R.M.K GROUP OF ENGINEERING INSTITUTIONS

R.M.K
GROUP OF INSTITUTIONS

R.M.K
GROUP OF
INSTITUTIONS

Please read this disclaimer before proceeding:

This document is confidential and intended solely for the educational purpose of RMK Group of Educational Institutions. If you have received this document through email in error, please notify the system manager. This document contains proprietary information and is intended only to the respective group / learning community as intended. If you are not the addressee you should not disseminate, distribute or copy through e-mail. Please notify the sender immediately by e-mail if you have received this document by mistake and delete this document from your system. If you are not the intended recipient you are notified that disclosing, copying, distributing or taking any action in reliance on the contents of this information is strictly prohibited.

R.M.K
GROUP OF
INSTITUTIONS

DIGITAL NOTES
ON
20CS501
COMPUTER NETWORKS

Department : Computer Science and Engineering

Batch/Year : 2020-2024/III

Created by : Ms.Srijayanthi,AP/ADS

Ms. K.RAMYA DEVI,AP/CSE

Mr. KINGSLEY,AP/CSE

Date : 10.08.2022

R.M.K GROUP OF INSTITUTIONS

Table of Contents

R.M.K GROUP OF INSTITUTIONS

COURSE OBJECTIVES

- To understand the protocol layering and physical level communication.
- To analyze the performance of a network.
- To understand the various components required to build different
- networks. To learn the functions of network layer and the various routing
- protocols.

  To familiarize the functions and protocols of the Transport layer.

PREREQUISITE

- IT8201 INFORMATION TECHNOLOGY ESSENTIALS
- EC8394 ANALOG AND DIGITAL COMMUNICATION

SYLLABUS

20CS501 COMPUTER NETWORKS 3 0 0 3

UNIT I INTRODUCTION AND PHYSICAL LAYER 9

Data Communications – Network Types – Protocol Layering – Network Models (OSI, TCP/IP) Networking Devices: Hubs, Bridges, Switches – Performance Metrics – Transmission media - Guided media -Unguided media- Switching- Circuit Switching - Packet Switching.

UNIT II DATA-LINK LAYER & MEDIA ACCESS 11

Introduction – Link-Layer Addressing- Error Detection and Correction - DLC Services – Data Link Layer Protocols – HDLC – PPP - Wired LANs: Ethernet - Wireless LANs – Introduction – IEEE 802.11, Bluetooth

UNIT III NETWORK LAYER 9

Network Layer Services – Packet switching – Performance – IPV4 Addresses – Forwarding of IP Packets - Network Layer Protocols: IP, ICMP v4 – Unicast Routing Algorithms – Protocols – Multicasting Basics – IPV6 Addressing – IPV6 Protocol.

UNIT IV TRANSPORT LAYER 8

Introduction – Transport Layer Protocols – Services – Port Numbers – User Datagram Protocol –Transmission Control Protocol – SCTP.

UNIT V APPLICATION LAYER 8

Application layer-WWW and HTTP – FTP – Email –Telnet –SSH – DNS – SNMP.

Course Outcomes

Course Code	Course Outcome Statement	Cognitive/ Affective Level of the Course Outcome	Expected Level of Attainment
Course Outcome Statements in Cognitive Domain			
C302.1	Explain the basic layers and its functions, and transmission media in computer networks	Understand K2	60%
C302.2	Examine the performance of different types of networks	Analyse K4	60%
C302.3	Inspect the functionalities of data link and media access control protocols	Analyse K4	60%
C302.4	Examine different routing algorithms	Analyse K4	60%
C302.5	Identify appropriate protocol to be used at the transport layer	Apply K3	60%
C302.6	Explain the working of various application layer protocols.	Understand K2	60%
Course Outcome Statements in Affective domain			
C302.7	Attend the classes regularly	Respond (A2)	95%
C302.8	Submit the Assignments regularly.	Respond (A2)	95%
C302.9	Participation in Seminar/Quiz/ Group Discussion/ Collaborative learning and content beyond syllabus	Valuing (A3)	95%

CO- PO/PSO Mapping

Overall Correlation Matrix of the Course as per Curriculum

Course Code	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
C302	3	1	2									

Correlation Matrix of the Course Outcomes to Programme Outcomes and Programme Specific Outcomes Including Course Enrichment Activities

Course Outcomes (COs)		Programme Outcomes (POs), Programme Specific Outcomes (PSOs)													
		PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
		K3	K4	K5	K5	K3/K5	A2	A3	A3	A3	A3	A3	A2	K3	K3	K3
C302.1	K2	2	1											2	2	2
C302.2	K4	3	3	2	2									3	3	3
C302.3	K4	3	3	2	2									3	3	3
C302.4	K4	3	2	2	2									3	3	3
C302.5	K3	3	2	1	1									3	3	3
C302.6	K2	2	1											2	2	2
C302.7	A2												3			
C302.8	A2								2	2	2		3			
C302.9	A3						3	3		3	3		3			
C302		3	3	2	2		1	1	1	3	3		3	3	3	3

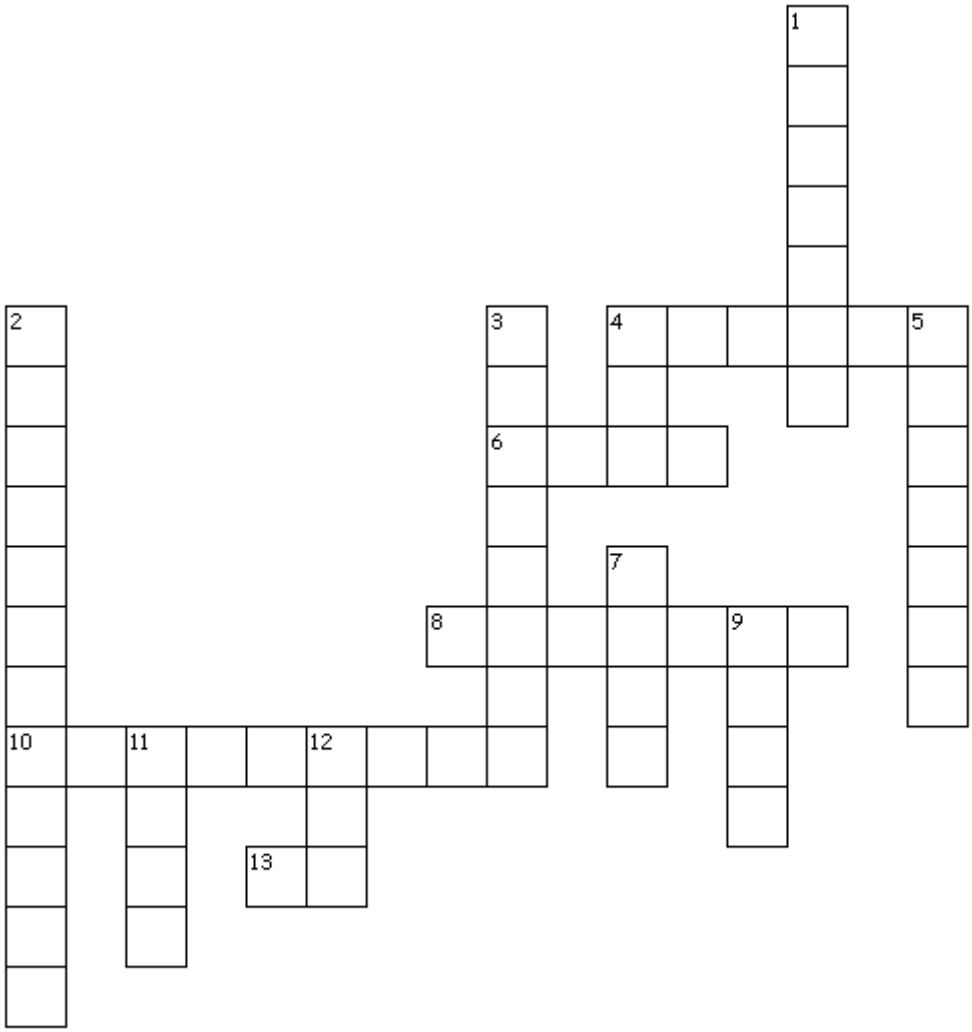
LECTURE PLAN

UNIT – III

S No	Topics	No of periods	Proposed date	Actual Date	pertaining CO	Taxonomy level	Mode of delivery
1	Network Layer Services	1	23.09.2022		CO4	K2	ICT TOOLS
2	Packet switching	1	24.09.2022		CO4	K2	ICT TOOLS
3	Performance	1	28.09.2022		CO4	K3	ICT TOOLS
4	IPV4 Addresses	1	29.09.2022		CO4	K2	ICT TOOLS
5	Forwarding of IP Packets	1	30.09.2022		CO4	K2	ICT TOOLS
6	Network Layer Protocols - IP	1	01.10.2022		CO4	K2	ICT TOOLS
7	ICMP v4	1	06.10.2022		CO4	K2	ICT TOOLS
8	Unicast Routing Algorithms	1	07.10.2022		CO4	K2	ICT TOOLS
9	Protocols	1	08.10.2022		CO4	K2	ICT TOOLS
10	Multicasting Basics	1	12.10.2022		CO4	K2	ICT TOOLS
11	IPV6 Addressing	1	13.10.2022		CO4	K2	ICT TOOLS
12	IPV6 Protocol	1	14.10.2022		CO4	K2	ICT TOOLS

ACTIVITY BASED LEARNING : UNIT – III

CROSSWORD PUZZLE ON NETWORK LAYER



ACTIVITY BASED LEARNING : UNIT – III

CROSSWORD PUZZLE ON NETWORK LAYER – CLUES

Across

4. networking device
6. link state routing protocol
8. type of switching
10. forwarding packets
13. network layer protocol for internet

Down

1. unit of data in network layer
2. routing for one to many
3. packetsentthrougheveryoutlink
4. distance vector routing protocol
5. selecting a path in a network
7. error and diagnostic functionprotocol
9. 32-bit address space
11. 32-bit address space
12. this count refers to number of devices

UNIT III NETWORK LAYER

1. NETWORK LAYER SERVICES

- The network layer in the TCP/IP protocol suite is responsible for the ***host-to-host delivery of datagrams***.
- It provides services to the transport layer and receives services from the data-link layer.
- The network layer is involved at the source host, destination host, and all routers in the path.
- At the source host, the network layer accepts a packet from a transport layer, encapsulates the packet in a datagram, and delivers the packet to the data-link layer.
- At the destination host, the datagram is decapsulated, and the packet is extracted and delivered to the corresponding transport layer.
- A router in the path is receives a packet from one network and delivers it to another network.

SERVICES

1. Packetizing
2. Routing and Forwarding
3. Other Services

1. Packetizing

- The first duty of the network layer is definitely packetizing. **Encapsulating the payload at the source and decapsulating the payload at the destination.**
- The source is not allowed to change the content of the payload unless it is too large for delivery and needs to be fragmented.
- If the packet is fragmented at the source or at routers along the path, the network layer waits until all fragments arrive, reassembling them, and delivering them to the upper-layer protocol.

The routers in the path are not allowed to decapsulate the packets and change source and destination addresses either.

2. Routing and Forwarding

Routing

- The network layer is responsible for routing the packet from its source to the destination.
- A physical network is a combination of networks (LANs and WANs) and routers that connect them.

This means that there is more than one route from the source to the destination.

- The network layer is responsible for finding the best one among these possible routes.

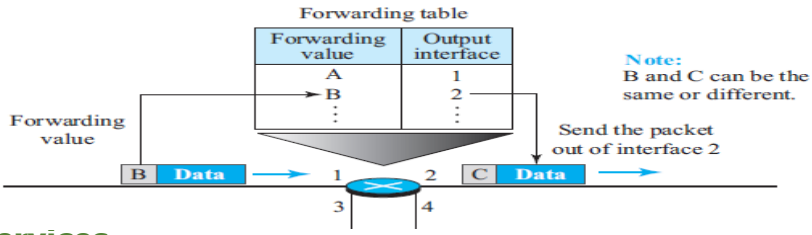
Forwarding

- ***Forwarding*** can be defined as the action applied by each router when a packet arrives at one of its interfaces.

It is also called the ***forwarding table*** and sometimes (Figure 3.1) the ***routing table***.

When a router receives a packet from one of its attached networks, it needs to forward the packet to another attached network.

- To make this decision, the router uses a piece of information in the packet header, which can be the destination address or a label, to find the corresponding output interface number in the forwarding table.
- The following diagram shows the idea of the forwarding process in a router.



3. Other Services

a) Error Control

- Error control also can be implemented in the network layer; the packet in the network layer may be ***fragmented at each router***, which makes ***error checking at this layer inefficient.***
- A ***checksum field*** is added to the datagram to control any c***orruption in the header.***
- This checksum may prevent any corruptions in the header of the datagram.
- Internet uses an auxiliary protocol, ICMP, that provides error control if the datagram is discarded

b) Flow Control

- ***Flow control regulates the amount of data a source can send without overwhelming the receiver.***
- If the source computer produces data faster than the destination computer can consume it, the receiver will be overwhelmed with data.
- To control the flow of data, the receiver needs to send some feedback to the sender to inform the latter that it is overwhelmed with data.

c) Congestion Control

- Congestion - is a situation in which too many datagrams are present in an area of the Internet. Congestion may occur if the number of datagrams sent by source computers is ***beyond the capacity of the network.***
- Some routers may drop some of the datagrams.
- As more datagrams are dropped, the situation may become worse because the sender may send duplicates of the lost packets.
- If the congestion continues, sometimes a situation may reach a point where the system collapses and no datagrams are delivered.

d) Quality of Service

As the Internet has allowed new applications such as multimedia, the quality of service (QoS) of the communication has become more important.

The Internet has thrived by providing better quality of service to support these applications.

e) Security

2. PACKET SWITCHING

- A ***router*** is a switch that creates a connection between an input port and an output port.
- ***Packet switching*** is preferred at the network layer because the unit of data at this layer is a packet.
- At the network layer, a message from the upper layer is divided into manageable packets and each packet is sent through the network.
- The source of the message sends the packets one by one; the destination of the message receives the packets one by one.
- The destination waits for all packets belonging to the same message to arrive before delivering the message to the upper layer.
- The connecting devices in a packet-switched network still need to decide how to route the packets to the final destination.

Approaches:

- A packet-switched network can use two different approaches to route the packets:

1. The datagram approach

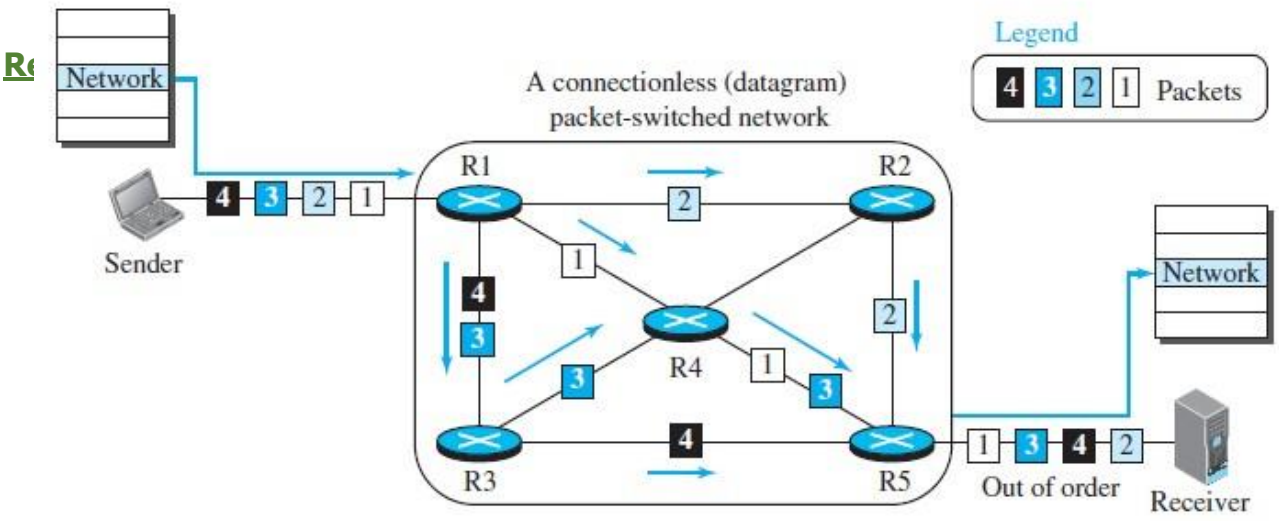


Figure 3.2 – Datagram Approach

1. Datagram Approach – Connectionless Service

- This approach is a ***connectionless service*** in which the network-layer protocol treats
- ***each packet independently***.
- The network layer is only responsible for ***delivery of packets from the source to the destination (Figure 3.2).***
- The packets in a message may or may not travel the same path to their destination
- When the network layer provides a connectionless service, each packet travelling in the Internet is an independent entity.
- The switches in this type of network are called routers.

A packet may be followed by a packet coming from the same or from a different source.

- Each packet is routed based on the information contained in its header:
  - **Source and destination addresses.**
    - The destination address defines where it should go;
    - The source address defines where it comes from.
- The router routes the packet based only on the destination address.
- The source address may be used to send an error message to the source if the packet is discarded.

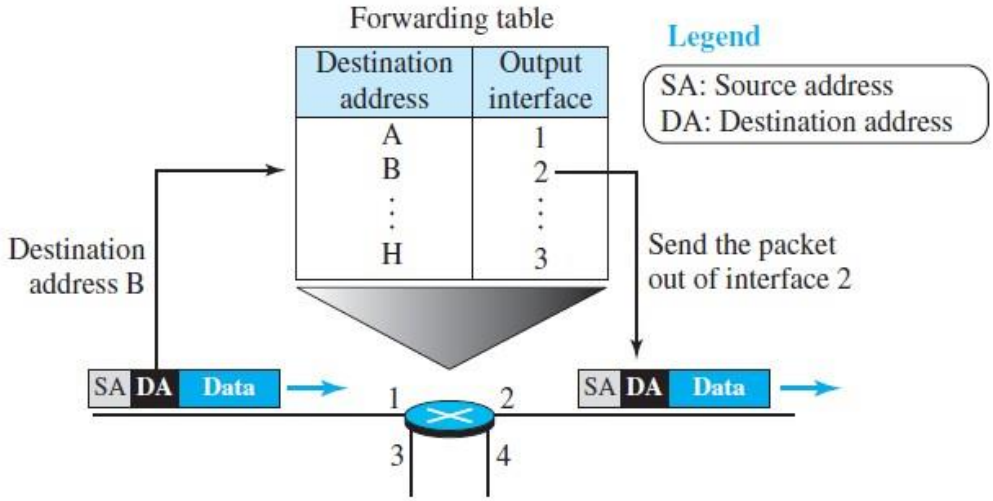


Figure 3.3 -Forwarding process in a router when used in a connectionless network

- Figure 3.3 shows the forwarding process in a
- router. We have used symbolic addresses such as
- A and B.

In a
of t

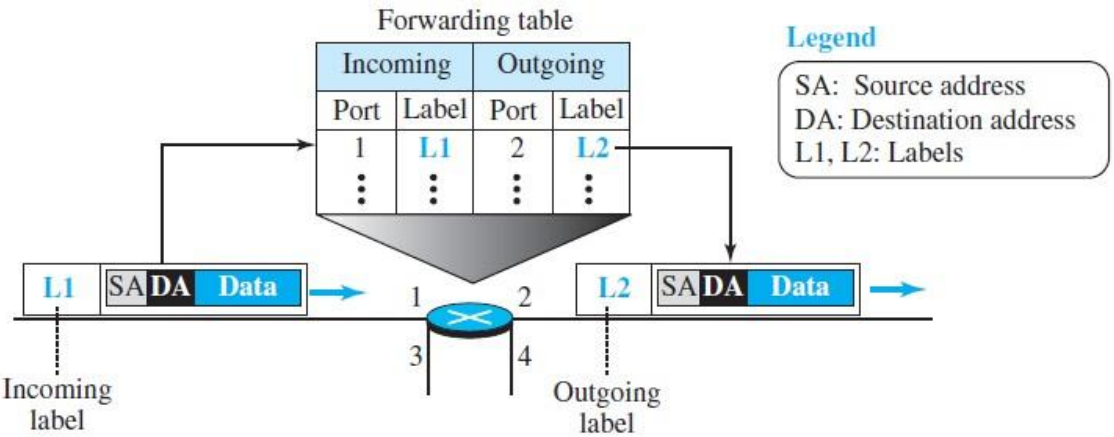


Figure 3.5 - Forwarding process in a router when used in a virtual-circuit network

2. Virtual-Circuit Approach – Connection Oriented

- In a connection-oriented service (also called virtual-circuit approach), there is a relationship between all packets belonging to a message.

- Before all datagrams in a message can be sent, a virtual connection should be set up to define the path for the datagrams.
- After connection setup, the datagrams can all follow the same path.
- The packet should contain the source and destination addresses and also contain a flow label, a virtual circuit identifier that defines the virtual path the packet should follow.
- Figure 3.4 shows the concept of connection-oriented service.
- Each packet is forwarded based on the label in the packet (Figure 3.5).
- The packet has a label when it reaches the router.
- The forwarding decision is based on the value of the label, or virtual circuit identifier.

In a virtual-circuit approach the forwarding decisions are made based on the label of the packet.

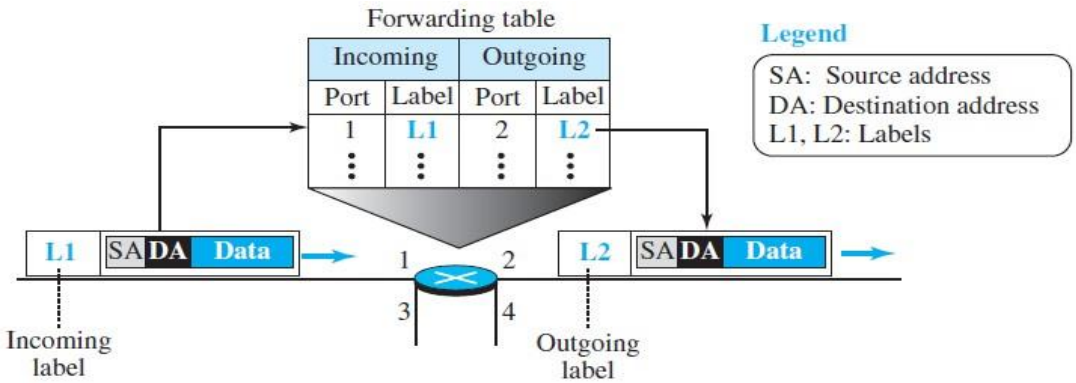


Figure 3.5 - Forwarding process in a router when used in a virtual-circuit network

Three Phases:

- To create a connection-oriented service, a three-phase process is used: **1. Setup 2. Data transfer 3. Teardown**
- In the setup phase, the source and destination addresses of the sender and receiver are used to make table entries for the connection-oriented service.
- In the teardown phase, the source and destination inform the router to delete the corresponding entries.
- Data transfer occurs between these two phases.

1. Setup Phase

- In the setup phase, a router creates an entry for a virtual circuit.
- For example, suppose source A needs to create a virtual circuit to destination B. Two auxiliary packets need to be exchanged between the sender and the receiver:
- **1. The request packet**
- **2. The acknowledgment packet.**

- **Request Packet**

A request packet is sent from the source to the destination. This auxiliary packet carries the source and destination addresses. Figure 3.6 shows the process.

