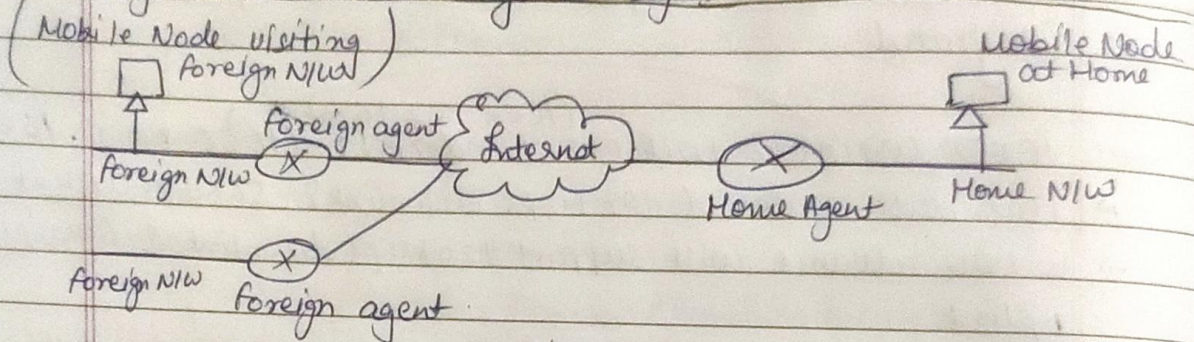
UMC UNIT 4.

(*). Mobile IP:

→ IETF RFC 2002, De facto Standard communication Protocol.
→ Created by extending IP
→ Allows mobile devices to move from one N/w to another while maintaining the same permanent IP address.
→ Makes communication flawless.
→ The mobility function of mobile IP is performed on N/w layer rather than Physical layer.



Architecture.

Components of Mobile IP technology:

① Mobile Node: Device that frequently changes n/w positions without changing its original IP Address. Eg. Cell phone.
② Home Agent (HA): A router on the home n/w. Serves as anchor point for communication with mobile node.
③ Foreign Agent (FA): Router that provides services whenever a mobile node visit a foreign n/w. Responsible for delivering packets from home Agent to Mobile Node.
④ Home N/w (HN): Base Station N/w to which the mobile Node originally belongs.
⑤ Foreign Network (FN): N/w other than home N/w on which mobile nodes have a registered IP.
⑥ Corresponding Node (CN): Partner nodes which are used for communication with mobile nodes.
⑦ Care of Address (CoA): Used to define the Mobile Node's current

position. Used to deliver data packets through the process of tunneling.

(iv) Working of Mobile IP:

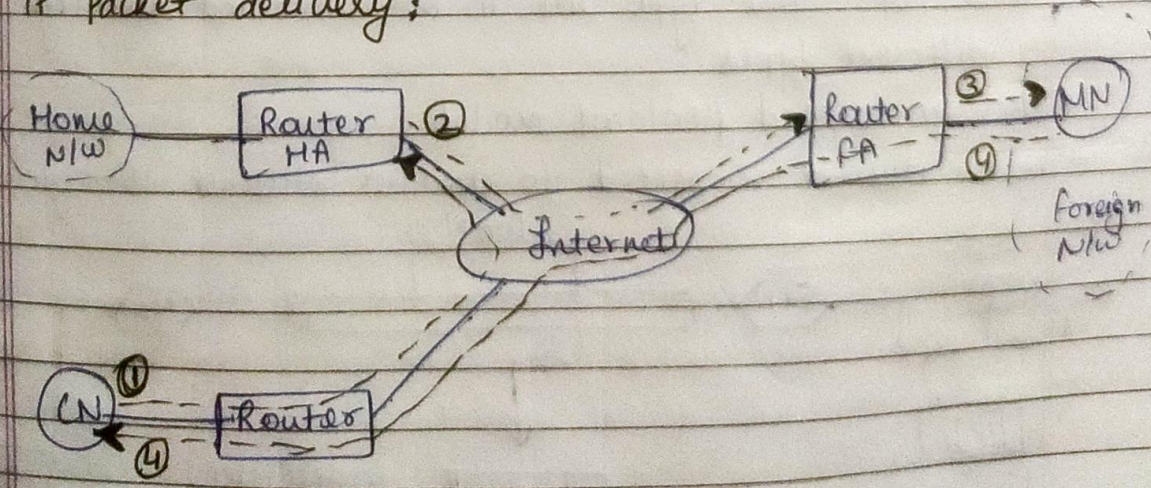
① Agent Discovery: Mobile nodes discover their foreign & Home Agents.
The agents advertise their services on N/w using the ICMP Router Discovery Protocol (IRDP).

② ~~Registering~~ Registration: Responsible for informing the current location of home agent & foreign agent for correct forwarding of packets.

③ Tunneling: Used to establish a virtual connection for moving the data b/w a tunnel entry & tunnel end point.

