Unit-III

Mobile IP network layer

* **IP Layer**

- The Internet Layer is a group of internetworking methods, protocols & specifications in the IP suite that are used to transport datagram (pkts) from the originating host across n/w boundaries, if necessary, to the destination host specified by a n/w address (IP address) which is defined for this purpose by the IP.

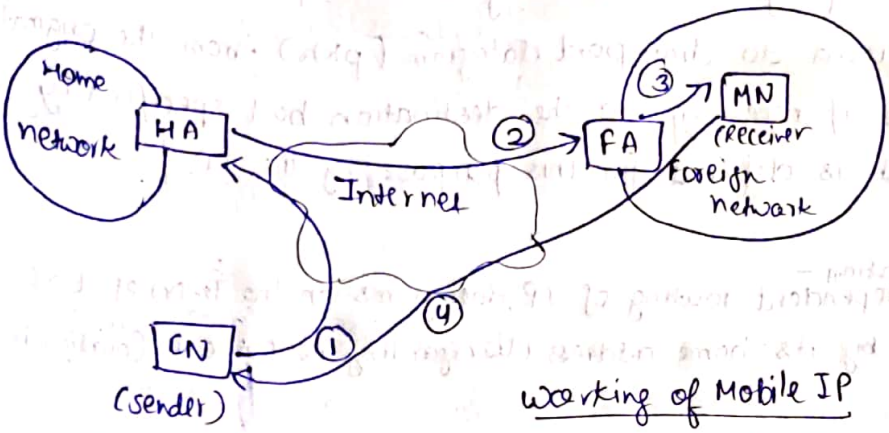
* **Mobile IP N/w layer**

- Mobility IP allows for location-Independent routing of IP datagrams on the Internet. Each mobile node is identified by its home address disregarding its current location in the Internet.
- Mobility is the ability of a node to change its point-of-attachment while maintaining all existing communications & using the same IP address.
- Nomadicity allows a node to move but it must terminate all existing communications & then can initiate a new connections with a new address.
- Mobile IP is a n/w layer soln for homogenous & heterogenous mobility on the global Internet which is scalable, robust, secure & which allows nodes to maintain all ongoing communications while moving.
- Design goals: Developed as a means for transparently dealing with problems of mobile user, Designed to avoid soln's that require mobile nodes to use multiple addresses.
- Several requirements for Mobile IP to make it as a standard:
  → Compatibility → Transparency → Scalability & Efficiency → Security
- Care-of-Address [COA]: Defines the current locn of MN from IP point of view.
- Foreign Agent COA: COA could be located at FA, i.e., COA is an IP address of FA.
- Co-located COA: COA is co-located if MN temporarily acquired an additional IP address which acts as COA. This address is now topologically correct, if the tunnel endpoint is at MN.
- Home Agent (HA) maintains a location registry.
- While away from its home n/w, a MN is associated with COA & its home address is associated with local endpoint of a tunnel to its home agent.
- Mobile IP specifies how a MN registers with its HA & how the HA routes datagrams to the mobile node through the tunnel.

* **Packet Delivery:**

- Say a correspondant node (CN) wants to send an IP packets to MN. CN doesn't need to know anything about MN's current location.
- CN sends the IP packet with MN as destination address and CN as source address.

This packet is routed to home network of MN. HA router then intercepts packet & knowing that MN is not in home network, forwards it to FA of the foreign network in which MN is present with COA as address for MN. FA receives this & transfers it to MN. Then MN directly replies to the CN.



① Sender sends to IP address of MN, HA intercepts packet
② HA tunnels packet to COA, here FA, by encapsulation
③ FA forwards the packet to MN
④ MN now responds back to CN as usual, FA works a default router.

Working of Mobile IP

- Mobile IP has two addresses for a mobile host: one home address and one care of (COA) address. The Home address is permanent; COA changes as mobile host moves from one network to another. When mobile host & foreign agent are same, COA is called a co-located COA.
- CN (Correspondent Node) – An MN or fixed IP host linked to a router, which communicate IP packets to another MN in a home or foreign network.

Case I: CN & a fixed node & MN at home network
→ CN transmits for connection establishment or a packet using the IP protocol.
→ HA (Home Agent of MN) receives the msg or pkt &, using the info. that destined MN is at home n/w itself, it delivers the msg or pkt to MN.
→ Receives response pkt or msg from MN
→ Delivers it to CN using IP protocol.

Case II: CN & a mobile node (MN_k) & MN_1 both at home n/w HA_K & HA_1.
→ MN_K msg for connection establishment or a pkt using the IP protocol transmits through HA_K
→ Pkt delivers to HA_1 & then to MN_1
→ MN_1 response like in case I
→ HA_K & HA_1 deliver pkts from one end to another and vice versa by just forwarding the pkts to their respective MNs using IP protocol.

* Handoff Management
→ CN transmits a msg for connection establishment or a pkt using IP protocol.
→ HA_1 receives pkt & uses info that destined MN_1 is not at home n/w & is in foreign n/w reachable via foreign agent FA_j.
→ HA_1 encapsulates received IP pkt using a new header.
→ COA at new header over IP pkt sent by HA_1.
→ Handover - pkt encapsulated with new ~~broadcast~~ header with COA transmits to FA_j by tunnelling.

→ FAj reads CoA & decapsulates IP pkt.
→ Reads destination IP & transfers pkt to MN1

* Location Management

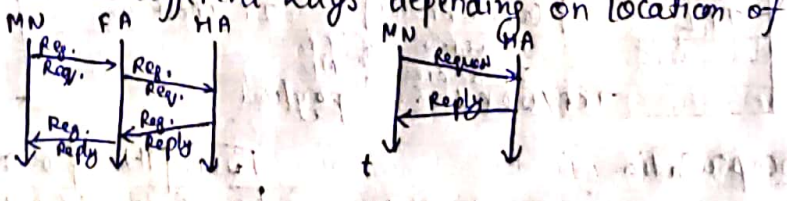
- Location Areas (LA): → A hybrid of paging and update
  - → Used in current cellular n/ws such as GSM
  - → Partitions cells into LA :- ex, around 10 cells in diameter in current systems
  - → Each cell (BTS) periodically announces its LA id.
  - → If a MS arrives at a new LA, it updates it base station about its presence
  - → when locating a MS, the n/w pages the cells in a LA.
- Dynamic / Distributed location Management:
  - → Timer based: A MS sends an update after some given time T
  - → Movement based: A MS ~~updates~~ sends an update after it has visited N different cells
  - → Distance based: A MS sends an update after it has moved away for D distance
  - → Profile based: A MS predicts its mobility model & updates the n/w when necessary.
- To communicate with a remote host, a mobile host goes through three phases:
  (i) Agent Discovery (ii) Agent Registration (iii) Data Transfer

(i) Agent Discovery

→ A MN has to find FA when it moves away from its Home n/w using two methods: agent advertisement & agent solicitation.
→ Agent advertisement: FA & HA advertise their presence periodically using special agent advertisement msgs, which are broadcast into the subnet. Mobile IP does not use a new pkt type; uses router advertisement pkt of ICMP.
→ Agent Solicitation: If no agent advertisements are present or inter-arrival time is too high & MN has not received a CoA by other means, the mobile node must send agent solicitations. Solicitation msgs do not flood the network. If a node doesn't receive an answer to its solicitations it must decrease the rate of solicitations exponentially to avoid flooding the network until it reaches a maximum interval between solicitations (typically one minute).
→ After these, MN can now receive a CoA, either one for an FA or colocated CoA.

