2018 exam :

Application , presentation , session , transport , network , datalink , physical

Caesar cipher is an example of a substitution cipher , where plaintext is converted to different, unintelliglbe characetres called ciphertext. This is encryption . the characters are all encrypted using the same rule (Eg + 3) , to create a new message in ciphertext. Caesar text has the problem that it can be broken by frequency analysis, because of how easy it is to spot common letters. Since the frequency of letters doesn’t change, it will be easy to guess common characetrs such as spaces , ‘a’s or ‘e’es. This makes guessing which letters are which much easier .

In the asymmetric key cryptosystem, there are 2 differnet keys, a public and a private key. The public key is only able to encrypt data to transmit, whereas the private key is only able to decrypt data. The public key (encryption ) is publicly distributed and the private key ( decryption) is kept secret.

Distingusih between circuit switching , message switching and packet switching :

Circuit : message is received in the same order it is sent . example is the telephone system . establish a connection , use it , release it. Connection-oriented service .

Message switching : connectionless service . whole message is sent to a node, received and stored untilthe next node is available to be sent . message may be sent over several routes . takes a longer time.

Packet switching : mix of connectionless and connection oriented . message is split into packets and sent individually/indepentendyl of each other . each packet is sent and received and stored until it can be transferred to next node. Packtes may different routes .

Distinguish between static and adapative routing : dis/advantages too

In static routing , it assumes that no nodes are added/delete from the network , as the routing table is created once the network is created. If any are added or deleted , the routing table has to be manually updated. It costs to add and remove nodes. Static oruting is good for a network that isn’t expected to change , however when it does need to change , it costs .

Dynamic routing allows a routing table to respond to changes , and update it . it is difficult to implement efficiently , as it increases network traffic due to the updates . its good for a network that changes often , however hard to implement and can increase network traffic .

How does distance vector routing protocol work ?

Backwards search to learn the cost of each of its neighbours and work out the shortest back to the source . each routers sends each neighbor its distances so a router can keep updating the rotugin tbalbe and this protocol can be accurate . was used in arpanet. Each routeruses an echo packet to learn the codt of its neighbours . if a route exists and its smaller than the current cost , update to new route .

Give three reasons why IPv6 can route packets more quickly than IPv4 .

IPv6 can route faster because the fragmentation doesn’t happen at routers , its main job is just to route packets . IPv6 only has 8 fields and less data. No header checksum in IPv6 .

<http://reubencrimp.com>

Explain how fragmentation is done at the IP layer in IPv4 and IPv6:

IPv4 routers perform fragmentation whereas in IPv6 routers simply drop their packets if they are alrger than the MTU . For IPv6 the endpoints is where fragmentations happens , source and destination , and the fragmentation is stored in an extension header rather than the basic header . In IPv4 the packet contains all information in the header to allow routers to to perform the fragmentation .

Distingusih between IP name , IP address and MAC address.

Ip name : the url of an IP so google.com

IP address : a 32/128 bit number : 139.80.256.25

MAC address : usually in HEX , the mac address is 48 bits and is permanent . eg 00:1B:XX:XX:XX:XX ( 6 octets)

How to map an IP name to its IP address, and how to map an IP address to its MAC address:

IP names are mapped to addresses by the DNS (domain name system) which is a hierarchical distributed database system. When you query a name sever, the name server either returns the IP address or it passes the query to a higher layer , recursively until the IP is returned . otherwise the query fails.

IP addresses are mapped to MAC addresses using ARP . when a router receives a frame with the destination IP address of a device in its LAN , it queuries all devices in the LAN with the IP address to see if it matches a MAC address . the relevant device responds with its mac address which the router sends the frame to.

What is the transport layer address?

A port . from 0 to 65535 . there is one IP address per device, but multiple ports. Transport layer deals with process-to-process interaction , and since a device can have mutlie process running , there needs to be multiple layer addresses per device : hence the need for ports.

Describe 3 major functions performed at transport layer :

Setup/release connections

Flow control between end users

Error detection . correction : guarantee error free transmission between source and destination.

Qualty of service . reliability, delay , thorugput.

Explain how TCP deals with lost segments and duplicated segments.

