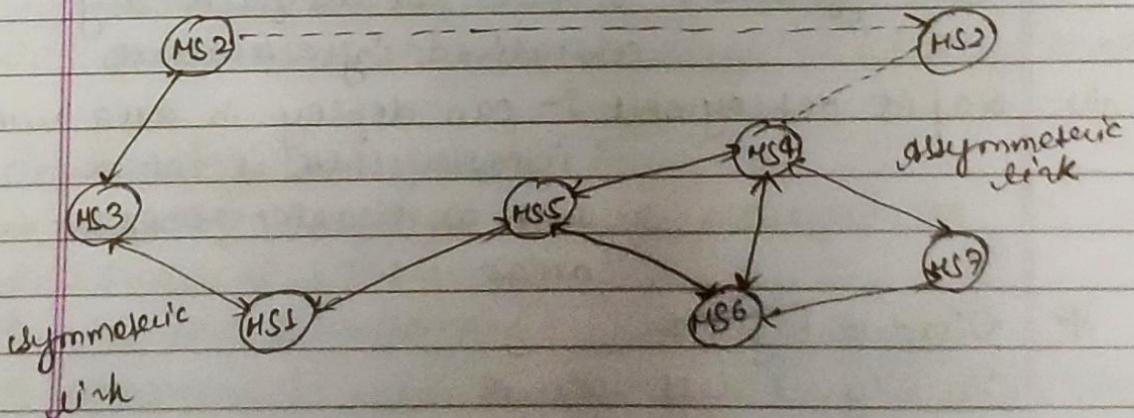


* Internet Based Mobile Ad-hoc Networking :-

- A mobile Adhoc network (MANET) is an autonomous system of mobile nodes connected by wireless links.
- A MANET does not necessarily need support from any existing n/w infrastructure like an Internet gateway or others fixed station.
- The n/ws wireless topology may dynamically change in an unpredictable manner since nodes are free to move.
- Syo- is transmitted in a store and forward manner using multi-hop routing.
- Each node is equipped with a wireless transmitter and a receiver with an appropriate antenna.
- It is not possible to have all nodes within each other's radio range.
When the nodes are close by i.e., within radio range, there is no routing issue.
- Each node behaves as a router as they forward traffic to other specified nodes in the n/w.



* Characteristics of Ad-Hoc Networks :-

- (i) Dynamic Topologies :- Network topology may change dynamically as nodes are加入或移除.
- (ii) Bandwidth constraint, variable capacity :- Wireless links usually have lower reliability, efficiency, stability and capacity as compared to wired networks.
- (iii) Autonomous behaviour :- Each node acts as a host and router.
- (iv) Limited security :- more prone to security threats.
- (v) Less Human intervention :- requires less human intervention, as it is dynamically autonomous in nature.

* Advantages :-

- (i) Flexibility :- highly flexible and can deploy in diff. environment
- (ii) Scalability :- easily accommodate large no. of nodes.
- (iii) Cost-effective :- as it does not require any centralized infrastructure
- (iv) Rapid deployment :- can deploy in area where infrastructure is not available, such as disaster zones or rural areas.

* Disadvantages :-

- (i) Security → less secure
- (ii) Reliability → less reliable and diff. factors affect the quality of connection.

- (iii) Bandwidth is limited bandwidth
- (iv) Routing is complex Routing
- (v) Power consumption is high.

* Applications :-

- (i) Virtual navigation
- (ii) Tele-medium
- (iii) Tele-processing
- (iv) Crisis management
- (v) Education via internet

* Routing in MANETS :-

- (i) Provides max^m reliability \rightarrow uses alternative routes if an intermediate node fails.
- (ii) Choose a route with least cost metric.
- (iii) Route computation must be distributed. Centralized routing is usually very expensive.
- (iv) Every node must have quick access to routes on demand.
- (v) Each node must be only concerned about the routes to its destination.
- (vi) Broadcasts should be avoided (highly unreliable).

* Routing classification :-

\rightarrow Routing protocols can be classified as

- (P) Proactive (Table-driven)
- (R) Reactive (On-demand)
- (P) Proactive :- when a packet needs to be forwarded route is already known
- (R) Reactive :- Determine route on demand

<u>Predictive</u>	<u>Reactive</u>
(i) level of delay is low because routes are pre-determined	High
(ii) Period update is always required	does not require
(iii) Routes are always available	Compute on demand
(iv) Structure of Route is flat / hierarchical	flat

- * Routing protocols may also be categorized as,
 - Table Driven protocols
 - Source Initiated (on-demand) protocols

- * Table - Driven Routing protocols :-
 - Each node maintains routing info. to all other nodes in the n/w.
 - When topology changes, updates are propagated throughout the n/w.
 - Examples are :-
 - Destination Sequenced Distance Vector Routing (DSDV)
 - Cluster- Head Gateway Switch Routing (CCSR)
 - Wireless Routing Protocol (WRP)

(OSPF)

- * Destination sequenced Distance Vector Routing :-
- DSDV is a hop-by-hop vector Routing algo. requiring each node to periodically broadcast routing updates.
- It uses proactive protocol and is based on Bellman-Ford routing mechanism.
- Each node maintains a routing Table with entries as no. of hops to each destination, sequence no. which helps to distinguish * stale (already visited) routes from new ones thereby avoiding loops.
- To minimize routes variable sized update packets are used depending on the no. of topological changes.
- Routing tables updates in DSDV are distributed by 2-different types of update packets :-

 - (i) Full-Dump :- This type of update packet contains all the routing info. available at a node.
 - (ii) Incremental :- Contains only the info. that has changed since the latest full dump was sent out by the node