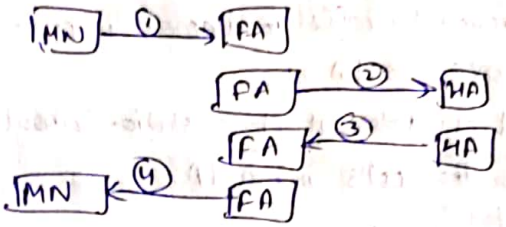
(ii) Agent Registration

→ It can be done in 2 different ways depending on location of the CoA.



→ If CoA is at FA, MN sends request containing CoA to FA which forwards the request to the HA. HA now sets up a mobility binding, containing MN's home IP address & current CoA & also lifetime of registration. After this, HA sends ~~back~~ reply back to FA which forwards it to MN.
→ If CoA is co-located, MN sends request directly to HA & vice versa.
→ UDP pkts used for registration request using port no. 434.

* Registering:
- Mobile Node sends an update (called registration request) to its HA with CoA info
- Home agent approves / disapproves the request
- HA adds necessary info to its Routing Table
- HA sends a registration reply back to MN



* Tunnelling and Encapsulation
- A tunnel establishes a virtual pipe for data pkts b/w tunnel entry & endpoint.
- Encapsulation (Higher to lower layer) is the mechanism of taking a pkt consisting of pkt header & data & putting it into data part of new pkt. It describes process of placing an IP datagram inside a network packet or frame. The reverse process of taking a pkt out of data part of another pkt is called decapsulation. (Lower to Higher layer)
- Tunnelling refers to use of a high level transport service to carry pkts or msgs from another service. Key difference b/w tunnelling & encapsulation lies in whether IP transmits datagram in b/w pkts or uses a high level transport service. IP encapsulates each datagram in a pkt when it uses h/w directly. It creates a tunnel when it uses a high level transport delivery service to send datagrams from one point to another.
- IP-in-IP encapsulation

→ Mandatory for mobile IP is IP-in-IP encapsulation.

ver.	IHL	DS (TOS)	length
IP identification		flags	fragment offset
TTL	IP-in-IP	IP checksum	
IP address of HA			
Care-of-address of CoA			
ver	IHL	DS (TOS)	length
IP identification		flags	fragment offset
TTL	lay. 4. protocol	IP Checksum	
IP address of CN			
IP address of MN			
TCP/UDP/... payload			

IHL - Inner Header Length

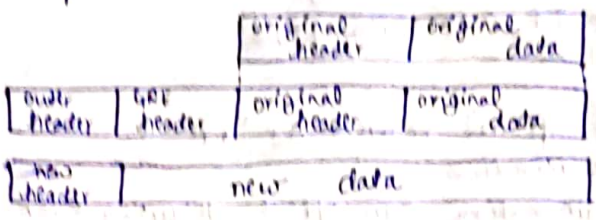
- Minimal Encapsulation

→ optional encapsulation method for Mobile IP which avoids repetitions of identical fields in IP-in-IP encapsulation.

ver.	IHL	DS (TOS)	length
IP identi-fication		flags	fragment offset
TTL	min. encap	IP checksum	
IP address of HA			
Care-of-address of CoA			
lay. 4 protocol	S	reserved	IP checksum
IP address of MN			
Original Sender IP address (if S=1)			
TCP/UDP/... payload			

- Generic Routing Encapsulation (GRE)

→ GRE allows encapsulation of pkts of one protocol suite into the payload portion of a pkt of another protocol suite as shown below:



→ If C is set, valid checksum of GRE header & payload

→ If R is set, offset & routing field valid info

→ If Key fields for authentication, K bit is set.

→ Sequence no. bit S indicates if seq. no. field is present.

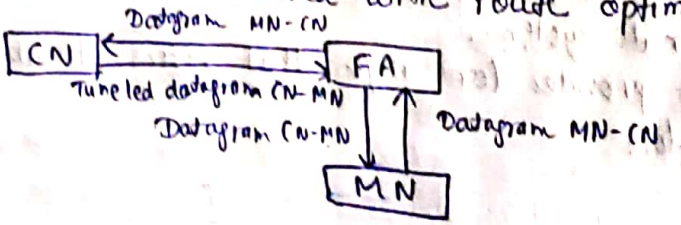
→ If s is set, strict source routing is used.

→ If rec. (recursion ctrl.) field represents a counter that shows the no. of allowed recursive encapsulation.

ver.	IHL	DS (TOS)	length
IP identification		flags	fragment offset
TTL	GRE	IP checksum	
IP address of HA			
Care-of-address of COA			
C R K S s Rec. rsv. ver.			Protocol
checksum (optional)			offset (optional)
Key (optional)			
Sequence number (optional)			
routing (optional)			
ver.	IHL	DS (TOS)	length
IP identification		flags	fragment offset
TTL	lay 4 prot.	IP checksum	
IP address of CN			
IP address of MN			
TCP / UDP / ... payload			

* Route Optimization

- Route optimization enables the datagrams to be routed directly in both directions.
- Route optimization also provides support for smooth handoffs by letting the previous foreign agent tunnel datagrams to mobile node's current location.
- The route optimization extension adds a conceptual data structure, the binding cache, to the correspondent node and to the foreign agent.
- The binding cache contains bindings for mobile nodes' home addresses and their current care-of-address. With the binding, the CN can tunnel datagrams directly to the mobile node's COA.
- Every time the HA receives a datagram that is destined to a mobile node currently away from home, it sends a binding update to the correspondent node to update the information in the correspondent node's binding cache.
- After this the CN can directly tunnel pkts to the MN. Thus direct bi-directional communication is achieved with route optimization.



- HA informs CN of loc^n. It needs four additional msgs:
  → Binding Request → Binding Update → Binding Acknowledgement
  → Binding warning

- Mobile IP support in IPv6 (Mobile IPv6)
  → integrated into IPv6
  → no need to deploy special routers as "FA"
  → support for route optimizations
  → Mobile IPv6 route optimization can operate securely even without pre-arranged security associations.
  → IPv6 neighbour unreachability detection assures symmetric reachability b/w MN & its default router in the current loc^n.
  → No IP encapsulation. Pkt sent using IPv6 routing header
  → More robustness

* DHCP (Dynamic Host Configuration Protocol)

- DHCP is a standardized automatic configuration protocol used on IP n/ws. DHCP allows a computer to join an IP-based n/w without having a pre-configured IP address. DHCP is a protocol that assigns unique IP addresses to devices, then releases and renews these addresses as devices leave and re-join the n/w.
- DHCP is based on client/server model. DHCP clients send a request to a server to which server reponds. A client sends requests using MAC broadcasts to reach all devices in the LAN. A DHCP relay might be used to forward requests across inter-working units to a DHCP server.
- DHCP is controlled by a DHCP server that dynamically distributes n/w config. parameters. A router or a residual gateway can be enabled to act as a DHCP server. A DHCP server enables computers to request IP addresses and n/w ing parameters automatically, reducing the need for a n/w admin or a user to configure these settings manually.
- In the absence of a DHCP server, each computer or other device on the n/w needs to be statically assigned to an IP address.

