SEMESTER VI

17BECS6E02 **NETWORK ROUTING ALGORITHMS** **3H-3C**

Instruction Hours/week: L:3 T:0 P:0 **Marks:** Internal**:40** External**:60** Total**:100**

End Semester Exam:3 Hours

COURSE OBJECTIVES:

- To expose the students to the layered architecture for communication networks
- To discuss specific functionality of the network layer.
- To enable the student to understand the basic principles of routing and implementation in conventional networks and the evolving routing algorithms based on Internetworking requirements, optical backbone and the wireless access part of the network.
- To enable the student to understand the different routing algorithms existing and their performance characteristics.

COURSE OUTCOMES:

Upon completion of the course, the students will be able to:

- Understand layered architecture and its significance.
- Learn network layer and various routing techniques available.
- Apply knowledge for identifying a suitable routing algorithm ,implementing it and analyzing its performance for any given network and user requirements and the type of channel over which the network has to operate,
- Design a new algorithm or modify an existing algorithm to satisfy the evolving demands in the network and by the user applications.

UNIT I Introduction (7)

ISO OSI Layer Architecture, TCP/IP Layer Architecture, Functions of Network layer, General Classification of routing, Routing in telephone networks, Dynamic Non hierarchical Routing (DNHR), Trunk status map routing (TSMR), real-time network routing (RTNR), Distance vector routing, Link staterouting, Hierarchical routing.

UNIT II Internet Routing (10)

Interior protocol : Routing Information Protocol (RIP), Open Shortest Path First(OSPF), Bellman Ford Distance Vector Routing. Exterior Routing Protocols: Exterior Gateway Protocol (EGP) and Border Gateway Protocol (BGP). Multicast Routing: Pros and cons of Multicast and Multiple Unicast Routing, Distance Vector Multicast Routing Protocol (DVMRP), Multicast Open Shortest Path First (MOSPF), MBONE, Core Based Tree Routing.

UNIT III Routing In Optical WDM Networks (10)

Classification of RWA algorithms, RWA algorithms, Fairness and Admission Control, Distributed Control Protocols, Permanent Routing and Wavelength Requirements,Wavelength Rerouting-Benefits and Issues, Lightpath Migration, Rerouting Schemes, Algorithms- AG, MWPG.

UNIT IV Mobile - IP Networks **(9)**
Macro-mobility Protocols, Micro-mobility protocol:Tunnel based : Hierarchical Mobile IP, Intra domain Mobility Management, Routing based: Cellular IP, Handoff Wireless Access Internet Infrastructure (HAWAII).

UNIT V Mobile Ad –Hoc Networks **(9)**
Internet-based mobile ad-hoc networking communication strategies, Routing algorithms – Proactive routing: destination sequenced Distance Vector Routing (DSDV), Reactive routing: Dynamic Source Routing (DSR), Ad hoc On-Demand Distance Vector Routing (AODV), Hybrid Routing: Zone Based Routing (ZRP).

Total Hours: 45

TEXT BOOKS:

1. DeepankarMedhi, Karthikeyan Ramasamy, Network Routing: Algorithms, Protocols, and Architectures, Morgan Kaufmann Publishers, Elsevier, 2007
2. William Stallings, High speed networks and Internets Performance and Quality of Service, 2nd Edition, Pearson Education Asia. Reprint India 2002
3. C.Siva Rama Murthy and Mohan Gurusamy, WDM Optical Networks – Concepts, Design and Algorithms, Prentice Hall of India Pvt. Ltd, New Delhi 2002

REFERENCES:

1. C.E Perkins, Ad Hoc Networking, Addison – Wesley, 2001
2. S. Keshav, An engineering approach to computer networking, Addison Wesley 1999.
3. William Stallings, High speed Networks TCP/IP and ATM Design Principles, Prentice-Hall, New York, 1998

WEBSITES:

1. https://nptel.ac.in/content/storage2/courses/117105076/pdf/8.1%20Lesson%2026.pdf
2. http://opti.tmit.bme.hu/~cinkler/TMP/MYPUBwithcitations/pdf/J_200302_ieeeNetwork_Grooming_c.pdf
3. https://pdfs.semanticscholar.org/9206/4a40da71f5f78b0a33d7ee2e546908ff4909.pdf

KARPAGAM ACADEMY OF HIGHER EDUCATION

Department of Computer Science and Engineering

Faculty of Engineering

Lecture Plan

Network Routing - An Introduction, Basics and Foundation, Shortest path and Widest Path, Framework and Principles, Network Flow Modelling

Session No	Topics to be covered	Reference	Teaching Method	Testing Method
1	Network Routing	1,2	BB	1.Group discussion 2.Self-test questions
2	An Introduction	1,2	BB	1..Quiz 2. Self- Test Questions
3	Basics and Foundation	1,2	BB	1.Self-test questions 2.Group discussion
4	Shortest path	1,2	BB	Group discussion
5	Widest Path	1,2	BB	1.Self test questions
6	Framework	1,2	BB	1.Self test questions
7	Principles	1,2	BB	1.Self test questions
8	Network Flow Modelling	1,2	BB	1.Self test questions
9	Review of Network routing	1,2	PPT	1.Self test questions

Routing IP Networks-IP Routing and Distance vector routing Protocol family, OSPF and Integrated IS-IS, IP traffic Engineering, BGP, Internet Routing Architectures.

10	Routing IP Networks	1,2	BB	1.Quiz 2.Self test questions
11	IP Routing	1,2	BB	1.Quiz 2.Self test questions
12	Distance vector routing Protocol family	1,2	BB	Self test questions
13	OSPF and Integrated IS-IS	1,2	BB	Review
14	IP traffic Engineering	1,2	BB	1.Quiz 2.Self test questions
15, 16	BGP	1,2	BB	1.Quiz 2.Self test questions
17, 18	Internet Routing Architectures	1,2	BB	1.Group discussion 2.Self test questions

Routing in the PSTN- Hierarchical and Dynamic Call routing, Traffic engineering, SS7, PSTN architecture and routing.				
19, 20	Routing in the PSTN	1,2,3	BB	1.Quiz 2.Self test questions
21, 22	Hierarchical and Dynamic Call Routing	1,2,3	BB	1.Quiz 2.Self test questions
23, 24	Traffic engineering	1,2,3	BB	1.Quiz 2.Self test questions
25	SS7	1,2,3	BB	Group discussion
26, 27	PSTN architecture & Routing	1,2,3	BB	Group discussion
Router Architectures-IP address lookup algorithms, IP packet filtering and classification				
28, 29	Router Architectures	2,3	BB	1.Quiz 2.Self test questions
30, 31	IP address lookup algorithms	2,3	BB	1.Quiz 2.Self test questions
32,33	IP packet filtering	2,3	BB	1.Quiz 2.Self test questions

34,35	IP packet classification	2,3	BB	Group discussion
36	Review of Router Architectures	-	BB	
Towards next Generation - QOS routing, MPLS and GMPLS, routing and traffic engineering with MPLS, VoIP routing, Interoperability through IP and PSTN				
37, 38	Towards next Generation	2,3	PPT	1.Quiz 2.Self test questions
39	QOS routing	2,3	PPT	1.Quiz 2.Self test questions
40	MPLS	2,3	PPT	1.Quiz 2.Self test questions
41	GMPLS	2,3	PPT	Group discussion
42	Routing and traffic engineering with MPLS	2,3	PPT	1.Quiz 2.Self test questions
43	VoIP routing	2,3	PPT	1.Quiz 2.Self test questions
44	Interoperability through IP and PSTN	2,3	PPT	1.Quiz 2.Self test questions
45	Review of Entire Syllabus	-	PPT	1.Quiz 2.Self test questions

TEXT BOOKS:

4. DeepankarMedhi, Karthikeyan Ramasamy, Network Routing: Algorithms, Protocols, and Architectures, Morgan Kaufmann Publishers, Elsevier, 2007
5. William Stallings, High speed networks and Internets Performance and Quality of Service, 2nd Edition, Pearson Education Asia. Reprint India 2002
6. C.Siva Rama Murthy and Mohan Gurusamy, WDM Optical Networks – Concepts, Design and Algorithms, Prentice Hall of India Pvt. Ltd, New Delhi 2002

REFERENCES:

4. C.E Perkins, Ad Hoc Networking, Addison – Wesley, 2001
5. S. Keshav, An engineering approach to computer networking, Addison Wesley 1999.
6. William Stallings, High speed Networks TCP/IP and ATM Design Principles, Prentice-Hall, New York, 1998

WEBSITES:

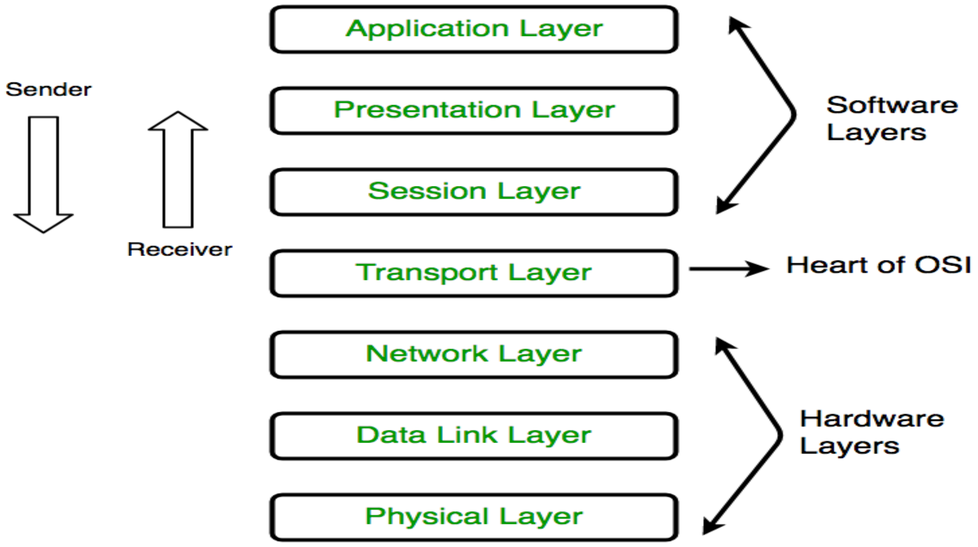
4. https://nptel.ac.in/content/storage2/courses/117105076/pdf/8.1%20Lesson%2026.pdf
5. http://opti.tmit.bme.hu/~cinkler/TMP/MYPUBwithcitations/pdf/J_200302_ieeeNetwork_Grooming_c.pdf
6. https://pdfs.semanticscholar.org/9206/4a40da71f5f78b0a33d7ee2e546908ff4909.pdf

LECTURE NOTES

UNIT-1

Layers of OSI Model

OSI stands for Open Systems Interconnection. It has been developed by ISO – 'International Organization of Standardization', in the year 1984. It is a 7 layer architecture with each layer having specific functionality to perform. All these 7 layers work collaboratively to transmit the data from one person to another across the globe.



1. Physical Layer (Layer 1) :

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.

The functions of the physical layer are :

1. Bit synchronization: The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at bit level.

2. Bit rate control: The Physical layer also defines the transmission rate i.e. the number of bits sent per second.

3. Physical topologies: Physical layer specifies the way in which the different, devices/nodes are arranged in a network i.e. bus, star or mesh topolgy.

4. Transmission mode: Physical layer also defines the way in which the data flows between the two connected devices. The various transmission modes possible are: Simplex, half-duplex and full-duplex.

* Hub, Repeater, Modem, Cables are Physical Layer devices.

** Network Layer, Data Link Layer and Physical Layer are also known as Lower Layers or Hardware Layers.

2. Data Link Layer (DLL) (Layer 2) :

The data link layer is responsible for the node to node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of DLL to transmit it to the Host using its MAC address.

Data Link Layer is divided into two sub layers :

1. Logical Link Control (LLC)

2. Media Access Control (MAC)

The packet received from Network layer is further divided into frames depending on the frame size of NIC(Network Interface Card). DLL also encapsulates Sender and Receiver’s MAC address in the header.

The Receiver’s MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking “Who has that IP address?” and the destination host will reply with its MAC address.

The functions of the data Link layer are :

1. Framing: Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.

2. Physical addressing: After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in the header of each frame.

3. Error control: Data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.

4. Flow Control: The data rate must be constant on both sides else the data may get corrupted thus , flow control coordinates that amount of data that can be sent before receiving acknowledgement.

5. Access control: When a single communication channel is shared by multiple devices, MAC sub-layer of data link layer helps to determine which device has control over the channel at a given time.

* Packet in Data Link layer is referred as Frame.

** Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.

*** Switch & Bridge are Data Link Layer devices.

3. Network Layer (Layer 3) :

Network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP address are placed in the header by the network layer.

The functions of the Network layer are :

1. Routing: The network layer protocols determine which route is suitable from source to destination. This function of network layer is known as routing.

2. Logical Addressing: In order to identify each device on internetwork uniquely, network layer defines an addressing scheme. The sender & receiver's IP address are placed in the header by network layer. Such an address distinguishes each device uniquely and universally.

* Segment in Network layer is referred as Packet.

** Network layer is implemented by networking devices such as routers.

4. Transport Layer (Layer 4) :

Transport layer provides services to application layer and takes services from network layer. The data in the transport layer is referred to as Segments. It is responsible for the End to End Delivery of the complete message. The transport layer also provides the acknowledgement of the successful data transmission and re-transmits the data if an error is found.

• At sender's side:

Transport layer receives the formatted data from the upper layers, performs Segmentation and also implements Flow & Error control to ensure proper data transmission. It also adds Source and Destination port number in its header and forwards the segmented data to the Network Layer.

Note: The sender need to know the port number associated with the receiver's application.

Generally, this destination port number is configured, either by default or manually. For example, when a web application makes a request to a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default port assigned.

• At receiver's side:

Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.

The functions of the transport layer are :

1. Segmentation and Reassembly: This layer accepts the message from the (session) layer , breaks the message into smaller units . Each of the segment produced has a header associated with it. The transport layer at the destination station reassembles the message.

2. Service Point Addressing: In order to deliver the message to correct process, transport layer header includes a type of address called service point address or port address. Thus by specifying this address, transport layer makes sure that the message is delivered to the correct process.

The services provided by the transport layer :

1. Connection Oriented Service: It is a three-phase process which include

- Connection Establishment
- Data Transfer
- Termination disconnection

In this type of transmission, the receiving device sends an acknowledgement, back to the source after a packet or group of packet is received. This type of transmission is reliable and secure.

2. Connection less service: It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.

.

5. Session Layer (Layer 5) :

This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.

The functions of the session layer are :

1. Session establishment, maintenance and termination: The layer allows the two processes to establish, use and terminate a connection.

2. Synchronization : This layer allows a process to add checkpoints which are considered as synchronization points into the data. These synchronization point help to identify the error so that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.

3. Dialog Controller : The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

SCENARIO:

Let’s consider a scenario where a user wants to send a message through some Messenger application running in his browser. The “Messenger” here acts as the application layer which provides the user with an interface to create the data. This message or so-called Data is compressed, encrypted (if any secure data) and converted into bits (0’s and 1’s) so that it can be transmitted.

6. Presentation Layer (Layer 6) :

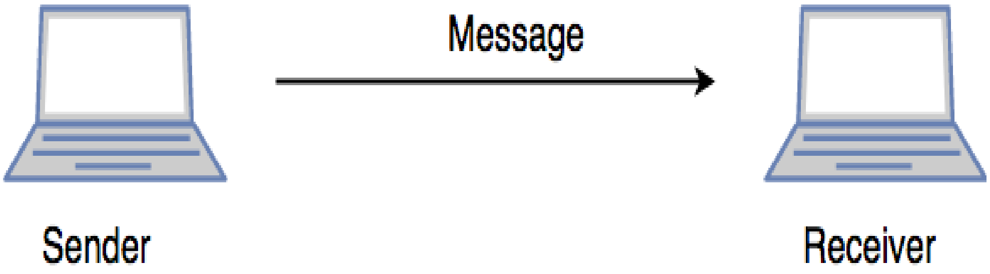
Presentation layer is also called the Translation layer.The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

The functions of the presentation layer are :

1. Translation : For example, ASCII to EBCDIC.

2. Encryption/ Decryption : Data encryption translates the data into another form or code. The encrypted data is known as the cipher text and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.

3. Compression: Reduces the number of bits that need to be transmitted on the network.



7. Application Layer (Layer 7) :

At the very top of the OSI Reference Model stack of layers, we find Application layer which is implemented by the network applications. These applications produce the data, which has to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Ex: Application – Browsers, Skype Messenger etc.

**Application Layer is also called as Desktop Layer.

The functions of the Application layer are :

1. Network Virtual Terminal

2. FTAM-File transfer access and management

3. Mail Services

4. Directory Service

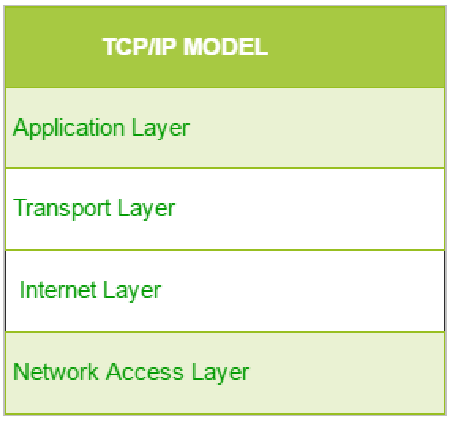
TCP/IP Model

Prerequisite – Layers of OSI Model

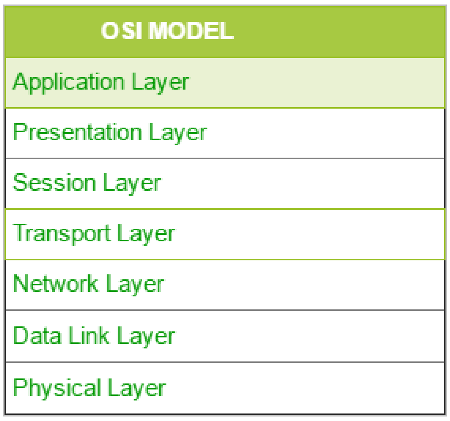
The OSI Model we just looked at is just a reference/logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components. But when we talk about the TCP/IP model, it was designed and developed by Department of Defense (DoD) in 1960s and is based on standard protocols. It stands for Transmission Control Protocol/Internet Protocol. The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model. The layers are:

1. Process/Application Layer
2. Host-to-Host/Transport Layer
3. Internet Layer
4. Network Access/Link Layer

The diagrammatic comparison of the TCP/IP and OSI model is as follows :



TCP/IP MODEL
Application Layer
Transport Layer
Internet Layer
Network Access Layer



OSI MODEL
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Difference between TCP/IP and OSI Model:

TCP/IP	OSI
TCP refers to Transmission Control	OSI refers to Open Systems

Protocol.	Interconnection.
TCP/IP has 4 layers.	OSI has 7 layers.
TCP/IP is more reliable	OSI is less reliable
TCP/IP does not have very strict boundaries.	OSI has strict boundaries
TCP/IP follow a horizontal approach.	OSI follows a vertical approach.
TCP/IP uses both session and presentation layer in the application layer itself.	OSI uses different session and presentation layers.
TCP/IP developed protocols then model.	OSI developed model then protocol.

The first layer is the Process layer on the behalf of the sender and Network Access layer on the behalf of the receiver. During this article, we will be talking on the behalf of the receiver.

1. Network Access Layer –

This layer corresponds to the combination of Data Link Layer and Physical Layer of the OSI model. It looks out for hardware addressing and the protocols present in this layer allows for the physical transmission of data.

We just talked about ARP being a protocol of Internet layer, but there is a conflict about declaring it as a protocol of Internet Layer or Network access layer. It is described as residing in layer 3, being encapsulated by layer 2 protocols.

2. Internet Layer –

This layer parallels the functions of OSI's Network layer. It defines the protocols which are responsible for logical transmission of data over the entire network. The main protocols residing at this layer are :

1. IP – stands for Internet Protocol and it is responsible for delivering packets from the source host to the destination host by looking at the IP addresses in the packet headers. IP has 2 versions:

IPv4 and IPv6. IPv4 is the one that most of the websites are using currently. But IPv6 is growing as the number of IPv4 addresses are limited in number when compared to the number of users.

2. ICMP – stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.

3. ARP – stands for Address Resolution Protocol. Its job is to find the hardware address of a host from a known IP address. ARP has several types: Reverse ARP, Proxy ARP, Gratuitous ARP and Inverse ARP.

3. Host-to-Host Layer

This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are :

1. Transmission Control Protocol (TCP) – It is known to provide reliable and error-free communication between end systems. It performs sequencing and segmentation of data. It also has acknowledgment feature and controls the flow of the data through flow control mechanism. It is a very effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.

2. User Datagram Protocol (UDP) – On the other hand does not provide any such features. It is the go-to protocol if your application does not require reliable transport as it is very cost-effective. Unlike TCP, which is connection-oriented protocol, UDP is connectionless.

4. Process Layer

This layer performs the functions of top three layers of the OSI model: Application, Presentation and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some of the protocols present in this layer are: HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, LPD. Have a look at Protocols in Application Layer for some information about these protocols. Protocols other than those present in the linked article are :

1. HTTP and HTTPS – HTTP stands for Hypertext transfer protocol. It is used by the World Wide Web to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL(Secure Socket Layer). It is efficient in cases where the browser need to fill out forms, sign in, authenticate and carry out bank transactions.

2. SSH – SSH stands for Secure Shell. It is a terminal emulations software similar to Telnet. The reason SSH is more preferred is because of its ability to maintain the encrypted connection. It sets up a secure session over a TCP/IP connection.

3. NTP – NTP stands for Network Time Protocol. It is used to synchronize the clocks on our computer to one standard time source. It is very useful in situations like bank transactions. Assume the following situation without the presence of NTP. Suppose you carry out a transaction, where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very badly if it’s out of sync.

FUNCTIONS OF THE NETWORK LAYER

The network layer provides the means of transferring variable-length network packets from a source to a destination host via one or more networks. Within the service layering semantics of the OSI network architecture, the network layer responds to service requests from the transport layer and issues service requests to the data link layer.

Functions of the network layer include:

Connectionless communication

For example, IP is connectionless, in that a data packet can travel from a sender to a recipient without the recipient having to send an acknowledgement. Connection-oriented protocols exist at other, higher layers of the OSI model.

Host addressing

Every host in the network must have a unique address that determines where it is. This address is normally assigned from a hierarchical system. For example, you can be :

"Fred Murphy" to people in your house,

"Fred Murphy, 1 Main Street" to Dubliners,

"Fred Murphy, 1 Main Street, Dublin" to people in Ireland,

"Fred Murphy, 1 Main Street, Dublin, Ireland" to people anywhere in the world.

On the Internet, addresses are known as IP addresses (Internet Protocol).

Message forwarding

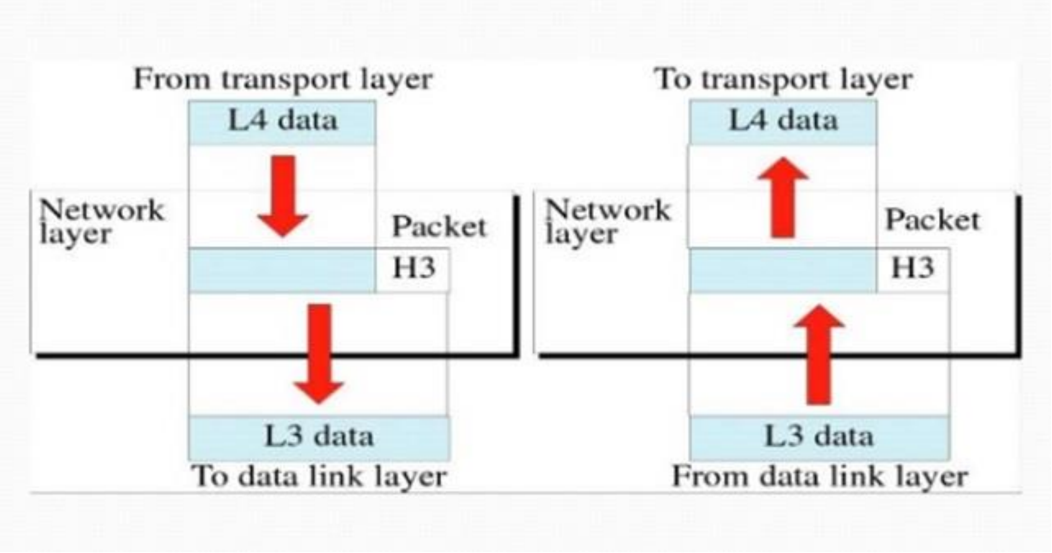
Since many networks are partitioned into subnetworks and connect to other networks for wide-area communications, networks use specialized hosts, called gateways or routers, to forward packets between networks.

Protocols used in network layer

The following are examples of protocols operating at the network layer.

- CLNS, Connectionless-mode Network Service
- DDP, Datagram Delivery Protocol
- EGP, Exterior Gateway Protocol
- EIGRP, Enhanced Interior Gateway Routing Protocol
- ICMP, Internet Control Message Protocol

- IGMP, Internet Group Management Protocol
- IPsec, Internet Protocol Security
- IPv4/IPv6, Internet Protocol
- IPX, Internetwork Packet Exchange
- OSPF, Open Shortest Path First
- PIM, Protocol Independent Multicast
- RIP, Routing Information Protocol



Types of Routing

Routing is a process which is performed by layer 3 (or network layer) devices in order to deliver the packet by choosing an optimal path from one network to another.

There are 3 types of routing:

1. Static routing –

Static routing is a process in which we have to manually add routes in routing table.

Advantages –

- No routing overhead for router CPU which means a cheaper router can be used to do routing.

- It adds security because only administrator can allow routing to particular networks only.

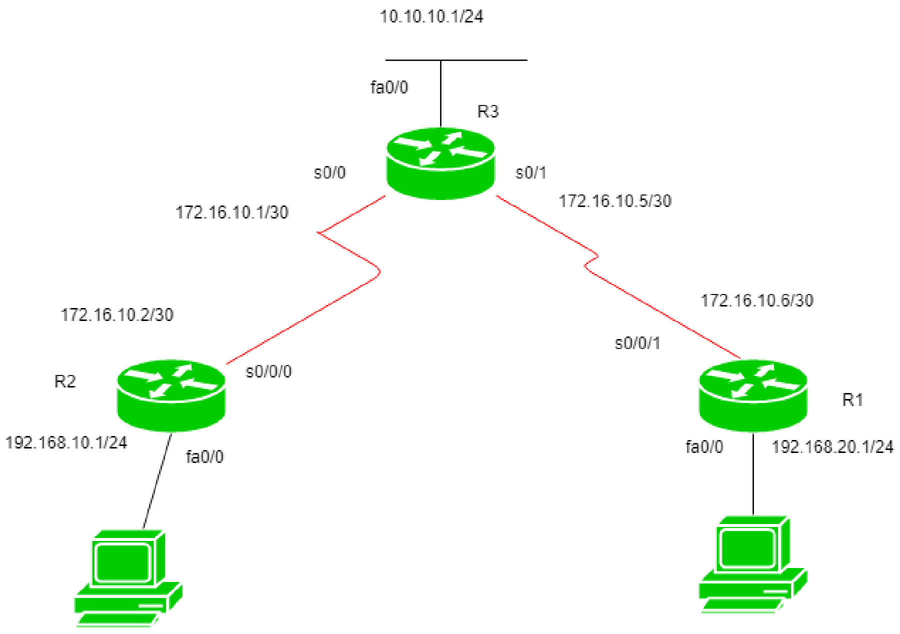
- No bandwidth usage between routers.

Disadvantage –

- For a large network, it is a hectic task for administrator to manually add each route for the network in the routing table on each router.

- The administrator should have good knowledge of the topology. If a new administrator comes, then he has to manually add each route so he should have very good knowledge of the routes of the topology.

Configuration –



R1 having IP address 172.16.10.6/30 on s0/0/1, 192.168.10.1/24 on fa0/0.

R2 having IP address 172.16.10.2/30 on s0/0/0, 192.168.20.1/24 on fa0/0.

R3 having IP address 172.16.10.5/30 on s0/1, 172.16.10.1/30 on s0/0, 10.10.10.1/24 on fa0/0.

Now configuring static routes for router R3:

```
R3(config)#ip route 192.168.10.0 255.255.255.0 172.16.10.2

R3(config)#ip route 192.168.20.0 255.255.255.0 172.16.10.6
```

Here, provided the route for 192.168.10.0 network where 192.168.10.0 is its network I’d and 172.16.10.2 and 172.16.10.6 are the next hop address.

