MOBILE IP

Dr. A. Beulah

AP/CSE

LEARNING OBJECTIVES

- To understand the basic concepts of mobile IP

MOTIVATION FOR MOBILE IP

- Routing
  - Based on IP destination address, network prefix (e.g. 129.13.42) determines physical subnet
  - Change of physical subnet implies change of IP address to have a topological correct address (standard IP) or needs special entries in the routing tables
- Specific routes to end-systems?
  - Change of all routing table entries to forward packets to the right destination
  - Does not scale with the number of mobile hosts and frequent changes in the location, security problems
- Changing the IP-address?
  - Adjust the host IP address depending on the current location
  - Almost impossible to find a mobile system, DNS updates take to long time
  - TCP connections break, security problems

DESIRABLE FEATURES OF MOBILE IP

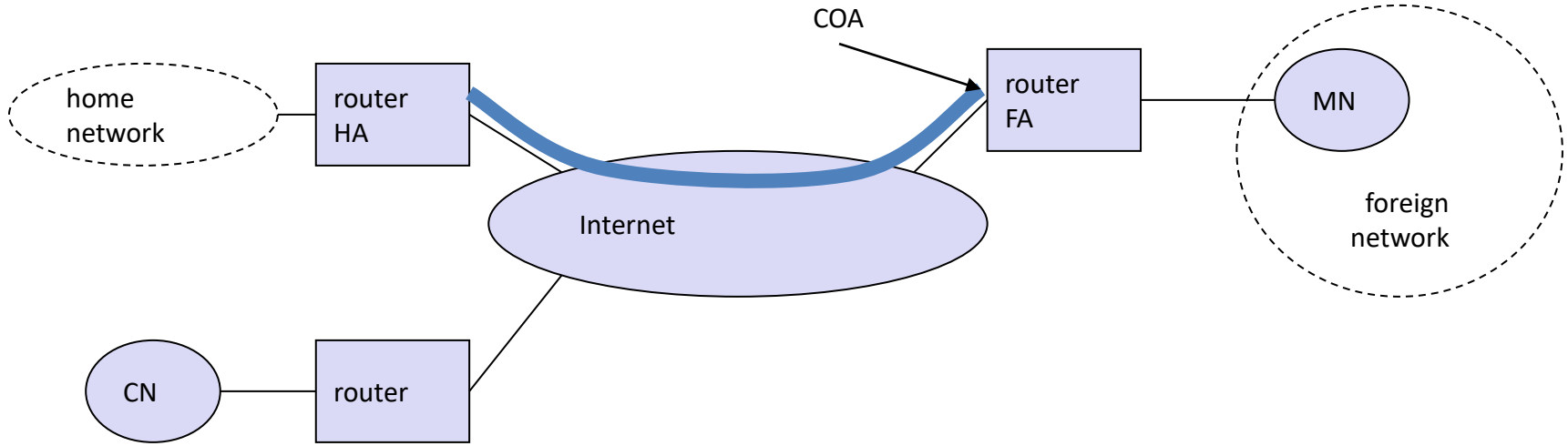
- Transparency
  - Mobile end-systems should keep their IP address
  - Continuation of communication after interruption of link is possible
  - Point of connection to the fixed network can be changed
- Compatibility
  - Support of the same layer 2 protocols as IP
  - No changes to current end-systems and routers required
  - Mobile end-systems can communicate with fixed systems
- Security
  - Authentication of all registration messages
- Efficiency and scalability
  - Only little additional messages to the mobile system required (connection typically via a low bandwidth radio link)
  - World-wide support of a large number of mobile systems in the whole Internet

MOBILE IP

- Entities and Terminology
- IP packet delivery
- Agent discovery
- Tunnelling and encapsulation

ENTITIES AND TERMINOLOGY

- Mobile Node (MN)
  - System (node) that can change the point of connection to the network without changing its IP address
  - 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



ENTITIES AND TERMINOLOGY

- Home Network
  - Provides home address to the mobile device.
  - The home network is the subnet the MN belongs to with respect to its IP address.
  - No mobile IP support is needed within the home network.
- Home Agent (HA)
  - System in the home network of the MN, typically a router
  - Maintains a location directory of the mobile nodes belonging permanently to the home network
  - Tunnel starts at the home agent.

ENTITIES AND TERMINOLOGY

- Foreign Agent (FA)
  - System in the current foreign network of the MN, typically a router
  - Functions as point of attachment for a mobile node when it roams to the foreign network.
  - Packets from the home agent are sent to the foreign node which delivers it to mobile node.
- Care-of Address (COA)
  - Address which identifies MN's current location
  - Actual location of the MN from an IP point of view can be chosen, e.g., via DHCP
  - The packets sent to the mobile node(MN) are delivered to COA using tunneling.
  - COA is the tunnel end point.

ENTITIES AND TERMINOLOGY

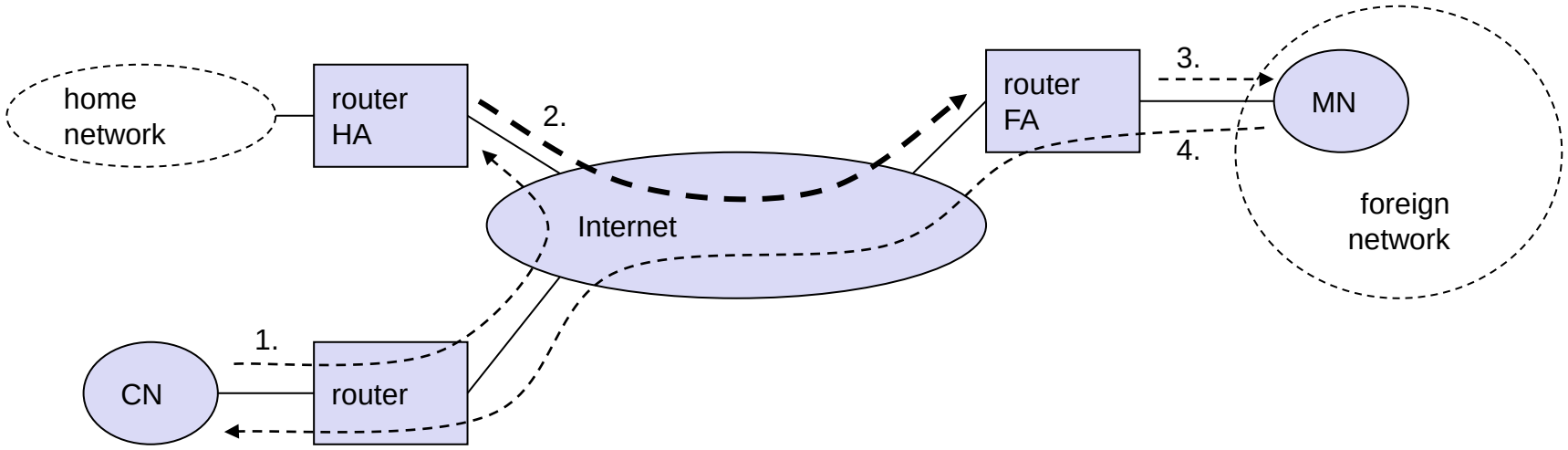
- 2 types of COA
  - Foreign Agent COA
    - Usually the IP address of the FA
    - Many MN using FA can share COA as common COA
    - FA is the tunnel end point, and FA forwards packet to the MN
  - Co-Located COA
    - When the MN temporarily acquires an additional IP address, that acts as the COA.
    - MN is the tunnel end point.
- Correspondent node (CN)
  - At least one partner is needed for communication.
  - The CN can be a fixed or mobile node.

TUNNELLING AND ENCAPSULATION

- Tunnel
  - Virtual pipe for packets available between a tunnels entry point and an end point
- Tunnelling
  - The process of sending a packet via tunnel and achieved by a mechanism called encapsulation
- Encapsulation
  - Assembling old packet(packet header and data) in data part of new packet
- Decapsulation
  - Disassembling the data part of an encapsulated packet.

IP PACKET DELIVERY

- Mobile IP → Hides the mobility of the MN
- Data Transfer to the Mobile Node
- Data Transfer from the Mobile Node



DATA TRANSFER TO THE MOBILE NODE

1. CN transmits to the IP address of MN, HA intercepts packet (proxy ARP)
   - SA →CN IP, DA→ MN IP
   - No knowledge about MN's current location
   - Standard routing mechanisms of the internet
2. HA tunnels packet to COA (FA), by encapsulation
   - New header on top of old IP (encapsulation)
   - SA → HA, DA → COA
   - Tunnel → The path taken by the encapsulated packets.
   - Tunneling.
3. FA forwards the packet to the MN
   - Decapsulation
   - SA →CN IP, DA→ MN IP
   - Mobility not visible by MN

DATA TRANSFER FROM THE MOBILE NODE

4. CN transmits packet to the IP address of the receiver as usual.
   - SA → MA IP, DA → CN IP
   - FA works as default router and forwards the packet in standard manner (CN → Fixed Node).
   - CN → Mobile node, steps 1 through 3

AGENT DISCOVERY

- How to find a foreign agent is the major problem.
- How does the MN discover that it has moved?
- 2 methods:
  - Agent advertisement
  - Agent solicitation

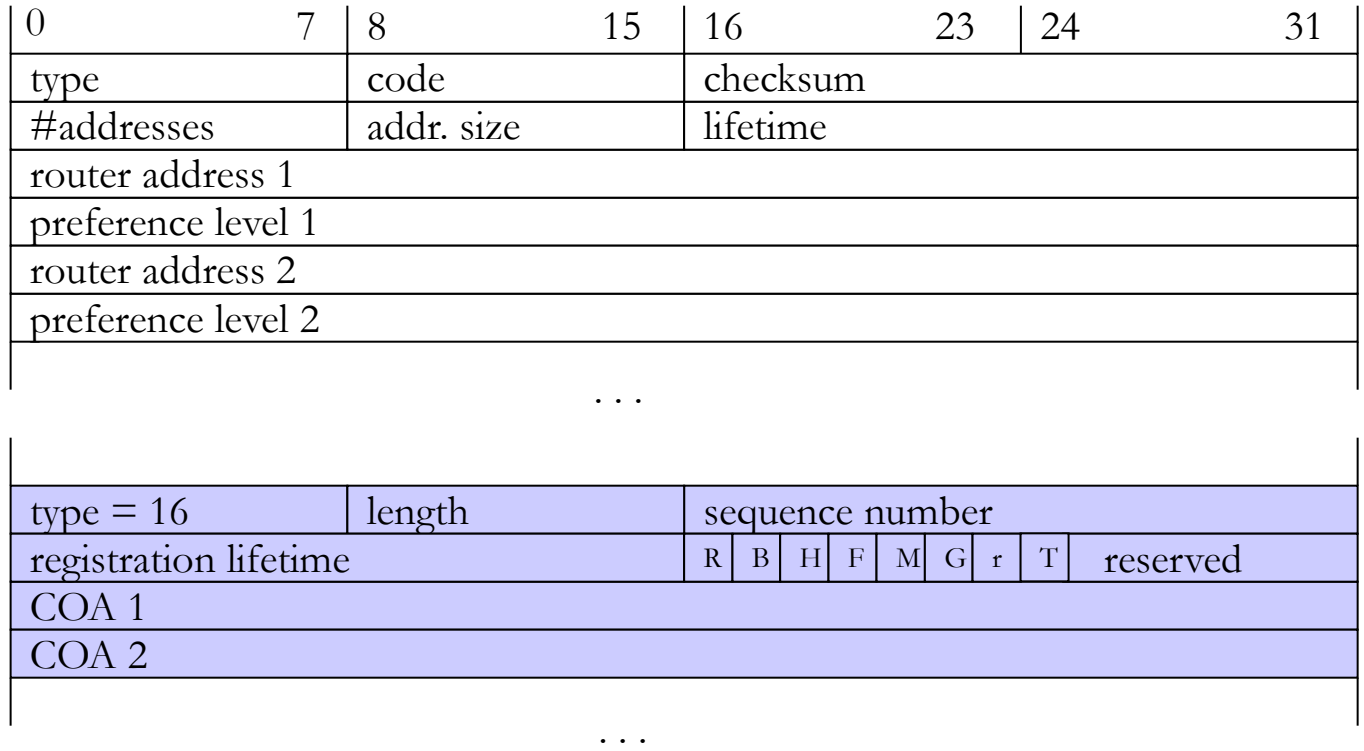
AGENT ADVERTISEMENT

- Home Agents and Foreign Agents periodically send **advertisement messages** into their physical subnets
- Advertisement is similar to Beacon Broadcast
- MN listens to these messages and detects, if it is in the home or a foreign network (standard case for home network)
- MN reads a COA from the FA advertisement messages

AGENT ADVERTISEMENT

RFC 1256 +mobility extension
(upper ICMP, lover mobility)
Type=9
Code 0 (normal)or 16(only mobile)

type = 16
length = 6 + 4 * #COAs
(6 = the number of bytes in the seq. no.,
Lifetime, Flags, and Reserved +
another 4 bytes per each COA)
R: registration required
B: busy, no more registrations
H: home agent
F: foreign agent
M: minimal encapsulation
G: Generic Routing Encapsulation
r: =0, ignored (former Van Jacobson compression)
T: FA supports reverse tunneling
reserved: =0, ignored



AGENT SOLICITATION

- The mobile node must send **agent solicitations** when it enters a foreign network**.**
- When a mobile node enters into a new network it can send out three solicitations, one per second
- If a MN does not get a new address, many packets will be lost
- If a MN does not receive an answer to its solicitations it must decrease the rate of solicitations exponentially to avoid flooding the network
- When the MN discovers a new agent it stops sending agent solicitation.
- A MN understands its FA by receiving an advertisement

SUMMARY

- Motivation for Mobile IP
- Desirable Features of Mobile IP
- Mobile IP
  - Entities and Terminology
  - IP packet delivery
  - Agent discovery

TEST YOUR KNOWLEDGE

- What is a dual stack?
  - The host or router uses both IPv4 and IPv6, but at different times
  - The host or router uses both IPv4 and IPv6 at the same time
  - The host or router uses IPv4 at different times
- What is one major difference between IPv4 and IPv6 configuration?
  - The router doesn't enable the routing of IPv6 packets by default, so you would need to use the global command to enable IPv6 routing
  - You can use the network router subcommand to enable IPv6 routing
  - IP addresses are shortened from 128 bits to 32 bits

TEST YOUR KNOWLEDGE

- When IPv4 addresses are exhausted and you're using IPv4 connections to access the Internet, you
  - won't be able to access IPv6 websites at all
  - may still be able to access some IPv6 websites with some limitations
  - will still be able to access IPv6 website with no problem at all

REFERENCES

- Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007.
- Prasant Kumar Pattnaik, Rajib Mall, “Fundamentals of Mobile Computing”, PHI Learning Pvt. Ltd, New Delhi – 2012.

MOBILE IP

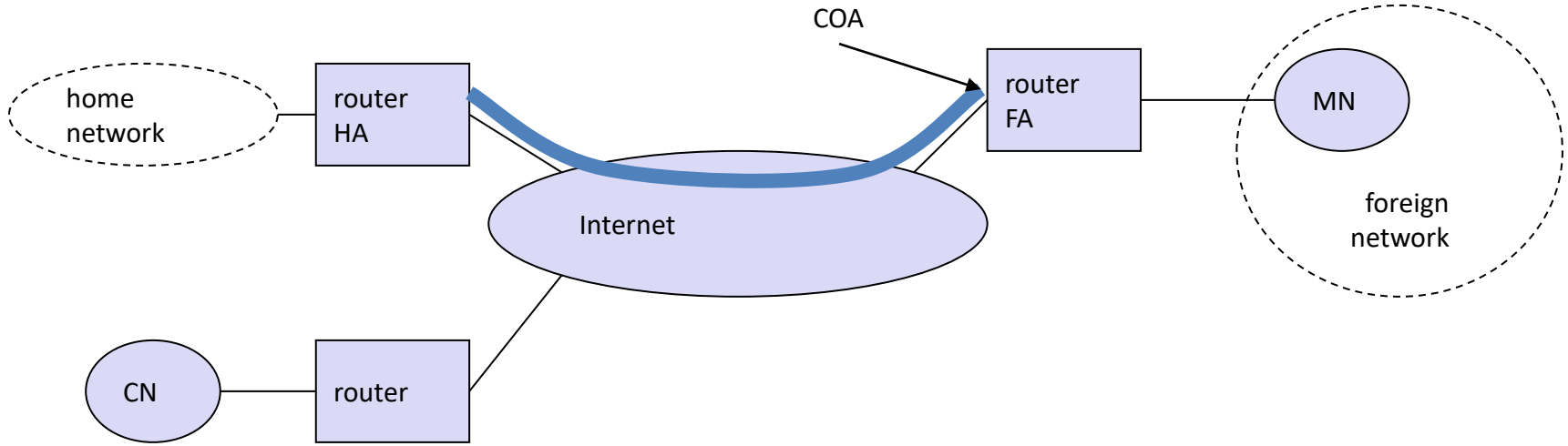
Dr. A. Beulah

AP/CSE

LEARNING OBJECTIVES

- To understand the basic concepts of Mobile IP, Registration

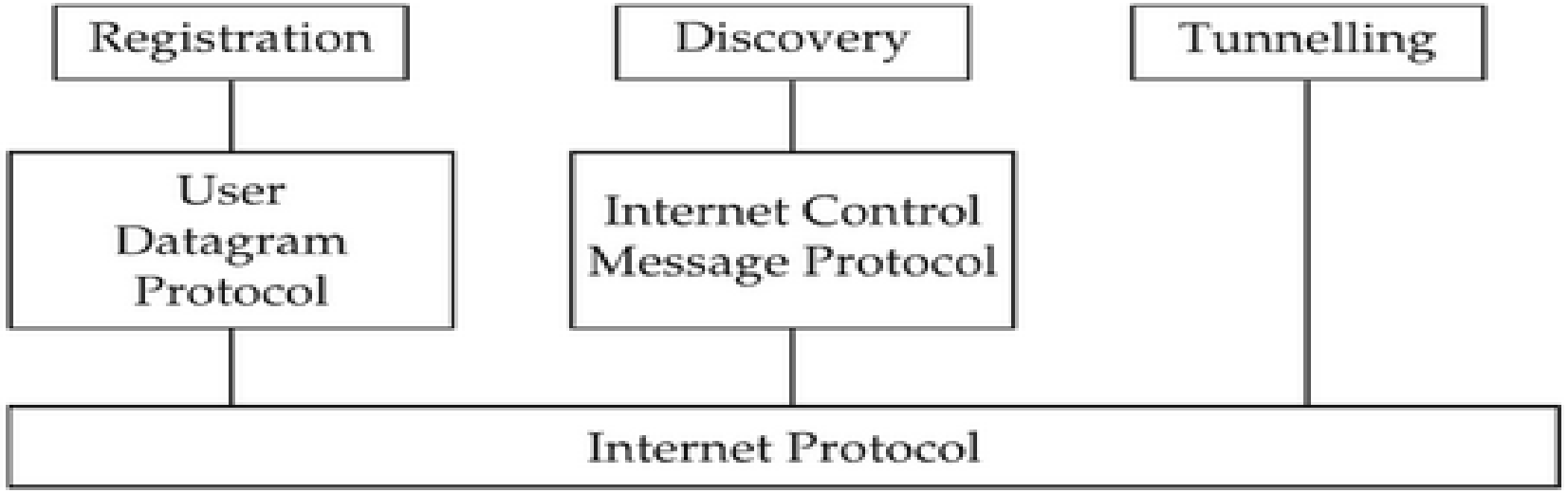
SCENARIO


COA
home
network
router
HA
router
FA
MN
Internet
foreign
network
CN
router

KEY MECHANISM USED IN MOBILE IP

- 3 Basic Mechanism
  - Discovering the COA (Agent Discovery)
  - Registering the COA (Registration)
  - Tunneling to the COA (Tunneling)

Schematic Model of Mobile IP



DISCOVERING THE COA

- Each MN uses a discovery protocol to identify the respective home and foreign agent.
- Discovery of COA consists of following steps:
  1. Mobile Agent periodically broadcast "Agent Advertisement" msg
  2. On receiving "Agent Advertisement" msg, the MN can determine if it is in home network or foreign network.
  3. If the MN does not wish to wait, it transmits "Agent Solicitation" msg. A mobile agent will respond for this.

