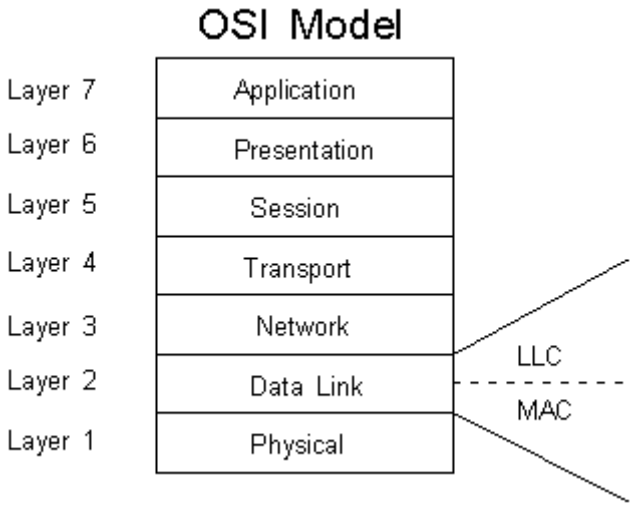
MAC Sublayer [RGPV JUNE 2011]

In the seven-layer OSI model of computer networking, **media access control** (**MAC**) data communication protocol is a sublayer of the data link layer (layer 2). The MAC sublayer provides addressing and channel access control mechanisms that make it possible for several terminals or network nodes to communicate within a multiple access network that incorporates a shared medium, e.g.Ethernet. The hardware that implements the MAC is referred to as a *media access controller*.

The MAC sublayer acts as an interface between the logical link control (LLC) sublayer and the network's physical layer. The MAC layer emulates a full-duplex logical communication channel in a multi-point network. This channel may
provide unicast, multicast orbroadcast communication service.



MAC Addressing (Media Access Control address)

In a local area network (LAN) or other network, the MAC (Media Access Control) address is your computer's unique hardware number.

In a local area network (LAN) or other network, the MAC (Media Access Control) address is your computer's unique hardware number. (On an Ethernet LAN, it's the same as your Ethernet address.) When you're connected to the Internet from your computer (or host as the Internet protocol thinks of it), a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN.

What Is a MAC Address?

The MAC address is a unique value associated with a network adapter. MAC addresses are also known as **hardware** addresses or **physical** addresses. They uniquely identify an adapter on a LAN.

MAC addresses are 12-digit hexadecimal numbers (48 bits in length). By convention, MAC addresses are usually written in one of the following two formats:

MM:MM:MM:SS:SS:SS

MM-MM-MM-SS-SS-SS

The first half of a MAC address contains the ID number of the adapter manufacturer. These IDs are regulated by an Internet standards body (see sidebar). The second half of a MAC address represents the serial number assigned to the adapter by the manufacturer. In the example,

00:A0:C9:14:C8:29

The prefix

00A0C9

indicates the manufacturer is Intel Corporation.

Why MAC Addresses?
Recall that TCP/IP and other mainstream networking architectures generally adopt the OSI model. In this model, network functionality is subdivided into layers. MAC addresses function at the data link layer (layer 2 in the OSI model). They allow computers to uniquely identify themselves on a network at this relatively low level.

MAC vs. IP Addressing
Whereas MAC addressing works at the data link layer, IP addressing functions at the network layer (layer 3). It's a slight oversimplification, but one can think of IP addressing as supporting the software implementation and MAC addresses as supporting the hardware implementation of the network stack. The MAC address generally remains fixed and follows the network device, but the IP address changes as the network device moves from one network to another.

IP networks maintain a mapping between the IP address of a device and its MAC address. This mapping is known as the **ARP cache** or **ARP table**. ARP, the Address Resolution Protocol, supports the logic for obtaining this mapping and keeping the cache up to date.
DHCP also usually relies on MAC addresses to manage the unique assignment of IP addresses to devices.

Binary Exponential Back-off (BEB) Algorithm

In a variety of computer networks, **binary exponential backoff** or **truncated binary exponential backoff** refers to an algorithm used to space out repeated retransmissions of the same block of data, often as part of network congestion avoidance.

Examples are the retransmission of frames in carrier sense multiple access with collision

avoidance (CSMA/CA) and carrier sense multiple access with collision detection(CSMA/CD) networks, where this algorithm is part of the channel access method used to send data on these networks. In Ethernet networks, the algorithm is commonly used to schedule retransmissions after collisions. The retransmission is delayed by an amount of time derived from the slot time and the number of attempts to retransmit.