Now, configuring for R2:

```
R2(config)#ip route 192.168.20.0 255.255.255.0 172.16.10.1

R2(config)#ip route 10.10.10.0 255.255.255.0 172.16.10.1

R2(config)#ip route 172.16.10.4 255.255.255.0 172.16.10.1
```

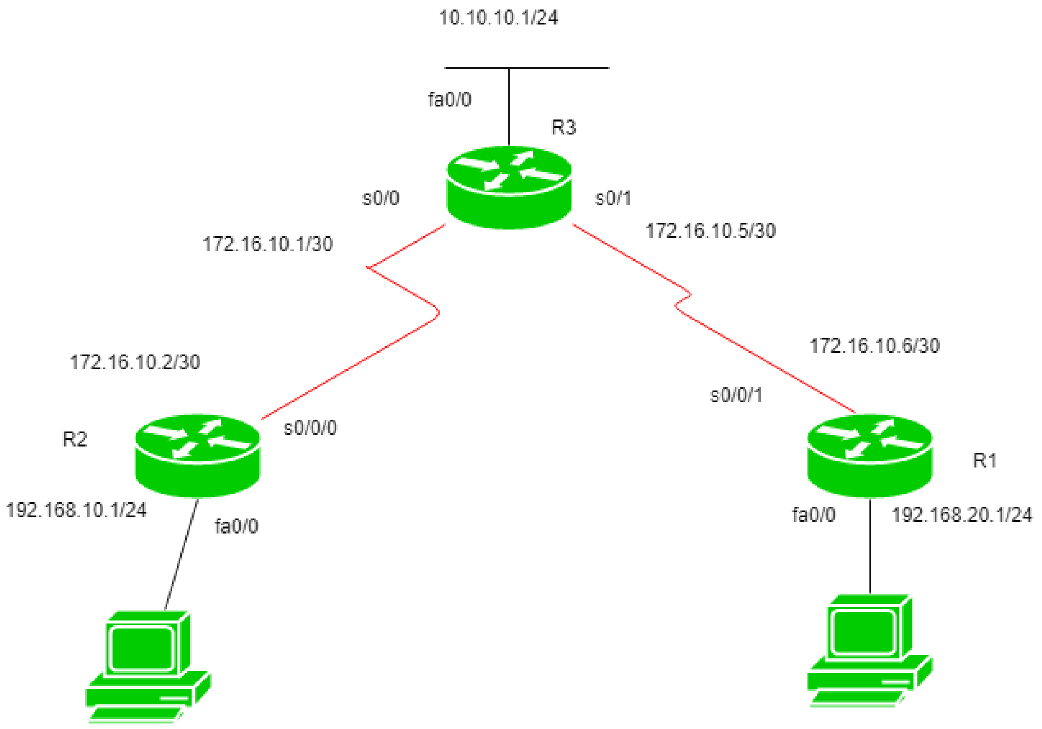
Similarly for R1:

```
R1(config)#ip route 192.168.10.0 255.255.255.0 172.16.10.5

R1(config)#ip route 10.10.10.0 255.255.255.0 172.16.10.5

R1(config)#ip route 172.16.10.0 255.255.255.0 172.16.10.5
```

Default Routing

This is the method where the router is configured to send all packets towards a single router (next hop). It doesn’t matter to which network the packet belongs, it is forwarded out to router which is configured for default routing. It is generally used with stub routers. A stub router is a router which has only one route to reach all other networks.

Configuration



Using the same topology which we have used for the static routing before.

In this topology, R1 and R2 are stub routers so we can configure default routing for both these routers.

Configuring default routing for R1:

R1(config)#ip route 0.0.0.0 0.0.0.0 172.16.10.5

Now configuring default routing for R2:

R2(config)#ip route 0.0.0.0 0.0.0.0 172.16.10.1

3. Dynamic Routing:

Dynamic routing makes automatic adjustment of the routes according to the current state of the route in the routing table. Dynamic routing uses protocols to discover network destinations and the routes to reach it. RIP and OSPF are the best examples of dynamic routing protocol. Automatic adjustment will be made to reach the network destination if one route goes down.

A dynamic protocol have following features:

1. The routers should have the same dynamic protocol running in order to exchange routes.

2. When a router finds a change in the topology then router advertises it to all other routers.

Advantages –

- Easy to configure.

- More effective at selecting the best route to a destination remote network and also for discovering remote network.

Disadvantage –

- Consumes more bandwidth for communicating with other neighbors.

- Less secure than static routing.

ROUTING IN THE TELEPHONE NETWORK

In this section, we will focus on concepts and techniques for routing in the telephone network. A good reference that covers this material in greater depth is [Girard 90].

A national telephone network is structured as a fairly rigid three-level hierarchy, where the levels represent subscriber telephone instruments or modems, central offices, and long-distance or toll switching offices We will refer to the set of toll switches as the network core. A local exchange carrier, such as Bell Atlantic in the eastern United States, provides local telephone service and manages many central offices interconnected with one-hop links. Every central office in each local exchange carrier's domain logically connects to one node (or, rarely, two nodes) in the core. Each element in the core, such as the Lucent 4ESS switch we mentioned in Chapter 8, can switch up to 120,000 simultaneous calls and costs several million dollars.

The core is structured as a fully connected mesh or clique, with every toll switch connected to every other toll switch by a logical one-hop path. The number of interconnections is truly enormous. For example, the AT&T wide-area network core has around 135 switches interconnected by nearly 5 million trunks. This dense connectivity simplifies routing. The routing algorithm is as follows:

(a) If a call's source and destination are within a central office, directly connect them.

(b) If the call is between central offices within a local exchange carrier, use a one hop path between central offces.

(c) Otherwise send the call to (one of) the core(s).

The only major decision is at a toll switch, which chooses either a one-hop or a two-hop path to a destination switching system. It is not necessary to consider longer paths because the core is a logical clique. Thus, for an m-element core, each direct path corresponds to m — 1 alternative two-hop paths. The essence of telephone-network routing is in determining which one-hop path to choose in the core, and if this is fully used, the order in which to try two-hop paths.

Over the past hundred years, many different routing policies have been used in the telephone network. The computational limitations of electromechanical relays highly constrained the earliest policies. As computerized switching systems have replaced these, the routing policies have become increasingly sophisticated. However, all telephone routing policies have the same features, which we discuss next.

Features of telephone network routing and a comparison with Internet routing

All telephone routing policies draw upon the fact that aggregated telephone traffic is very predictable. Thus, it is possible to compute the approximate load between every pair of toll switches in advance, for every interval of every day. This allows routes to be chosen in advance. Second, telephone switches and links are extremely reliable. Switches go down no more than an average of a few minutes per year, and links are out of commission no more than a few hours every year. Therefore, unlike the Internet, where we can rarely count upon links to stay up, in the telephone network, the normal situation is that nearly all trunks and switches are up. This allows the routing protocol to be highly optimized: instead of just trying to maintain connectivity, network administrators can use sophisticated load-balancing strategies.

The third feature of a long-distance telephone network is that a single organization controls the entire network. Thus, traffic measurement and management policies can be universally implemented. Moreover, upgrades to routing policies can be carried out uniformly. In contrast, in the Internet, network administrators in different domains may choose differing policies, or worse, run out-of-date and inconsistent routing protocols.

Fourth, the network is very highly connected, with many equal-length alternative paths. In contrast, the Internet is rather sparse, so there are few choices for alternative paths in the core. (If this changes, some techniques used might become applicable to the Internet.)

Finally, routes in the telephone network are associated with a quality of service guarantee. Therefore, unlike the Internet, mere connectivity is not sufficient to complete a call: the path must also have sufficient resources available. Note, however, that all voice calls require the same, simple quality of service, so the admission control decision is trivial.

The cost of telephone network routing

Telephone network routing is simple because, historically, the electromechanical relays used for network control could not execute sophisticated programs. This simplicity, however, comes at a cost. For example, if a switch in the core crashes, the telephone network routing protocol cannot find an alternative path to an end system reached through that switch, We conclude that to make the system reliable, every switch must be reliable. Similarly, the routing protocol requires every pair of switches to be connected by a one-hop logical trunk group. Although the physical connectivity is much sparser, creating and maintaining this logically fully con nested clique is expensive. Would it not be cheaper to build a network where sophisticated routing algorithms lower the requirements for connectivity and com ponent reliability? This is a hundred-billion dollar question!

If we could build a network that has all the features of the telephone network (low blocking probability, very high reliability, global coverage) using newer switching systems, the new network need riot require a fully interconnected and reliable core, thus reducing costs. However, the switching, billing, signaling, and operations support systems that currently sit on top of this relatively simple core are so extensive, and so coupled to the existing architecture, that making a sudden change is too expensive.

Eventually, the telephone network core will run over ATM, allowing greater flexibility in routing and network topology. However, a complete cut over to ATM is likely to take at least a decade, if not longer. So, the short answer is, yes, current telephone network routing leads to increased cost, but, in the near term, the topology of the core is too ingrained to change.

In any case, note that a good rule of thumb is that about 80% of the cost of the entire telephone network is in the local loop, and about 90% of the local loop cost is in the labor of installation. Elhe expense of nonoptimal routing in the core pales in comparison with these costs!

DYNAMIC NONHIERARCHICAL ROUTING

The simplest possible routing algorithm in the network core is for it to accept a call if and only if the one-hop path is available. This algorithm is nonoptimal, in that a call may be rejected though a two-hop path was available. A major advance in telephone routing was the introduction of dynamic nonhierarchical routing (DNHR). DNHR divides the day into approximately ten periods. In each period, each toll switch is assigned a primary (one-hop) path to another toll switch, and an ordered set of alternative (twohop) paths. Incoming call-setup packets are first forwarded on the primary path. If sufficient resources are not available on the primary path, then the switch tries each of the allocated two-hop paths in turn (we call this spilling or overflow). The switch rejects the call if all the alternative paths are busy. The process in which a call rejected on a primary path is retried on an alternative path is called crankback. Crankback is necessary in any routing policy that supports quality-of-service constraints and wants to achieve a low call rejection rate.

DNHR draws upon the predictability of aggregated telephone traffic, and the fact that switches and links are usually available, to select optimal alternative two-hop paths. DNHR performance suffers when traffic changes unexpectedly, so that the list of alternative paths ought to change, but does not. This might increase load on trunk groups that are already heavily loaded while leaving other trunks underutilized..

The Erlang map

An important idea associated with routing in general, and with telephone routing in particular, is the Erlang map [Girard 90, p. 1591. The Erlang blocking formula, described in Section 14.11.2, allows us to compute the blocking probability of a trunk group if we know the load on the group and its capacity. Given a fixed external call load on the network core, a routing strategy determines the load on each trunk group, and therefore the blocking probability for that trunk group. DNHR assigns a set of alternative paths to toll switches so that the expected blocking probability for an incoming call is minimized. Thus, the path of a new call depends on the expected load on each trunk group, which depends, in turn, on the routing! This circular dependency between routing and blocking probability leads to a system of equations called the Erlang map. We can show that the Erlang map has a unique fixed-point solution called the Erlang fixed point.

More precisely, we define B (k) to be the blocking probability on trunk k, where B(k) = E(L(k), C(k)), E(...) is the Erlang formula, L(k) is the load on link k, and C(k) is its capacity. Now, if a route r is denoted by a set of links, and v(r) represents the external load on r, then we can approximate L(k) by :

L(k) = fl (1 B(j)) (1.1)

r:k€r

To see this, note that "(r) is the intrinsic load on route r. Each factor of (1 — B (j)) represents a "thinning" of the load, so that the load on trunk k is just the thinned sum of the loads on all the routes that share trunk k. B (k) clearly depends on some number of other B (j)s, through B (k) — E(L(k), C (k)) and Equation 1.1. Thus, each of the B (k)s is implicitly defined by the others and forms the Erlang map.

Metastability in DNHR

Though the Erlang map has a unique solution, which represents a long-term mean blocking rate on each link, this solution is often the time-average of two distinct values, one high and the other low. In other words, given a blocking probability for a particular link, b, as the solution to Equation 1.1, we achieve b as the mean of two other values and blow. The underlying physical mechanism is that given a particular traffic load, the network periodically changes from a state where most blocking probabilities are low (blow) to a state where most blocking probabilities are high (bhigh). The mean bloc:'ing probability, b, is their average, and, in practice, the network may never achieve it. L-us see why.

Consider a network where a sudden burst of activity between toll switches A and B forces traffic to be off-loaded (spilled) onto paths ACB and ADB, adding extra load to links AC, CB, AD, and DB If more traffic now appears on any one of these links, this traffic may, in turn, be diverted to other two-hop paths, making the situation worse. The key point is that every time a toll switch spills traffic to a two-hop alternative path, it increases the blocking probability for two other one-hop paths that use these links. We can show that the network, under a heavy load, can reach a metastable state where almost every call takes a two-hop path. Moreover, even with no change in mean offered load, the network can suddenly return to a "norrnal" state, where most paths are single hop. This is the physical mechanism underlying the multiple blocking probabili-

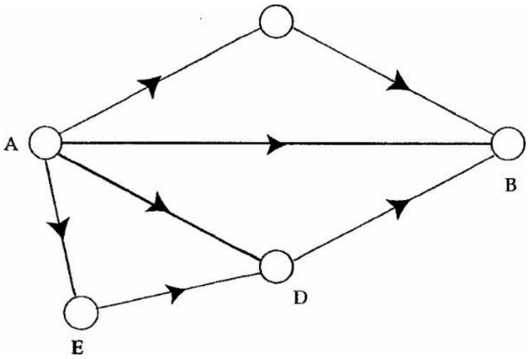


Figure: Metastability in telephone networks. Suppose the one-hop path from A to B is full (indicated by the heavy line), so that calls spill to two-hop paths A—C—B and A—D—B. ms increases the load on trunks AC, AD, CB, and CB. The additional load may cause trunk AD to fill, causing calls from A to D to further spill to trunks AE and ED. If this continues, all calls take only two-hop paths through the core, although by rearranging calls, most or all of them can be diverted to one-hop paths. This is called metastability. in the telephone network

ties we mentioned in the previous paragraph. Metastability is undesirable because it can lead to a high call blocking rate even with moderate loads.

The existence of metastability in the telephone network is a cause of much concern. However, we can prevent it by simply reserving some part of the capacity on each trunk for one-hop calls [Akinpelu 841. Continuing with our example, when the trunk AB is busy, AC and CB are allowed to carry no more than a given fraction of two-hop calls. Thus, new calls requiring, say, the CB trunk, would always have a good chance of being carried on a one-hop path. It can be shown that this technique (called trunk reservation) prevents the network from entering a metastable state . The cost of trunk reservation is that the network may block a call even when it has sufficient capacity, thus increasing call blocking probability. However, because the network never reaches the metastable state, the overall blocking probability drops.

Shadow prices

How should the network allocate the set of alternative paths to a toll switch?. The idea is that if a call is carried on a trunk, it increases the blocking probability for future calls on that trunk. We quantify this increase in blocking probability as a shadow price. When a call comes in, we can compute the sum of the shadow prices for every alternate path. If the sum is larger than the revenue gained from a single call on every path, then the network should drop the call. Otherwise, the network should route it on the trunk that has the least cost. Given past traffic history, a network administrator can compute the expected least cost trunks for each period. These, then, form the set of alternative paths allocated to each toll switch by DNHR. If we can measure trunk loads dynamically, the shadow price approach allows a toll switch to compute optimal alternative paths for each call, instead of once every time period, as in DNHR.

TSMR

In DNHR, a central computer gives each toll switch a set of alternative paths based on past measurements, which are updated once a week. If a sudden surge of calls arrives on a trunk, the only adaptability in the network is to start trying the previously prescribed alternate paths. Although this was suitable for earlier toll switches that had very limited computational power, modern switch controllers can do much better. One step in this direction is trunk status map routing, or TSMR. In this scheme, each switch controller measures the load on each of its outgoing links and tells this to a central computer. The central computer periodically computes optimal alternative paths for each toll switch (based, for example, on the current load and the corresponding shadow prices) and loads these into all the toll switches. Thus, the central computer updates the choice of alternative paths more often than with DNHR. To dampen routing changes, a toll switch updates its load measurement only if this load changes "significantly," meaning, typically, 12.5%.

RTNR

The latest in the series of telephone routing algorithms is real-time network routing (telephone routing algorithms seem to require four-letter acronyms, and this is called RTNR).

RTNR, which typifies the current generation of telephone routing algorithms, replaced DNI-IR in AT&T's long-distance network in 1991. Unlike DNHR and TSMR, RTNR does not use centralized control. Instead, each toll switch monitors the loading of every outgoing trunk and computes a list of lightly loaded trunks. If the primary path for a call is busy, the originating toll switch asks the destination for the destination's list. Since calls are symmetric, the logical AND of the two lists is the set of lightly loaded alternative paths from the originating switch to the destination. For example, toll switch A may have light loads on links AB, AC, and AE. If the destination is D, D may report light loads on DC, DE, and DG. If DC is lightly loaded, from symmetry, so is CD So, A knows that AC and CD are both lightly loaded, and discovers that A—C—D is a good alternative path.

RTNR allows a trunk to be partitioned among multiple traffic classes. Each class has its own blocking probability goal and trunk reservation level. When the network is lightly loaded, we give a class as much bandwidth as it can use, but under heavy loads, admission control ensures that the network meets the class's reservation level. Note that the traffic class here is used in a rather restricted sense to mean a voice call, a data call, or a multiplexed (N* 64 kbps) call.

RTNR is very effective in practice For example, AT&T's long distance network carries up to 260 million call attempts on busy days- Of these attempts, only about one or two are blocked in the core! Other telephone companies, with similarly engineered network cores, have similar call-blocking statistics.

DISTANCE-VECTOR ROUTING

Telephone network routing is specialized to take advantage of the unique features of the telephone network, such as a predictable traffic flow, and a relatively small network core. Large packet networks, such as the Internet, present a very different environment. In the Internet, links and routers are unreliable, alternative paths are scarce, and traffic patterns can change unpredictably within minutes. It is not surprising that routing in the Internet, and in ATM networks, which are likely to have Internet-like characteristics, follows a different path. The two fundamental routing algorithms in packet-switched networks are distance-vector and link-state.

Both algorithms assume that a router knows (a) the address of each neighbor, and (b) the cost of reaching each neighbor (where the cost measures quantities like the link's capacity, the current queuing delay, or a per-packet charge). Both algorithms allow a router to find global routing information, that is, the next hop to reach every destination in the network by the shortest path, by exchanging routing information with only its neighbors. Roughly speaking, in a distance-vector algorithm, a node tells its neighbors its distance to every other node in the network, and in a link-state algorithm, a node tells every other node in the network its distance to its neighbors. Thus, both routing protocols are distributed and are suitable for large internetworks controlled by multiple administrative entities

UNIT-2

INTERNET PROTOCOL:

The **Internet Protocol** (**IP**) is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing function enables internetworking, and essentially establishes the Internet.

IP has the task of delivering packets from the source host to the destination host solely based on the IP addresses in the packet headers. For this purpose, IP defines packet structures that encapsulate the data to be delivered. It also defines addressing methods that are used to label the datagram with source and destination information.

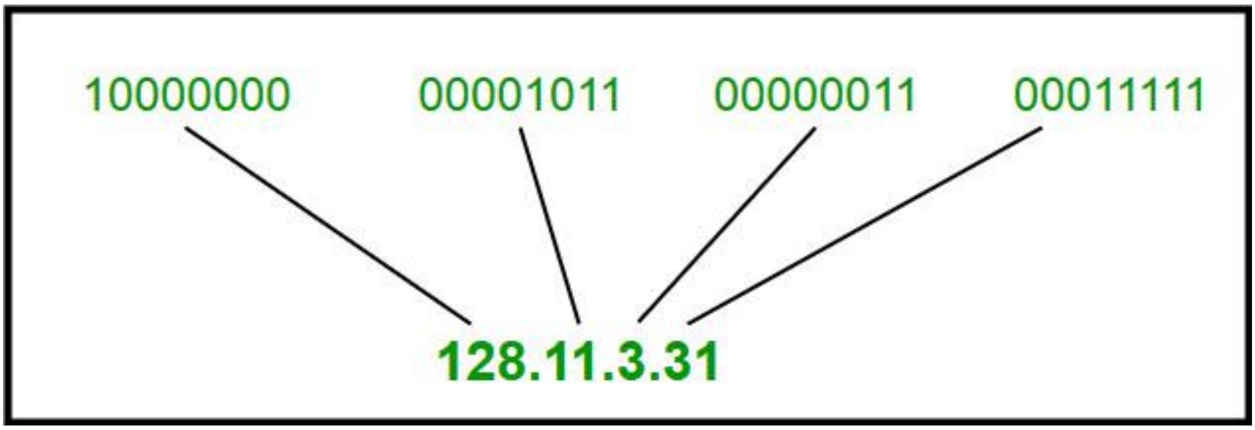
Historically, IP was the connectionless datagram service in the original Transmission Control Program introduced by Vint Cerf and Bob Kahn in 1974, which was complemented by a connection-oriented service that became the basis for the Transmission Control Protocol (TCP). The Internet protocol suite is therefore often referred to as *TCP/IP*.

The first major version of IP, Internet Protocol Version 4 (IPv4), is the dominant protocol of the Internet. Its successor is Internet Protocol Version 6 (IPv6)

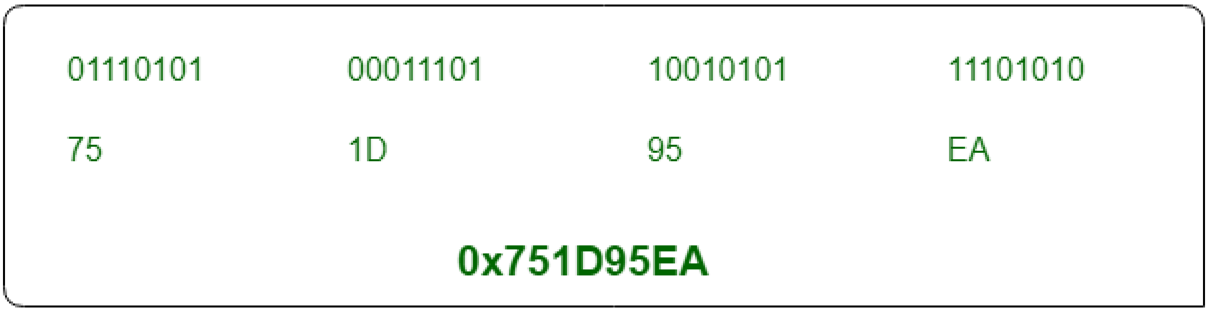
Introduction of Classful IP Addressing

IP address is an address having information about how to reach a specific host, especially outside the LAN. An IP address is a 32 bit unique address having an address space of 2^{32}. Generally, there are two notations in which IP address is written, dotted decimal notation and hexadecimal notation.

Dotted Decimal Notation:



HexadecimalNotation:



Some points to be noted about dotted decimal notation:

1. The value of any segment (byte) is between 0 and 255 (both included).
2. There are no zeroes preceding the value in any segment (054 is wrong, 54 is correct).

ClassfulAddressing:

The 32 bit IP address is divided into five sub-classes. These are:

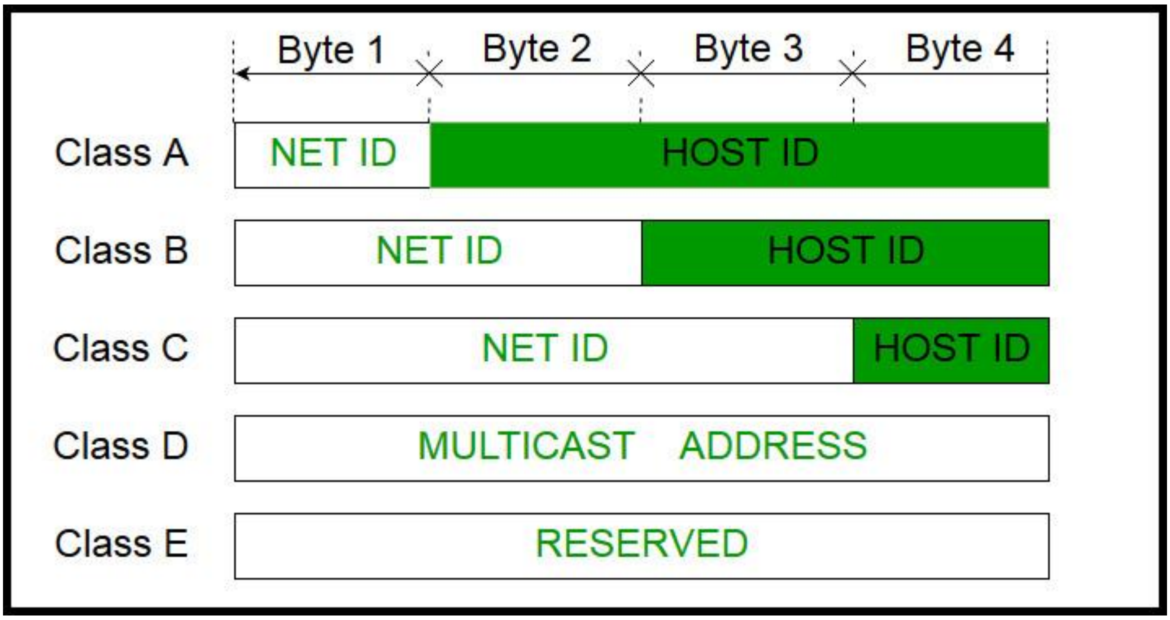
- Class A
- Class B
- Class C
- Class D
- Class E

Each of these classes has a valid range of IP addresses. Classes D and E are reserved for multicast and experimental purposes respectively.

The order of bits in the first octet determine the classes of IP address. IPv4 address is divided into two parts:

- **Network ID**
- **Host ID**

The class of IP address is used to determine the bits used for network ID and host ID and the number of total networks and hosts possible in that particular class. Each ISP or network administrator assigns IP address to each device that is connected to its network.



Note: IP addresses are globally managed by Internet Assigned Numbers Authority(IANA) and regional Internet registries(RIR).

Note: While finding the total number of host IP addresses, 2 IP addresses are not counted and are therefore, decreased from the total count because the first IP address of any network is the network number and whereas the last IP address is reserved for broadcast IP.

Class A:

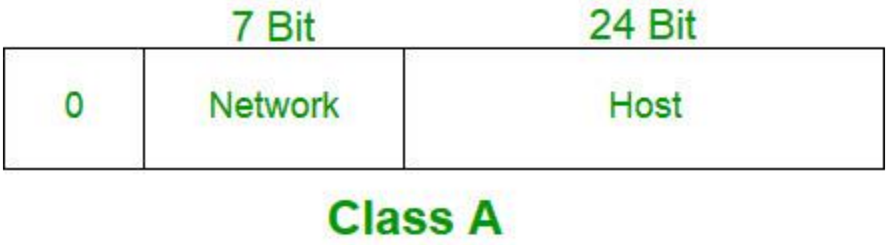
IP address belonging to class A are assigned to the networks that contain a large number of hosts.

- The network ID is 8 bits long.
- The host ID is 24 bits long.

The higher order bit of the first octet in class A is always set to 0. The remaining 7 bits in first octet are used to determine network ID. The 24 bits of host ID are used to determine the host in any network. The default subnet mask for class A is 255.x.x.x. Therefore, class A has a total of:

- 2^7-2= 126 network ID(Here 2 address is subracted because 0.0.0.0 and 127.x.y.z are special address.)
- 2^24 – 2 = 16,777,214 host ID

IP addresses belonging to class A ranges from 1.x.x.x – 126.x.x.x



Class B:

IP address belonging to class B are assigned to the networks that ranges from medium-sized to large-sized networks.

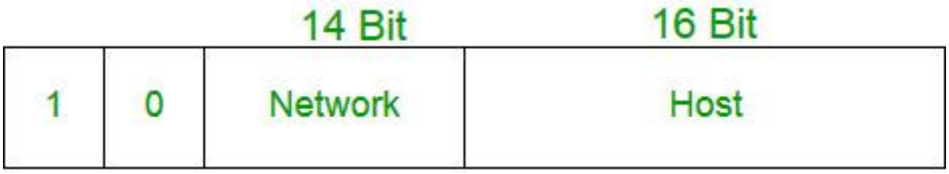
- The network ID is 16 bits long.
- The host ID is 16 bits long.

The higher order bits of the first octet of IP addresses of class B are always set to 10. The remaining 14 bits are used to determine network ID. The 16 bits of host ID is used to determine the host in any network. The default sub-net mask for class B is 255.255.x.x. Class B has a total of:

- 2^14 = 16384 network address

- 2^16 – 2 = 65534 host address

IP addresses belonging to class B ranges from 128.0.x.x – 191.255.x.x.



Class B

Class C:

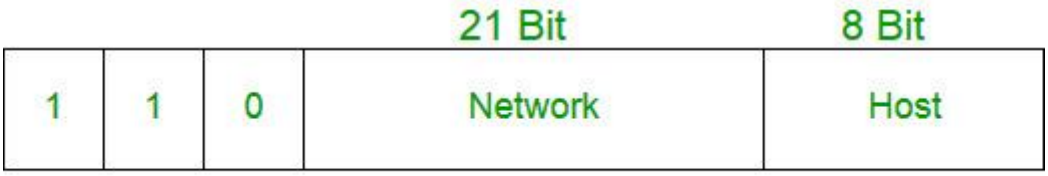
IP address belonging to class C are assigned to small-sized networks.

- The network ID is 24 bits long.
- The host ID is 8 bits long.

The higher order bits of the first octet of IP addresses of class C are always set to 110. The remaining 21 bits are used to determine network ID. The 8 bits of host ID is used to determine the host in any network. The default sub-net mask for class C is 255.255.255.x. Class C has a total of:

- 2^21 = 2097152 network address
- 2^8 – 2 = 254 host address

IP addresses belonging to class C ranges from 192.0.0.x – 223.255.255.x.

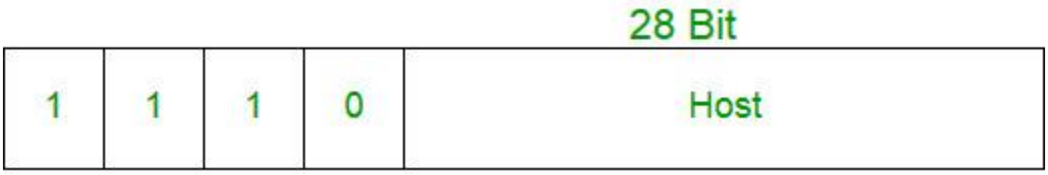


Class C

Class D:

IP address belonging to class D are reserved for multi-casting. The higher order bits of the first octet of IP addresses belonging to class D are always set to 1110. The remaining bits are for the address that interested hosts recognize.

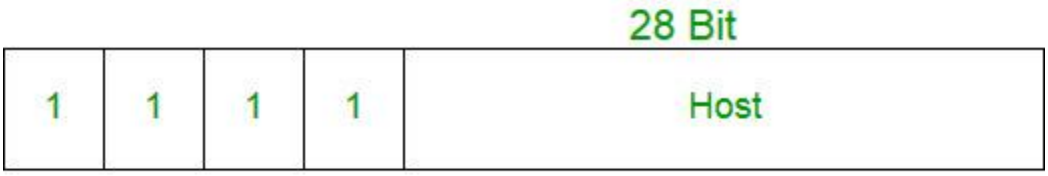
Class D does not possess any sub-net mask. IP addresses belonging to class D ranges from 224.0.0.0-239.255.255.255.