AGENT DISCOVERY

- How to find a foreign agent is the major problem.
- How does the MN discover that it has moved?
- 2 methods:
  - Agent advertisement
  - Agent solicitation

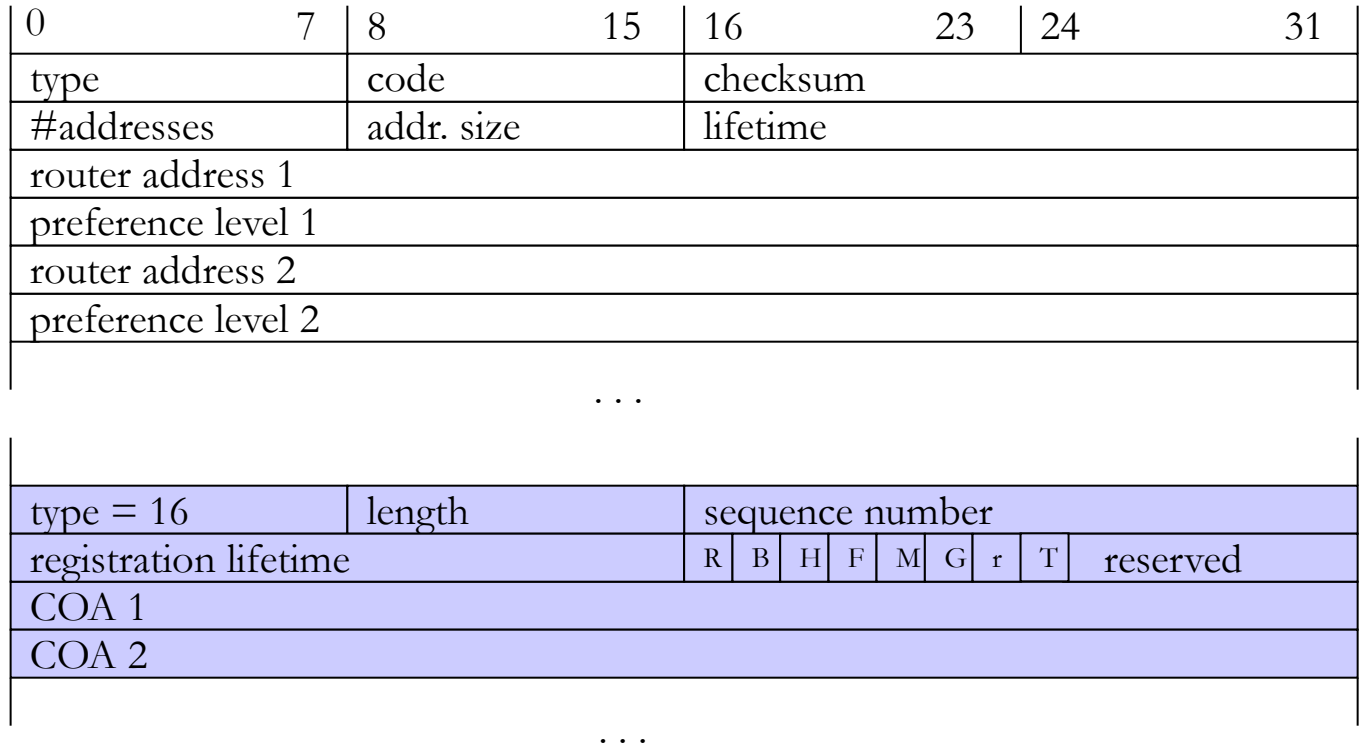
AGENT ADVERTISEMENT

- Home Agents and Foreign Agents periodically send **advertisement messages** into their physical subnets
- Advertisement is similar to Beacon Broadcast
- MN listens to these messages and detects, if it is in the home or a foreign network (standard case for home network)
- MN reads a COA from the FA advertisement messages

AGENT ADVERTISEMENT

RFC 1256 +mobility extension
(upper ICMP, lover mobility)
Type=9
Code 0 (normal)or 16(only mobile)

type = 16
length = 6 + 4 * #COAs
(6 = the number of bytes in the seq. no.,
Lifetime, Flags, and Reserved +
another 4 bytes per each COA)
R: registration required
B: busy, no more registrations
H: home agent
F: foreign agent
M: minimal encapsulation
G: Generic Routing Encapsulation
r: =0, ignored (former Van Jacobson compression)
T: FA supports reverse tunneling
reserved: =0, ignored

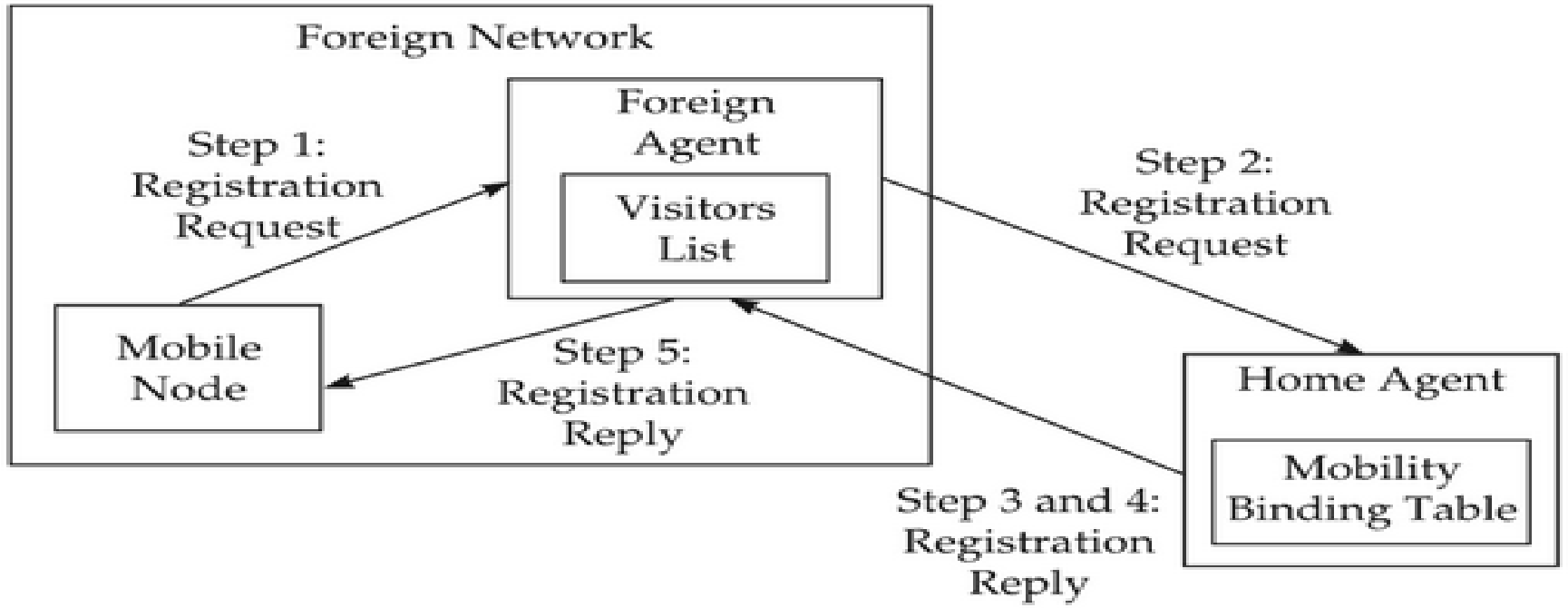


AGENT SOLICITATION

- The mobile node must send **agent solicitations** when it enters a foreign network**.**
- When a mobile node enters into a new network it can send out three solicitations, one per second
- If a MN does not get a new address, many packets will be lost
- If a MN does not receive an answer to its solicitations it must decrease the rate of solicitations exponentially to avoid flooding the network
- When the MN discovers a new agent it stops sending agent solicitation.
- A MN understands its FA by receiving an advertisement

REGISTERING THE COA

- MN Home network → No mobility services
- MN Foreign Network → Has COA
- Register the COA with HA.



REGISTERING THE COA

- Step 1: Registration Request (MN → FA)
  - Registration request msg includes MN's IP Address (permanent), IP address of HA
- Step 2: Registration Request (FA→ HA)
  - Registration request msg includes MN's IP Address (permanent), IP address of FA
- Step 3: Updation of mobility binding table (HA)
  - Bind COA of MN with HA
- Step 4: Registration Reply (HA → FA)
  - Ack to FA
- Step 5: Registration Reply
  - Updates visitors list
  - Ack to MN

TABLES MAINTAINED ON ROUTERS

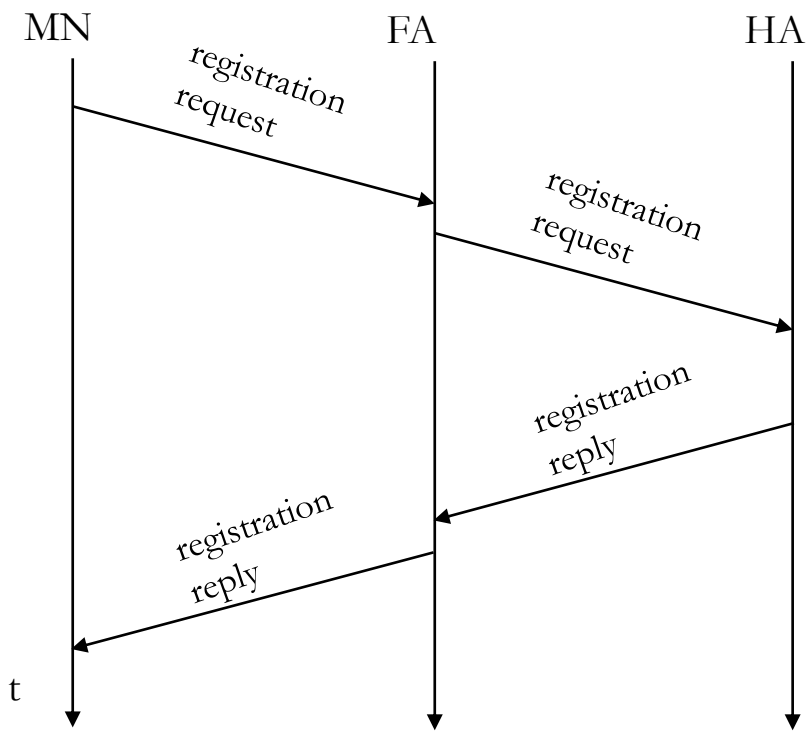
- Mobility Binding Table

Home Address	Care-of Address	Lifetime (in sec)
131.193.171.4	128.172.23.78	200
131.193.171.2	119.123.56.78	150

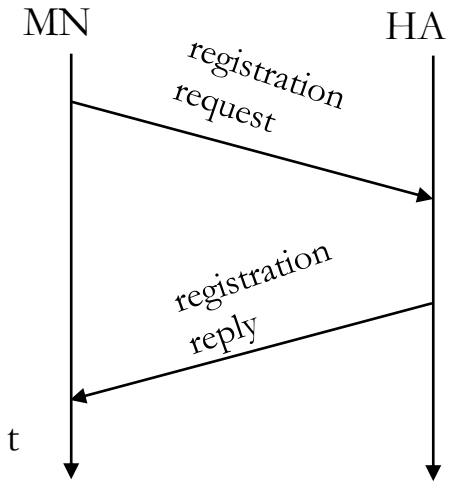
- Visitor List

Home Address	Home Agent Address	Media Address	Lifetime (in s)
131.193.44.14	131.193.44.7	00-60-08-95-66-E1	150
131.193.33.19	131.193.33.1	00-60-08-68-A2-56	200

REGISTERING THE COA

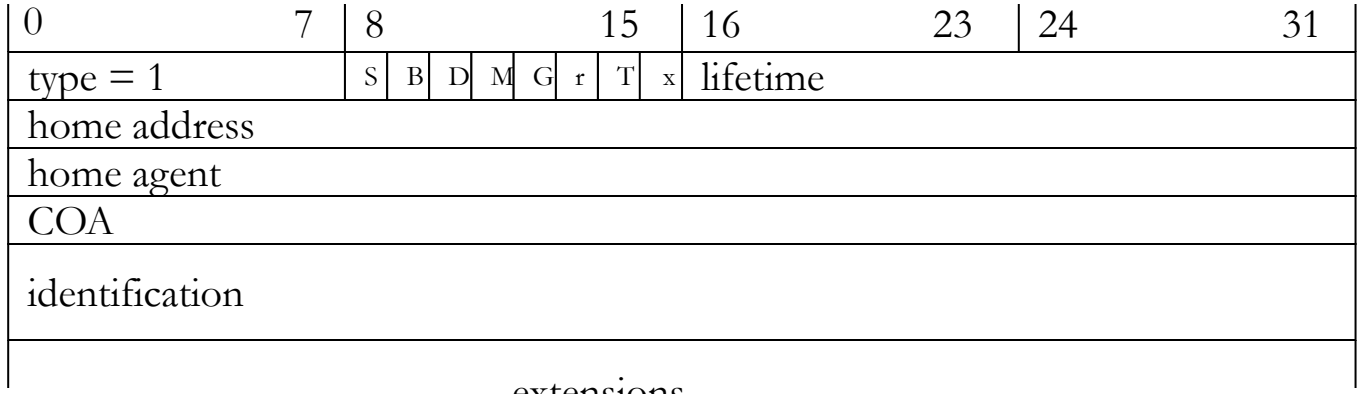


Foreign Agent COA



Co-located COA

REGISTRATION REQUEST



S: simultaneous bindings (If MN wants HA to retain prior mobility bindings)
B: broadcast datagrams (MN receives broadcast msgs which are broadcasted in Home network)
D: decapsulation by MN (Colocated COA→ Decapsulation at MN)
M: mininal encapsulation
G: GR Encapsulation
r: =0, ignored
T: reverse tunneling requested
x: =0, ignored
Identification : 64 bit id generated by MN to identify a request and match it with registration replies.

REGISTRATION REPLY

0 7	8 15	16 31
type = 3	code	lifetime
home address		
home agent		
identification		
extensions . . .		

Example codes:

registration successful

0 registration accepted

1 registration accepted, but simultaneous mobility bindings unsupported

registration denied by FA

65 administratively prohibited

66 insufficient resources

67 mobile node failed authentication

68 home agent failed authentication

69 requested Lifetime too long

registration denied by HA

129 administratively prohibited

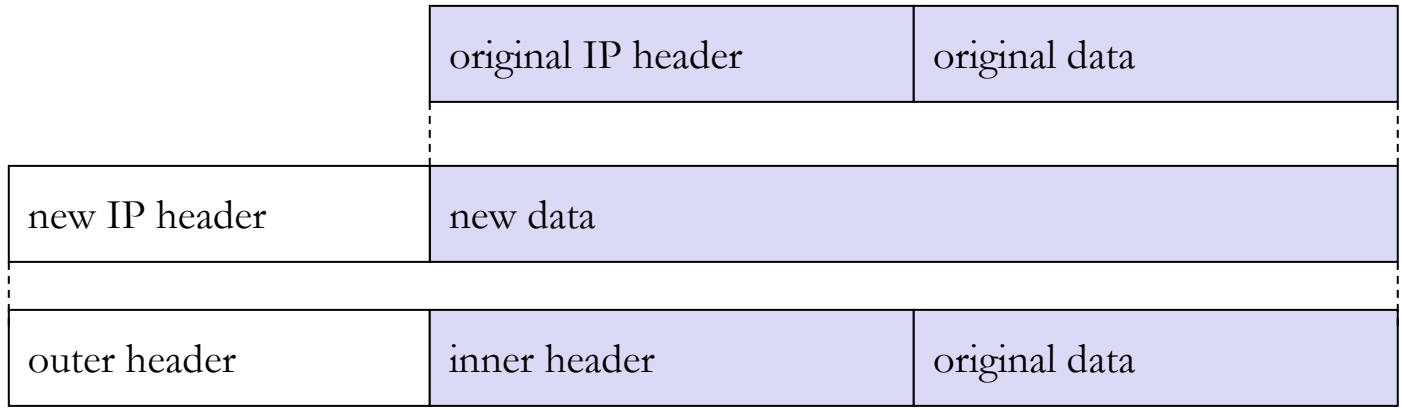
131 mobile node failed authentication

133 registration Identification mismatch

135 too many simultaneous mobility bindings

TUNNELING TO THE COA

- Tunnel establishes a virtual pipe for data packets between a tunnel entry and a tunnel end point.
- Tunneling→ sending a pkt through a tunnel is achieved by encapsulation
- Encapsulation → Taking a pkt (data + header), putting it into the data part of a new pkt.
- Decapsulation



ENCAPSULATION

- e.g. IPv6 in IPv4 (6Bone), Multicast in Unicast (Mbone)
- here: e.g. IP-in-IP-encapsulation, minimal encapsulation or GRE (Generic Record Encapsulation)
- IP-in-IP
  - Tunnel between HA and COA

ver.	IHL	DS (TOS)	length	
IP identification			flags	fragment offset
TTL		*IP-in-IP (4)*	IP checksum	
IP address of HA				
Care-of address COA				
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				

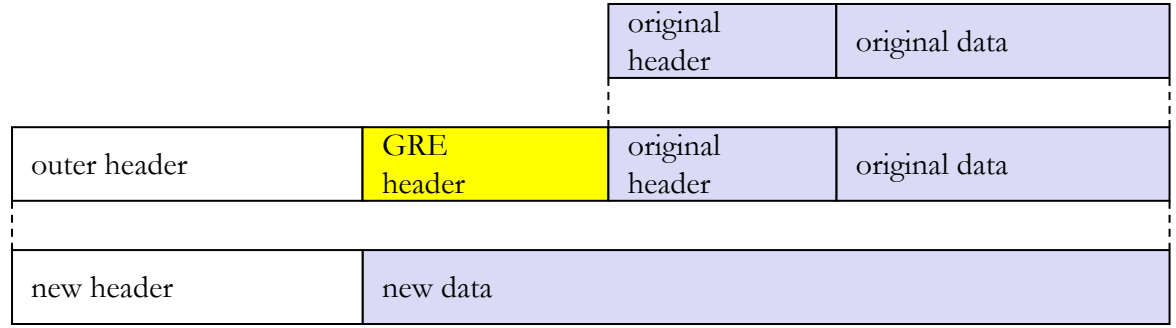
ENCAPSULATION

- Minimal encapsulation (optional)
  - avoids repetition of identical fields
  - e.g. TTL, IHL, version, DS (RFC 2474, old: TOS)
  - only applicable for non fragmented packets, no space left for fragment identification

ver.	IHL	DS (TOS)	length		
IP identification			flags	fragment offset	
TTL		*min. encap (55)*	IP checksum		
IP address of HA					
care-of address COA					
lay. 4 protoc.	S	reserved	IP checksum		
IP address of MN					
original sender IP address (if S=1)					
TCP/UDP/ ... payload					

ENCAPSULATION

- Generic Routing Encapsulation



RFC 1701

ver.	IHL	DS (TOS)	length					
IP identification			flags	fragment offset				
TTL		*GRE(47)*	IP checksum					
IP address of HA								
Care-of address 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								

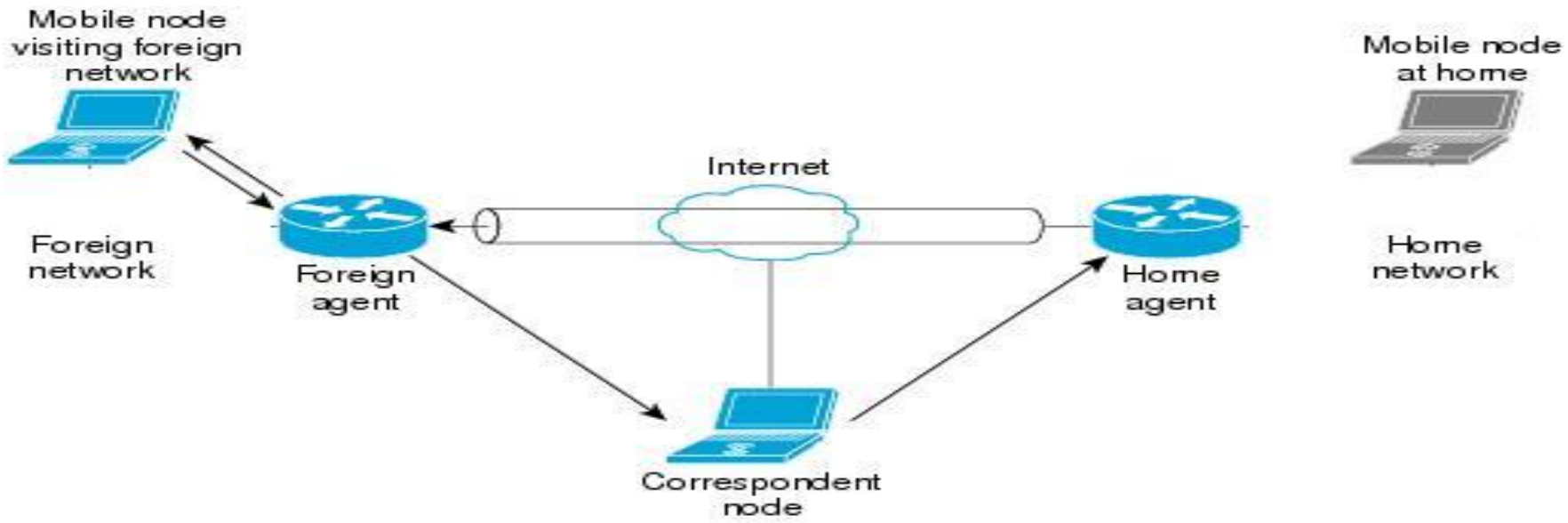
RFC 2784 (updated by 2890)

C	reserved0	ver.	protocol
checksum (optional)			reserved1 (=0)

C: Valid checksum
R:Routing fields are present
K: valid key for authentication
S:Sequence number is present
s: strict source routing
rec: recursion control (no. of recursive encapsulation allowed)
res: 0
ver: 0

ROUTE OPTIMIZATION

- Triangular Routing (CN – HA, HA – COA/MN, MN – CN)
- 3 steps to optimize the route
  - Direct notification to CN
  - Direct tunnelling between CN and MN
  - Binding cache maintained at CN

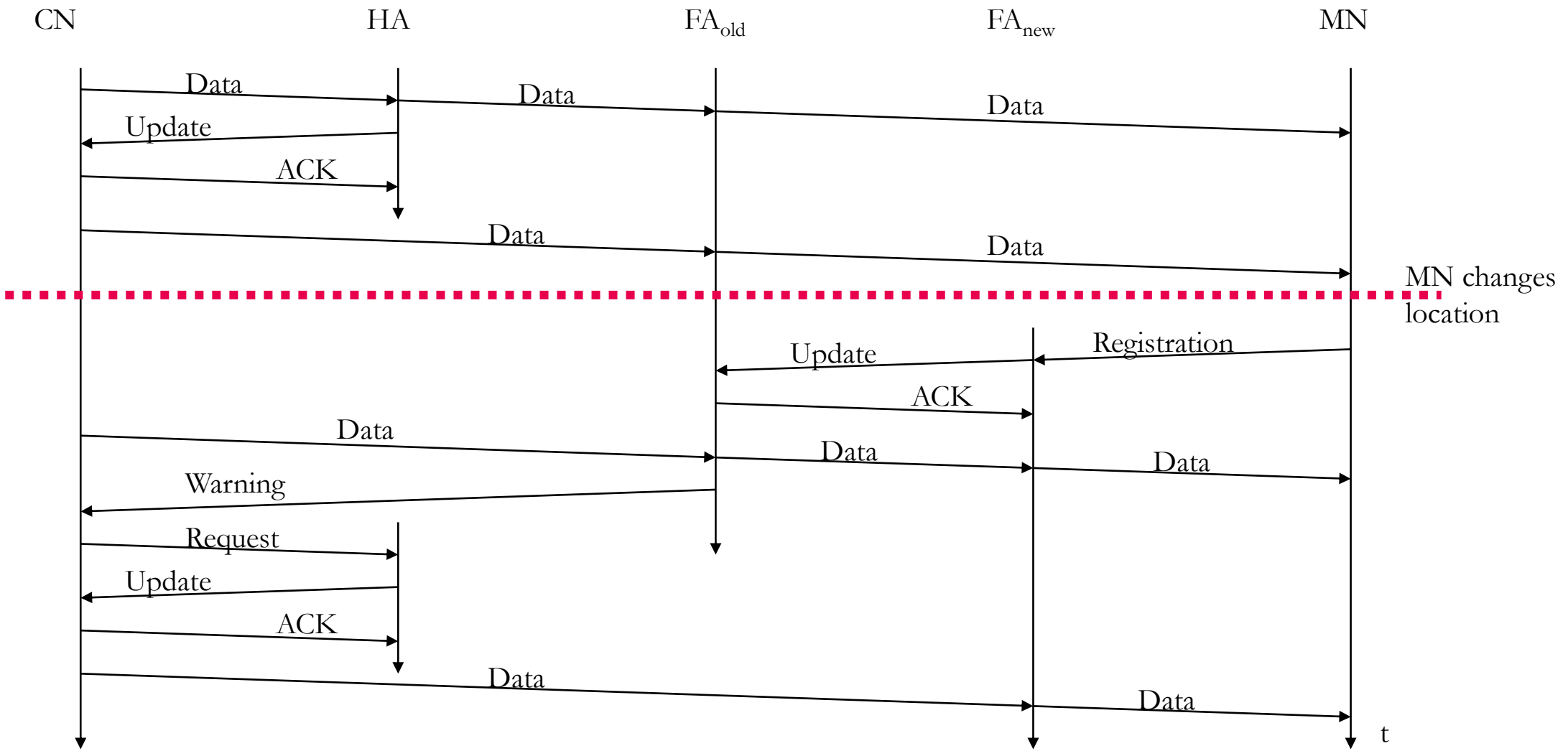


ROUTE OPTIMIZATION

- Binding → the association of Home address (IP of MN) with COA

Message type	*Description*
1. Binding request	If a node wants to know the current location of a mobile node (MN), it sends a request to home agent (HA).
2. Binding acknowledgement	On request, the node will return an acknowledgement message after getting the binding update message.
3. Binding update	This is a message sent by HA to CN mentioning the correct location of MN. The message contains the fixed IP address of the mobile node and the care-of-address. The binding update can request for an acknowledgement.
4. Binding warning	If a node decapsulates a packet for a mobile node (MN), but it is not the current foreign agent (FA), then this node sends a binding warning to the home agent (HA) of the mobile node (MN).