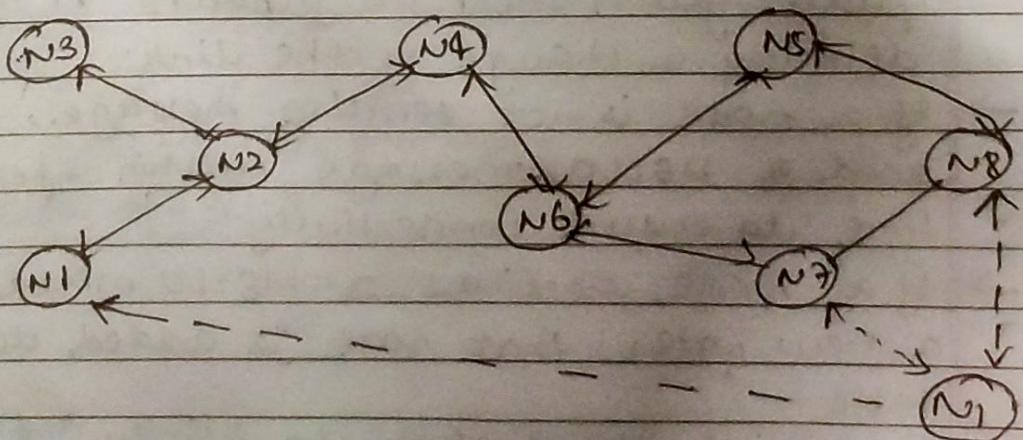


Table-1

Routing Table at Node 4

<u>Dest.</u>	<u>Metric</u>	<u>Seq. no.</u>
N1	2	S906 - N2
N2	1	S128 - N2
N3	2	S864 - N2
N4	0	S710 - N6
N5	2	S392 - N6
N6	1	S076 - N6
N7	2	S128 - N6

Table-2

R.T. ~~is~~ updated yet node

<u>Dest.</u>	<u>Metric</u>	<u>Seq. no.</u>
N1	3	S816 - N6
N2	1	S238 - N2
N3	2	S634 - N2
N4	0	S820 - N4
N5	2	S502 - N6
N6	1	S186 - N6
N7	2	S238 - N6

* The wireless routing Protocol :-

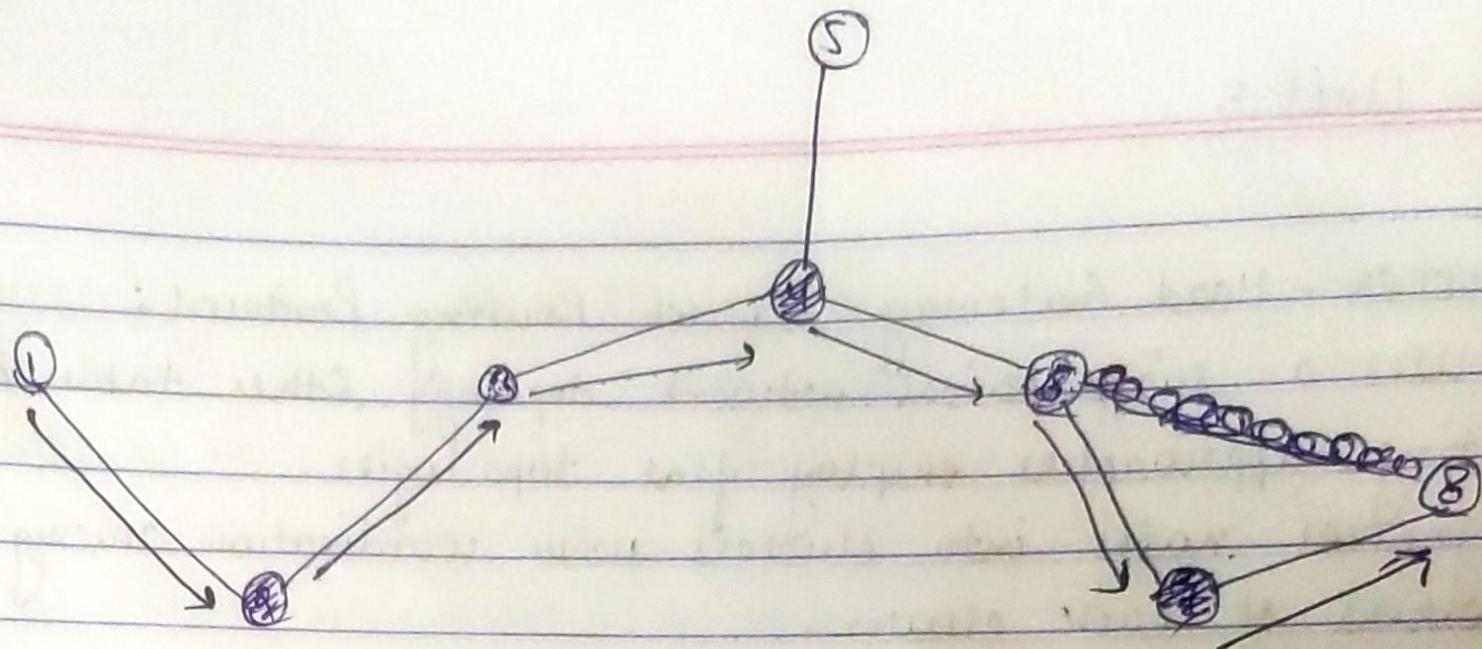
- Each node maintains 4-tables.
- ① Distance table
- ② Routing table
- ③ Link cost table
- ④ Message Retransmission List Table (MRL)
- Nodes inform each other of link changes using update messages.
- Nodes send update messages after few cycles of updates from their neighbours or after detecting a change in the link.
- If a node is not sending messages, it must send a HELLO message within specified time to ensure connectivity.
- If a node receives a HELLO message from a new node, that node is added to the table.
- It avoids the "count to infinity" problem.

* On-Demand Routing Protocol :-

- ① Ad-hoc On-Demand Distance vector (AODV)
- ② Dynamic Source Routing (DSR)
- ③ Temporary ordered routing algo. (TORA)
- ④ Associativity Based routing (ABR)
- ⑤ Signal stability Routing (SSR)

NRA Unit 5

- (*) Cluster - Head Gateway Switch Routing Protocol:
- It uses a hierarchical network topology. Other table driven routing approaches employ flat topologies.
 - Organizes nodes into clusters with coordination among the members of each cluster.
 - Cluster head is employed dynamically by using least Cluster Change (LCC) algorithm.
 - According to LCC, a node ceases to be the cluster head only if it comes in the range of another cluster head.
 - Clustering provides a method to allocate bandwidth.
 - All the member nodes within a cluster can be reached by the cluster head within a single hop. This improves coordination among nodes.
 - CGSR assumes that all communication passes through cluster-head.
 - Communication b/w two clusters take place through the common member nodes.
 - These nodes which are members of more than one cluster are called gateways.
 - Performance of routing is influenced by token scheduling and code scheduling that are handled at cluster heads and gateways respectively.
 - The routing protocol used in CGSR is an extension of TDIV.
 - Every member node contains a routing table containing destination cluster head for every node.
 - Every node maintains a cluster member table. Routing table also keeps the list of next-hop nodes.
 - When a node with packets is to be transmitted to a destination gets token from its cluster head, obtains destination cluster head and next hop node from cluster member table & routing table.
 - Main disadvantages are increase in path length and instability in the system at high mobility.



