COMPUTER NETWORKS

(CS610)

HANDOUTS

LECTURERS # 01 – 45

PREPARED BY:

HAMMAD KHALID KHAN

Table of contents

Lecture No. 1

INTRODUCTION

NETWORK:

A network is defined as a system for connecting computers using a single transmission technology. The computers can communicate with each other in a network. They can send and receive data from each other when they are in a network.

INTERNET:

The Internet is defined as the set of networks connected by routers that are configured to pass traffic among any computers attached to any network in the set. By internet many computers which are at longer distances from each other can communicate with each other.

CLASSIFICATION OF NETWORKS

Computer networks are classified by four factors which are as follow:

1) BY SIZE:
2) BY CONNECTIVITY:
3) BY MEDIUM:
4) BY MOBILITY:

Long Q

1) BY SIZE:

According to their size there are two classifications of networks.

1. Local Area Network. (LAN)
2. Wide Area Network (WAN)

In LAN network occupies the smaller area like a room a floor or a building.

In WAN, network occupies larger areas like cities & countries. Internet is a Wide Area Network.
LAN & WAN are compared by the speed of transmission, bandwidth and latency, management, security, reliability, billing and their standards.

2) BY CONNECTIVITY:

Networks are also classified by connectivity in which two topologies are discussed.

a) Point-to-Point
b) Broadcast

a) POINT-TO-POINT:

In *Point-to-Point* topology there are two topologies.

1) STAR topology
2) TREE topology

In *star* topology each computer is connected to a central hub. The communication takes place through the hub. It is shown in the figure below.

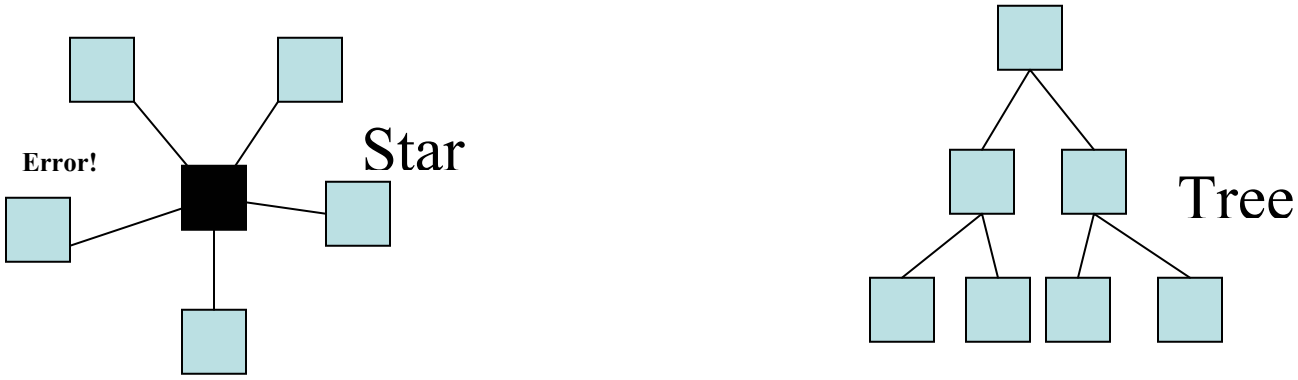


Figure 1.1: star and tree topologies

In Tree topology all computers are connected to each other in such a way that they make a tree as shown in the figure above.

b) BROADCAST:

In broadcast topology there are further two categories

1) SATELLITE\RADIO 2) RING TOPOLOGY

In a satellite or radio topology all computers are connected to each other via satellite or radio wave as shown in the figure.

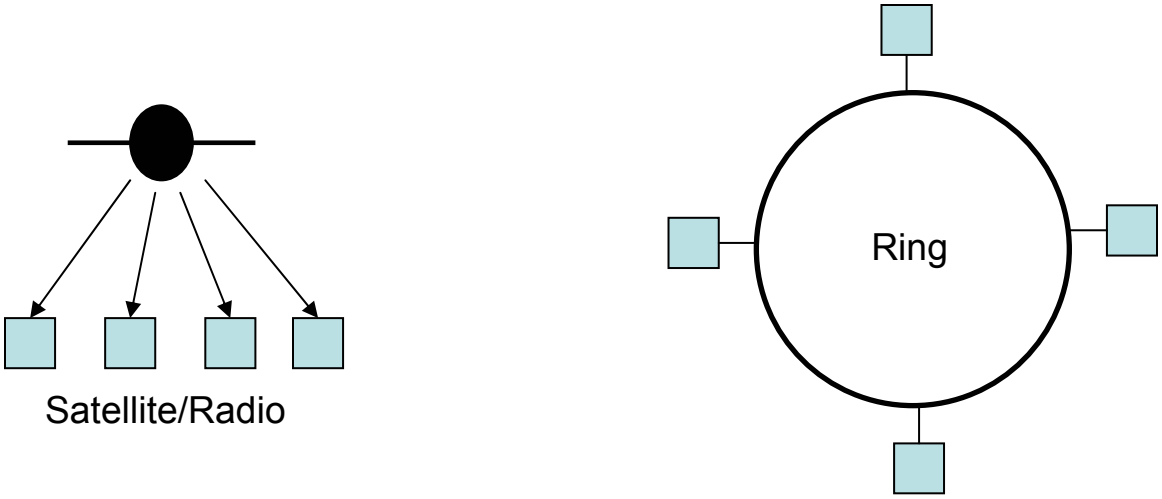


Figure: 1.2 Satellite and Ring topologies: In a ring topology each computer is connected to other thorough a ring as shown in the figure above.

3) BY MEDIUM:

The classification of networks is also based on the Medium of transmission.
Following are the mediums of transmission:

- Copper wire
- Co-axial cable
- Optical fiber
- Radio waves

All these mediums differ from each other with respect different parameters. These parameters are speed of transmission, range of the receiver and transmitter computer, sharing of information, topology, installation & maintenance costs and reliability.
For example the range of radio waves will be much more than an optical fiber. Similarly other mediums differ from each other and appropriate medium is selected for the sake of transmission.

4) BY MOBILITY:

The networks are also classified according to their mobility.
In this respect there are two types of networks.

- Fixed networks
- Mobile networks

In these days mobile networks are the hot case. Mobile networks have been emerged in the last decade. In this regard there are some issues which are attached with the mobility of networks which are as follows:

- Location and tracking
- Semi persistent connections
- Complex administration and billing as devices and users move around the network.

NETWORKS IN DAILY LIFE:

The major use of networks is in business side. Networks are used for advertising, production, shipping, planning, billing and accounting purposes. In fact now there is an entire industry that develops networking equipment.

In addition to this networks are being used in homes as well for example, to switch and control different devices from one place.

Networks are very much useful at government level as federal government, local government and military organization use networks for communication purposes.

In education we have online libraries which we can visit at our home PC. This is all just due to the networks.

COMPLEXITY OF NETWORK SYSTEMS:

A computer network is a complex subject due to the following reasons:

• MANY DIFFERENT TECHNOLOGIES EXIST:

The first reason for the complexity of networks is that there are many different technologies exist for networking and each technology features is different from the other. This is because many companies have developed networking standards, which are not compatible with each other. In this way multiple technologies exist that are used to connect different networks.

• NO SINGLE UNDERLYING THEORY OR MODEL:

The second reason for the complexity of networks is that there is no single underlying theory or model, which specifies or defines different aspects of networking. Rather, various organizations and research groups have developed conceptual models that can be used to explain differences and similarities between network hardware and software.

• MODELS ARE EITHER SO SIMPLISTIC OR SO COMPLEX:

Another reason for the complexity of networks is that the conceptual models made by organization are either so simplistic that they do not distinguish between details, or they are so complex that they do not simplify the subject.

• NO SIMPLE OR UNIFORM TERMINOLOGY:

One reason for the complexity of networks is that there is no simple or uniform terminology that can be used for the same feature. Different technologies use different terminologies. In this way terms are confused with product names.

MASTERING THE COMPLEXITY

To master the complexity one must follow the following points.

• CONCENTRATE IN UNDERSTANDING THE CONCEPTS:

Instead of details of wires used to connect computers to a specific network, it is important to understand a few basic categories of wiring schemes their advantages and disadvantages.
For example:

Instead of how a specific protocol handles congestion, we should concentrate on what congestion is and why it must be handled.

• LEARNING THE NETWORKING TERMINOLOGY:

The second tool for mastering the complexity is to learn the networking terminology. In addition to this one must concentrate the concepts and not details, concentrate on breath and not the depth of technologies, also one should understand the analogies and illustrations
Network terminology is introduced with new concepts so it is much helpful to learn the terminology to overcome the complexity of networks.

Lecture No. 2

Motivation and Tools

One of the reasons of motivation towards networking was resource sharing which is discussed as follows.

Resource sharing:

Resource sharing means to share the resources available among many users.
In an office as it is very expensive to give a separate printer to each worker. So if the printer is shared among the workers then a single printer will be accessible to each worker. This leads to the motivation of resource sharing.

Goal of resource sharing:

The goal of resource sharing is to make all programs, equipment and date available to anyone in the network without regard to physical location of the resource and the user.
For example: the sharing of a printer among the workers in an office and also the sharing of information is a goal of resource sharing.

Main reason for early resource sharing:

The main reason for early resource sharing was not to share the peripheral devices rather to share the large-scale computational power because computer were extremely expensive in those days and the government budgets were not sufficient to provide computers for all scientist and engineers. By resource sharing a researcher could use whichever computer was best suited to perform a given task.

Efforts of advanced research project AGENCY (ARPA):

The efforts of ARPA was to enable all its research groups have access to latest computers. For this purpose ARPA started investing in ways to do data networking ARPA use a new approach consisting of packet switching and internetworking to fulfill the purpose of resource sharing. As a result of ARPA research the first network was established which was named ARPANET.
In this way the internet was emerged in 1970's and it has grown drastically since then as shown in the figure below.

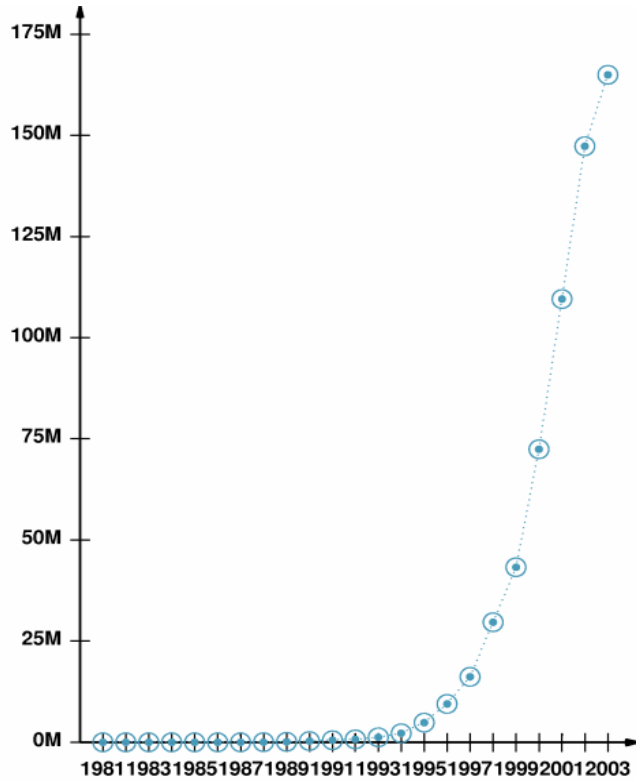


Figure. 2.1 Growth of the Internet

As shown in another figure below. In log scale the position on y-axis is proportional to the log of the number being represented. So the values along y-axis represent the power of 10.

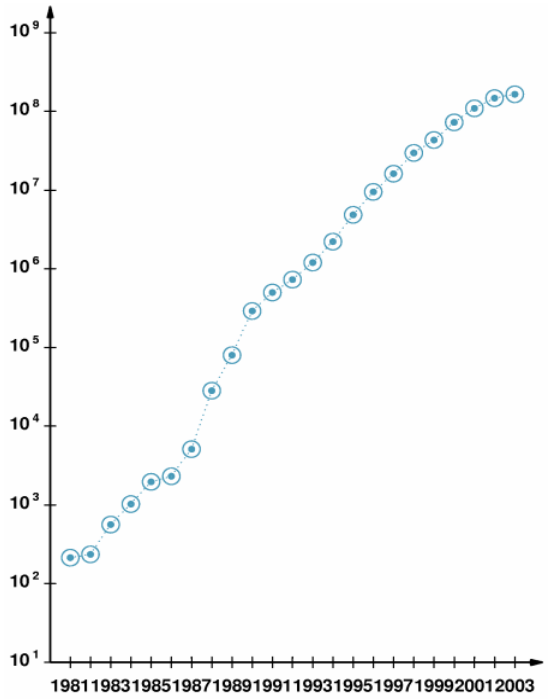


Fig. 2.2 Growth of the internet on Log Scale

We see that on log scale the growth appears almost linear it means that internet experienced an exponential growth. We also observed that internet has been doubled every nine to twelve months.

PROBING THE INTERNET:

Let us see how are the figures in above graphs obtained?
In the early days when there were some dozen computers on the network, it was done manually but now as we have seen that there are millions of computers on the internet so how can we calculate the number of computers connected to the internet. This is done through probing the Internet.
Now an automated tool is required that tests to see whether the given computer is online or not. For this purpose the first tool is the `PING program` which is shown in the figure below.

```
PING sears.com: 56 data bytes
64 bytes from 32.97.168.129: icmp_seq=0. time=49. ms
64 bytes from 32.97.168.129: icmp_seq=1. time=50. ms
64 bytes from 32.97.168.129: icmp_seq=2. time=48. ms
64 bytes from 32.97.168.129: icmp_seq=3. time=50. ms
64 bytes from 32.97.168.129: icmp_seq=4. time=48. ms
----sears.com PING Statistics----
5 packets transmitted, 5 packets received, 0% packet loss
round-trip (ms)  min/avg/max = 48/49/50
```

Type text here

Figure 2.3 THE PING Command

We see that 5 packets of 64 bytes are sent to sears.com and 5 packets are received. We see that ping has also given some additional information such the IP addresses of sears.com, the sequence of packets and the times of transmission known as the round-trip time, as there is no packet loss so it means that sears.com is connected to the internet.

PROBLEM WITH 'PING':

Ping, as a tool seems to be simplistic. Now let's see what are the problems attached with ping. If ping does not review any responses from host computer it can not tell the reason of problem. Because one of the following reasons occurs, but ping will not specify the reason.

- Remote computer might have a problem.
- Local computer might have a problem.
- Ping sometimes fails because of congestion.

Some networks or computers reject the ping packets. They do this to avoid denial of service of flooding attack.

Inspite of these problems ping is still heavily used as a diagnostic tool.
Network administrators use ping as soon as they learn about the failure.

Tracing a Route:

There is another probing tool i-e Trace Route. To get more detail it is used.

```
traceroute to DANDELION-PATCH.MIT.EDU (18.181.0.31), 40 byte packets
 1  cisco1 (128.10.2.250)  2 ms  1 ms  2 ms
 2  cisco-tel-252.tcom.purdue.edu (128.210.252.22)  2 ms  1 ms  1 ms
 3  abilene.tcom.purdue.edu (192.5.40.10)  6 ms  8 ms  7 ms
 4  clev-ipls.abilene.ucaid.edu (198.32.8.26)  14 ms  14 ms  12 ms
 5  nycm-clev.abilene.ucaid.edu (198.32.8.30)  24 ms  27 ms  24 ms
 6  192.5.89.45 (192.5.89.45)  31 ms  34 ms  35 ms
 7  192.5.89.10 (192.5.89.10)  33 ms  33 ms  33 ms
 8  NW12-RTR-FDDI.MIT.EDU (18.168.0.16)  59 ms  34 ms  33 ms
 9  DANDELION-PATCH.MIT.EDU (18.181.0.31)  62 ms *  79 ms
```

Figure 2.4

As shown in the figure about the route to DANDELION-PATCH.MIT.EDU was traced out and the program showed all eight computers that were in the way. The additional information is also shown in the figure.

Thus we see that tracing a route is more interesting tool than Ping as it tells about each computer that falls in the way of source and destination computers.

Lecture No. 3

Overview of Data Communication

NOTE: -

Chapter 4, 5, 6 deals with the course of DATA COMMUNICATION, which has been studied as a separate, course earlier. So these chapters are just overviewed and can be seen in the third lecture video.

It should also be noted that these chapters will contain no assignment, or quizzes and these chapters will also be out of the examination.

Lecture No. 4

PACKETS, FRAMES AND ERROR DETECTION

INTRODUCTION:

The previous chapters of data communication described how bits are transmitted across a physical network using a transmission medium.

This chapter introduces the concept of packets of data rather than bits for communication.

CONCEPT OF 'PACKET':

Network systems divide data in small blocks or junks called packets, which they send individually. Why we need packets rather than bits? The answer to this question is because a sender and receiver need to coordinate to detect transmission errors. Also the individual connection between each pair of computers is not possible. That's why to solve these problems shard network connections are made among many workstations.

PROBLEMS WITH SHARING:

The demand of sharing is very high because many computers need to use the shared networks. In addition to this some applications have large data transfer. In this way they hold the network for long time. But on the other hand some applications cannot wait so long. So we need a mechanism for fairness.

SOLUTION FOR FAIRNESS:

To the fairness, the solution is to divide the data into small block or chunks called 'PACKETS'. Computers take turns to send one packet at a time over the shared connection.

Because each packet is small so no computer experiences a long delay.

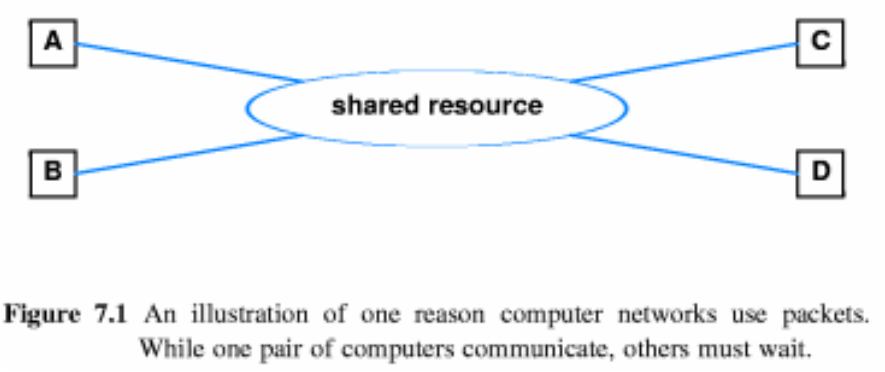


Figure 7.1 An illustration of one reason computer networks use packets. While one pair of computers communicate, others must wait.

Example:

In the figure one reason for using the packets is illustrated. We see that in a shared resource when one pair of computer communicates, the other must wait. To understand the use of packet here, let's suppose a transmission with packets in the figure.

WITHOUT PACKETS:

A 5MB file transferred across network with 56Kpbs capacity will require 12 minutes.
This means that all that computers will be forced to wait for 12 minutes before initiating other transfers.

$$\frac{5x10^6 \text{ bytes } * \text{ 8 bits / byte}}{60 \text{ secs / minute } * \text{ } 56x10^3 \text{ bits / second}} = 11.9 \text{ minutes}$$

WITH PACKETS:

Now if the file is broken into packets, other computers must only wait until packet (not entire file) has been sent.
Suppose file is broken into 1000 byte packets.
Now each packet takes less than 0.2 seconds to transmit. Here other computers must only

$$\frac{1000 \text{ bytes } * \text{ 8 bits / byte}}{56x10^3 \text{ bits / second}} = .143 \text{ seconds}$$

wait for 0.14 sec before beginning to transmit.
Note: - if both files are 5MB long, each now takes 24 minutes to transmit. But if the second file is 10MB long it sill be transmitted in only 2.8 seconds while 5MB file still takes roughly 12 minutes.

PACKETS AND TDM:

Dividing data into small packets allow time division multiplexing. In TDM each packet leaves the source and is switched on the shared communication channel through a multiplexer. At the destination the packet is switched through a demultiplexer to the destination.
In the figure this process is illustrated with a multiplexing circuit shown.

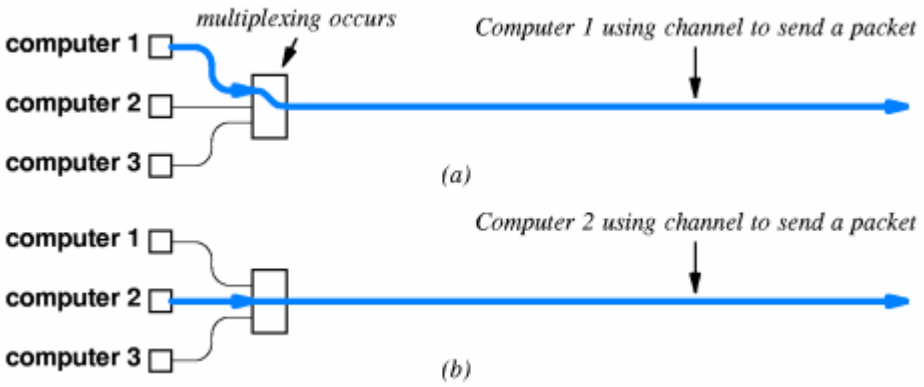


Figure 4.2 illustration of TDM

PACKETS AND FRAMES:

PACKETS:

Packet is a generic term that refers to small block of data. Packet have different format. Each hardware uses different packet format.

FRAME:

A frame or hardware frame denotes a packet of a specific format on a specific hardware technology.

FRAME FORMAT:

We need to define a standard format for data to indicate the beginning and end of the frame. Header and tail are used to frame the data as shown in the figure below.

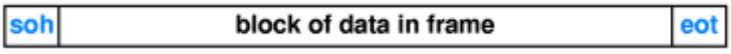


Figure 4.3 illustration of a Frame

We see that in the figure soh and eot are used to denote the start of header and end of tail.

FRAMING IN PRACTICE:

In practice there is a disadvantage of overhead. To avoid the no delay between two frames each frame sends an extra character between block of data.
The framing in practice also has some transmission problems just like:

- Missing eot indicates sending computer crashed.
- Missing soh indicates receiving computer missed beginning of message.
- Bad frame is discarded.

Lecture No. 5

BYTE STUFFING

Sometimes the special character (i-e soh and eot) may appear in data and as a part of data they will be misinterpreted as framing data.
The solution to this problem is Byte stuffing.

Long Q

In general to distinguish between data being sent and control information such as frame delimiters network systems arrange for the sending side to change the data slightly before it is sent because systems usually insert data or bytes to change data for transmission, the technique is known as Data Stuffing.

There are two types of data stuffing:

- Byte Stuffing
- Bit Stuffing

Byte stuffing refers stuffing with character oriented hardware and bit stuffing refers to bit oriented hardware.

Byte stuffing translates each reserved byte into two unreserved bytes. For example: it can use esc as prefix followed by x for soh, y for eot and z for eco.

The receiver then replaces each occurrence of esc x, esc y and esc z by the corresponding single character. This is shown in figure below:

Character In Data	Characters Sent
soh	esc x
eot	esc y
esc	esc z

Figure 5.1

Byte stuffing is illustrated in another figure below we can see the replacement of characters.

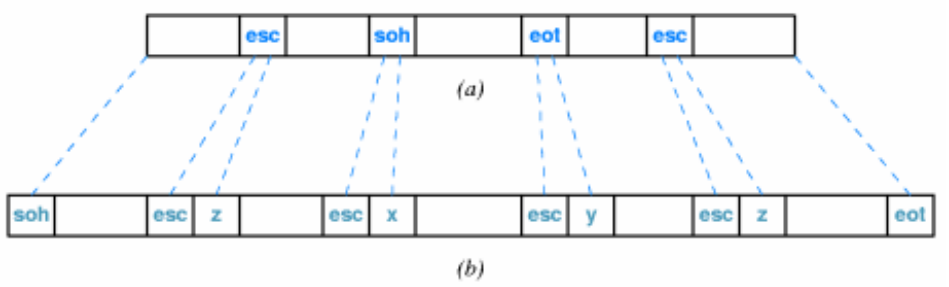


Figure 7.5 Illustration of byte stuffing, where (a) is an example of data that includes characters such as *soh*, and (b) is the frame after byte stuffing. The dashed lines show the locations in the original data where characters have been replaced or new characters added.

TRANSMISSION ERRORS:

Transmission errors may occur due to different causes for example interference or power surges may destroy data during transmission. In result of which the bits are lost or the bit value may be changed.

ERROR DETECTION AND CORRECTION:

To detect and correct errors, frames include additional information, which is inserted by the sender and checked by the receiver. In this way incorrect data can be rejected. Also the incorrect data can be corrected and accepted.

PARITY CHECKING:

To detect the error there are different schemes in which parity checking is also commonly used. In parity checking, parity refers to the number of bits set to 1 in the data item.
There are two types:

- Even Parity
- Odd Parity

EVEN PARITY:

In an even parity the no. of 1's in data should be an even number.

ODD PARITY:

In an Odd parity the no. of bits should be an odd number.

PARITY BIT:

A parity bit is an extra bit transmitted with data item chose to give the resulting bit even or odd parity.

For example an even parity data 10010001 has parity bit 1 as it has odd number of 1's. An odd parity data 10010111 has parity bit 0 as it has odd number of 1's.

Let us consider another example, if noise or other interference introduces an error one of the bits in the data will be changed from a 1 to a 0 or from a 0 to a 1. Thus the parity of resulting bits will be large.

Suppose original data and parity is 10010001+1 (even parity). After interference the incorrect data is 10110001+1 and it has become an odd parity.

Long Q

LIMITATIONS OF PARITY CHECKING:

Parity can only detect errors that change in odd number of bits for example the original data and parity is 10010001+1 (even parity) and the incorrect data is 10110011+1 (even parity). We see that even no. of bits have been changed due to noise so parity checking can not detect this error.
Parity usually is used to detect on bit error.

ALTERNATIVE ERROR DETECTION SCHEMES:

In addition to parity checking alternative error detection mechanisms have been introduced. These mechanisms differ from each other by the following respects.

- The size of the additional information (transmission overhead)
- Computational complexity of the algorithm (computational overhead)
- The number of bits errors that can be detected (how well errors are detected)

CHECKSUM

The second procedure used to detect errors is checksum. In this procedure data is treated as a sequence of integers and their arithmetic sum is computed and the carry bits are added to the final sum. Then checksum is calculated by transmission then it is sent along the data and the receiver and the same calculation is performed and then compared with the original checksum transmitted. In this way errors are detected if the received checksum is different from the sent.
The figure illustrates the example.

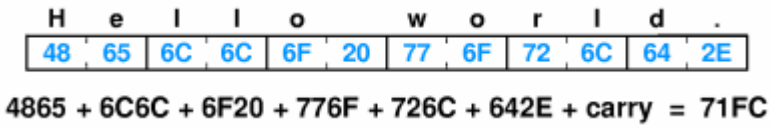


Figure 5.3

The integers can be 8, 16 or 32 bits. Checksum is easy to do. It uses only addition but it has also limitations and can not detect all errors. As shown below.

Data Item In Binary	Checksum Value	Data Item In Binary	Checksum Value
0001	1	0011	3
0010	2	0000	0
0011	3	0001	1
0001	1	0011	3
totals	7		7

Figure 5.4

CYCLIC REDUNDANCY CHECK (CRC):

To enable a network system to detect move error without increasing the amount of information in each packet another most successful approach is made which is called CRC.

To understand the concepts of CRC consider data in a message as co-efficient of a polynomial. Their co-efficient set is divided by a known polynomial.

The remainder of this division is then transmitted as CRC and checked at the receiver to detect errors.

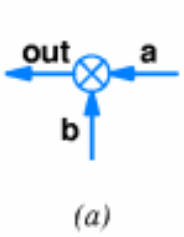
CRC has good error detection properties. It is easy to implement in hardware.

HARDWARE COMPONENTS USED IN CRC:

CRC uses just two hardware components:

- Shift register
- Exclusive OR (XOR unit)

The XOR unit is shown in the figure below.



