[1]

The syllabus states that specific pre-requisites must be met for this course. I am taking Fundamentals of Computer Engineering in parallel to this course for Spring 2020. Programming languages include C, C++ and C# with Visual Studio.NET. HDL include Verilog and System Verilog with Incisive. I have reviewed and jotted down important concepts of the Fundamentals of Computer Networking textbook 6th edition by Kurose Ross.

Chapter 1: Computer Networks and the Internet

Basics and Foundation

If the propagation delay from source to destination transmission is L/R seconds where the source end systems or packet switch is sending a packet of L bits over a link and R is the transmission rate R bits/sec then then time to transmit the packet is L/R seconds. The end to end delay with a path of N links is N*L/R seconds.

Forwarding Tables and Routing Protocols

When a packet arrives at a router in the network, the router examines a portion of the packet's destination address and forwards the packet to an adjacent router. Each router has a forwarding table that maps destination addresses to that router's outbound links. Upon arrival at a router, the router examines the address and searches its forwarding table using the destination address to the appropriate outbound link. The router then directs the packet to this outbound link.

Section 1.2 R12

Circuit switched network over packet switched network

Fundamental approaches to data transmission in the network is circuit switching and packet switching. To explain the fundamental difference: An example would be that with circuit switching, 100kbps should be *reserved* for *each* user at all times.

With circuit switched TDM, one-second frame is divided into 10 time slots of 100ms each, hence each user would be allocated one time slot per frame. Thus, the circuit switched link can support only 10 (=1Mbps/100kbps) simultaneous users. Under TDM circuit switching one active user can only use

[1]

one time slot per frame to transmit data even if the other 9 frames are idle. If the active user has one million bits of data to transmit it will be 10 seconds before all of the active user's one millions bits of data has been transmitted.

In case of packet switching, the active user can send its packets at the full link rate of 1Mbps. Hence packet switching is more efficient compared to circuit switching. The only advantages with circuit switching is that the probability of having only one active user. However, with packet switching if the probability of there being 10 active users is high then the aggregate arrival rate of packets exceeds the output capacity of the link and hence the output queue will grow.

Once gain the fundamental difference is that circuit switching pre-allocates the use of the transmission link with allocated but unneeded time going unused and packet switching on the other hand allocates link use *on demand*.

Section 1.4 R16
Delay variables

Concepts: Transmission delay is the amount of time required for the router to push out the entire packet, it is a function of the packet's length and the transmission rate of the link. The propagation delay is the time it takes a bit to propagate from one router to the next.

Propagation, queueing and transmission delays equates to the total nodal delay.

dnodal = dproc + dqueue + dtrans + dprop

Section 1.4 R18:
Distance of 2500km, prop speed of 2.5*10^8 m/s , transmission rate of 2Mbps.

Delay = distance / speed = 0.01 seconds, transmission delay is 0.5seconds, total delay is 0.501 seconds.

[2]

[2]

Section 1.4 R19:

Slowest possible link which is R1 since it's the bottleneck.

Section 1.5 R23

Application Layer: The application layers is where the network applications and their application layer protocols reside. The internet's application layer includes many protocols such as the HTTP protocol, SMTP and FTP. The application layer protocol is distributed over multiple end systems. The application in one end system using the protocol to exchange packets of information with the application in another end system. This packet of information at the application layer as a *message.*

Transport Layer: The internet's transport layer transports application-layer messages between application endpoints. There are two transport protocols: TCP and UDP, either of which can transport application layer *messages*. A transport protocol can encrypt data transmitted by the sending process and in the receiving host, the transport layer protocol can decrypt the data before delivering the data to the receiving process. The transport layer packet is referred to as a *segment*. Services of the transport layer protocol are reliable data transfer, throughput, timing and security.

The TCP protocol:

Connection-oriented service that guarantees delivery of application-layer messages to the destination and flow control.

It also provides congestion control algorithm where the transmission rate is adjusted when the network is congested.

The UDP protocol:

Provides a connectionless service to its applications. It provides no reliability, no flow control and no congestion control.