Class D

Class E:

IP addresses belonging to class E are reserved for experimental and research purposes. IP addresses of class E ranges from 240.0.0.0 – 255.255.255.254. This class doesn’t have any sub-net mask. The higher order bits of first octet of class E are always set to 1111.



Class E

Range of special IP addresses:

169.254.0.0–169.254.0.16 :Link local addresses
127.0.0.0–127.0.0.8 : Loop-back addresses
0.0.0.0 – 0.0.0.8 : used to communicate within the current network
.

Rules for assigning Host ID:

Host ID’s are used to identify a host within a network. The host ID are assigned based on the followingrules:

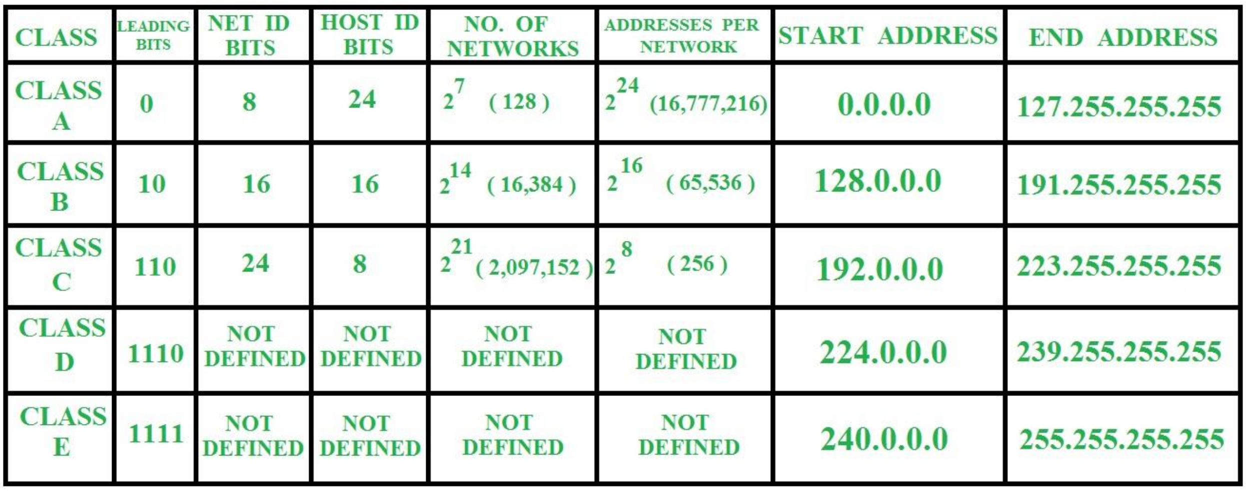
- Within any network, the host ID must be unique to that network.
- Host ID in which all bits are set to 0 cannot be assigned because this host ID is used to represent the network ID of the IP address.
- Host ID in which all bits are set to 1 cannot be assigned because this host ID is reserved as a broadcast address to send packets to all the hosts present on that particular network.

Rules for assigning Network ID:

Hosts that are located on the same physical network are identified by the network ID, as all host on the same physical network is assigned the same network ID. The network ID is assigned based on the following rules:

- The network ID cannot start with 127 because 127 belongs to class A address and is reserved for internal loop-back functions.
- All bits of network ID set to 1 are reserved for use as an IP broadcast address and therefore, cannot be used.
- All bits of network ID set to 0 are used to denote a specific host on the local network and are not routed and therefore, aren't used.

Summary of Classful addressing :



CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO. OF NETWORKS	ADDRESSES PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^{7} (128)	2^{24} (16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14} (16,384)	2^{16} (65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21} (2,097,152)	2^{8} (256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	224.0.0.0	239.255.255.255
CLASS E	1111	NOT DEFINED	NOT DEFINED	NOT DEFINED	NOT DEFINED	240.0.0.0	255.255.255.255

Differences between IPv4 and IPv6

IPv4 and IPv6 are internet protocol version 4 and internet protocol version 6, IP version 6 is the new version of Internet Protocol, which is way better than IP version 4 in terms of complexity and efficiency.

Difference Between IPv4 and IPv6:

IPV4	**IPV6**
IPv4 has 32-bit address length	IPv6 has 128-bit address length

IPV4	**IPV6**
It Supports Manual and DHCP address configuration	It supports Auto and renumbering address configuration
In IPv4 end to end connection integrity is Unachievable	In IPv6 end to end connection integrity is Achievable
It can generate 4.29×109 address space	Address space of IPv6 is quite large it can produce 3.4×1038 address space
Security feature is dependent on application	IPSEC is inbuilt security feature in the IPv6 protocol
Address representation of IPv4 in decimal	Address Representation of IPv6 is in hexadecimal
Fragmentation performed by Sender and forwarding routers	In IPv6 fragmentation performed only by sender
In IPv4 Packet flow identification is not available	In IPv6 packetflow identification are Available and uses flow label field in the header
In IPv4 checksumfield is available	In IPv6 checksumfield is not available
It has broadcast Message Transmission Scheme	In IPv6 multicast and any cast message transmission scheme is available
In IPv4 Encryption and Authentication facility not provided	In IPv6 Encryption and Authentication are provided
IPv4 has header of 20-60 bytes.	IPv6 has header of 40 bytes fixed

Routing Information Protocol (RIP)

Routing Information Protocol (RIP) is a dynamic routing protocol which uses hop count as a routing metric to find the best path between the source and the destination network. It is a distance vector routing protocol which has AD value 120 and works on the application layer of OSI model. RIP uses port number 520.

HopCount:

Hop count is the number of routers occurring in between the source and destination network. The path with the lowest hop count is considered as the best route to reach a network and therefore placed in the routing table. RIP prevents routing loops by limiting the number of hopes allowed in a path from source and destination. The maximum hop count allowed for RIP is 15 and hop count of 16 is considered as network unreachable.

Features of RIP :

1. Updates of the network are exchanged periodically.
2. Updates (routing information) are always broadcast.
3. Full routing tables are sent in updates.
4. Routers always trust on routing information received from neighbor routers. This is also known as Routing on rumours.

RIP versions :

There are three vesions of routing information protocol – RIP Version1, RIP Version2 and RIPng.

RIP V1	**RIP V2**	**RIPNG**
Sends update as broadcast	Sends update as multicast	Sends update as multicast
Broadcast at 255.255.255.255	Multicast at 224.0.0.9	Multicast at FF02::9 (RIPng can only run on IPv6 networks)

Doesn’t support authentication of update messages	Supports authentication of RIPv2 update messages	–
Classful routing protocol	Classless protocol, supports classful	Classless updates are sent

RIP v1 is known as *Classful* Routing Protocol because it doesn’t send information of subnet mask in its routing update.
RIP v2 is known as *Classless* Routing Protocol because it sends information of subnet mask in its routing update.

>> Use debug command to get the details :

```
# debug ip rip
```

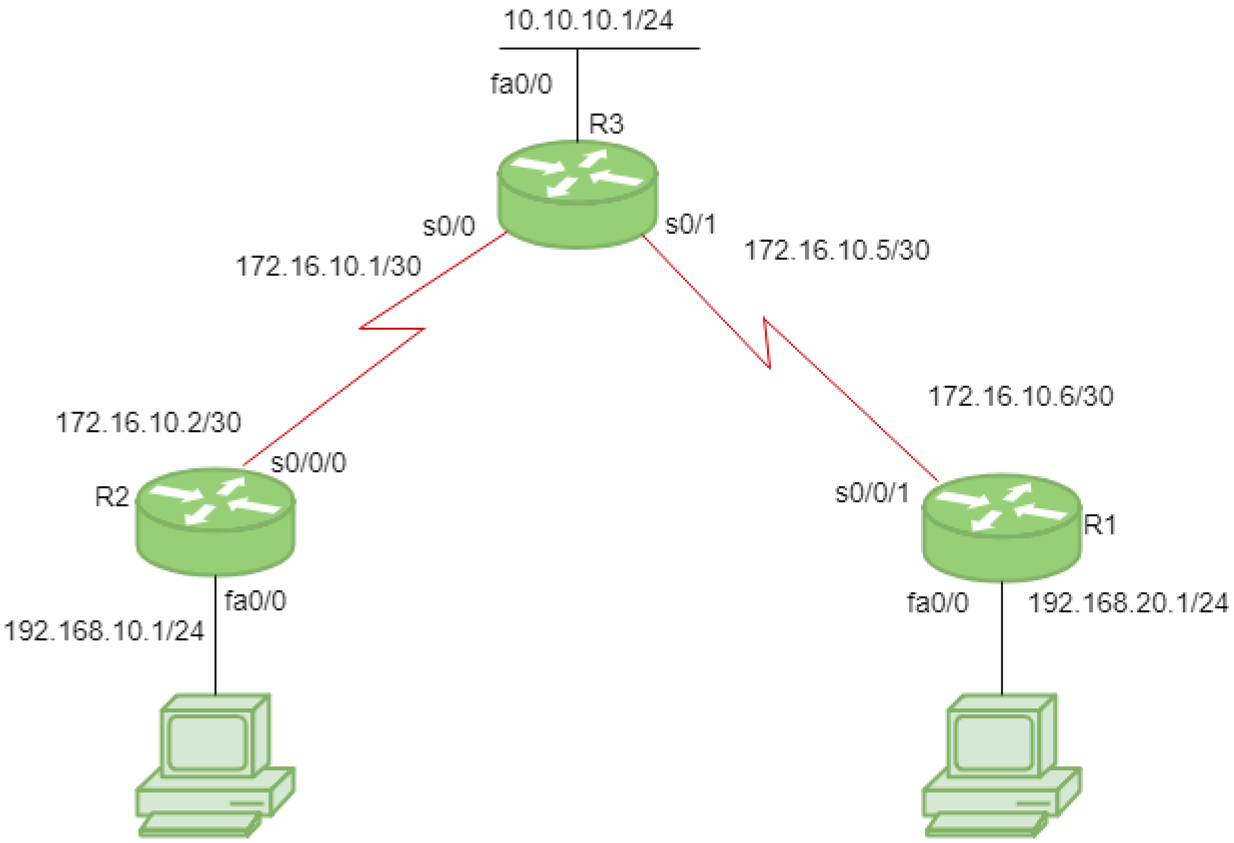
>> Use this command to show all routes configured in router, say for router R1 :

```
R1# show ip route
```

>> Use this command to show all protocols configured in router, say for router R1 :

```
R1# show ip protocols
```

Configuration :



Consider the above given topology which has 3-routers R1, R2, R3. R1 has IP address 172.16.10.6/30 on s0/0/1, 192.168.20.1/24 on fa0/0. R2 has IP address 172.16.10.2/30 on s0/0/0, 192.168.10.1/24 on fa0/0. R3 has IP address 172.16.10.5/30 on s0/1, 172.16.10.1/30 on s0/0, 10.10.10.1/24 on fa0/0.

Configure RIP for R1 :

```
R1(config)# router rip
R1(config-router)# network 192.168.20.0
R1(config-router)# network 172.16.10.4
R1(config-router)# version 2
R1(config-router)# no auto-summary
```

Note : no auto-summary command disables the auto-summarisation. If we don’t select no auto-summary, then subnet mask will be considered as classful in Version 1.

Configureg RIP for R2 :

```
R2(config)# router rip
R2(config-router)# network 192.168.10.0
```

```
R2(config-router)# network 172.16.10.0
R2(config-router)# version 2
R2(config-router)# no auto-summary
```

Similarly, Configure RIP for R3 :

```
R3(config)# router rip
R3(config-router)# network 10.10.10.0
R3(config-router)# network 172.16.10.4
R3(config-router)# network 172.16.10.0
R3(config-router)# version 2
R3(config-router)# no auto-summary
```

RIP timers:

- **Update timer:** The default timing for routing information being exchanged by the routers operating RIP is 30 seconds. Using Update timer, the routers exchange their routing table periodically.
- **Invalid timer:** If no update comes until 180 seconds, then the destination router consider it as invalid. In this scenario, the destination router mark hop count as 16 for that router.
- **Hold down timer :** This is the time for which the router waits for neighbour router to respond. If the router isn’t able to respond within a given time then it is declared dead. It is 180 seconds by default.
- **Flush time :** It is the time after which the entry of the route will be flushed if it doesn’t respond within the flush time. It is 60 seconds by default. This timer starts after the route has been declared invalid and after 60 seconds i.e time will be 180 + 60 = 240 seconds.

Open Shortest Path First (OSPF) protocol States

Prerequisite – OSPF fundamentals

Open Shortest Path First (OSPF) is a link-state routing protocol which is used to find the best path between the source and the destination router using its own Shortest Path First). OSPF is developed by Internet Engineering Task Force (IETF) as one of the Interior Gateway Protocol (IGP), i.e, the protocol which aims at moving the packet within a large autonomous system or routing domain. It is a network layer protocol which works on the protocol number

89 and uses AD value 110. OSPF uses multicast address 224.0.0.5 for normal communication and 224.0.0.6 for update to designated router(DR)/Backup Designated Router (BDR).

OSPF terms –

1. **Router I'd –** It is the highest active IP address present on the router. First, highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.
2. **Router priority –** It is a 8 bit value assigned to a router operating OSPF, used to elect DR and BDR in a broadcast network.
3. **Designated Router (DR) –** It is elected to minimize the number of adjacency formed. DR distributes the LSAs to all the other routers. DR is elected in a broadcast network to which all the other routers shares their DBD. In a broadcast network, router requests for an update to DR and DR will respond to that request with an update.
4. **Backup Designated Router (BDR) –** BDR is backup to DR in a broadcast network. When DR goes down, BDR becomes DR and performs its functions.

DR and BDR election – DR and BDR election takes place in broadcast network or multi access network. Here is the criteria for the election:

1. Router having the highest router priority will be declared as DR.
2. If there is a tie in router priority then highest router I'd will be considered. First, highest loopback address is considered. If no loopback is configured then the highest active IP address on the interface of the router is considered.

OSPF states – The device operating OSPF goes through certain states. These states are:

1. **Down –** In this state, no hello packet have been received on the interface.
   Note – The Down state doesn't mean that the interface is physically down. Her, it means that OSPF adjacency process has not started yet.
2. **INIT –** In this state, hello packet have been received from the other router.
3. **2WAY –** In the 2WAY state, both the routers have received the hello packets from other routers. Bidirectional connectivity has been established.
   Note – In between the 2WAY state and Exstart state, the DR and BDR election takes place.
4. **Exstart –** In this state, NULL DBD are exchanged.In this state, master and slave election take place. The router having the higher router I'd becomes the master while other becomes the slave. This election decides Which router will send it's DBD first (routers who have formed neighbourship will take part in this election).

5. **Exchange –** In this state, the actual DBDs are exchanged.
6. **Loading –** In this sate, LSR, LSU and LSA (Link State Acknowledgement) are exchanged.

   Important – When a router receives DBD from other router, it compares it's own DBD with the other router DBD. If the received DBD is more updated than its own DBD then the router will send LSR to the other router stating what links are needed. The other router replies with the LSU containing the updates that are needed. In return to this, the router replies with the Link State Acknowledgement.
7. **Full –** In this state, synchronization of all the information takes place. OSPF routing can begin only after the Full state.

Distance Vector Routing (DVR) Protocol

A **distance-vector routing (DVR)** protocol requires that a router inform its neighbors of topology changes periodically. Historically known as the old ARPANET routing algorithm (or known as Bellman-Ford algorithm).

Bellman Ford Basics – Each router maintains a Distance Vector table containing the distance between itself and ALL possible destination nodes. Distances,based on a chosen metric, are computed using information from the neighbors' distance vectors.

Information kept by DV router -

- Each router has an ID
- Associated with each link connected to a router,
- there is a link cost (static or dynamic).
- Intermediate hops

Distance Vector Table Initialization -

- Distance to itself = 0
- Distance to ALL other routers = infinity number.

Distance Vector Algorithm –

1. A router transmits its distance vector to each of its neighbors in a routing packet.
2. Each router receives and saves the most recently received distance vector from each of its neighbors.
3. A router recalculates its distance vector when:
    - It receives a distance vector from a neighbor containing different information than before.
    - It discovers that a link to a neighbor has gone down.

The DV calculation is based on minimizing the cost to each destination

Dx(y) = Estimate of least cost from x to y

C(x,v) = Node x knows cost to each neighbor v

Dx = [Dx(y): y ∈ N] = Node x maintains distance vector

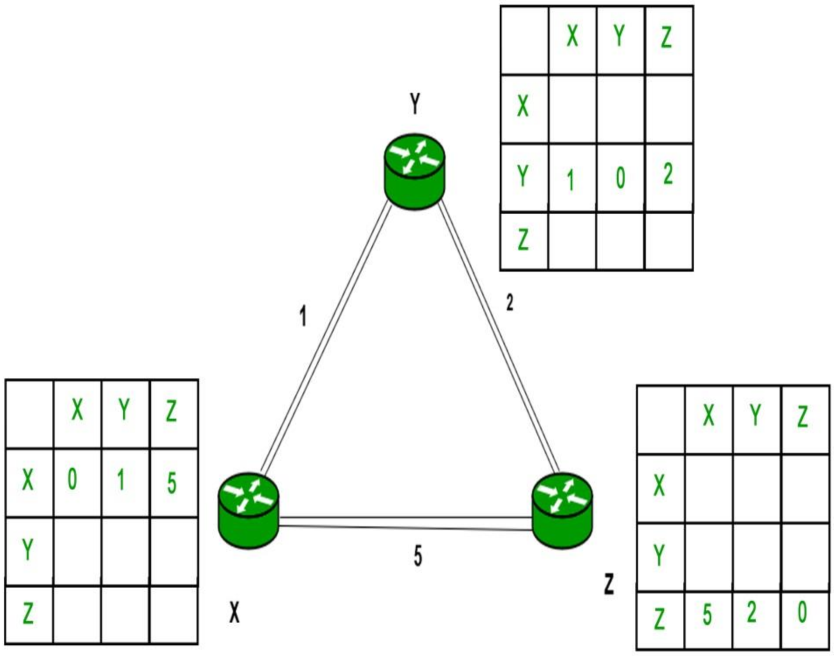
Node x also maintains its neighbors' distance vectors

– For each neighbor v, x maintains Dv = [Dv(y): y ∈ N]

Note –

- From time-to-time, each node sends its own distance vector estimate to neighbors.
- When a node x receives new DV estimate from any neighbor v, it saves v's distance vector and it updates its own DV using B-F equation:
- Dx(y) = min { C(x,v) + Dv(y), Dx(y) } for each node y ∈ N

Example – Consider 3-routers X, Y and Z as shown in figure. Each router have their routing table. Every routing table will contain distance to the destination nodes.



	X	Y	Z
X			
Y	1	0	2
Z			

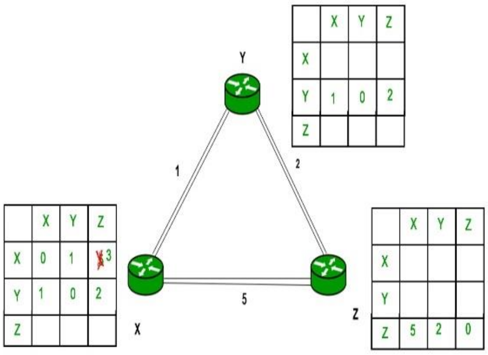
	X	Y	Z
X	0	1	5
Y			
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

Consider router X , X will share it routing table to neighbors and neighbors will share it routing table to it to X and distance from node X to destination will be calculated using bellmen- ford equation.

Dx(y) = min { C(x,v) + Dv(y)} for each node y ∈ N

As we can see that distance will be less going from X to Z when Y is intermediate node(hop) so it will be update in routing table X.

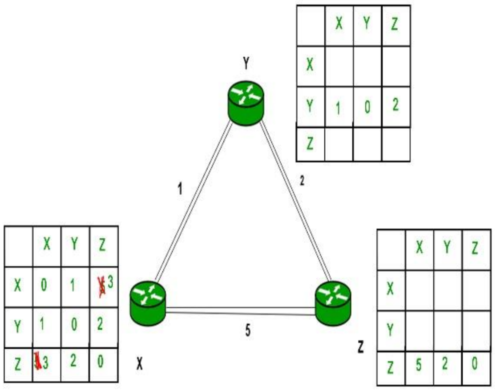


	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	~~5~~ 3
Y	1	0	2
Z			

	X	Y	Z
X			
Y			
Z	5	2	0

Similarly for Z also

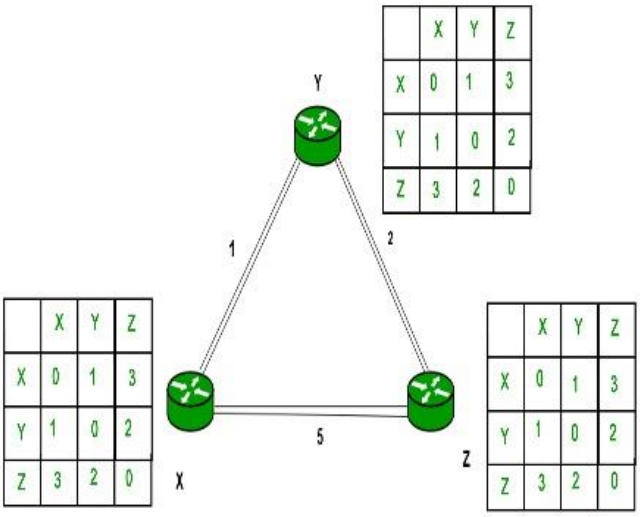


	X	Y	Z
X			
Y	1	0	2
Z			

	X	Y	Z
X	0	1	~~5~~3
Y	1	0	2
Z	~~5~~3	2	0

	X	Y	Z
X			
Y			
Z	5	2	0

Finally the routing table for all –



	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

	X	Y	Z
X	0	1	3
Y	1	0	2
Z	3	2	0

Advantages of Distance Vector routing –

- It is simpler to configure and maintain than link state routing.

Disadvantages of Distance Vector routing –

- It is slower to converge than link state.
- It is at risk from the count-to-infinity problem.
- It creates more traffic than link state since a hop count change must be propagated to all routers and processed on each router. Hop count updates take place on a periodic basis, even if there are no changes in the network topology, so bandwidth-wasting broadcasts still occur.

- For larger networks, distance vector routing results in larger routing tables than link state since each router must know about all other routers. This can also lead to congestion on WAN links

Border Gateway Protocol (BGP)

Border Gateway Protocol (BGP) is used to Exchange routing information for the internet and is the protocol used between ISP which are different ASes.

The protocol can connect together any internetwork of autonomous system using an arbitrary topology. The only requirement is that each AS have at least one router that is able to run BGP and that is router connect to at least one other AS's BGP router. BGP's main function is to exchange network reach-ability information with other BGP systems. Border Gateway Protocol constructs an autonomous systems' graph based on the information exchanged between BGP routers.

Characteristics of Border Gateway Protocol (BGP):

- **Inter-Autonomous System Configuration:** The main role of BGP is to provide communication between two autonomous systems.
- BGP supports Next-Hop Paradigm.
- Coordination among multiple BGP speakers within the AS (Autonomous System).
- **Path Information:** BGP advertisement also include path information, along with the reachable destination and next destination pair.
- **Policy Support:** BGP can implement policies that can be configured by the administrator. For ex:- a router running BGP can be configured to distinguish between the routes that are known within the AS and that which are known from outside the AS.
- Runs Over TCP.
- BGP conserve network Bandwidth.
- BGP supports CIDR.
- BGP also supports Security.

Functionality of Border Gateway Protocol (BGP):

BGP peers performs 3 functions, which are given below.

1. The first function consist of initial peer acquisition and authentication. both the peers established a TCP connection and perform message exchange that guarantees both sides have agreed to communicate.

2. The second function mainly focus on sending of negative or positive reach-ability information.
3. The third function verifies that the peers and the network connection between them are functioning correctly.

BGP Route Information Management Functions:

- Route Storage:

  Each BGP stores information about how to reach other networks.
- Route Update:

  In this task, Special techniques are used to determine when and how to use the information received from peers to properly update the routes.
- Route Selection:

  Each BGP uses the information in its route databases to select good routes to each network on the internet network.
- Route advertisement:

  Each BGP speaker regularly tells its peer what is knows about various networks and methods to reach them.

Exterior Gateway Protocol (EGP)

Exterior gateway protocols are **routing protocols** used on the Internet for exchanging **routing** information between Autonomous Systems, such as Border **Gateway Protocol** (BGP), Path Vector **Routing Protocol**. **Exterior gateway protocols** should not be confused with **Exterior Gateway Protocol** (EGP), an obsolete **routing protocol**.

EGP, or Exterior Gateway Protocol, is a type of routing protocol used to distribute routing information between different autonomous systems in large internetworks based on the TCP/IP protocol.

What is EGP (Exterior Gateway Protocol)?

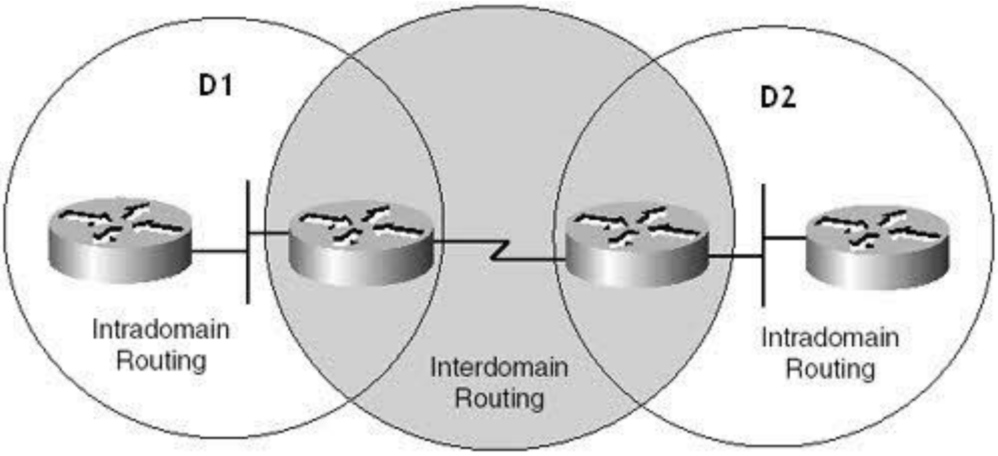
A type of routing protocol used to distribute routing information between different autonomous systems in large internetworks based on the TCP/IP protocol.

The Internet is one example of an Exterior Gateway Protocol (EGP). EGPs specify how networks within an autonomous system are advertised to routers outside the given autonomous system.

EGPs thus facilitate the exchange of inter-autonomous-system routing information between different autonomous systems, independent of whether these autonomous systems employ the same Interior Gateway Protocols (IGPs) within their networks.

The EGP was the original routing protocol developed for communicating routing information between autonomous systems on the Internet. It is no longer used because of its poor support for multipath networking environments, and the Border Gateway Protocol (BGP) has replaced it.

The term “Exterior Gateway Protocol” now refers both to the particular protocol itself and to the class of protocols it describes.



Intradomain and Interdomain Routing

Figure A shows two routing domains, D1 and D2, and an overlapping (shaded) region depicting the interconnection between border routers from each domain. In more current routing terminology, a routing domain also is referred to as an autonomous system. An autonomous system is an independent routing domain under the control of a single administrative authority.

An exterior gateway protocol provides the capability for sharing routing information between the two domains.

Exterior Gateway Protocol development

The Exterior Gateway Protocol was developed by Bolt, Beranek and Newman in the early 1980s. It was first described in RFC 827 and formally specified in RFC 904 (1984). (see external references)

Distance Vector Multicast Routing Protocol

The Distance Vector Multicast Routing Protocol (DVMRP), defined in RFC 1075, is a routing protocol used to share information between routers to facilitate the transportation of IP multicast packets among networks. It formed the basis of the Internet's historic multicast backbone, Mbone.

Operation:

The protocol is based on the Routing Information Protocol (RIP). The router generates a routing table with the multicast group of which it has knowledge with corresponding distances (i.e. number of devices/routers between the router and the destination). When a multicast packet is received by a router, it is forwarded by the router's interfaces specified in the routing table.

DVMRP operates via a reverse path flooding technique, sending a copy of a received packet (specifically IGMP messages for exchanging routing information with other routers) out through each interface except the one at which the packet arrived. If a router (i.e. a LAN which it borders) does not wish to be part of a particular multicast group, it sends a "prune message" along the source path of the multicast.

MULTICAST EXTENSIONS TO OSPF (MOSPF)

Version 2 of the Open Shortest Path First (OSPF) routing protocol is defined in RFC-1583 . It is an Interior Gateway Protocol (IGP) specifically designed to distribute unicast topology information among routers belonging to a single Autonomous System. OSPF is based on link-state algorithms which permit rapid route calculation with a minimum of routing protocol traffic. In addition to efficient oute calculation, OSPF is an open standard that supports hierarchical routing, load balancing, and the import of external routing information.

The Multicast Extensions to OSPF (MOSPF) are defined in RFC-1584 . MOSPF routers maintain a current image of the network topology through the unicast OSPF link-state routing protocol. MOSPF enhances the OSPF protocol by providing the ability to route multicast IP traffic. The multicast extensions to OSPF are built on top of OSPF Version 2 so that a multicast routing capability can be easily introduced into an OSPF Version 2 routing domain. The enhancements that have been added are backwards compatible so that routers running MOSPF will interoperate with non-multicast OSPF routers when forwarding unicast IP data traffic. MOSPF, unlike DVMRP, does not provide support for tunnels.

