Module 5
Mobile Network Layer

Contents:

- Mobile IP
- Dynamic Host Configuration Protocol
- Mobile Ad-hoc Routing Protocols

1. Mobile IP

- Mobile IP is an emerging set of protocols created by Internet engineering Task Force (IETF).
- It is a modification to IP that allows nodes to continue to receive packets independently of their connection point to the Internet.
- It allows transparent routing of IP datagram on the Internet.

- Mobile IP was developed as a means for transparently dealing with problems of mobile users.
  - Enables hosts to stay connected to the Internet regardless of their location.
  - Enables hosts to be tracked without needing to change their IP address.
  - Requires no changes to software of non-mobile hosts/routers.
  - Requires addition of some infrastructure.
  - Has no geographical limitations.
  - Requires no modifications to IP addresses or IP address format.
  - Supports security
    - Could be even more important than physically connected routing.

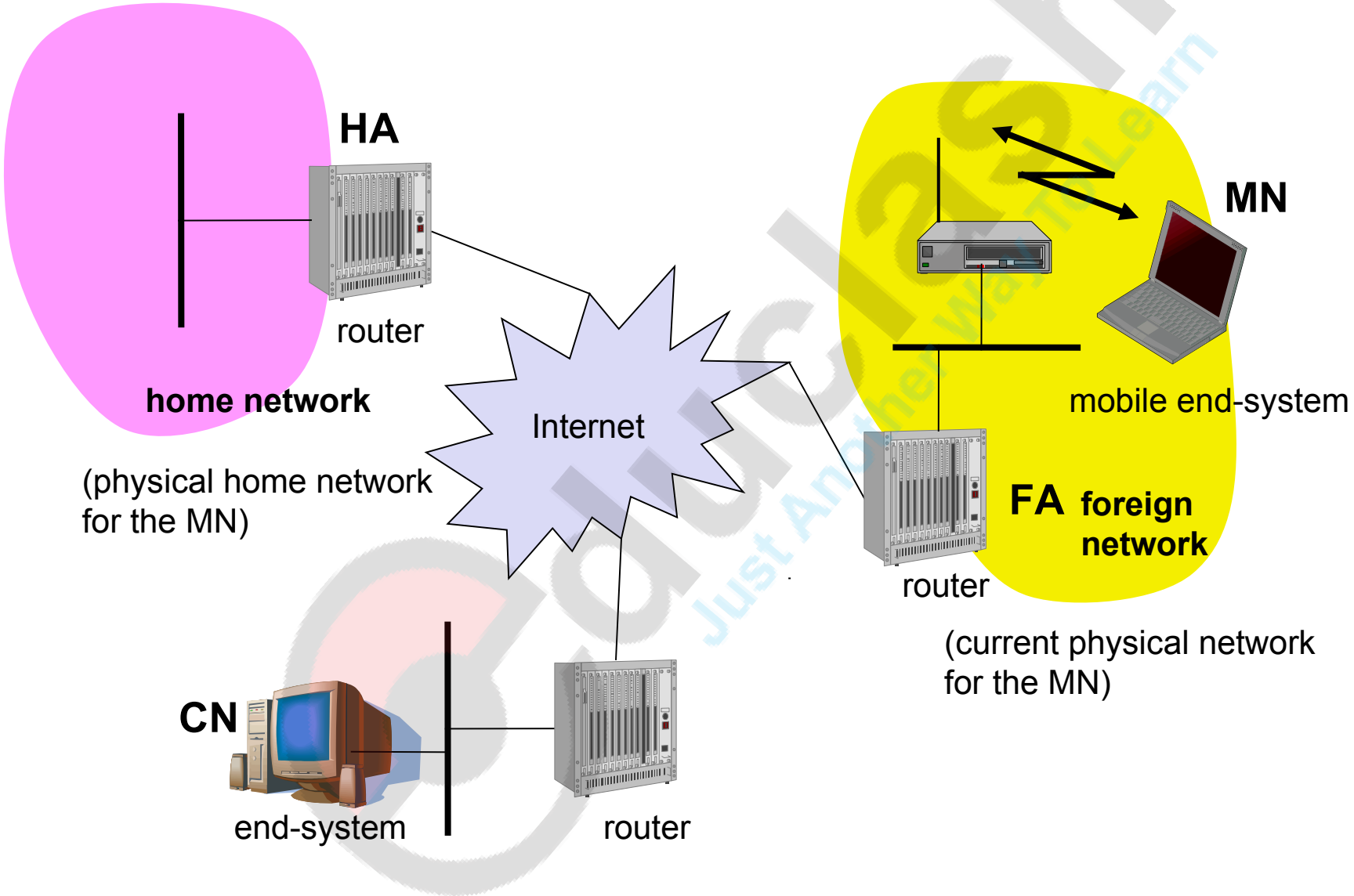
Limitations of traditional IP

- The IP has limitation due to its proper characteristics
  - To send a packet on the Internet, a computer must have an IP address.
  - This IP address is associated with the computer's physical location.
  - TCP/IP protocol routes packets to their destination according to the IP address.
  - Hence once a computer changes its IP address, it can no longer receive any packets.

Mobile IP goals

- Give mobile users the full internet experience.
- Work indoors and outdoors to both stationary and mobile users.
- It should be simple to implement mobile node software.

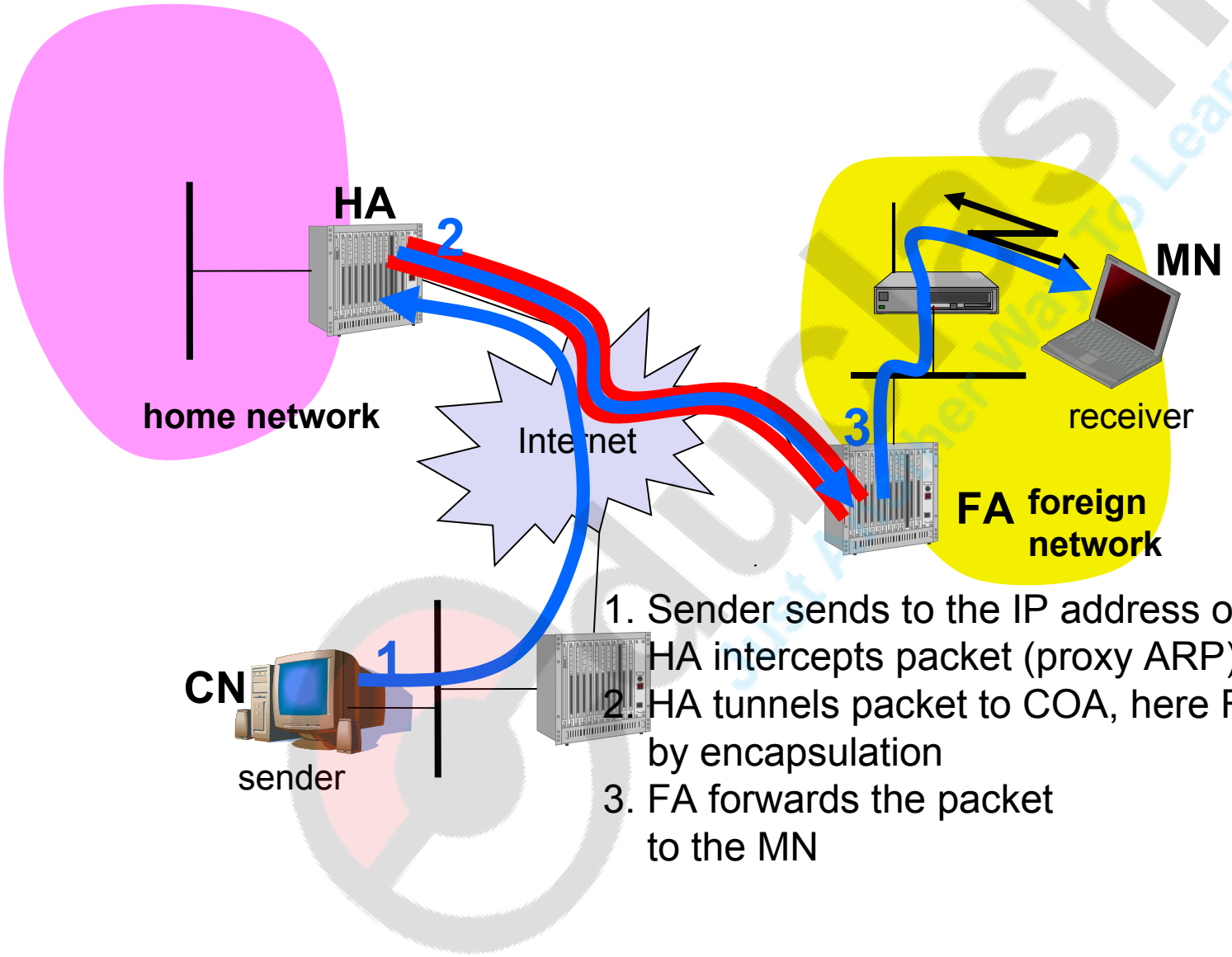
Example network



Terminology

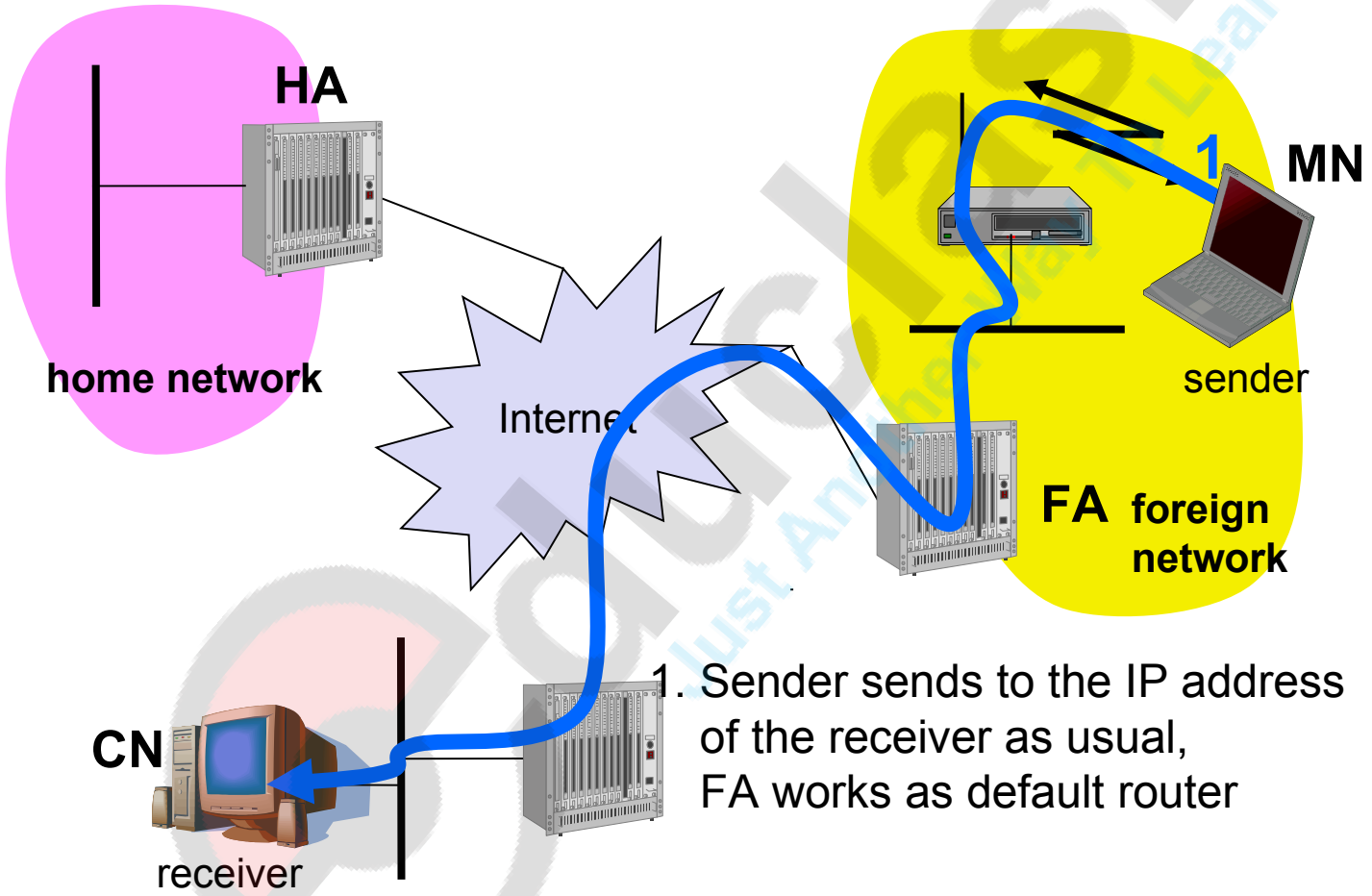
- **Mobile Node (MN)**
  - system (node) that can change the point of connection to the network without changing its IP address.
- **Home Agent (HA)**
  - system in the home network of the MN, typically a router.
  - registers the location of the MN, tunnels IP datagrams to the COA.
- **Foreign Agent (FA)**
  - system in the current foreign network of the MN, typically a router.
  - forwards the tunneled datagrams to the MN, typically also the default router for the MN.
- **Care-of Address (COA)**
  - address of the current tunnel end-point for the MN (at FA or MN)
  - actual location of the MN from an IP point of view
  - can be chosen, e.g., via DHCP
- **Correspondent Node (CN)**
  - communication partner- can be fixed or mobile node.

