Dr. Vishwanath Karad
MIT WORLD PEACE UNIVERSITY | PUNE
TECHNOLOGY, RESEARCH, SOCIAL INNOVATION & PARTNERSHIPS

CET4004B: Wireless and Mobile Device Security

SCHOOL OF COMPUTER ENGINEERING AND TECHNOLOGY

T. Y. B. TECH. COMPUTER SCIENCE AND ENGINEERING

CET4004B: Wireless and Mobile Device Security

Teaching Scheme
Theory: 3Hrs. / Week

Credits: 03 + 01 = 04
Practical: 2 Hrs./Week

Course Objectives:

1) Knowledge:

i. To understand wireless networks technologies and applications
ii. To study Ad-Hoc, sensor networks architecture, challenges and applications
iii. To understand basic security needs and issues in wireless networks
iv. To understand mobile device security architecture and security dynamics

2) Skills:

i. This course gives understanding of how to design and configure your own network

3) Attitude:

i. To deploy the network as well as provide various security aspects to the mobile device

Course Outcomes:

i. Compare different wired and wireless technologies
ii. Simulate and analyze wireless Ad-Hoc networks for different protocols
iii. Analyze the security threats in wireless sensor networks
iv. Configure or Program security needs in mobile devices

Module
Ad-Hoc Wireless Networks

Disclaimer:

a. Information included in these slides came from multiple sources. We have tried our best to cite the sources. Please refer to the references to learn about the sources, when applicable.

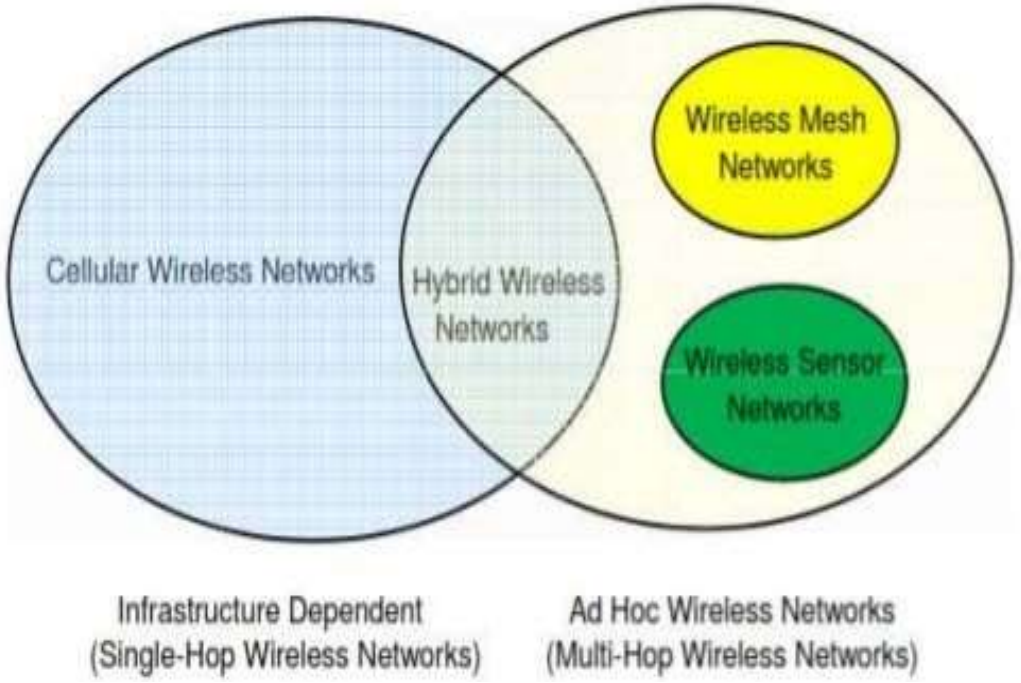
b. The slides should be used only for preparing notes, academic purposes (e.g. in teaching a class), and should not be used for commercial purposes.

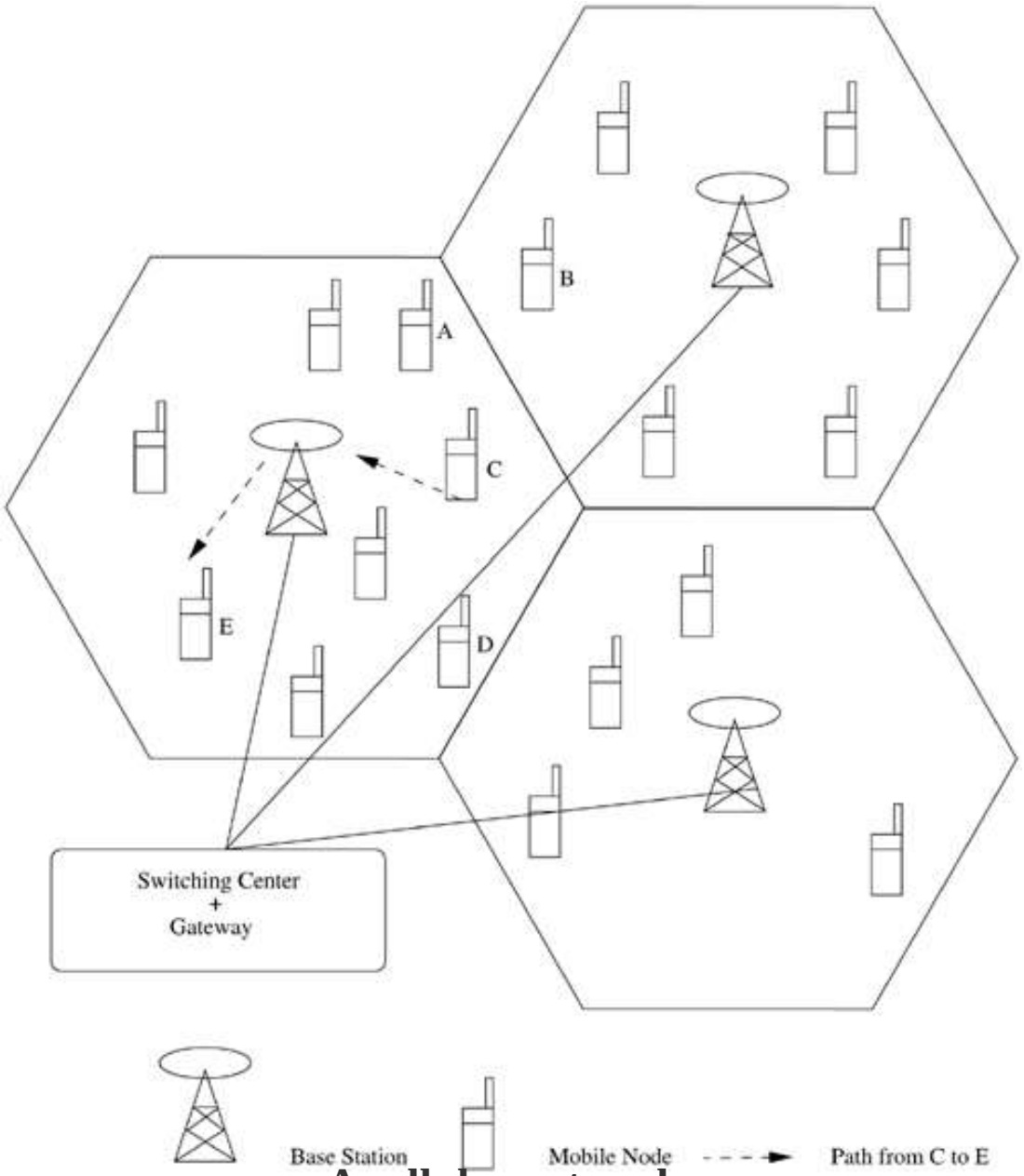
Points to be covered

- Introduction to Ad-Hoc Wireless Networks
- Properties and Challenges
- Applications and Issues in MAC design in Ad-Hoc wireless networks
- Design Goals of MAC
- Routing design issues in Ad-Hoc networks
- Classifications of Routing protocols,
- Table Driven: DSDV (Destination Sequenced Distance-Vector Routing Protocol), WRP (Wireless Routing Protocol), CGR (Cluster-Head Gateway Switch Routing Protocol).
- ON-DEMAND ROUTING PROTOCOLS: DSR (Dynamic Source Routing Protocol), AODV(Ad Hoc On-Demand Distance-Vector Routing Protocol) and TORA(Temporally Ordered Routing Algorithm)
- Introduction to Multicast Routing Protocols

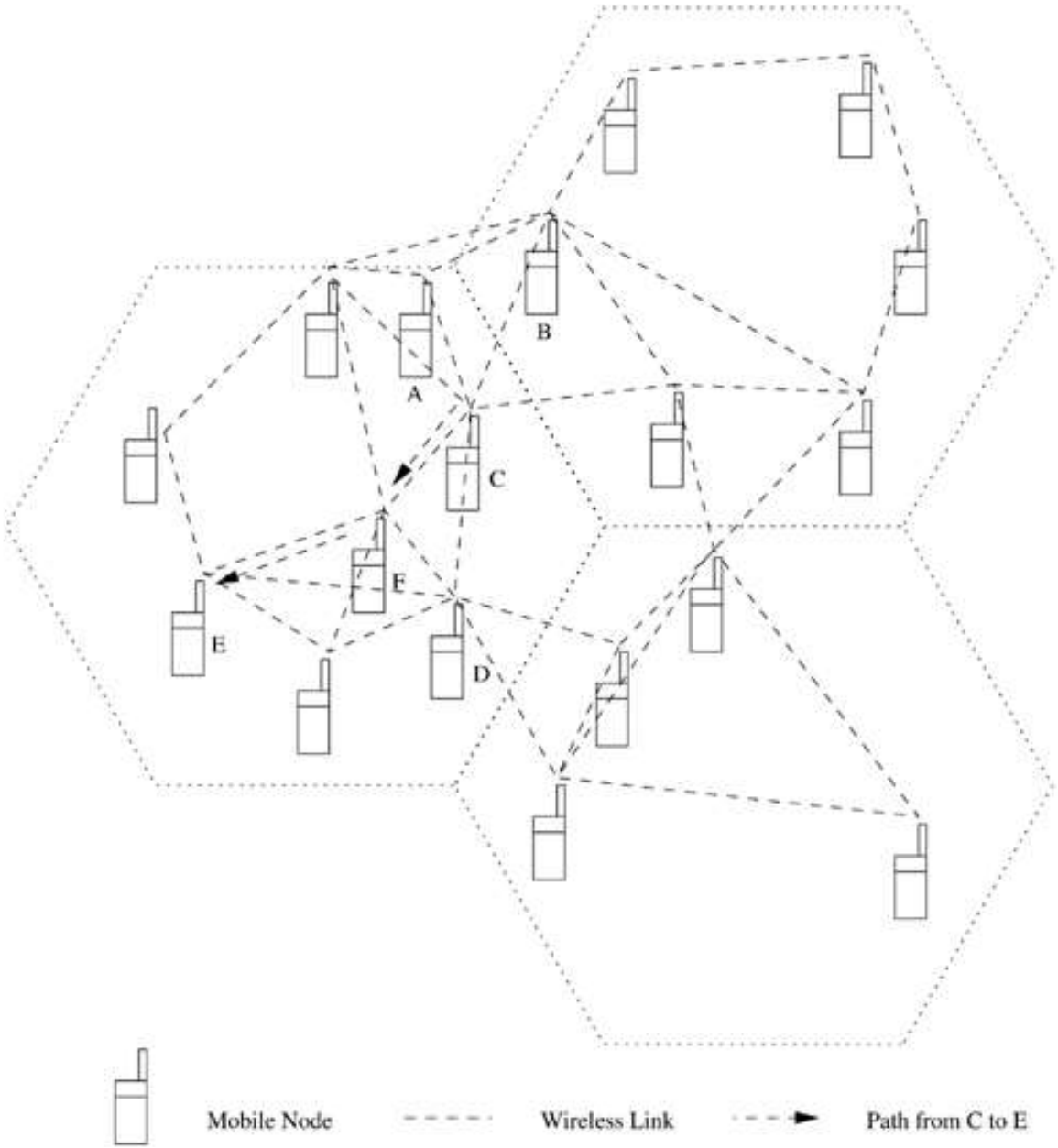
Introduction to Ad-Hoc Wireless Networks

- It is defined as the category of wireless networks that utilize multi-hop radio relaying
- They are capable of operating without the support of any fixed infrastructure
- Also called infrastructureless networks
- The absence of any central coordinator or base station makes the routing a complex one compared to cellular networks.
- Wireless mesh networks and wireless sensor networks are specific examples of ad hoc wireless networks





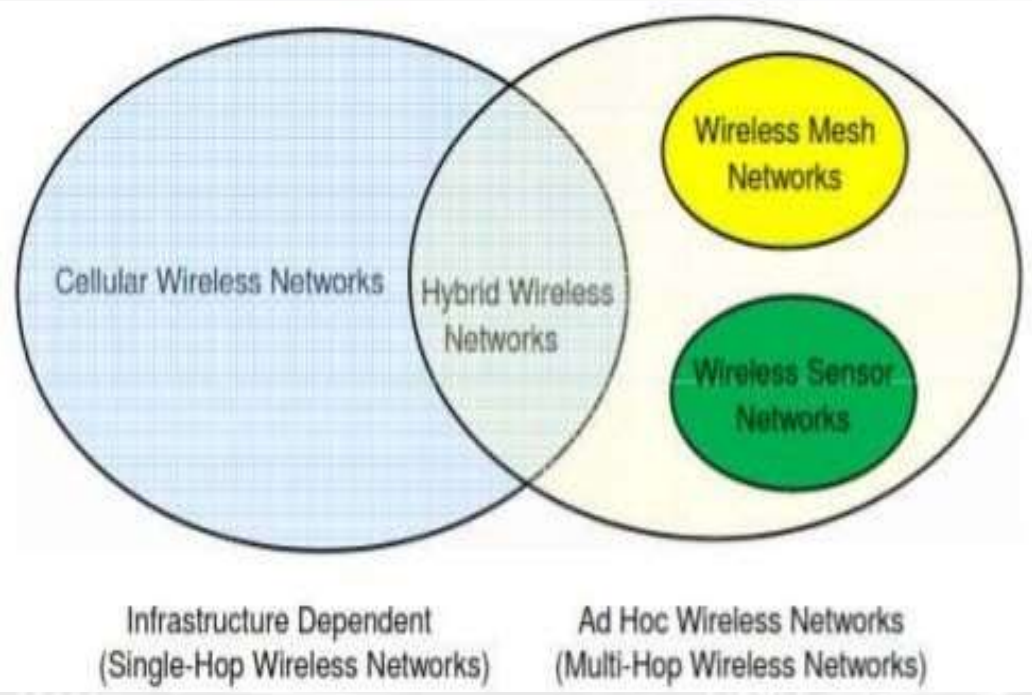
A cellular network



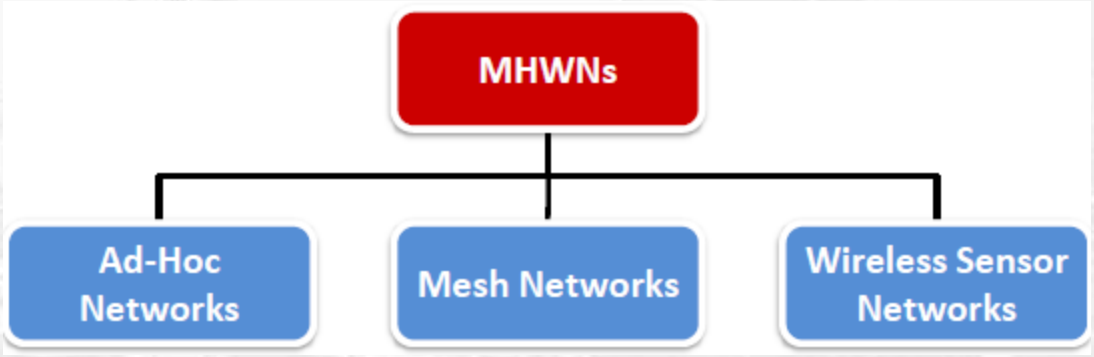
An ad hoc wireless network

Ad-Hoc Wireless Networks

- Multi Hope Wireless Networks (MHWNs): a collection of nodes that communicate with each other wirelessly by using radio signals with a shared common channel.
- There are several names for MHWNs; it could be called Packet Radio Network, Ad-hoc Network or Mobile Network.



Cellular and ad hoc wireless networks



MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Differences between Cellular Networks and Ad hoc Wireless Networks

- The presence of base stations simplifies routing and resource management in a cellular network as the routing decisions are made in a centralized manner with more information about the destination node.
- But in an ad hoc wireless network, the routing and resource management are done in a distributed manner in which all nodes coordinate to enable communication among themselves.
- This requires each node to be more intelligent so that it can function both as a network host for transmitting and receiving data and as a network router for routing packets from other nodes.
- Hence the mobile nodes in ad hoc wireless networks are more complex than their counterparts in cellular networks.

Difference Between Cellular Networks and Ad-Hoc Networks

Sr. No	Cellular Networks	Ad-Hoc Wireless Networks
1	Fixed infrastructure-based	Infrastructure less
2	Single Hop Wireless Links	Multihop Wireless Links
3	Guaranteed Bandwidth	Not Guaranteed Bandwidth/Shared radio channel
4	Circuit Switched	Packet Switched
5	High Cost	Cost Effective
6	Deployment Time - More	Deployment Time - Less
7	High Cost of Network Maintenance	Less Cost of Maintenance
8	Seamless Connectivity	Frequent Path Breaks due to Mobility
9	Easy Time Synchronization	Difficult Time Synchronization
10	Frequency Reuse Spectrum	Dynamic Frequency Reuse

Main Features of Ad-hoc Networks

- Decentralized
- Do not rely on preexisting infrastructure
- Each node participates in routing by forwarding data to neighbor nodes
- Fast network topology changes due to nodes' movement

Ad Hoc Networks

Why do we need ad-hoc networks?

- More laptop users
- More smartphones users (e.g.. Android phones, iPhones)
- More devices with Wi-Fi-support (e.g.. televisions, hi-fi, home-theaters, media servers etc.)
- Moving users, vehicles, etc.
- Outdoors places

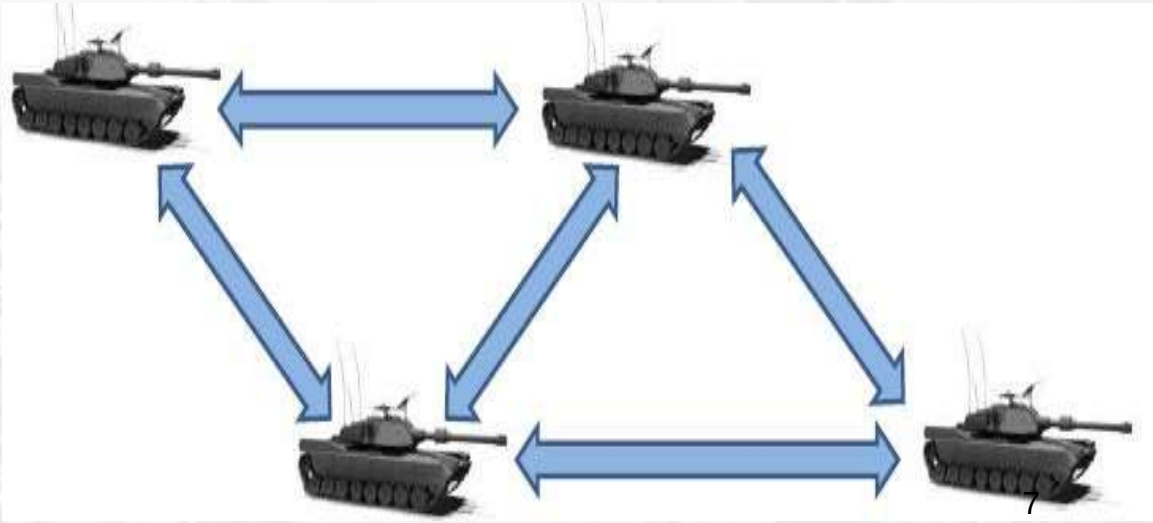
- ✓ In all these occasions there is no centralized infrastructure (such APs)
- ✓ So ad-hoc network is a necessity

Applications of Ad Hoc Wireless Networks

- Military applications:
  - Useful in communication among a group of soldiers for tactical operations.
  - For example leader of the soldiers want to give any order to all soldiers OR set of selected persons are involved in the operation.
  - The routing protocol in these applications should be able to provide quick, secure, and reliable multicast communication with support for real-time traffic.

- Incase if we need to exchange information and the network's infrastructure has been destroyed.

- It is suitable for military communications at battlefield where there is no network infrastructure.



Ad hoc wireless network formed by a fleet of military tanks

Applications of Ad Hoc Wireless Networks

❖ Collaborative and Distributed Computing:

- To give information in a group of peoples using conference.
- For example group of researchers want to share their research among group of people.
- Distributed file sharing applications, though this application does not demand the communication to be interruption-free, the goal of the transmission is that all the desired receivers must have the replica of the transmitted file.

Applications of Ad Hoc Wireless Networks

❖ Emergency operations:

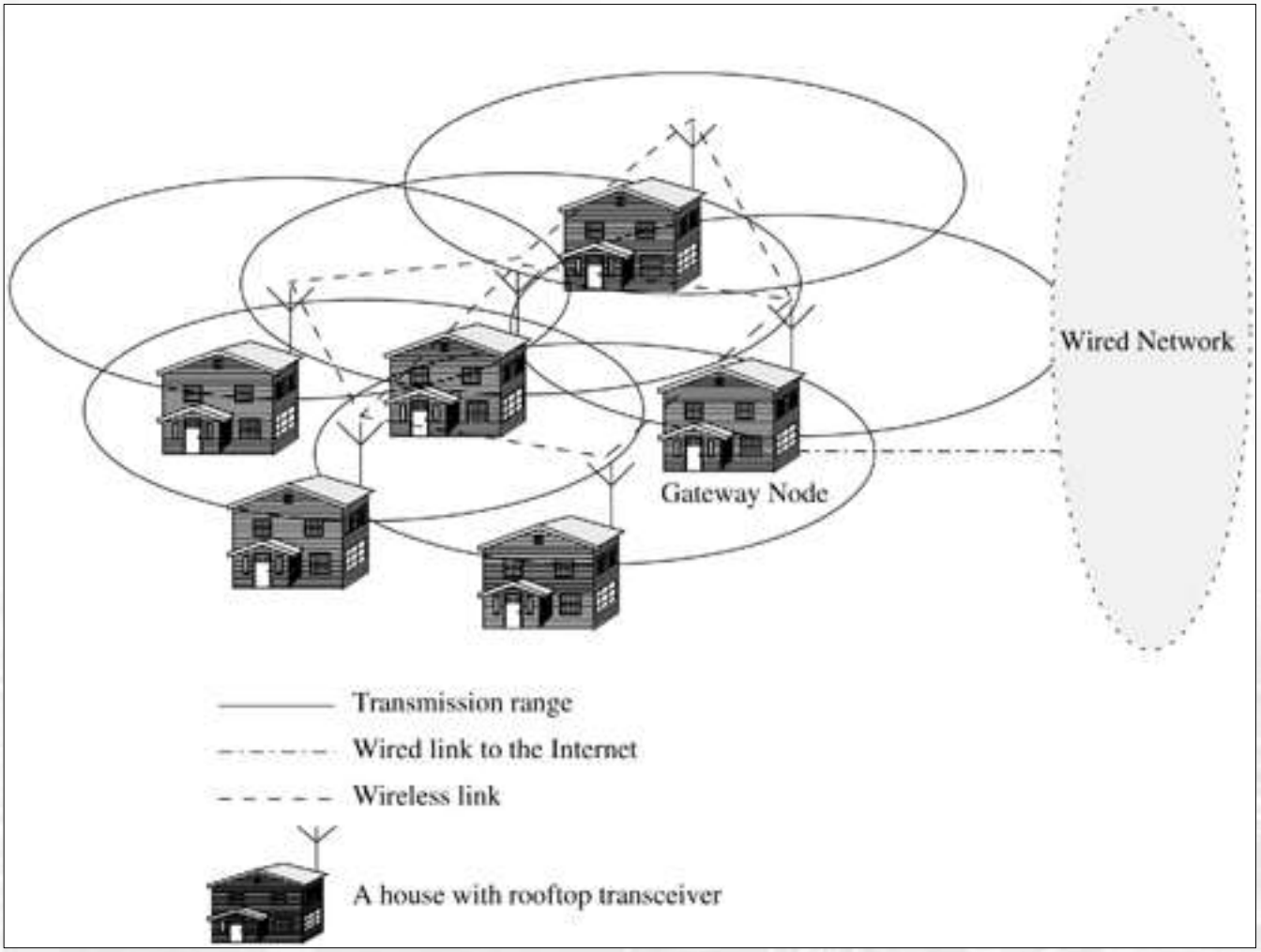
- Ad hoc is used in search and rescue operations, crowd control and commando operations.
- Due to the natural disaster like earthquake, flood, conventional communication facilities are destroyed in that case ad hoc network is used for rescue activities.

❖ Wireless mesh networks:

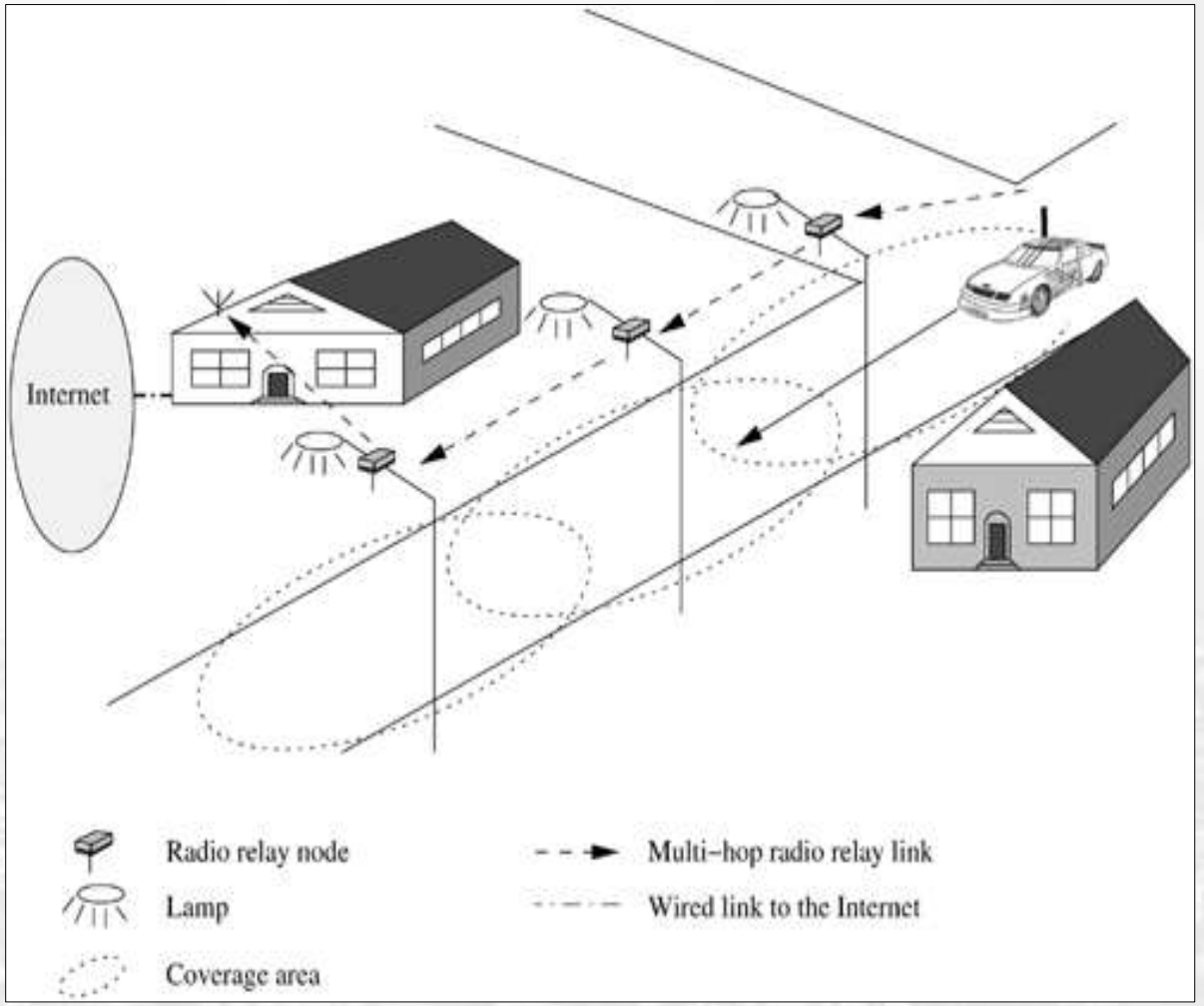
- Wireless Mesh Network are the ad hoc wireless network that provide, many alternate path from source to destination when existing paths fails.
- Mesh Networks are used in residential zones, business zones, important civilian zones and university campus.
- Mesh Network support high data rate, quick and low cost deployment, enhanced services, high scalability and high availability.

Applications of Ad Hoc Wireless Networks

Wireless Mesh Network Operations



Wireless mesh network operating in a residential zone

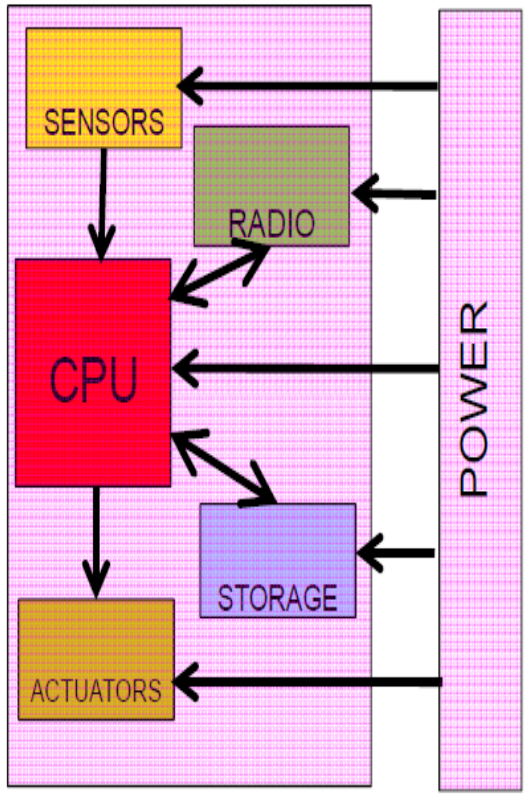


Wireless mesh network covering a highway

Applications of Ad Hoc Wireless Networks

Wireless Sensor Networks

- A sensor network is a collection of large number of sensor nodes that are deployed in particular region.
- As we know that the sensors are the tiny devices that have capability ofsensing some parameter, processing the data and communicate over the network.
- A sensing can be periodic or sporadic.
- Military, Health Care, Home security and environmental monitoring are the application areas of wireless sensor network (not limited too).