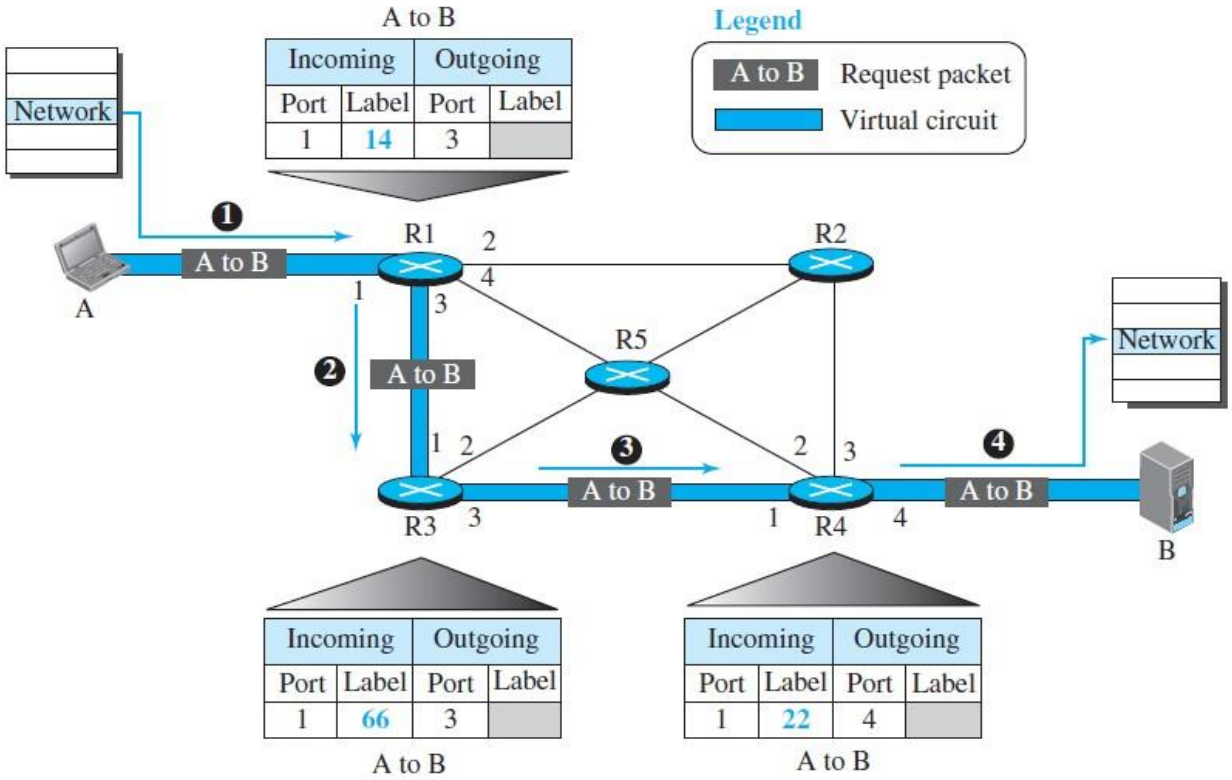


Figure 3.6 – Sending Request Packet in a Virtual Circuit Network

1. Source A sends a request packet to router R1.
2. Router R1 receives the request packet. It knows that a packet going from A to B goes out through port 3. The router creates an entry in its table for this virtual circuit.
   a) The router assigns the incoming port (1) and chooses an available incoming label (14) and the outgoing port (3).
   b) The router then forwards the packet through port 3 to router R3.
3. Router R3 receives the setup request packet.
   a) The same in this case, incoming port (1), incoming label (66), and outgoing port (3).
4. Router R4 receives the setup request packet.
   1. Again, three columns are completed: incoming port (1), incoming label (22), and outgoing port (4).
5. Destination B receives the setup packet.

Acknowledgement Packet

- A special packet, called the acknowledgment packet, completes the entries in the switching tables. (Figure 3.7)
- The destination sends an acknowledgment to router R4. The acknowledgment carries the global source and destination addresses so the router knows which entry in the table is to be completed. The packet also carries label 77, chosen by the destination as the incoming label for packets from A. Router R4 uses this label to complete
- Router R4 sends an acknowledgment to router R3 that contains its incoming label in the table, chosen in the setup phase. Router R3 uses this as the outgoing label in the table.

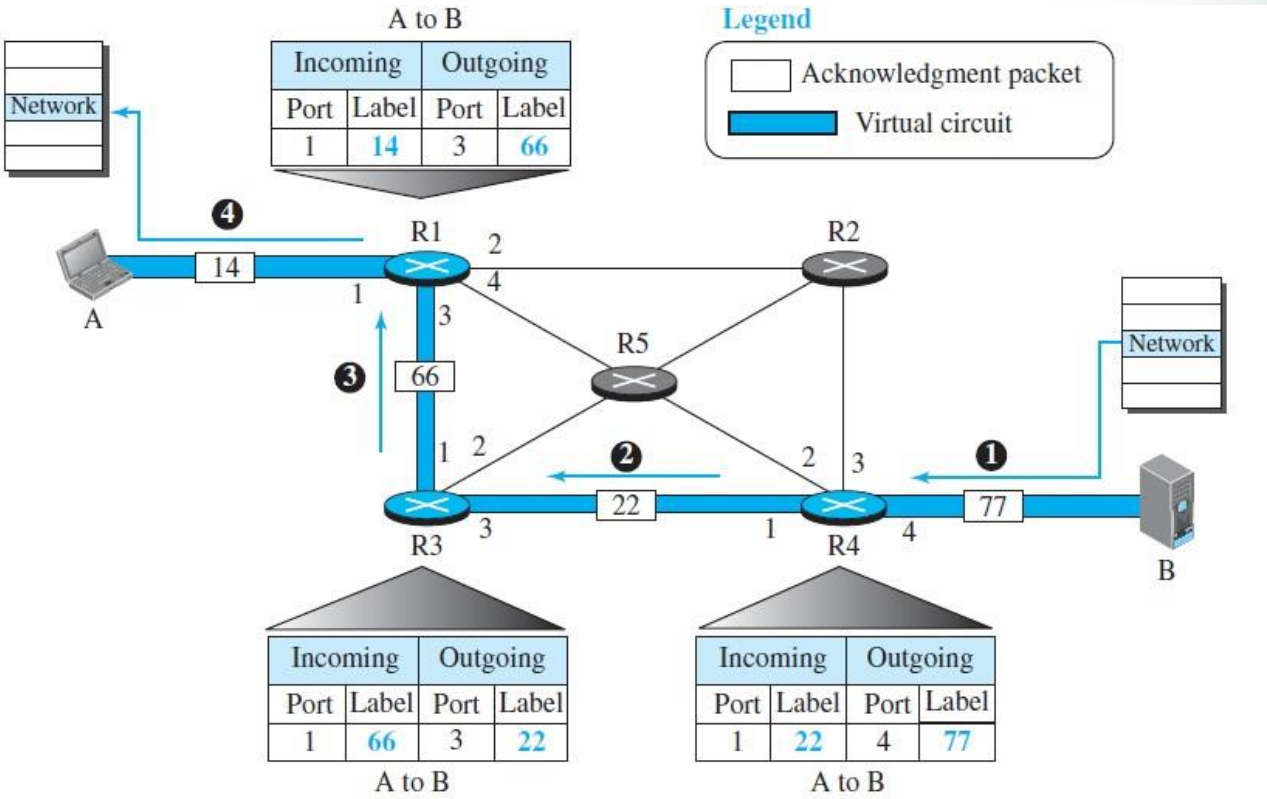
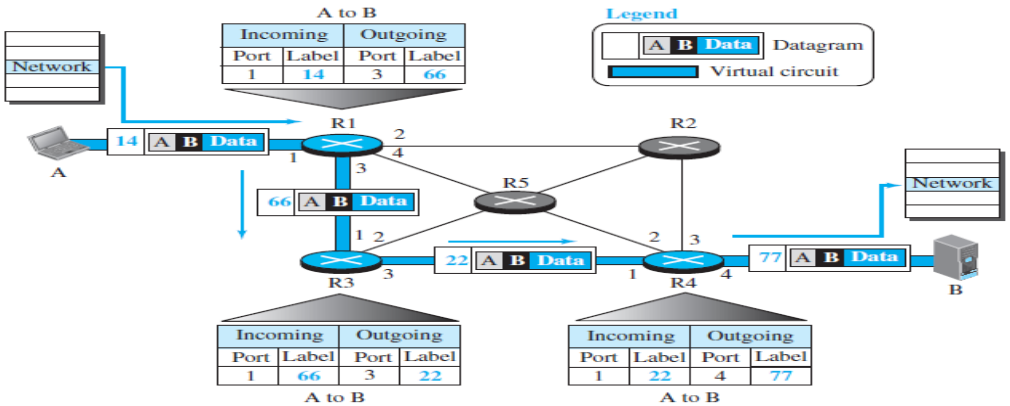


Figure 3.7 – Acknowledgement Packet

- Router R3 sends an acknowledgment to router R1 that contains its incoming label in the table, chosen in the setup phase. Router R1 uses this as the outgoing label in the table.
- Finally router R1 sends an acknowledgment to source A that contains its incoming label in the table, chosen in the setup phase.
- The source uses this as the outgoing label for the data packets to be sent to destination B.

2. Data Transfer Phase

The second phase is called the data-transfer phase. After all routers have created their forwarding table for a specific virtual circuit, then the network-layer packets belonging to or



3. Teardown Phase

In the teardown phase,

Source A, after sending all packets to B, sends a special packet called a teardown packet.

Destination B responds with a confirmation packet.

All routers delete the corresponding entries from their tables.

3. NETWORK LAYER PERFORMANCE

The performance of a network can be measured in terms of

1. **Delay**
2. **Throughput**
3. **Packet loss**
4. **Congestion control**

1. DELAY

The delays in a network can be divided into four types:

1. **Transmission delay**
2. **Propagation delay**
3. **Processing delay**
4. **Queuing delay.**

Transmission

Delay

- A source host or a router cannot send a packet immediately.
- A sender needs to put the bits in a packet on the line one by one.
- If the first bit of the packet is put on the line at time t1 and the last bit is put on the line at time t2, transmission delay of the packet is (t2−t1).
- The transmission delay is

$$\textbf{Delay}_{tr}\textbf{=(Packet length) / (Transmission rate)}$$

- **Example:** In a Fast Ethernet LAN with the transmission rate of 100 million bits per second and a packet of 10,000 bits, it takes (10,000)/(100,000,000) or 100 microseconds for all bits of the packet to be put on the line.

Propagation Delay

- Propagation delay is the time it takes for a bit to travel from point A to point B in the transmission media.
- The propagation delay for a packet-switched network depends on the propagation delay of each network (LAN or WAN).

The propagation speed of the media, which is 3×10^8 meters/second in a vacuum the distance of the link.

In other words, propagation delay is .

$$\textbf{Delay}_{pg}\textbf{=(Distance) / (Propagation speed)}$$

Example: if the distance of a cable link in a point-to-point WAN is 2000 meters and the propagation speed of the bits in the cable is 2×10^8 meters/second, then the propagation delay is 10 microseconds.

Processing Delay

- The processing delay is the time required for a destination host to receive a packet from its input port, remove the header, perform an error detection procedure, and deliver the packet to the output port.
- The processing delay may be different for each packet, but normally is calculated as an average.

$Delay_{pr}$=Time required to process a packet in a router or a destination host

Queuing Delay

- Queuing delay can normally happen in a router.
- The queuing delay for a packet in a router is measured as the time a packet waits in the input queue and output queue of a router.

$Delay_{qu}$ =The time a packet waits in input and output queues in a router

Total Delay

- Assuming equal delays for the sender, routers, and receiver, the total delay (source-to destination delay) a packet encounters can be calculated if we know the number of routers, n, in the whole path.

Total delay =$(n+1)$ ($Delay_{tr}$+$Delay_{pg}$+$Delay_{pr}$) +(n) ($Delay_{qu}$)

- If we have n routers, we have (n +1) links.
- (n +1) transmission delays related to n routers and the source, (n +1) propagation delays related to (n +1) links, (n +1) processing delays related to n routers and the destination, and only n queuing delays related to n routers.

2. THROUGHPUT

- Throughput is defined as the number of bits passing through the point in a second, which is actually the transmission rate of data at that point.
- In a path from source to destination, a packet may pass through several links (networks), each with a different transmission rate.
- To determine the throughput of the whole path assume that we have three links, each with a different transmission rate, as shown in figure 3.8.
- In the Figure 3.8, the data can flow at the rate of 200 kbps in Link1.
- However, when the data arrives at router R1, it cannot pass at this rate. Data needs to be queued at the router and sent at 100 kbps.

When data arrives at router R2, it could be sent at the rate of 150 kbps, but there is not enough data to be sent.

In other words, the average rate of the data flow in Link3 is also 100 kbps. We can conclude that the average data rate for this path is 100 kbps, the minimum of the three different data rates.

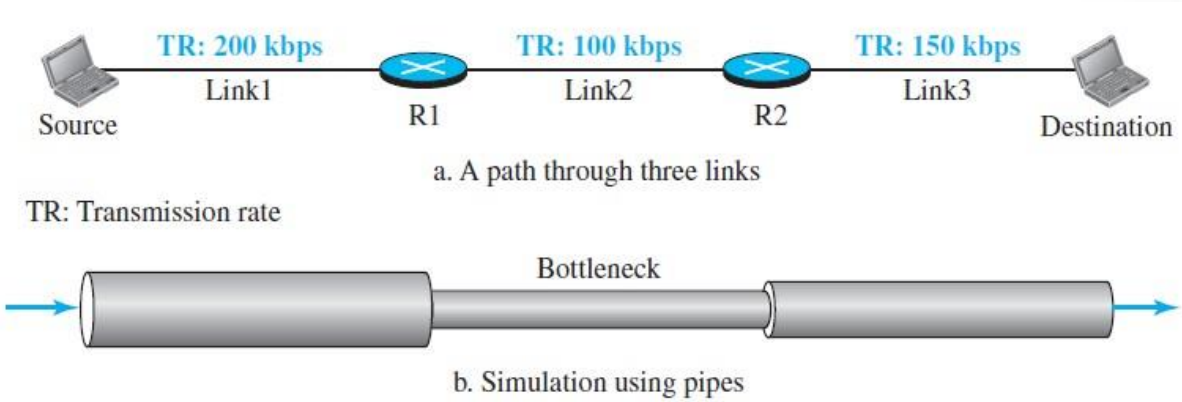


Figure 3.8 – Throughput in a path with three links in a series

- In the Figure 3.8, the data can flow at the rate of 200 kbps in Link1.
- However, when the data arrives at router R1, it cannot pass at this rate. Data needs to be queued at the router and sent at 100 kbps.
- When data arrives at router R2, it could be sent at the rate of 150 kbps, but there is not enough data to be sent.
- In other words, the average rate of the data flow in Link3 is also 100 kbps. We can conclude that the average data rate for this path is 100 kbps, the minimum of the three different data rates.

  It shows that we can simulate the behaviour of each link with pipes of different sizes; the average throughput is determined by the bottleneck, the pipe with the smallest diameter. In general, in a path with n links in series, we have

- **Throughput =minimum {TR1, TR2,...TRn}**

  Although the situation in the above diagram shows how to calculate the throughput when the data is passed through several links, the actual situation in the Internet is that the data normally passes through two access networks and the Internet backbone, as shown in the Figure 3.9.

- The Internet backbone has a very high transmission rate, in the range of gigabits

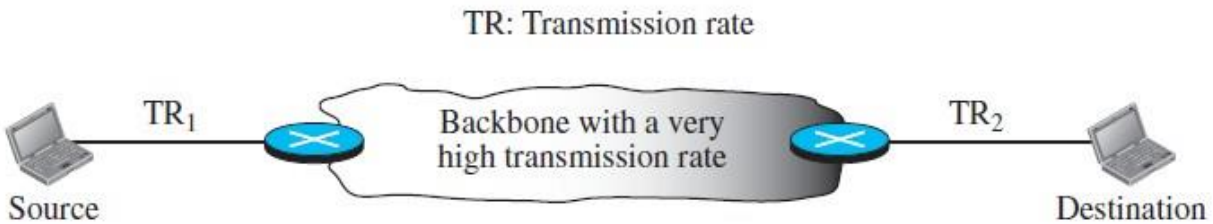


Figure 3.9 – A path through the Internet backbone

- **Example:** if a server connects to the Internet via a Fast Ethernet LAN with the data rate of 100 Mbps, but a user who wants to download a file connects to the Internet via a dial-up telephone line with the data rate of 40 kbps, the throughput is 40 kbps.

3. PACKET LOSS

- The performance of communication is the number of packets lost during transmission.
- When a router receives a packet while processing another packet, the received packet needs to be stored in the input buffer waiting for its turn.
- A router, however, has an input buffer with a limited size.
- A time may come when the buffer is full and the next packet needs to be dropped.
- The effect of packet loss on the Internet network layer is that the packet needs to be resent, which in turn may create overflow and cause more packet loss

4. CONGESTION CONTROL

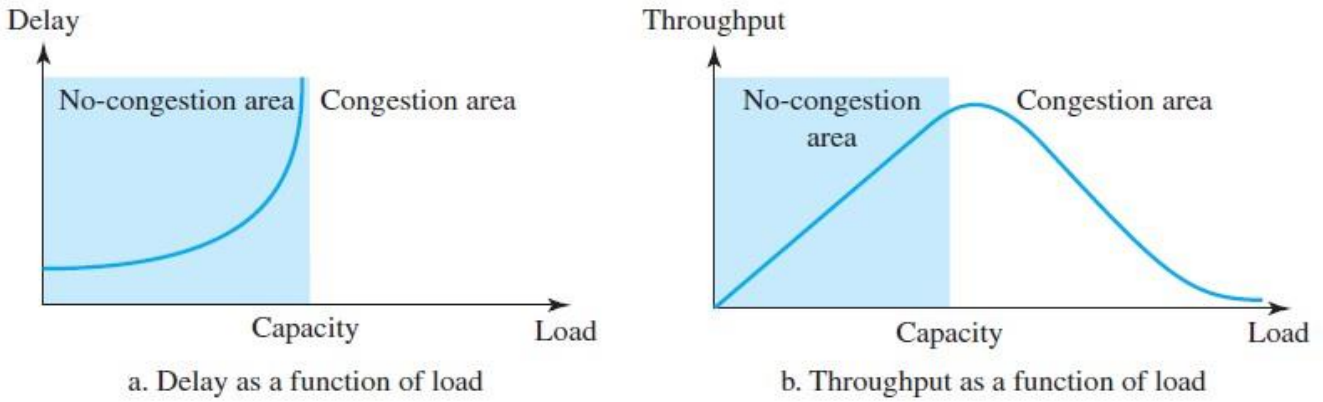
- Congestion control is a mechanism for improving performance.
- Congestion at the network layer is related to two issues, ***throughput and delay.***

Delay as a function of load

- When the load is much less than the capacity of the network, the delay is at a minimum. [Figure 3.10]
- This minimum delay is composed of propagation delay and processing delay
- When the load reaches the network capacity, the delay increases sharply because we now need to add the queuing delay to the total delay.

Throughput as a function of load

- When the load is below the capacity of the network, the throughput increases proportionally with the load. [Figure 3.10]



a. Delay as a function of load

b. Throughput as a function of load

Figure 3.10 – Packet Delay and Throughput as functions of load

Two Broad Categories

- In general, we can divide congestion control mechanisms into two broad categories: ***open-loop congestion control (prevention) and closed-loop congestion control (removal).***

Open-Loop Congestion Control

- In open-loop congestion control, policies are applied to prevent congestion before it happens.
- In these mechanisms, congestion control is handled by either the source or the destination. We give a brief list of policies that can prevent congestion.

Retransmission Policy

- If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted.
- Retransmission may increase congestion in the network. However, a good retransmission policy can prevent congestion.

Window Policy

- The type of window at the sender may also affect congestion. The Selective Repeat window is better than the Go-Back-N window for congestion control.
- In the Go-Back-N window, when the timer for a packet times out, several packets may be resent. This duplication may make the congestion worse.
- The Selective Repeat window tries to send the specific packets that have been lost or corrupted.

Acknowledgment Policy

- The acknowledgment policy imposed by the receiver may also affect congestion.
- If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion.
- A receiver may send an acknowledgment only if it has a packet to be sent or a special timer expires.
- A receiver may decide to acknowledge only N packets at a time.

Discarding Policy

- A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission.

Admission Policy

- An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual-circuit networks.
- Switches in a flow first check the resource requirement of a flow before admitting it to the network.
- A router can deny establishing a virtual-circuit connection if there is congestion in the network or if there is a possibility of future congestion.

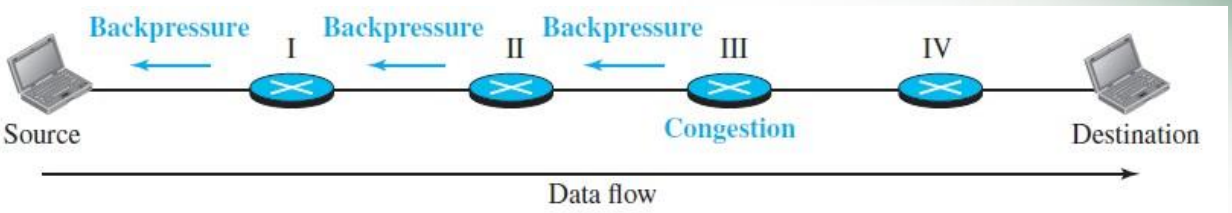


Figure 3.11 – Backpressure method for alleviating Congestion

Closed-Loop Congestion Control

- Closed-loop congestion control mechanisms try to alleviate congestion after it happens. Several mechanisms have been used by different protocols. We describe a few of them here.

Backpressure

- The technique of backpressure refers to a congestion control mechanism in which a congested node stops receiving data from the immediate upstream node or nodes.
- This may cause the upstream node or nodes to become congested, and they, in turn, reject data from their upstream node or nodes, and so on.
- ***Backpressure is a node-to-node congestion control that starts with a node and propagates, in the opposite direction of data flow, to the source.***
- Node III in the figure has more input data than it can handle. It drops some packets in its input buffer and informs node II to slow down.
- Node II, in turn, may be congested because it is slowing down the output flow of data. If node II is congested, it informs node I to slow down, which in turn may create congestion.
- If so, node I informs the source of data to slow down. This, in time, alleviates the congestion.
- Note that the pressure on node III is moved backward to the source to remove the congestion.

Choke Packet

- A ***choke packet*** is a packet sent by a node to the source to inform it of congestion.

In
he

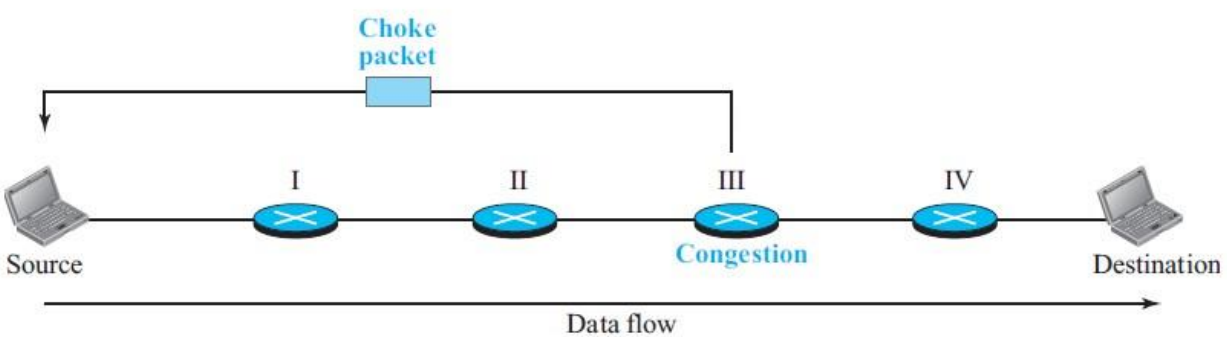


Figure 3.12- Choke Packet

- In the choke-packet method, the warning is from the router, which has encountered congestion, directly to the source station.
- The intermediate nodes through which the packet has travelled are not warned. The warning message goes directly to the source station; the intermediate routers do not take any action. The following diagram shows the idea of a choke packet.

Implicit Signalling

- In implicit signalling, there is no communication between the congested node and the source.
- For example, when a source sends several packets and there is no acknowledgment for a while, one assumption is that the network is congested.

Explicit Signalling

- The node that experiences congestion can explicitly send a signal to the source or destination.
- In the explicit-signalling method, the signal is included in the packets that carry data. Explicit signalling can occur in either the forward or the backward direction.

3.4 IPV4 ADDRESSES

- The IP layer of the TCP/IP protocol suite to identify the connection of each device to the Internet is called the Internet address or IP address.
- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet.
- The IP address is the address of the connection because if the device is moved to another network, the IP address may be changed.
- If a device has two connections to the Internet, via two networks, it has two IPv4 addresses.