Network Layer: The internet's network layer is responsible for moving network-layer packets known as *datagrams* from one host to another. The (*TCP or UDP)* in a source host passes a transport layer segment and a destination address to the network layer which then delivers the segment to the transport layer in the destination host. The internet's network layer contains routing protocols that determines the routes that datagrams take between sources and destinations. The internet's network layer also contains routing protocols that determine the routes that datagrams take between sources and destinations.

Link Layer: The internet's network layer routes a datagram through a series of routers between source and destination.

To move a packet from one node to the next node in the route the link layer is utilized. The network layer passes the datagram down to the link layer and delivers the datagram to the next node along the route. The link layer also passes the datagram up to the network layer.

The services provided by the link layer depend on the specific link layer protocol. Link layer protocols include Ethernet, WiFi and cable access network's DOCSIS protocol. Since the datagrams need to traverse several links to travel from source to destination, the datagram may be handled by different link layer protocols at different links along its route. The link layer packets are called *frames*.

Physical Layer: The link layer transports entire frames from one network element to an adjacent network element, the physical layer transfers individual bits within the frame through various physical layer protocols.

Chapter 2: Application Layer

The application architecture which is very different from the network application architecture is designed by the application developer and dictates who the application is structures over the various end systems. In selecting the application architecture, the application developer will select between client-server architecture or the peer-to-peer (P2P) architecture. In a client-server architecture, there is always-on host called the *server* which services requests from many other hosts called *clients*. Applications with a client-server architecture include the *Web, FTP, Telnet* and *e-mail*. In P2P architecture, there is minimal reliance on dedicated servers in data centers. Peers communicate without passing through a dedicated server hence the architecture is called peer-to-peer. Self-scalability is the key advantage for P2P architectures. They also do not require server infrastructure and server bandwidth. Challenges for future P2P architectures include * *ISP friendly:* Much more downstream than upstream traffic. * *Security:* Can be a challenge due their highly distributed and open nature, they can also be a challenge to secure. * *Incentives:*

Success of future P2P applications depends on convincing user to volunteer bandwidth, storage and computation resources to the applications.

A socket is the interface between the application process and the transport layer protocol. A process sends messages into and receives messages from the network through a software interface called a socket. The transport layer protocol offers the following services to the application layer: reliable data transfer, throughput, timing and security. *Throughput*: Certain applications are bandwidth-sensitive and fixed requirements, while other applications are elastic applications an can make use of as much or as little throughput as available. Electronic mail, file transfer and web transfers are all elastic applications. *Timing*: A transport layer protocol also provides timing guarantees. A transport layer protocol also provides timing guarantees. Internet telephony, virtual environments, teleconferencing and multiplayer games all require tight timing constraints on data delivery in order to be effective. *Security:* A transport protocol can provide an application with one or more security services. *Web cache*: A web cache is also called a proxy server is a network entity that satisfies HTTP requests on the behalf of an origin web server. The web cache has it's own disk storage and keeps copies of recently requested objects in this storage.

File transfer (FTP): HTTP and FTP are both file transfer protocols that have many common characteristics, for example they both run on top of TCP. FTP uses two parallel TCP connections to transfer a file – a control connection and a data connection. Simple Mail Transfer Protocol (SMTP): Is the principal application layer protocol for internet electronic mail, it uses the reliable data transfer service of TCP to transfer mail from the sender's mail server to the recipient's mail server. HTTP transfers files from a web server to a web client and SMTP transfer files from one mail server to another
mail server. Post office protocol (POP3): Internet Mail Access Protocol (IMAP) is a simple mail access protocol. It begins with a client opens a TCP connection to the mail server on port 110, with the TCP connection established, POP3 progresses through three phases: authorization, transactions and update. In the authorization phase, the user agent sends a username and a password to authenticate the user. During the second phase, the user agent retrieves messages and marks messages for deletion, remove deletion marks and obtain mail statistics. The third phase occurs after the client has issued the quit command hence ending the POP3 session. IMAP is a mail access protocol and it has more features than POP3.