- A sensing node has 3 basic components:
a CPU, a radio transceiver, and a sensor array.
- Any kind of sensor, interfaced through an ADC.
- Nodes are normally battery-powered.
- On-board storage
- May have actuators, too

Applications of Ad Hoc Wireless Networks

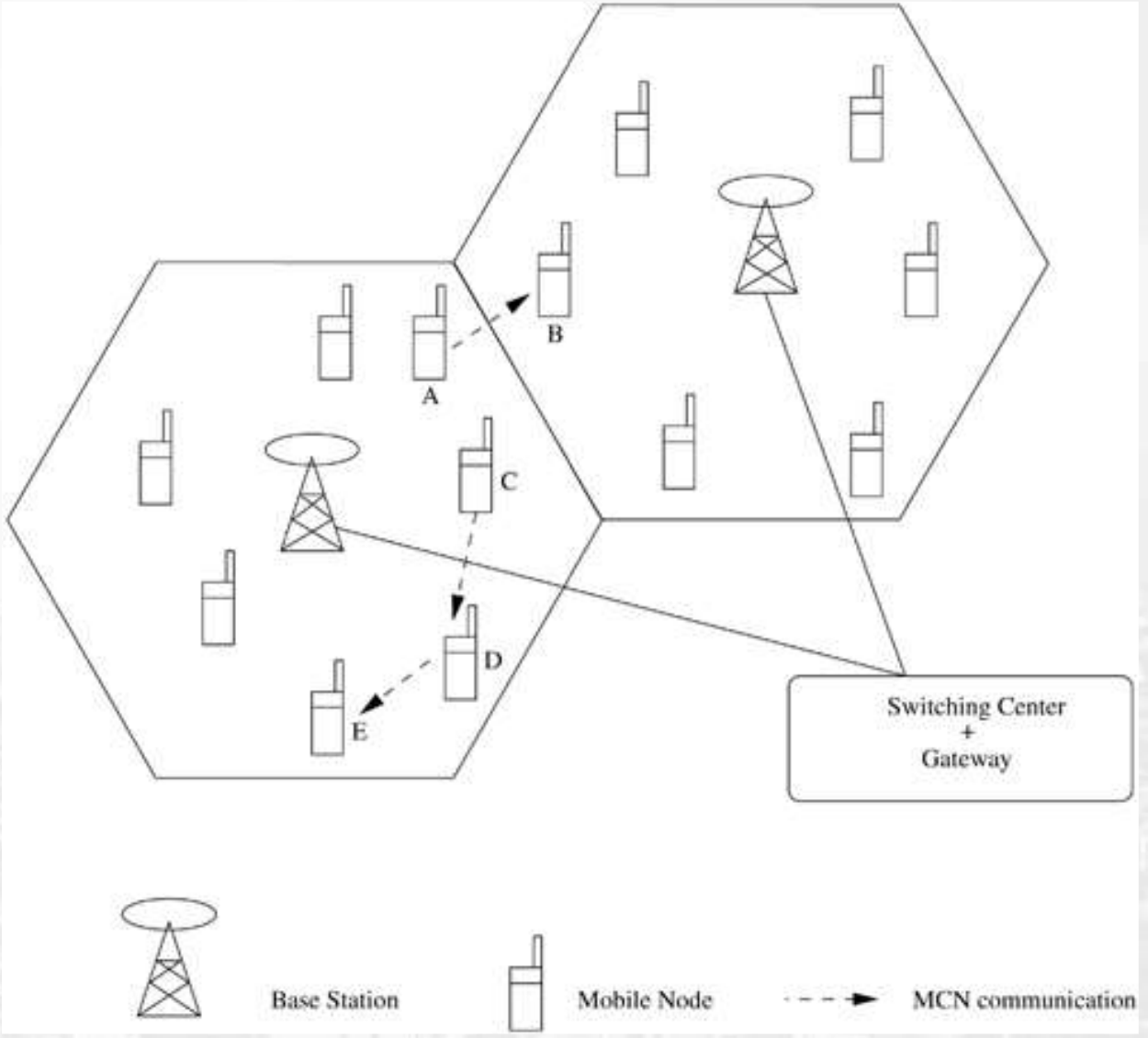
Hybrid Wireless Network Architectures

- One of the major application areas of ad hoc wireless networks is in hybrid wireless architectures such as multi-hop cellular networks (MCNs) and integrated cellular ad hoc relay (iCAR) networks
- Hybrid wireless networks are the combination of multi-hop cellular network and integrated cellular ad hoc relay network
- Hybrid network have the higher capacity than the cellular network
- Increased flexibility and reliability in routing
- Better coverage and connectivity in holes
- MCNs combine the reliability and support of fixed base stations of cellular networks with flexibility and multi-hop relaying of ad hoc wireless networks.

Applications of Ad Hoc Wireless Networks

Multi-hop Cellular Networks (**MCN) Architecture**

- When two nodes (which are not in direct transmission range) in the same cell want to communicate with each other, the connection is routed through multiple wireless hops over the intermediate nodes.
- The base station maintains the information about the topology of the network for efficient routing.
- The base station may or may not be involved in this multi-hop path.
- Suppose node A wants to communicate with node B.
- If all nodes are capable of operating in MCN mode, node A can reach node B directly if the node B is within node A's transmission range.
- When node C wants to communicate with node E and both are in the same cell, node C can reach node E through node D, which acts as an intermediate relay node.



Issues and Challenges in Ad hoc Wireless Networks

1. Medium access scheme
2. Routing
3. Multicasting
4. Transport layer protocol
5. Pricing scheme
6. Quality of Service provisioning
7. Self-organization
8. Security
9. Energy management
10. Addressing and service discovery
11. Scalability
12. Deployment considerations

1. Medium Access Control:

MAC protocol in ad hoc wireless network is distributed and shared channel for the transmission of packets.

- **Distributed Operation:** The design of MAC protocol should be fully distributed with minimum control overhead.
- **Synchronization:** MAC protocol should be synchronized with time.
- **Hidden Terminal:** The presence of hidden terminal reduced the throughput of MAC protocol. Hence MAC protocol should be able to handle the effects of hidden terminal.
- **Exposed Terminal:** To improve the efficiency of MAC protocol the exposed nodes should be allowed to transmit without causing collision to the on-going data transfer.
- **Throughput:** MAC protocol should maximize the throughput with minimizing the occurrence of collision, maximizing channel utilization and minimizing control overhead.

- **Access Delay:** Access delay refers to the average delay that any packet experiences to get transmitted. The MAC protocol should attempt to minimize the delay.
- **Fairness:** It refers to the ability of the MAC protocol to provide equal bandwidth to all competing nodes.

Some Other Issues of MAC:

- Real time traffic support
- Resource reservation
- Ability to measure resource availability
- Capability for power control
- Adaptive rate control
- Use of directional antennas

2. Routing in Ad-Hoc Network:

- Routing refers to the exchanging the route information and finding feasible and appropriate path to destination based on the criteria such as minimum power required, hop length and utilizing minimum bandwidth.

The major challenges of routing protocol are:

- **Mobility:** Due to the mobility frequent path breaks, packet collision, transient loops are occur in the network. Routing protocol should be able to solve all these problems in efficient manner.
- **Bandwidth Constraint:** Bandwidth is equally distributed or shared between all the nodes in the broadcast region.
- **Location Dependent Contention:** A good routing protocol should have built in mechanism for distributing the network load uniformly across the network which is dependent on the number of nodes in the network.
- **Other Resource Constraints:** Routing protocol should be able to handle issues related with computing power, battery power and buffer storage.

3. Multicasting:

- Multicasting plays an important role in application of Ad-Hoc wireless network, namely emergency search , rescue operation and military communication.

Design Issues of Multicast Routing Protocol:

- Robustness: Recover and configure quickly from link break
- Efficiency: minimum no. of transmission to deliver data packets
- Control Overhead: minimum
- Quality of Service(QoS)
- Efficient Group Management: minimum exchange of control messages
- Scalability: add the nodes any time
- Security: access denied for non-authenticate user

4. Transport Layer Protocol:

- The main objective of transport layer protocol is establish and maintain end-to-end connection, reliable end-to-end delivery of packets, flow control, and congestion control.

5. Quality of Service Provisioning:

- QoS is the performance level of services offered by service provider or a network to the user.
- QoS would be measure on per flow, per link, per node basis.
- QoS have following important terms:
  - **QoS Parameters:** Bandwidth, Delay, Security, Reliability, Throughput, Packet delivery ratio
  - **QoS Aware Routing:** QoS aware routing means routing with QoS parameters.
  - **QoS Framework:** A framework for a QoS is a complete system that attempts to provide promised services to each user or application.

6. Self Organization:

- Self organization is the important property of Ad hoc wireless network in which organizing and maintaining the network by itself.
- Activities of self organization in Ad-Hoc wireless networks are :

- **Neighbor Discovery:** In neighbor discovery phase every node in the network gather information about its neighbor and maintain this information in appropriate data structure.
- **Topology Organization:** If any change is occur in the network topology due the mobility or failure of nodes this is automatically organized.
- **Topology Re-Organization:** Means Recovery from the major topological changes in the network.

7. Security:

- Security is important in Ad hoc wireless network especially in military application. There are two types of attacks in Ad hoc Wireless network:
- Passive Attack (Don't distrusts operation of the N/W)
- Active Attack (Disrupts the operation of the network)

Major Security Threats in Ad hoc Wireless Network:

- **Denial of Service:** Due to this attack network resources are unavailable to other nodes by consuming bandwidth or overloading the system.
- **Resource Consumption:** Resource consumption is done by energy depletion battery power of nodes using heavy traffic and buffer overflow. In case of buffer overflow attack filling the routing table with unwanted entries or packet data.
- **Host Impersonation:** A fake node act as a actual node and respond as a actual or original node and create wrong entries in routing table.
- **Information Discloser:** A compromised node can act as a informer by disclose confidential information to unauthorized nodes.
- **Interference:** A common attack in defense application is to jam the wireless communication by creating a wide spectrum noise.

8. Addressing and Service Discovery:

Every node which is participated in communication have its own unique global address.

- Auto configuration technique is used to allocate the addresses to the nodes.
- Service Discovery protocols are used in authentication, billing and privacy services.

9. Energy Management:

- It is the process of managing energy resources for improving the lifetime of the network.
- Energy management is deals with managing energy resources by means of controlling the battery discharge, adjusting the transmission power and scheduling of power sources.
- Energy Management is classified into :
  - **Battery Energy Management:** Battery energy management is used to improve the battery lifetime with its chemical properties.
  - **Processor Power Management**
    - Clock Speed
    - No. of instruction per unit time
  - **Device Power Management**

MAC Protocol for Ad hoc Wireless Networks

- Nodes in an ad hoc wireless network share a common broadcast radio channel.
- The radio spectrum, the bandwidth available for communication is limited.
- Access to this shared medium should be controlled in such a manner that all **nodes receive a fair share of the available bandwidth**, and that the bandwidth is utilized efficiently.
- Since the characteristics of the wireless medium are completely different from those of the wired medium
- Since ad hoc wireless networks need to address unique issues (such as **node mobility**, **limited bandwidth availability**, **error-prone broadcast channel**, **hidden and exposed terminal problems**, and **power constraints**) that are not applicable to wired networks.
- A different set of protocols is required for controlling access to the shared medium in such networks

Issues in Designing a MAC Protocol for Ad hoc Wireless Networks

- Bandwidth Efficiency:
  - Bandwidth must be utilized in efficient manner
  - Minimal Control overhead
  - BW = ratio of BW used for actual data transmission to the total available BW

- Quality of Service Support:
  - Essential for supporting time-critical traffic sessions such as in military communications
  - They have resource reservation mechanism that takes into considerations the nature of wireless channel and the mobility of nodes

Issues in Designing a MAC Protocol for Ad hoc Wireless Networks

❖ Synchronization:

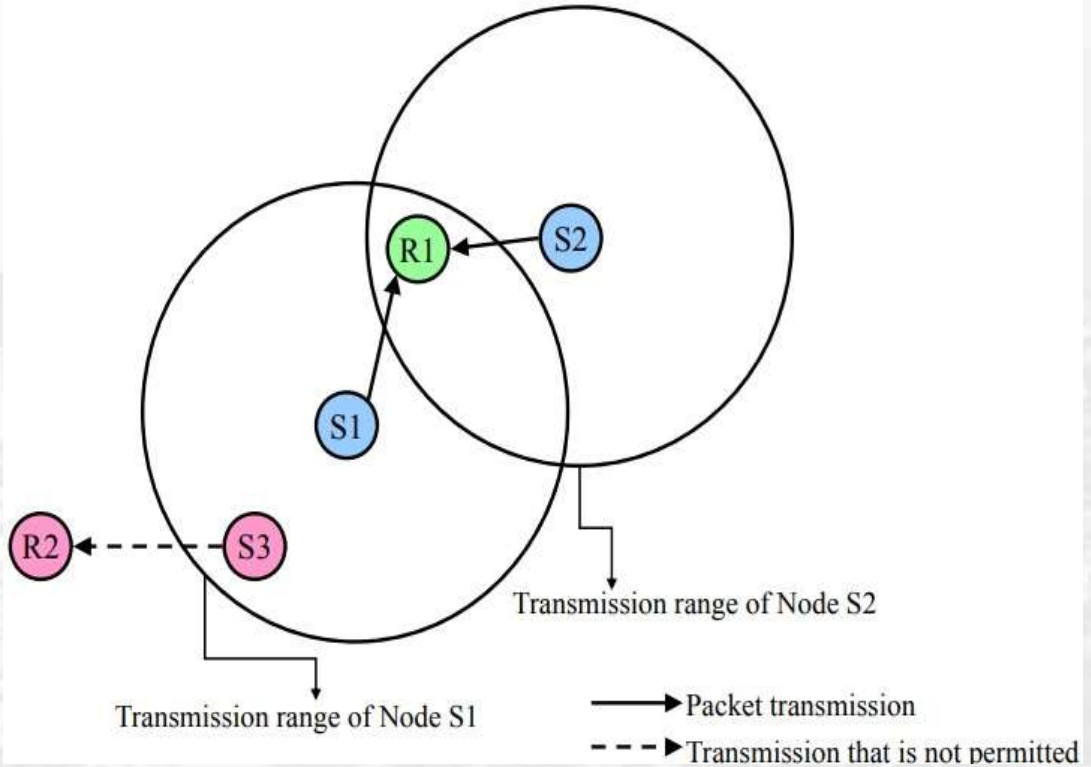
- MAC protocol must consider synchronization between nodes in the network
- Synchronization is very important for BW (time slot) reservation by nodes
- Exchange of control packets may be required for achieving time synchronization among nodes

❖ Hidden and Exposed Terminal Problems:

- The hidden terminal problem refers to the collision of packets at a receiving node due to the simultaneous transmission of those nodes that are not within the direct transmission range of the sender but are within the transmission range of the receiver.
- Collision occurs when both nodes transmit packets at the same time without knowing about the transmission of each other

Issues in Designing a MAC Protocol for Ad hoc Wireless Networks

- S1 and S2 are hidden from each other & they transmit simultaneously to R1 which leads to collision.
- The exposed terminal problem refers to the inability of a node, which is blocked due to transmission by a nearby transmitting node, to transmit to another node .
- If S1 is already transmitting to R1, then S3 cannot interfere with on-going transmission & it cannot transmit to R2.
- The hidden & exposed terminal problems reduce the throughput of a network when traffic load is high



Issues in Designing a MAC Protocol for Ad hoc Wireless Networks

❖ Error-Prone Shared Broadcast Channel

- When a node is receiving data, no other node in its neighborhood should transmit.
- A node should get access to the shared medium only when its transmission do not affect any ongoing session.
- MAC protocol should grant channel access to nodes in such a manner that collisions are minimized.
- Protocol should ensure fair BW allocation.

Issues in Designing a MAC Protocol for Ad hoc Wireless Networks

❖ Distributed Nature/ Lack of Central Coordination:

- Do not have centralized coordinators
- Nodes must be scheduled in a distributed fashion for gaining access to the channel
- MAC protocol must make sure that additional overhead, in terms of BW consumption, incurred due to this control information is not very high.

❖ Mobility of Nodes

- Nodes are mobile most of the time
- The protocol design must take this mobility factor into consideration so that the performance of the system is not affected due to node mobility.

Design Goals of a MAC Protocol for Ad hoc Wireless Networks

The following are the important goals to be met while designing MAC protocol for ad hoc wireless networks:

- The operation of the protocol should be distributed.
- The protocol should provide QoS support for real-time traffic.
- The access delay must be kept low.
- The available bandwidth must be utilized efficiently.
- The protocol should ensure fair allocation of bandwidth to nodes.
- Control overhead must be kept as low as possible.
- The protocol should minimize the effects of hidden and exposed terminal problems.
- The protocol must be scalable to large networks.

Design Goals of a MAC Protocol for Ad hoc Wireless Networks

- It should have power control mechanisms in order to efficiently manage energy consumption of the nodes.
- The protocol should have mechanisms for adaptive data rate control.
- It should try to use directional antennas which can provide advantages such as reduced interference, increased spectrum reuse, and reduced power consumption.
- The protocol should provide time synchronization among nodes.

Issues in Designing a Routing Protocol for Ad hoc Wireless Networks

- Mobility:
  - Ad hoc is highly dynamic due to the movement of nodes
  - Node movement causes frequent path breaks
  - The path repair in wired network has slow convergence

- Bandwidth Constraint:
  - Wireless has less bandwidth due to the limited radio band, Less data rate and difficult to maintain topology information.
  - Frequent change of topology causes more overhead of topology maintenance

Issues in Designing a Routing Protocol for Ad hoc Wireless Networks

- Error-Prone Shared Broadcast Radio Channel
  - Wireless links have time varying characteristics in terms of link capacity and link-error probability.
  - Hidden terminal problem causes packet collision.
  - Target: Interact with MAC layer to find better-quality link and find routes with less crowding.
- Hidden and Exposed Terminal Problems
- Resource Constraints
  - Limited battery life and limited processing power

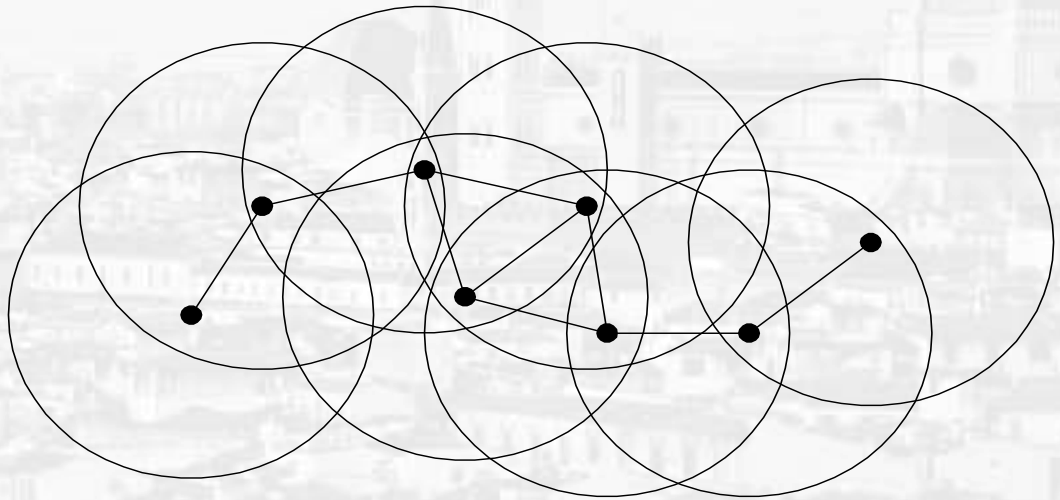
Routing Protocol for Ad Hoc Wireless Networks

Characteristics of an Ideal Routing Protocol for Ad Hoc Wireless Networks

The Routing protocol for ad-hoc wireless networks should have the following characteristics:

- It must be fully distributed
- It must be adaptive to frequent topology changes caused by the mobility of nodes.
- Route computation and maintenance must involve a minimum number of nodes.
- It must be localized, as global state maintenance involves a huge state propagation control overhead.
- It must be loop-free and free from hard/old routes.

- The number of packet collisions must be kept to a minimum by limiting the number of broadcasts made by each node.
- It must converge to optimal routes once the network topology becomes stable.
- Optimally use scarce resource such as bandwidth, computing power, memory, and battery.
- Provide quality of service and support for time sensitive traffic.

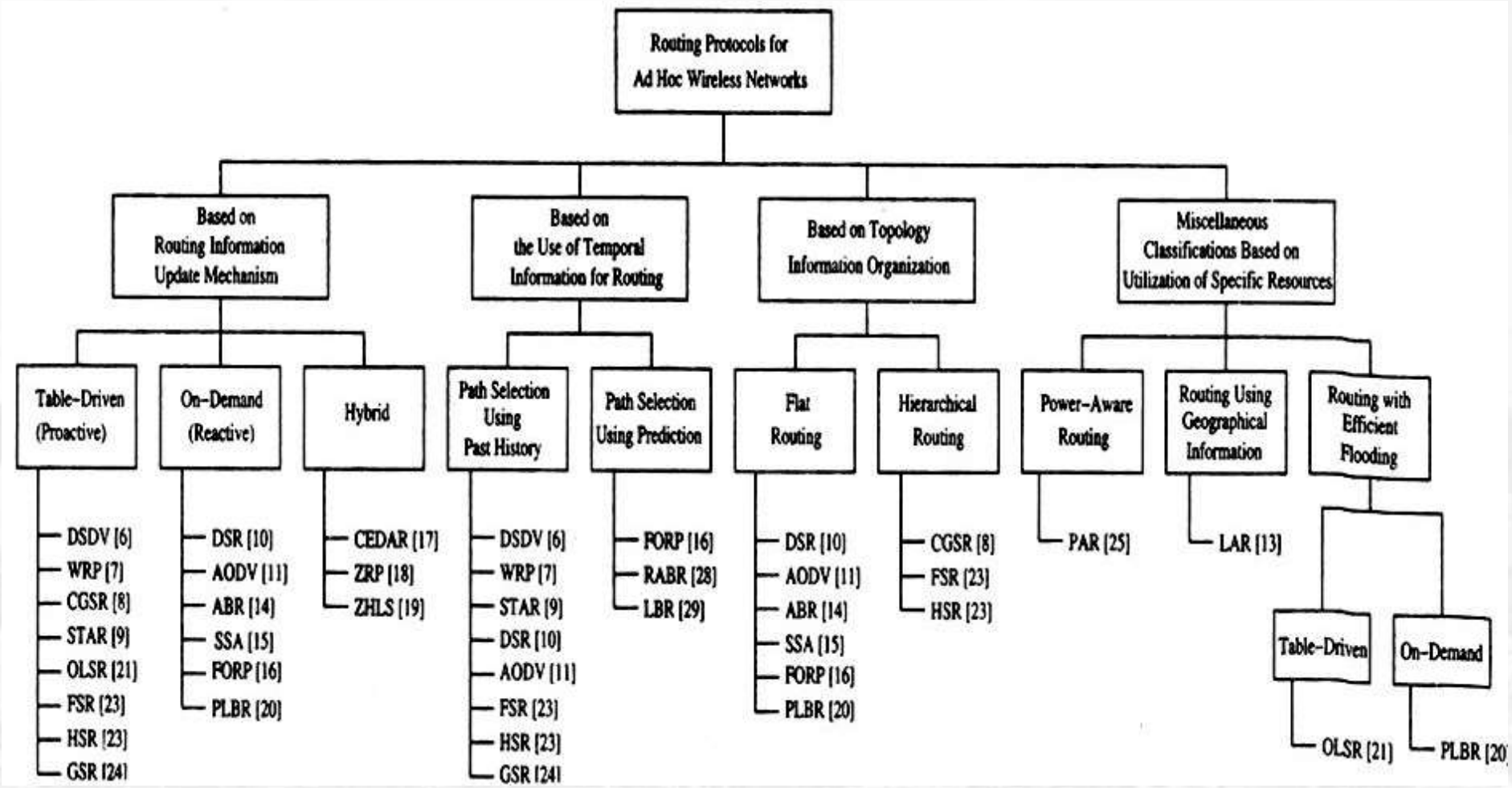


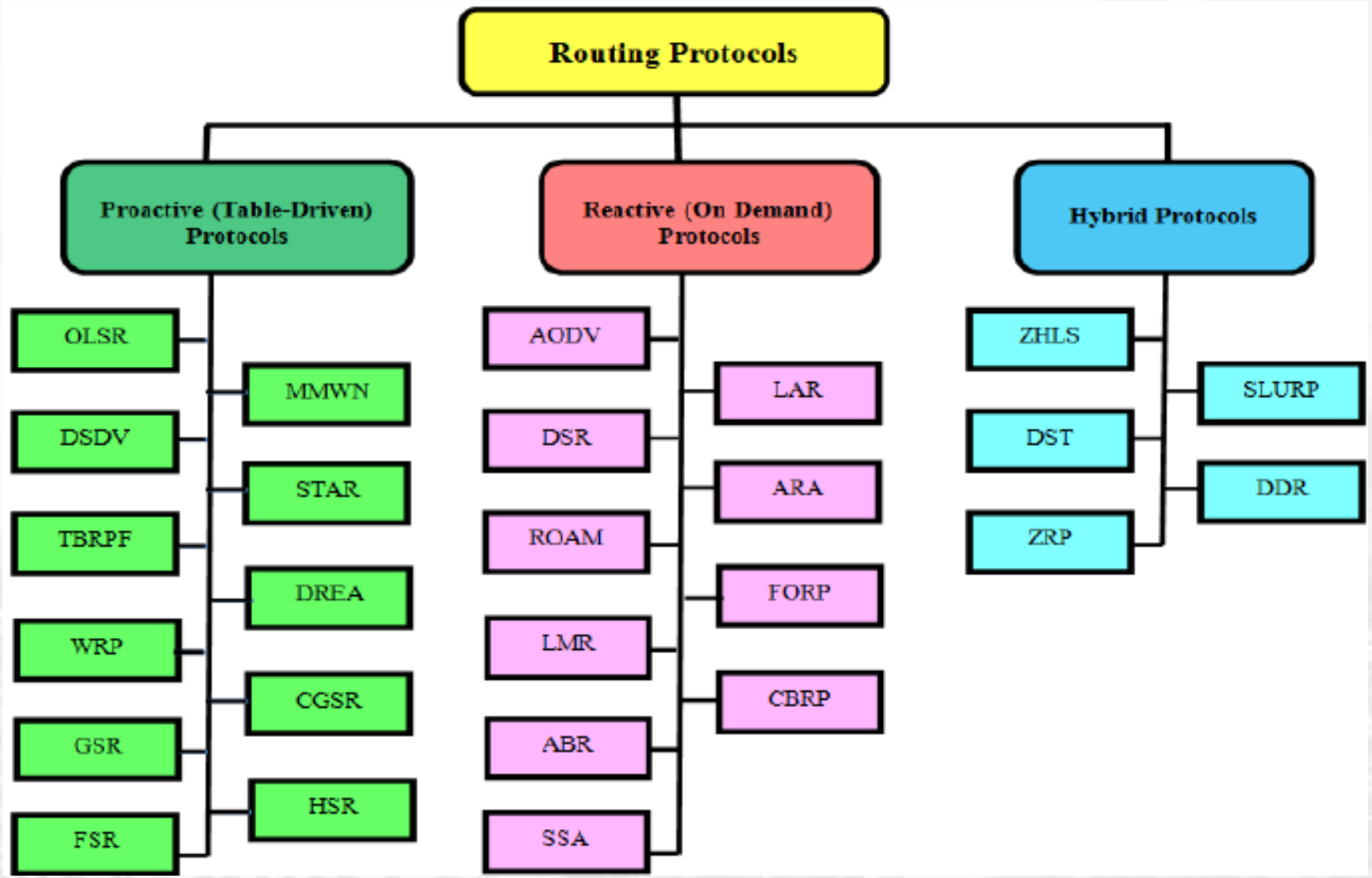
Classifications of Routing Protocols

The routing protocols for ad hoc wireless networks can be broadly classified into four categories based on

- Routing information update mechanism
- Use of temporal information for routing
- Routing topology
- Utilization of specific resources

Classifications of Routing Protocols




Routing Protocols
Proactive (Table-Driven) Protocols
Reactive (On Demand) Protocols
Hybrid Protocols
OLSR
DSDV
TBRPF
WRP
GSR
FSR
MMWN
STAR
DREA
CGSR
HSR
AODV
DSR
ROAM
LMR
ABR
SSA
LAR
ARA
FORP
CBRP
ZHLS
DST
ZRP
SLURP
DDR

- **Based on routing information update mechanism**
  - Proactive (table-driven) routing protocols;
  - Reactive (on-demand) routing protocols;
  - Hybrid protocols.
- **Based on usage of temporal information**
  - Based on past temporal information;
  - Based on future temporal information.
- **Based on the routing topology**
  - Flat topology routing protocols:
  - Hierarchial topology routing protocols:
- **Routing based on utilization of specific resources:**
  - Power-aware routing;
  - Geographical information assisted routing

❖ Proactive protocols:

- These protocols calculate path in advance for all source and destination pairs
- Need periodically exchange topology information to maintain route up to date
- E.g. DSDV (Destination-Sequenced Distance Vector Routing)

❖ Reactive protocols:

- These find the route only when there is data to be transmitted
- E.g. AODV (Adhoc On-demand Distance Vector routing protocol).
- DSR (Dynamic Source Routing protocol).

Routing Protocols

- **Dynamic Source Routing (DSR)**
  On demand source route discovery
- **Ad Hoc On-Demand Distance Vector (AODV)**
  Combination of DSR and DSDV: on demand route discovery with hbh routing
- **Destination-Sequenced Distance Vector (DSDV)**
  DV protocol, destinations advertise sequence number to avoid loops, not on demand
- **Wireless Routing Protocol (WRP)**
  Uses multiple tables
- **Temporally-Ordered Routing Algorithm (TORA)**
  On demand creation of hbh routes based on link-reversal

TABLE-DRIVEN ROUTING PROTOCOLS

TABLE-DRIVEN ROUTING PROTOCOLS

- These protocols are extensions of the wired network routing protocols.
- They maintain the global topology information in the form of tables at every node.
- These tables are updated frequently in order to maintain consistent and accurate network state information.

Examples of protocols

1. Destination Sequenced Distance-Vector routing protocol (DSDV),
2. Wireless Routing Protocol (WRP)
3. Source-tree Adaptive Routing protocol (STAR), and
4. Cluster-head Gateway Switch Routing protocol (CGSR)

Destination-Sequenced Distance-Vector (DSDV)

Destination-Sequenced Distance-Vector (DSDV)

- Enhanced version of the distributed Bellman-Ford algorithm
- Each node maintains a table that contains
  - ✓ the shortest distance and
  - ✓ the first node on the shortest path to every other node in the network.
- Incorporates table updates with increasing sequence number tags to
  - Prevent loops
  - Counter the count-to-infinity problem
  - Faster convergence
- As it is a table-driven routing protocol, routes to all destinations are readily available at every node at all times.
- The tables are exchanged between neighbors at regular intervals to keep an up-to-date view of the network topology.