Address Space

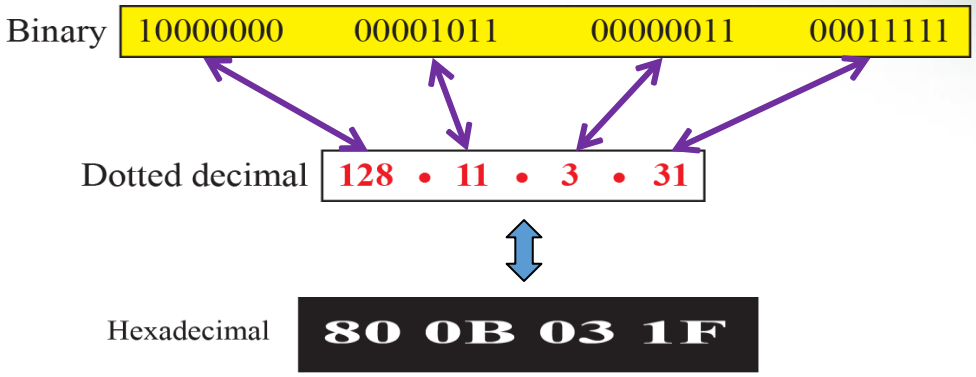
- IPv4 defines addresses has an address space.
- An address space is the total number of addresses used by the protocol.
- If a protocol uses _n` bits to define an address, the address space is _2n` because each bit
can have two different values (0 or 1).
- IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296
- If there were no restrictions, more than 4 billion devices could be connected to the Internet

Notation

There are three common notations in an IPv4 address:

binary notation (base 2), dotted-decimal notation (base 256), and hexadecimal notation (base 16).

In binary notation, an IPv4 address is displayed as 32 bits. To make the address more readable, one or more spaces are usually inserted between each octet (8 bits).



- To make the IPv4 address more compact and easier to read, it is usually written in
- decimal form with a decimal point (dot) separating the bytes.
- This format is referred to as dotted-decimal notation. Each byte (octet) is only 8 bits, each number in the dotted-decimal notation is between 0 and 255.
- Sometimes we can see an IPv4 address in hexadecimal notation.
- Each hexadecimal digit is equivalent to four bits.

This notation is often used in network programming.

- Figure shows an IP address in the three discussed notations.

Hierarchy in Addressing

- In any communication network, the addressing system is hierarchical.
- A 32-bit IPv4 address is also hierarchical, but divided only into two parts.
- The first part of the address, called the prefix, defines the network;
- The second part of the address, called the suffix, defines the node
- The prefix length is n bits and the suffix length is (32 – n) bits.
- A prefix can be fixed length or variable length.
- The network identifier in the IPv4 was first designed as a fixed-length prefix. This scheme is referred to as classful addressing (Figure - 3.13).

The new g, uses a variable-length n a 32-bit IPv4 address.

The pref its.

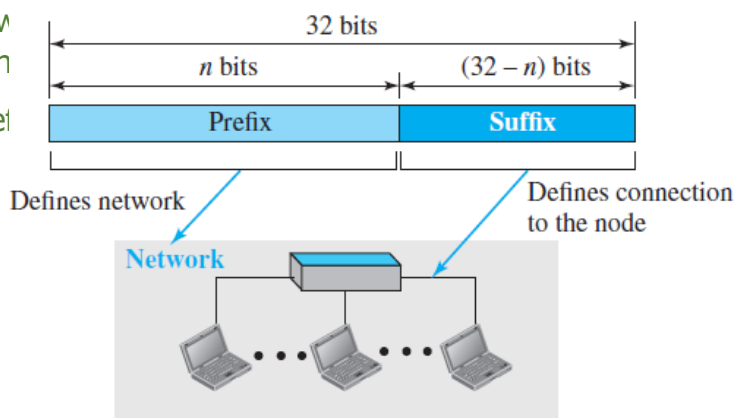


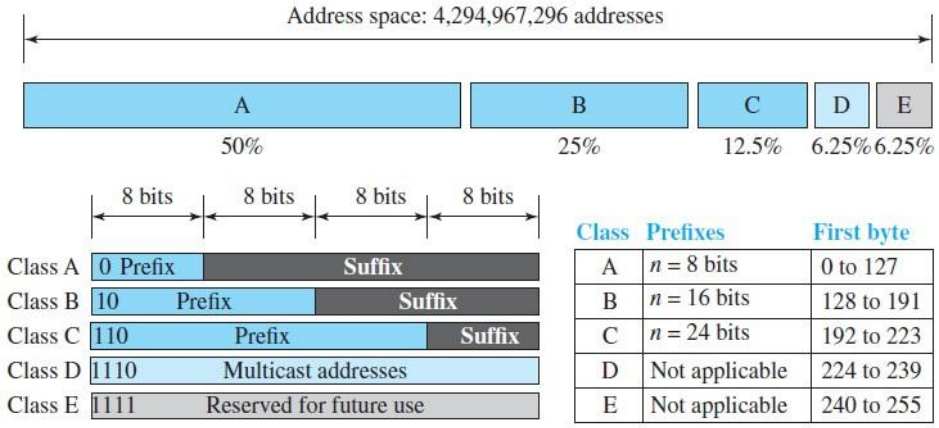
Figure – 3.13 – Hierarchy in addressing

3.4.1 CLASSFUL ADDRESSING

- When the Internet started, an IPv4 address was designed with a fixed-length prefix, but to accommodate both small and large networks, three fixed-length prefixes were designed instead of one (n = 8, n = 16, and n = 24).
- The whole address space was divided into five classes (class A, B, C, D, and E)
- This scheme is referred to as classful addressing.
- In class A, the network length is 8 bits, but since the first bit, which is 0, defines the class, we can have only seven bits as the network identifier.
- This means there are only 2^7 = 128 networks in the world that can have a class A address.
- In class B, the network length is 16 bits, but since the first two bits define the class,
- We can have only 14 bits as the network identifier. This means there are only 2^14 = 16,384 networks in the world that can have a class B address.
- In class C, the network length is 24 bits,
- We can have only 21 bits as the network identifier. This means there are 221 = 2,097,152 networks in the world that can have a class C address.
- Class D is not divided into prefix and suffix. It is used for multicast addresses.

  All addresses that start with 1111 in binary belong to class E.

  Class D, Class E is not divided into prefix and suffix and is used as reserve.



Class	Prefixes	First byte
A	n = 8 bits	0 to 127
B	n = 16 bits	128 to 191
C	n = 24 bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

Figure 3.14 – Occupation of the address space in classful addressing

Subnetting

- To alleviate address depletion, two strategies were proposed and, to some extent, implemented: subnetting and supernetting.
- Dividing a network into two or more network is called **subnet.** It is a logical subdivision of an IP address.
- In subnetting, a class A or class B block is divided into several subnets.
- Each subnet has a larger prefix length than the original network.

Benefits

- 1. Reduce network traffic
- 2. Optimized network performance
- 3. Simplified network management

Subnet masks code:

- 1Represent network or subnet address
- 0-Represent the host address

Designing Subnets

- The subnetworks in a network should be carefully designed to enable the routing of packets.
- We assume the total number of addresses granted to the organization is N, the prefix length is n, the assigned number of addresses to each subnetwork is N_{sub}, and the prefix length for each subnetwork is n_{sub}. Then the following steps need to be carefully followed to guarantee the proper operation of the subnetworks.

1. The number of addresses in each subnetwork should be a power of 2.
2. The prefix length for each subnetwork should be found using the following formula:

First address = (prefix in decimal) X 2^{32-n} = (prefix in decimal) X N

$$n_{sub} = 32 - \log_2 N_{sub}$$

1. The starting address in each subnetwork should be divisible by the number of addresses in that subnetwork. This can be achieved if we first assign addresses to larger subnetorks.

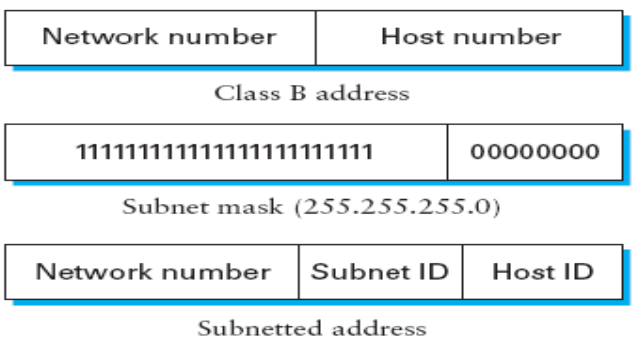


Figure 3.15 – Variable length blocks in classless addressing

Supernetting

- Supernetting is the opposite of Subnetting.
- Insubnetting, a single big network is divided into multiple smaller subnetworks.
- In Supernetting, multiple networks are combined into a bigger network termed as a Supernetwork or Supernet.
- ***Advantage of Classful Addressing***
- We can easily find the class of the address
- The prefix length for each class is fixed
- We can find the prefix length immediately.

3.4.2 CLASSLESS ADDRESSING

- In classless addressing, variable-length blocks are used that belong to no classes.
- We can have a block of 1 address, 2 addresses, 4 addresses, 128 addresses, and so on.
- In classless addressing, the whole address space is divided into variable length blocks.
- The prefix in an address defines the block (network); the suffix defines the node (device). Figure shows the division of the whole address space into non overlapping blocks.
- **Prefix Length: Slash Notation**
- The prefix length in classless addressing is variable.
- In this case, the prefix length, n, is added to the address, separated by a slash.
- The notation is informally referred to as slash notation and formally as classless interdomain routing or CIDR (pronounced cider) strategy.

An address in classless addressing can then be represented as shown in Figure

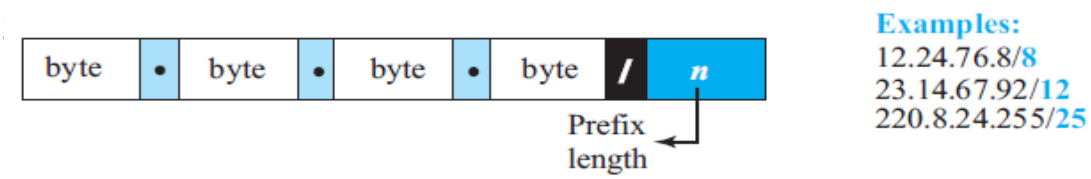


Figure 3.16 – Slash notation (CIDR)

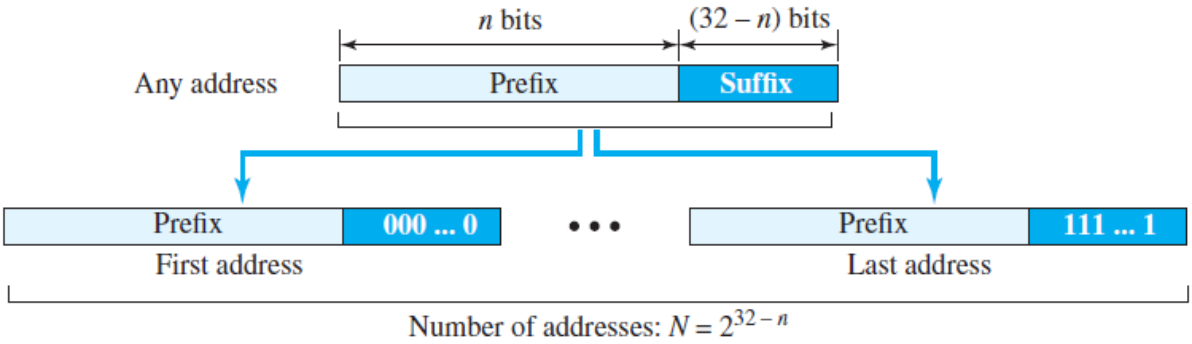


Figure 3.17 – Information extraction in classless addressing

Extracting Information from an Address

- Given any address in the block, we normally like to know three pieces of information
- The number of addresses, the first address in the block, and the last address.
- Since the value of prefix length, n, is given, we can easily find these three pieces of information
- 1. The number of addresses in the block is found as N = 2^32−n.
- 2.To find the first address, we keep the n leftmost bits and set the (32 – n) rightmost bits all to 0s.
- 3. To find the last address, we keep the n leftmost bits and set the (32 – n) rightmost bits all to 1s.

Example:1

- A classless address is given as 167.199.170.82/27. We can find the above three pieces of information as follows. The number of addresses in the network is $2^{32-n} = 2^5 = 32$ addresses.

The first address can be found by keeping the first 27 bits and changing the rest

```
Address: 167.199.170.82/27      10100111  11000111  10101010  01010010
First address: 167.199.170.64/27  10100111  11000111  10101010  01000000
```

The last address can be found by keeping the first 27 bits and changing the rest of the bits to 1s.

```
Address: 167.199.170.82/27      10100111  11000111  10101010  01011111
Last address: 167.199.170.95/27   10100111  11000111  10101010  01011111
```

Address Mask

- Another way to find the first and last addresses in the block is to use the address mask.
- The address mask is a 32-bit number in which the n leftmost bits are set to 1s and the rest of the bits (32 – n) are set to 0s.
- A computer can easily find the address mask because it is the complement of ($2^{32-n} - 1$).
- The reason for defining a mask in this way is that it can be used by a computer program to extract the information in a block, using the three bit-wise operations NOT, AND, and OR.
- 1. The number of addresses in the block N = NOT (mask) + 1.
- 2. The first address in the block = (Any address in the block) AND (mask).
- 3. The last address in the block = (Any address in the block) OR [(NOT (mask)].
- **Example:2**

  A classless address is given as 167.199.170.82/27.The mask in dotted-decimal notation is 256.256.256.224. The AND, OR, and NOT operations can be applied to

Number of addresses in the block:	N = NOT (mask) + 1 = 0.0.0.31 + 1 = 32 addresses
First address:	First = (address) AND (mask) = 167.199.170.82
Last address:	Last = (address) OR (NOT mask) = 167.199.170.255

Example:3

In classless addressing, an address cannot per se define the block the address belongs to. For example, the address 230.8.24.56 can belong to many blocks. Some of them are shown below with the value of the prefix associated with that block.

Prefix length:16	→	Block:	230.8.0.0	to	230.8.255.255
Prefix length:20	→	Block:	230.8.16.0	to	230.8.31.255
Prefix length:26	→	Block:	230.8.24.0	to	230.8.24.63
Prefix length:27	→	Block:	230.8.24.32	to	230.8.24.63
Prefix length:29	→	Block:	230.8.24.56	to	230.8.24.63
Prefix length:31	→	Block:	230.8.24.56	to	230.8.24.57

Address Aggregation

- One of the advantages of the CIDR strategy is address aggregation. When blocks of addresses are combined to create a larger block, routing can be done based on the prefix of the larger block.
- ICANN assigns a large block of addresses to an ISP.
- Each ISP in turn divides its assigned block into smaller subblocks and grants the subblocks to its customers.

Reference video: https://www.youtube.com/watch?v=9MAI53t9tLk

Special Addresses Five special addresses that are used for special purposes:

- This-host address
- Limited-broadcast address
- Loopback address
- Private addresses
- Multicast addresses

This-host Address

- The only address in the block 0.0.0.0/32 is called the this-host address.
- It is used whenever a host needs to send an IP datagram but it does not know its own address to use as the source address.

Limited-broadcast Address

- The only address in the block 255.255.255.255/32 is called the limited-broadcast address.
- It is used whenever a router or a host needs to send a datagram to all devices in a network.

  The routers in the network, however, block the packet having this address as the destination; the packet cannot travel outside the network.

Loopback Address

- The block 127.0.0.0/8 is called the loopback address.
- A packet with one of the addresses in this block as the destination address never leaves the host; it will remain in the host.

  Any address in the block is used to test a piece of software in the machine.

Private Addresses

- Four blocks are assigned as private addresses: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16,

  and 169.254.0.0/16.

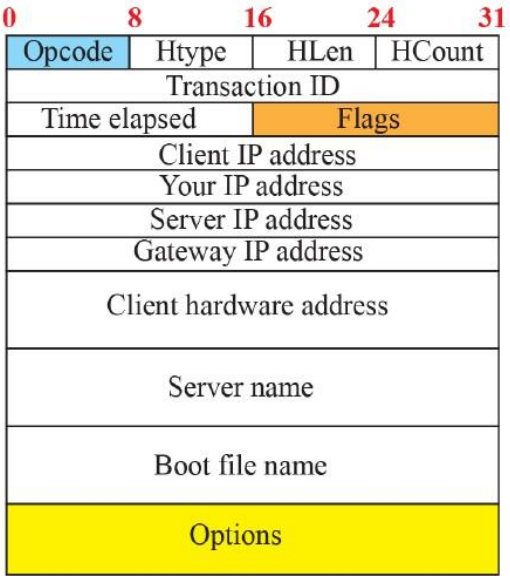
Multicast Addresses

- The block 224.0.0.0/4 is reserved for multicast addresses.

3.4.3 DYNAMIC HOST CONFIGURATION PROTOCOL (DHCP)

- Address assignment in an organization can be done automatically using the Dynamic Host Configuration Protocol (DHCP).
- DHCP is an application-layer program, using the client-server paradigm that actually helps TCP/IP at the network layer.

  DHCP is often called a plug and play protocol.
- A network manager can configure DHCP to assign permanent IP addresses to the host and routers.
- Four pieces of information are normally needed: the computer address, the prefix, the address of a router, and the IP address of a name server.



Fields:

Opcode: Operation code, request (1) or reply (2)
Htype: Hardware type (Ethernet, ...)
HLen: Lengh of hardware address
HCount: Maximum number of hops the packet can travel
Transaction ID: An integer set by client and repeated by the server
Time elapsed: The number of seconds since the client started to boot
Flags: First bit defines unicast (0) or multicast (1); other 15 bits not used
Client IP address: Set to 0 if the client does not know it
Your IP address: The client IP address sent by the server
Server IP address: A broadcast IP address if client does not know it
Gateway IP address: The address of default router
Server name: A 64-byte domain name of the server
Boot file name: A 128-byte file name holding extra information
Options: A 64-byte field with dual purpose described in text

Figure 3.18 – DHCP Message Format

DHCP Message Format

- DHCP is a client-server protocol in which the client sends a request message and the server returns a response message.
- The 64-byte option field has a dual purpose. It can carry either additional information or some specific vendor information.

DHCP Operation

1. DHCP discover message

- The DHCP client broadcasts a DHCPDISCOVER message on the network subnet using the destination address 255.255.255.255 (limited broadcast) or the specific subnet broadcast address (directed broadcast).
- A DHCP client may also request its last known IP address. If the client remains connected to the same network, the server may grant the request.
- Client broadcast to locate available servers.

2. DHCP offer message

- The DHCP server responds with a DHCPOFFER message in which the address field defines the offered IP address for the joining host and the server address field includes the IP address of the server. The message also includes the lease time for which the host can keep the IP address.

3. DHCP request message

- In response to the DHCP offer, the client replies with a DHCPREQUEST message, broadcast to the server, requesting the offered address.
- A client can receive DHCP offers from multiple servers, but it will accept only one DHCP offer.

  Based on required server identification option in the request and broadcast messaging, servers are informed whose offer the client has accepted.

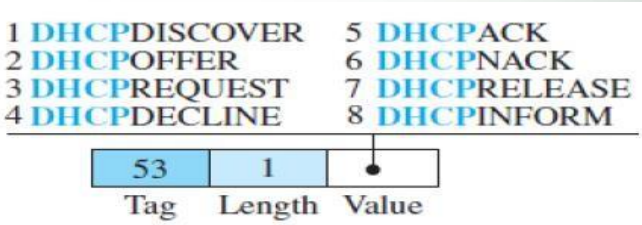


Figure 3.19 – DHCP Option format

- **3. DHCP request message**
- In response to the DHCP offer, the client replies with a DHCPREQUEST message, broadcast to the server, requesting the offered address.
- A client can receive DHCP offers from multiple servers, but it will accept only one DHCP offer.
- Based on required server identification option in the request and broadcast messaging, servers are informed whose offer the client has accepted.
- **4. DHCP acknowledgement message**
- Finally, the selected server responds with a DHCPACK message to the client if the offered IP address is valid.
- If the server cannot keep it's the server sends a DHCPNAK message and the client needs to repeat the process.
- This message is also broadcast to let other servers know that the request is accepted or rejected.
- **5.DHCPNAK** - Server to client indicating client's notion of network address is incorrect (e.g., client has moved to new subnet) or client's lease as expired
- **6. DHCPDECLINE** - Client to server indicating network address is already in use.
- **7.DHCPRELEASE** - Client to server relinquishing network address and cancelling remaining lease.

DHC ırameters; client

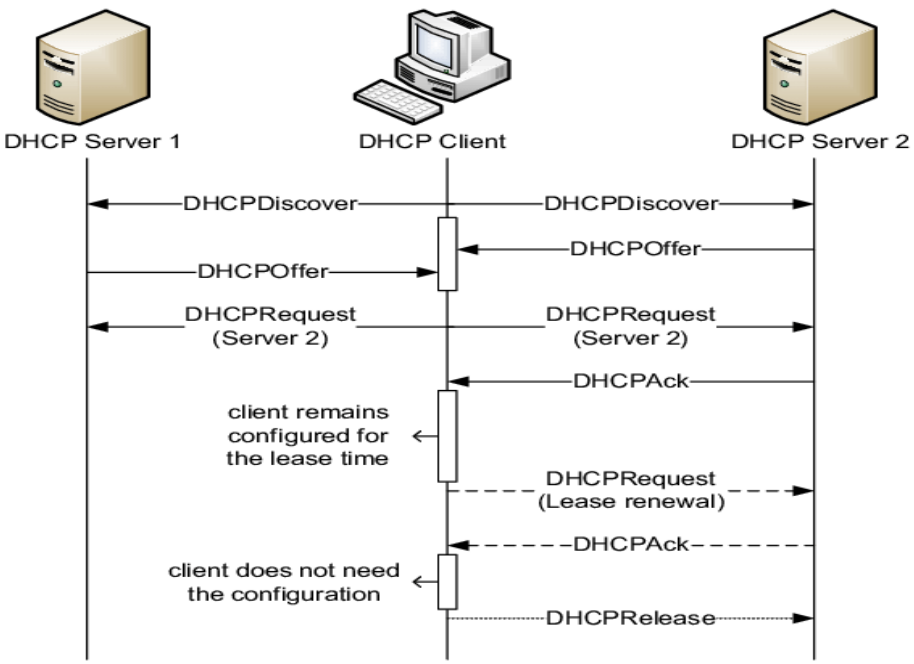


Figure 3.20 – Operation

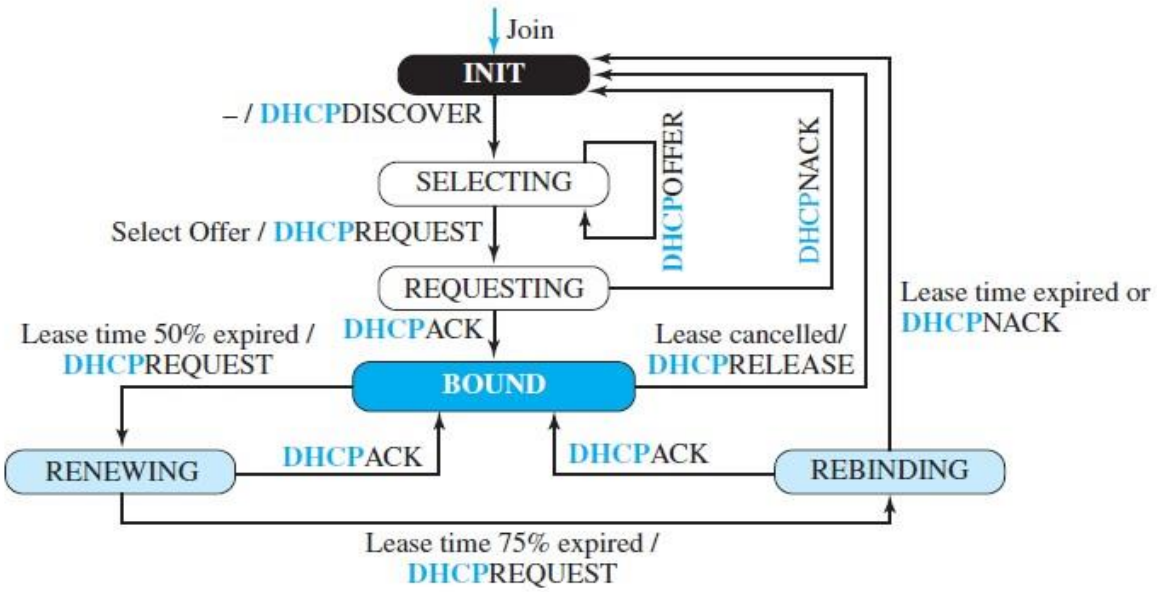


Figure 3.21 – FSM for the DHCP Client

Transition States

- To provide dynamic address allocation, the DHCP client acts as a state machine that performs transitions from one state to another depending on the messages it receives or sends.
- Figure 3.21 shows the transition diagram with the main states.
- When the DHCP client first starts, it is in the INIT state (initializing state).
- The client broadcasts a discover message.
- When it receives an offer, the client goes to the SELECTING
- state. While it is there, it may receive more offers.
- After it selects an offer, it sends a request message and goes to the REQUESTING state.
- If an ACK arrives while the client is in this state, it goes to the BOUND state and uses the IP address.
- When the lease is 50 percent expired, the client tries to renew it by moving to the RENEWING state.
- If the server renews the lease, the client moves to the BOUND state again.
- If the lease is not renewed and the lease time is 75 percent expired, the client moves to the REBINDING state.
- If the server agrees with the lease (ACK message arrives), the client moves to the BOUND state and continues using the IP address; otherwise, the client moves to the INIT state and requests another IP address.
- Note that the client can use the IP address only when it is in the BOUND, RENEWING, or REBINDING state.