* Applications of Mobile IP:
→ Used in many applications where sudden changes in N/w can cause problems.
→ designed to support seamless & continuous Internet connectivity.
→ Used in many wired and wireless environments.
→ often used in 3G systems.

(v) IP Packet delivery:



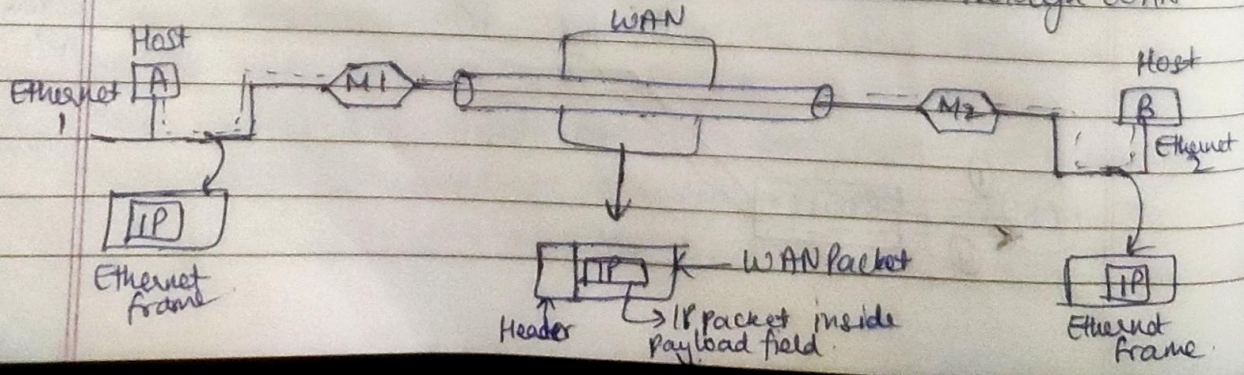
Step 1: → CN sends IP packet with MN as destination Address and CN as source address. CN does not need to know anything about MN's current address.
→ The internet, not having info on current location of MN, routes the packet to the router responsible for home network of MN.

Step 2: → HA intercepts the packet knowing that MN is not currently in its home N/w.
→ A new header is put showing COA as destination & HA as source of the encapsulated packet.

Step 3: → Foreign agent decapsulates the packet (removes additional header) and forwards the original packet with CN as source & MN as destination.
→ For the MN, mobility is not visible.

Step 4: → The MN sends the packet with its own fixed IP address as source and CN's address as destination.
→ The router with FA acts as default router and forwards the packet to CN.

(X). Tunneling:
→ An inter-networking technique when source and destination n/ws of same type are to be connected through a N/w of different types.
→ Uses a layered protocol model.
→ Eg, an ethernet connected to another ethernet through WAN.



Steps

① Host A constructs a packet that contains IP address of Host B.
② It then puts this IP packet into Ethernet frame. Frame is addressed to Multiprotocol Router.
③ Host A puts this frame on Ethernet.
④ When M1 receives this frame, it removes the IP packet, inserts in the payload packet of WAN NW layer protocol and addresses the WAN packet to M2.
⑤ Multiprotocol router M2 removes the IP packet and sends it to Host B in Ethernet frame.

Encapsulation: Process of adding a new packet within the existing packet or a packet inside packet. In an encapsulated packet, the header part of the first packet remains surrounded by the payload section of the surrounding packets.

→ In the given example, IP packet does not have to deal with WAN.
→ Host A and Host B also do not need to deal with WAN.
→ Only the multiprotocol routers M1 & M2 will have to deal with WAN.
→ Therefore, WAN can be imagined to be equivalent to a big tunnel and technique is called Tunnelling.
→ Types of Tunneling Protocols:
① Generic Routing Encapsulation: Encapsulating IP packets in a GRE Header that hides original IP packet.
→ Only routers between which GRE is configured can decrypt and encrypt the GRE header.
→ Original IP packet enters a router, travels in encrypted form and emerges out of another GRE configured router. This process is called GRE tunneling.

② Internet Protocol Security (IPsec):
→ Standard suite of protocols b/w 2 communication points that provide data authentication, integrity & confidentiality.
→ Also defines encrypted, decrypted and authenticated packets as well as the protocols needed for secure key exchange
③ IP in IP: For encapsulating IP packets inside another IP packet
④ Secure Shell (SSH): Used for transfering encrypted data over the ~~Internet~~ N/W.
→ It allows you to connect to a server or multiple servers without having to remember or enter your password for each system.
⑤ Point to point Tunneling Protocol: (PPTP)
→ Generates a tunnel and confines data packet.
→ Used to encrypt data b/w connection.
→ One of the most widely used VPN protocols.
⑥ Secure Socket Tunneling Protocol:
→ A VPN protocol that uses SSL to secure the connection.
→ Only available for windows.
⑦ Layer 2 Tunneling Protocol (L2TP):
→ Designed to support VPN connections.
→ Combines the best features of PPTP and L2F (layer 2 forwarding)
⑧ Virtual Extensible local Area Network (VXLAN):
→ Stretches layer 2 connections over layer 3 networks by encapsulating ethernet frames in a VXLAN packet.
⑨ SSL Tunneling: → Involves a client that requires SSL connection to a backend server or secures a server via a proxy server.
→ This proxy server opens connection and copies data to both sides without any direct interference from SSL connection.