Intra-Area Routing with MOSPF

Intra-Area Routing describes the basic routing algorithm employed by MOSPF. This elementary algorithm runs inside a single OSPF area and supports multicast forwarding when the source and all destination group members reside in the same OSPF area, or when the entire Autonomous System is a single OSPF area. The following discussion assumes that the reader is familiar with the basic operation of the OSPF routing protocol.

Local Group Database

Similar to DVMRP, MOSPF routers use the Internet Group Management Protocol (IGMP) to monitor multicast group membership on directly attached subnetworks. MOSPF routers are required to implement a "local group database" which maintains a list of directly attached group members and determines the local router's responsibility for delivering multicast datagrams to these group members.

On any given subnetwork, the transmission of IGMP Host Membership Queries is performed solely by the Designated Router (DR). Also, the responsibility of listening to IGMP Host Membership Reports is performed only by the Designated Router (DR) and the Backup

Designated Router (BDR). This means that in a mixed environment containing both MOSPF and OSPF routers, an MOSPF router must be elected the DR for the subnetwork if IGMP Queries are to be generated. This can be achieved by simply assigning all non-MOSPF routers a RouterPriority of 0 to prevent them from becoming the DR or BDR, thus allowing an MOSPF router to become the DR for the subnetwork.

The DR is responsible for communicating group membership information to all other routers in the OSPF area by flooding Group-Membership LSAs. The DR originates a separate Group- Membership LSA for each multicast group having one or more entries in the DR's local group database. Similar to Router-LSAs and Network-LSAs, Group Membership-LSAs are flooded throughout a single area only. This ensures that all remotely-originated multicast datagrams are forwarded to the specified subnetwork for distribution to local group members.

Datagram's Shortest Path Tree

The datagram's shortest path tree describes the path taken by a multicast datagram as it travels through the internetwork from the source subnetwork to each of the individual group members. The shortest path tree for each (source, group) pair is built "on demand" when a router receives the first multicast datagram for a particular (source, group) pair.

When the initial datagram arrives, the source subnetwork is located in the MOSPF link state database. The MOSPF link state database is simply the standard OSPF link state database with the addition of Group-Membership LSAs. Based on the Router-LSAs and Network-LSAs in the MOSPF link state database, a source-rooted shortest-path tree is constructed using Dijkstra's algorithm. After the tree is built, Group-Membership LSAs are used to prune those branches that do not lead to subnetworks containing individual group members. The result of the Dijkstra calculation is a pruned shortest-path tree rooted at the datagram's source.

```
======================================================================

                      S
                      |
                      |
                   A  #
                     / \
                    /   \
                   1     2
                  /       \
               B #         # C
                / \         \
               /   \         \
              3     4         5
             /       \         \
          D #         # E       # F
                     / \         \
                    /   \         \
                   6     7         8
                  /       \         \
               G #         # H       # I

LEGEND

 #   Router

             □Shortest Path Tree for (S, G)
======================================================================
```

To forward a multicast datagram to downstream members of the group, each router must determine its position in the datagram's shortest path delivery tree. Assume that figure above illustrates the shortest path tree for a particular (source, group) pair. Router E's upstream node is Router B and there are two downstream interfaces: one connecting to Subnetwork 6 and another connecting to Subnetwork 7.

Note the following properties of the basic MOSPF routing algorithm:

- For a given multicast datagram, all routers within an OSPF area calculate the same source-rooted shortest path delivery tree. Tie-breakers have been defined to guarantee that if several equal- cost paths exist, all routers agree on a single path through the area. Unlike unicast OSPF, MOSPF does not support the concept of equal-cost multipath routing.

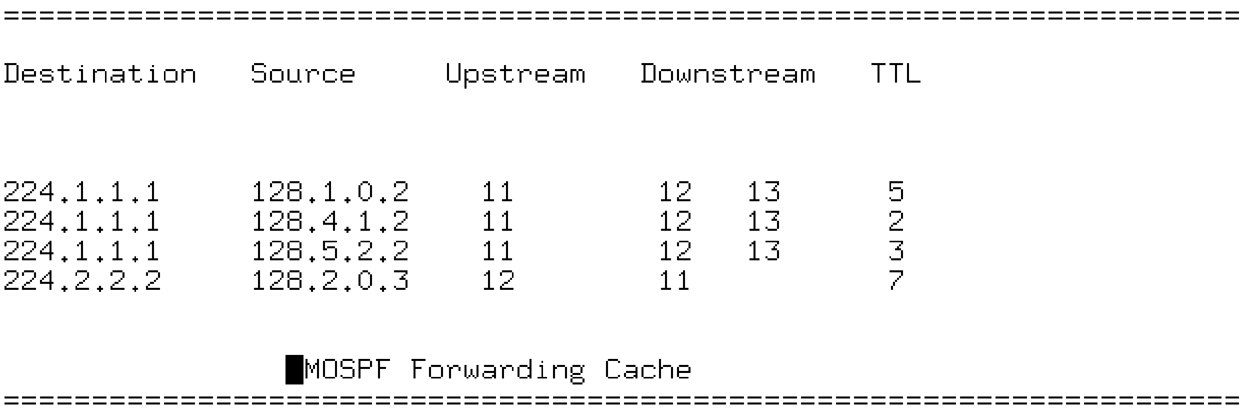
- Synchronized link state databases containing Group-Membership LSAs allow an MOSPF router to perform the Reverse Path Multicasting (RPM) computation "in memory." Unlike

DVMRP, this means that the first datagram of a group transmission does not have to be forwarded to all routers in the area.

- The "on demand" construction of the shortest-path delivery tree has the benefit of spreading calculations over time, resulting in a lesser impact for participating routers.

Forwarding Cache

Each MOSPF router makes its forwarding decision based on the contents of its forwarding cache. The forwarding cache is built from the source-rooted shortest-path tree for each (source, group) pair and the router's local group database. After the router discovers its position in the shortest path tree, a forwarding cache entry is created containing the (source, group) pair, the upstream node, and the downstream interfaces. At this point, the Dijkstra shortest path tree is discarded releasing all resources associated with the creation of the tree. From this point on, the forwarding cache entry is used to forward all subsequent datagrams for the (source, group) pair.



```
======================================================================
Destination   Source     Upstream   Downstream   TTL


224.1.1.1     128.1.0.2    11         12   13      5
224.1.1.1     128.4.1.2    11         12   13      2
224.1.1.1     128.5.2.2    11         12   13      3
224.2.2.2     128.2.0.3    12         11           7

                █MOSPF Forwarding Cache
======================================================================
```

Above figure displays the forwarding cache for a typical MOSPF router. The elements in the display include the following items:

Destination-- The destination group address to which matching datagrams are forwarded.

Source-- The datagram's source subnetwork. Each Destination/Source pair identifies a separate forwarding cache entry.

Upstream-- The interface from which a matching datagram must be received

Downstream-- The interfaces over which a matching datagram should be forwarded to reach Destination group members

TTL-- The minimum number of hops a datagram will travel to reach the multicast group members. This allows the router to discard datagrams that do not have a chance of reaching a destination group member.

The information in the forwarding cache is not aged or periodically refreshed. It is maintained as long as there are system resources available (i.e., memory) or until the next topology change. In general, the contents of the forwarding cache will change when:

- The topology of the OSPF internetwork changes forcing all of the datagram shortest-path trees to be recalculated.

- There is a change in the Group-Membership LSAs indicating that the distribution of individual group members has changed.

Mixing MOSPF and OSPF Routers

MOSPF routers can be combined with non-multicast OSPF routers. This permits the gradual deployment of MOSPF and allows experimentation with multicast routing on a limited scale. When MOSPF and non-multicast OSPF routers are mixed within an Autonomous System, all routers will interoperate in the forwarding of unicast datagrams.

It is important to note that an MOSPF router is required to eliminate all non-multicast OSPF routers when it builds its source-rooted shortest-path delivery tree. An MOSPF router can easily determine the multicast capability of any other router based on the setting of the multicast bit (MC-bit) in the Options field of each router's link state advertisements. The omission of non-multicast routers can create a number of potential problems when forwarding multicast traffic:

- Multicast datagrams may be forwarded along suboptimal routes since the shortest path between two points may require traversal of a non-multicast OSPF router.

- Even though there is unicast connectivity to a destination, there may not be multicast connectivity. For example, the network may partition with respect to multicast connectivity since the only path between two points requires traversal of a non-multicast OSPF router.

- The forwarding of multicast and unicast datagrams between two points may follow entirely different paths through the internetwork. This may make routing problems somewhat more difficult to debug.

- The Designated Router for a multi-access network must be an MOSPF router. If a non-multicast OSPF router is elected the DR, the subnetwork will not be selected to forward multicast datagrams since a non-multicast DR cannot generate Group- Membership LSAs for its subnetwork.

Inter-Area Routing with MOSPF

Inter-area routing involves the case where a datagram's source and some of its destination group members reside in different OSPF areas. It should be noted that the forwarding of multicast datagrams continues to be determined by the contents of the forwarding cache which is still built from the local group database and the datagram shortest-path trees. The major differences are related to the way that group membership information is propagated and the way that the inter-area shortest-path tree is constructed.

Inter-Area Multicast Forwarders

In MOSPF, a subset of an area's Area Border Routers (ABRs) function as "inter-area multicast forwarders." An inter-area multicast forwarder is responsible for the forwarding of group membership information and multicast datagrams between areas. Configuration parameters determine whether or not a particular ABR also functions as an inter-area multicast forwarder.

Inter-area multicast forwarders summarize their attached areas' group membership information to the backbone by originating new Group-Membership LSAs into the backbone area. It is important to note that the summarization of group membership in MOSPF is asymmetric. This means that group membership information from non-backbone areas is flooded into the backbone. However, the backbone does not readvertise either backbone group membership information or group membership information learned from other non-backbone areas into any non-backbone areas.

```
======================================================================

 -------------------------
/      Backbone Area      \
|                          |
|      ^           ^       |
|   ___|___     ___|___    |
\__|       |___|       |__/
   |---*---|   |---*---|
   / Area 1\   / Area 2\
   |       |   |       |
   |       |   |       |
   |-------|   |-------|


LEGEND

   ^
   |    Group Membership LSAs
 _____
|_____| Area Border Routher and
        Inter-Area Multicast Forwarder

*       Wild-Card Multicast
        Receiver Interface

      █Inter-Area Routing Architecture
======================================================================
```

To permit the forwarding of multicast traffic between areas, MOSPF introduces the concept of a "wild-card multicast receiver." A wild-card multicast receiver is a router that receives all multicast traffic generated in an area, regardless of the multicast group membership. In non-backbone areas, all inter- area multicast forwarders operate as wild-card multicast receivers. This guarantees that all multicast traffic originating in a non-backbone area is delivered to its inter-area multicast forwarder, and then if necessary into the backbone area. Since the backbone has group membership knowledge for all areas, the datagram can then be forwarded to group members residing in the backbone and other non-backbone areas. The backbone area does not require wild-card multicast receivers because the routers in the backbone area have complete knowledge of group membership information for the entire OSPF system.

Inter-Area Datagram Shortest-Path Tree

In the case of inter-area multicast routing, it is often impossible to build a complete datagram shortest-path delivery tree. Incomplete trees are created because detailed topological and group membership information for each OSPF area is not distributed to other OSPF areas. To overcome these limitations, topological estimates are made through the use of wild-card receivers and OSPF Summary-Links LSAs.

There are two cases that need to be considered when constructing an inter-area shortest-path delivery tree. The first involves the condition when the source subnetwork is located in the same area as the router performing the calculation. The second situation occurs when the source subnetwork is located in a different area than the router performing the calculation.

If the source of a multicast datagram resides in the same area as the router performing the calculation, the pruning process must be careful to ensure that branches leading to other areas are not removed from the tree. Only those branches having no group members nor wild-card multicast receivers are pruned. Branches containing wild-card multicast receivers must be retained since the local routers do not know if there are group members residing in other areas.

```
======================================================================
 ----------------------------------
|              S                   |
|              |     Area 1        |
|              |                   |
|              #                   |
|             / \                  |
|            /   \                 |
|           /     \                |
|          /       \               |
|       O-#         #-O            |
|        / \         \             |
|       /   \         \            |
|      /     \         \           |
|     /       \         \          |
|  O-#         #         #-O       |
|             / \         \        |
|            /   \         \       |
|           /     \         \      |
|          /       \         \     |
|       O-#         #-O       ---  |
 ----------------------------| ? |-
                              ---
                               To Ba□kbone

LEGEND

S   Source Subnetwork
O   Subnet Containing Group Members
#   Intra-Area MOSPF Router
?   WildCard Multicast Receiver

      Datagram Shortest Path Tree -Source in Same Area
======================================================================
```

If the source of a multicast datagram resides in a different area than the router performing the calculation, the details describing the local topology surrounding the source station are not known. However, this information can be estimated using information provided by Summary Links LSAs for the source subnetwork. In this case, the base of the tree begins with branches directly connecting the source subnetwork to each of the local area's inter-area multicast forwarders. The inter-area multicast forwarders must be included in the tree since any multicast datagrams originating outside the local area will enter the area via an inter-area multicast forwarder.

```
======================================================================
               S
               |
               #
               |
       Summary-Links LSA
               |
              ---
 ------------| ? |-----------------
|             ---     Area 1       |
|              |                   |
|              #                   |
|             / \                  |
|            /   \                 |
|           /     \                |
|          /       \               |
|       O-#         #-O            |
|        / \         \             |
|       /   \         \            |
|      /     \         \           |
|     /       \         \          |
|  O-#         #         #-O       |
|             / \         \        |
|            /   \         \       |
|           /     \         \      |
|          /       \         \     |
|       O-#         #-O       #-O  |
 ----------------------------------


LEGEND

S   Source Subnetwork
O   Subnet Containing Group Members
#   Interarea MOSPF Router
?   Intra-Area Multicast Forwarder

     Fig 5.█Shortest Path Tree -Source in Different Area
======================================================================
```

Since each inter-area multicast forwarder is also an ABR, it must maintain a separate link state database for each attached area. This means that each inter-area multicast forwarder is required to calculate a separate forwarding tree for each of its attached areas. After the individual trees are calculated, they are merged into a single forwarding cache entry for the (source, group) pair and then the individual trees are discarded.

Inter-Autonomous System Multicasting with MOSPF

Inter-Autonomous System Multicasting involves the situation where a datagram's source and at least some of its destination group members reside in different Autonomous Systems. It should be emphasized that in OSPF terminology "inter-AS" communication also refers to connectivity between an OSPF domain and another routing domain which could be within the same Autonomous System.

To facilitate inter-AS multicast routing, selected Autonomous System Boundary Routers (ASBRs) are configured as "inter-AS multicast forwarders." MOSPF makes the assumption that each inter-AS multicast forwarder executes an inter-AS multicast routing protocol (such as DVMRP) which forwards multicast datagrams in a reverse path forwarding (RPF) manner. Each inter- AS multicast forwarder functions as a wild-card multicast receiver in each of its attached areas. This guarantees that each inter-AS multicast forwarder remains on all pruned shortest- path trees and receives all multicast datagrams, regardless of the multicast group membership.

Three cases need to be considered when describing the construction of an inter-AS shortest-path delivery tree. The first occurs when the source subnetwork is located in the same area as the router performing the calculation. For the second case, the source subnetwork resides in a different area than the router performing the calculation. The final case occurs when the source subnetwork is located in a different AS (or in another routing domain within the same AS) than the router performing the calculation.

The first two cases are similar to the inter-area examples described in the previous section. The only enhancement is that inter-AS multicast forwarders must also be included on the pruned shortest path delivery tree. Branches containing inter-AS multicast forwarders must be retained since the local routers do not know if there are group members residing in other Autonomous Systems. When a multicast datagram arrives at an inter-AS multicast forwarder, it is the responsibility of the ASBR to determine whether the datagram should be forwarded outside of the local Autonomous System. Figure 6 illustrates a sample inter-AS shortest path delivery tree when the source subnetwork resides in the same area as the router performing the calculation.

```
======================================================================

 -----------------------------------
|              S     Area 1         |
|              |                    |
|              #                    |
|             / \                   |
|            /   \                  |
|           /     \                 |
|          /       \                |
|       O-#         #-O             |
|        / \         \              |
|       /   \         \             |
|      /     \         \            |
|     /       \         \           |
|  O-#         #         #-O        |
|             / \         \         |
|            /   \         \        |
|           /     \         \       |
|          /       \         \      |
|         /         #-O       \     |
|       ---                    ---  |
 ------| & |------------------| ? |-
        ---                    ---
 To other Autonomous     To Backbone
     Systems

LEGEND

S   Source Subnetwork
O   Subnet Containing Group Members
#   Intra-Area MOSPF Router
?   Inter-Area Multicast Forwarder
&   Inter-AS Multicast Forwarder

Figure 6 . Inter-AS Datagram Shortest Path Tree -Source in Same Area
======================================================================
```

If the source of a multicast datagram resides in a different Autonomous System than the router performing the calculation, the details describing the local topology surrounding the source station are not known. However, this information can be estimated using the multicast-capable AS External links describing the source subnetwork. In this case, the base of the tree begins with branches directly connecting the source subnetwork to each of the local area's inter-AS multicast forwarders.

Figure 7 shows a sample inter-AS shortest-path delivery tree when the inter-AS multicast forwarder resides in the same area as the router performing the calculation. If the inter-AS multicast forwarder is located in a different area than the router performing the calculation, the topology surrounding the source is approximated by combining the Summary-ASBR Link with the multicast capable AS External Link.

```
======================================================================
               S
               |
               :
               |
       AS External links
               |
               |
              ---
 ------------| & |-----------------
|             ---                  |
|             / \                  |
|            /   \     Area 1      |
|           /     \                |
|          /       \               |
|       O-#         #-O            |
|        / \         \             |
|       /   \         \            |
|      /     \         \           |
|     /       \         \          |
|  O-#         #         #-O       |
|             / \         \        |
|            /   \         \       |
|           /     \         \      |
|          /       \         \     |
|         /         #-O       #-O  |
|       ---                        |
 ------| ? |-----------------------
        ---
 To Backbone

LEGEND

S    Source Subnetwork
O    Subnet Containing Group Members
#    Intra-Area MOSPF Router
?    Inter-Area Multicast Forwarder
&    Inter-AS Multicast Forwarder

Figure 7: Inter-AS Datagram Shortest Path Tree -Source in Different AS
======================================================================
```

Version 2 of the Open Shortest Path First (OSPF) routing protocol is defined in RFC-1583. It is an Interior Gateway Protocol (IGP) specifically designed to distribute unicast topology information among routers belonging to a single Autonomous System. OSPF is based on link-state algorithms which permit rapid route calculation with a minimum of routing protocol traffic. In addition to efficient oute calculation, OSPF is an open standard that supports hierarchical routing, load balancing, and the import of external routing information.

The Multicast Extensions to OSPF (MOSPF) are defined in RFC-1584. MOSPF routers maintain a current image of the network topology through the unicast OSPF link-state routing protocol. MOSPF enhances the OSPF protocol by providing the ability to route multicast IP traffic. The multicast extensions to OSPF are built on top of OSPF Version 2 so that a multicast routing capability can be easily introduced into an OSPF Version 2 routing domain. The enhancements that have been added are backwards compatible so that routers running MOSPF will interoperate with non-multicast OSPF routers when forwarding unicast IP data traffic. MOSPF, unlike DVMRP, does not provide support for tunnels.

UNIT III

MBone (Multicast Internet)

The MBone, now sometimes called the Multicast Internet, is an arranged use of a portion of the Internet for Internet Protocol (IP) multicasting (sending files - usually audio and video streams - to multiple users at the same time somewhat as radio and TV programs are broadcast over airwaves). Although most Internet traffic is unicast (one user requesting files from one source at another Internet address), the Internet's IP protocol also supports multicasting, the transmission of data packets intended for multiple addresses. Since most IP servers on the Internet do not currently support the multicasting part of the protocol, the MBone was set up to form a network within the Internet that could transmit multicasts. The MBone was set up in 1994 as an outgrowth of earlier audio multicasts by the Internet Engineering Task Force (IETF) and has multicast a number of programs, including some well-publicized rock concerts.

The MBone consists of known servers (mostly on UNIX workstations) that are equipped to handle the multicast protocol. Tunneling is used to forward multicast packets through routers on the network that don't handle multicasting. An MBone router that is sending a packet to another MBone router through a non-MBone part of the network encapsulates the multicast packet as a unicast packet. The non-MBone routers simply see an ordinary packet. The destination MBone router unencapsulates the unicast packet and forwards it appropriately. The MBone consists of a backbone with a mesh topology which is used by servers that redistribute the multicast in their region in a star topology. The MBone network is intended to be global and includes nodes in Europe.

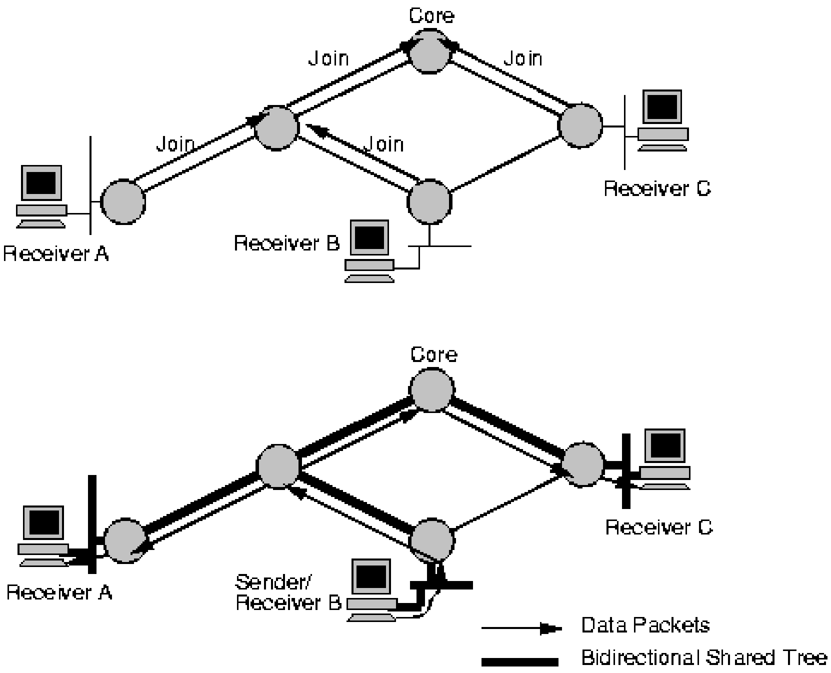
The channel bandwidth for MBone multicasts is 500 kilobits per second and actual traffic is from 100-300 kilobits depending on content. MBone multicasts usually consist of streaming audio and video.

Core-Based Trees :

CBT was the earliest center-based tree protocol, and is the simplest.

When a receiver joins a multicast group, its local CBT router looks up the multicast address and obtains the address of the Core router for the group. It then sends a Join message for the group towards the Core. At each router on the way to the core, forwarding state is instantiated for the group, and an acknowledgment is sent back to the previous router. In this way, a multicast tree is built, as shown in figure C.

Figure C: Formation of a CBT bidirectional shared tree



If a sender (that is a group member) sends data to the group, the packets reach its local router, which forwards them to any of its neighbours that are on the multicast tree. Each router that receives a packet forwards it out of all it its interfaces that are on the tree except the one the packet came from. The style of tree CBT builds is called a "bidirectional shared tree", because the routing state is "bidirectional" - packets can flow both up the tree towards the core and down the tree away from the core depending on the location of the source, and "shared" by all sources to the group. This is in contrast to "unidirectional shared trees" built be SM-PIM as we shall see later.

IP Multicast does not require senders to a group to be members of the group, so it is possible that a sender's local router is not on the tree. In this case, the packet is forwarded to the next hop towards the Core. Eventually the packet will either reach a router that is on the tree, or it will reach the core, and it is then distributed along the multicast tree.

CBT also allows multiple Core routers to be specified which adds a little redundancy in case the core becomes unreachable. CBT never properly solved the problem of how to map a group address to the address of a core. In addition, good core placement is a hard problem. Without good core placement, CBT trees can be quite inefficient, and so CBT is unlikely to be used as a global multicast routing protocol.

However, within a limited domain, CBT is very efficient in terms of the amount of state that routers need to keep. Only routers on the distribution tree for a group keep forwarding state for that group, and no router needs to keep information about any source, and thus CBT scales much better than flood-and-prune protocols, especially for sparse groups where only a small proportion of subnetworks have members.

UNIT - 4

Macro-mobility protocols

Mobile IP is the most widely used protocol for macro-mobility management. In addition to Mobile IP, three macro-mobility architectures are discussed in the section. These protocols are: Session Initiation Protocol (SIP)-based mobility management, multi-tier hybrid SIP and Mobile IP protocol, and network inter-working agent-based mobility protocol.

Mobile IP: Mobile IP (Perkins, 2008) is the most well-known macro mobility scheme that solves the problem of node mobility by redirecting the packets for the MN to its current location. It introduces seven elements:

(i) Mobile node (MN) – a device or a router that can change its point of attachment to the Internet,

(ii) Correspondent node (CN) – the partner with which MN communicates,

(iii) Home network (HN) – the subnet to which MN belongs

(iv) Foreign network (FN) – the current subnet in which the MN is visiting,

(v) Home agent (HA) – provides services for the MN and is located in the HN,

(vi) Foreign agent (FA) – provides services to the MN while it visits in the FN,

(vii) Care-of-address (CoA) – defines the current location of the MN; all packets sent to the MN are delivered to the CoA. Mobile IP protocol has three steps: (i) agent discovery, (ii) registration, and (iii) routing and tunneling.

Agent discovery: An MN is able to detect whether it has moved into a new subnet by two methods – agent advertisement and agent solicitation. In the agent advertisement method, FAs and HAs advertise their presence periodically using agent advertisement messages. These advertisement messages can be seen as beacon broadcasts into the subnets. An MN in a subnet can receive agent advertisements. If no agent advertisement messages are found or the inter-arrival time is too high, the MN may send agent solicitations. After the step of agent advertisement or solicitation, the MN receives a CoA. The CoA may be either an FA or a co-located CoA (Perkins, 2008). A co-located CoA is found by using Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol (PPP).

Registration: After the MN receives its CoA, it registers it with the HA. The main objective of the registration is to inform the HA about the current location of MN. The registration may be done in two ways depending on the location of the CoA. If the CoA is the FA, the MN sends its registration request to the FA which in turn forwards it to the HA. If the CoA is co-located, the MN may send the request directly to the HA.

Routing and tunneling: When a CN sends an IP packet to the MN, the packet is intercepted by the HA. The HA encapsulates the packet and tunnels it to the MN’s CoA. With FA CoA, the encapsulated packet reaches the FA serving the MN. The FA decapsulates the packet and forwards it to the MN. With co-located CoA, the encapsulated packets reach the MN, which decapsulates them. In Figure 1, the tunneling (step b) ends at the MN instead of at the FA.

Paging Extension for Mobile IP: For saving battery power at MNs, IP paging mechanism has been proposed Paging typically includes transmitting a request for an MN to a set of locations, in one of which the MN is expected to be present. The set of locations is called a paging area and it consists of a set of neighboring base stations. A network that supports paging allows the MNs to operate in two different states – an active state and a standby state. In an active state, the MN is tracked at the finest granularity such as its current base station (resulting in no need for paging). In the standby state, the MN is tracked at a much coarser granularity such as a paging area. The MN updates the network less frequently in stand by mode (every paging area change) than in active state (every base station). The cost of paging, however, is the complexity of the algorithms and the protocols required to implement the procedures, and the delay incurred for locating an MN.

Drawbacks of Mobile IP: The Mobile IP has the following shortcomings:

1. The packets sent from a CN to an MN are received by the HA before being tunneled to the MN. However, packets from the MN are sent directly to the CN. This inefficient mechanism of non-optimized Mobile IP is called triangular routing. It results in longer routes and more delay in packet delivery.

2. When an MN moves across two different subnets, the new CoA cannot inform the old CoA about MN's current location. Packets tunneled to the old CoA are lost.

3. Mobile IP is not an efficient mechanism in a highly mobile scenario as it requires an MN to send a location update to the HA whenever it changes its subnet. The signaling cost for location updates and the associated delay may be very high if the distance between the visited network and the home network is large.

Optimization in Mobile IP: In (Perkins & Johnson, 2001), an optimization technique has been proposed to solve the problem of triangular routing. The idea is to inform the CN about the current location of the MN so as to bypass the HA. The CN can learn the location of the CoAs of the MN by caching them in a binding cache in the CN. When a CN sends packets to an MN, it first checks if it has a binding cache entry for the MN. If there is an entry, the CN tunnels the packets directly to the CoA. If no binding cache entry is available, the CN sends the packets to the HA, which in turn tunnels them to the CoA. In optimized Mobile IP, the packets tunneled by the HA to the old CoA are not lost in transit. When an MN registers with a new FA, it requests the new FA to notify the previous FA about its movement. As the old FA now knows the location of the current FA, it can forward the packets to the new FA.

SIP-Based Mobility Management: In (Salsano et al., 2008), a Session Initiation Protocol (SIP)-based solution, called mobility management using SIP extension (MMUSE), has been proposed that supports vertical handoffs in next-generation wireless networks. SIP has been chosen by the Third Generation Partnership Project (3GPP) as the signaling protocol to set up and control real-time multimedia sessions. In MMUSE, a mobile host (MH) is assumed to be equipped with multiple network interfaces; each of them is assigned a separate IP address when connected to different access networks (ANs). The MH uses the SIP protocol to set up multimedia sessions. The architecture of the scheme is depicted in Figure 2. The session border controller (SBC) is a device that is typically located at the border of an IP network, and manages all the sessions for that network. A new entity, called the mobility management server (MMS) resides within the SBC. The MMS cooperates with another entity – mobility management client (MMC) that resides in each MH. Both the SIP user agents (UAs) on the MH and on the corresponding host (CH) remain unaware of all the handoff procedures, which are handled by the MMC and the MMS. On the MH, the UA sees only the MMC as its outbound proxy and forwards the normal SIP signaling and media flows to it. MMC relays the packets to the MMS/SBC. From there on, the packets follow the path determined by the usual SIP routing procedure. Every time the MH moves across two ANs, a location update SIP message is sent to the MMS. This is done over the new network so that the procedure can be completed even if the old network is suddenly not available. If the MMS receives a call addressed to one of its served MHs, it forwards the call to the correct interface. When the MH changes its AN while it is engaged in a call, the procedure is almost identical. However, in this case, the MMC sends to the MMS an SIP message that contains the additional information required to identify the call to be shifted to new interface. To minimize the handoff duration, the real-time transport protocol (RTP) flow coming from the MH during the handoff is duplicated using the MMC. When the MMC starts the handoff procedures, it sends the handover request to the MMS and at the same time, it starts duplicating the RTP packets over both interfaces. As soon as the MMS receives the handover message, the packets coming from the new interface are already available. The MMS performs the switching and sends the reply back to the MMC. When the MMC receives the reply message, it stops duplicating the packets.