After *c* collisions, a random number of slot times between 0 and 2^c - 1 is chosen. For the first collision, each sender will wait 0 or 1 slot times. After the second collision, the senders will wait anywhere from 0 to 3 slot times (inclusive). After the third collision, the senders will wait anywhere from 0 to 7 slot times (inclusive), and so forth. As the number of retransmission attempts increases, the number of possibilities for delay increases exponentially.

The 'truncated' simply means that after a certain number of increases, the exponentiation stops; i.e. the retransmission timeout reaches a ceiling, and thereafter does not increase any further. For example, if the ceiling is set at $i = 10$ (as it is in the IEEE 802.3 CSMA/CD standard), then the maximum delay is 1023 slot times.

Because these delays cause other stations that are sending to collide as well, there is a possibility that, on a busy network, hundreds of people may be caught in a single collision set. Because of this possibility, the process is aborted after 16 attempts at transmission.

Lecture-2

Distributed Random Access Schemes/Contention Schemes: for Data Services (ALOHA and Slotted ALOHA)

ALOHA: ALOHA is a system for coordinating and arbitrating access to a shared communication Networks channel. It was developed in the 1970s by Norman Abramson and his colleagues at the University of Hawaii. The original system used for ground based radio broadcasting, but the system has been implemented in satellite communication systems.
A shared communication system like ALOHA requires a method of handling collisions that occur when two or more systems attempt to transmit on the channel at the same time. In the ALOHA system, a node transmits whenever data is available to send. If another node transmits at the same time, a collision occurs, and the frames that were transmitted are lost. However, a node can listen to broadcasts on the medium, even its own, and determine whether the frames were transmitted.

Aloha means "Hello". Aloha is a multiple access protocol at the datalink layer and proposes how multiple terminals access the medium without interference or collision. In 1972 Roberts developed a protocol that would increase the capacity of aloha two fold. The Slotted Aloha protocol involves dividing the time interval into discrete slots and each slot interval corresponds to the time period of one frame. This method requires synchronization between the sending nodes to prevent collisions.

There are two different versior.s/types of ALOHA:

(i) Pure ALOHA

(ii) Slottecl ALOHA

(i) Pure ALOHA

• **In** pure ALOHA, the stations transmit frames whenever they have data to send.

• When two or more stations transmit simultaneously, there is collision and the frames are destroyed.

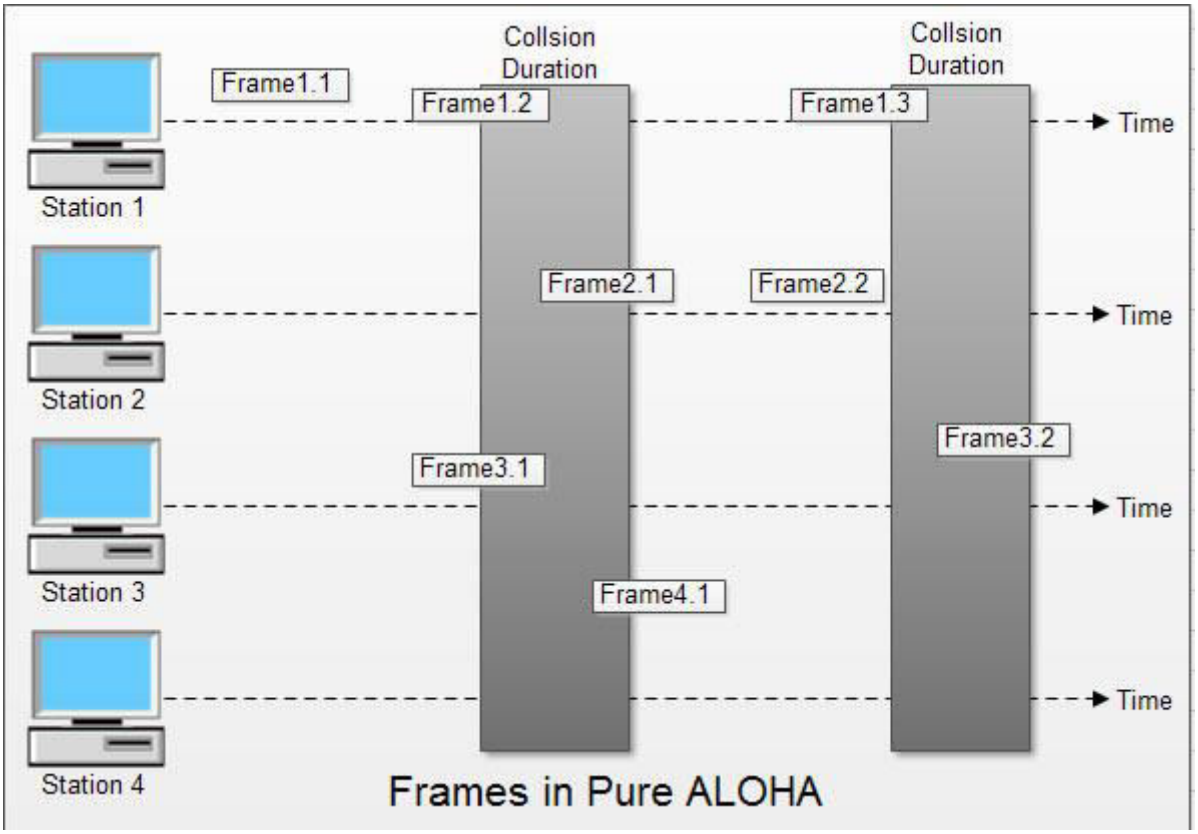
• In pure ALOHA, whenever any station transmits a frame, it expects the acknowledgement from the receiver.