Data transfer to the mobile system



1. Sender sends to the IP address of MN, HA intercepts packet (proxy ARP)
2. HA tunnels packet to COA, here FA, by encapsulation
3. FA forwards the packet to the MN

Data transfer from the mobile system



- **Mobile Node (MN)**
  - The entity that may change its point of attachment from network to network in the Internet
    - Detects it has moved and registers with "best" FA
  - Assigned a permanent IP called its ***home address*** to which other hosts send packets regardless of MN's location
    - Since this IP doesn't change it can be used by long-lived applications as MN's location changes

- **Home Agent (HA)**
  - This is router with additional functionality
  - Located on home network of MN
  - Does mobility binding of MN's IP with its COA
  - Forwards packets to appropriate network when MN is away
    - Does this through encapsulation

- **Foreign Agent (FA)**
  - Another router with enhanced functionality
  - If MN is away from HA then it uses a FA to send/receive data to/from HA
  - Advertises itself periodically
  - Forward's MN's registration request
  - Decapsulates messages for delivery to MN

- **Care-of-address (COA)**
  - Address which identifies MN's current location
  - Sent by FA to HA when MN attaches
  - Usually the IP address of the FA

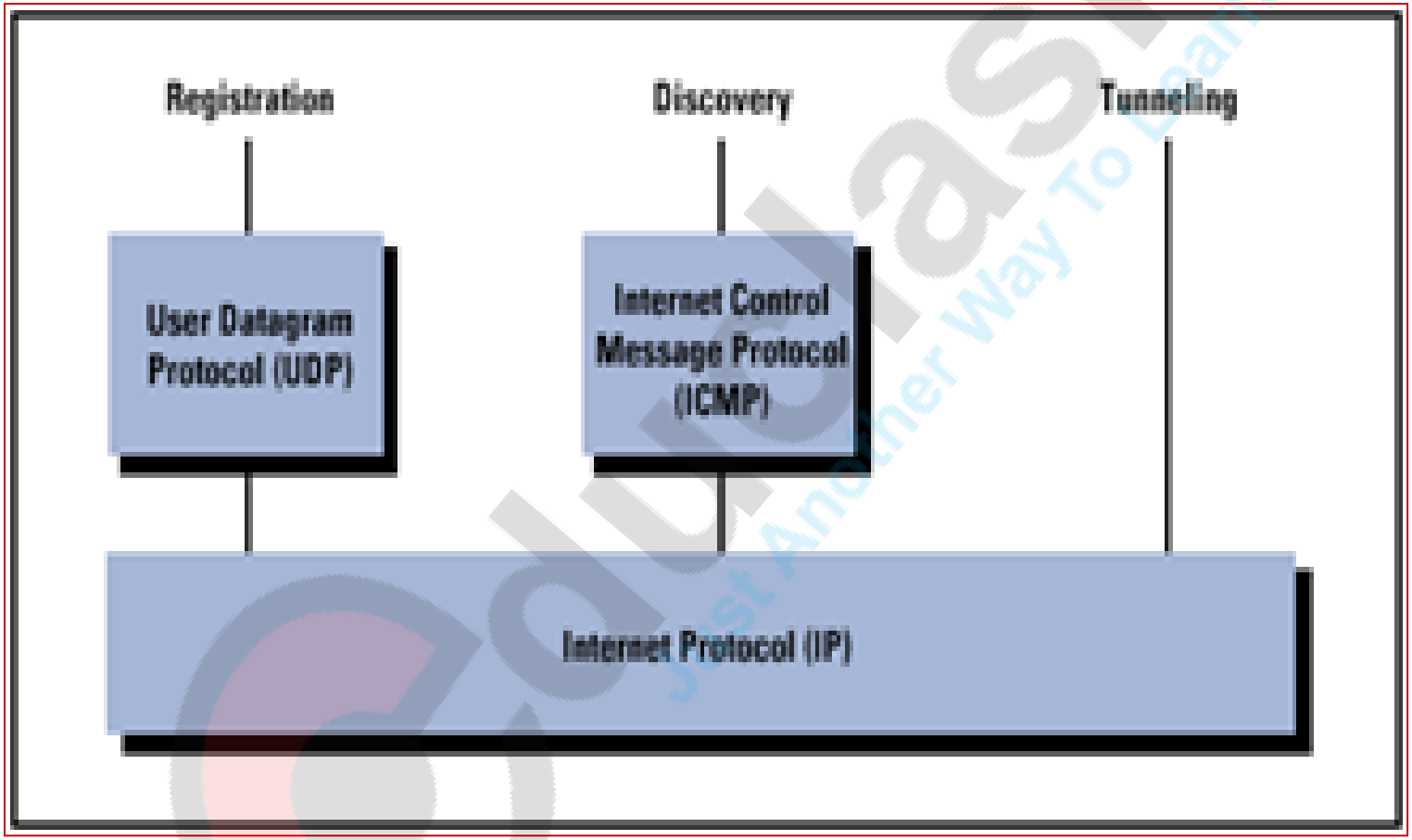
- **Correspondent Node (CN)**
  - End host to which MN is corresponding (e. g. a web server)

Mobile IP Support Services

- **Discovery** – mobile node (A) uses a discovery procedure to identify prospective home and foreign agents
  - HA's and FA's broadcast their presence on each network to which they are attached
    - Broadcast messages via ICMP Router Discovery Protocol (IRDP)
  - MN's listen for advertisement and then initiate registration

- **Registration** – mobile node uses an authenticated registration procedure to inform its home agent of its care-of address
  - When MN is away, it registers its COA with its HA
    - Typically through the FA with strongest signal
  - Registration control messages are sent via UDP to well known port

- **Tunneling** – used to forward IP datagrams from a home address to a care-of address ; using encapsulation
  - Encapsulation – just like standard IP only with COA
  - Decapsulation – again, just like standard IP


Registration
Discovery
Tunneling
User Datagram Protocol (UDP)
Internet Control Message Protocol (ICMP)
Internet Protocol (IP)

Mobile IP Support Services: Agent Discovery

- Mobile node is responsible for ongoing discovery process
  - Must determine if it is attached to its home network or a foreign network

- Transition from home network to foreign network can occur at any time without notification to the network layer (therefore must be continuous)

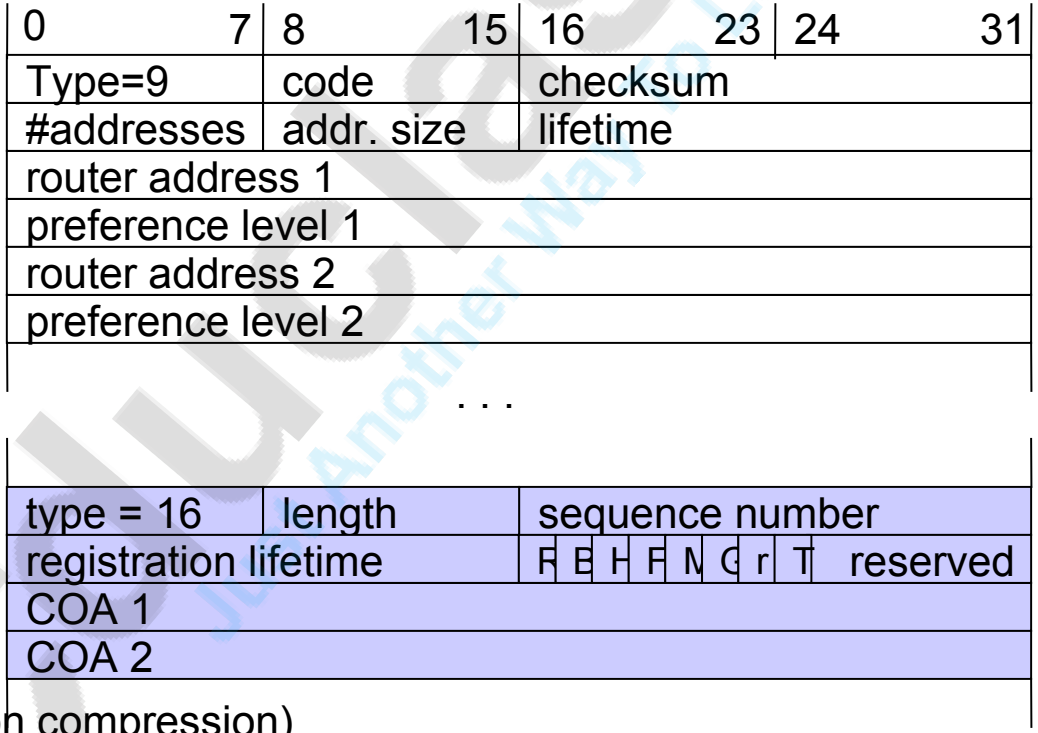
- Mobile node listens for agent advertisement messages
  - Compares network portion of the router's IP address with the network portion of home address

- 2 methods:
  - Agent advertisement
  - Agent solicitation

Agent Advertisement

- The functions performed by an agent advertisement are as follows
  - Allows the detection of HA and FA
  - List one COA
  - Informs the MN about special features provided by FA, say for example a list of alternative encapsulation techniques supported
  - Permits MN to determine the network number and congestion status of their link to the internet
  - Lets the MN know, whether it is its home network or in a foreign network by identifying whether the agent is HA, FA or both.

Agent advertisement packet



type = 16
length = 6 + 4 * #COAs
R: registration required
B: busy, no more registrations
H: home agent
F: foreign agent
M: minimal encapsulation
G: GRE encapsulation
r: =0, ignored (former Van Jacobson compression)
T: FA supports reverse tunneling
reserved: =0, ignored

Agent Solicitation

- If a mobile node does not receive an agent advertisement within a specified duration, it can send an Agent Solicitation to request the sending of an advertisement.
- Any agent that receives the solicitation message then transmits a single agent advertisement in response.
- MN sends three solicitation message in one second.
- If it does not receive a reply soon, it should reduce the sending rate to avoid flooding in network.

Move Detection

- Mobile node may move from one network to another due to some handoff mechanism without IP level being aware.
  - Agent discovery process is intended to enable the agent to detect such a move.
  - Two Algorithms used for this purpose:
    - **Use of lifetime field** – mobile node uses lifetime field as a timer for agent advertisements.
    - **Use of network prefix** – mobile node checks if any newly received agent advertisement messages are on the same network as the node's current care-of address.

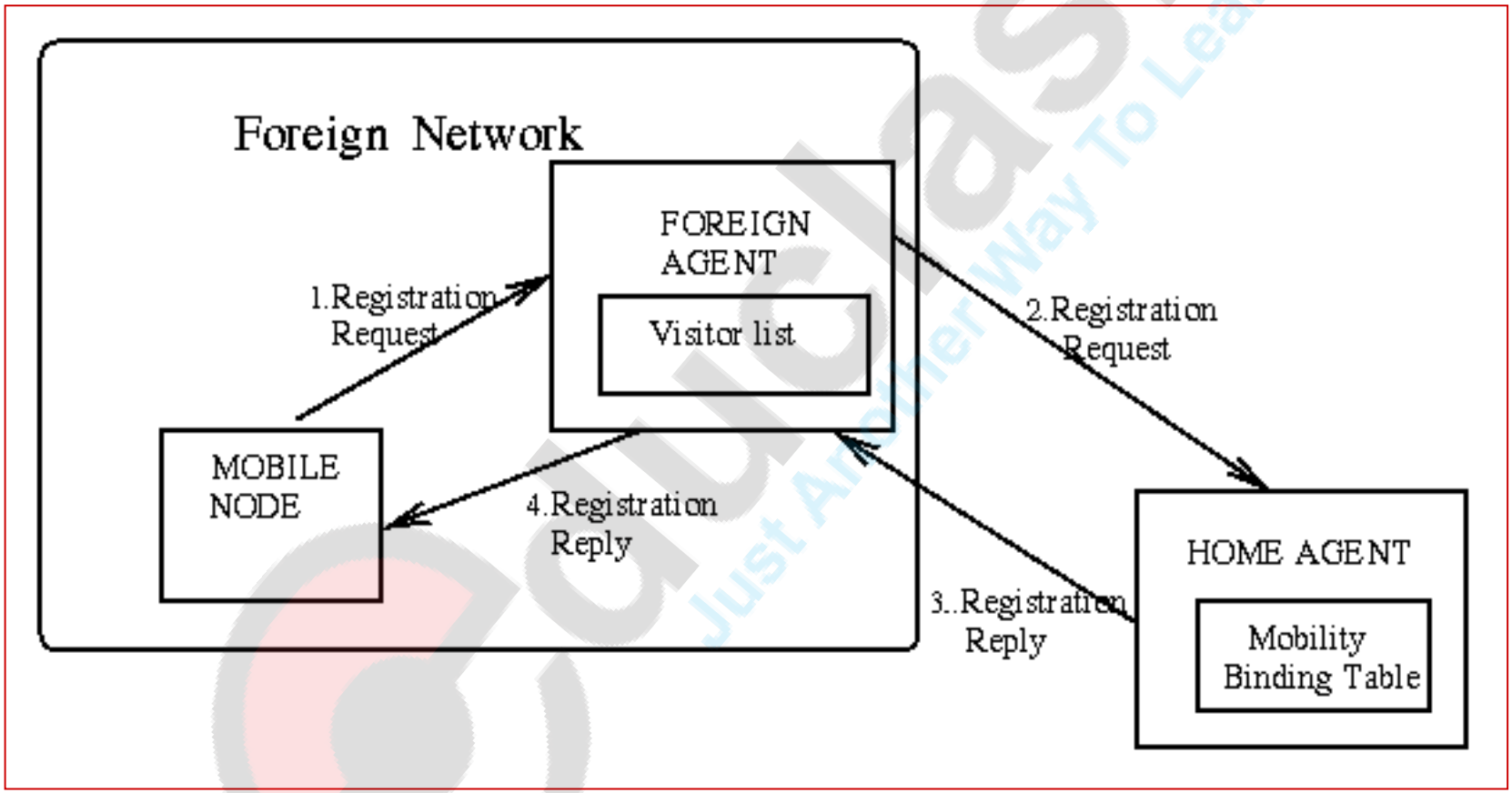
Co-Located Addresses

- If mobile node moves to a network that has no foreign agents, or all foreign agents are busy, it can act as its own foreign agent.
- Mobile agent uses co-located care-of address
  - IP address obtained by mobile node associated with mobile node's current network interface.
- Means to acquire co-located address:
  - Temporary IP address through an Internet service, such as DHCP.
  - Another alternative is, address may be owned by the mobile node as a long-term address for use while visiting a given foreign network.