(a)

a	b	out
0	0	0
0	1	1
1	0	1
1	1	0

(b)

Figure 5.5

Shift register is also shown in figure. It performs two operations.

- Initialize: sets all bits to zero
- Shift: moves all bits to the left position.

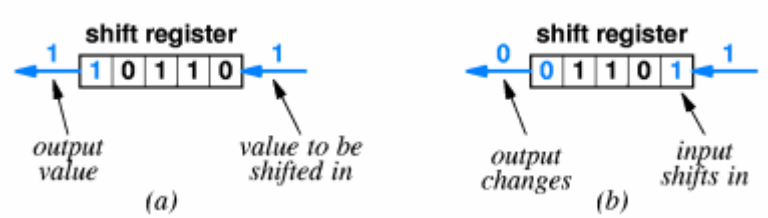


Figure 5.6

Lecture No. 6

SHIFT OPERATION

This operation shifts all bits to the left one position. For example in the figure below a 16-bit CRC hardware is shown, which uses three shift registers and three Exclusive OR (XOR) units.

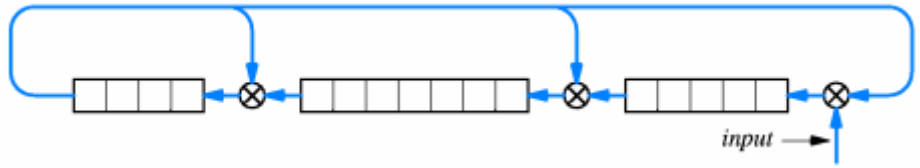


Figure 6.1

We see that this hardware can compute 16-bit CRC. Also in the figure, we see that the registers are initialized to zero and the bits of message are shifted through the input. When all 16 bits are shifted then the CRC is found in the registers.

In another figure, we see that input data is all 1s and CRC shown after 15, 16, 17 bits are shifted and feedback introduces 0s in CRC.

TYPES OF ERRORS:

CRC can check the following errors better than check sums.

a) Vertical errors b) Burst errors

a) VERTICAL ERRORS:

This type of error occurs due to a hardware failure. e.g. the second bit of every character will damage.

b) BURST ERRORS:

When a small set of bits changes near a specific location due to lighting or electric motor starting nearby etc. then these types of errors are called Burst errors.

FRAME FORMAT AND ERROR DETECTION:

The modified frame format also includes CRC. If there is an error occurred in frame, then it typically causes receiver to discard frame. The frame including CRC is shown in the figure.

Figure 6.2

LAN TECHNOLOGY AND NETWORK TOPOLOGY

Most networks are local and are designed to share resources among multiple computers. Hardware technologies used for local networks allow multiple devices to connect with a shared network. In this shared medium the computers must take turns using the shared medium.

DIRECT POINT-TO-POINT COMMUNICATION:

Early networks used direct point-to-point communication. In such a mode of communication each communication channel connects exactly two computers. In this way it forms a mesh or point-to-point network, which is shown in the figure below.

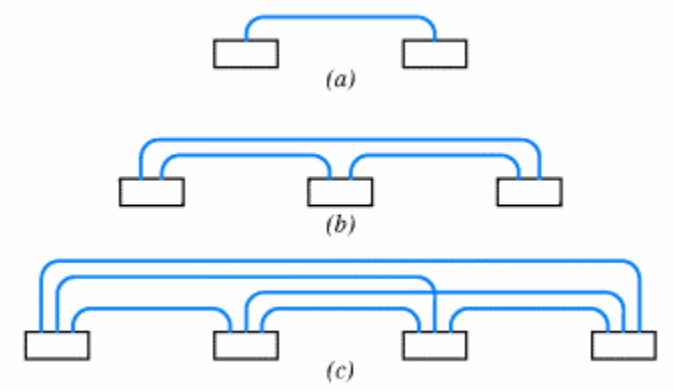


Figure 6.3

ADVANTAGES:

Direct point-to-point communication has the following advantages:

- The connection type of individual connections can be different.
- Individual connections can choose a different frame format and error detection mechanism etc.
- It is easy to enforce security and privacy.

DISADVANTAGES:

Direct point-to-point communication has the following disadvantages:

- The no. of connections grow more rapidly than the no. of computers
- For ‘n’ computers connections = (n^2 – n)/2.
- Most computers use the same physical path.
- Direct point-to-point communication is expensive due to a no. of connections.
- Another disadvantage is that adding a new computer to the network requires N-1 new connections as shown in the above figure.

Lecture No. 7

GROWTH OF LAN TECHNOLOGY

The development of shared communication channels (LANs) started in 1960s and early 1970.
The key idea behind was to reduce the number of connections by sharing connection among many computers

Each LAN consists of a single shared medium. The computers take turns using the medium. First one computer uses the medium to send its data over the channel then second and son on. But sharing a single medium over long distances is efficient, due to the long delays.

LAN technologies reduce cost by reducing no. of connections. But attached computers compete for use of shared connections. The local communication consists of LAN exclusively. But the long distance communication is point-to-point exclusively.

SIGNIFICATION OF LANs AND LOCALITY OF REFERENCE:

LANs are most popular form of computer networks. One of its bright features is that this technology is inexpensive. The demand of LANs is related to a principle known as "Locality of Reference Principle".

"LOCALITY OF REFERENCE" PRINCIPLE:

Principle of "Locality of Reference" helps predict computer communication patterns. There are two patterns given as follows:

A) SPATIAL LOCALITY OF REFERENCE
B) TEMPORAL LOCALITY OF REFERENCE

a) SPATIAL LOCALITY OF REFERENCE:

In this pattern computers are likely to communicate with other computers that are located nearby.

b) TEMPORAL LOCALITY OF REFERENCE:

In this pattern computers are likely to communicate with the same computers repeatedly. Thus LANs are effective because of spatial locality of reference. Temporal locality of reference may give insight into which computers should be on a LAN.

LAN TOPOLOGIES:

Network can be classified by shape. According to which there are three most popular topologies, which are given as follows;

- Star
- Ring
- Bus

STAR TOPOLOGY:

In this topology, all computers are attached to a central point, which is sometimes called the "Hub" as shown in the figure below.

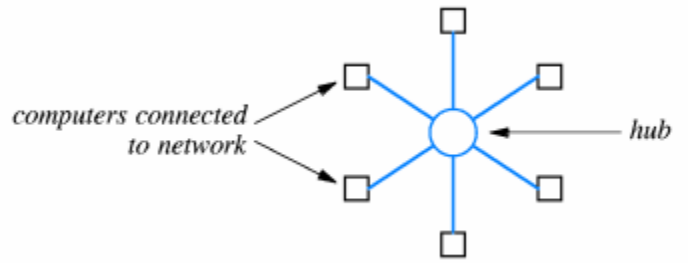


FIGURE 7.1 AN IDEALIZED STAR NETWORK

It is important to note that these networks are not physically like stars but they are logically like stars. It means that their shape does not look like a star but their connections are just like a star. The above diagram is idealized. Here is shown a star network in practice in the figure below:

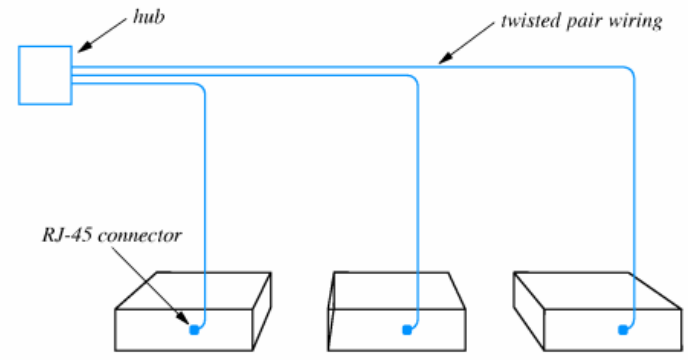


FIGURE 7.2 STAR NETWORK IN PRACTICE

RING TOPOLOGY:

In this topology of network the computers are connected to each other in closed loop. In this network first computer passes data to the second and then second passes data to third and so on, as shown in the figure.

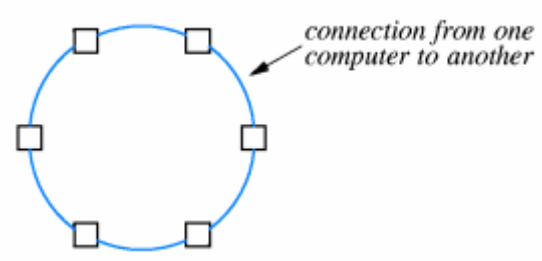


FIGURE 7.3

Like star topology the ring network are also logically ring and not physically.

BUS TOPOLOGY:

In a bus topology all computers are attached to a single long cable and any computer can send data to any other computer.

For this purpose, coordination is required to decide which computer has to use the line at what time. The bus topology is shown below:

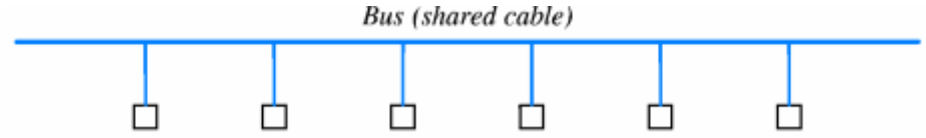


FIGURE 7.4 BUS TOPOLOGY

REASON FOR MULTIPLE TOPOLOGIES:

Each topology has advantages and disadvantages, which are discussed below:

IN A RING:

It is easy to coordinate access to other computers however entire network is disabled if a cable cut occurs.

IN A STAR:

On the other hand only once computer is affected when a cable cut occurs.

IN A BUS:

The network needs fewer wires than a star, however entire network is disabled when a cable cut occurs.

EXAMPLE BUS NETWORK; ETHERNET:

Ethernet is a widely used LAN technology. It was invented at EXROX PARC (Palo Alto Research Center) in 1970s.
Xerox, Intel and Digital defined it in a standard so it is also called DIX standard. The standard is now managed by IEEE in which 802.3 standard of IEEE defines formats, voltages of cable length etc.

The Ethernet uses bus topology. It uses a single coaxial cable. To which multiple computers connect.

One Ethernet cable is sometimes called a segment. This segment is limited to 500 meters in length. The minimum separation between connections is 3 meters.

ETHERNET SPEEDS:

The Ethernet speed was originally 3Mbps, and the current standard is 10Mbps the fast Ethernet operates at 100Mbps. There are also gigabits Ethernet available now.

ENCODING USED IN ETHERNET:

The encoding used in Ethernet is Manchester encoding. It uses signal changes to encode data.
e.g. A change from positive voltage to 0 encodes as shown in the figure below:

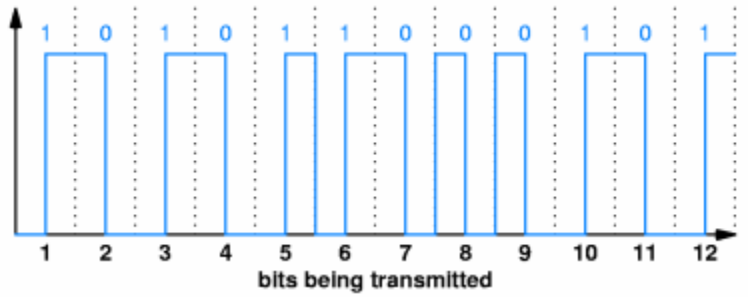


FIGURE 7.5

Lecture No. 8

CARRIER SENSE MULTIPLE ACCESS (CSMA)

There is no central control management when computers transmit on Ethernet. For this purpose the Ethernet employs CSMA to coordinate transmission among multiple attached computers.

CSMA is a coordination scheme that defines how to take turns using a shared cable.

A computer listen to the codes i.e. it senses the carrier. If the cable is idle it starts transmitting and if the cable is in use then it waits.

If simultaneous transmission occurs, the frames interfere with each other and this phenomenon is called collision.

COLLISION DETECTION:

As explained above, the signals from two computers will interfere with each other and the overlapping of frames is called a collision.
It does not harm to the hardware but data from both frames is grabbled.

ETHERNET CD:

To detect the collision, Ethernet interfaces include hardware to detect transmission. It performs two operations:

- It monitors outgoing signals.
- Grabbled signal is interpreted as a collision.

After collision is detected computers stop transmitting. So Ethernet uses CSMA/CD to coordinate transmission.

RECOVERY FROM COLLISION:

Computer that detects a collision sends special signal to force all other interfaces to detect collision.

Computer then waits for other to be idle before transmission. But if both computers wait for same length of time, frames will collide again. So the standard specifies maximum delay and both computers choose random delay, which is lesser. After waiting, computers use carrier sense to avoid subsequence collision.
The computer with shorter delay will go first and other computer may transmit later.

EXPONENTIAL BACK OFF:

Even with random delays, collision may occur especially likely with busy segments. Computers double delay with each subsequent collision. It reduces likely hood of sequence of collision.

802.11 WIRELESS LANs AND CSMA/CA:

IEEE 802.11 is standard wireless LAN that uses radio signals at 2.4GHz. Its data rate is 11Mbps. The older devices use radio signals at 900MHz and data rate of 2Mbps. Bluetooth specifies a wireless LAN for short distances. It uses shared medium and radio waves instead of coaxial cable.

Long Q

LIMITED CONNECTIVITY WITH WIRELESS:

In contrast with wired LANs, not all participants may be able to reach each other. Because:

- It has low signal strength.
- In wireless LANs the propagation is blocked by walls etc.
- It can't depend on CD to avoid interference because not all participants may hear.

This is shown in the figure below:

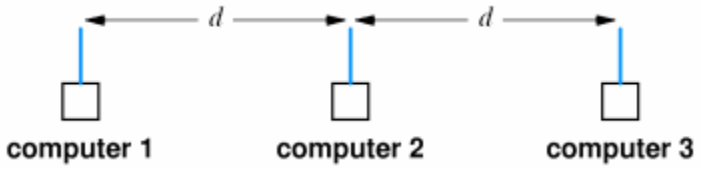


FIGURE 8.1

CSMA/CA:

Wireless uses collision avoid ness rather than collision detection. Transmitting computer sends very short message to receiver. Receiver responds with short message reserving slot for transmitter. The response from receiver is broadcast, so all potential transmitters receive reservation.

COLLISION:

The receiver may receive simultaneous requests, which results in collision at receivers and both requests lost and in this way no transmitter receives reservations and both use back off and retry. The receiver may receive closely spaced requests. It selects

one of them and then the selected transmitter sends message and the transmitter not selected uses back off and retries.

LOCAL TALK:

Apple invented the LAN technology that uses bus topology. Its interface is included with all Macintosh computers.
It has relatively low speed i.e. 230.4Kbps. Also it is of low cost and we can get a free with a Macintosh, which is easy to install and connect. It uses CSMA/CA.

TOKEN RING:

Many LAN technologies that are ring topology use token passing for synchronized access to the ring. The ring itself is treated as a single shared communication medium. Both pass from transmitter passed by other computers and are copied by destination.

Hardware must be designed to pass token ever if attached computer powered down. This is shown in figure below.

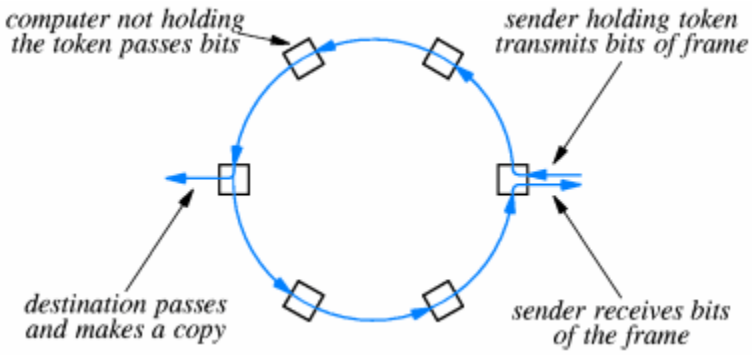


FIGURE 8.2

USING THE TOKEN:

When a computer waits to transmit it waits a token. After transmission computer transmits token on ring. Next computer is then ready to transmit, receive and then transmits.

TOKEN AND SYNCHRONIZATION:

Because there is only one token, only one computer will transmit at a time.
Token is a short reserved frame that can not appear in data.

Hardware must regenerate token if lost. Token gives computer permission to send one frame. If all computers are ready to transmit it enforces Round-Robin access. But if now computer is ready to transmit, token circulates around ring.

IBM TOKEN RING:

It is very widely used. It was originally 4Mbps and now it is upto 16Mbps. It uses special connection cable between the computer and the Ring interface.

FDDI: Fiber distributed data interconnect (FDDI) is another ring technology. Its most important features are:
It uses fiber optics between stations and transmits data at 100Mbps.
It uses pair of fibers to form two concentric rings.

FDDI AND RELIABILITY:

FDDI uses counter rotating rings in which data flows in opposite directions.

In case of fiber a station failure, remaining stations loop back and reroute data through spare ring. In this way all stations automatically configure loop back by monitoring data ring. It is shown in figure below

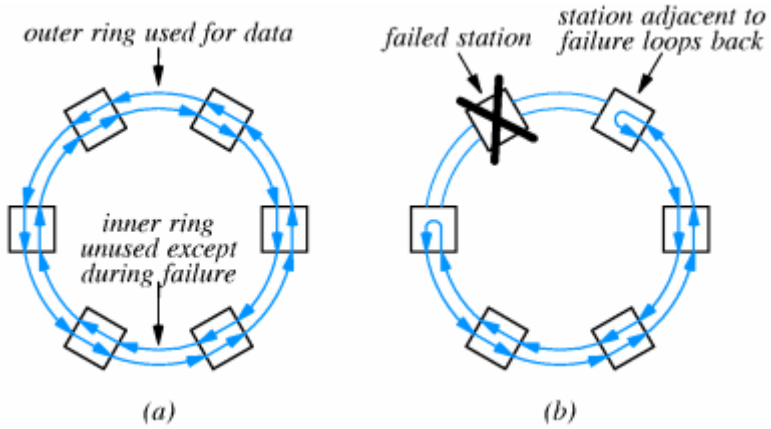


FIGURE 8.3 FDDI AND RELIABILITY:

ATM ----STAR NETWORK:

The ATM (Asynchronous Transferred Mode) technology consists of electronic packet switches to which the computers can connect.
ATM switches form a hub into which computers can connect in a star topology.
Computer gets point-to-point connections. Data from transmitters is routed directly through hub switches to destination. An ATM star network is shown in the figure below:

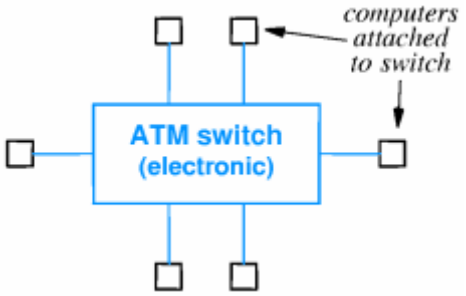


FIGURE 8.4 ATM SWITCH

ATM DETAILS:

- It transmits data at over 100Mbps.
- It uses fiber optics to connect computer to switch.
- Each connection includes two fibers.
- It is also shown in figure.

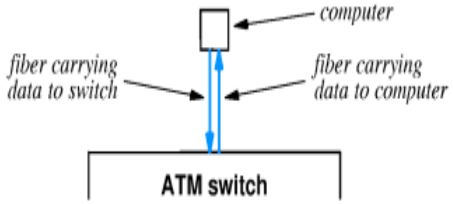


FIGURE 8.5

Lecture No. 9

HARDWARE ADDRESSING

We need to devise technique for delivering message through LAN medium to single, specific destination computer. Sending computer uses a hardware address to identify the intended destination of a frame. The sending computer also identifies type of data carried in the frame.

SPECIFYING A DESTINATION:

The data sent across a shared network reaches all attached stations - for all LAN topologies. Interface hardware detects delivery of frame and extracts frame from medium. But most applications want data to be delivered to one specific application on another computer but not all computers.

HARDWARE ADDRESSING:

Most network technologies have a hardware-addressing scheme that identifies stations on the network. Each station is assigned a numeric hardware address or physical address. . Sender also includes hardware address in each transmitted frame. In this way only station identified in frame receives copy of frame. Most LAN technologies include sender's hardware address in frame too.

LAN HARDWARE AND PACKET FILTERING:

The figure below illustrates the LAN hardware:

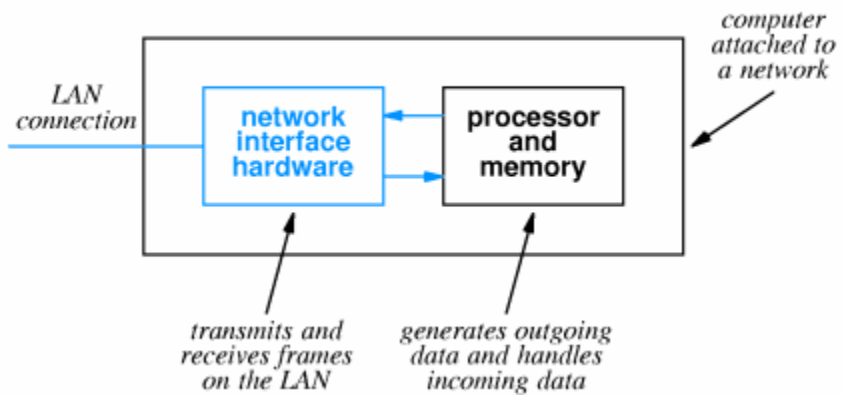


Figure 9.1

LAN INTERFACE:

LAN interface handles all details of frame transmission and reception which are given as follows:

- It adds hardware addresses, error detection codes, etc. to outgoing frames.
- It may use DMA to copy frame data directly from main memory.
- It obeys access rules (e.g., CSMA/CD) when transmitting.
- It checks error detection codes on incoming frames.
- It may use DMA to copy data directly into main memory.
- It checks destination address on incoming frames.
- The frames not addressed to the local computer are ignored and don't affect the local computer in any way.

FORMAT OF HARDWARE ADDRESS:

It consists of a numeric value and its size is selected for specific network technology. The length of the format is one to six bytes.

ASSINGING HARDWARE ADDRESS:

The hardware address must be unique on a LAN. How can those addresses be assigned and who is responsible for uniqueness? The answer to these questions depends on the particular LAN technology being used. There are three categories of address forms:

- Static
- Configurable
- Dynamic

STATIC:

In this category the hardware manufacturer assigns permanent physical address to each network interface and manufacturer must ensure that every interface has a unique address.

CONFIGURABLE:

In this category, the address can be set by the end user either manually e.g. switches or jumpers on the interface or electronically (e.g. through software).
The system administrators must coordinate to avoid the conflict.

DYNAMIC:

In this category the interface automatically assigns physical address each time it is powered up. This automatic scheme must be reliable to prevent conflicts.

BROADCASTING:

Some applications want to broadcast messages to all stations on the LAN. For this purpose shared communication channel can make broadcast efficient in such a way that message is delivered to all stations. A special broadcast address is used to identify broadcast message, which are captured by all stations.

Lecture No. 10

FRAME TYPE IDENTIFICATION

There are some problems with the broadcast. For every broadcast frame on the network each computer uses computational resources and places the contents into memory, which interrupt the CPU. It allows system software to make the decision whether to discard or use the frames.

Another problem is that if a pair of computer use broadcasting instead of sending them directly all other computers waste CPU time while discarding the frames.

MULTICASTING:

The solution to above problem is multicasting. It is the restricted form of broadcasting. It works like broadcasting however it does not forward frames automatically to the CPU.

The interface hardware is programmed in advance to accept certain frames that have multicast address as the destination address.

If an application program wishes to receive certain frames then it program the interface hardware to accept an additional set of addresses.

The interface hardware frame then begins accepting three types of frames:

- Multicast frames
- Broadcast frames
- The frames that are distend to the station itself.

MULTICAST ADDRESSING:

We take an example of computers running an audio application. We see that they can receive audio frames if the interface are programmed to received them and the other computers that are not running that audio application will not waste resources

.

IDENTIFYING PACKET CONTENTS:

The destination must get some clue about how to interpret frame data. For this purpose it can use two types which are given as follows.

EXPLICIT FRAME TYPE:

In this type the identifying value is included with frame describes types of included data.

Long Q

IMPLICIT FRAME TYPE:

In implicit frame the receiver must infer from frame data.

HEADERS AND FRAME FORMAT:

LAN technology standards define frame format for each technology. All contemporary standards use the following general format.

a) Frame header b) payload

Frame header has address and other identifying information.
Information typically in fields has fixed size and location. The data area may vary in size.

The Ethernet frame format is shown in the figure.

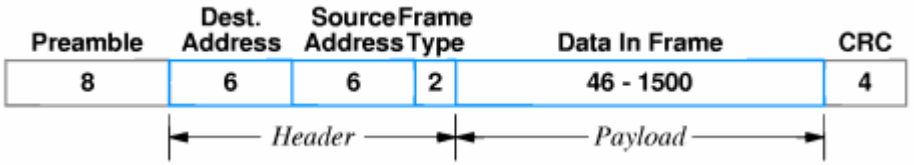


Figure 10.1 the Ethernet frame format

The different friends of ether frame format and their purposes is explained below:

FIELD	PURPOSE
Preamble	Receiver synchronization
Destination Address	Identifies intended receiver
Source Address	Hardware address of sender
Frame Type	Type of data carried in frame
Data	Frame payload
CRC	32-bit CRC code

ETHERNET FIELDS:

In Ethernet fields the preamble and CRC is often not shown in frame. The destination address of all is the broadcast address. There is special value reserved for frame type field.

FRAME WITHOUT TYPE FIELDS:

Some LAN technologies do not include a type field.
Sender and receiver can agree on interpretation, which is as follows:
They agree on single data format and use only that format this limits to one type of data. In this way all computers on LAN must use one format. Also they agree to encode the data format into first few bytes of the data field.

ENCODING THE DATA TYPE:

The figure illustrates a frame in which the data type is specified by using the data area.

Figure 10.2. Encoding the data type

To ensure interoperability format of encoding area must be universally agreed upon it typically set by standards only.

IEEE 802.2 LLC:

IEEE 802.2 standard includes logical link control (LLC) sub network attachment point (SNAP) header. SNAP/LLC format is widely used for example by Ethernet.
This is shown in figure below:

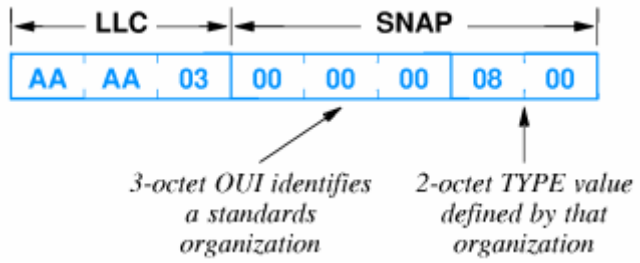


Figure 10.3. SNAP/LLC format

In the figure LLC portion indicates SNAP field to follow OUI (organizationally unique identifier) identifies Ethernet specification organization.

Also the type field is interpreted as in Ethernet (in this case, IP) as shown in figure above.

UNKNOWN TYPES:

For either encoding format some computer may not be prepared to accept frames of some types, which are unknown e.g. protocol type is not installed and the newly defined type.
The receiving computer examines the field and discards any frame with unknown type.

NETWORK ANALYZERS:

A network analyzer also called network monitor or a network sniffer is used to examine the performance of or debug a network.

It can report statistics such as capacity utilization, distribution of frame size, collision rate or token circulation time.

OPERATION OF NETWORK ANALYZERS:

The basic idea behind the operation of network analyzer is a computer with a network interface that receives all frames, which is called promiscuous mode.
Many desktop computers have interface that can be configured for promiscuous mode.
When combined with software computer can examine any frame on LAN. In this way the communication across LAN is guaranteed to be private. This computer receives and displays (but does not respond to) frames on the LAN.