* Ad-Hoc N/w

→ An ad hoc n/w is a LAN that is built spontaneously as devices connect. Instead of relying on a base station to coordinate the flow of msgs to each node in the n/w, the individual n/w nodes forward pkts to & from each other.

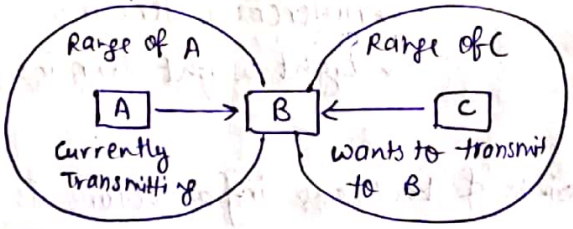
* Localization

→ Physical Localization occurs when exact physical loc^n of nodes is provided in reference to a coordinate system.
→ Symbolic localization only provides loc^n info. that refers to abstract predefined notions of place.

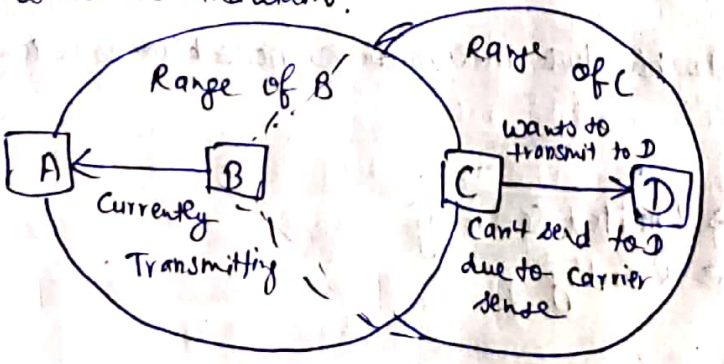
→ In fine-grained localization the nodes in the n/w can measure their distance or angle estimate to (a no. of) their neighbours, & thus infer their position.
→ In coarse-grained localization only proximity (connectivity) info is available. A node is in the position to detect its neighbouring nodes, but it does not possess any info. regarding its distance to them, except perhaps an upper bound of it implied by its detection capability range.

* MAC issues:

- Hidden Terminal Problem:
  → A hidden node is one that is within range of intended destination but out of range of sender.
  → Node B can communicate with A & C both.
  → A & C can't hear each other.
  → When A transmits to B, C can't detect transmission using carrier sense mechanism. C falsely thinks that the channel is idle.
  → If C transmits, collision will occur at node B.



- Exposed Terminal Problem
  → An exposed node is one that is within the range of the sender but out of range of destination.
  → Consider the case that node B is attempting to transmit to A.
  → Node C can hear transmission of B. When B senses the channel it finds the channel to be busy.
  → However, any transmission by C can't reach A (not in range), hence does not interfere with any reception at A.
  → In theory C can therefore have a parallel transmission with any node that can't hear transmission from B, i.e., out of range of B.
  → But C will not transmit to any node because its an exposed node. Exposed nodes waste bandwidth.



* MANETs (Mobile Ad Hoc NETworks)

- MANETs are wireless n/ws which are characterized by dynamic topologies & no fixed infrastructure. Each node in a MANET is a computer that may be required to act as both a host and a router and, as much, may be required to forward packets between nodes which cannot directly communicate with one another.
- A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. A mobile adhoc is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre-existing fixed n/w infrastructure.

- **MANET characteristics:**
  - → Dynamic n/w topology
  - → Energy constrained nodes
  - → Limited security
  - → Distributed operation
  - → Bandwidth constraint & variable link capacity
  - → Multi-hop communications
  - → Autonomous terminal
  - → Light-weight terminals

- **Need for Adhoc N/ws**
  - → Setting up of fixed access points & backbone infrastructure is not always viable.
  - → Adhoc n/ws:
    - ⇒ Do not need backbone infrastructure support
    - ⇒ Are easy to deploy
    - ⇒ Useful when infrastructure is absent, destroyed or impractical.

- **Properties of MANET**
  - → MANET enables fast establishment of n/ws.
  - → MANET's node has ability to discover its neighbouring node & service.
  - → MANET nodes have independent computational, switching (or routing), and communication capabilities.
  - → Wireless connectivity range in MANETs include only nearest node connectivity.
  - → There is no access point requirement in MANET.
  - → MANET nodes interact seamlessly when they move with the nearby wireless nodes, sensor nodes.
  - → Limited bandwidth available b/w two intermediate nodes becomes a constraint for MANET.

- **MANET Challenges**
  - → Dynamic Topology
  - → Limited Bandwidth
  - → Limited Security
  - → Routing

- **Applications of MANETs**
  - → Military Battlefield
  - → Vehicular Adhoc N/ws
  - → Sensor n/ws
  - → Civilian environments
  - → Local level
  - → Emergency operations
  - → PAN

* Routing Protocols

- Routing in MANET is an important issue as these n/ws donot have fixed infrastructure & routing requires distributed & cooperative actions from all nodes in the n/w. Routing protocols must use entire address to decide next hop.
- Some of the fundamental differences b/w wired n/ws & ad-hoc n/ws are
  → Asymmetric links → Redudant links → Interference
  → Dynamic Topology

— Types of MANET Routing Algorithms

(1.) Based on Info. used to Build Routing Tables

→ Shortest Distance Algorithms → Link State Algorithms (Build Topology Graph)

(2.) Based on Routing Tables are Built

→ Proactive Algorithms: # Always maintain routes # Ex:- DSDV, GSR, STAR, OLSR etc.
Consume bandwidth to keep routes upto date.
Maintain routes which may never be used.
Advantages: Low route latency, state information, QOS guarantee related to connection setup or real-time requirements.
Disadvantages: High overhead (periodic updates) & route repair depends on update-frequency.

→ Reactive Algorithms: # only obtain route information when needed.
Advantages: no overhead from periodic update, scalability as long as there is only light traffic & low mobility.
Disadvantages: High route latency, route caching can reduce route latency.
Ex:- AODV, TORA, ABR etc.

→ Hybrid Algorithms: Ex:- ZRP (Zone Routing Protocol)

* Global State Routing (GSR) Protocol

- Similar to DSDV. It take idea of link state Routing but improves it by & avoiding flooding of routing msgs.
- In this algorithm, each node maintains a neighbour list, a topology list, a next hop table & a distance table.
- Neighbour list of a node contains list of its neighbours. For each destination node, topology table contains the link state information as reported by destination & timestamp of info.
- For each destination, the next hop table contains next hop to which pkts for this destination must be forwarded.
- The distance table contains shortest distance to each destination node. The routing msgs are generated on a link change as in link state protocols. On receiving a routing msg, the node updates its topology table if the sequence no. of the msg is newer than seq. no. stored in table.
- After this the node reconstructs its routing table & broadcasts the info. to its neighbours.