The above procedure requires that the client uses three timers: renewal timer (set to 50 percent of the lease time), rebinding timer (set to 75 percent of the lease time), and expiration timer (set to the lease time).

3.4.4 NETWORK ADDRESS TRANSLATION (NAT)

- Network Address Translation (NAT) is a process in which one or more local IP address is translated into one or more Global IP address and vice versa in order to provide Internet access to the local hosts.
- Also, it does the translation of port numbers i.e. masks the port number of the host with another port number, in the packet that will be routed to destination.
- It then makes the corresponding entries of IP address and port number in the NAT table. NAT generally operates on router or firewall.

Address Translation

- All of the outgoing packets go through the NAT router, which replaces the source address in the packet with the global NAT address.
- All incoming packets also pass through the NAT router, which replaces the destination address in the packet with the appropriate private address.

Translation Table

- There may be tens or hundreds of private IP addresses, each belonging to one specific host. The problem is solved if the NAT router has a translation table.

Using One IP Address

- In its simplest form, a translation table has only two columns: the private address and the external address.
- When the router translates the source address of the outgoing packet, it also makes note of the destination address— where the packet is going.
- When the response comes back from the destination, the router uses the source address of the packet (as the external address) to find the private address of the packet.

Using a Pool of IP Addresses

- The use of only one global address by the NAT router allows only one private-network host to access a given external host. To remove this restriction, the NAT router can use a pool of global addresses.
- For example, instead of using only one global address (200.24.5.8), the NAT router can use four addresses (200.24.5.8, 200.24.5.9, 200.24.5.10, and 200.24.5.11). In this case, four private-network hosts can communicate with the same external host at the same time because each pair of addresses defines a separate connection.
- However, there are still some drawbacks. No more than four connections can be made to the same destination.
- No private-network host can access two external server programs (e.g., HTTP and TELNET) at the same time.
- And, likewise, two private-network hosts cannot access the same external server program (e.g., HTTP or TELNET) at the same time.

Using Both IP Addresses and Port Addresses

- To allow a many-to-many relationship between private-network hosts and external server programs, we need more information in the translation table.
- For example, suppose two hosts inside a private network with addresses 172.18.3.1 and 172.18.3.2 need to access the HTTP server on external host 25.8.3.2.
- If the translation table has five columns, instead of two, that include the source and destination port addresses and the transport-layer protocol, the ambiguity is eliminated.

Advantages of NAT

- NAT conserves legally registered IP addresses.
- It provides privacy as the device IP address, sending and receiving the traffic, will be hidden.
- Eliminates address renumbering when a network evolves.

Disadvantage of NAT

- Translation results in switching path delays.
- Certain applications will not function while NAT is
- enabled. Complicates tunneling protocols such as IPsec.

Also, router being a network layer device, should not tamper with port numbers (transport layer) but it has to do so because of NAT.

5. FORWARDING OF IP PACKETS

- When IP is used as a **connectionless protocol, forwarding is based on the destination address of the IP datagram;**
- When the IP is used as a **connection-oriented protocol, forwarding is based on the label attached to an IP datagram.**

1. Forwarding Based on Destination Address

Forwarding requires a host or a router to have a forwarding table.

- When a host has a packet to send or when a router has received a packet to be forwarded, it looks at this table to find the next hop to deliver the packet to.
- In classless addressing, the whole address space is one entity; there are no classes. This means that forwarding requires one row of information for each block involved.

Datagram Forwarding in IP

Forwarding is the process of taking a packet from an input and sending it out on the appropriate output.

Routing is the process of building up the tables that allow the correct output for a packet to be determined.

Datagram Forwarding Algorithm

```
if (NetworkNum of destination = NetworkNum of one of my interfaces) then
        deliver packet to destination over that interface
else
        if (NetworkNum of destination is in my forwarding table)    then
                deliver packet to NextHop router
        else
                deliver packet to default router
```

Note :For a host with only one interface and only a default router

```
if (NetworkNum of destination = my NetworkNum) then
                deliverpacket to destination directly
else
                deliver packet to default router
```

A classless forwarding table needs to include four pieces of information:

1. **The mask**
2. **The network addresses**
3. **The interface number**
4. **The IP address of the next router**

- For example, if n is 26 and the network address is 180.70.65.192, then one can combine the two as one piece of information: 180.70.65.192/26.
- Figure shows a simple forwarding module and forwarding table for a router with only three interfaces.
- The job of the forwarding module is to search the table, row by row.
- In each row, the n leftmost bits of the destination address (prefix) are kept and the rest of the bits (suffix) are set to 0s.
- If the resulting address, matches with the address in the first column, the information in the next two columns is extracted; otherwise the search continues.

Normally, the last row has a default value in the first column, which indicates all

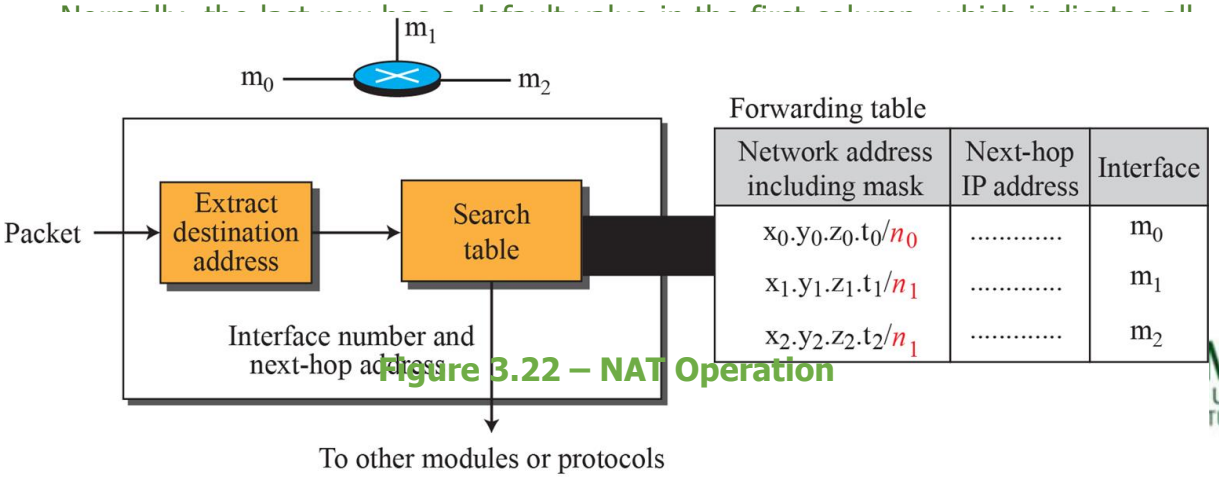
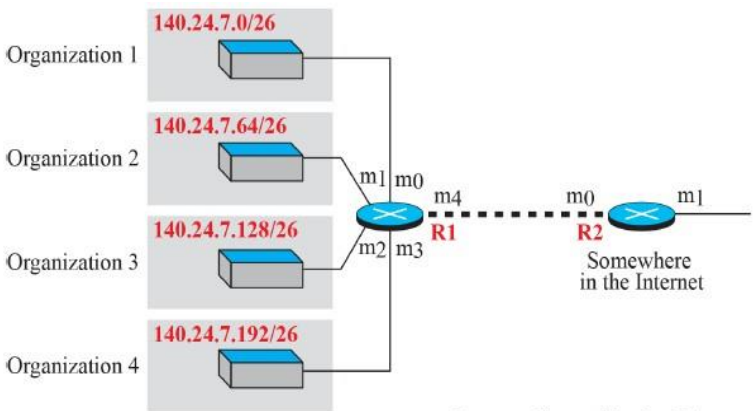


Figure 3.22 – NAT Operation

- For example, instead of giving the 180.70.65.192/26, we can give the value of the 26 leftmost bits as shown
- below. address-mask 10110100 01000110 combination of 01000001 11

Address Aggregation

- **When we use classful addressing,**
- There is only one entry in the forwarding table for each site outside the organization.
- The entry defines the site even if that site is subnetted.
- When a packet arrives at the router, the router checks the corresponding entry and forwards the packet accordingly.
- **When we use classless addressing,**
- The number of forwarding table entries will increase.
- This is because the intent of classless addressing is to divide up the whole address space into manageable blocks.
- The increased size of the table results in an increase in the amount of time needed to search the table.
- In Figure 3.23 we have two routers.
- R1 is connected to networks of four organizations that each use 64 addresses.
- R2 is somewhere far from R1.
- R1 has a longer forwarding table because each packet must be correctly routed to the appropriate organization.
- R2 can have a very small forwarding table.



Forwarding table for R2

Network address/mask	Next-hop address	Interface
140.24.7.0/24	----------	m0
0.0.0.0/0	default router	m1

Forwarding table for R1

Network address/mask	Next-hop address	Interface
140.24.7.0/26	----------	m0
140.24.7.64/26	----------	m1
140.24.7.128/26	----------	m2
140.24.7.192/26	----------	m3
0.0.0.0/0	address of R2	m4

Figure 3.23 – Address Aggregation

- This is called address aggregation because the blocks of addresses for four organizations are aggregated into one larger block.
- R2 would have a longer forwarding table if each organization had addresses that could not be aggregated into one block.

Hierarchical Routing

- National ISPs are divided into regional ISPs, and regional ISPs are divided into local ISPs.
- If the forwarding table has a sense of hierarchy like the Internet architecture, the forwarding table can decrease in size.

Local ISP.

- A local ISP can be assigned a single, but large, block of addresses with a certain prefix length.
- The local ISP can divide this block into smaller blocks of different sizes, and assign these to individual users and organizations, both large and small.
- If the block assigned to the local ISP starts with a.b.c.d/n, the ISP can create blocks starting with e.f.g.h/m, where m may vary for each customer and is greater than n.
- All customers of the local ISP are defined as a.b.c.d/n to the rest of the Internet.
- Every packet destined for one of the addresses in this large block is routed to the local ISP.

Geographical Routing

- To decrease the size of the forwarding table even further, we need to extend hierarchical routing to include geographical routing.
- We must divide the entire address space into a few large blocks.

Forwarding Table Search Algorithms

- The forwarding table can be divided into buckets, one for each prefix.
- The router first tries the longest prefix.
- If the destination address is found in this bucket, the search is complete.
- If the address is not found, the next prefix is searched, and so on.
- It is obvious that this type of search takes a long time.

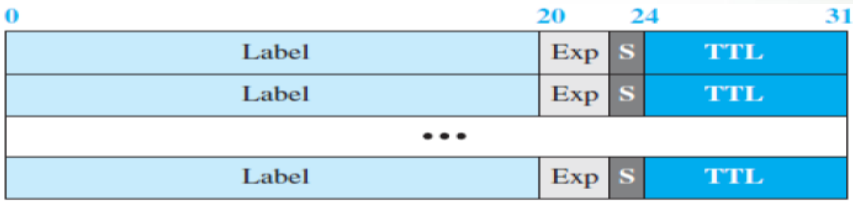


Figure 3.24- MPLS Header made of a stack of labels

3.5.2 Forwarding Based on Label

- In a connectionless network, a router forwards a packet based on the destination address in the header of the packet.
- In a connection-oriented network, a switch forwards a packet based on the label attached to the packet.
- Routing is normally based on searching the contents of a table; switching can be done by accessing a table using an index.

Multi-Protocol Label Switching (MPLS)

- In this standard, some conventional routers can be replaced by MPLS routers, which can behave like a router and a switch.
- When behaving like a router, MPLS can forward the packet based on the destination address;
- When behaving like a switch, it can forward a packet based on the label.

A New Header

- The IPv4 packet format does not allow this extension.
- The solution is to encapsulate the IPv4 packet in an MPLS packet.
- The whole IP packet is encapsulated as the payload in an MPLS packet and an MPLS header is added.
- The MPLS header is actually a stack of subheaders that is used for multilevel hierarchical switching.
- Figure shows the format of an MPLS header in which each subheader is 32 bits (4 bytes) long.
- **Label.** This 20-bit field defines the label that is used to index the forwarding table in the router.
- **Exp.** This 3-bit field is reserved for experimental purposes.
- **S.** The one-bit stack field defines the situation of the subheader in the stack. When the bit is 1, it means that the header is the last one in the stack.

TTL. This 8-bit field is similar to the TTL field in the IP datagram. Each visited router decrements the value of this field. When it reaches zero, the packet is discarded to prevent looping.

NETWORK LAYER PROTOCOLS

3.6 INTERNET PROTOCOL (IP)

- The main protocol, Internet Protocol version 4 (IPv4), is responsible for packetizing, forwarding, and delivery of a packet at the network layer.
- IPv4 is an unreliable datagram protocol—a best-effort delivery service.
- The term best-effort means that IPv4 packets can be corrupted, be lost, arrive out of order, or be delayed, and may create congestion for the network.
- If reliability is important, IPv4 must be paired with a reliable transport-layer protocol such as TCP.
- IPv4 is also a connectionless protocol that uses the datagram approach.
- This means that each datagram is handled independently, and each datagram can follow a different route to the destination.

  This implies that datagrams sent by the same source to the same destination could arrive out of order.

PACKET FORMAT

- The IP datagram, like most packets, consists of a header followed by a number of bytes of data. The format of the header is shown in Figure 3.25
- **Version**: The **Version field** specifies the version of IP. The current version of IP is 4, and it is sometimes called IPv4.
- **HLen**: The next field, **HLen,** specifies the length of the header in 32-bit words. When there are no options, which is most of the time, the header is 5 words (20 bytes) long

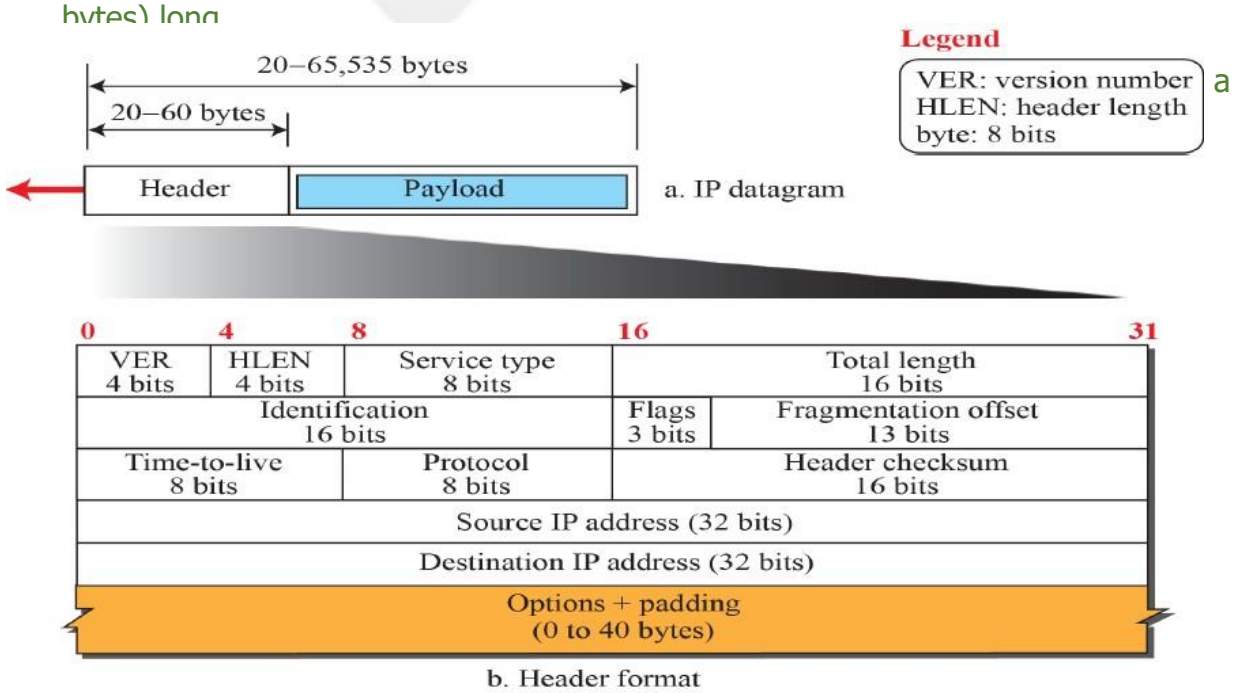


Figure 3.25 – IPv4 Packet Format

- **Length**: The next 16 bits of the header contain the **Length** of the datagram, including the header. Unlike the HLen field, the Length field counts bytes rather than words. Thus, the maximum size of an IP datagram is 65,535 bytes.
- **TTL** : T**ime To Live** field is used to catch packets that have been going around in routing loops and discard them, rather than let them consume resources indefinitely. TTL is set to a specific number of seconds that the packet would be allowed to live, and routers along the path would decrement this field by 1asthey forwarded the packet. Set it too high and packets could circulate rather a lot before getting dropped; set it too low and they may not reach their destination. The value 64 is the current default.
- **Ident :** It allows the destination host to determine which datagram a newly arrived fragment belongs to. All the fragment of a datagram contain the same identification value
- **Flags :** DF – Don't fragment, MF- More fragment
- **Offset :** Max 8192 fragment per datagram
- **Protocol**: This field is simply a demultiplexing key that identifies the higher-level protocol to which this IP packet should be passed.
- **Checksum**: This field is used to detect transmission errors.
- ***Source and Destination Addresses***:
- These 32-bit source and destination address fields define the IP address of the source and destination respectively.
- The source host should know its IP address. The source address is required to allow recipients to decide if they want to accept the packet and to enable them to reply.
- The destination IP address is either known by the protocol that uses the service of IP or is provided by the DNS
- ***Options***:
- A datagram header can have up to 40 bytes of options.
- Options can be used for network testing and debugging.
- Although options are not a required part of the IP header, option processing is required of the IP software.
- This means that all implementations must be able to handle options if they are present in the header.
- ***Payload***:

Payload, or data, is the main reason for creating a datagram.

Payload is the packet coming from other protocols that use the service of IP.

Comparing a datagram to a postal package, payload is the content of the package; the header is only the information written on the package.

Example:1

- An IPv4 packet has arrived with the first 8 bits as (01000010)2 the receiver discards the packet. Why?
- **Solution**
- There is an error in this packet. The 4 leftmost bits (0100)2 show the version, which is correct. The next 4 bits (0010)2 show an invalid header length (2 × 4 = 8). The minimum number of bytes in the header must be 20. The packet has been corrupted in transmission.

Example:2

- In an IPv4 packet, the value of HLEN is (1000)2. How many bytes of options are being carried by this packet?
- **Solution**

The HLEN value is 8, which means the total number of bytes in the header is 8 × 4, or 32 bytes. The first 20 bytes are the base header, the next 12 bytes are the options.

Example:3

- In an IPv4 packet, the value of HLEN is 5, and the value of the total length field is (0028)16. How many bytes of data are being carried by this packet?
- **Solution**

The HLEN value is 5, which means the total number of bytes in the header is 5 × 4, or 20 bytes (no options). The total length is (0028)16 or 40 bytes, which means the packet is carrying 20 bytes of data (40 – 20).

Example:4

- An IPv4 packet has arrived with the first few hexadecimal digits as shown.

$(45000028000100000102\ldots)_{16}$

- How many hops can this packet travel before being dropped? The data belong to what upper-layer protocol?

Solution

To find the time-to-live field, we skip 8 bytes (16 hexadecimal digits). The time-to-live field is the ninth byte, which is (01)16. This means the packet can travel only one hop. The protocol field is the next byte (02)16, which means that the upper-layer protocol is IGMP.

3.6.1 FRAGMENTATION AND REASSEMBLY

- The physical network, over which IP is running, may not support long packets. For this reason, IP supports a **fragmentation and reassembly process**.
- For example, an Ethernet can accept packets up to 1500 bytes long, while FDDI packets may be 4500 bytes long.
- The central idea here is that every network type has a ***maximum transmission unit*** **(MTU),** which is the largest IP datagram that it can carry in a frame.

When a host sends an IP datagram, it can choose any size that it wants.

- A reasonable choice is the MTU of the network to which the host is directly attached.
- Fragmentation typically occurs in a router when it receives a datagram that it wants to forward over a network that has an MTU that is smaller than the received datagram.
- To enable these fragments to be reassembled at the receiving host, they all carry the same identifier in the **Ident field.**
- **Example:** H5 wants to send a datagram to H8
- The unfragmented packet, shown in figure (a) , has 1400 bytes of data and a 20-byteIP header.
- When the packet arrives at router R2, which has MTU of532 bytes, it has to be fragmented.

A first fr

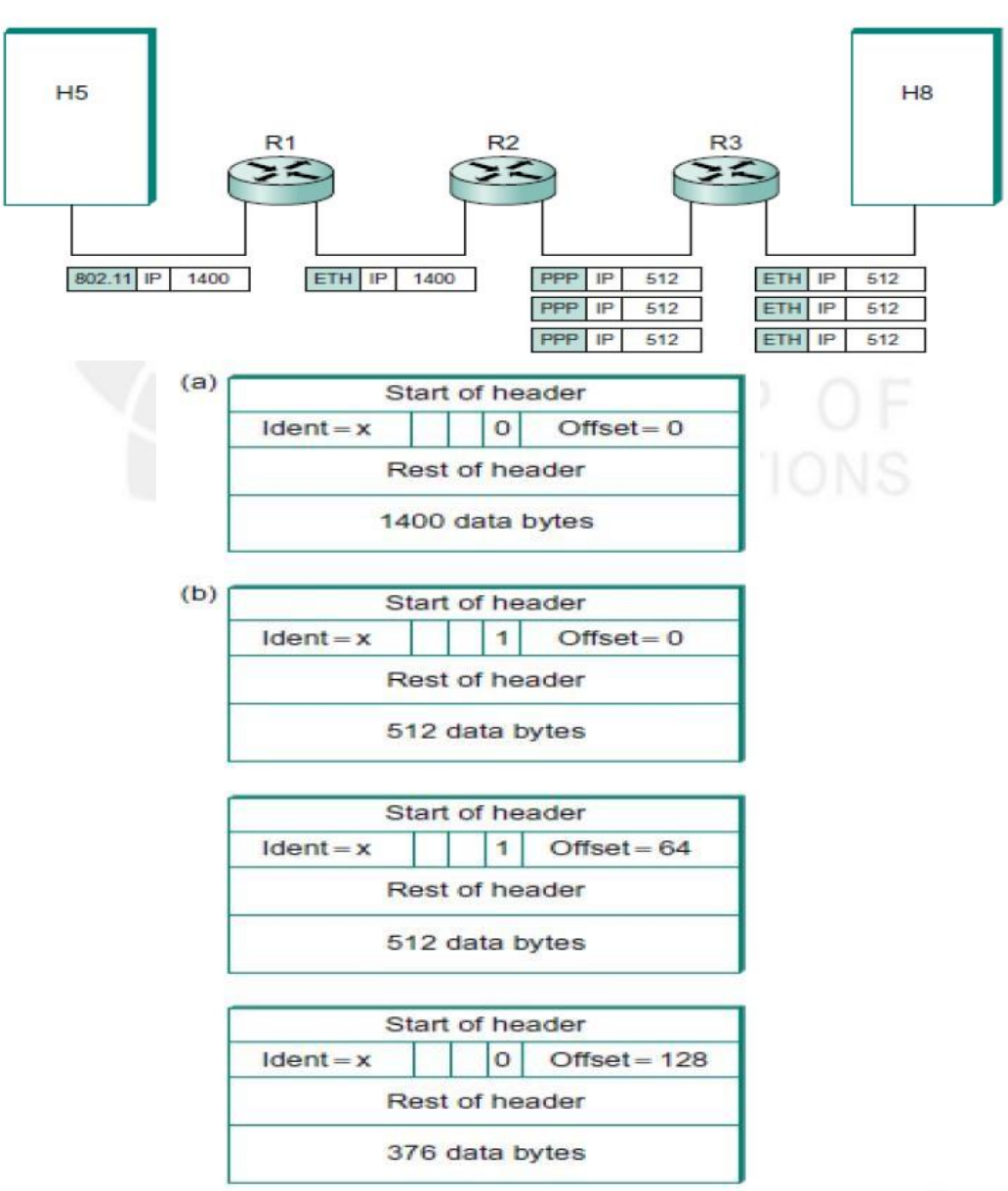


Figure 3.26 - Header fields used in IP fragmentation: (a) unfragmented packet; (b) fragmented packets.