Network analyzer can be configured to filter and process frames. It can count frames of specific type of size.
It displays only frames from or to specific computers. In general it can be configured to match any value of any field and capture only these frames meeting the filter specifications.
`

Lecture No. 11

INTERFACE HARDWARE

LAN data transmission speeds are typically fast relative to CPU speeds. LANs speeds are defined independent of any specific processor speeds, which allows for mix of any attached systems. In this way new computers can be attached without affecting LAN speeds.

NETWORK INTERFACE HARDWARE:

CPU can't process data at network speeds. So in order to connect to the network computer systems use special purpose hardware for network connections which consists of typically a separate card in the back plane which is called Network Adapter Card or Network Interface Card (NIC).

The connector on NIC at the back of computer then accepts cable to physical network. The CPU structure is shown in the figure.

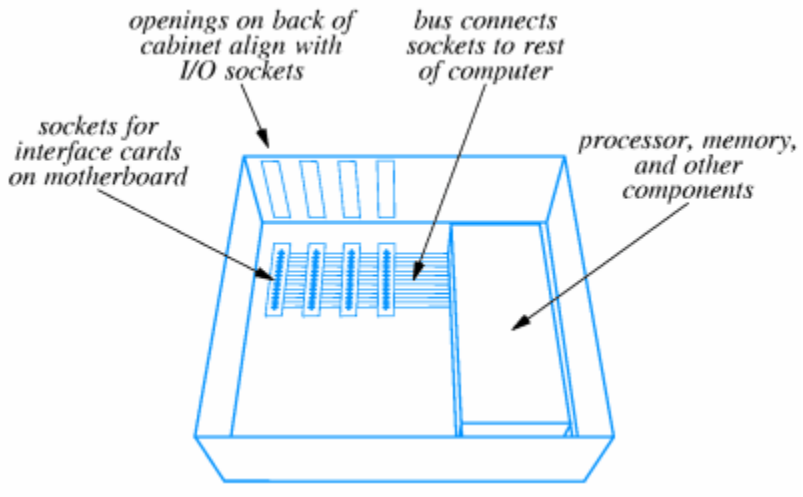


Figure 11.1

The Network Connector is also shown in the figure below.

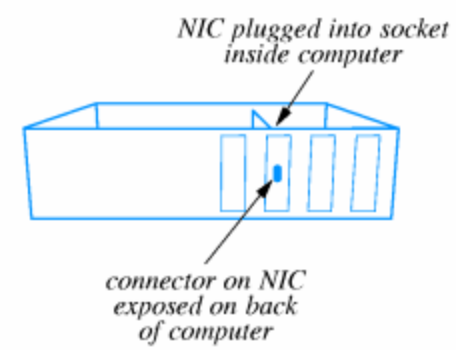


Figure 11.2

NICs AND NETWORK HARDWARE:

NIC is built for one kind of physical network. For example Ethernet interface can not be used with token ring and similarly ATM interface cannot be used with FDDI.

Some NICs can be used with different but similar hardware for example thick, thin and 10 Base-T Ethernet, 10Mbps and 100Mbps Ethernet.

Long Q

NIC AND CPU PRCESSING:

NIC contains sufficient hardware to process data independent of system CPU. In which some NICs contain separate microprocessor. In addition to this it also include analog circuitry interface to system bus, buffering and processing.

NIC looks like any other I/O device to system CPU. The system CPU forms message request and sends instructions to NIC to transmit data. NIC also receives interrupt on incoming data.

CONNECTION BETWEEN NIC AND PHYSICAL NETWORK:

TWO ALTERNATIVES:

NIC contains all circuitry and connects directly to network medium. A cable from NIC connects to additional circuitry that then attaches to the network medium.

THIN ETHERNET VERSUS 10BASE-T:

Thin Ethernet and 10Base-T are both Ethernet. The network technology is not limited to one style of connection.

THICK ETHERNET WIRING:

It uses thick coax cable. AUI cable (or transceiver or drop cable) connects from NIC to transceiver. AUI cable carries digital signal from NIC to transceiver. The transceiver generates analog signal on coax cable. The wires in AUI carry digital signals power and other control signals. Thick Ethernet also requires terminators to avoid signal reflectance. This is shown in the figure below:

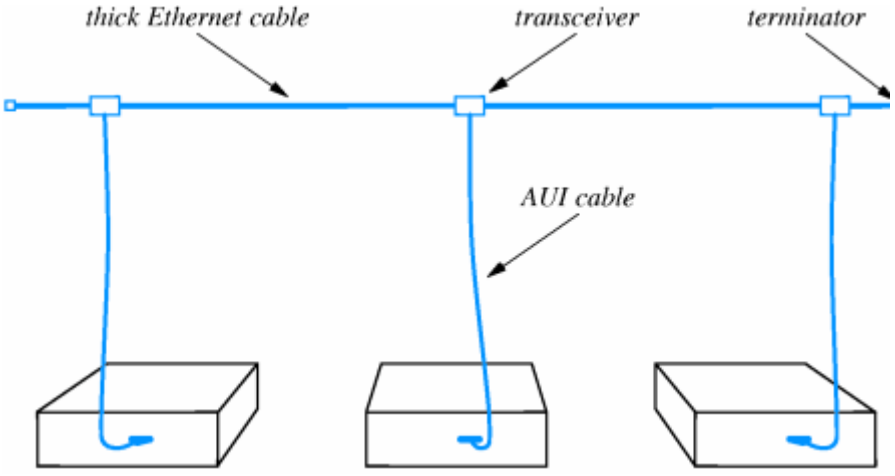


Figure 11.3

CONNECTION MULTIPLEXING:

In some circumstances transceiver may be in convenient e.g. workstations in a LAN. Connection multiplexer connects multiple computers to a single transceiver. Each computer's AUI cable connects to connection multiplexer. One AUI from multiplexer to Ethernet coax. Connection multiplexing is shown in the figure below.

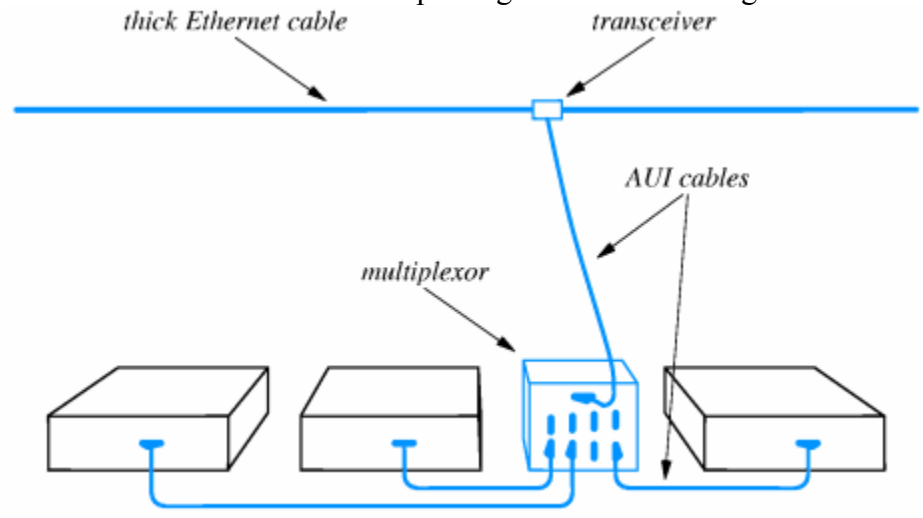


Figure 11.4

THIN ETHERNET WIRING:

Thin Ethernet uses thin coax cable that is cheaper and easier to install than thick Ethernet coax. In this case transceiver electronics are built into NIC and NIC connects directly to network medium.

Coax cable use BNC connector on NIC. Coax runs directly to back of each connected computer by T-connector. The T-connector directly attaches to NIC. This is shown in the figure below.

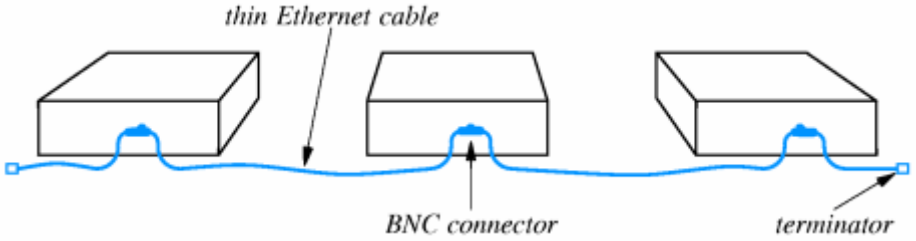


Figure 11.5

Thin Ethernet is useful when many computers are located close to each other. It may be unreliable because any disconnection disrupts entire net.

Lecture No. 12

LAN WIRING AND PHYSICAL TOPOLOGY

10BASE-T:

This is another standard of wiring scheme. It is commonly called 10Base-T, Twisted Pair or TP Ethernet. It replaces AUI cable with twisted pair cable and thick coax with hub.

This makes it cheaper and that 's why it is most useful technology of today. It is shown in the figure below:

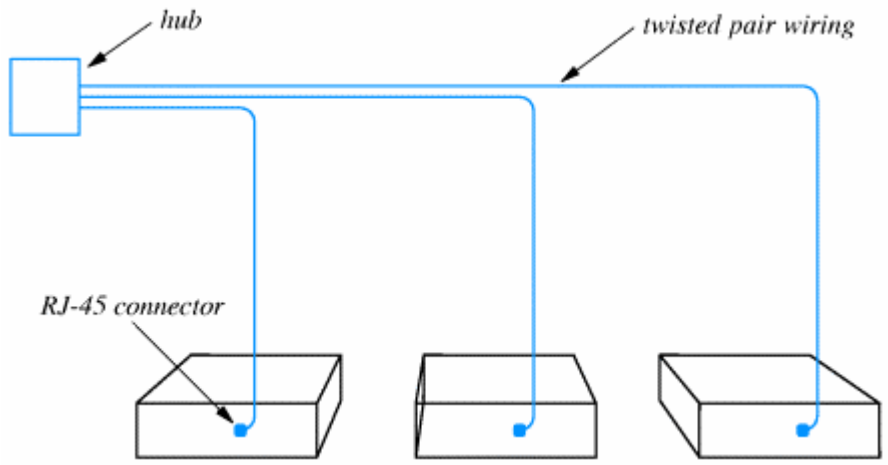


Figure12.1

HUBS:

They are used for extension of connection with multiplexing concept. They are sometimes called Ethernet-in-a-box. It is effectively a very short Ethernet with very long AUI cables. It can be connected into larger Ethernet.

PROTOCOL SOFTWARE AND ETHERNET WIRING:

All wiring technologies use identical Ethernet specifications. e.g. they use same frame format. They use same CSMA/CD algorithms. They can mix different technologies in an Ethernet.

NICs can provide all three-connection technologies. The protocol software can't differentiate among wiring technologies. The NIC is shown in the figure below with three connectors.

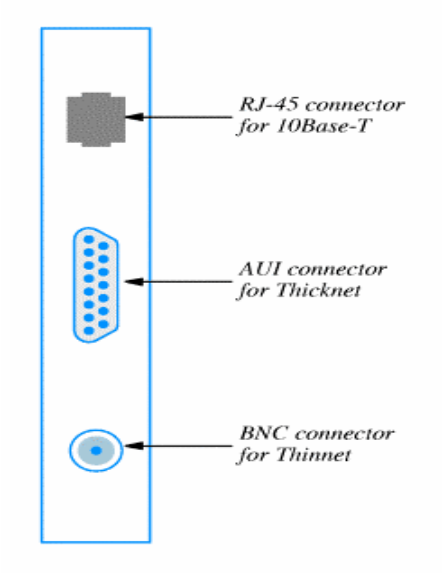


Figure 12.2

COMPARISON OF WIRING SCHEME:

The wiring schemes are compared as follows:

Separate transceiver allows computers to be powered off or disconnected from network without disrupting other communication.

Transceiver may be located in an inconvenient place, so finely malfunction transceiver can be hard.

In other case, thin coax cable takes minimum of cable. Disconnecting one computer (on one loose connection) can disrupt entire network.

Hub wiring centralizes electronics and connections. It makes management easier. Bottom line 10Base-T is most popular because of lowest cost.

TOPOLOGIES AND NETWORK TECHNOLOGIES:

10Base-T network topology is a bus but wiring topology is a star. The token ring network topology is a ring but wiring topology is a star.

We should remember to distinguish between logical and physical topologies. A topology is logically a star or it is physically a star.

FILTERING INCOMING FRAMES:

An analyzer can be configured to filter and process frames. It can count frames of a specific type or size. It can also display only frames from or to specific computers.

In general, it can be configured to match value of any field and capture only those frames making the filter specification.

ADVANTAGE AND DISADVANTAGE OF WIRING SCHEMES:

Each of three wiring schemes has advantages and disadvantages, which are explained as follows:

RELIABILITY ISSUES:

Wiring that uses a transceiver for each connection does not affect the entire network if a transceiver cable is disconnected. A cable cut occurring in hub wiring only affects one computer.

COST ISSUES:

Twisted pair Ethernet is the cheapest wiring that makes it so popular. Thicknet is the most costly wiring, which is no longer used.

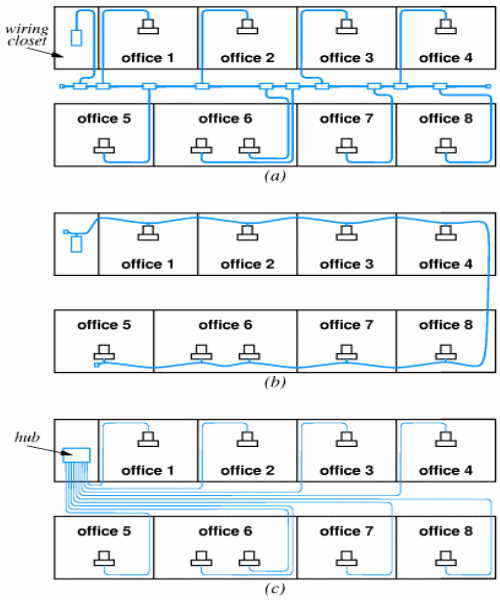


Figure 12.3

As shown in the figure eight offices are wired with

a) Thick Ethernet b) Thin Ethernet c) Twisted pair Ethernet

We can see that the length of wired varies in three schemes so cost varies in three schemes.

THE TOPOLOGY PARADOX:

The main feature of twisted pair Ethernet is that it forms a classic star topology however functions like a bus. 10Base-T Ethernet is often called a star shaped bus.

Two different types OF TOPOLOGIES:

LOGICAL TOPOLOGY:

It is defined by the specific network technology.

PHYSICL TOPOLOGY:

It depends on the wiring scheme.

NETWORK INTERFACE CARD AND WIRING SCHEMES:

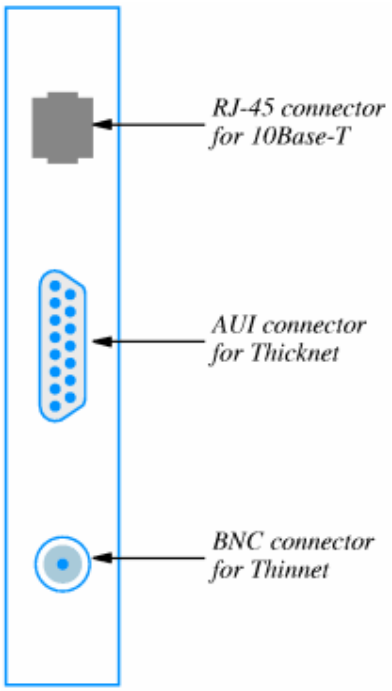


Figure 12.4

To allow changing the wiring without changing the interface hardware, NICs support multiple wiring schemes. it is shown in the figure below.

10/100 NETWORK INTERFACES AND AUTONEGATIATION:

10Base-T version of twisted pair Ethernet operated at 10Mbps. 10Base-T Twisted pair Ethernet operates at 100Mbps.

Long Q

100Base-T technology is backward compatible and allows the participants to negotiate a speed when connection is established. This process is known as auto negotiation.

CATEGORIES OF WIRES:

Cable used for wiring should match the following:

- The intended data rate
- The distance between devices
- The amount of em-noise
- Anticipated future needs
- Cost

Some categories and their typical uses are shown in the figure below.

Category	Bandwidth	Typical Uses
3	16 MHz	older, low-speed networks; analog telephones
4	20 MHz	short distance 10Base-T
5	100 MHz	10Base-T Ethernet; some 100Base-T
5E	100 MHz	100Base-T (Fast Ethernet); some 1000Base-T
6	250 MHz	1000Base-T Gigabit Ethernet) or ATM
7	600 MHz	future (possibly 10 Gigabit Ethernet)

Figure 12.5

WIRING SCHEMES AND OTHER NETWORK TECHNOLOGIES:

Multiple wiring schemes are not limited to Ethernet technology. Almost all-together network technologies use different wiring schemes. e.g., local talk uses hubs (physical star) to simulate a bus topology.

IBM's token ring also uses hubs (physically a star topology) to simulate a logical ring network.

Lecture No. 13

FIBER MODEMS AND REPEATOERS

LAN technologies are designed to operate within the same building. However most companies or institutions have offices located far apart from each other.

DISTANCE LIMITATION AND LAN DESIGN:

The maximum cable length of a LAN is fixed because the electrical signal level gets weaker as it travels. The delays must be short to allow access mechanisms (CSMA/CD, token passing) work properly.

However in most cases a LAN needs to be extended layer distances than the maximum Cable length limit.

For example: extending a company LAN to another building.

LAN EXTENSIONS:

Several techniques extend diameter of LAN medium. In this purpose most techniques use additional hardware. LAN signals relayed between LAN segments.

Resulting mixed technology stays within original engineering constraints while spanning greater distance.

FIBER OPTIC EXTENSION:

The LAN extension using fiber optic is shown in the figure below:

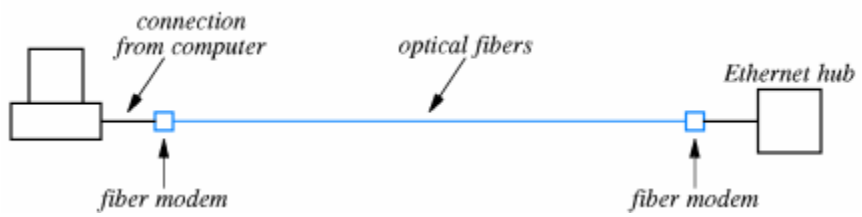


Figure 13.1

The fiber-modem coverts digital data into pulses of light then transmits over the optical fiber. It also receives light and converts into digital data.

This mechanism will successfully extend the optical fiber across several kilometers because delays on optical fiber are very low and bandwidth is very high.

REPEATERS:

Repeaters are used when copper wire communication is carries out. According to the fact that electrical signal gets weaker while traveling over copper wires. A repeater is used to increase the signal strength. It amplifies the weakening signal received from one segment and then retransmits onto another segment.
It is shown in the figure below:

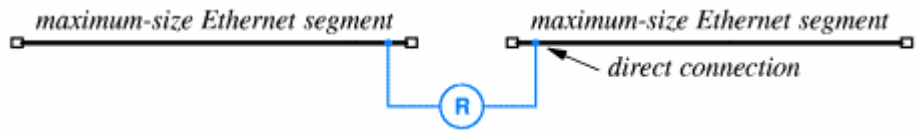


Figure13.2

Long Q

One repeater doubles, two repeaters triple the maximum cable length limitation.

Computers attached to different segments communicate as if they are connected to the same cable.

It is to be noted that we cannot increase the maximum cable length as many times as we wish by just adding repeaters. The reason for this is that every repeater introduces a delay and the access mechanism such as CSMA/CD does not work with long delays.

Ethernet standard specifies that any two stations cannot be separated by more than four repeaters.

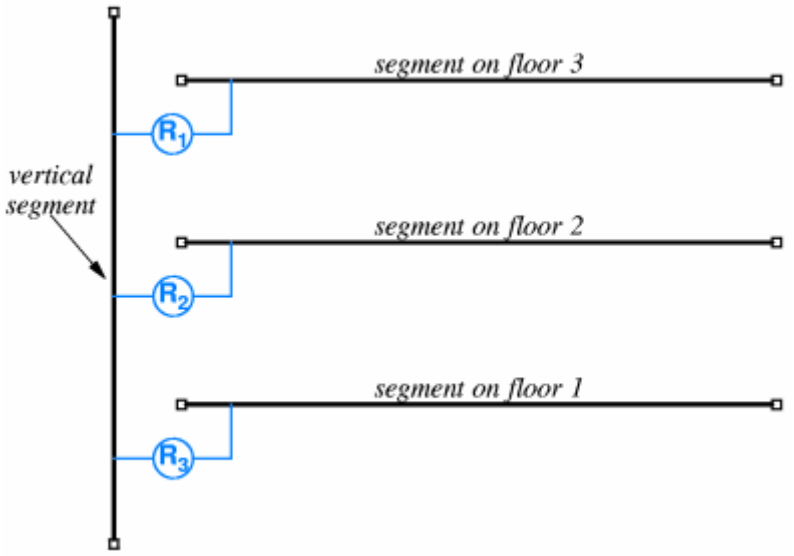


Figure13.3

The figure shows repeaters using the vertical segment. We see that only two repeaters separate any two stations in this scheme.

DISADVANTAGES OF REPEATERS:

Repeaters do not recognize frame formats, they just amplify and retransmit the electrical signal. If a collision or error occurs in one segment, repeaters amplify and retransmit also the error onto the other segments.

BRIDGES:

A bridge is a hardware device also used to connect two LAN segments to extend a LAN. Unlike a repeater, a bridge uses two NICs to connect two segments. It listens to all traffic and recognizes frame format. It also forwards only correct complete frames and discards the collided and error frames.

A typical bridge has two NICs, a CPU a memory and a ROM. It only runs the code stored in its ROM.

FRAME FILTERING:

The most important task a bridge performs is frame filtering. If both the source and destination are on the same segment, it does not forward the frame to the other segment. A frame is forwarded to the other segment, if it id destined to that segment. Broadcast and multicast frames are also forwarded.

A bridge keeps a list for each segment that consists of physical addresses of the computer attached to that segment. In this way a bridge knows on which segment a destination computer is attached.

Most bridges are self learning bridges. As soon as a frame arrives to a bridge, it extracts a source address from its header and automatically adds it in the list for that segment. In this way a bridge builds up address lists. This is shown in the figure below:

Event	Segment 1 List	Segment 2 List
Bridge boots	–	–
U sends to V	U	–
V sends to U	U, V	–
Z broadcasts	U, V	Z
Y sends to V	U, V	Z, Y
Y sends to X	U, V	Z, Y
X sends to W	U, V	Z, Y, X
W sends to Z	U, V, W	Z, Y, X

Figure 13.4

Lecture No. 14

BRIDGES

STARTUP AND STEADY STATE:

When a bridge first boots the address lists are empty (start up state). The bridge forwards frames to the other segment if it can not find its destination address in its lists.

After some time when the bridge has received at least one frame from every computer, it has the lists built (steady state) it forwards frames as far it is necessary.

PLANNING A BRIDGE NETWORK:

In a steady state, a bridge allows simultaneous use of each segment. When designing a LAN, bridges can be installed to divide the LAN into segments to improve performance.

For example:

Frequently contacting computers can be attached to the same segment. The frame traffic on one segment does not affect the other segments.

BRDGING BETWEEN BUILDINGS:

If two buildings are located far from each other, a bridge, a pair of fiber modems and an optical fiber can be used to connect two LANs as shown in the figure below.

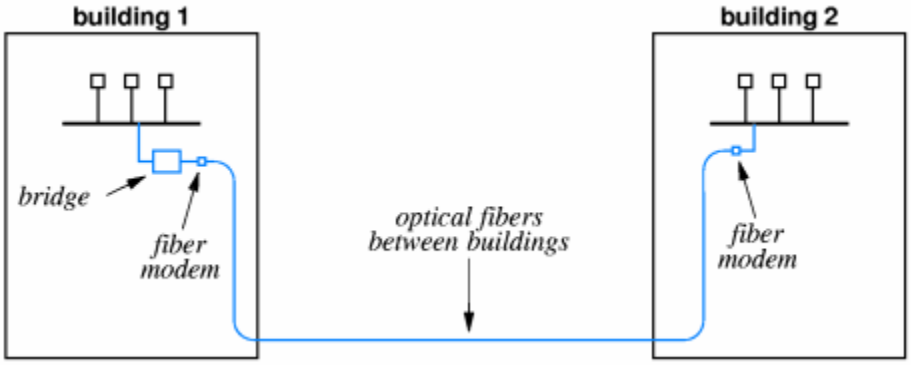


Figure14.1

BRIDGING BETWEEN BUILDINGS:

ADVANTAGES:

COST:

An optical fiber modem pair is sufficient to connect many computers located on separate buildings.

MAINTAINANCE:

There is no need to change the wiring between the buildings when installing and removing a computer.

PERFORMANCE:

The traffic on each building does not affect the other.

BUIDING ACROSS LONGER DISTANCES:

It is not always possible to connect two sites with optical fiber because the distance may be too long. It is usually not allowed to lay an optical fiber if the land does not belong to you.

There are two common methods to connect two distant sites.

LEASED SERIAL LINE CONNECTION:

Which is less distant.

LEASED SATELLITE CHANNEL:

It can span arbitrarily long distance. It is shown in the figure below.

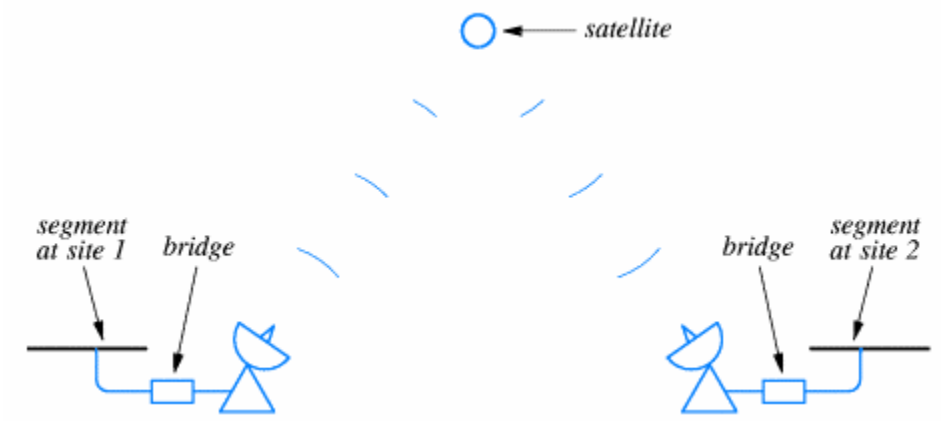


Figure14.2

Unlike optical fibers, satellite connections are low bandwidth to save cost. Because the frames arrived from local network are much faster than they can be sent across a satellite link.

The bridge must use buffering (saving a copy of frame into memory until it can be sent). It may run out of memory. The communication software usually waits for a response after sending a few frames.

A CYCLE OF BRIDGES:

A bridges network can connect many segments. One bridge is needed to connect each segment to the rest of the bridge network. This is shown in the figure below:

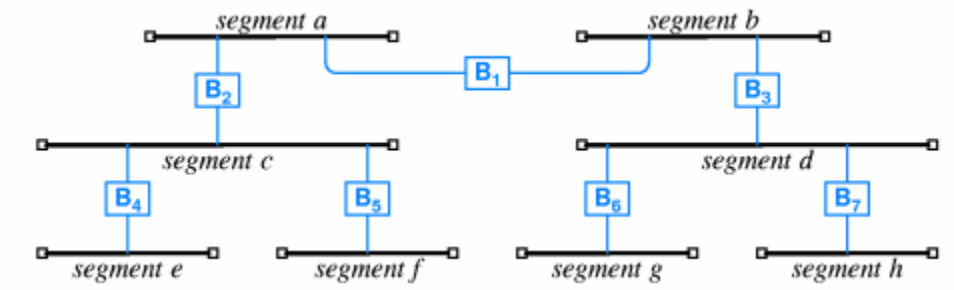


Figure14.3

If the bridges on the longer network form a cycle, then broadcasting frames introduce a problem i.e. the copies of broadcast frame continuously flows around the cycle (each computer receiving an infinite number of copies). This is shown below.