Destination Sequenced Distance Vector (DSDV) Routing

- DSDV is an example of proactive algorithm and an enhancement to DVR for ad-hoc n/ws. DVR is used as routing information protocol (RIP) in wired n/ws.
- DSDV is a table-driven routing scheme for adhoc mobile n/ws based on the Bellman-Ford algorithm.
- Each entry in the routing table contains a sequence number, the sequence numbers are generally even if a link is present, else an odd number is used.
- The number is generated by the destination, and the emitter needs to send out the next update with this number.
- Routing information is distributed b/w nodes by sending full dumps infrequently and smaller incremental updates more frequently.

When X receives info from Y about a route to Z

→ Let dest. seq. no. for Z at X be S(X), S(Y) is sent to Y

→ If S(X) > S(Y), then X ignores routing info. received from Y

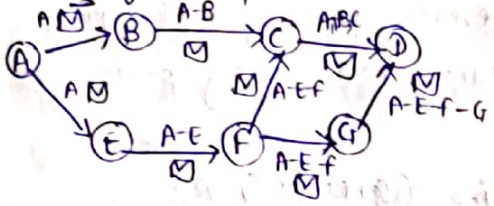
→ If S(X) = S(Y), & cost of going through Y is smaller than route known to X, then X sets Y as the next hop to Z.

→ If S(X) < S(Y), then X sets Y as the next hop to Z, & S(X) is updated to equal S(Y).

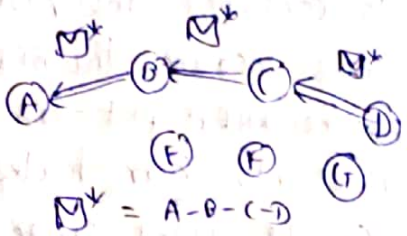
* Dynamic Source Routing (DSR)

- DSR is a source-routed on-demand routing protocol designed specifically for use in multi-hop wireless ad-hoc n/ws of mobile nodes. DSR allows the n/w to be completely self-organizing and self-configuring, without the need for any existing n/w infrastructure or administration.
- A node maintains route caches containing the source routes that it is aware of. The node updates entries in the route cache as & when it learns about new routes.
- The two major phases of protocol are route discovery and route maintenance which work together to allow nodes to discover & maintain routes to arbitrary destinations in the ad hoc n/w.
- When the source node wants to send a packet to a destination, it looks up its route cache to determine if it already contains a route to the destination. If it finds that an unexpired route to the destination exists, then it uses this route to send the pkt. But if the node does not have such a route, then it initiates the route discovery process by broadcasting a route request pkt.

- The route pkt contains the address of source & destination, and a unique identification number. Each intermediate node checks whether it knows of a route to the destination. If it does not, it appends its address to the route record of pkt & forwards pkt to its neighbours.
- To limit no. of route requests propagated, a node processes the route request pkt only if it had not already seen the pkt and it's address is not present in the route record of the pkt.



Propagation of Route Req. (RREQ)
A → D



Propagation of Route Reply (RREP)
D → A

* Ad Hoc On Demand Distance Vector (AODV) Routing

- Advantages:
  - → Route maintained only b/w nodes who need to communicate - reduces overhead of route maintenance
  - → Routing caching can further reduce route discovery overhead
  - → A single route discovery may yield many routes to the destination, due to intermediate nodes replying from local caches.
- Disadvantages
  - → Pkt header size grows with route length due to source routing.
  - → Flood of route req. may potentially reach all nodes in the n/w.
  - → Care must be taken to avoid collisions b/w route req. propagated by neighbouring nodes - insertion of random delays before forwarding RREQ.
  - → Increased contention if too many route replies come back due to nodes replying using their local cache - Route Reply storm problem. Reply storm may be eased by preventing a node from sending RREP if it hears another RREP with a shorter route.
  - → An intermediate node may send RREP using a stale cached route, thus polluting other caches.

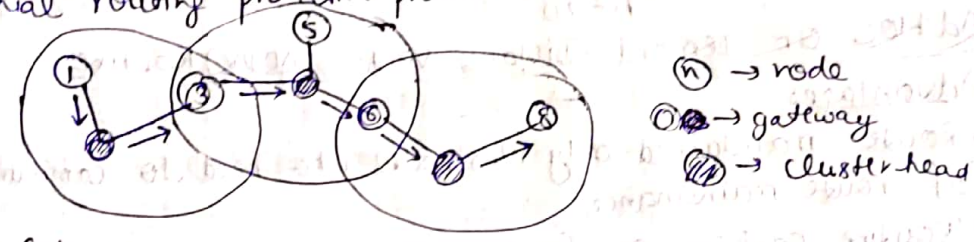
* Ad Hoc On Demand Distance Vector (AODV) Routing

- AODV is a reactive protocol & is an improvement on DSDV algorithm.
- AODV minimizes the no. of broadcasts by creating routes on-demand as opposed to DSDV that maintains the list of all the routes.
- To find a path to the destination, the source broadcasts a route request pkt. The neighbour in turn broadcast the pkt to their neighbours till it reaches an intermediate node that has a recent info. about destination or till it reaches the destination.

- A node discards a route request pkt that it has already seen. The route req. pkt uses seq. no. to ensure that routes are loop-free and to make sure that if the intermediate nodes reply to RREQ, they reply with latest info. only.
- When a node forwards a RREQ pkt to its neighbours, it also records in its tables the node from which first copy of req. came. This info. is used to construct the reverse path for route reply pkt. AODV uses only symmetric links because the RREP pkt follows reverse path of RREQ pkt.
- As the RREP pkt traverses back to source, nodes along path enter the forward route into their tables.

* Cluster-Head Gateway Switch Routing (CGSR)

- It is a hierarchial routing proactive protocol.



- CGSR works as follow:
  - → Periodically, every nodes sends a hello msg containing its ID & a monotonically increasing sequence number.
  - → Using these msgs, every cluster-head maintains a table containing the IDs of nodes belonging to it and their most recent seq. nos.
  - → Cluster-heads exchange these tables with each other through gateways; eventually, each node will have an entry in the affiliation table of each cluster-head. This entry shows the node's ID & cluster-head of that node.
  - → Each cluster-head & each gateway maintains a Routing Table with an entry for every cluster-head that shows the next gateway on the shortest path to that cluster head.
- Disadvantages:
  - → The same disadvantage common to all hierarchial algorithms related to cluster formation & maintenance.

* Hierarchial State Routing (HSR)

- A hierarchal link state routing protocol that solves loc^n management problem ~~find~~ found in MMWN by using logical subnets.
- HSR Procedure
  1. Based on physical distance, nodes are grouped together into clusters that are supervised by cluster heads. There are more than one-level of clustering.
  2. Every node has two address:
     - a) hierarchial-ID (HID), composed of node's MAC address prefixed by IDs of its parent cluster.

⑵ a logical address in the form <subnet, host>.

⑶ Every logical subnet has a home agent, i.e., a node that keeps track of the HID of all members of that subnet.

⑷ HIDs of HA are known to all cluster-heads, & the cluster-head can translate the subnet part of the node's logical address to HID of corresponding HA.