ROUTE OPTIMIZATION



SUMMARY

- Key mechanisms in Mobile IP
  - Agent Discovery
  - Registration
  - Tunneling and Encapsulation
- Route Optimization
- DHCP
  - Different messages and steps in DHCP

TEST YOUR KNOWLEDGE

- Which Internet Protocol (IP) number is used by a computer to send a message back to itself?
  - 0.0.0.0
  - 127.0.0.1
  - 255.255.255.255
- Which TCP/IP model layer does DHCP work at?

REFERENCES

- Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007.
- Prasant Kumar Pattnaik, Rajib Mall, “Fundamentals of Mobile Computing”, PHI Learning Pvt. Ltd, New Delhi – 2012.

DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

Dr. A. Beulah

AP/CSE

Purpose of DHCP

- DHCP automates the assignment of
  - Unique IP addresses
  - Subnet masks
  - Default gateways
  - Other IP parameters to individual computers and devices on the network.
- DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

Without DHCP Servers

- Network Administrators would be over-worked, and underpaid.
- The desktop client would be responsible for assigning a proper IP address within the appropriate range.
- Two different clients may end up claiming the same IP address.
- Desktop clients will need too much knowledge about IP address ranges, etc. This for example could lead to problems when the network ranges change.
- Will make it difficult to move a computer from one subnet to another.

Preliminary

- (DHCP) Message → DHCP-PDU (A-PDU)
- Client → DHCP Client
- Server → DHCP Server
- Well-known port numbers
  - DHCP Server → UDP port 67
  - DHCP Client → UDP port 68
- Broadcast and Unicast used for PDU's in both directions

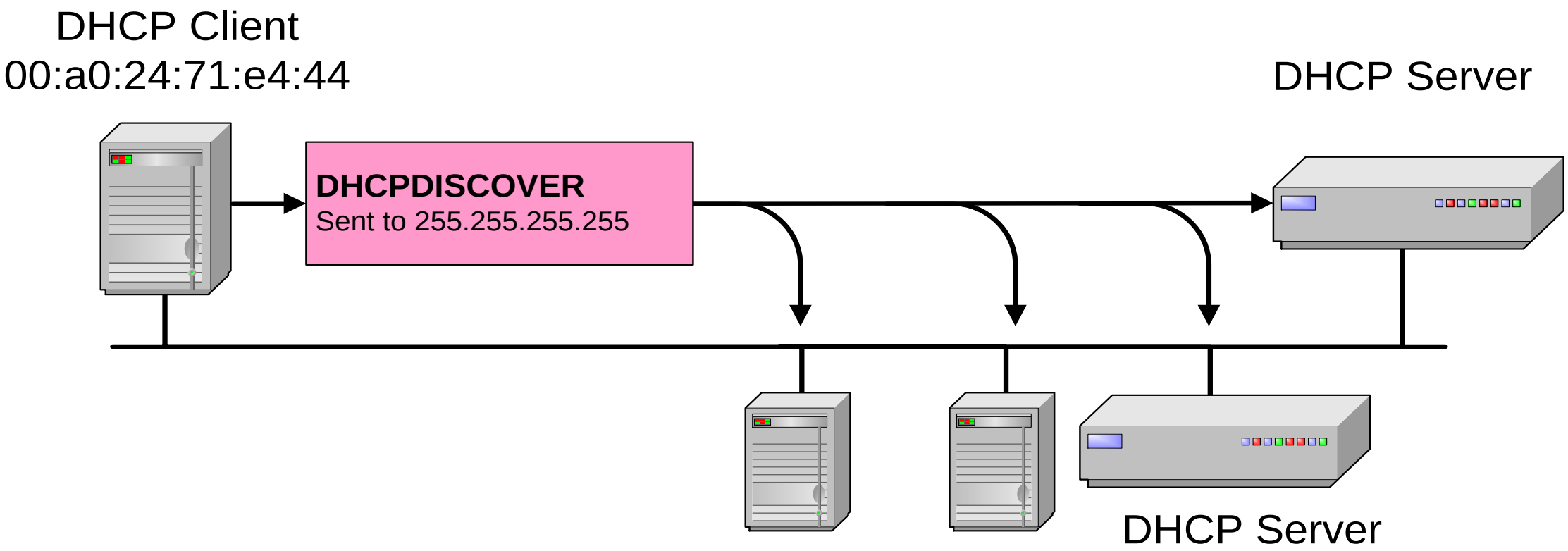
Phases of DHCP

- Discover Phase
- Offer Phase
- Request Phase
- Acknowledgement Phase
- Release Phase

Discover Phase

- When a DHCP configured devices connect to the network, the client sends a broadcast request (called a DISCOVER or DHCPDISCOVER) looking for a DHCP server to answer.
- The router directs the DHCPDISCOVER packet to the correct DHCP server.
- The DHCP server receives the DHCPDISCOVER packet.
- Based up on availability the server determines an appropriate IP address to give to the client.

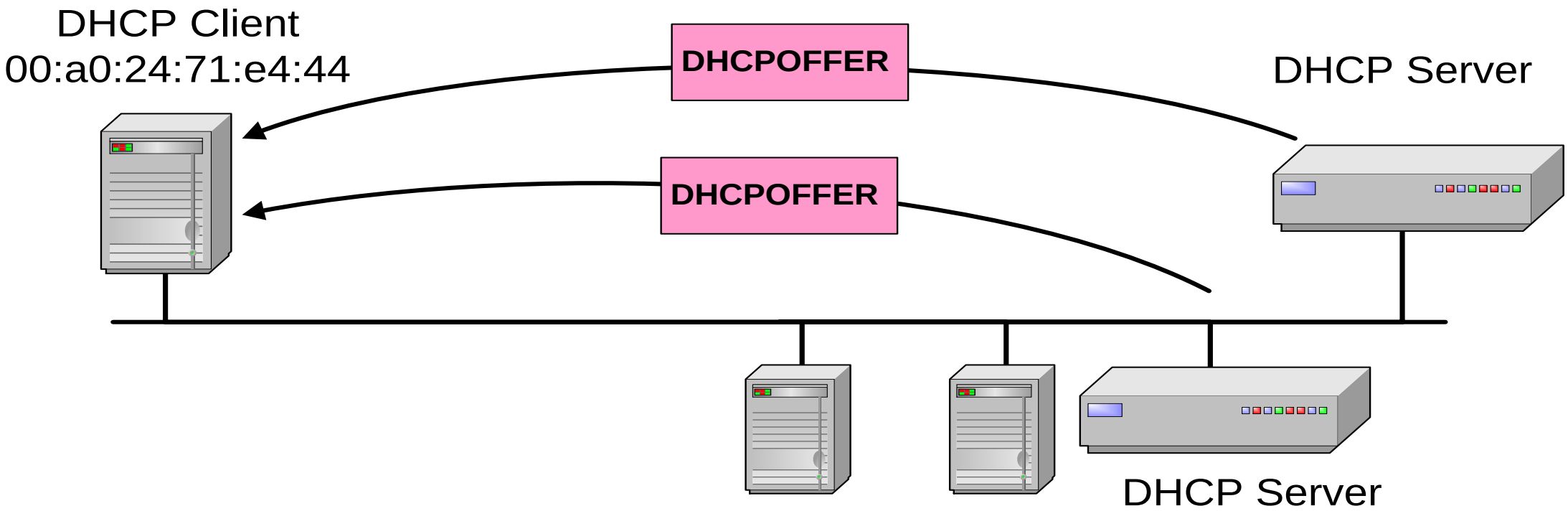
Discover Phase



Offer Phase

- The server temporarily reserves the IP address and response the client an Offer (DHCPOFFER) packet with the address information
- The server also configures the clients DNS servers, WINS servers, NTP servers, etc.

Offer Phase


DHCP Client
00:a0:24:71:e4:44
DHCPOFFER
DHCP Server
DHCPOFFER
DHCP Server

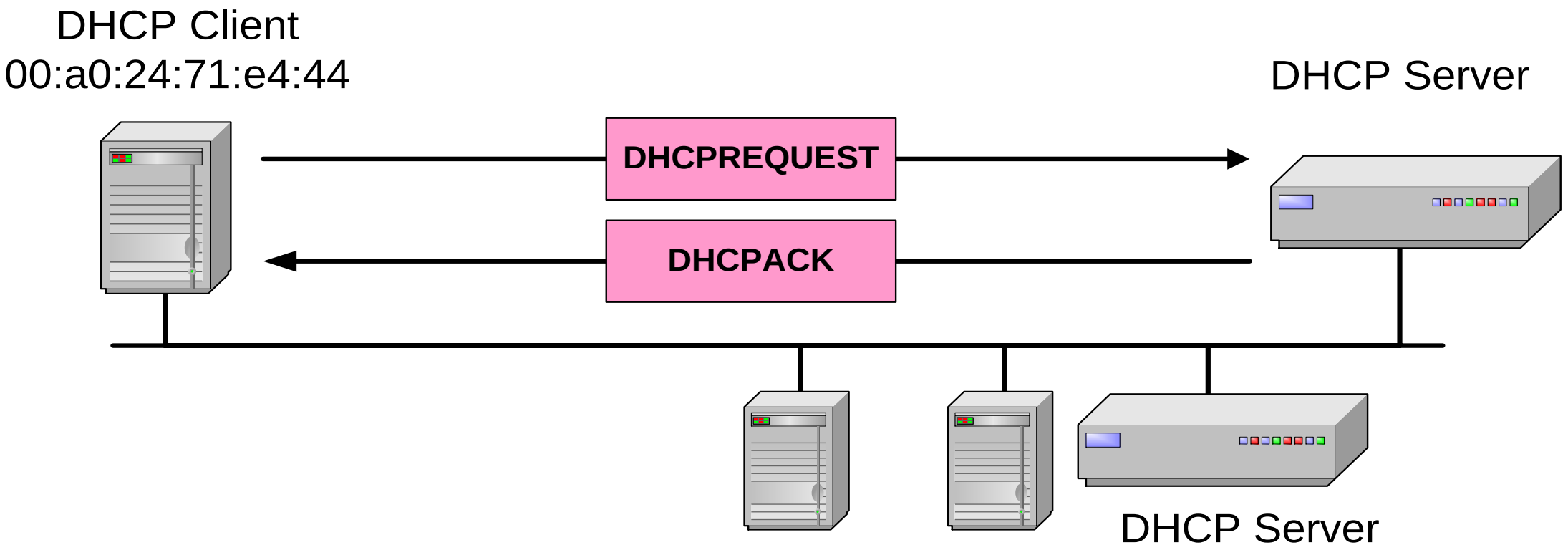
Request Phase

- The client sends a Request (DHCP REQUEST) packet, letting the DHCP server know that it intends to use that address.

Acknowledgement Phase

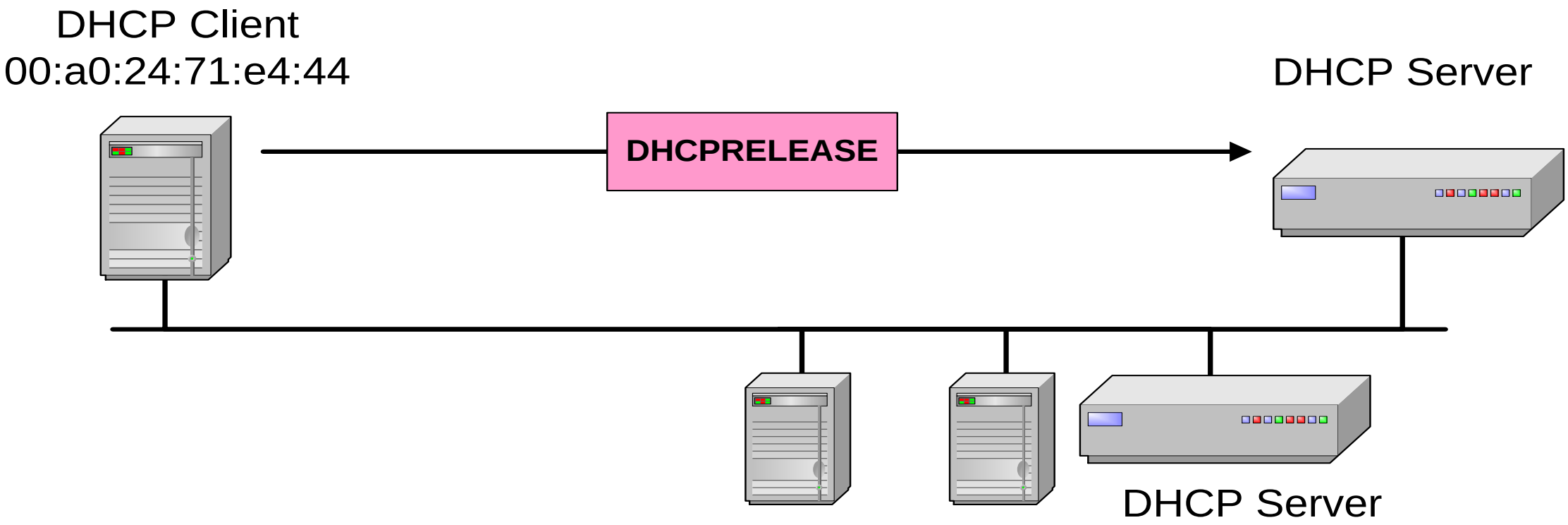
- The Server sends an Acknowledgement (DHCPACK) packet confirming client has been given a lease on the address
- A DHCP Lease is the amount of time a DHCP server grants the client permission to use a particular IP address.
- The Administrator of the DHCP server can set this.

Request and Acknowledgement Phase

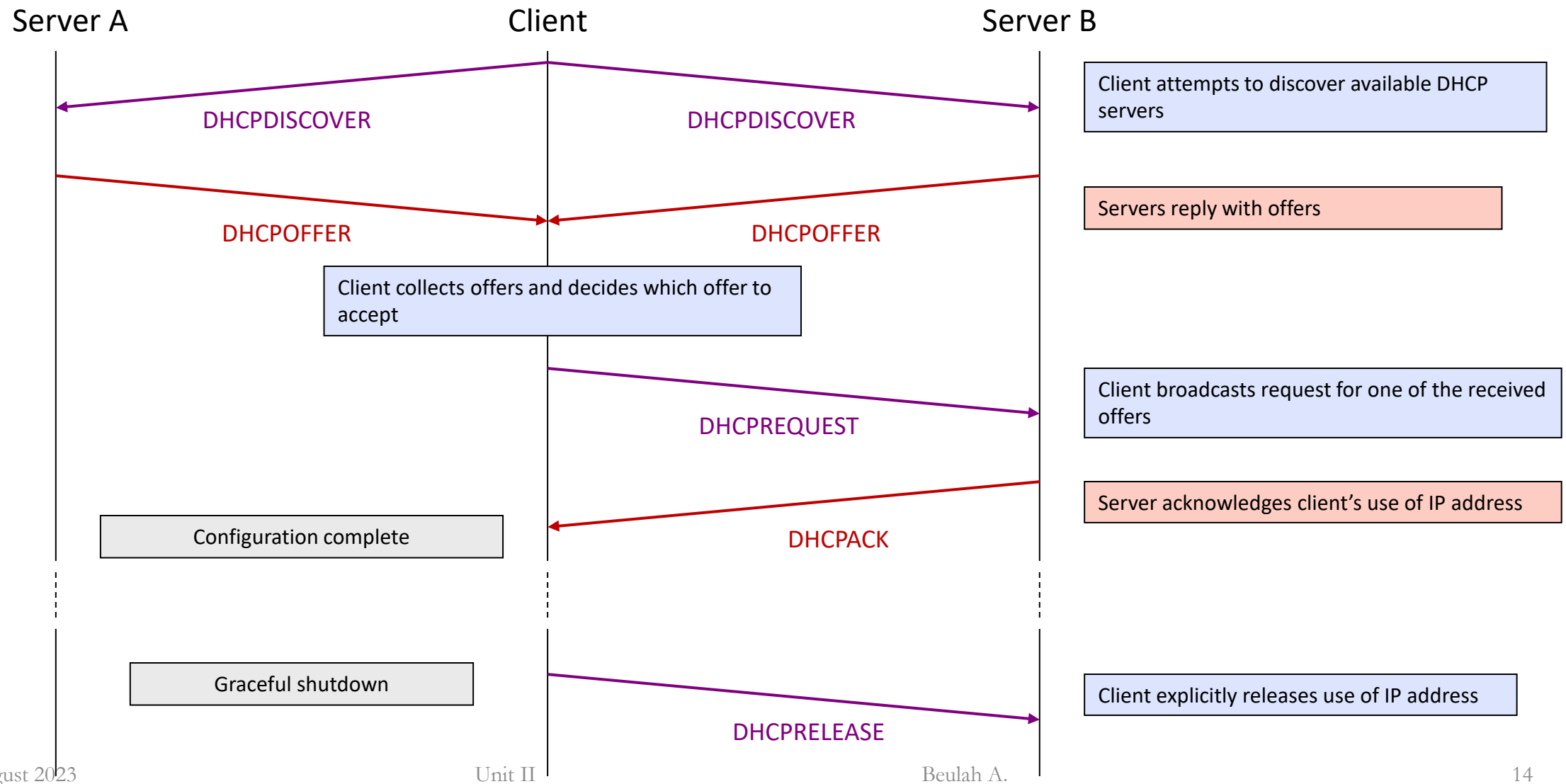


Release Phase

- The DHCP client releases the IP address



DHCP - Protocol Mechanisms



DHCP Message Types

DHCP Message	Use
DHCPDISCOVER	Client broadcast to locate available servers
DHCPOFFER	Server to client response offering configuration parameters
DHCPREQUEST	Client broadcast requesting offered parameters
DHCPDECLINE	Client to server notification that IP address is in use
DHCPACK	Server to client response confirming a request
DHCPNAK	Server to client response denying a request
DHCPRELEASE	Client to server request to relinquish IP address
DHCPINFORM	Client to server request for configuration parameters

Ways of allocating IP Addresses

- **Manual allocation:** (static IP addresses): The server's administrator creates a configuration for the server that includes the MAC address and IP address of each DHCP client that will be able to get an address.
- **Automatic allocation:** The server's administrator creates a configuration for the server that includes only IP addresses, which it gives out to clients. An IP address, once associated with a MAC address, is permanently associated with it until the server's administrator intervenes.
- **Dynamic allocation**: Like automatic allocation except that the server will track leases and give IP addresses whose lease has expired to other DHCP clients.

Test your Knowledge

- Explain how DHCP can be used when the size of the block assigned to an organization is less than the number of hosts in the organization.

Summary

- Dynamic Host Configuration Protocol (DHCP)
  - Its working Principle
  - Different messages

References

Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007.

MANET – DESIGN ISSUES

Dr. A. Beulah

AP/CSE

Design Issues

- Network Size and Node Density
  - 2 important parameters
  - Network size → Geographical coverage area of the network
  - Node Density → No. Of nodes per unit geographical area
  - Clustering is essential to keep the communication overheads low
- Connectivity
  - Connectivity of a node→ No. Of neighbours it has (ie. Within the transmission range of the node)
  - Connectivity also refers to the link between two nodes.
  - Link capacity → Bandwidth of the link.
  - The no. of neighbours and the capacities of the links to different neighbours vary significantly.

Design Issues

- Topology
  - Denotes the connectivity among various nodes of the network
  - Mobility of nodes affect the network topology
  - Due to mobility , new links are formed and some links are dissolved
  - Nodes can also become inoperative due to discharged batteries, hardware failures which causes change in the topology
- User Traffic
  - A traffic in network can be of various types

1. Bursty Traffic
2. Large packets sent periodically

  - Combination of the above 2 types of traffic

Design Issues

- Operational Environment
  - Urban, Rural and Maritime
  - Node density and mobility values may differ in operational environment
- Energy Constraint
  - Nodes in MANET acts as routers.
  - Therefore all nodes has an extra overhead to perform as a router which consumes more energy.

Test your Knowledge

- Explain how DHCP can be used when the size of the block assigned to an organization is less than the number of hosts in the organization.

References

Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007.

MANET – ROUTING

Dr. A. Beulah

AP/CSE

Routing MANET vs Traditional N/ws

- 3 important differences
- MANET
  - All nodes act as routers
  - Dynamic Topology (Routing Table expire quickly)
  - IP address encapsulated in the subnet structure does not work

- Traditional N/ws
  - Nodes do not participate in routing
  - Static Topology
  - IP addressing scheme

Types of Communications

- Unicast
- Multicast
- Broadcast
  - Unrestricted broadcast communication can choke MANET.
  - Therefore applications usually do not use broadcast communication.