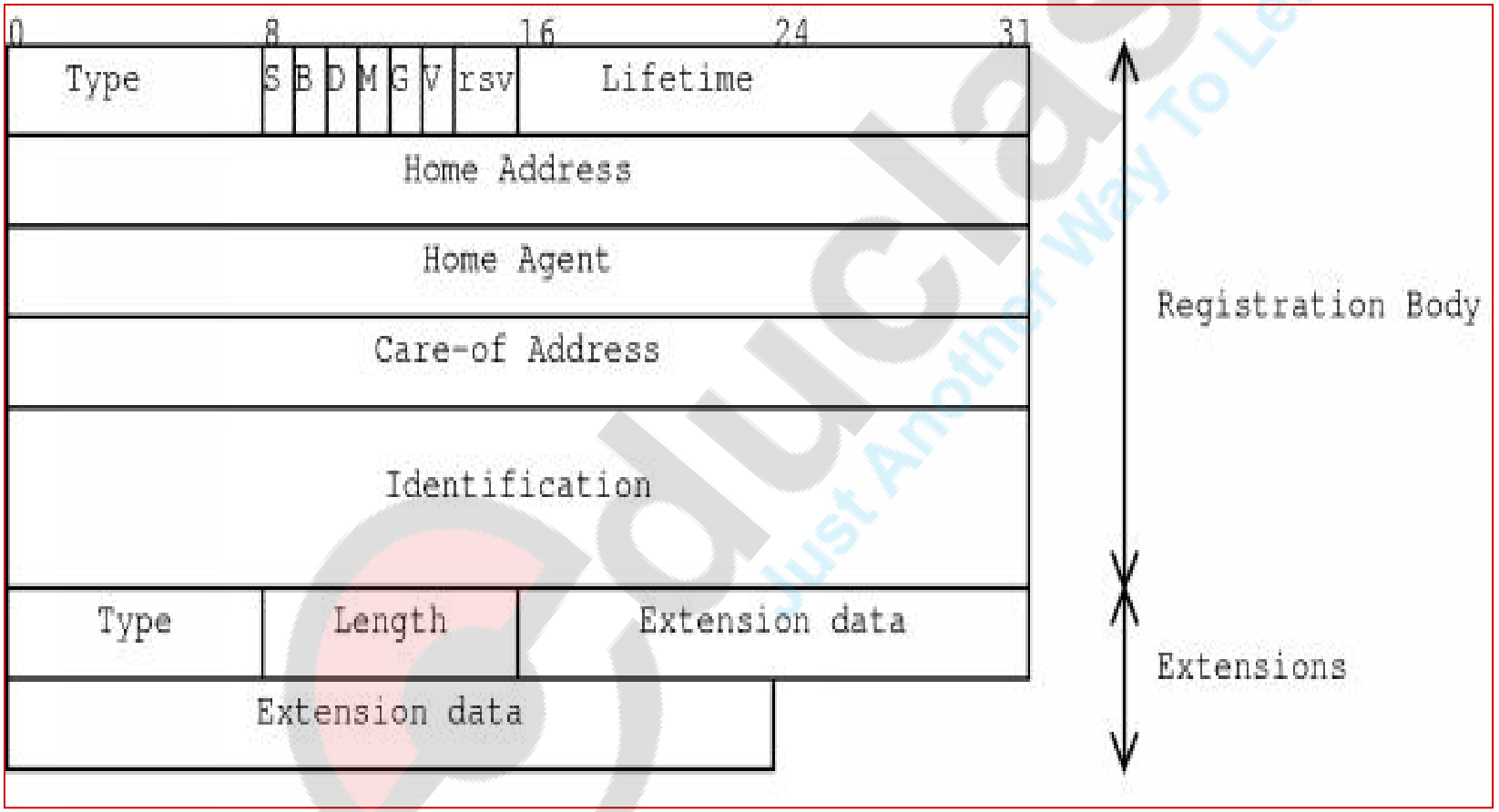
Mobile IP Support Services: Registration Process

- Mobile node (A) sends registration request to foreign agent requesting forwarding service.
- Foreign agent relays request to home agent.
- Home agent accepts or denies request and sends registration reply to foreign agent.
- Foreign agent relays reply to mobile node.

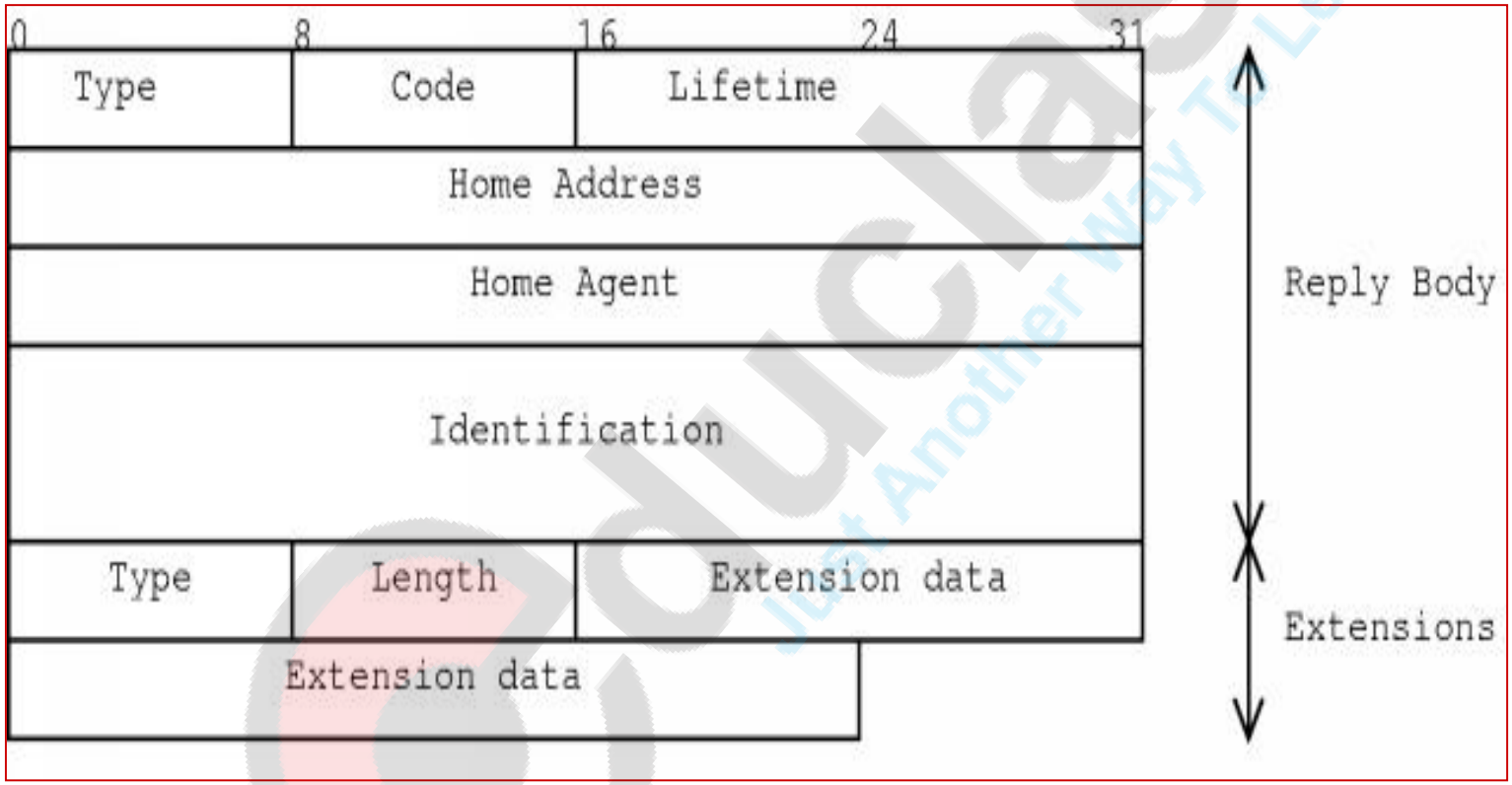
Registration Process



Mobile IP registration request



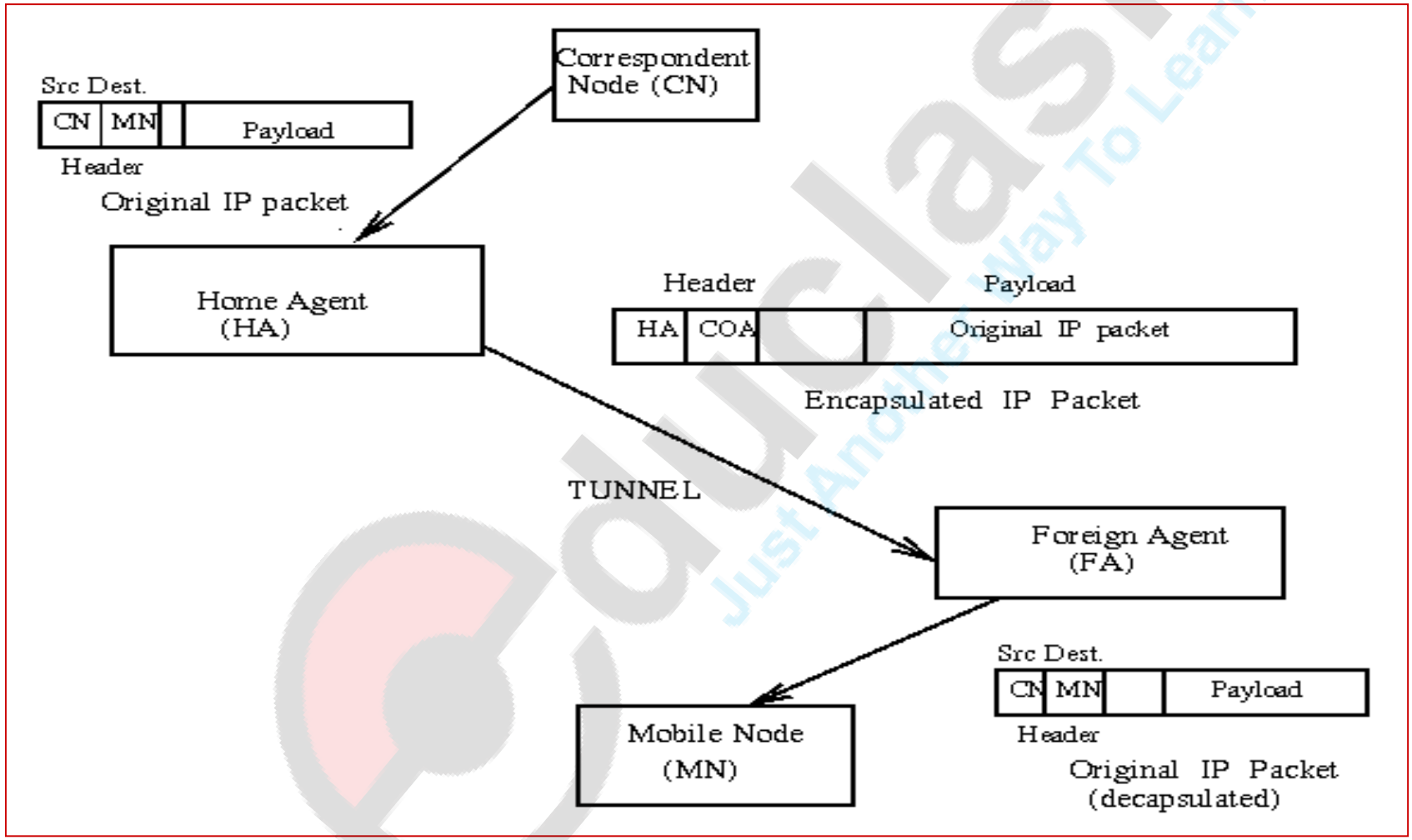
Registration reply message



Mobile IP Support Services: Tunneling and Encapsulation

- If MN moves out of HN the HA sends the packets destined for MN via tunnel to the COA of the MN.
- A tunnel establishes virtual pipe for data packets.
- End point of tunnels are called as encapsulator.
- The flow of packet is Source (CN) → Encapsulator (HA) → Decapsulator (FA) → destination (MN).
- It is the mechanism of taking a packet that has a header part and data part and putting it in the data part of new packet.
- Decapsulation is reverse process.

Mobile IP Tunneling



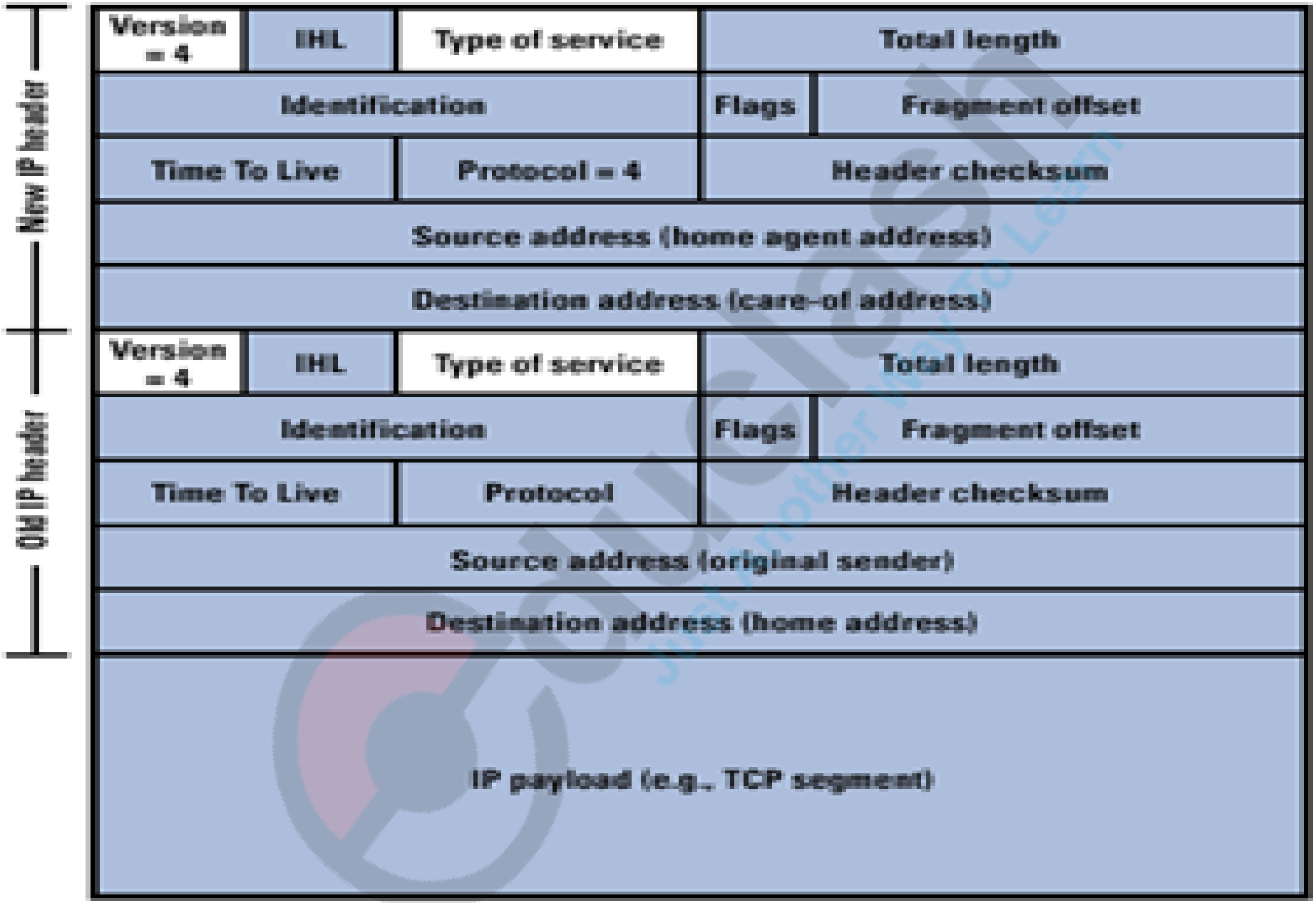
Mobile IP Encapsulation Options

- **IP-within-IP** – entire IP datagram becomes payload in new IP datagram
  - Original, inner IP header
  - Outer header is a full IP header