⑸ when a node moves to a new cluster, the head of the cluster detects it & informs the node's HA about node's new HID.

⑹ when a HA moves to a new cluster, the head of cluster detects it and informs all other cluster-heads about HA's new HID.

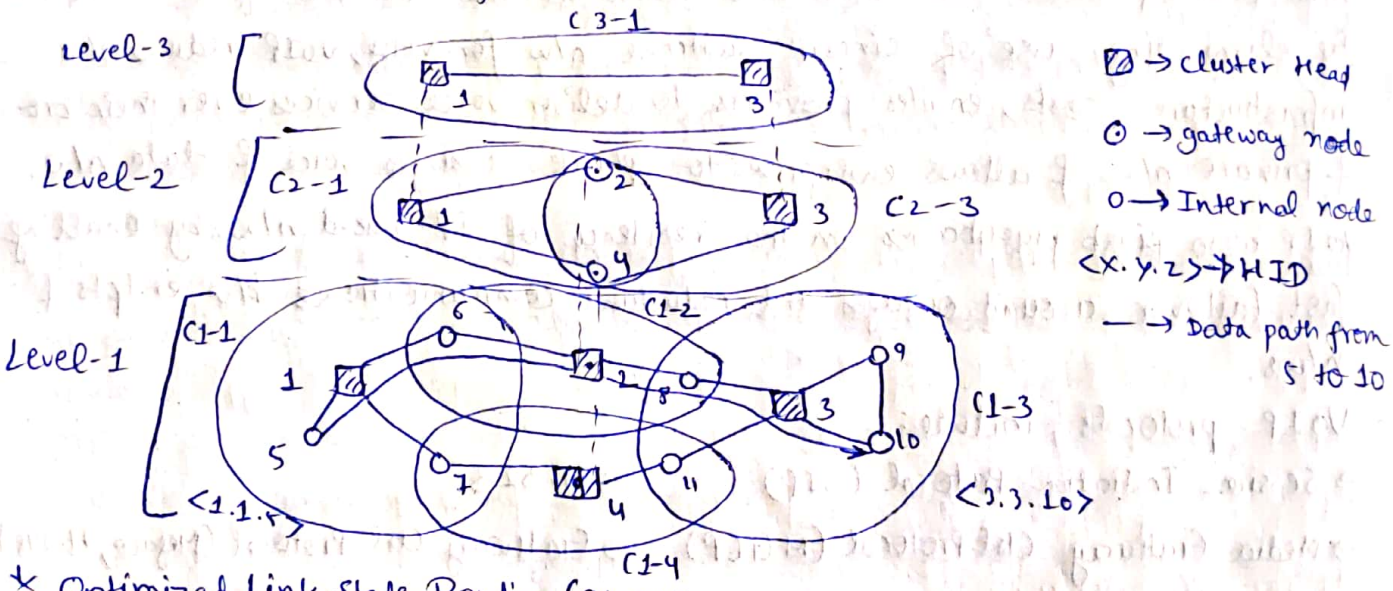
– To start a session

① source node informs its cluster head about the logical address of dest. node.

② cluster-Head looks up HID of dest. node's HA and uses it to send query to the HA asking about destination's HID.

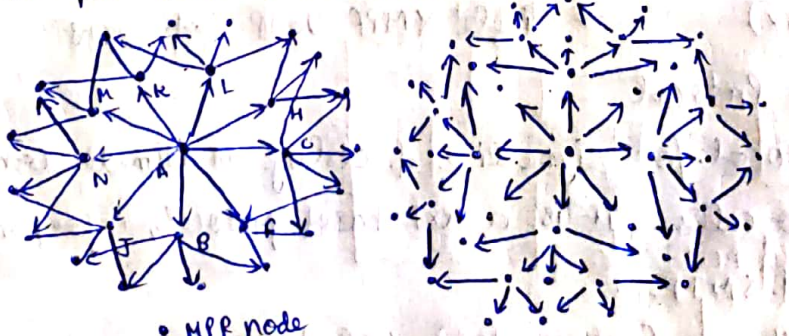
③ After knowing dest.'s HID, cluster head uses its topology map to find a route to the dest.'s cluster-head.

– Disadvantages: Cluster formation & maintenance



* Optimized Link State Routing (OLSR)

– It only required updates are sent to routing database. This reduces overhead ctrl pkt size & numbers.



– OSLR uses controlled-flood to disseminate link state info of each node.

→ Every nodes creates a list of its one hop neighbours

→ Neighbour nodes exchange their lists with each other

→ Based on received lists, each node creates its MPR. The multipoint relays of each node, (MPR), is the minimal set of 1 hop nodes that covers all hop points.

→ The members of the MPR are the only nodes that can retransmit the link state info. in an attempt to limit the flood.

* Security Attacks in MANET

- External Attack - Internal Attack - DOS Attack - Impersonation
- Eavsdropping - Routing Attacks

* Voice Over IP (VoIP)

- Voice Over Internet Protocol (Voice Over IP, VoIP & IP telephony) is a methodology and group of technologies for delivery of voice communications & multimedia sessions over Internet Protocol (IP) n/ws, such as Internet. The terms Internet telephony, broadband telephony, & broadband phone service specifically refer to provisioning of communications services (voice, fax, SMS, voice-msging) over public Internet, rather than via PSTN.
- Digital info is pktized & transmission occurs as IP pkts over a ~~PSDN~~ public switched n/w.
- VoIP is the transmission of voice & multimedia content over IP n/w. VoIP encapsulates audio via a codec into data pkts, transmits them across an IP n/w & decapsulates them back into audio at the other end of the connection.
- By eliminating use of circuit-switched n/w for voice, VoIP reduces n/w infrastructure costs, enables providers to deliver voice services over their broadband & private n/ws, & allows enterprises to operate a single voice & data n/w.
- VoIP also ~~pigyb~~ piggybacks on the resilency of IP-based n/ws by enabling fast failover around outages and reducdant communications b/w endpts & n/ws.
- VoIP protocols include:
  - → Session Initiation Protocol (SIP) → H.323
  - → Media Gateway Ctrl Protocol (MGCP) → Gateway Ctrl Protocol (Megaco, H.248)
  - → Real-time Transport protocol (RTP) → Real-time Transport Ctrl Protocol (RTCP)
  - → Secure Real-time transport protocol (SRTP) → Session Description Protocol (SDP)
  - → Inter-Asterisk eXchange (IAX) → Jingle XMPP VoIP extensions
  - → Skype Protocol
- SIP is a communications protocol for signalling & ctrling multimedia communication session such as voice & video calls. It is a text-based protocol, incorporating many elements of ~~HTTP~~ HTTP & SMTP.
- For transmission of media streams (voice, video), SIP typically employs RTP or SRTP. For secure transmissions of SIP msgs, protocol may be encrypted with Transport Layer Security (TLS).