1, 5, 8 → Node

3, 6 → Gateway

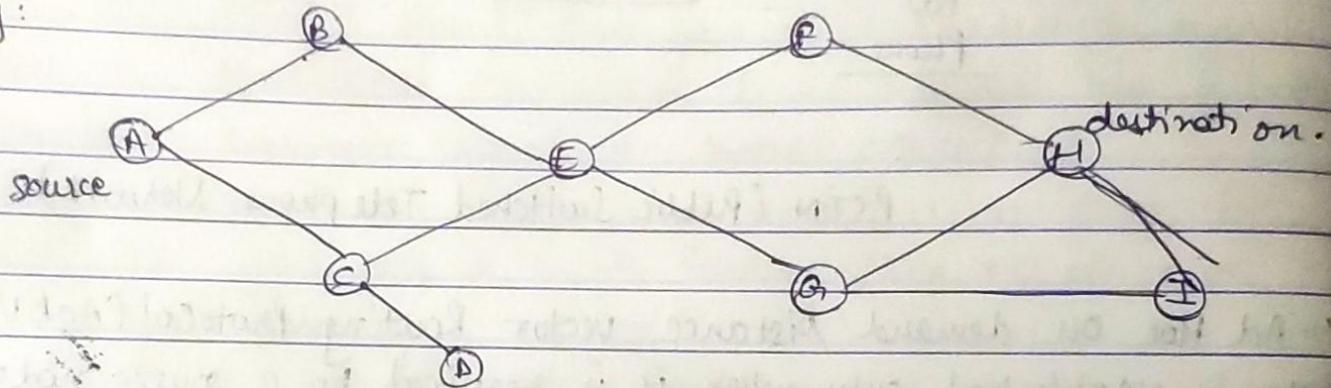
2, 4, 7 → Cluster Head

- (*) Ad Hoc On demand Distance vector Routing Protocol (AODV)
- Route is established only when it is required by a source node for transmitting ~~packets~~ datapackets.
 - It employs destination sequence number to identify most recent path.
 - Source node and intermediate nodes contain the next hop information.
 - Destination Sequence Number is used to determine an up-to-date path to destination.
 - A Route Request carries:
 - Source Identifier, destination identifier, source sequence number, destination sequence number, broadcast identifier and time to live field.
 - When an intermediate node receives a Route request, it either forwards it or prepares a Route Reply if there is a valid route to the destination.
 - If a route request is received multiple times, then the duplicate copies are discarded.
 - AODV does not repair a broken path locally. When a link breaks, the end nodes are notified. The source node re-establishes the route to destination if required.

Operations: → ① Route Discovery ② Route Maintenance
 ↳ RREQ packet ↳ RERR packet
 ↳ RREP packet

- The source node will not carry the complete path.
- Each node knows the previous & the next hop.

Eg:



3 possible routes:

① A → B → E → F → H Hop count = 4

② A → C → E → G → H Hop count = 4

③ A → C → E → G → J → H Hop count = 5 Max Hop count

In this way we can find the route by calculating Hop Count.

Advantages: ① Connection setup delay is less.

② Routes are established on demand.

Disadvantages: ① Intermediate nodes can lead to inconsistent routes.

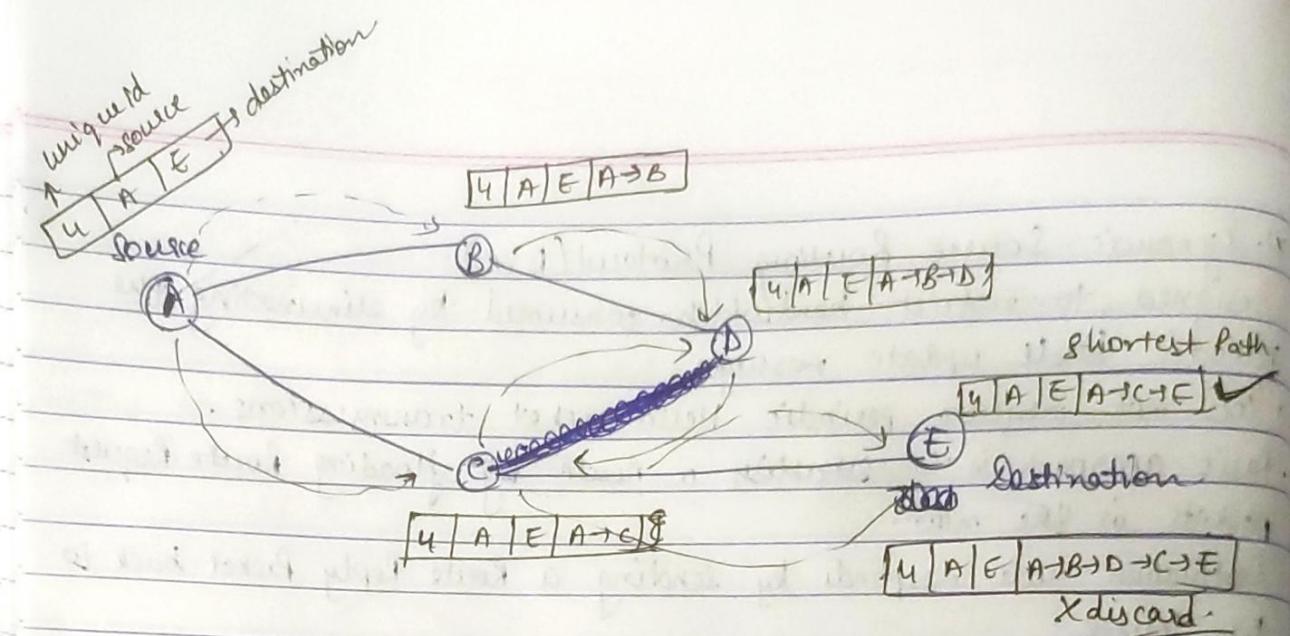
② Multiple Route Reply packets to single Route Request packet can lead to heavy control overhead.