Unicast MANET Routing Protocols

- Classification of Unicast MANET Routing Protocols
  - Proactive Protocols (Table Driven)
  - Reactive Protocols (On - Demand)
  - Hybrid Routing Protocols

Proactive Protocols (Table Driven)

- Each node maintains routing table (Information about the routes to every other node in the network)
- The node itself finds the shortest path to reach the destination.
- Periodic Updation happens.
- As topology changes frequently, large number of control messages are used.
- More bandwidth is used by control messages.
- This protocol not suitable for large networks as the routing table will be large. (Communication overhead, Memory overhead)
- DSDV – Destination Sequenced Distance Vector Routing

Reactive Protocols (On - Demand)

- No up-to-date routing table maintenance.
- New routes are discovered only when required.
  - ie Routing table also updated on demand.
- Uses flooding technique to determine the route
- Reduces the overhead incurred by proactive protocols
- DSR – Dynamic Source Routing
- AODV – Ad-hoc On-demand Distance Vector Routing

Hybrid Routing Protocols

- Have the characteristics of both Proactive and Reactive protocols.
- Combine the good features of both.
- Consider a small Geographical area as a zone
- Routing within a zone is proactive (Table driven)
- Destination outside a zone is reactive (on-demand)
- ZRP – Zone Routing Protocol

Features of MANET Routing Protocols

- Identification of network topology after changes due to mobility
- Topology maintenance
- Transmission scheduling and channel assignment

Popular MANET Routing Protocols

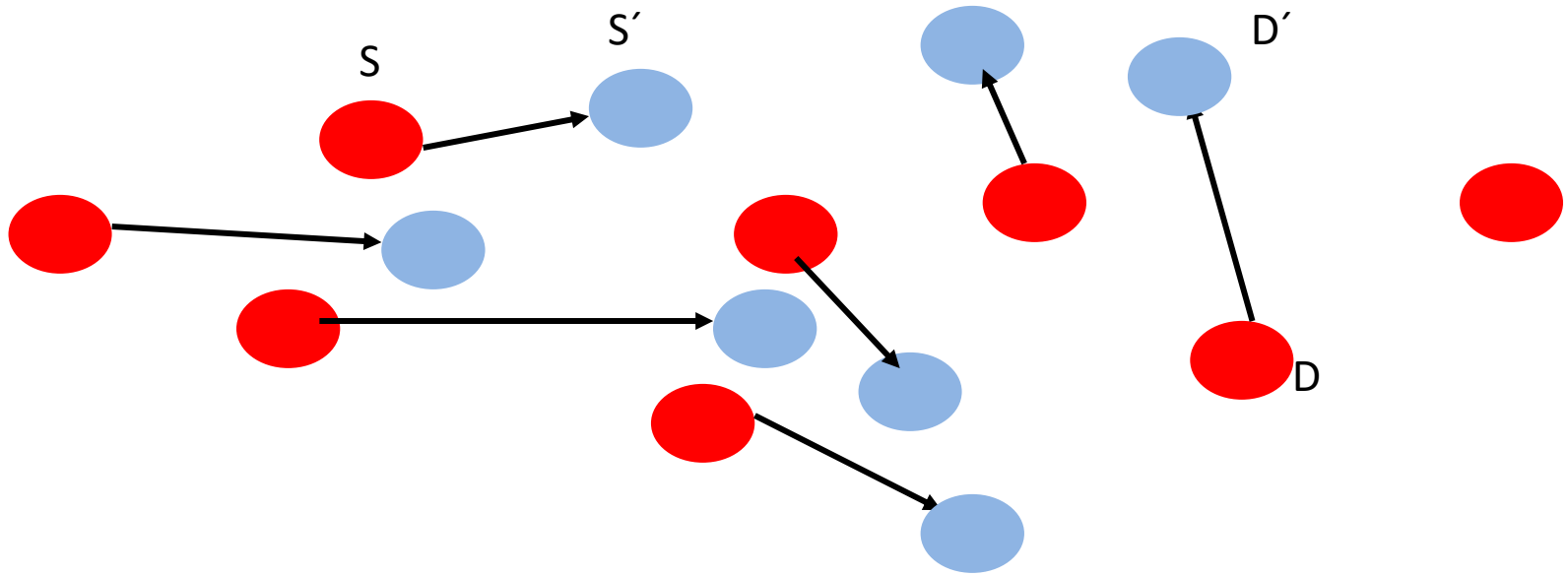
- Unicast Routing Protocols
  - DSDV – Destination Sequenced Distance Vector Routing
  - DSR – Dynamic Source Routing
  - AODV – Ad-hoc On-demand Distance Vector Routing
  - ZRP – Zone Routing Protocol
- Multicast Routing Protocols
  - Tree - Based Protocol
  - Mesh - Based Protocol

Destination-Sequenced Distance-Vector (DSDV)

- Each node maintains a routing table which stores
  - Next hop, cost metric towards each destination
  - A sequence number that is created by each node
- Each node periodically forwards routing table to its neighbors
  - Each node increments and appends its sequence number when sending its local routing table
- Each route is tagged with a sequence number; routes with greater sequence numbers are preferred
- Each node advertises a monotonically increasing even sequence number for itself
- When a node finds that a route is broken, it increments the sequence number of the route and advertises it with infinite metric.

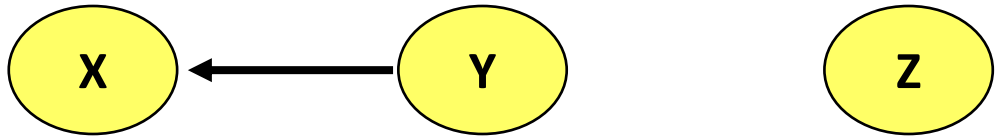
DSDV Cont…

- Consider a source node S and a destination node D.
- Each routing table entry in S is tagged with a sequence number that is originated by the destination node.
- For example, the entry for D is tagged with a sequence number that S received from D (may be through other nodes).



DSDV Cont…

- When X receives information from Y about a route to Z
  - Let destination sequence number for Z at X be S(X), S(Y) is sent from Y



  - If S(X) > S(Y), then X ignores the routing information received from Y
  - If S(X) = S(Y), and cost of going through Y is smaller than the 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, and S(X) is updated to equal S(Y)

DSDV Cont…

- The nodes perform routing in the same way as the Distributed Bellman-Ford algorithm.
- Packets are transmitted between the nodes using routing tables stored at each node.
- Each routing table lists all available destinations and the number of hops to each destination.
- Each node knows which of its neighbours leads to the shortest path to the destination.

DSDV Cont…

- The consistency of the routing tables should be maintained in a dynamically varying topology.
- Each node periodically transmits updates. This is done by each node when significant new information is available.
- Do not assume any clock synchronization among the mobile nodes.
- The route-update messages indicate which nodes are accessible from each node and the number of hops to reach them.
- Consider the hop-count as the distance between two nodes.
- However, the DSDV protocol can be modified for other metrics as well.

DSDV Cont…

- A neighbour in turn checks the best route from its own table and forwards the message to its appropriate neighbour.

- There are two issues in this protocol :
  - How to maintain the local routing tables
  - How to collect enough information for maintaining the local routing tables

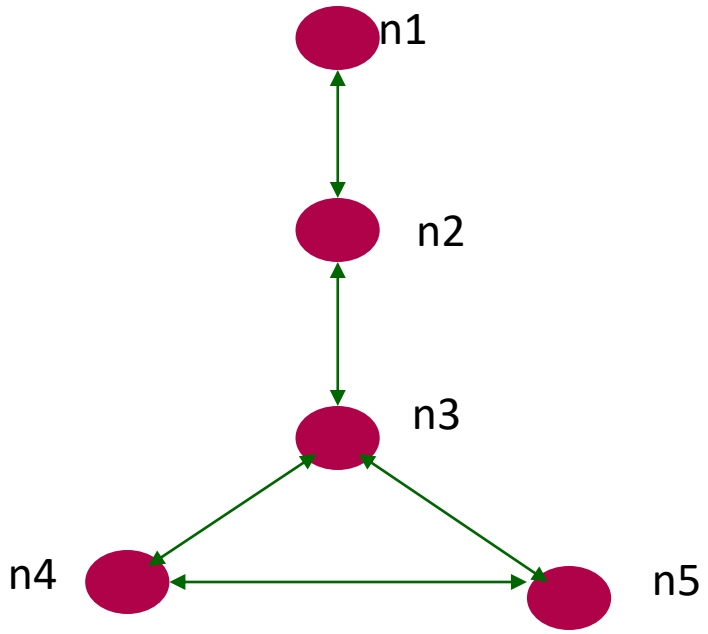
Route Advertisements

- The DSDV protocol requires each mobile node to advertise its own routing table to all of its current neighbours.
- Since the nodes are mobile, the entries can change dynamically over time.
- The route advertisements should be made whenever there is any change in the neighbourhood or periodically.
- Each mobile node agrees to forward route advertising messages from other mobile nodes.
- This forwarding is necessary to send the advertisement messages all over the network.
- In other words, route advertisement messages help mobile nodes to get an overall picture of the topology of the network.

Route Advertisements

- The route advertisement broadcast by each mobile node has the following information for each new route :
  - The destination's address
  - The number of hops to the destination
  - The sequence number of the information received from that destination. This is the original sequence number assigned by the destination.

An Example of Route Update

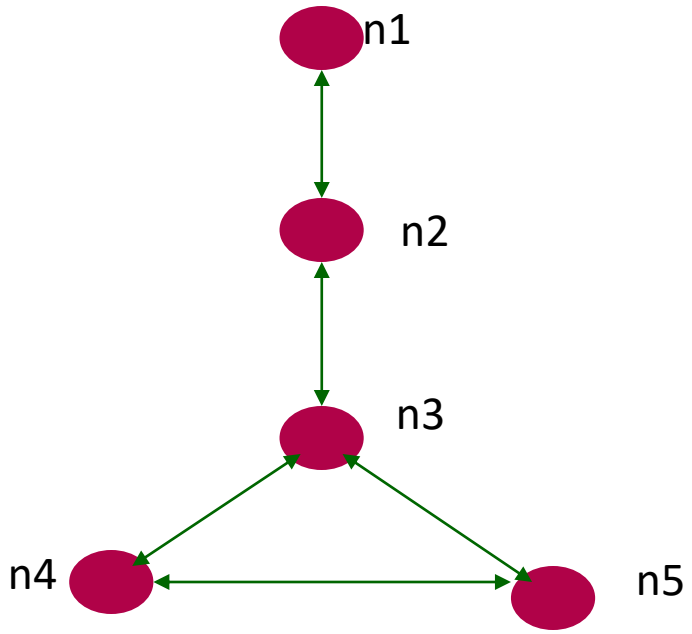


- At the start, each node gets route updates only from its neighbour.
- For n4, the distances to the other nodes are :

  n5=1, n3=1, n2= ∞

  n1 = ∞
- All nodes broadcast with a sequence number 1

An Example of Route Update

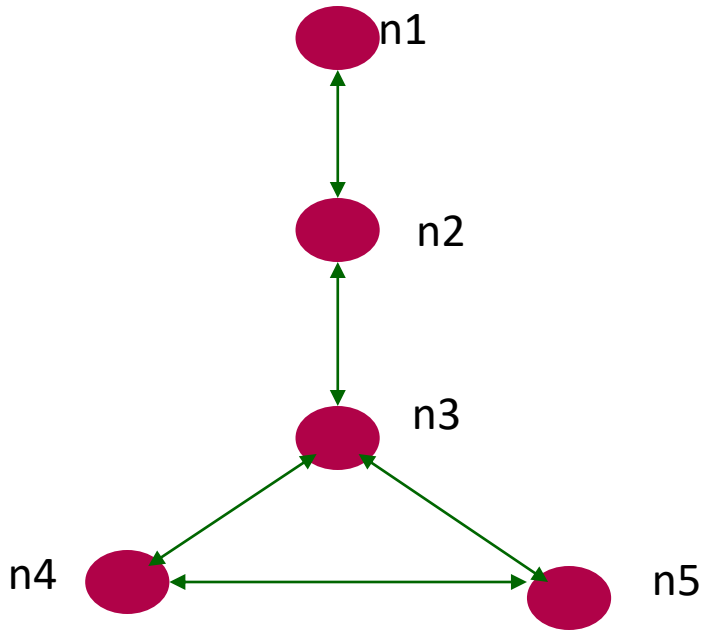


- After this, nodes forward messages that they have received earlier.
- n2 forwards RT to n3 and n3 to n4
- For n4, the distances are now

  n5=1, n3=1, n2=2, n1= ∞

All messages have sequence number 1

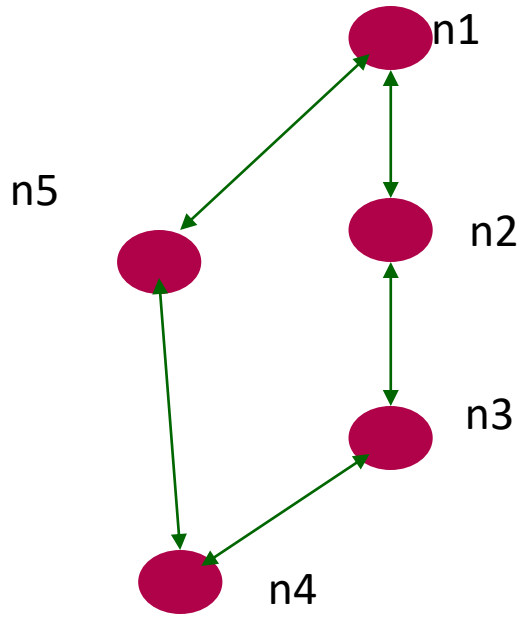
An Example of Route Update



- Finally, after second round of forwarding, n4 gets the following distances :

n5=1, n3=1, n2=2, n1=3

An Example of Route Update



- Suppose n5 has moved to its new location.
- Also, n5 receives a new message from n1 with a sequence number 2
- This message is forwarded by n5 to n4
- Two distances to n1 in n4
  - Distance 3 with seqence number 1
  - Distance 2 with sequence number 2
- Since the latter message has a more recent sequence number, n4 will update the distance to n1 as 2

Route Advertisements

- For example, a node n may receive two different messages originating from another node m.
- However, node n will forward the most recent message from m to its neighbours.
- Usually n will add one extra hop to the routes in the message received from m as the destination is one more hop away.

Responding to Topology Changes

- Some of the links in a mobile network may be broken when the nodes move.
- A broken link is described by a distance
- When a link to a next hop is broken, any route through that next hop is given a distance
- This is considered as a major change in the routing table and immediately broadcast.
- The number of routing updates may be quite high in a large network with high level of mobility.
- It is necessary to avoid excessive control traffic (route update information) in such networks. Otherwise, the bandwidth will be taken up by control traffic.
- The solution is to broadcast two types of updates.

Responding to Topology Changes

- A full dump carries complete routing table. A node broadcasts a full dump infrequently.
- An incremental dump carries minor changes in the routing table. This information contains changes since the last full dump.
- When the size of an incremental dump becomes too large, a full dump is preferred.

Route Selection Criteria

- When a node i receives incremental dump or full dump from another node j, the following actions are taken :
  - The sequence number of the current dump from j is compared with previous dumps from j
  - If the sequence number is new, the route table at i is updated with this new information.
  - Node i now broadcasts its new route table as an incremental or a full dump.

How frequently should a node broadcast?

- A node decides on a new route based on one of the two criteria :
  - If a route has a smaller metric (distance) to a destination
  - Or, if an update from the destination with a new sequence number has been received.

- However, it is not desirable that a node broadcasts an update every time it has updated its routing table.

Routing Table

Destination	Next	Cost	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.

Advantages of DSDV

- DSDV is an efficient protocol for route discovery.
- Whenever a route to a new destination is required, it already exists at the source.
- Hence, latency for route discovery is very low.
- DSDV also guarantees loop-free paths.

Disadvantages

- However, DSDV needs to send a lot of control messages. These messages are important for maintaining the network topology at each node.
- This may generate high volume of traffic for high-density and highly mobile networks.
- Special care should be taken to reduce the number of control messages.

Dynamic Source Routing

- Split routing into discovering a path and maintaining a path
- Route discovery
  - Only if a route for sending packets to a certain destination is needed and no route is currently available
- Route Maintenance
  - Only while the route is in use one has to make sure that it can be used continuously
- No periodic updates needed!

Dynamic Source Routing

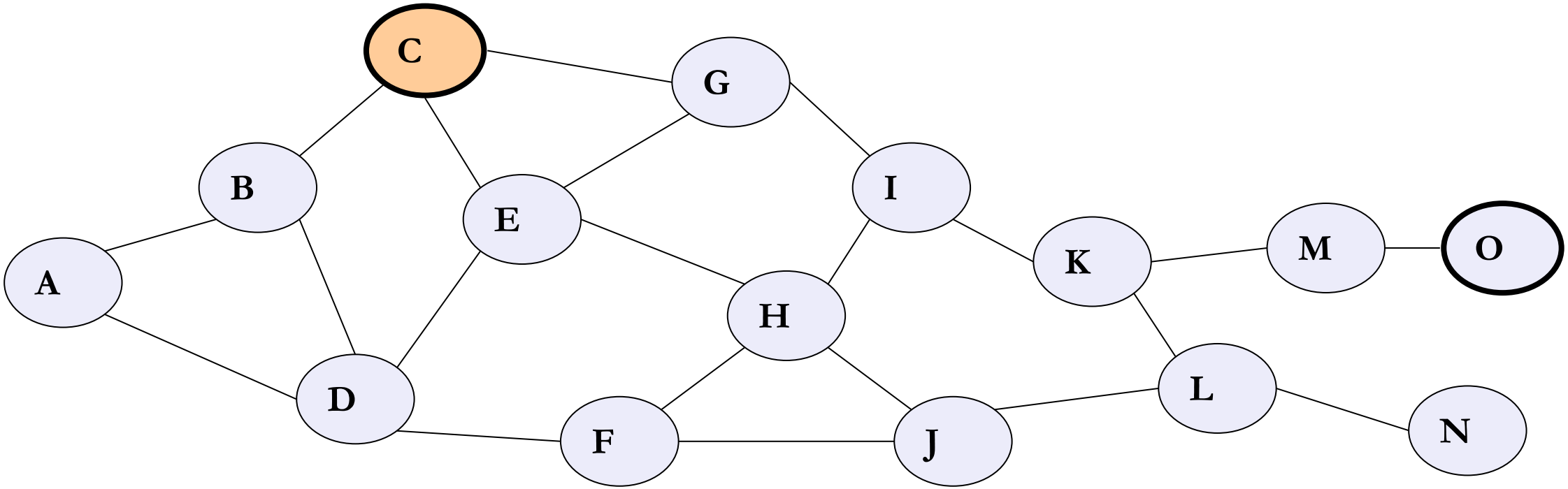
- Route discovery
  - Broadcast a packet with destination address and unique ID
  - If a station receives a broadcast packet
    - If the station is the receiver (i.e., has the correct destination address) then return the packet to the sender (path was collected in the packet)
    - If the packet has already been received earlier (identified via ID) then discard the packet
    - Otherwise, append own address and broadcast packet
  - Sender receives packet with the current path (address list)

Route discovery

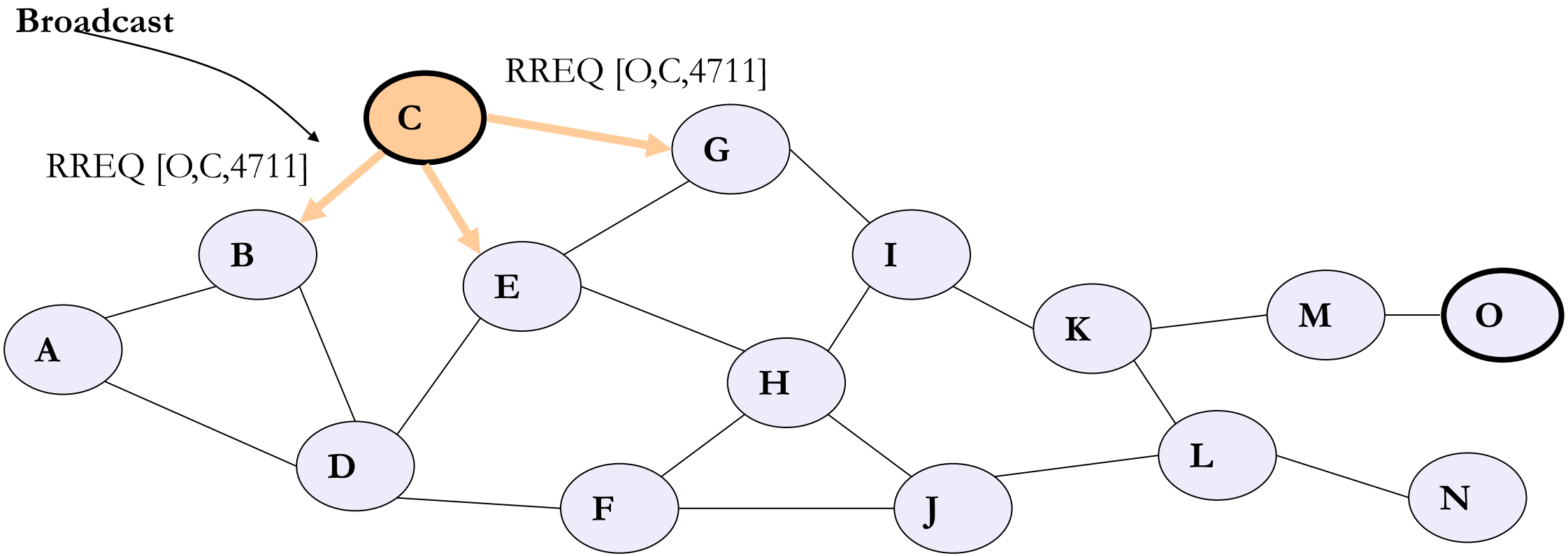
- When node C wants to send a packet to node O, but does not know a route to O, node C initiates a route discovery
- Source node C floods Route Request (RREQ)
- Each node appends own identifier when forwarding RREQ