DNS (Internet Directory Service): The DNS is employed by other application layer protocols including HTTP, SMTP and FTP. Host aliasing, mail server aliasing and load distribution services is provided by the DNS.

A distributed, hierarchical database: There are three classes of DNS servers – root DNS servers, top level domain (TLD) DNS servers, and authoritative DNS servers. With peer to peer architecture there is no minimal reliance on always-on infrastructure servers and instead pairs of intermittently connected hosts called peers communicate directly with each other. Socket programming can be accomplished with UDP and TCP.

Lab examples include web designing and programming.

Chapter 3: Transport Layer

A transport-layer protocol provides for logical communications between application processes running on different hosts. Transport-layer protocols are implemented in the end systems but not in network of routers.

There are two distinct transport layer protocols available in the application layer -> one of these protocols is UDP (User Datagram Protocol) - unreliable, connectionless service to the invoking application and the second of these protocols is TCP (transmission control protocol) - reliable, connection-oriented service to the invoking application.

Extending host to host delivery to process to process delivery is called transport layer multiplexing and demultiplexing. TCP provides reliable data transfer and congestion control. Delivering the data in a transport layer segment to the correct socket is called demultiplexing and vice versa collecting data from the source host from different sockets encapsulated with data and header information to create segments and pass the segments to the network layer is called multiplexing.

The transport layer requires the four values in the connection request segment: * Source port number in the segment * IP address of the source host * Destination port number in the segment and * IP address.

Advantages of UDP over TCP

DNS is an example of an application layer protocol that uses UDP. IP + multi/ demulti + error checking. UDP takes messages from the application process, attaches source and destination port number fields for the multi/demulti services, adds two other fields and passes the resulting segment to the network layer.

UDP	*TCP*
• *Finer application-level control over what data is sent and when:*	
Passes immediately to the network layer	TCP has congestion control mechanism which throttles the transport-layer TCP when multiple links between the source and destination host become excessively congested.
• *No prior connection establishment:*	
UDP utilizes an immediate connection	TCP uses a three-way handshake before it starts to transfer data

- *No connection state:* CP maintains connection state in the end systems, this connection state includes receive and send buffers, congestion-control parameters, sequence and acknowledgement # parameters.
- *Small packet header overhead:*

The TCP segment has 20 bytes of header over head in every segment whereas UDP has only 8 bytes of overhead.

- *UDP Checksum*

The UDP checksum provides for error detection. The checksum is used to determine whether bits within the UDP segment have been altered as it moves from source to destination. UDP at the sender side performs the 1s complement of the sum of all the 16-bit words in the segment with any overflow encountered during the sum of all 16-bit words in the segment. The bit errors occur in the physical components of a network as a packet is transmitted, propagated or buffered. 32 bits is the source port #, destination port #, length, checksum and application data (message).

In a computer network setting, reliable data transfer protocols based on such retransmission are known as **ARQ** (Automatic Repeat reQuest) protocols.

- ARQ

Error detection, receiver feedback and retransmission are the capabilities of the ARQ protocols.

Flow Control

The TCP provides a flow-control service to its applications to eliminate the possibility of the sender overflowing the receiver's buffer. Congestion control is when a TCP sender can be throttled due to the congestion within the IP network. The TCP provides flow control by having the sender maintain a variable called the *receive window.*

Lastbytereceived – last byteread <= receiver buffer.

The receive window is the following: rwnd = RcvBuffer – [lastbytercvd – lastbyteread]

Principles of Congestion Control

Packet re-transmission treats a symptom of network congestion but does not treat the cause of network congestion, hence too many sources attempting to send data at too high of a rate. To treat the cause of network congestion, mechanisms are needed to throttle senders in the face of network congestion. Available bit-rate (ABR) service in asynchronous transfer mode (ATM) networks.