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 the destination itself
- Each node periodically forwards routing table to 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 decides that a route is broken, it increments the sequence number of the route and advertises it with infinite metric
- Destination advertises new sequence number

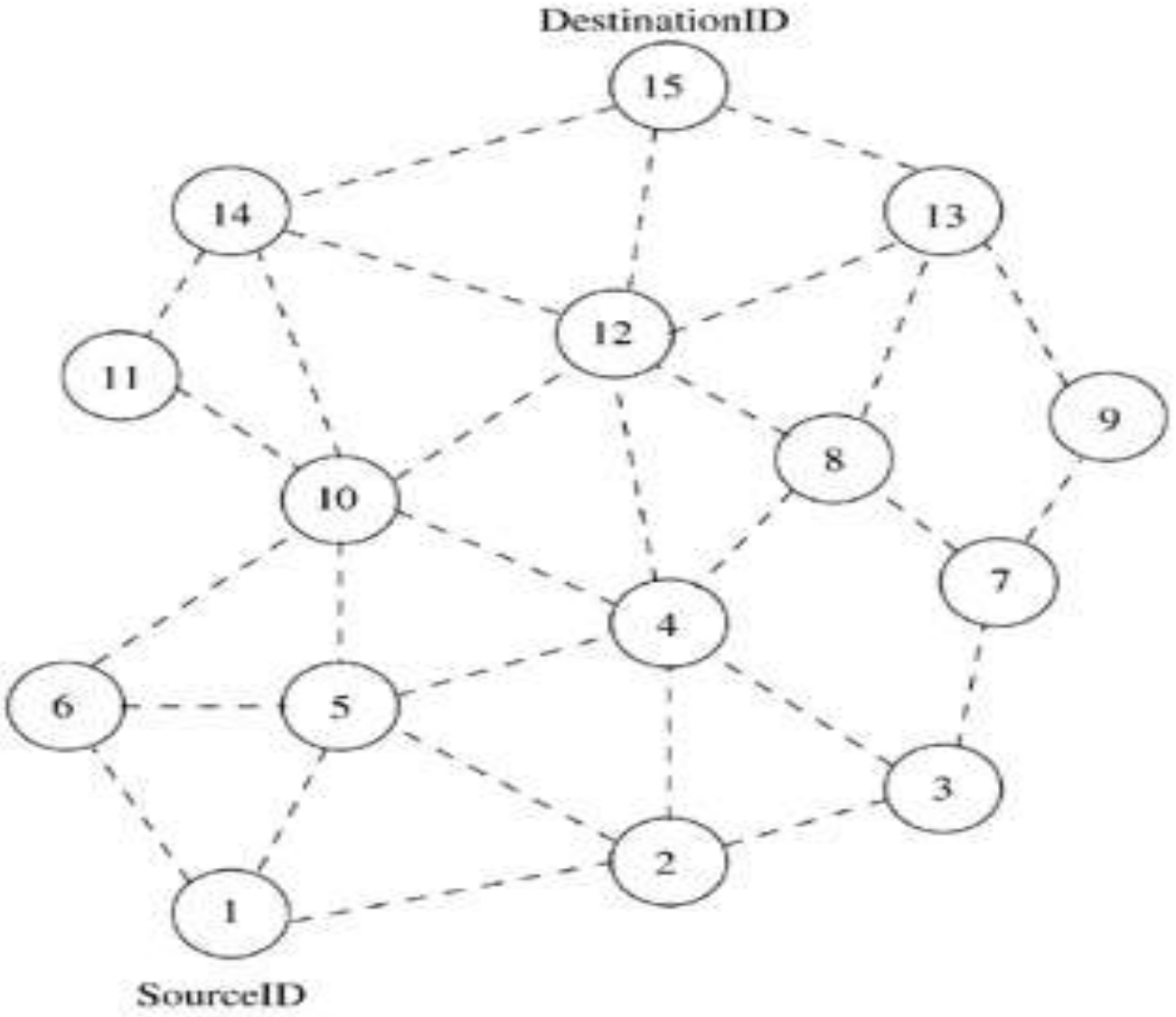
Destination-Sequenced Distance-Vector (DSDV)

- Exchange table between neighbors at regular time interval
- Two types of table updates
  - Incremental update
    - Takes a single Network Data Packet Unit (NDPU)
      - When no significant change in the local topology
  - Full dumps update
    - Takes multiple NDPUs:
      - When local topology changes significantly
      - Or incremental update requires more than a single NDPU

Destination-Sequenced Distance-Vector (DSDV)

- Table updates are initiated by the destination with the new sequence number which is always greater than the previous one.
- Upon receiving an updated table, a node either updates its tables based on the received information or holds it for some time to select the best metric (which may be the lowest number of hops) received from multiple versions of the same update table from different neighboring nodes.
- Based on the sequence number of the table update, it may forward or reject the table.
- Single link break cause propagation of table update information to the whole network
  - With odd sequence (A node always assigns an odd sequence number to the link break update to differentiate it from the even sequence number generated by the destination)
- The changed node informs neighbors about new shortest path while receiving the table update message
  - With even sequence

Route establishment in DSDV

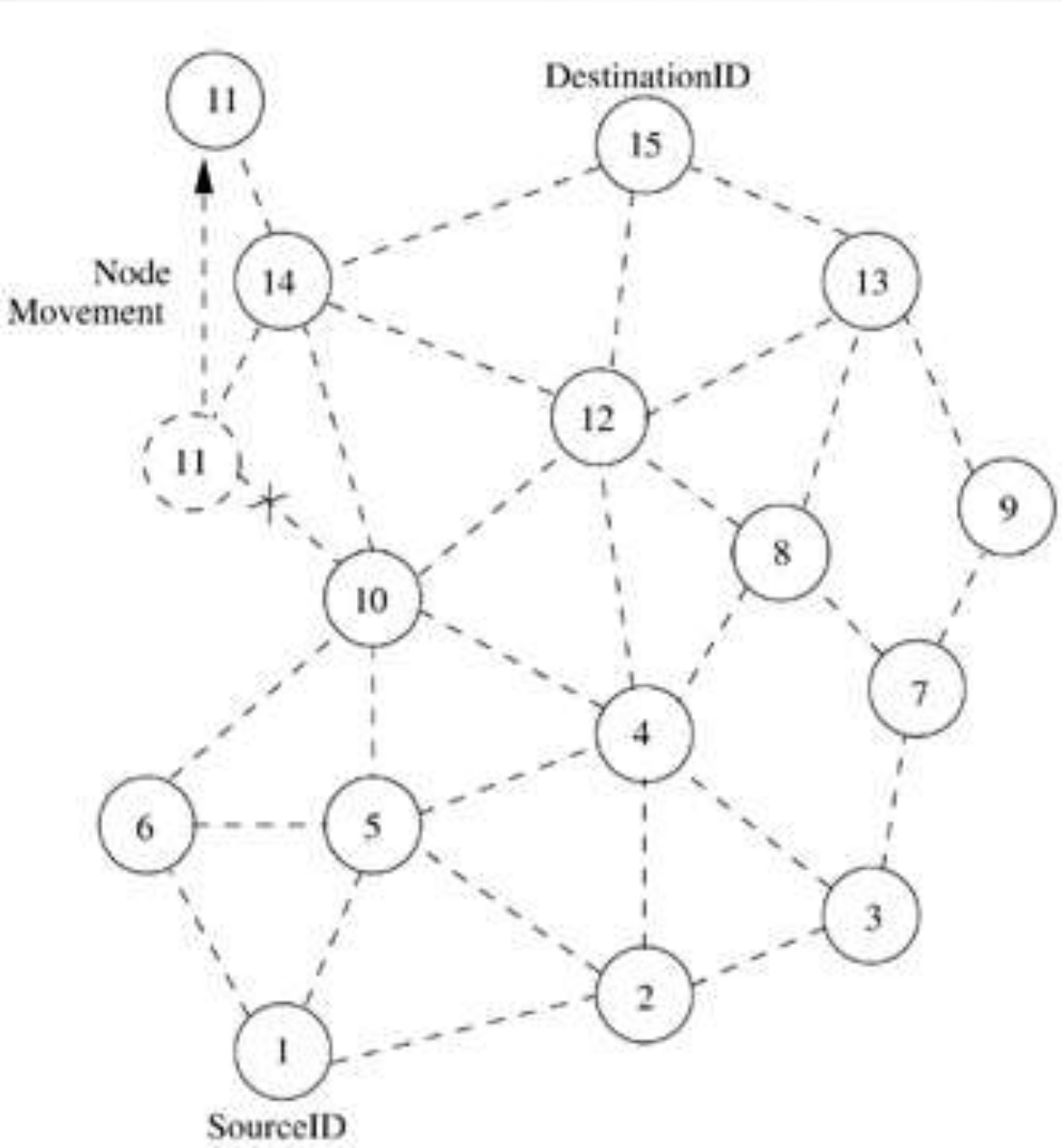


(a) Topology graph of the network

Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	6	3	176
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

(b) Routing table for Node 1

Route maintenance in DSDV



Routing Table for Node 1

Dest	NextNode	Dist	SeqNo
2	2	1	22
3	2	2	26
4	5	2	32
5	5	1	134
6	6	1	144
7	2	3	162
8	5	3	170
9	2	4	186
10	6	2	142
11	5	4	180
12	5	3	190
13	5	4	198
14	6	3	214
15	5	4	256

Destination-Sequenced Distance-Vector (DSDV)

- Advantages:
  - The availability of routes to all destinations at all times implies that much less delay is involved in the route setup process.
  - i.e. Route setup process is very fast
  - Make the existing wired network protocol apply to ad hoc network with fewer modifications

- Disadvantages:
  - Excessive control overhead during high mobility
  - Node must wait for a table update message initiated by the destination node
    - Cause stale routing information at nodes

Wireless Routing Protocol (WRP)

- Similar to DSDV, but it uses multiple tables for routing processes
- Inherits the properties of the distributed Bellman-Ford algorithm
- It employs a unique method of maintaining information regarding the shortest distance to every destination node in the network and the penultimate hop node on the path to every destination node.
- Differs from table maintenance and in the update procedure
  - Uses a set of tables to maintain more accurate information instead of single topology information
  - Not only updates distance for transmitted neighbor but also checks the other neighbors' distance
- The tables that are maintained by a node are the following:
- **Distance Table (DT)**, **Routing Table (RT)**, **Link Cost Table (LCT)**, and **a Message Retransmission List** (MRL).

Wireless Routing Protocol (WRP)

- Distance table
  - Contains the network view of the neighbors of a node, matrix where each element contains the distance and the penultimate node reported by a neighbor for a particular destination

- Routing table
  - contains the up-to date view of the network for all known destinations.
  - Also keeps shortest distance, predecessor node, successor node, and flag indicating status of the path.
  - The path status may be a simple path (correct), or a loop (error), or the destination node not marked (null).

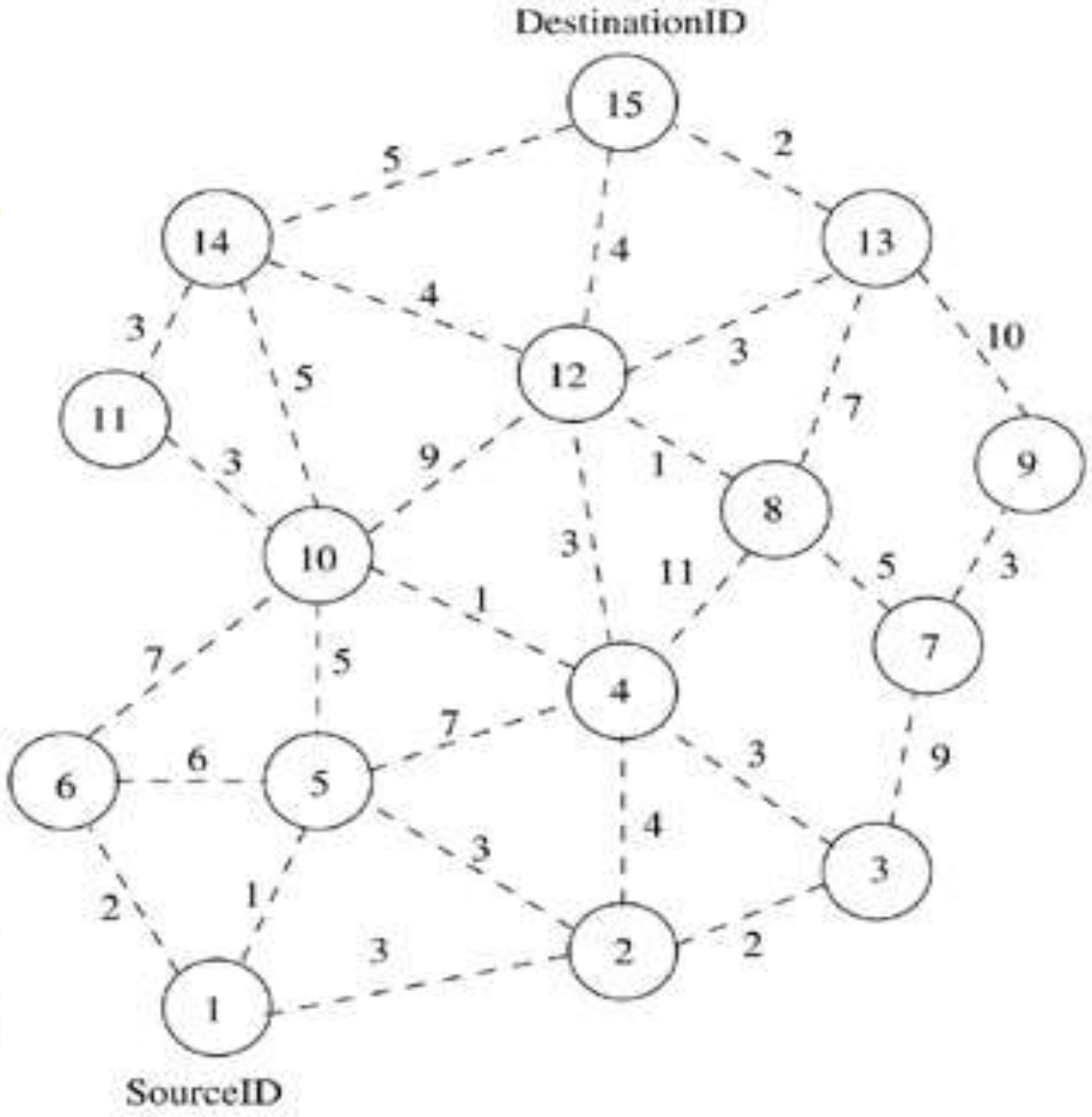
Wireless Routing Protocol (WRP)

- **Link Cost Table**
  - Contains the cost (e. g., the number of hops to reach the destination) of relaying messages through each link.
  - The cost of a broken link is ∞.
  - Also contains the number of update periods (intervals between two successive periodic updates) passed since the last successful update was received from that link. This is done to detect link breaks.

- **Message Retransmission List**
  - Contains an entry for every update message that is to be retransmitted and maintains a counter for each entry.
  - This counter is decremented after every retransmission of an update message.
  - Each update message contains a list of updates.
  - A node also marks each node in the RT that has to acknowledge the update message it transmitted.

Route establishment in WRP

- Here the source of the route is node 1 and the destination is node 15.
- WRP proactively maintains the route to all the destinations, the route to any destination node is readily available at the source node.
- From the routing table shown, the route from node 1 to node 15 has the next node as node 2.
- The predecessor node of 15 corresponding to this route is node 12.
- The predecessor information helps WRP to converge quickly during link breaks.

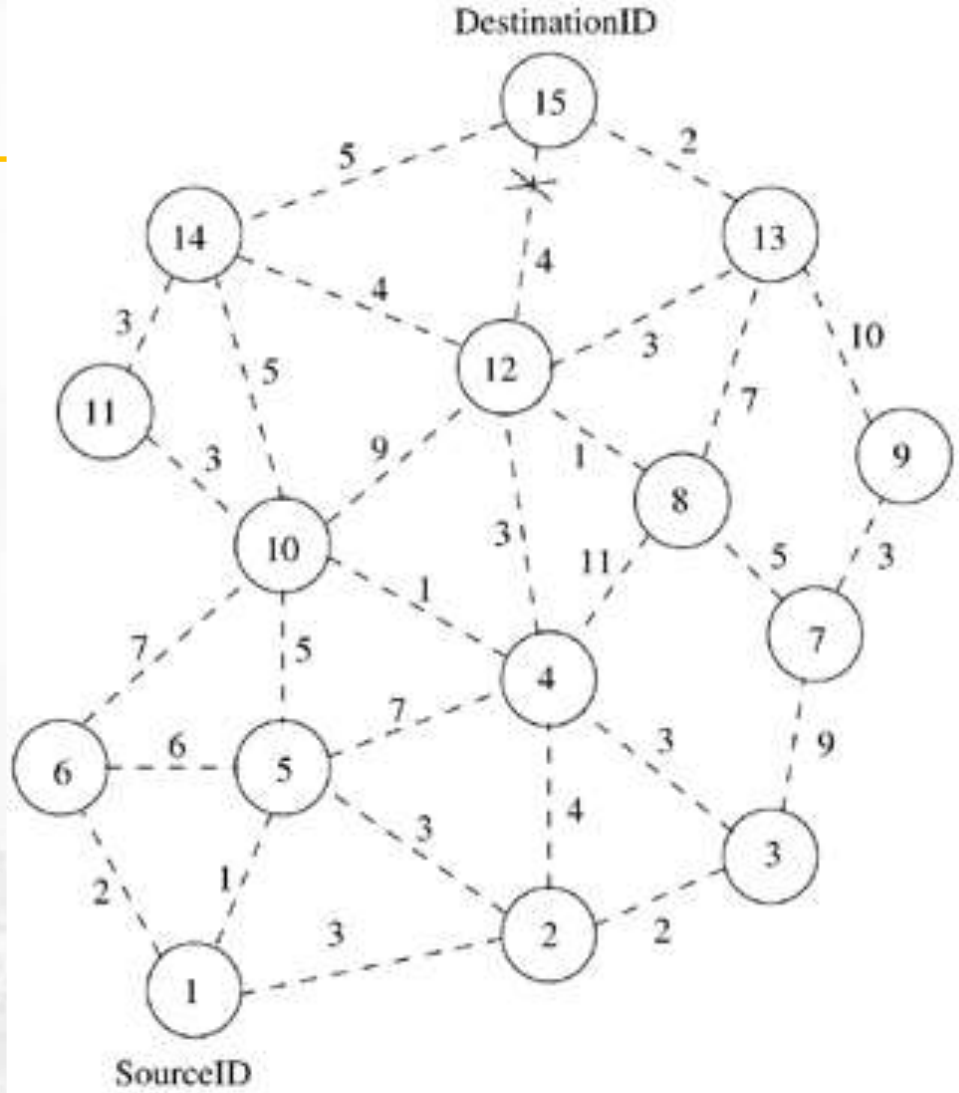


Routing Entry at Each Node for DestinationID 15

Node	NextNode	Pred	Cost
15	15	15	0
14	15	14	5
13	15	13	2
12	15	12	4
11	14	14	8
10	4	12	8
9	13	13	12
8	12	12	5
7	8	12	10
6	10	12	15
5	10	12	13
4	12	12	10
3	4	12	7
2	4	12	11
1	2	12	14

Route maintenance in WRP

- When a node detects a link break, it sends an update message to its neighbors with the link cost of the broken link set to ∞.
- After receiving the update message, all affected nodes update their minimum distances to the corresponding nodes (including the distance to the destination).
- The node that initiated the update message then finds an alternative route, if available from its DT.

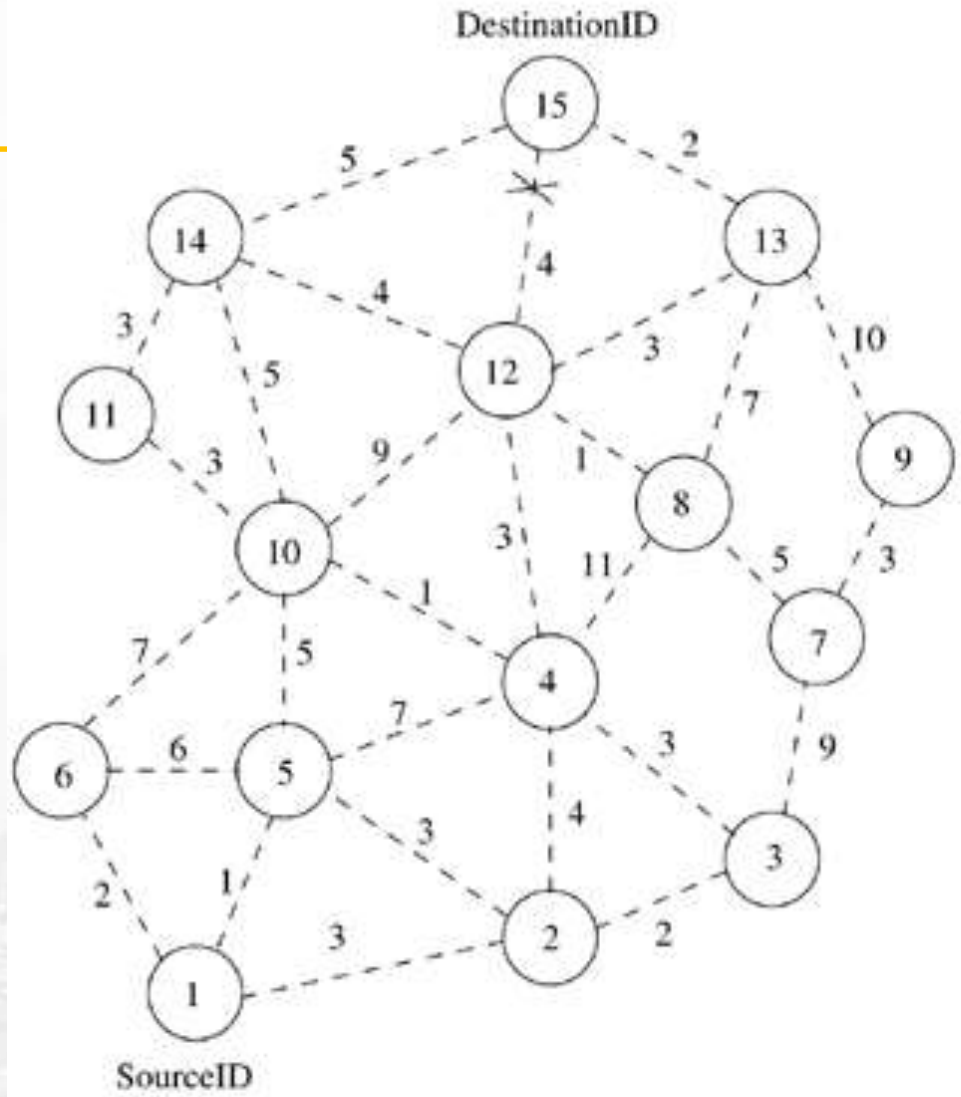


Routing Entry at Each Node for DestinationID 15

Node	NextNode	Pred	Cost
15	15	15	0
14	15	14	5
13	15	13	2
12	15	13	5
11	14	14	8
10	4	13	9
9	13	13	12
8	12	13	6
7	8	13	11
6	10	13	16
5	10	13	14
4	12	13	8
3	4	13	11
2	4	13	12
1	2	13	15

Route maintenance in WRP

- When the link between nodes 12 and 15 breaks, all nodes having a route to the destination with predecessor as node 12 delete their corresponding routing entries.
- Both node 12 and node 15 send update messages to their neighbors indicating that the cost of the link between nodes 12 and 15 is ∞.
- If the nodes have any other alternative route to the destination node 15, they update their routing tables and indicate the changed route to their neighbors by sending an update message.
- A neighbor node, after receiving an update message, updates its routing table only if the new path is better than the previously existing paths.

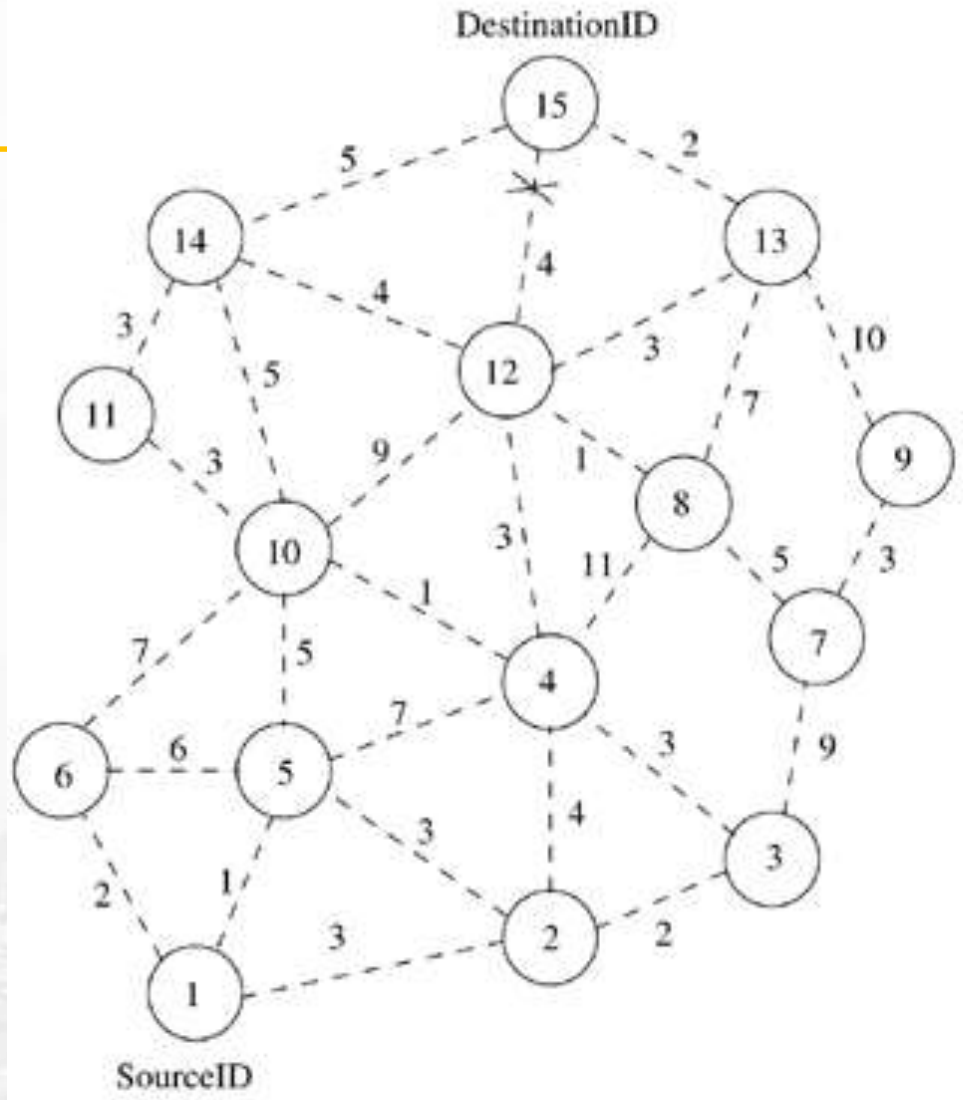


Routing Entry at Each Node for DestinationID 15

Node	NextNode	Pred	Cost
15	15	15	0
14	15	14	5
13	15	13	2
12	15	13	5
11	14	14	8
10	4	13	9
9	13	13	12
8	12	13	6
7	8	13	11
6	10	13	16
5	10	13	14
4	12	13	8
3	4	13	11
2	4	13	12
1	2	13	15

Route maintenance in WRP

- For example, when node 12 finds an alternative route to the destination through node 13, it broadcasts an update message indicating the changed path.
- After receiving the update message from node 12, neighboring nodes 8, 14, 15, and 13 do not change their routing entry corresponding to destination 15 while node 4 and node 10 modify their entries to reflect the new updated path.
- Nodes 4 and 10 again send an update message to indicate the correct path to the destination for their respective neighbors.
- When node 10 receives node 4's update message, it again modifies its routing entry to optimize the path to the destination node (15) while node 4 discards the update entry it received from node 10.



Routing Entry at Each Node for DestinationID 15

Node	NextNode	Pred	Cost
15	15	15	0
14	15	14	5
13	15	13	2
12	15	13	5
11	14	14	8
10	4	13	9
9	13	13	12
8	12	13	6
7	8	13	11
6	10	13	16
5	10	13	14
4	12	13	8
3	4	13	11
2	4	13	12
1	2	13	15

Wireless Routing Protocol (WRP)

- Advantages:
  - WRP has the same advantages as that of DSDV
  - Has faster convergence and involves fewer table updates

- Disadvantages:
  - Need large memory and greater computing power because of the multiple tables
  - At high mobility, the control overhead for updating table entries is almost the same as DSDV
    - Not suitable for highly dynamic and large ad hoc network

Cluster-Head Gateway Switch Routing Protocol (CGSR)

- Uses hierarchical network topology
- Organizes nodes into clusters, with coordination among the members of each cluster entrusted to a special node named as **Cluster Head**.
- Cluster-head is elected dynamically by employing a least cluster change (LCC) algorithm.
- According to this algorithm, a node ceases to be a cluster-head only if it comes under the range of another cluster-head, where the tie is broken either using the lowest ID or highest connectivity algorithm.
- Clustering provides a mechanism to allocate bandwidth, which is a limited resource, among different clusters, thereby improving reuse.

Cluster-Head Gateway Switch Routing Protocol (CGSR)

- Clustering uses CDMA to allocate bandwidth between different clusters
  - Every cluster has its own spreading code
- Cluster-head coordinate channel access based on token-based polling protocol
- All member nodes of a cluster can be reached by the cluster-head within a single hop, thereby enabling the cluster-head to provide improved coordination among nodes that fall under its cluster.

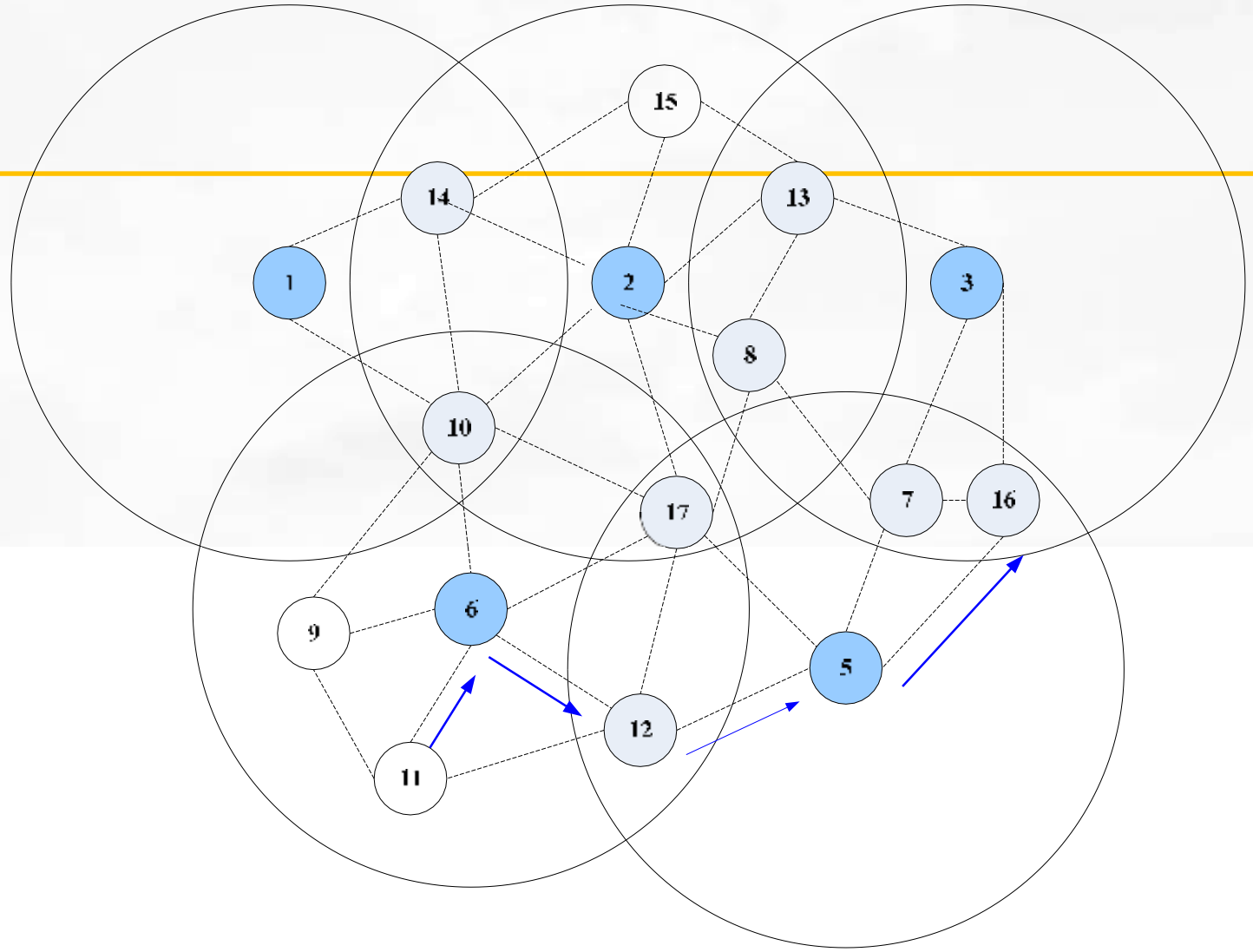
Cluster-Head Gateway Switch Routing Protocol (CGSR)

- Communication passes through the cluster-head
- Communication between two clusters takes place through the common member nodes that are members of both the clusters.
- These nodes which are members of more than one cluster are called as ***gateways***.
  - Listens to multiple spreading codes that are currently in operation in the clusters
  - Becomes a bridge between cluster
  - Gateways are capable of simultaneously communicating over two interfaces can avoid conflict
- Performance of routing is influenced by:
  - Token scheduling for cluster-head
  - Code scheduling for gateway

Cluster-Head Gateway Switch Routing Protocol (CGSR)

- Routing in CGSR is an extension of DSDV
- Each node maintains a routing table containing
  - Destination cluster-head for every node in the network
  - The list of next-hop nodes for reaching every destination cluster
- Route reconfiguration is necessitated by two factor:
  - Cluster-head changes
  - Stale entries in the cluster member table and routing table

- CGSR improves the routing performance by routing packets through the cluster-heads and gateways.



Cluster Member Node Cluster-head Cluster Gateway

Route establishment in CGSR.

