Application , presetntiaton, session , transprto , netowkr , data link , physical

Why use ? makes understanding it easier .. splits it up so creating/defining functions is simpler and specific to each layer . easier to debug. Provides compatitibility , accelearets evolution of technology , simplifies learning

Caesar cipher . example of a substitution cipher where each plaintext is displaced by a set amount (e.g +3) . frequency analysis can crack it , because letter frequency stays the same for the message. So spotting common patterns, or figuring out where spaces are makes it very easy to guess which letters are which . or guessing common letters like a , e , space ‘the’ etc.

Polyalphabetic also substitution cipher , uses a matrix the letter frequency so the plaintext is not always replaced by the same character. Can be spotted because looking for clues is easy. Eg TIG is always alphabetically successor to SHF.

Transposition is done by rearrange the plaintext of a message, ordering the characters in a 2d array but sending the columns out of order. Letter frequencies will be the same, implying a transposition cipher was used . to decode , try and array he colums in order so it makes common substrings like ING , THE , IS , etc.

Bit level uses the idea that not all data are characters. The cipher performs an XOR operation between the dat and key. To decrypt , perform the same operation . short keys may result in repeated strings , which would help break aptterns. Performed on a bit level. Can be used on any data type which is good .

Data encryption : process of turning information (plaintext) trhough some rule , to create unintelliglbe ciphertext that is unreadable without the key. Data decryption is the opposite, takng the unlegible ciphertext and turning it back into readable text that anyone can understand.

Data Encryption Standard (DES) is a compelx combination of transpotisotn, subsitutibon s and XOR operatins to produce 64 bits of encrypted data . it is divided into 64 bit blocks and uses a 56 bit key (2^56 possible keys) . its not sufficiently secure and can be broken in a few hours on massive computer.

Private key encryption : SYYMMMETTTRRIIICCC sender and receiver share the same encryption/decryption key (eg Caesar cipher ) . keeping the key secret is vital as anyone can decrypt the messag if they get the private key.

Public key encryption : sender and receiver uses AASSYYYMMETTRC keys , and the encryption key cannot be used to decrypt the message. The receiver sends the user the a public key to encrypt the plaintext , and uses their private decryption key to decrypt the ciphertext.

RSA algorithm dis : really slow ofr high data rate . don’t have to send private key . only pub

Adv : super safe . no one can be bothered to hack shit cause its takes ages

Authentication : a digital signature is when the s]ender signs the messag e using their public and private key and only they can decrypt the signature. Proving they sent the message. A message ‘digest’ is a smaller sm=ummar of the message , using hashing algorithms . its encrypted using the sender private key and sent to the receiver . the receiver then uses the senders public key to decrypt the digest , and then uses the same hashing algorithms the public key used on the mssage digest to see if it produces the same message. If they’re not exactly the same, the message has been tampered with.

comp

Prety good privacy : combination of hahing , compression ,symtettic key cryptography and phblic key cryptography. the mssage is encrypted using a symmetric key encryption allalgorithm , which requires a symmetric key (each key is a session key an only used once ) . the session key is encrypted using public key encryption . the encrypte message alng with the encrypted sess ion key is sent toth receiver . mixing algorithm strengths and weaknesses in others , its one of he strongest and fastest encrypting algorthms .

Netowkrs : an internconnection collection of autonomous computers that exchange information online .

Star : centralized , all computers go through central station . if the central goes down, all goes down . can all be responsible on central one. All monitored through it .

Bus : devices communicate through a single bus , and the only communicating dveices are involved . easy to add/remove devices . if all devices try to send data, the data rate will be slow as and have to wait for other devices . maybe high collisions rate

Ring : devices are connected circularly, unidrirecitonally or bi-direftionally . no focal point but failure of a dveice will cause a break . it takes lpmger to send information through this type of network .

MAC : media access control . creats a shared medium that multiple devices can acess .

Random access protocol s ; no scheduled time for a station to transmit , and they compete to send data and access other statiosn acrsossth medium ,.

Pure aloha : each station transmits whne it has a station to transmit . whne the receiver gets a frame, it sends an acknowledgment tot the sender. Otherwise th e receiver assums a collision and retransmits . if a collison occurs , it waits a random time before retransmission

The randomeness helps minimize collisions . the protocol works best when there is minimal traffic . a collision wastes up to 2T time .

Slotted aloha protocol . divde time intervals into T units each . and each station only sends one at the bgeginng of each slot , not randomly. Wasted time due to collisions is reduced to T . higher success rate than PAP .

Carrier sense multiple access ( CSMA ) : if a s\tation has a frame to send , it first checks the status of the medi um , if there is no activity , itr transmits .

Non persistnet : if te medium , it ways a random amount of time and then senses again . reduces collisions but reduces efficiency.