Approaches to congestion control: Network architectures and congestion control protocols embody these approaches. At the broadest level: End-to-end congestion control and network assisted congestion control. In end-to-end approach, the network layer provides no explicit support to the transport layer, the congestion behavior is inferred based on packet loss and delay. The TCP segment loss is taken as an indication of network congestion and TCP decreases its window size accordingly.

Network-assisted congestion control: The network-layer components provide feedback to the sender regarding the congestion state in the network, it's an explicit form of communication. Direct feedback may be sent from a network router to the sender and this form of notification takes the form of a choke packet. The second form of notification occurs when a router marks/updates a field in a packet flowing from sender to receive to indicate congestion.

TCP Congestion Control: TCP must use end-to-end congestion control rather than network-assisted congestion control. The sender limits the rate at which it sends traffic into its connection. The rate is a function of the perceived network congestion. It modulates the rates, if there is little congestion on the path then the TCP sender increases its send rate. The TCP congestion -control algorithm operating at the

sender keeps track of an additional variable, the *congestion window.* It imposes a constraint on the rate at which a TCP sender sends traffic into the network. TCP uses acknowledgements to trigger (or clock) it's increase in congestion window size, hence TCP is said to be *self-clocking.*

Estimated round-trip time for TCP timer management: EstimatedRTT = (1-α) * EstimatedRTT + α*SampleRTT

DevRTT is an estimate of how much SampleRTT deviates from estimatedRTT.

DevRTT = (1-B)*DevRTT + B(SampleRTT – EstimatedRTT)

Methods by which TCP determines the sending rate at which it sends includes:

- Lost segment implies congestion, hence the sender's rate should be decreased when a segment is lost.
- Acknowledgment segment indicates that the network is delivering the sender's segments to the receiver hence the sender's rate is increased when an ACK arrives.
- Bandwidth probing
- The TCP congestion control algorithm has three major components Slow start, Congestion avoidance and Fast recovery.

TCP throughput:

RTT: Roundtrip interval, the rate at which TCP sends data is a function of the congestion window and the current roundtrip time. Window size is w bytes then the TCP's transmission rate is *w/RTT.*

Average throughput of a connection =0.75W/RTT. The TCP connection as a function of the loss rate (L), round-trip time (RTT) and maximum segment size (MSS). We can achieve a throughput of 10Gbps in today's TCP congestion control algorithm.

*Average throughput of a connection = 1.22 MSS / RTT * √L .*

Summary

The chapter reviews the UDP (connectionless service) and TCP (connection-oriented service) protocols. The UDP is almost at the IP level with the exception of a multi/demulti function for communicating processes. The TCP protocol is a transport layer protocol that provides reliable delivery of data, delay guarantees and BW guarantees. However the transport layer depends on the delay and bandwidth guarantees that is provided by the network layer. Reliability depends on all four layers and is implemented through acknowledgements, timers, retransmissions and sequence numbers.

Key functions include forwarding, routing and connection setup. Computer networks that provide only a connection service at the network layer are called virtual-circuit (VC) networks, computer networks that provide only a connectionless service at the network layer are called datagram networks.

Datagram network:

In the connectionless service each time an end systems wants to transmit a packet it stamps the packet with the address of the destination end systems and then pops the packet into the network. There is no VC setup and routers are not required to maintain VC information. The schedule of tasks include:

- A packet is transmitted from source to destination, as it passes through the series of routers.
- The packet's destination address is utilized by the routers to forward the packet.
- The forwarding table maps the destination addresses to link interfaces
- Packet arrives at the router
- The destination address is looked up in the forwarding table
- Transferred to the appropriate interface link

Datagram package format:

- Version, header length, type of service, datagram length, identifier flags, fragmentation offset, time to live, protocol, header checksum, source and destination IP addresses, options, and data (payload)

Section 4.1 and 4.2: Network-layer functions and services

Packet switch: Is a general packet switching device that transfers a packet from input link interface to output link interface according to the value in a field in the header of the packet.

A few packet switches called link layer switches make decisions on how to forward the packet based on values in the fields of the link-layer frame, these switches are hence referred to as link layer devices.

