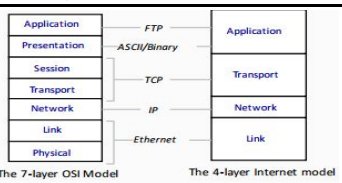
Application Layer:, is where applications requiring network communications live. Examples of these applications include email clients and web browsers. These applications use the Transport Layer to send requests to connect to remote hosts.**Transport Layer:** establishes the connection between applications running on different hosts. It uses **TCP** for reliable connections and UDP for fast connections. It keeps track of the processes running in the applications above it by assigning port numbers to them and uses the Network layer to access the **TCP**/IP network. **Network Layer:** responsible for creating the packets that move across the network. It uses IP addresses to identify the packet's source and destination. **Data Link Layer:** responsible for creating the frames that move across the network. These frames encapsulate the packets and use MAC addresses to identify the source and destination. **Physical Layer:** encodes and decodes the bits found in a frame and includes the transceiver that drives and receives the signals on the network.**Transmission Control Protocol (TCP)**: connection-oriented protocol, which means a connection is established and maintained until the application programs at each end have finished exchanging messages. in-sequence delivery. Congestion control. Error detection: Checksum mandatory for IPv4 & IPv6. **Application-Programming Interface (API). UDP** (User Datagram Protocol) is an alternative communications protocol used primarily for establishing low-latency and loss tolerating connections between applications on the Internet.

Hours: WE, 11:30AM - 12:30PM - James Kurose and Keith Ross. Computer Networking: A Top-Down Approach (7th ed) NRZ (hight 1, low 0), NRZI(invert on 1) b Manchester(l-h 0, h-l 1),



Layer 7 (Application) **HTTP, SMTP, NFS, Telnet** Layer 4 (Transport)**TDP, UDP** Layer 3 (Network) **IPv4, IPv6** Layer 2 (Link) **Ethernet, WiFi (802.11), SONET**

congestion:
- informally: "too many sources sending too much data too fast for *network* to handle"
- different from flow control!
- manifestations:
  - lost packets (buffer overflow at routers)
  - long delays (queueing in router buffers)

Flow Control vs. Congestion Control
- Flow control
  - Keeping one fast sender from overwhelming a slow receiver
- Congestion control
  - Keep a set of senders from overloading the network

Random Early Detection (RED): It is a congestion avoidance mechanism. The main goal is to provide congestion avoidance by controlling the average queue size. **Explicit Congestion Notification (ECN)** allows end to end notification of network congestion without dropping packets. ECN must be used on both endpoints. ECN provides some level of performance improvement over a packet drop. With large bulk data transfers, the improvement is moderate, based on the difference between the packet retransmission and congestion-window adjustment.
Distance Vector (DV): A lowest-cost-path algorithm used in intra-domain routing. Each node advertises reachability information and associated costs to its immediate neighbors and uses the updates it receives to construct its forwarding table. The routing information protocol (RIP) uses a distance-vector algorithm. It has less computational complexity and message overhead. (Adv) does not advertise entire network topology, (DiAdv)Slow Convergence (speed) due to Count to infinity problem. A **path vector** protocol is a network routing protocol which maintains the path information that gets updated dynamically. Updates which have looped through the network and returned to the same node are easily detected and discarded. **Link-state protocol** require a router to inform all the nodes in a network of topology change.Routers running Link-state routing protocol knows about the full topology of the network. They have knowledge of the entire path to a destination.Link-state routing protocols have high computational complexity and message overhead, require more processing power and memory. Link state routing converges quickly. **PV/LS** - Link state routing protocols allow a router to have a complete map of the network, and use specific algorithms to find shortest paths to every object in the network.