Persistent : it continuously senses until the medium is free .

p-Persistent CSMA .- continues to monitor until its free . when it is , transmits with a probability p , otherwise waits for the next t time slot (probability 1-p) and repeat . ifp = 1 , it is 1-persistent CSMA and will alays tranmit when the medium is free . if p=0 , it is 0-persistent CSMA and will always wait 1 time slot .

collisins will still occur , and if p = 0.5 tand there are 2 stations , 4 possibilities exist whn th medium beceoms idle : both transmit immedialy , both wait, station a waits and b sends, station b waits and a sends . result : 0.5 probability one will transmit successfully , 0.25 prob wont be used , 0.25 probability pf collsiions .

CSMA ( carrier sense meultiple acces s , with collision detection ) : if it detects a collision when transmitting the frame, it stops the transmission and sends a short jamming signal . if it receives a short jamming signal , it stops the transmission. After a collision occurs , it waits a random amount of time according to the binary exponential backoff algoritm then repeats the above steps .

Binary exponential backoff algorithm : if a stations frame collides for the first time , wait 0 or 1 time slots. After n collisions , wait 0 to 2^n-1 slots if n<=10 if n > 10 then wait from 0 to 1024 slots . after 16 collisions , give up and report and error

Controlleda-access protocol s : opposite of random .

token passing . statiosn are ordered into a logical ring , and has a token ( a speicla frame ) that circulates the rging. A station can only transmit data when it has the token frame . when it receives the frame and wants to transmits the data , it insers the data into the token frame (now a data frame) and passes it to the next neighbor . when a station receives a data frame and is the destination station , it copies the data from the frame to its memory and passes the frame to the next neighbor . if it s the sender of the data, it removes the data from the frame ( making it a token frame) and passes the token to the next nehighobur .

Slotted ring : same as token passing except it contains several rotating token , a station cannot send any other frame until the previous data frame it sent returns back to the sender.

Ring problems : a break in the ring can bring the whole network down . like a ring topology.

A fault interface card can result in a lost/ imporpoerly formatted token .

If a station sends a data frame and fails before removing its datam the frame circulates forever

FDMA TDMA CDMA ?

Code division multiple access , usingonly once channel occupies the entire bandwidth, and all stations can send simultaneously . each station is assigned a code, and 2 properties on the codes. If you multiple the code by another you get 0 , but if you multiply each code

by itself , the value you get is equal to the number of stations .

Flow and error contro l :

flow control the way multiple frames are sent and tracked and when to stop/send the frames .

error control defines the how to check the frames for errors and what happens if there are errors. It ensures all frames arrive at their destination ,without errors. All flow and ctornol belong to the data link OSi MODEL LAYER !!!!!!!!

a frame is a group of bytes organized according to a specific format ( eg ethernet ) and can be carefully formatted for flow and error control . data is transmitted in frames at the data link layer : source , destination , number, ack, type, data , error checking bits .

unrestricted protocol : assumes the receiver has unlimited memory capacity and doesn’t consider any problems in transmission . just keeps sending data dn more data data ….

Stop and wait protocol : the sender transmits a frame and then waits to receive an ACK frame before it transmits the next frame. The receiver simply just needs to send an acK frame for each frame it gets. The sender sets a timer for the frame setn and if no ACK frame is received by the timer expires , it retransmits the frame .

Measures of protocol efficiency : unresetricted uses as much buffer space as it requires . stop and wait only needs 1 frame buffer .

Unrestricted is tranmsisting data frame 95% of the time . (7.6mbps)

Stop and wait ony transmits 75% of the time (5.7mbps)

Sliding window protocol : compromise between unrestricted and stop and wait.

A window is defined as a subset of consecutive frames. The window contains I frames numbered starting with w : every frame numbered less than w has been sent an acknowledged . no frame numbered bigger than w + 1 is sent. Every frame in the window has been sent, but not all acknlowedged , these are outstanding frames . if frame j is acknlowedgded , the window moves down to j+1 so more frames can be sent.

Analysis : it alllws multiple frames to be sent, without needing to wait for them to be acknowledged . if the maximum number window size is 1, it is the stop and wait protocol,. If it unrestricted size, it is the unrestricted protocol. Adjusting the window size can help control the traffic con a network .

Go back N protocol : frames must be received in the same order as they were sent, and the sender buffers the frame in the window in case it has to resend them,. When the receiver gets a frame, if it is out of order it will send a NAK . if the frame is the expected one , it will send an ACK . the receiver uses the piggyback approach for acknlowedlgements wherever possible (Send data too ) .

When the sender gets a NAK , it will resent all frames in the window, if it receives an ACK for frame j, it knows all frames before j were received so it increase the window size to j + 1 , so more frames can be sent.

A frame timer is used , and the sender will retransmit all outstanding frames if it does not receive an ACK . an ACK timer is also used , and the receiver will send a separate ACK frame if the timer expires.