- SIP n/w elements are user agent, proxy server, registrar, redirect server, session border ctrller, gateway, SIP msgs, REQUEST, RESPONSES
- SIP for Instant Messaging & Presence Leveraging Extensions (SIMPLE) is a SIP-based suite of standards for instant msging & presence info. MSRP (Msg Session Relay Protocol) allows instant msg sessions & file transfer.
- A SIP connection is a marketing term for VoIP services offered by many Internet telephony service providers (ITSPs).
- H.323 is a system specification that describes use of several ITU-T & IETF protocols
- H.323 system defines several n/w elements that work together in order to deliver rich multimedia communication capabilities. Those elements are Terminals, Multipoint Ctrl Units (MCUs), Gateways, Gatekeepers, & Border Elements. Collectively terminals, MCUs & gateways are often referred as endpoints.
- The MGCP is a signalling & call ctrl communications protocol used in VoIP telecommunication systems. It implements media gateway ctrl protocol architecture for ctrling media gateways on IP n/ws connected to PSTN. It is successor of Simple Gateway Ctrl Protocol (SGCP) & the Internet Protocol Device Ctrl (IPDC)
- Gateway Ctrl Protocol (H.248) is an implementation of the media gateway ctrl protocol architecture for providing telecommunication services across a converged internetwork consisting of traditional PSTN & modern pkt n/ws such as the Internet.
- The primary func^n of RTCP is to provide feedback on QOS in media distribution by periodically sending statistics info to participants in a streaming multimedia session.
- SDP is a format for describing streaming media initialization parameters.
- IAX is a communication protocol native to Asterisk private branch exchange (PBX) s/w & is supported by few other software switches, PBX systems & soft phones.
- Jingle is an extension to the Extensible Msging & Presence Protocol (XMPP) which adds peer-to-peer (P2P) session ctrl (signaling) for multimedia interactions such as VoIP or videoconferencing communications.
- XMPP is a communications protocol for msg-oriented middleware based on XML. It enables near-real-time exchange of structured yet extensible data b/w any two or more n/w entities.
- Skype protocol is a proprietary Internet telephony n/w based on peer-to-peer architecture, used by Skype.

* IPSEC (Internet Protocol Security)

- IPsec is a protocol suite for secure IP communications that works by authenticating & encrypting each IP pkt of a communication session.
- IPsec includes protocols for establishing mutual authentication b/w agents at the beginning of the session & negotiation of cryptographic keys for use during the session.
- IPsec can protect data flows b/w a pair of hosts (host-to-host), b/w a pair of security gateways (n/w-to-n/w), or b/w a security gateway & a host (n/w to host)
- IPsec uses cryptographic ~~set~~ security services to protect communications over IP n/ws.
- IPsec supports n/w-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption) & replay protection.

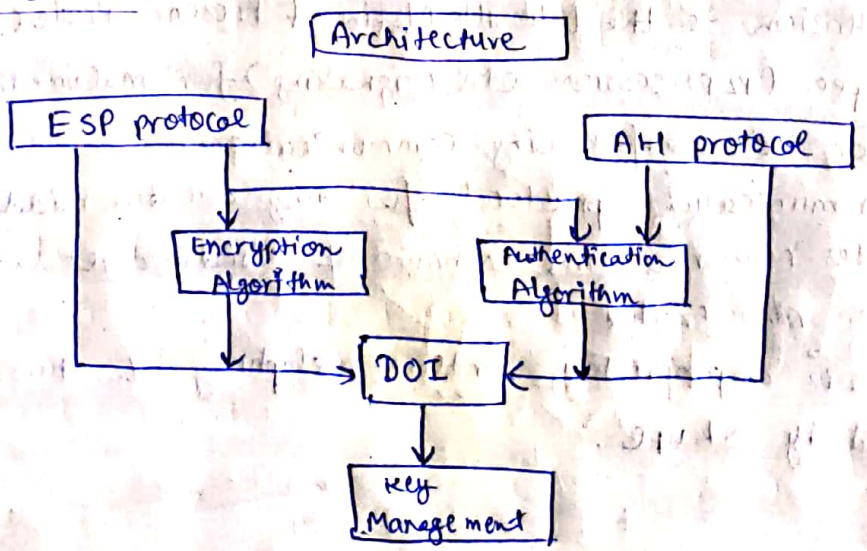
- Appl^{n}s of IPsec

→ Secure branch office connectivity over the Internet
→ Secure remote access over the Internet
→ Establishing extranet & intranet connectivity with partners
→ Enhancing electronic commerce security.

- Benefits of IPsec

→ when IPsec is implemented in a firewall or router, it provides strong security that can be applied to all traffic crossing the perimeter.
→ IPsec is below transport layer & so is transparent to appl^{n}s.
→ IPsec can be transparent to end users
→ IPsec can provide security for individual users if needed.

- IPsec architecture



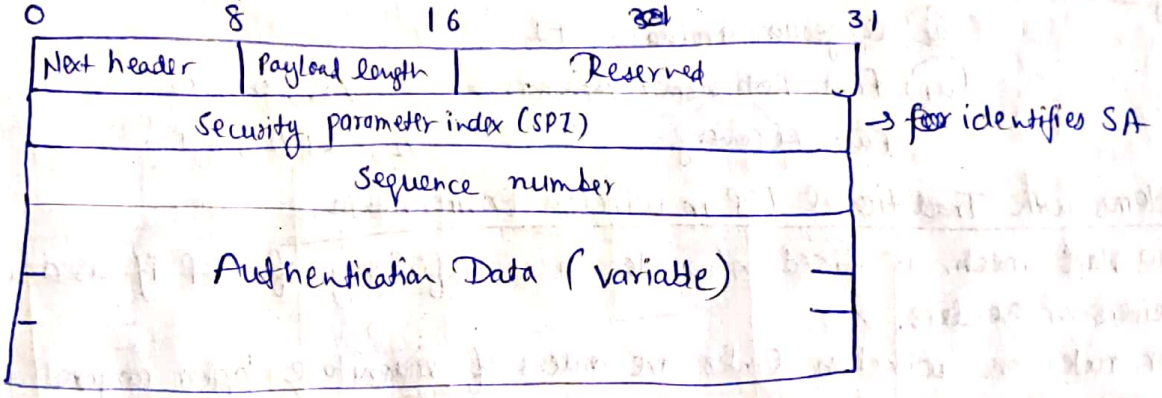
ESP - Encapsulating Security Payload
AH - Authentication Header
DOI - Domain of Interpretation

IPsec document overview

- IPsec services are:
  → Access Ctrl → Connectionless integrity → Data origin authentication
  → Rejection of replayed pkts → Confidentiality → Limited traffic flow Confidentiality

	AH	ESP (Encryption only)	ESP (Encryption + Authentication)
Access Ctrl	✓	✓	✓
Conn. less Integrity	✓		✓
Data origin Auth.	✓		✓
Rejection of Replayed Pkts	✓	✓	✓
(Encryption) Confidentiality		✓	✓
Limited Traffic flow confidentiality		✓	✓

	Transport Mode Security Association (SA)	Tunnel Mode SA
AH	Authenticates IP payload & selected portions of IP header & IPv6 extension headers.	Authenticates entire IP header + selected portions of outer IP header & outer IPv6 extension headers
ESP	Encrypts IP payload & any IPv6 extension headers following ESP header.	Encrypts entire inner IP pkt
ESP with Authentication	Encrypts IP payload & any IPv6 extension headers	Encrypts entire inner IP pkt. Authenticates inner IP pkt.