R.M.K GROUP OF INSTITUTIONS

- The router sets the Mbit in the Flags field, and it sets the Offset to 0, since this fragment contains the first part of the original datagram. The data carried in the second fragment starts with the 513th byte of the original data, so the Offset field in this header is set to 64, which is 512÷8.
- The third fragment contains the last 376 bytes of data, and the offset is now 2×512÷8 = 128.Since this is the last fragment, the Mbit is not set.

Example:5

A packet has arrived with an M bit value of 0. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?

Solution

If the M bit is 0, it means that there are no more fragments; the fragment is the last one. However, we cannot say if the original packet was fragmented or not. A non fragmented packet is considered the last fragment.

Example:6

A packet has arrived with an M bit value of 1. Is this the first fragment, the last fragment, or a middle fragment? Do we know if the packet was fragmented?

Solution

If the M bit is 1, it means that there is at least one more fragment. This fragment can be the first one or a middle one, but not the last one. We don't know if it is the first one or a middle one; we need more information (the value of the fragmentation offset).

Example:7

A packet has arrived with an M bit value of 1 and a fragmentation offset value of 0. Is this the first fragment, the last fragment, or a middle fragment?

Solution

Because the M bit is 1, it is either the first fragment or a middle one. Because the offset value is 0, it is the first fragment.

Example:8

A packet has arrived in which the offset value is 100. What is the number of the first byte? Do we know the number of the last byte?

Solution

To find the number of the first byte, we multiply the offset value by 8. This means that the first byte number is 800. We cannot determine the number of the last byte unless we know the length of the data.

Example:9

A packet has arrived in which the offset value is 100, the value of HLEN is 5, and the value of the total length field is 100. What are the numbers of the first byte and the last byte?

Solution

The first byte number is 100 × 8 = 800. The total length is 100 bytes, and the header length is20 bytes (5 × 4), which means that there are 80 bytes in this

3.6.2 OPTIONS

- The header of the IPv4 datagram is made of two parts: a fixed part and a variable part.
- The fixed part is 20 bytes long.
- The variable part comprises the options that can be a maximum of 40 bytes to preserve the boundary of the header.
- Options, as the name implies, are not required for a datagram. They can be used for network testing and debugging.
- Although options are not a required part of the IPv4header, option processing is required of the IPv4 software.
- This means that all implementations must be able to handle options if they are present in the header. Options are divided into two broad categories: single-byte options and multiple-byte options.

Single-Byte Options

- There are two single-byte options.

No Operation

- A no-operation option is a 1-byte option used as a filler between options.

End of Option

- An end-of-option option is a 1-byte option used for padding at the end of the option field. It, however, can only be used as the last option.

Multliple-Byte Options

- There are four multiple-byte options.

Record Route

- A record route option is used to record the Internet routers that handle the datagram. It can list up to nine router addresses. It can be used for debugging and management purposes.

Strict Source Route

- A strict source route option is used by the source to predetermine a route for the datagram as it travels through the Internet.
- Dictation of a route by the source can be useful for several purposes.
- The sender can choose a route with a specific type of service, such as minimum delay or maximum throughput.

Loose Source Route

A loose source route option is similar to the strict source route, but it is less rigid. Each router in the list must be visited, but the datagram can visit other routers as well.

Timestamp

- A timestamp option is used to record the time of datagram processing by a router.
- The time is expressed in milliseconds from midnight, Universal time or Greenwich meantime. Knowing the time a datagram is processed can help users and managers track the behavior of the routers in the Internet.

3.6.3 SECURITY OF IPV4 DATAGRAMS

- There are three security issues that are particularly applicable to the IP protocol: packet sniffing, packet modification, and IP spoofing.

Packet Sniffing

- An intruder may intercept an IP packet and make a copy of it.
- Packet sniffing is a passive attack, in which the attacker does not change the contents of the packet.
- This type of attack is very difficult to detect because the sender and the receiver may never know that the packet has been copied.
- Although packet sniffing cannot be stopped, encryption of the packet can make the attacker's effort useless. The attacker may still sniff the packet, but the content is not detectable.

Packet Modification

- The second type of attack is to modify the packet.
- The attacker intercepts the packet, changes its contents, and sends the new packet to the receiver.
- The receiver believes that the packet is coming from the original sender.
- This type of attack can be detected using a data integrity mechanism.
- The receiver, before opening and using the contents of the message, can use this mechanism to make sure that the packet has not been changed during the transmission.

IP Spoofing

- An attacker can masquerade as somebody else and create an IP packet that carries the source address of another computer.
- An attacker can send an IP packet to a bank pretending that it is coming from one of the customers. This type of attack can be prevented using an origin authentication mechanism.

IPSec

- The IP packets today can be protected from the previously mentioned attacks using a protocol called IPSec (IP Security).
- This protocol, which is used in conjunction with the IP protocol, creates a connection-oriented service between two entities in which they can exchange IP packets without worrying about the three attacks discussed above.
- IPSec provides the following four services:
- ***Defining Algorithms and Keys*.** The two entities that want to create a secure channel between them can agree on some available algorithms and keys to be used for security purposes.
- ***Packet Encryption*.** The packets exchanged between two parties can be encrypted for privacy using one of the encryption algorithms and a shared key agreed upon in the first step. This makes the packet sniffing attack useless.
- ***Data Integrity*.** Data integrity guarantees that the packet is not modified during the transmission. If the received packet does not pass the data integrity test, it is discarded. his prevents the second attack, packet modification, described above.
- ***Origin Authentication*.** IPSec can authenticate the origin of the packet to be sure that the packet is not created by an imposter. This can prevent IP spoofing attacks as described above.

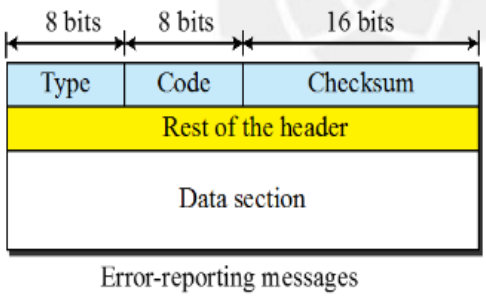
3.7 ICMP v4

- The IPv4 has no error-reporting or error-correcting mechanism.
- The **Internet Control Message Protocol version 4 (ICMPv4)** has been designed to compensate for the above two deficiencies.
- It is a companion to the IP protocol. ICMP itself is a network-layer protocol.
- However, its messages are not passed directly to the data-link layer as would be expected.
- Instead, the messages are first encapsulated inside IP datagrams before going to the lower layer.
- When an IP datagram encapsulates an ICMP message, the value of the protocol field in the IP datagram is set to 1 to indicate that the IP payroll is an ICMP message.

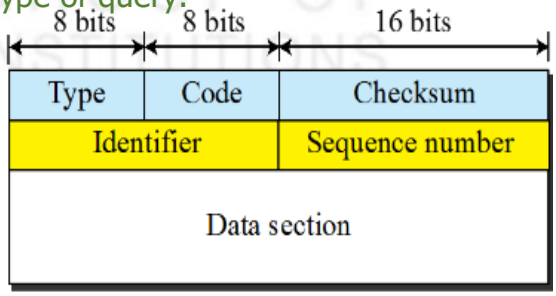
3.7.1 MESSAGES

- ICMP messages are divided into two broad categories: error-reporting messages and query messages.
- The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.
- The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host.
- For example, nodes can discover their neighbours. Also, hosts can discover and learn about routers on their network and routers can help a node redirect its messages.
- An ICMP message has an 8-byte header and a variable-size data section.
- Although the general format of the header is different for each message type, the first 4 bytes are common to all.
- As Figure shows, the first field, ICMP type, defines the type of the message.
- The code field specifies the reason for the particular message type.
- The last common field is the checksum field (to be discussed later in the chapter). The rest of the header is specific for each message type.

The data section in error messages carries information for finding the original packet that had the error. In query messages, the data section carries extra information based on the type of query.



Error-reporting messages



Query messages

Type and code values

Error-reporting messages	Query messages
03: Destination unreachable (codes 0 to 15)	08 and 00: Echo request and reply (only code 0)
04: Source quench (only code 0)	13 and 14: Timestamp request and reply (only code 0)
05: Redirection (codes 0 to 3)	
11: Time exceeded (codes 0 and 1)	
12: Parameter problem (codes 0 and 1)	

Note: See the book website for more explanation about the code values.

Figure 3.27 – ICMP Message

Error Reporting Messages

- Since IP is an unreliable protocol, one of the main responsibilities of ICMP is to report some errors that may occur during the processing of the IP datagram. ICMP does not correct errors, it simply reports them.
- Error correction is left to the higher-level protocols. Error messages are always sent to the original source because the only information available in the datagram about the route is the source and destination IP addresses. ICMP uses the source IP address to send the error message to the source (originator) of the datagram.
- To make the error-reporting process simple, ICMP follows some rules in reporting messages.
  - First, no error message will be generated for a datagram having a multicast address or special address (such as this host or loopback).
  - Second, no ICMP error message will be generated in response to a datagram carrying an ICMP error message.
  - Third, no ICMP error message will be generated for a fragmented datagram that is not the first fragment.
- Note that all error messages contain a data section that includes the IP header of the original datagram plus the first 8 bytes of data in that datagram. The original datagram header is added to give the original source, which receives the error message, information about the datagram itself. The 8 bytes of data are included because the first8 bytes provide information about the port numbers (UDP and TCP) and sequence number (TCP). This information is needed so the source can inform the protocols (TCP or UDP) about the error.

Note that all error messages contain a data section that includes the IP header of the original datagram plus the first 8 bytes of data in that datagram. The original datagram header is added to give the original source, which receives the error message, information about the datagram itself. The 8 bytes of data are included because, the first 8 bytes provide information about the port numbers (UDP and TCP) and sequence number (TCP). This information is needed so the source can inform the protocols (TCP or UDP) about the error. ICMP forms an error packet, which is 3..28).

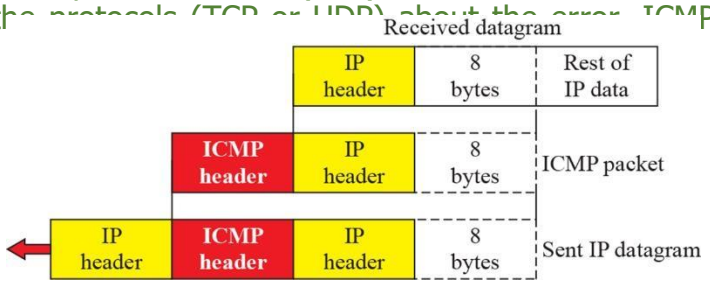


Figure 3.28 – Contents of data field for the error messages

Destination Unreachable

- The most widely used error message is the destination unreachable (type 3).
- This message uses different codes (0 to 15) to define the type of error message and the reason why a datagram has not reached its final destination.
- For example, code 0 tells thesource that a host is unreachable.
- This may happen, for example, when we use theHTTP protocol to access a web page, but the server is down.
- The message —destinationhost is not reachable‖ is created and sent back to the source.

Source Quench

- Another error message is called the source quench (type 4) message, which informs the sender that the network has encountered congestion and the datagram has been dropped.
- The source needs to slow down sending more datagrams.
- In other words, ICMP adds a kind of congestion control mechanism to the IP protocol by using this type of message.

Redirection Message

- The redirection message (type 5) is used when the source uses a wrong router to send out its message.
- The router redirects the message to the appropriate router, but informs the source that it needs to change its default router in the future. The IP address of the default router is sent in the message.
- When the TTL value becomes 0, the datagram is dropped by the visiting router and a time exceeded message (type 11) with code 0 is sent to the source to inform it about the situation.

  The time-exceeded message (with code 1) can also be sent when not all fragments of a datagram arrive within a predefined period of time.

Parameter Problem

A parameter problem message (type 12) can be sent when either there is a problem in the header of a datagram (code 0) or some options are missing or cannot be interpreted (code 1).

Query Messages

- Interestingly, query messages in ICMP can be used independently without relation to an IP datagram. Of course, a query message needs to be encapsulated in a datagram, as a carrier.
- Query messages are used to probe or test the liveliness of hosts or routers in the Internet, find the one-way or the round-trip time for an IP datagram between two devices, or even find out whether the clocks in two devices are synchronized. Naturally, query messages come in pairs: request and reply.
- The echo request (type 8) and the echo reply (type 0) pair of messages are used by a host or a router to test the liveliness of another host or router.
- A host or router sends an echo request message to another host or router; if the latter is alive, it responds with an echo reply message.
- It has two debugging tools: ping and trace route.
- The timestamp request (type 13) and the timestamp reply (type 14) pair of messages are used to find the round-trip time between two devices or to check whether the clocks in two devices are synchronized.
- The timestamp request message sends a 32-bitnumber, which defines the time the message is sent.
- The timestamp reply resends that number, but also includes two new 32-bit numbers representing the time the request was received and the time the response was sent.
- If all timestamps represent Universal time, the sender can calculate the one-way and round-trip time.

3.8 UNICAST ROUTING ALGORITHMS

- **FORWARDING:** Forwarding consists of taking a packet, looking at its destination address, consulting a table, and sending the packet in a direction determined by that table.
- **ROUTING:** Routing is the process by which forwarding tables are built.

DIFFERENCE BETWEEN FORWARDING TABLE AND ROUTING TABLE

- The **forwarding table** as shown in Figure 3.29 is used when a packet is being forwarded and contains mapping from a network prefix to an outgoing interface and some MAC information, such as the Ethernet address of the next hop.

(a)

Prefix/Length	Next Hop
18/8	171.69.245.10

Figure 3.29 Forwarding table

- The routing table as shown in Figure 3.30 is the table that is built up by the routing algorithms.

Prefix/Length	Interface	MAC Address
18/8	if0	8:0:2b:e4:b:1:2

Figure 3.30 Routing Table

NETWORK AS A GRAPH

- A network can be represented as a graph. Nodes are denoted as Vertices and Links are denoted as Edges.

UNICAST ROUTING ALGORITHMS:

1. Intra domain routing Algorithm
    1. Distance vector routing
    2. Link state routing
2. Inter Domain Routing Algorithm
    1. Path Vector Routing Algorithm

3.8.1 DISTANCE-VECTOR ROUTING ALGORITHM

- Each node constructs a one-dimensional array (a vector) containing the —distances‖ (costs) to all other nodes.

Each node knows the cost of the link to each of its directly connected neighbors.

Working of Distance Vector Routing Algorithm(Figure 3.31)

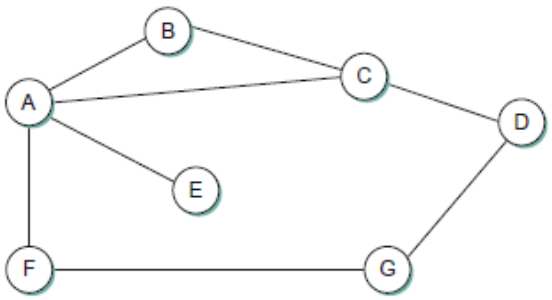


Figure 3.31 Distance Vector Routing Algorithm

- The initial distances stored at each node to reach every other node is shown in figure 3.32.
- The initial routing table of node A is shown in figure 3.33.
- Every node sends a message to its directly connected neighbours containing its personal list of distances.
- The initial routing table of all nodes is shown below:

Destination	Cost	NextHop
B	1	B
C	1	C
D	∞	—
E	1	E
F	1	F
G	∞	—

Figure 3.32 Initial Routing Table

Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	∞	1	1	∞
B	1	0	1	∞	∞	∞	∞
C	1	1	0	1	∞	∞	∞
D	∞	∞	1	0	∞	∞	1
E	1	∞	∞	∞	0	∞	∞
F	1	∞	∞	∞	∞	0	1
G	∞	∞	∞	1	∞	1	0

Figure 3.33 Initial routing table of all nodes

Distance Vector Algorithm

- The algorithm is run by its node independently and asynchronously.

Step: 1 Initialize or create initial vectors for the node

Distance to itself = 0.

Distance to ALL other nodes directly = 1.

Distance to ALL other nodes indirectly = infinity number.

Step: 2 Update or improve the vector with the vector received from a neighbour.

- Allows all entries (cells) in the vector to be updated after receiving a new vector.

Step: 3 End of Distance vector

Example:

- Node F tells node A that it can reach node G at a cost of 1.
- A also knows it can reach F at a cost of 1, so it adds these costs to get the cost of reaching G by means of F.
- This total cost of 2 is less than the current cost of infinity, so A records that it can reach G at a cost of 2 by going through F.
- The final routing table at A is shown in figure 3.34.

Destination	Cost	NextHop
B	1	B
C	1	C
D	2	C
E	1	E
F	1	F
G	2	F

Figure 3.34 Final routing table at A

- Thus all nodes in the network apply a similar step as of A to generate their final routing tables.
- The process of getting consistent routing information to all the nodes is called ***convergence***.
- When does a given node decide to send a routing update to its neighbors?
- Periodic update - each node automatically sends an update message periodically even if nothing has changed.
- Triggered update – whenever a node notices a link failure or receives an update from one of its neighbors that causes it to change one of the routes in its routing table.

Shown in figure 3.35 are the final distances stored at each node.

Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	1	1	2	1	1	2
B	1	0	1	2	2	2	3
C	1	1	0	1	2	2	2
D	2	2	1	0	3	2	1
E	1	2	2	3	0	2	3
F	1	2	2	2	2	0	1
G	2	3	2	1	3	1	0

Figure 3.35 Final distances stored at each node

Reference video :
https://www.youtube.com/watch?v=dmS1t2twFrI

What happens when a link or node fails?

- The nodes that notice first send new lists of distances to their neighbors, and normally the system settles down fairly quickly to a new state.

How does a node detect a failure?

- A node continually tests the link to another node by sending a control packet and seeing if it receives an acknowledgment.
- A node determines that the link (or the node at the other end of the link) is down if it does not receive the expected periodic routing update for the last few update cycles.

Count to Infinity

- A problem with distance-vector routing is that any decrease in cost propagates quickly, but any increase in cost will propagate slowly.
- For a routing protocol to work properly, if a link is broken (cost becomes infinity), every other router should be aware of it immediately, but in distance-vector routing, this takes some time.
- The problem is referred to as count to infinity. Ex: A→E Link is failure.
- It sometimes takes several updates before the cost for a broken link is recorded as infinity by all routers.

Split Horizon

- The technique to improve the time to stabilize routing is called split horizon. The idea is that when a node sends a routing update to its neighbours, it does not send those routes it learned from each neighbour back to that neighbour.

Poison Reverse

- Using the split-horizon strategy has one drawback.
- Normally, the corresponding protocol uses a timer, and if there is no news about a route, the node deletes the route from it stable.
- The idea is that when a node sends a routing update to its neighbours, it does not send those routes it learned from each neighbour back to that neighbour.

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.

3.8.2 LINK STATE ROUTING ALGORITHM

- Link-state routing is an intra-domain routing protocol.
- Each node is capable of finding out the state of the link to its neighbours (up or down) and the cost of each link.
- Every node knows how to reach its directly connected neighbours.
- Link-state routing protocols use two mechanisms:
- **Reliable Flooding** - reliable dissemination of link-state information,
- **Route calculation** - calculation of routes from the sum of all the accumulated link-state knowledge.

Reliable flooding

- It is the process of making sure that all the nodes participating in the routing protocol get a copy of the link-state information from all the other nodes.
- A node sends its link-state information out on all of its directly connected links.
- Each node that receives this information then forwards it out on all of its links.
- This process continues until the information has reached all the nodes in the network.
- Each node creates a packet called as a link-state packet (LSP), which contains the following information:
- The ID of the node that created the LSP.
- A list of directly connected neighbours of that node, with the cost of the link to each one.
- A sequence number.
- A time to live for this packet.

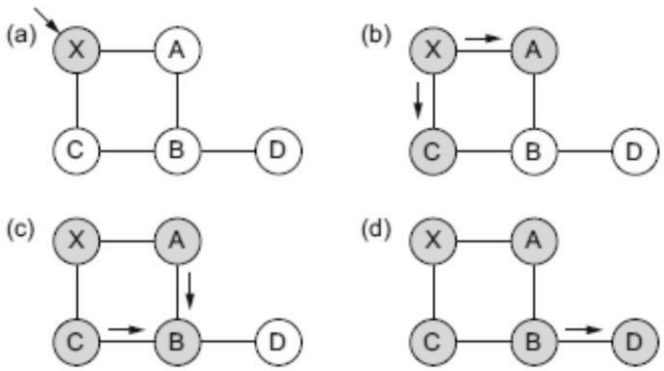


Figure 3.36 Reliable flooding

Working of Reliable Flooding(Figure 3.36)

- LSP arrives at node X, which sends it to neighbours A and C .
- A and C do not send it back to X, but send it on to B.
- Since B receives two identical copies of the LSP, it will accept whichever arrived first and ignore the second as a duplicate.
- It then passes the LSP onto D, which has no neighbours to flood it to, and the process is complete.

When are LSPs generated?

- On expiry of a periodic timer.
- When there is a change in topology.

Design goals of a link-state protocol's flooding mechanism

- The newest information must be flooded to all nodes as quickly as possible.
- Old information must be removed from the network and not allowed to circulate.

Why do LSPs have sequence numbers?

- To make sure that old information is replaced by newer information.
- Each time a node generates a new LSP, it increments the sequence number by 1.
- LSPs also carry a time to live. This is used to ensure that old link-state information is eventually removed from the network.

A node always decrements the TTL of a newly received LSP before flooding it to its neighbours.

Forward search algorithm. [Dijkstra's Algorithm]

Two lists known as Tentative and Confirmed are used.

- Each of these lists contains a set of entries of the form (Destination, Cost, NextHop) as shown in Figure 3.38.
- The algorithm works as follows:
- Initialize the Confirmed list with an entry for myself; this entry has a cost of 0.
- For the node just added to the Confirmed list in the previous step, call it node Next and select its LSP.
- For each neighbor (Neighbor) of Next, calculate the cost (Cost) to reach this Neighbor as the sum of the cost from myself to Next and from Next to Neighbor.
- (a) If Neighbor is currently on neither the Confirmed nor the Tentative list, then add (Neighbor, Cost, NextHop) to the Tentative list, where NextHop is the direction I go to reach Next.
- (b) If Neighbor is currently on the Tentative list, and the Cost is less than the currently listed cost for Neighbor, then replace the current entry with (Neighbor, Cost, nNextHop), where NextHop is the direction I go to reach Next.
- If the Tentative list is empty, stop. Otherwise, pick the entry from the Tentative list with the lowest cost, move it to the Confirmed list, and return to step 2.
- **Properties of the link-state routing algorithm**
- It stabilizes quickly.
- It does not generate much traffic.
- It responds rapidly to topology changes or node failures.
- **Difference between the distance-vector and link-state algorithms**
- In distance-vector, each node talks only to its directly connected neighbors, but it tells them everything it has learned (i.e., distance to all nodes).
- In link-state, each node talks to all other nodes, but it tells them only what it knows for sure (i.e., only the state of its directly connected links).