Bellman-Ford algorithm is one where routes are selected based on the distance betw. Networks.
Three-way handshake is a method used in a TCP/IP network to create a connection between a local host/client and server. It is a three-step method that requires both the client and server to exchange SYN and ACK (acknowledgment) packets before actual data communication begins
Nagle's algorithm is used by TCP senders to determine when to transmit a segment. The algorithm allows to send full segment if the window permits. It also allows to send small amount of data if there are no segments in transit. Otherwise, if there is anything in flight, the TCP sender must wait for an ACK before transmitting the next segment. **Fast Retransmit** is a congestion control algor. that makes it possible to quickly recover lost data packets. Without FR, the TCP uses a timer that requires a retransmission timeout if a packet is lost. No new or duplicate packets can be sent during the timeout period.
Slow-start is part of the congestion control strategy used by TCP. Slow-start is used in conjunction with other algorithms to avoid sending more data than the network is capable of transmitting, that is, to avoid causing network congestion.Its main purpose is to quickly get the window size up to the connection's capacity, so that the link's bandwidth is not wasted.
Congestion avoidance tries to detect when the link quality is degrading, usually due to congestion (too many users trying to send
too many packets), and quickly decreases the window size to decrease usage of it. It halves the window size to play it safe.
TCP window size is simply an advertisement of how much data (in bytes) the receiving device is willing to receive at any point in time. The receiving device can use this value to control the flow of data, or as a flow control mechanism
Flow control is the management of data flow between computers or devices or between nodes in a network so that the data can be handled at an efficient pace. Too much data arriving before a device can handle it causes data overflow, meaning the data is either lost or must be retransmitted..
Counting to infinity can occur when a link breaks in the network, and the algorithm in the routing protocol tries to calculate new shortest paths.
Spanning tree protocol is designed to eliminate loops in the forwarding topology. It provides a distributed manner for individual switches to cooperatively form a spanning tree topology: each switch first declares itself as the root and passes the configuration messages out to each of its interfaces identifying itself as the root with distance 0. Switches periodically receive these messages from their neighbours and update their view of the root. Upon receiving a message, a switch checks the root id. If the new id is smaller than the recorded one, it starts viewing that switch as root

Why not a de facto ISN of 0?Practical issue
- IP addresses and port #s uniquely identify a connection
- Eventually, though, these port #s do get used again
- … and there is a chance an old packet is still in flight
- … and might be associated with the new connection
***Network Address Translation* (NAT)** process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses an organiz.or comp.must use, for both economy and security purposes. NAT can be configured to advertise only one address for the entire network to the outside world. This provides additional security by effectively hiding the entire internal network behind that address. NAT offers the dual functions of security and address conservation and is typically implemented in remote-access environments. Difficult to support peer-to-peer applications. Routers are not supposed to look at port #s. violates the end-to-end argument. - Network nodes should not modify the packets. IPv6 is a cleaner solution. **OpenFlow** is an open standard network protocol used to manage traffic between commercial Ethernet switches, routers and wireless access points. OF enables software-defined networking (SDN) for programm. networks and is based on an Ethernet switch, with an internal flow-table and a standardized interface to add and remove flow entries. The basic idea behind OpenFlow is that you can connect multiple switches -- and even networks -- together to create a flow, and then manage the entire infrastructure, setting policies and managing traffic type accordingly. It allows for deployment of innovative routing and switching protocols in your network for many different applications, including virtual machine mobility and high-security networks.
A **middlebox** or network appliance is a computer networking device that transforms, inspects, filters, or otherwise manipulates traffic for purposes other than packet forwarding. EX: **firewalls**, which filter unwanted or malicious traffic, and NATs.**Address resolution protocol (ARP)** is a protocol used by the Internet Protocol (IP), specifically IPv4, to map IP network addresses to the hardware addresses used by a data link protocol. The protocol operates below the network layer as a part of the interface between the OSI network and OSI link layer. It is used when IPv4 is used over Ethernet.**Tier-2 providers**: - Provide transit service to downstream customers. need at least one provider of their own **Stub Autonomous System (AS)** A group of networks and routers, subject to a common authority and using the same intra-domain routing Protocol. Do not provide transit service to others and Connect to one or more upstream providers **Autonomous System (AS)** is used to capture the concept of groups of routers. An AS is a contiguous set of networks and routers all under control of one administrative authority. There is no exact meaning for administrative authority (the term is sufficiently flexible to accommodate many possibilities, but normally it means an organization, company or an ISP). Two type of routing protocols used in the autonomous system.: **IGP and EGP**