Figure14.4

DISTRIBUTED SPANNING TREE:

If a bridge network forms a cycle, then not all bridges on the network must be allowed to forward broadcast frames.

The bridges configure themselves automatically to decide which bridge will forward broadcast frames and which bridge will not.

The bridges communicate with each other on the network and use Distributed Spanning Tree (DST) algorithm to decide which bridge will not forward frames if a cycle occurs.

Lecture No. 15

SWITCHES AND WAN TECHNOLOGIES

SWITCHING:

A switched LAN consists of a single electronic device that transfers frames among the connected computers. A hub with multiple ports simulates a single shared medium. However a switch simulates a bridged LAN with one computer per segment.
A switch is shown in the figure below.

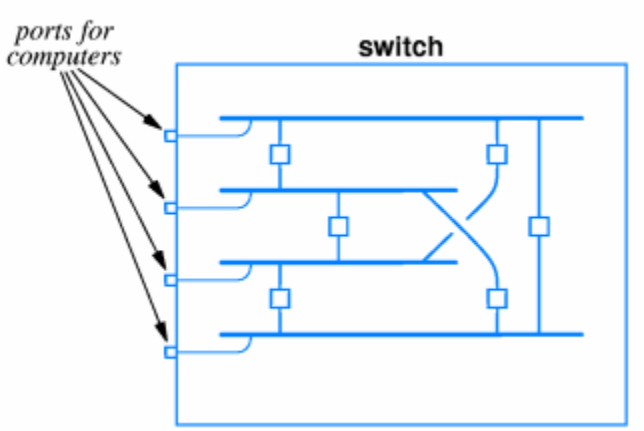


Figure 15.1

If a hub is used to connect among computers on a LAN, then only two computers can communicate at a given time. However if a switch is used, the communication between two computers will not affect the other pair of computers. They can communicate at the same time.

COMBINING SWITCHES AND HUBS:

To reduce costs, computers can be connected and distributed to a number of hubs, and then the hubs can be connected to a switch. Hubs simulate single shared LAN segments and a switch simulates a bridged LAN connecting segments.

BRIDGING AND SWITCHING WITH OTHER TECHNOLOGIES:

Hubs, Bridges and Switches are not limited to Ethernet logical bus topology. They are available also for other networking technologies such as token ring, FDDI etc. like FDDI hub and Token ring hub.

WAN TECHNOLOGIES AND ROUTING;

INTRODUCTION:

LANs can be extended using techniques in previous chapter. They can not be extended arbitrarily for or to handle many computers. Because there are distance limitations even with extensions so we need other technologies for larger networks.

CHARACTERIZATION OF NETWORKS:

There are three types of characterization of networks.

LOCAL AREA NETWORK (LAN):
It is used for a single building.

METROPOLOTAN AREA NETWORK (MAN):
It is used for a single city.

WIDE AREA NETWORK (WAN):
It is used for a country level networking and even for continents.

DIFFERENCE BETWEEN LAN AND WAN:

Although LAN is for a local area but satellite bridge can extend LAN across large distances. But it still can't accommodate arbitrarily many computers.

On the other hand WAN must be scalable to long distances and many computers.

PACKET SWITCHES:

To span long distances or many computers, networks must replace shared medium with packet switches. Each switch moves an entire packet from one connection to another. That's why they are called packet switches. A packet switch consists of a small computer with network interfaces, a memory and a program dedicated to packet switching function.

A packet switch is shown in the figure below.

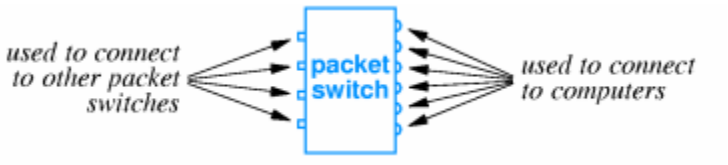


Figure 15.2

CONNECTION TO PACKET SWITCHES:

A packet switch many connect to computers and to other packet switches. But the speeds are different in both cases. There are typically high-speed connections to other packet switches but lower speed connections to the computers. The technology details depend upon desired speed.

PACKET SWITCHES AS A BUILDING BLOCKS:

Packet switches can be linked together to form WAN. WAN need not be symmetric or have regular connections. Each switch may connect to one or more other switches and one or more other computers as shown in the figure below.

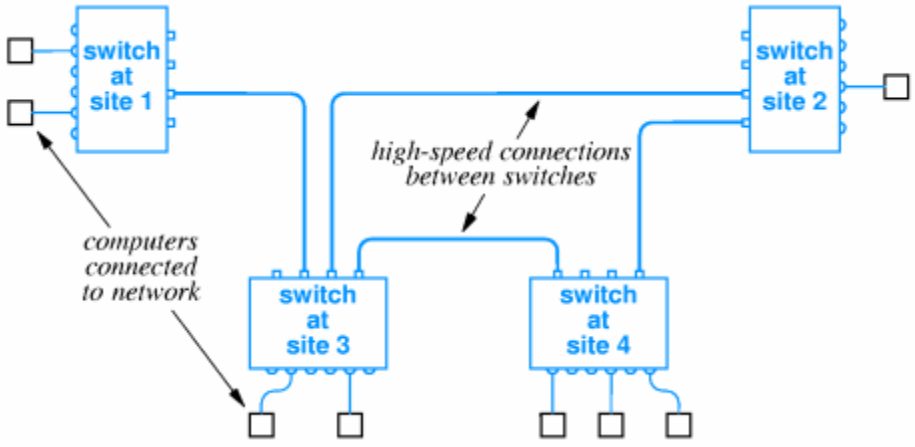


Figure 15.2

STORE AND FORWARD:

Data delivery from one computer to another is accomplished through store and forward technology. In this technology packet switch stores incoming packet and also forwards that packet to another switch or computer. For this purpose packet switch has internal memory into which it can hold packet if outgoing connection is busy. Packets for each connection held on queue.

PHYSICAL ADDRESSING IN A WAN:

The physical addressing in a WAN is similar as in LAN in the following way:

- The data is transmitted in packets equivalent to frames.
- Each packet has a format with header.
- The packet header includes destination and source addresses.
- Many WANs use hierarchical addressing for efficiency. One part of address identifies destination switch. Other part of address identifies port on switch. This is shown in the figure below.

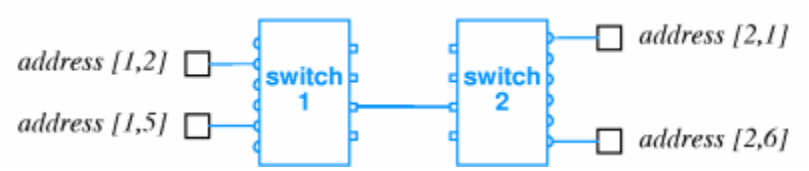


Figure 15.4

NEXT HOP FORWARDING:

Packet switch must choose outgoing connection for forwarding the packet. There are two cases.

- If the destination is local computer, packet switch delivers computer port.
- If the destination is attached another switch, this packet switch forwards to next hop through connection to another switch.
- The choice of another switch is based on destination address in packet.

Lecture No. 16

ROUTING

SOURCE INDEPENDENCE:

Next hop to destination does not depend on source of packet. This phenomenon is called 'Source Independence'. It has several benefits. It allows fast and efficient routing. Packet switch need not hove complete information about all destinations in spite it just has next hop so reduces total information and increases dynamic robustness. The network can continue to function even if topology changes without notifying entire network.

HIERARCHICAL ADDRESSING AND ROUTING:

The process of forwarding the packets of information is called routing. The information about destinations is kept in routing tables. Note that many entries have same next hop. It is shown in the figure.

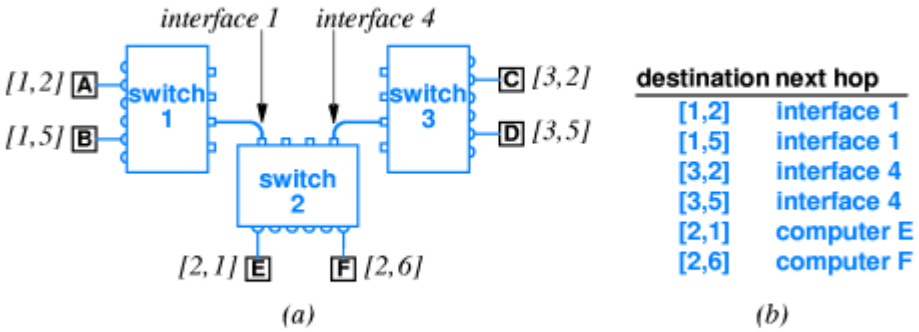


Figure 16.1

In particular all destinations on same switch have same next hop. These routing tables can be collapsed. A specific routing table is shown in the figure.

Destination	Next Hop
(1, anything)	interface 1
(3, anything)	interface 4
(2, anything)	local computer

Figure 16.2

ROUTING IN A WAN:

As there will be more computers there will be more traffic of information. We can add capacity to WAN by adding more links and packet switches. Packet switches need not have computers attached. There are two types of switch according to the attached computers.

INTERIOR SWICH:

The switch that has no attached computers is called an interior switch.

EXTERIOR SWITCH:

The switch that has computers attached with it is called exterior switch.
Both interior and exterior switches forward packets and they also need routing tables. The routing table must have two things.

UNIVERSAL ROUTING:

It should have next hop for each possible destination.

OPTIMAL ROUTES:

The next hop in table must be on shortest path to destination.

MODELING A WAN:

To model a WAN, we use a graph in which the nodes model switches and the edges model direct connection between switches. The modeling captures essence of network and it ignores attached computers as shown in the figure below. Modeling of a specific WAN is shown.

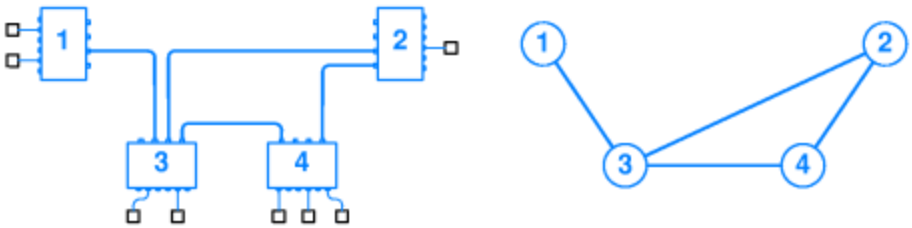


Figure 16.3

ROUTE COMPUTATION WITH A GRAPH:

We can represent routing table with edges as shown in the figure below:

destin-ation	next hop
1	-
2	(1,3)
3	(1,3)
4	(1,3)

node 1

destin-ation	next hop
1	(2,3)
2	-
3	(2,3)
4	(2,4)

node 2

destin-ation	next hop
1	(3,1)
2	(3,2)
3	-
4	(3,4)

node 3

destin-ation	next hop
1	(4,3)
2	(4,2)
3	(4,3)
4	-

node 4

Figure 16.4

The graph algorithms can be applied to find routes.

REDUNDANT ROUTING INFORMATION:

Notice duplication of information in routing table for node 1 as shown above in the figure. We see that switch has only outgoing connection, all traffic must traverse that connection.

DEFAULT ROUTES:

Routing table entries can be collapsed with a default route. If the destination does not have in explicit routing table entry, then it use a default route. Default routes for 4 nodes are shown in the figure below.

Figure 16.5

Lecture No. 17

ROUTING ALGORITHMS

BUILDING ROUTING TABLES:

There are basically two methods for building routing tables, which are as follows:

- Manual entry
- Software

Further there are two methods for computing routing table information.

- Static routing
- Dynamic routing

STATIC ROUTING:

It is done at boot time. It is simple and has low network overhead. It is inflexible.

DYNAMIC ROUTING:

It allows automatic updates by a programmer. It can work around network failures automatically.

COMPUTING SHORTEST PATH IN A GRAPH:

While computing shortest path, first we assume graph representation of network at each node then we use Djikstra's algorithm to compute shortest path from each node to every other node. Then extract next hop information from resulting path information and insert next hop information into routing tables.

WEIGHTED GRAPH:

Djikstra's algorithm can accommodate weights on edges in graph. The shortest path is then the path with lowest total weight (sum of the weight with all edges). It should be noted that the shortest path is not necessarily with fewest edges (or hops). For example as shown in the figure below:

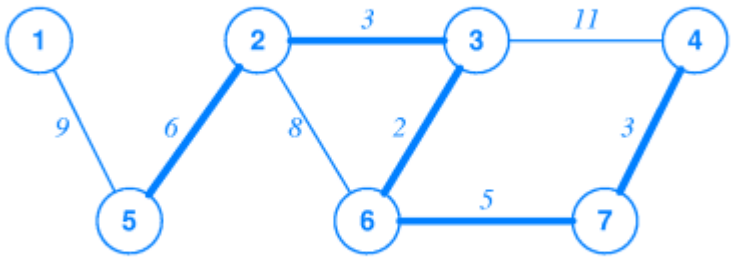


Figure 17.1

The shortest path in the figure from node 2 to node 6 is 2 to 3 and 3 to 6 as this path has the smallest weight so it is the shortest path.

DISTANCE MATRICS:

Weights on graph edges reflect cost of traversing edge. This cost may be in time, dollars or hop counting (weight == 1). The resulting shortest path may not have fewest hops.

DISTRIBUTED ROUTE COMPUTATION:

Each packet switch computes its routing table locally and sends messages to the neighbors. It also updates information periodically. If a link or a packet switch fails then the network adapts its failure. The packet switch then modifies the tables to avoid failed hardware.

Long Q

DISTANCE-VECTOR ROUTING:

Local information is next hop routing table and distance from each switch. The switches periodically broadcast topology information i.e. destination, distance.

Other switches update routing table based on received information.

VECTOR-DISTANCE ALGORITHM:

It is explained in more detail below:

Packet switches wait for next update message and they iterate through entries in message. If entry has shortest path to destination, insert source as next hop to destination and record distance as distance from next hop to destination plus distance from this switch to next hop.

LINK-STATE ROUTING:

In link-state routing network topology is separated from route computation. Switches send link-state information about local connections. Each switch builds own routing tables. It uses link-state information to update global topology and runs Djikstra's algorithm.

COMPARISON:

DISTANCE-VECTOR ROUTING:

- It is very simple to implement.
- Packet switch updates its own routing table first.
- It is used in RIP.

Long Q

Difference

LINK-STATE ALGORITHM:

- It is much more complex.
- Switches perform independent computations.
- It is used in OSPF.

EXAMPLE WAN TECHNOLOGIES:

Some multiple WAN technologies are discussed below.

ARPANET:

It began in 1960's. It was funded by Advanced Research Project Agency, which is an organization of US defense department. It was incubator for many of current ideas, algorithms and Internet technologies.

X.25:

It was early standard for connection-oriented networking. It began from IFU, which was originally CCITT. It predates computer connections, which are used for terminal/time sharing connection.

FRAME RELAY:

It is used for Telco service for delivering blocks of data. It is connection based service and must contract with Telco for circuit between two endpoints. It is typically 56kbps or 1.5Mbps and can run to 100Mbps.

SMDS:

Switched Multi megabit Data Service (SMDS) is also a Telco service. It is a connection less service. Any SMDS station can send information to any station on the same SMDS cloud. It is typically ranges from 1.5Mbps to 1000Mbps.

ATM (ASYNCHRONOUS TRANSFER MODE):

It was designed as a single technology for voice, video and data and has low jitter (variance in delivery time) and high capacity.

It uses fixed size, small cells, 48 octet's data and 5 octets header. It can also connect multiple ATM switches into a network.

Lecture No. 18

CONNECTION-ORIENTED NETWORKING AND ATM

Long Q

LANs and WANs can both connect multiple computers, but they have different base technologies and meet different goals. ATM is a single technology that is designed to meet the goals of both LANs and WANs.
ATM uses the concept of connection-oriented networking.

ASYNCHRONOUS TRANSFER MODE (ATM):

Telephone companies (Telco's) introduced ATM to meet several goals. It provides universal service for all subscribers and support for all users for voice, video and data. It has a single unified infrastructure (no separate LANs and WANs). It gives guaranteed service when it is appropriate and support for low cost devices.

Long Q

JITTER:

Jitter is the term used for variance in transmission delays.
Jitter is significance for voice, video and data. In LANs, jitter can occur when a packet is delayed because the network is busy.

PACKET SIZES:

Large packets result in fewer overheads because a smaller fraction of the packet is used for header information.
Optimum networks use 4kB packets or larger.

Large packets can't easily be used for voice for example 8-bit samples (at 125usec per sample) would require half a second to fill a 4kB packet. Echo cancellation can only be used with low transmission delays.

ATM CELLS:

To meet its goals, ATM uses small, fixed sized packets called cells. Each cell has 53 octets. VPI/VCI fields identify the cells destination.

PRIO tell if cell can be discarded CRC checks the header bits only. ATM header is about the 10% of the cell. Ethernet can have overhead of only 1%. Engineers sometimes call the ATM overhead the cell tax. An ATM is shown below.

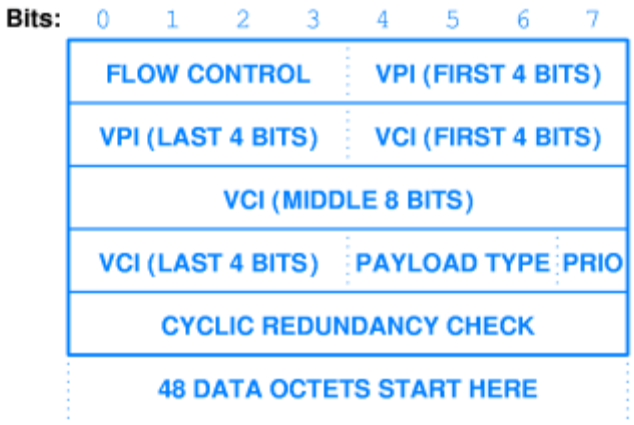


Figure.18.1

CONNECTION-ORIENTED SERVICE:

The connection-oriented service paradigm for networking is similar to the manner in which telephones are used. This is given as follows:

A caller dials a number of the destination. The telephone at the destination signals the arrival of a connection request. If the called person does not answer; the caller gives up after waiting for a timeout. If the called person does answer, then the connection is established.

In data communication, as binary connection identifier is given to each of the two parties to enable identification of the connection.

VIRTUAL CHANNEL (OR CIRCUITS):

Connections in ATM are called virtual channels (VC) or virtual circuits (a term preferred by some). These are called virtual, since connections are formed in ATM by starting values in memory locations (tables) in ATM switches as opposed to making actual electrical connections.

The VC is identified by a 24-bit value formed from the VPI or Virtual Path Indicator (8-bit), which identifies a particular path through the network and the VCI or Virtual Channel Indicator (16-bits), which identifies the channel in the virtual path being used by the connection.

Most frequently, the 24-bit pair is treated as just a single connection identifier by computers.

Lecture No. 19

ATM: VIRTUAL CIRCUITS

LABELS AND LABEL SWITCHING:

An ATM network is built from interconnected ATM switches. The attachment points or ports can be connected to computers or other ATM switches. As cells arrive at an ATM switch, their VPI/VCI is modified using a forwarding table that gives the new VPI/VCI for the next leg of the cell's trip.

The forwarding table is essentially indexed by the incoming cell's VPI/VCI and the contents yield the new VPI/VCI.

LABEL REWRITING:

The replacement of the incoming cell's VPI/VCI with a probably different VPI/VCI is called rewriting.

ATM is thus called a label rewriting or label switching system. Thus two computers with a connection through an ATM network will likely have different VPI/VCI values for each end of the connection as shown in the figure below.

Figure 19.1

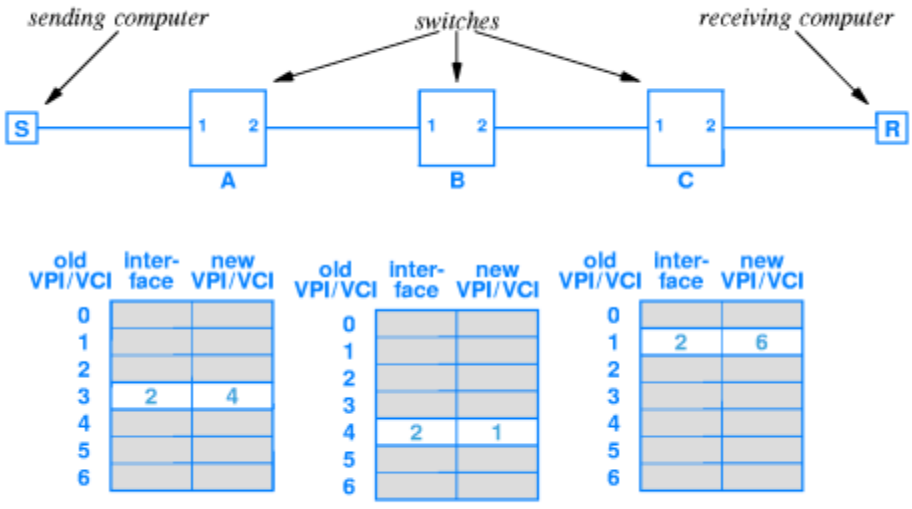


Figure 19.2

EXAMPLE:

As an example, in the figure we see that the sending computer S uses a VPI/VCI of 3 and sends a cell.

Switch A receives the cell and looks up 3, then rewrites the VPI/VCI as 4, and sends the cell out of its port 2.

Switch B receives the cell and looks up 4 then rewrites the VPI/VCI as 1 and sends the cell at its port 2.

Switch C receives the cell and looks up 1 then rewrites the VPI/VCI as 6 and sends the cell out of its port 2.

The receiving computer R receives the cell with a VPI/VCI of 6, which is the value it is using for the connection. Forwarding tables in each switch must be coordinated to define meaningful 'paths' through the network.

PERMANENT VIRTUAL CIRCUITS:

ATM can provide customers with virtual circuits that look like traditional leased digital circuits. Such permanent virtual circuits (PVC) last as long as the customer pay the periodic fee for its use. The forwarding tables are automatically restored after power of equipment failure. The forwarding table entries for such permanent VC's are statically configured, the terms used by Telco's for this is provisioning.

Provisioning requires two steps:

1. To determine a complete path (that is, identify the switches that will be used).
2. To choose appropriate VPI/VCI for each step in the path, and configure each adjacent pair of switches (easy, since each switch rewrites the VCI/VPI).

SWITCHED VIRTUAL CIRCUITS:

Most networks offer dynamic connections, which last for a relatively short time. To handle this, ATM can dynamically establish a switched virtual circuit (SVC), allow it last as long as necessary and then terminate it.

The terminology comes from the Telco's where switching system normally refers to all switching.

ESTABLISHING AN SVC:

Long Q

The computer sends a connection request to the switch to which it is attached. Software in the switch finds a network path to the destination and sends along the connection request.

Each pair of switches in the path communicates to choose a VPI/VCI for their tables. Once the connection is established by the destination, a message is sent back to the originating computer to indicate the SVC is ready.

If any switch or the destination computer does not agree to setting up the VC, an error message is sent back and the SVC is not established.

SIGNALING:

The term signaling is used to describe communication about the network, as opposed to communication that just uses the network.

A computer uses signaling with reserved VCI/VPI values to communicate with a switch to establish a connection or send other network control messages. These connection requests and network control messages are also sent in cells and since the VPI/VCI use in these cells are reserved there is no confusion between data and control cells.

QUALITY OF SERVICE:

Networks are more frequently being designed to allow specification of the quality of service required by users.

For example: - a typical voice telephone call might give a QoS parameter for throughput of 64kbps and delay less than 500msec. A user sending video might require throughput of 2Mbps.

PROVIDING DESIRED QoS:

QoS desires are specified at connection setup time and one never altered for the connection duration. Switches along the path must reserve resources to guarantee the QoS.

If a switch cannot provide the resources, it rejects the connection requests and an appropriate error message is returned.

ATM QoS SPECIFICATIONS:

There are three types of QoS specifications, which are given as follows:

CONSTANT BIT RATE (CBR):

It is used for audio and video, since these have predefined maximum data rates.

VARIABLE BIT RATE (VBR):

It is used for compressed audio and video where the data rate depends on the level of compression that can be achieved.

AVAILABLE BIT RATE (ABR):

It is used for typical data applications (where the data rate may be unknown and bursty) and allows use of whatever bandwidth is available at a given time.

Lecture No. 20

ATM AND NETWORK OWNERSHIP

CELLS VS PACKETS:

ATM designers chose cells over packets because of the following reasons:

- Cells are not variable length and memory management for them is simpler. Handling variable length packets leads to memory fragmentation.
- Variable length packets require hardware to accommodate the largest possible packet, and thus to detect the end of the packet. With cells bits can just be counted as they arrive.
- The length of time required to send a variable length packet is variable and requires complicated interrupt scheme to detect completion of transmission. QoS can't be guaranteed with variable length packets as easily as it can with fixed length cells.

ATM SPEED:

ATM designers also chose cells to meet the need for speed. Since it was designed to handle arbitrarily large numbers of users, each of which could be willing to pay for high throughput.

ATM is designed to work on fiber (but can be used with twisted pair). A typical port on an ATM switch operates at OC-3 speed (155Mbps) or higher.

ATM CRITIQUE:

ATM is far more expensive than typical LAN hardware. Connection setup time may be excessive for short communications. Cell tax consumes 10% of network capacity QoS requirements might be unknown, leading to applications picking values that are too high or too low.

Broadcast is inefficient and has to be simulated by sending the same message to each computer separately.

ATM as a single universal networking technology has only minimal provision for interoperation with other technologies.

NETWORK OWNERSHIP:

There are two categories in this case:

PRIVATE NETWOK:

Single organization or company owns this. They are often LAN technologies. There can be multiple LANs in a building or campus linked together. They are sometimes called Intranet.

PRIVATE NETWORK ARCHITECTURE:

It operates autonomously from other networks (e.g. internet).
It usually includes one or few closely managed external connections. They may restrict access at connections.

MANAGING PRIVATE NETWORKS:

An organization buys its own equipment and hires staff to design, implement, maintain and upgrade network. It is responsible for all network management.

EXTENDING PRIVATE NETWORK:

The large organizations may have multiple buildings or campuses. They can only install cables on their own property. They may contract for leased lines from common carrier.

PUBLIC NETWORK:

This is owned by common carrier e.g. Phone Company. The public networks are those networks, which are operated by common carriers. It may be a telephone company or another organization that builds network out of leases lines. Multiple organizations subscribe and connect. Data transits public network to other organizations.

ADVANTAGES AND DISADVANTAGES:

The advantages and disadvantages of Public and Private Networks are given in the table below:

NETWORKS	ADVANTAGES	DISADVANTAGES
PUBLIC	They are flexible.	There are no decision-making equipment or policies.
PRIVATE	The owner has complete control over both the technical decision and policies.	They are expensive to install and maintain.

Lecture No. 21

NETWORK SERVICE PARADIGM

VIRTUAL PRIVATE NETWORK:

Virtual Private Network (VPN) combines the features of both private and public networks. It is limited to single organization and uses public network for connectivity.

These connections are sometimes called tunnels and connect sites. Each site sees tunnel as point-to-point link. There is no access for other users of public networks.

GUARANTEEING ABSOLUTE PRIVACY:

In addition to restricting packets, VPN systems use encryption to guarantee absolute privacy. Even if an outside does manage to obtain a copy of the packet the outside will be unable to interpret the contents.

SERVICE PARADIGM:

At the lowest level most networks transfer individual packets of data and the network requires each packet to follow an exact format dictated by the hardware, which is called Interface paradigms or service paradigms.
There are two types of service paradigms:

CONNECTION-ORIENTED:

It is similar to the telephone system: endpoints establish and maintain a connection as long as they have data to exchange.

CONNECTIONLESS:

Similar to postal system: endpoints put data to send into a packet and hand to network for delivery.

CONNECTION-ORIENTED SERVICE:

One endpoint requests connection from network. Other endpoint agrees to connection. Computers exchange data through connection. One-endpoint requests network to break connection when transmission is complete.