• If acknowledgement is not received within specified time, the station assumes that the frame (or acknowledgement) has been destroyed.

• If the frame is destroyed because of collision the station waits for a random amount of time and sends it again. This waiting time must be random otherwise same frames will collide again and again.

• Therefore pure ALOHA dictates that when time-out period passes, each station must wait for a random amount of time before resending its frame. This randomness will help avoid more collisions.

• Figure shows an example of frame collisions in pure ALOHA.



In fig there are four stations that .contended with one another for access to shared channel. All these stations are transmitting frames. Some of these frames collide because multiple frames are in contention for the shared channel. Only two frames, frame 1.1 and frame 2.2 survive. All other frames are destroyed.

• Whenever two frames try to occupy the channel at the same time, there will be a collision and both will be damaged. If first bit of a new frame overlaps with just the last bit of a frame almost finished, both frames will be totally destroyed and both will have to be retransmitted.

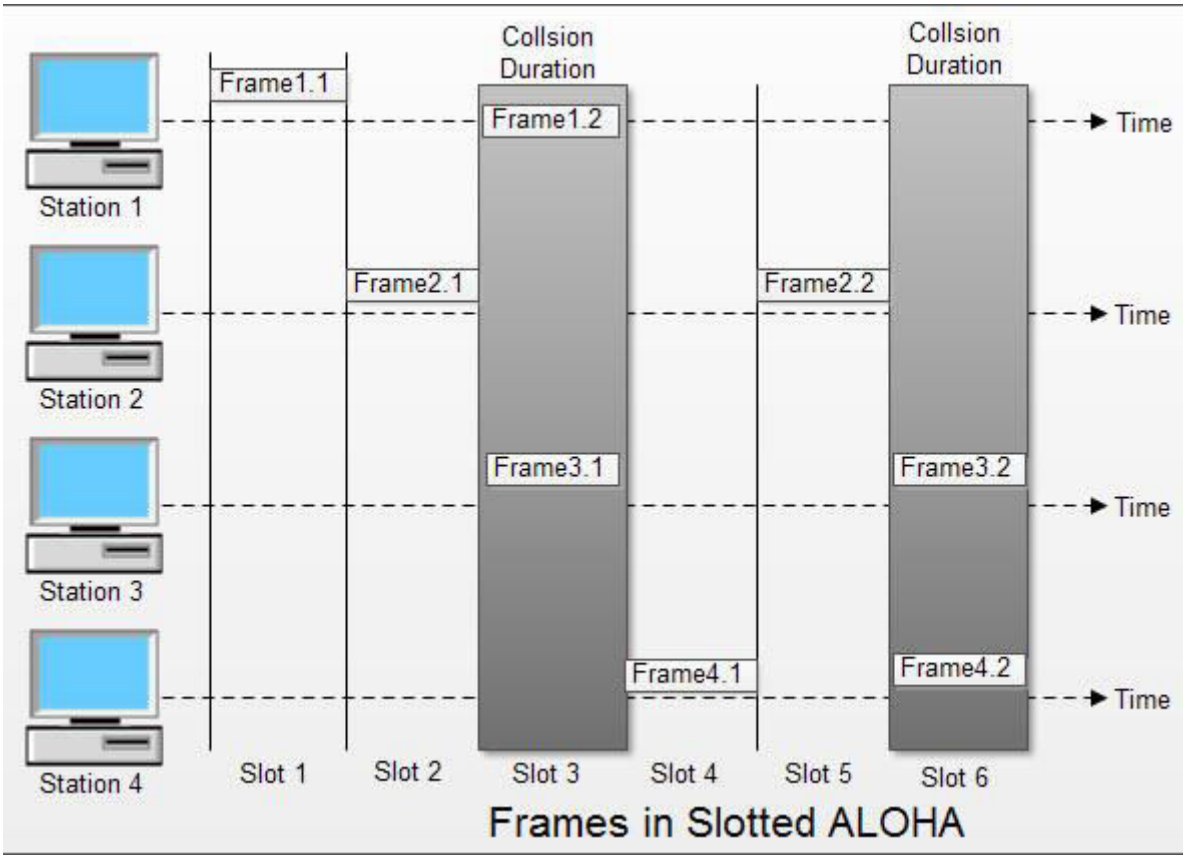
(ii) Slotted ALOHA

• Slotted ALOHA was invented to improve the efficiency of pure ALOHA as chances of collision in pure ALOHA are very high.