Multiplexing/Demultiplexing
multiplexing at sender:handle data from multiple
demultiplexing at receiver:
sockets, add transport header
demultiplexing at receiver:use header info to deliver received segments to correct socket
When does Fast Retransmit work best?
- Long data transfers - High likelihood of many packets in flight - High window size - High likelihood of many packets in flight**Fast retrans.** Sender retransmits data after the triple duplicate ACK.
Maximum segment size (MSS) is the largest amount of data, specified in bytes, that a computer or communic.s device can handle in a single, unfragmented piece. For optimum communications, the number of bytes in the data segment and the header must add up to less than the number of bytes in the maximum transmission unit (MTU) A **maximum transmission unit (MTU)** is the largest size packet or frame, specified in octets (eight-bit bytes), that can be sent in a packet- or frame-based network such as the Internet. The Internet's Transmission Control Protocol (TCP) uses the MTU to determine the maximum size of each packet in any transmission.
BGP (Border Gateway Protocol)path vector protocol that manages how packets are routed across the internet through the exchange of routing and reachability information between edge routers. BGP directs packets between **(AS)** -- networks managed by a single enterprise or service provider. Traffic that is routed within a single network AS is referred to as internal BGP, or **iBGP**. More often, BGP is used to connect one AS to other autonomous systems, and it is then referred to as an external BGP, or **eBGP**. **IGP (Interior Gateway Protocol)** is a protocol for exchanging routing information between gateways (hosts with routers) within an autonomous network (for example, a system of corporate local area networks). The routing information can then be used by the Internet Protocol (IP) or other network protocols to specify how to route transmissions. **Exterior Gateway Protocol (EGP)** is a protocol for exchanging routing information between two neighbor gateway hosts (each with its own router) in a network of autonomous systems. EGP is commonly used between hosts on the Internet to exchange routing table information. The routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen.
SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.
RIP (Routing Information Protocol) Uses distance vector (distributed Bellman-Ford algorithm). Updates sent every 30 seconds.No authentication.
OSPF (Open Shortest Path First) Link-state updates sent (using flooding) as and when required. Every router runs Dijkstra's algorithm. Authenticated updates.
End-to-end Principle: Design principle for the Internet that says you should keep functionalities at the end-hosts.
Software defined networking (SDN) is an approach to using open protocols, such as OpenFlow, to apply globally aware software control at the edges of the network to access network switches and routers that typically would use closed and proprietary firmware.

TCP flow control: receiver window. **TCP congestion control**: congestion window. **TCP window:** min{congestion window, receiver window}

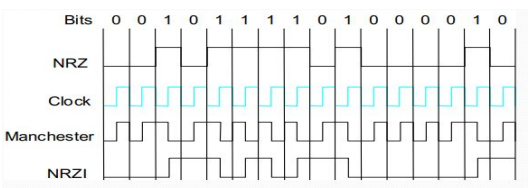
Connection and usedby:	TCP is a connection-oriented protocol. HTTP, HTTPs, FTP, SMTP, Telnet	Protocol used in message transport or transfer. This is not connection based which means that one program can send a load of packets to another and that would be the end of the relationship.DNS, SNMP, RIP, VOIP.TFTP
Usage	For applications that require high reliability, and transmission time is relatively less critical.	UDP is suitable for applications that need fast, efficient transmission, such as games. UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients.
Ordering of data packets Speed of transfer	TCP rearranges data packets in the order specified. Slower	UDP has no inherent order as all packets are independent of each other. If ordering is required, it has to be managed by the application layer. is faster because error recovery is not attempted. It is a "best effort" protocol.
Reliability	There is absolute guarantee that the data transferred remains intact and arrives in the same order in which it was sent.	There is no guarantee that the messages or packets sent would reach at all.
Header Size and Fields	TCP header size is 20 bytes. Source port, Destination port, Check Sum	UDP Header size is 8 bytes. Source port, Destination port, Check Sum
Streaming of data	Data is read as a byte stream, no distinguishing indications are transmitted to signal message (segment) boundaries.	Packets are sent individ. and are checked for integ. only if they arrive. Pack. have definite boundaries which are honored upon receipt, meaning a read oper. at the receiver socket will yield an entire mess as it was originally sent.
Weight	TCP is heavy-weight. TCP requires three packets to set up a socket connection, before any user data can be sent. TCP handles reliability and congestion control.	UDP is lightweight. There is no ordering of messages, no tracking connections, etc. It is a small transport layer designed on top of IP.
Data Flow Control	TCP does Flow Control. Requires three packets to set up a socket connection, before any user data can be sent. Handles reliability and cong. control.	UDP does not have an option for flow control