(*) Dynamic Source Routing Protocol (DSR)

- Designed to restrict bandwidth consumed by eliminating the periodic table update messages.
- Does not require periodic Hello packet transmissions.
- basic approach is to establish a route by flooding Route Request packets in the network.
- Destination node responds by sending a Route Reply Packet back to the source.
- Each Route Request carries a sequence no. generated by source node.
- The packet is forwarded only if it is not a duplicate Route Request.
- The sequence number on the packet is used to prevent loop formations and multiple transmissions.
- This protocol uses a route cache that stores all the possible information extracted from the source route.
- for optimization, the intermediate nodes are also allowed to originate Route Reply packets.
- The source node selects the best route from multiple replies and then uses that for sending data packets.
- Each data packet carries complete path to its destination.
- If a link breaks, source node again initiates the route discovery process
- Phases:
 - Route Discovery
 - Route Maintenance
 - ↳ RREQ packet (broadcast)
 - ↳ RREP message

```
graph TD; Source[Source Node ID] -->|RREQ| Destination[Destination Node ID]; Destination -->|RREP| Source
```

↳ RREP packet (unicast)



We find the shortest path that is $A \rightarrow C \rightarrow E$.

Now E will reply to C with complete packet and C will reply to A with complete packet.

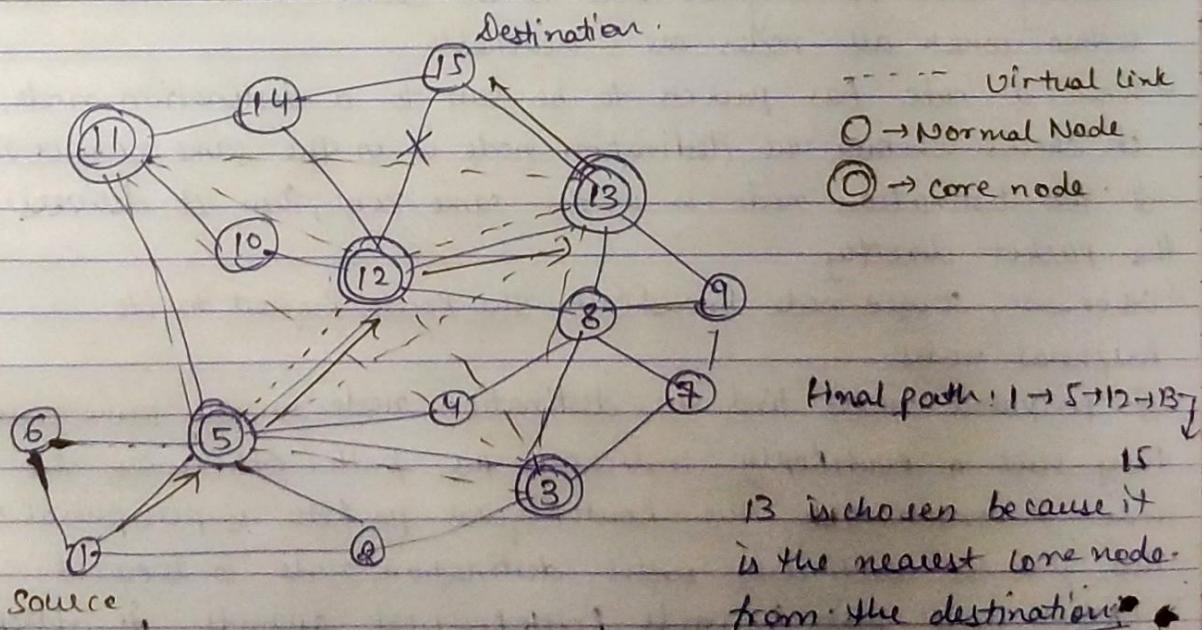
Now A will have complete information about the path.

(*) Hybrid Routing Protocols:

- (*) Core Extraction Distributed Ad Hoc Routing Protocol (CEDAR)
- CEDAR integrates routing and support for ~~self~~ QoS.
- Based on extracting Core Nodes (also called Dominator Nodes) in the Network.
- Core nodes together approximate the minimum dominating set.
- There exists atleast one core node within every three hops.
- The nodes that choose ~~as~~ the core node as their dominating node are called core member nodes ~~of~~ of the core node concerned.
- The path between two core nodes is termed as a virtual link.
- CEDAR employs a distributed Algo. to select core nodes.
- Selection of core nodes represent the core extraction phase.

- CEDAR uses core broadcast mechanism to transmit any packet throughout the network in the unicast ~~mode~~ mode.
- Transmission involves minimum no. of nodes possible.

- Route establishment in CEDAR is done in two phases:
 - first Phase finds a core path from source to destination.
 - In the second phase, the Del feasible path is found over the core path.
- A node initiates a Route Request if the destination is not in the local topology table of its core node. Otherwise the path is established immediately.
- A core node which has destination node as its core member replies to the source core.
- A node after which break occurred → sends the notification of failure.
 - Begins to find a new path from it to destination.
 - Rejects every received packet till it finds the new path to destination.
- Meanwhile, as the source receives the notification message:
 - It stops to transmit.
 - It tries to find a new path to destination.



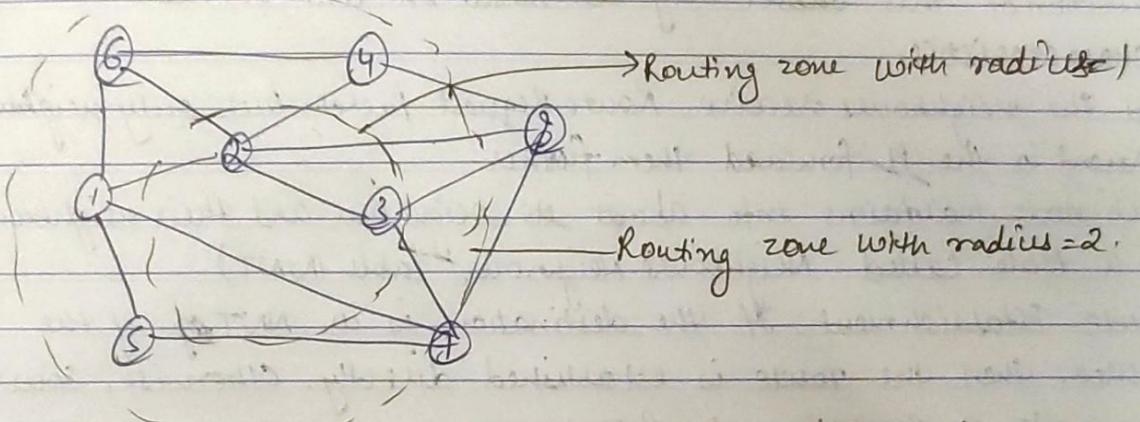
- (*) Advantages:
- (i) Performs both routing & QoS path computation efficiently with the help of core nodes.
 - (ii) Utilization of core nodes reduces traffic overhead.
 - (iii) Reliable mechanism for establishing paths.