• In slotted ALOHA, the time of the shared channel is divided into discrete intervals

called slots.

• The stations can send a frame only at the beginning of the slot and only one frame is sent in each slot.



In slotted ALOHA, if any station is not able to place the frame onto the channel at the beginning of the slot *i.e.* it misses the time slot then the station has to wait until the beginning of the next time slot.

• In slotted ALOHA, there is still a possibility of collision if two stations try to send at the beginning of the same time slot as shown in fig.

• Slotted ALOHA still has an edge over pure ALOHA as chances of collision are reduced to one-half.

Lecture-3

For Local-Area Networks (CSMA, CSMA/CD, CSMA/CA) [RGPV DEC 2012]

Carrier sense multiple access (**CSMA**) is a probabilistic media access control (MAC) protocol in which a node verifies the absence of other traffic before transmitting on a shared transmission medium, such as an electrical bus, or a band of the electromagnetic spectrum.

Carrier sense means that a transmitter uses feedback from a receiver to determine whether another transmission is in progress before initiating a transmission. That is, it tries to detect the presence of a carrier wave from another station before attempting to transmit. If a carrier is sensed, the station waits for the transmission in progress to finish before initiating its own transmission. In other words, CSMA is based on the principle "sense before transmit" or "listen before talk".

Multiple access means that multiple stations send and receive on the medium. Transmissions by one node are generally received by all other stations connected to the medium.

CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance) is a protocolfor carrier transmission in 802.11 networks. Unlike CSMA/CD (Carrier Sense Multiple Access/Collision Detect) which deals with transmissions after a collision has occurred, CSMA/CA acts to prevent collisions before they happen.

CSMA/CD - Carrier Sense Multiple Access / Collision Detection

Short for **C***arrier* **S***ense* **M***ultiple* **A***ccess* **/ C***ollision* **D***etection,* a set of rules determining how network devices respond when two devices attempt to use a data channel simultaneously (called a*collision*). Standard Ethernet networks use CSMA/CD to physically monitor the traffic on the line at participating stations. If no transmission is taking place at the time, the particular station can transmit. If two stations attempt to transmit simultaneously, this causes a collision, which is detected by all participating stations. After a random time interval, the stations that collided attempt to transmit again. If another collision occurs, the time intervals from which the random waiting time is selected are increased step by step. This is known as exponential back off.

CSMA/CD is a type of contention protocol. Networks using the CSMA/CD procedure are simple to implement but do not have deterministic transmission characteristics. The CSMA/CD method is internationally standardized inIEEE 802.3 and ISO 8802.3.

CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance

Short for ***C****arrier* ***S****ense* ***M****ultiple* ***A****ccess/****C****ollision* ***A****voidance*,
network contention protocol that listens to a network in order to avoid collisions,
unlike CSMA/CD that deals with network transmissions once collisions have been detected.
CSMA/CA contributes to network traffic because, before any real data is transmitted, it has to broadcast a signal onto the network in order to listen for collision scenarios and to tell other devices not to broadcast.

What is CSMA/CA?

The Carrier-Sense Multiple Access/Collision Avoidance (*CSMA/CA*) access method, as the name indicates, has several characteristics in common with CSMA/CD. The difference is in the last of the three components: Instead of *detecting* data collisions, the CSMA/CA method attempts to avoid them altogether.

Although it sounds good in theory, the method it uses to do this causes some problems of its own, which is one reason CSMA/CA is a far less popular access method than CSMA/CD.

How CSMA/CA works?

On a network that uses the CSMA/CA access method, when a computer has data to transmit, its NIC first checks the cable to determine if there is already data on the wire. So far, the process is identical to CSMA/CD.

However, if the NIC senses that the cable is not in use, it still does not send its data packet. Instead, it sends a signal of intent--indicating that it is about to transmit data--out onto the cable.