Cluster-Head Gateway Switch Routing Protocol (CGSR)

- Advantages:
  - Better bandwidth utilization
  - Easy to implement priority scheduling scheme

- Disadvantages:
  - Increase in path length
  - Instability when cluster-head are high mobility
  - Battery-draining rate at cluster-head is more than a normal node
    - Frequent changes in the cluster-head = multiple path break

ON-DEMAND ROUTING PROTOCOLS

On-Demand Routing Protocols

- On-demand routing protocols execute the path-finding process and exchange routing information only when a path is required by a node to communicate with a destination.
- **Examples**
  - ✓ *Dynamic Source Routing Protocol (**DSR**)*
  - ✓ *Ad Hoc On-Demand Distance-Vector Routing Protocol (**AODV**)*
  - ✓ *Temporally Ordered Routing Algorithm (**TORA**)*

Dynamic Source Routing (DSR) Protocol

- Designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach.
- It is *beacon-less*
- Does not require periodic *hello* packet (*beacon*) transmissions, which are used by a node to inform its neighbors of its presence.
- The basic approach of all on-demand routing protocols during the route construction phase is to establish a route by flooding **RouteRequest** packets in the network.
- The destination node, on receiving a ***RouteRequest*** packet, responds by sending a ***RouteReply*** packet back to the source, which carries the route traversed by the ***RouteRequest*** packet received.

DSR Route Discovery

Route discovery - basic idea

- **Source** broadcasts route-request to **Destination**
- Each node forwards request by adding own address and re-broadcasting
- Requests propagate outward until:
  - Target is found, or
  - A node that has a route to Destination is found

Dynamic Source Routing Protocol (DSR)

The basic approach of this protocol is as follows:

- During route contraction DSR floods a RouteRequest packets in the network
- Intermediate nodes forward RouteRequest if it is not redundant
- Destination node replies with RouteReply
- The RouteReply packet contains the path traversed by RouteRequest packet
- The receiver responds only if this is a first RouteRequest (not duplicate).

- The difference between DSR and other on-demand routing protocols is:
  - on-demand protocols periodically exchange the so-called beacon (hello) packets:
    - hello packets are used to inform neighbors about existence of the node.
  - DSR does not use hello packets.

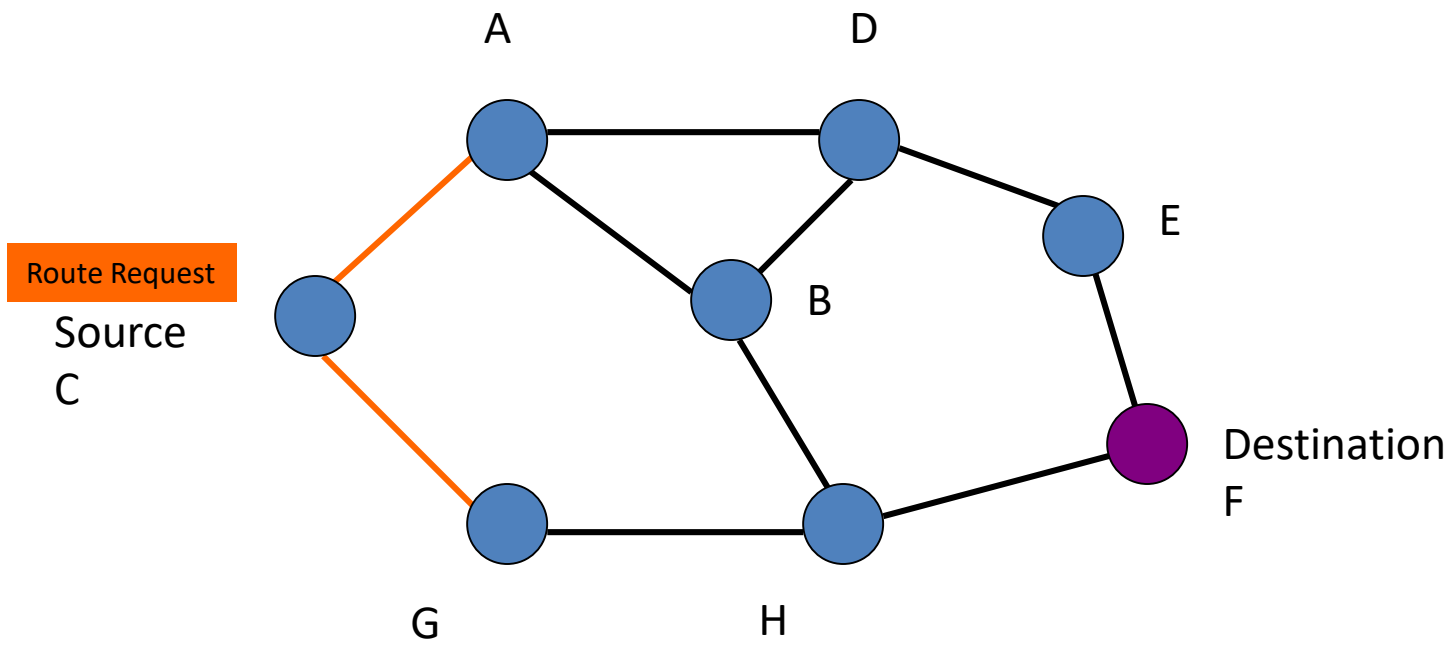
Forwarding Route Requests

A request is forwarded if:

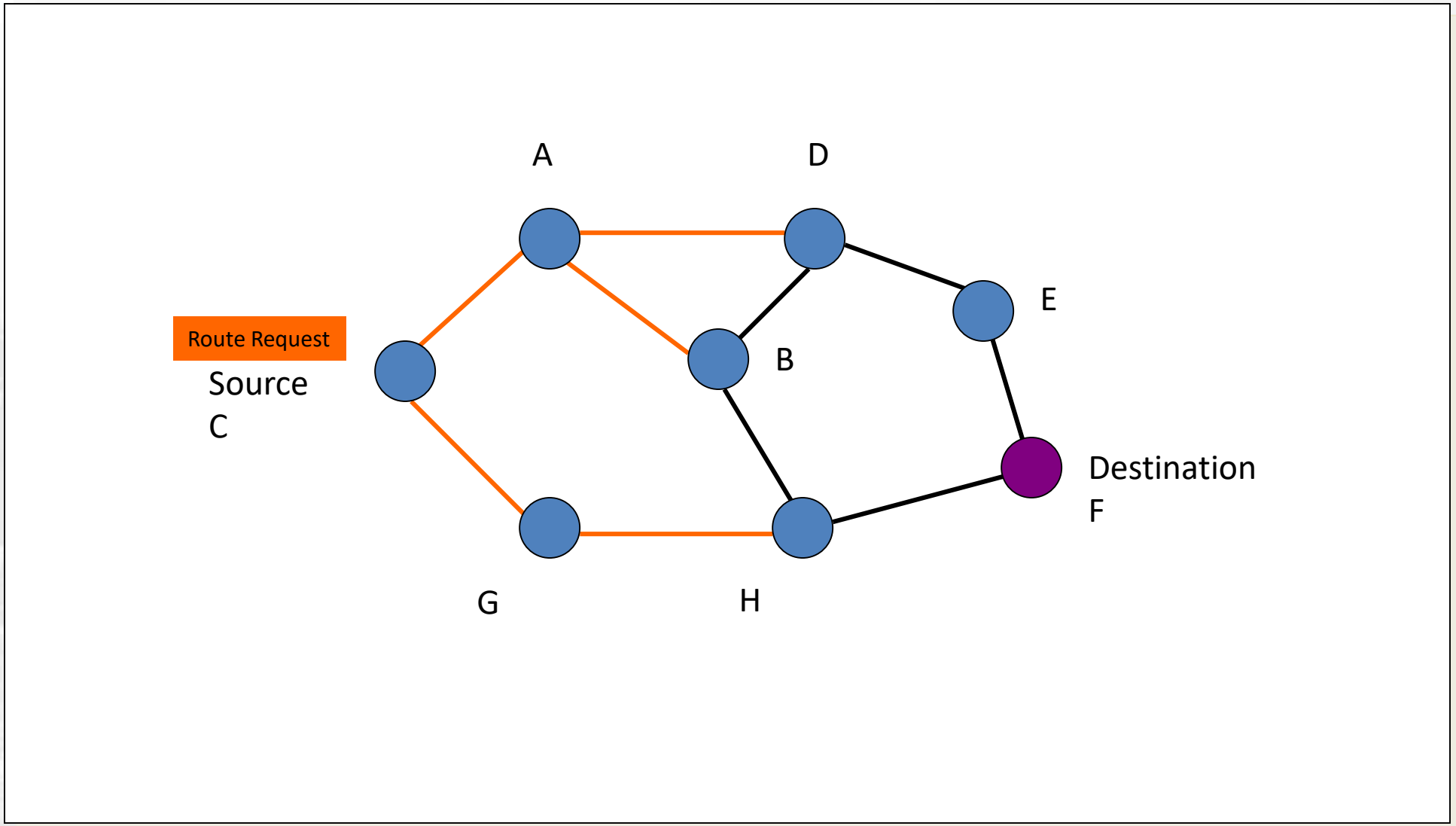
- Node is not the destination
- Node not already listed in recorded source route
- Node has not seen request with same sequence number
- IP TTL field may be used to limit scope

Destination copies route into a Route-reply packet and sends it back to **Source**

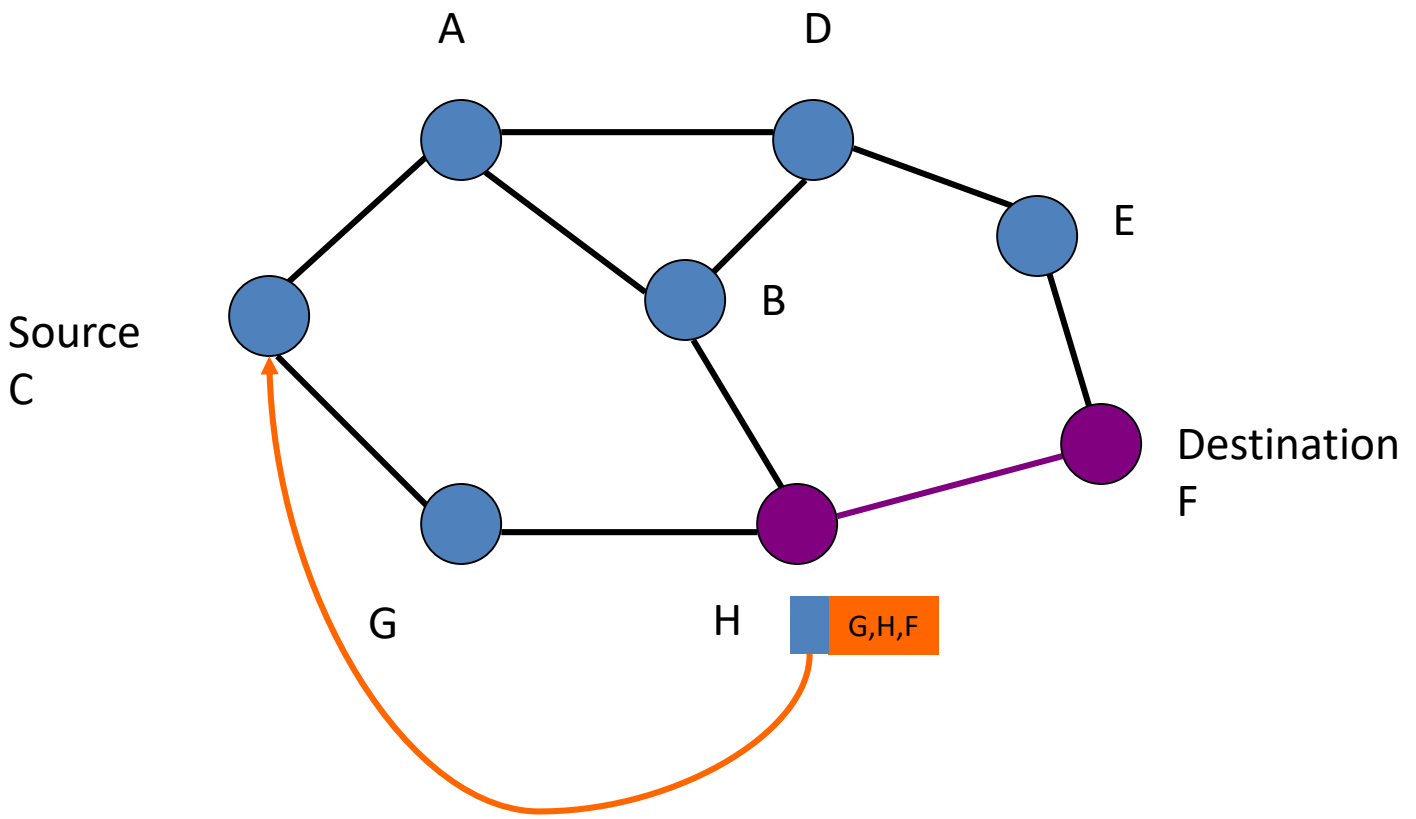
C Broadcasts Route Request to F



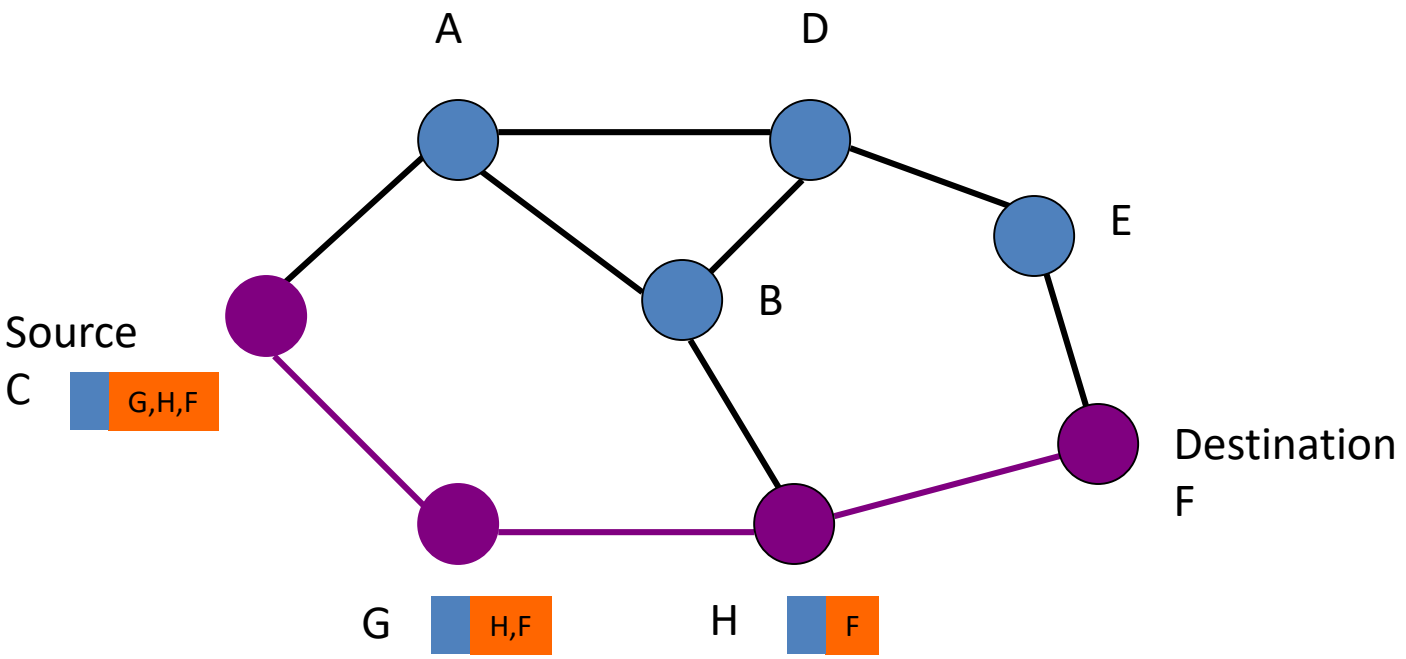
C Broadcasts Route Request to F



H Responds to Route Request



C Transmits a Packet to F



Dynamic Source Routing (DSR) Protocol

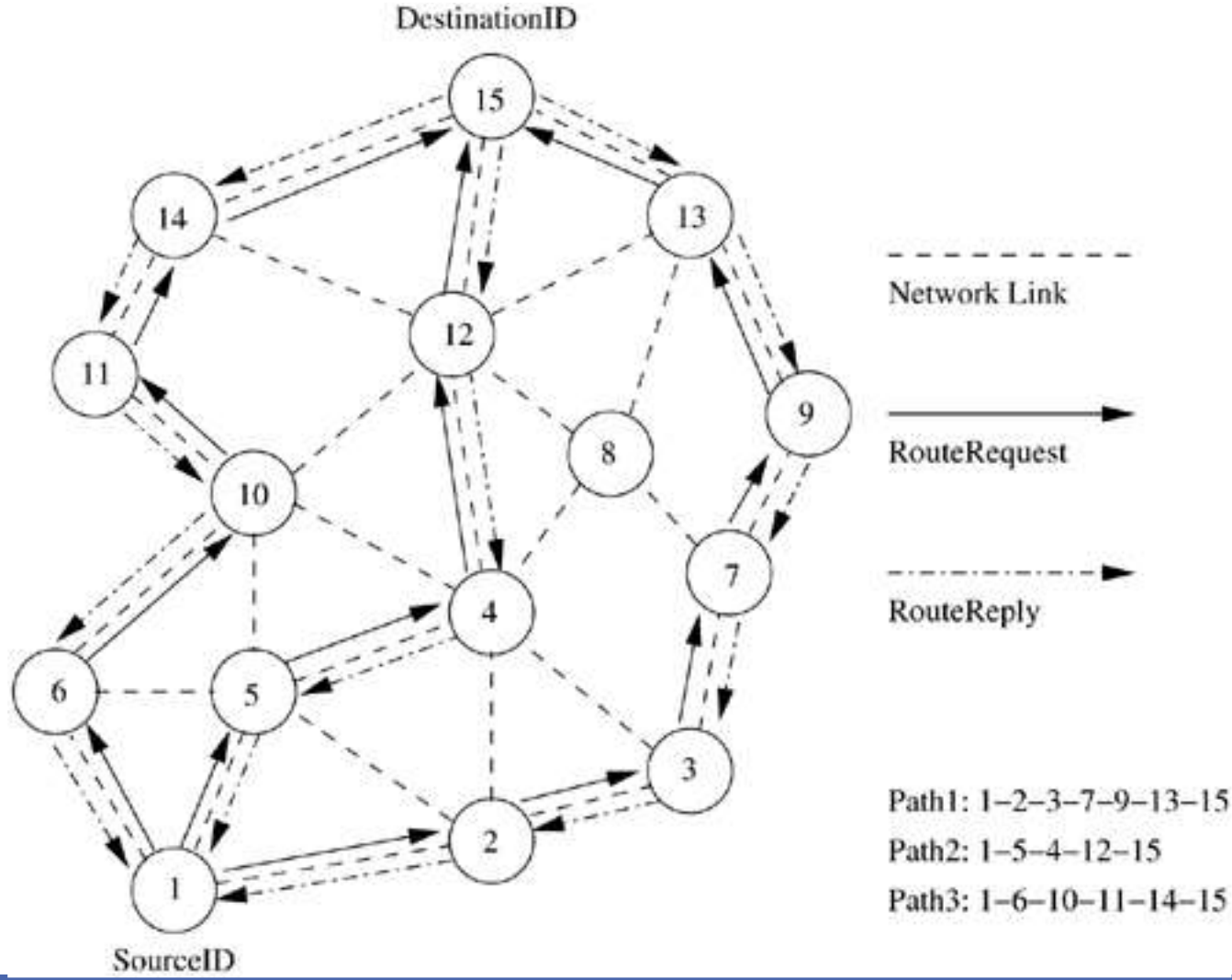
- Consider a source node that does not have a route to the destination.
- When source node has data packets to be sent to that destination, it initiates a RouteRequest packet.
- This RouteRequest is flooded throughout the network.
- Each node, upon receiving a RouteRequest packet, rebroadcasts the packet to its neighbors if it has not forwarded already or if the node is not the destination node, provided the packet's time to live (TTL) counter has not exceeded.

Dynamic Source Routing (DSR) Protocol

- Each ***RouteRequest*** carries a sequence number generated by the source node and the path it has traversed.
- A node, upon receiving a ***RouteRequest*** packet, checks the sequence number on the packet before forwarding it.
- The packet is forwarded only if it is not a duplicate ***RouteRequest***.
- The sequence number on the packet is used to prevent loop formations and to avoid multiple transmissions of the same ***RouteRequest*** by an intermediate node that receives it through multiple paths.
- Thus, all nodes except the destination forward a ***RouteRequest*** packet during the route construction phase.
- A destination node, after receiving the first ***RouteRequest*** packet, replies to the source node through the reverse path the ***RouteRequest*** packet had traversed.

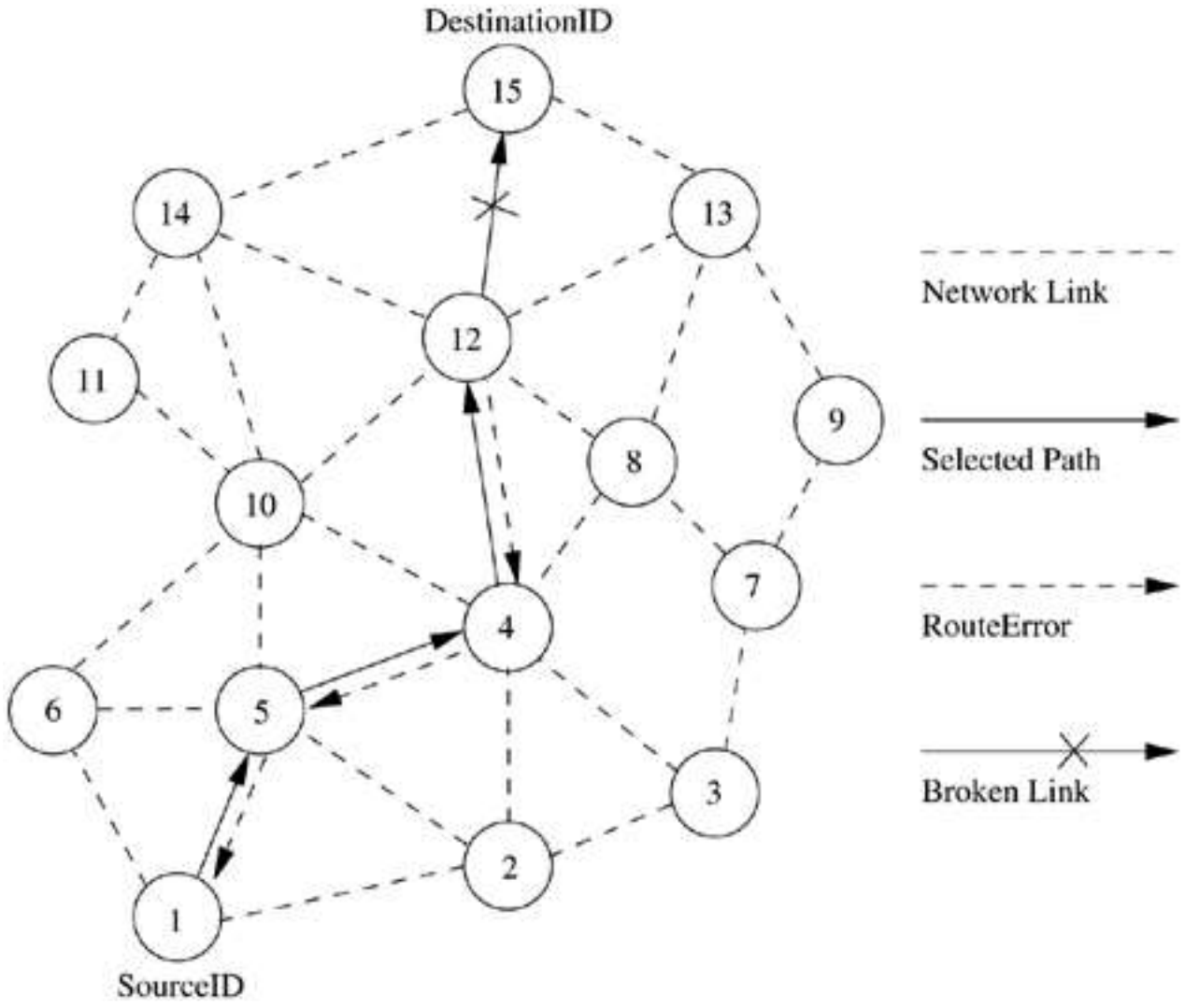
Route establishment in DSR

- Source node 1 initiates a **RouteRequest** packet to obtain a path for destination node 15.
- This protocol uses a route cache that stores all possible information extracted from the source route contained in a data packet.
- Nodes can also learn about the neighboring routes traversed by data packets if operated in the promiscuous mode (the mode of operation in which a node can receive the packets that are neither broadcast nor addressed to itself).
- This route cache is also used during the route construction phase.
- If an intermediate node receiving a **RouteRequest** has a route to the destination node in its route cache, then it replies to the source node by sending a **RouteReply** with the entire route information from the source node to the destination node.



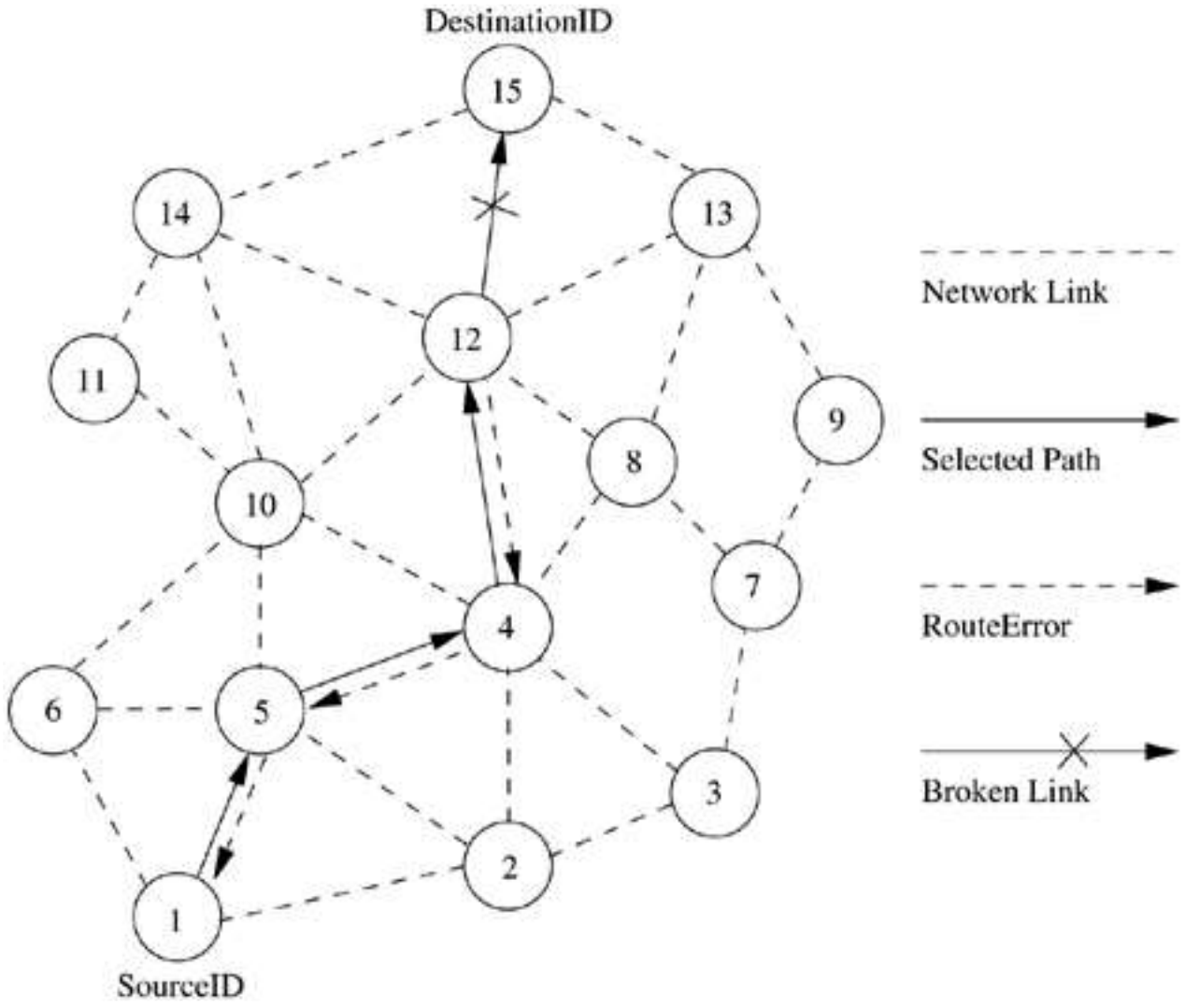
Route maintenance in DSR

- As part of optimizations, if the intermediate nodes are also allowed to originate **RouteReply** packets, then a source node may receive multiple replies from intermediate nodes.
- For example, from Figure, if the intermediate node 10 has a route to the destination via node 14, it also sends the **RouteReply** to the source node.
- The source node selects the latest and best route, and uses that for sending data packets.
- Each data packet carries the complete path to its destination.



Route maintenance in DSR

- When an intermediate node in the path moves away, causing a wireless link to break, for example, the link between nodes 12 and 15 as shown in Figure.
- A **RouteError** message is generated from the node adjacent to the broken link to inform the source node.
- The source node reinitiates the route establishment procedure.
- The cached entries at the intermediate nodes and the source node are removed when a **RouteError** packet is received.
- If a link breaks due to the movement of edge nodes (nodes 1 and 15), the source node again initiates the route discovery process.



Advantages and Disadvantages

- This protocol uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table driven approach.

- In a reactive (on-demand) approach such as this, a route is established only when it is required and hence the need to find routes to all other nodes in the network as required by the table-driven approach is eliminated.

- The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead.

Advantages and Disadvantages

- The disadvantage of this protocol is that the route maintenance mechanism does not locally repair a broken link.
- Stale route cache information could also result in inconsistencies during the route reconstruction phase.
- The connection setup delay is higher than in table-driven protocols.
- Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility.
- Also, considerable routing overhead is involved due to the source-routing mechanism employed

Advantages of DSR:

1. It uses a reactive approach, it means eliminates the need to periodically flood the packet in the network
2. To reduce the control overhead, Route caching mechanism is used

Disadvantages of DSR:

1. The route maintenance mechanism does not locally repair a broken link.

Ad-Hoc on-demand Distance Vector Routing (AODV)

- Reactive algorithms like AODV create routes on-demand.
- Uses an on demand approach for finding routes
- **Route is established only when it is required by a source node for transmitting data packets.**
- It employs destination sequence numbers to identify the most recent path.
- AODV uses symmetric links between neighboring nodes.
- It does not attempt to follow paths between nodes when one of the nodes can not hear the other one

Difference between AODV and DSR

- DSR uses source routing, in which a data packet carries the complete path to be traversed.
- However, in AODV, the source node and the intermediate nodes store the next-hop information corresponding to each flow for data packet transmission.
- In an ondemand routing protocol, the source node floods the ***RouteRequest*** packet in the network when a route is not available for the desired destination.
- It may obtain multiple routes to different destinations from a single ***RouteRequest***.
- The major difference between AODV and other on-demand routing protocols is that **AODV uses a destination sequence number (DestSeqNum) to determine an up-to-date path to the destination.**
- A node updates its path information only if the DestSeqNum of the current packet received is greater than the last DestSeqNum stored at the node.