(*) Reverse Tunnel: Tunnel node that starts at the Mobile node's care of Address and terminates at Home Agent. (Reverse of Tunneling).

(*) IPV6: Internet Protocol Version 6.
→ Developed by IETF (Internet Enginnering Task force) to deal with the problem of IPV4 exhaustion.
→ 128 bit address having address space of 2^{128} (way bigger than IPV4)
→ Uses Hexadecimal format seperated by colon (:).
Components:
① 8 Groups, each represents 2 Bytes - (16-Bits).
② Each Hex digit is of 4 bits.
③ Delimeter used - colon (:)

ABCD:EF01:2345:6789:ABCD:B201:5482:D023

← 16 Bytes →

Need for IPV6: ① Support for multimedia.
② Need for security.

Main changes:
① Large Address space: IPV6 - 128 bits IPV4 → 32 bits.
② Better Header format: Speeds up routing process.
③ New options: for additional functionalities.
④ Allowance for extension: allows extension if required.
⑤ Support for resource allocation: to support traffic.
⑥ Support for more security: Encryption and authentication options provide confidentiality and integrity.

(*) Addressing Methods: (a) Unicast
(b) Multicast
(c) Anycast.

→ Broadcast is not defined in IPV6.

(1). Unicast Address: Identifies a single n/w Interface.

→ A packet sent to unicast address is delivered to the interface identified by that address.

(2). Multicast Address: Used by multiple hosts, called as groups.

→ Hosts need not be geographically together

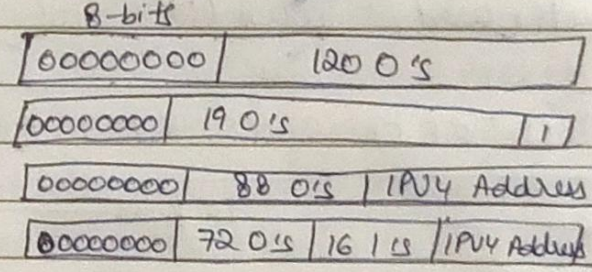
→ If any packet is sent to multicast address, it will be distributed to all interfaces corresponding to that M. address.

→ One data packet is sent to multiple destinations simultaneously

(3). Anycast Address: Assigned to a group of Interfaces.

→ Any packet sent to anycast address will be delivered to the nearest host.

(*). Some special addresses:



① Unspecified

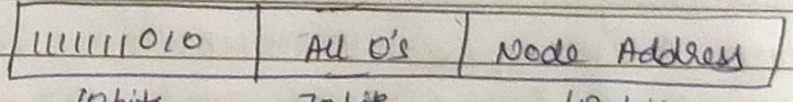
② Loopback

③ IPV4 compatible

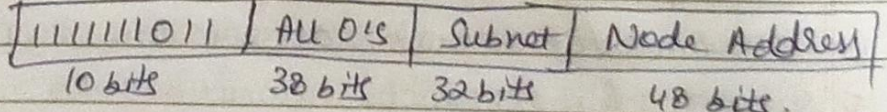
④ IPV4 mapped

→ Local unicast Address → Link local
→ Site local.

(*) Link local:



(*) Site local:



(*) Advantages of IPV6:

① Realtime Data Transmission: Process of transmitting data very fast or immediately Example, live streaming

② It supports authentication. Data sent = Data received.

③ It performs encryption: Encrypts messages at N/w layer.

⑤ Faster Processing at Router: Able to process data packets much faster due to smaller base header.

(x) Dynamic Host Configuration Protocol (DHCP):
→ N/w management protocol used to dynamically assign an IP address to a new device or node on a N/w to allow them to communicate using IP.
→ It automates and centrally manages these configurations.
→ No need to manually assign IP addresses.
→ No requirement for user configuration.
→ Can be implemented on local as well as large enterprise N/w.
→ Default protocol used by most routers & N/w equipments.
→ Also called RFC (Request for comments).
→ It manages the provision of all the nodes/devices added to/dropped from the n/w.
→ Maintains a unique IP address of host using DHCP server.
→ It sends a request to DHCP server whenever a client/node/device, which is configured to work with DHCP, connects to N/w
→ It (server) acknowledges by providing IP Address to the client node/device
→ It runs at the application layer of TCP/IP protocol stack
→ Based on client server protocol. Server manages a pool of unique IP addresses as well as information about clients.
→ DHCP lease process:
① Client must be connected to the Internet.
② DHCP Client request an IP address. Client broadcasts a query for it.
③ Server responds to the request by providing IP address other configuration information.
This configuration info includes time period, called a lease, for which the allocation is valid.
④ On refreshing, DHCP client requests the same parameters,

but the server may assign a new IP Address.
This is based on policies set by the administrator.