Lecture-4

Collision Free Protocols: Basic Bit Map, BRAP, Binary Count Down

Collision Free Protocols

A collision-free protocol for transmitting frames between stations connected over a shared transmission medium such as an IEEE 802.3 Ethernet LAN. A logical ring is formed and a token is circulated among the connected stations part of the logical ring (not all connected stations are required to be part of the logical ring). Transmitting from any one station, part of the logical ring, is permitted only while holding the token, therefore preventing collisions. A collision-free protocol, over a standard Ethernet infrastructure, becomes feasible, yet remains compatible with the standard collision protocol, thus improving performances.

Basic Bit Map

This is how the Basic Bit-Map Protocol works.

1. Assume N stations are numbered from 1 to N.
2. There is a contention period of N slots (bits).
3. Each station has one slot time during the contention period, numbered 1 to N.
4. Station J sends a 1-bit reservation during Jth slot time if it wants to transmit a frame.
5. Every station sees all the 1-bit reservation transmitted during the contention period, so each station knows which stations want to transmit.
6. After the contention period, each station that asserted its desire to transmit sends its frame in the order of station number.

BRAP

Backup Route Aware Routing Program (BRAP) is a protocol that provides interdomain routing. BRAP uses reverse paths and backup paths to ensure fast failure recovery in networking systems.

Binary Count Down

One problem with Basic Bit-Map Protocol is that the overhead is 1 bit per frame per station. We can do better by using binary station addresses.

- A station wanting to use the channel now broadcasts its address as a binary bit string in serial fashion.
- As soon as a station sees that a high-order bit position that is 0 in its address has been overwritten by a 1, it gives up (meaning some high order station wants to transmit).
- The remaining stations keep sending their addresses on the network, until a winner merges.

- The wining station sends out the frame. The bidding process repeats.

For exapmle, if stations 0010, 0100, 1001, and 1010 are all trying to get the channel, in the first bit time the four stations transmit 0, 0, 1, and 1, respectively. These are ORed together resulting in a 1. Stations 0010 and 0100 see the 1 and know that a higher-numbered station is competing for the channel, so they give up for the current round. Stations 1001 and 1010 continue. The next bit sent from both stations is 0, both continues. The next bit is 1, so station 1001 gives up. The winner is 1010. This station transmits its frame. Then a new bidding process begins. The channel efficiency is now $d/(d + ln\ N)$

Lecture-5

MLMA Limited Contention Protocols: Adaptive Tree Walk

Under conditions of light load, contention is preferable due to its low delay. As the load increases, contention becomes increasingly less attractive, because the overload associated with channel arbitration becomes greater. Just the reverse is true for contention - free protocols. At low load, they have high delay, but as the load increases , the channel efficiency improves rather than getting worse as it does for contention protocols.

Obviously it would be better if one could combine the best properties of the contention and contention - free protocols, that is, protocol which used contention at low loads to provide low delay, but used a cotention-free technique at high load to provide good channel efficiency. Such protocols do exist and are called Limited contention protocols.

It is obvious that the probablity of some station aquiring the channel could only be increased by decreasing the amount of competition. The limited contention protocols do exactly that. They first divide the stations up into (not necessarily disjoint) groups. Only the members of group 0 are permitted to compete for slot 0. The competition for aquiring the slot within a group is contention based. If one of the members of that group succeeds, it aquires the channel and transmits a frame. If there is collision or no node of a particular group wants to send then the members of the next group compete for the next slot. The probablity of a particular node is set to a particular value (optimum).

Adaptive Tree Walk Protocol

The following is the method of adaptive tree protocol. Initially all the nodes are allowed to try to aquire the channel. If it is able to aquire the channel, it sends its frame. If there is collision then the nodes are divided into two equal groups and only one of these groups compete for slot 1. If one of its member aquires the channel then the next slot is reserved for the other group. On the other hand, if there is a collision then that group is again subdivided and the same process is followed. This can be better understood if the nodes are thought of as being organised in a binary tree .

What is MLMA protocol?

Multi-Level Multi-Access (MLMA): The problem with BRAP is the delay when the channel is lightly loaded. When there is no frame to be transmitted, the N-bit headers just go on and on until a station inserts a 1 into its mini slot. On average, the waiting time would be N=2. MLAM scheme [41] is nearly as efficient under high channel load, but has shorter delay under low channel load. In MLAM, a station wants to transmit a frame sends its identification in a particular format. A group of 10 bits (called decade) is used to represent a digit of the station number [48].

Lecture-6

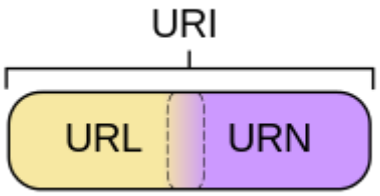
URN Protocol

Uniform resource name

In computing, a uniform resource name (URN) is the historical name for a uniform resource identifier (URI) that uses the urn scheme. A URI is a string of characters used to identify a name of a web resource. Such identification enables interaction with representations of the web resource over a network, typically the World Wide Web, using specific protocols.