Selective repeat protocol : this protocol allows the receiver to receives the frame out of order and sort them before the delivery to the user . the receiver uses a window to buffer out of order frams. The receiveing station window buffers all the frames into the correct order once all the frames have arrive dsuccessfully. When an out of order frame arrives , it sends a NAK for the expected frame, and sends an ACK when the expect frame arrives correctly . the sending station resends just the frame it received a NAK for , and reseneds the timedout frame if a frame time expires.

Sliding window size: the sending window of go back n must be less than 2^k and the receiving window is always 1.

Both the sending windows and receiving windows of selective repeatmust be at most ½ of 2^k

Ieee 802.3 ethernet bus

Ieee 802.5 token ring , ring topology

IEEE 802.3 standard for ethernet , uses bus . can be extended by repeats . CSMA/CD protocol . in the physical layer of the OSI model . uses coax , twisted pair or fibre optic cables. It uses Manchester digital encoding . a repeater (device that receives and retransmits signal )

Hardware components network interface card . receives packets from PC software. Formats frame . executes binary exponential backoff algorithm , performs CRC error checking . a MAC address is a uniqure address assigned to a NIC . to communicate with transceiver .

Ethernet hardware address : six octects . 2^48 . 56,000 MAC addresses for each person on the planet .

Transceiver . interface between PC and cable . listens for collisions . puts bits on cable from interface card . cable has 5 twisted pair, 2 for sending data dn control , 2 for receiving , 1 for power.

Ethernet frame format : preamble , start of frame delimeter , destinationaddress, source address, data field length , data fiedld , padding , frame check sequence .

Advacnce ethernet techniques : fast ethernet 100mbps : mainly differ at physical layer

Gigabit ethnert : burst frame for sending multiple frames , full-duplex mode with CSMA/CD

10 gigabit ethnert : for backbone network , no CSMA/CD

IEEE standard 802.5 : standard for token ring LAN , consisting of point to point links . it can be coax, twisted pair or fibre as well . . token means no collisions . any failure in a station can bring down network . DIFFERENTIAL]Manchester encoding . most 802.5 lans use wire centres to improve reliability – wire centres can bypass a failed station .

Token frame format : starting delimeter . access control . frame control . destination address , source address , data , padding , frame chec k sequence (CRC) ending indelimeter . frame status (data or token ? )

Ring maintenance :

Designates a monitor host to monitor and keep check on the ring . an orphan frame is a data frame that cannot be sued cause the parent died and no longer available. To make sure a token is always circulating , monitor sets a timer ewhenerver it sends a token or frame and if the timer expires before the montiro recievse the frame, sends again .

Fibre distributed data interface ( FDDI ) : modellleed on token ring . high data rates or distance up to 200k . up to 1000 hosts can connect .

How are loops eliminated in LANS ? the spanning tree algorithm . associates a cost with each bridge port. Then creats a graph of the topology with each cost . eventually the algorithm turns into one in which the cheapest inerconnect the network with no loops .

Flooding algorithm in bridges: every node broadcasts what the yknow about each neighbor , giving an overall picture of the netowkr . a mimimum spanning tree is made from this .

WANS :

Repeater . reconstructs signal and retransmits

Bridge : connects LANS or a router and the internet, filters using MAC addresses

Switch : operates on data link layer . very similar to a bridge. Connects LANS and allows connections to multiple devices . manages ports . no protocol conversions . switches can link to other switches following a tree format. Addresses devices by MAC address .

Router : connects different types of LANS and maintsins routing tables . sendings routing packets using IP addresses. Operates on network layer .

Difference between switch and router : switch operates on DL , router on N , routers are used to route packers between LAN’s , creating a WAN , address data by IP address.

Gateway : uses character codes, encryption , compression. Has different rules for establishing connections and being secure.

Connection types : connectionless and connection oriented .

Connectionless : similar to postal system . not a set route , independent routes to other messages. Order of messages not guaranteed . independent packet is datagram .

Connection oriented : received in same order as sent . telephone system. Establishh , use , release.

Switching :

Circuit : physical connection is established before statrt of communciaiton . telephone system . constan\t bit rate . type of connection-oriented service : used solely by the communicating devces..

Message switching : connectionless . the whole message is stored and then forwarded to t he next switch whne route is available . message may travel over differnetnt routes . disadvantage is that a long message may occupy the route for a long time.

Packet switching : message broken into packets and sent independtely of each other . packets received and stored until they forwarded to next. Connectioneless and connection-oriented.

LANS vs WANS :

Protocol conversion . simple in LANS bridges . convers between different LAN protocols in WANS routers.

Routing : simple in LANS according to LAN address ( eg ethenet address ) . complex in WANS according to WAN addreessse (eg ip) much morecomplex strategeies and can experience failures easily

Routing : routing metric is the major factor. Includes : length of path, number of hops , transport time , in-route delays . in routing tables , specifcy next hop node and distance / cost.