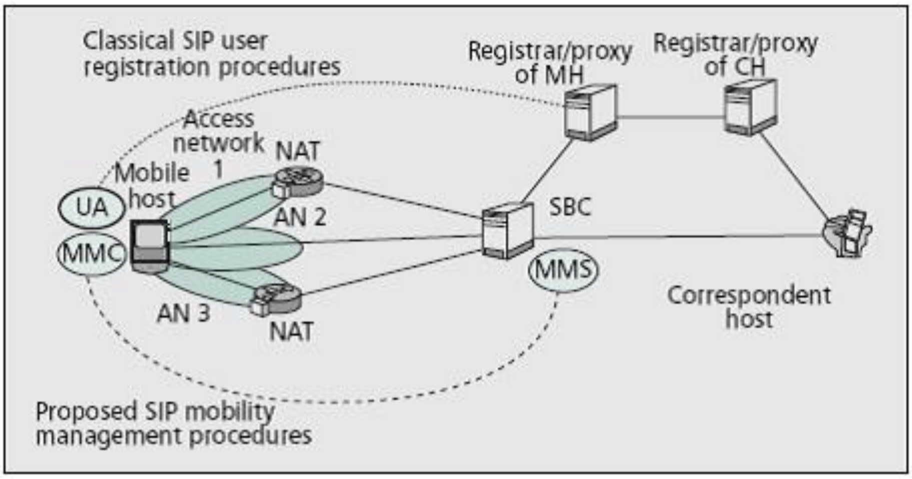


Figure 1 : Architecture of MMUSE

Multi-Layer Mobility Management using Hybrid SIP and Mobile IP: In mobility management architectures based on SIP and Mobile IP are presented. The two approaches provide mobility in two different layers: application and network layers respectively. The scheme is therefore called multi-layer mobility management scheme. The SIP-based protocol uses SIP in combination with IP encapsulation mechanisms on CHs to support mobility for all types of traffic from/to the MH. The second approach performs separation of traffic and employs SIP in combination with network address translation (NAT) mechanisms to support mobility for real-time traffic over UDP. The mobility for non-real-time traffic (mainly TCP-based applications) is supported by Mobile IP. In the SIP-based approach, if the MH moves during a session, the SIP UA sends a SIP re-INVITE request message to each of its CHs. If a CH runs a TCP session, IP encapsulation is used to forward packets to MH. However, if a CH runs a UDP session, the packets are sent directly to the MH's new address. The MH completes the handoff by sending a SIP REGSITER message to the SIP server. For the hybrid SIP/Mobile IP scheme, the inter-domain mobility is based on the synergy of SIP with Mobile IP. Traffic from/to an MH is separated on the domain edge routers. SIP signaling is used to support inter-domain mobility for real-time (RTP over UDP) traffic, while Mobile IP supports non-real-time traffic.

Network Inter-Working Agent-Based Mobility Management: In (Akyildiz et al., 2005) an architecture has been proposed for next-generation all-IP wireless systems. Different wireless networks are integrated through an entity called the network inter-working agent (NIA). In Figure 3, an NIA integrates one WLAN, one cellular network, and one satellite network. NIA also handles authentication, billing, and mobility management issues during inter-system (inter-domain) roaming. Two types of movement of an MH are considered: movement between different subnets of one domain (intra-domain mobility) and movement between different access networks belonging to different domains (inter-domain mobility). For inter-domain mobility, a novel cross-layer mobility management protocol is proposed, which makes an early detection of the possibility of an inter-domain handoff and allows authentication, authorization and registration of the MH in the new domain before the actual handoff. These interoperability operations are executed by the NIA.

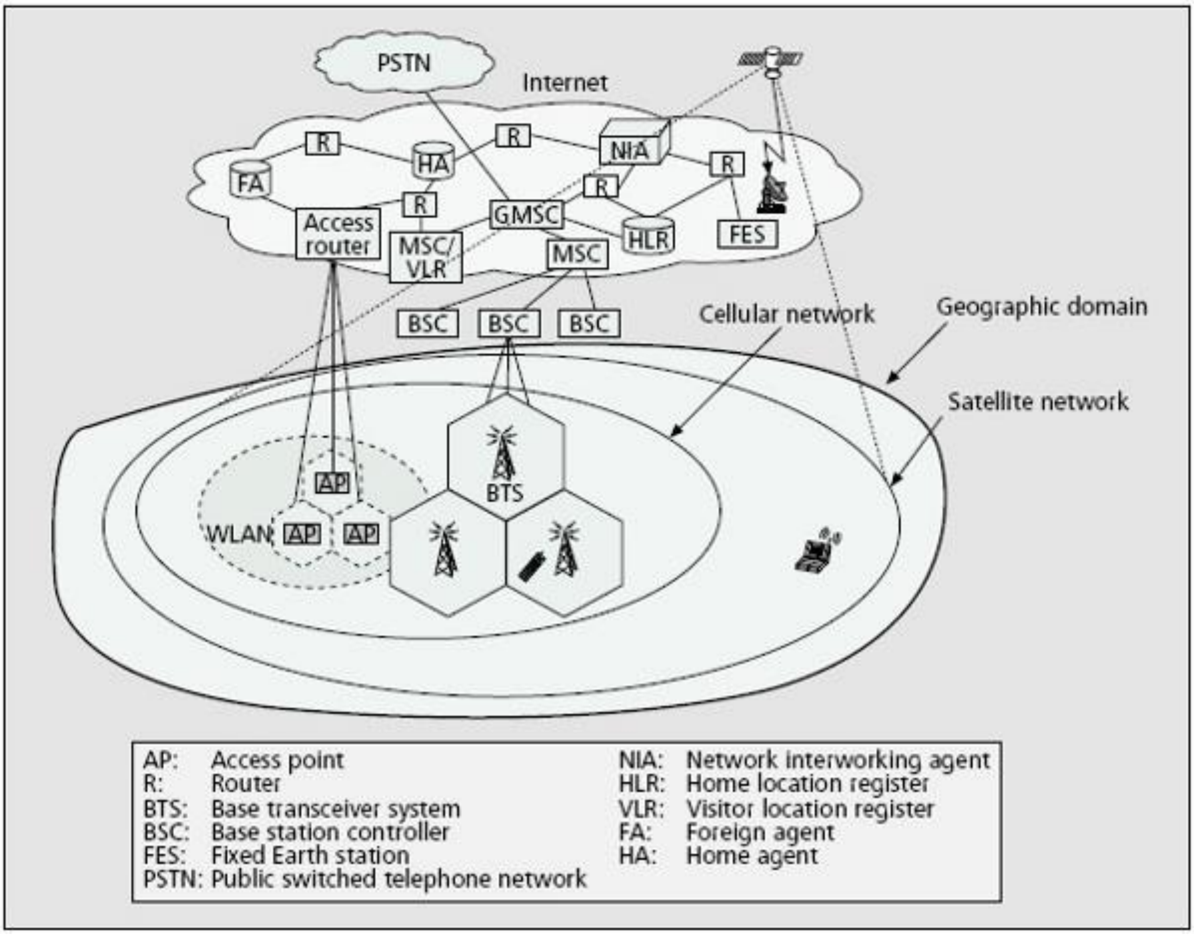


Figure 2:NIA-Based Mobility Management Architecture

Micro-mobility protocols

Over the past several years a number of IP micro-mobility protocols have been proposed, designed and implemented that complement the base Mobile IP (Campbell & Gomez, 2001) by providing fast, seamless and local handoff control. IP micro-mobility protocols are designed for environments where MHs changes their point of attachment to the network so frequently that the base Mobile IP mechanism introduces significant network overhead in terms of increased delay, packet loss and signaling. For example, many real-time wireless applications, e.g. VOIP, would experience noticeable degradation of service with frequent handoff. Establishment of new tunnels can introduce additional delays in the handoff process, causing packet loss and delayed delivery of data to applications. This delay is inherent in the round-trip incurred by the Mobile IP as the registration request is sent to the HA and the response sent back to the FA. Route optimization (Perkins & Johnson, 2001) can improve service quality but it cannot eliminate poor performance when an MH moves while communicating with a distant CH. Micro-mobility protocols aim to handle local movement (e.g., within a domain) of MHs without interaction with the Mobile IP-enabled Internet. This reduces delay and packet loss during handoff and eliminates registration between MHs and possibly distant HAs when MHs remain inside their local coverage areas. Eliminating registration in this manner also reduces the signaling load experienced by the network.

The micro-mobility management schemes can be broadly divided into two groups: (i) tunnel-based schemes and (ii) routing-based schemes. In tunnel-based approaches, the location database is maintained in a distributed form by a set of FAs in the access network. Each FA reads the incoming packet's original destination address and searches its visitor list for a corresponding entry. If an entry exists, it is the address of next lower level FA. The sequence of visitor list entries corresponding to a particular MH constitutes the MH's location information and determines the route taken by downlink packets. Mobile IP regional registration (MIP-RR) (Fogelstroem et al., 2006), hierarchical Mobile IP (HMIP) (Soliman et al., 2008), and intra-domain mobility management protocol (IDMP) (Misra et al., 2002) are tunnel-based micro-mobility protocol.

Routing-based approaches forward packets to an MH's point of attachment using mobile-specific routes. These schemes introduce implicit (snooping data) or explicit signaling to update mobile-specific routes. In the case of Cellular IP, MHs attached to an access network use the IP address of the gateway as their Mobile IP CoA. The gateway decapsulates packets and forwards them to a BS. Inside the access network, MHs are identified by their home address and data packets are routed using mobile-specific routing without tunneling. Cellular IP (CIP) (Campbell et al., 2000) and handoff-aware wireless access Internet infrastructure (HAWAII) (Ramjee et al., 2002) are routing-based micro-mobility protocols.

Mobile IP Regional Registration: In Mobile IP, an MN registers with its HA each time it changes its CoA. If the distance between the visited network and the home network of the MN is large, the signaling delay for these registrations may be long. MIP-RR (Fogelstroem et al., 2006) attempts to minimize the number of signaling messages to the home network and reduce the signaling delay by performing registrations locally in a regional network. This reduces the load on the home network, and speeds up the process of handover. The scheme introduces a new network node called the gateway foreign agent (GFA). The address of the GFA is advertised by the FAs in a visited domain. When an MN first arrives at this visited domain, it performs a home registration - that is, a registration with its HA. At this time, the

MN registers the address of the GFA as its CoA. When the MN moves between different FAs within the same visited domain, it only needs to make a regional registration to the GFA. When the MN moves from one regional network to another, it performs a home registration with its HA. The packets for the MN are first intercepted by its HA, which tunnels them to the registered GFA. The GFA checks its visitor list and forwards the packets to the corresponding FA of the MN. The FA further relays the packets to the MN. The use of the GFA avoids any signaling traffic to the HA as long as the MN is within a regional network.

Hierarchical Mobile IPv6: The basic idea of hierarchical Mobile IP (Soliman et al., 2008) (HMIP) is the same as that of regional registration scheme. HMIP introduces a new Mobile IP node called the mobility anchor point (MAP). An MN is assigned two CoAs - regional CoA (RCoA) and on-link CoA (LCoA). The MN obtains the RCoA from the visited networks. RCoA is an address on the MAP’s subnet. The LCoA is the CoA that is based on the prefix advertised by the access router (AR). The AR is the default router of the MN and receives all outbound traffic from it. When an MN enters a new network, it receives router advertisement that contains the available MAPs and their distances from the MN. The MN selects a MAP, gets the RCoA in the MAP’s domain and the LCoA from the AR. The MN sends a binding update to the MAP. The MAP records the binding and inserts it in its binding cache (foreign registration). The MAP sends the binding update message also to the MN’s HA and to the CNs (home registration). When MN is outside its home network, the incoming data to MN goes through MAP hierarchy. Messages from CN or HA are received by the MAP, which tunnels them to LCoA. As the MN roams locally, it gets a new LCoA from its new AR. The RCoA remains unchanged as long as the MN is within the same network.

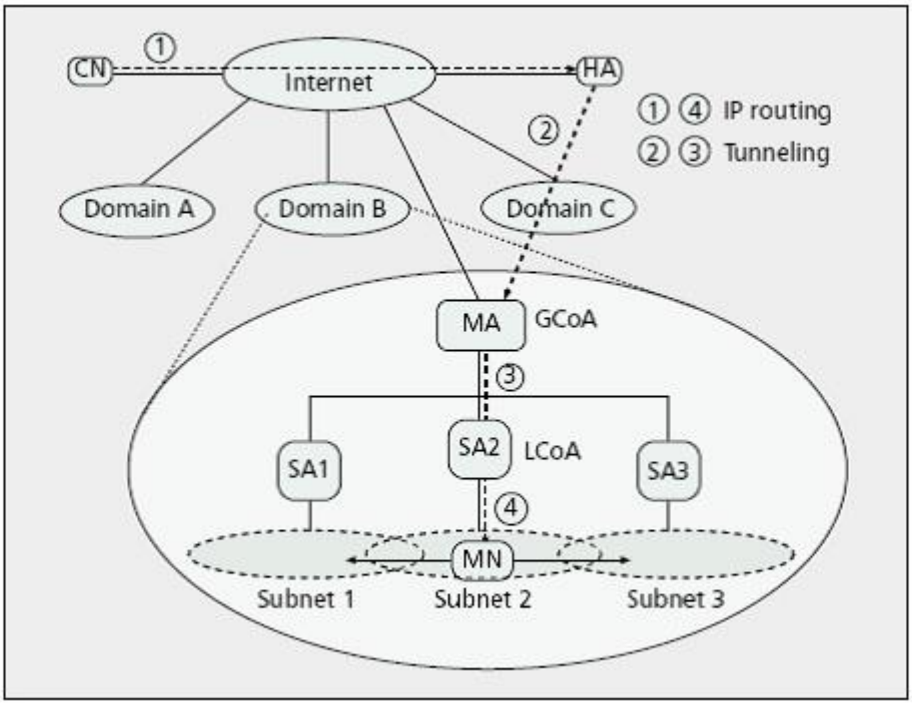


Figure3: The Architecture of IDMP

Intra-Domain Mobility Management Protocol: Intra-domain mobility management protocol (IDMP) (Misra et al., 2002) is a two-level, hierarchical, multi-CoA, intra-domain mobility management protocol. The first level of the hierarchy consists of different mobility domains. The second level consists of IP subnets within each domain. This hierarchical approach localizes the scope of intra-domain location update messages and thereby reduces both the global signaling load and update latency. The two-level hierarchical architecture defined by IDMP is shown in Figure 4. IDMP consists of two types of entities: (i) mobility agent (MA) and (ii) subnet agent (SA). The MA provides a domain-wide stable access point for an MN. An SA handles the mobility of MNs within a subnet. Similar to HMIP, each MN can get two CoAs - global CoA (GCoA) and local CoA (LCoA). The GCoA specifies the domain to which the MN is currently attached. The LCoA identifies the MN’s present subnet. The packets destined to an MN are first received by the HA. The HA tunnels the packets to the MA using the MN’s GCoA. The MA first decapsulates the packets, determines the current LCoA of the MN using its internal table, and tunnels them to the LCoA. The encapsulated packets are received by the SA. Finally, the SA decapsulates the packets and forwards them to the MN. When the MN moves from one subnet to another inside the same domain, it is assigned a new LCoA. The MN registers the address of the new LCoA with its MA. Till the registration of the new LCoA is complete, the MA forwards all packets for the MN to the old

LCoA. This results in packet drops. A fast handoff procedure has been proposed to avoid this packet loss (Misra et al., 2002). It eliminates intra-domain update delay by anticipating the handover in connectivity between the networks and the MNs. The anticipation of MN’s movement is based on a link layer trigger which initiates a network layer handoff before the link layer handoff completes. Once the MN senses a handoff, it sends a request to the MA to multicast the packets to its SAs. The MA multicasts incoming packets to each neighboring SAs. Each SA buffers the packets in order to prevent any loss of packets in transit during the handoff. After the MN finishes registration, the new SA transfers all buffered packets to the MN.

Cellular IP: Cellular IP (Campbell et al., 2000) is a mobility management protocol that provides access to a Mobile IP-enabled Internet for fast moving MHs. The architecture of Cellular IP is shown in Figure 5. It consists of three major components: (i) cellular IP node or the base station (BS), (ii) cellular IP gateway (GW), and (iii) cellular IP mobile host (MH). A Cellular IP network consists of interconnected BSs. The BSs route IP packets inside the cellular network and communicate with MHs via wireless interface. The G

W is a cellular IP node that is connected to a regular IP network by at least one of its interfaces. The BSs periodically emit beacon signals. MHs use these beacon signals to locate the nearest BSs. All IP packets transmitted by an MH are routed from the BS to the GW by hop-by-hop shortest path routing, regardless of the destination address. The BSs maintain route cache. Packets transmitted by the MH create and update entries in BS’s cache. An entry maps the MH’s IP address to the neighbor from which the packet arrived to the host. The chain of cached mappings referring to an MH constitutes a reverse path for downlink packets for the MH.

To prevent timing out of these mappings, an MH periodically transmits control packets. MHs that are not actively transmitting or receiving data themselves may still remain reachable by maintaining paging caches. MHs listen to the beacons transmitted by BSs and initiate handoff based on signal strength. To perform a handoff, an MH tunes its radio to the new BS and sends a route update packet. This creates routing cache mappings on route to the new BS. Handoff latency is the time that elapses between the handoff and the arrival of the first packet through the new route. The mappings associated with the old BS are cleared after the expiry of a timer. Before the timeout, both the old and new downlink routes remain valid and packets are delivered through both the BSs. This feature used in Cellular IP semi-soft handoff algorithms improves handoff performance.

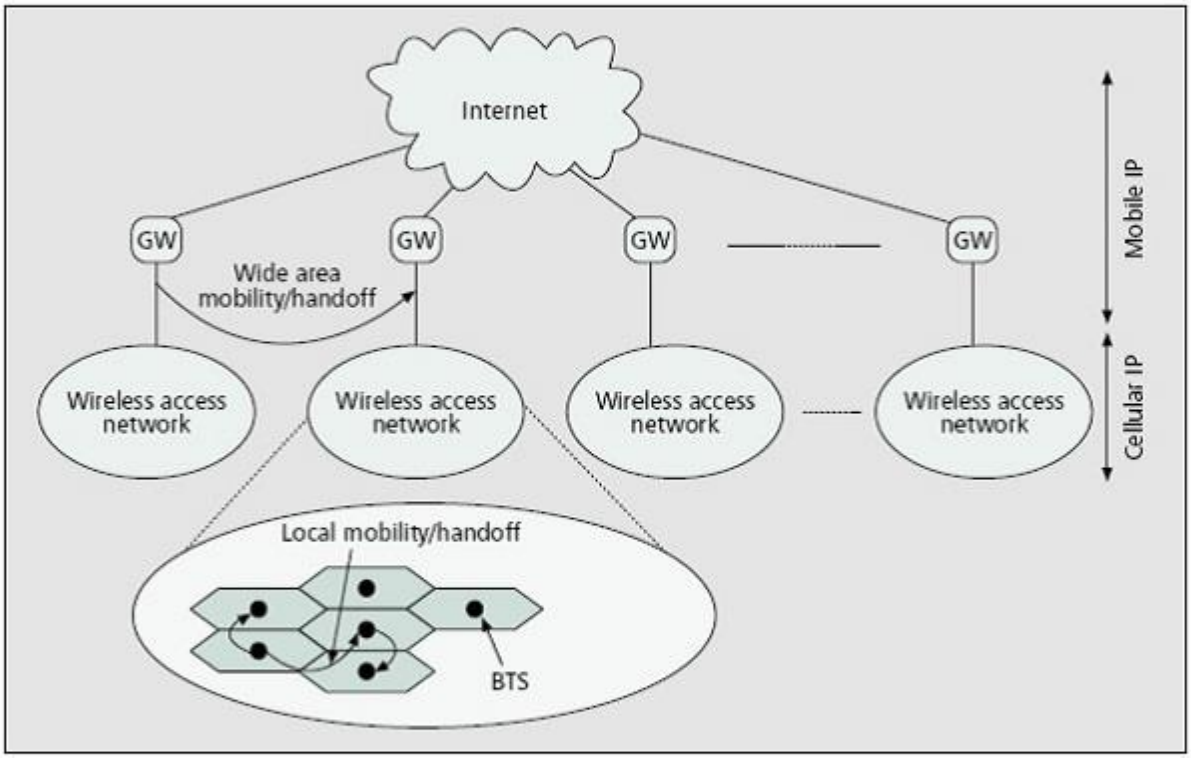


Figure 5. Architecture of Cellular IP

Handoff Aware Wireless Access Internet Infrastructure: Handoff-Aware Wireless Access Internet Infrastructure (HAWAII) (Ramjee et al., 2002) is a domain-based approach for supporting mobility. The network architecture of HAWAII is shown in Figure 6. Mobility management within a domain is handled by a gateway called a domain root router (DRR). Each MH is assumed to have an IP address and a home domain. While moving in its home domain, the MN retains its IP address. The packets destined to the MH reach the DRR based on the subnet address of the domain and are then forwarded to the MH. The paths to MH are established dynamically. When the MH is in a foreign domain, packets for the MH are intercepted by its HA. The HA tunnels the packets to the DRR of the MH. The DRR routes the packets to the MH using the host-based routing entries. If the MH moves across different subnets in the same domain, the route from the DRR to the BS serving the MN is modified, while the other paths remain unchanged. This causes a reduction in signaling message and handoff latency during intra-domain handoff. In traditional Mobile IP, the MH is directly attached either to the HA (i.e. the home domain router) or the FA (i.e. the foreign domain router). Thus, every handoff causes a change in the IP address for the MH, resulting in lack of scalability. HAWAII also supports IP paging. It uses IP multicasting to page idle MHs when packets destined to an MH arrive at the domain root router and no recent routing information is available.

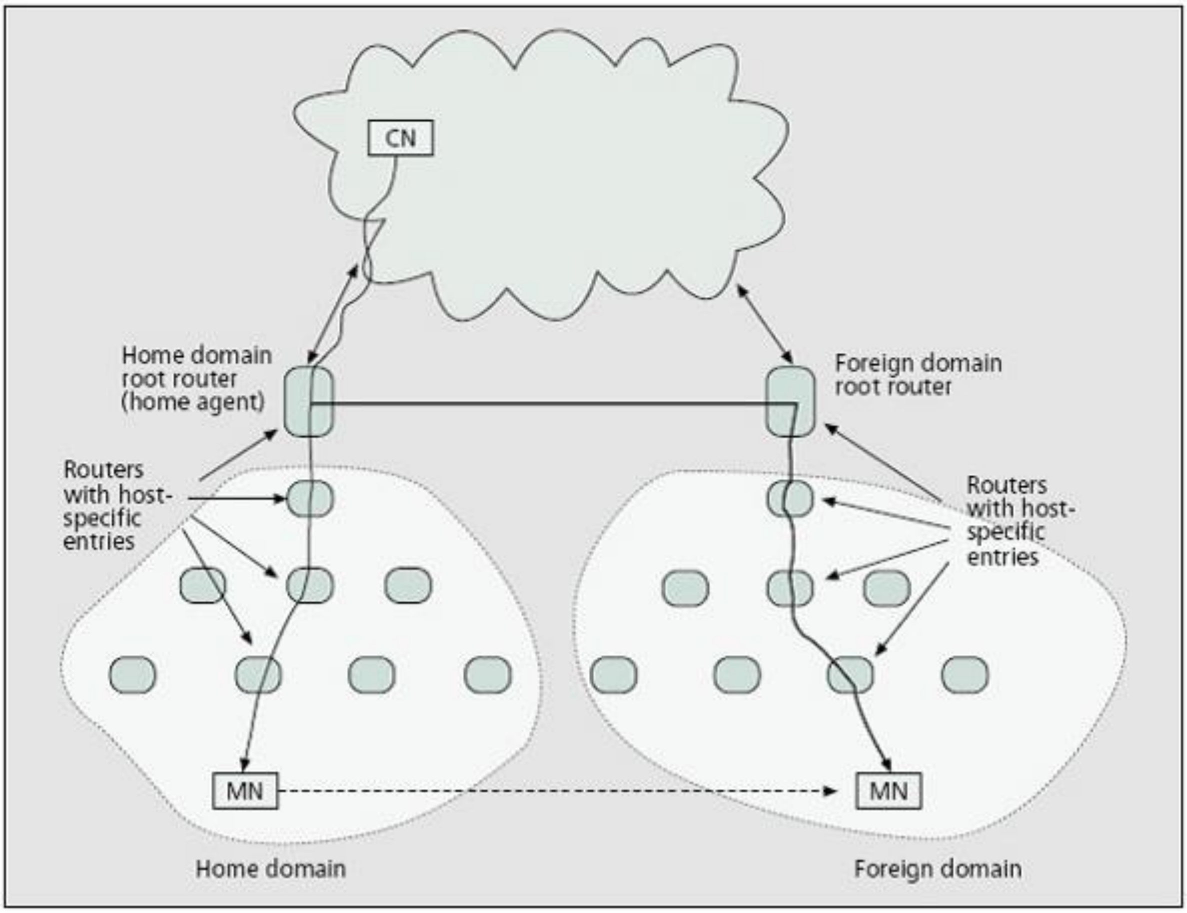

CN
Home domain root router (home agent)
Foreign domain root router
Routers with host-specific entries
Routers with host-specific entries
MN
MN
Home domain
Foreign domain

Figure 6. Architecture of HAWAII Protocol

Summary: Various network layer micro-mobility management schemes have been compared based on their features (Chiussi et al., 2002; Ramjee et al., 1999; Campbell et al., 2002). Each protocol uses the concept of domain root router. In all the protocols, signaling traffic is largely localized in a domain so as to reduce the global signaling traffic overhead. Routing-based schemes utilize the robustness of IP forwarding mechanism. Mobile-specific address lookup tables are maintained by all the mobility agents within a domain. In tunnel-based schemes, registration of the mobile nodes and encapsulation of the IP packets are performed in a local or hierarchical manner. Routing-based schemes avoid tunneling overhead, but suffer from the high cost of propagating host-specific routes in all routers within the domain. Moreover, the root node in routing schemes is a potential single point of failure (Chiussi et al., 2002). Tunnel-based schemes are modular and scalable. However, they introduce more cost and delays (Campbell et al., 2002).

Hierarchical Mobile IP

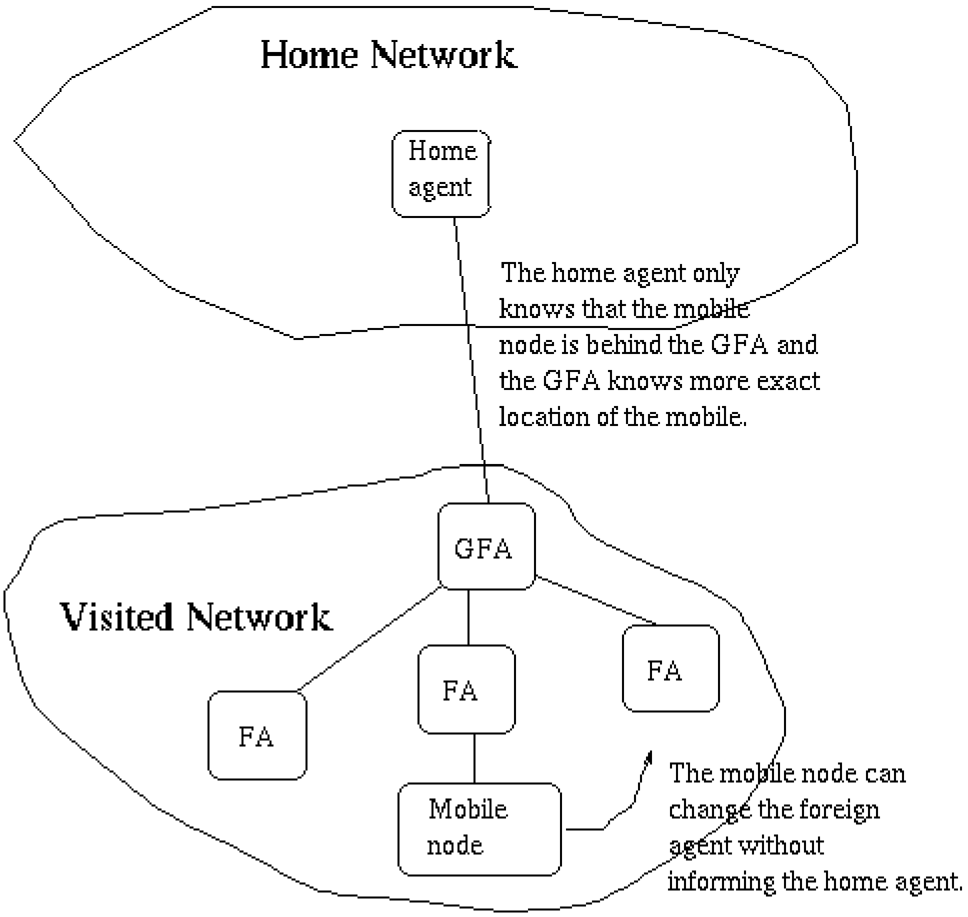
There are several protocol suggestions that have the same basic idea of hierarchical structure of visited networks. In all these proposals, the mobile node does not have to inform its home agent of every movement it performs inside the visited network. Instead there is a network element that takes care of the mobile node's registrations.