URNs were intended to serve as persistent, location-independent identifiers, allowing the simple mapping ofnamespaces into a single URN namespace.[1] The existence of such a URI does not imply availability of the identified resource, but such URIs are required to remain globally unique and persistent, even when the resource ceases to exist or becomes unavailable.

Since RFC 3986[2] in 2005, the use of the term has been deprecated in favor of the less-restrictive "URI", a view proposed by a joint working group between the World Wide Web Consortium (W3C) and Internet Engineering Task Force (IETF). Both URNs and uniform resource locators (URLs) are URIs, and a particular URI may be a name and a locator at the same time.URNs were originally intended in the 1990s to be part of a three-part information architecture for the Internet, along with URLs anduniform resource characteristics (URCs), a metadata framework. However, URCs never progressed past the conceptual stage, and other technologies such as the Resource Description Framework later took their place.



(**U**niform **R**esource **N**ame) A name that identifies a resource on the Internet. Unlike URLs, which use network addresses (domain, directory path, file name), URNs use regular words that are protocol and location independent. Providing a higher level of abstraction, URNs are persistent (never change) and require a resolution service similar to the DNS system in order to convert names into real addresses. For the most part, URNs have evolved into XRI identifiers (see XDI). See URI and URL.

Lecture-7

High Speed LAN: Fast Ethernet, Gigabit Ethernet

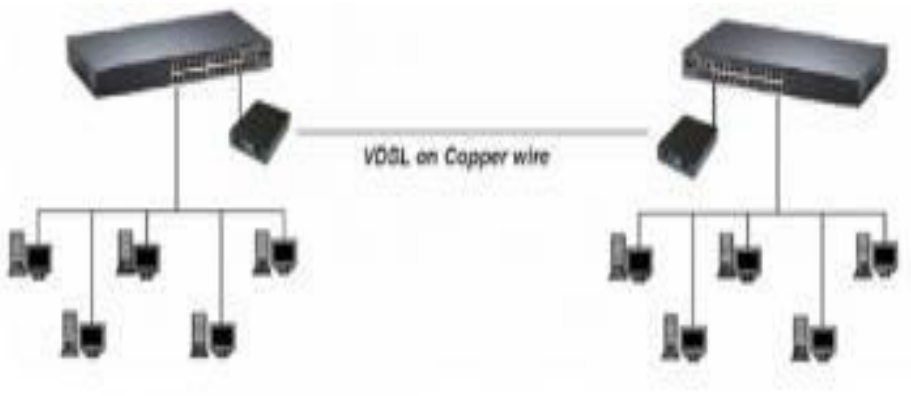
What is high speed LAN?

Most modern local networks use cables, adaptors and connecting devices that can communicate at a maximum speed of 100Mbits/sec (quick enough - in theory - to move an 8Mb file from one computer to another in 1 second).

This is a high speed LAN. There is a newer standard of network which has a maximum speed of 1000Mbits/sec (x10 speed), which requires new adaptors and hardware.

HCL VM -10 - Very High Speed LAN Extender

HCL VM -10 LAN Extender is a Long Reach Ethernet media converter with one Ethernet port (RJ-45 connector) and one VDSL port (RJ-11 connector) This model is a bridge mode modem, well accommodating VDSL2 (Very-high-data-rate Digital Subscribe Loop) technologies to extend Ethernet service over single-pair phone line. Supporting both symmetric and asymmetric transmission, it can reach up to 100/75 Mbps bandwidth (line rate) within 300M or 10/10 Mbps (line rate) for 1 Km long range connections. By providing ultra-high speed, HCL VM -10 LAN Extender makes your telephone line achieve its best performance than before. It has the advantage of minimum installation time (simply as plug-n-play) and minimum expense by allowing video streaming and data to share the same telephone pair without interference.



- Cost effective bridge function to connect two Ethernet LAN
- Support flow control on Fast Ethernet port via PAUSE frame or Back Pressure
- IEEE 802.1Q VLAN tag transparent
- Easy installation via simple plug-and-play

- Selectable CPE and CO mode via DIP switch:
- Two working modes are built in the same unit, which keep the flexibility of installation and easy provision of service but lower inventory of service provider.
- Selectable fast and interleaved mode:
- Fast mode guarantees a minimum end to end latency less than1 ms. Interleaved mode provides impulse noises protection for any impulse noise with a duration less than 250 us, Interleaved mode has a maximum end to end latency of 10 m sec. Interleaved mode is the default mode.
- Selectable target data rate and target SNR margin:
- User has the ability to select fixed SNR margin (9 dB) or fixed target data rate.
- When fixed SNR margin is selected, the systems will maintain the SNR margin at 9 dB across all usable loop length. When fixed target data rate is selected, the system will lock the data rate up to 50 Mbps/30 Mbps whenever the calculated SNR margin is higher than 9 dB. This gives best system stability and is the default mode.