Ad-Hoc on-demand Distance Vector Routing (AODV)

- Nodes that have not yet participated in any packet exchange (inactive nodes), they do not maintain routing information

- They do not participate in any periodic routing table exchanges

Ad-Hoc on-demand Distance Vector Routing (AODV)

- Each node can become aware of other nodes in its neighborhood by using local broadcasts known as hello messages

- Neighbor routing tables organized to :
  - optimize response time to local movements
  - provide quick response time for new routes requests

Ad-Hoc on-demand Distance Vector Routing (AODV)

AODV main features:

- Broadcast route discovery mechanism
- Bandwidth efficiently (small header information)
- Responsive to changes in network topology
- Loop free routing

Ad-Hoc on-demand Distance Vector Routing (AODV)

- Initiated when a source node needs to communicate with another node for which it has no routing info

- Every node maintains two counters:
  - node_sequence_number
  - broadcast_id

- The source node broadcast to the neighbors a route request packet (called RREQ)

RREQ structure

A ***RouteRequest*** carries

- The source identifier (srcid),
- The destination identifier (destid),
- The source sequence number (srcseqnum),
- The destination sequence Number (destseqnum),
- The broadcast identifier (bcastid), and
- The time to live (TTL) field.

(AODV) Path Discovery

- src_addr and broadcast_id uniquely identifies a RREQ
- broadcast_id is incremented whenever source node issues a RREQ
- Each neighbor either satisfy the RREQ, by sending back a routing reply (RREP), or rebroadcast the RREQ to its own neighbors after increasing the hop_count by one.

(AODV) Path Discovery

- DestSeqNum indicates the freshness of the route that is accepted by the source.
- When an intermediate node receives a *RouteRequest,* it either forwards it or prepares a *RouteReply* if it has a valid route to the destination.
- The validity of a route at the intermediate node is determined by comparing the sequence number at the intermediate node with the destination sequence number in the *RouteRequest* packet.
- If a *RouteRequest* is received multiple times, whichis indicated by the BcastID-SrcID pair, the duplicate copies are discarded
- All intermediate nodes having valid routes to the destination, or the destination node itself, are allowed to send*RouteReply* packets to the source.

(AODV) Path Discovery

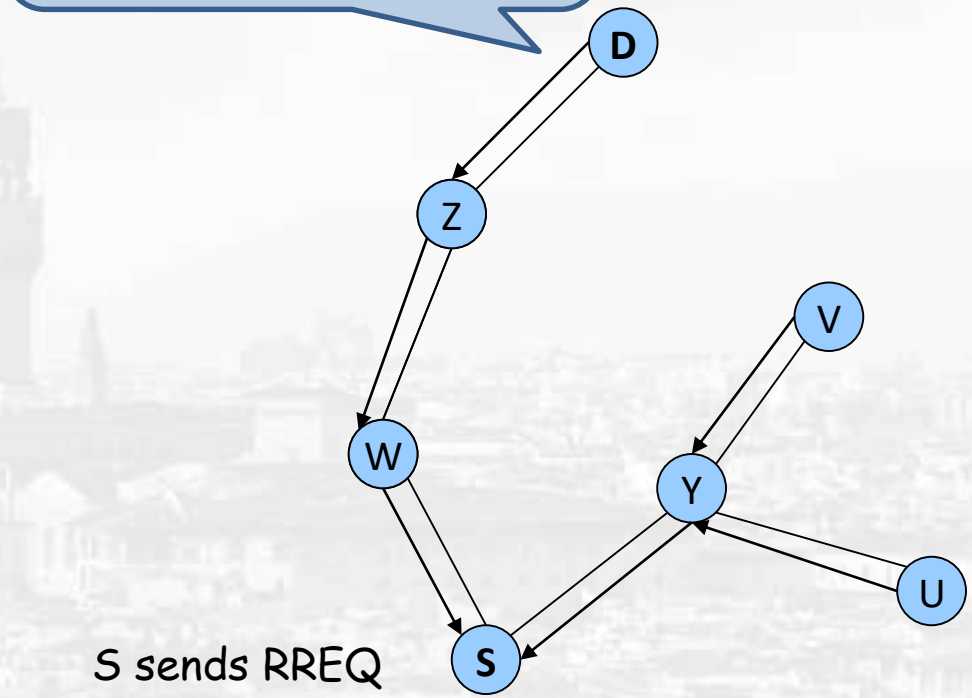
- Every intermediate node, while forwarding a *RouteRequest,* enters the previous node address and its BcastID.
- A timer is used to delete this entry in case a *RouteReply* is not received before the timer expires.
- This helps in storing an active path at the intermediate node as AODV does not employ source routing of data packets.
- When a node receives a *RouteReply* packet, information about the previous node from which the packet was received is also stored in order to forward the data packet to this next node as the next hop toward the destination.

Ad-Hoc on-demand Distance Vector Routing (AODV)

(AODV) Path Discovery

Reverse Path Setup

RREQ reached destination
Reversed path is fully set up
From which RREP can travel back to S



S sends RREQ

S Source node

D Destination node

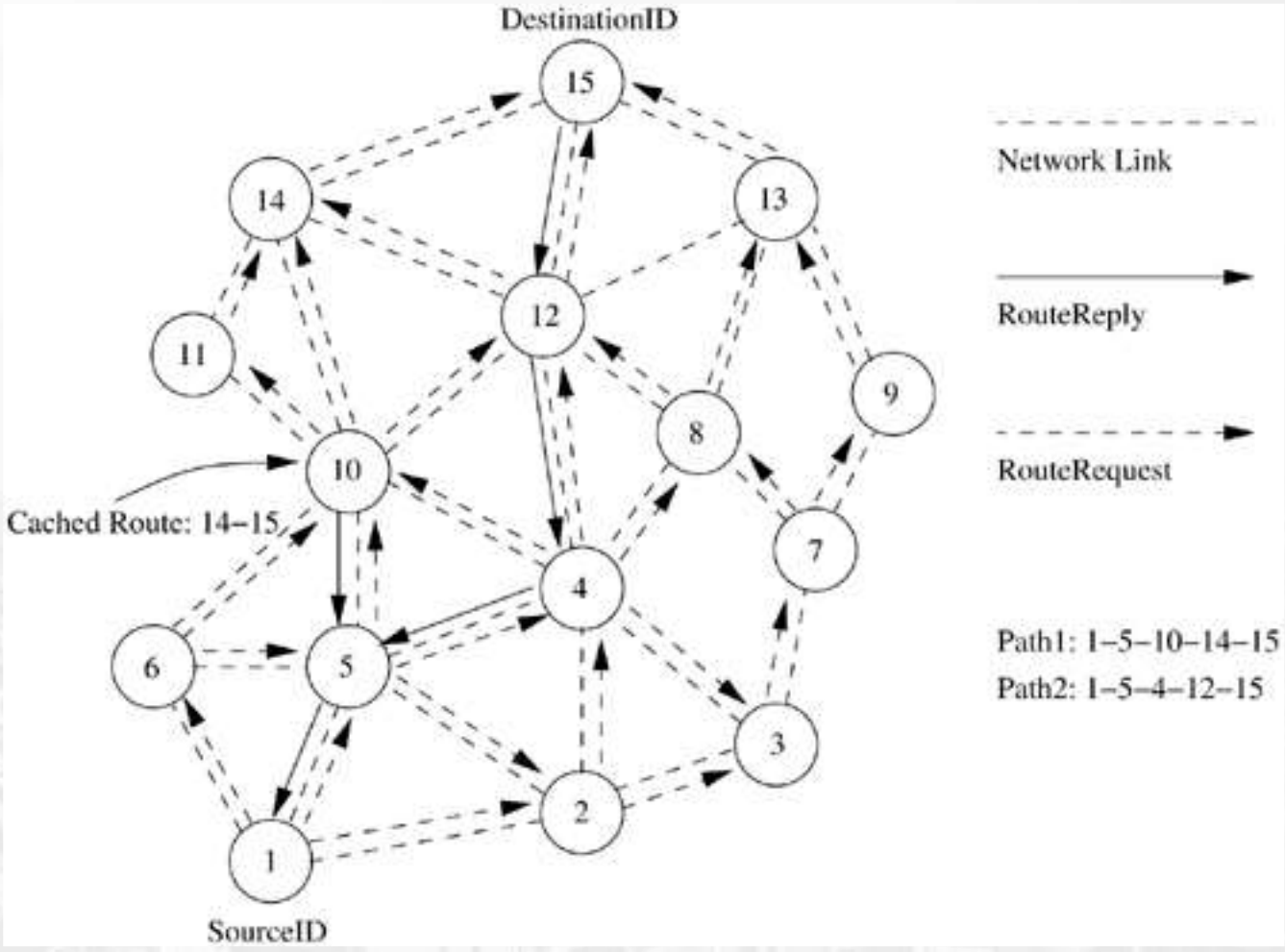
W — Z Neighbor nodes

W, Y can not satisfy RREQ
i. Set up reverse path
ii. Rebroadcast RREQ to neighbors

Z, V, U can not satisfy RREQ
i. Set up reverse path
ii. Rebroadcast RREQ to neighbors

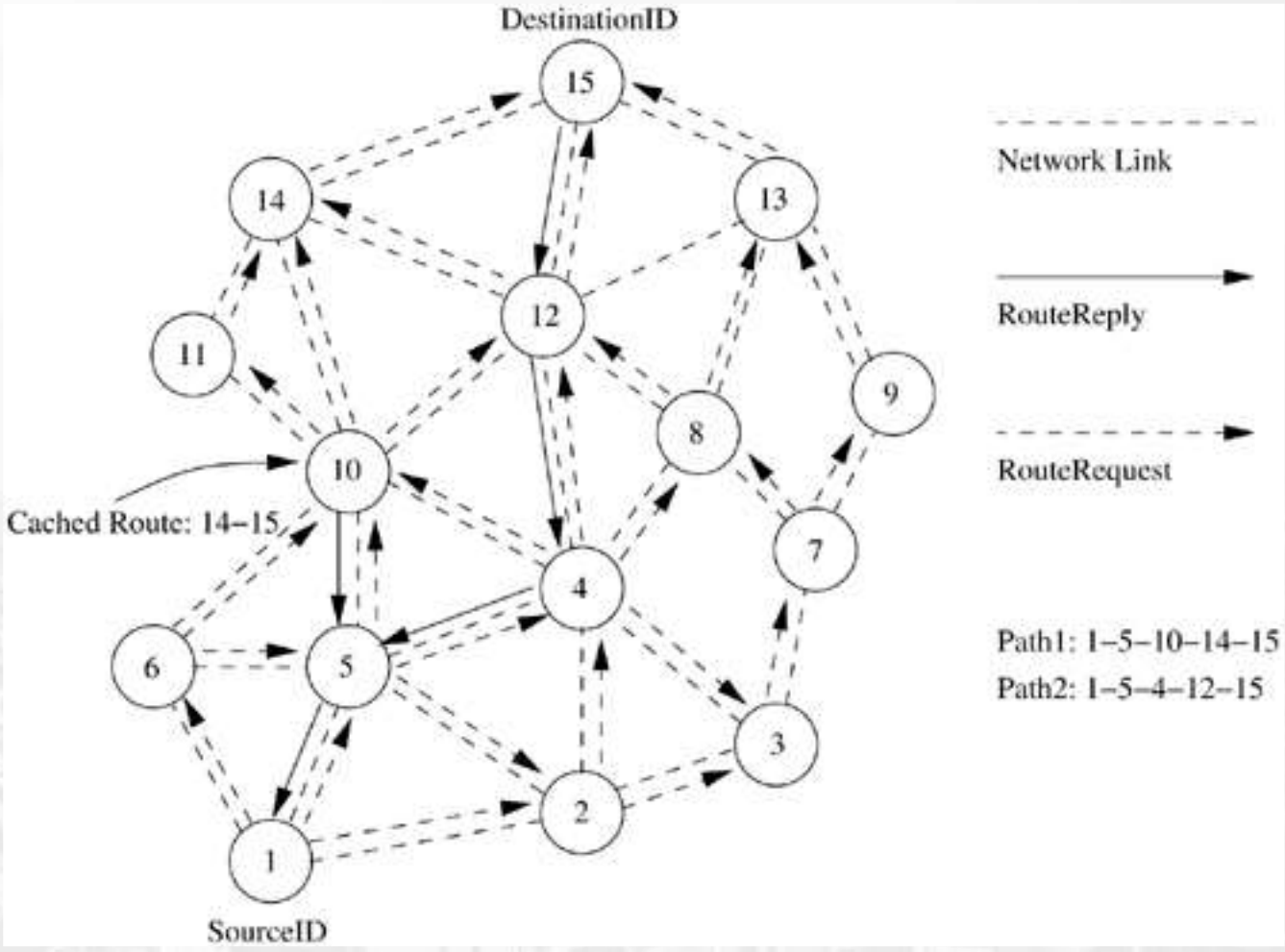
Route establishment in AODV

- Consider, source node 1 initiates a path-finding process by originating a *RouteRequest* to be flooded in the network for destination node 15, assuming that the *RouteRequest* contains the destination sequence number as 3 and the source sequence number as 1.
- When nodes 2, 5, and 6 receive the *RouteRequest* packet, they check their routes to the destination. In case a route to the destination is not available, they further forward it to their neighbors.
- Here nodes 3, 4, and 10 are the neighbors of nodes 2, 5, and 6.
- This is with the assumption that intermediate nodes 3 and 10 already have routes to the destination node, that is, node 15 through paths 10-14-15 and 3-7-9-13-15, respectively.



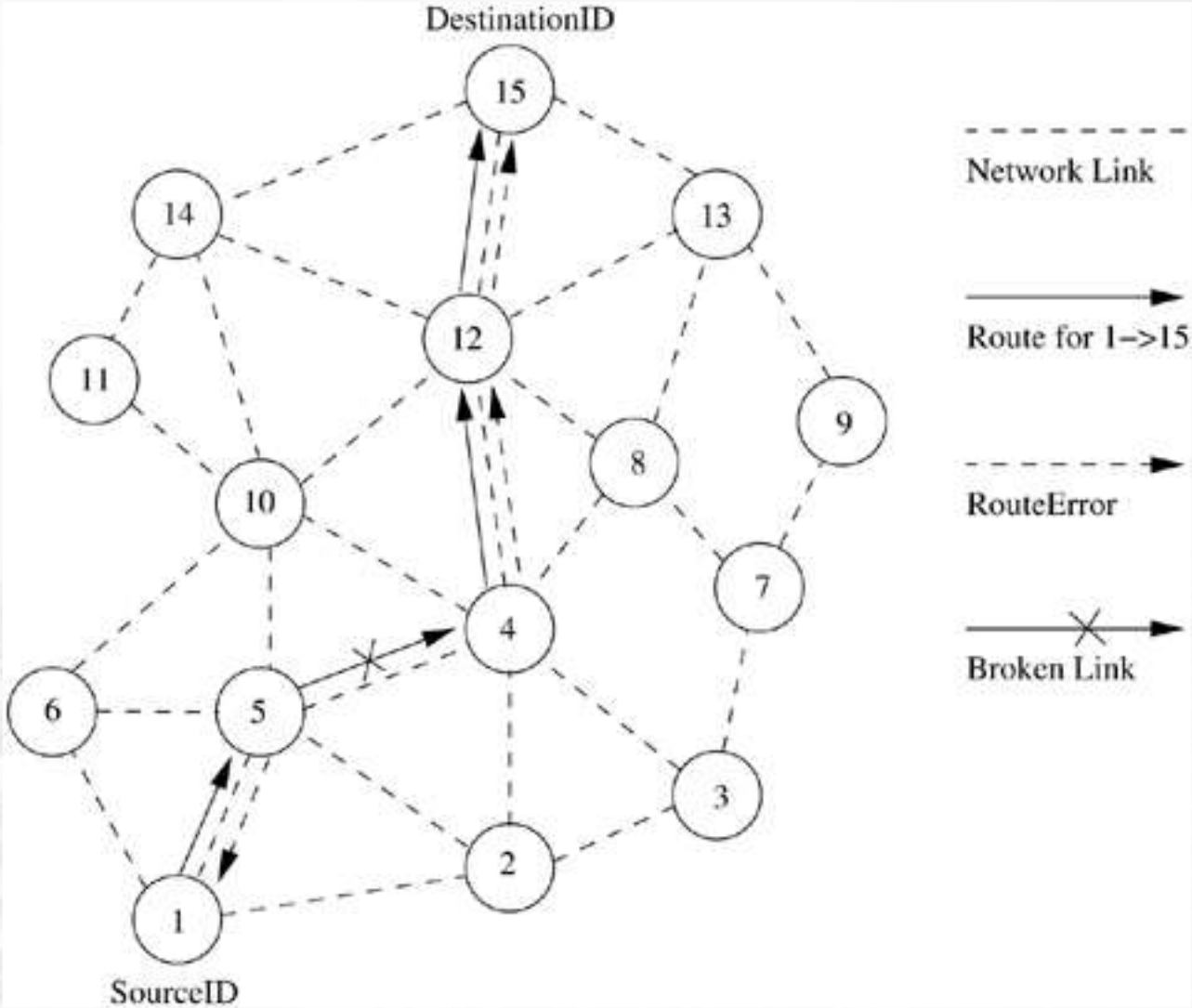
Route establishment in AODV

- If the destination sequence number at intermediate node 10 is 4 and is 1 at intermediate node 3, then only node 10 is allowed to reply along the cached route to the source.
- This is because node 3 has an older route to node 15 compared to the route available at the source node (the destination sequence number at node 3 is 1, but the destination sequence number is 3 at the source node), while node 10 has a more recent route (the destination sequence number is 4) to the destination.
- If the *RouteRequest* reaches the destination (node 15) through path 4-12-15 or any other alternative route, the destination also sends a *RouteReply* to the source.
- In this case, multiple*RouteReply* packets reach the source. All the intermediate nodes receiving a *RouteReply* update their route tables with the latest destination sequence number.
- They also update the routing information if it leads to a shorter path between source and destination.



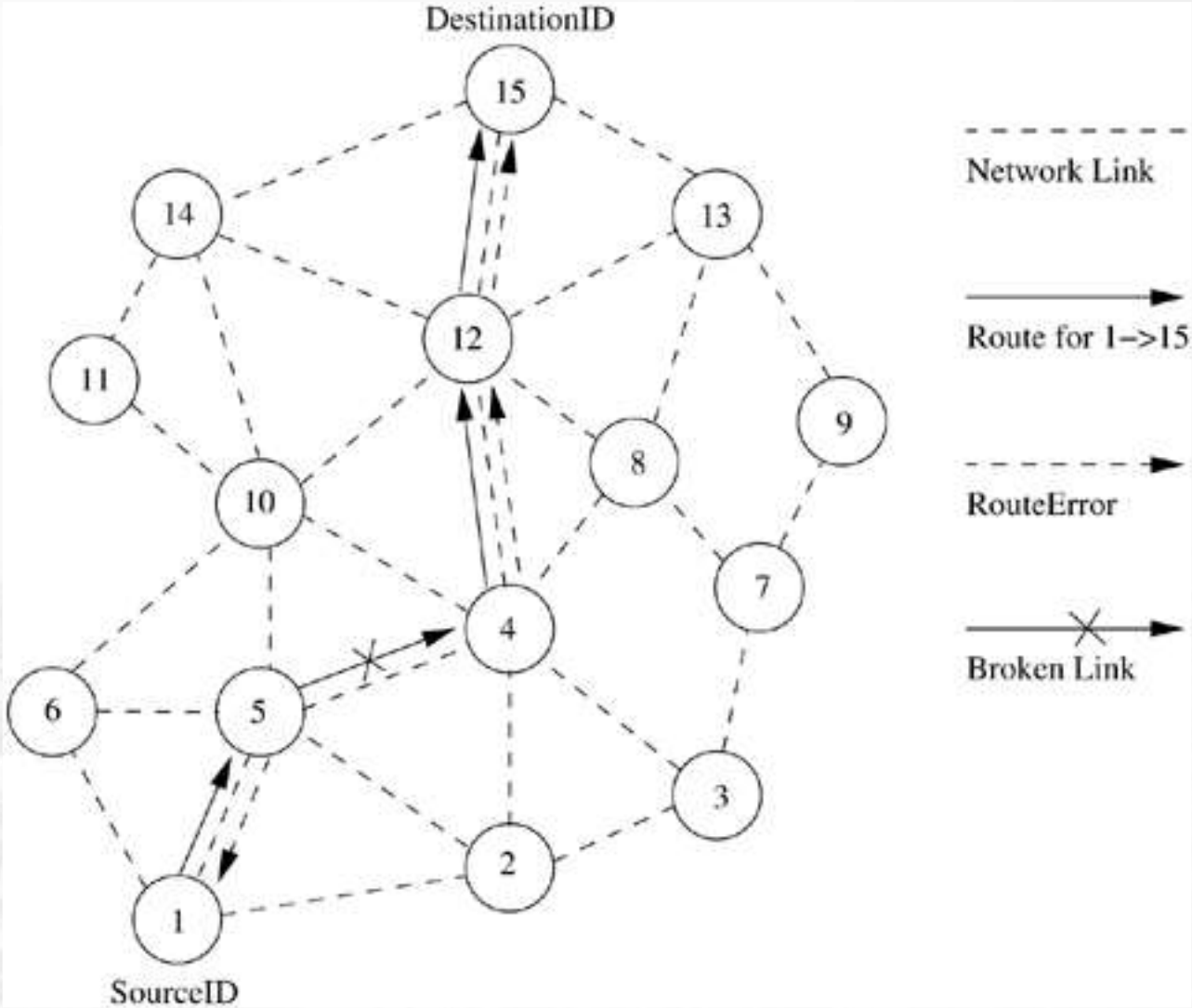
Route maintenance in AODV

- AODV does not repair a broken path locally.
- When a link breaks, which is determined by observing the periodical *beacons* or through link-level acknowledgments, the end nodes (*i.e.*, source and destination nodes) are notified.
- When a source node learns about the path break, it reestablishes the route to the destination if required by the higher layers.
- If a path break is detected at an intermediate node, the node informs the end nodes by sending an unsolicited *RouteReply* with the hop count set as ∞.



Route maintenance in AODV

- Consider, When a path breaks, for example, between nodes 4 and 5, both the nodes initiate RouteError messages to inform their end nodes about the link break.
- The end nodes delete the corresponding entries from their tables.
- The source node reinitiates the path finding process with the new BcastID and the previous destination sequence number.



Advantages of AODV:

1. Routes are maintained only between nodes that need to communicate. This reduces the overhead of route maintenance.
2. Route caching can further reduce route discovery overhead

Disadvantages of AODV:

1. Multiple RouteReply packets can lead to heavy control overhead.
2. The periodic beaconing packets leads to unnecessary bandwidth consumption

Comparison of AODV and DSR

Main common features:

- On-demand route requesting
- Route discovery based on requesting and replying control packets
- Broadcast route discovery mechanism

Comparison of AODV and DSR

Main common features: (continue)

- Route information is stored in all intermediate nodes along the established path
- Inform source node for a broken links
- Loop-free routing

Comparison of AODV and DSR

Main differences:

- DSR can handle uni and bi-directional links, AODV uses only bi-directional
- In DSR, using a single RREQ - RREP cycle, source and intermediate nodes can learn routes to other nodes on the route
- DSR maintains many alternate routes to the destination, instead of AODV that maintains at most one entry per destination

Comparison of AODV and DSR

Main differences: (continue)

- DSR doesn’t contain any explicit mechanism to expire stale routes in the cache , In AODV if a routing table entry is not recently used , the entry is expired
- DSR can’t prefer “fresher” routes when faced multiple choices for routes. In contrast, AODV always choose the fresher route (based on destination sequence numbers)

Comparison of AODV and DSR

Main differences: (continue)

- DSR's RREQ has variable length depending on the nodes that the packet has traveled. AODV's RREQ size is constant

- As a result DSR's header overhead may increase as more nodes become active, so we expect that AODV throughput in those scenarios to be better

Temporally Ordered Algorithm (TORA)

Temporally Ordered Algorithm (TORA)

- A source-initiated on-demand routing protocol which uses a link reversal routing algorithms
- Provide loop-free multipath routes to a destination node
- Beacon-base
- In TORA, each node maintains its one-hop local topology information and also has the capability to detect partitions.
- TORA has the unique property of limiting the control packets to a small region during the reconfiguration process initiated by a path break.
- Three main functions
  - Route Establishing: when a node requires a path to a destination but does not have any directed link
    - Query packet
  - Route Maintenance: Update packet
  - Route Erasing: CLR packet

illustration of temporal ordering in TORA

- Figure shows the distance metric used in TORA which is nothing but the length of the path, or the height from the destination.
- H(N) denotes the height of node N from the destination.
- TORA has three main functions: establishing, maintaining, and erasing routes.
- The route establishment function is performed only when a node requires a path to a destination but does not have any directed link.
- This process establishes a destination-oriented directed acyclic graph (DAG) using a *Query/Update* mechanism.

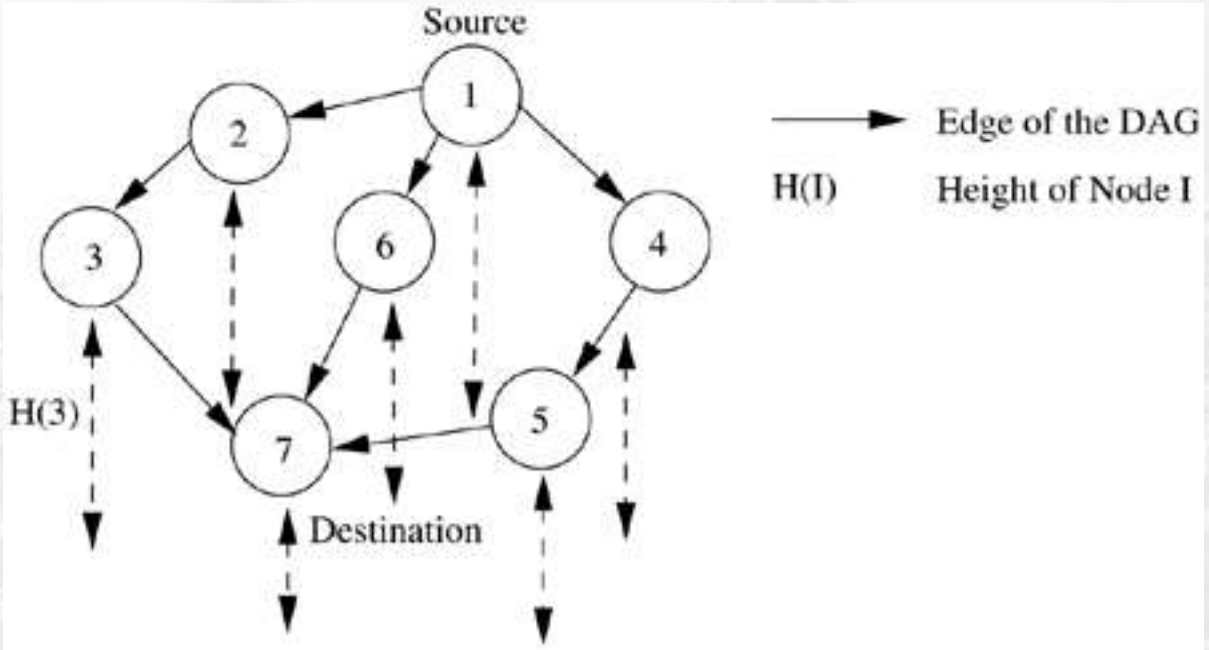


illustration of temporal ordering in TORA

- Consider the network topology shown in Figure
- When node 1 has data packets to be sent to the destination node 7, a Query packet is originated by node 1 with the destination address included in it.
- This Query packet is forwarded by intermediate nodes 2, 3, 4, 5, and 6, and reaches the destination node 7, or any other node which has a route to the destination.
- The node that terminates (in this case, node 7) the Query packet replies with an Update packet containing its distance from the destination (it is zero at the destination node).

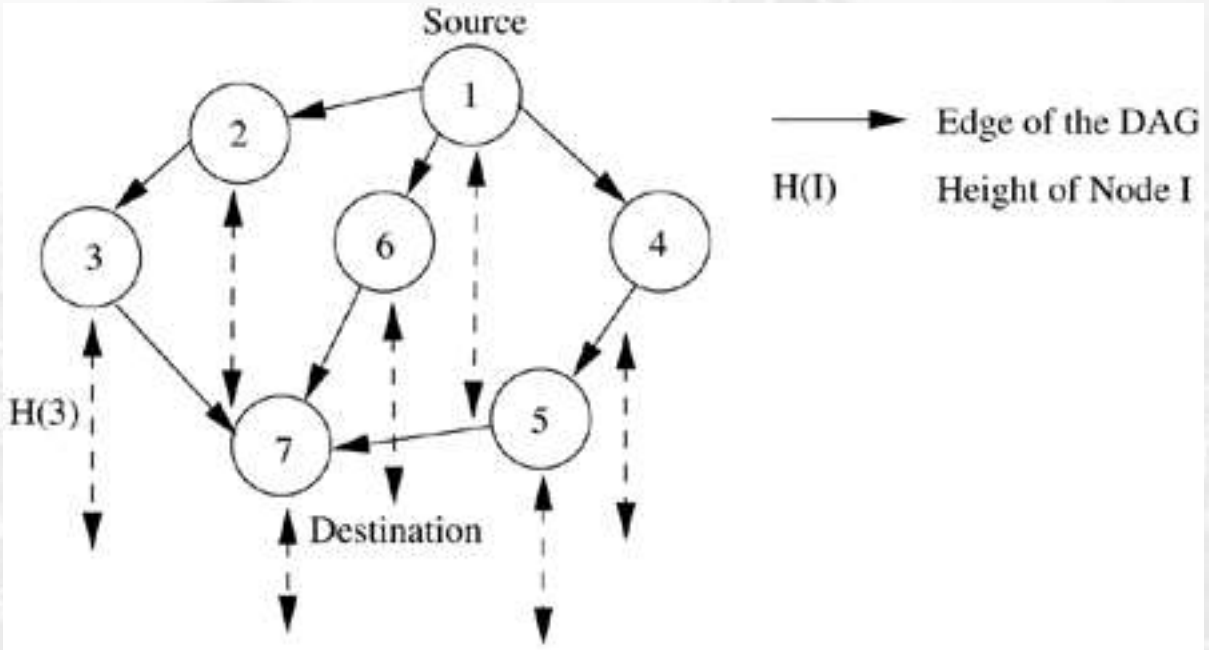


illustration of temporal ordering in TORA

- In the example, the destination node 7 originates an Update packet. Each node that receives the Update packet sets its distance to a value higher than the distance of the sender of the Update packet.
- By doing this, a set of directed links from the node which originated the Query to the destination node 7 is created.
- This forms the DAG depicted in Figure
- Once a path to the destination is obtained, it is considered to exist as long as the path is available, irrespective of the path length changes due to the reconfigurations that may take place during the course of the data transfer session.