Each sent segment has a sequence number included in the header which can be used to determine if a received segment is out of order or duplicate . duplicate segments are discard by receiver.

When the sender sends a segment, it starts an RTO timer and if it doesn’t receive an ACKsegment for that sent segment before the RTO timer expires ,it auto retransmits .

Distinguish between IP name and IP address .

IP name is a domain name that humans know and can input into a browser to access .

Eg [www.google.com](http://www.google.com)

An IP name is translated to an address using DNS (domain name system)

IP address ist he actual address of the website that the compiter understands . for example 192.168.12.2

application presentation session transport network datalink physical .

application transport internet network access layer .

reduces complexity , makes it easier to create functions , provides compatibility , accelerates evolution of tech, simplifies learning .

key features of WSNs , give 3 apps :

three applications , fridges with wifi , auto driving cars , smart house . internet of things . traffic control .

Drawbacks of current network architecture :

HCII . closed equipment ,vendor capture can lead to equipment whichi s only compatibility with that brand . exampes are apple . inconsistent polocies . inability to scale , because of no central planning or direction . ist just growing by itsel f .

Software defined networking advantages can overcome such drawbacks :

Software defined can let us have a break from hardware issues , allowing admins to control applications and networks created from their physical location and takin advantage of shard computing power .

What is mimo ? explain how It owrks.

Multiple input , multiple inoput . all data is sent down mult’iple pathsb( multiple propagation ) and the receiver reconstructs the message from the combined signals . the idea is that some paths are stronger than other s , so sends down own to find fastest route and compensate for weaker paths . MIMO can also use ‘spatial multiplexing ‘ i.e sending different info along each singal path to speed up data rate.

Key idea of code division multiple access :

One channel occupies entire bandwidth , every station can broadcast simulataneously . enabled by having each station with a unique code. If you multiple a station by another , u get 0 . if u multiply a code by itsel,f u get the number of stations .

Explain why the hidden station problem can degrade WANS . How would you solve by using RTS/CTS handshaking ?

Hidden station occurs when 2 stations can see 1 station in common , but not each other. Problems occur when the 2 staitosn try and send information simulaaeneously . this will cause interference and the middle station will notbe able to receive all the information successfully . one solution is to use request to send and clear to sends . sending station sends a request to send to the receiving station , and if the receiving station is free it will senda clear to send bakck, and the sender transmits . allows hidden stations to synchronize their broadcasts in a non-ointerfering order, without ever even knowing the other statin is there.

Direct-sequence spread spectrum : DSSS takes each indivudal bit and splits into a pseudo random bit string of length n. this string is called a chipping sequence . the original bit is then combined with the chipped sequence (eg using XOR) which creats a chip code . this chip code is broadcast.

Frequency hoppign spread spectrum means broadcasting over several channel in the broadcast range , in a pseudo random order . broadcast begins on one channel , then after 1T it switches to another channel , and broadcast, waits 1T , then another . the sequence of channels is determined pseudo-randomly and is known to the receiver and sender.

SMTP : clients can send and receive emails from sender to mail server, then mail server to recipient. Port number 25 .

POP is protocol used for connecting a client to a mail server and allows the client to download mail from their server side mailbox to their local mailbox. And not synchronized .this means if u download or delete on ur local mailbox it may not delete or server side, so if u log into other device they wont have deleted .

Explain firewals :

Its like a digital bridge . anything wanting to get in or out needs to be checked to make sure it is not malicious or sensitive information we don’t want getting leaked . be inspected . admins can set up blacklists to auto stop any recipient/sender or whitelist to allow . to restrict files enter and exit network .

Explain how TCP deals with lost and duplicate segments :

TCP has a sequence number to check for any missing segments . it can tell if the received segment is duplicate or out of order . TCP discards any duplicate segments . buffers a out of order segment .

When the sender sends a packet, starts with an RTO timer . retransmission time out , if it doesn’t receive an ACK by the time the timer expires , it will retransmit it and presumed lost .

Describe functions at the transport layer:

Flow control . provide flow control between end users .

Error control . guarantees error free data transmission between source and destination .

Quality of service.

Connection management . set up and release connections

What is a transport layer address? Why are they needed?