- (**) Disadvantages:
- (i) Movement of core nodes adversely affects the performance of protocol.
 - (ii) Core node update information causes control overhead.

(*) Zone Routing Protocol:

- Combines the best features of both Proactive and Reactive routing protocols.
- Uses the proactive scheme within a limited zone in the 1-hop neighbourhood of every node.
- Uses the reactive scheme for nodes beyond this.
- Intra zone ^(IARP) Routing Protocol is used for Proactive scheme.
- Inter zone ^(IERP) Routing Protocol is used for Active scheme.
- Routing zone of a given node is the subset of the n/w within which all nodes are reachable.
- When a node has packets to be sent to a destination node, it checks whether the destination node is in the same zone or not.
- If the destination node is in the same zone, then it delivers the packet directly.
- Otherwise, source node broadcasts the Route Request to its peripheral nodes.
- If peripheral nodes find the destination node in the same zone, they send a RouteReply indicating the path. Otherwise, the node rebroadcasts the RouteRequest packets to peripheral nodes.
- This process continues until destination node is located.
- Every node that forwards RouteRequest appends its address to it.

- This info is used for delivering the Route Reply packet back to the source.
- When an intermediate node detects a broken link, it performs a local path reconfiguration by means of a short alternate path connecting the ends of the broken link.



- Advantage: Reduce control overhead by combining best features of Proactive and Reactive protocols.
- Disadvantage: Control overhead may increase due to the large overlapping of nodes routing zones.

(*) Routing Protocols with efficient flooding mechanisms:

- Many protocols flood the net with Route Request packets in order to obtain a path to the destination.
- Flooding of control packets ~~cannot~~ results in → wastage of bandwidth.
→ Increase in no. of collisions.

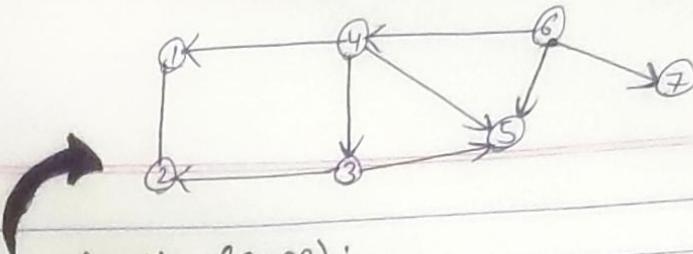
→ Protocols with efficient flooding mechanism:

① Preferred link-based Routing Protocol (PLBR)

② Optimized Link State Routing Protocol (OLSR)

(*) Preferred Link Based Routing Protocol:

- Uses the preferred link approach by processing ~~the~~ a Route Request Packet only if it is achieved through a strong link.
- A Node selects the subset of nodes from its Neighbours List (NL). This subset is ~~Preferred~~ referred to as the Preferred List (PL).
- Selection of this subset may be based on link or node characteristics.
- All the neighbours receive Route Request Packet but only neighbours present in the PL forward them further.
- Each node maintains info about its neighbour and their neighbours in a table called Neighbour Neighbour Table (NNT)
- Route Establishment: If the destination is in NNT ~~of~~ of the source, then the route is established directly. Otherwise, source transmits a Route Request Packet.
- A node is eligible for forwarding Route Request only if:
 - It should be present in PL.
 - RREQ packet must not have been already forwarded by the node and the TTL on the packet must be greater than zero.
- If dest is in the eligible node's NNT, the Route Request is forwarded as a unicast packet to the neighbours.
- If the RREQ packet reaches the destination, then the route selection is done.
- When multiple RREQ packets reach dest, the best path is selected.
- Criteria can be shortest path, or least delay path or most stable path.
- Destination starts a timer after receiving 1st RREQ packet. After a particular time, no RREQ packets are accepted.
- Algorithms for preferred links computation:
 - NDPL (Neighbour-degree - Based preferred link Algorithm)
 - WBPL (Weight Based Preferred link Algorithm).



(*) Optimized Link State Routing (OLSR) :

- Proactive Routing Protocol that employs an efficient link state packet forwarding mechanism called multipoint Relaying (MPR).
 - This protocol optimizes the pure link state Routing Protocol.
 - Optimizations are done in two ways:
 - (a) By reducing size of control packets -
 - (b) By reducing the no. of links that are used to forward the link state packets.
 - The subset of links or neighbours that are designated for link state updates and are assigned the responsibility of packet forwarding are called multipoint Relays.
 - The set consisting of nodes that are multipoint Relays is referred to as MPR set.
 - Each node in the net selects the MPR set that processes and forwards every link state packet that the node originates.
 - The neighbour nodes that do not belong to MPR set process the packets but do not forward them.
 - In order to decide on the membership of the nodes in the MPR set, a node periodically sends Hello messages which contain:
 - (a) list of neighbours with which the node has bidirectional links.
 - (b) list of neighbour whose transmission was received in recent past but with whom bidirectional links have not yet been confirmed.
 - The nodes that receive this Hello packet update their own two-hop topology tables.
 - The Neighbour table is used to store the lists of neighbours, the two hop neighbours, and the status of neighbour nodes.
- Advantages:
- (a) Reduces Routing overhead.
 - (b) Reduces the no. of broadcasts done.
 - (c) Low connection setup time.