- **Minimal encapsulation** – new header is inserted between original IP header and original IP payload
  - Original IP header modified to form new outer IP header

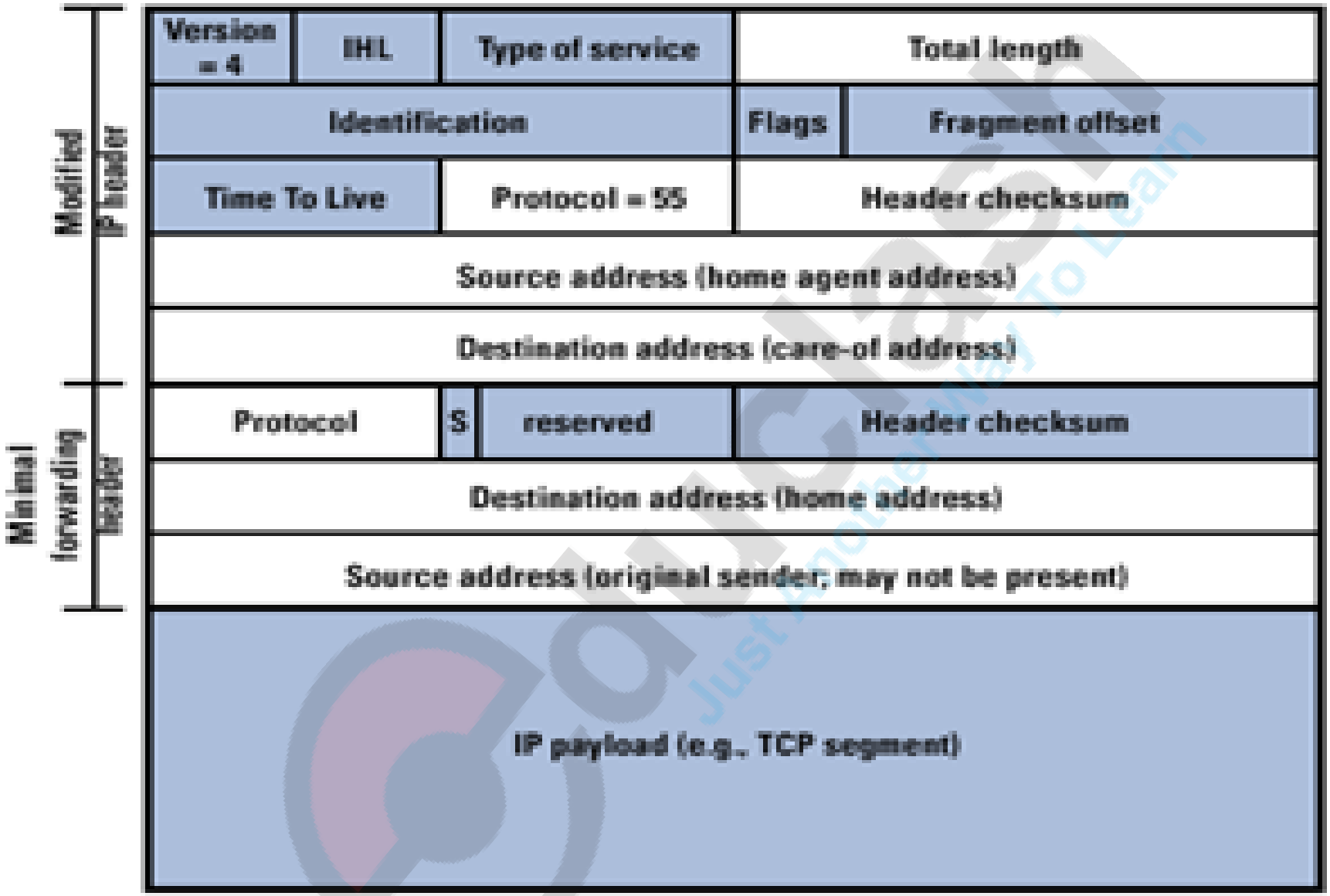
- **Generic routing encapsulation (GRE)** – developed prior to development of Mobile IP

(a) IP-within-IP encapsulation



Unshaded fields are copied from the inner IP header to the outer IP header.

(b) Minimal encapsulation



Unshaded fields in the inner IP header are copied from the original IP header.
Unshaded fields in the outer IP header are modified from the original IP header.

Problems with mobile IP

- **Security**
  - authentication with FA problematic, for the FA typically belongs to another organization.
  - no protocol for key management and key distribution has been standardized in the Internet.
- **Firewalls**
  - typically mobile IP cannot be used together with firewalls, special set-ups are needed.
- **QoS**
  - tunneling makes it hard to give a flow of packets a special treatment needed for the QoS.

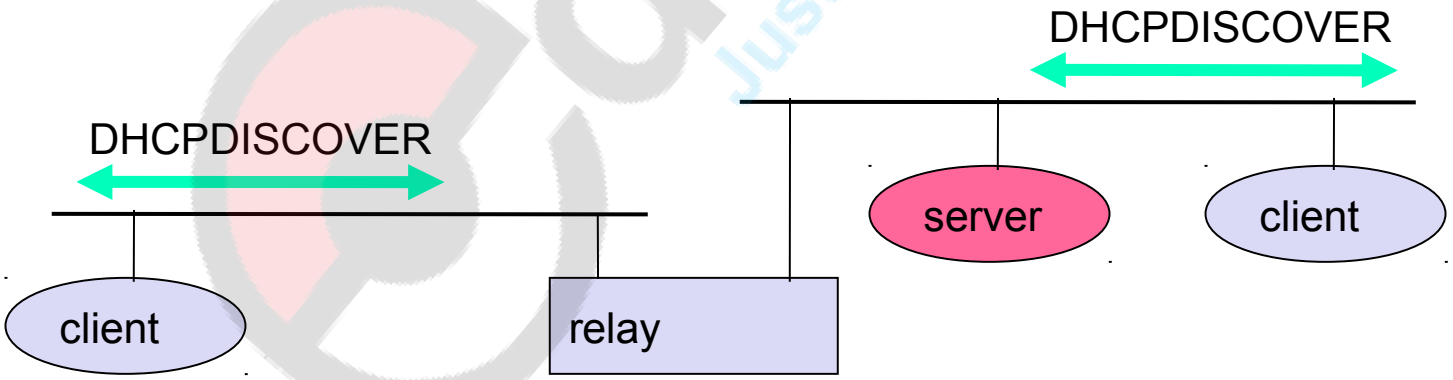
2. DYNAMIC HOST CONFIGURATION PROTOCOL

DHCP: Dynamic Host Configuration Protocol

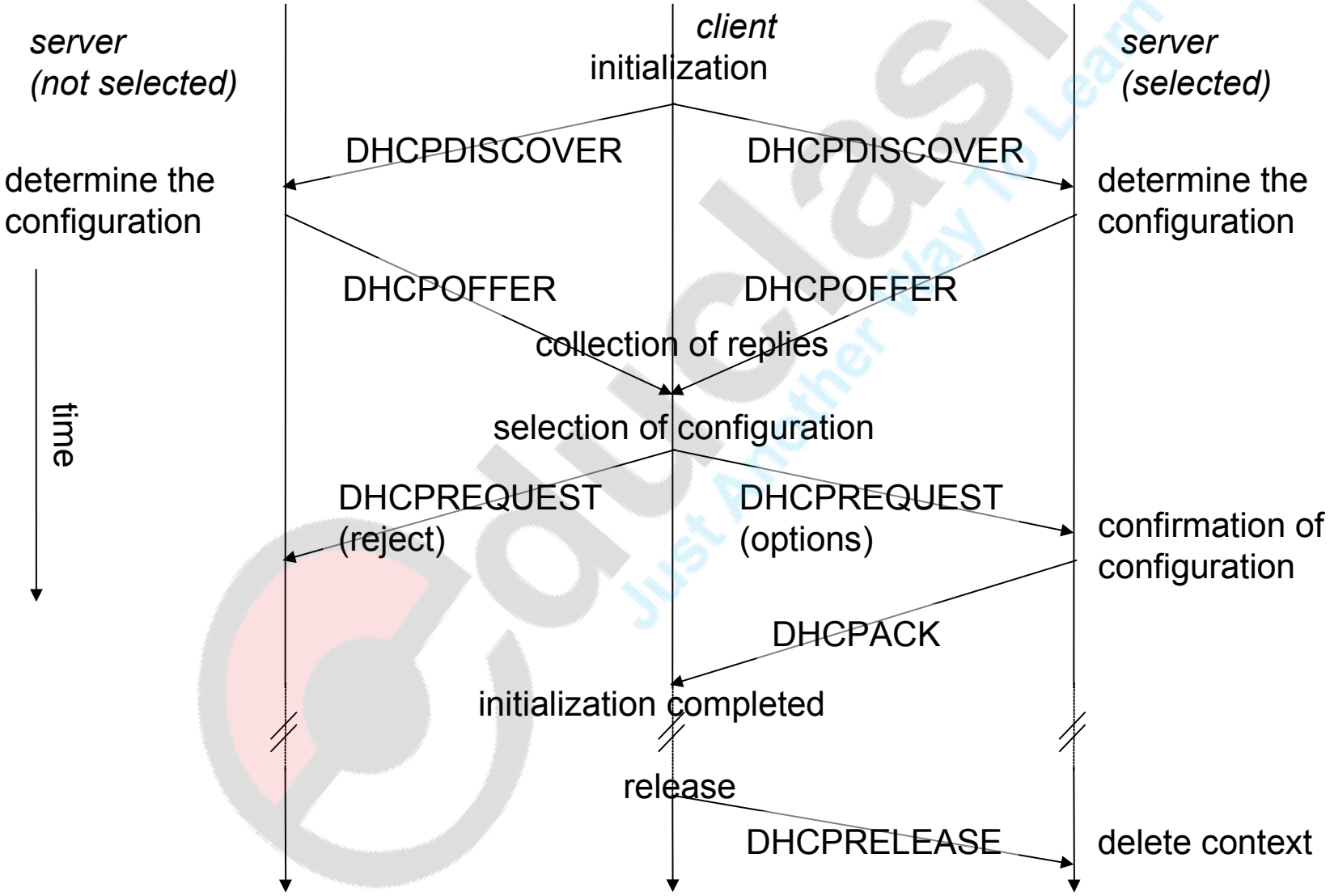
- DHCP is protocol used by network device to obtain various parameters necessary to operate In an IP network
- When DHCP configured client connects to a network, it sends a broadcast query requesting necessary information from DHCP server
- Upon receipt of a valid request, the server will assign the computer,
  - A valid IP address
  - A domain name
  - A subnet mask
  - A default gateway
  - Address of DNS server and router
- Using DHCP, client in mobile IP can easily acquire a new COA.

Basic DHCP Configuration

- **Client/Server-Model**
  - the client sends request using MAC broadcast to reach all the devices in LAN.
  - If needed a DHCP relay can be used to forward the request.



DHCP - protocol mechanisms: Client initiation via DHCP



- The client broadcasts a DHCPDISCOVER into the subnet. There might be a relay to forward this broadcast.
- In the case shown, two servers receive this broadcast and determine the configuration they can offer to the client.
- Servers reply to the client's request with DHCPOFFER and offer a list of configuration parameters.
- The client can now choose one of the configurations offered.
- The client in turn replies to the servers, accepting one of the configurations and rejecting the others using DHCPREQUEST.
- If a server receives a DHCPREQUEST with a rejection, it can free the reserved configuration for other possible clients.

- The server with the configuration accepted by the client now confirms the configuration with DHCPACK.
- This completes the initialization phase.
- If a client leaves a subnet, it should release the configuration received by the server using DHCPRELEASE.
- Now the server can free the context stored for the client and offer the configuration again.
- The configuration a client gets from a server is only leased for a certain amount of time, it has to be reconfirmed from time to time.
- Otherwise the server will free the configuration.

DHCP characteristics

- **Server**
  - several servers can be configured for DHCP, coordination not yet standardized (i.e., manual configuration).
- **Renewal of configurations**
  - IP addresses have to be requested periodically, simplified protocol.
- **Options**
  - available for routers, subnet mask, NTP (network time protocol) timeserver, SLP (service location protocol) directory, DNS (domain name system).

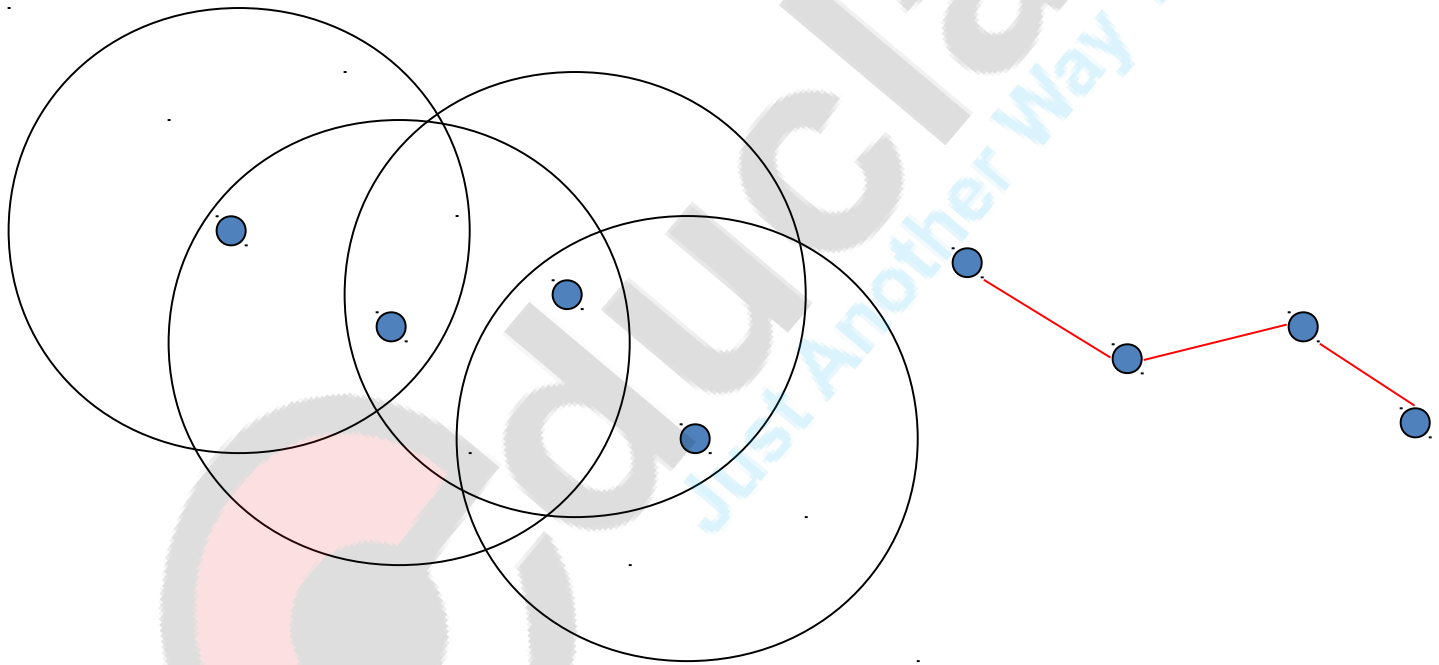
3. MOBILE AD-HOC NETWORKS

Cellular Wireless Network

- Single hop wireless connectivity to the wired world
  - Space divided into cells.
  - A base station is responsible to communicate with hosts in its cell.
  - Mobile hosts can change cells while communicating.
  - Hand-off occurs when a mobile host starts communicating via a new base station.