The following subsection concentrates around the regional tunnel management [3]. However, other hierarchical proposals exist, for example, the RAFA [10] and Dynamics HUT Mobile IP .

Regional tunnel management

In regional tunnel management, the mobile node can move inside a visited domain without informing its home agent about every movement. When a mobile node first arrives at the visited network, it performs normal registration with its home agent. After that the mobile node is doing regional registrations inside the visited network.

If the foreign network supports regional tunnel management, there is a special kind of foreign agent called a gateway foreign agent (GFA). The mobile node uses the GFA's IP address as its care-of address when it registers with the home agent. This care-of address does not change when the mobile node moves between the foreign agents that are located under the same GFA. After first registration, the mobile node makes its registrations with the GFA. Registrations are not done with the home agent as long as it is moving under the same GFA. If the mobile node changes GFA, within or between visited domains, it must again register with the home agent. Because the binding of the mobile node must not expire at the home agent, there also has to be regular registrations with the home agent. [3] The Figure 3 illustrates the basic idea of hierarchical Mobile IP.


Home Network
Home agent
The home agent only knows that the mobile node is behind the GFA and the GFA knows more exact location of the mobile.
GFA
Visited Network
FA
FA
FA
Mobile node
The mobile node can change the foreign agent without informing the home agent.

Regional tunnel management

The mobile node does require extra support for regional tunnel management. The changes are caused by different types of registration messages and security issues. Also changes are needed to the home agent, if it is acting as a key distributor for the GFA and the mobile node. Otherwise, the home agent assumes that the mobile node is not at all moving in the visited network because its care-of address remains the same.

Intra domain Mobility Management:

a lightweight Intra-domain Management Protocol (IDMP) for managing mobility within a domain, commonly known as micro-mobility management, for next generation wireless networks. IDMP is modular and simple because it leverages existing protocols, such as Mobile IP or SIP (Session Initiated Protocol) as global mobility management, for locating roaming nodes. Unlike other proposed intra-domain mobility management schemes, IDMP uses two dynamically autoconfigured care-of addresses (CoAs) for routing the packets destined to mobile nodes.

The global care-of address (GCoA) is relatively stable and identifies the mobile node's attachment to the current domain, while the local care-of address (LCoA) changes every time the mobile changes subnets and identifies the mobile's attachment to the subnet level granularity.

INTRODUCTION

In recent years, there has been much interest in developing efficient IP-based micro-mobility management schemes to handle node mobility within a domain in next-generation wireless networks. Such schemes are essential to achieve seamless integration of cellular networks with existing IP-based data networks, popularly known as the Internet. Many cellular network providers and operators have already realized the need for an IP-based mobility management solution to support real and non-real time applications in next-generation networks. However, Internet protocols are currently unable to support the additional performance guarantees that these applications require at the user level. Based on a survey of requirements, we can identify, at a high level, the following features desired of any intra-domain mobility management solution:

Support for fast handoffs: The mobility management architecture and protocol should be able to seamlessly redirect packets to the mobile's new point of attachment with minimum latency. To support real-time IP applications, including Voice-over-IP (VoIP), the latency typically associated with the registration process must be decreased and bounded.

Reduction in packet loss during movement: With new emerging applications especially for cellular networks, that use non reliable transport protocols for packet transport, the packet loss during handoffs should be minimum.

Support for paging: Paging is important in power-conscious environments since it enables a mobile node to significantly reduce its mobility-related signaling traffic. Next generation cellular networks are likely to see a proliferation of power conscious miniature devices and appliances. Any mobility management protocol for such networks should have the option to provide paging support.

Support for multi-path distribution techniques: The intra-domain mobility management protocol should be able to support multiple traffic paths, typically used for providing redundancy and greater transmission reliability. This support must be optional and configurable only when the link and physical layer technologies permit. At this point, it is not very clear whether such support is necessary for currently emerging wireless access technologies.

The current standard for IP-based mobility management, namely Mobile IP [2], was designed primarily for environments where the mobile node (MN) was assumed to have a well-defined home network and a topologically correct care-of address (CoA) in the foreign network. In such predominantly static environments, the frequency and volume of global registration messages generated by mobile nodes are not a major concern. Mobile IP ensures transparency to TCP connections by preserving the fixed home address of the MN and performing packet redirection (using tunneling) at the network layer. In the absence of a set of viable real-time or delay sensitive applications, the latency involved in updating the remote home agent (HA) or correspondent node (CN) on every subnet change was also not a topic of practical concern. Moreover, the base Mobile IP assumes that the rate of subnet change by an MN is not too rapid; the specifications state that Mobile IP is intended for situations where the MN does not change subnets more than once every second [2].

On the other hand, the signaling overhead in next-generation wireless networks, where every active node is likely to exhibit significant mobility, can become very large. In practical wide-area cellular networks, topology considerations, frequency and address space limitations (in case of IPv4 for example) may also cause an IP subnet to span a fairly limited geographical area. Thus, a mobile may change subnets fairly frequently, especially if the trend towards pico-cellular networks in urban areas continues. Therefore, a separate protocol for supporting intra-domain mobility becomes necessary. The intra-domain mobility management protocol (IDMP) proposed in this paper fosters a more modular network architecture and allows static Internet hosts to communicate with mobile nodes without any changes. This fits nicely with the requirements for a variety of applications in next generation cellular networks. Additionally, unlike the conventional Internet, where backward compatibility is not a major concern, cellular networks have no ‘IP legacy’ issues.

IDMP OVERVIEW

The Intra Domain Mobility Management Protocol (IDMP) proposed in this paper is an extension to the base intra-domain protocol used in TeleMIP. An Internet draft on IDMP [16] has been recently proposed for supporting several additional mobility features, such as minimally interrupted handoff and paging, within the mobility domain for highly mobile users. This separation of intra-domain mobility from inter-domain mobility is intended to allow a common base protocol to coexist with multiple alternatives for global mobility management, including Mobile IP and SIP. An architecture called Dynamic Mobility Agent (DMA) [17] has also been recently proposed which uses IDMP as the base mobility management protocol to provide a scalable and robust mobility management framework.

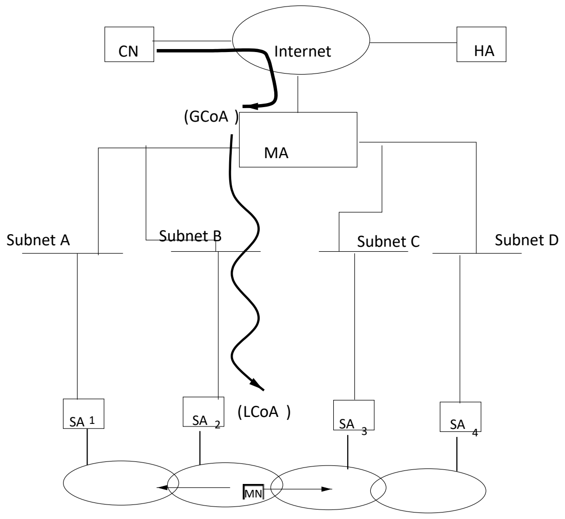
A. Base Protocol

IDMP offers intra-domain mobility by using multi-CoAs. However, unlike HAWAII, MIP-RR or HMIPv6, our protocol IDMP is designed as a stand-alone solution for intra-domain mobility and does not assume the use of MIP for global mobility management. Figure 1 depicts the functional layout of IDMP. The Mobility Agent (MA) is similar to a MIP-RR GFA and acts as a domain-wide point for packet redirection. A Subnet Agent (SA) (similar to a MIP FA in CoA mode and DHCP/DRCP [19], [20] server in co-located CoA mode) provides subnet-specific mobility services. Under IDMP, an MN obtains two concurrent CoAs:

Local Care-of Address (LCoA): This identifies the MN’s attachment to the subnet. Unlike MIP’s CoA, the LCoA in IDMP only has local (domain-wide) scope. By updating its MA of any changes in the LCoA, the MN ensures that packets are correctly forwarded within the domain.

Global Care-of Address (GCoA): This address resolves the MN’s current location only up to a domain-level granularity and hence remains unchanged as long as the MN stays within a single domain. By issuing global binding updates that contain this GCoA, the MN ensures that packets are routed correctly to its present domain.

Under IDMP, packets from a remote CN are forwarded (with or without tunneling) to the GCoA and are intercepted by the MA. As shown in Figure 1, the MA then tunnels these packets to the MN’s current LCoA. Since global binding updates are generated only when the MN changes domains and obtains a new GCoA, this approach drastically reduces the global signaling load.

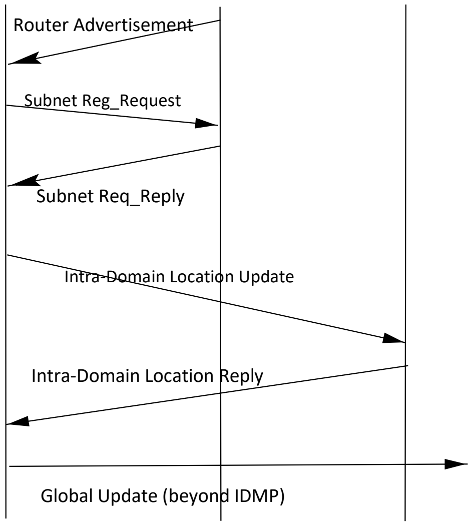


IDMP Logical Elements & Architecture

A.1 Basic Packet Redirection and Mobility Support

When the MN first moves into a domain, it obtains a local care-of address (this LCoA is ’s address in Figure 1) by performing a subnet-specific registration using IDMP. As requested by IDMP, the serving SA (in this case) dynamically assigns the MN a Mobility Agent (MA) during this subnet-specific registration process. The MN then performs an intra-domain location update by communicating its current LCoA to the designated MA. The MA includes either its address or a separate GCoA in the intra-domain location update reply. Subsequently, the mobile node is responsible for generating a global location update (registration) to the necessary remote nodes (e.g., HA if Mobile IP is used for global mobility management or Registrar (LR) if SIP is used); this is however independent of the IDMP specifications. The IDMP call flow when the MN first moves into a new domain is illustrated in Figure

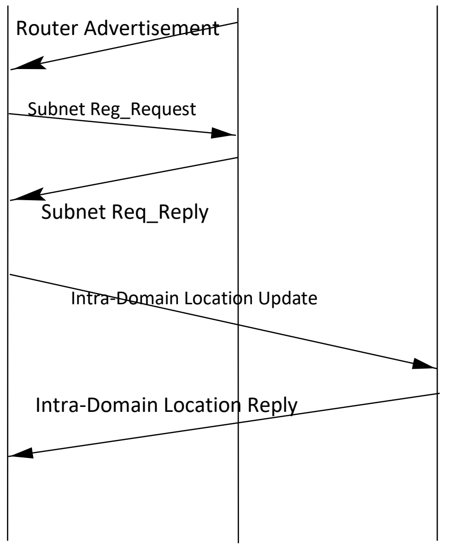
MN SA MA


Router Advertisement
Subnet Reg_Request
Subnet Req_Reply
Intra-Domain Location Update
Intra-Domain Location Reply
Global Update (beyond IDMP)

IDMP Message Flow during the Initial Intra-Domain Location Update

After the initial intra-domain registration process, IDMP now allows the MN to retain its global care-of address as long it stays within the same domain. Whenever MN changes subnets within this domain, it performs a new subnet-specific registration with the new SA. Since the MN indicates that it has an existing valid registration, the SA does not allocate it a new MA address in this case. The MN then performs a new intra-domain location update and informs its MA of its new local care-of address. No global messages are generated in this case, since the global care-of address remains unchanged. As with other hierarchical mobility management schemes, the localization of intra-domain mobility significantly reduces the latency of handoffs across subnets within the same domain and also dramatically decreases the frequency of global signaling traffic. Figure describes the IDMP call flow during subsequent intra-domain movement.

MN SA MA



IDMP Call Flow during Subsequent Intra-Domain Movement

FAST HANDOFF SCHEME IN IDMP

In the basic mode of IDMP, the handoff delay (or the service interruption time) equals the time taken from a disconnection until the MA becomes aware of the MN's new point of attachment (LCoA) and begins redirecting packets correctly again. In a cellular network architecture where IP-based base station (IPBS) is used, this delay essentially consists of three components:

Radio-channel Establishment Delay ( ): The MN must establish a new radio-channel at the new BS. This is a link-layer specific function, and could involve even operations such as slot-specification in TDMA or code synchronization in CDMA.

IP Subnet Configuration Delay ( ): An MN must use IP-layer configuration protocols to obtain the new LCoA. If IDMP's SA mode is used, then the MN must obtain an 'Agent Advertisement' through router discovery or some other beacon and then request a new LCoA. The subnet agent (SA) will then respond with an acknowledgement message. If the co-located mode is used, the MN must exchange DHCP configuration messages with the DHCP server before obtaining a valid CoA.

Intra-domain Update Delay ( ): The MN must finally inform the MA of this new LCoA via an intra-domain location update message. The MA will redirect packets to the MN's new LCoA only after receiving this message.

The parameter , although link-layer specific, can be expected to be quite low. For example, in CDMA-based soft handoffs, is effectively , since in such a network, communication with the old BS is not discontinued until the connection with the new BS is firmly established (commonly known as soft handoff). Even under the hard handoff scenario, no disruption to the radio-level connectivity should occur in a well-designed system: the various elements should coordinate to ensure a synchronized switch to the new point of attachment. IDMP's fast handoff mechanism is designed to eliminate the component in the handoff delay. To make IDMP's operation independent of current or future link-layer techniques, we do not provide IP-level connectivity until the MN has performed a subnet-level configuration at the new BS. IDMP's fast handoff process, thus, does not eliminate , the delay incurred in the subnet-level configuration process.

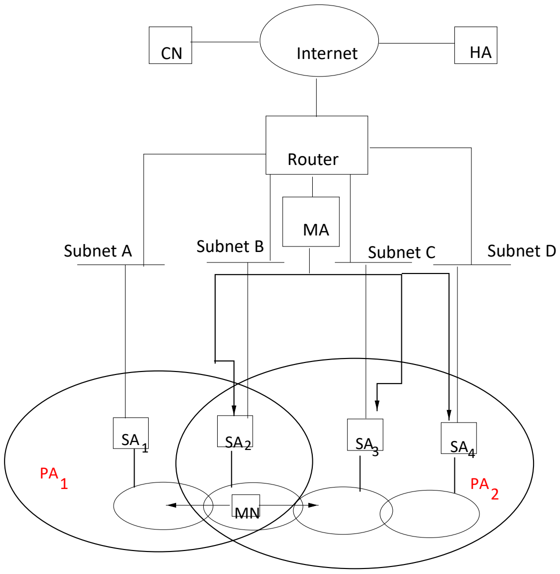
The Fast Handoff Procedure

IDMP's fast handoff procedure is based on the assumption that a layer-2 trigger will be available (either to the MN or to the old BS) indicating an imminent change in connectivity. We explain the fast handoff mechanism with the help of Figure 4, which shows an MN moving from to . To minimize the service interruption during the handoff process, IDMP requires either the MN or the old SA ( ) to generate a Movement Imminent message to the MA serving the MN. Upon reception of this message, the MA multicasts all inbound packets to the entire set of neighboring SAs (and in this case). Each of these candidate SAs buffers such arriving packets in individual MN buffers, thus minimizing the loss of in-flight packets during the handoff transient. When the MN subsequently performs a subnet-level configuration (using IDMP messages) with , the latter can immediately forward all such buffered packets over the wireless interface, without waiting for the MA to receive the corresponding intra-domain location update. Several features of this proposal make it attractive for future IP-based networks, such as, (i) unlike other fast handoff proposals, IDMP's Movement Imminent message does not specify the IP address of the target (new) BS in this message; (ii) IDMP utilizes a network-controlled (network or mobile-initiated) handoff technique; (iii) IDMPs' fast handoff scheme does not eliminate from the service interruption time; it merely delays the transmission of packets arriving during this instant. Details of this proposal are described in [17].

Figure 4: IDMP Fast Handoff

V. PAGING SUPPORT IN IDMP

While IDMP's use of multicasting for fast handoffs minimizes the loss of in-flight packets during an intra-domain handoff, it does not reduce the frequency of intra-domain location updates. In the absence of paging support, an MN must obtain a local care-of address and re-register with its MA every time it changes its current subnet. This can lead to significant power wastage, especially in future 4G networks where a single device may maintain multiple simultaneous bindings with multiple radio technologies. IDMP's IP-layer paging solution provides a flexible and radio-technology independent solution to this important problem.



IDMP Paging Mechanism

A. Paging Operation for Idle Hosts

To motivate IDMP's paging solution, we refer to the 'multicasting' scheme described for fast handoff support in the last section. In fast handoff, the MA essentially sends multiple copies of the same data to multiple SAs/subnet routers that are judged to be in the vicinity of the MN's current point of attachment. Since limited broadcast of solicitations is really the central feature of paging, the idea of multicast groups can be extended to provide paging support as well. IDMP's paging operation assumes that SAs (subnets or IPBSs) are grouped into Paging Areas (PAs) identified by some unique identifiers. An MN in passive/idle mode is then able to detect changes in its current PA by listening to these unique identifiers in the subnet-level advertisements (e.g., Subnet Agent Advertisements). In fact, such IP-layer advertisements may optionally be combined with link-layer beacons.

IDMP's paging scheme is illustrated in Figure 5. In this model of operation, subnets B, C and D belong to the same PA , while subnet A is part of a different PA, PA . We assume that the MN switches to idle state in subnet B. Then, as long as it moves to C or D, it detects changes in its subnet of attachment but no change in its current PA. Consequently, not only does the MN not update its MA about its current LCoA, but also does not bother to obtain a new LCoA. However, when it moves to subnet A and realizes that it has changed to a new PA, the MN obtains a new LCoA at and sends a location update to the MA, indicating the new paging area.

When the MA receives packets for an MN which is currently registered, but does not have a valid LCoA assigned, it multicasts a PageSolicitation packet to all the subnets associated with the MN's current PA (i.e., to , and) and buffers the incoming packets. When the MN re-registers with the MA, the buffered packets are forwarded to the MN.

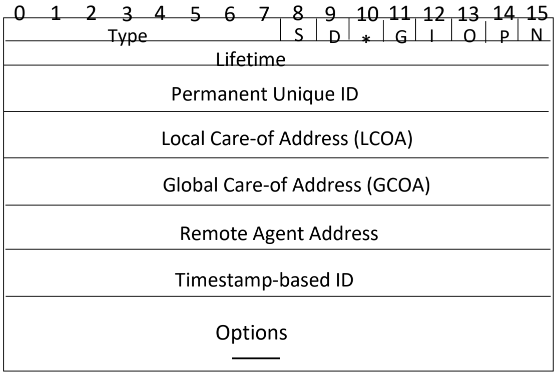
IMPLEMENTATION OF IDMP

The Mobility Agent (MA) handles local registration requests from MNs that are currently in its domain, and provides temporary bindings to the MNs as long as they remain in the domain. As far as the handling of such registration (or location update) requests is concerned, there is little functional difference between HA and MA. Unlike the HA, which has a permanent list of mobility bindings for each MN associated with its home network, the MA maintains a dynamic list of mobility bindings for currently registered MNs. The major functional difference between HA and MA is in terms of packet forwarding to the MN. When the MN is away from the home network, the HA is responsible for collecting all the packets directed at the MN's permanent IP address and tunneling the packets to the global care-of address (which is also the IP address of the MA interface). The task of the MA is simpler; it receives the packets automatically, and after decapsulating the packets, redirects the inner IP packet to the MN's local care-of address.

In fact, the HA is potentially unaware of the use of IDMP and the presence of the MA. As in conventional Mobile IP, it simply has to intercept all packets intended for the MN from the home network, encapsulate them and forward them to the care-of address specified in the MN-HA registration message. The registration request and reply message formats for global registrations are, in fact, identical to Mobile IP with a single exception: the reserved bit in flags field in [18] is now used to indicate whether the MN is operating in a DMA-based network.

A. IDMP Packet Formats

Mobile nodes in our architecture use IDMP messages to register their local care-of address with the designated MA. While IDMP packet formats and location update messages are based on Mobile IP, they have been modified to support additional intradomain mobility features. Figures 6 and 7 show the IDMP packet formats for intra-domain registration request and reply messages respectively. Our current implementation supports only the co-located mode for local addressing. An MN thus uses DHCp or DRCP to obtain a local care-of address; subnet-level registrations (between the MN and an SA) are consequently not described in this paper. For additional details on the individual message fields. Since support for paging and fast handoff is not supported in our current implementation, the corresponding flags (P and O bits) are set to 0.



IDMP Intra-domain Location Update Packet Format

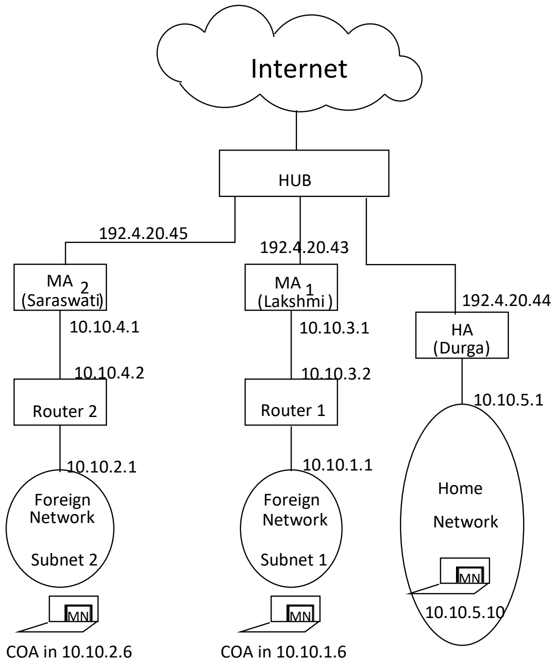
For the ease of implementation, we use Mobile IP as the global mobility management protocol. The permanent home IP address is assumed to be the unique identifier for the MN. The MN uses the IP address of its HA in the remote agent address field in its location update message. timestamp-based replay protection in the location update process, with two distinct timestamps for the local (MN-MA) and global (MN-HA) registrations. Similarly, the security association between the HA and the MN is distinct from the security association between the MN and MA; currently the only authentication method supported being keyed-MD5.

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

Type	P	N	O	G	I	Code

Lifetime
Permanent Unique ID
Local Care-of Address (LCOA)
Global Care-of Address (GCOA)
Remote Agent Address
Timestamp-based ID
Options ——

IDMP intra-domain Registration Reply Packet Format



Test Network Configuration Test Bed Setup

Figure 8 shows our experimental network test-bed used for evaluating IDMP. We considered a single MN served by its HA (Durga=192.4.20.44) in its home network (10.10.5.0), with home IP address 10.10.5.10. The home interface address of Durga is 10.10.5.1. Two MAs, viz., (Lakshmi=192.4.20.43) and (Saraswati=192.4.20.45) are connected to routers serving subnets 10.10.1.0 and 10.10.2.0 respectively. We assume that our mobility domain comprises both subnets 10.10.1.0 and 10.10.2.0. Accordingly, both Lakshmi and Saraswati can serve as mobility agents for our MN as long as it stays within this domain.

As the MN enters into the subnet 10.10.1.0, it receives a locally scoped co-located address 10.10.1.6 and the IP address of

(192.4.20.43) as its global care-of address. The MN accordingly first informs of its local care-of address (10.10.1.6) and subsequently registers with the HA using 192.4.20.43 as its care-of address. Afterwards, the MN roams into the subnet 10.10.2.0 and gets a new local care-of address 10.10.2.6. Since is still its MA, the MN simply performs an intra-domain location update, informing of its new local care-of address.

To test the case of inter-domain (global) mobility, we subsequently configured the DRCP server to provide a new MA address, say (Saraswati=192.4.20.45), to the MN. In this case, the MN performs both the intra-domain and inter-domain registrations.

Cellular IP

The cellular IP protocol provides mobility and handoff support for very frequently moving hosts. However, it is also capable of handling rarely moving and totally static hosts as well. The cellular IP is intended to be used in local or metropolitan area networks. It is a Mobile IP protocol extension, not replacement.

One of the main differences to the other micro mobility solutions is that in cellular IP the location management for idle mobile hosts is different from hosts that are actively transmitting or receiving data.

Figure A1 illustrates the basic structure of Internet containing networks implementing the cellular IP protocol.

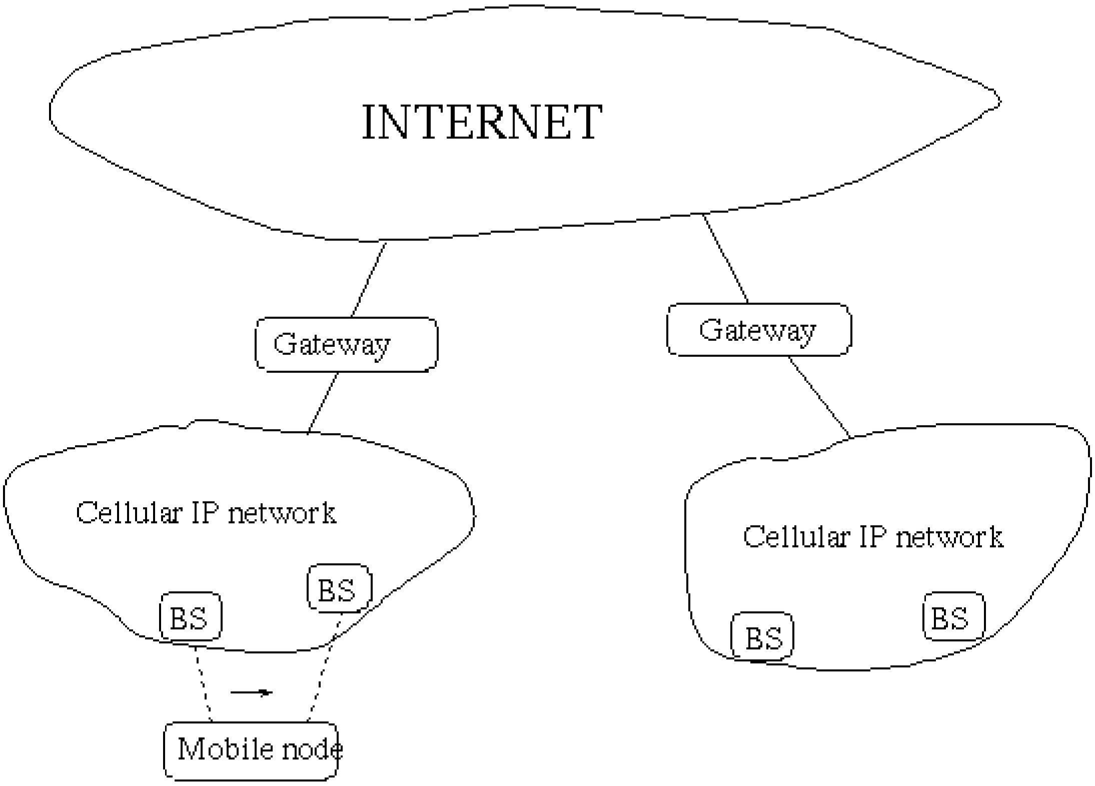


Figure A1: Micro mobility with Cellular IP

The base stations periodically broadcast beacon signals and mobile hosts use them to locate the nearest base station. A mobile host can send an IP packet to the Internet by sending it to the nearest base station. The base station then routes the packet to the cellular IP gateway providing access to the Internet.

All the cellular IP nodes are responsible of maintaining a cache containing routing information. An entry in the cache binds the mobile node's IP address with the direction where the mobile node is located. When a mobile node sends an IP packet, it goes through the necessary cellular IP nodes and after that the nodes have the necessary information about the mobile node's location. Every cellular IP node knows only the next hop to the downlink direction. The mobile node's reverse direction packets can be delivered through the same path. The Downlink and uplink idea is illustrated in the Figure A2

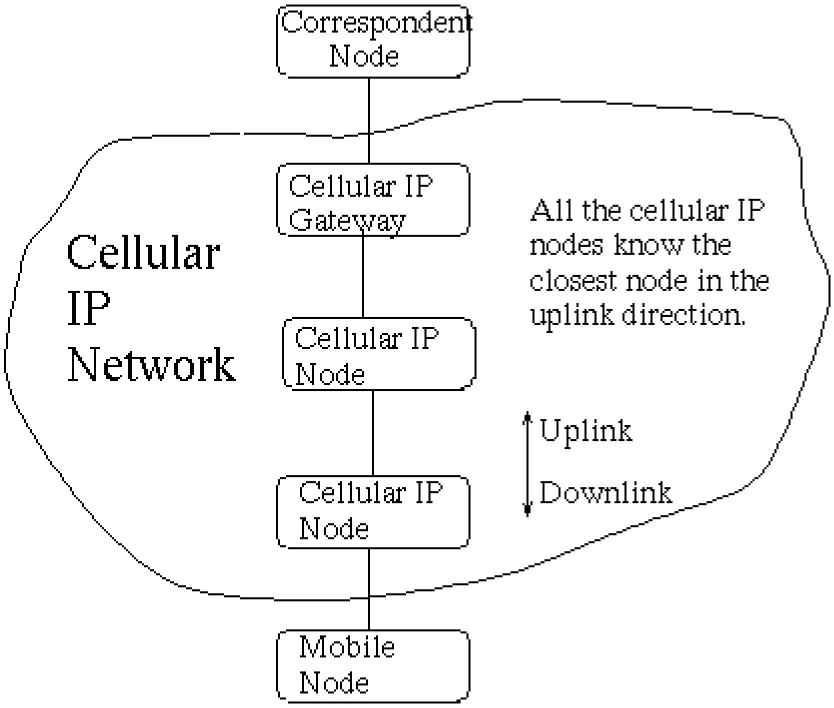


Figure A2: Cellular IP network

The bindings in cellular IP nodes' caches have time out values. A mobile node can keep the network aware of its exact location by sending regularly control packets through the path.