Features of the basic link-state algorithm

- **Authentication of routing messages**— As information is dispersed from one node to many other nodes, the entire network can be impacted by bad information from one node. Hence authenticating routing messages is required. Strong cryptographic authentication is used.

Additional hierarchy— A router within a domain does not necessarily need to know how to reach every network within that domain—it may be able to get by knowing only how to get to the right area. Thus, there is a reduction in the amount of information that must be transmitted to and stored in each node.

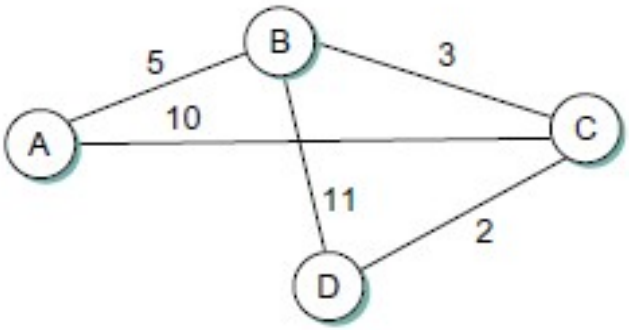


Figure 3.37 Dijkstra's algorithm

Step	Confirmed	Tentative	Comments
1	(D,0,–)		Since D is the only new member of the confirmed list, look at its LSP.
2	(D,0,–)	(B,11,B) (C,2,C)	D's LSP says we can reach B through B at cost 11, which is better than anything else on either list, so put it on Tentative list; same for C.
3	(D,0,–) (C,2,C)	(B,11,B)	Put lowest-cost member of Tentative (C) onto Confirmed list. Next, examine LSP of newly confirmed member (C).
4	(D,0,–) (C,2,C)	(B,5,C) (A,12,C)	Cost to reach B through C is 5, so replace (B,11,B). C's LSP tells us that we can reach A at cost 12.
5	(D,0,–) (C,2,C) (B,5,C)	(A,12,C)	Move lowest-cost member of Tentative (B) to Confirmed, then look at its LSP.
6	(D,0,–) (C,2,C) (B,5,C)	(A,10,C)	Since we can reach A at cost 5 through B, replace the Tentative entry.
7	(D,0,–) (C,2,C) (B,5,C) (A,10,C)		Move lowest-cost member of Tentative (A) to Confirmed, and we are all done.

Figure 3.38 Tentative and Confirmed lists

3.8.3 PATH VECTOR ROUTING ALGORITHM

- It is to allow the packet to reach its destination more efficiently without assigning costs to the route.
- Path-vector routing does not have the drawbacks of LS or DV routing because it is not based on least-cost routing.
- The best route is determined by the source using the policy it imposes on the route.
- In other words, the source can control the path.

Spanning Trees

- In path-vector routing, the path from a source to all destinations is also determined by the best spanning tree.
- The best spanning tree, however, is not the least-cost tree; it is the tree determined by the source when it imposes its own policy.
- If there is more than one route to a destination, the source can choose the route that meets its policy best.
- A source may apply several policies at the same time.
- Another common policy is to avoid some nodes as the middle node in a route.
- The spanning tree selected by A and E is such that the communication does not pass through D as a middle node.
- Similarly, the spanning tree selected by B is such that the communication does not pass through C as a middle node.

Creation of Spanning Trees(Figure 3.39)

- Path-vector routing, like distance-vector routing, is an asynchronous and distributed routing algorithm.
- The spanning trees are made, gradually and asynchronously, by each node.
- When a node is booted, it creates a path vector based on the information it can obtain about its immediate neighbor (Figure 3.40).

A pi

Figure 20.11 *Spanning trees in path-vector routing*

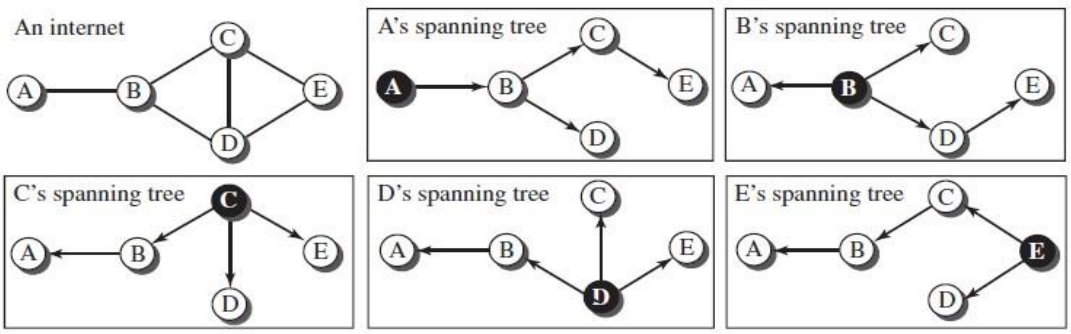


Figure 20.12 *Path vectors made at booting time*

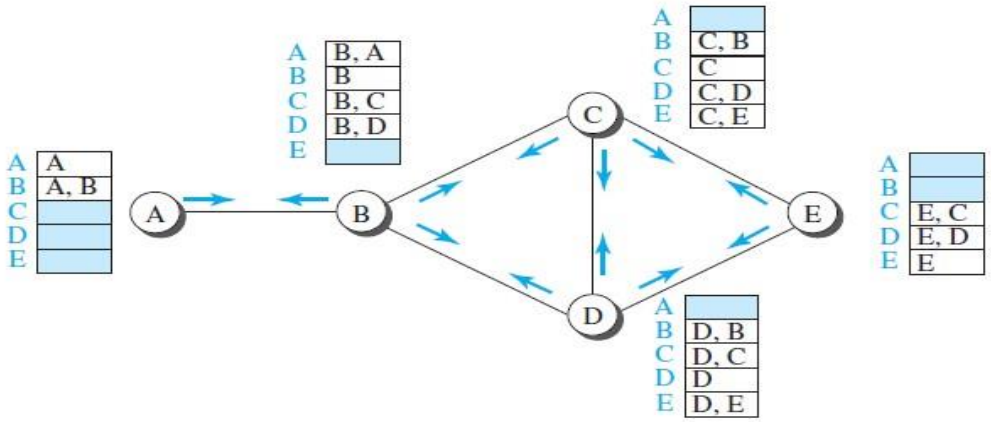


Figure 3.40 Path vectors at booting time

- Each node, after the creation of the initial path vector, sends it to all its immediate neighbours. Each node, when it receives a path vector from a neighbour, updates its path vector (as shown in Figure 3.41) using an equation
- We can define this equation as shown below.
- In this equation, the operator (+) means to add ***x*** to the beginning of the
- path. The policy is defined by selecting the best of multiple paths.
- Path-vector routing also imposes one more condition on this equation:
- If Path (**v**,***y***) includes ***x***, that path is discarded to avoid a loop in the
- path. In other words, ***x*** does not want to visit itself when it selects a
- path to ***y***. Figure shows the path vector of node C after two events.
- In the first event, node C receives a copy of B's vector, which improves its vector: now it knows how to reach node A.
- In the second event, node C receives a copy of D's vector, which does not change its vector.

As a matter of fact the vector for node C after the first event is stabilized and

$$\text{Path}(x, y) = \text{best}\ \{\text{Path}(x, y), [(x + \text{Path}(v, y)]\} \quad \text{for all } v\text{'s in the internet.}$$

9. UNICAST ROUTING PROTOCOLS

- A protocol needs to define its domain of operation, the messages exchanged, communication between routers, and interaction with protocols in other domains. There are three common protocols used in the Internet:
- Routing Information Protocol (RIP), based on the distance-vector algorithm, Open Shortest Path First (OSPF), based on the link-state algorithm, and
- Border Gateway Protocol (BGP), based on the path-vector algorithm.

a. ROUTING INFORMATION PROTOCOL (RIP)

- Widely used routing protocols in IP networks.
  RIP is the routing protocol built on the distance-vector algorithm.
  The routers advertise the cost of reaching networks.

Hop Count

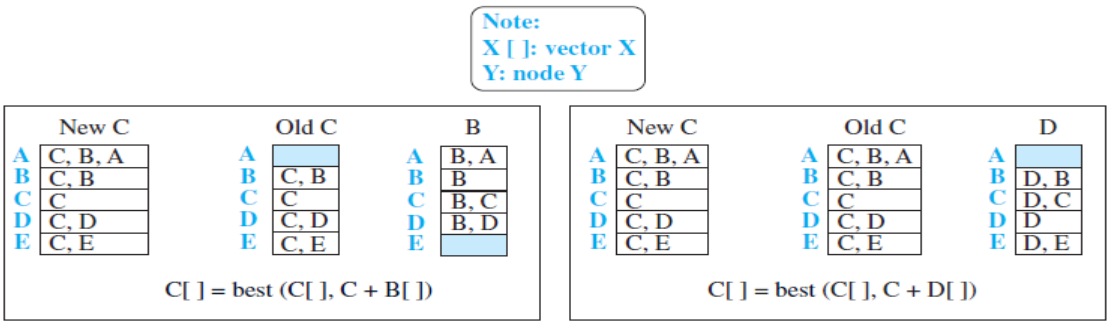
- A router in this protocol basically implements the distance-vector routing algorithm
- However, the algorithm has been modified as described below.
- RIP routers advertise the cost of reaching different networks instead of reaching other nodes in a theoretical graph.
  The cost is defined between a router and the network in which the destination host is located.
- To make the implementation of the cost simpler, the cost is defined as the number of hops, which means the number of networks a packet needs to travel through from the source router to the final destination host.

Forwarding Tables

- The routers in an autonomous system need to keep forwarding tables to forward packets to their destination networks.
- A forwarding table in RIP is a three-column table in which
  The first column is the address of the destination network,
  The second column is the address of the next router to which the packet should be forwarded, and
  The third column is the cost (the number of hops) to reach the destination network.

Reference video: https://www.youtube.com/watch?v=0efXawUgNZg

Figure 20.13 *Updating path vectors*



Event 1: C receives a copy of B's vector

Event 2: C receives a copy of D's vector

Figure 20.15 *Hop counts in RIP*

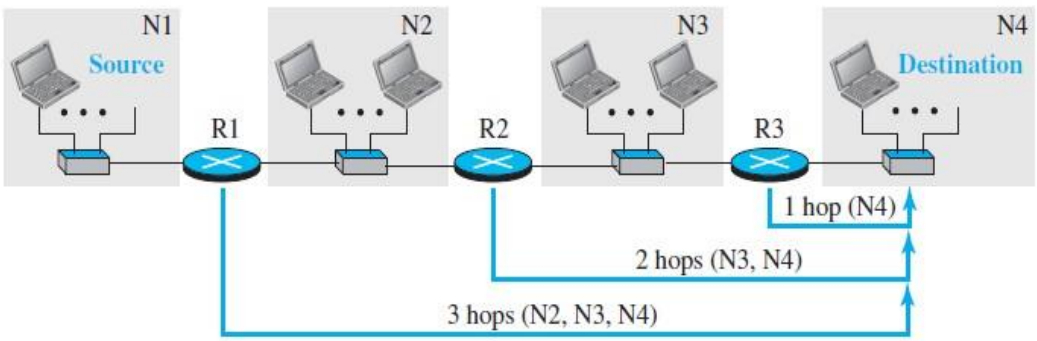


Figure 20.16 *Forwarding tables*

Forwarding table for R1

Destination network	Next router	Cost in hops
N1	——	1
N2	——	1
N3	R2	2
N4	R2	3

Forwarding table for R2

Destination network	Next router	Cost in hops
N1	R1	2
N2	——	1
N3	——	1
N4	R3	2

Forwarding table for R3

Destination network	Next router	Cost in hops
N1	R2	3
N2	R2	2
N3	——	1
N4	——	1

RIP Message Format

Two RIP processes, a client and a server, need to exchange

- messages. RIP-2 defines the format of the message, as shown in
- Figure 20.17.
- Part of the message, which we call entry, can be repeated as needed in a message.
- Each entry carries the information related to one line in the forwarding table of the router that sends the message.
- RIP has two types of messages: **Request and Response.**

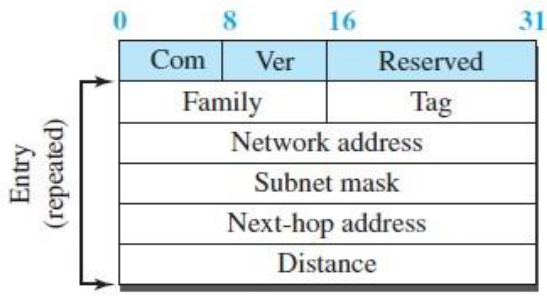
Request

- A request message is sent by a router that has just come up or by a router that has some time-out entries. A request message can ask about specific entries or all entries.

Response

- A response (or update) message can be either solicited or unsolicited.
- A solicited response message is sent only in answer to a request message.
- It contains information about the destination specified in the corresponding request message.
- An unsolicited response message, on the other hand, is sent periodically, every 30 seconds or when there is a change in the forwarding table.

Figure 20.17 *RIP message format*



Fields

Com: Command, request (1), response (2)
Ver: Version, current version is 2
Family: Family of protocol, for TCP/IP value is 2
Tag: Information about autonomous system
Network address: Destination address
Subnet mask: Prefix length
Next-hop address: Address length
Distance: Number of hops to the destination

RIP Algorithm

- RIP implements the same algorithm as the distance-vector routing algorithm
- The changes need to be made to the algorithm to enable a router to update its forwarding table:
- Instead of sending only distance vectors, a router needs to send the whole contents of its forwarding table in a response message.
- The receiver adds one hop to each cost and changes the next router field to the address of the sending router.

Timers in RIP

- RIP uses three timers to support its operation.
- The **periodic timer** controls the advertising of regular update messages.
- Each router has one periodic timer that is randomly set to a number between 25 and 35 seconds
- The timer counts down; when zero is reached, the update message is sent, and the timer is randomly set once again.
- The **expiration timer** governs the validity of a route.
  - When a router receives update information for a route, the expiration timer is set to 180 seconds for that particular route.
  - Every time a new update for the route is received, the timer is reset.
  - Every route has its own expiration timer.
- The **garbage collection timer** is used to purge a route from the forwarding table.
- When the information about a route becomes invalid, the router does not immediately purge that route from its table.
- Instead, it continues to advertise the route with a metric value of 16.
- At the same time, a garbage collection timer is set to 120 seconds for that route.
- When the count reaches zero, the route is purged from the table.
- This timer allows neighbours to become aware of the invalidity of a route prior to purging.

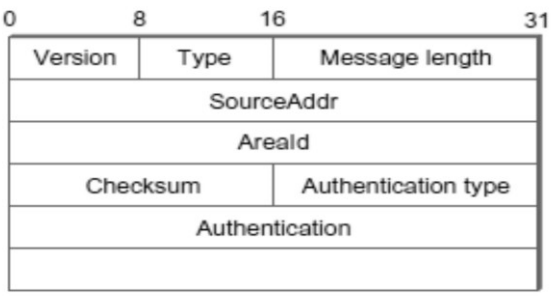
3.9.2 Open Shortest Path First (OSPF)

Open Shortest Path First (**OSPF**) is also an intradomain routing protocol like RIP, but it is based on the link-state routing protocol.

OSPF is an open protocol, which means that the specification is a public document.

OSPF Packet Format

- Version field is currently set to 2.
- Type field may take the values 1 through 5.
- The hello message (type 1) is used by a router to introduce itself to the neighbors and announce all neighbors that it already knows.
- The database description message (type 2) is normally sent in response to the hello message to allow a newly joined router to acquire the full LSDB.
- The linkstate request message (type 3) is sent by a router that needs information about specific LS.
- The link-state update message (type 4) is the main OSPF message used for building the LSDB. This message, in fact, has five different versions (router link, network link, summary link to network, summary link to AS border router, and external link), as we discussed before.
- The link-state acknowledgment message (type 5) is used to create reliability in OSPF; each router that receives a link-state update message needs to acknowledge it.
- Source Addr identifies the sender of the message
- Area Id is a 32-bit identifier of the area in which the node is located.
- The entire packet, except the authentication data, is protected by a 16-bit checksum.
- The Authentication type is 0 if no authentication is used; 1 if a simple password is used, or 2crypto



<table>
<tr><td colspan="4">LS Age</td><td>Options</td><td>Type = 1</td></tr>
<tr><td colspan="6">Link-state ID</td></tr>
<tr><td colspan="6">Advertising router</td></tr>
<tr><td colspan="6">LS sequence number</td></tr>
<tr><td colspan="4">LS checksum</td><td colspan="2">Length</td></tr>
<tr><td>0</td><td colspan="2">Flags</td><td>0</td><td colspan="2">Number of links</td></tr>
<tr><td colspan="6">Link ID</td></tr>
<tr><td colspan="6">Link data</td></tr>
<tr><td colspan="2">Link type</td><td colspan="2">Num_TOS</td><td colspan="2">Metric</td></tr>
<tr><td colspan="6">Optional TOS information</td></tr>
<tr><td colspan="6">More links</td></tr>
</table>

Packet format for a type 1 link-state advertisement (LSA)

LS Age is the equivalent of a time to live.

- Type field tells us that this is a type 1 LSA.
- In a type 1 LSA, the Link state ID and the Advertising router field are identical. Each carries a 32-bit identifier for the router that created this LSA.
- The LS sequence number is to detect old or duplicate LSAs.
- The LS checksum is used to verify that data has not been corrupted.
- Length is the length in bytes of the complete LSA.
- Link ID is used to represent each link in the LSA
- The first two of these fields identify the link.
- Link Data is used to disambiguate among multiple parallel links. TOS information is present to allow OSPF to choose different routes for IP packets based on the value in their TOS field.

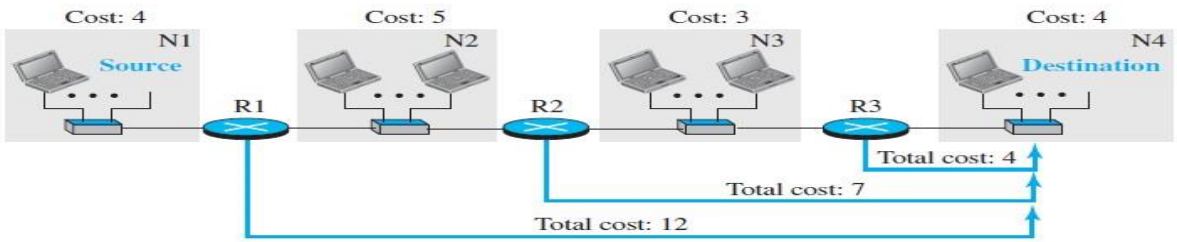
Metric

In OSPF, like RIP, the cost of reaching a destination from the host is calculated from the source router to the destination network.

- However, each link (network) can be assigned a weight based on the throughput, round-trip time, reliability, and so on.

  An administration can also decide to use the hop count as the cost. OSPF can have different weights as the cost.

Figure 20.19 *Metric in OSPF*



Forwarding Tables

- Figure 3.48 shows the forwarding tables for the simple AS in Figure. Comparing the forwarding tables for the OSPF and RIP in the same AS, we find that the only difference is the cost values.
- In other words, if we use the hop count for OSPF, the tables will be exactly the same. The reason for this consistency is that both protocols use the shortest-path trees to define the best route from a source to a destination.

Figure 20.20 *Forwarding tables in OSPF*

Forwarding table for R1

Destination network	Next router	Cost
N1	——	4
N2	——	5
N3	R2	8
N4	R2	12

Forwarding table for R2

Destination network	Next router	Cost
N1	R1	9
N2	——	5
N3	——	3
N4	R3	7

Forwarding table for R3

Destination network	Next router	Cost
N1	R2	12
N2	R2	8
N3	——	3
N4	——	4

3.9.3 BORDER GATEWAY PROTOCOL (BGP)

- The **Border Gateway Protocol version 4 (BGP4)** is the only inter domain routing protocol used in the Internet today.
- BGP4 is based on the path-vector algorithm we described before, but it is tailored to provide information about the reachability of networks in the Internet.

Autonomous Systems

- Internet is organized as autonomous systems (AS).
- Each AS is under the BGP control of a single administrative entity.
- The following figure shows a simple network with two autonomous systems.

Basic idea of AS

- To provide an additional way to hierarchically aggregate routing information in a large internet, thus improving scalability.
- Routing problem is divided into two parts:

a. Routing within a single autonomous system - intradomain routing
b. Routing between autonomous systems - interdomain routing

- There are two major interdomain routing protocols – EGP and BGP

BGP:

- BGP makes virtually no assumptions about how autonomous systems are interconnected—they form an arbitrary graph.
- ***Local traffic*** is traffic that originates at or terminates on nodes within an AS.

Transit traffic is traffic that passes through an AS.

Classification of AS

- **Stub AS**—an AS that has only a single connection to one other AS; such an AS will only carry local traffic. (eg) small corporation in the figure is a stub AS.
- **Multi-homed AS**—an AS that has connections to more than one other AS but that refuses to carry transit traffic, (eg) large corporation in the figure is a multi-homed AS.
- **Transit AS**—an AS that has connections to more than one other AS and that is designed to carry both transit and local traffic, (eg) the backbone providers in the figure is a transit AS.

Peering Point-Many providers arrange to interconnect with each other at a single point.

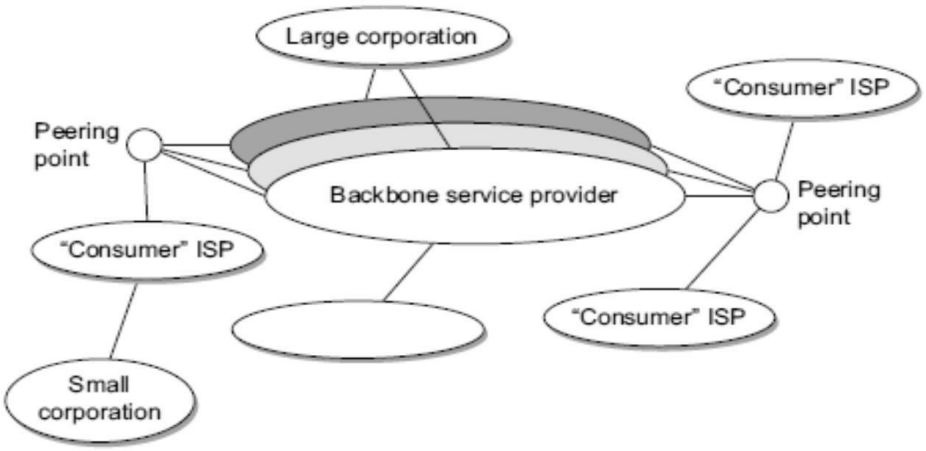


Figure 3.49 BGP

Basics of BGP

- Each AS has one or more border routers through which packets enter and leave the
- AS. A border router is simply an IP router that is charged with the task of forwarding packets between autonomous systems.
- Each AS that participates in BGP must also have at least one BGP speaker.

BGP speaker

- A router that —speaks‖ BGP to other BGP speakers in other autonomous
- systems. Border routers can also act as BGP speakers.
- BGP advertises complete paths as an enumerated list of autonomous systems to reach a particular network.
- It is sometimes called a path-vector protocol.

Types:

1. External BGP (eBGP)

2. Internal BGP (iBGP)

1. External BGP (eBGP)

- The circled number defines the sending router in each case.
- For example, message number 1 is sent by router R1 and tells router R5 that N1, N2, N3, and N4 can be reached through router R1 (R1 gets this information from the corresponding intra-domain forwarding table).
- Router R5 can now add these pieces of information at the end of its forwarding table.
- When R5 receives any packet destined for these four networks, it can use its forwarding table and find that the next router is R1.

