COMPUTER NETWORK

B.TECH CSE

3rd Year – 1st Sem

UNIT – III

Network Layer

DEPARTMENT OF CSE

VIGNAN INSTITUTE OF TECHNOLOGY & SCIENCE

DESHMUKHI

Network Layer

The **network layer** is a crucial component of the OSI (Open Systems Interconnection) model and the TCP/IP (Transmission Control Protocol/Internet Protocol) protocol suite. It operates at Layer 3 of the OSI model and is responsible for routing packets of data between devices across different networks.

The **network layer** is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links). Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination. Communication at the network layer is host-to-host (computer-to-computer); a computer somewhere in the world needs to communicate with another computer somewhere else in the world.

The network layer is responsible for the delivery of individual packets from the source to the destination host.

The packet transmitted by the sending computer may pass through several LANs or WANs before reaching the destination computer. The term IP address to mean a logical address in the network layer of the TCP/IP protocol suite. The Internet addresses are 32 bits in length; this gives us a maximum of 2^{32} addresses.

These addresses are referred to as IPv4 (IP version 4) addresses or simply IP addresses if there is no confusion.
As:- IPAddress: 117.149.29.2

- **Network layer:** Handles the routing and sending of data between different networks.
  - ✓ The most important protocols at this layer are IP and ICMP.
- **Network Protocol:** A protocol is an agreed-upon way of formatting data so that two or more devices are able to communicate with and understand each other.
- A number of different protocols make connections, testing, routing, and encryption possible at the network layer, including IP, IPsec, ICMP, IGMP, GRE, OSPF, RIP, NAT, VRRP.

Functions performed by the network layer:

- ✓ **Logical Addressing**: The network layer uses logical addressing (such as IP addresses) to uniquely identify devices on a network. This is in contrast to the data link layer, which deals with physical addressing (e.g., MAC addresses).

- ✓ **Routing:** The network layer is responsible for determining the best path for data packets to travel from the source to the destination across multiple interconnected networks. This involves making decisions based on the logical addresses of the source and destination.

- ✓ **Packet Forwarding**: Once the route is determined, the network layer is responsible for forwarding packets of data from one router to another along the chosen path until they reach their destination.

- ✓ **Fragmentation and Reassembly**: The network layer can fragment large packets into smaller ones for transmission over networks that have a smaller maximum frame size. At the destination, these fragments are reassembled into the original packet.

- ✓ **Quality of Service (QoS):** The network layer can provide services to optimize the performance of the network, including managing traffic congestion, prioritizing certain types of traffic, and ensuring reliable and timely delivery.

- ✓ **Error Handling:** While the network layer does not perform error detection and correction like the data link layer, it may detect errors and initiate actions to handle them, such as requesting packet retransmission.

Network Layer: Design issues

An introduction to some of the issues that the designers of the network layer must grapple with.

A number of design issues exist for the layer to layer approach of computer networks. Some of the main design issues are as follows –

i. Store-and-Forward Packet Switching
ii. Services Provided to the Transport Layer
iii. Implementation of Connectionless Service
iv. Implementation of Connection-Oriented Service
v. Comparison of Virtual-Circuit and Datagram Networks

Store-and-Forward Packet Switching

The host sends the packet to the nearest router.

✓ This packet is stored there until it has fully arrived once the link is fully processed by verifying the checksum then it is forwarded to the next router till it reaches the destination.

✓ This mechanism is called “Store and Forward packet switching.

In packet-switched networks, store-and-forward is a fundamental technique where network devices receive, store, process, and transmit data packets individually. It ensures reliable data delivery by introducing several key steps:

1. **Packet Reception:** The network device (e.g., router) receives a data packet on an incoming link.
2. **Storage:** The entire packet is buffered in memory, waiting for complete reception.
3. **Error Checking:** The packet's integrity is verified using error detection codes (e.g., CRC).
4. **Routing:** Based on the destination address, the next path or hop is determined.
5. **Forwarding:** If error-free, the packet is transmitted to the next device on the chosen path.
6. **Buffer Management:** Buffers are monitored and packets may be discarded if storage space becomes unavailable.

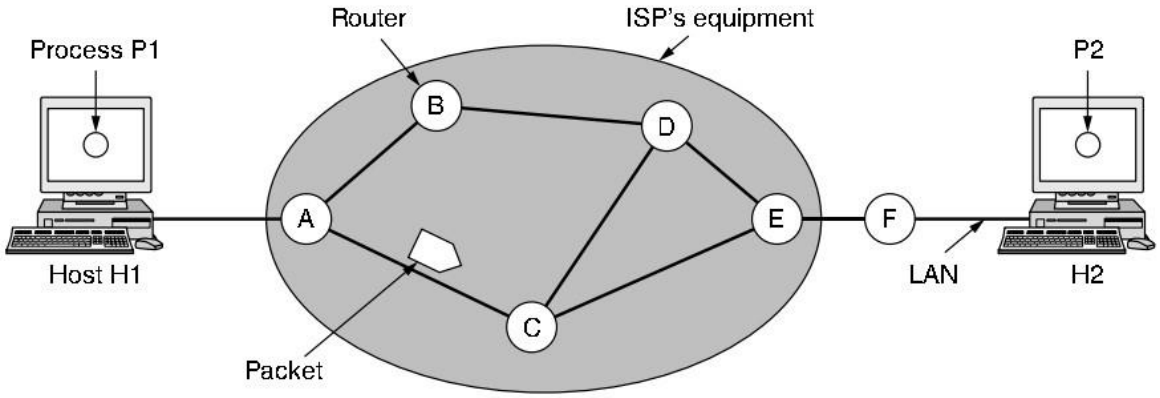


Figure 5-1. The environment of the network layer protocols.