Unit 5 - (NRA)

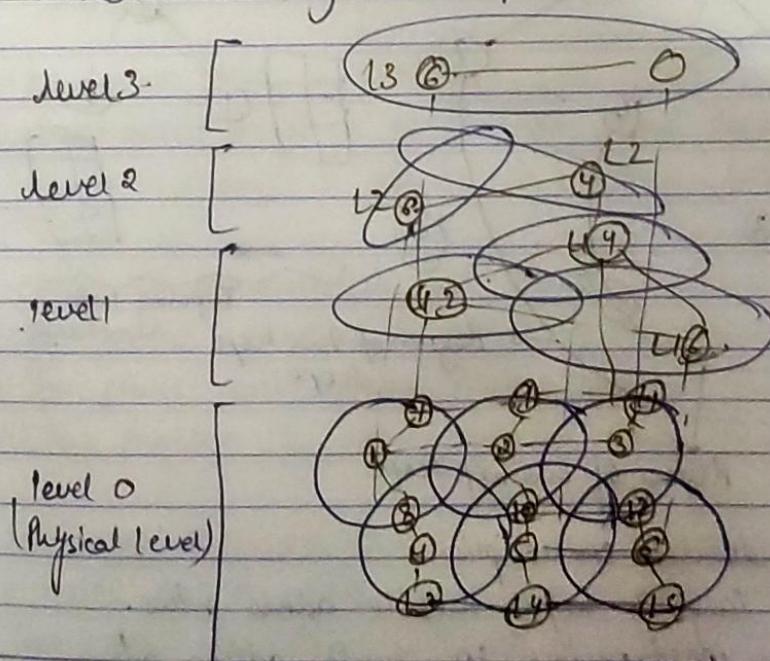
(*) Hierarchical Routing Protocols:

- Advantages in use of routing Hierarchy:
 - (a) Better Scalability
 - (b) Reduction in size of Routing Tables.

(**) Hierarchical State Routing Protocol:

- Distributed multi-level hierarchical routing protocol.
- Employs clustering at different levels.
- Each cluster has its leader.
- Levels of Clustering:
 - (a) Physical : b/w nodes that have physical wireless one-hop link.
 - between them -
 - (b) logical : based on certain relations.

- Cluster Leader is entrusted with responsibilities such as exchange of Routing Info, handling route breaks, etc.
- Nodes marked at a higher level refer to the nodes of lower level.
- Nodes that belong to multiple clusters → Cluster gateway nodes.

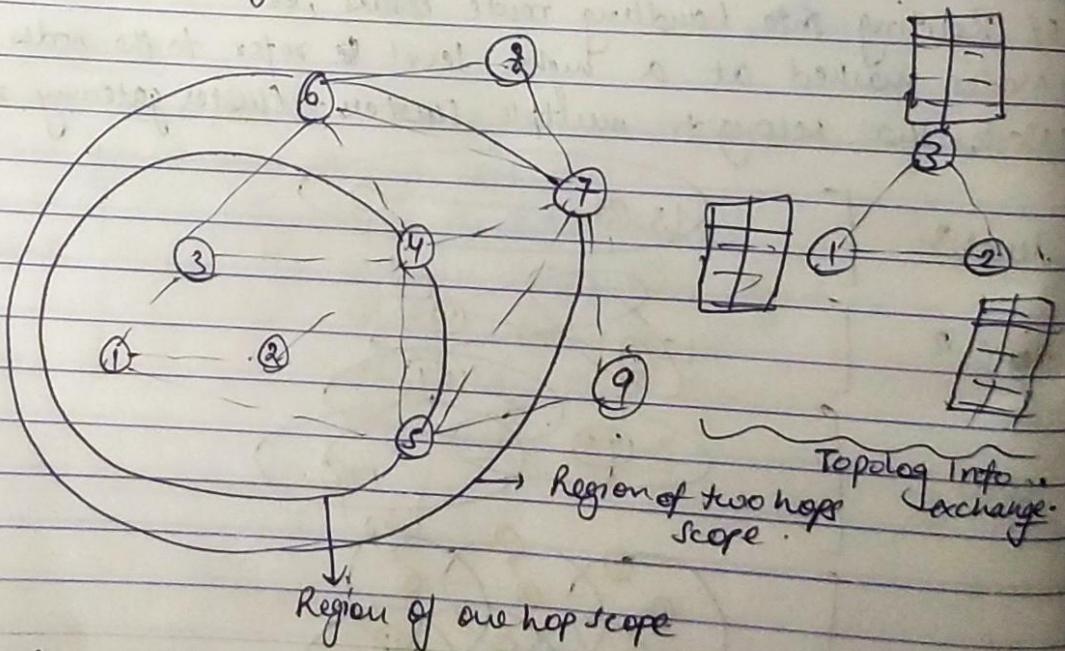


Disadvantage: ① Process of exchanging info. at all levels of hierarchy is difficult.

② Process of ~~choosing~~ selecting leader for all clusters is difficult.

(2) Fish Eye State Routing Protocol (FCSR)

- Uses fish eye technique to reduce overhead.
- Can capture pixel info. with greater accuracy. center of
- This accuracy decreases with increase in distance from focal point.
- Each node maintains accurate info about near nodes.
- Nodes exchange topology info only with their neighbours.
- Link level info exchange of distance vector RPF & complete topology info exchange of link state protocols.
- FCSR defines the set of nodes reachable in specific no. of hops.
- Routing overhead is significantly reduced.



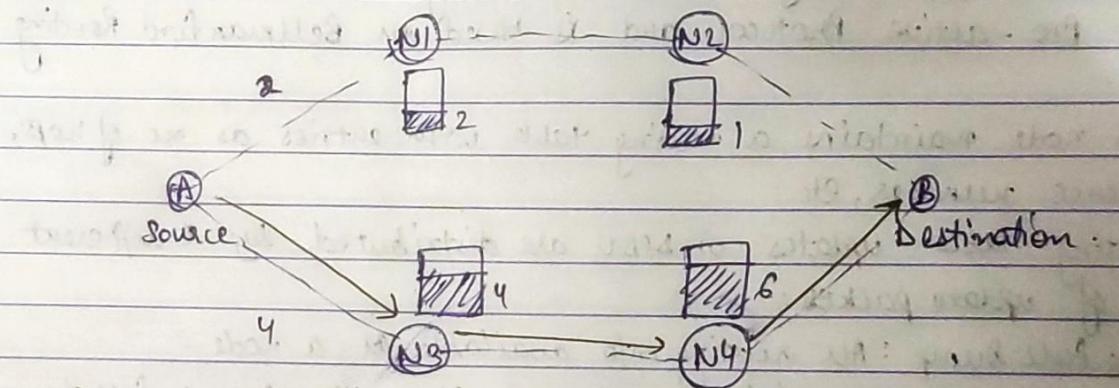
Advantages: ① Reduced bandwidth consumption.