Finer control over what data is sent and when
- As soon as an application process writes into the socket
- … UDP will package the data and send the packet

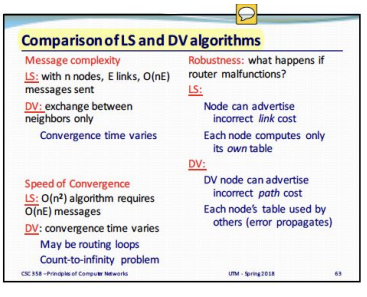
No delay for connection establishment
- UDP just blasts away without any formal preliminaries
- … which avoids introducing any unnecessary delays

No connection state
- No allocation of buffers, parameters, sequence #s, etc.
- … making it easier to handle many active clients at once

Small packet header overhead
- UDP header is only eight-bytes long



Subnet mask bits	Number of /24 subnets	Number of addresses	Bits stolen
/24	1	256	0
/25	2	128	1
/26	4	64	2
/27	8	32	3
/28	16	16	4
/29	32	8	5
/30	64	4	6
/31	128	2	7



Transmission delay – time it takes to push the packet's bits onto the link.: = message (bits)/rate (bps) **Propagation delay** – time for a signal to reach its destination: = distance /speed of flight in media How quickly a message travels over the wire. **IP address** is the address assigned to your mobile,printer or computer by the network that uses Internet protocol for communication . Your IP can change with the change in network.IP addresses are divided into classes . A,B,C,D,E mostly we use class B and D . **MAC address** is your machine address . This address will never change . It is the unique machine address given to your device MAC addresses are used at the link layer within a single network, whereas IP addresses are used at the network layer between networks.
Distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.
Best effort refers to a network service that attempts to deliver messages to their intended destinations but which does not provide any special features that retransmit corrupted or lost packets. Thus, there are no guarantees regarding delivery. The domain name system (**DNS)** is the way that internet domain names are located and translated into internet protocol (IP) addresses. The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate a website.

Error Checking	TCP does error checking & error recovery. Erroneous packets are retransmitted from the source to the destination.	UDP does error checking but simply discards erroneous packets. Error recovery is not attempted.

Otto Pilot built a home-brew network with 20 computers. The RTT between each computer is 10 ms.
- Use exponential backoff in the timeout mechanism while retrying queries. - . If a query is not answered within a timeout interval, multiplicatively reduce the maximum rate at which the client application sends query packets.

When a TCP segment belonging to an existing connection arrives at a host, in order to direct the segment to the appropriate socket the operating system's network stack uses the following fields - the source IP address. - the destination IP address - the source port number -the destination port number. -transport protocol number

TCP. Which one of the following statements is true about TCP? - TCP learns of congestion via packet loss or variations in delay - There is no performance benefit to having a window size larger than the receiver window size.

Which of the following statement(s) are TRUE?
Ethernet switches, like IP routers, use a table to determine which output links to send a packet.

Which are true about Ethernet protocols? - The Ethernet spanning tree may take a longer path through a network than that which would be calculated by a link-state algorithm (assuming both have converged).
- CRC error detection, as used in Ethernet, cannot always detect if there is a frame error.

Which of the following are true about Ethernet networks?
Bridges provide greater scalability for Ethernet networks than hubs.

Which of the following is/are true about routers?
- Routers can arbitrarily drop packets if they want.
-In their line cards, routers lookup forwarding tables in the incoming direction and queue packets in the outgoing direction.

Which of the following is/are true about Address Resolution Protocol (ARP) and learning bridges? A host's ARP table maintains state that maps IP addresses to hardware (MAC) addresses.