IPsec authentication header

- A replay attack is one in which an attacker obtains a copy of an authenticated pkt & later transmits it to the intended dest. which may disrupt service.
- Key management portion of IPsec involves determination & distribution of secret keys.
- IPsec architecture document mandates support for two types of key management:
  → Manual → Automated (Protocol → ISAKMP / Oakley)
- Oakley key Determination Protocol: Oakley is a key exchange protocol based on Diffie Hellman algo. but providing added security. Oakley is generic in that it does not dictate specific formats.
- Internet Security Association & Key Management Protocol (ISAKMP): It provides a framework for Internet key management & provides the specific protocol support, including formats, for negotiation of security attributes.

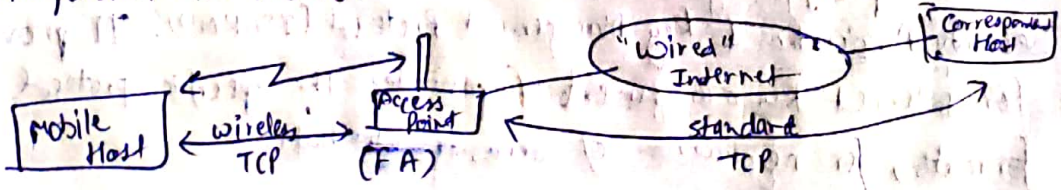
Traditional TCP/IP

- TCP/IP is the basic communication language or protocol of the Internet. It can also be used as a communication protocol in a private network (either an intranet or extranet).
- TCP/IP is a two-layer program. The higher layer, TCP, manages the assembling of a message or file into smaller pkts that are transmitted over the Internet and received by a TCP layer that reassembles the pkts into the original msg.
- The lower layer, IP, handles the address part of each pkt so that it gets to the right destination. Each gateway computer on the n/w checks this address to see where to forward the msg.
- Even though some pkts from the same msg are routed differently than others, they'll be reassembled at the destination.
- The major responsibilities of TCP in an active session are to:
  - → Provide reliable in-order transport of data : To not allow losses of data
  - → Control congestions in the n/ws : To not allow degradation of the n/w performance
  - → Control a pkt flow b/w the transmitter & the receiver : To not exceed the receiver's capacity.
- Congestion Ctrl: (i) slow start 2x
  (ii) Congestion avoidance +1
  (iii) Fast Retransmit /2, 0, x2
  Fast Recovery /2, /2, +1
- Problems with Traditional TCP in wireless Environments
  - → slow start mech. is fixed n/w decreases efficiency of TCP if used with mobile receivers or senders.
  - → Error rates on wireless links are orders of magnitude higher compared to fixed fiber or copper. This makes compensation for pkt loss by TCP quite difficult.
  - → Mobility itself can cause pkt loss
  - → slow start mxn of TCP results in severe performance degradation with wireless links or mobile nodes.

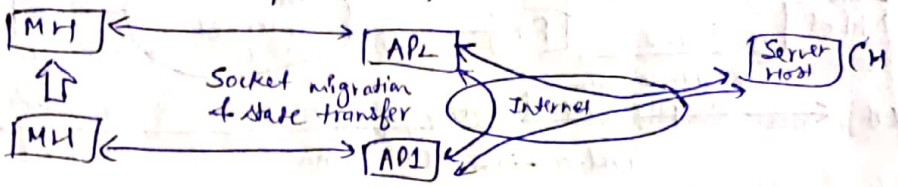
Classical TCP Improvements

Indirect TCP (I-TCP)

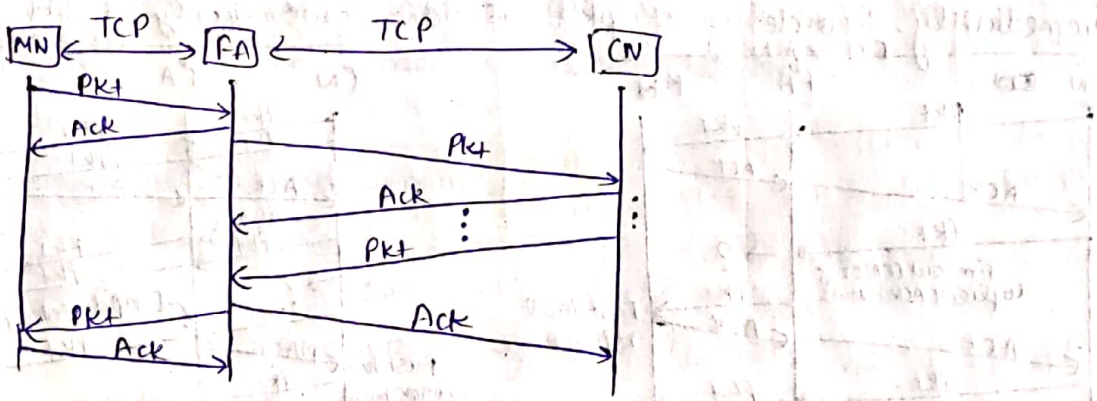
→ It segments a TCP conn. into fixed part & wireless part. Ex:- with mobile host connected via a wireless link & an access point to the 'wired' internet where the correspondent host resides.



- Standard TCP is used b/w fixed computer & access point (AP). The AP now terminates standard TCP conn., acting as proxy. This means that AP is now seen as the MH for fixed host & as the fixed host for MH. B/w AP & MH, a special TCP, adapted to wireless links, is used. However, changing TCP for wireless link is not a requirement. A suitable ~~post~~ place for segmenting the conn. is at FA.



- The FA acts as a proxy & relays all data in both directions. If Correspondant Host (CH) sends a pkt to MH, FA acknowledges it & forwards it to MH. MH acknowledges on successful reception, but this is only used by FA. If a pkt is lost on wireless link, CH doesn't observe it & FA tries to retransmit it locally to maintain reliable data transport. If MH sends a pkt, FA acknowledges it & forwards it to CH. If pkt is lost on wireless link, the MH notices this & much-faster due to lower round trip time and can directly retransmit the pkt. Pkt loss in wired n/w is now handled by the FA.
- During handover, buffered pkts, as well as system state must migrate to new agent. No new conn. may be established for mobile host, & CH must not see any changes in conn. state.