Lecture-8

FDDI [RGPV JUNE 2011]

FDDI (Fiber Distributed Data Interface) is a set of ANSI and ISO standards for data transmission on fiber optic lines in a local area network (LAN) that can extend in range up to 200 km (124 miles). The FDDI protocol is based on the token ring protocol. In addition to being large geographically, an FDDI local area network can support thousands of users. FDDI is frequently used on the backbone for a wide area network (WAN).

Fiber Distributed Data Interface (**FDDI**) is a standard for data transmission in a local area network. It uses optical fiber as its standard underlying physical medium, although it was also later specified to use copper cable, in which case it may be called **CDDI** (Copper Distributed Data Interface), standardized as **TP-PMD** (Twisted-Pair Physical Medium-Dependent), also referred to as TP-DDI (Twisted-Pair Distributed Data Interface).

Performance Measuring Metrics

Network Performance Evaluation

For a given network, one might be interested to know how well it is performing. One might also wish to know what could be done to further improve the performance, or if the network is giving the peak performance. Thus, one needs to do a comparative study of the network by considering different options. This performance evaluation helps the user to determine the suitable network configuration that serves him best.

For example consider a new startup organization which has setup its own web portal. As the portal gradually becomes popular then network traffic increases which would degrade its performance. Therefore, one should have a well configured network with proper load balancing capabilities.

Performance Evaluation Metrics

Before we can proceed with performance evaluation, we must choose the different metrics that would help us in making comparisons. There could be different metrics to determine the performance like throughput, delay, jitter, packet loss. The choice of metric would depend upon the purpose the network has been setup for. The metrics could be related to the different layers of the network stack. For example, TCP throughput is based on the application layer, whereas IP round trip time is based on the network layer. For example, a network supporting multimedia applications should have minimum delay and jitter.Packet loss might not be a critical issue for such network. However, packet loss might be a considerable factor for networks supporting textual data oriented applications, say someone downloading by FTP.

Once the metrics have been chosen, one goes for their quantitative evaluation by subjecting the network under diverse conditions. For example, one could make step by step increments in bandwidth of the links, which in turn improve the throughput. However, the throughput

might get saturated beyond the certain point. That is, further increase in bandwidth would not improve throughput. Thus, the optimum value of bandwidth has been determined.

The table below shows different metrics of evaluation, and categories

Category	Metric	Units
productivity	throughput effective capacity	Mbps
responsiveness	delay round trip time queue size	milliseconds packets
utilization	channel utilization	percentage of time busy
losses	packet loss rate frame retries	loss percentage
buffer problems	AP queue overflow playout buffer underflow	packet drops rebuffer events

- It might not be always possible or feasible to obtain best performance from a network due to various factors like high cost,complexity, compatibility. In such cases one would like to obtain optimum performance by balancing different factors.

Following are some of the performance measurement metrics:

- Latency: It can take a long time for a packet to be delivered across intervening networks. In reliable protocols where a receiver acknowledges delivery of each chunk of data, it is possible to measure this as round-trip time.
- Packet loss: In some cases, intermediate devices in a network will lose packets. This may be due to errors, to overloading of the intermediate network, or to intentional discarding of traffic in order to enforce a particular service level.
- Retransmission: When packets are lost in a reliable network, they are retransmitted. This incurs two delays: First, the delay from re-sending the data; and second, the delay resulting from waiting until the data is received in the correct order before forwarding it up the protocol stack.
- Throughput: The amount of traffic a network can carry is measured as throughput, usually in terms such as kilobits per second. Throughput is analogous to the number of lanes on a highway, whereas latency is analogous to its speed limit.

Parameters Affecting the Performance of a Network

- Different parameters can together or independently determine how well a network would perform. A few such are mentioned below:

- Bandwidth: Its is the maximum data transfer rate which a link allows.It is expressed in bits per second(bps).
- Propagation Delay: It is the amount of time required to for a packet to travel from one node to another.If the propagation delay is high then throughput will be low i.e they are inversely proportional to each other.
- Queue type and queue size: The queue of a node is implemented as a part of a link whose input is that node to handle the overflow at the queue.But if the buffer capacity of the output queue is exceeded then the last packet arrived is dropped.We do set the buffer capacity by using queue size.

Performance Evaluation Techniques

- Before starting with tuning the performance of a network one must remember that the performance, to some extent, depends on the workload as well as the topology. A given topology might give different throughputs under CBR and exponential traffic. Keeping this in mind, one can go for studying an actual network. Otherwise one can simulate its performance using suitable parameters. these simulations would largely depend on queuing theory.