If the mobile host is not actively sending or receiving data, but it wants to remain reachable, it can let routing caches in cellular nodes expire. Some of the cellular IP nodes contain so called paging cache that has longer time out. finding the mobile node is bit a more difficult if there is only an entry in the paging cache and not in the routing caches. When the mobile node is in the active state, it has to inform the network of each handoff and because of this the routing caches are uptodate. When the mobile node is not in the active state, it is better that it does not inform network about every movement, because usually the mobile nodes have limited batteries.

HAWAII

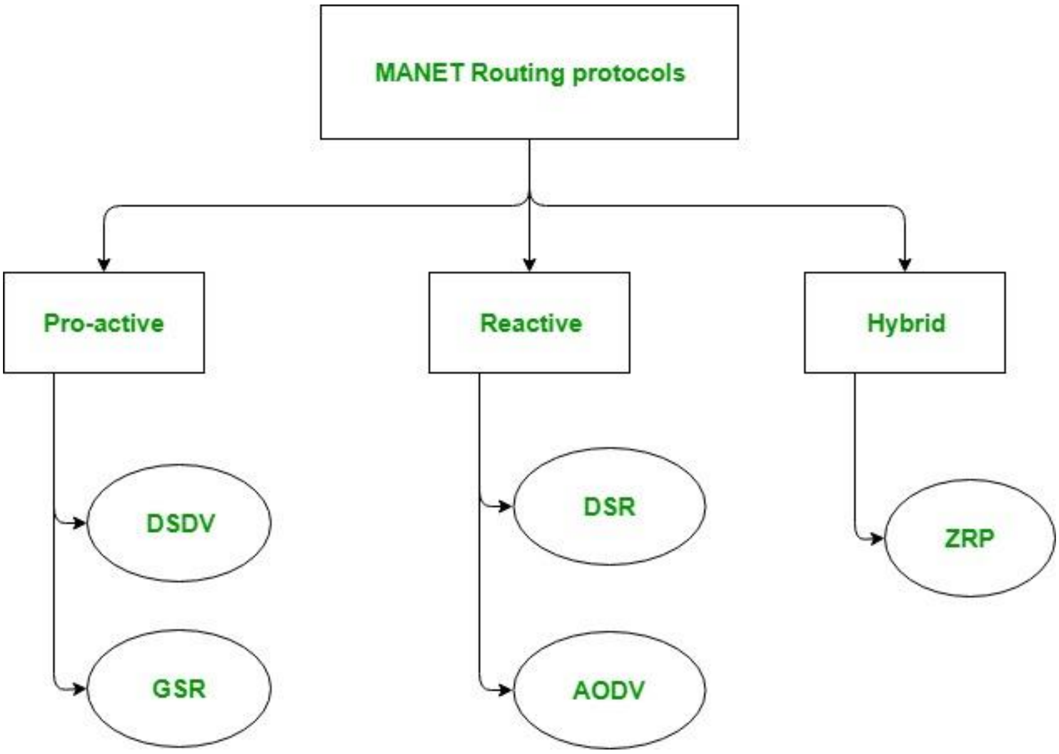
Handoff-Aware Wireless Access Internet Infrastructure (HAWAII) has been designed to take care of the micro mobility inside the visited domain. The HAWAII is not totally transparent to the mobile nodes. They use the standard Mobile IP protocol with NAI, route optimization and challenge/response extensions. The processing and generation of the Mobile IP registration messages are splitted into two parts: between the mobile host and the base station and between the base and the home agent. Because of this division to two parts, the HAWAII is a close relative with the regionalized tunnel management protocol proposals.

In the HAWAII, the mobile nodes can use the co-located care addresses (CCOA). This means that the end point of the IP within IP tunnel is always at the mobile node and that the mobile node responsible of decapsulating the IP packets. If the mobile node is connected to the visited with a slow connection, this is a disadvantage because the extra IP layer is transferred all the way to the mobile node. The use of CCOA is also in conflict with reducing the frequency of updates to the home agent. This has been solved so that In the HAWAII the mobile nodes are able to register with a base station even while using the CCOA. The base station handles the registrations locally and so reduces the amount of updates to the home agent. So in the HAWAII the normal IP data packets are sent directly from the home agent to the mobile node and the registrations are processed in two stages at the base station and the home agent.

UNIT-5

MANET Routing Protocols:

In Mobile Ad hoc Network (MANET), nodes do not know the topology of their network, instead they have to discover it by their own as the topology in the ad-hoc network is dynamic topology. The basic rules is that a new node whenever enters into an ad-hoc network, must announce its arrival and presence and should also listen to similar announcement broadcasts made by other mobile nodes.



1. Pro-active routing protocols:
These are also known as table-driven routing protocols. Each mobile node maintains a separate routing table which contains the information of the routes to all the possible destination mobile nodes.

Since the topology in the mobile ad-hoc network is dynamic, these routing tables are updated periodically as and when the network topology changes. It has a limitation that is doesn't work well for the large networks as the entries in the routing table becomes too large since they need to maintain the route information to all possible nodes.

1. **Destination Sequenced Distance Vector Routing Protocol (DSDV):**
   It is a pro-active/table driven routing protocol. It actually extends the distance vector routing protocol of the wired networks as the name suggests. It is based on the Bellman-ford routing algorithm. Distance vector routing protocol was not suited for mobile ad-

hoc networks due to count-to-infinity problem. Hence, as a solution Destination Sequenced Distance Vector Routing Protocol (DSDV) came into picture.

Destination sequence number is added with every routing entry in the routing table maintained by each node. A node will include the new update in the table only if the entry consists of the new updated route to the destination with higher sequence number.

2. **Global State Routing (GSR):**
   It is a pro-active/table driven routing protocol. It actually extends the link state routing of the wired networks. It is based on the Dijkstra's routing algorithm. Link state routing protocol was not suited for mobile ad-hoc networks because in it, each node floods the link state routing information directly into the whole network i.e. Global flooding which may lead to the congestion of control packets in the network.

   Hence, as a solution Global State Routing Routing Protocol (GSR) came into the picture. Global state routing doesn't flood the link state routing packets globally into the network. In GSR, each of the mobile node maintains one list and three tables namely, adjacency list, topology table, next hop table and distance table.

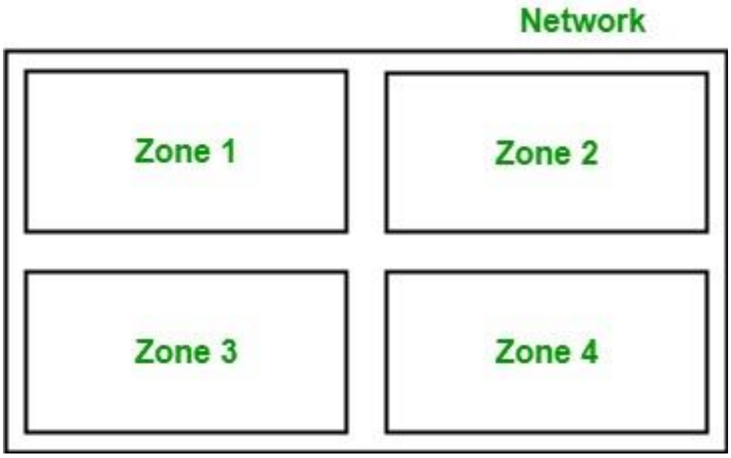
3. **Reactive routing protocols:**
   These are also known as on-demand routing protocol. In this type of routing, the route is discovered only when it is required/needed. The process of route discovery occurs by flooding the route request packets throughout the mobile network. It consists of two major phases namely, route discovery and route maintenance.

1. **Dynamic Source Routing protocol (DSR):**
   It is a reactive/on-demand routing protocol. In this type of routing, the route is discovered only when it is required/needed. The process of route discovery occurs by flooding the route request packets throughout the mobile network.
   It consists of two phases:
   - **Route Discovery:**
     This phase determines the most optimal path for the transmission of data packets between the source and the destination mobile nodes.

- **Route Maintenance:**
  This phase performs the maintenance work of the route as the topology in the mobile ad-hoc network is dynamic in nature and hence, there are many cases of link breakage resulting in the network failure between the mobile nodes.

2. **Ad-Hoc On Demand Vector Routing protocol (AODV):**
   It is a reactive/on-demand routing protocol. It is an extension of dynamic source routing protocol (DSR) and it helps to remove the disadvantage of dynamic source routing protocol. In DSR, after route discovery, when the source mobile node sends the data packet to the destination mobile node, it also contains the complete path in its header. Hence, as the network size increases, the length of the complete path also increases and the data packet's header size also increases which makes the whole network slow.
   Hence, Ad-Hoc On Demand Vector Routing protocol came as solution to it. The main difference lies in the way of storing the path, AODV stores the path in the routing table whereas DSR stores it in the data packet's header itself. It also operates in two phases in the similar fashion: Route discovery and Route maintenance.

3. Hybrid Routing protocol:
It basically combines the advantages of both, reactive and pro-active routing protocols. These protocols are adaptive in nature and adapts according to the zone and position of the source and destination mobile nodes. One of the most popular hybrid routing protocol is **Zone Routing Protocol (ZRP)**.
The whole network is divided into different zones and then the position of source and destination mobile node is observed. If the source and destination mobile nodes are present in the same zone, then proactive routing is used for the transmission of the data packets between them. And if the source and destination mobile nodes are present in different zones, then reactive routing is used for the transmission of the data packets between them.



proactive routing protocols Proactive protocols perform routing operations between all source destination pairs periodically, irrespective of the need of such routes. These protocols attempt to maintain shortest path routes by using periodically updated views of the network topology. These are typically maintained in routing tables in each node and updated with the acquisition of new information. Proactive protocols have the advantage of providing lower latency in data delivery and the possibility of supporting applications that have quality-of-service constraints. Their main disadvantage is due to the wastage of bandwidth in sending update packets periodically even when they are not necessary, such as when there are no link breakages or when only a few routes are needed Examples of Proactive MANET Protocols include: Optimized Link State Routing (OLSR), Fish-eye State Routing (FSR), DestinationSequenced Distance Vector (DSDV) etc. B. Reactive routing protocols Reactive protocols are designed to minimize routing overhead. Instead of tracking the changes in the network topology to continuously maintain shortest path routes to all destinations, these protocols determine routes only when necessary. Typically, these protocols perform a route discovery operation between the source and the desired destination when the source needs to send a data packet and the route to the destination is not known. As long as a route is live, reactive routing protocols only perform route maintenance operations and resort to a new route discovery only when the existing one breaks. The advantage of this ondemand operation is that it usually has a much lower average routing overhead in comparison to proactive protocols. However, it has the disadvantage that a route discovery may involve flooding the entire network with query packets. Flooding is wasteful, which can be required quite frequently in case of high mobility or when there

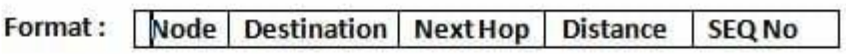
are a large number of active source-destination pairs. Moreover, route discovery adds to the latency in packet delivery as the source has to wait till the route is determined before it can transmit. Despite these drawbacks, on-demand protocols receive comparatively more attention than proactive routing protocols, as the bandwidth advantage makes them more scalable.

Destination Sequenced Distance Vector Routing (DSDV) : Introduction

- **Destination Sequenced Distance Vector Routing protocol is a modified version of Bellman Ford Algorithm and is based upon the concepts of Distance Vector Routing.**
- **In Distance Vector Routing(DVR), each node broadcasts a table containing its distance from nodes which are directly connected and based upon this, other nodes broadcasts the updated routing. Those nodes which are unreachable directly are labelled as “infinite”.**
- **But, this updation of routing tables keeps on happening and an infinite loop is generated which is commonly known as Count-To-Infinity problem.**
- **To overcome this problem of count to infinity by generating sequence number in the routing table, every time the routing table is updated. The process of DSDV is same as that of Distance Vector Routing but an extra attribute of sequence number is added.**

Destination Sequenced Distance Vector Routing : Concept

- **DSDV protocol uses and maintains a single table only, for every node individually. The table contains the following attributes.**
    - **Routing Table : It contains the distance of a node from all the neighboring nodes along with the sequence number(SEQ No means the time at which table is updated).**



Format :

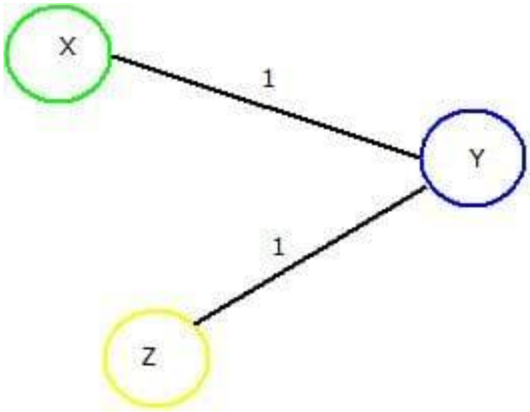
Node	Destination	Next Hop	Distance	SEQ No

Destination Sequenced Distance Vector Routing : Format

- This table is updated on every step and ensures that each node broadcast as well as receives correct information about all the nodes including their distance and sequence number.

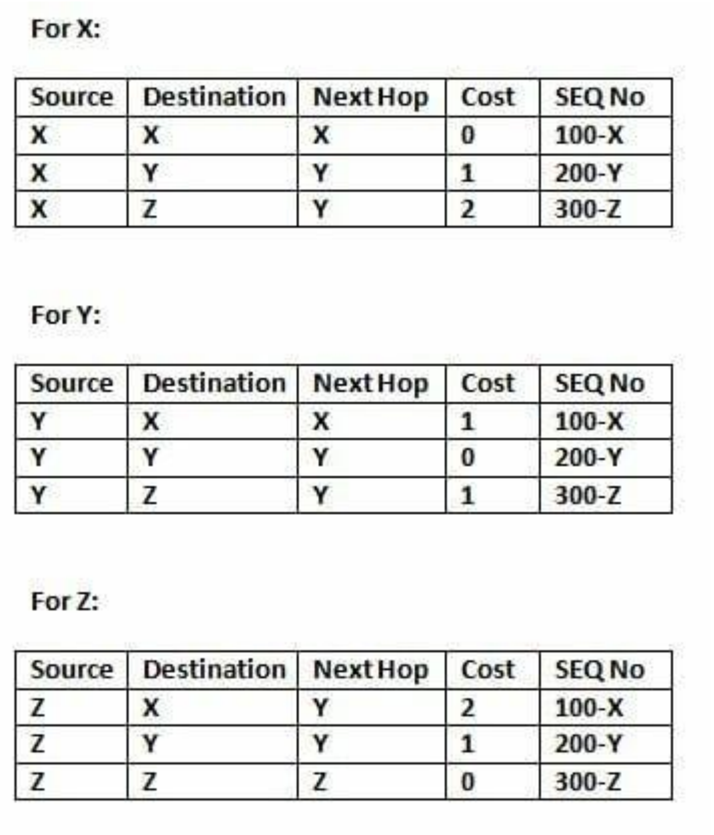
Destination Sequenced Distance Vector Routing Protocol : Working

- In DSDV, nodes broadcasts their routing tables to immediate neighbors with the sequence number. Every time any broadcasting occurs, the sequence number is also updated along with distances of nodes.
- Consider a network of 3 nodes having distances of “1” on each of the edges respectively. Below mentioned steps will let you know how DSDV works and routing tables are updated.



Destination Sequenced Distance Vector Routing : Sample Network

- Step-1: Draw separate tables for all the nodes “X”, “Y” & “ Z” along with the distance and sequence number.



For X:

Source	Destination	Next Hop	Cost	SEQ No
X	X	X	0	100-X
X	Y	Y	1	200-Y
X	Z	Y	2	300-Z

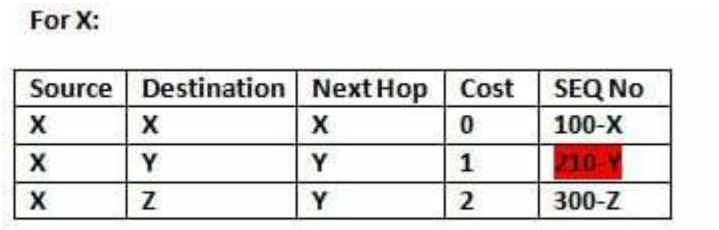
For Y:

Source	Destination	Next Hop	Cost	SEQ No
Y	X	X	1	100-X
Y	Y	Y	0	200-Y
Y	Z	Y	1	300-Z

For Z:

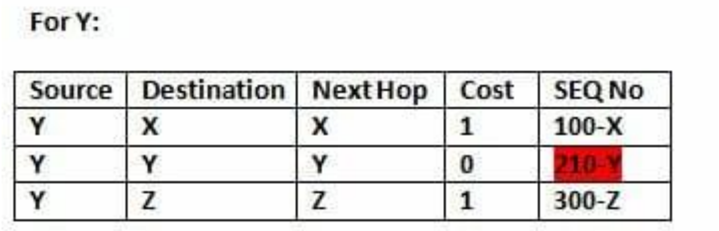
Source	Destination	Next Hop	Cost	SEQ No
Z	X	Y	2	100-X
Z	Y	Y	1	200-Y
Z	Z	Z	0	300-Z

- **If "Y" wants to broadcast the routing table. Then updated routing tables of all the nodes in the network will look like as depicted in the below tables where red marked cell denotes the change in sequence number.**



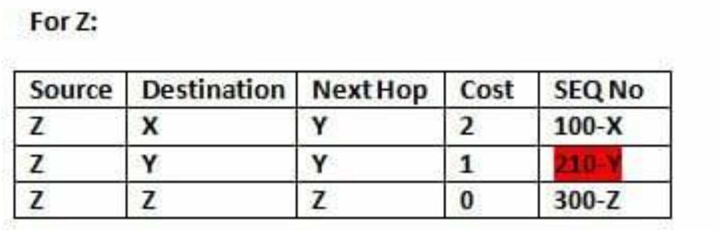
For X:

Source	Destination	Next Hop	Cost	SEQ No
X	X	X	0	100-X
X	Y	Y	1	210-Y
X	Z	Y	2	300-Z



For Y:

Source	Destination	Next Hop	Cost	SEQ No
Y	X	X	1	100-X
Y	Y	Y	0	210-Y
Y	Z	Z	1	300-Z



For Z:

Source	Destination	Next Hop	Cost	SEQ No
Z	X	Y	2	100-X
Z	Y	Y	1	210-Y
Z	Z	Z	0	300-Z

Advantages : Destination Sequenced Distance Vector Routing Protocol

- **Can’t be implemented commercially or on larger scale.**
- **Efficient results will be produced if applied on small networks.**

Disadvantages : Destination Sequenced Distance Vector Routing Protocol

- **Slower protocol processing time.**
- **Less bandwidth.**
- **Not suitable for large number of networks which are dynamic in nature.**

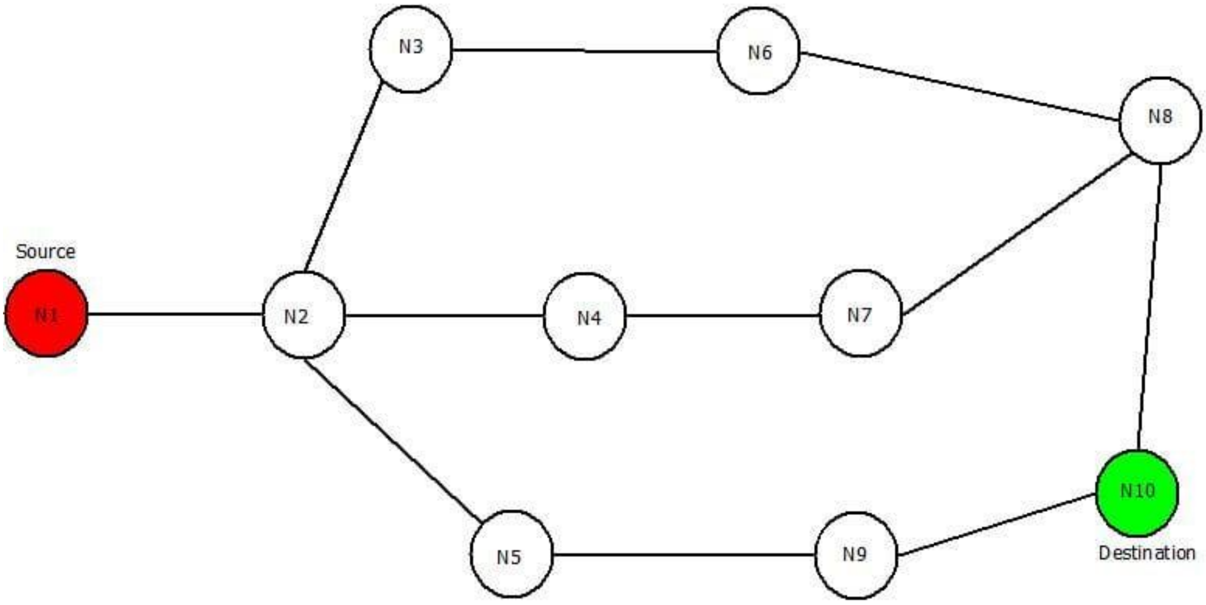
Dynamic Source Routing : Introduction

- **Dynamic Source Routing (DSR) comes under the reactive routing protocol category, as it is capable of discovering the route from source to destination only when required and needed.**
- **Dynamic Source Routing protocol uses a process called “Route Discovery Mechanism” that is capable of discovering the route for data packets from source node to destination nodes using intermediate nodes.**

- **As like proactive routing protocols such as Global State Routing an Dynamic Sequence Distance Vector Routing no separate table is maintained.**
- **The major change in DSR as compare to GSR and DSDV is, in DSDV after asking a requirement of route from source to destination, path via intermediate nodes is checked for its length. Then a “Re-Request” packet is sent back from destination to source via the smallest route possible in the whole network. The “Re-Request” packet does contains its unique ID also.**
- **This process of separately sending a “Re-Request” packet from destination to source makes it easier for the sender to send the data packets on fixed path rather than sending it on multiple paths to check for total distance.**

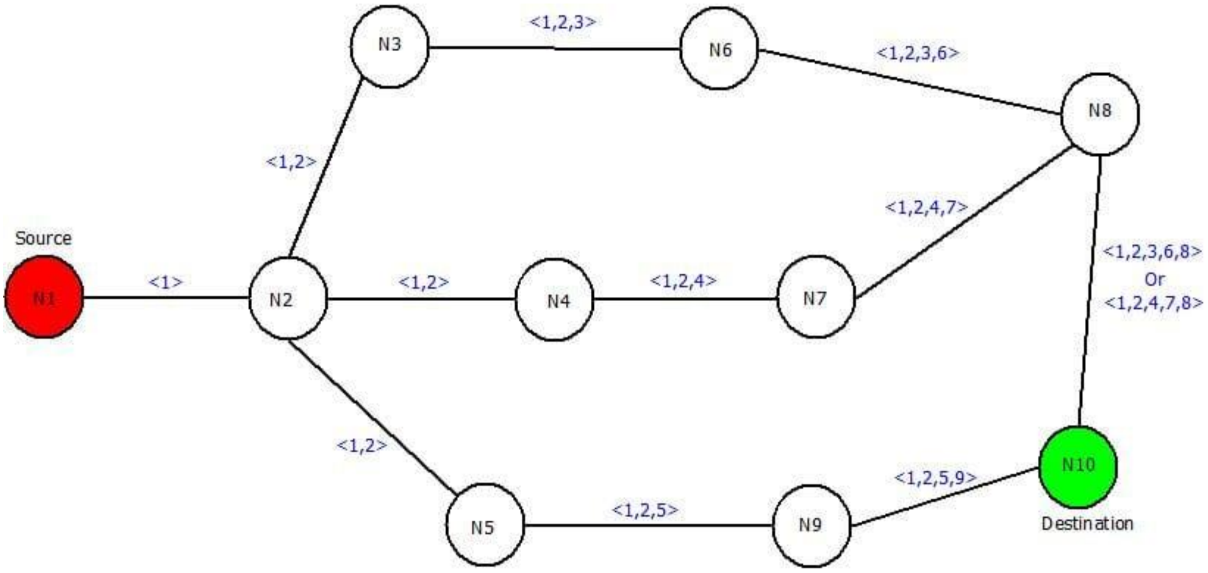
Dynamic Source Routing Protocol : Working

- **Dynamic Source Routing does broadcast the route to its neighbors but does not floods the information. It only trace the route by calculating the total distance or by calculating the number of nodes present in between source and destination nodes.**
- **Consider a network containing 10 nodes where node N1 being the source and node N10 being the destination nodes. Below mentioned steps will let you know how DSR protocol works and how Re-Request packet is transmitted through the network.**



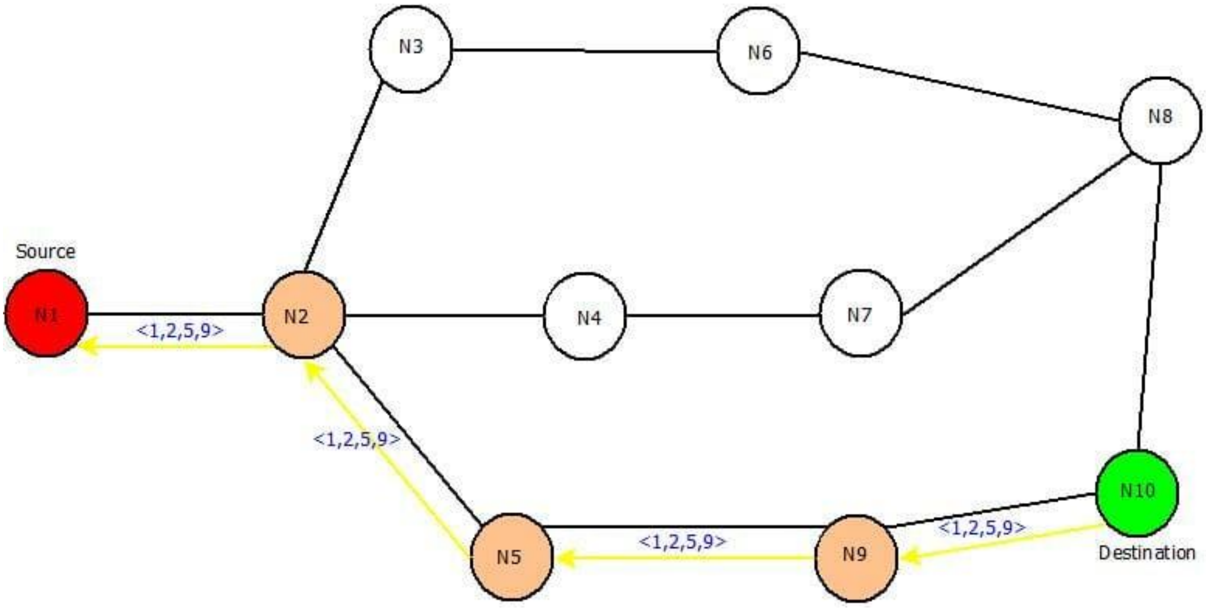
Dynamic Source Routing : Network

- **Step 1: Start from source node N1 and broadcast the information about it to its neighbors i.e. in this case the route information is "<1>", because of its one-to-one link between node N1 and N2.**
- **Step 2: Broadcast previous route information to neighbors of node N2 i.e. to node N3, N4, N5. The new route will remain same "<1,2>" in all the cases.**
- **Step 3: Take node N3 and broadcast previous route(<1,2>) to next neighboring nodes i.e. node N6. New route till node N6 will be "<1,2,3>" and same process can be done for other nodes i.e. Node N4 and N5.**
- **Step 4 : Further, broadcast the new routes i.e. <1,2,3,6> , <1,2,4> , <1,2,5> to nodes N8, N7 & N9 respectively.**
- **Step 5: Repeat the above steps until destination node is reached via all the routes.**
- **The updated routes will be as:**



Dynamic Source Routing : Updated Network

- **After this, “Re-Request” packet will be sent in backward direction i.e. from destination node “N10” to source node “N1”. It will trace the shortest route by counting the number of nodes from route discovered in previous steps.**
- **The three possible routes are :**
    - **Route 1: <1,2,3,6,8>**
    - **Route 2: <1,2,4,7,8>**
    - **Route 3: <1,2,5,9>**
- **Route 3 i.e. "<1,2,5,9>” will be chosen as it contains the least number of nodes and hence it will definitely be the shortest path and then data can be transferred accordingly.**
- **The Re-Request Packet route can be located as:**



Dynamic Source Routing

Advantages : Dynamic Source Routing Protocol

- **A perfect route is discovered always.**
- **Highly efficient.**
- **Low bandwidth Consumption.**

Disadvantages : Dynamic Source Routing Protocol

- **If the route gets broke, data transmission cannot happen.**
- **Time taking algorithm-Slow.**
- **If network is large , then it is impossible for the data packets header to hold whole information of the routes.**

Ad hoc On-Demand Distance Vector (AODV) Routing

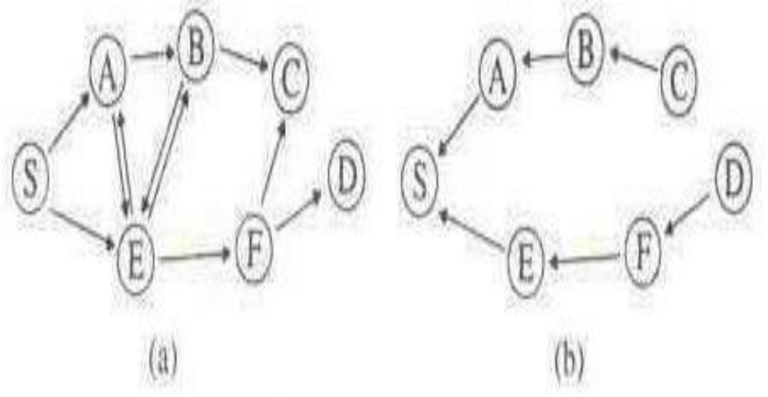
Ad Hoc on Demand Distance Vector (AODV) The ad hoc on-demand distance-vector (AODV) routing protocol is an on-demand routing protocol; all routes are discovered only when needed, and are maintained only as long as they are being used. Routes are discovered through a route discovery cycle, whereby the network nodes are queried in search of a route to the destination node. When a node with a route to the destination is discovered, that route is reported back to the source node that requested the route the following sections describe the features of AODV that allow it to discover and maintain loop free route.