(*) DHCP Components:

1. DHCP Server: Holds IP Addresses and related configuration info. Acts as a host.
2. DHCP Client: Endpoint that receives configuration info from server Eg. Computer, laptop, etc.
3. IP address Pool: Range of available addresses for DHCP clients. Typically handled out sequentially from lowest to highest.
4. Subnet: Partitioned segments of IP N/w. Used to keep the N/ws manageable.
5. Lease: Length of time for which the client holds the IP Address info.
6. DHCP relay: A host / router that listens for client messages and then forwards them to a server.

(*) Benefits of DHCP:

1. Centralized Administration of IP configuration.
2. Dynamic Host Configuration.
3. Seamless (Accurate & Timely) IP host configuration.
4. Flexibility and scalability.

(*) Traditional TCP: Transmission control Protocol.

→ Transport layer Protocol. Serves as an Interface b/w client & server.
→ Used to transfer data packets b/w tranport & N/w layer.
→ Traditional TCP → wired N/w, Classical TCP → wireless N/w.

1. Congestion Control:

→ Sometimes, the data packets get lost due to temporary overload at some point in the transmission path. This temporary overload is called congestion.
→ The transmission speed of receiver ≠ Transmission speed of sender.

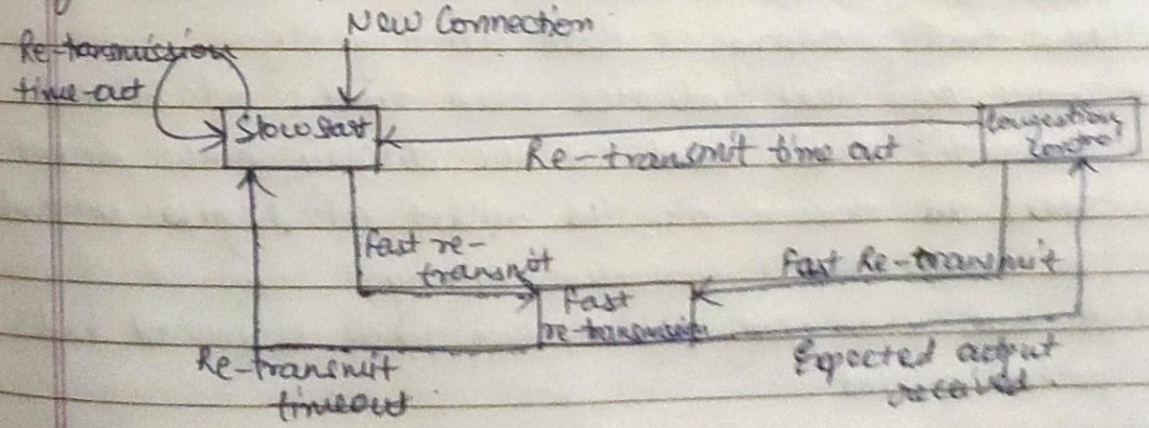
- If capacity of sender is more than that of all link, then the packet buffer of a router is filled and the router cannot forward the packets fast enough.
- The only thing a router can do is drop some packets.
- Sender notices the missing acknowledgement from the receiver due to packet loss & slowsdown.

② Slow Start:

- The behaviour TCP shows after detection of congestion is called Slow Start.
- Sender calculates a congestion window. At first it sends a packet and waits for Ack. Once ack is received it doubles the packet size and sends 2 packets. After receiving ack, it again doubles and this process continues.
This is called Exponential Growth. EG stops at Congestion Threshold. As it reaches threshold, increase in rate of transmission becomes linear.

③ Fast Re-Transmission:

- If there is a gap in ack due to packet loss, the sender immediately re-transmits the missing packet before the given time expires. This is called Fast re-transmission.



(*) Congestion Control:

→ Occurs in N/w layer when message traffic is so heavy that it slows down N/w response time.
→ Delay ↑ performance ↓
→ Delay ↑ retransmission occurs, making situation worse.
→ It is a mechanism that controls the entry of data packets into N/w
→ Avoids congestive collapse.
→ Congestive Avoidance Algorithms (CAA) are implemented at TCP layer to avoid congestive collapse in a N/w.
→ 2 Algorithms: (a). Leaky Bucket Algo.
(b). Token Bucket Algo.

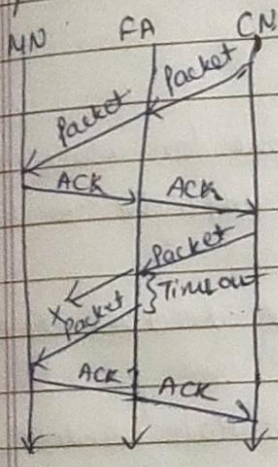
(*). Leaky Bucket Algo:

→ Traffic shaping algorithms.
→ Controls the rate at which traffic is sent to the N/w.
→ Shapes the burst traffic to a steady traffic stream.
→ Disadvantage: Inefficient use of available N/w resources.
→ Bandwidth not used effectively.