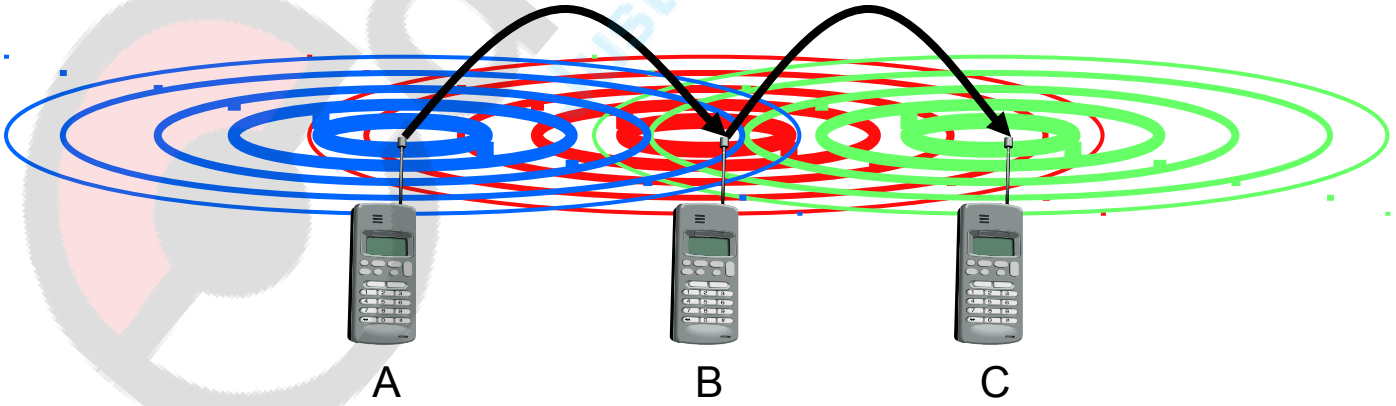
Multi-Hop Wireless

- May need to traverse multiple links to reach destination.
- Mobility causes route changes.



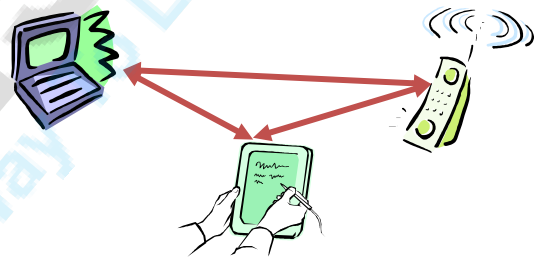
Need of Mobile ad-hoc networks

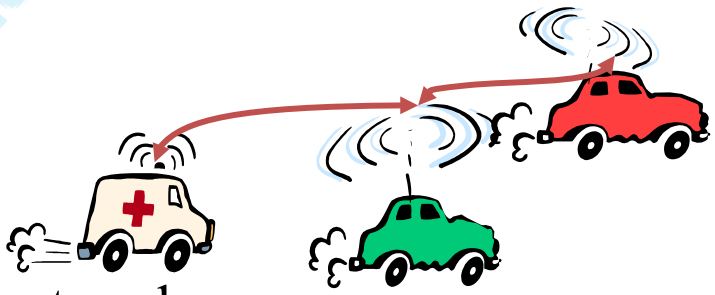
- Standard Mobile IP needs an infrastructure
  - Home Agent/Foreign Agent in the fixed network
  - DNS, routing etc. are not designed for mobility
- Sometimes there is no infrastructure!
  - remote areas, ad-hoc meetings, disaster areas
  - cost can also be an argument against an infrastructure!
- Main topic: routing
  - no default router available
  - every node should be able to forward



Solution: Wireless ad-hoc networks

- Network without infrastructure
  - Use components of participants for networking
- Examples
  - Single-hop: All partners max. one hop apart
    - Bluetooth piconet, PDAs in a room, gaming devices…
  - Multi-hop: Cover larger distances, circumvent obstacles
    - Bluetooth scatternet, TETRA police network, car-to-car networks…
- Internet: MANET (Mobile Ad-hoc Networking) group





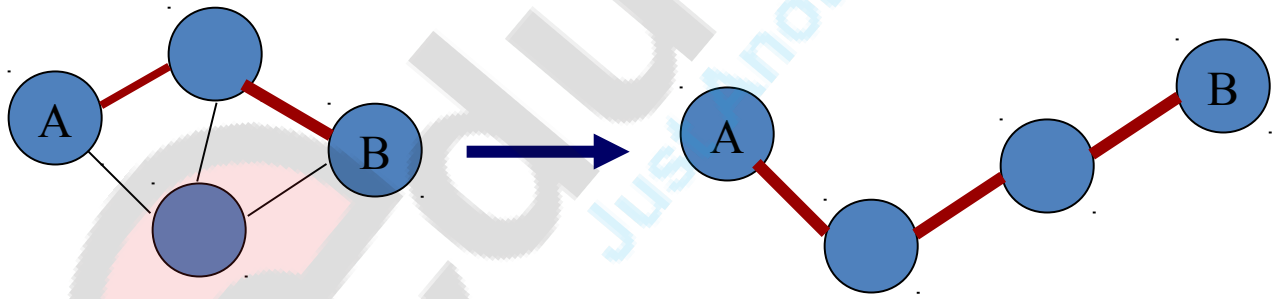
Significance of Routing in Ad-hoc network

- While in wireless networks with infrastructure support, a base station always reaches all mobile nodes, this is not always the case in an ad-hoc network.
- A destination node might be out of range of a source node transmitting packets.
- **Routing** is needed to find a path between source and destination and to forward the packets appropriately.

Cellular Network	Ad-hoc wireless network
Infrastructured network	Infrastructureless network
Fixed, pre-located cell sites and base station	No base station and rapid deployment
Static backbone network topology	Highly dynamic network topologies
Detailed planning before base station can be installed	Ad-hoc networks automatically forms and adapts to change
High setup cost	Cost effective

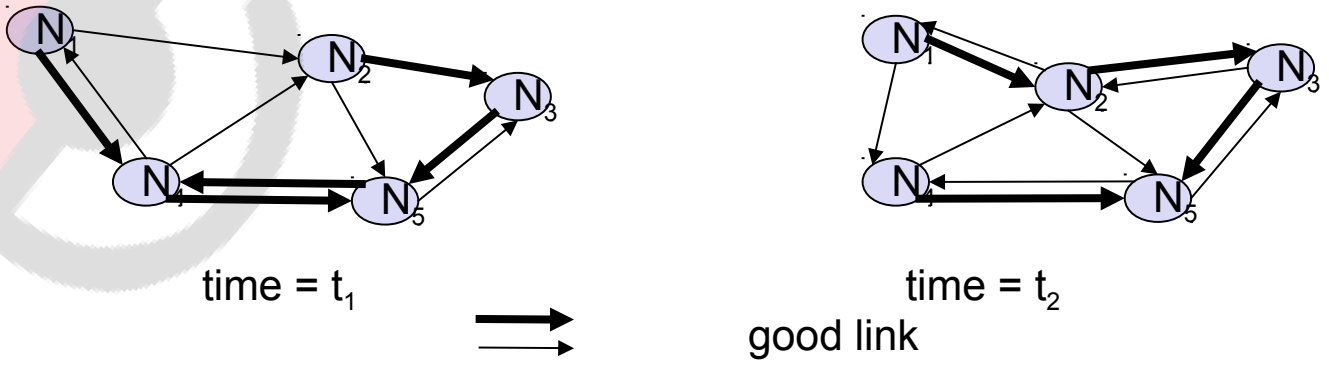
Mobile Ad Hoc Networks (MANET)

- Host movement frequent
- Topology change frequent
- No cellular infrastructure. Multi-hop wireless links.
- Data must be routed via intermediate nodes.



Example: Ad Hoc Networks

- At a certain time t1 the network topology…
- Five nodes, N1 to N5, are connected depending on the current transmission characteristics between them.
- In this N4 can receive N1 over a good link, but N1 receives N4 only via a weak link.
- Links do not necessarily have the same characteristics in both directions.
- The reasons for this are, e.g., different antenna characteristics or transmit power.
- N1 cannot receive N2 at all, N2 receives a signal from N1.
- the snapshot at t2 shows. N1 cannot receive N4 any longer, N4 receives N1 only via a weak link.
- But now N1 has an asymmetric but bi-directional link to N2 that did not exist before.



- fundamental differences between wired networks and ad-hoc wireless networks related to routing:
  - **Asymmetric links:** Node A receives a signal from node B. But this does not tell us anything about the quality of the connection in reverse.
  - **Redundant links: no central controller** responsible for controlling redundancy**.** Routing algorithms for wired networks can handle some redundancy, but a high redundancy can cause a large computational overhead for routing table updates.no of redundant link increases and may lead to fully meshed topology.
  - **Interference:** Links come and go depending on transmission characteristics, one transmission might interfere with another, and nodes might overhear the transmissions of other nodes.
  - **Highly dynamic topology- topology may change rapidly.**

Problems in Ad-hoc routing

- Following are the issues arises for routing in ad-hoc network:
  - **New routing algorithm required:** traditional routing algorithms will not work efficiently because these algorithms were not designed for networks with highly dynamic topology, asymmetric link…
  - **Connection-less networks:**
  - **Enhancements in MN required:** as ad-hoc networks are usually formed without any prior information, many MN need to have routing capabilities

Flat Ad-hoc routing

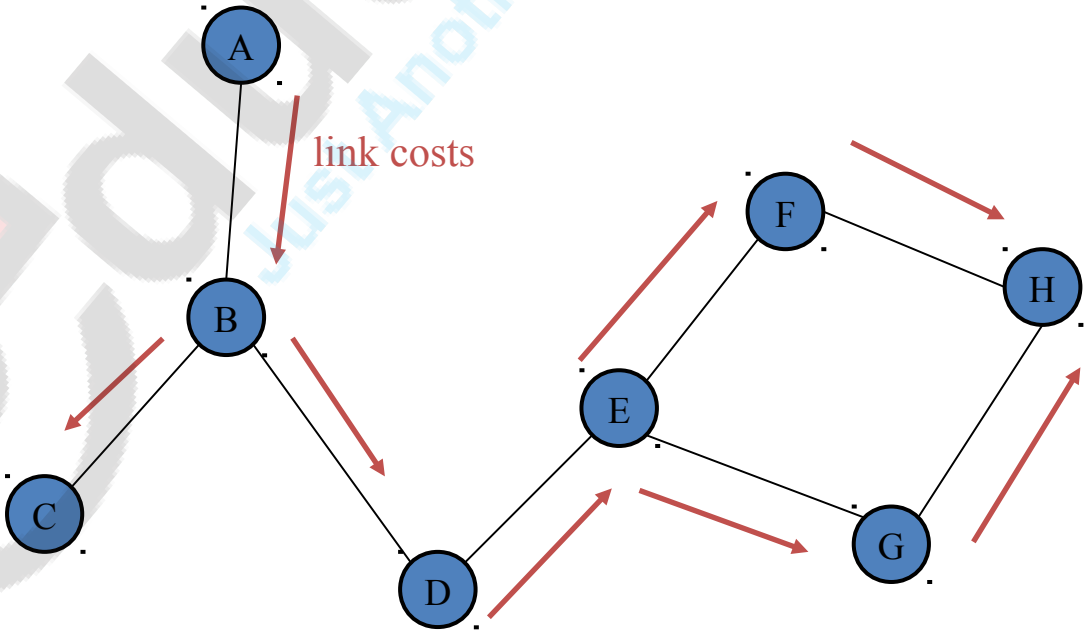
- This routing strategy comprises of those protocols in which the routing responsibility is Equally shared among all the nodes.
- No node treated as special.
- It uses flat addressing scheme.
- The protocols of this scheme are divided into two types.
- **Proactive protocols/table driven protocols** :
  - In this scheme the routing tables are set up and maintained.
  - Source node can get routing path immediately when it needs one
  - Destination sequence distance vector(DSDV)
  - Advantages: gives better QoS
  - Disadvantage: continuous updating in routing table generates a lot of unnecessary traffic

Flat Ad-hoc routing:Cont..

- **Reactive protocol/ on demand routing protocol:**
  - A path is setup between sender and receiver only when the sender has some data to send.
  - Reactive protocols are
    - Dynamic source routing
  - Advantages: high scalability as light network load.
  - Disadvantage: latency increases because path has to set up between sender and receiver before any data has to send.

Link-State

- Like the shortest-path computation method.
- Each node maintains a view of the network topology with a cost for each link.
- Periodically broadcast link costs to its outgoing links to all other nodes.