② Suitable for large & highly mobile adhoc netw.

Disadvantage: ① Very poor performance in small adhoc netw.

(*) Power Aware Routing Protocols:

- The battery in the nodes of adhoc NWP is limited.
- Power consumption is a crucial concern here.
- Power Aware Routing is a consideration in a way that it minimizes the energy consumption while Routing the traffic.
- Routers are also power-constrained like nodes. It has limited power supply.
- The path must be selected in a way that power is conserved.
- We must also be aware of the state of battery.
- The energy consumption per packet should be minimum.
- Maximize NWP connectivity.
- Minimum variance in power levels of nodes.
- Minimum cost per packet.
- Minimize maximum node cost.



We would have selected the path $A \rightarrow N1 \rightarrow N2 \rightarrow B$ because of its low cost. But by using Power Aware Routing we will select the path $A \rightarrow N3 \rightarrow N4 \rightarrow B$, because the battery of nodes N3 & N4 is more than the battery of nodes N1 and N2.

(x) Quality of Service Routing for next Generation:

- The upcoming high speed networks are expected to support a wide range of communication intensive real time applications.
- One of the key issues is Quality of Service Routing.
- It selects network routes with sufficient resources.
- The goal is : (a). Satisfying QoS requirements for every connection.
(b). Achieving global efficiency in resource utilization.
- The routing algorithms to achieve QoS Routing can be divided into:
 - (i) Source Routing Algorithms
 - (ii) Distributed Routing Algorithms
 - (iii) Hierarchical Routing Algorithms.
- QoS Routing is expected to direct new traffic in an efficient way that can maximize the total new throughput.
- One common scheme is to always choose short path b/c longer path means using more new resources.

(*) Multiprotocol Label Switching (MPLS)

- MPLS is an IP packet Routing Technique that routes IP packets through paths via labels instead of looking at complex routing tables of routers.
- This feature helps in increasing the delivery rate of IP packets.
- It uses layer 3 service, i.e., Internet Protocol and uses router as a forwarding device.
- The traffic of different customers is separated from each other b/c MPLS works ~~like~~ somewhat like VPN.
- It does not encrypt but makes sure packet from one customer cannot be received by other customer.
- MPLS header is added to packets that lie between layers 2 & 3.
- Hence, it is also called layer 2.5 protocol.

→ MPLS Header: 32 bits long divided into 4 parts:

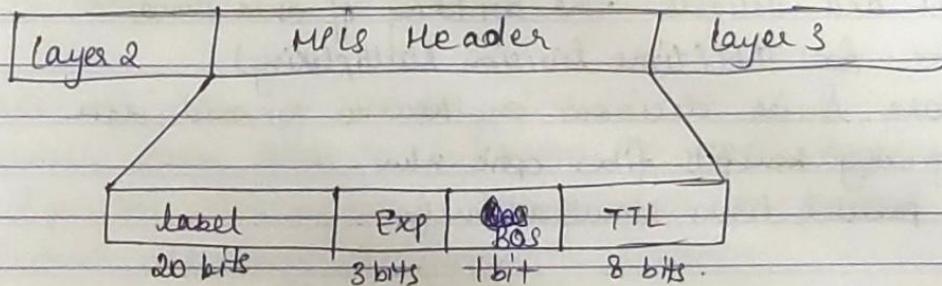
(i) Label : (20 bit)

(ii) Exp : 3 bit (~~for QoS~~) (used for QoS)

(iii) Bottom of Stack (S): 1 Bit.

(iv) Time to live (TTL): 8 bit long. Value is decreased by 1 at every hop.

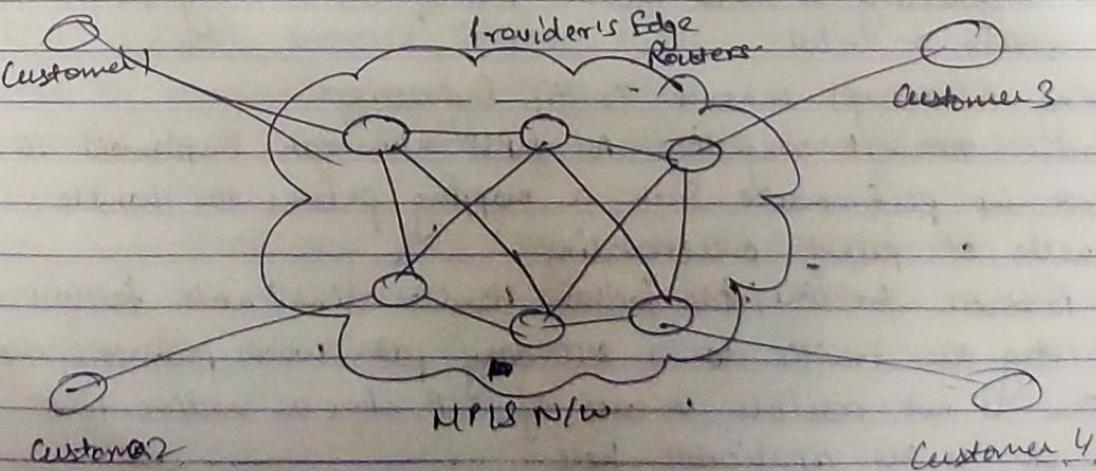
MPLS labels are stacked one over other. If there is only one label remained in MPLS header, then the value is 1 otherwise 0.



→ Label Switch Router (LSR) receives an IP packet and adds MPLS header.

→ MPLS forwarding is based on label attached to IP packet.

→ This label attachment is regulated by a protocol called Label Distribution Protocol (LDP).