A port is a transport layer adderss. There is 1 IP address per device, but there are multiple ports per device. The transport layer deals with process-to-procss interaction , and since a device can have multiple processes running concurrently , it may need multiple ports per devices .

How to map an IP name to IP adderss and IP address to mac address..

An IP name checks the distributed database in the domain name system for its IP , and if its not found , it recursively goes up in the hierarchy until it is found, else it’s an error . you query and try and find the IP address .

An IP address are mapped using the ARP . address resolution protocol . when a router receives a frame with an IP address attatched , it sends the IP to all devices querying whether a device has that matching IP address ,and it returns it MAC address if its that one , and the router routes the frame to it .

Distingusih between IP name and IP address and MAC address

IP name is the Uniform resource location of an IP address s: [www.google.com](http://www.google.com)

IPaddress is a 32bit (IPv4) or 128 bit (IPv6) address : 139.131.12.32

Mac address : in hex, 48 bits and permanent . eg having 6 octets in hex eg BB 54 4F 23 FF AA

3 reasons why IPv6 can route better than IPv4 :

Shorter frame format ( 8 fields compared to 13 )

No header checksum in IPv6

Fragmentation doesn’t happen at the router , happens at source and destination .

Explain how fragmentation si done in IPv4 and IPv6 :

IPv4 perform fragmentation at routers , if the packet is larger than their MTU (maximum transfer unit ) ( in bytes ) . in IPv6 , routers simply just drop packets larger than their MTU and tell the source that . for the IPv6 the end points are responsible for fragmentation . IPv6 fragmentation is done at the source of the packet , and includes info to reassemble the packets in the extension header.

Benefits of hierarchical routing : smaller sizes of routing tables . substantially less calculations , and don’t have to update each table , just the affected one . auto does the othes .

Link State Routing :

1. ) node gathers info on the status of each link to each neighbor.
2. the node builds a link state packet for each link
3. a node receiving link state packets forwards them to all its neighoburs except the one from which it received the packet .
4. as link state packets are exchanged among nodes , each node eventually learns about the whole topology , and the cost and status of every other node.
5. Each node can execute a shortest path algorthimth such as dijkstraas to create its routing table.

Differences between switches and routers:

Routers create routing tables and send frames , responsible for routing packets from sources to destination . operates on network layer . addresses data by IP address.

Switch : operates on data link layer . connects comps in LAN . address data by MAC in oruting table .

Connects to other switches in a tree structure . pretty much a bridge with more ports and no protcoo lconeversiains .

How are loops eliminated in LANS ?

Minimum spanning tree algorithm. Associates a cost to each node with each bridge port . then creates a graph of the topology of its costs . eventually the algorithm tunr sthe graph into one in which the cheapest briges interconnecte the network with no loops .

Explain the flooding algorithm used for routin in bridges : every node broadcasts what they know about the cost and destination and stauts of each other node so it creats a bgi picture of the neetwork .

Describe how go back n and selective repeat would work differently with out of order frames . in selective repeat , frames can be sent in any order. Receiver keeps the frame in a buffer window so it can reorder any out of order frames before passing to device. Sender and receive both have a window. When the window gets an in order packet , It sends an ACK and shifts the window along so it cant receive more . each frame has an RTO , if its doesn’t receive an ACK for each frame , it retransmits just that frame .

Go – back – n must be in order .

If the sender receives an out of order frame, sends a NAK back to the sender, requesting the correct frame . if it receives the right frame, sends an ACK frame and knows all frame until j have been received properly . 2 timers . RTO , in which it sends the whole window again if it doesn’t receive a ACK for them . the receiver h as atime to wait for data , if it doesn’t receive data before the timer expires , send a blank ACK . when 3 duplicate ACKs are sent, whole thingi se sent again .

In frame format, there is an ACK field for piggyback . explain .

Sender can send data and an ACK in same frame so it is quicker and more efficient. In the ack field , adds an intgeger to it to say ‘yo I got frames 123, 124, 125, cant wait for 126’

What is p persistent CSMA ? if there are 2 stations using it , whats the probaoblitlity that one sation will tranmist successfully .