CONTINUOUS AND BURST TRAFFIC:

Networks handling voice or video are engineered to accept and deliver continuous data at fixed rate. Others are designed to handle burst traffic typical of computer networks. Connection does not disappear when no data is sent.

Long Q

SIMPLEX & FULL DUPLEX CONNECTION:

Some connection-oriented technologies provide full duplex while other allow on simplex connection. To communicate using a simplex design a pair of computers must establish two connections one from computer A to computer B and another from computer B to A.

CONNECTION DURATION AND PERSISTANCE:

Connection can be made on demand set up permanently. There are two types:

- Switched Connection or Switched Virtual Circuit (SVC).
- Permanent Connection or Permanent Virtual Circuit (PVC).

Permanent connections are originally hardwired and now configured at system unit time. In switched connections, computer maintains permanent connection to network and networks make connections on demand. Internal components are switched networks is a switched data network.

SERVICE GUARANTEES:

Some connection-oriented networks provide guarantees about the service that computer will receive. They may guarantee a throughput rate maximum packet loss rate.

For example, ATM provides statistical guarantee about performance.

STREAM OR MESSAGE INTERFACE:

Some connection-oriented networks provide stream interfaces. In which no boundaries are recorded that receiver may receive a single block of 60 characters.

Others provide a message interface that delivers data in the same size chunks that the sender transmitted.

CONNECTIONLESS SERVICE:

In connectionless service, there is no connection necessary. The source of data adds destination information in data and delivers to the network. Network delivers each data item individually.

INTERIOR AND EXTERIOR SERVICE PARADIGM:

A network providing one service paradigm to the attached computers can use an entirely different service paradigm internally.

For example ARPANET is connection oriented internally and connectionless externally.

COMPARISON:

CONNECTION-ORIENTED:

- Accounting is easier.
- Application can learn of network problems immediately.

CONNECTIONLESS:

- It has fewer overheads.
- It is easier to implement network.

An example of service paradigm is shown in the figure below.

Technology	Connection-Oriented	Connectionless	used for LAN	used for WAN
Ethernet		•	•	
Token Ring		•	•	
FDDI		•	•	
Frame Relay	•			•
SMDS		•		•
ATM	•		•	•
LocalTalk		•	•	

Figure 21.1

ADDRESSES AND CONNECTION IDENTIFIERS:

Address is a complete unique identifier. Connectionless delivery requires address on each packet.

Connection-oriented delivery can use a short hand that identifies the connection rather than the destination.

As an example let's consider an ATM with 16-bit address, 24-bit connection identifier and connection identifier includes.

-8-bit Virtual Path Identifier (VPI)

-16-bit Virtual Circuit Identifier (VCI)

The connection identifier is local to each computer and it may be different at different parts of the ATM switch.

Lecture No. 22

NETWORK PERFORMANCE

There are two types of characteristics in case of network performance.

- Delay
- Throughput

DELAY:

It is an important quantitative property of networks. Delay is a measure how long it takes for a bit of data to travel across the network from one compute to the other.
It is measured in seconds or fractions of seconds.

TYPES OF DELAY:

There are following types of delay:

PROPAGATION DELAY:

It defined as the time to travel across medium.

SWITCHING DELAY:

It is the time required for network component (hub, bridge, packet switch) to forward data.

ACCESS DELAY:

It is the time required to get control of medium (CSMA/CD, token).

QUEUING DELAY:

It is the time enquired in packet switches.

THROUGHPUT:

Throughput is a measure of the rate at which data can be sent through the network. The throughput capability of the underlying hardware is called bandwidth.

Because each frame contains headers, the effective throughput is less than the hardware bandwidth.

Networking professional often use the term speed as a synonym for throughput.

RELATIONSHIP BETWEEN DELAY AND THROUGHPUT:

If a packet switch has a queue of packets waiting when a new packet arrives. The new packet will be placed on the entire queue and will need to wait while the switch forwards the previous packets.

Throughput and delay are not completely independent. As traffic in a computer network increase, delays increase a network that operates at close to 100% of its throughput capacity experiences severe delay.

DELAY THROUPUT PRODUCT:

It is computed as delay time multiplied by effective throughput. It measures amount of data that can be present in the network. In fast network with long delay times, sending computer can generate large amounts of data before destination receives first bit.

JITTER:

The amount of delay that a network introduces is called jitter. A network with zero jitter takes exactly the same amount of time to transfer each packet. A network with high jitter takes much longer to deliver some packets than others.

Lecture No. 23

INTERNETWORKING: CONCEPTS, ARCHITECTURE AND PROTOCOLS

THE MOTIVATION FOR INTERNETWORKING:

There is no single networking technology that is best for all needs. A large organization with diverse networking requirements needs multiple physical networks. If the organization chooses the type of network that is best for each task, the organization will need several types of networks.

The interconnection of two or more networks, usually local area networks so that data can pass between hosts on the different networks as though they were one network, this requires some kind of Router or Gateway, which led to the motivation for internetworking.

THE CONCEPT OF UNIVERSAL SERVICE:

The chief problems with multiple networks are as follows:

- A computer attached to a given network can only communicate with other computers attached to the same network.
- In the 1970s large organizations began to acquire multiple networks. Each network in the organization formed island. Employees needed to choose a computer appropriate for each task. So they needed multiple screens, keyboards and computers.

UNIVERSAL SERVICES:

A communication system that supplies universal services allows arbitrary pairs of computers to communicate.

Universal service is desirable because it increases individual productivity.

UNIVERSAL SERVICES IN A HETEROGENEOUS WORLD:

Although universal service is highly desirable incompatibilities among network hardware and physical addressing prevent an organization from building a bridged network that includes arbitrary technologies.

Extension techniques such as bridging cannot be used with heterogeneous network because of incompatible packet formats.

INTERNETWORKING:

Despite the incompatibilities among networks, researchers have devised a scheme that provides universal service among heterogeneous networks called 'internetworking'. It uses both hardware and software.

PHYSICAL NETWORK CONNECTION WITH ROUTERS:

A router is a special purpose system dedicated to the task of interconnecting networks. A router can interconnect networks that use different technologies including different media, physical addressing schemes or frame formats. A router connecting two physical networks is shown in the figure below.

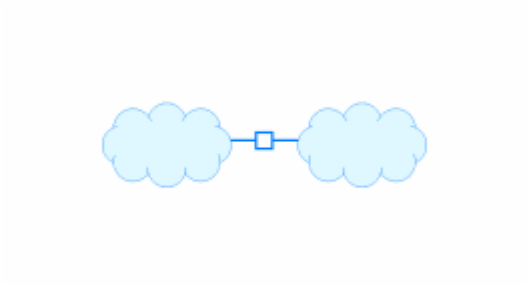


Figure 23.1

INTERNET ARCHITECTURE:

Organization seldom uses a single router to connect its entire network for two reasons.

- Because the router must forward each packet, the processor in a given router is insufficient to handle the traffic.
- Redundancy improved Internet reliability.

An Internet consists of a set of networks interconnected by routers.
The Internet scheme allows each organization to choose the number and type of network, the number of routers to use to interconnect them, and the exact interconnection topology. Three routers connecting four networks in series is shown in the figure below.

Figure 23.2

ACHIEVING UNIVERSAL SERVICES:

The goal of internetworking is universal service across heterogeneous networks. To provide this service all computers and routers must agree to forward information from a source on one network to a specified destination. The task is complicated as frame formats and addressing schemes may differ. The key of achieving universal service is universal protocol software (TCP/IP).

A virtual network is shown in the figure that TCP/IP software provides to users and applications.

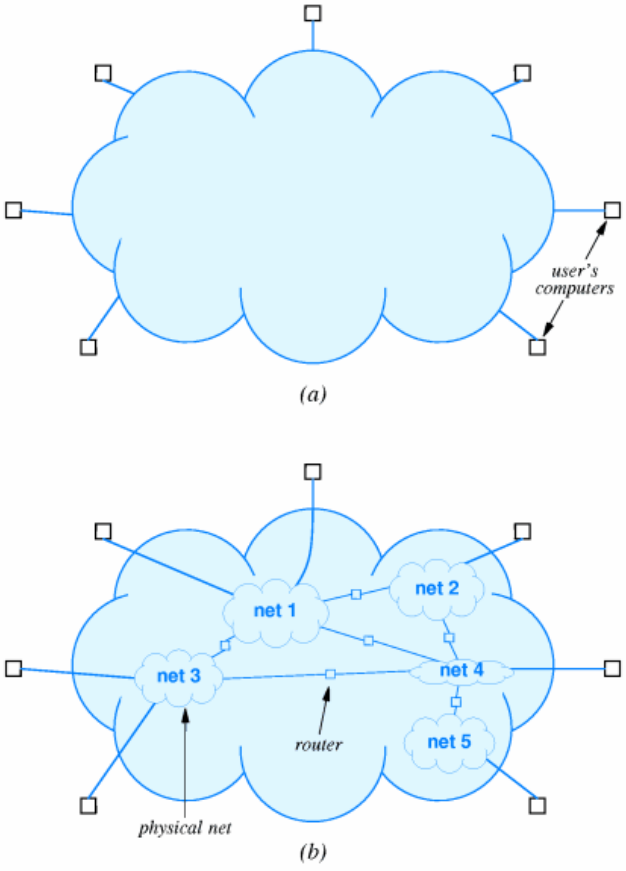


Figure 23.3

LAYERING AND TCP/IP PROTOCOLS:

TCP/IP protocols are organized into five conceptual layers. Although some layers of the TCP/IP reference model correspond to layers of the ISO reference model, the ISO layers scheme does not have a layer that corresponds to TCP/IP Internet Layer.

TCP/IP reference model is shown in the figure below.

Long Q

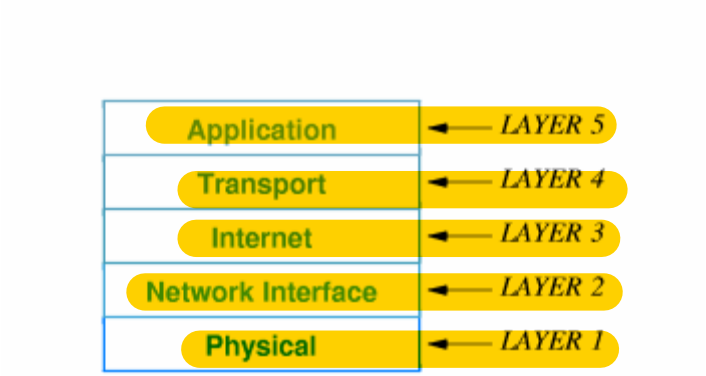


Figure 23.4

LAYER 1:

Corresponds to basic network hardware layer in OSI.

LAYER 2:

Specifies how to organize data in frames.

LAYER 3:

Specifies the format of packets sent across an Internet and forwards packets.

LAYER 4:

Specifies how to ensure reliable transfer.

LAYER 5:

Like 6 and 7 in OSI model, it specifies how one application uses an Internet.

HOST COMPUTERS, ROUTERS AND PROTOCOL LAYERS:

TCP/IP defines the term host computer to refer to any computer system that connects to an Internet and runs applications. A TCP/IP protocol makes it possible for any pair of hosts to communicate despite hardware differences.

Both host and routers need TCP/IP protocol software but routers do not need layer 5 protocols for applications, as they do not run applications.

Lecture No. 24

IP: INTERNET PROTOCOL ADDRESSES

ADDRESSES FOR THE VIRTUAL INTERNET:

To provide uniform addressing in Internet, protocol software defines an abstract addressing scheme that assigns each host a unique protocol address.

Users, application programs and higher layers of protocol software use the abstract protocol software addresses to communicate.

THE IP ADDRESSING SCHEME:

An Internet address (IP address) is a unique 32-bit binary number assigned to a host and used for all communication with the host. Each packet sent across an Internet contains the 32-bit IP address of the sender (source) as well as the intended recipient (destination).

THE IP ADDRESS HIERARCHY:

Each 32-bit IP address is divided into two parts:

PREFIX:

It identifies the physical network to which the computers are attached.

SUFFIX:

It identifies an individual computer on the network.

The physical network in an Internet is assigned a unique value known as a network number. No two networks can be assigned the same network number and no two computers on the same network can be assigned the same suffix. A suffix value can be used on more than one network.

The IP address hierarchy guarantees two important principles:

1. Each computer is assigned a unique address.
2. Although network number assignment must be coordinated globally, suffixes can be assigned locally.

ORIGINAL CLASSES OF IP ADDRESSES:

The original IP address scheme divides host addresses into three primary classes. The class of an address determines the boundary between the network prefix and suffix. The original classes of IP addresses are shown in the figure below.

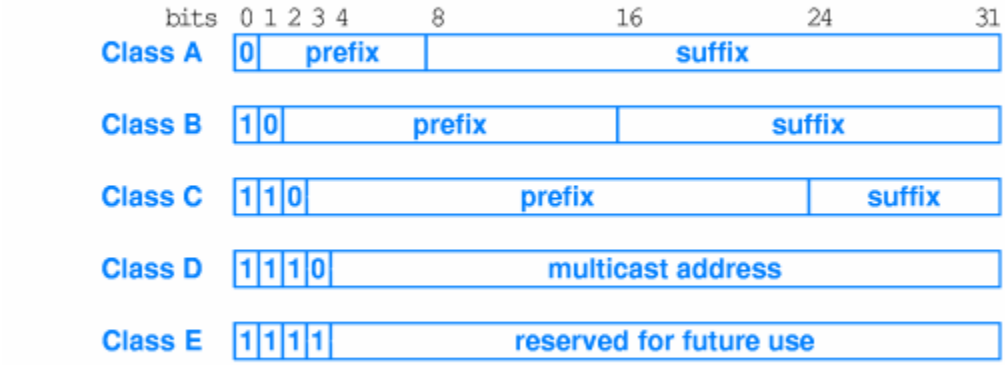


Figure: 24.1

Lecture No. 25

INTERNET PROTOCOL ADDRESS NOTATIONS

COMPUTING THE CLASS OF AN ADDRESS:

Long Q

Whenever it handles a packet, IP software needs to separate the destination address into a prefix and suffix. Classful IP addresses are self-identifying because the class of the address can be computed from the address itself. The table shows in the figure below how the class of address can be computed.

First Four Bits Of Address	Table Index (in decimal)	Class of Address
0000	0	A
0001	1	A
0010	2	A
0011	3	A
0100	4	A
0101	5	A
0110	6	A
0111	7	A
1000	8	B
1001	9	B
1010	10	B
1011	11	B
1100	12	C
1101	13	C
1110	14	D
1111	15	E

Figure: 25.1

DOTTED DECIMAL NOTATION:

Dotted decimal notation is a syntactic form the IP software uses to express 32-bit binary values when interacting with humans. Dotted decimal represents each octet in decimal and uses a dot to separate octets. This is shown in the figure below.

32-bit Binary Number	Equivalent Dotted Decimal
10000001 00110100 00000110 00000000	129 . 52 . 6 . 0
11000000 00000101 00110000 00000011	192 . 5 . 48 . 3
00001010 00000010 00000000 00100101	10 . 2 . 0 . 37
10000000 00001010 00000010 00000011	128 . 10 . 2 . 3
10000000 10000000 11111111 00000000	128 . 128 . 255 . 0

Figure 25.2

CLASSES AND DOTTED DECIMAL NOTATION:

The relationship between classes and dotted decimal notation is given as follows.
In class A the three octets correspond to a host suffix.
In class B the last two octets are the host octets.
Class C has only one octet to represent the host.
The range of decimal values found in the first octet of each address class is given below in the figure.

Class	Range of Values
A	0 through 127
B	128 through 191
C	192 through 223
D	224 through 239
E	240 through 255

Figure: 25.3

DIVISION OF THE ADDRESS SPACE:

The IP class scheme does not divide the 32-bit address space into equal size class and the classes do not contain the same number of networks.

A prefix of n bits allows 2n unique network number, while a suffix of n bits allows 2n host numbers to be assigned on a given network. This is shown in the table below.

Address Class	Bits In Prefix	Maximum Number of Networks	Bits In Suffix	Maximum Number Of Hosts Per Network
A	7	128	24	16777216
B	14	16384	16	65536
C	21	2097152	8	256

Figure 25.4

AUTHORITY FOR ADDRESSES:

Throughout the Internet, each network prefix is unique. Networks obtain their network numbers from their Internet service provider (ISP). The Internet service providers coordinate with the Internet assigned number authority to obtain their network numbers.

CLASSFUL ADDRESSING EXAMPLE:

Here we have a private TCP/IP network, which consists of four physical networks as shown in the figure below.

The first step is to assign IP addresses in which usually class C addresses are assigned. Network administrator computes the ultimate size of each physical network and assigns a prefix.

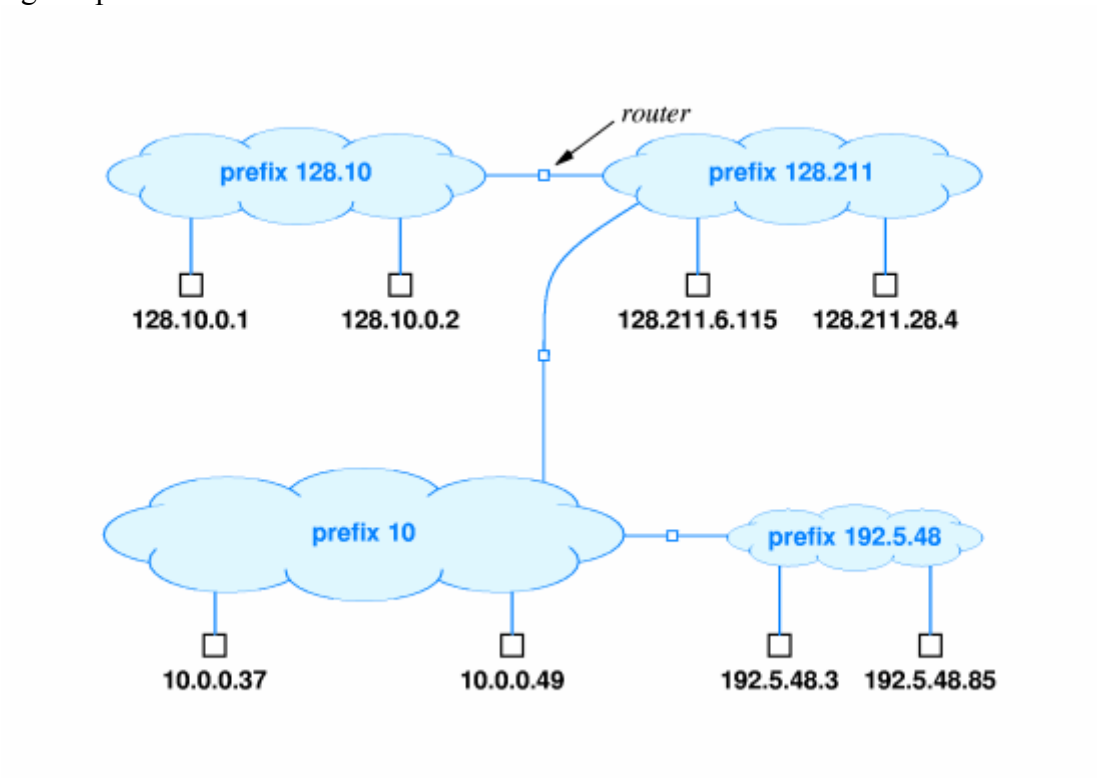


Figure: 25.5

Lecture No. 26

IP SUBNETING

Long Q

SUBNETS AND CLASSLESS ADDRESSING:

As the Internet grew, the original Classful addressing scheme became a limitation. The IP address space was being exhausted because all networks had to choose one of three possible sizes. Many addresses were unused.

Two new mechanisms were invented to overcome the limitations, which are as follows:

- Subnet addressing
- Classless addressing

Instead of having three distinct address classes, allow the division between prefix and suffix to occur on an arbitrary boundary. The classless addressing scheme solves the problem by allowing an ISP to assign a prefix that is, 28 bits long (allowing the host to have up to 14 hosts).

SUBNET/ADDRESS MASK:

How can an IP address be divided at an arbitrary boundary? To use a classless or subnet address, table inside hosts and routers that contain address must keep two pieces of information with each address: the 32-bit address itself and another 32-bit value that specifies the boundary that is known as the Address Mask or Subnet Mask.

Suppose

D = Destination Address

(A, M)= (32-bit IP Address, 32-bit Address Mask)

A = = (D & M)

Now as an example consider a 32-bit mask:

11111111 11111111 00000000 00000000

Which can be denoted in dotted decimal as 255.255.0.0.

Consider a network prefix:

10000000 00001010 00000000 00000000

Which can be denoted in dotted decimal value as 128.10.0.0.

Consider a destination address: 128.10.2.3

That has Binary equivalent as:

10000000 00001010 00000010 00000011

A logical 'and' between D and M produces the binary result as:

10000000 00001010 00000000 00000000

Which is equal to prefix 128.10.0.0.

CIDR NOTATION:

Inside a computer, each address mask is stored as a 32-bit value. When we enter a prefix and an address mask they use a modified form of dotted decimal addressing called CIDR addressing, which is known as CIDR Notation.

As an example how CIDR adds flexibility, suppose a single class B prefix (e.g. 128.211.0.0) i.e. 216 host addresses 16-bit CIDR mask denoted as:

128.211.0.0/16

That is, by making CIDR mask corresponds exactly to the old Classful interpretation. It will be fine if 216 hosts are attached. If it does have two customers with only twelve computers each, the ISP can use CIDR to partition the address into three pieces.

- Two of them each big enough for one of two customers.
- Remainder available for future customers.

For example one customer can be assigned 128.211.0.16/28 and the other customer can be assigned 128.211.0.32/28. Both customers have same mask size, the prefix differs i.e. each customer has a unique prefix.

CIDR HOST ADDRESSES:

The example below in the figure shows the CIDR host addresses:

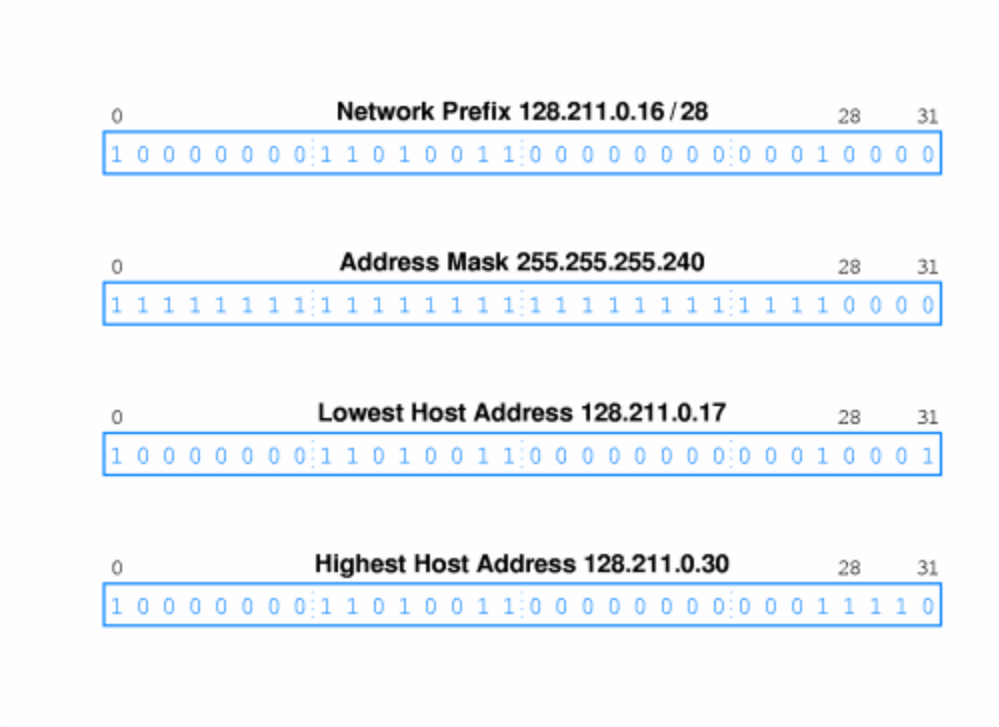


Figure: 26.1

SUMMARY OF SPECIAL IP ADDRESSES:

The table below shows a summary of special IP addresses.

Prefix	Suffix	Type Of Address	Purpose
all-0s	all-0s	this computer	used during bootstrap
network	all-0s	network	identifies a network
network	all-1s	directed broadcast	broadcast on specified net
all-1s	all-1s	limited broadcast	broadcast on local net
127	any	loopback	testing

Figure 26.2

Lecture No. 27

ADDRESS REOLUTION PROTOCOL (ARP)

PROTOCOL ADDRESSES AND PACKET DELIVERY:

Protocol addresses are abstractions provided by software. Physical network hardware does not know how to locate a computer from it protocol address. The protocol address of the next hop must be translated to an equivalent hardware address before a packet can be sent.

ADDRESS RESOLUTION:

Long Q

Mapping between a protocol address and a hardware address is called Address Resolution. A host or router uses address resolution when it needs to send a packet to another computer on the same physical network. A computer never resolves the address of a computer that attaches to a remote network.

In the figure below a simple Internet with routers R1 & R2 connecting three physical networks is shown each network has two host computers attached.

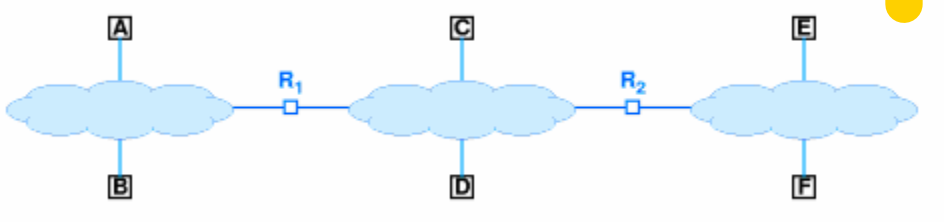


Figure 27.1

In the figure, A resolves protocol address for B for protocol messages from an application on A sent to an application on B. A does not resolve a protocol address for F. Through the Internet layer, A delivers to F by routing through R1 and R2. A resolves R1 hardware address.

Network layer on A passes packet containing destination protocol address F for delivery to R1.

ADDRESS RESOLUTION TECHNIQUES:

Address resolution algorithms can be grouped into three basic categories:

- Table lookup
- Closed-form computation

- Message Exchange

1. TABLE LOOKUP:

In Table Lookup, binding or mapping is stored in a table in memory, which the software searches when it needs to resolve an address.

2. CLOSED-FORM COMPUTATION:

In Closed-form computation, the protocol address assigned to a computer is chosen carefully so that computer's hardware address can be computed from the protocol address using basic Boolean and arithmetic operations.

3. MESSAGE EXCHANGE:

In Message Exchange, Computers exchange messages across a network to resolve an address. One computer sends a message that requests an address binding (translation) and another computer sends a reply that contains the requested information.
Now we discuss in some detail these three categories.

ADDRESS RESOLUTION WITH TABLE LOOKUP:

Resolution requires data structure that contains information about address binding. A separate address-binding table is used for each physical network. The chief advantage of the table lookup approach is generality; a table can store the address bindings for an arbitrary set of computers.

For less than a dozen hosts, a sequential search can suffice. For large networks the sequential approach uses too much CPU time. In the table below the hardware addresses for their corresponding IP addresses are given.

IP Address	Hardware Address
197.15.3.2	0A:07:4B:12:82:36
197.15.3.3	0A:9C:28:71:32:8D
197.15.3.4	0A:11:C3:68:01:99
197.15.3.5	0A:74:59:32:CC:1F
197.15.3.6	0A:04:BC:00:03:28
197.15.3.7	0A:77:81:0E:52:FA

Figure 27.2

There are two standard implementations to improve computational efficiency:

- Hashing
- Direct indexing

HASHING:

Hashing is the transformation of a string of characters into a usually shorter fixed-length value or a key that represents the original string. Hashing is used to index and retrieve items in a database because it is faster to find the item using the shorter hashed key than to find it using the original value. It is also used in many encryption algorithms.