Figure 20.25 *eBGP operation*

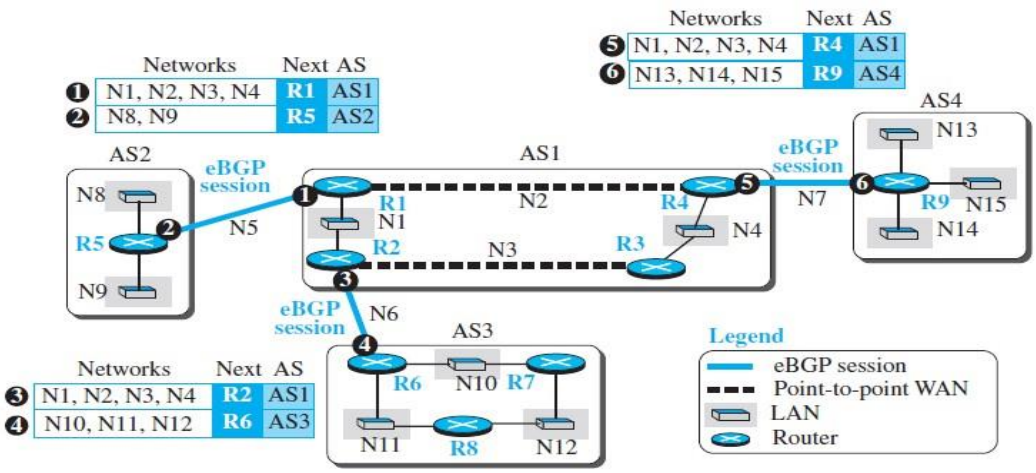


Figure 3.50

- The figure 3.50 also shows the simplified update messages sent by routers involved in the eBGP sessions.

There are two problems that need to be addressed:

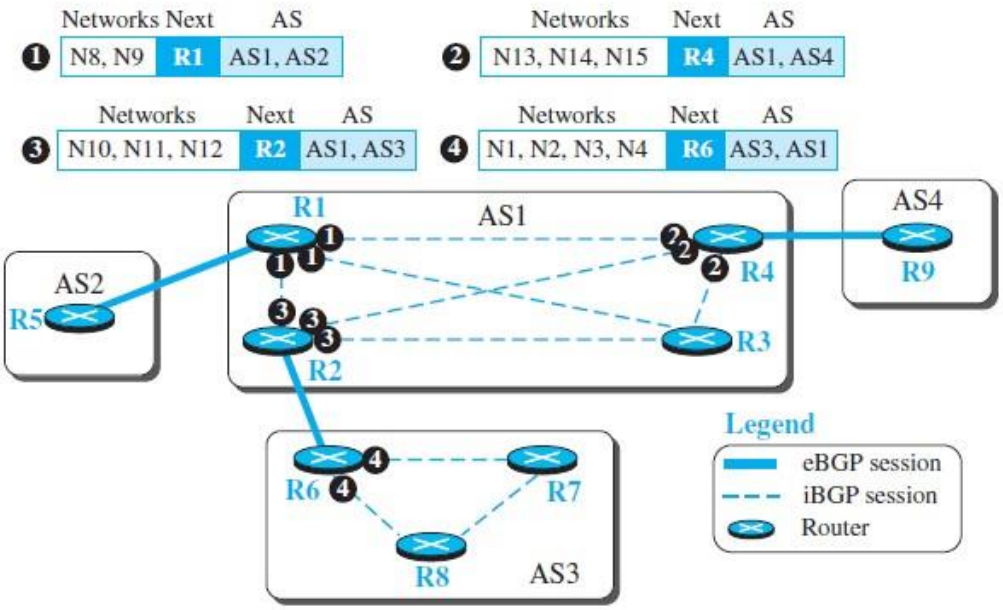
- 1.Some border routers do not know how to route a packet destined for non neighbor ASs. For example, R5 does not know how to route packets destined for networks in AS3 and AS4. Routers R6 and R9 are in the same situation as R5: R6 does not know about networks in AS2 and AS4; R9 does not know about networks in AS2 and AS3.
- 2.None of the nonborder routers know how to route a packet destined for any networks in other ASs.
- 3.To address the above two problems, we need to allow all pairs of routers (border or nonborder) to run the second variation of the BGP protocol, iBGP.

2. Internal BGP (iBGP)

- First, if an AS has only one router, there cannot be an iBGP session. For example, we cannot create an iBGP session inside AS2 or AS4 in our internet.
- Second, if there are n routers in an autonomous system, there should be [n × (n – 1) / 2] iBGP sessions in that autonomous system (a fully connected mesh) to prevent loops in the system.
- In other words, each router needs to advertise its own reachability to the peer in the session instead of flooding what it receives from another peer in another session.

The first message (numbered 1) is sent by R1 announcing that networks N8 and N9 are reachable through the path AS1-AS2, but the next router is R1.

Figure 20.26 *Combination of eBGP and iBGP sessions in our internet*



- As shown in Figure 3.51, the message is sent through separate sessions, to R2, R3, and R4. Routers R2, R4, and R6 do the same thing but send different messages to different destinations.
- The interesting point is that, at this stage, R3, R7, and R8 create sessions with their peers, but they actually have no message to send.

Messages

BGP uses four types of messages for communication between the BGP speakers across the ASs and inside an AS: open, update, keepalive, and notification. All BGP packets share the same common header.

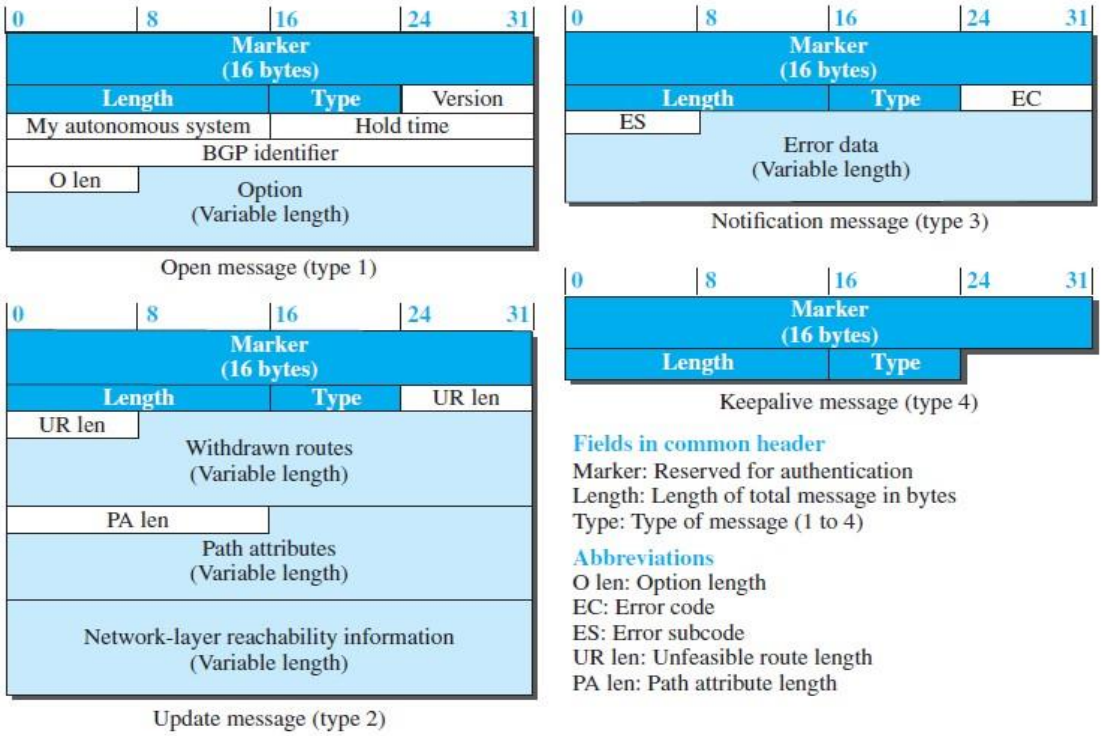
- **Open Message.** To create a neighborhood relationship, a router running BGP opens a TCP connection with a neighbor and sends an open message.
- **Update Message.** The update message is the heart of the BGP protocol. It is used by a router to withdraw destinations that have been advertised previously, to announce a route to a new destination, or both. Note that BGP can withdraw several destinations that were advertised before, but it can only advertise one new destination (or multiple destinations with the same path attributes) in a single update message.

- **Keep alive Message.** The BGP peers that are running exchange keep alive messages regularly (before their hold time expires) to tell each other that they are alive.
- **Notification.** A notification message is sent by a router whenever an error condition is detected or a router wants to close the session.

Performance

BGP performance can be compared with RIP. BGP speakers exchange a lot of messages to create forwarding tables, but BGP is free from loops and count-to-infinity.

Figure 20.31 *BGP messages*



10. MULTICASTING BASICS

1. Multicast Addresses

- In multicast communication, the sender is only one, but the receiver is many.
- If a new group is formed with some active members, an authority can assign an unused multicast address to this group to uniquely define it.
- A host, which is a member of n groups, actually has (n + 1) addresses:
  - one unicast address that is used for source or destination address in unicast communication
  - n multicast addresses that are used only for destination addresses to receive messages sent to a group.

Multicast Addresses in IPv4

- Multicast addresses in IPv4 belong to a large block of addresses that are specially designed for this purpose.
- In classful addressing, all of class D was composed of these addresses;
- Classless addressing used the same block, but it was referred to as the block 224.0.0.0/**4** (from 224.0.0.0 to 239.255.255.255).(as shown in Figure 3.53)
- Four bits define the block; the rest of the bits are used as the identifier for the group.
- The number of addresses in the multicast block is huge (228).

  We definitely cannot have that many individual groups.

  However, the block is divided into several subblocks and each subblock is used in a particular multicast application.
- The following gives some of the common sub blocks:

Local Network Control Block.

- The subblock 224.0.0.0/24 is assigned to a multicast routing protocol to be used inside a network, which means that the packet with a destination address in this range cannot be forwarded by a router.

  In this subblock, the address 224.0.0.0 is reserved, the address 224.0.0.1 is used to send datagrams to all hosts and routers inside a network, and the address 224.0.0.2 is used to send datagrams to all routers inside a network.

Figure 3.53 Group identifier

Internetwork Control Block.

- The subblock 224.0.1.0/24 is assigned to a multicast routing protocol to be used in the whole Internet, which means that the packet with a destination address in this range can be forwarded by a router.

Source-Specific Multicast (SSM) Block.

- The block 232.0.0.0/8 is used for source specific multicast routing

GLOP Block.

- The block 233.0.0.0/8 is called the GLOP block.
- This block defines a range of addresses that can be used inside an autonomous system.
- Each autonomous system is assigned a 16-bit number.

Administratively Scoped Block.

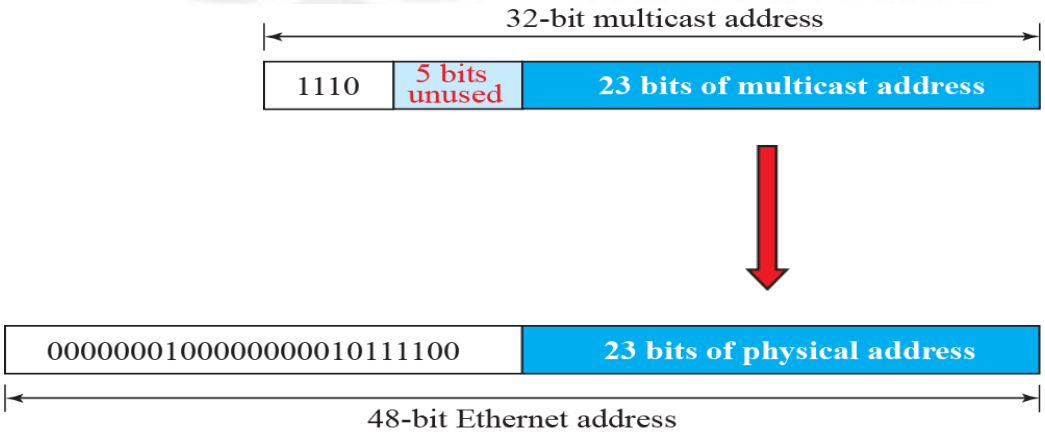
- The block 239.0.0.0/8 is called the Administratively Scoped Block.
- The addresses in this block are used in a particular area of the Internet.
- The packet whose destination address belongs to this range is not supposed to leave the area.
- In other words, an address in this block is restricted to an organization.

Selecting Multicast Address

- To select a multicast address to be assigned to a group is not an easy task.

The selection of address depends on the type of application.

Figure 3.54 Multicast address and Ethernet address



- Most LANs support physical multicast addressing. Ethernet is one of them.
- An Ethernet physical address (MAC address) is six octets (48 bits) long.
- If the first 25 bits in an Ethernet address are 00000001 00000000 01011110 0, this identifies a physical multicast address for the TCP/IP protocol. The remaining 23 bits can be used to define a group.
- To convert an IP multicast address into an Ethernet address, the multicast router extracts the least significant 23 bits of a multicast IP address and inserts them into a multicast Ethernet physical address.
- However, the group identifier of a multicast address block in an IPv4 address is 28bits long, which implies that 5 bits are not used.
- This means that 32 (25) multicast addresses at the IP level are mapped to a single multicast address.
- In other words, the mapping is many to one instead of one to one.
- If the 5 leftmost bits of the group identifier of a multicast address are not all zeros, a host may receive packets that do not really belong to the group in which it is involved.

  For this reason, the host must check the IP address and discard any packets that do not belong to it.

An Ethernet multicast physical address is in the range

- 01:00:5E:00:00:00 to 01:00:5E:7F:FF:FF.

Example 21.1

- Change the multicast IP address 232.43.14.7 to an Ethernet multicast physical address.

Solution

We can do this in two steps:

a. We write the rightmost 23 bits of the IP address in hexadecimal. This can be done bychanging the rightmost 3 bytes to hexadecimal and then subtracting 8 from the leftmostdigit if it is greater than or equal to 8. In our example, the result is 2B:0E:07.

b. We add the result of part a to the starting Ethernet multicast address, which is01:00:5E:00:00:00.

The result is

01:00:5E:2B:0E:07

Example 21.2

- Change the multicast IP address 238.212.24.9 to an Ethernet multicast address.

Solution

- a.The rightmost 3 bytes in hexadecimal are D4:18:09. We need to subtract 8 from the leftmostdigit, resulting in 54:18:09.
- b. We add the result of part a to the Ethernet multicast starting address.

The result is

01:00:5E:54:18:09

3.10.3 Multicast Forwarding

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

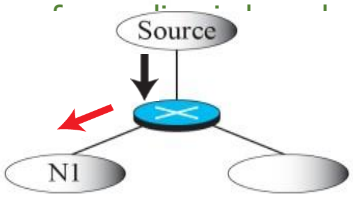
1.In multicast communication, the destination of the packet defines one group, but that group may have more than one member in the internet.

- To reach all of the destinations, the router may have to send the packet out of more than one interface.

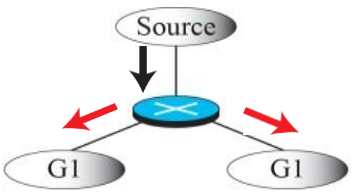
Figure shows the concept. In unicasting, the destination network N1 cannot be in more than one part of the internet; in multicasting, the group G1 may have members in more than one part of the internet.

2.Forwarding decisions in multicast communication depend on both the destination and the source address of the packet.

In other words, in unicasting, forwarding is based on where the packet should go; in multicast [illegible] where the packet should go and where the packet has



a. Destination in unicasting is one



b. Destination in mulicasting is more than one

Figure 3.55 unicasting and multicasting

3.10.4 Two Approaches to Multicasting

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

1. Routing using source-based trees

2.Routing using group-shared trees.

Source-Based Tree Approach

- In the **source-based tree** approach to multicasting, each router needs to create a separate tree for each source-group combination.
- In other words, if there are m groups and n sources in the internet, a router needs to create (m × n) routing trees.
- In each tree, the corresponding source is the root, the members of the group are the leaves, and the router itself is somewhere on the tree.
- We can compare the situation with unicast routing in which a router needs only one tree with itself as the root and all networks in the internet as the leaves.

Group-Shared Tree Approach

- In the **group-shared tree** approach, we designate a router to act as the phony source for each group.
- The designated router, which is called the core router or the rendezvous point router, acts as the representative for the group.
- Any source that has a packet to send to a member of that group sends it to the core center and the core center is responsible for multicasting.
- The core center creates one single routing tree with itself as the root and any routers with active members in the group as the leaves
- In this approach, there are m core routers and each core router has a routing tree, for the total of m trees. This means that the number of routing trees is reduced from (m × n) in the source-based tree approach to m in this approach.

The reader may have noticed that we have divided a multicast delivery from the source to all group members into two deliveries.

The first is a unicast delivery from the source to the core router; the second is the delivery from the core router to all group members. Note that the first part of the delivery needs to be done using tunneling.

- The multicast packet created by the source needs to be encapsulated in a unicast packet and sent to the core router.
- The core router decapsulates the unicast packet, extracts the multicast packet, and sends it to the group members.

3.11 IP VERSION 6 (IPv6)

- **Motivation for a new version of IP**
- To deal with exhaustion of the IP address space.
- IP addresses are assigned to mobile phones, televisions, and other household appliances.

All of these possibilities show the need for a bigger address space than that provided by 32 bits.

Birth of IPv6

- Since the IP address is carried in the header of every IP packet, increasing the size of the address requires a change in the packet header.
- There is a need for new software for every host and router in the Internet.
- The effort to define a new version of IP was known as IP Next Generation or IPng.
- An official IP version number was assigned, so IPng is now known as IPv6.

Version number 5 was used for an experimental protocol some years ago.

Expected features of new version of IP

- Support for real-time services
- Security support
- Auto configuration (i.e., the ability of hosts to automatically configure themselves with such information as their own IP address and domain name)
- Enhanced routing functionality, including support for mobile hosts.

Address Space Allocation

IPv6 provides a 128-bit address space.

- The IPv6 address space is predicted to provide over 1500 addresses per square foot of the earth's surface.
- IPv6 addresses are also classless. But the address space is still subdivided in various ways based on the leading bits.

The leading bits specify different uses of the IPv6 address. (as shown in Figure 3.56)

Reference video: https://www.youtube.com/watch?v=iR8ve5tTWAA

Prefix	Use
00. . . 0 (128 bits)	Unspecified
00. . . 1 (128 bits)	Loopback
1111 1111	Multicast addresses
1111 1110 10	Link-local unicast
Everything else	Global Unicast Addresses

Figure 3.56 Prefix and its uses

- The entire functionality of IPv4's three main address classes (A, B, and C)is contained inside the —everything else‖ range.
- Multicast addresses start with a byte of all 1s.
- Link-local unicast addresses enable a host to construct an address that will work on the network to which it is connected without being concerned about the global uniqueness of the address.
- Global unicast address
  - A node may be assigned an IPv4-compatible IPv6address by zero-extending a 32-bit IPv4 address to 128 bits.
  - A node that is only capable of understanding IPv4 can be assigned an IPv4-mappedIPv6 address by prefixing the 32-bit IPv4 address with 2 bytes of all 1s and then zero-extending the result to 128 bits.

Types:

- UnicastAddress
  - A unicast address defines a single interface (computer or router).
  - The packet with a unicast address will be delivered to the intended recipient.
- AnycastAddress
  - An anycast address defines a group of computers that all share a single address.
  - A packet with an anycast address is delivered to only one member of the group.
  - The member is the one who is first reachable.
- MulticastAddress
  - A multicast address also defines a group of computers.
- Difference between anycasting and multicasting
  - In anycasting, only one copy of the packet is sent to one of the members of the group.
  - In multicasting each member of the group receives a copy.

Address Notation

- The standard representation is x:x:x:x:x:x:x:x, where each —x‖ is a hexadecimal representation of a 16-bit piece of the address.
- 47CD:1234:4422:ACO2:0022:1234:A456:0124
- An address with a large number of contiguous 0s can be written more compactly by omitting all the 0 fields. Thus,
- 47CD:0000:0000:0000:0000:0000:A456:0124
- could be written as 47CD::A456:0124
- IPv4-mapped IPv6 address of a host whose IPv4 address was 128.96.33.81 could be written as::FFFF:128.96.33.81

Note: The double colon at the front indicates the leading 0s.

How does IPv6 handle options?

- Each option has its own type of extension header.
- The type of each extension header is identified by the value of the NextHeader field in the header that precedes it, and each extension header contains a NextHeader field to identify the header following it.
- The last extension header will be followed by a transport-layer header (e.g., TCP) and in this case the value of the NextHeader field is the same as the value of the Protocol field would be in an IPv4 header.
- Consider the example of the fragmentation header, shown in the figure 3.57.
- The NextHeader field of the IPv6 header would contain the value 44, which is the value assigned to indicate the fragmentation header.
- The NextHeader field of the fragmentation header itself contains a value describing the header that follows it.
- The next header might be the TCP header, which results in NextHeader containing the value 6.

If the fragmei ıder, then the fragmentation .

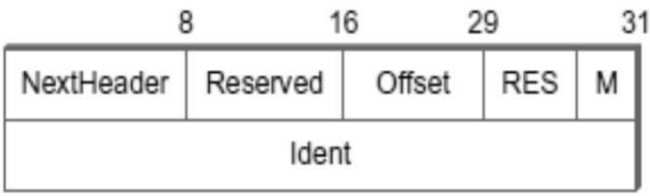


Figure 3.57 Fragmentation header

Auto configuration

- One goal of IPv6, therefore, is to provide support for auto configuration, sometimes referred to as plug-and-play operation.
- Auto configuration is possible for IPv4, but it depends on the existence of a server that is configured to hand out addresses and other configuration information to Dynamic Host Configuration Protocol (DHCP) clients.
- The longer address format in IPv6 provides a useful, new form of auto configuration called ***stateless* auto configuration**, which does not require a server.
- The auto configuration problem is subdivided into two parts:
  - **Obtain an interface ID that is unique on the link to which the host is attached.**

Every host on a link must have a unique link-level address. For example, all hosts on an Ethernet have a unique 48-bit Ethernet address. This can be turned into a valid link-local use address by adding the appropriate prefix (1111 1110 10) followed by enough 0s to make up 128 bits.

This address may be perfectly adequate for some devices on a network that do not connect to any other networks.

Obtain the correct address prefix for this subnet.

Those devices that need a globally valid address depend on a router on the same link to periodically advertise the appropriate prefix for the link. This requires that the router be configured with the correct address prefix, and that this prefix be chosen in such a way that there is enough space at the end (e.g., 48 bits) to attach an appropriate link-level address.

3.12 IPv6 PROTOCOL

Changes from IPv4 to IPv6 (Advantages ofIPv6)

HeaderFormat

- IPv6 uses a new header format.
- Options are

→ separated from the base-header

- → inserted between the base-header and the data.
- This speeds up the routing process (because most of the options do not need to be checked by routers).

NewOptions

IPv6 has new options to allow for additional functionalities.

Extension

IPv6 is designed to allow the extension of the protocol if required by new technologies or applications.

Resource Allocation

- InIPv6,
- → type-of-service (TOS) field has been removed
- → two new fields: 1) traffic class and 2) flow label, are added to enable the source to request special handling of the packet.
  - This mechanism can be used to support real-time audio and video.

Security

- The encryption option provides confidentiality of thepacket.
- The authentication option provides integrity of thepacket.

Packet Format(Figure 3.58)

- Version field is set to 6 for IPv6.
- The TrafficClass and FlowLabel fields both relate to quality of service issues.
- The PayloadLen field gives the length of the packet, excluding the IPv6 header, measured in bytes.
- The NextHeader field cleverly replaces both the IP options and the Protocol field of IPv4.
- If options are required, then they are carried in one or more special headers following the IP header, and this is indicated by the value of the NextHeader field.
- If there are no special headers, the NextHeader field is the demux key identifying the higher-level protocol running over IP (e.g., TCP or UDP).
- Fragmentation is handled as an optional header, which means that the fragmentation related fields of IPv4 are not included in the IPv6 header.
- The HopL
- The sourc bits) long.

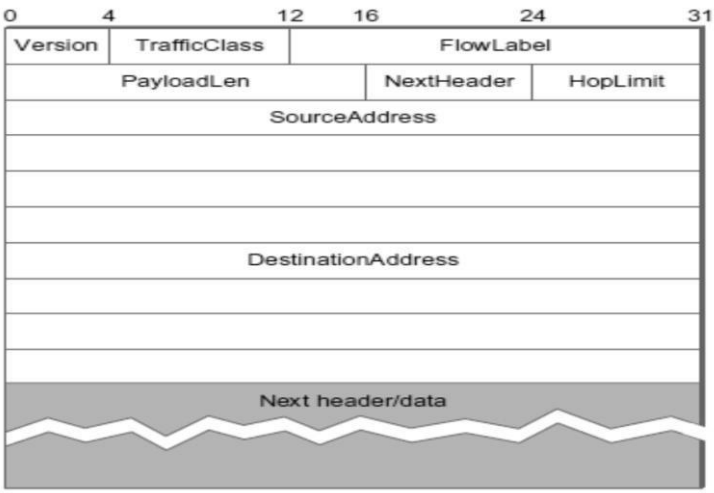


Figure 3.58 Packet format

Concept of Flow & Priority inIPv6

- To a router, a flow is a sequence of packets that share the same characteristics such as
- → traveling the same path
- → using the same resources or
- → having the same kind of security
- A router that supports the handling of flow labels has a flow label table.
- The table has an entry for each active flow label.
  - Each entry defines the services required by the corresponding flow label.
- When a router receives a packet, the router consults its flow label table.
- Then, the router provides the packet with the services mentioned in the
- entry.
- A flow label can be used to support the transmission of real-time audio/video.
- Real-time audio/video requires resources such as
- → highbandwidth
- → large buffersor

  → long processing time
- Resource reservation guarantees that real-time data will not be delayed due to a lack of resources.