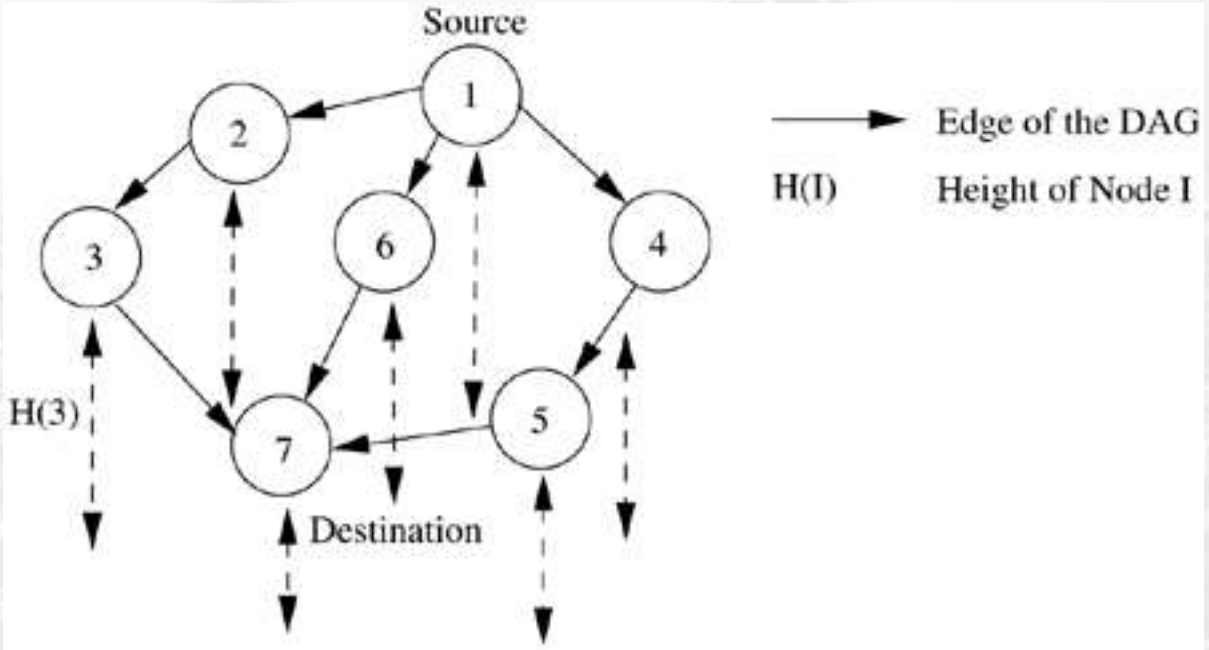
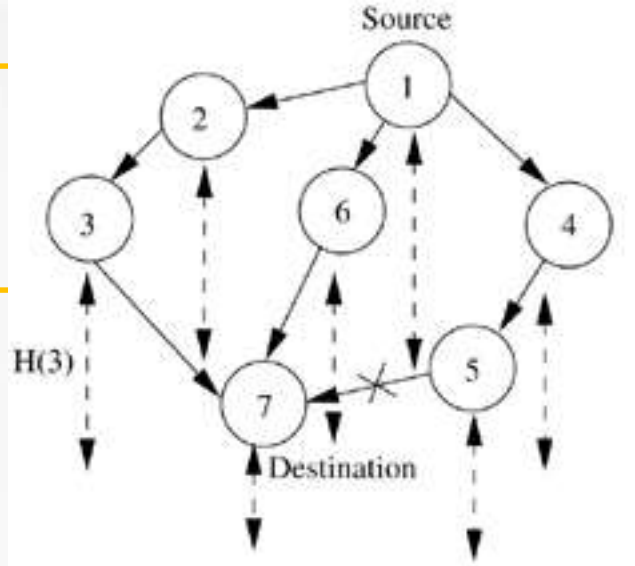
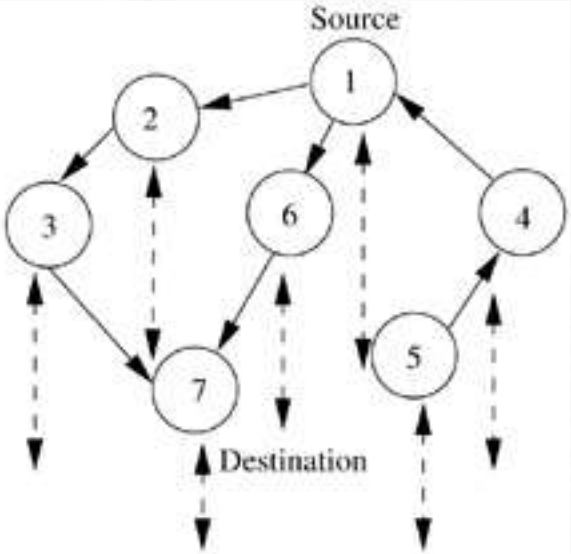


illustration of route maintenance in TORA

- When an intermediate node (say, node 5) discovers that the route to the destination node is invalid, as illustrated in Figure, it changes its distance value to a higher value than its neighbors and originates an Update packet.
- The neighboring node 4 that receives the Update packet reverses the link between 1 and 4 and forwards the Update packet.
- This is done to update the DAG corresponding to destination node 7.
- This results in a change in the DAG.



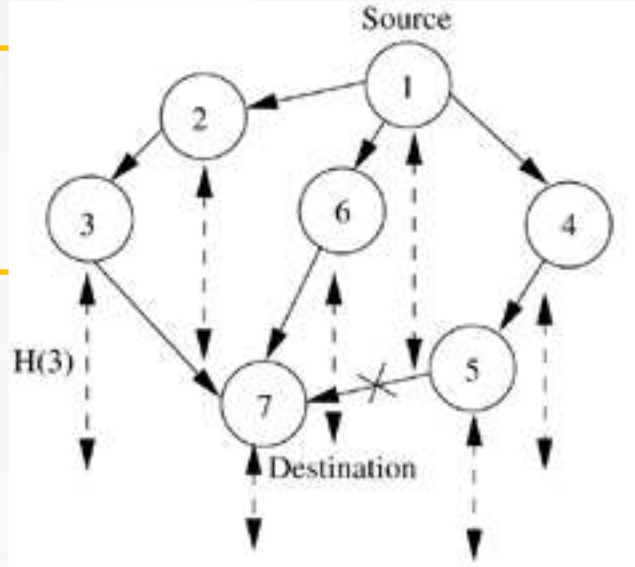
Link break beween Nodes 5 and 7



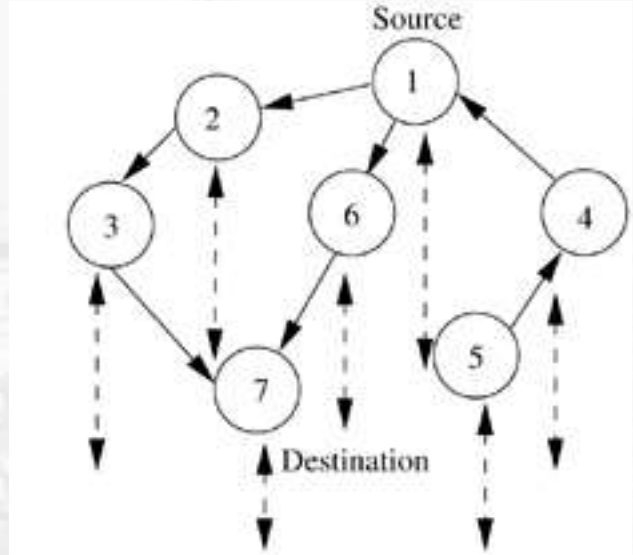
Nodes 4 and 5 reverse their links in order to update the path

illustration of route maintenance in TORA

- If the source node has no other neighbor that has a path to the destination, it initiates a fresh Query/Update procedure.
- Assume that the link between nodes 1 and 4 breaks.
- Node 4 reverses the path between itself and node 5, and sends an update message to node 5.
- Since this conflicts with the earlier reversal, a partition in the network can be inferred.
- If the node detects a partition, it originates a Clear message, which erases the existing path information in that partition related to the destination.
- By limiting the control packets for route reconfigurations to a small region, TORA incurs less control overhead.
- Concurrent detection of partitions and subsequent deletion of routes could result in temporary oscillations and transient loops.
- The local reconfiguration of paths results in non-optimal routes.



Link break beween Nodes 5 and 7

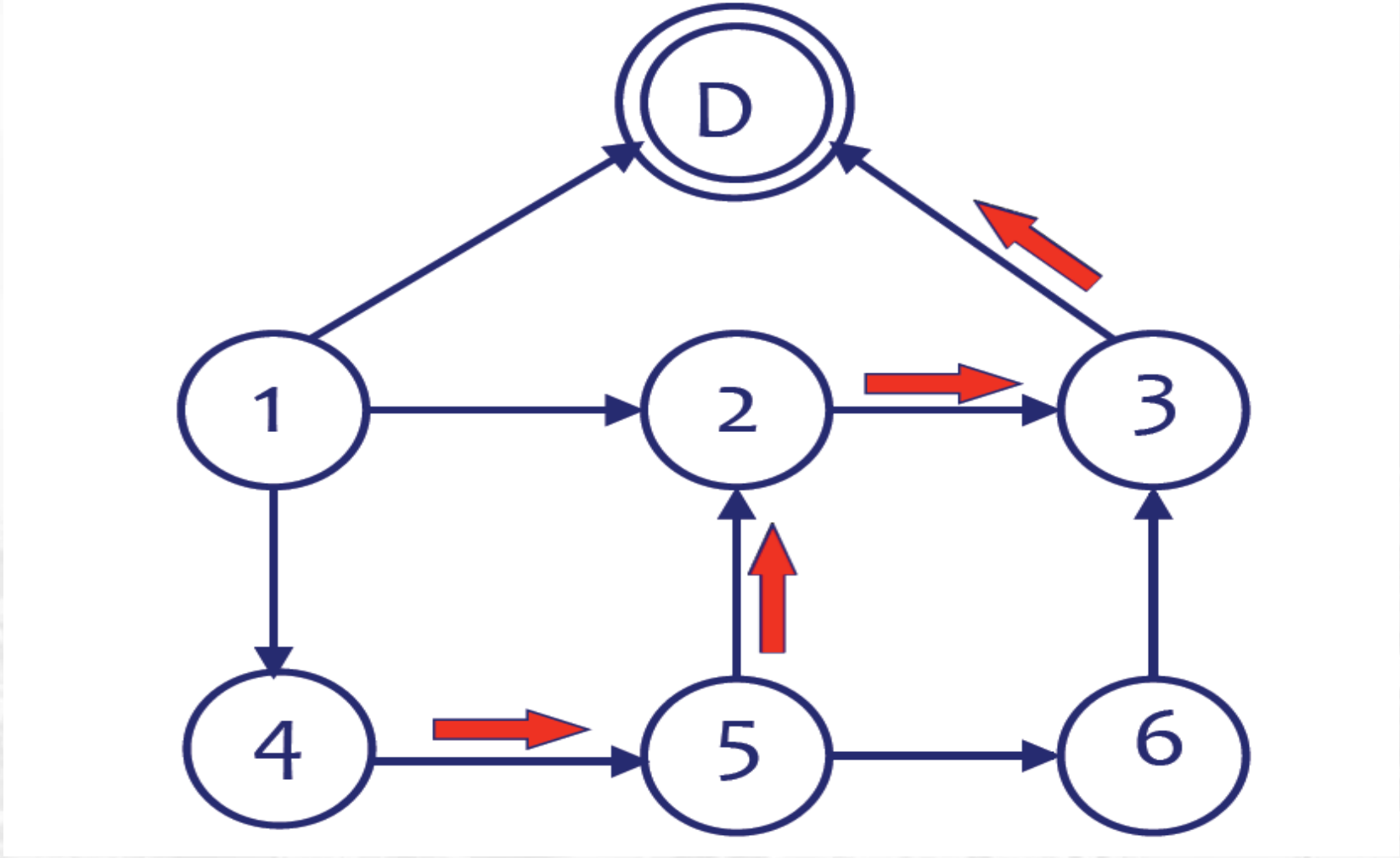


Nodes 4 and 5 reverse their links in order to update the path

Link reversal routing algorithms

- Distributed algorithm design technique
- Used in solutions for a variety of problems
  - routing, leader election, mutual exclusion, scheduling, resource allocation,…
- Model problem as a directed graph and reverse the direction of links appropriately
- Use **local** knowledge to decide which links to reverse

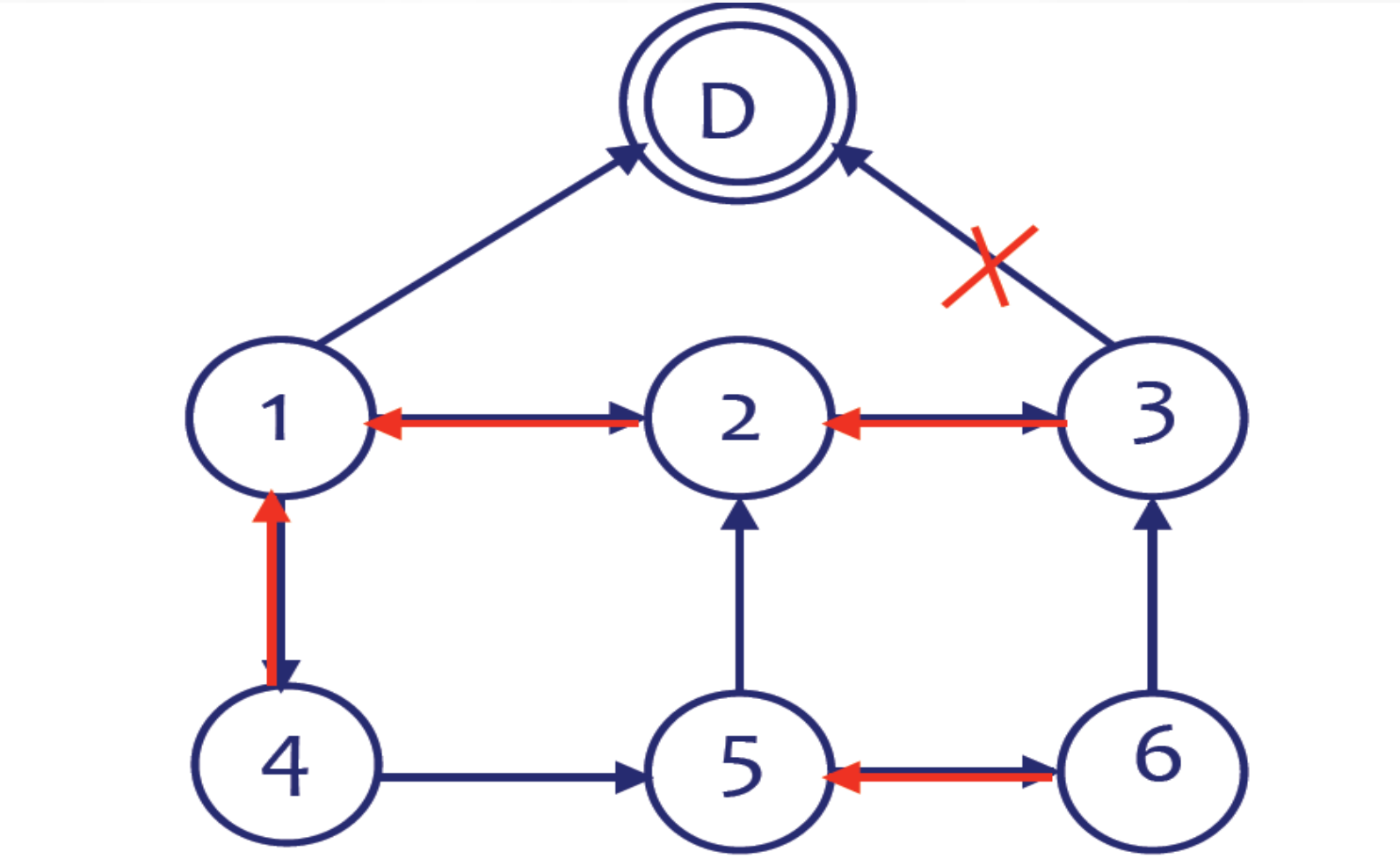
Link reversal routing algorithms



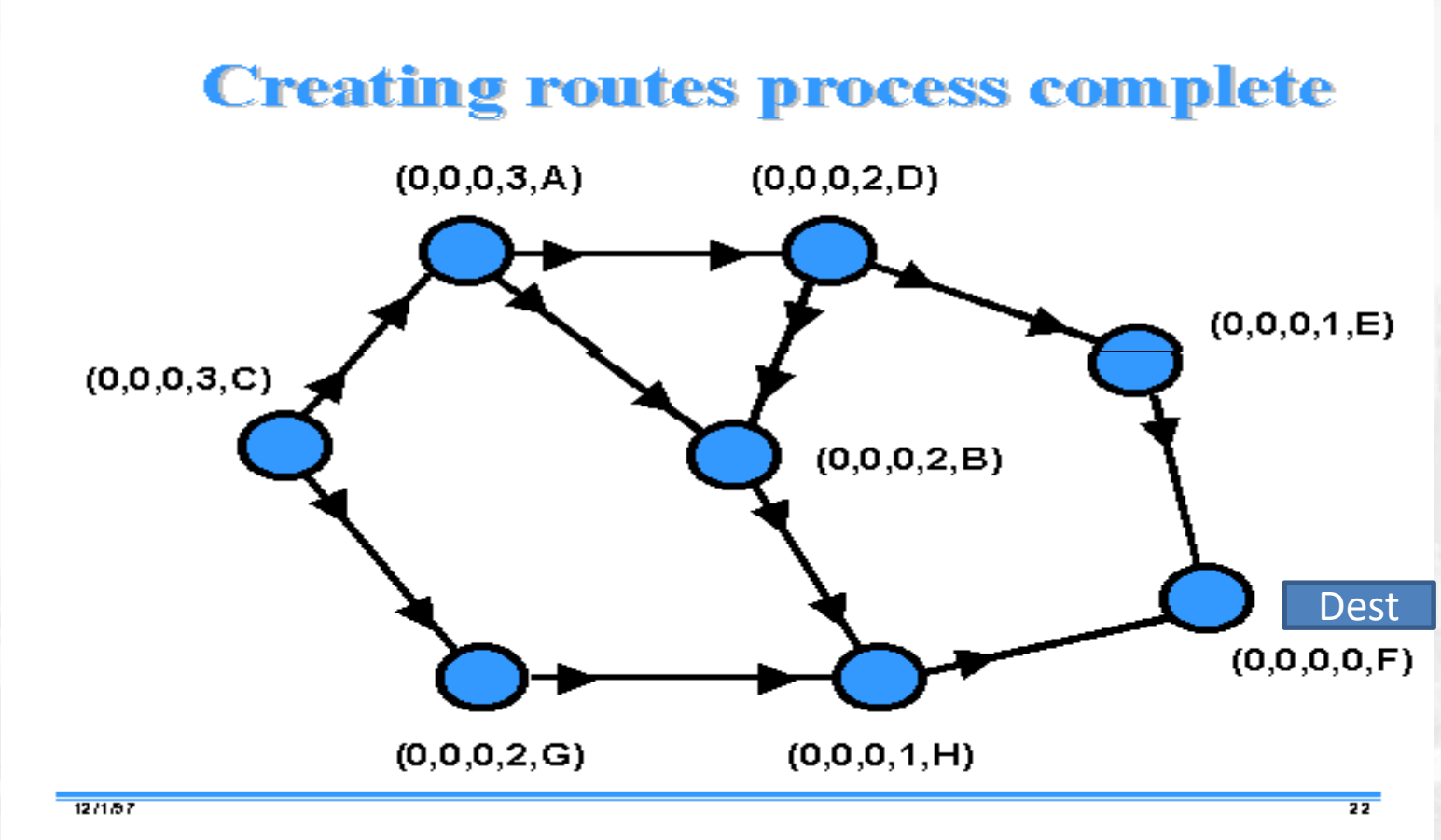
Link reversal routing algorithms

- What happens if some edges go away?
  - Might need to change the virtual directions on some remaining edges (reverse some links)
- More generally, starting with an arbitrary directed graph, each node should decide independently which of its incident links to reverse

Link reversal routing algorithms



Link reversal routing algorithms



(logical time,NodeID',Height',Height,NodeID)

Temporally Ordered Algorithm (TORA)

- Advantage
  - Less control overhead
- Disadvantage
  - The local reconfiguration of paths result in no optimal routes.

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

Other Routing Protocols…

- Table-Driven Routing Protocols
- On-Demand Routing Protocols
- Hybrid Routing Protocols
- Routing Protocol With Efficient Flooding Mechanisms
- Hierarchical Routing Protocols
- Power-Aware Routing Protocols

Introduction to Multicast Routing Protocols in Adhoc Wireless Networks

Introduction to Multicast Routing Protocols

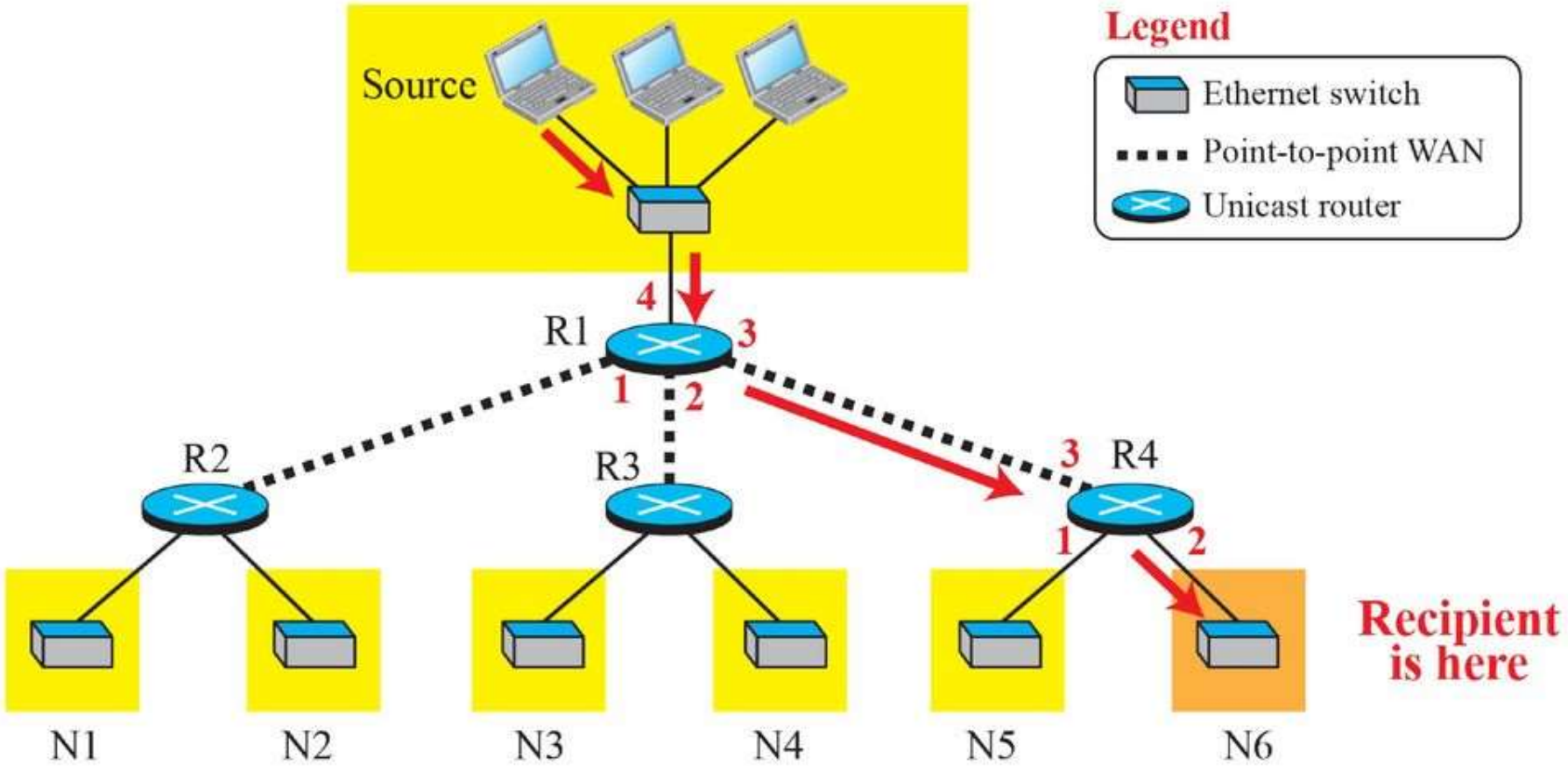
Communication in the todays world is not only uses Unicasting ;

Multicasting communication is also growing fast and various routing protocols are used.

Unicasting

In unicasting, there is one source and one destination network. The relationship between the source and the destination network is one to one. Each router in the path of the datagram tries to forward the packet to one and only one of its interfaces.

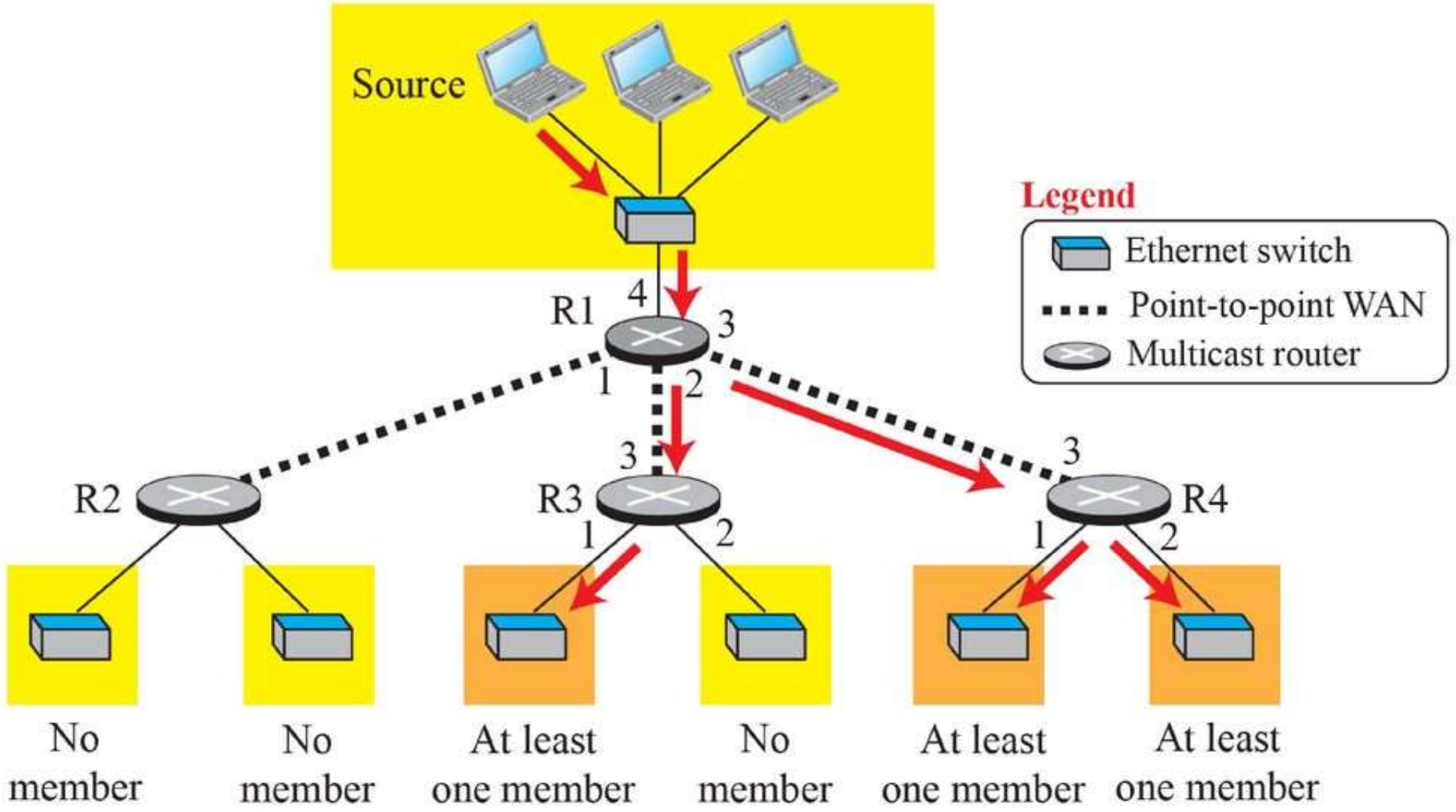
Unicasting


Source
Legend
Ethernet switch
Point-to-point WAN
Unicast router
R1
R2
R3
R4
4
3
1
2
3
1
2
N1
N2
N3
N4
N5
N6
Recipient is here

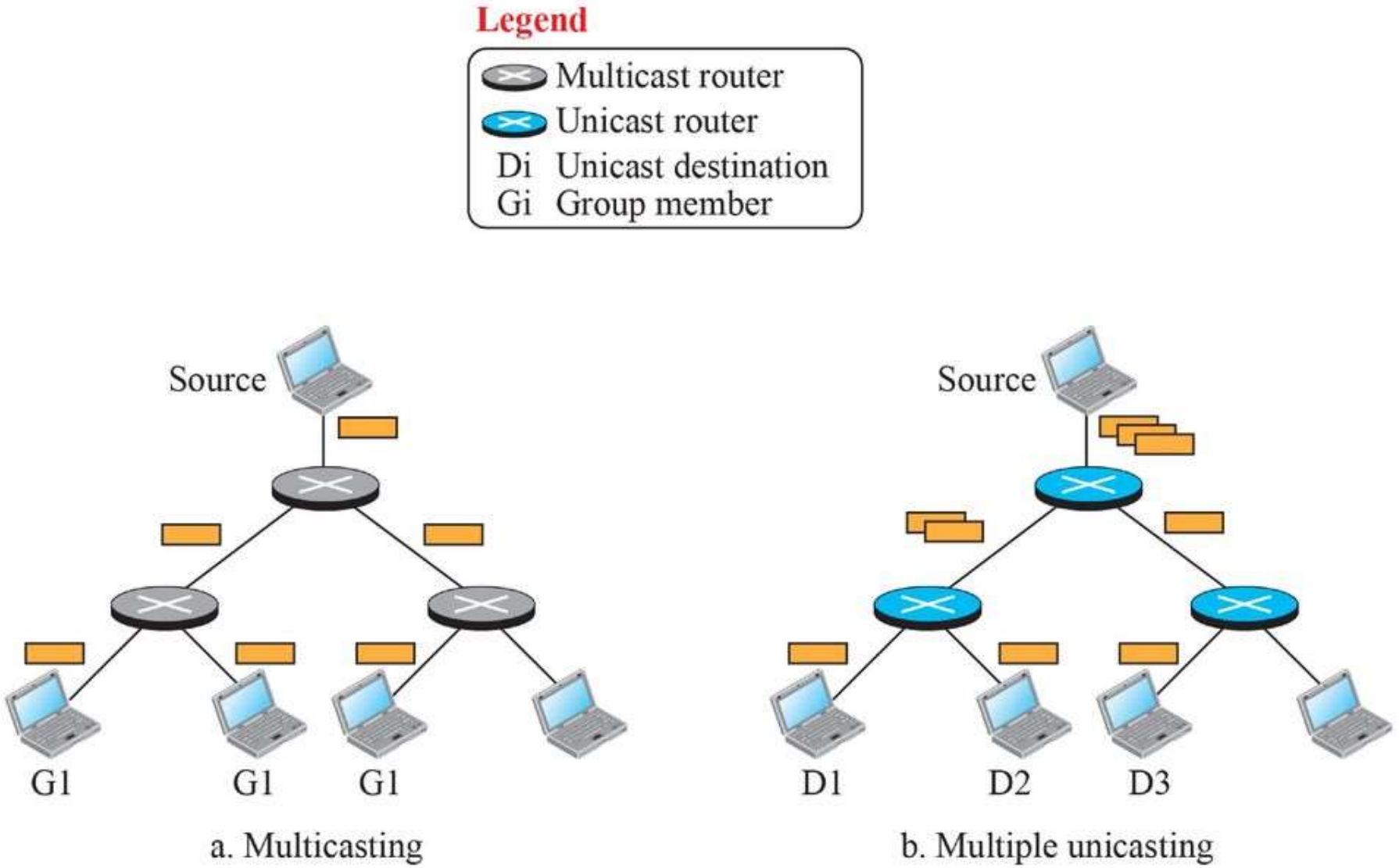
Multicasting

In multicasting, there is one source and a group of destinations. The relationship is one to many. In this type of communication, the source address is a unicast address, but the destination address is a group address, a group of one or more destination networks in which there is at least one member of the group that is interested in receiving the multicast datagram. The group address defines the members of the group.