DIRECT INDEXING:

It is less generally known technique. It is possible only is cases where protocols address are assigned from a compact range. In the figure below an example of direct lookup for a class C network is shown.

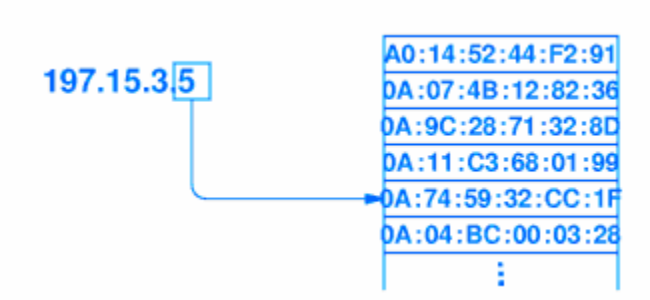


Figure 27.3

ADDRESS RESOLUTION WITH CLOSED-FORM COMPUTATION:

For networks use configurable addressing, it is possible to choose an address that makes closed-form address resolution possible.
A re-solver is used to compute a mathematical function that maps an IP address to a hardware address.

When a computer connects to a network that uses configurable address, the local network administrator must choose a hardware address as well as an IP address. The two values can be chosen to make address resolution trivial. Let's consider an example.

EXAMPLE:

Suppose a configurable network number:

220.123.5.0/24
The IP address of first host = 220.123.5.1
Hardware Address = 1
The IP address of second host = 220.123.5.2

Hardware Address = 2
The IP address of router = 220.123.5.101
Hardware Address = 101
A simple Boolean 'and' operation can compute the computer's hardware address.
Hardware Address = ip_address & 0xff

ADDRESS RESOLUTION WITH MESSAGE EXCHANGE:

An alternative to local computations is a distributed approach. A computer that needs to resolve an address sends a message across a network and receives a reply. The message carries a request that species the protocol address and reply carries the corresponding hardware address.

In this category there are two possible designs:

- Centralized
- Distributed

CENTRALIZED:

A network includes one or more servers that are assigned the task of answering address resolution requests. It has an advantage that resolution is easier to configure, manage and control.

DISTRIBUTED:

Each computer on the network participates in address resolution by agreeing to answer resolution request for its address. It also has an advantage that address resolution servers can become a bottleneck and reduce cost.

Lecture No. 28

ARP MESSAGE FORMAT

ADDRESS RESOLUTION SUMMARY:

It is shown in the figure below, in which T stands for Table lookup, C for Closed-form Computation and D for Data Exchange.

Feature	Type Of Resolution
Useful with any hardware	T
Address change affects all hosts	T
Protocol address independent of hardware address	T, D
Hardware address must be smaller than protocol address	C
Protocol address determined by hardware address	C
Requires hardware broadcast	D
Adds traffic to a network	D
Produces resolution with minimum delay	T, C
Implementation is more difficult	D

Figure 28.1

ADDRESS RESOLUTION PROTOCOL:

TCP/IP can use any of the three address resolution methods depending on the addressing scheme used by the underlying hardware. To guarantee that all computers agree on the exact format and meaning of message used to resolve addresses. The TCP/IP protocol suite includes an Address Resolution Protocol (ARP).

The ARP standard defines two basic message types:

- Request
- Response

REQUEST:

This contains and IP address and requests the corresponding hardware address.

RESPONSE:

This contains both the IP address sent in the request and the hardware address.

ARP MESSAGE DELIVERY:

ARP message delivery is shown in the figure below.

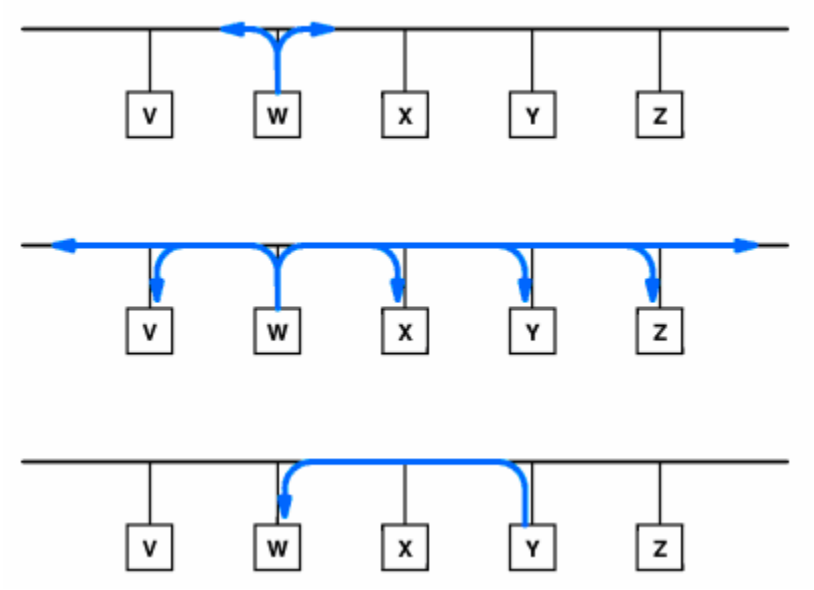


Figure 28.2

ARP MESSAGE FORMAT:

Although the ARP message format is sufficiently general to allow arbitrary protocol and hardware addresses. ARP is almost always used to bind a 32-bit IP address to a 48-bit Ethernet address.

ARP format is shown in the figure below:

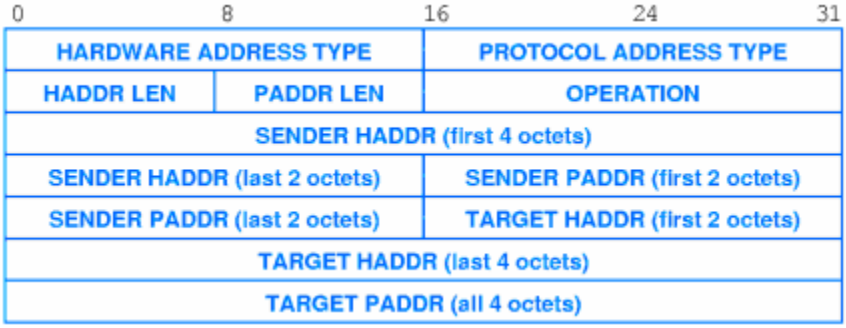


Figure 28.3

SENDING AN ARP MESSAGE:

When one computer sends an ARP message to another the message travels inside the hardware frame. Technically, placing a message inside a frame for transport is called encapsulation as shown in the figure below.

Figure 28.4

IDENTIFYING ARP RESPONSES:

Let's find out how a computer knows whether an incoming frame contains an ARP message. The type field in the frame header specifies that the frame contain an ARP message. The Ethernet standard species that the type field in an Ethernet frame carrying an ARP message must contain the hexadecimal value 0 x 806, as shown in the figure below.

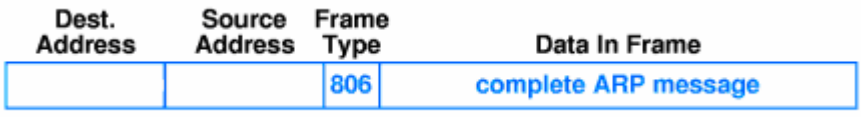


Figure 28.5

CASHING ARP RESPONSES:

Although message exchange can be used to bind addresses, sending a request for each binding is hopelessly inefficient. To reduce network traffic, ARP software extracts and saves the information from a response so that it can be used for subsequent packets. ARP manages the Table as a cache short-term storage.

PROCESSING AN INCOMING ARP MESSAGE:

When an ARP message arrives, the protocol specifies that the receiver must perform two basic steps.

First the receiver extracts the sender's addresses binding and checks to see if
It is present in the cache. If not, it updates the cache.

The receiver examines the operation field of the message to determine whether the message is a request or a response. If the message is a request, the receiver compares

the field TARGET PADDR with the local protocol address. If the two are identical, the computer is the target of the request and must send an ARP response.

LAYERING, ADDRESS RESOLUTION AND PROTOCOL ADDRESSES:

Address resolution (ARP) is a network interface layer function. Protocol addresses are used in all higher layers. Address resolution software hides ugly details and allows generality in upper layers. This is shown in the figure below.

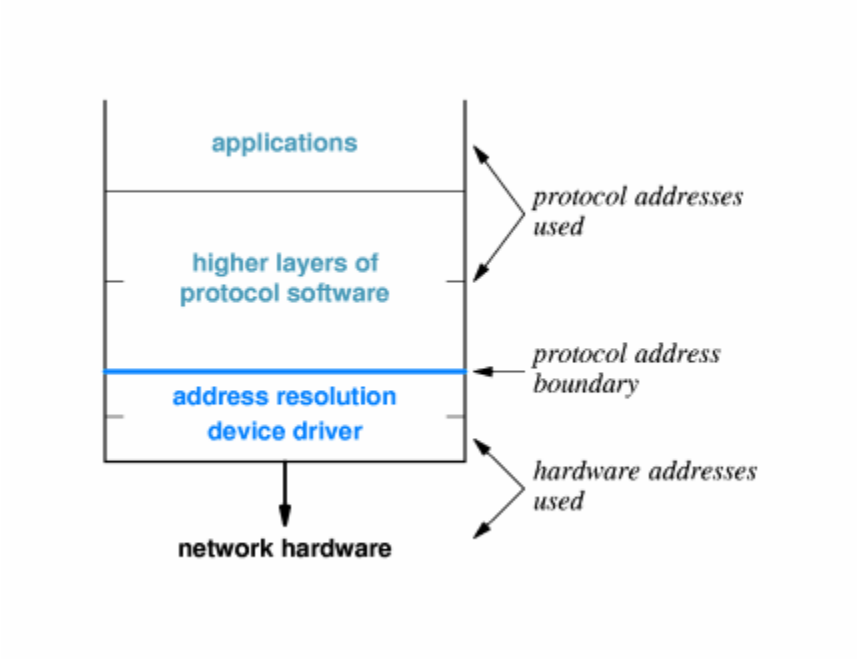


Figure 28.6

Lecture No. 29

IP DATAGRAMS AND DATAGRAM FORWARDING

CONNECTIONLESS SERVICE:

End-to-end delivery service is connection less. The main features of connectionless service are as follows:

It includes extension of LAN abstraction. It has universal addressing and the data is delivered in packets (frames), each with a header. It combines collection of physical networks into a single virtual network.

Transport protocols use this connectionless service to provide:

- Connectionless data delivery (UDP)
- Connection-oriented data delivery (TCP)

VIRTUAL PACKETS:

These packets serve same purpose in Internet as frames on LAN. Each packet has a header. Routers, which are formally gateways, forward packets between physical networks.

These packets have a uniform hardware-independent format. They include header and data and can't use format from any particular hardware. They are encapsulated in hardware frames from delivery across each physical network.

IP DATAGRAM FORMAT:

Formally, the unit of IP data delivery is called a Datagram. It includes header area and data area as shown in the figure below.

Figure 29.1

IP DATAGRAM SIZE:

Long Q

Datagrams can have different sizes i.e.

Header area is usually fixed (20 octets) but can have options. Data area can contain between 1 octet and 65.535 octets (216-1).
Usually, data area is much larger than header.

FORWARDING DATAGRAMS:

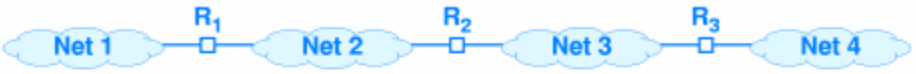
Header contains all information needed to deliver datagram to the destination computer. It contains:

- Destination address
- Source address
- Identifier
- Other delivery information

Router examines header of each datagram and forwards datagram along path to destination.

ROUTING TABLE:

For efficiency, information about forwarding is stored in a routing table, which is initialized at system initialization and must be updated as network topology changes.
The routing table contains list of destination networks and next hop for each destination.
An example routing table is shown in the figure below.



(a)

Destination	Next Hop
net 1	R_1
net 2	deliver direct
net 3	deliver direct
net 4	R_3

(b)

Figure 29.2

ROUTING TABLES AND ADDRESS MASKS:

In practice, additional information is kept in routing table. Destination is stored as network address. Next hop is stored as IP address of router. Address mask defines how many bits of address are in prefix. Prefix defines how much of address used to identify network.

For example, class A mask is 255.0.0.0 which is used for subnetting. A routing table with address masks is shown in the figure below:

(a)

Destination	Mask	Next Hop
30.0.0.0	255.0.0.0	40.0.0.7
40.0.0.0	255.0.0.0	deliver direct
128.1.0.0	255.255.0.0	deliver direct
192.4.10.0	255.255.255.0	128.1.0.9

(b)

Figure 29.3

ADDRESS MASKS:

To identify destination, network apply address mask to destination address and compare to network address in routing table. It can use Boolean 'and' to compute the ith entry in the table.

i.e.

if ((Mask[i] & D) == Dest[i]) forward to NextHop[i]

FORWARDING, DESTINATION ADDRESS AND NEXT-HOP:

Destination address in IP datagram is always ultimate destination. Router looks up next-hop address and forwards datagram. Network interface layer takes two parameters:

- IP datagram
- Next-hop address

Next-hop address never appears in IP datagram.

BEST-EFFORT DELIVERY:

IP provides service equivalent to LAN. It does not guarantee to prevent duplicate datagrams, delayed or out-of-order delivery, corruption of data and datagram loss.

Transport layer provides reliable delivery. Network layer – IP – can detect and report errors without actually fixing them. It focuses on datagram delivery. Application layer is not interested in differentiating among delivery problems at intermediate routers.

Lecture No. 30

IP ENCAPSULATION, FRAGMENTATION AND REASSEMBLY

It is shown in the figure below:

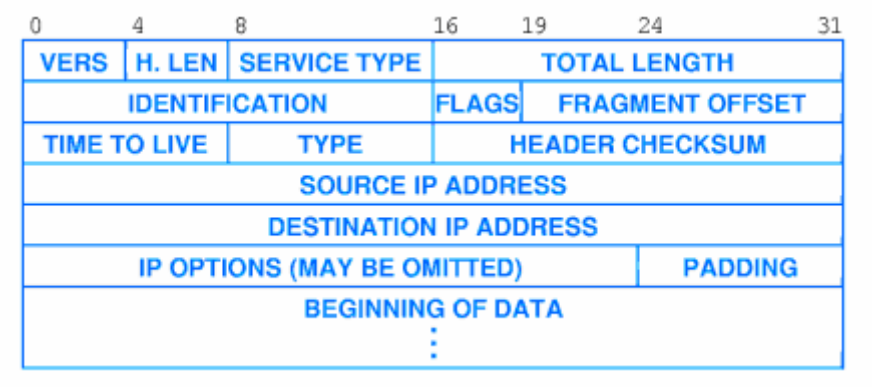


Figure 30.1

In the figure:
VERS shows the version of IP.
H.LEN shows the header length in units of 32-bits.
SERVICE TYPE shows sender's preference for low latency, high reliability that is rarely used.
TOTAL LENGTH shows total octets in datagram.
IDENT, FLAGS, FRAGMENT OFFSET show the values used with fragmentation.
TTL shows time to live decremented in each router; datagram discarded when TTL = 0.
TYPE shows type of protocol carried in datagram e.g., TCP, UDP.
HEADER CHECKSUM shows 1's complement of 1's complement sum.
SOURCE DIST IP ADDRESS shows IP addresses of original source and ultimate destination.

IP DATAGRAM OPTIONS:

Several options can be added to IP header, e.g., record route, source route and timestamp. Header with no options has H. LEN field value 5; data begins immediately after DESTINATION IP ADDRESS. Options are added between DESTINATION IP ADDRESS and data in multiples of 32 bits. Header with 96 bits of options has H. LEN field value 8.

DATAGRAM TRANSMISSION AND FRAMES:

IP Internet layer has following tasks:

- It constructs datagram, determines next hop and hands to network interface layer.

Network interface layer has following tasks:

- It binds next hop address to hardware address and prepares datagram for transmission. But hardware frame doesn't understand IP how datagram is transmitted?

ENCAPSULATION:

Network interface layer encapsulates IP datagram as data area in hardware frame. Hardware ignores IP datagram format. Standards for encapsulation describe details. Standard defines data type for IP datagram, as well as others (e.g., ARP). Receiving protocol stack interprets data area based on frame type. The encapsulation process is shown in the figure below.

Figure 30.2

ENCAPSULATION ACROSS MULTIPLE HOPS:

Each router in the path from the source to the destination un-encapsulates incoming datagram from frame, processes datagram and determines next hop and encapsulates datagram in outgoing frame. Datagram may be encapsulated in different hardware format at each hop. Datagram itself is (almost) unchanged as shown in the figure below.

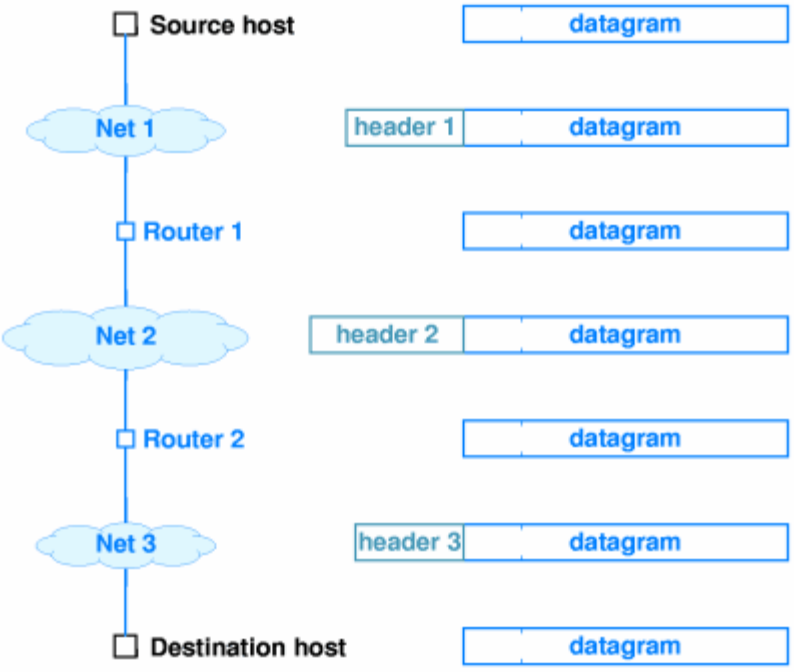


Figure 30.3

MTU: Long Q

Every hardware technology specification includes the definition of the maximum size of the frame data area, which is called the Maximum Transmission Unit (MTU). Any datagram encapsulated in a hardware frame must be smaller than the MTU for that hardware.

MTU AND HETEROGENEOUS NETWORKS:

An Internet may have networks with different MTUs as shown in the figure below. Suppose downstream network has smaller MTU than local network.

Figure 30.4

FRAGMENTATION:

One technique is to limit datagram size to smallest MTU of any network. IP uses fragmentation i.e. datagrams can be split into pieces to fit in network with small MTU.

Router detects datagram larger than network MTU and then it splits into pieces and each piece is smaller than outbound network MTU.

Each fragment is an independent datagram. It includes all header fields. Bit in header indicates that the datagram is a fragment. Other fields have information for reconstructing original datagram. Fragment offset gives original location of fragment.

Router has local MTU to computer size of each fragment. It puts part of data from original datagram in each fragment and puts other information into header. The fragmentation process is shown in the figure below.

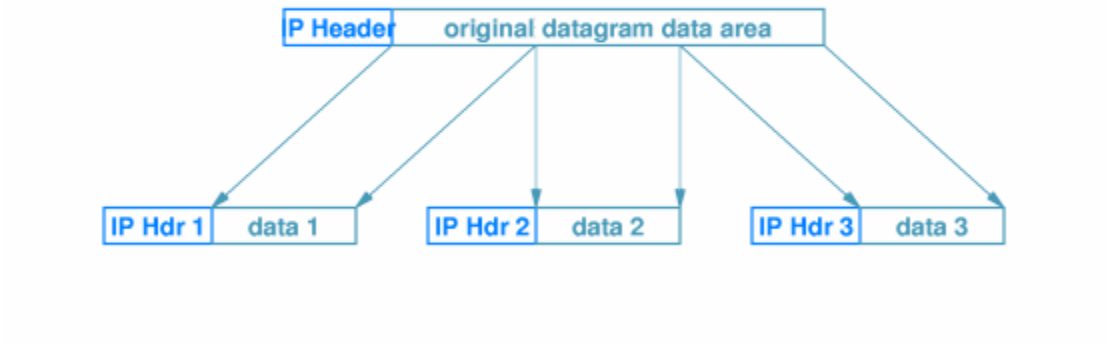


Figure 30.5

DATAGRAM REASSEMBLY:

Reconstruction of original datagram is called reassembly. Ultimate destination performs reassembly as shown below.

Figure 30.6

Fragments may arrive out of order. Header bit identifies fragments containing end of data from original datagram. In the figure 30.5 fragment 3 is identified as last fragment.

FRAGMENT IDENTIFICATION:

Let's see how fragments are associated with original datagram. IDENT field in each fragment matches IDENT field in original datagram. Fragments from different datagrams can arrive out of order and still be sorted out.

FRAGMENT LOSS:

IP may drop fragment because destination drops entire original datagram. Destination sets timer with each fragment to identify lost fragment. If timer expires before all fragments arrive, fragment is assumed lost and datagram is dropped. Source (application layer protocol) is assumed to retransmit.

FRAGMENTING A FRAGMENT:

Fragment may encounter subsequent network with even smaller MTU. Router fragments the fragment to fit. Resulting sub-fragments look just like original fragments (except for size). There is no need to reassemble hierarchically as sub-fragments include position in original datagram.

Lecture No. 31

THE FUTURE IP (IPV6)

INTRODUCTION:

The current version of IP- Version 4 (IPV4) is 20 years old. IPV4 has shown remarkable ability to move to new technologies. IEFT has proposed entirely new version to address some specific problems.

SUCCESS OF IP:

IP has accommodated dramatic changes since original design. But basic principles are still appropriate today. There are many new types of hardware.

SCALING:

Scale is also dramatically changed. Size from a few tens to a few tens of millions of computers has been revolutionized. Speed has increased from 56Kbps to 1Gbps. Also there is an increased frame size in hardware.

MOTIVATION FOR CHANGE:

Reasons for which IPV6 need to be changed.

Long Q

One of the parameters, which motivated IP for change is address space. The 32-bit address space allows for over a million networks.
But most networks are class C and too small for many organizations.
214 class B network addresses already almost exhausted (and exhaustion was first predicted to occur, a couple of years ago).
The second parameter is type of service, the IP provides.
Different applications have different requirements for delivery reliability and speed. Current IP has type of service that is not often implemented. Another factor for the motivation for change is multicast.

NAME AND VERSION NUMBER:

A preliminary version of IP was called IP- Next Generation (IPng). There were several proposals and all called IPng. One name was selected and it used next available version number i.e. 6. The result is IP version 6 (IPV6).

NEW FEATURES:

The new features of IPV6 are as follows:

Long Q

- IPV6 addresses are 128 bits.
- Header format is entirely different.
- Additional information is stored in optional extension headers, followed by data.
- Flow label and quality of service allows audio and video applications to establish appropriate connections.
- New features can be added more easily. So it is extensible.

IPV6 DATAGRAM FORMAT:

It is shown in the figure below:

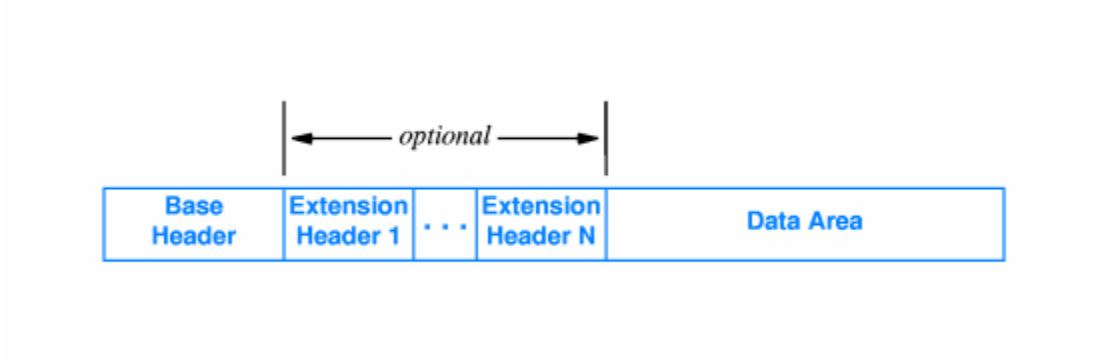


Figure: 31.1

IPV6 BASE HEADER FORMAT:

It contains less information than IPV4 header. Next header points to first extension header. Flow label is partitioned into a TRAFFIC CLASS field and a separate FLOW LABEL field used to identify a specific path thorough the network.

Routers use flow label to forward datagrams along prearranged path.
It is shown in the figure below:

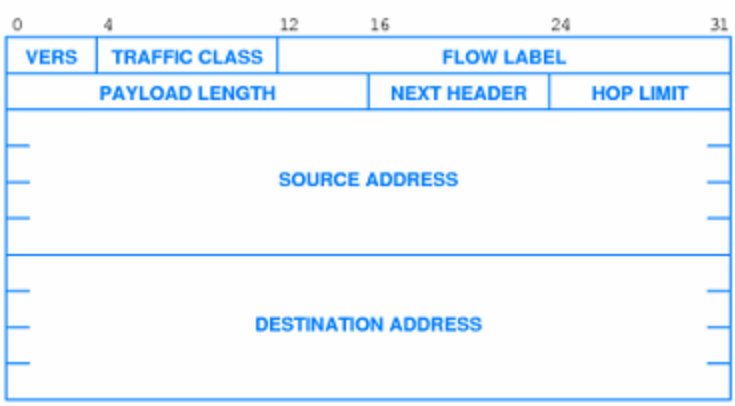


Figure 31.2

IPV6 NEXT HEADER:

It is shown in the figure below:

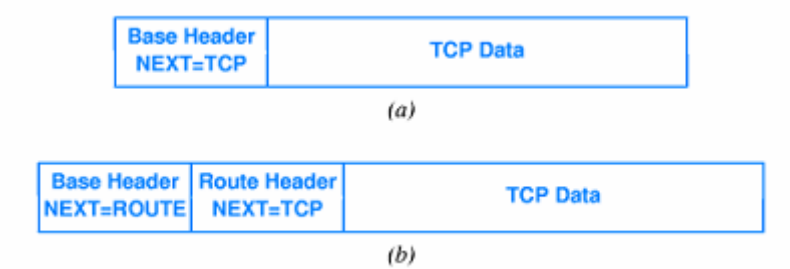


Figure 31.3

PARSING IPv6 HEADERS:

Long Q

Base header is fixed size i.e. 40 octets. NEXT HEADER field in the base header defines type of header and it appears at end of fixed-size base header. Some extension headers are variable sized. NEXT HEADER field in extension header defines type. HEADER LEN field gives size of extension header as shown in the figure below:

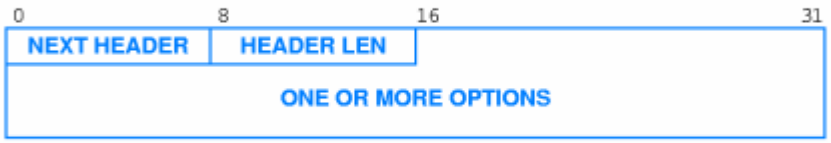


Figure 31.4

Lecture No. 32

IPv6 AND AN ERROR REPORTING MECHANISM

FRAGMENTATION:

Long Q

Fragmentation information is kept in separate extension header. Each fragment has base header and (inserted) fragmentation header. Entire datagram including original header may be fragmented. This process is shown in the figure below.