DSR: Route Discovery

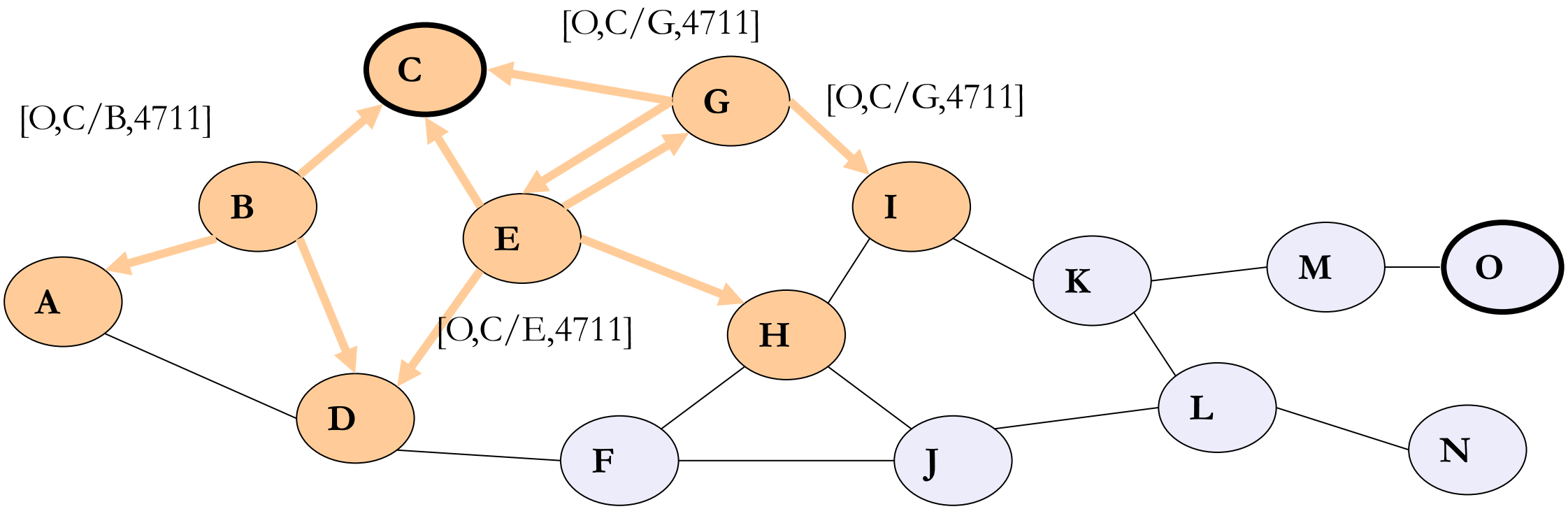
Sending from C to O



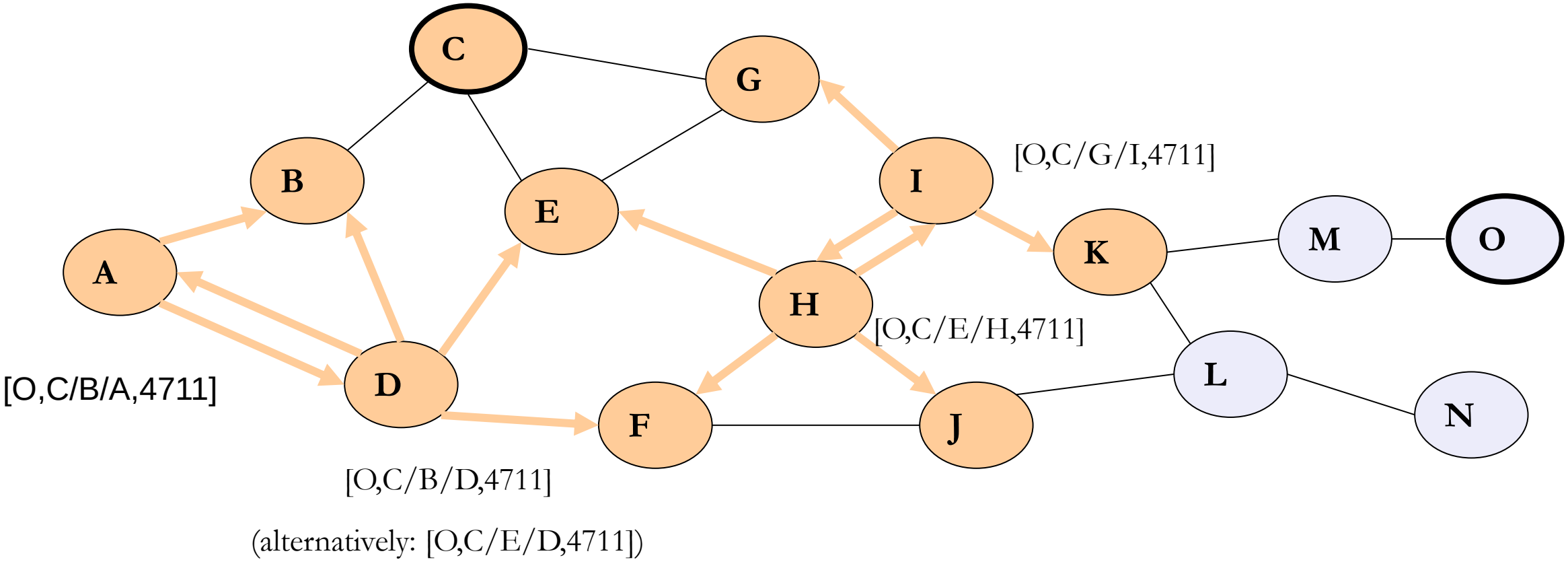
DSR: Route Discovery



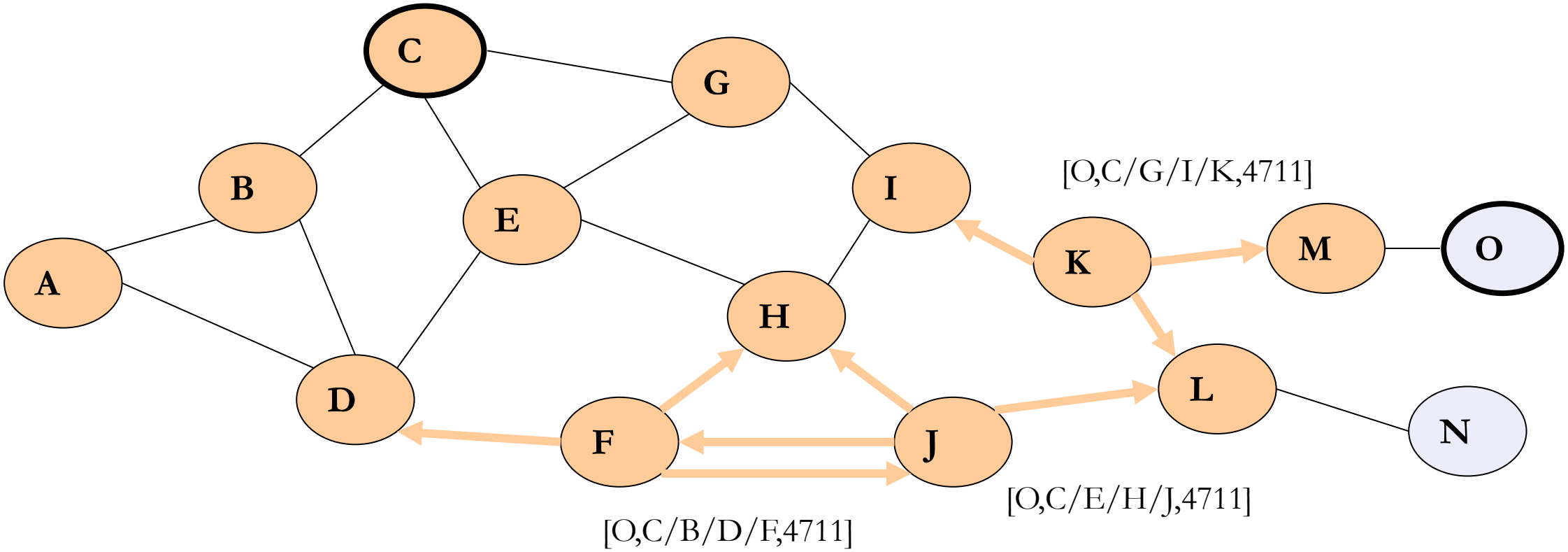
DSR: Route Discovery



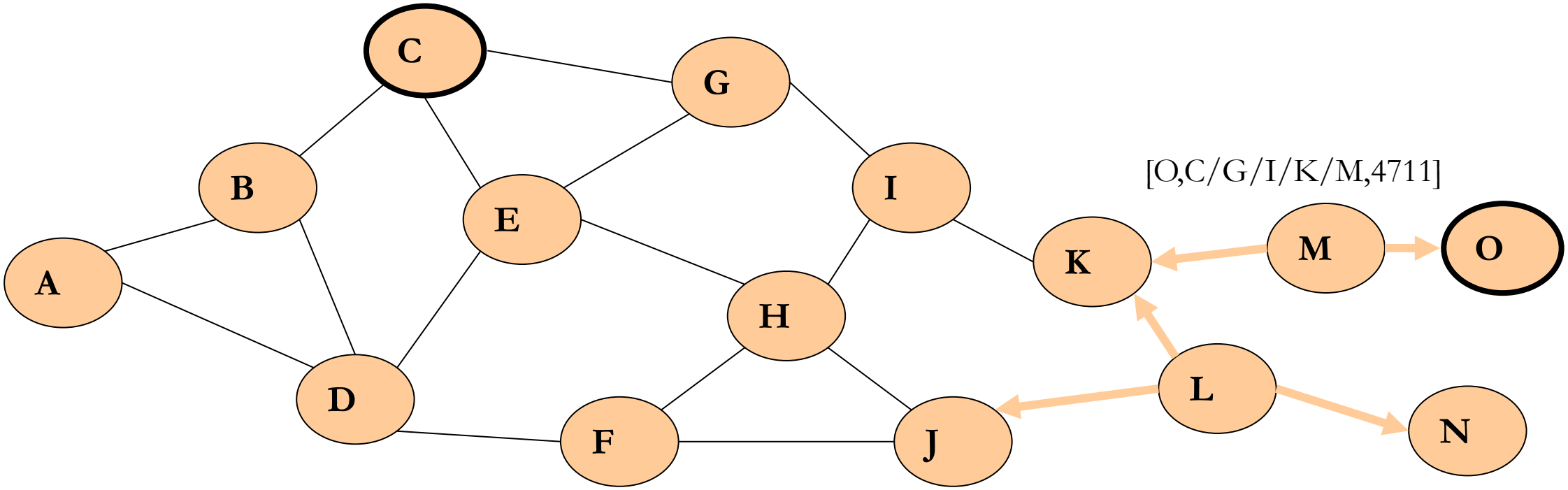
DSR: Route Discovery



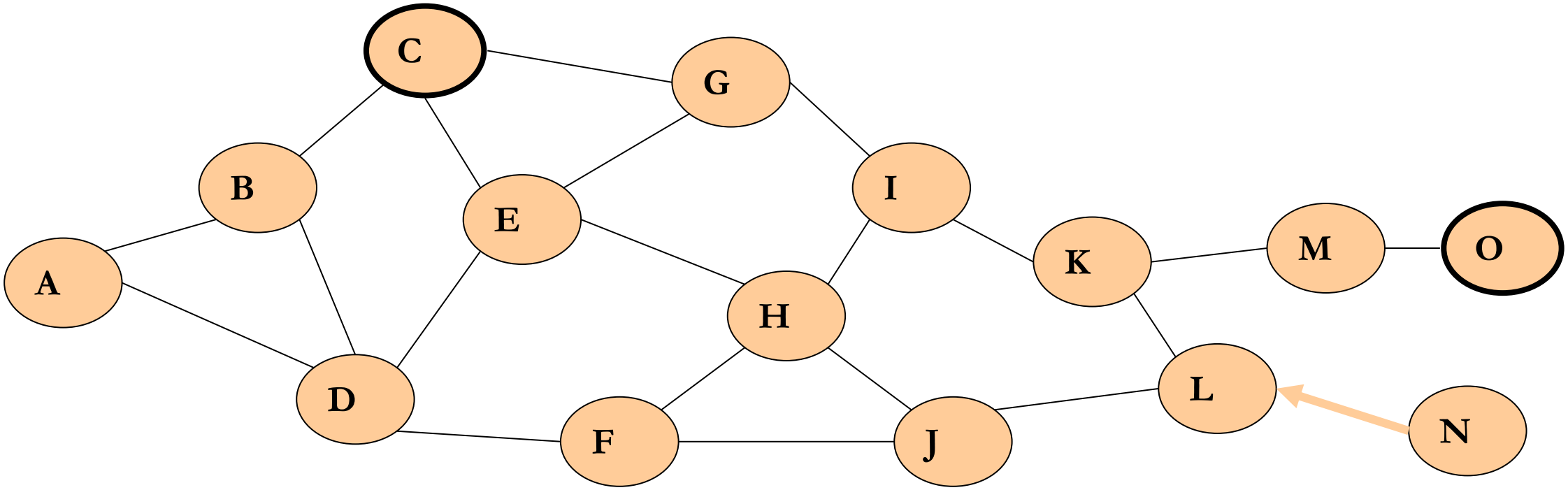
DSR: Route Discovery



DSR: Route Discovery

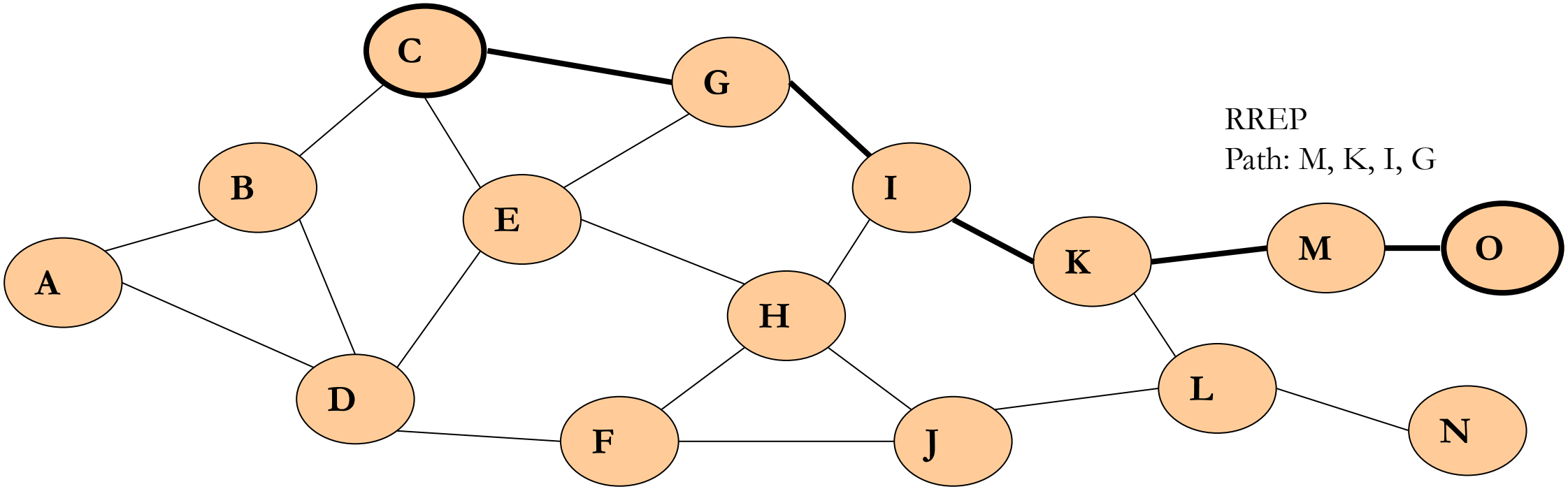


DSR: Route Discovery



[O,C/E/H/J/L/N,4711]

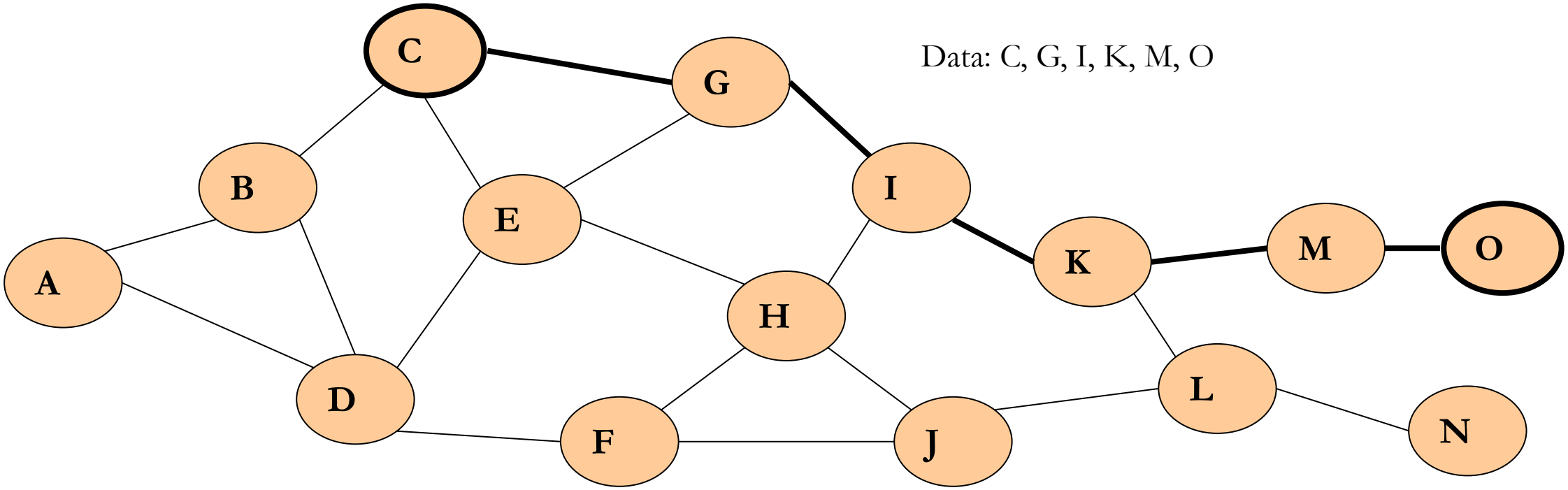
DSR: Route Discovery



Route Discovery

- Node C on receiving RREP, caches the route included in the RREP
- When node C sends a data packet to O, the entire route is included in the packet header
  - hence the name source routing
- Intermediate nodes use the source route included in a packet to determine to whom a packet should be forwarded

DSR: Route Discovery



Data: C, G, I, K, M, O

Dynamic Source Routing

- Optimizations
  - Limit broadcasting if maximum diameter of the network is known
  - Caching of address lists (i.e. paths) with help of passing packets (Route Caching)
    - Stations can use the cached information for path discovery (own paths or paths for other hosts)

Route Caching

- Each node caches a new route it learns by any means
- When node S finds route [C, G, I, K, M, O] to node O, node C also learns route [C, G, I] to node I
- When node K receives Route Request [C, G, I] destined for node, node K learns route [K,I,G,C] to node C
- When node F forwards Route Reply RREP [C, G, I, K, M, O], node I learns route [I, K, M, O] to node O
- A node may also learn a route when it overhears Data
- When node G forwards Data [C, G, I, K, M, O] it learns route [G, I, K, M, O] to node O
- Problem: Stale caches may increase overheads

Dynamic Source Routing

- Route Maintenance
  - After sending a packet
    - Wait for a layer 2 acknowledgement (if applicable)
    - Listen into the medium to detect if other stations forward the packet (if possible)
    - Request an explicit acknowledgement
  - If a station encounters problems it can inform the sender of a packet or look-up a new path locally

DSR : Advantages

- Routes maintained only between nodes who need to communicate
  - reduces overhead of route maintenance
- Route 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

DSR : 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
  - Route Reply *Storm* problem
- Stale caches will lead to increased overhead

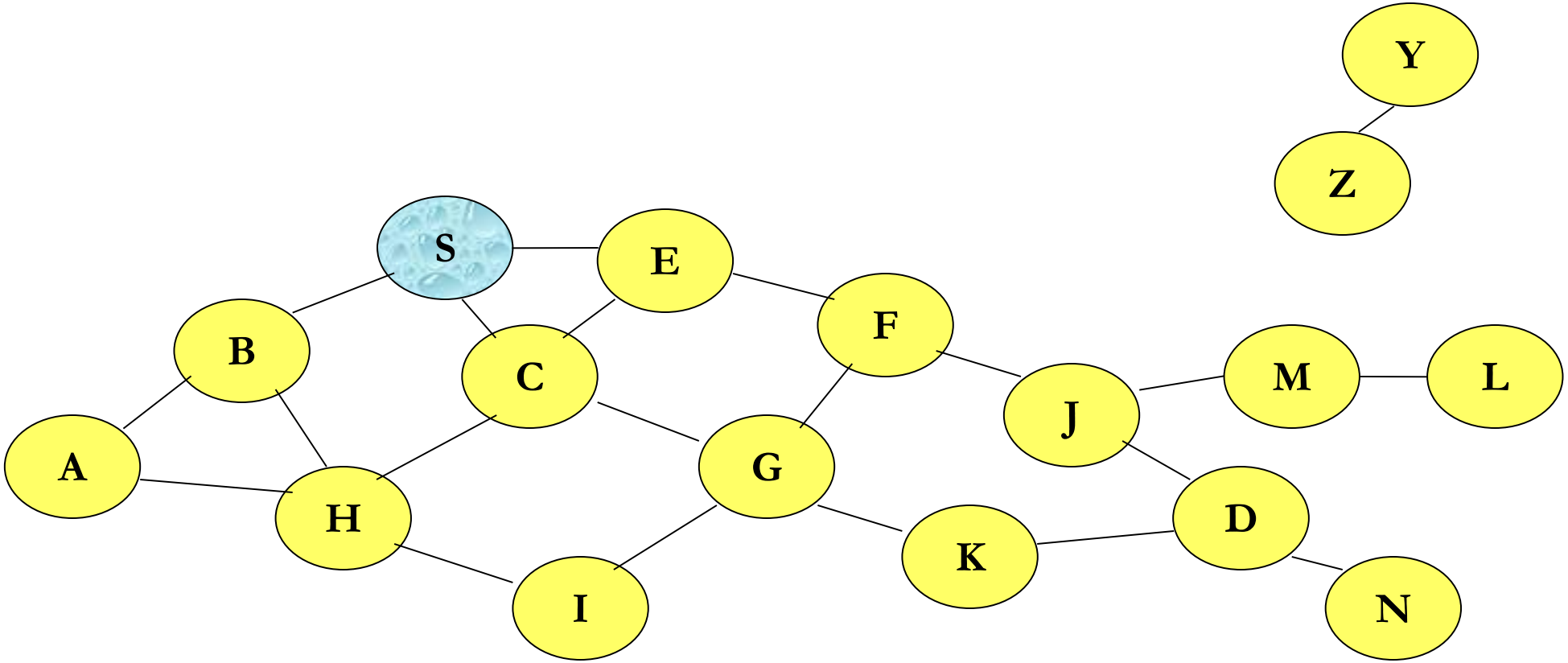
AdHoc On-Demand Distance Vector Routing

- DSR includes source routes in packet headers
- Resulting large headers can sometimes degrade performance
  - Particularly when data contents of a packet are small
- AODV attempts to improve on DSR by maintaining routing tables at the nodes, so that data packets do not have to contain routes
- AODV retains the desirable feature of DSR that routes are maintained only between nodes which need to communicate