Multicasting



Multicasting vs Multiple Unicasting



ISSUES IN DESIGNING A MULTICAST ROUTING PROTOCOL

- Robustness
- Efficiency
- Control overhead
- Quality of service
- Dependency on the unicast routing protocol
- Resource management

OPERATION OF MULTICAST ROUTING PROTOCOLS

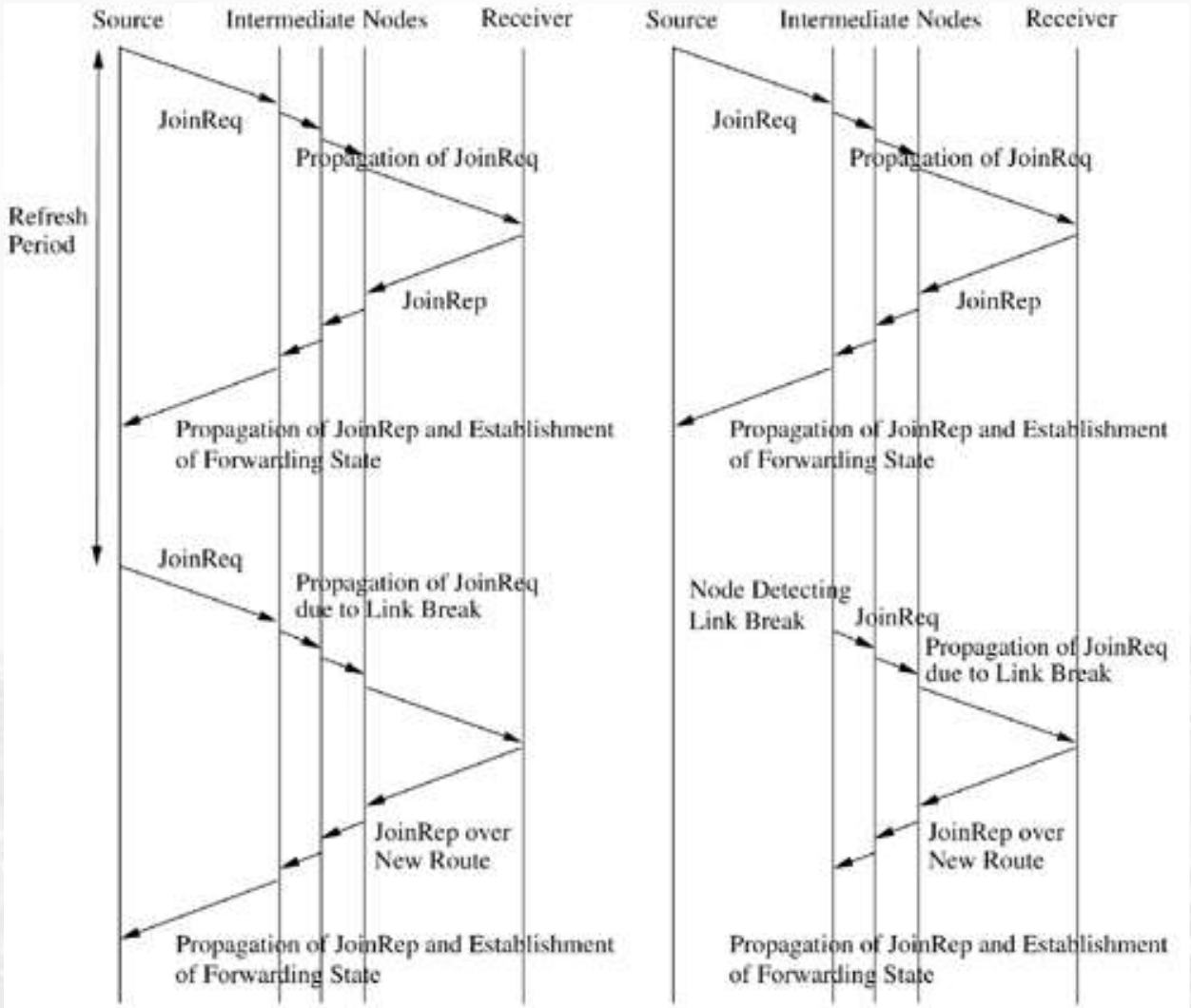
Multicast protocols classified into two types:

1. *source-initiated* protocols and

2. *Receiver-initiated* protocols

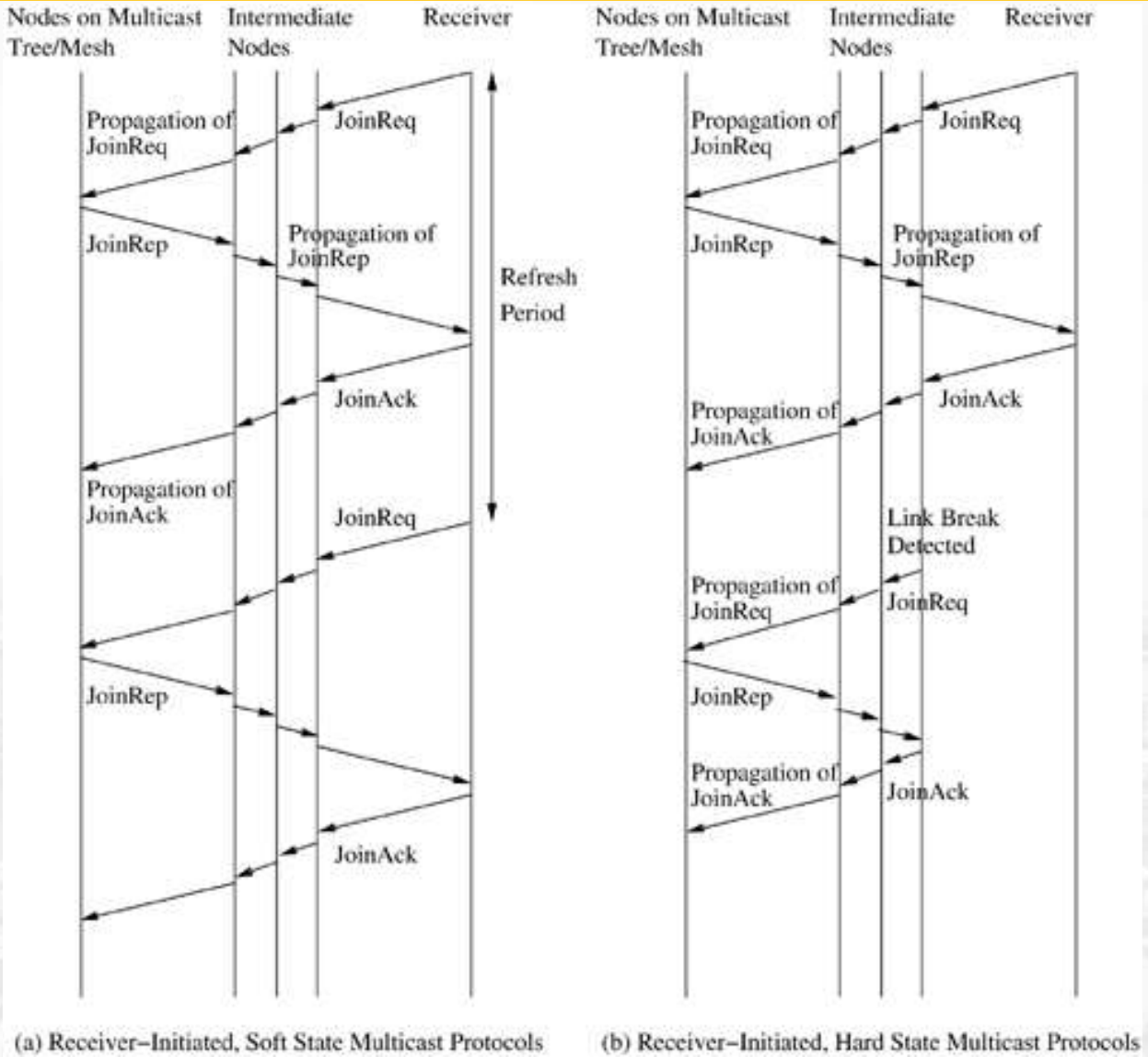
There exist certain other multicast protocols such as MCEDAR and AMRoute which may not strictly fall under the above two types

Source-initiated multicast protocols



(a) Source–Initiated, Soft State Multicast Protocols (b) Source–Initiated, Hard State Multicast Protocols

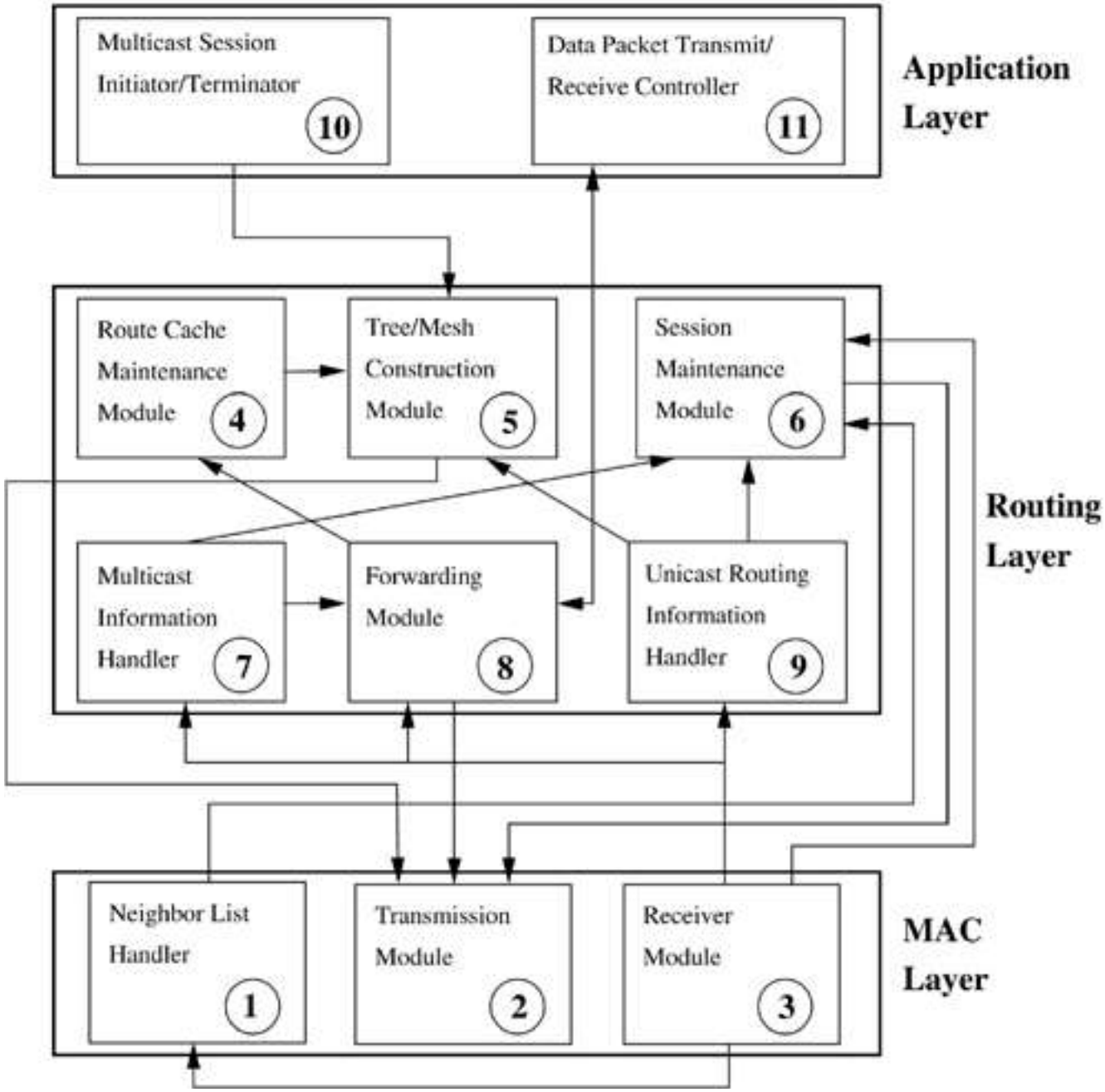
Receiver-initiated multicast protocols



(a) Receiver–Initiated, Soft State Multicast Protocols

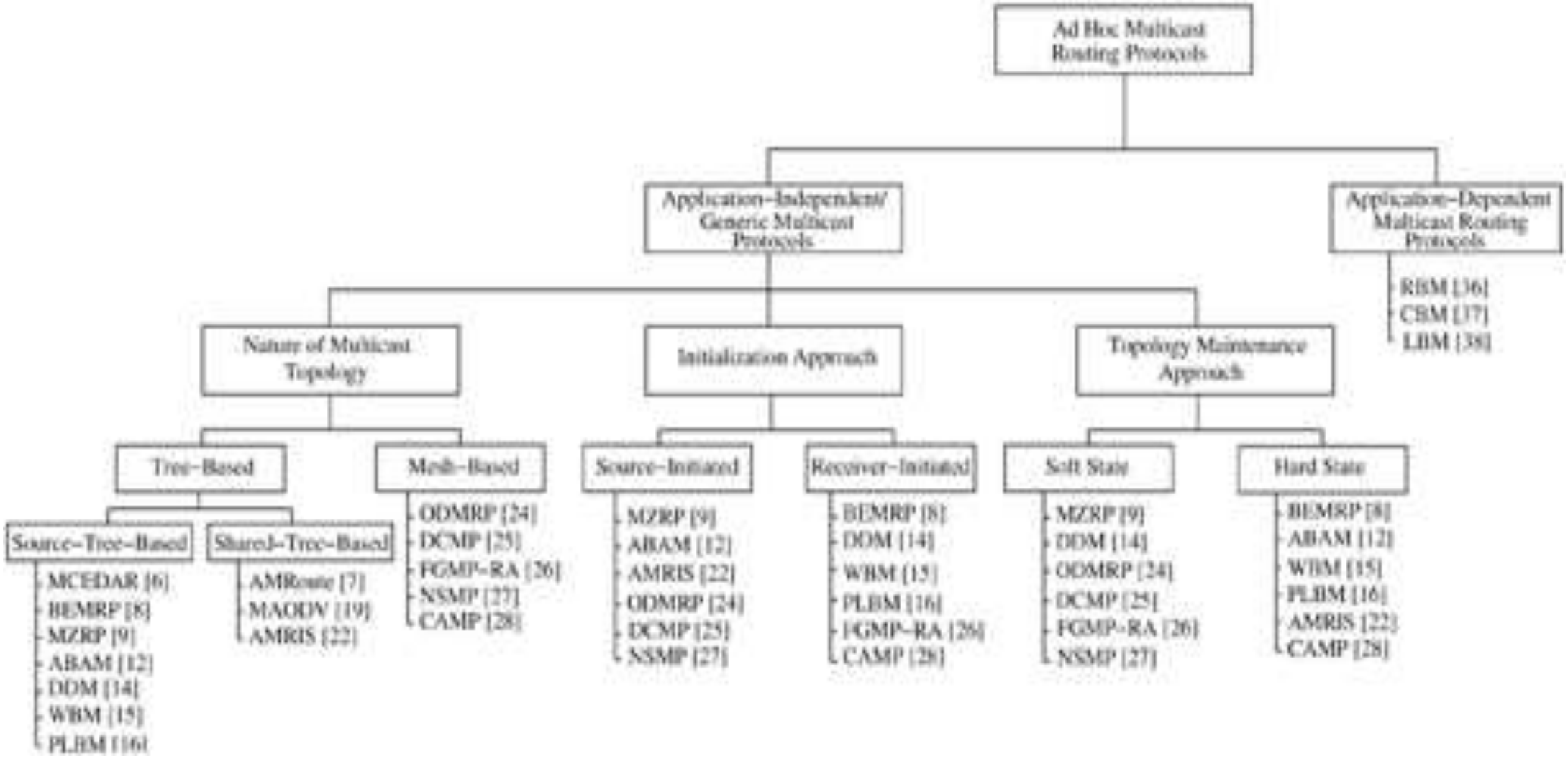
(b) Receiver–Initiated, Hard State Multicast Protocols

AN ARCHITECTURE REFERENCE MODEL FOR MULTICAST ROUTING PROTOCOLS



Architectural framework of an ad hoc multicast protocol

CLASSIFICATIONS OF MULTICAST ROUTING PROTOCOLS



Additional Reading

MIT-WPU

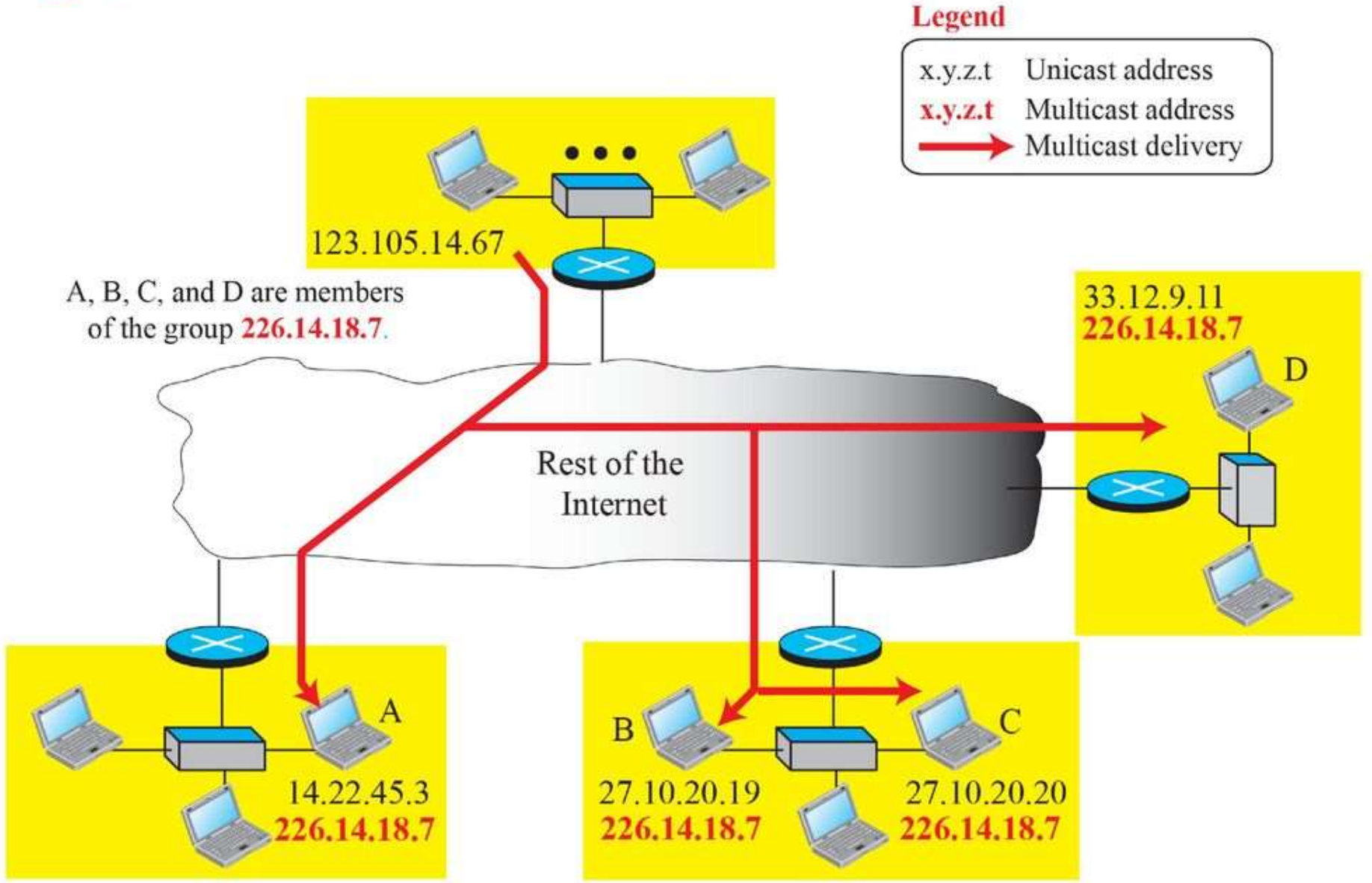
॥ विश्वशान्तिर्भुवं ध्रुवा ॥

Multicast basics

Multicast Addresses

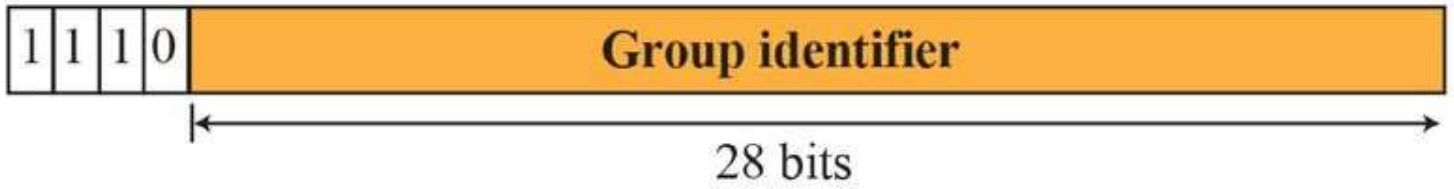
In multicast communication, the sender is only one, but the receiver is many, sometimes thousands or millions spread all over the world. It should be clear that we cannot include the addresses of all recipients in the packet. The destination address of a packet, as described in the Internet Protocol (IP) should be only one. For this reason, we need multicast addresses. A multicast address defines a group of recipients, not a single one. In other words, a multicast address is an identifier for a group.

Needs for Multicast Addresses



Multicast Address in Binary

Block: 224.0.0.0/4

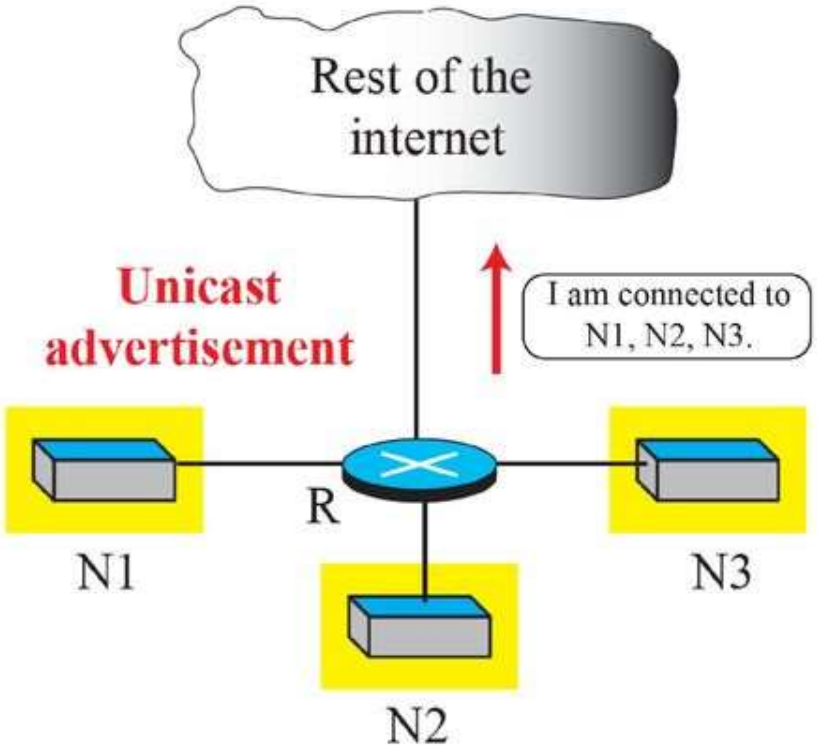


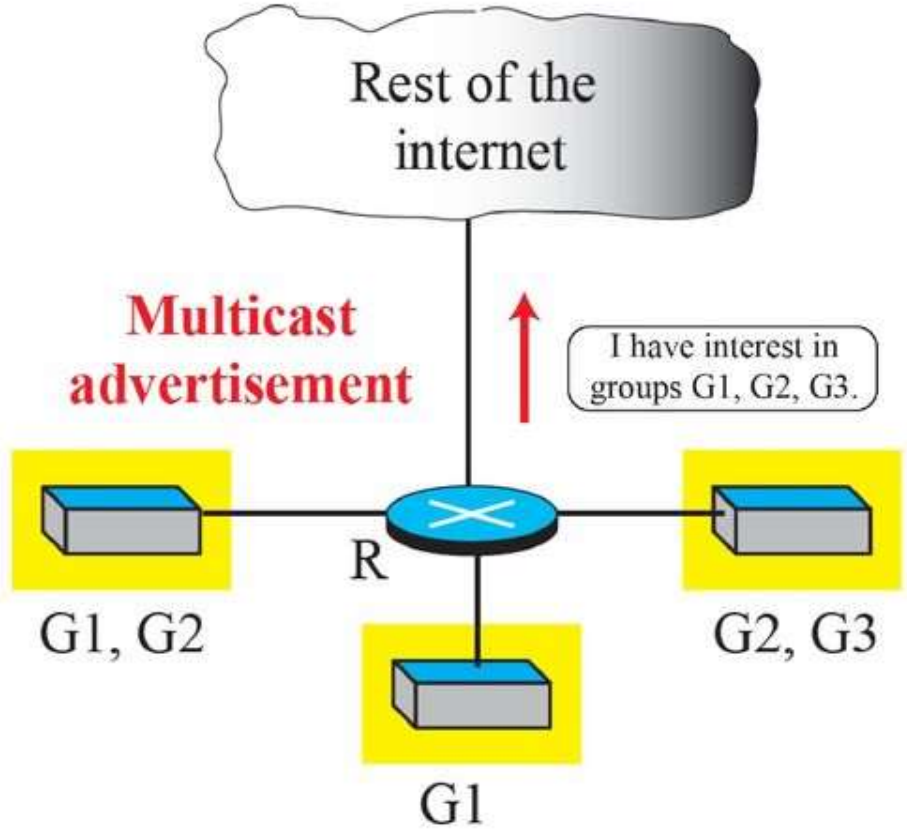
Collecting information

Creation of forwarding tables in both unicast and multicast routing involves two steps:

1. ***A router needs to know to which destinations it is connected.***
2. ***Each router needs to propagate information obtained in the first step to all other routers so that each router knows to which destination each other router is connected.***

Unicast Vs Multicast advertising

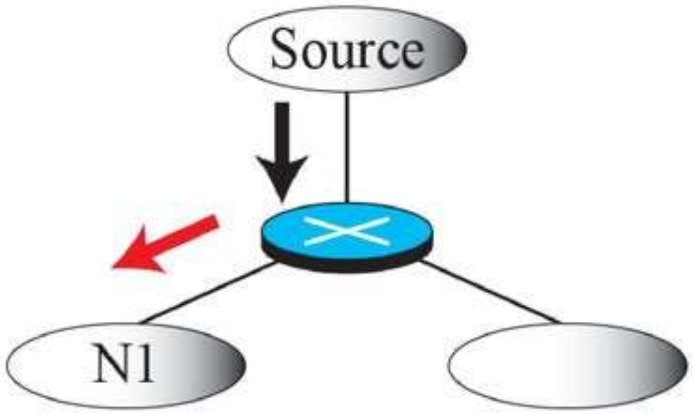




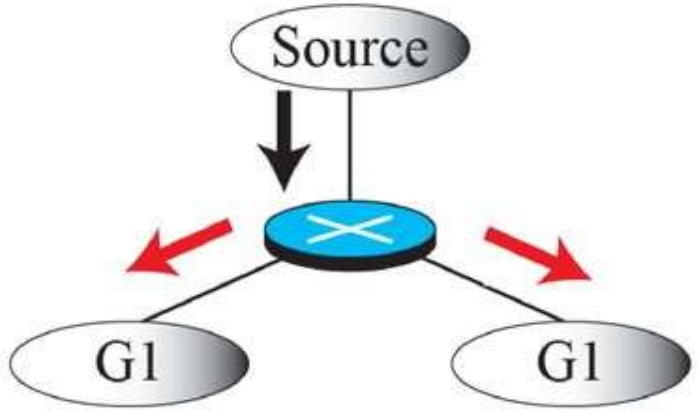
Multicast forwarding

Another important issue in multicasting is the decision a router needs to make to forward a multicast packet. Forwarding in unicast and multicast communication is different.