Even if the receiver is idle , the sender will use a probabliltistic chance whether it sends data or not . there are 4 possibilities when station have 0.5 persistnece : A sends , B waits , A waits , B sends, both transmit and it fais , both wait and transmit with 0.5p .. 0.5 chance of success .

Explain diff between aloha , slotted aloha and csma

Pure aloha : transmits when it wants to , waits for an ACK . if ACK not received then wait a random time and retransmit . a collisionin pure aloha wasts up to 2T time , where T is the time transmitssion takes .

Slotted aloha : if theres a collision, wait time T before transmitting again . slotted time slot . senders can only send at start of time slot.

CSM : checks to see if anyone is transmitting before transmitting . non-persistent, checks the medium ,if its busy, wait random time , check again . persistent :keep checking til its idle then use the p-persistent method .

Explain public and private key :

Asymmetric key cryptosystem . 2 diff keys , public and private key . public key is only able to encrypt data and the private key is only able to decrypt data . the public key is distributed publicy and common knowledge whereas only he receiver knows the receving key ( for decryption n)..

Pros : only public key must be sent . cant find private key unless you get o the source . incalculable amount of time to crack it .

Cons : very slow to work out . no authneticaniton ( no guarantee who the file is from when the encrypted key is sent back )

What is Caesar cipher ?

Example of a substitutin cipher . which encryptes plaintext by same equation . rule set . eg +3 . letter frequency stays the same . allows you to guess common rules like spaces , a’s and e’s .

Transposition ncipher : orders charactes in a 2d array and sends the arrays in random order. Hackers can try and order the columns so it says ‘the ‘ or ‘ing ‘ or common words .

Bit level ciphers recognize not all plaintext will be characters. Happens on a bit level . performs an XOR betweendata and key . problem is the short keys may result in common substrings and hackers can spot .

Application – human computer interaction layer

Presentation – ensures the data is human readable , encryption , trnalation

Session – maintsains connectiosn and is responsbiel for controlling ports and sessions

Transport – transmits data using transmission protocosl including TCP and UDP .

Network – decides which physical pathseach frame will take

Datalink – defines the format of data on the netowkr node to node .

Physicaltransmits the raw bit stream over the network . bit to bit .

User datagram protocol : simple interface between IP and higher layer protocols .

Key idea of software defined networking

Allows admins to manage network services through abstraction of lower level functionality . create an operating system for networks . allows admins to directly monitor everything . how packets are routed .

MIMO ?

Multiple input , multiple out.

Sendig data down multiple paths . uses spatial diversity . use multiple paths to send the same signal and the receiver reconstructs the signal from all the partial messages it got from each path . spatial multiplexing to decrease the amount of time it takes to transmit the signal . increases data rate.

Frequency-reuse principle ?

Neighoburing cells cannot use the same set of frequencies for communicaition . set of frequencies avialabe is limited and a frequency reuse pattern is a factor of N cells wher N is the reuse factor .

Explain hidden station , and how CTS / RTS helps :

Different stations have diff transmission ranges .

If 2 stations both want to talk to a mutual station but cannt see each other , they wont know when the station is free to receive data . if they both send data there will be issues on the receiving end with colliding received data dn can cause data loss .

So a statiin sends a request to send frame . if the station isn’t receiving from anywhere else , it sends a clear to send and the station can send data .

Frequency Hopping Spread Spectrum :

FHSS operateas on a set of frequencies that all lie in the broadcast range . key idea is that the signal being transmitted can be less prone to interference while also making it secure as an intruder would only be able to listen to a small part of the signal . transmits using one frequency for a fixed time slot , then uses a pseudo random generator to hop to another frequency and broadcast on there . repeats . uses pseudo random generator with an algorimth the receiver and sender know so they can be on the same frequency .

SMTP : port 25 . secure . SMTP retrieves mail and establishes a connection via TCP and then delivers via its protocols . client sends a user/pass to authetnticate the session , the server then authenticates and transfers message to the client, then logs the client out .

POP : people connect to a mail server and it allows the client to download the mail to their local server . changes are not synchronized back to the user . causes issues when u use email on more than 1 device .

Internet mail access protocol : server that can be accessed by multiple client . uses web email apps . changes are synchronized back to the major copy on the mail sever .

Multiplepurpose internet mail extense : used to encode binary data and specify the schemes used in the body .