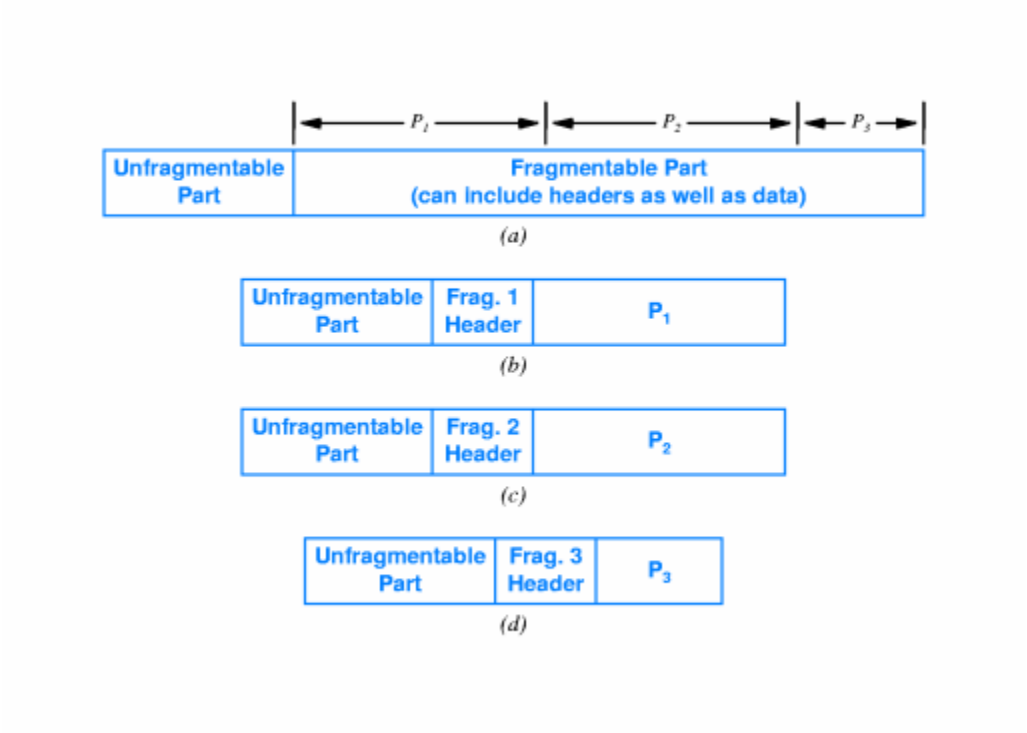


Figure 32.1

FRAGMENTATION AND PATH MTU:

IPv6 source (not intermediate routers) is responsible for fragmentation. Routers simply drop datagrams larger than network MTU (Maximum Transmission Unit). So source must fragment datagram to reach destination.

Source determines path MTU. The smallest MTU on any network between source and destination and it fragments datagram to fit within that MTU.

The process of learning the path MTU is known as path MTU discovery. Path MTU discovery is used. Source sends probe message of various sizes until destination reached. It must be dynamic i.e. path may change during transmission of datagrams.

USE OF MULTIPLE HEADERS:

It has following advantages:

- **Efficiency:** Header is only as large as necessary.
- **Flexibility:** it can add new headers for new features.
- **Incremental development:** It can add processing for new features to testbed, other routers will skip those headers.

IPv6 ADDRESSING:

Long Q

IPv6 uses 128-bit addresses. A 128-bit address includes network prefix and host suffix. An advantage of IPv6 addressing is that it has no address classes i.e. prefix/suffix boundary can fall anywhere.

Following are special types of addresses, IPv6 uses:

Unicast: It is used for single destination computer.
Multicast: It is used for multiple destinations; possibly not at same site.
Cluster: This type of address is used for collection of computers with same prefix, datagram is delivered to one out of cluster.

IPv6 ADDRESS NOTATION:

Long Q

128-bit addresses unwidely in dotted decimal; requires 16 numbers:
105.220.136.100.255.255.255.255.0.0.18.128.140.10.255.255

Groups of 16-bit numbers in hex separated by colons – colon hexadecimal (or colon hex).
69DC: 8864:FFFF: FFFF: 0:1280:8C0A:FFFF

Zero-compression – series of zeroes indicated by two colons
FF0C: 0:0:0:0:0:0:B1 Long Q
FF0C::B1

IPv6 address with 96 leading zeros is interpreted to hold an IPv4 address.

AN ERROR REPORTING MECHANISM (ICMP)

INTRODUCTION:

IP provides best-effort delivery. Delivery problems can be ignored; datagrams can be 'dropped on the floor'. Internet Control Message Protocol (ICMP) provides error-reporting mechanism.

BEST-EFFORT SEMANTICS AND ERROR DETECTION:

Internet layer can detect a variety of errors: e.g.

- Checksum (header only)
- TTL expires
- No route to destination network.
- Can't deliver to destination host (e.g., no ARP reply).

Internet layer discards datagrams with problems. Some - for example, checksum error – can't trigger error messages.

INTERNET CONTROL MESSAGE PROTOCOL:

Some errors can be reported. Router sends message back to source in datagram. Message contains information about problem. It is encapsulated in IP datagram.

TYPES OF MESSAGES:

Long Q

Internet control Message Protocol (ICMP) defines error and informational messages. These are given as follows:

1. ERROR MESSAGES:

These are as follows:

- Source quench
- Time exceeded
- Destination unreachable
- Redirect
- Fragmentation required

2. INFORMATIONAL MESSAGES:

These are as follows:

- Echo request/reply
- Address mask request /reply
- Router discovery

Lecture No. 33

AN ERROR REPORTING MECHANISM (ICMP)

ICMP MESSAGE TRANSPORT:

ICMP message transport is acted upon by getting ICMP encapsulated in IP. This is shown in the figure below:

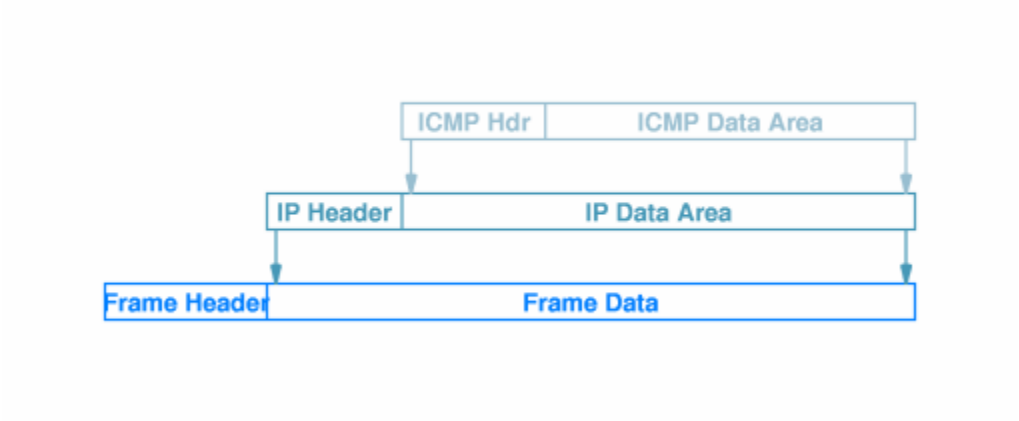


Figure 32.2

ICMP message is sent in response to incoming datagrams with problems. ICMP message is not sent for ICMP message.

Long Q

USING ICMP TO TEST REACHABILITY:

ICMP can also be used to test different tools. An Internet host A, is reachable from another host B, if datagrams can be delivered from A to B. Ping program tests reachability. It sends datagram from B to A, that echoes back to B. it uses ICMP echo request and echo reply messages. Internet layer includes code to reply to incoming ICMP echo request messages.

USING ICMP TO TRACE A ROUTE:

List of all routers on path from A to B is called the route from A to B. The intermediate routers send ICMP time exceeded message to the source and destination sends an ICMP destination unreachable message to the source.

Tracert (Windows version) sends ICMP echo messages with increasing TTL. Router that decrements TTL to 0 sends ICMP time exceeded message, with router's address as source address. First, with TTL 1, gets to first router, which discards and sends time exceeded message. Next, with TTL 2 gets through first router to second router. It continues until an ICMP echo reply message from destination is received.

Long Q

THE LAST ADDRESS PRINTED BY TRACE-ROUTE:

There are two possibilities used to detect the destination.

- Send and ICMP echo request, destination host will generate an ICMP echo reply.
- Send a datagram to a non-existent application, destination host will generate an ICMP destination unreachable message.

USING ICMP FOR PATH MTU:

Fragmentation should be avoided. Source can configure outgoing datagrams to avoid fragmentation. Source determines path MTU- smallest network MTU on path from source to destination. Source probes path using IP datagrams with don't fragment flag. Router responds with ICMP fragmentation required message. Source sends smaller probes until destination reached.

Lecture No. 34

UDP: DATAGRAM TRANSPORT SERVICE

TERMINOLOGY:

Long Q

IP:

- Provides computer-to-computer communication.
- Source and destination addresses are computers.
- This is also called machine-to-machine communication.

TRANSPORT PROTOCOLS:

- Provide application-to-application communication.
- Need extended addressing mechanisms to identify applications.
- Are called end-to-end communication.

INTRODUCTION:

UDP is the first of the transport protocols in TCP/IP protocol suite. UDP protocol allows applications on the computers to send and receive datagrams. UDP has a packet format. It uses best-effort delivery service.

THE NEED FOR TRANSPORT PROTOCOLS:

Internet protocol can not distinguish between application programs running on the same computer. Fields in the IP datagram header refer to computers, not applications. A protocol that allows an application program to serve as the end point of communication is known as a transport protocol or an end-to-end protocol.

THE USER DATAGRAM PROTOCOL (UDP):

TCP/IP contains two transport protocols:

- UDP
- TCP

UDP:

UDP is less complex and easier to understand. It does not provide the type of service a typical application expects.

CHARACTERISTICS OF UDP:

UDP has the following characteristics.

- It is an end-to-end protocol. It provides application-to-application communication.
- It provides connectionless service.
- It is a Message-Oriented protocol.
- It uses best-effort delivery service.
- It follows arbitrary interaction.
- It is operating system independent.

THE CONNECTIONLESS PARADIGM:

UDP does not need to pre-establish communication and also there is no need to terminate communication. UDP allows an application to delay long intervals between two messages. There are no Control Messages; only Data Messages. So it has very low overhead.

MESSAGE-ORIENTED INTERFACE:

Long Q

UDP offers application programs a Message-Oriented Interface. It does not divide messages into packets for transmission and does not combine messages for delivery.

Let's discuss its advantages and disadvantages.

ADVANTAGES:

- Applications can depend on protocol to preserve data boundaries.

DISADVANTAGES:

- Each UDP message must fit into a single IP datagram.
- It can result to an inefficient use of the underlying network.
-

UDP COMMUNICATION SEMANTICS:

UDP uses IP for all delivery, that is, same best effort delivery as IP.

To use UDP, an application must either be immune to the problems or programmer must take additional steps to detect and correct problems.

EXAMPLES:

- Audio transmission
- On-line shopping application

ARBITRARY INTERACTION:

UDP follows four types of interaction

- **1-to-1:** One application can communicate with one application.
- **1-to-many:** One application can communicate with many applications.
- **Many-to-1:** Many applications can communication with one application.
- **Many-to-many**: Many applications can communicate with many applications.

SUPPORT FOR UNICAST, MULTICAST AND BROADCAST:

UDP allows multicast 1-to-many interaction using multicast or a broadcast. Sender uses a broadcast address as the destination address to interact with many applications. It is especially useful for Ethernet networks.

ENDPOINT IDENTIFICATION WITH PROTOCOL PORT NUMBERS:

UDP identifies an application as an endpoint.

Mechanism cannot be the same as of the operating system. No common mechanisms exist. There are multiple identifiers like protocol identifiers, job names and task identifiers.

UDP defines a set of identifiers called ‘protocol ports.’

It is independent of the underlying operating system. Each computer using UDP provides a mapping between the protocol port number and the program identifiers of its operating system.

The address and protocol port specifications of an application define the type of communication. To engage in a 1-to-1 communication, the application specifies:

- The local port number
- Remote IP address
- The remote port number

Lecture No. 35

DATAGRAM FORMAT AND TCP: RELIABLE TRANSPORT SERVICE

UDP DATAGRAM FORMAT:

It is shown in the figure below:

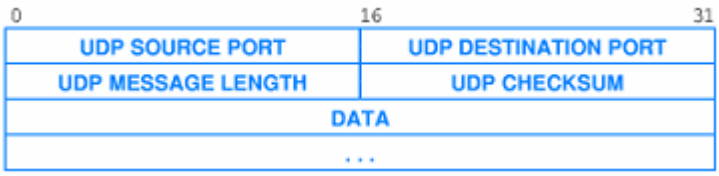


Figure 35.1

UDP ENCAPSULATION:

As shown in the figure below, UDP packet is encapsulated in IP datagram and the IP datagram is then encapsulated in the Frame.

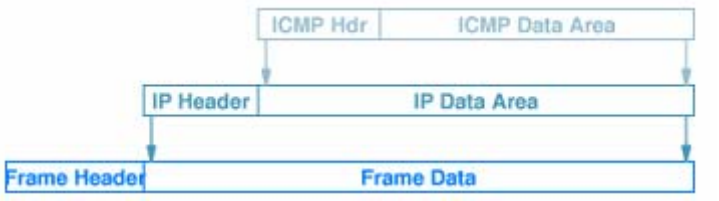


Figure 35.2

TCP:

INTRODUCTION:

TCP is the major transport protocol in the TCP/IP suite. It uses unreliable datagram service offered by IP when sending data to another computer. It provides reliable data delivery service to applications.

THE NEED FOR RELIABLE TRANSPORT:

Reliability is fundamental in a computer system. Software in the Internet must provide the same level of reliability as a computer system. Software must guarantee prompt and reliable communication without any loss, duplication, and change in the order.

TRANSMISSION CONTROL PROTOCOL:

Long Q

Reliability is the responsibility of the Transport layer. In TCP/IP, TCP provides reliable transport service. Most Internet applications use TCP as no other protocol has proved to work better.

SERVICE PROVIDED BY TCP:

Following are the services provided by TCP:

- Connection-oriented service
- Point-to-point
- Complete reliability
- Full-duplex communication
- Stream interface
- Reliable connection startup
- Graceful connection shutdown

Long Q

END-TO-END SERVICE AND DATAGRAMS:

Applications can request a connection. TCP connections are called Virtual Connections. They are created by software only. Internet does not provide software or hardware support for the connections. TCP software modules on two computers create an illusion of a connection.

TCP uses IP to carry messages. TCP message is encapsulated in IP datagram and sent to the destination. On the destination host, IP passes the contents to TCP. It is shown in the figure below.

How TCP and IP interact with each other?

Long Q

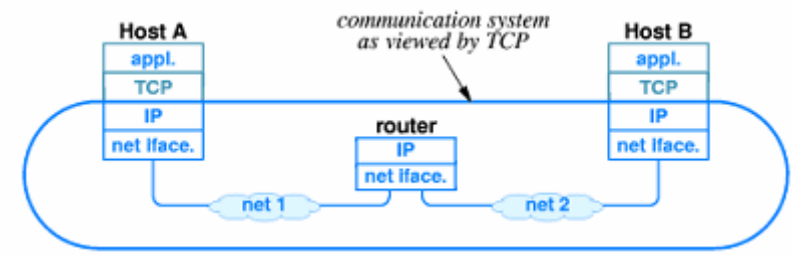


Figure 35.3

ACHIEVING RELIABILITY:

The major problems in the reliable delivery are:

- Unreliable delivery by the underlying communication system.
- System reboots.

Lecture No. 36

TCP: RELIABLE TRANSPORT SERVICE (Cont.)

PACKET LOSS AND RETRANSMISSION:

How TCP provide reliability?

Long Q

TCP achieves reliability by retransmission. An acknowledgement is used to verify that data has arrived successfully. If acknowledgement does not arrive, the previous data is retransmitted. This is shown in the figure below:

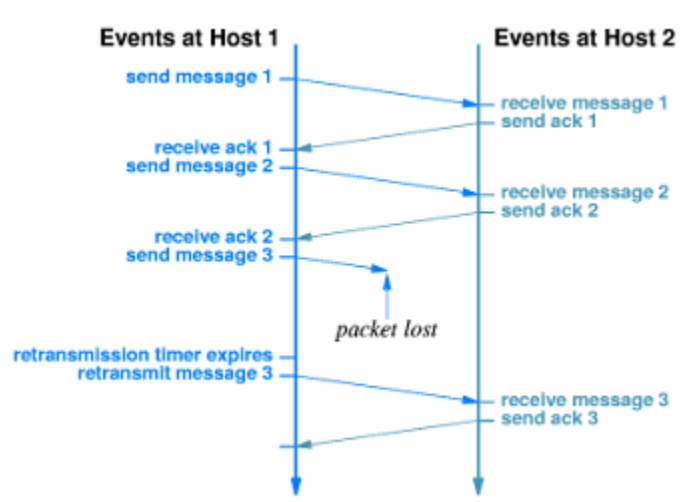


Figure 36.1

HOW LONG SHOULD TCP WAIT BEFORE RETRANSMITTING:

The time for acknowledgement to arrive depends on:

- Distance to destination
- Current traffic conditions

Multiple connections can be opened simultaneously. Traffic conditions change rapidly.

ADAPTIVE RETRANSMISSION:

Setting a timer sounds so easy but the question is "what time interval?" If the time interval is too large, you are spending time waiting for something that is just not going to happen. If the time interval is too short, you will resend needlessly.

So keep estimate of round trip time on each connection, and use current estimate to set transmission timer. This is known as 'Adaptive Retransmission'. This is a key to TCP's success.

COMPARISON OF RETRANSMISSION TIMES:

The figure shows a comparison of retransmission times. The network having short intervals has a short timeout and the network having large interval has large timeout.

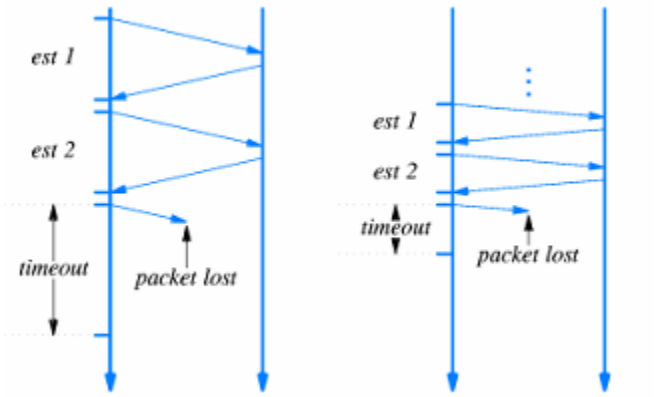


Figure 36.2

BUFFER, FLOW CONTROL AND WINDOWS:

TCP uses window mechanism to control the flow of data. The amount of buffer space available at any time is called the window and a notification that specifies the size is called the window advertisement.

In the figure below a sequence of messages that illustrates TCP flow control when the maximum segment size is 1000 octets. A sender can transmit enough data to fill the currently advertised window.

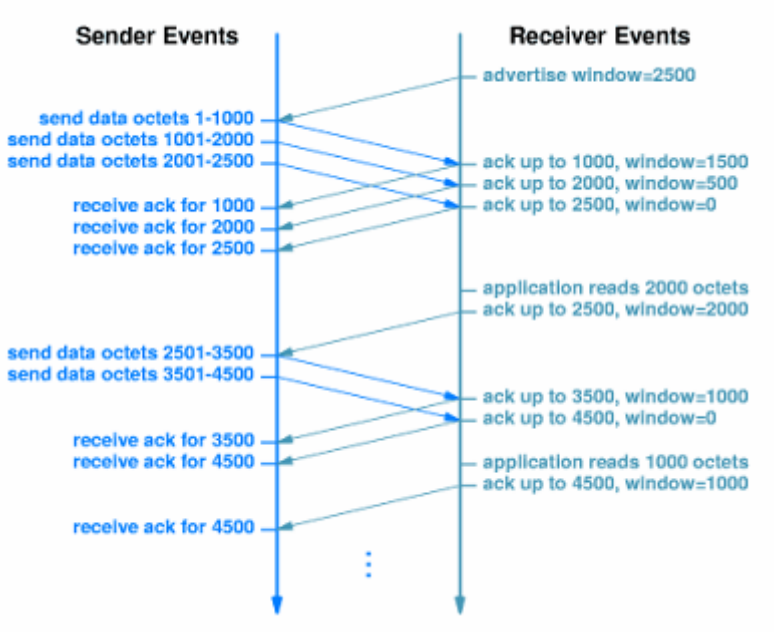


Figure 36.3

THREE WAY HANDSHAKES TO CLOSE A CONNECTION:

The figure below shows a three-way handshake to close a connection. Acknowledgements sent in each direction are used to guarantee that all data has arrived before the connection is terminated.

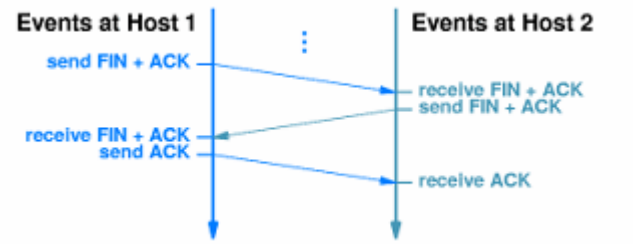


Figure 36.4

Long Q

THREE-WAY HANDSHAKE TO BEGIN A CONNECTION:

Part of the 3-way handshake used to create a connection, requires each end to generate a random 32-bit sequence number. If an application attempts to establish a new TCP connection after a computer reboots, TCP chooses a new random number.

Lecture No. 37

NETWORK ADDRESS TRANSLATION (NAT)

CONGESTION CONTROL:

Long Q

The goal of congestion control is to avoid adding retransmissions to an already congested network. Reducing the window size quickly in response to the lost messages does it. It is assumed that loss is due to congestion.

We have to resume carefully. Otherwise the network will swing wildly between congestion and under utilization.

TCP SEGMENT FORMAT:

It is shown in the figure below. TCP uses single format for all messages. TCP uses the term segment to refer to a message. Each message sent from TCP on one machine to TCP on another machine uses this format including data and acknowledgement.

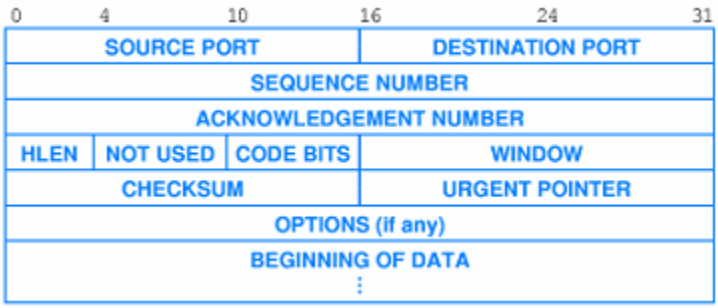


Figure 37.1

NETWORK ADDRESS TRANSLATION:

It is the extension of original addressing scheme and was motivated by exhaustion of IP address space. It allows multiple computers to share a single address. It requires device to perform packet translation.
Its implementations are available e.g.,

- Stand-alone hardware device
- IP router with NAT functionality embedded

NAT DETAILS:

Site that consists of more than one computer, obtains a single valid IP address. It assigns a private address to each computer and uses NAT box to connect to the Internet. NAT translates address in IP datagrams.

ILLUSTRATION OF NAT:

The figure illustrates the NAT functionality. When a computer in the site communicates to the internet, the NAT device, as shown in the figure below, translates its private address in the site to the global IP address and vice versa.

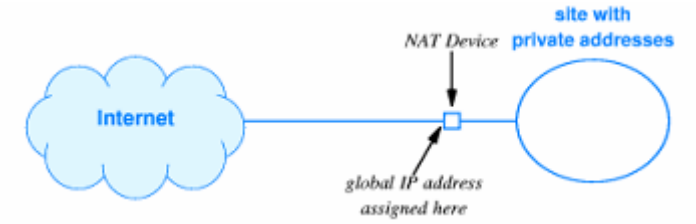


Figure 37.2

NAT EXAMPLE:

For example, a site uses private network 10.0.0.0/8 internally.
First computer is assigned 10.0.0.1, second computer is assigned 10.0.0.2 and so on…

Site obtains a valid IP address (e.g. 128.210.24.6). Let's assume that the computer 10.0.0.1 sends to 128.211.134.4 (another global IP address). NAT translates the IP source address of the outgoing datagram to the global IP address. NAT also translates the destination address of incoming datagram to the private site address. It is shown in the figure below.

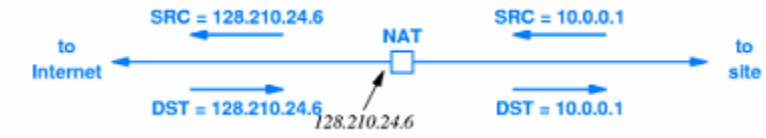


Figure 37.3

ILLUSTRATION OF NAT TRANSLATION:

It is transparent to each end i.e. computer at site sends and receives datagrams normally and computer at Internet receives datagrams from NAT box.

Long Q

IMPLEMENTATION OF NAT:

The figure below shows the implementation of NAT. We can see that the old and new values of IP source field and destination field are shown with their directions.

Direction	Field	Old Value	New Value
out	IP Source	10.0.0.1	128.10.24.6
in	IP Destination	128.10.24.6	10.0.0.1

Figure 37.4

NAT device stores state information in table. The value is entered in the table when NAT box receives outgoing datagram from new

Lecture No. 38

NETWORK ADDRESS TRANSLATION

VARIANTS OF NAT:

There are also some variants of NAT due to some of its drawbacks.

The basic NAT simply changes IP addresses. But Network Address and Port Translation (NAPT) (which is another modified form of NAT) changes IP addresses and protocol port numbers too. It is the most popular form of NAT.

Long Q

Twice NAT is another variant of NAT. it is used with site that runs server. In this process NAT box is connected to Domain Name.

NETWORK ADDRESS AND PORT TRANSLATION (NAPT):

It is by far the most popular form of NAT that can change TCP or DP protocol port numbers as well as IP addresses.

It allows multiple computers at site to communicate with single destination as well as multiple users on given computer to communicate with same destination.

EXAMPLE NAPT TRANSLATION TABLE:

An example NAPT translation table is shown in the figure below. We can see that not only the private addresses but also the port numbers are translated too.

Direction	Fields	Old Value	New Value
out	IP SRC:TCP SRC	10.0.0.1:30000	128.10.19.20:40001
out	IP SRC:TCP SRC	10.0.0.2:30000	128.10.19.20:40002
in	IP DEST:TCP DEST	128.10.19.20:40001	10.0.0.1:30000
in	IP DEST:TCP DEST	128.10.19.20:40002	10.0.0.2:30000

Figure 38.1

Each entry in the table records protocol port numbers as well as IP address. The port numbers are reassigned to avoid conflicts.

TCP SPLICING:

A popular use of NAPT is TCP Splicing. It interconnects two independent TCP connections and performs segment rewriting. It is extremely efficient and avoids overhead of extracting data from one connection and sending to the other. It uses extended translation table.

Long Q

TWICE NAT:

Basic NAT does not work well for communication initiated from the Internet. Twice NAT allows a site to run servers. It requires the DNS to interact with the NAT device. Twice NAT fails if an application uses the IP addresses instead of Domain Name.

CAT:

Cable TV providers offering Internet services through Cable Modems propose it. It includes NAPT plus additional functionality. The additional functionality allows the cable operator to communicate with the CAT device, inspect values and control network access.

Long Q

NAT AT HOME:

NAT is useful at a residence with Cable Modem or DSL connectivity as it allows the customer to have multiple computers at home without requiring an IP address for each of them. Instead a single IP address is used for all the computers. NAT software allows a PC to connect with the Internet and act as a NAT device at the same time.

It is shown in the figure below where multiple computers are connected to the dedicated hardware device implementing NAT.

Figure 38.2

Lecture No. 39

IP ROUTING (Part-1)

TERMINOLOGY:

The forwarding and Routing are two different concepts and explained as follows:

FORWARDING:

It refers to datagram transfer. It is performed by host or router. It uses routing table.