Centralized routing : global routing is created and maintained by a central device . all devices look to this table so they can create their own routing tables.

Distrbitued routing : no central control . each node must detmerine and maintina its own routing table . they need to know its neighbours and cost of getting to tehm . shares routing tables with neighbor so they can be more accurate .

Static routing : each routing tables is created once and assumes conditions never change . has to be updated manually. In reality , many nodes are inserted/deleted and costs will change.

Dynamic routing : will update when nodes are inserted/deleted automatically , hard to implement effectively because of network efficiency and will increase network traffic .

Centralized : simple – failure of central has severe effect

Distrubted – failure of node has no effect – exchange of information is complex

Static – simple , don’t have to keep running routing algoritmhs

Dynamic – always updating – high overhead and network traffic

Routing algorithms : process of selecting paths in a network along which to send network traffic . determines best route , creates routing tables.

Dijkstra’s from 242 . finds shorted path . centralizd algorithm .

Distance vector rotug in : basic idea is to backwards search to learn the cost of each of its neghbours . assembly line schedulinggggg . each roiuter sends each neighbours list of estimated costs of all destination it knows about . each router keeps updating table

Link stating routing : each node gathers information on the status of each link to each neighour , buils a link state packet for each link . identifies 2 nodes connected by the link and info about link. A node receiving these packets forwards them to all neighbours . each node can exectte dijkstra’s to determine its routing table .

Heiercharcical routing : might be too many nodes for each to have a complete routing table . nodes are divided into groups called domains . each domain is independent and separate network . routes beteen two nodes in a common domain are detemniered usignthe domains protocols .

Advantages of hierarchical routing : smaller sizes of routing tables. Substantially lesser calculations and updates of routing tables .

Routing in internet : autonomus system : a group of netowkrs and routers controlled by a single admin authority .

Intra- AS protco l : Routing information protocol : distance vector (RIP)

Open shortet path first (link state routing )

Inter-as : border gateway protocol : path-vector rotugin .

Internet Protocol : unreliable connectionless protocol that uses packet-switching . provide a datagram services between station , delivering packets , making routing decisions . packetrsarent guaranted to arrive in same roder.

IPv4 :

20-60 byte header and 536 bytes of data .

Address classes : class A , 8-bit network address , 24-bit node ID address, 126 networks of 16 million hosts .

Class B : 16-bit netowkr addres , 16-bit node ID addres, 16,384 of 64k hosts

The others are heaps of them

Problesm : only 2^32 addresses , so many organisations got a class B network because all of class A was being used . IPv4 cannot meet the requiresmnets of multimedia applciations , as theres no constant bit rate guarantee . its not very secure and doesn’t have good support for host mobility.

IP routing : an ip router keeps track of other networks and all local hosts by using routing tables .

Routers actions : verifies the checksum , decrements the time-to-live field, recomputes checksum , hten it extracts the IP address of the packet, and routes the packet according to the route. If theres no allocated route , it checks if the network ID matches any network the routers is aconnected to . and sends it there. If theres no match, it will find the netowkr ID in the routing table and send it to the router . otherwise sends it to the default router.

Address Resolution Protocol (ARP) : when the IP layer receives a frame with na iP addres on its own LAN , it determines the hardware address of the destination . it does this by the router broadcasting a frame onto the newrokr asking who owns the IP address , and the host with the specifided IPwill respond wih its hardware address , and the router sends the I P to the correct desintaiton .

Packet fragementation : different networks allow different maximum packet sizes called maxiumum transfer units (MTUs) if IPv4 router receives a packet larger than the MTU , it will break it into fragements . the identification , flags and fragements offset fields are used int his process .

IPv6 : developed to overcome IPv4’s probles . can co-exist with IPv4 . IPv6 makes it possible for a host to roam withot needing to change its address . IPv6 are 128 bits long .

IPv4 address – 32 bits . IPv6 - 128 .

IPv4 header – 13 fields, IPv6 – only 8 .

Fragmentation not allowed at routers in IPv6.

IPv6 has better support for options , supports more security ( authentication and privacy ) ,pays more attention to type of service ( header has a flow label ) .

Domain Name System : DNS : converts IP names to IP addresses , using a hierarchical scheme using a database scheme. The DNS name space is divided into non overlapping zones . each zone contains some part of the tree , and name servers holding information about that zone . DNS database is distributed among the name servers, and each zone contains at least one name server which maintains a file contain all IP names and addresses . there being 13 root level name servers that all know the top level name severs .

Internet Control Message Protocol (ICMP ) : used by routers to report errors and unexpected events , test state of network , perform congestion , update routers. Typical messages are things like dest unreachable, echo request , echo reply , timestamp reply .

Transport Control Protocol

TCP Conncection is connection-oriented , virtual (NOT PHYSICAL )

Connections are full duplex . end to end .does not support mulcadsting or broaccadsting .