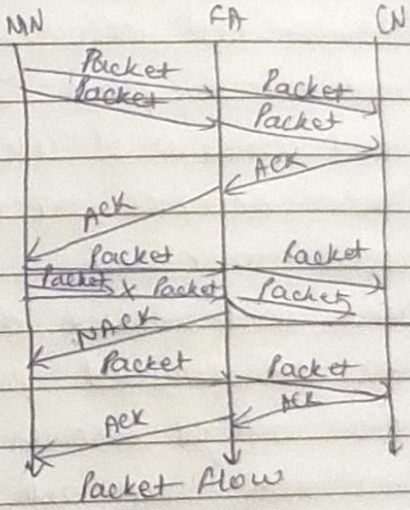
(*) Token Bucket Algorithm:

→ More flexible algo. When large bursts arrive, it is allowed to speed up.
→ N/w traffic shaping or Rate limiting Algo
→ Control Algo that indicates when traffic is to be sent.
→ This order comes based on the display in the bucket.
→ Tokens are thrown into the bucket at regular intervals.
→ This bucket has a maximum capacity.
→ If there is a ready packet, then token is removed and packet is sent.
→ If there is no token in the bucket, packet cannot be sent
→ For a packet to be transmitted, it must capture and destroy one token from the bucket.

(*) Snooping TCP: One of the classical TCP improvement approaches.
→ The foreign agent buffers the packet until it receives ack from mobile node.
→ A foreign agent snoops the packet flow & ack is both directions.
→ If a foreign agent does not receive ack, it believes that it is lost, so it immediately retransmits the packet from buffer.
→ foreign agent maintains its own timer in case it is lost on the wireless link.
→ It discards duplicates of packets already retransmitted and acknowledged by mobile node. This avoids unnecessary traffic on the wireless link.
→ To maintain transparency, foreign node does not acknowledge the packet to fixed node, the mobile node does.



Packet Flow
CN to MN



Packet Flow
MN to CN

(*) Advantages:
① Packet is not ack by Foreign Agent (FA).
② If FA fails, solution reverts to standard TCP.
③ No modifications at Fixed Host. Changes (Majority) are made to FA.
④ No packet loss during Handovers.

(*) Disadvantages:
① Transmission errors can spread to corresponding nodes.

② Mobile nodes needs additional mechanisms.
③ Encryption at end-to-end, Snooping is considered worthless.

(*) Fast Recovery Technique for loss Recovery in TCP:
→ When RTO expires and ack not received, the sender confirms that the packet is lost due to congestion.
→ Recovery is packet loss recovery technique.
→ It means becoming inactive for sometime & not transmitting any new packet.
→ When loss detected, sender does 4 things:
① Reduces the cwnd by 50%
② Reduces the ssthresh value by 50% of cwnd.
③ Retransmit the lost packet.
④ Enter fast recovery phase.
→ Fast recovery phase: 2 part.
(a) Half window of silence: Amount of time for which the sender becomes inactive & waits for inflight to become equal to cwnd.
Sender will receive dup-ack until the receiver receives the retransmitted packet.
(b) After inflight becomes equal to cwnd: Half window silence ends here. Dup-ack will keep coming.
→ Sender maintains inflight value = cwnd value.
→ When receiver finally gets the retransmitted packet, & it sends ack to sender, then sender will come out of Fast Recovery phase. (B/C it is confirmed that lost packet is received)

→ Half window of silence leads to under-utilization of resources.
→ When the Sender is silent, the nlw bandwidth is wasted.
→ Sender does not send data & receiver has to wait which results

is delay and bad user experience.

→ Solution is to improve estimation of inflight data. If the sender knows the updated inflight value, then half window of silence would be over soon.

→ Another solution → Rate halving technique.

→ One more solution is proportional Rate Reduction.

(a) Fast Recovery without SACK:

Before fast recovery: cwnd = 10 inflight = 10.

Initial stage when FR begins:

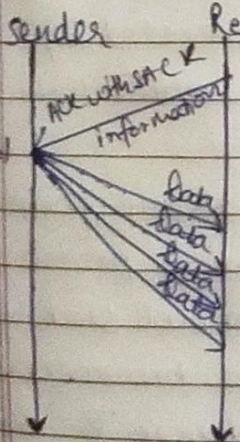
cwnd = 5 ssthresh = 5 & inflight = pipe = 10.

1. DupAck 1, pipe = 10 - 1 = 9
2. DupAck 2, pipe = 9 - 1 = 8
3. Dupack 3, pipe = 8 - 1 = 7
4. Dupack 4, pipe = 7 - 1 = 6
5. Dupack 5, pipe = 6 - 1 = 5 (cwnd = pipe), silence breaks.