Which of the following is/are true about a communications channel that uses time- division multiplexing?
A. There may be times when the channel is idle, even if a sender has data to send on the channel. B. The channel requires the sender's and receiver's clocks to be closely synchronized.

How does explicit congestion notification (ECN) differ from traditional ways of … Internet paths? Describe one benefit for using ECN and one reason it might .. ECN signals to senders that congestion has occurred by marking packets explicitly, as opposed to signalling by "dropped" packets. This allows end-hosts to react to congestion without unnec. loss, especially useful, for example, when routers might be using RED, or for interactive application-level protocols such as telnet and web browsing that are very sensitive to the delay caused by loss and retransmission. ECN is not widely used today, however, in that it requires that both the sender, recipient, and network elements (routers) all support ECN, so it creates a deployment challenge.

Which of the following is true about ECN? ECN allows the router to notify the source about congestion without dropping the packet.

Which of the following is/are true about increase/decrease policies for fairness and efficiency in congestion control?
- Add. increase impr. efficiency. - Multip. decrease improves fairness.

Which of the following is/are true about DNS?
- A query for an A record may return multiple IP addresses in the response. - A short TTL on an NS record reply runs the risk of increasing traffic at the root or GTLD nameservers.

Which of the following is true of distance-vector routing (DV) in a network whose longest path is of length N hops ?
DV would still work if the metric was propagation delay.

Why don't we simply assign IP addresses to network adapters, instead of dealing with both IP addresses and MAC (Ethernet) addresses? End hosts would have to participate in routing protocol and announce addresses when they migrate, like a global ARP, which doesn't scale.

How to Forward in an IP Router
Lookup packet DA in forwarding table. If known, forward to correct port. If unknown, drop packet. Decrement TTL, update header Checksum. Forward packet to outgoing interface. Transmit packet onto link.

Congest formu:. Power = load /delay; lastbyteSent -lastbyteReceived =< CWND; TCP sending rate ~ CWND bytes / RTT sec or
R = W/RTT; # packets per window = CWND /MSS;

Which of the following is/are true about wireless networks?
- Collisions are minimized when RTS/CTS mechanisms are used.
- TCP congestion control mechanisms work poorly in wireless environments if link-layer retransmission is not performed - Wireless networks generally have higher loss rates than wired networks.

Why does TCP congestion control perform poorly on wireless networks, compared to wired networks?
TCP treats packet loss as a sign of congestion. However, in wireless networks, interference can cause packet loss. As such, the TCP sender sometimes erroneously drops its sending rate.

Which of the following statements is true about software-defined networking(SDN). Horizontal open interfaces are one of the main reasons change and innovation is easier in SDN.

What are the differences between message confidentiality and message integrity? Can you have confidentiality without integrity? Can you have integrity without confidentiality?
message confidentiality: Two or more hosts communicate securely, typically using encryption. The communication cannot be monitored (sniffed) by untrusted hosts. The communication between trusted parties is confidential.message integrity: The message transported has not been tampered with or altered. A message has integrity when the payload sent is the same as the payload received. Sending a message confidentially does not guarantee data integrity. Even when two nodes have authenticated each other, the integrity of a message could be compromised during the transmission of a message. Yes, you can have integrity of a message without confidentiality. One can take a hash or sum of the message on both sides to compare. Often we share downloadable files and provide data integrity using md5 hash sums.

Which of the following statements is/are true about physical and link-layer protocols?When many hosts seek to actively communicate, token-ring schemes can achieve higher total goodput on a shared LAN than Ethernet.

Which are true about network switches and routers?
Ethernet switches learn the location of hosts on their network by observing the frames they process.

Q) Suppose your boss calls …. . left a 250,000 byte file.. site is 2 million bits/second. Assuming that all band..
250,000 bytes * (8 bits / 1 byte) * 1/2,000,000 bits/s = 1 second

Now assume that you are sending the file via TCP, with a maximum segment size of 1000 bytes. ...How many network round trip times (RTTs)..
TCP needs to first establish a connection via a handshake (SYN/SYN-ACK) - 1 RTT TCP then enters slow-start to transmit the file, so we run slow-start either until we've transmitted the file or until we experience a loss (at 2Mbps). In slow-start, TCP will initially transmit a window of 1 MSS (=1000 bytes) per RTT, then double the window size each round (RTT). So, we have: 1 MSS, 2 MSS, 4, 8, 16, 32, 64, 128 The sum of the above 8 transfers is 255 MSS = 255,000 bytes > 250,000 byte file, so we declare ourselves finished after the 8th RTT. Thus, the total time to transmit the file would be 1 + 8 = 9 RTT.