TCP is stream-oreinted protocol . provides reliable end to end stream over an unrel’iabe network such as IP .

Transport : process to process

Internet : host to host:

Host-tonetowkr : node to node

Transport Layer

End to end communication. Ensures the message arrives intact and in order. It overseas error and flow control at the source to destination level , not others. Sets up and releases connections . provides qos , reliability , delay , throughput

Address ( PORT NUMBER ) 16 bit integer . between 0 and 65535. Ssh 22 http 80 dns 53 smtp 25 . TCP / UDP on the transport layer .

TCP segment is like a packet . 20-byte header, followed by data bytes.

TCP Connection Establishment :

Two way handshaking . station requests a connection , receiving entity accepst connection , connection established . problems occur between if a station transmits data but the person has already disconnected , lose packets / info . would be very bad for a bank . if someone requests the bank to send money then disconnects and received moneys .

Three way handshaking . entity 1 sends a syn segment (cant carry date ) . entity 2 sends back a SYN + ACK segment, which also cannot carry data. Entity sends back an ACK segment and the connection is established .

Connection termination : three way handshaking . if entity 1 wants to terminate connection , they send a FIN segment (can include data ) . entity 2 sends back a FIN + ACK segment (this can also include data ) , entity 1 sends back a FIN to acknowledge the FI N+ ACK , cannot include data . this can result in data loss , so the half close protocol approach is used where he connection in each direction is released indepenednetly of each other.

Threeway handshaking disconnect with a timer . a timer is used and if the enetity doesn’t receive a segment before expires , it disconnects . the sender may not know and keep sending information . this is called half open co[nnection . the protocol can fail if all transmissions except the final are lost . ended .

Error control . checksum : exach segment includes a checksum field checkin for corrupted segment. If found , its lsot .

Acknloweldgement , each segment sends back an ack on recept .

Retransmission : an RTO timer is running , when it expires and no ACK has been received, retransmits . timer is set based on RTT . three duplicate ACK’s rule : retransmit after receiving 3 duplicate ACK segments . this happens wwn eth ereceives many out of order segments and cannot be buffered. This feature is referreed to as fast transmission .

Duplicate segments are detected form their sequence number . discarded.

Out of order segments : also detected using sequence number . but no discarded . maintained in sliding window temporarily until all the missing segments arrive

Lost/corrupted : retransmissted it the sender doesn’t receive an ACK and RTO timer expires.

Flow control : schemes are not at data link becaue router only has few links to others .

TCP sliding window is byte oriented , nmot frame orientted , has variable size . size of window is determined by minimum of receiver weindow and congestion nwindow . sender requests certain number of buffers C(redit ) based on perceived needs. The receiver grants as many of these ars it can . the credits will be decremente eah time it receives a TPDU , stopping when it reaches 0 . the receiver sends both acknoweldgesments and buffer allocations (Ciredt ) can be piggybacked with data .

Congestion control : slow start : the cwnd starts with 1 maximum segment size (MASS) and increases one MSS each time na ACK is received . it starts slowly but grows exponentially .

Congestion avoidance : use additive increase instead of exponential , and when the congestion window reaches the slow start threshold , the slow start hphase stops and the additive phase begins

Congestion detection : multiplicative decrease ; the size of the cwnd is dropped to ½

User Datagram protocol (UDP ) : simple interface between IP and higher layer protcols

Tha add nothing to services. Provides process to process communication ,. Useful in applciatino that require simple request-resposne communication with little flo and err control .

User dgram format : after the head section , provides no error or flow control .

Socket programmgn : software component characterized by unique combination of a local socket address (local IP and port number ) . remote socket address (only for TCP socket ) . uses TCP / UDP.

A socket address eg : 192.126.234.12:54552

Intenet appcliations :

Client/server/ model : client requests services from server , sendinga request message and waiting for a response .

Telnet : 1969 . telnet clients use ‘telnet <hostname> to request to conncet . not secure . no guarantee of encryption (in fact no encryption at all . in cldudgin user/pass ) . no prevention of man in the middle attacks.

Secure shell (SSH ) is a cryptographic network protocol for secure data co,mmunication , remote command line login between 2 networked computers. 2 ways to use SSH.

Automatically generated key pairs : every host has a key, whne client connects , the remote daemon responds with its public host key. The client wanting to connet compares the key against its database to verify its not changed . the client then generates a 256 bit random number and encrypts this number with host key. Sends back to sever . both sides then use this encrypted number key as a session key to encrypt all data .

Manually generated keys ; te client generates an asymmetric public.rpviate key pair. The public key is co[ied to the sevrev. The clients private key is encrypted with a passphrase . when the client wants to connect , sends an encrypted message with the public key . if the client can decrypt the message and send it back using the private key m the connection will be accepted . this is done in the background .