Route Discovery

When a source node has data packets to send to some destination, it checks its routing table to determine whether it already has a route to that destination. If so, it can then utilize that route to transmit the data packets. Otherwise, the node must perform a route discovery procedure to determine a route to the destination. To initiate route discovery, the source node creates a Route Request (RREQ) packet. In that packet the node places the IP address of the destination, the last known sequence number for the destination, its own IP address, its current sequence number, and a hop count that is initialized to zero. If there is no last known sequence number for the destination, it sets this value to zero. The source then broadcasts the RREQ to its neighbors. When a neighboring node, or any other more distant node, receives the RREQ, it first increments the hop count value in the RREQ and creates a reverse route entry in its routing table for both the source node and the node from which it received the request. In this way, if the node later receives a RREP to forward to the source, it will know a path to the source along which it can forward the RREP. After creating this entry, the node then determines its response to the request. The node can send a reply to the request if it either

- is the destination, or
- has a current route to the destination.

A current route is an unexpired route entry for the destination whose sequence number is at least as great as that contained in the RREQ. If this condition holds, the node creates a Route Reply (RREP) for the destination node. Otherwise, if the node does not have a current route to the destination, it simply rebroadcasts the RREQ to its neighbors. Fig. 1.1(a) illustrates the flooding of a RREQ, originating at the source node S, through the network. In this example, we assume nodes C and D have routes to the destination D. A node creates a RREP by placing the IP address of the destination node, as well as its record of the destination’s sequence number, into the RREP. It also includes the source node IP address and it distance, in hops, to the destination. The node then unicasts the RREP to the next hop towards the source node. In Fig 1.1(b), both nodes C and D have routes to the destination D that meet the reply criteria. Hence, both nodes generate a RREP.



Route Discovery 1.1 (a) RREQ broadcast and (b) RREP propagation. When the next hop receives the RREP, it first increments the hop count value in the RREP and then creates a forward route entry to both the destination node and the node from which it received the reply. This ensures that all nodes along the path will know the route to the destination in the event that the source selects this route for data packet transmission. The node then unicasts the RREP to its next hop towards the source node. This hop-by-hop forwarding continues until the RREP reaches the source. Once the source receives a RREP, it can begin using that path for data packet transmission. In the event that the source receives multiple RREPs along different paths, it selects the route with the greatest destination sequence number and the smallest hop count for communication with the destination.

Route discovery operations often require processing and communications capacity at every node in the ad hoc network. For this reason, we often describe the discovery operation as ―flooding‖ even though the RREQs are only locally broadcast messages. Since the messages are changed at each hop by AODV processing, we could not use any system-wide broadcast or multicast address. Nevertheless, it is of great importance to use careful broadcast techniques to minimize any spurious retransmission of RREQ packets.

For instance, each node is required to keep track of which RREQ messages it has received, and to discard duplicates that it receives from multiple neighboring nodes. In order to detect duplication, the node identifies each RREQ by using the IP address of the originating node, and the RREQ ID for the RREQ message data. In Fig 1.1(a), by this algorithm node E would discard RREQs it hears from nodes A, B, and F after receiving the original RREQ from the source S. These identifying values have to be stored for a time that is long enough to ensure no other node in the ad hoc network could still be processing messages resulting from the same route discovery operation. It is difficult to predict how long this time is, because it depends on the present state of congestion in the network as well as the size and current topology of the network. For correctness, it is better to maintain the broadcast identification information for few minutes.

3oute maintenance

In an ad hoc network, links are likely to break due to the mobility of the nodes and the ephemeral nature of the wireless channel. Hence, there must be a mechanism in place to repair routes when links within active routes break. An active route is defined to be a route that has recently been utilized for the transmission of data packets. When such a link break occurs, the node upstream of the break (i.e., the node closer to the source node), invalidates in its routing table all destinations that become unreachable due to the loss of the link. It then creates a Route Error (RERR) message, in which it lists each of these lost destinations. The node sends the RERR upstream towards the source node. If there are multiple previous hops that were utilizing this link, the node broadcasts the RERR; otherwise, it is unicast. In Fig. 1.2, the link between nodes B and C on the path from S to D is broken.
Node B invalidates its route table entries for both nodes C and D, creates a RERR message listing these nodes, and sends the RERR upstream towards the source.

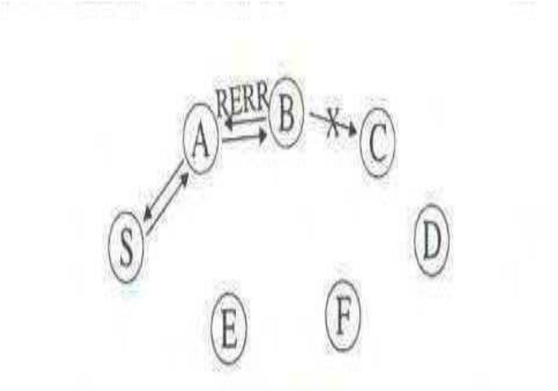


Figure 1.2 Link breaks Notification

When a node receives a RERR, it first checks whether the node that sent the RERR is its next hop to any of the destinations listed in the RERR. If the sending node is the next hop to any of these destinations, the node invalidates these routes in its route table and then propagates the RERR back towards the source. The RERR continues to be forwarded in this manner until it is received by the source. Once the source receives the RERR, it can re-initiate route discovery if it still requires the route

The Zone Routing Protocol

Motivation

As seen, proactive routing uses excess bandwidth to maintain routing information, while reactive routing involves long route request delays. Reactive routing also inefficiently floods the entire network for route determination. The Zone Routing Protocol (ZRP) [11]– [13] aims to address the problems by combining the best properties of both approaches. ZRP can be classed as a hybrid reactive/proactive routing protocol. [10]

In an ad-hoc network, it can be assumed that the largest part of the traffic is directed to nearby nodes. Therefore, ZRP reduces the proactive scope to a zone centered on each node. In a limited zone, the maintenance of routing information is easier. Further, the amount of routing information that is never used is minimized. Still, nodes farther away can be reached with reactive routing. Since all nodes proactively store local routing information, route requests can be more efficiently performed without querying all the network nodes. [10]

Despite the use of zones, ZRP has a flat view over the network. In this way, the organizational overhead related to hierarchical protocols can be avoided. Hierarchical routing protocols depend on the strategic assignment of gateways or landmarks, so that every node can access all levels, especially the top level. Nodes belonging to different subnets must send their communication to a subnet that is common to both nodes. This may congest parts of the network. ZRP can be categorized as a flat protocol because the zones overlap. Hence, optimal routes can be detected and network congestion can be reduced. [15]

Further, the behavior of ZRP is adaptive. The behavior depends on the current configuration of the network and the behavior of the users. [10]

Architecture

The Zone Routing Protocol, as its name implies, is based on the concept of zones. A routing zone is defined for each node separately, and the zones of neighboring nodes overlap. The routing zone has a radius ρexpressed in hops. The zone thus includes the nodes, whose distance from the node in question is at most ρhops. An example routing zone is shown in Figure 1, where the routing zone of S includes the nodes A–I, but not K. In the illustrations, the radius is marked as a circle around the node in question. It should however be noted that the zone is defined in hops, not as a physical distance. [10]

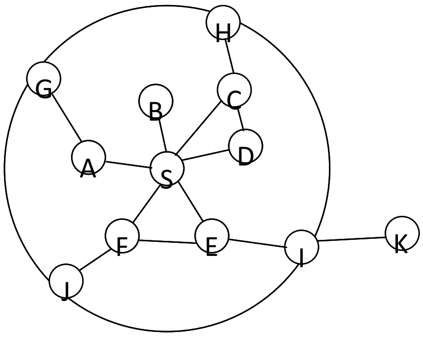


Figure 1: Example routing zone withρ=*2*

The nodes of a zone are divided into peripheral nodes and interior nodes. Peripheral nodes are nodes whose minimum distance to the central node is exactly equal to the zone radius ρ. The nodes whose minimum distance is less than ρare interior nodes. In Figure 1, the nodes A–F are interior nodes, the nodes G–J are peripheral nodes and the node K is outside the routing zone. Note that node H can be reached by two paths, one with length 2 and one with length 3 hops. The node is however within the zone, since the shortest path is less than or equal to the zone radius. [10] [11]

The number of nodes in the routing zone can be regulated by adjusting the transmission power of the nodes. Lowering the power reduces the number of nodes within direct reach and vice versa. The number of neighboring nodes should be sufficient to provide adequate reachability and redundancy. On the other hand, a too large coverage results in many zone members and the update traffic becomes excessive. Further, large transmission coverage adds to the probability of local contention. [10]

ZRP refers to the locally proactive routing component as the IntrA-zone Routing Protocol (IARP). The globally reactive routing component is named IntEr-zone Routing Protocol (IERP). IERP and IARP are not specific routing protocols. Instead, IARP is a family of limited-depth, proactive link-state routing protocols. IARP maintains routing information for nodes that are within the routing zone of the node. Correspondingly, IERP is a family of reactive routing protocols that offer enhanced route discovery and route maintenance services based on local connectivity monitored by IARP. [11] [12]

The fact that the topology of the local zone of each node is known can be used to reduce traffic when global route discovery is needed. Instead of broadcasting packets, ZRP uses a concept called *bordercasting*. Bordercasting utilizes the topology information provided by IARP to direct query request to the border of the zone. The bordercast packet delivery service is provided by the Bordercast Resolution Protocol (BRP). BRP uses a map of an extended routing zone to construct bordercast trees for the query packets. Alternatively, it uses source routing based on the normal routing zone. By employing *query control* mechanisms, route requests can be directed away from areas of the network that already have been covered. [13]

In order to detect new neighbor nodes and link failures, the ZRP relies on a Neighbor Discovery Protocol (NDP) provided by the Media Access Control (MAC) layer. NDP transmits “HELLO” beacons at regular intervals. Upon receiving a beacon, the neighbor table is updated. Neighbors, for which no beacon has been received within a specified time, are removed from the table. If the MAC layer does not include a NDP, the functionality must be provided by IARP. [14]

The relationship between the components is illustrated in Figure 2. Route updates are triggered by NDP, which notifies IARP when the neighbor table is updated. IERP uses the routing table of IARP to respond to route queries. IERP forwards queries with BRP. BRP uses the routing table of IARP to guide route queries away from the query source. [15]

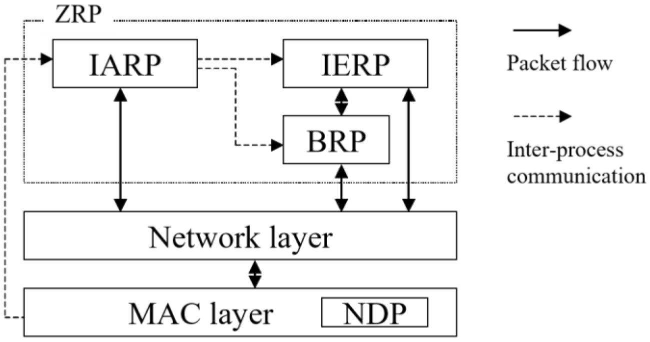


Figure 2: ZRP architecture

Routing

A node that has a packet to send first checks whether the destination is within its local zone using information provided by IARP. In that case, the packet can be routed proactively. Reactive routing is used if the destination is outside the zone. [13]

The reactive routing process is divided into two phases: the *route request* phase and the *route reply* phase. In the route request, the source sends a route request packet to its peripheral nodes using BRP. If the receiver of a route request packet knows the destination, it responds by sending a route reply back to the source. Otherwise, it continues the process by bordercasting the packet. In this way, the route request spreads throughout the network. If a node receives several copies of the same route request, these are considered as redundant and are discarded [12], [13]

The reply is sent by any node that can provide a route to the destination. To be able to send the reply back to the source node, routing information must be accumulated when the request is sent through the network. The information is recorded either in the route request packet, or as next-hop addresses in the nodes along the path. In the first case, the nodes forwarding a route request packet append their address and relevant node/link metrics to the packet. When the packet reaches the destination, the sequence of addresses is reversed and copied to the route reply packet. The sequence is used to forward the reply back to the source. In the second case, the forwarding nodes records routing information as next-hop addresses, which are used when the reply is sent to the source. This approach can save transmission resources, as the request and reply packets are smaller. [12]

The source can receive the complete source route to the destination. Alternatively, the nodes along the path to the destination record the next-hop address in their routing table. [12]

In the bordercasting process, the bordercasting node sends a route request packet to each of its peripheral nodes. This type of one-to-many transmission can be implemented as multicast to reduce resource usage. One approach is to let the source compute the multicast tree and attach routing instructions to the packet. This is called Root-Directed Bordercasting (RDB). Another approach is to reconstruct the tree at each node, whereas the routing instructions can be omitted. This requires that every interior node knows the topology seen by the bordercasting node. Thus, the nodes must maintain an extended routing zone with radius $2\rho\text{-}1$ hops. Note that in this case the peripheral nodes where the request is sent are still at the distance ρ. This approach is named Distributed Bordercasting (DB). [13] [15]

The zone radius is an important property for the performance of ZRP. If a zone radius of one hop is used, routing is purely reactive and bordercasting degenerates into flood searching. If the radius approaches infinity, routing is reactive. The selection of radius is a tradeoff between the routing efficiency of proactive routing and the increasing traffic for maintaining the view of the zone. [12]

Route maintenance

Route maintenance is especially important in ad-hoc networks, where links are broken and established as nodes move relatively to each other with limited radio coverage. In purely reactive routing protocols, routes containing broken links fail and a new route discovery or route repair must be performed. Until the new route is available, packets are dropped or delayed. [12]

In ZRP, the knowledge of the local topology can be used for route maintenance. Link failures and sub-optimal route segments within one zone can be bypassed. Incoming packets can be directed around the broken link through an active multi-hop path. Similarly, the topology can be used to shorten routes, for example, when two nodes have moved within each other's radio coverage. For source-routed packets, a relaying node can determine the closest route to the destination that is also a neighbor. Sometimes, a multi-hop segment can be replaced by a single hop. If next-hop forwarding is used, the nodes can make locally optimal decisions by selecting a shorter path. [12]

Example

Consider the network in Figure 3. The node S has a packet to send to node X. The zone radius is ρ=*2*. The node uses the routing table provided by IARP to check whether the destination is within its zone. Since it is not found, a route request is issued using IERP. The request is bordercast to the peripheral nodes (gray in the picture). Each of these searches their routing table for the destination.

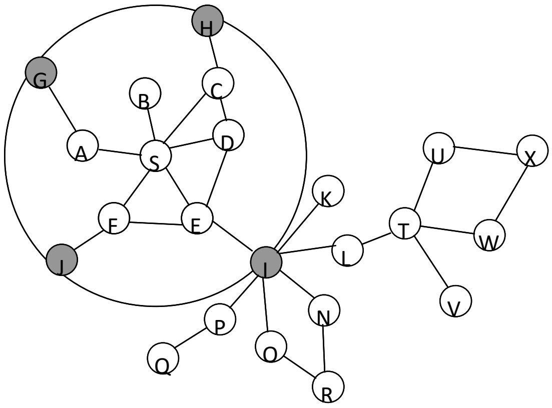


Figure 3: The routing zone of node S

Node I does not find the destination in its routing table. Consequently, it broadcasts the request to its peripheral nodes, shown in gray in Figure 4. Due to query control mechanisms, the request is not passed back to nodes D, F and S.

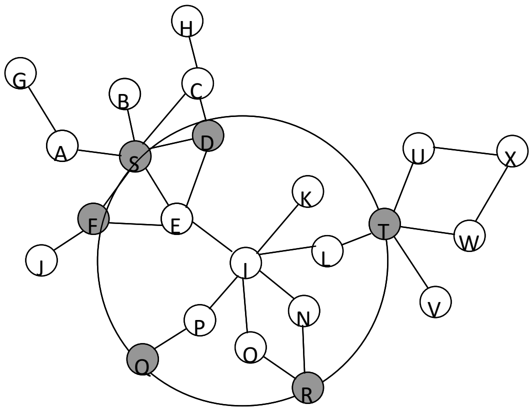


Figure 4: The routing zone of node I

Finally, the route request is received by node T, which can find the destination in its routing zone, shown in Figure 5. Node T appends the path from itself to node X to the path in the route request. A route reply, containing the reversed path is generated and sent back to the source node. If multiple paths to the destination were available, the source would receive several replies.

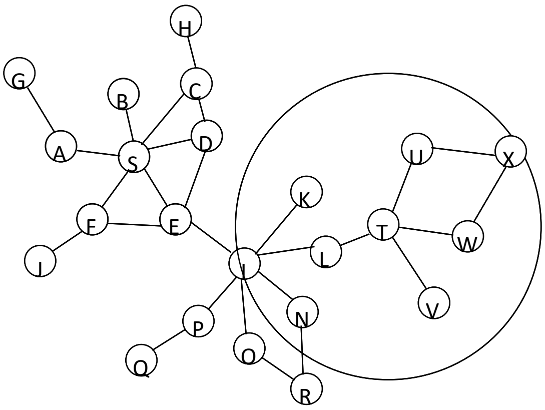


Figure 5: The routing zone of node TS

Reg. No ……………………………….

[17BECS6E02]

KARPAGAM ACADEMY OF HIGHER EDUCATION

(Under Section 3 of UGC Act 1956)

COIMBATORE-641 021

(For the candidates admitted from 2017 onwards) – FULL TIME

B.E DEGREE EXAMINATION, APRIL 2020

COMPUTER SCIENCE AND ENGINEERING

NETWORK ROUTING ALGORITHMS

Time : 3 Hours **Max marks:100 Marks**

PART – A (20 x 1 = 20 Marks)

(Question no. 1 to 20 Online Examinations)

1. In Unicast Routing, If instability is between three nodes, stability cannot be

a) Stablized
b) Reversed
c) Guaranteed
d) Minimized

2. In Unicast Routing, Dijkstra algorithm creates a shortest path tree from a

a) Graph
b) Chart
c) Station
d) Link

3. In Multicast Routing Protocol, flooding is used to broadcast packets but it creates

a) Gaps

b) loops

c) Errors

d) long strings

4. RPF stands for

a) Reverse Path Forwarding

b) Reverse Path Failure

c) Reverse Packet Forwarding

d) Reverse Protocol Failure

5. LSP stands for

a) Link Stable Packet

b) Link State Packet

c) Link State Protocol

d) Link Status Path

6. A network can receive a multicast packet from a particular source only through a

a) Designated parent resolver

b) Designated protocol router

c) Designated parent table

d) Designated parent router

7. In periodic update, a node sends its routing table normally after every

a) 10s

b) 20s

c) 30s

d) 40s

8. To convert broadcasting to multicasting, protocol uses

a) Three Procedures

b) Two Procedures

c) One Procedure

d) Multi Procedures

9. Network layer supervises handling of packets by

a) Physical Networks

b) Data Networks

c) Application Networks

d) Transport Networks

10. Technique to simplify routing is called the

a) Network Method

b) Error-Control Method

c) Route Method

11. Multidestination routing

a) is same as broadcast routing

b) contains the list of all destinations

c) **data is not sent by packets**

d) none of the mentioned

12. A subset of a network that includes all the routers but contains no loops is called

a) **spanning tree**

b) spider structure

c) spider tree

d) none of the mentioned

13. Which one of the following algorithm is not used for congestion control?

a) traffic aware routing

b) admission control

c) load shedding

d) **none of the mentioned**

14. The network layer protocol of internet is

a) ethernet

b**) internet protocol**

c) hypertext transfer protocol

d) none of the mentioned

15. ICMP is primarily used for

a) **error and diagnostic functions**

b) addressing

c) forwarding

d) none of the mentioned

16. For a direct deliver, the …….. flag is on.
a) up
b) host specific
c) **gateway**

d)added by redirection

17. A ………. AS has connections to two or more autonomous systems and carries both local and transit traffic.
a) Stub

b) Multi-homed
c) **Transit**
d) All of the above

18. In unicast routing, each router in the domain has a table that defines a ……… path tree to possible destinations.
a) average
b) longest
c) shortest
d) very longest

19. ………….. supports the simultaneous use of multiple unequal cost paths to a destination.
a) OSPF
b) **EIGRP**
c) BGP
d) RIP

20. In multicast routing, each involved router needs to construct a ……… path tree for each group.
a) average
b) longest
c)**shortest**
d) very longest

PART-B (5x2 = 10 Marks)

Answer ALL the questions

ALL THE QUESTIONS CARRY EQUAL MARKS

21. What is adaptive routing?
22. Define Fairness.
23. What are the two major sub-tasks in Location Management?
24. What is Proactive routing?
25. What is Core Based Tree Routing?

PART-C (5x14 = 70 Marks)

Answer ALL the questions

ALL THE QUESTIONS CARRY EQUAL MARKS

26. a) i) Explain the features of telephone network routing and compare with internet routing. (7)

ii) Explain the function of network layer. (7)

(OR)

b) Explain dynamic non hierarchical routing and Trunk status map routing. (14)

27. a) Discuss in detail about Routing information Protocol. (14)

(OR)

b) Explain Multicast and Multiple Unicast Routing algorithms in detail. (14)

28. a) i) Explain table driven protocol DSDV. (8)

ii) State and explain the classification of routing protocols used in Adhoc network. (6)

(OR)

b) i) What is Light path Migration? Explain. (7)

ii) Explain Distributed Control Protocols. (7)

29. a) Explain HAWAII Infrastructure in detail with an example. (14)

(OR)

b) Discuss the Micro-mobility protocols and its implementation in detail. (14)

30. a) Explain Zone based Routing in detail.
(14)

(OR)

b) Write short notes on Internet based mobile ad-hoc networking communication strategies.
(14)

Prepared By: Dr.R.Dhanapal

: AP/CSE

KARPAGAM ACADEMY OF HIGHER EDUCATION

COIMBATORE-21

Faculty of Engineering

Department of Computer Science and Engineering

ONLINE EXAMINATION

Subject Code	**: 17BECS6E02**		
Name of the Course	**: III B.E CSE**	**Time**	**: 2 hr - 10.00AM to 12.00 PM**
Title of the paper	**: NETWORK ROUTING ALGORITHM**	**Marks**	**: 60 Marks**
Semester	**: VI**	**Date**	**: 02/05/2020**

Instructions

1. The answers to be written in a plain paper scanned and posted in Google Classroom Assignment
2. Answers should be handwritten only.
3. The Time for answering is 10.00 am to 12.00 pm.
4. After completing ,the answers to be scanned and to be uploaded within 12.30pm
5. The Name and Roll no of the student to be written in each paper at the right hand corner of the EACH Paper.
6. The Answer scripts are to be shown when you come to the college for validation.

PART-A (9*2=18 Marks)

Answer the following question

1. What is BOOTP??
2. Define Socket System call?
3. What is meant by TCP/IP?

4. Define Finite State Machine.
5. What is the difference between FTP and TFTP protocol?
6. Discuss about the various data structures used in TCP implementation.
7. What is congestion?
8. Explain the advantages of IPv6 when compared with IPv4?
9. What is mean by TCP allocation and initialization?

PART-B (3*14=42)

ANSWER all the Questions

10. a) Discuss the properties of Routing algorithm and briefly describe any two of the adaptive routing technique with suitable example. (14)

(OR)

b) State the principle of optimality with regards to routing (14)

11. a) What is adaptive routing? With the help of an example explain flow based routing? (14)

(OR)

b) Explain RSVP protocol in detail (14)

12. a) Explain mixed LAN architecture. (14)

(OR)

b) Why is transport layer necessary even if its services are very similar to that of the network layer? (14)

ONLINE 1 MARK QUESTION

1) Alternate and adaptive routing algorithm belongs to ……….
A. static routing
B. permanent routing
C. standard routing
D. dynamic routing
2) ………. protocol is a popular example of a link-state routing protocol.
A. SPF
B. BGP
C. RIP
D. OSPF

3) An example of the routing algorithm is …
A. TELNET
B. TNET
C. ARPANET
D. ARNET

4) The Enhanced Interior Gateway Routing Protocol(EIGRP) is categorized as a ……..
A. Distance vector routing protocols
B. Link state routing protocols
C. Hybrid routing protocols
D. Automatic state routing protocols

5) In ………. routing, the routing table hold the address of just the next hop instead of complete route information.
A. next-hop

. host-specific

C. network-specific

D. default

6) ………. was originally developed to provide a loop-free method of exchanging routing information between autonomous systems.

A. OSPF

B. EIGRP

C. BGP

D. RIP

7) In ………… routing, the destination address is a network address in the routing tables.

A. next-hop

B. host-specific

C. network-specific

D. default

8) Logical partitioning of the network, authentication and faster convergence rate are the advantages of ….

A. OSPF

B. EIGRP

C. BGP

D. RIP

9) The ……… flag indicates the availability of a router.

A. up

B. host-specific

C. gateway

D. added by redirection

10) The types of autonomous system defined by BGP is/are ..

A. Stub

B. Multi-homed

C. Transit

D. All of the above

11) For a direct deliver, the …….. flag is on.

A. up

B. host specific

C. gateway

D. added by redirection

12) A ………. AS has connections to two or more autonomous systems and carries both local and transit traffic.

A. Stub

B. Multi-homed

C. Transit

D. All of the above

13) In unicast routing, each router in the domain has a table that defines a ……… path tree to possible destinations.

A. average

B. longest

C. shortest

D. very longest

14) ………….. supports the simultaneous use of multiple unequal cost paths to a destination.

A. OSPF

B. EIGRP

C. BGP

D. RIP

15) In multicast routing, each involved router needs to construct a ……… path tree for each group.

A. average

B. longest

C. shortest

D. very longest

16) Which of the following is/are the benefits provided by EIGRP?

i) Faster convergence

ii) partial routing updates

iii) High bandwidth utilization

iv) Route summarization

A. i, iii and iv only

B. i, ii and iii only

C. ii, iii and iv only

D. i, ii and iv only

17) In OSPF, a ………. link is a network is connected to only one router.

A. point-to-point

B. transient

C. stub

D. multipoint

18) ……… is the process of consolidating multiple contiguous routing entries into a single advertisement.

A. Faster convergence

B. Partial routing updates

C. Route summarization

D. Multiple protocols

19) In OSPF, when the link between two routers is broken, the administration may create a …….. link between them using a longer path that probably goes through several routers.

A. point-to-point

B. transient

C. stub

D. multipoint

20) ……….. is the process of introducing external routers into an OSPF network.

A. Route redistribution

B. Route summarization

C. Route reintroducing

D. Route recreation

21) Which of the following is not the requirement of routing function?
A. Correctness

B. Robustness
C. Delay time
D. Stability
22) The ……… protocol allows the administrator to assign a cost, called the metric, to each route.
A. OSPF
B. RIP
C. BGP
D. BBGP
23) If there is only one routing sequence for each source destination pair, the scheme is known as …..
A. static routing
B. fixed alternative routing
C. standard routing
D. dynamic routing

24) The Open Shortest Path First(OSPF) protocol is an intra domain routing protocol based on …….. routing.
A. distance vector
B. link state
C. path vector
D. non distance vector
25) An/A ……….routing scheme is designed to enable switches to react to changing traffic patterns on the network.
A. static routing

B. fixed alternative routing
C. standard routing
D. dynamic routing

26) The Routing Information Protocol(RIP) is an intra domain routing based on ……..routing.
A. distance vector
B. link state
C. path vector
D. distance code
27) The term …….. refers to which node or nodes in the network are responsible for the routing decision.
A. decision place
B. routing place
C. node place
D. switching place
28) In ……. routing the least cost route between any two nodes is the minimum distance.
A. path vector
B. distance vector
C. link state
D. switching
29) For centralized routing the decision is made by some designated node called ……
A. designated center
B. control center

C. network center
D. network control center
30) For purposes of routing, the Internet is divided into …….
A. wide area networks
B. autonomous networks
C. local area networks
D. autonomous system

31) In ………. a route is selected for each destination pair of nodes in the network.
A. flooding
B. variable routing
C. fixed routing
D. random routing
32) To create a neighborhood relationship, a router running BGP sends an ………. message.
A. open
B. update
C. keep alive
D. close
33) The technique which requires no network information required is ….
A. flooding
B. variable routing

C. fixed routing
D. random routing
34) An area is ….
A. part of an AS
B. composed of at least two AS
C. another term for an AS
D. composed more than two AS
35) Which of the following produces high traffic network?
A. Variable routing
B. Flooding
C. Fixed routing
D. Random routing

36) In ……….. routing, we assume that there is one node (or more) in each autonomous system that acts on behave of the entire autonomous system.
A. distant vector
B. path vector
C. link state
D. multipoint
37) When a direct delivery is made, both the deliverer and receiver have the same ….
A. routing table
B. host id

C. IP address
D. Net id
38) In OSPF, a ……… link is a network with several routers attached to it.
A. point-to-point
B. transient
C. stub
D. multipoint
39) In ……. routing, the mask and the destination address are both 0.0.0.0 in routing table.
A. next-hop
B. host-specific
C. network-specific
D. default
40) In ……… the router forwards the receive packet through only one of its interfaces.
A. unicasting
B. multicasting
C. broadcasting
D. point to point