Which of the following is/are true about web caches?
- A web cache, or proxy server, is a network entity that satisfies HTTP requests from clients. - A web cache is both a client and a server at the same time

Random Early Detection (RED). Which of the following is true?The probability of RED dropping a packet belonging to a flow is proportional to the number of the flow's packets queued at the router. -RED solves the full queue problem. -RED solves the lockout problem for TCP flows. **Which of the following are advantages that RED has over drop-tail queuing?** - Has fewer burst losses. -Ensures roughly equal throughput for all TCP flows

Which of the foll statement true about link layer protocs?When many hosts seek to actively communicate, collision will be detected, therefore each host will backup exponentially.

What is congestion collapse? Increase in network load results in a decrease of useful work done

Which of the following are true statements about reliable flooding?It is used in Link State table exchange protocols enabling routers to distribute the state of their links. - Can be achieved, in part, if packets contain a sequence number and "time to live" field to prevent packets from looping endlessly in the network

a) Suppose Ethernet was the only existing LAN technology, so every host in the Internet was part of a local Ethernet and thus had a globally-unique Ethernet address. -Flooding doesn't scale for broadcast transmission (when address hasn't been learned yet by switch) -Even if switched Ethernet, flooding doesn't scale for ARP or spanning tree. - MAC addresses aren't hierarchical – switches couldn't aggregate addresses for more compact routing tables, unless in IP prefixes. **b)What about the other way around, why do we not simply assign IP addresses to network adaptors, instead of dealing with both Ethernet and IP addresses?** Approach would give up ability to have topological addressing and hence not support aggregation, again leading to large routing table sizes. End-hosts would have to be part of routing protocol and announce addresses when they migrate, or the equivalent of global "ARP" for an IP address, neither which scale. **Would you recommend getting rid..**No. It would not scale due to (1) the need for broadcast for discovery and (2) forwarding tables would be large as MAC addresses are not topologically assigned and thus cannot be aggregated.

What does it mean for a wireless network to be operating in "infrastructure mode"? If the network is not in infrastructure mode,... what is the difference between that mode of operation and infrastructure mode?In infrastructure mode of operation, each wireless host is connected to the larger network via a base station (access point). If not operating in infrastructure mode, a network operates in ad-hoc mode. In ad-hoc mode, wireless hosts have no infrastructure with which to connect. In the absence of such infrastructure, the hosts themselves must provide for services such as routing, address assignment, DNS-like name translation, and more.

Give two reasons that sites use Network Address Translators (NATs):
Allows multiple private addresses behind single public (dedicated) address, which is very helpful if sites lack a sufficient number of public IP addresses (e.g., "space" pressure). In general, NATs have helped "scale" IPv4. NATs provide privacy about internal deployments. NATs can allow easily management of internal devices, so that machines can be internally renumbered without changing their external (public) addresses. If explicit forwarding rules aren't configured in NATs, they often provide some security mechanisms by playing the role of firewalls, e.g., only allowing TCP connections to be initiated from internal nodes, as opposed to allowing ext.l mach. to connect to internal machines.

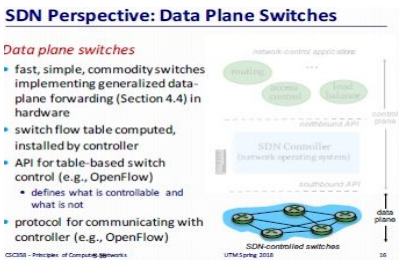
Which of the following are true about queue management and scheduling policies in IP routers? Routers implementing RED lead to greater fairness between TCP flows than those implementing drop-tail policies.