File Transfer protocol ( and SFTP)

FTP is the oldest application protocol used in internet , and is now replaced by SFTP . it requires exchanging commands as well as data . SFTP encryption for authenitacan and transfer (SSH) .

Electronic Mail

Simple Mail Transport Protocol ( SMTP ) . port 25 .

Simple ascii . secure for authentican . SMTP retrives mail and establishes a remote connection via TCP and the n delivers via its protocol .

Post office protocol ( POP) severs hold emails form macihiens which are not reguarl mail server s . POP3 I used to fetch mail from remote mail server, store locally . BOTH poP3 and SMTP manipulate mail , so 2 severs msst coordinate access to mailbox . client sends a user/pass to authenticate the session , then client retriesves and transfers message, then logs oit client .

IMAP an intermernet message access protocol sevrver tha can be adccessedd by multiple cleints, tha has master copy . used with web/eamail apps and allows multilple client access. Changes are synchornizned back to the major copy .

MIME multipurposeinternt mail extensions : are used to encode binary data and they specify the schemes used in the body.

Differences between SMTP and POP : SMTP is the protocol fof sending messages from user to mail server . and from mail sevr to recipient , port nunm 25.

POP is a protocol that connects to a client to a mail server and allows client to download amail from thei seerverside mailbox to their kocal mailbox . port num 110 . any changes are not synchronized back to the server . thos means if u download ur email on more than 1 device problesm can occur Such as emails being unread or not being deleted .

WorldWIDE WEB - originally the arapanet . 1989 .

Hypertext transfer protocol l (HTTP ) is used for comms between servers and browsers . HTTPS is modern secure version . uses transport layer security . new TC P connection is established for each HTTP interaction.

Uniform resource locations (URL ) are used to locare a document using the format : protocol://mach/pathtofile

Hypertext markup language is used to write web pages .

Web server – complex structure , of sevral large software compneonenst that work together to provide a seamless serveice . consists of clients , interpreteers and a controller managing them . interprets web page to display tex ton the users display dveice .

Peertopeer model . bittorrent , bitcoin , distributed storage . no centralized control , self organization . take advantage of disttributd shared resouces (CPU , bandwidth , storage ).

Firewal s . everyone/thing trying to enter or levae thenetwork has to be checked by a firewall. Stops sensitive data from getting stole n , and bad things from getting in .

ADSL , ATM .

Modems : enable the coms between comp and telephone system , by converting telephones analog signal to comp’s digital signal . there aer phone-line disalup modems ( old ) , cable modms , broadboand modems , mobile modems .

These are slow as and reach speed limimts fast. Because they use the telephones bandwidth , cant use tlepehones and internet at same time . you have to dial an ISP eachtime u wann connect .

Digitial subscriber line . Assymmetric DSL . ( faster ) . these are fast and always connected . still use telephone lines though . doesn’t require any special wiring . ADLS si base don a technique discrete multitone . ( DMT ) . divide the frequency rnage from 0Hz to 1.104MHz into 256 sep channels , each with a bandwidth of 4.3124 KHz . five lowest channels are for the telephone , rest are for upstream and downstream transmissions . heaps more downstream than upstream .

Asynchronous transfer mode (ATM) : connection oriented service, designed for real time video and voice applications , using fixed size cells . the cells are mall , arrive in order , at highspeed and low delay transmission .

Small fixed size cells . 53 bytes . 5 bytes for the header , 48 bytes of data . they are simpler to manipulate/use/sender because of their fixed size . makes outgoing queues smaller , and bytes arrive at a more consisnte rate .

Swithing : to set up a connection , a virtual circuit is established . data cells contains virtual path/channel ID in header . switch maintains a tabe of inoput/output port , vrtual path , virtual channel . whne it stwtiches it looks up table entry using port and virtual path id . and the cell is sent rthough that port .

IP Security (IPsec) . network layer security applied between 2 hosts , 2 routers or a host and a router. To protect applications that use network layer directly .

Transport mode : protects only the data from the transport layer, not protecting the IP header. Sending host uses IPSec to authenticate / encrypt the payload . receiving host uses IPSEC t oauthenticate/decrypt the payload .

Tunnel mode : protects the e etntiere IP packet . normally used between 2 roiters , or ahost and a router . the flow is from the network layer to IPSec layer and then back to network layer.

Securtiyt porotocols :

Authentication Headerv( AH) protocol : authetniceate the source host and ensure data integrity . doesn’t provide confidentiality . uses a hash function and a symmetric key to generate a digest .

Encapsulate Security Payload ( ESP ) : better than AH . provides source authenticati on , integrity, confidnetaility .

Wireless Techmologies : IEEE 802.11

Architecutres . basic service set (BSS) is a stationary or mobile wireless statiosn with an optional access point (AP ) . its configured that withput an AP , cannot send data to other BSS’s . configurations : adhoc architecture , without an AP , canont send data to other BBS’s . infrastructure ; with an a P , most coommmonly used .