ROUTING:

It refers to propagation of routing information. It is performed by routers. It inserts or changes values in routing table.

TWO FORMS OF INTERNET ROUTING:

STATIC ROUTING:

Long Q

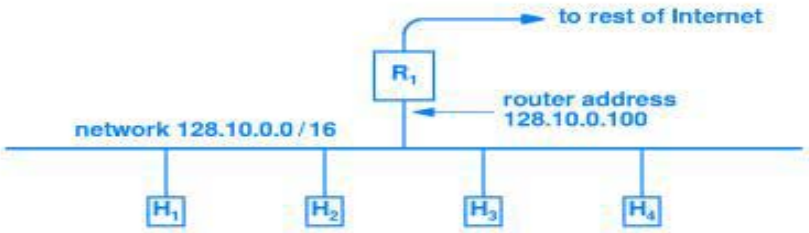
It is one of the forms of Internet routing. In Static routing, the table is initialized when system boots and there is no further changes.

DYNAMIC ROUTING:

In dynamic routing the table is initialized when system boots. It includes routing software which learns routes and updates table. In this way continuous changes are possible due to routing software.

STATIC ROUTING:

It is used by most Internet hosts. The typical routing table has two entries as shown in the figure. For the local network it has direct delivery and for the communication to some other network it follows the nearest default route. The example is shown in the figure below where four hosts are attached to an Ethernet which connects to the rest of the internet through router R1.



(a)

Net	Mask	Next hop
128.10.0.0	255.255.0.0	direct
default	0.0.0.0	128.10.0.100

(b)

DYNAMIC ROUTING:

It is used by IP routers. It requires special software which continuously updates the routing information. Each router communicates with neighbors. It passes routing information and uses Route Propagation Protocol to exchange the information with other routers.

EXAMPLE OF ROUTE PROPAGATION:

In this example three networks are connected by two routers. In such a situation, dynamic routing can be used to propagate information about remote networks.

Lecture No. 40

IP ROUTING (Part-2)

ROUTING IN THE GLOBAL INTERNET

As the route information protocol allows one router to exchange routing information with another, however this scheme cannot scale to the entire Internet because, if all routers attempted to exchange information, the resulting traffic would overwhelm the backbone networks. To solve the problem the routers and networks in the Internet are divided into groups. All routers within a group exchange routing information. Then at least one router in the group summarizes information before sending it to other groups.

AUTONOMOUS SYSTEM CONCEPT:

An autonomous system can be thought of as a set of networks and routers under one administrative authority. The term is flexible. It can be or correspond to an entire intuition or a single corporation. It is needed because no routing protocol can scale to entire Internet. Each Autonomous System chooses a routing protocol to exchange routing information which is summarized before being passed to another group.

CLASSIFICATION OF INTERNET ROUTING PROTOCOLS:

Long Q

There are two broad classes of Internet Routing Protocol:

INTERIOR GATEWAY PROTOCOLS (IGPs):

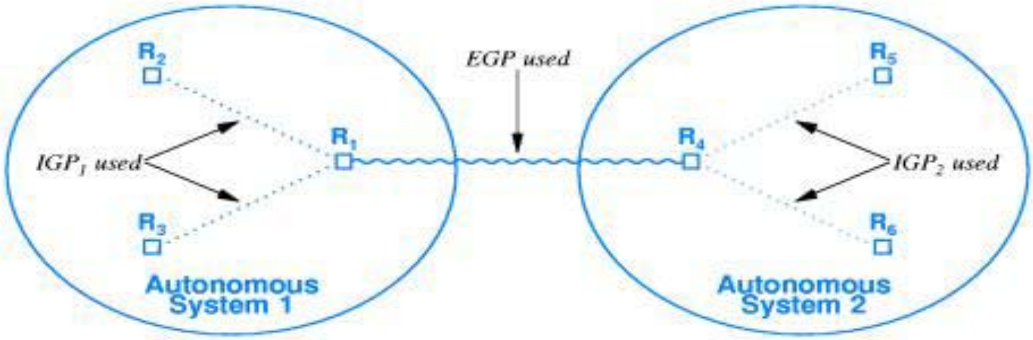
It is used among routers within autonomous system. The destinations lie within IGP.

EXTERIOR GATEWAY PROTOCOLS (EGPs):

It is used among autonomous systems. The destinations lie throughout Internet

ILLUSTRATION OF IGP/EGP USE:

The following figure illustrates the IGP/EGP use.



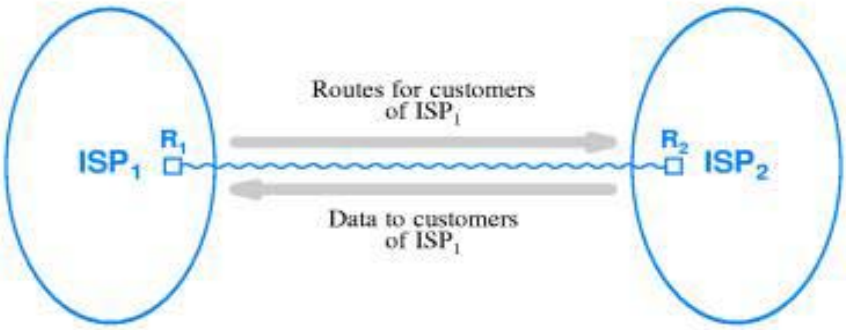
An Internet routing architecture is shown. Each autonomous system used to communicate among autonomous systems chooses an IGP to use

Lecture No. 41

IP ROUTING (Part-3)

ROUTES AND DATA TRAFFIC:

Each ISP is an autonomous system that uses an Exterior Gateway Protocol to advertise its customer's networks to other ISPs. After an ISP advertises destination D, datagram destined for D can begin to arrive.



The flow of routers and data is illustrated with ISPs. After a router in ISP advertises routes to customers, data can arrive for these customers.

INTERNET ROUTING PROTOCOLS:

Following are the Internet Routing Protocols.

"Border Gateway Protocol (BGP)

"Routing Information Protocol (RIP)

"Open Shortest Path First Protocol (OSPF)

Long Q

BORDER GATEWAY PROTOCOL:

It is most popular Exterior Gateway Protocol in Internet. It has following characteristics:

"It provides routing among autonomous systems (EGP).

"It provides policies to control routes advertised.

"It uses reliable transport (TCP).

"It gives path of autonomous systems for each destination.

"Currently the EGP is of choice in the Internet.

"The current version is four (BGP-4).

"It provides facilities for Transit Routing.

ROUTING INFORMATION PROTOCOL (RIP):

It has the following characteristics:

Long Q

"It is used for routing within an autonomous system (IGP).

"Hop Count Metric: RIP measures distance in network hops, where each network between the source and destination counts as a single hop.

"It uses UDP for all message transmissions.

"RIP is used over LAN. Version 1 of RIP uses hardware broadcast and version 2 allows delivery via multicast.

"It can be used to advertise default route propagation. An organization can use RIP to install a default route in each router.

"It uses distance vector algorithm.

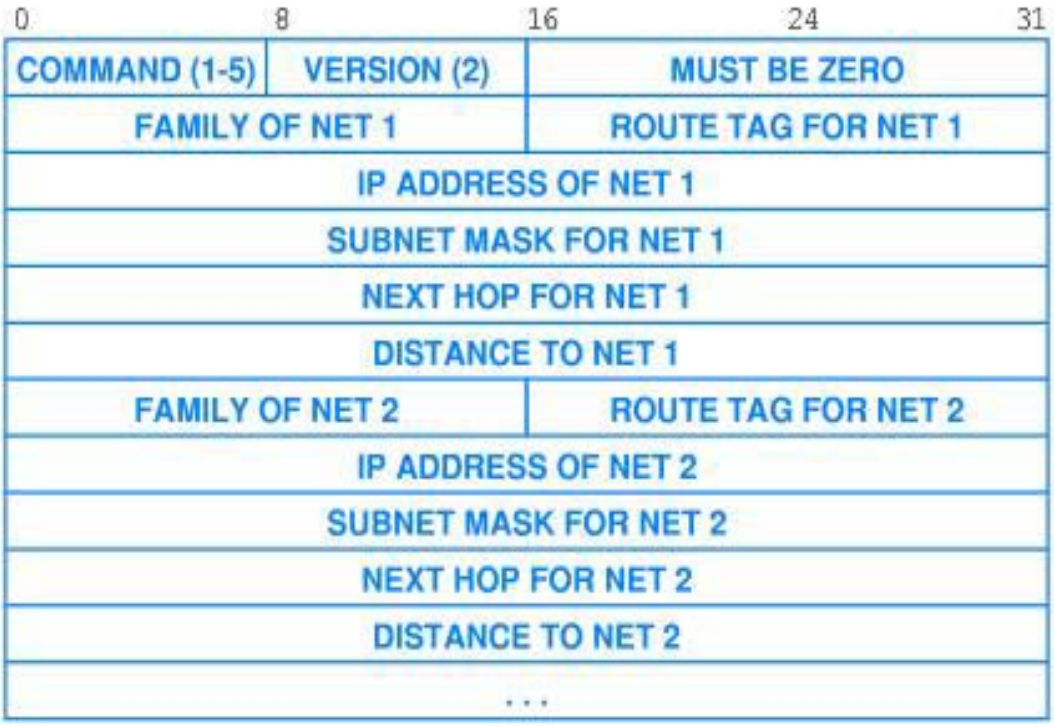
"RIP allows hosts to listen passively and update its routing table

Lecture No. 42

IP ROUTING (Part-4)

ILLUSTRATION OF RIP PACKET FORMAT:

The format of a RIP version 2 update messages is shown in the figure below. The message contains a list of destinations and a distance to each. RIP measures distance in hops.



THE OPEN SHORTEST PATH FIRST PROTOCOL (OSPF):

As the internet grew in size, so did organizations. In particular, large ISPs appeared. To satisfy demand for a routing protocol that can scale to large organizations, the IETF devised an IGP known as the Open Shortest Path First Protocol (OSPF).

THE CHARACTERISTICS OF OSPF:

OSPF has following characteristics:

"ROUTING WITHIN AN AUTONOMOUS SYSTEM:

OSPF has designed as an Interior Gateway Protocol used to pass routing information among routers within an autonomous system.

"FULL CIDR AND SUBNET SUPPORT:

OSPF includes a 32-bit address mask with each address, which allows the address to be classful, classless, or subnetted.

"AUTHENTICATED MESSAGE EXCHANGE:

A pair of routers using OSPF can authenticate each message to ensure that messages are only accepted from a trusted source.

"IMPORTED ROUTES:

OSPF allows a router to introduce routes learned from another means (e.g., from BGP).

"LINK-STATE ALGORITHM:

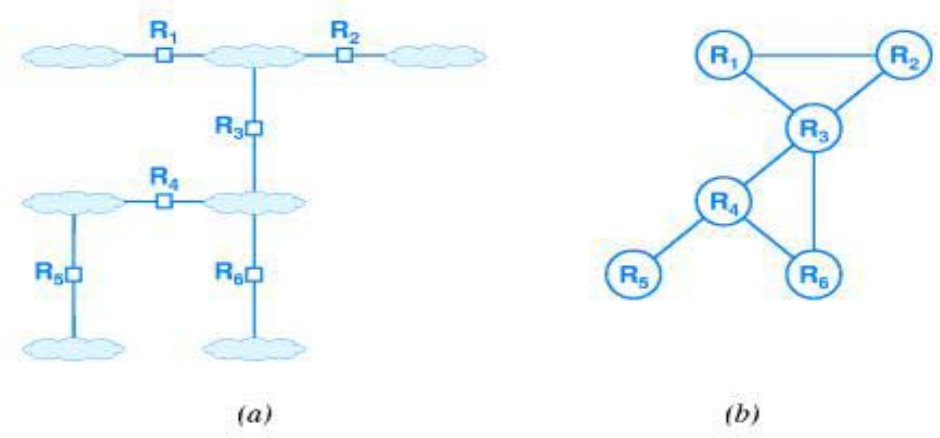
OSPF uses link-state routing.

"SUPPORT FOR MULTI-ACCESS NETWORKS:

Traditional link state routing is inefficient across a multi-access network, such as an Ethernet, because all routers attached to the network broadcast link status. OSPF optimizes by designing a single router to broadcast on the network.

OSPF GRAPH:

Networks and Routers can be illustrated using OSPF graph. Routers correspond to nodes in OSPF graph. Networks correspond to edges. The adjacent pair of routers periodically test connectivity and broadcast link-status information to area. Each router uses link-status messages to compute shortest paths. An internet consisting of seven networks interconnected by routers is shown in the figure below. A corresponding OSPF graph is also shown in figure b. In the simplest case; each router corresponds to a node in the graph.



OSPF AREAS:

Long Q

OSPF allows subdivision of Autonomous System into areas. The link-status information is propagated within an area. The routes are summarized before being propagated to another area. It reduces overhead (less broadcast traffic). Because it allows a manager to partition the routers and networks in an autonomous system into multiple areas, OSPF can scale to handle a larger number of routers than other IGPs.

Lecture No. 43

IP ROUTING (Part-5)

INTERNET MULTICAST ROUTING:

Long Q

Internet multicast routing is difficult because internet multicast allows arbitrary computer to join multicast group at any time. It allows arbitrary member to leave multicast group at any time. It also allows arbitrary computer to send message to a group (even if not a member).

IP MULTICAST SEMANTICS:

IP multicast group is anonymous in two ways:

1. Neither a sender nor a receiver knows the identity or the number of group members.

2. Routers and hosts do not know which applications will send a datagram to a group.

IGMP:

How host join and leave the group?

Long Q

A standard protocol exists that allows a host to inform a nearby router whenever the host needs to join or leave a particular multicast group known as Internet Group Multicast Protocol (IGMP). The computer uses IGMP to inform the local router about the last application when it leaves.

FORWARDING AND DISCOVERY TECHNIQUES:

Routers not hosts have responsibility for the propagation of multicast routing information. The size and topology of groups may vary e.g. Teleconferencing often creates small groups and on the other side web casting can create a large group.

APPROACHES FOR DATAGRAM FORWARDING:

In practice multicast protocols have followed three different approaches for datagram forwarding:

FLOOD-AND-PRUNE:

Flood-and-prune is ideal in a situation where the group is small and all members are attached to contiguous Local Area Networks. To avoid routing loops, flood-and-prune protocols use a technique known as Reverse Path Broadcasting (RPB) that breaks cycles.

CONFIGURATION-AND-TUNNELING:

Configuration-and-tunneling is ideal in a situation where the group is geographically dispersed (i-e., has a few members at each site, with sites separated by long distances). When a multicast datagram arrives, the routers at a site transmit the datagram on all directly attached LANs via hardware multicast. The router then consults its configuration table to determine which other sites should receive a copy. The router uses IP-in-IP tunneling to transfer a copy of the multicast datagram to other sites.

CORE-BASED DISCOVERY:

To provide smooth growth, some multicast routing protocols designate a core unicast address for each multicast group. Whenever a router R1 needs to reach a group, R1 sends a datagram to the groups core address. As the datagram travels through the Internet, each router examines the contents. When the datagram reaches a router R2 that participates in the group, R2 removes and processes the message. If the message contains a multicast datagram switch a destination address equal to the group_s address, R2 forwards the datagram to members of the group. If the message contains a request to join the group, R2 adds the information to its routes, and then uses IP-in-IP to forward a copy of each multicast datagram to R1. Thus the set of routers participating in a multicast group grows from the core outward. In graph theoretic terms, the set forms a tree.

Lecture No. 44

IP ROUTING (Part-6)

Names of multicast routing protocols?

Long Q

MULTICAST PROTOCOLS:

Several multicast protocols exist. Some of the proposed protocols are:

DISTANCE VECTOR MULTICAST ROUTING PROTOCOL (DVMRP):

This protocol is used by the Unix program *mrouted* and the Internet *Multicast backBONE* (MBONE). DVMRP performs local multicast and uses IP-in-IP encapsulation to send multicast datagrams from one site on the Internet to another.

CORE BASED TREES (CBT):

A multicast routing scheme in which the protocol software builds a delivery tree from a central point. When a user joins a group, routers send a message toward the central point (i.e., the core) to search for the nearest participating router.

Long Q

PROTOCOL INDEPENDENT MULTICAST_ *SPARSE MODE (PIM-SM):*

This is a protocol that uses the same approach as CBT to form a multicast routing tree. The designers chose the term protocol independent to emphasize that although unicast datagrams are used to contact remote destinations when establishing multicast forwarding. PIM-SM does not depend on any particular unicast routing protocol.

PROTOCOL INDEPENDENT MULTICAST _ *DENSE MODE (PIM-DM):*

A protocol designed for use within an organization. Routers that use PIM-DM broadcast (i.e. flood) multicast packets to all locations within the organization. Each router that has no member of a particular group sends back a message to prune the multicast routing tree ((i.e., a request to stop the flow of packets). The scheme works well for short-lived multicast sessions (e.g., a few minutes) because it does not require setup before transmission begins.

MULTICAST EXTENSIONS TO THE OPEN SHORTEST PATH FIRST PROTOCOL (MOSPF):

A protocol designed for use within an organization. MOSPF builds on OSPF and reuses many of the same basic concepts and facilities.

None of the above mentioned protocols is best in all circumstances.

CLIENT-SERVER INTERACTION:

Although an internet system provides basic communication service, the protocol software cannot initiate contact with, or accept contact from, a remote computer. Instead two application programs must participate in any communication i.e. one application initiates communication and the other accepts it.

HOW TWO APPLICATION PROGRAMS MAKE CONTACT?

The two application programs make contact in the following way:

One application actively begins execution first and another application waits passively at prearranged location. This process is called client-server interaction.

Long Q

CLIENT-SERVER PARADIGM:

It is used by all network applications. The passive program is called a server and the active program is called a client.

CHARACTERISTICS OF A CLIENT:

The characteristics of a client are explained below:

"Client is an arbitrary application program.

"It becomes client temporarily.

"It can also perform other computations.

Long Q

"It is invoked directly by the user.

"It runs locally on the user's computer.

"It actively initiates contact with a server.

"It contacts one server at a time.

CHARACTERISTICS OF A SERVER:

The characteristics of a server are explained below:

"It is a special-purpose, privileged program.

"It is dedicated to provide one service.

Long Q

"It can handle multiple remote clients simultaneously.

"It invoked automatically when system boots.

"It executes forever.

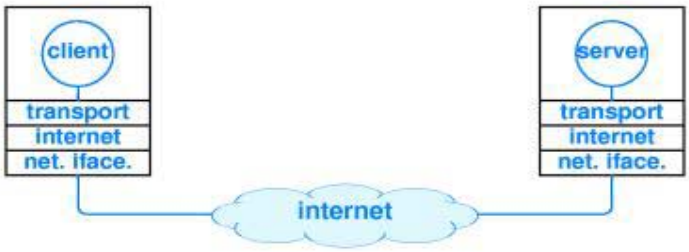
"It needs powerful computer and operating system.

"It waits for client contact.

"It accepts requests from arbitrary clients.

TRANSPORT PROTOCOLS AND CLIENT-SERVER NTERACTION

Like most application programs, a client and server use a transport protocol to communicate. For example, the figure below illustrates a client and server using the TCP/IP stack.



In the figure, a client and server using TCP/IP protocols to communicate across an Internet are shown. The client and server each interact with a protocol in the transport layer.

Lecture No. 45

COURSE REVISION

COURSE SUMMARY

(This lecture contains the summary of the topics that were covered during the course.)

SYLLABUS FOR FINALS:

The syllabus of the course is given as follows:

PACKET TRANSMISSION:

- Packets, Frames and Error Detection
- LAN Technologies and Network Topologies
- Hardware Addressing and Frame Type Identification
- LAN Wiring, Physical Topology, And Interface Hardware
- Extending LANs
- WAN Technologies and Routing
- Connection-Oriented Networking and ATM
- Network Characteristics

INTERNETWORKING:

- Internetworking Concepts, Architecture and Protocols
- IP Addressing
- Binding Protocol Addresses (ARP)
- IP Datagrams and Datagram Forwarding
- IP Encapsulation, Fragmentation and Reassembly
- UDP: Datagram Transport Service
- TCP: Reliable Transport Service
- Internet Routing

PACKET TRANSMISSION

In this portion, following chapters were covered. The topics are also given below:

PACKETS, FRAMES AND ERROR DETECTION

- The Concepts of Packets
- Packets and Time-Division Multiplexing
- Packets and Hardware Frames
- Byte Stuffing
- Transmission Errors
- Parity Bits and Parity Checking
- Probability, Mathematics, and Error Detection
- Detecting Errors with Checksums
- Detecting Errors with Cyclic Redundancy Checks
- Combining Building Blocks
- Burst Errors
- Frame Format and Error Detection Mechanisms

LAN TECHNOLOGY AND NETWORK TOPOLOGY

- Direct Point-to-Point Communication
- Shared Communication Channels
- Significance of LANs and Locality of Reference
- LAN Topologies
    - Star Topology
    - Ring Topology
    - Bus Topology
- Example Bus Network: Ethernet
- Carrier Sense on Multi-Access Networks (CSMA)
- Collision Detection and Backoff with CSMA/CD
- 802.11 Wireless LANs and CSMA/CA
- Local Talk
- IBM Token Ring
- FDDI
- ATM

HARDWARE ADDRESSING AND FRAME TYPE DENTIFICATION

- How LAN Hardware uses Addresses to Filter Packets
- Format of a Physical Address
- Broadcasting
- Multicasting
- Multicast Addressing
- Identifying Packet Contents
- Frame Headers and Frame Format
- Network Analyzers, Physical Addresses, Frame Types

LAN WIRING, PHYSICAL TOPOLOGY, AND INTERFACE HARDWARE

- Speeds of LANs and Computers
- Network Interface Hardware
- Original Thick Ethernet Wiring
- Connection Multiplexing
- Thin Ethernet Wiring
- Twisted Pair Ethernet
- Advantages and Disadvantages of Wiring Schemes
- The Topology Paradox
- Network Interface Cards and Wiring Schemes
- 10/100 Network Interfaces
- Categories of Wires
- Wiring Schemes and Other Network Technologies

EXTENDING LANs: FIBER MODEMS, REPEATERS, BRIDGES, AND SWITCHES

- Distance Limitation and LAN Design
- Fiber Optic Extensions
- Repeaters
- Bridges
- Frame Filtering
- Planning a Bridged Network
- Bridging Between Buildings
- Bridging across Longer Distances

- A Cycle of Bridges
- Distributed Spanning Tree
- Switching
- Combining Switches and Hubs
- Bridging and Switching with Other Technologies

WAN TECHNOLOGIES AND ROUTING

- Large Networks and Wide Areas
- Packet Switches
- Forming A WAN
- Store and Forward
- Physical Addressing in a WAN
- Next-Hop Forwarding
- Source Independence
- Relationship of Hierarchical Addresses to Routing
- Routing in a WAN
- Use of Default Routes
- Routing Table Computation
- Shortest Path Computation in a Graph
- Distributed Route Computation
- Distance Vector Routing
- Link-State Routing (SPF)
- Example WAN Technologies
    - ARPANET
    - FRAME RELAY
    - SMDS
    - ATM

CONNECTION-ORIENTED NETWORKING AND ATM

- A Single Global Network
- ISDN and ATM
- ATM Design and Cells
- Connection-Oriented Service
- VPI/VCI
- Labels and Label Switching
- Permanent Virtual Circuits
- Switched Virtual Circuits
- Quality of Service
- The Motivation for Cells and Label Switching

- ATM Data Transmission and AAL5
- Critique of ATM

NETWORK CHARACTERISTICS: OWNERSHIP, SERVICE PARADIGM AND PERFORMANCE

- Network Ownership
- Privacy and Public Networks
- Advantages and Disadvantages
- Virtual Private Networks
- Guaranteeing Absolute Privacy
- Service Paradigm
- Connection-Oriented Service Paradigm
- Connectionless Service Paradigm
- Interior and Exterior Service Paradigm
- Comparison of Service Paradigm
- Addresses of Connection Identifiers
- Network Performance Characteristics
    - Delay
    - Throughput
- Jitter

INTERNETWORKING

In this portion the following chapters were covered. The topics are also given below:

INTERNETWORKING: CONCEPTS, ARCHITECTURE, AND PROTOCOLS

- The Motivation for Internetworking
- The Concept of Universal Service
- Universal Service in a Heterogeneous World
- Internetworking
- Physical Network Connection with Routers
- Internet Architecture
- Achieving Universal Service
- A Virtual Network
- Protocols for Internetworking
- Layering and TCP/IP Protocols
- Host Computers, Routers and Protocol Layers

IP: INTERNET PROTOCOL ADDRESSES

- Addresses for the Virtual Internet
- The IP Addressing Scheme
- The IP Address Hierarchy
- Original Classes of IP Addresses
- Computing the Class of an Address
- Dotted Decimal Notation
- Classes and Dotted Decimal Notation
- Division of the Address Space
- Authority for Addresses
- A Classful Addressing Example
- Subnet and Classless Addressing
- Address Masks
- CIDR Notation
- A CIDR Address Block Example
- CIDR Host Addresses
- Special IP Addresses
- The Berkeley Broadcast Address Form
- Routers and the IP Addressing Principle
- Multi-Homed Hosts

BINDING PROTOCOL ADDRESSES (ARP)

- Protocol Addresses and Packet Delivery
- Address Resolution
- Address Resolution Techniques
- Address Resolution with Table Lookup
- Address Resolution with Closed-Form Computation
- Address Resolution with Message Exchange
- Address Resolution Protocol
- ARP Message Delivery
- ARP Message Format
- Sending an ARP Message
- Identifying ARP Frames
- Caching ARP Responses
- Processing an Incoming ARP Message
- Layering, Address Resolution, Protocol Addresses

IP DATAGRAMS AND DATAGRAM FORWARDING

- Connectionless Service
- Virtual Packets
- The IP Datagram
- Forwarding an IP Datagram
- IP Addresses and Routing Table Entries
- The Mask Field and Datagram Forwarding
- Destination and Next-Hop Addresses
- Best-Effort Delivery
- The IP Datagram Header Format

IP ENCAPSULATION, FRAGMENTATION, AND REASSEMBLY

- Datagram Transmission and Frames
- Encapsulation
- Transmission across an Internet
- MTU, Datagram Size, and Encapsulation
- Reassembly
- Identifying a Datagram
- Fragment Loss
- Fragmenting a Fragment

THE FUTURE IP (IPv6)

- The Success of IP
- The Motivation for change
- A Name and a Version Number
- IPv6 Datagram Format
- IPv6 Base Header Format
- How IP v6 handles Multiple Headers
- Fragmentation, Reassembly, and Path MTU
- The Purpose of Multiple Headers
- IPv6 Addressing
- IPv6 Colon Hexadecimal Notation

UDP: DATAGRAM TRANSPORT SERVICE

- Need for End-to-End Transport Protocols
- The User Datagram Protocol
- Connection-less Paradigm
- Message Oriented Interface
- UDP Communication Semantics
- Arbitrary Interaction
- End Point Identification with Protocol Port Numbers
- UDP Datagram Format

TCP: RELIABLE TRANSPORT SERVICE

- The Need for Reliable Transport
- The Transmission Control Protocol
- The Service TCP Provides to Applications
- End-To-End Service and Datagrams
- Achieving Reliability
- Packet Loss and Retransmission Times
- Adaptive Retransmission
- Buffers, Flow Control, and Windows
- Three-Way Handshake
- Congestion Control
- TCP Segment Format

INTERNET ROUTING

- Static Vs Dynamic Routing
- Static Routing In Hosts and a Default Route
- Dynamic Routing and Routers
- Routing in the Global Internet
- Autonomous System Concept
- The Two Types of Internet Routing Protocols (IGP & EGP)
- Routes and Data Traffic
- Border Gateway Protocol (BGP)
- The Routing Information Protocol (RIP)
- RIP Packet Format

- The Open Shortest Path First Protocol (OSPF)
- An Example OSPF Graph
- OSPF Areas
- Multicast Routing