Network Performance Evaluation using NS2

- In this section we discuss how to evaluate performance of a network by simulating it with ns2.

- Choose and generate a network topology to be used throughout the simulation. This could be a wired network, in which case the topology remains fixed. However, for a wireless network with mobile nodes the topology would change with time, or randomly.
- Once the topology has been generated, traffic source(s) and destination(s) are fixed. Assign suitable traffic sources to the source nodes, and traffic sinks to the destination nodes.
- Some of the parameters that can be used for comparative study of performance of the network are: link bandwidth, propagation delay, node queue type. For example: In ns2 we do create a link by using this code:

- 1 $ns simplex-link $n2 $n3 0.3Mb 100ms DropTail
  In this code there could be three parameters namely bandwidth, propagation delay and queue type.
  We can vary these parameters and could possibly obtain different throughputs. From there we can determine the conditions that provide higher throughput values.In general, we can alter different parameters and study their effects on one or more performance metrics and thereby filter out the combination of parameters that gives best performance.

- Performance of the network can be determined by considering different metrics for example 'Throughput'
- We can vary these parameters and could possibly obtain different throughputs, which can be plotted using xgraph
- From there we can determine the conditions that provide higher throughput values
- Make suitable combinations with the parameters that wil bring some changes in the throughput
- Use the best combination of parameters which will bring the best throughput and implement it
- We are considering only one performance metric i.e throughput in our experiment.Other metrics like packet loss,latency,retransmission can measured to evaluate the performance of a network in a more accurate way which will help us to setup the network in a proper way.

Lecture-9

IEEE Standards 802 series & their variant

IEEE 802 refers to a family of IEEE standards dealing with local area networks and metropolitan area networks.

More specifically, the IEEE 802 standards are restricted to networks carrying variable-size packets. (By contrast, in cell relay networks data is transmitted in short, uniformly sized units called cells. Isochronous networks, where data is transmitted as a steady stream of octets, or groups of octets, at regular time intervals, are also out of the scope of this standard.) The number 802 was simply the next free number IEEE could assign,[1] though "802" is sometimes associated with the date the first meeting was held — February 1980.

The services and protocols specified in IEEE 802 map to the lower two layers (Data Link and Physical) of the seven-layer OSI networking reference model. In fact, IEEE 802 splits the OSI Data Link Layer into two sub-layers named Logical Link Control (LLC) and Media Access Control (MAC), so that the layers can be listed like this:

- Data link layer
  - LLC Sublayer
  - MAC Sublayer
- Physical layer

The IEEE 802 family of standards is maintained by the IEEE 802 LAN/MAN Standards Committee (LMSC). The most widely used standards are for the Ethernet family, Token Ring, Wireless LAN, Bridging and Virtual Bridged LANs. An individual Working Group provides the focus for each area.

The IEEE 802.x Standard

The bottom two layers of the OSI reference model pertain to hardware: the NIC and the network cabling. To further refine the requirements for hardware that operate within these layers, the Institute of Electrical and Electronics Engineers (IEEE) has developed enhancements specific to different NICs and cabling. Collectively, these refinements are known as the *802 project*. This lesson describes these enhancements and how they relate to OSI.

The 802 Project Model

When local area networks (LANs) first began to emerge as potential business tools in the late 1970s, the IEEE realized that there was a need to define certain LAN standards. To accomplish this task, the IEEE launched what became known as Project 802, named for the

year and month it began (1980, February).

Although the published IEEE 802 standards actually predated the ISO standards, both were in development at roughly the same time, and both shared information that resulted in the creation of two compatible models.

Project 802 defined network standards for the physical components of a network (the interface card and the cabling) that are accounted for in the physical and data-link layers of the OSI reference model.

The *802 specifications* set standards for:

- Network interface cards (NICs).
- Wide area network (WAN) components.
- Components used to create twisted-pair and coaxial cable networks.

The 802 specifications define the ways NICs access and transfer data over physical media. These include connecting, maintaining, and disconnecting network devices.

RGPV PAPER QUESTIONS
Q.1 Define FDDI? [RGPV June 2011],[RGPV Dec 2012],[RGPV June 2013]
Q.2 Explain MAC Sublayer? [RGPV June 2011], [RGPV June 2013]
Q.3 Explain ALOHA Protocol? [RGPV June 2012] ,[RGPV Dec 2012], [RGPV June 2014]
Q.4 Explain Contention Protocol?[RGPV June 2012]
Q.5 How does CSMA/CD different from CSMA/CA?[RGPV Dec 2012],[RGPV June 2013]