Distance-Vector Protocol: In traditional Networks

- known also as Distributed Bellman-Ford or RIP (Routing Information Protocol).
- Every node maintains a routing table
  - all available destinations
  - the next node to reach to destination
  - the number of hops to reach the destination
- Periodically send table to all neighbors to maintain topology.
- DV not suited for ad-hoc networks!
  - Loops
  - Count to Infinity
- New Solution -> DSDV Protocol

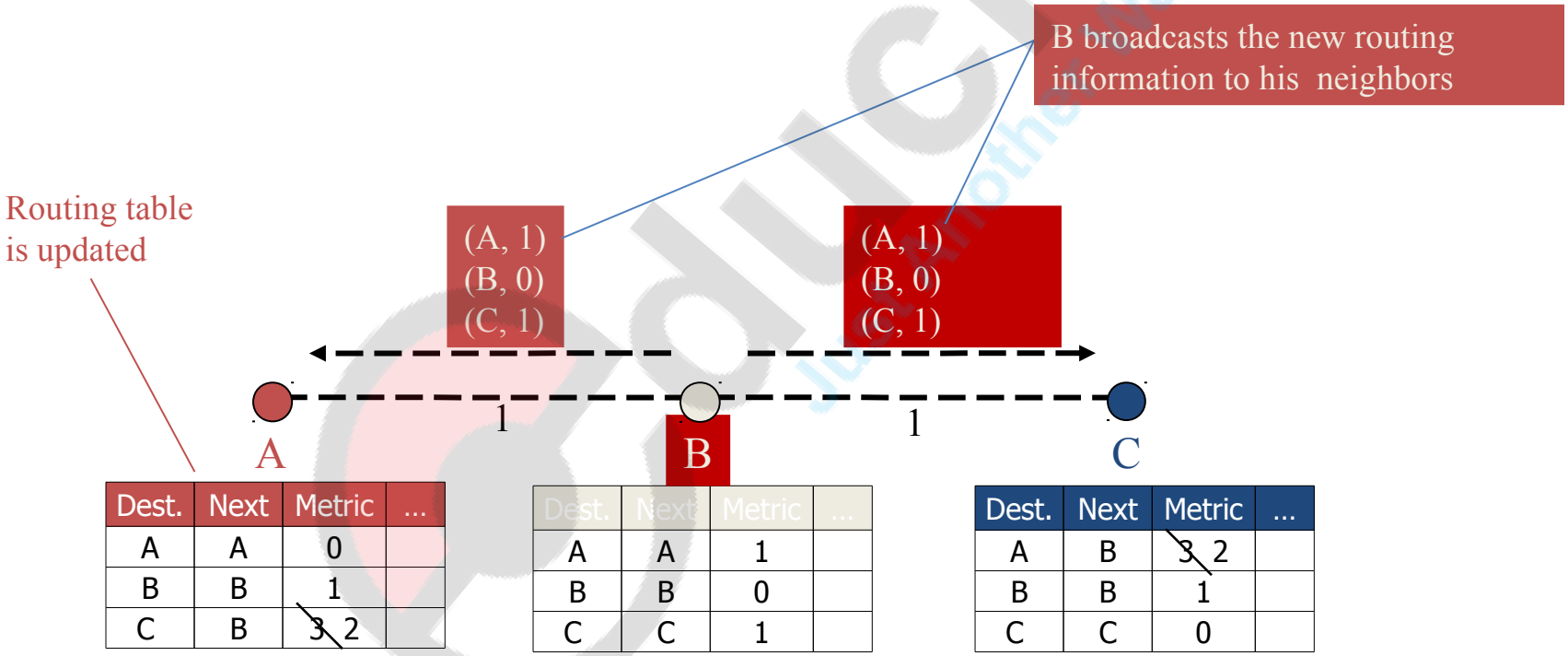
Distance Vector (Tables)

Dest.	Next	Metric	...
A	A	0	
B	B	1	
C	B	3	

Dest.	Next	Metric	...
A	A	1	
B	B	0	
C	C	2	

Dest.	Next	Metric	...
A	B	3	
B	B	2	
C	C	0	

Distance Vector (Update)

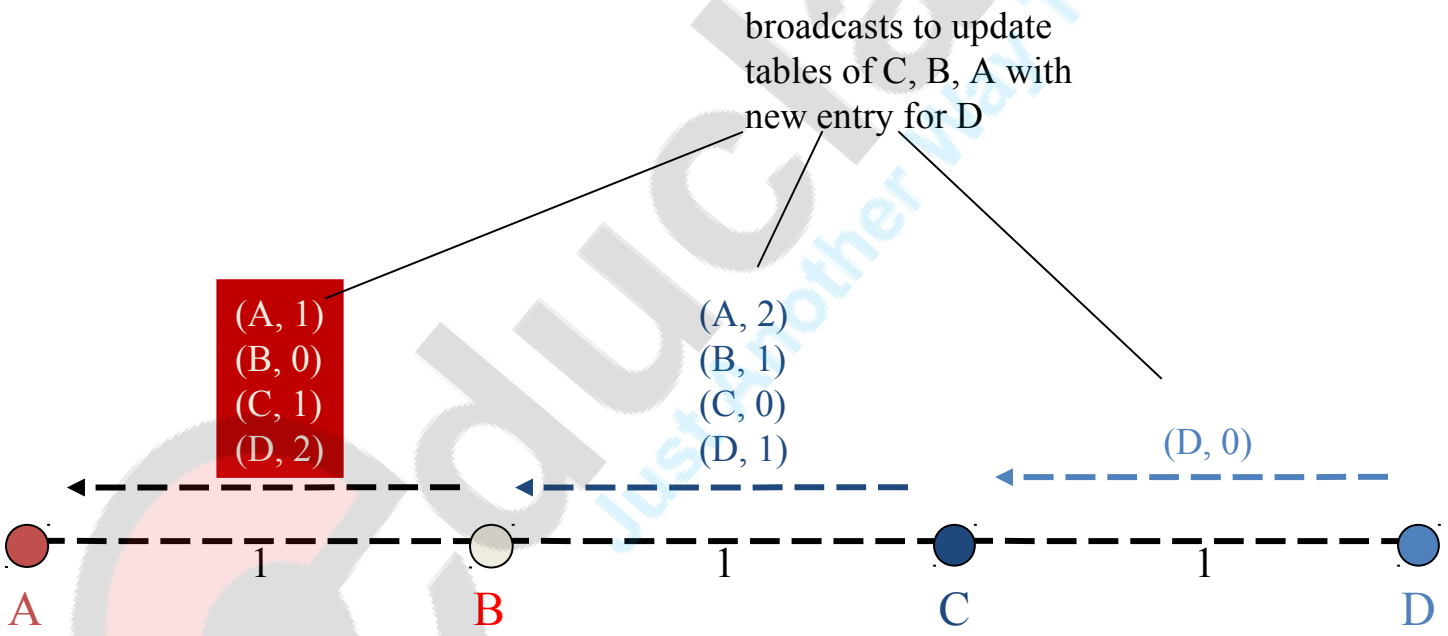


Dest.	Next	Metric	...
A	A	0	
B	B	1	
C	B	~~3~~ 2	

Dest.	Next	Metric	...
A	A	1	
B	B	0	
C	C	1	

Dest.	Next	Metric	...
A	B	~~3~~ 2	
B	B	1	
C	C	0	

Distance Vector (New Node)

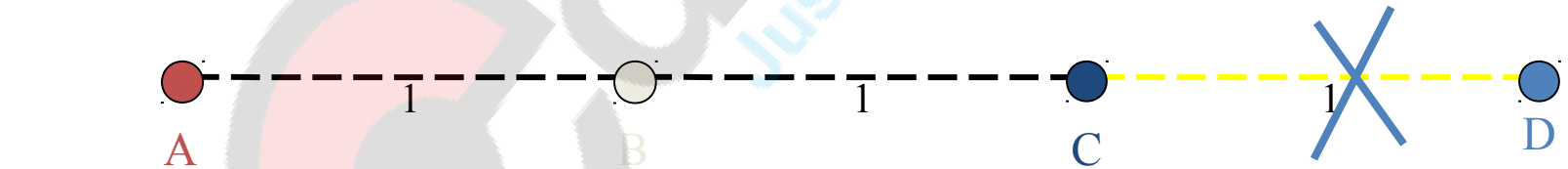


Dest.	Next	Metric	...
A	A	0	
B	B	1	
C	B	2	
D	B	3	

Dest.	Next	Metric	...
A	A	1	
B	B	0	
C	C	1	
D	C	2	

Dest.	Next	Metric	...
A	B	2	
B	B	1	
C	C	0	
D	D	1	

Distance Vector (Broken Link)

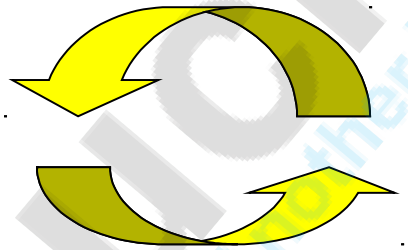


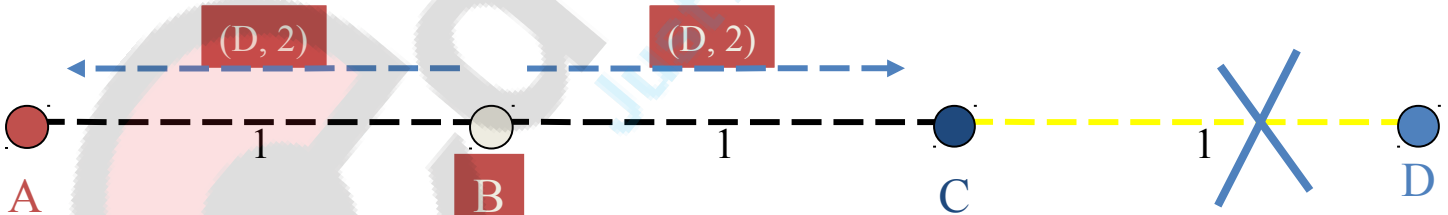
Dest.	Next	Metric	...
...	...	...	
D	B	3	

Dest.	Next	Metric	...
...	...	...	
D	C	2	

Dest.	Next	Metric	...
...	...	...	
D	D	∞	
		1	

Distance Vector (Loops)





Dest.	Next	Metric	...
...	...	...	
D	B	3	

Dest.	Next	Metric	...
...	...	...	
D	C	2	

Dest.	Next	Metric	...
...	...	...	
D	B	3	

DSDV(Destination sequence distance vector) Protocol

- DSDV is Destination Based.
- No global view of topology.
- **Destination sequence distance vector (DSDV)** routing is an enhancement to distance vector routing for ad-hoc networks.
- Distance vector routing is used as routing information protocol (RIP) in wired networks.

DSDV adds:

- **Sequence numbers:**
  - Each routing advertisement comes with a sequence number.
  - Helps to apply the advertisements in correct order.
  - This avoids loops.
- **Damping:**
  - it prevents temporary changes in the network topology from destabilizing the entire network.
  - Such temporary changes last for short duration.
  - A node waits with dissemination if the changes are probably unstable.
  - Waiting time depends on the time between the first and last announcement of a path to a certain destination.

DSDV Protocol: Cont..

- DSDV is Proactive (Table Driven)
  - Each node maintains routing information for all known destinations
  - Routing information must be updated periodically
  - Traffic overhead even if there is no change in network topology
  - Maintains routes which are never used
- Keep the simplicity of Distance Vector
- Guarantee Loop Freeness
  - New Table Entry for Destination Sequence Number
- Allow fast reaction to topology changes
  - Make immediate route advertisement on significant changes in routing table
  - but wait with advertising of unstable routes (damping fluctuations)

DSDV (Table Entries)

Destination	Next	Metric	Seq. Nr	Install Time	Stable Data
A	A	0	A-550	001000	Ptr_A
B	B	1	B-102	001200	Ptr_B
C	B	3	C-588	001200	Ptr_C
D	B	4	D-312	001200	Ptr_D

- **Sequence number** originated from destination. Ensures loop freeness.
- **Install Time** when entry was made (used to delete stale entries from table)
- **Stable Data** Pointer to a table holding information on how stable a route is. Used to damp fluctuations in network.

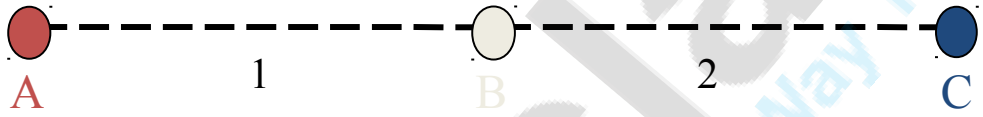
DSDV (Route Advertisements)

- Advertise to each neighbor own routing information
  - Destination Address
  - Metric = Number of Hops to Destination
  - Destination Sequence Number
- Rules to set sequence number information
  - On each advertisement, increase own destination sequence number (use only even numbers)
  - If a node is no more reachable (timeout) ,increase sequence number of this node by 1 (odd sequence number)

DSDV (Route Selection)

- Update information is compared to own routing table
  - 1. Select route with higher destination sequence number (This ensure to use always newest information from destination)
  - 2. Select the route with better metric when sequence numbers are equal.

DSDV (Tables)



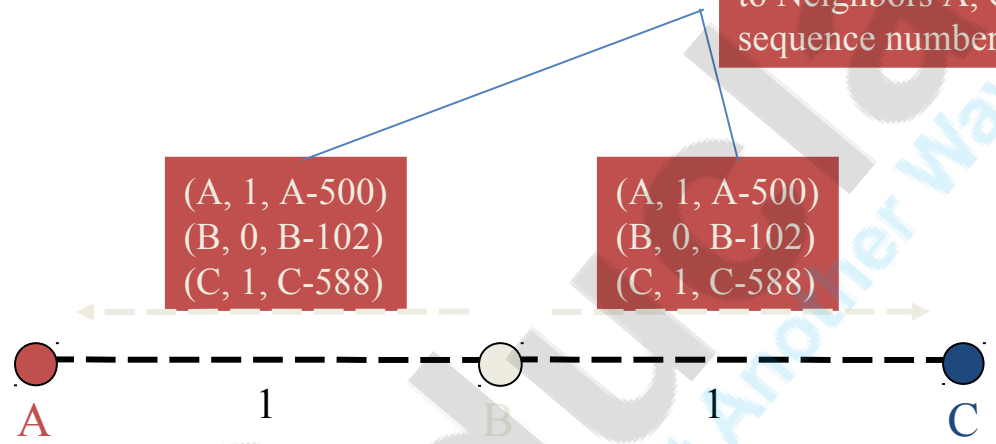
Dest.	Next	Metric	Seq
A	A	0	A-550
B	B	1	B-100
C	B	3	C-586

Dest.	Next	Metric	Seq
A	A	1	A-550
B	B	0	B-100
C	C	2	C-588

Dest.	Next	Metric	Seq.
A	B	1	A-550
B	B	2	B-100
C	C	0	C-588

DSDV (Route Advertisement)

B increases Seq.Nr from 100 -> 102
B broadcasts routing information to Neighbors A, C including destination sequence numbers



Dest.	Next	Metric	Seq
A	A	0	A-550
B	B	1	B-102
C	B	2	C-588

Dest.	Next	Metric	Seq
A	A	1	A-550
B	B	0	B-102
C	C	1	C-588

Dest.	Next	Metric	Seq.
A	B	2	A-550
B	B	1	B-102
C	C	0	C-588

Dynamic source routing Protocol

- **Route discovery:** A node only tries to discover a route to a destination if it has to send something to this destination and there is currently no known route.
- **Route maintenance:** If a node is continuously sending packets via a route, it has to make sure that the route is held upright.
- As soon as a node detects problems with the current route, it has to find an alternative.