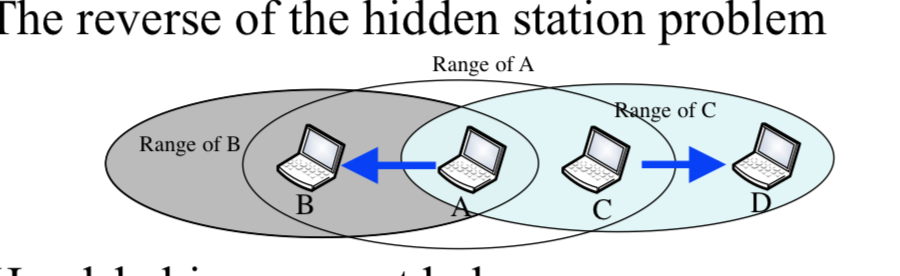
802.11 physcal layer : spread spectrum , spreads the signals spectral energy over a wide range of frequencies (larger bandwidth ) . less prone to interference . more secure as a intruder triyn gto listen to a particular frequency gets onl y small part fothe signal ..

Frequency hopping spread spectrum : works on set of frequencies in broadcast rnage . transmit using 1 frequency for a bit , then switch to the next frequency . using a pseudo random number gen to gen frequency sequence . so sender and receiver have same sequence .

Direct sequence spread spectrum ; expands a single data bit into n bits . transmitter stats with a string of data bits . fore ach bit, generate a pseudornaomd bit string , called a chippngsequence , containing n bits . combine each data bit and chipping sequence to create a chip code , transmit that.

Hidden STaiion Proble m : diff stations may have diff transmission range . solution , handshaking . imagine A B C . C cant sent to B while A is sending to B . C sends a Request to send and B sends a clear to send back when its free.

Exposed Station Problem : reverse of hidden station . imageine A B C D . B is sending to A . D cants to send to C but thinks that C si being used .



Carrier Sense Multiple Access with Collission Avoidance (CSMA / CA ) . try to avoid collisisons instead of detecting collisions . collisisons can still occur . then use binary exponential backoff algorithm . BEBA .

Three strategies to reduce collisions : INTERFRAME SPACE , CONTENTION WINDOW , ACKNOWLEDGMENT .

INTERFRAME SPACE ( IFS ) . a period of time waiting after an idle channel is found . prioritize stations or frame types. Station assigned a shorter IFS has higher priority .

Contention window . an amount of time divided into slots . a station is ready to send chooses a randomnumber of slots as its wait time . binary exponential backoff algorithm : double the window size each time the station cannot detect an idle channel after IFS time .

Acknowledgement : frame may stil l get collided so it guarantees the receiver gest the frame

Blujetooth ; device has transceiver embedded so its wireless .

Eg mouse , keyboard , share info between phones , airdrop .

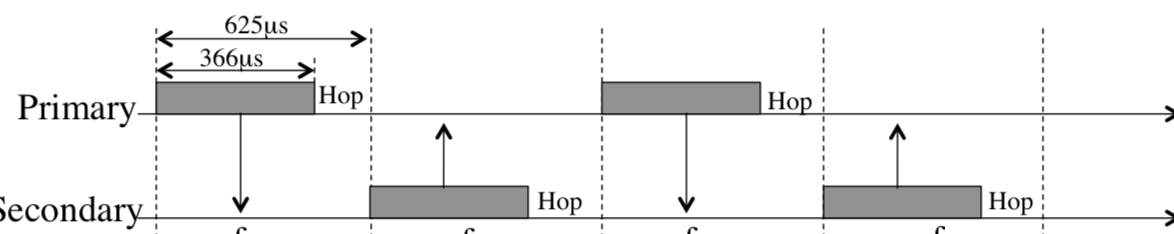
Bluteooth LAN : adhoc network formed spontaneously by bluetoth devives . WIRELESS PERSONALA AREAN ETWROK . PAN . IEEE802.15

Piconets (small nets ) : up to 8 stations , one primary , rest secondary .

Scatternet : consist of two or more piconets . secondary station in 1 piconet can be the primary in anpther piconet .