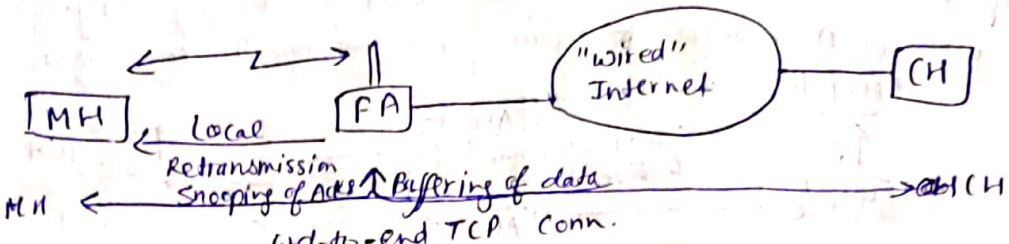
Pkt Delivery in I-TCP

- Advantages: (i) No changes in fixed n/w ~~necessary, no~~, hosts necessary.
  (ii) Simple to Ctrl, mobile TCP used only for one hop b/w FA & MH.
  (iii) Transmission error in wireless don't propagate to fixed part. Thus, fast retransmission possible & short delay on mobile hops known.
  (iv) New optimizations can be tested at last hop, without jeopardizing stability of Internet.
  (v) Easy to use different protocols for wired & wireless n/ws.
- Disadvantages: (i) Loss of end-to-end semantics
  (ii) Higher latency possible
  (iii) Security issue

* Snooping TCP

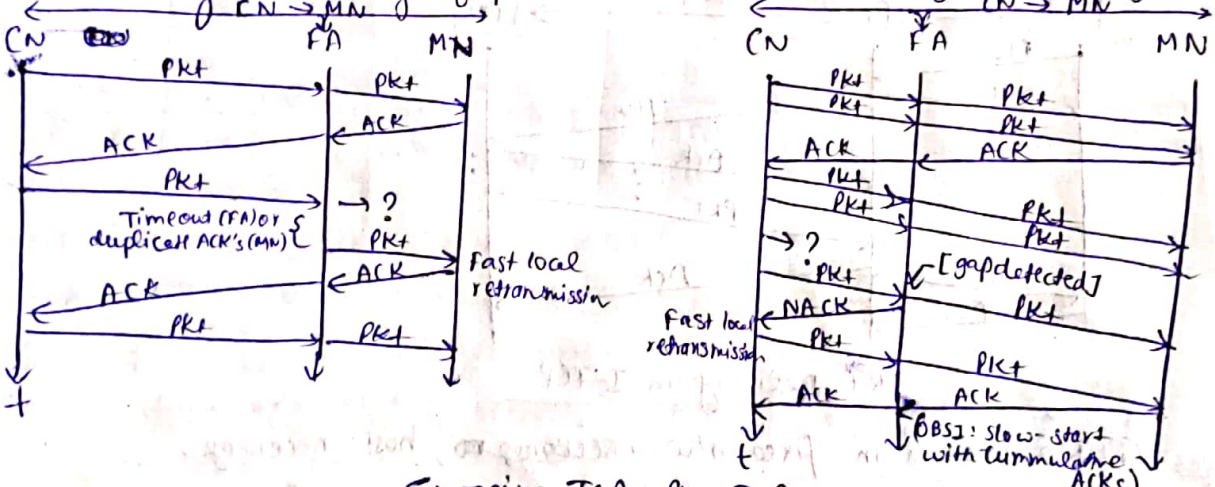
- The main drawback of I-TCP is the segmentation of single TCP conn. into two TCP conn. (s), which loses original end-to-end TCP semantic. A new enhancement

which leaves TCP conn. intact & is completely transparent, is Snooping TCP. The main funcn is to buffer data close to MH to perform fast local retransmission in case of ~~loss~~ pkt loss.



Snooping TCP as transparent TCP extension

- Here, FA buffers all pkts with dest. MH & additionally 'snoops' the pkt flow in both directions to recognize acknowledgements. The FA buffers every pkt until it receives an ~~A~~ ack. from MH within time limit, either pkt or ack have been lost. A FA could receive a duplicate ACK which also shows the loss of a pkt. Now, FA retransmits the pkt directly from buffer thus performing a faster retransmission cmped to CH. FA can filter duplicate acks. to avoid unnecessary retransmissions of data from CH.
- For data transfer from MH with dest. CH, FA snoops into pkt stream to detect gaps into seq. nos. of TCP. As soon as FA detects a missing pkt, it returns a negative ACK (NACK) to MH. The MH can now retransmit missing pkt immediately. Reordering of pkt is done automatically at CH by TCP.



Snooping TCP: Pkt Delivery

- Advantages: # End-to-End TCP semantic is preserved
  # Most of enhancements done in FA itself which keeps CH unchanged.
  # Handover of state not required as soon as MH moves to another FA.
  # No problem arises if ~~a~~ new FA uses enhancement or not.
- Disadvantages:
  # Snooping TCP does not isolate wireless link as good as I-TCP
  # Snooping & buffering may be useless if pkts are encrypted.

* Mobile TCP

- M-TCP is especially adapted to problems arising from lengthy or frequent discon.
- M-TCP splits up the conn. into two parts:
  - → An unmodified TCP is used on standard host - Supervisory Host section
  - → An optimised TCP is used on supervisory host - Mobile Host section.
- The Supervisory Host (SH) adorns the same role as the proxy (FA) in I-TCP. The SH is responsible for exchanging data to both Standard host and mobile host.
- Here in this approach, we assume that the error bit rate is less as cmped to other wireless links. So if any pkt is lost, the retransmission has to occur from original sender and not by the SH. (This also maintains end-to-end TCP semantic)
- The SH monitors the ACKs (ACK means acknowledgement) being sent by MH. If for a long period ACKs have not been received, then SH assumes that MH has been disconnected (maybe due to failure or moved out of range, etc...).
- If so the SH chokes the sender by setting its window size to 0. Because of this sender goes into persistent mode, i.e., the sender's state will not change no matter how long the receiver is disconnected. This means that the sender will not try to retransmit the data. Now when SH detects a connectivity established again with the MH (the old SH or new SH if hand-over), the window of the sender is restored to original value

- Advantages:
  - → Maintain TCP end-to-end semantics
  - → Avoids useless retransmissions, slow starts or breaking conn. by simply shrinking sender's window to 0 in case MH is disconnected.
  - → There is no need to forward buffers to new SH. Lost pkts will be automatically retransmitted to the SH.
- Disadvantages:
  - → M-TCP assumes low bit error rates, which is not always a valid assumption. As the SH does not act as proxy as in I-TCP, pkt loss on wireless link due to bit errors is propagated to the sender.
  - → A modified TCP on the wireless link not only requires modifications to the MH protocol s/w but also new n/w elements like the bandwidth manager.

* A comparison of classical enhancements to TCP for Mobility

Approach	Mechanism	Advantages	Disadvantages
Indirect TCP	splits TCP connection into two connections	Isolation of wireless link, simple	Loss of TCP semantics, higher latency at handover
Snooping TCP	"snoops" data & acknowledgements, local retransmission	Transparent for end-to-end conn., MAC integration possible	Problematic with encryption, bad isolation of wireless link
Mobile TCP	Splits TCP connection, chokers sender via window size	Maintains end-to-end semantics, handles long term and frequent disconnections	Bad isolation of wireless link, processing overhead due to bandwidth management
Fast Retransmit/ Fast Recovery	Avoids slow-start after foaming	Simple & efficient	Mixed layers, not transparent
Transmission/ Time-out freezing	Freezes TCP state at disconnect, resumes after reconnection	Independent of content or encryption, works for longer interrupts	Changes in TCP required, MAC dependent
Selective Retransmission	Retransmit only lost data	Very efficient	Slightly more complex receiver s/w, more buffer needed
Transaction oriented TCP	Combine connection setup/ release and data transmission	Efficient for certain applications	Changes in TCP required, not transparent