POP : extracts and retrieves from a mial sever . not synchronized .

IMAP : always synched with mail server. Multiple clients .

SMPT : simple , not synchronized .

Telnet is not secure . nothing , not even user/pass when a client logs into Telnet is encrypted . no guarantee not sunject toa man in the middle attack listening to yoyur data .

Ssh is an cryptographic network protocol used for data communication and remote command line that aim to fix this :

2 ways to use SSH .

Automatically generate an asymmetric key pair and use a pw

Manually generate an assymetric pair .

Auto : server encrypts a message with users public key and receiver decrypts using their own private key and returns to server , proving their identity .

Manually : server supplies client with its host key and user comparesthis against his own database to check it wasn’t change . client generates a 256 bit random number and encrypts with this to use as a session key .

How TCP deals with lost segments and duplicated segments :

When a frame is sent , an RTO timer (Retrnasmssiiin time out ) timer is startedand if it doesn’t receive an ACK by the n , it retransmits . if 3 ACK’s arerecevied , retransmits .

Each segments has a sequence number ,fi receiver receives duplicates frame it will discard.

Congestion contro l :

Slow start, cwnd starts with a maximum segment size of 1.

As frame are received , MSS increases multiplicatively so its exponential . slow start but grows fast.

Each time there is a collision the size of the threshold is dropped to one half . when the size of the cwnd reaches the slow start threshold , the slow start phase stops and the additive phase begins .

What is a transport layer address ?

Port number . 16 bit integer between 0 and 65535 . used to choose among processes on the same host / device .

Domain name system : converts IP names to IP address . scheme that allows to query a IP name and waits for a return of an IP address . recursive .

IP name : [www.google.com](http://www.google.com) , domain name humans can understand .

IP is translated to an IP address using DNS

IP address is the actual address of the website the computer understands . 32/128 bit s .

IPv4 and IPv6 .

No header checksum in IPv6.

Fragmentation doesn’t in ipv6 , router simpy drp[s the packet . uses extension header if it wants to do fragmentationat eache end .

IPv4 will fragment packet in router and includes info in header on how to reassemble at other end .

IPv4 is 32 bits , IPv6 is 128 .

IPv4 has 13 fields . IPv6 has 8 . simpler.

IPv6 is more secure . more addresses .

IPv6 can coexist with ipv4 .

How does distance vector routing protocol work ? :

Backwards search . each router uses an echo packet to learn the cost of each of its neighbours .

Each router sends each neighbor a list of what it knows about each other and so each router can make a routing table most update .

So if a shorting route is foud , it will be updated and used .

Distinguish between static and dynamic routing.

Static assumes no nodes will ever be insert/added . created once . has t be changed manually . costs to add remove nodes . good for networks that don’t change often , bad because it costs when networ changes.

Dynamic is constantly being updated when nodes are updated . upates routing tables . difficult to implement efficiently , increases network traffic due to routing updates.

Good for a networkthat changes a lot , bad because its hard to do efficiently .

Distinghuis between ircuit , messsge, packet switching.

Circuit switching is based on the telephone sysmte (eg ) . a physical connection must be made before the transmission can be started . establish connection , use it, terminate . connection oriented . message received in same order as sent.

Message switching . stored at each station until a route is available. Whole message is sent at once . send entire message and router stores message until next route is available. Example is the postal system .connectionless.

Packet swtich : message split into packets , each packet may be sent in different routes . packets can arrive out of order and mst be buffered til they all arrive. Both connection oriented ad connectionless.

Switch : operates on datalink layer . connects multiple devices, manages prots . pretty mucha bridge, but more ports and no protocol conversion . uses physical (MAC address)

Router : operates on network layer . uses IP address ( logical ) . sets routes for packets to be sen . knows how to get to various network s.

Spanning tree algorithm :

Gives some nodes and connections to create a graph that shows the minmum overall cost of getting fro m A to B , or a whole network to be connected . cannot be the minimum path as the nodes would still be connected if u took away one of the connections in the loop .

Dijkstars in a na example . associates a cost with each bridge port .

Explain route learning :

As frames are sent around the network the bridges build their own routing tables . they do this by examining where each packet is coming from .