AdHoc On-Demand Distance Vector Routing

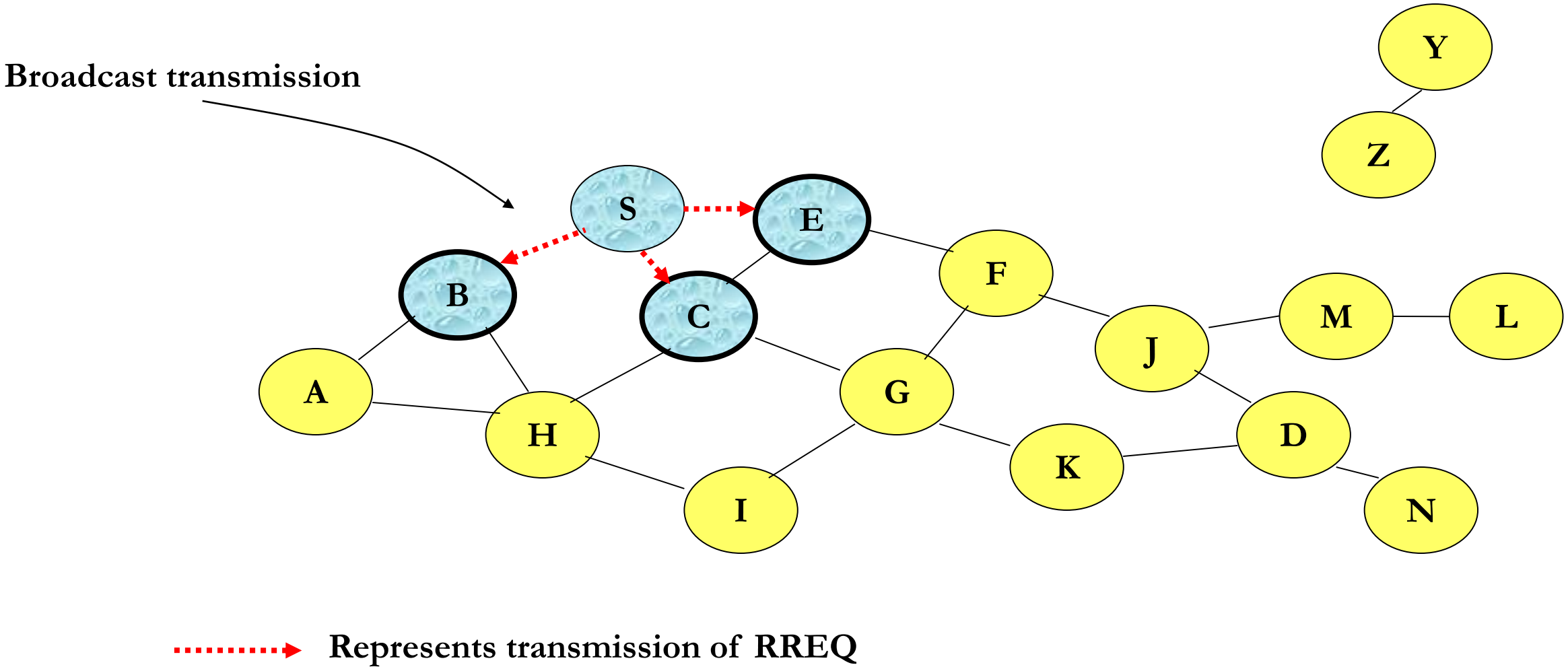
- Route Requests (RREQ) are forwarded in a manner similar to DSR
- When a node re-broadcasts a Route Request, it sets up a reverse path pointing towards the source
  - AODV assumes symmetric (bi-directional) links
- When the intended destination receives a Route Request, it replies by sending a Route Reply (RREP)
- Route Reply travels along the reverse path set-up when Route Request is forwarded

Route Requests in AODV

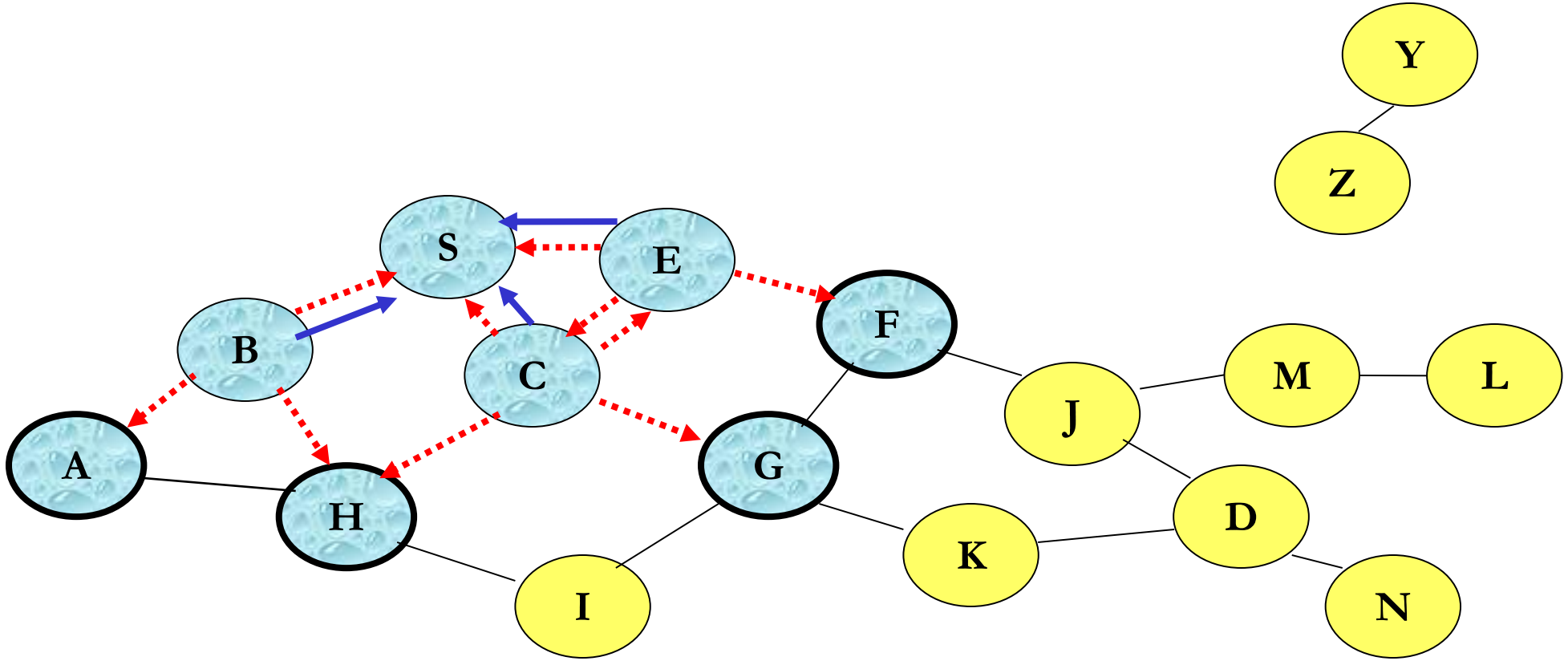


Represents a node that has received RREQ for D from S

Route Requests in AODV

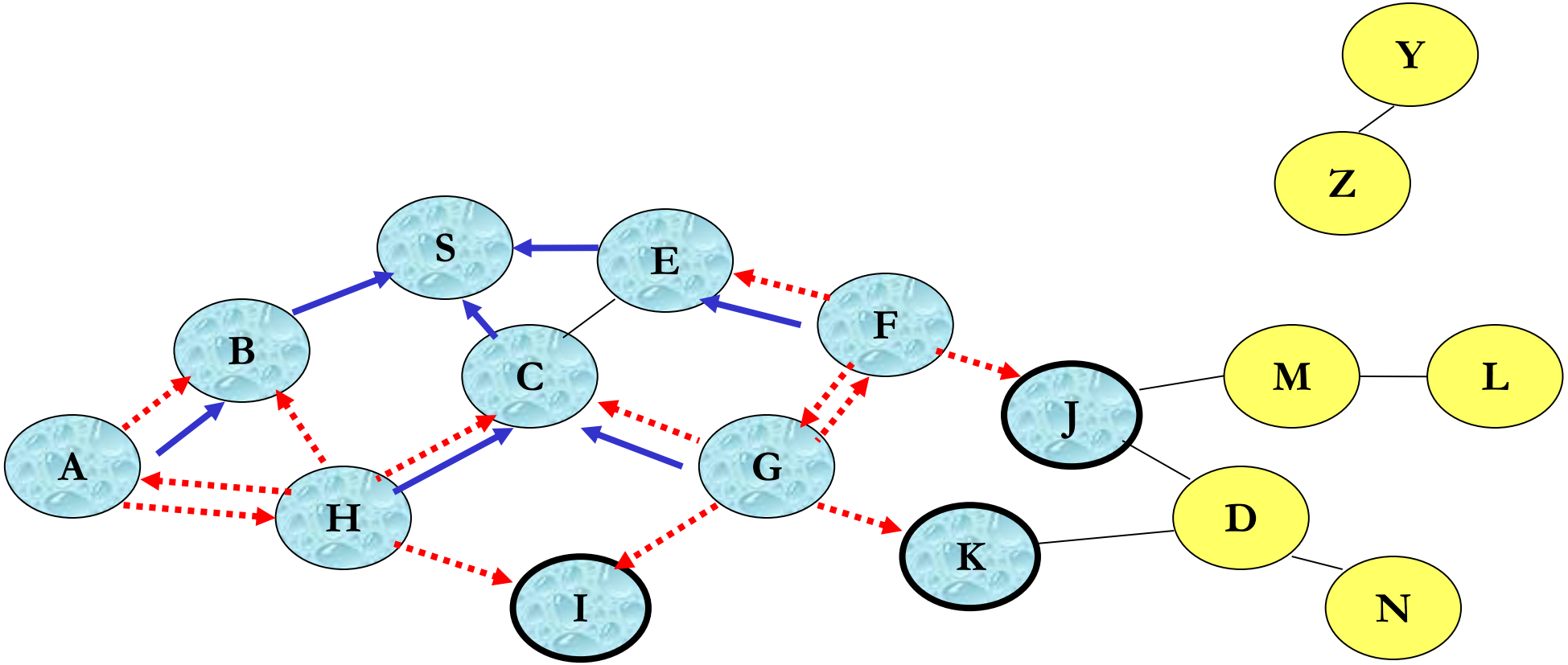


Route Requests in AODV



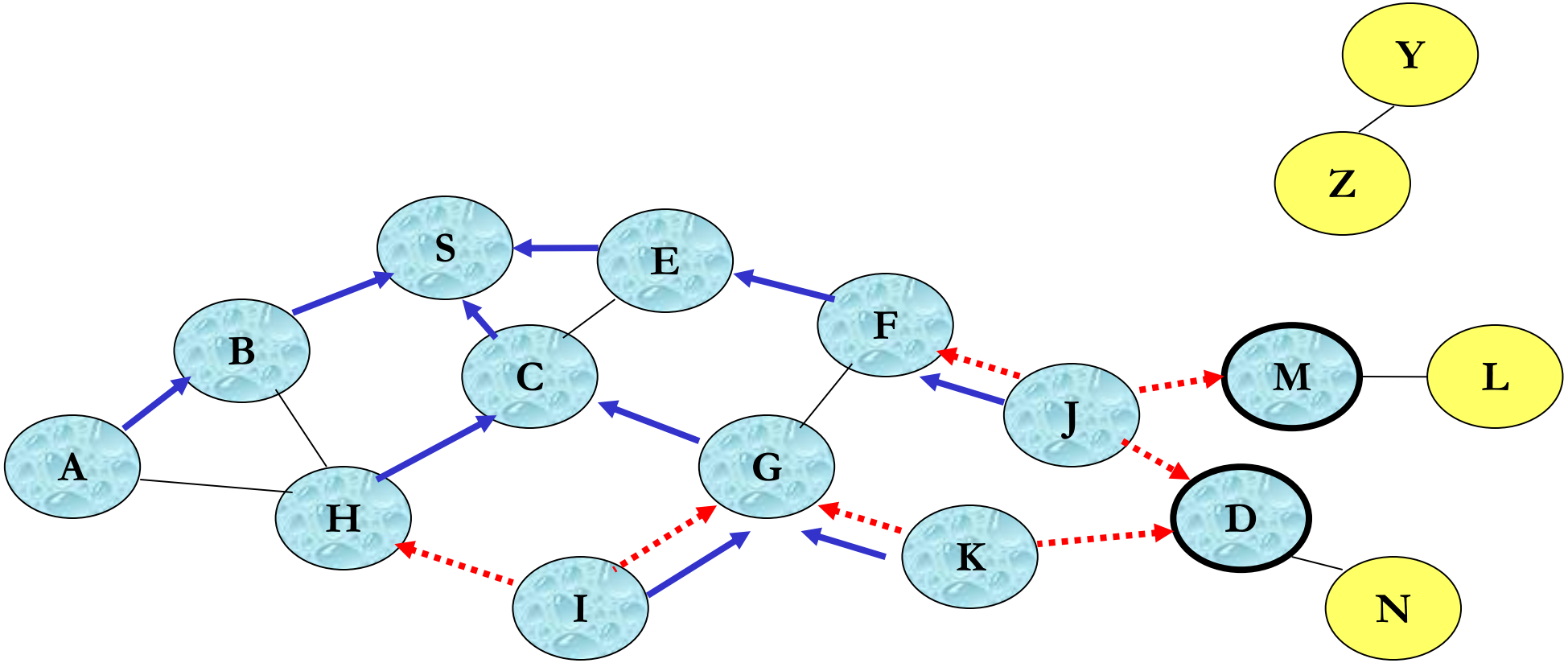
Represents links on Reverse Path

Route Requests in AODV

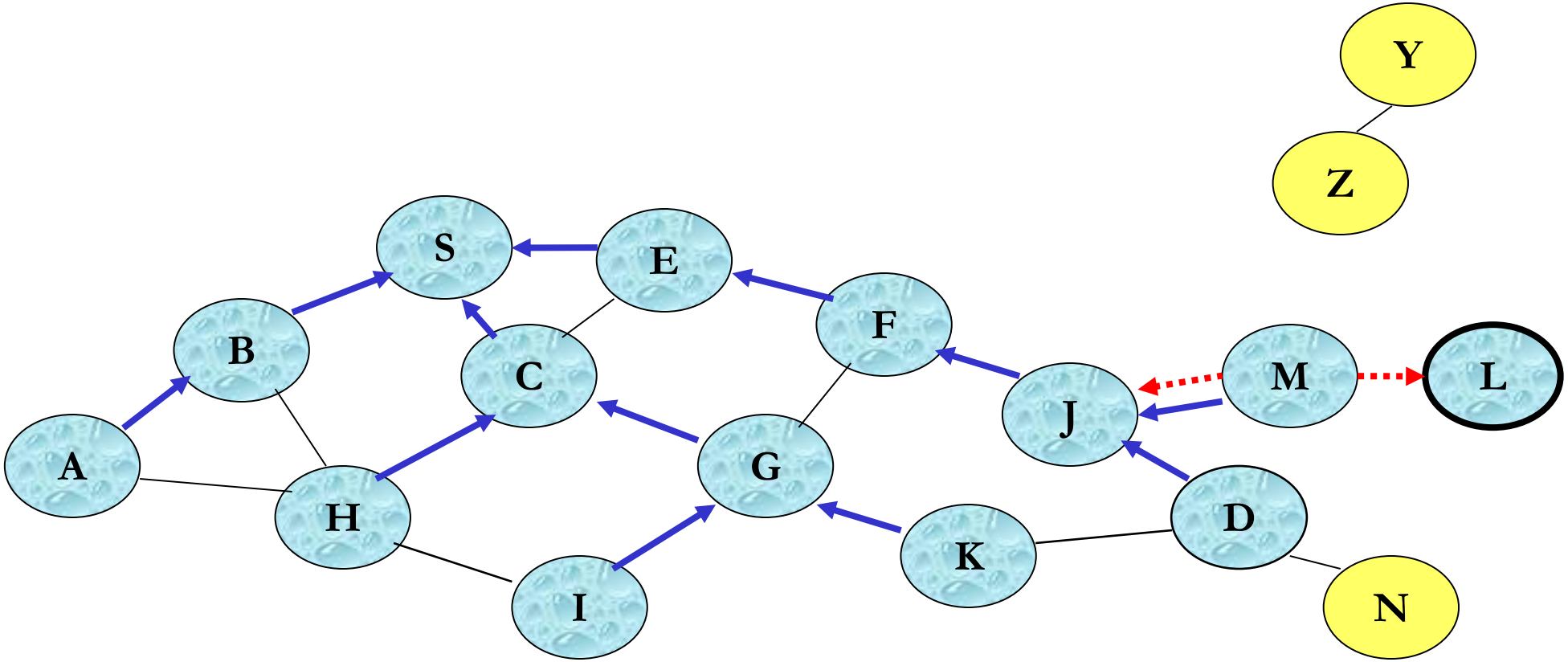


- **Node C receives RREQ from G and H, but does not forward it again, because node C has already forwarded RREQ once**

Route Requests in AODV

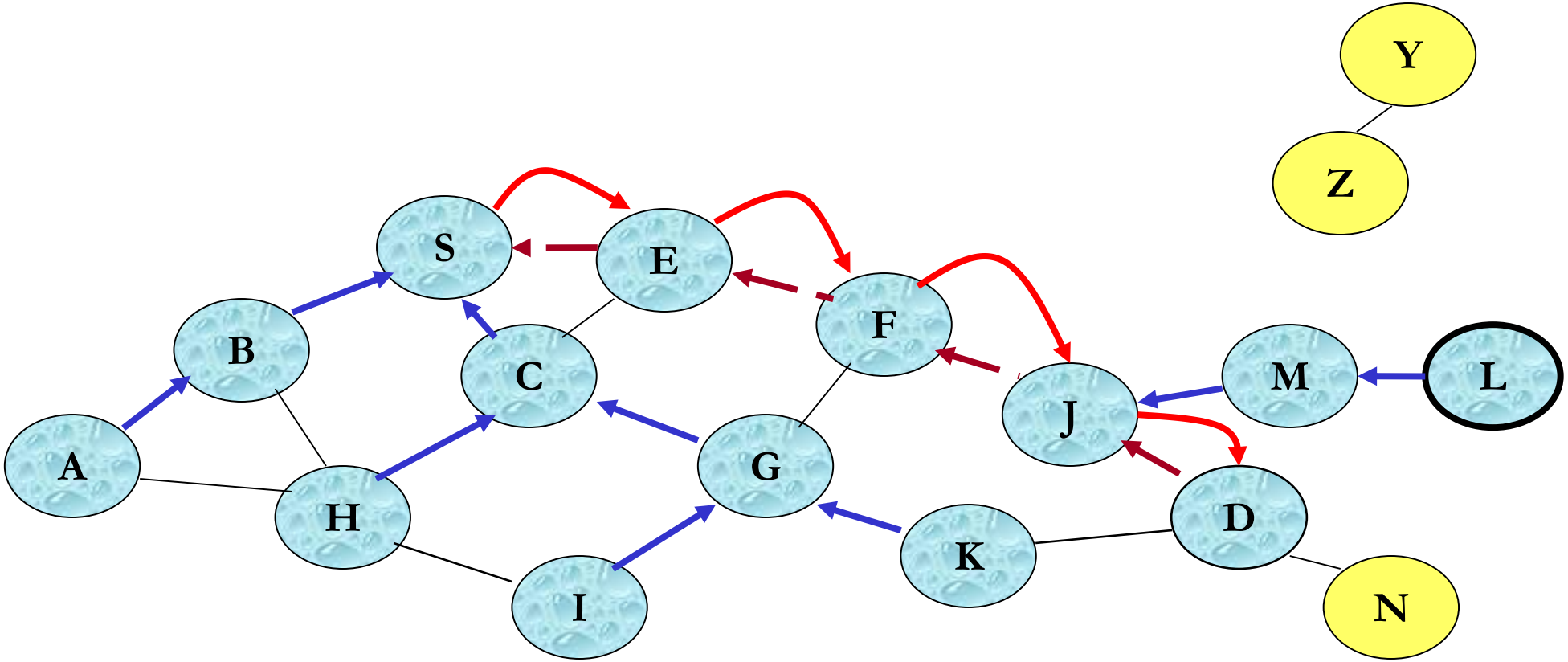


Route Requests in AODV



- **Node D does not forward RREQ, because node D is the intended target of the RREQ**

Route Requests in AODV



Forward links are setup when RREP travels along the reverse path

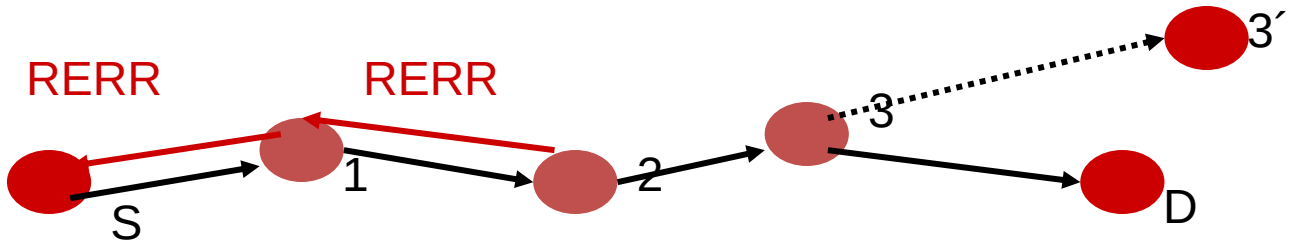
Represents a link on the forward path

Lifetime of a Route-Table Entry

- A lifetime is associated with the entry in the route table.
- This is an important feature of AODV. If a route entry is not used within the specified lifetime, it is deleted.
- A route is maintained only when it is used. A route that is unused for a long time is assumed to be stale.