Fragmentation &Reassembly

- Fragmentation of the packet is done only by the source, but not by the routers. The reassembling is done by the destination.
- At routers, the fragmentation is not allowed to speed up the processing in the router.
- Normally, the fragmentation of a packet in a router needs a lot of processing. This is because the packets need to be fragmented.
- All fields related to the fragmentation need to be recalculated.
- The source will
- → check the size of the packet and

  → make the decision to fragment the packet or not.

  If packet-size is greater than the MTU of the network, the router will drop the packet.

  Then, the router sends an error message to inform the source.

Extension Header

- An IP packet is made of
- → base-header &
- → some extension headers.
- Length of base header = 40bytes.
- To support extra functionalities, extension headers can be placed b/w base header
- and payload. Extension headers act like options inIPv4.

Six types of extension headers:
1) Hop-by-hop option 2) Source routing 3) Fragmentation
4) Authentication 5) Encrypted security 6) Destination option.
payload

Hop-by-Hop Option

- This option is used when the source needs to pass information to all routers visited by the datagram.
- Three options are defined: i) Pad1, ii) Pad N, and iii) Jumbo payload.
- **Pad1**
  - This option is designed for alignment purposes.
  - Some options need to start at a specific bit of the 32-bitword.
  - Pad1 is added, if one byte is needed for alignment.
- **PadN**
  - PadN is similar in concept toPad1.
  - The difference is that PadN is used when 2 or more bytes are needed foralignment.
- **JumboPayload**
  - This option is used when larger packet has to be sent. (> 65,535bytes)
  - Large packets are referred to as jumbopackets.
  - Maximum length of payload = 65,535bytes.

DestinationOption

- This option is used when the source needs to pass information to the destination only.
- Intermediate routers are not allowed to access this information.
- Two options are defined: i) Pad1 & ii)PadN

Source Routing

- This option combines the concepts of
- → strict source routing and
- → loose source routing.

Fragmentation

- In IPv6, only the original source can fragment.
- A source must use a —Path MTU Discovery technique‖ to find the smallest MTU along the path from the source to the destination.
- Minimum size of MTU=1280bytes. This value is required for each network connected to the Internet.
- IfasourcedoesnotuseaPathMTUDiscoverytechnique,thesourcefragmentsthedatagra mtoa
- size of 1280 bytes.

Authentication

- This option has a dual purpose:
  - Validates the message sender: This is needed so the receiver can be sure that a message is from the genuine sender and not from an attacker.
  - Ensures the integrity of data: This is needed to check that the data is not altered in transition by some attacker.

Encrypted Security Payload (ESP)

- This option provides confidentiality and guards against attacker.

ASSIGNMENT

Divide the given address space 172.16.0.0 / 16 into 7 networks whose requirement is given below

Net 1 500 hosts

Net 2 200 hosts

Net 3 100 hosts

Net 4 60 hosts

Net 5 20 hosts

Net 6 2 hosts

Net 7 2 hosts

NOTE: Use Variable Length Subnetting (15) (K4,CO3)

miniproject

Implement transmission of ping messages/trace route over a network topology consisting of 6 nodes and find the number of packets dropped due to congestion (K4,CO3)

UNIT III QUESTION BANK

PART –A

1) Define routing. ***(Nov12,15) (K1,CO3)***

- It is the process of building up the tables that allow the collect output for a packet to be determined. It is a lot harder to create the forwarding tables in large, complex networks with dynamically changing topologies and multiple paths between destinations. Routing is a process that takes place in the background so that, when a data packet turns up, we will have the right information in the forwarding table to be able to forward, or switch, the packet.

2) What are the types of source routing? ***(Nov 13) (K1,CO3)***

- Rotation, stripping off and using pointers are the different types of source routing approach.

3) What is the function of a router? ***(Nov 10) (K1,CO3)***

- Routers relay packets among multiple interconnected networks. They route packets from one network to any of a number of potential destination networks on internet. A router operates as the physical, data link and network layer of the OSI model. A router is termed as an intelligent device. Therefore, its capabilities are much more than those of a repeater or a bridge. A router is useful for interconnecting two or more heterogeneous networks that differ in their physical characteristics such as frame size, transmission rates, topologies, addressing etc. A router has to determine the best possible transmission path among several available paths. Destination, Cost and Next Hop are the important fields in a routing table

4) What is the role of VCI? ***(May 11) (K1,CO3)***

- An Incoming virtual circuit identifier (VCI) uniquely identifies the connection at this switch and that will be carried inside the header of the packets that belong to this connection. It is a potentially different outgoing VCI that will be used for outgoing packets. The combination of incoming interface and incoming VCI uniquely identifies the virtual connection.

5) What is packet switching? ***(Nov 12) (K1,CO3)***

- In a packet-switched network, it's not necessary to dedicate transmission capacity along a path through the network. Rather, data are sent out in a sequence of small chunks, called packets. Packet switching is mainly used in terminal-to-computer and computer-to-computer communications.

6) Identify the class of the following IP Address: ***(Nov 15) (K3,CO3)***

- **110.34.56.45 (b) 212.208.63.23**
- 110.34.56.45: This IP address belongs to Class A.

  212.208.63.23: This IP address belongs to Class C.

7)How many network addresses and host addresses are supported by class A, class B networks? *(K3,CO3)*

- Class A:Number of networks = 127

  Number of hosts = 2^{24} -1
- Class B: Number of networks = 2^{14} -1

  Number of hosts = 2^{16} – 1 = 65,535.

8) What is subnetting? *(Nov 11,13,15) (K1,CO3)*

- The whole network can't manage by single server, so that the entire network divided into small network in order to manage the network easily. Subnetting provides an elegantly simple way to reduce the total number of network numbers that are assigned. The idea is to take a single IP network number and allocate the IP address with that network to several physical networks, which are now referred to as subnets.

9)What is subnet mask? *(K1,CO3)*

- A subnet mask is a number that defines a range of IP addresses available within a network. A single subnet mask limits the number of valid IPs for a specific network. Multiple subnet masks can organize a single network into smaller networks (called subnetworks or subnets).

10)Define CIDR? *(K1,CO3)*

- CIDR, which stands for Classless Inter-Domain Routing, is an IP addressing scheme that improves the allocation of IP addresses. It replaces the old system based on classes A, B, and C. This helped to extend the life of IPv4 as well as slow the growth of routing tables.

11)What does a router do when it receives a packet with a destination address that it does not have an entry for, in its routing table? *(K1,CO3)*

- **Default Router:** If IP Software is not able to find the destination, from routing table then it sends the datagram to default router. It is useful when a site has small set of local address connected to it and connected to the rest of the Internet.

12)List out the functions of IP. *(K1,CO3)*

- IP services are unreliable, best-effort, connectionless packet delivery system
- Unreliable – delivery is not guaranteed, Connectionless – each pocket is treated independent from others, Best-effort delivery – it makes an earnest attempt to deliver packets. It defines basic unit of data transfer through TCP/IP.

  IP s/w performs routing function and finds a path from source to destination.

  IP includes a set of rules that embody the idea of unreliable packet delivery.

13)State the rules of non boundary-level masking*? (May 12) (K3,CO3)*

- The bytes in the IP address that corresponds to 255 in the mask will be repeated in the sub network address
- The bytes in the IP address that corresponds to 0 in the mask will change to 0 in the sub network address
- For other bytes, use the bit-wise AND operator.

Example-

IP address	45	123	21	8
Mask	255	192	0	0
Subnet	45	64	0	0
123	0 1 1 1 1 0 1 1			
192	1 1 0 0 0 0 0 0			
64	0 1 0 0 0 0 0 0			

14)What is the network address in a class A subnet with the IP addresses of one of the hosts as 25.34.12.56 and mask 255.255.0.0? *(May 14) (K1,CO3)*

- IP Address - 25.34.12.56
- Mask 255.255.0.0
- Network Address - 25.34.0.0

15)What is IP address? *(K1,CO3)*

- An Internet Address is made of four bytes (32 bits) that define a host‟s connection to a network. There are currently 5 different field lengths patterns, each define a class of addresses. These are designed to cover the needs of different types of organizations, class A, B, C, D, E.

16)Write the difference between Distance vector routing and Link state routing. *(K2,CO3)*

Distance Vector Routing	Link state routing
Basic idea is each node sends its knowledge about the entire network to its neighbors.	Basic idea is every node sends its knowledge about its neighbors to the entire network
It is dynamic routing	It is dynamic routing
RIP uses Distance vector routing	OSPF uses link state routing

17) What is the goal of LSP? *(K1,CO3)*

- The main goals is that the newest information must be flooded to all nodes as quickly as possible, while old information must be removed from the network and not allowed to circulate.

18)What is count to infinity problem? *(K1,CO3)*

- This network cycle stops only when the distances reach some number that is large enough to be considered infinite. In the meantime, none of the nodes actually knows that a particular node is unreachable, and the routing tables for the network do not stabilize. This situation is known as the count to infinity problem.

19)What is RIP? *(K1,CO3)*

- RIP (Routing Information Protocol) is a widely-used protocol for managing router information within a self-contained network such as a corporate local area network or an interconnected group of such LANs. Using RIP, a gateway host (with a router) sends its entire routing table (which lists all the other hosts it knows about) to its closest neighbor host every 30 seconds. The neighbor host in turn will pass the information on to its next neighbor and so on until all hosts within the network have the same knowledge of routing paths, a state known as network convergence.

20) Explain about OSPF. *(K1,CO3)*

- OSPF (Open Shortest Path First) is a router protocol used within larger autonomous system networks in preference to the Routing Information Protocol (RIP), an older routing protocol that is installed in many of today's corporate networks. Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately multicasts the information to all other hosts in the network so that all will have the same routing table information.

21)What do you mean by ICMP? *(K1,CO3)*

- ICMP is an error reporting mechanism. It does not specify the action to be taken for each possible error. The source must relate the error to an individual application program and take other actions to correct the problem.

22) To whom ICMP reports error message will be sent? *(K1,CO3)*

- **ICMP** allows routers to send error messages to other router or hosts. ICMP is an error reporting mechanism. It does not specify the action to be taken for each possible error. It is informing the source that the error has occurred and the source has to take actions to rectify the errors.

23) When ICMP redirect message is used?*(May 17) (K1,CO3)*

- An ICMP redirect is an error message sent by a router to the sender of an IP packet. ICMP redirect message is used to redirect the messages through alternate path when there is an unexpected link failure in the already devised network path.

24) Expand ICMP and write the function. *(K1,CO3)*

- Internet Control Message Protocol. ICMP is an error reporting mechanism. It does not specify the action to be taken for each possible error. The source must relate the error to an individual application program and take other actions to correct the problem

25) Define flooding and pruning. *(K1,CO3)*

- **Flooding:** Whenever a router receives a multicast packet from source S, the router forwards the packet on all outgoing links except the one on which the packet arrived.
- **Pruning:** Prune the set of networks that receives each packet addressed to group G to exclude those that have no hosts that are members of G. This is done in two stages.
- Recognize when a leaf network has no group members.
- Propagate this —no members of G here‖ information up the shortest-path tree.

26) What is the main function of BGP? *(K1,CO3)*

- The main function of BGP is to prevent establishment of looping paths.

27) Give the classification of AS? *(K1,CO3)*

- Stub AS
- Multihomed AS
- Transit AS

28) What is local traffic and Transit Traffic? *(K1,CO3)*

- ***Local traffic*** is traffic that originates at or terminates on nodes within an AS.
- ***Transit traffic*** is traffic that passes through an AS.

29) Define Border Gateway Protocol (BGP) (Nov/Dec 2014) *(K1,CO3)*

- BGP makes virtually no assumptions about how autonomous systems are interconnected—they form an arbitrary graph.

30) What is ABR? *(K1,CO3)*

- **Area Border Router:** The area border routers summarize routing information that they have learned from one area and make it available in their advertisements to other areas.

31)Write on the packet cost referred in distance vector and link state routing. *(May 2012) (K1,CO3)*

- In distance vector routing, cost refer to hop count while in case of link state routing, cost is a weighted value based on a variety of factors such as security levels, traffic or the state of the link.

32) Explain Multicast routing? *(K1,CO3)*

- Multicast IP Routing protocols are used to distribute data (for example, audio/video streaming broadcasts) to multiple recipients. Using multicast, a source can send a single copy of data to a single multicast address, which is then distributed to an entire group of recipients.

33) Explain IPV4 protocol. *(K1,CO3)*

- IPv4 (Internet Protocol Version 4) is the fourth revision of the Internet Protocol (IP) used to identify devices on a network through an addressing system. The Internet Protocol is designed for use in interconnected systems of packet-switched computer communication networks.IPv4 is the most widely deployed Internet protocol used to connect devices to the Internet. IPv4 uses a 32-bitaddress scheme

34) What are the differences between IPV4 and IPV6? *(K1,CO3)*

IPV4	IPV6
A 32-bit numeric address in IPv4 is written in decimal as four numbers separated by periods. Each number can be zero to 255. For example, 1.160.10.240 could be an IP address.	IPv6 addresses are 128-bit IP address written in hexadecimal and separated by colons. An example IPv6 address could be written like this: 3ffe:1900:4545:3:200:f8ff:fe21:67cf

35) Explain IPV6 protocol. *(K1,CO3)*

- IPv6 (Internet Protocol version 6) is a set of basics of IPv6 are similar to those of IPv4. The IP addresses are lengthened from 32 bits to 128 bits. This extension anticipates considerable future growth of the Internet and provides relief for what was perceived as an impending shortage of network addresses. IPv6 also supports auto-configuration to help correct most of the shortcomings in version 4, and it has integrated security and mobility features.

36) List the features of IPv6. (Nov/Dec 2012) *(K1,CO3)*

- Support for real-time services
- Security support
- Auto configuration
- Enhanced routing functionality, including support for mobile hosts

37) Why is IPV4 to IPV6 transition required?*(May 17) (K1,CO3)*

- IPv4 and IPv6 networks are not directly interoperable, transition technologies are designed to permit hosts on either network type to communicate with any other host.

38) What are the metrics used by routing protocols? (May/June 2015) *(K1,CO3)*

- Router metrics can contain any number of values that help the router determine the best route among multiple routes to a destination. A router metric typically based on information like path length, bandwidth, load, hop count, path cost, delay, Maximum Transmission Unit (MTU), reliability and communications cost.

39)How do routers differentiate the incoming unicast, multicast and broadcast IP packets? (May 2017) *(K1,CO3)*

- Routers differentiate the incoming unicast, multicast and broadcast IP packets by using their IP addresses, Class A, B and C are used for Unicast, Class D is used for multicast and all ones in Network part of IP address is used for broadcast.

40) Expand and define MTU. (May/June 2012) *(K1,CO3)*

- Maximum transmission unit (MTU) is the largest IP datagram that it can carry in a frame.

41) Mention any four applications of multicasting. (May/June 2012) *(K1,CO3)*

- Network assisted multicast may also be implemented at the Data Link Layer using one-to-many addressing and switching such as Ethernet multicast addressing, Asynchronous Transfer Mode (ATM) point-to-multipoint virtual circuits (P2MP) or Infiniband multicast.

42) What is multicasting? (Nov/Dec 2011, Nov/Dec 2010) *(K1,CO3)*

- The motivation for developing multicast is that there are applications that want to send a packet to more than one destination host. Instead of forcing the source host to send a separate packet to each of the destination hosts, we want the source to be able to send a single packet to a multicast address, and for the network—or internet, in this case—to deliver a copy of that packet to each of a group of hosts.

43) What are the different kinds of Multicast routing? (May/June 2011) *(K1,CO3)*

- Distance-vector Multicast Routing Protocol (DVMR)
- Multicast Extensions to OSPF (MOSPF)
  - Intra-Area routing
  - Inter-Area
  - routing Inter-AS
- Routing
- Protocol Independent Multicast (PIM) routing protocols

44)What are the two major mechanisms defined to help transition from IPv4 to IPv6? (May 2019) *(K1,CO3)*

- Dual Stack
- Tunneling mechanism

45) Write the supporting protocols used by IP. *(K1,CO3)*

- Address Resolution Protocol (ARP)
- Reverse Address Resolution Protocol (RARP) Internet Control Message Protocol (ICMP) Internet Group Message Protocol (IGMP)

46) What is DHCP? (Nov/Dec 2012) *(K1,CO3)*

- The configuration process is very error-prone, since it is necessary to ensure that every host gets the correct network number and that no two hosts receive the same IP address.

For these reasons, automated configuration methods are required. The primary method uses a protocol known as the Dynamic Host Configuration Protocol (DHCP).

DHCP relies on the existence of a DHCP server that is responsible for providing configuration information to hosts. There is at least one DHCP server for an administrative domain.

47) Compare ARP and RARP.
(K1,CO3)

ARP	RARP
Address Resolution Protocol.	Reverse Address Resolution Protocol.
Retrieves the physical address of the receiver.	Retrieves the logical address for a computer from the server.
ARP maps 32-bit logical (IP) address to 48-bit physical address.	RARP maps 48-bit physical address to 32-bit logical (IP) address.

UNIT III – PART B

1) Explain Virtual circuit switching techniques. Or In the virtual circuit service model, before a virtual circuit is setup, the source router needs to specify a path from the source to the destination. What additional information do we need to maintain in the routing table to support this function? Write down the resulting routing table. ***(May 12) (K3,CO3)***

1) Explain Packet Switching in detail. ***(K1,CO3)***

2) With a neat diagram explain about IPV4 Service Model, Packet format, fragmentation and reassembly. **(Nov/Dec 2016)** ***(K2,CO3)***

1) Write an algorithm for datagram forwarding in IP. **(May 2018)** ***(K3,CO3)***

1) Explain in detail i) ICMP ii)ARP iii)RARP. **(Nov 2015, May/June 2016)** ***(K1,CO3)***

6) Discuss about Link-state routing and routers. **(Nov 12)(May 15)** ***(K1,CO3)***

7) Explain the distance vector routing algorithm. Mention the limitations of the same. **(May/June 2015, May/June 2016, Nov/Dec 2015)** ***(K4,CO3)***

8) Explain the RIP algorithm with a simple example of your choice. **(May 2019, May 2018, May/June 2014)** ***(K4,CO3)***

6) Explain in detail the operation of OSPF protocol by considering a suitable network**.(May 17)** ***(K3,CO3)***

10)Explain about the inter domain routing (BGP) routing algorithms. ***(K1,CO3)***

11)Explain about IPV6?Compare IPV4 and IPV6 **(May 16)**

(K1,CO3) 12)Draw the IPv6 packet header format. **(May 2018)**

(K1,CO3) 13)Explain Link state routing with Dijkstra's algorithm.

(K1,CO3)

14)Explain Distance Vector Routing Algorithm for the graph given below.
(K1,CO3)

QUIZ

Dear students, You all are invited to attend the Quiz in the below mentioned link.

CONTENT BEYOND SYLLABUS : UNIT – III

Connectionless Network Service (CLNS) Protocol

- Connectionless Network Service (CLNS) is a Layer 3 protocol similar to IP version 4 (IPv4) for linking hosts (end systems) with routers (intermediate systems) in an Open Systems Interconnection (OSI) network.
- CLNS and its related OSI protocols, Intermediate System-to-Intermediate System (IS-IS) and End System-to-Intermediate System (ES-IS), are International Organization for Standardization (ISO) standards.
- CLNS networks can be connected over an IP MPLS network core using Border Gateway Protocol (BGP) and MPLS Layer 3 virtual private networks (VPNs).
- CLNS uses network service access points (NSAPs), similar to IP addresses found in IPv4, to identify end systems (hosts) and intermediate systems (routers). ES-IS enables the hosts and routers to discover each other. IS-IS is the interior gateway protocol (IGP) that carries ISO CLNS routes through a network.
- To configure CLNS use the following online reference :

https://www.juniper.net/documentation/en_US/junos/topics/task/configuration/clns-security-configuring.html

SUPPORTIVE ONLINE COURSES

S No	Course provider	Course title	Link
1	Udemy	Introduction to Networking for Complete Beginners	https://www.udemy.com/course/introduction-to-networking-for-complete-beginners/
2	Coursera	Fundamentals of Network Communication	https://www.coursera.org/learn/fundamentals-network-communications/
3	Coursera	Peer-to-Peer Protocols and Local Area Networks	https://www.coursera.org/learn/peer-to-peer-protocols-local-area-networks/
4	Coursera	Packet Switching Networks and Algorithms	https://www.coursera.org/learn/packet-switching-networks-algorithms
5	Coursera	TCP/IP and Advanced Topics	https://www.coursera.org/learn/tcp-ip-advanced
6	edX	Computer Networks and the Internet	https://www.edx.org/course/computer-networks-and-the-internet

REAL TIME APPLICATIONS IN DAY TO DAY LIFE AND TO INDUSTRY

Transport for Real-Time (RTP)

In the early days of packet switching, most applications were concerned with transfering files, although as early as 1981, experiments were under way to carry real-time traffic, such as digitized voice samples. We call an application "real-time" when it has strong requirements for the timely delivery of information. Voice over IP (VoIP) is a classic example of a real-time application because you can't easily carry on a conversation with someone if it takes more than a fraction of a second to get a response.

Multimedia applications—those that involve video, audio, and data—are sometimes divided into two classes: interactive applications and streaming applications. Figure shows the authors using an example conferencing tool that's typical of the interactive class. Along with VoIP, these are the sort of applications with the most stringent real-time requirements.

Streaming applications typically deliver audio or video streams from a server to a client and are typified by such commercial products as Spotify. Streaming video, typified by YouTube and Netflix, has become one of the dominant forms of traffic on the Internet. Because streaming applications lack human-to-human interaction, they place somewhat less stringent real-time requirements on the underlying protocols.

Timeliness is still important, however—for example, you want a video to start playing soon after pushing "play," and once it starts to play, late packets will either cause it to stall or create some sort of visual degradation. So, while streaming applications are not strictly real time, they still have enough in common with interactive multimedia applications to warrant consideration of a common protocol for both types of application.

It should by now be apparent that designers of a transport protocol for real-time and multimedia applications face a real challenge in defining the requirements broadly enough to meet the needs of very different applications. They must also pay attention to the interactions among different applications, such as the synchronization of audio and video streams. We will see below how these concerns affected the design of the primary real-time transport protocol in use today: Real-time Transport Protocol (RTP)

Assessment Schedule

- **Tentative schedule for the Assessment During 2022-2023 odd semester**

S.NO	Name of the Assessment	Start Date	End Date	Portion
1	IAT 1	16.09.2022	22.09.2022	UNIT 1 & 2
2	IAT 2	02.11.2022	08.11.2022	UNIT 3 & 4
3	REVISION	26.11.2022	29.11.2022	UNIT 5 , 1 & 2
4	MODEL	01.12.2022	10.12.2022	ALL 5 UNITS

Prescribed Text Books & Reference Books

TEXT BOOK

Data Communications and Networking, Behrouz A. Forouzan, McGraw Hill Education, 5th Ed., 2017.

REFERENCES

1. Computer Networking- A Top Down Approach, James F. Kurose, University of Massachusetts and Amherst Keith Ross, 8th Edition, 2021.
2. Computer Networks, Andrew S. Tanenbaum, Sixth Edition, Pearson, 2021.
3. Data Communications and Computer Networks, P.C. Gupta, Prentice-Hall of India, 2006.
4. Computer Networks: A Systems Approach , L. L. Peterson and B. S. Davie, Morgan Kaufmann, 3rd ed., 2003.

Thank you