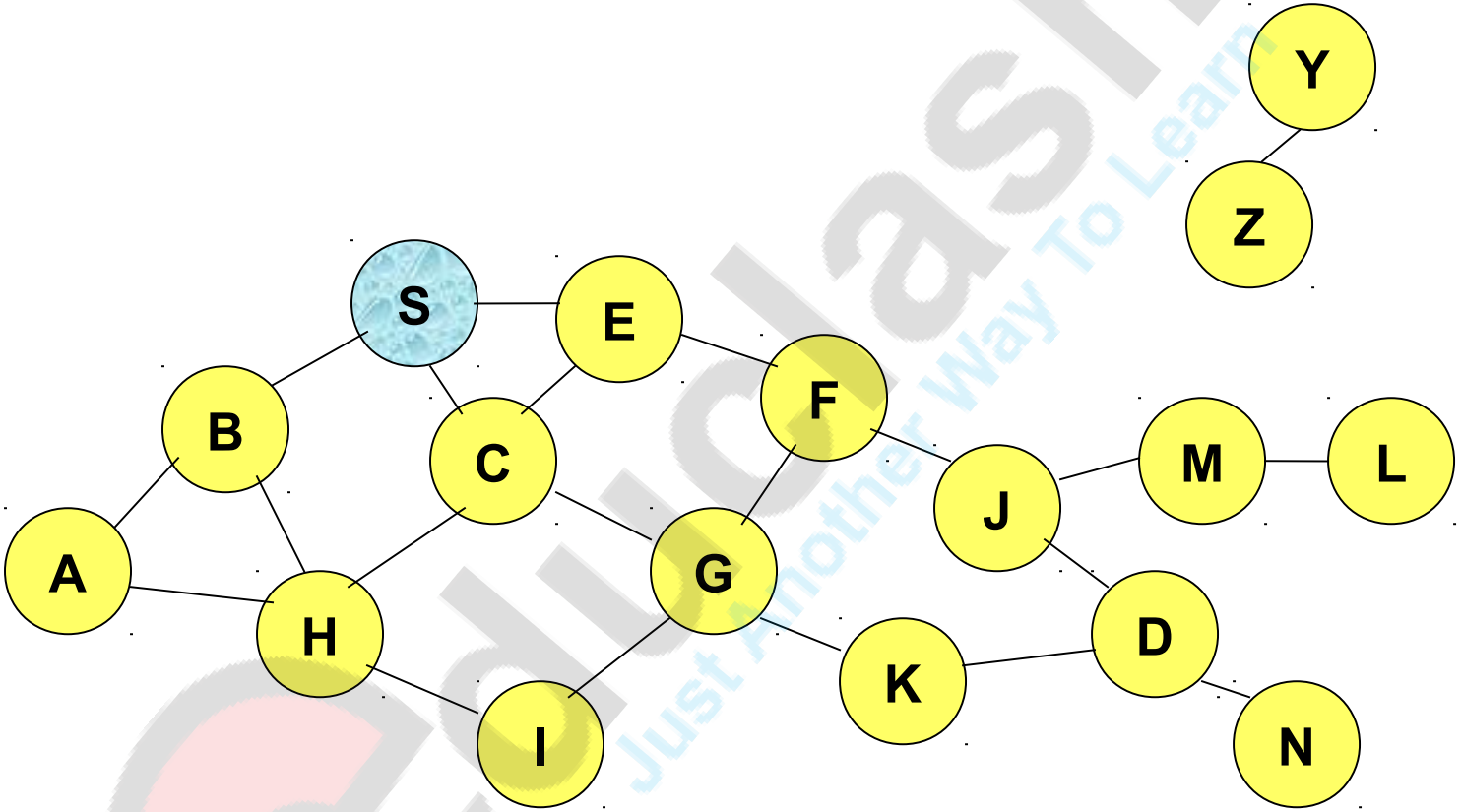
Dynamic source routing Protocol: Cont..

- If a node needs to discover a route, it **broadcasts** a **route request** with a **unique identifier** and the **destination address** as parameters.
- Any node that receives a route request does the following.
  - If the node has already received the request (which is identified using the unique identifier), it drops the request packet.
  - If the node recognizes its own address as the destination, the request has reached its target.
  - Otherwise, the node appends its own address to a list of traversed hops in the packet and broadcasts this updated route request.

Dynamic source routing Protocol: Cont..

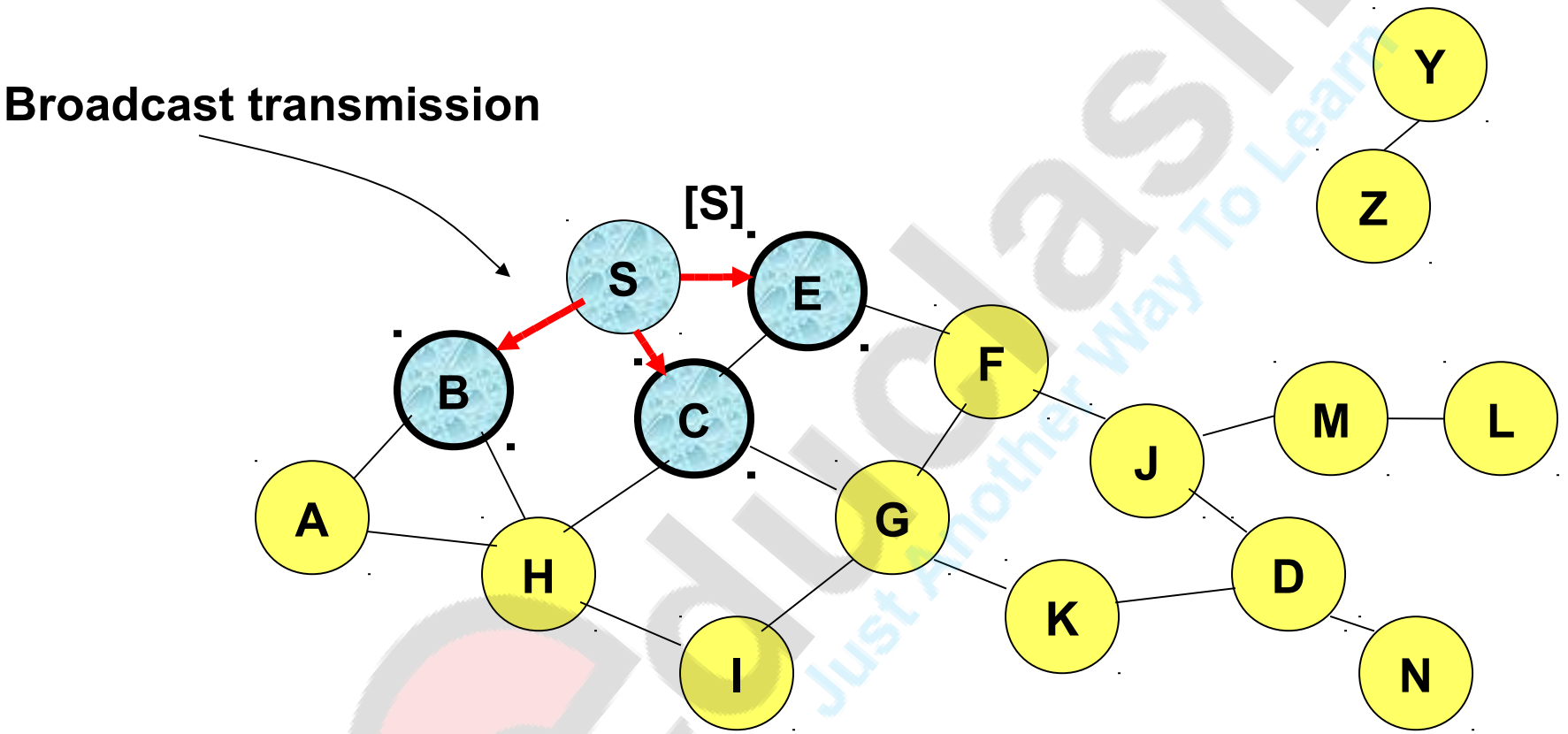
- Using this approach, the route request collects a list of addresses representing a possible path on its way towards the destination.
- As soon as the **request reaches the destination**, it can return the request packet containing the list to the receiver using this **list in reverse order.**
- One condition for this is that the **links** work **bi-directionally**.
- If this is not the case, and the **destination node** does not currently maintain a route back to the initiator of the request, it has to start a **route discovery** by itself.
- The destination may receive several lists containing different paths from the initiator.
- It could return the **best path**, the **first path**, **or several paths to offer** the initiator a choice.

Route Discovery in DSR



Represents a node that has received RREQ for D from S

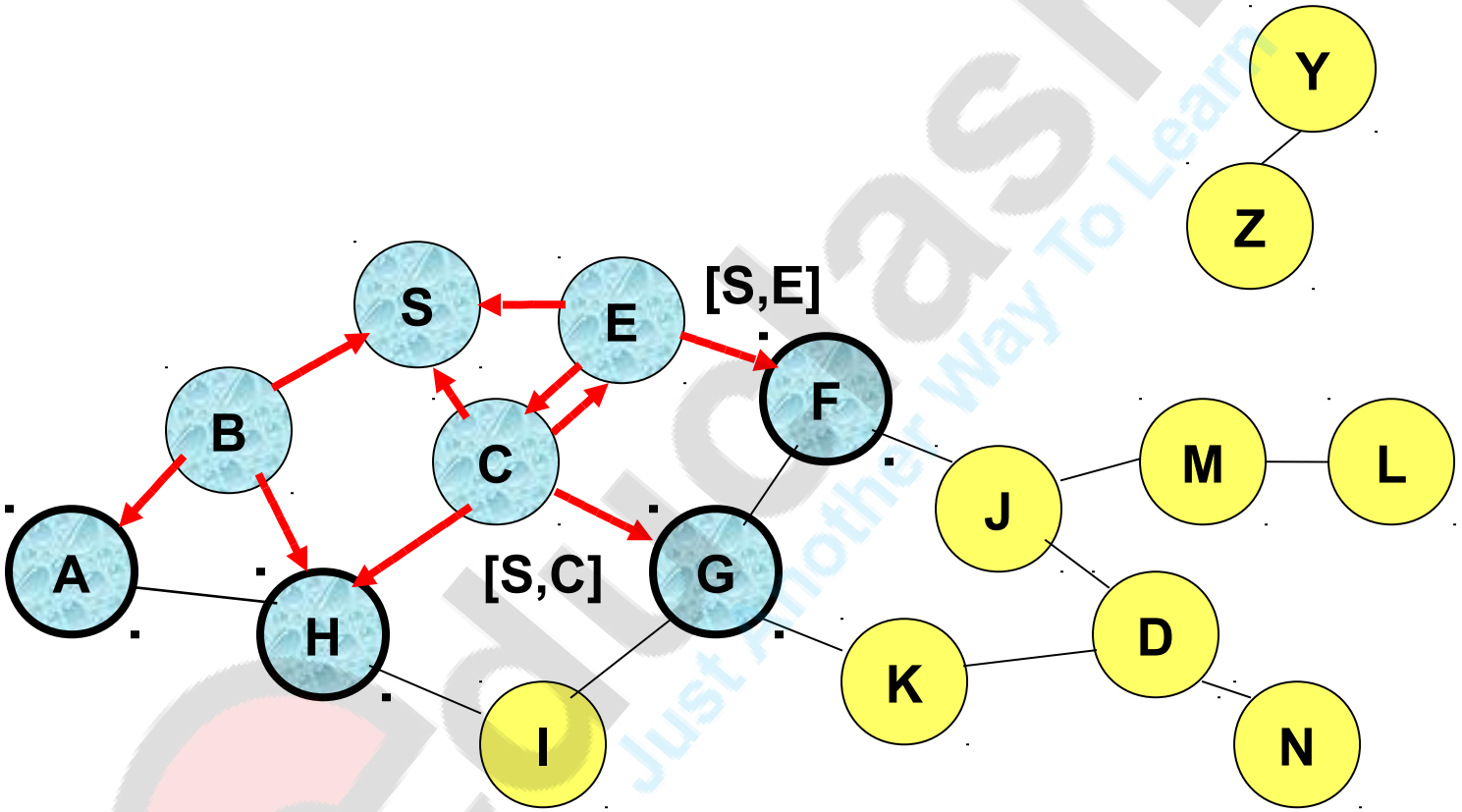
Route Discovery in DSR:Cont..