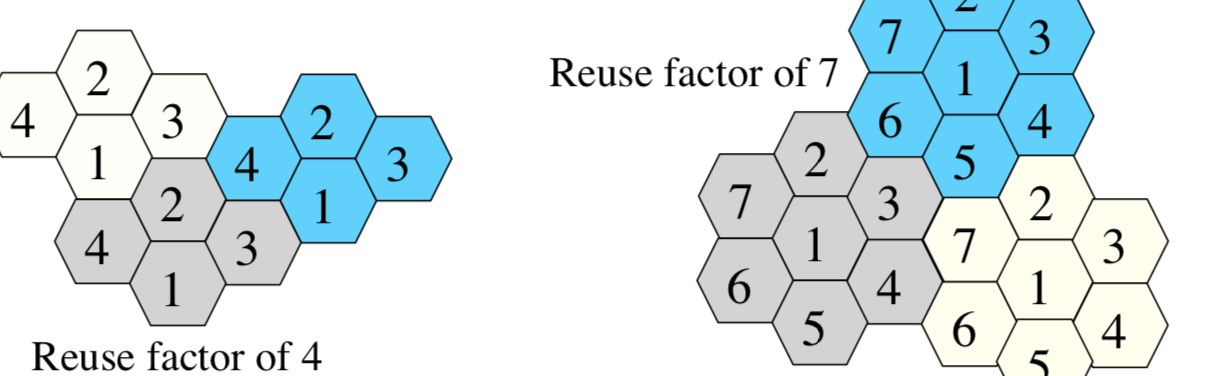
Bluetooth Radio Layer . rougly equivalent to physical layer in Int mode l . low power . FHSS : hops 1600 times per second . each frequency is 1/1600 of a second .

Bluetooth baseband layer. MAC layer in LANS . TDD-TDMA (time division duplex TDMA ) . half-duplex coms . time slot is 1/625 of a second . single secondary coms . primary uses even numbered slots (0,2,4….) . secondary uses odd numbered slots (1,3,5 .. … )



Multiple secondary coms . primary uses even numbered slots (0,2,4 … . )

Secondary sends in the next odd numbered slot if that packet in the previous slot was addressed to it .

Frequency reuse principel . neighbpuring cells cannot use same set of frequencies for communication . set of frequeinces is limited . frequencies need to be reused . frequency resuse pattern is a configuration of N cells where N is the reuse factor . 

Handoff , mobile station moving from one cell to another . MSC mointors the signal strength every few seconds . if it diminishes too low , MSC seeks a new base station it can better accomadae the coms.

Hard handoff : mobile can only communicate with 1 station at atime .

Soft handoff : multiple , transitions from one to the other smoothly .

Roaming : serveice provider has limited coverage . so people can pay to use neighbouring service providors . cellular customer can send data by means of a visited network .

Cellular netowkrs :

First generation . analog voice comms . advanced mobile phone system (AMPS) . uses FDMA . 2 separate analog channels . cellular bands for AMPS

Second generation : digital voice communciatinon . D-AMPS digital amps. Uses TDMA and FDMA . GSM : global sysem for mobile comms : similar to damps .

CDMA : code division multiple access . only once channel occupies the entire bandwidth . all station can send simulatensously .

Each station assigned a code . multiply code by another , get 0 . if we multiply each code by itself , value you get is = to num of stations . no idea . a \* a = num stations . a \* b = 0.

3rd generation : combination of technologies . fulfill internet mobile comms . first mobile broadband .

4th gen : designed for data . IP based protocol . true mobile broadband . provides comprehensive and secure all-IP based mobile broadband solution to lappy . internatnion mob’ile telecoms . 100mbits .

5g : massive MIMO , millimeter wave MIMO , small cell .

MIMO : multiple input , multiple output . take advantage of multipath propagation . spatial diversity to maek comms robust , same info is sent via multiple paths , receiver reconstructs info base on multiple copies of received signals . spatial multiplexing to increase data rate . each channel carries independent info . phones use millimtere-wave mimo . big stuff uses massive MIMO .

Cloud computing : software as a service. Cloud proivdor . hardware and software infrastructure that supports the cloud applications . benefits : achieve economies of scale. Reduce spending on tech infrastructure . reduce capital costs . improve accessibility . less personel training is needed . stored online .

Intra cloud Netwrok : data center network . servers . storage . connectivity ( switches , routers ) . data center design . 2 tiers. Servers , access switch, enterprise core .

Limitations of current network architecture . expensive , buggy software, hard to manage.

Closed equipment . inability to scale. Inconsisten policies , have to configure thousands of devics . hundreds or thousands of network devives must be configurd and magnaged.

Need for new network architectures . changing traffic patterns . client-server to enterprise data center. Big data means need more bandwidth . rise of cloud services . IT becoming more popular .

Software defind networking : decouple network control and forwarding functions . allow admisn to manage network services through abstractions of low level functinonality .

Open flow : communicating protocol that gives access to the forward plane , allows remote admimistration of a switch’s packet forwarding table .

Challenged networks : networks may operate poorly in environments characterized by very long delay paths and frequent network patritiatiosngonsdfjg.

Internet of things : network of items – each embedded with sensors . all connected to internet. Cars . fridges . plugs . robots . shopping . connected devices . LoRA : a patnted wirless comm tech . 2012 . chirp spread , frequency increases up through time in very linear way .

Wireless sensor network : sensor network massive number of small , inexpensive device so tha it can moniror and control most saspsects of our physical world . tight resource constriants . batt power . limited computation so far.