Destination in Unicasting and Multicasting

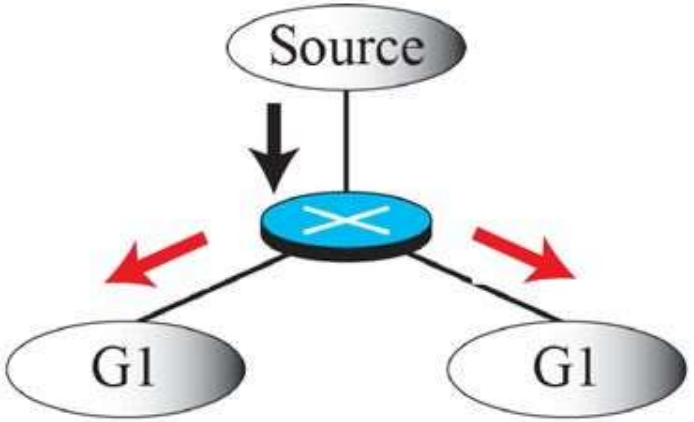


a. Destination in unicasting is one

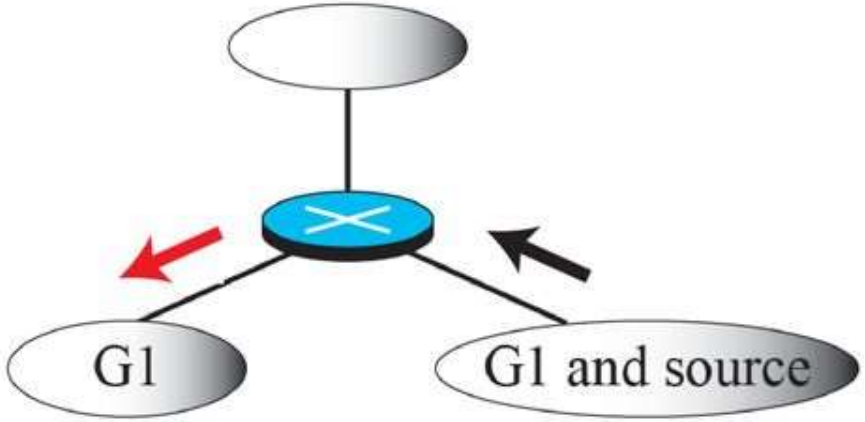


b. Destination in mulicasting is more than one

Forwarding depends on the destination and source



a. Packet sent out of two interfaces



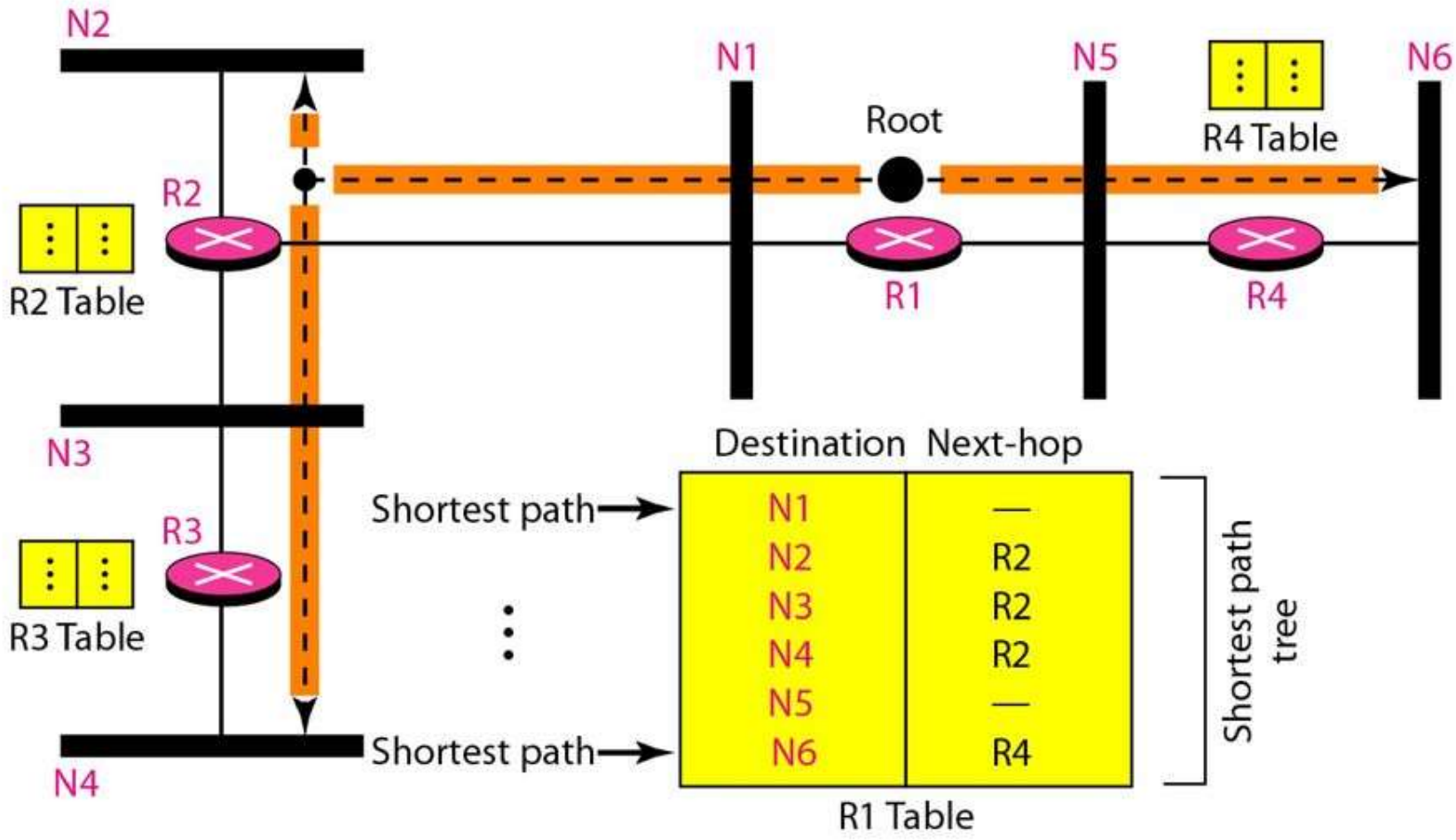
b. Packet sent out of one interface

MIT-WPU
॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

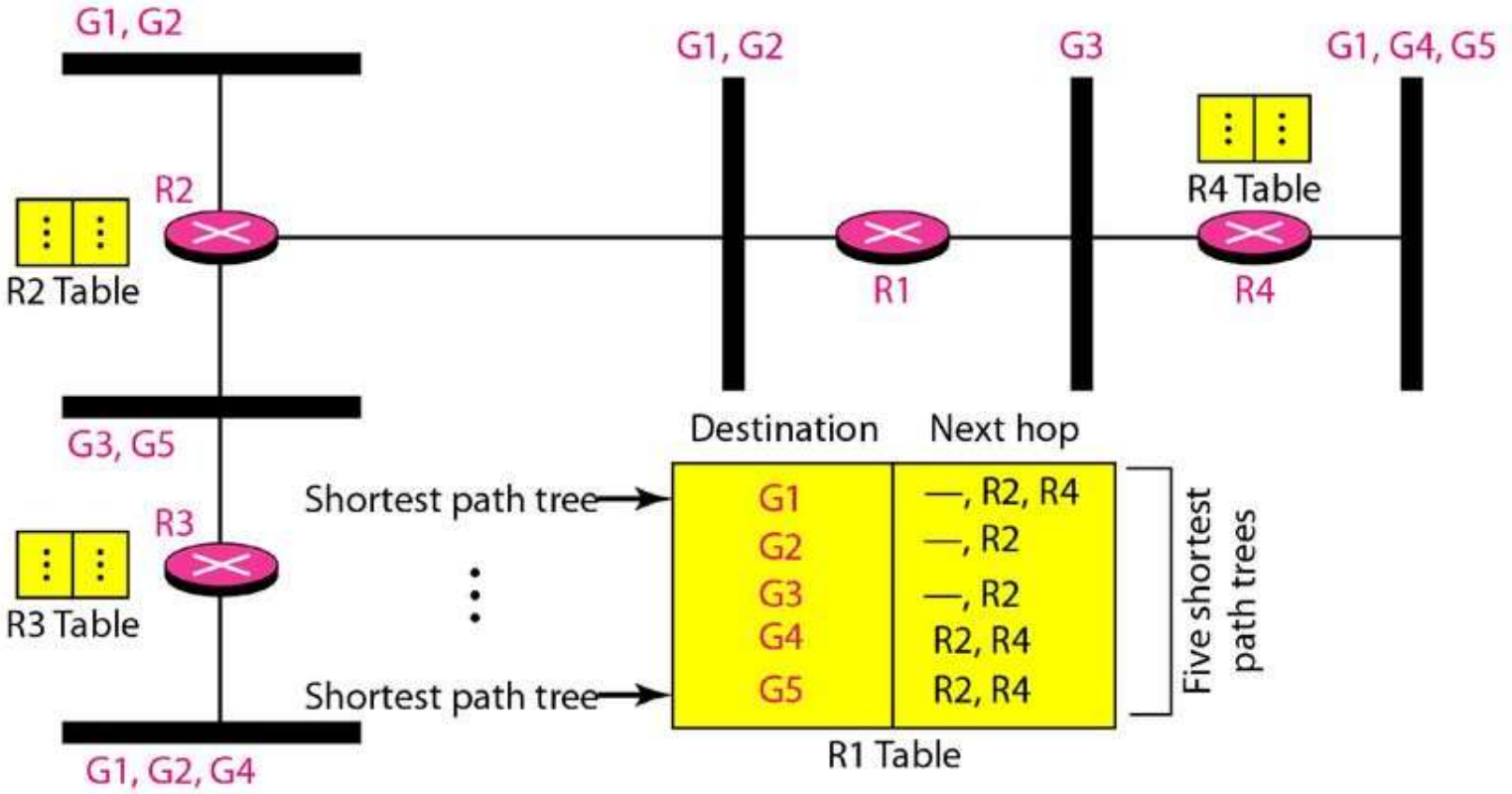
Two approaches to Multicasting

In multicast routing, as in unicast routing, we need to create routing trees to optimally route the packets from their source to their destination. However, as we discussed before, the multicast routing decision at each router depends not only on the destination of the packet, but also on the source of the packet. The involvement of the source in the routing process makes multicast routing much more difficult than unicast routing. For this reason, two different approaches in multicast routing have been developed: routing using source-based trees and routing using group-shared trees.

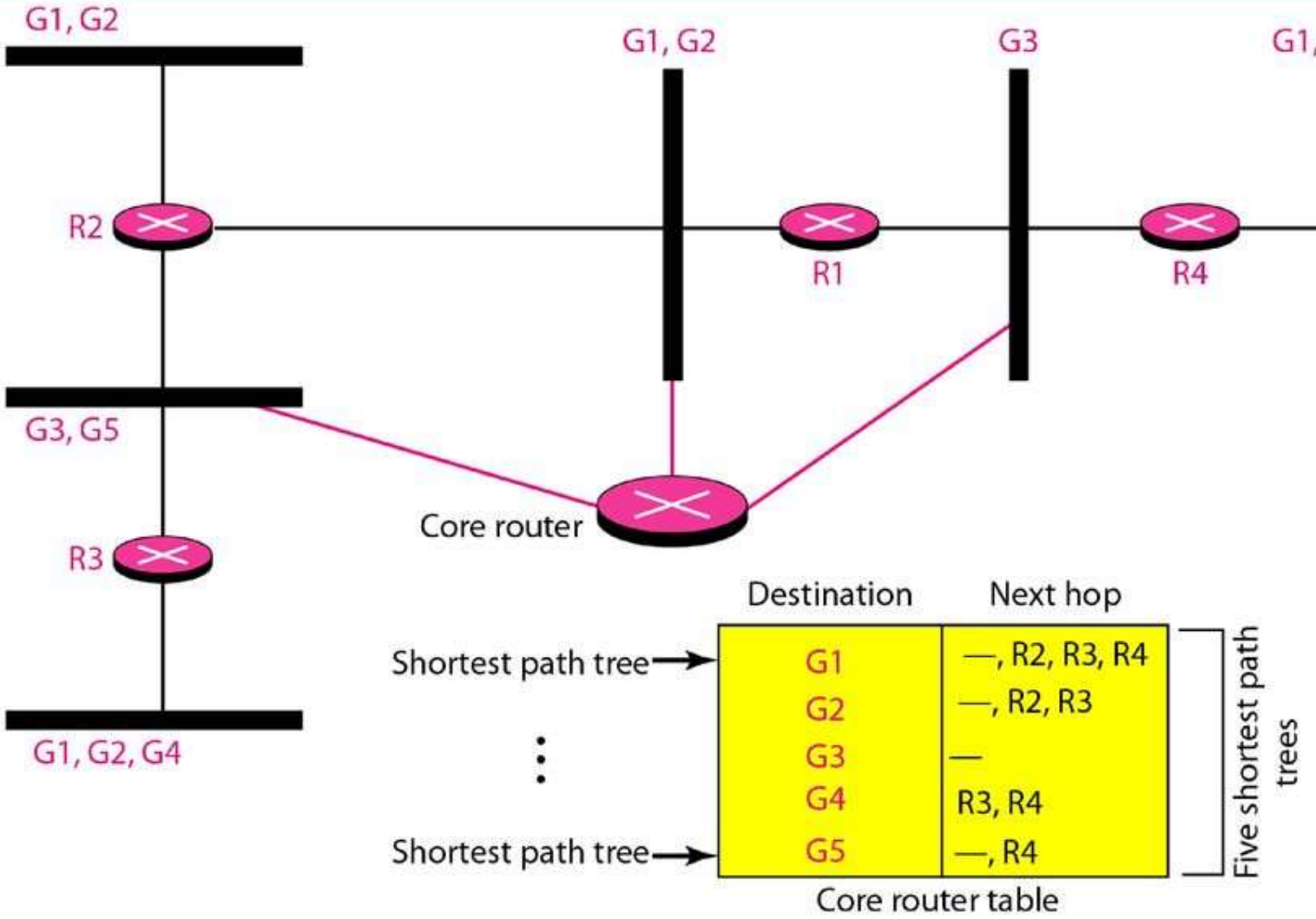
Shortest path tree in Unicast routing



Source–based tree approach



Group share tree approach



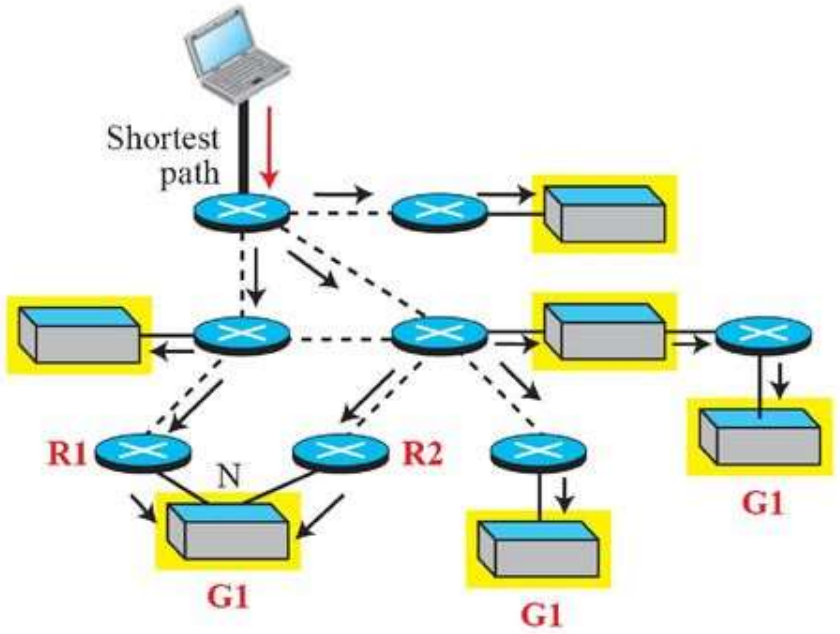
Intra domain Protocols

During the last few decades, several intradomain multicast routing protocols have emerged. In this section, we discuss three of these protocols. Two are extensions of unicast routing protocols (RIP and OSPF), using the source-based tree approach; the third is an independent protocol which is becoming more and more popular.

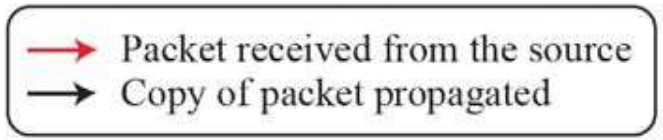
DVMRP

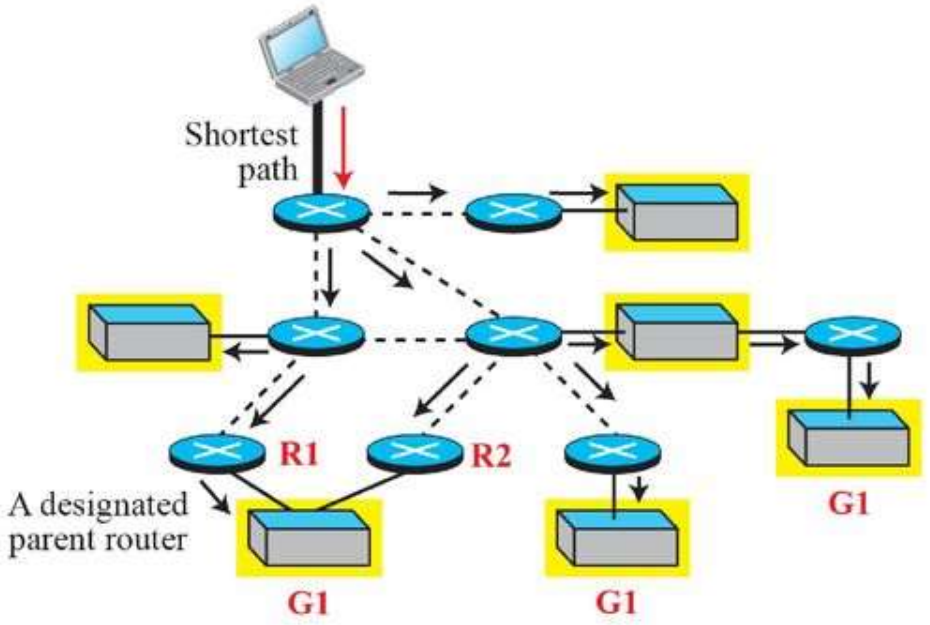
The Distance Vector Multicast Routing Protocol (DVMRP) is the extension of the Routing Information Protocol (RIP) which is used in unicast routing. It uses the source-based tree approach to multicasting. It is worth mentioning that each router in this protocol that receives a multicast packet to be forwarded implicitly creates a source-based multicast tree in three steps:

RPF vs RPB



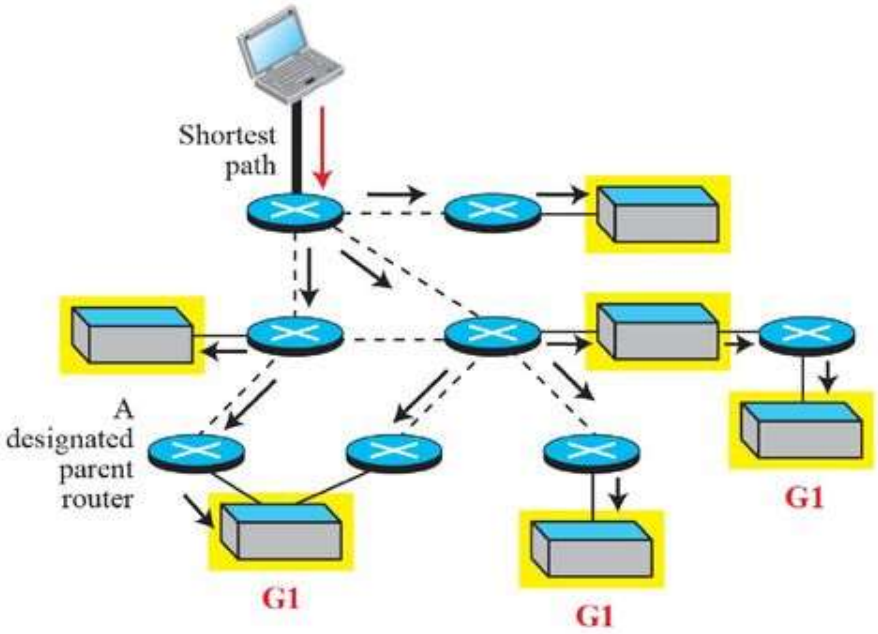
a. Using RPF, N receives two copies.



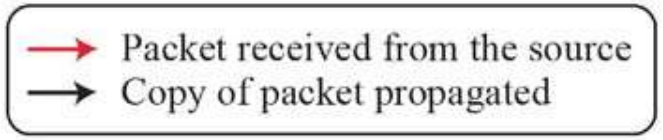


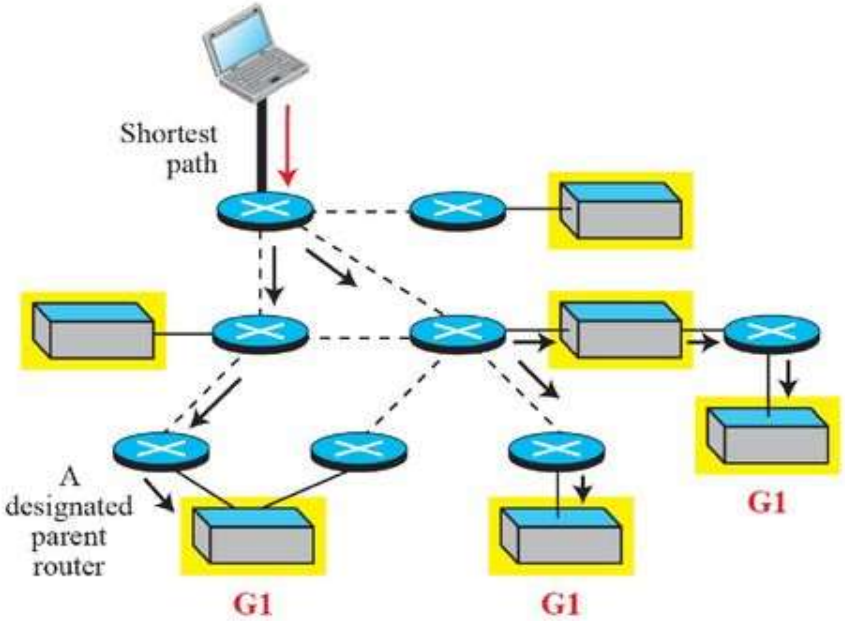
b. Using RPB, N receives only one copy.

RPB vs RPB



a. Using RPB, all networks receive a copy.



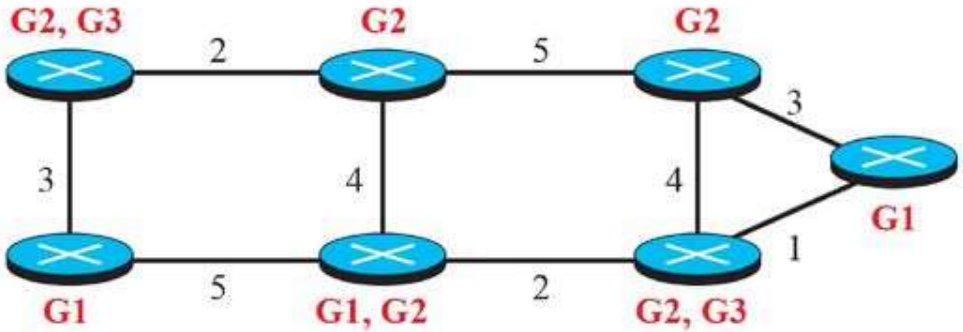


b. Using RPM, only members receive a copy.

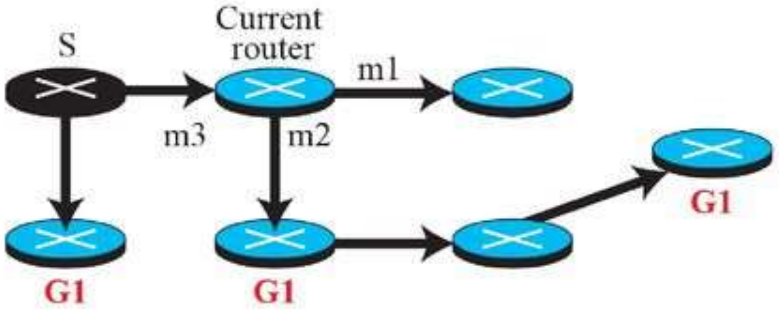
Multicast Link State (MOSPF)

Multicast Open Shortest Path First (MOSPF) is the extension of the Open Shortest Path First (OSPF) protocol, which is used in unicast routing. It also uses the source-based tree approach to multicasting. If the internet is running a unicast link-state routing algorithm, the idea can be extended to provide a multicast link-state routing algorithm. To extend unicasting to multicasting, each router needs to have another database, as with the case of unicast distance-vector routing, to show which interface has an active member in a particular group.

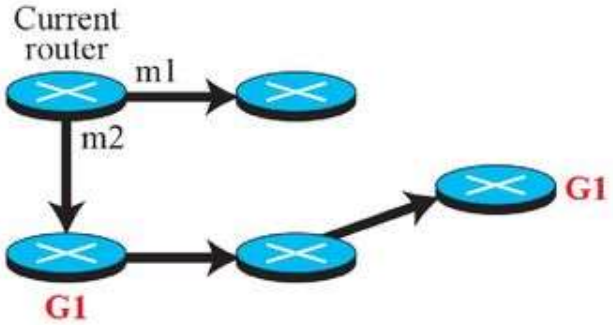
Example of Tree formation in MOSPF



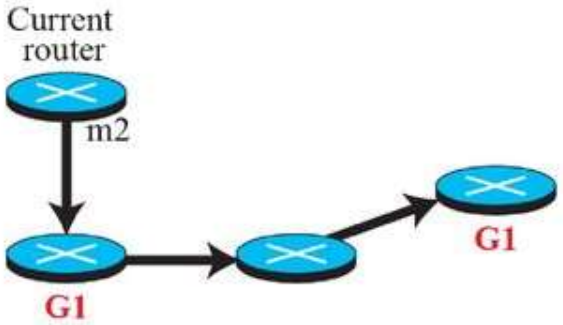
a. An internet with some active groups



b. S-G1 shortest-path tree



c. S-G1 subtree seen by current router



d. S-G1 pruned subtree

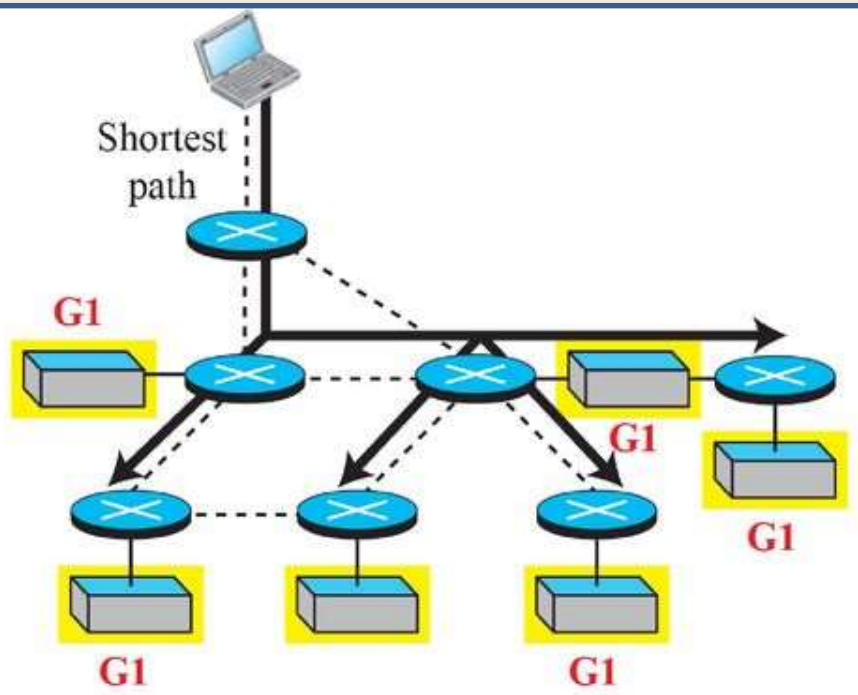
Forwarding table for current router

Group-Source	Interface
S, G1	m2
...	...

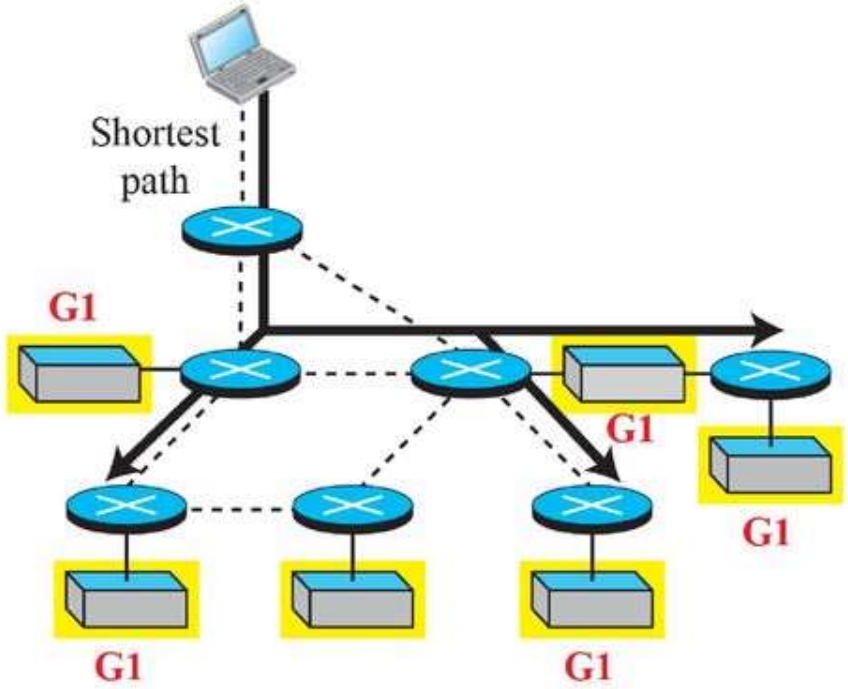
PIM

Protocol Independent Multicast (PIM) is the name given to a common protocol that needs a unicast routing protocol for its operation, but the unicast protocol can be either a distance-vector protocol or a link-state protocol. In other words, PIM needs to use the forwarding table of a unicast routing protocol to find the next router in a path to the destination, but it does not matter how the forwarding table is created. PIM has another interesting feature: it can work in two different modes: dense and sparse.

Idea behind PIM-DM

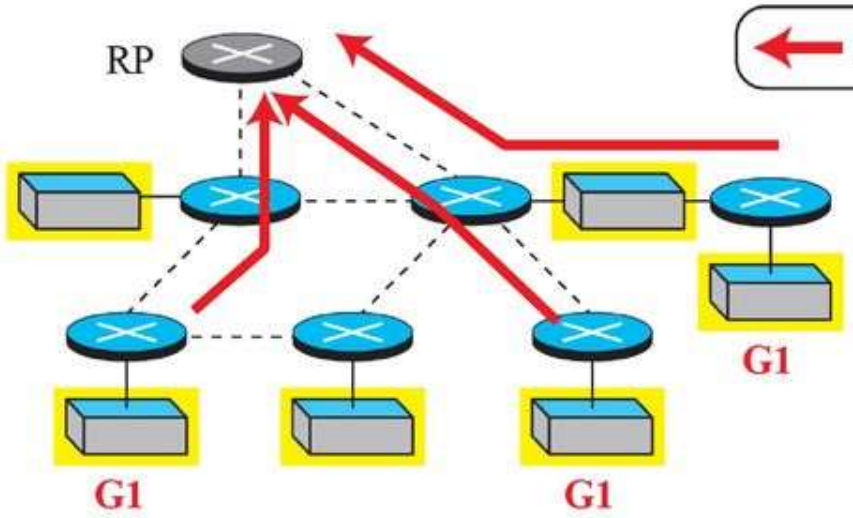


a. First packet is broadcast.

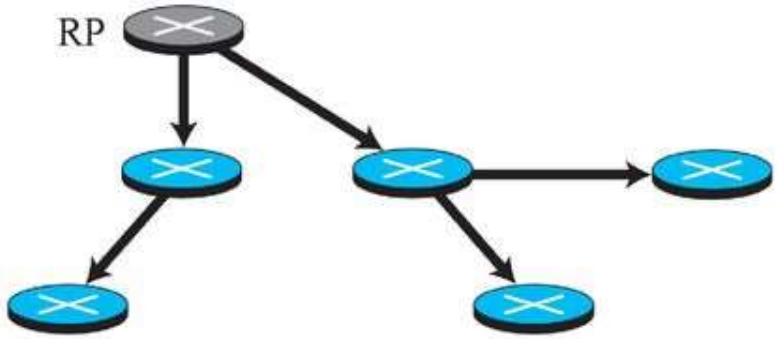


b. Second packet is multicast.

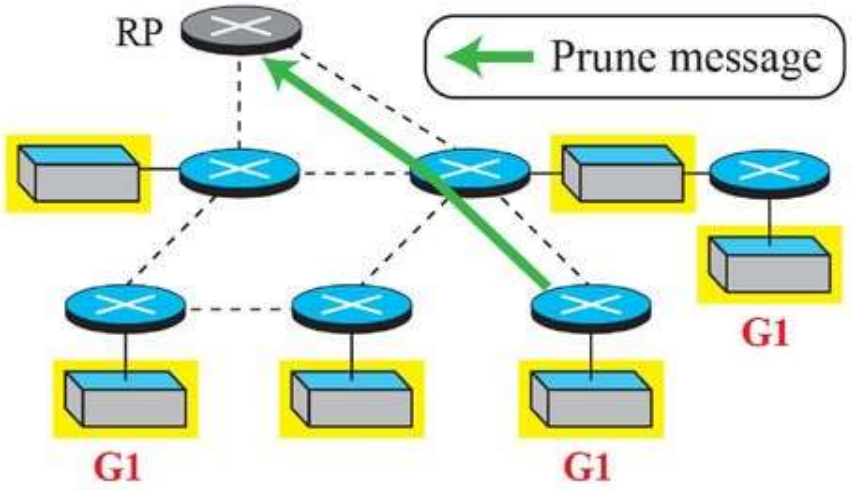
Idea behind PIM-SM



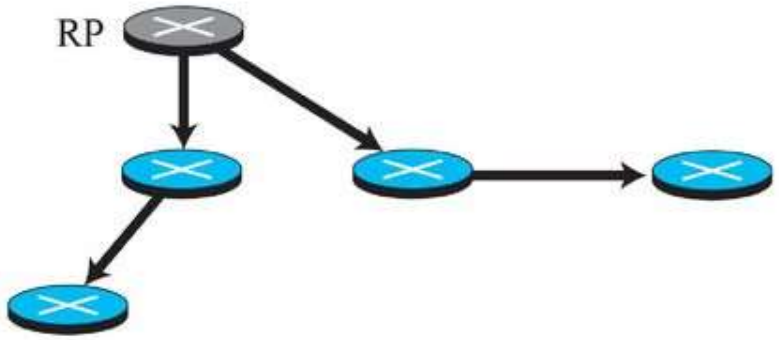
a. Three networks join group G1



b. Multicast tree after joins



c. One network leaves group G1



d. Multicast tree after pruning

Learning Resources

Text books

1. C. Siva Ram Murthy, B.S. Manoj, “Adhoc Wireless Networks Architectures and Protocols”, PHI, ISBN - 9788131706885, 2007.
2. Nekoley Elenkov, “Android Security internals”, No Starch Press, ISBN-10: 1-59327-581-1 ISBN-13: 978-1-59327-581

Reference Books

1. KiaMakki, Peter Reiher, “Mobile and Wireless Network Security and Privacy “, Springer, ISBN 978-0-387-71057-0, 2007.
2. Hakima Chaouchi, Maryline Laurent-Maknavicius , “Wiress and Mobile Networks Security”, Wiley publication, ISBN 978-1-84821-117-9
3. Noureddine Boudriga, “Security of Mobile Communications”, ISBN 9780849379413, 2010.
4. Kitsos, Paris; Zhang, Yan, “RFID Security Techniques, Protocols and System-On-Chip Design”, ISBN 978-0-387-76481-8, 2008.
5. Johny Cache, Joshua Wright and Vincent Liu,” Hacking Wireless Exposed: Wireless Security Secrets & Solutions “, second edition, McGraw Hill, ISBN: 978-0-07-166662-6, 2010
6. Tim Speed, Darla Nykamp,Mari Heiser,Joseph Anderson,Jaya Nampalli, "Mobile Security: How to Secure, Privatize, and Recover Your Devices", Copyright © 2013 Packt Publishing, ISBN 978-1-84969-360-8

Learning Resources

Web Resources:

i. http://whatis.techtarget.com/definition/mobile-security

ii. http://techgenix.com/security/mobile-wireless-security/

Weblinks

i. https://en.wikipedia.org/wiki/Mobile_security

MOOCs:

i. https://www.ntnu.edu/studies/courses/TTM4137#tab=omEmnet
ii. http://nptel.ac.in/courses/106105160/37
iii. https://www.eccouncil.org/
iv. https://www.csoonline.com/article/2122635/mobile-security/wireless-security--the-basics.html

MIT-WPU

॥ विश्वशान्तिर्ध्रुवं ध्रुवा ॥

THANK YOU FOR LISTENING ANY QUESTION?