Route Maintenance

- Once a unicast route has been established between two nodes S and D, it is maintained as long as S (source node) needs the route.
- If S moves during an active session, it can reinitiate route discovery to establish a new route to D.
- When D or an intermediate node moves, a route error (RERR) message is sent to S.
- The link from node 3 to D is broken as 3 has moved away to a position 3´.
- Node 2 sends a RERR message to 1 and 1 sends the message in turn to S.
- S initiates a route discovery if it still needs the route to D.



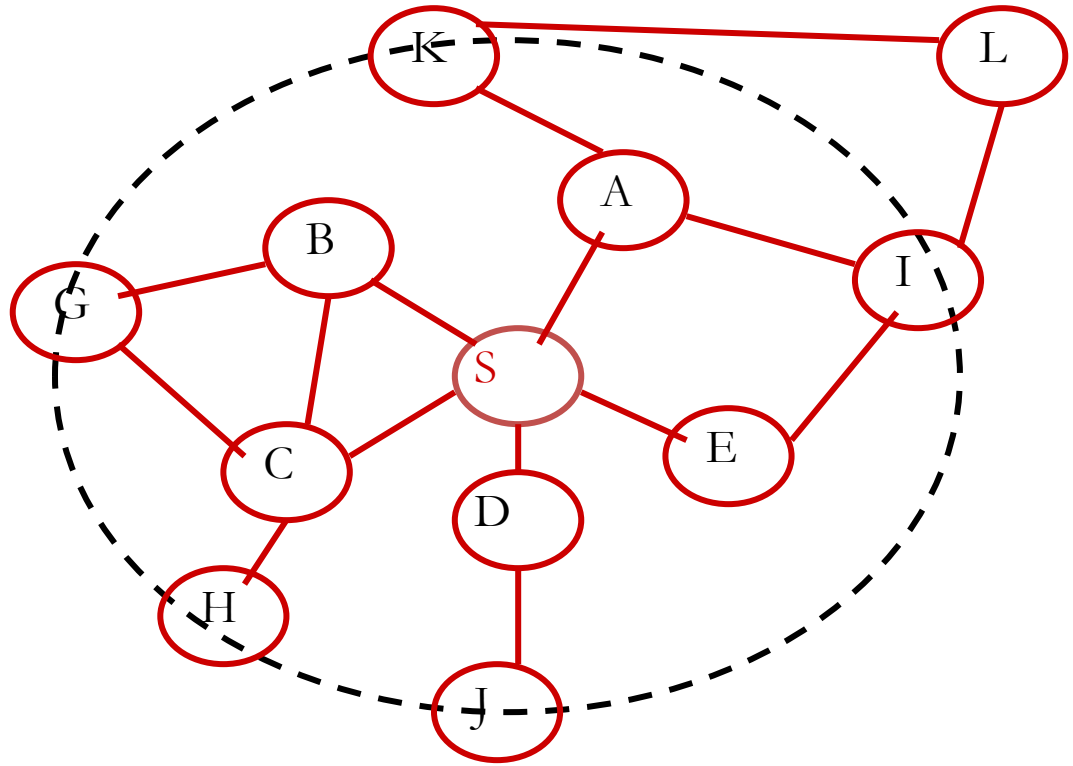
Zone Routing Protocol

- It is possible to exploit the good features of both reactive and proactive protcols and the Zone routing protocol does that.
- The proactive part of the protocol is restricted to a small neighbourhood of a node and the reactive part is used for routing across the network.
- This reduces latency in route discovery and reduces the number of control messages as well.

Routing Zones

- Each node S in the network has a routing zone. This is the proactive zone for S as S collects information about its routing zone in the manner of the DSDV protocol.
- If the radius of the routing zone is k, each node in the zone can be reached within k hops from S.
- The minimum distance of a peripheral node from S is k (the radius).

Routing Zones



- All nodes except L are in the routing zone of S with radius 2.

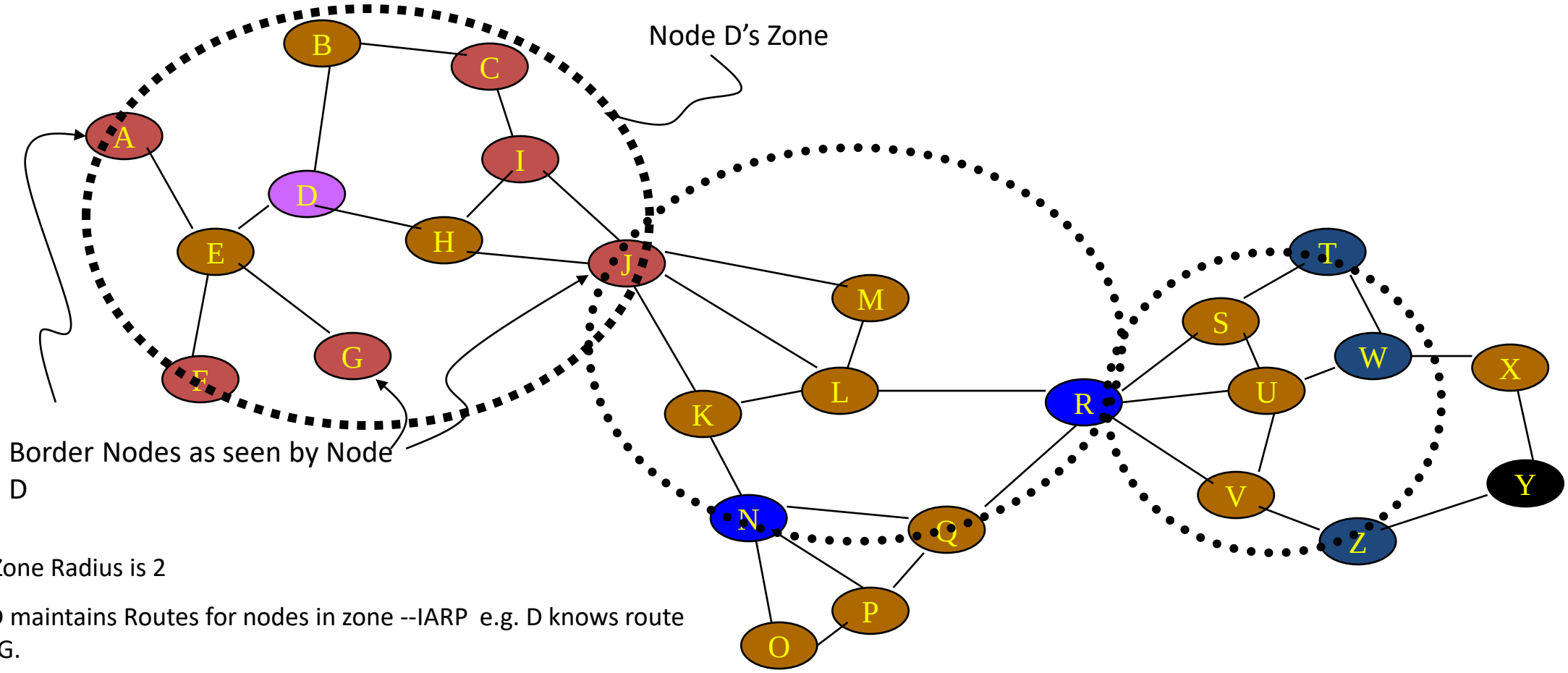
Routing Zones

- The coverage of a node´s trasmitter is the set of nodes in direct communication with the node. These are also called neighbours.
- In other words, the neighbours of a node are the nodes which are one hop away.
- For S, if the radius of the routing zone is k, the zone includes all the nodes which are k-hops away.
- The routing in ZRP is divided into two parts
  - Intrazone routing : Proactively maintain routes to all nodes within the source node's own zone.
  - Interzone routing : Use an on-demand protocol (similar to DSR or AODV) to determine routes to outside zone..

Intrazone Routing Protocol (IARP)

- Each node collects information about all the nodes in its routing zone proactively. This strategy is similar to a proactive protocol like DSDV.
- Each node maintains a routing table for its routing zone, so that it can find a route to any node in the routing zone from this table.

Intrazone Routing Protocol (IARP)



- Zone Radius is 2
- D maintains Routes for nodes in zone --IARP e.g. D knows route to G.
- If node not found, resort to Inter zone search.

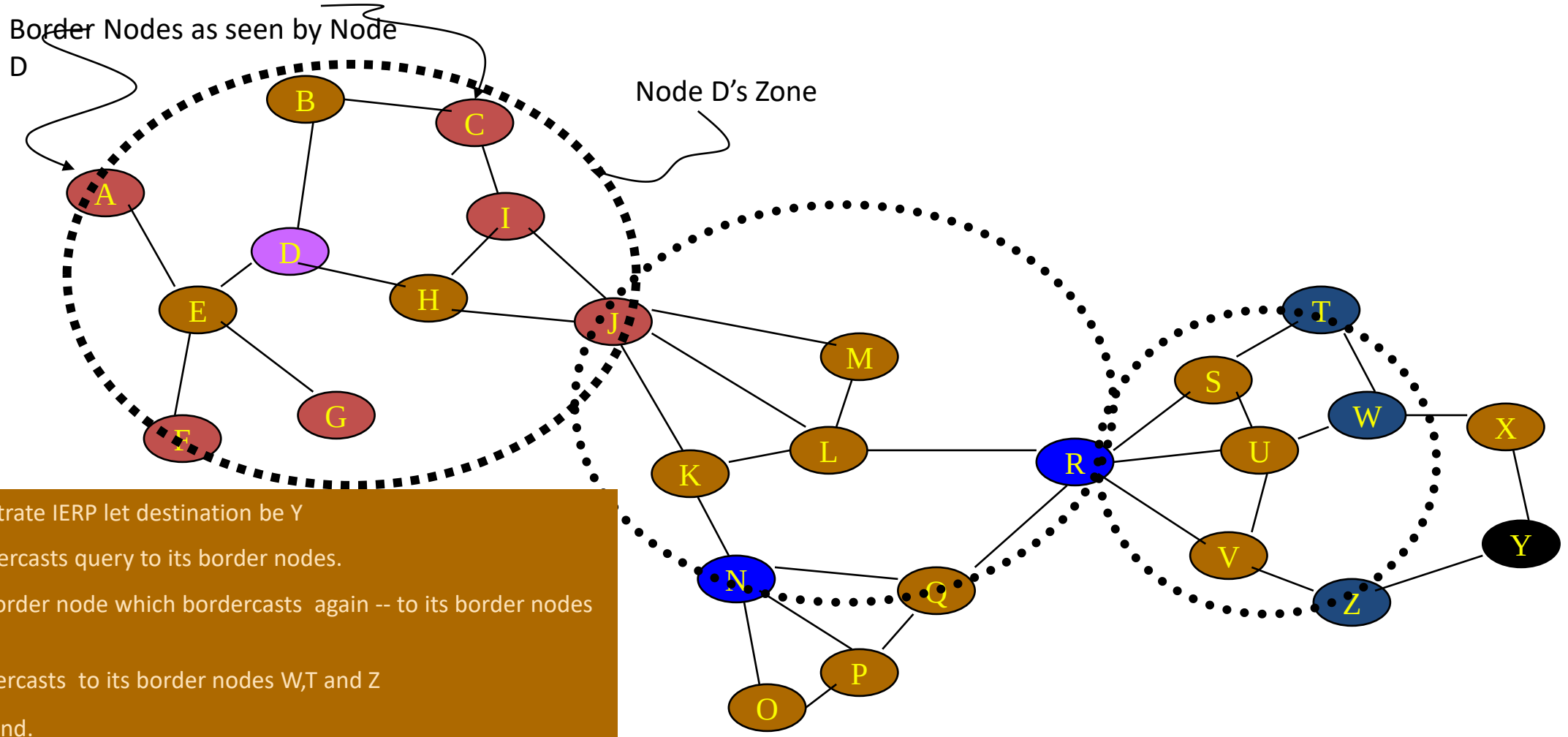
Interzone Routing Protocol (IERP)

- The interzone routing discovers routes to the destination reactively.
- Consider a source (S) and a destination (D). If D is within the routing zone of S, the routing is completed in the intrazone routing phase.
- Otherwise, S sends the packet to the peripheral nodes of its zone through bordercasting.

Bordercasting

- The node would direct the query message out only to its peripheral nodes.
- These nodes would execute the same algorithm that the primary node executed which is:
  - Check to see if the destination can be found within its zone. (How ?).
  - If yes, send a route-reply back to the source, indicating the route to the destination.
  - If not, forward the route-request to its peripheral nodes which execute the same procedure.

Interzone Routing Protocol (IERP)



- To illustrate IERP let destination be Y
- D bordercasts query to its border nodes.
- J is a border node which bordercasts again -- to its border nodes N and R.
- R bordercasts to its border nodes W,T and Z
- Y is found.

Multicast Routing Protocols for MANET

- Multicast → group transmission
- Efficient operation → Minimize unnecessary packet transmission – which minimizes energy consumption

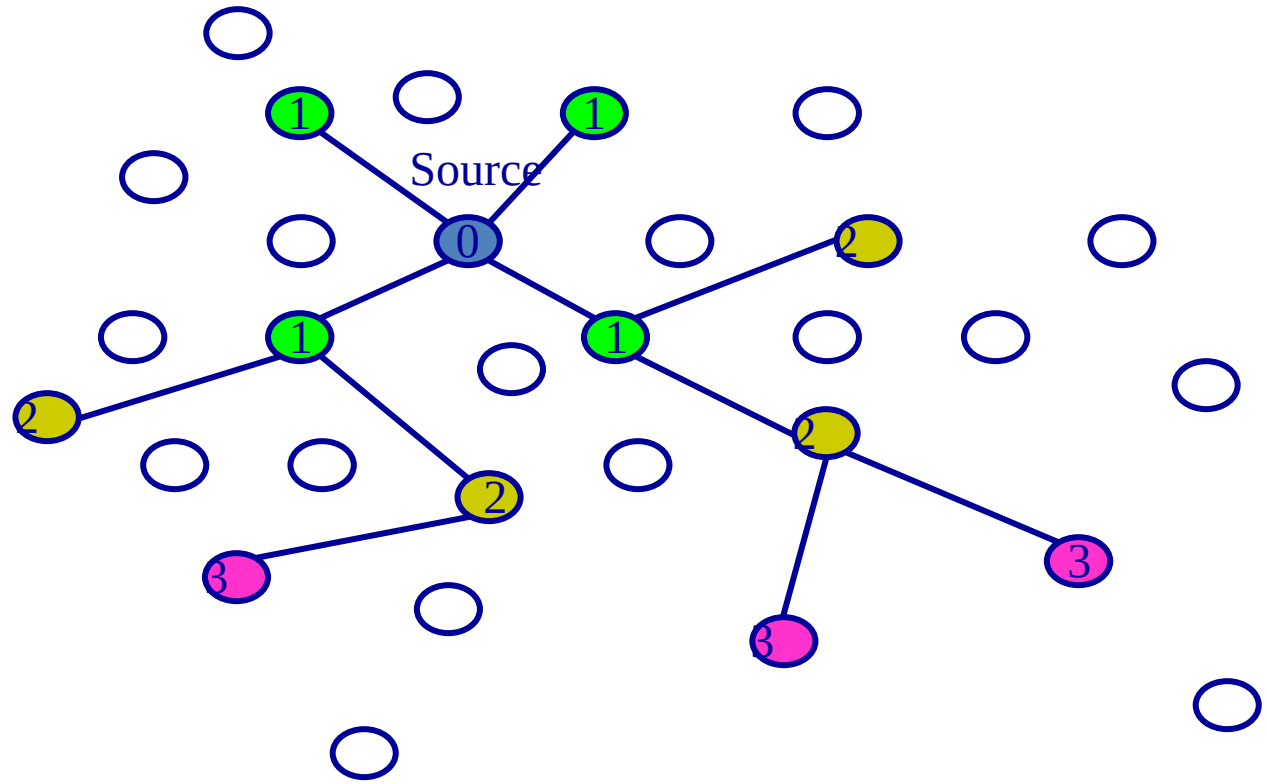
Types of Multicast Routing

- Tree-based
  - One path between a source-receiver pair
  - AMRoute -Ad hoc Multicast Routing protocol
  - AMRIS- Ad Hoc Multicast Routing Protocol Utilizing Increasing ID Numbers
  - MAODV - Multicast Ad hoc On-Demand Distance Vector

- Mesh-based
  - Multiple paths between a source-receiver pair
  - ODMRP - On-demand Multicasting Routing Protocol
  - CAMP - Core Assisted *Mesh* protocol

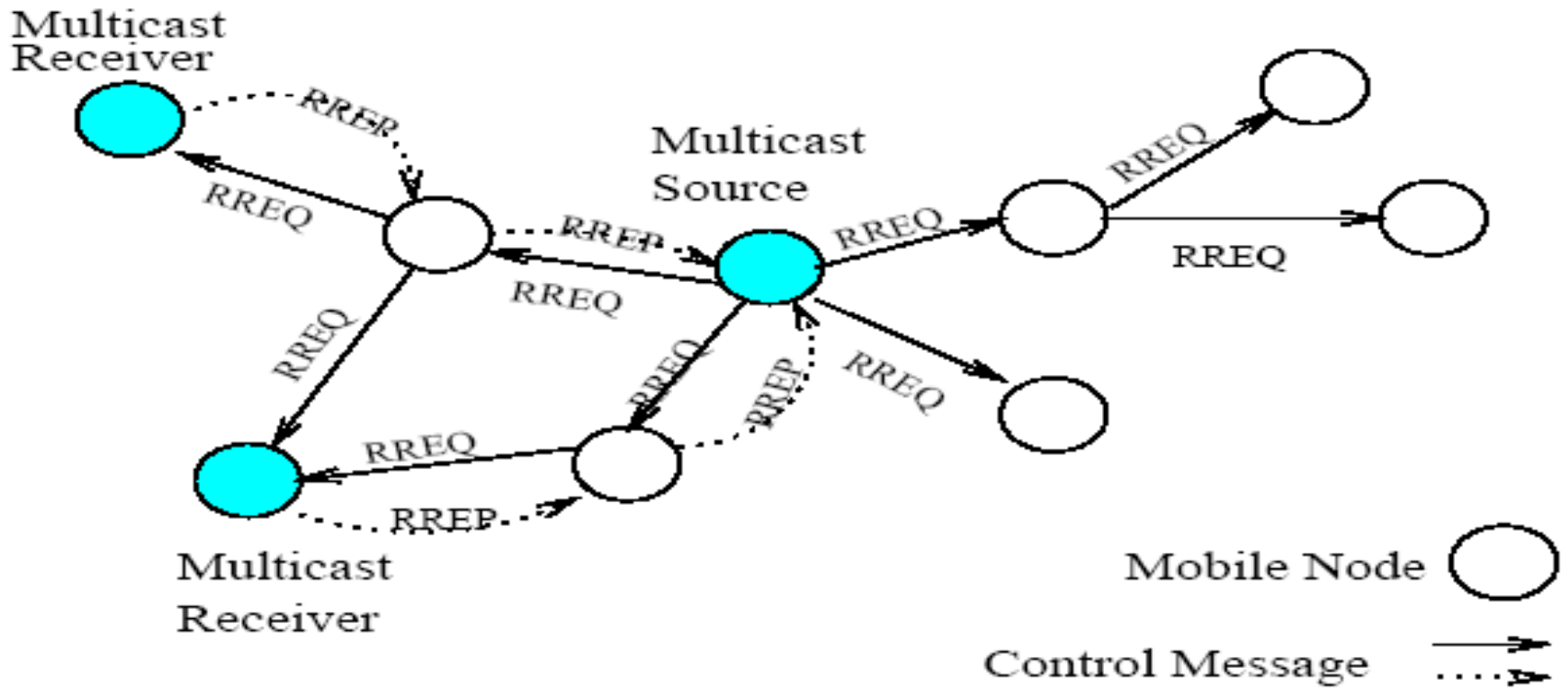
Tree – Based Protocol

- A packet traverses each hop and node in a tree at most once
- Tree structure built representing shortest paths amongst nodes, and a loop-free data distribution structure
- Even a link failure could mean reconfiguration of entire tree structure, could be a major drawback



Tree – Based Protocol

- Multicast Ad hoc On-Demand Distance Vector Protocol
  - Follows directly from the unicast AODV



Mesh Based Protocol

- Mesh-based multicast protocols may have multiple paths between any source and receiver pairs
- Mesh-based protocols seem to outperform tree-based proposals due to availability of alternative paths
- A mesh has increased data-forwarding overhead
- The redundant forwarding consumes more bandwidth
- The probability of collisions is higher when a larger number of packets are generated

On-demand Multicasting Routing Protocol - ODMRP

- Multicast Messages:
  - JOIN-QUERY (J-Q);
  - JOIN-REPLY (J-R);

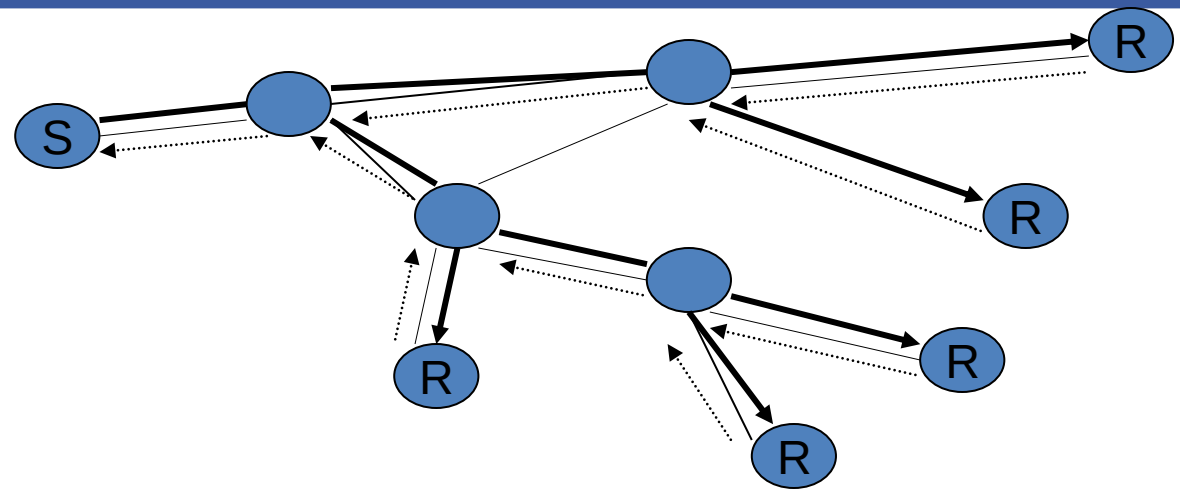
- Similar to Route Request and Route Reply in AODV and DSR

Basic Operation of ODMRP

On Demand Route and Mesh Creation

Join Query →

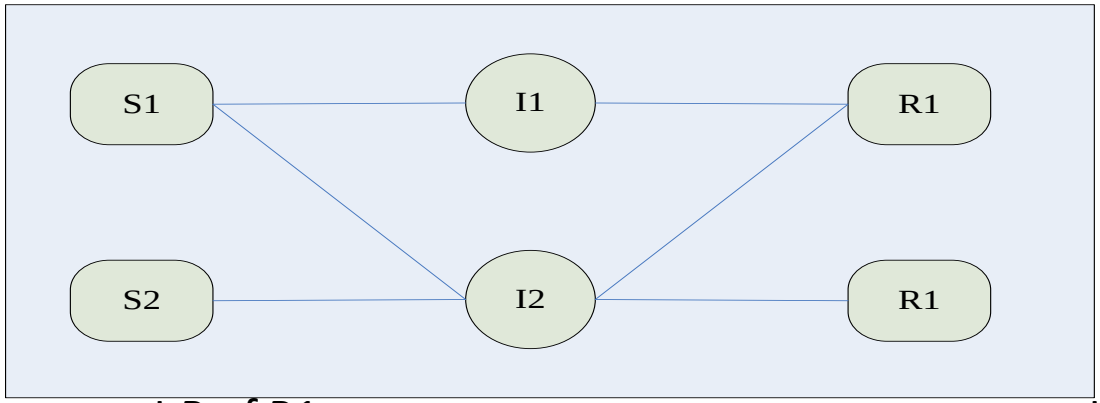
Join Reply ⇠



- S floods a Join Query to entire network to refresh membership.
- Receiving node stores the backward learning into routing table and rebroadcasts the packet.
- Finally when query reaches a receiver creates a Join Reply and broadcasts to its neighbors.
- Node receiving the Join Reply checks whether the next node id in Join Reply matches it own. If yes , it is a part of the forwarding group, sets its FG_FLAG and broadcasts its join reply built upon matched entries.
- Join Reply is propagated by each forwarding group member until it reaches source via a shortest path.
- Routes from sources to receivers builds a mesh of nodes called **"forwarding group"**.