- (*) Generalized Multi Protocol Label Switching:
 - Extending MPLS to manage further classes of switching technology other than packet switching.
 - Extends support to multiple types of switching such as TDM, wavelength
 - It is based on Generalized labels.
 - The MPLS label can represent:
 - a single fiber in a bundle.
 - a single wavelength within fiber.
 - a single wavelength within a waveband.
 - a set of time slots within a wavelength.
 - Enables fast and reliable new switching of data flows.
 - Adds support for TDM (Time Division Multiplexing).
 - Helps to make quick decisions on how to forward data.
 - It's use greatly benefits fiber optic networks.
 - It supports parallel links simultaneously.

(*) MPLS Traffic Engineering:

- Traffic Engineering refers to selecting paths in order to balance load on various links, routers, switches, etc.
- Goal of Traffic Engineering is to facilitate efficient IP/ICM operations.
- Traffic Engineering in MPLS involves technique of directing traffic that flows within a network.
- Following Advantages enhance Traffic Engineering:
 - Minimize network congestion: An MPLS network can implement TE to boost up performance. Such a mapping process can handle bottlenecks of packet overcrowding.
 - Fast reroute for link/node failure: Handles link/node failures by directing the traffic to a secondary path when primary one fails. This is not possible in case of IP networks as redirecting mechanism is not applicable here.

(iii) Deployment flexibility: A TE system is efficient even when MPLS n/w is under-developed. It is flexible during situations when the overflowing packets from links are transferred to available links.

(iv) Class of service: 3 bit field. Based on this field, the traffic in its priority queue is used for transmission.

(v) Customer traffic identification: MPLS TE classifies the customer traffic based on the service provider used in MPLS N/W.

→ Limitations of MPLS Traffic Engineering:

(i) Over-utilization of secondary links.

(ii) Manual path setup: To implement TE, paths require manual configuration. This manual setting needs professional solution providers.

(iii) Protocol dependency for automatic rerouting:

(iv) Performance variation in MPLS fast reroute.

(v) Configuring intermediate nodes in MPLS is manually not achievable.

(vi) Lack of systematic mapping system: The dynamic mapping of IP traffic on MPLS TE paths is not achievable.

★ PSTN (Public Switched Telephone N/W):

→ Works by using underground copper wires.

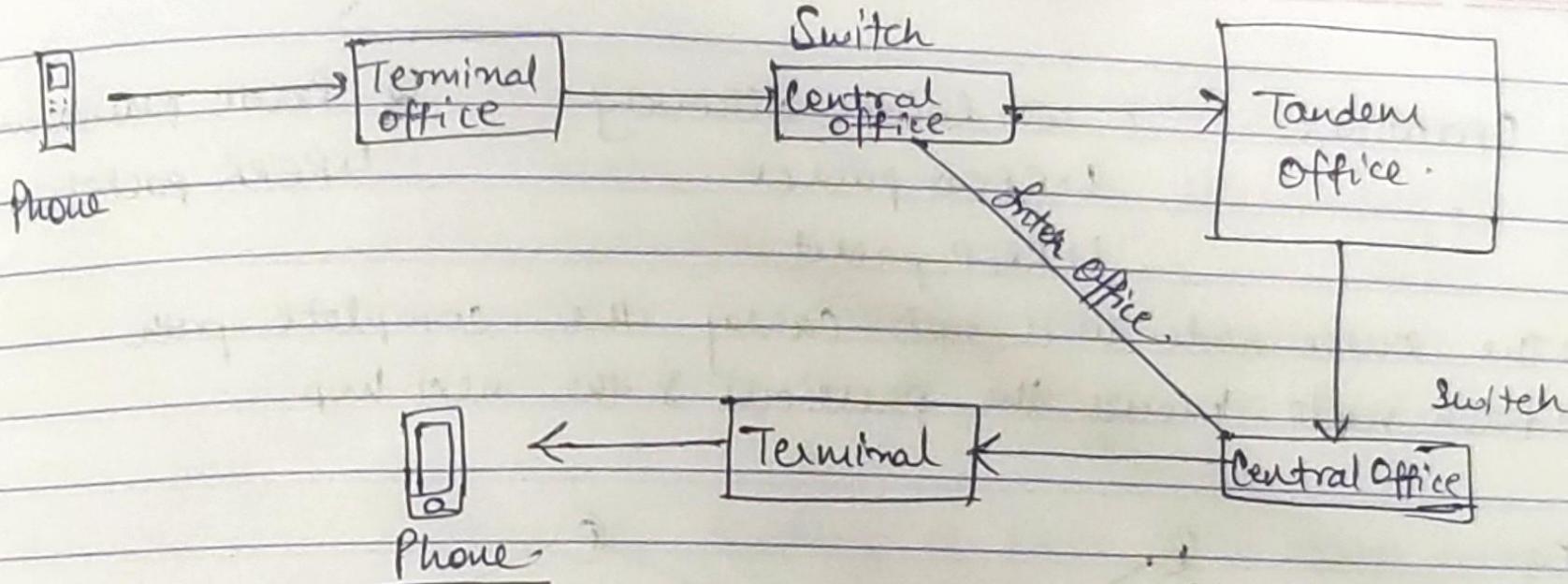
→ It carries voice signals from your telephone through the n/w to the recipient's phone.

→ Costly and challenging. VoIP (Voice over IP) overcomes this.

→ VoIP sends and receives voice communication over the Internet rather than through old school PSTN.

(*) Working of PSTN:

- ① You dial a number to indicate how you would like the call to be routed. The first 3 digits of the number is the area code, the next 3 are the exchange and last 4 represent recipient's unique ~~also~~ phone id.
- ② Telephone converts sound from your voice to electrical signals that are ~~telephonated~~ transmitted to the terminal via a cable.
- ③ Terminal transmit signal to Central office (CO)
- ④ Depending on where you are and where ^{the} call is going, CO will route your call to a CO, tandem office, toll office or International gateway.
 - ⑤ CO → If you are in the same neighbourhood as your recipient.
 - ⑥ Tandem Office: If you are in another part of town in the same city as that of recipient.
The call will go to local CO → tandem office → local CO of recipient → recipient.
 - ⑦ Toll office: If you're in another city from your recipient.
Tandem office connects to toll office.
 - ⑧ International Gateway: If you're in a different country from your recipient.
- ⑨ Once the call has been routed to the right destination, the electrical signals are routed to the terminal & sent to the right number.
- ⑩ Phone rings, when the recipient picks up, the electrical signals are transformed back into sound waves.



PSTN (Public Switched Telephone Network).