Now sender transmits a new packet.

(b) Fast Recovery with SACK: suffers from burst transmissions.

→ When nlw is loosing packets, sender is sending a bunch of packets which affects the nlw badly.



initial state = 5 segments.

cwnd = 5, ssthresh = 5.

SACK tells that 3 packets are lost. pipe = 5 - 1 - 3 = 1

pipe < cwnd

New packets to be transmitted = cwnd - pipe

= 5 - 1 = 4

This is called burst transmission.

(*) TCP over 2.5G/3G Networks:

→ Optimizing TCP over wireless WANs.

(*) Characteristics:

(a) Data Rates: Data rates are asymmetric as it is expected that users will download more data as compared to upload.

→ for 2.5G → 10-20 kbps uplink, 20-50 kbps downlink.

→ for 3G & future 2.5G → 64 kbps uplink & 115-384 kbps downlink.

(b) latency: Error checking loads the Round Trip Time to ↑.

(c) Jitter: Sudden increase in latency due to high-priority traffic, handovers, etc.

(d) Packet Loss: May be lost due to handovers or corruption.

(*) Configuration Parameters:

(a) Large window size: to increase performance.

(b) Limited transmit: Useful when small amount of data is to be transmitted.

(c) Large MTU: (Maximum Transmission Unit) To increase performance.

(d) Selective Acknowledgement (SACK): Allows selective retransmission of packets.

(e) Explicit Congestion Notification (ECN): Allows receiver to inform sender about congestion in network.

(f) Timestamp: Higher delay spikes can be tolerated by TCP.

(g) No header compression: HC is not compatible with TCP.

(*) Wireless Application Protocol (WAP) in Mobile Computing:

→ Programming model, set of communication protocols.

→ Hierarchical design similar to TCP/IP protocol stack design.

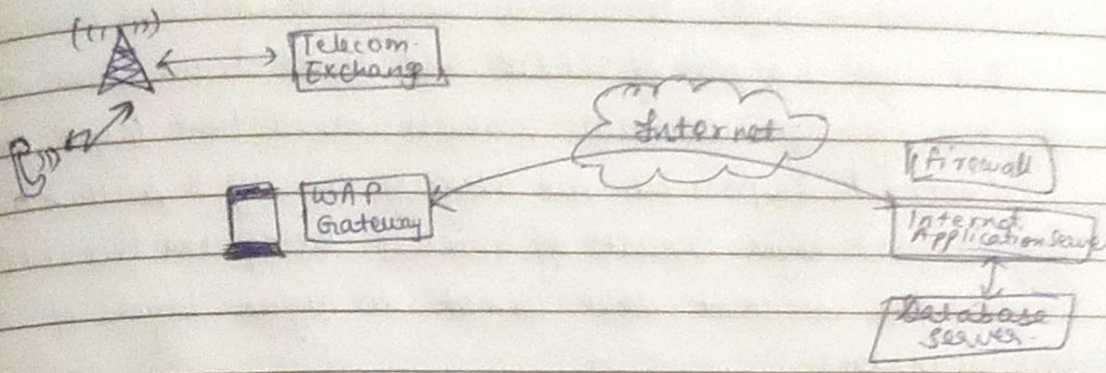
→ De-facto standard, designed for micro-browsers.

→ Enables mobile devices to interact, exchange & transmit information over the Internet.

→ Functioning is similar to www but uses Markup language.

Wireless Markup language to access WAP services.

→ Has the ability to create web applications for mobile devices.



Working:

① WAP model consists of 3 levels: Client, Gateway & Origin Server.

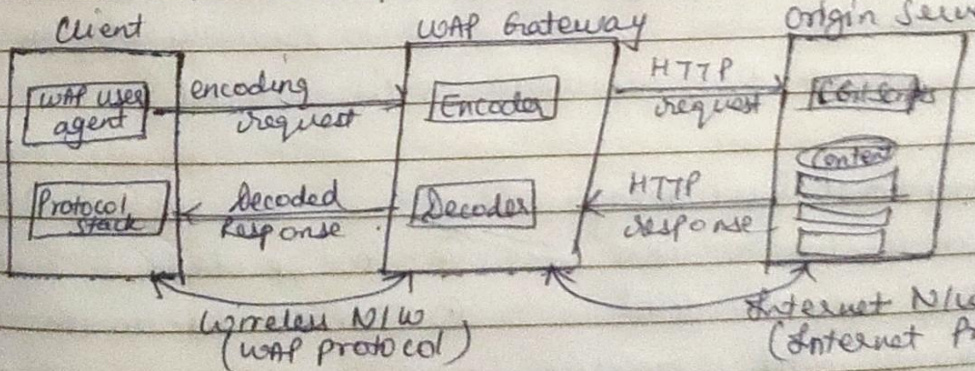
② When a user opens browser and selects a website that they want to view, the mobile device sends URL encoded request via a n/w to WAP Gateway using WAP protocol.