ODMRP: Join Reply

- JOIN-REPLY message



J-R of R1

Sender	Next Node
S1	I1
S2	I2

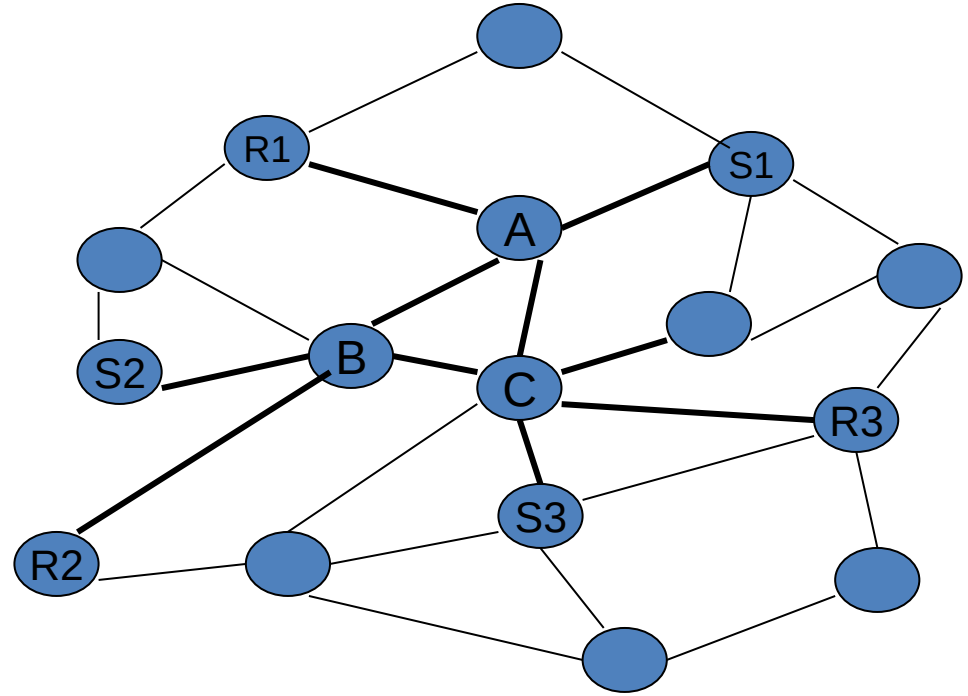
J-R of I1

Sender	Next Node
S1	S1

Why a mesh?

Links

Multicast Routes



Initial Route from S1 to R2 is < S1 -A- B- R2>

Redundant Route < S1- A- C- B- R2>

ODMRP: Sender Actions

Sender actions:

- Downstream
  - Generate J-Q message;
  - Broadcast J-Q ;
- Upstream
  - Receive J-R (include the path info);

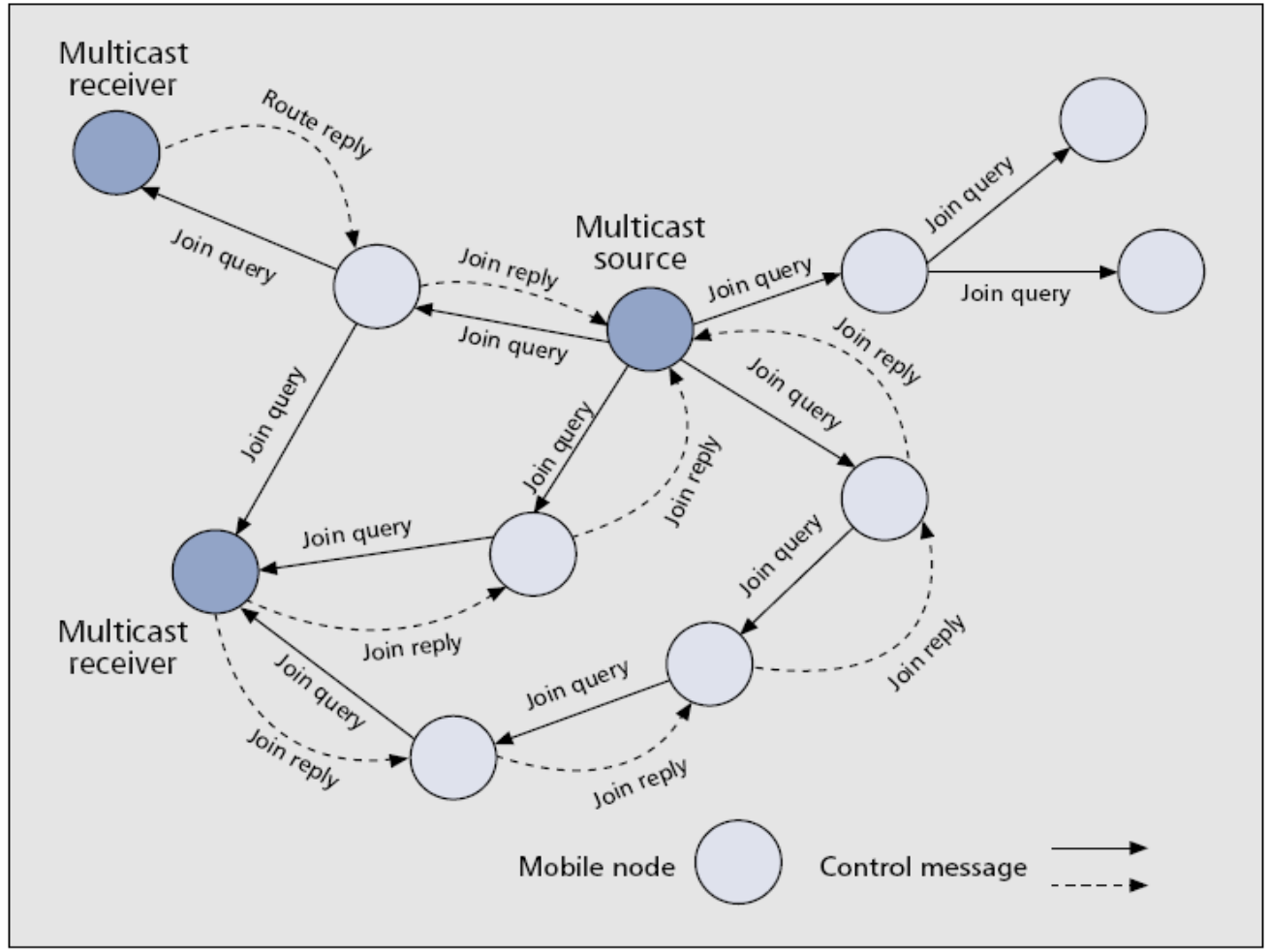


Figure 4. *Mesh creation in ODMRP.*

ODMRP: Intermediate Nodes (downstream)

Intermediate node actions: (downstream)

- Receive J-Q, omit duplicated ones (use cached sequence numbers);
- Store upstream node info;
- Re-broadcast J-Q;

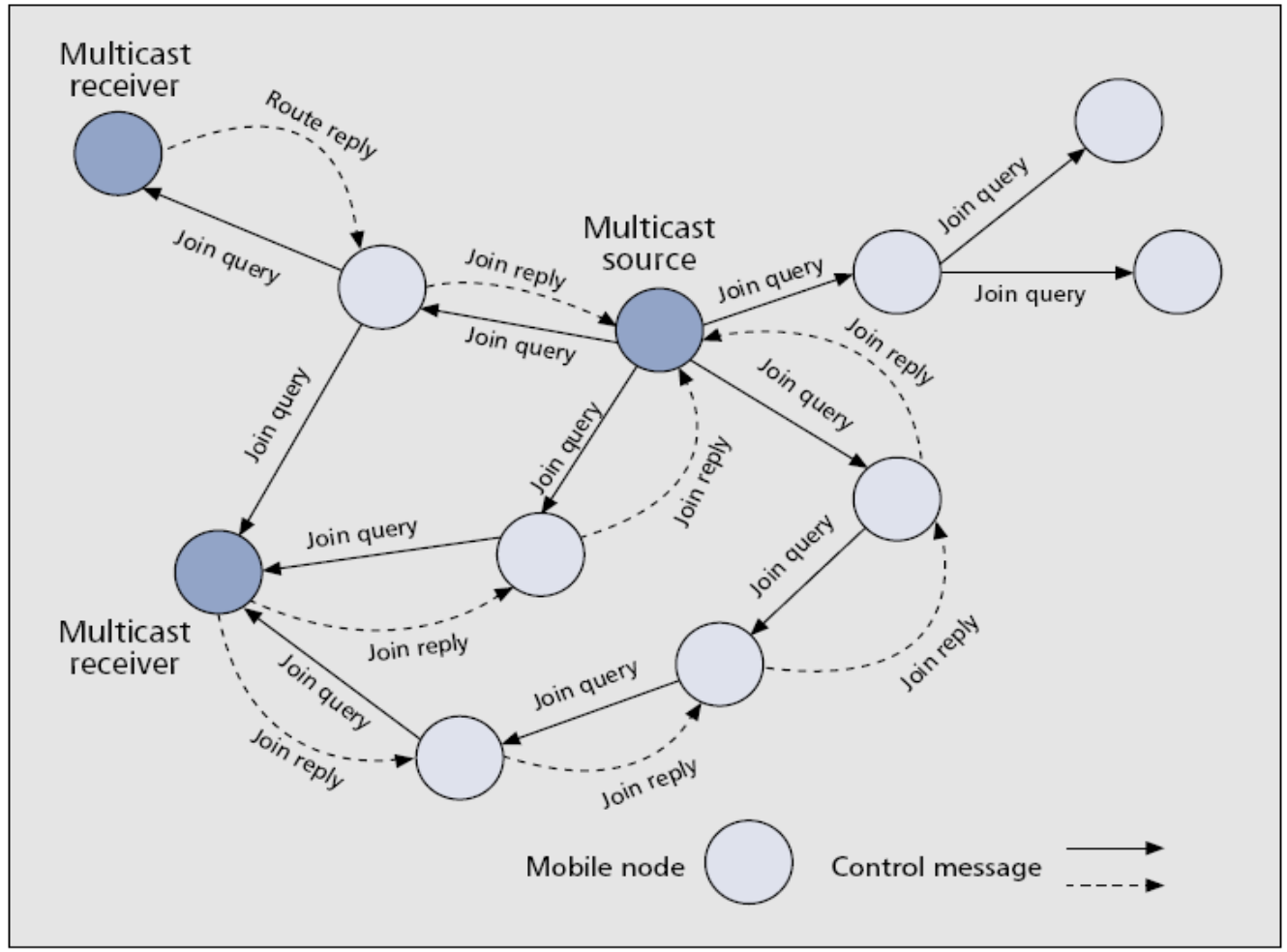


Figure 4. *Mesh creation in ODMRP.*

ODMRP: Intermediate Nodes (upstream)

Intermediate node actions: (upstream)

- Received J-R;
- If node is on the path
  - Generate new J-R with node info and broadcast, route established!

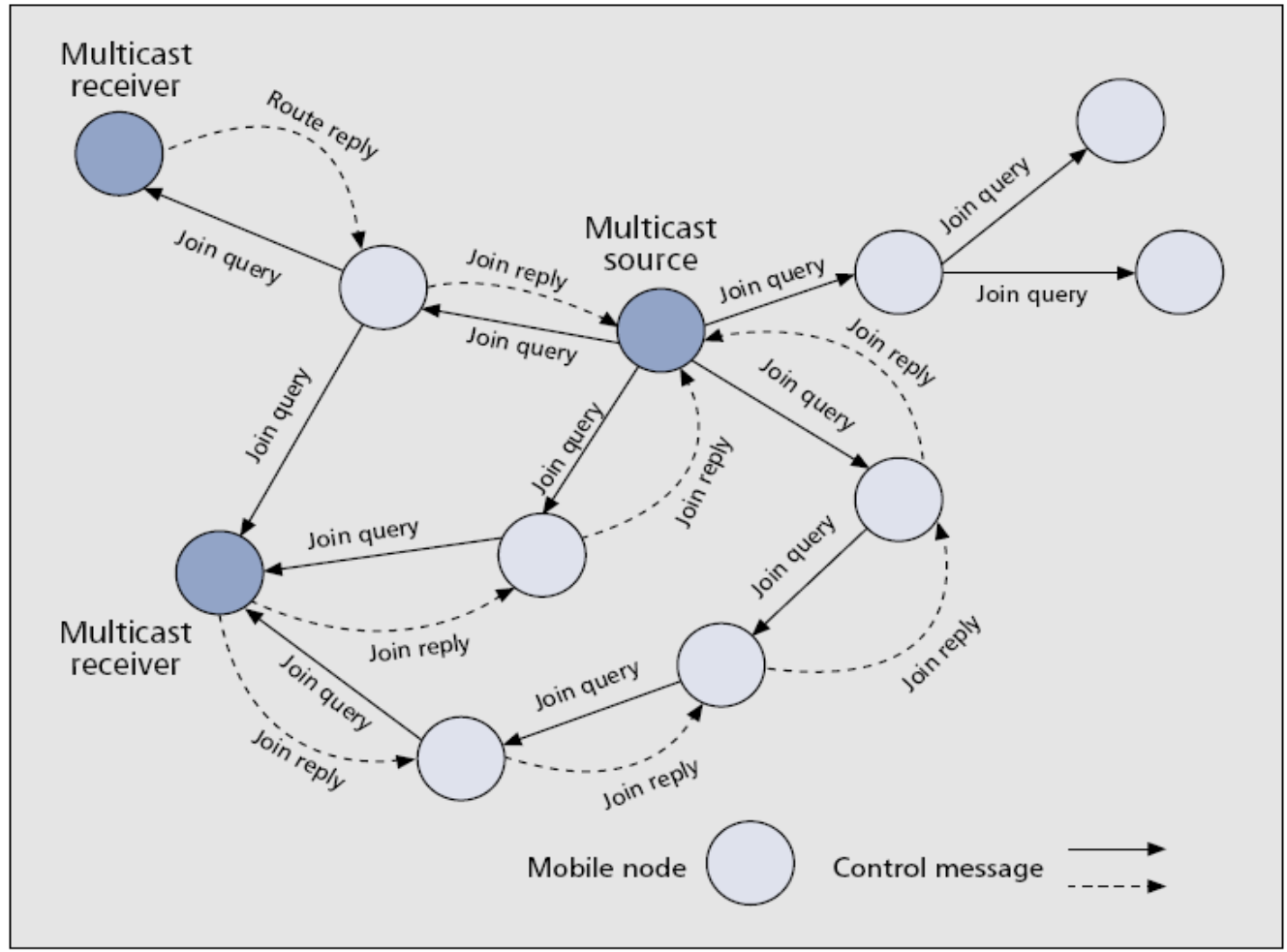


Figure 4. *Mesh creation in ODMRP.*

ODMRP: Receiver Actions

Receiver actions:

- Downstream
  - Received J-Q;
  - Generate J-R with path info
- Upstream
  - Broadcast J-R;

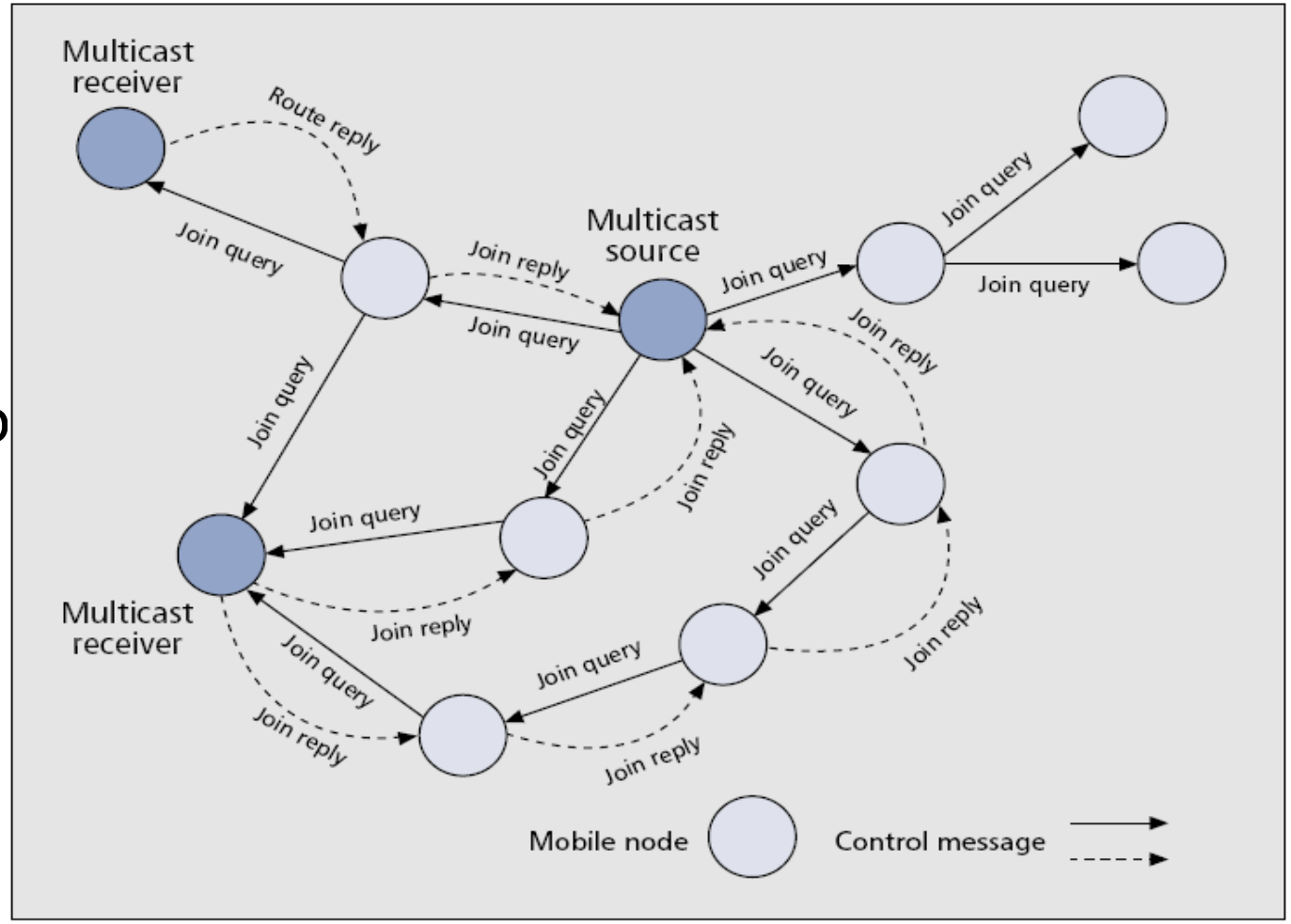


Figure 4. *Mesh creation in ODMRP.*

ODMRP: Maintenance phase

Soft state approach

- Sender repeat J-R periodically to maintain mesh.
- Node joins
  - Sending J-R as discusses before.
- Node leaves
  - Sender: stops sending J-Q;
  - Receiver: stops sending J-R;
- Links break
  - Receiver: receives new J-Q and replies with J-R;

Test your Knowledge

- Explain how DHCP can be used when the size of the block assigned to an organization is less than the number of hosts in the organization.

Summary

	MAODV	ODMRP
Big difference		
Topology	Shared (Core-based) Tree	Mesh of Nodes
Main Similarity		
Mobility support	Yes, based on MANET	
Driven mode	On-demand, do not store whole network topology	
Advantages	simple topology low overheads	mobility robustness
Disadvantages	sensitive to mobility (low delivery ratio)	complex topology high overheads

References

Jochen H. Schller, “Mobile Communications”, Second Edition, Pearson Education, New Delhi, 2007.