Routers (packet switches) base their forwarding decision on the value in the network layer field. Hence routers are network-layer devices and must implement layer 2 protocols as well. Layer 3 devices require the services of layer 2 to implement their functionality. Network layer has two important functions, forwarding and routing. Network layer provides the following possible services: Guaranteed delivery,

guaranteed delivery with bounded delay. Constant bit rate ATM network service and available bit rate ATM network service.

Following services could be provided to a flow of packets between a given source and destination.

- In-order packet delivery, guaranteed minimal bandwidth, guaranteed maximum jitter and security services.
- *Virtual circuit and datagram networks*. The network-layer connections are called virtual circuits (VCs). A VC consists of (1) a path between source and destination hosts (2) VC #, one number for each link along the path (3) entries in the forwarding table in each router along the path.
- *VC setup*: During the setup phase, the sending transport layer contacts the network layer, specifies the receiver's address and waits for the network to setup the VC.
- *Data transfer:* Once the VC has been established, packets can begin to flow along the VC.
- *VC teardown*: The network layer typically informs the end system on the other side of the network of call termination and update the forwarding tables in each of the packet routers on the path to indicate that the VC no longer exists.

What's inside a router:

- The forwarding function is the actual transfer of packets from a router's incoming links to the outgoing links at that router. *Forwarding* and *switching* are used interchangeably by computer-networking researchers and practitioners.

Input ports / switching fabric / output ports/ routing processor

Basic Router Functions

Input ports: It performs the physical layer function of terminating an incoming physical link at a router. The input port performs link-layer functions needed to interoperate with the link layer at the other side of the incoming link which is represented by the middle boxes in the input and output ports. The input port's termination function and link-layer processing implement the physical and link layers for that individual input link. The forwarding table consists of line termination; data link processing (protocol, decapsulation); lookup forwarding, queuing and switch fabric.

Switching fabric: The switching fabric connects the router's input ports to its output ports. This switching fabric is contained within the router. Blocking, queuing and scheduling of packets are key concepts. The switching fabric is at the very heart of the router. Processes to accomplish switching are *switching via memory.* Other options include *switching via a bus:* An input port transfers a packet to the output port over a shared bus without intervention of the routing processor. *Switching via an interconnection network:* One way to overcome the bandwidth limitation of a single, shared bus is to use a more sophisticated interconnection network such as those that have been used in the past to interconnect processors in a multiprocessor computer architecture.

Output ports: An output port stores packets received from the switching fabric and transmits these packets on the outgoing link with the necessary link-layer and physical-layer function. The output port processing takes packets that have been stored in the output port's memory and transmits them over the output link. This includes selecting and de-queuing packets for transmission, performing the needed link layer and physical layer transmission functions.

Routing processor: The routing processor executes the routing protocols and maintains routing tables and link state information and computes the forwarding table for the router.

Router forwarding plane: A router's input ports, output ports and switching fabric implement the forwarding function and are almost implemented in hardware. A packet can be sent into the switching fabric once the packet's output port has been determined via the lookup table.

Queueing: The router's memory can be exhausted, and packet loss will occur when no memory is available to store the arriving packets. The router's memory can be exhausted, and packet loss can occur when no memory is available to store the arriving packets. If the input and output line speeds have transmission rates of R_{line} packets per second, then there are N input ports and N output ports. The switching fabric transfer rate R_{switch} as the rate at which packets move from input port to output port. Minimal queueing will occur when the switching time is N times faster than the transmission rate. In the time it takes to send a single packet onto the outgoing link, N new packets will arrive at this output port. The output port can transmit only a single packet in a unit of time, the N arriving packets will have to queue (wait) for transmission over the outgoing link. The rule of thumb for buffer sizing is that the amount of buffering (B) should be equal to an average round-trip time (RTT) times the link capacity (C). A 10Gbps link with an RTT of 250msec requires buffering equal to B = RTT*C = 2.5Gbits of buffers.