③ This request is called encoding request.

④ Sent request is transmitted through WAP gateway & then forwarded in the form of conventional HTTP URL request over the Internet.

⑤ When request reaches the server, the server processes it and sends back a response to mobile device through WAP gateway.

⑥ Now WML file's response can be seen in the browser.



→ WAP Protocol Stack:

① Application layer: Consists of Wireless Application Environment, development programming languages, etc.

② Session layer: Consists of Wireless Sessions Protocol. Responsible for fast connection, suspension & reconnection.

③ Transaction layer: Consists of Wireless Transaction Protocol (WTP). This layer is a part of TCP/IP and offers transaction support.

④ Security layer: Contains Wireless Transaction layer security (WTLS). Responsible for integrity, privacy & authentication.

⑤ Transport layer: Consists of Wireless Datagram Protocol (WDP). Provides consistent data format to higher layers of stack.

(*) Advantages:

① Fast Paced Technology.
② Open Source Tech.
③ Free of Cost.
④ Independent of N/w standards.
⑤ Can be implemented on multiple platforms.
⑥ Provides Higher controlling options.
⑦ You can send/receive real time data.
⑧ Most devices support WAP.

(*) Disadvantages:

① Slow connection speed.
② Limited Availability.
③ less secure
④ It provides a small User Interface.
⑤ In some areas, Internet access is entirely unavailable.

(*) Applications: Access Internet, play games, access E-mails, mobile banking, Internet based services, etc (ringtones, positioning, etc).

Additional Advantages:

① Portability.
② Development time reduction.
③ No hardware obsolescence.
④ Personalized.

Additional Disadvantages:

① Not familiar to users.
② Third party is includd.
③ Business model is expensive.
④ Low speeds.
⑤ Limited bandwidth.

(v) WAP Gateway: Software that encodes and decodes requests and responses b/w smartphone & micro browsers & internet.
→ A request for accessing a website is sent via WAP Gateway.
→ It helps devices to communicate with applications & internet websites.
→ It is a server that functions as intermediary in access request.

(vi) WAP Browser: Enables mobile devices to access web pages.
→ Converts web pages to plain text.
→ XHTML and Compact Hypertext Markup language (CHTML) are supported.

(vii) Wireless Datagram Protocol:
→ offers a consistent datagram transport service.
→ To offer this consistent service, adaption is needed in transport layer.
→ The closer the bearer service is to IP, the smaller the adaption can be.
→ If the bearer already offers IP services UDP is used as WDP.
→ It offers more or less the same services as UDP.
→ Offers source & destination port numbers for multiplexing & demultiplexing.
→ Service primitive to send a datagram is TDUnitdata.Req with Destination Address, destination port, Source Address, source Port & User data as mandatory fields.
→ TDUniddata.ind indicates reception of data. Here Destination Address & port are optional parameters.
→ Error is indicated with TDError.ind
→ An Error code is returned indicating the reason for error.
→ If any error happens when WDP datagrams are sent from one WDP entity to another, Wireless Control Message Protocol (WCMP) provides error handling.
→ WCMP can be used by WDP nodes and gateways to report errors.

→ WCMP error messages should not be sent as a response to other WCMP error messages.
→ WCMP messages include:
destination unreachable, parameter problem, message too big, reassembly failure, echo request/reply.
→ WDP management entity supports WDP and provides information about changes in environment.
→ If the bearer already offers IP transmission, WDP relies on segmentation & reassembly capabilities of IP layer.

Wireless Transaction Protocol:

→ A layer of WAP intended to bring internet access to mobiles.
→ Runs on top of UDP and performs many same tasks as TCP but in an optimized way.
→ It has reduced amount of info. needed for each transaction
→ decrease in processing and memory cost.
→ designed to run on very thin clients like mobile phones.
→ provides improved reliability over datagram service.
→ Improved efficiency.
→ Transaction is defined as a request with its response
→ 3 Classes of transaction:
Class 0 → unreliable message tranfer w/o any result message.
Class 1 → reliable message transfer with no message.
Class 2 → reliable message transfer with 1 message.
→ Provides Duplicate removal, retransmission, acknowledgements.
→ Avoids unnecessary overhead on communication link.
→ Allows for asynchronous transactions, abort of transactions, concatenation of messages & report success & failure of reliable messages.

(a) Wireless Session Protocol:
→ designed to operate on top of datagram service.
→ Provides a shared state b/w a client and server.
→ tries to replace HTTP.
→ Client users can continue to work where they left the browsers or when the network was interrupted.
→ Users can get their customized environment everytime they start the browser.
→ WSP offers the following general features:
(a) Session management: Establish and release sessions, suspend, resume.
(b) Capability negotiation: Clients and servers can agree upon a common level of protocol functionality.
(c) Content encoding: defines efficient binary encoding for content.
(d) Exchange of session headers: Client and server can exchange the request / reply headers.
(e) Asynchronous requests: Supports a client that can send multiple requests to the server simultaneously.