Represents transmission of RREQ

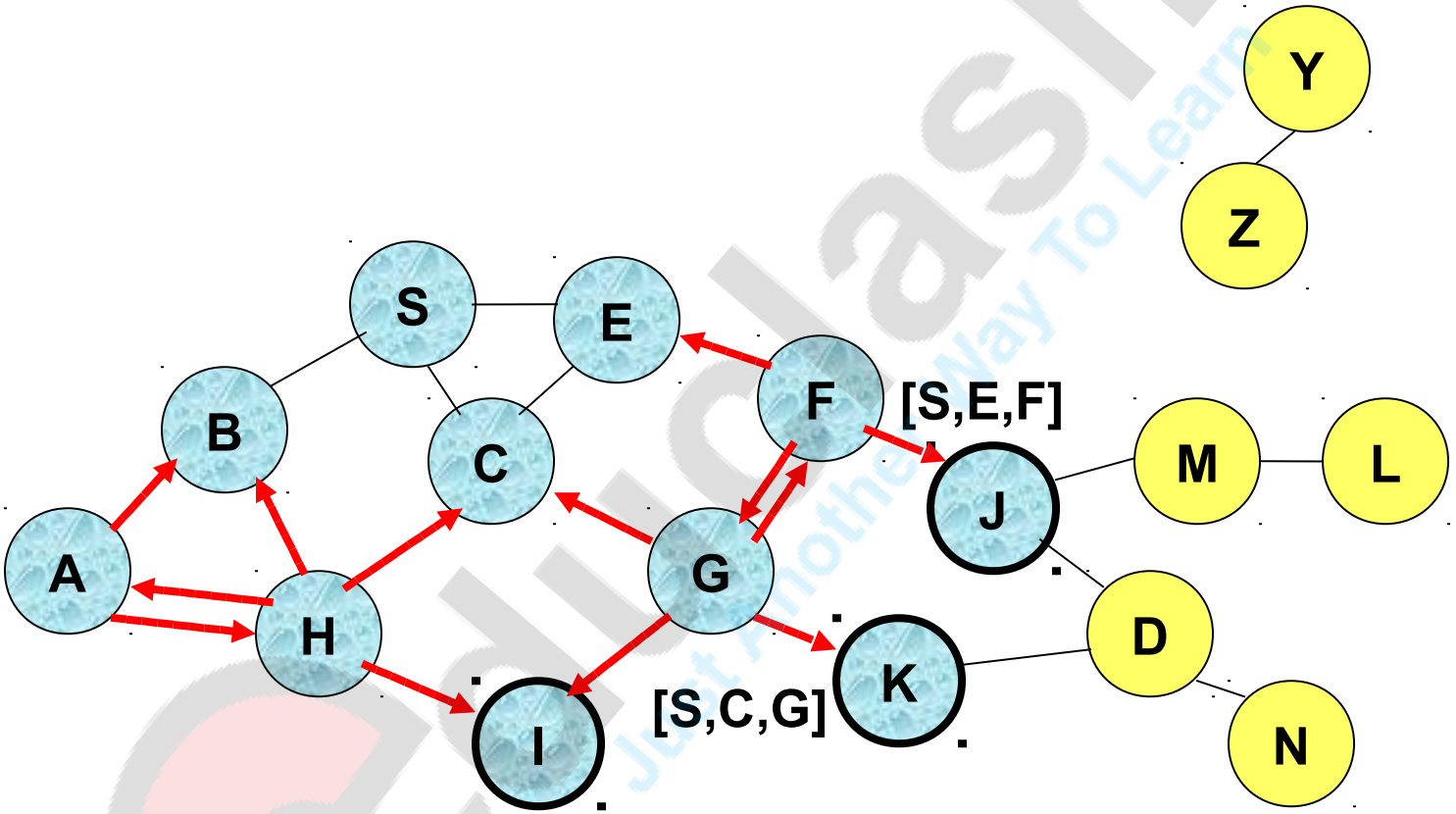
[X,Y] Represents list of identifiers appended to RREQ

Route Discovery in DSR



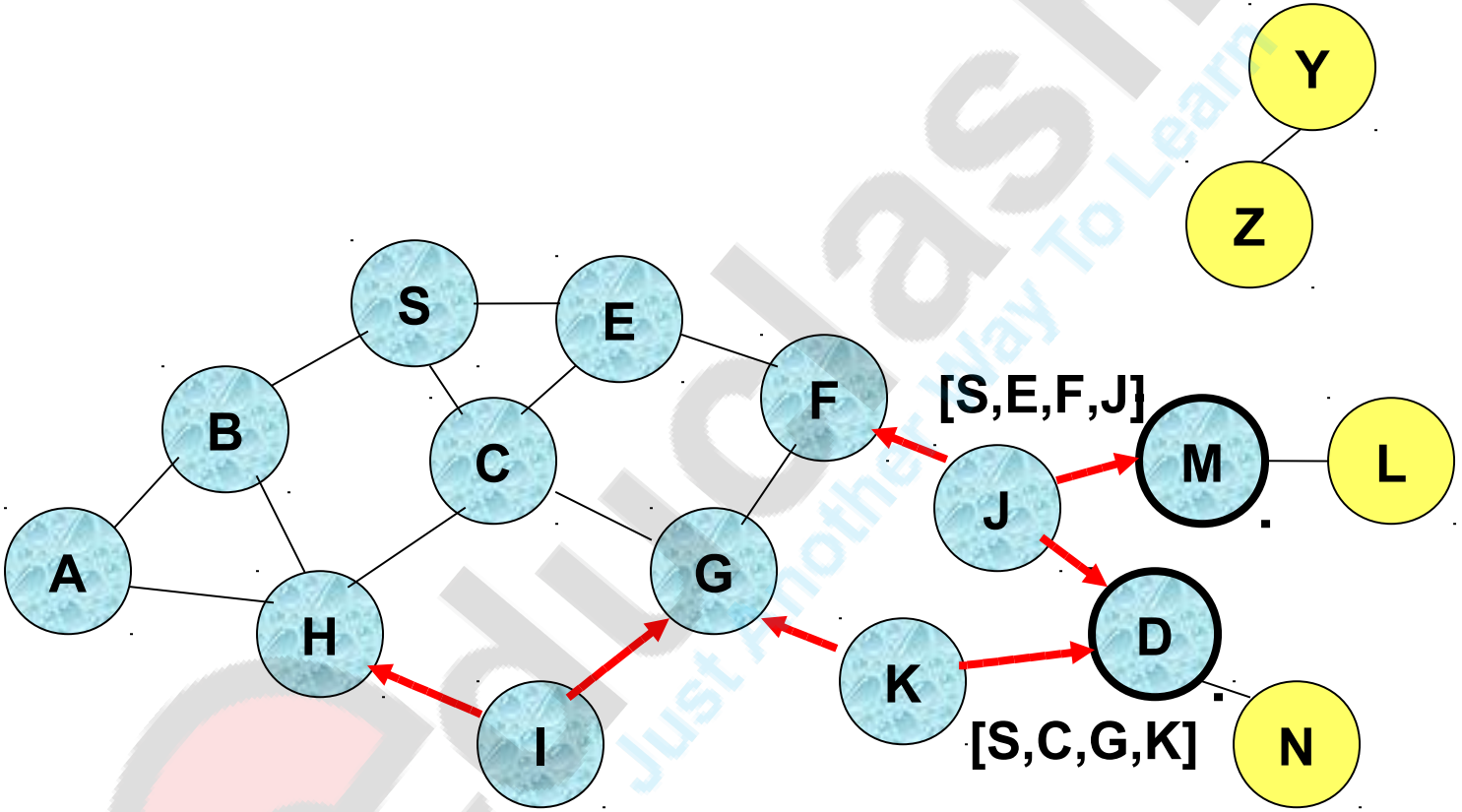
- Node H receives packet RREQ from two neighbors:
  potential for collision

Route Discovery in DSR:Cont..



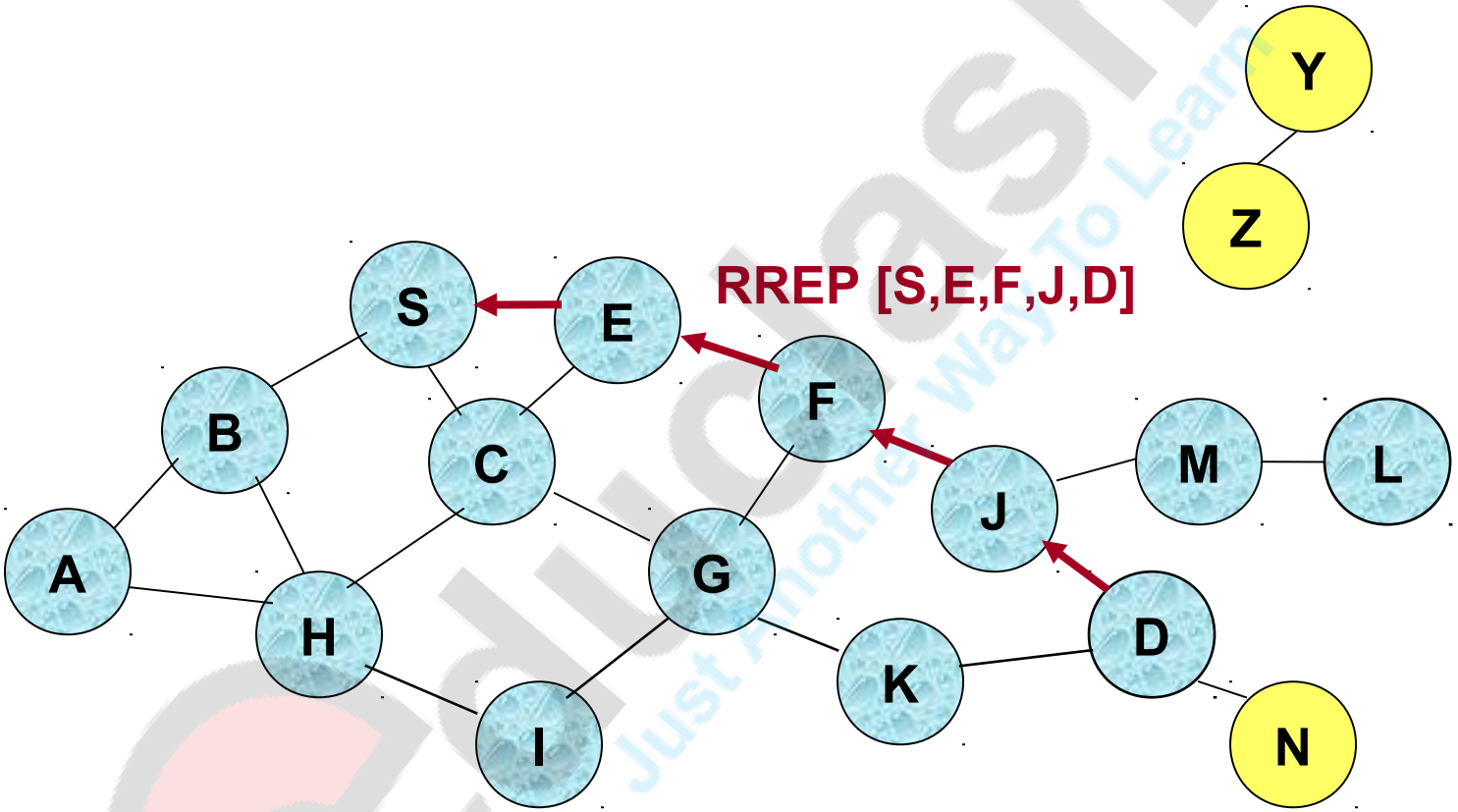
- Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once

Route Discovery in DSR:Cont..



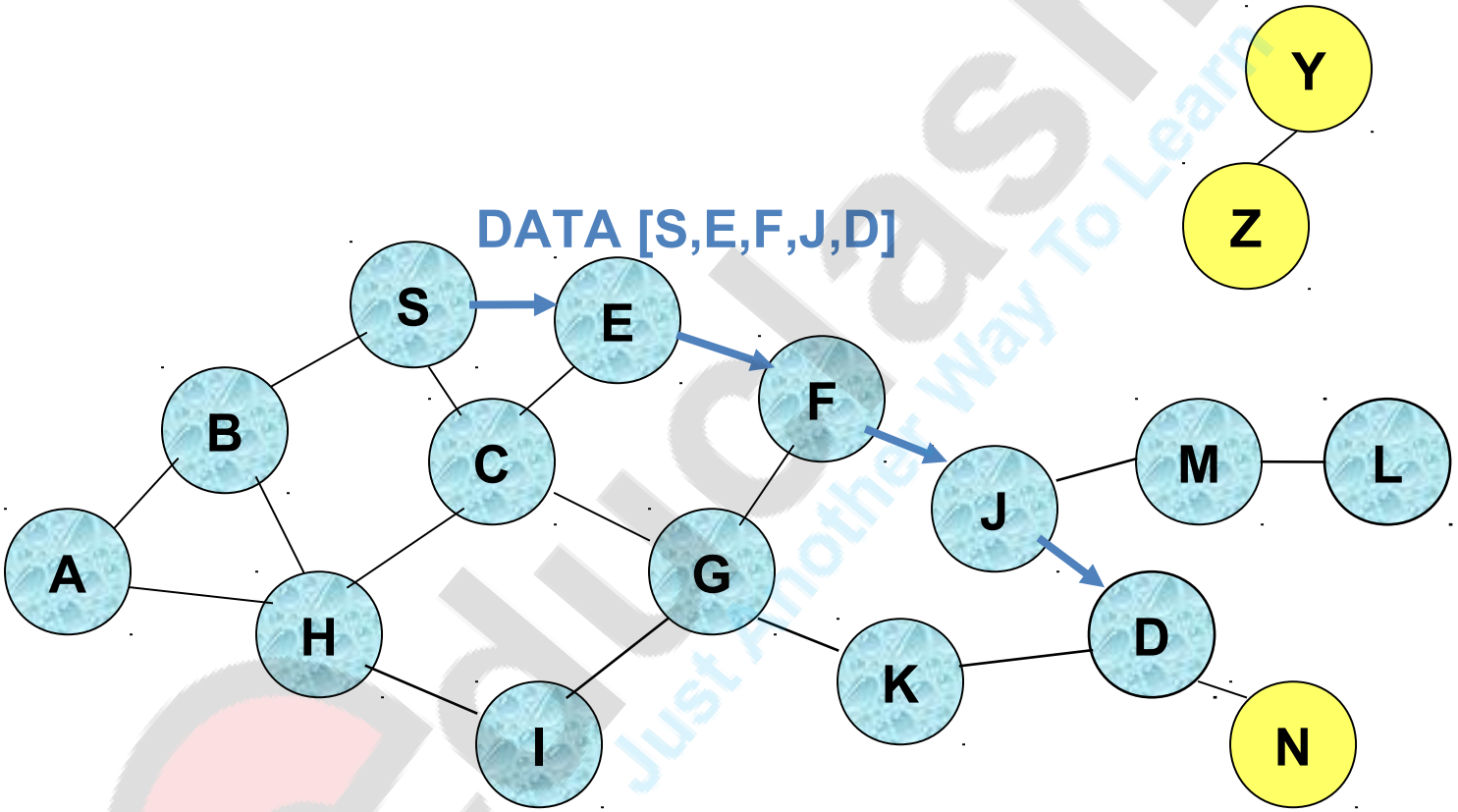
- Nodes J and K both broadcast RREQ to node D
- Since nodes J and K are hidden from each other, their transmissions may collide

Route Reply in DSR



Represents RREP control message

Data Delivery in DSR



Packet header size grows with route length

Dynamic Source Routing: Advantages

- Routes maintained only between nodes who need to communicate
  - reduces overhead of route maintenance
- Route caching can further reduce route discovery overhead
- More bandwidth efficient algorithm

Dynamic Source Routing: Disadvantages

- Packet header size grows with route length due to source routing.
- Flood of route requests may potentially reach all nodes in the network.
- Potential collisions between route requests propagated by neighboring 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.

References

- Mobile Communications, Second Edition, Jochen Schiller, Pearson Education- Chapter 8.