A consequence of output port queuing is that a packet scheduler at the output port must choose one packet among those queued for transmission. The selection is done a simple basis such as first-come and first-served (FCFS) scheduling. The head-of-the line (HOL) blocking in an input-queued switch.

Packet scheduler: Once the packets are queued at the output port, one packet is selected for transmission. It's can be FCFS scheduling or weighted fair queuing (WFQ). AQM algorithms include the Random Early Detection (RED) algorithm. At the input port, packet queueing can also occur, since the packets must join input port queues to wait their turn to be transferred through the switching fabric to the output port this can lead to *"The head-of-the line (HOL) blocking"*.

Routing Control Plane: The routing control plane resides and executes in a routing processor within the router.

Section 4.3 and 4.4: Covers forwarding: When a packet arrives at a router's input link, the router must move the packet to the appropriate output link. For a packet arriving from host H1 to router R1 must be forwarded to the next router on a path to H2. Every router has a forwarding table, the router forwards a packet by examining the value of a field in the arriving packet's header and then using this header value to index into the router's forwarding table. Forwarding refers to the router-local action of transferring a packet from an input link interface to the output link interface. Internet network layer consists of Transport layer TCP, UDP, Network layer, Link layer and Physical layer.

IPv4 Addressing: A host is a single link into the network, when IP in the host wants to send a datagram it does so over the link. The boundary between the host and the physical link is called an interface. IP requires each host and router interface to have its own IP address. There are about 4 billion possible IP addresses.

Routing Algorithms

Routing algorithms exchange and compute information that is used to configure these forwarding tables. The goal of the routing algorithms is as follows: given a set of routers, with links connecting the routers, a routing algorithm finds a "good" path from source router to destination router.

A global routing algorithm computes the least-cost path between a source and destination using complete global knowledge about the network. The algorithm takes connectivity between all nodes and all link costs as inputs, if the calculations are executed at one site, then it's a centralized global routing algorithm, it can also be replicated at multiple sites.

In a decentralized routing algorithm, the calculation of the least-cost path is carried out in an iterative distributed manner. Each node initiates the routing algorithm with knowledge of the costs of its own directly attached links.

Classifications of routing algorithms include: Static routing algorithm, dynamic routing algorithm and load-sensitive algorithm. The link-state routing algorithm is known as Dijkstra's algorithm.

Broadcast and multicast routing: In broadcast routing, the network layer provides a service of delivering a packet sent from a source not to all other nodes in the network. Multicast routing enables a single source node to send a copy of a packet to a subset of other network nodes.

Section 4.5 and 4.7: Covers routing: The network layer determines the route or path taken by packets as they flow from a sender to a receiver. The algorithms that calculate these paths are referred to as routing algorithms.

Summary:

Network layer provides a communication service between any two network hosts. The datagrams travel over a series of communication links, some wired and some wireless starting at the source host, passing through a series of packet switches (switches and routers) and ending at the destination host.

Overview

There are two different types of link-layer channels, the first type are broadcast channels, which connect multiple hosts in wireless LANs, satellite networks and hybrid fiber-coaxial cable (HFC) access networks.

The second type of link layer is the point-to-point communication link, such as that found between two routers connected by a long distance link or between a user's office computer and nearby Ethernet switch to which it is connected.

Introduction to link layer

Nodes include hosts, routers, switches and WiFi access points. The communication channels that connect adjacent nodes along the communication path as links. Datagram is passed through the following six links:

- WiFi link between sending host and WiFi access point
- Ethernet link between the access point and a link layer switch
- A link between the link-layer switch and the router
- A link between the two routers
- Ethernet link between router and link layer switch
- Ethernet link between switch and the server

A transmitting node encapsulates the datagram in a link layer frame and transmits the frame into the link., Hence the basic service of any link layer is to move a datagram from one node to an adjacent node over a single communication link.

Services provided by the link layer protocol include:

- Framing
- Link access
- Reliable delivery
- Error detection and correction

The link layer is implemented in a network adapter also known as a network interface card (NIC).