(b) Wireless Transport Layer Security:
→ Security level for WAP, applications that use WAP.
→ Developed to address issues like limited memory capacity, lower processing power, low bandwidth, etc.
→ It also provides authentication, integrity and privacy.
→ Designed to support datagrams in high latency low bandwidth environment.
→ Provides optimized handshake through Dynamic key refreshing.
→ Allows encryption keys to be regularly updated.
→ Helps clients and servers to communicate over a secure and authenticated connection.
→ It operates over transport Protocol layer.

→ TLS was modified to develop WTLS.
→ Modification was required for end-to-end data security.
→ Optimized for low bandwidth mobile devices.
→ More efficient than TLS & requires fewer message exchanges.
→ Packet sizes are reduced in WTLS.
→ TLS is stream based, WTLS is packet based.
→ Allows the use of SMS.
→ Features:
① Data Integrity
② Privacy
③ Authentication
④ DoS protection: rejects replayed messages and unverified messages to prevent Denial of Service (DoS) attacks.
⑤ It includes two layers ~~protocol~~ of protocols.

Steps:
①. Compression of Payload (via lossless compression algo).
②. Addition of Message Authentication Code (MAC) over compressed data using Hash based MAC (HMAC)
③. Compressed data with MAC is encrypted using symmetric encryption algorithm.
④. A header gets ~~prepended~~ to the encrypted payload.

(v) Handshake Protocol (WTLS)
→ Allows the server and client to authenticate each other.
→ Generates a pre-master secret, then master secret & then cryptographic keys.
→ It must be used before the application data is transmitted

(vi) Wireless Markup Language:
→ A markup language for wireless devices.

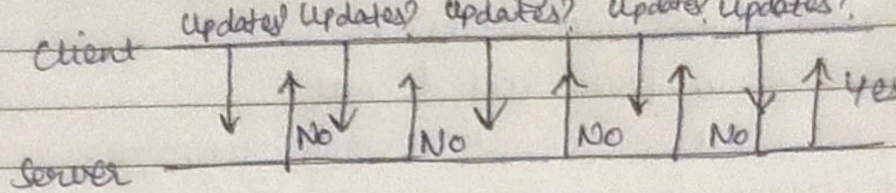
↳ limited capacity rechargeable batteries.

→ Have limited processing capability.
→ Designed to handle issues like small window size, limited user input capabilities, etc.
→ It is written in plain text format.
→ It uses WML script for client side scripting.
→ Supported image format is WBMP.
→ A micro browser is used to run WML. Regular browsers run HTML.
→ WML is case sensitive. HTML is not.
→ Has fewer tags as compared to HTML.
→ A deck is a set of WML cards. Site is a set of HTML pages.

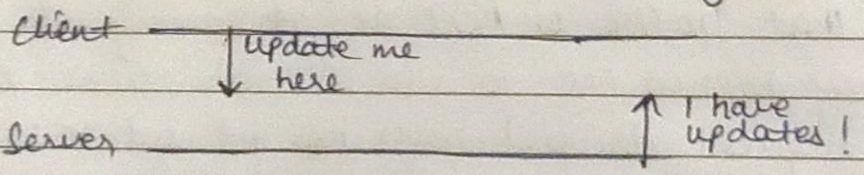
(*). PUSH vs PULL API Architecture:

→ No. of internet users have increased in the past few years and handling an enormous number is a big challenge.
→ Choosing an appropriate architecture plays a significant role.
→ Ensure that traffic is kept at a manageable level.
→ 2 primary approaches to n/w communications → push & pull.
(*). PULL (request driven) server does not need to store client details.
→ often referred to as polling.
→ The info. is static and there's no need of frequent updates.
→ The client needs to find out if there is any new info on server's side. Best way is to call and ask.
→ Client initiates the communication by requesting updates.
→ Servers receives the request, verifies it and sends the appropriate response back to the client.
→ This process takes 100s of milliseconds.
→ If there are many requests, it can slow down or overload your server, resulting in poor experience.
→ Many companies limit how often a client can ask for the same information.
→ Slower than PUSH API.

→ If you need the ability to communicate frequent updates, push architecture is likely a better choice.



(*). PUSH: (event driven). server needs to store client details.
→ Data is pushed upstream over a connection as soon as it becomes available.
→ One type of push based transport is called a web socket
→ Used in cases you have time-sensitive data that changes often and clients need to be updated as soon as data changes.
→ Client does not need to explicitly request updates.
→ Server pushes the data to client, no request needed.
→ More efficient for data that changes often.



→ Faster than PULL API.

Why PUSH APIs?
→ Used to minimize server load. in apps with frequent data exchange or real-time data.
→ Users need not make frequent requests.
→ Fewer resource utilization, enhanced efficiency.
→ More stable, cost-effective.
→ Make traffic Manageable.
→ Consumes less time & is easy to implement.