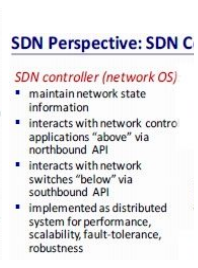
Let's now consider how TCP reacts when it encounters packet loss. Your boss now wants you to transmit a much larger file (say, 1 GB). ...How long (in terms of RTTs) will it take to reach 32,000 bytes per second again?
In that case, TCP reacts by "MD" -- multiplicative decrease -- cutting its window size by half and continuing by "AI" -- additive increase. So the next transmission rate is 16,000 bytes per second, and it will take 16 RTTs to recover to its prior levels (each RTT increases by 1 MSS = 1000 bytes).

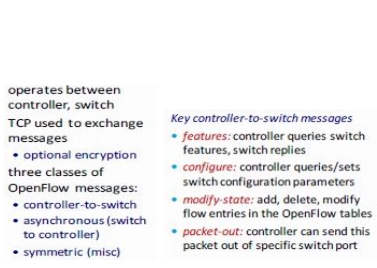
In the previous example of 1c, would anything be different if...If so, what is the next instantaneous rate TCP…. take to reach 32,000 bytes per second again?
Because all packets are lost, we only detect loss through a timeout. This causes the sender's window to be reduced to a single MSS (1000 bytes / RTT), at which time it enters "slow-start restart". Namely, it will perform slowstart until half of its prior cwnd (16,000 bytes/second), then do additive-increase from 16,000 to 32,000 bytes/second.
Slow-start from 1 MSS to 16 MSS = 4 RTTs, then additive increase 16-32 MSS = 16 RTTs Total = 20 RTTs

Which of the following is/are true about persistent HTTP connections? Only one TCP connection must be opened for downloading a "page", if that page does not include any embedded objects served by other servers.

Which of the following are true about HTTP headers and connection management? Persistent HTTP connections can have lower latency than non-persistent connections because they can avoid performing a new TCP handshake for each HTTP request. -The Host: field in HTTP allows the same web server to server content for multiple domains.







Transmission delay – time it takes to push the packet's bits onto the link.: = message (bits)/rate (bps) **Propagation delay** – time for a signal to reach its destination: = distance /speed of flight in media How quickly a message travels over the wire. **IP address** is the address assigned to your mobile,printer or computer by the network that uses Internet protocol for communication . Your IP can change with the change in network.IP addresses are divided into classes . A,B,C,D,E mostly we use class B and D . **MAC address** is your machine address . This address will never change . It is the unique machine address given to your device MAC addresses are used at the link layer within a single network, whereas IP addresses are used at the network layer between networks.

Distributed denial-of-service (DDoS) attack is an attack in which multiple compromised computer systems attack a target, such as a server, website or other network resource, and cause a denial of service for users of the targeted resource. The flood of incoming messages, connection requests or malformed packets to the target system forces it to slow down or even crash and shut down, thereby denying service to legitimate users or systems.

Best effort refers to a network service that attempts to deliver messages to their intended destinations but which does not provide any special features that retransmit corrupted or lost packets. Thus, there are no guarantees regarding delivery. The domain name system (**DNS)** is the way that internet domain names are located and translated into internet protocol (IP) addresses. The domain name system maps the name people use to locate a website to the IP address that a computer uses to locate a website.

ncrement per ACK (CWND) = MSS *(MSS/CWND) ;		**Which of the following are true about mobile devices and mobile IP: -** A home agent impersonates the network address of its mobile client while the client roams outside its home network .-A mobile client and a foreign agent can be on the same box. **Why Does Routing Matter?** 1) End-to-end performance - Quality of the path affects user performance; Propagation delay, throughput, and packet loss 2)Use of network resources - Balance of the traffic over the routers and links Avoiding congestion by directing traffic to lightly loaded links 3)Transient disruptions during changes - Failures, maintenance, and load balancing Limiting packet loss and delay during changes **Motivation for Gateways (after firewalls)** . Enable more detailed policies E.g., login id and password at Telnet gateway . Avoid rogue machines sending traffic E.g., e-mail server running on user machines . Enable a central place to perform logging E.g., forcing all Web accesses through a gateway … to log the IP addresses and URLs