A network adapter is the link layer controller which is a special purpose chip that implements many of the link layer services (framing, link access, error detection, parity checks, and so on). It's usually implemented in hardware.

On the sending side, the controller takes a datagram, encapsulates the data gram in a link layer frame and then transmits the frame into the communication link. On the receiving side, the controller receives the entire frame and extracts the network layer datagram. On the receiving side, the link layer SW responds to controller interrupts, handling error conditions and passing a datagram up to the network layer. Hence the link layer is a combination of hardware/software.

Error Correction and detection techniques

Bit-level error detection and correction techniques include parity checks, check summing methods and CRC.

Parity checks: Check the parity. The even parity bit is set for even # of 1s and an odd parity bit is set for odd # of 1s. With the 2D even parity, the parity of both column and row containing the flip bit will be in error. The ability of the receiver to both detect and correct errors is known as *forward error correction (FEC).*

Check summing: In check summing techniques, the d bits of data are treated as a sequence of k-bit integers. A simple check summing method is to sum these k-bit integers and use the resulting sum as the error-detection bits. The 1s complement of this sum forms the internet checksum that is carried in the segment header.

CRC: The CRC bits which are appended to the data bits. The sender and receiver agrees on an r+1 bit pattern called the generator denoted as G. The most significant bit of G is 1. The CRC code is r and is selected such that d+r bit pattern is exactly divisible by G using modulo-2 arithmetic. The receiver divides the d+r received bits by G.

Multiple access protocols: Nodes regulate their transmission into the shared broadcast channel. Dozens of multiple access protocols have been implemented in a variety of link-layer technologies. They can be categorized as channel partitioning protocols, random access protocols and taking turns protocols. TDM, FDM and CDMA are various channel partitioning protocols.

Random access protocols: In a random access protocol, a transmitting node always transmits at the full rate of the channel namely R bps, when there is a collision, each node involved in the collision retransmits its frame unit its frame gets through without a collision.

Slotted ALOHA protocol: When a node has a frame to send, it waits until the beginning of the next slot and then transmits the entire frame in the slot, if there isn't a collision, the node has transmitted its frame If there is a collision, the node detects the collision before the end of the slot and retransmits its frame in each slot with probability p until the frame is transmitted without a collision. The node can transmit at full rate R when that node is the only active node. Slotted ALOHA is also highly decentralized, since each node detects collisions and decides when to retransmit.

ALOHA protocol: The slotted ALOHA protocol requires that all nodes synchronize their transmissions to start at the beginning of a slot.

Carrier Sense Multiple Access (CSMA) protocol:

- The adapter receives a datagram from the network layer, prepares a link layer frame and places the frame adapter buffer. If the adapter senses that the channel is idle, it starts to transmit the frame. The adapter senses that the channel is busy it waits until it senses no signal energy and then starts to transmit the frame.
- While transmitting, the adapter monitors for the presence of signal energy from other adapters using the broadcast channel.
- If the adapter transmits the entire frame without detecting signal energy from other adapters, the adapter completes the frame.
- Efficiency equals to $1/ (1+ 5* d_{prop}/ d_{trans})$

DOCSIS: The link layer protocol for cable internet access:

- The data-over-cable service interface specifications specifies the cable data network architecture and its protocols.

Link Layer Addressing and ARP

Hosts and routers have link layer addresses. Address Resolution Protocol (ARP) provides a mechanism to translate IP addresses to link layer addresses.

MAC Addresses

A link layer address is called a LAN address, a physical address or a MAC address.

Ethernet

The ethernet frame structure consists of the preamble, destination address, source address, type, data and CRC. Ethernet technologies consist of 10BASE-T, 10BASE-2, 100BASE-T, 1000BASE-LX and 10GBASE-T

Properties of link-layer switching

The basic operation of a link layer switch is as follows, elimination of collisions, heterogeneous links and management

Summary

Link layer communication consists of error-detection , correction techniques, multiple access protocols, link layer addressing, virtualization and construction of extended switched LANs and data center networks.