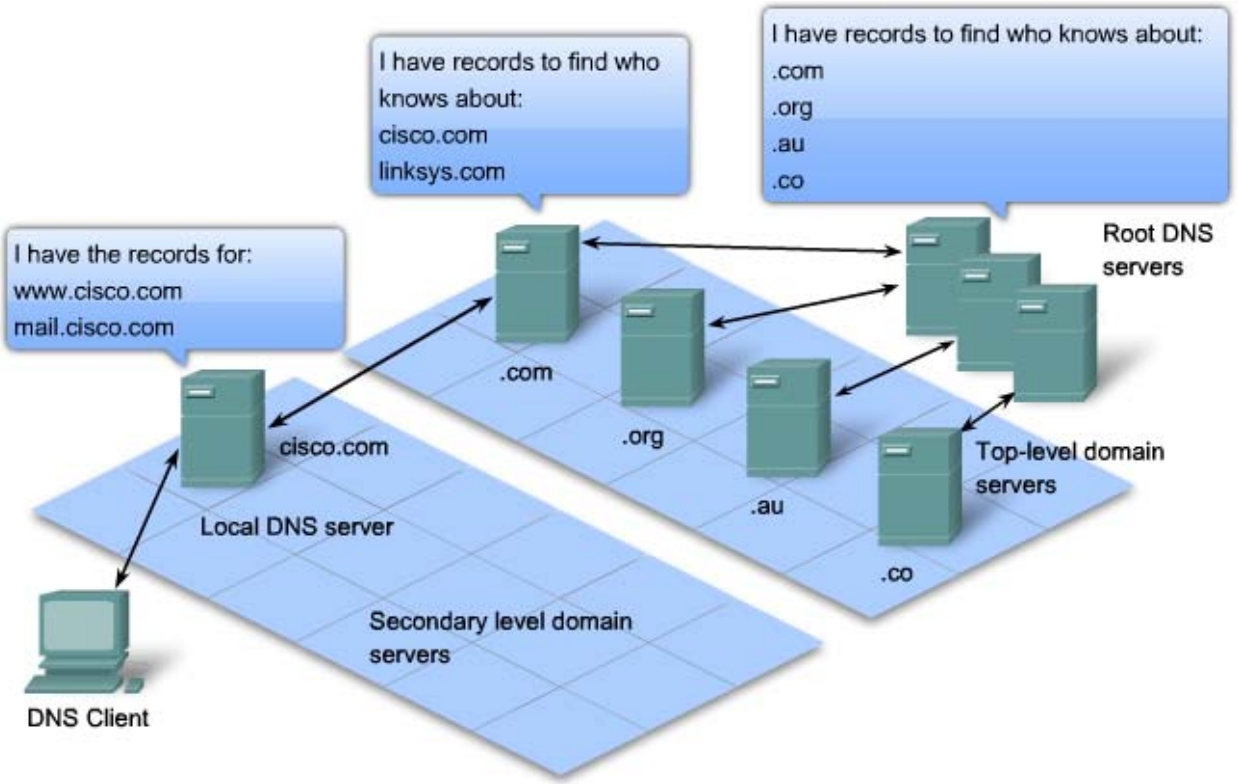
Resource Records

Every domain, whether it is a single host or a top-level domain, can have a set of **resource records** associated with it. For a single host, the most common resource record is just its IP address. When a resolver gives a domain name to **DNS**, what it gets back are the resource records associated with that name. thus the primary function of **DNS** is to map domain names onto resource records.

Name Servers

In theory at least, a single name server could contain the entire **DNS** database and respond to all queries about it. In practice, this server would so overloaded a s to be useless. Furthermore, if it ever went down, the entire Internet would be crippled.

To avoid the problem associated with having only a single source of information, the **DNS** name space is divided into nonoverlapping **zones** (as shown in the figure). Each zone contains some part of the tree and also contains name servers holding the information about that zone. Normally, a zone will have one primary name server, which gets its information from a file on its disk, and one or more secondary name servers, which get their information from the primary server.


I have records to find who knows about:
.com
.org
.au
.co
I have records to find who knows about:
cisco.com
linksys.com
I have the records for:
www.cisco.com
mail.cisco.com
Root DNS servers
.com
.org
.au
.co
Top-level domain servers
cisco.com
Local DNS server
Secondary level domain servers
DNS Client