Services Provided to the Transport Layer

The **network layer** provides services to the transport layer at the network layer/transport layer interface.

What kind of services the network layer provides to the transport layer?

- The services need to be carefully designed with the following goals in mind:

i The services should be independent of the router technology.

ii The transport layer should be shielded from the number, type, and topology of the routers present.

iii The network addresses made available to the transport layer should use a uniform numbering plan, even across LANs and WANs.

Based on the connections there are 2 types of services provided:

✓**Connectionless –** The routing and insertion of packets into subnet is done individually.

✓ No added setup is required.

✓**Connection-Oriented –** Subnet must offer reliable service and all the packets must be transmitted over a single route.

Core Services provided to Transport Layer:

- ✓ **Reliable Data Delivery:** Guarantees data arrives intact and in the correct order, often using protocols like TCP.
- ✓ **Flow Control:** Regulates data transmission rate to prevent overloading receivers, typically managed by algorithms like sliding windows.
- ✓ **Congestion Control:** Dynamically adjusts data flow based on network conditions to avoid congestion and packet loss.
- ✓ **Error Detection and Correction:** Identifies and corrects errors introduced during transmission using checksums and retransmissions.
- ✓ **Multiplexing and Demultiplexing:** Allows multiple applications on a single device to share the network connection efficiently.
- ✓ **Connection Management:** Establishes, maintains, and terminates connections between applications, providing session-like communication.

Services Provided by the Network Layer

Services in Network Layer

- **Guaranteed delivery:** The service which guarantees that the packet will arrive at its destination.
- **Guaranteed delivery with bounded delay:** The packet will be delivered within a specified host-to-host delay bound.
- **In-Order packets:** The packet arrives at the destination in the order in which they are sent.
- **Guaranteed max jitter:** The amount of time taken between two successive transmissions at the sender is equal to the time between their receipt at the destination.
- **Security services:** The network layer provides security by using a session key between the source and destination host.
  - ✓ The source host encrypts the payloads of datagrams being sent to the destination host.
  - ✓ The destination host would then decrypt the payload. In such a way, the network layer maintains the data integrity and source authentication services.

Core Services:

- **Logical Addressing:** Assigns unique logical addresses (e.g., IP addresses) to devices on the network, enabling identification and communication.
- **Routing:** Determines the best path for packets to take from source to destination, using protocols like IP routing and BGP.
- **Packet Forwarding:** Receives packets from the data link layer, analyzes routing information, and sends them towards the next hop on the chosen path.

- **Error Handling:** Detects and handles errors that might occur during transmission, potentially using mechanisms like ICMP messages.
- **Congestion Control:** Implements mechanisms to prevent network congestion, ensuring smooth data flow.
- **Internetworking:** Enables communication between different networks with varying technologies and protocols.

Implementation of Connectionless Service

Packet are termed as "datagrams" and corresponding subnet as "datagram subnets".

- ✓ When the message size that has to be transmitted is 4 times the size of the packet, then the network layer divides into 4 packets and transmits each packet to router via. a few protocol.
- ✓ Each data packet has destination address and is routed independently irrespective of the packets.

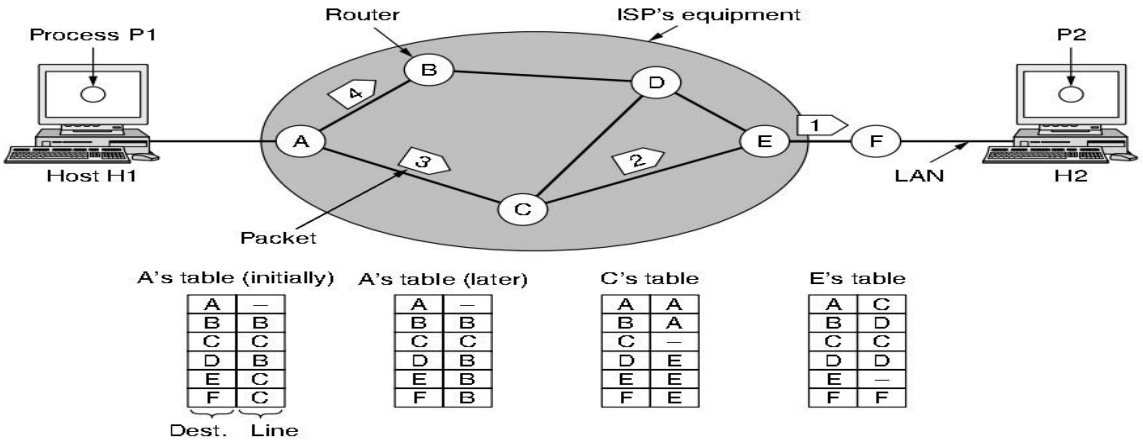


Figure 5-2. Routing within a datagram network.

Implementation of Connection-Oriented Service

A **connection-oriented service**, first establishes a connection, use it and then release it. The data packets are delivered to the receiver in the same order in which they have been sent by the sender.

- **It can be done in either Two ways :**

- **Circuit Switched Connection –** A dedicated physical path or a circuit is established between the communicating nodes and then data stream is transferred.
- **Virtual Circuit Switched Connection –** The data stream is transferred over a packet switched network, in such a way that it seems to the user that there is a dedicated path from the sender to the receiver.
  - ✓ A virtual path is established here.

✓ While, other connections may also be using the same path.

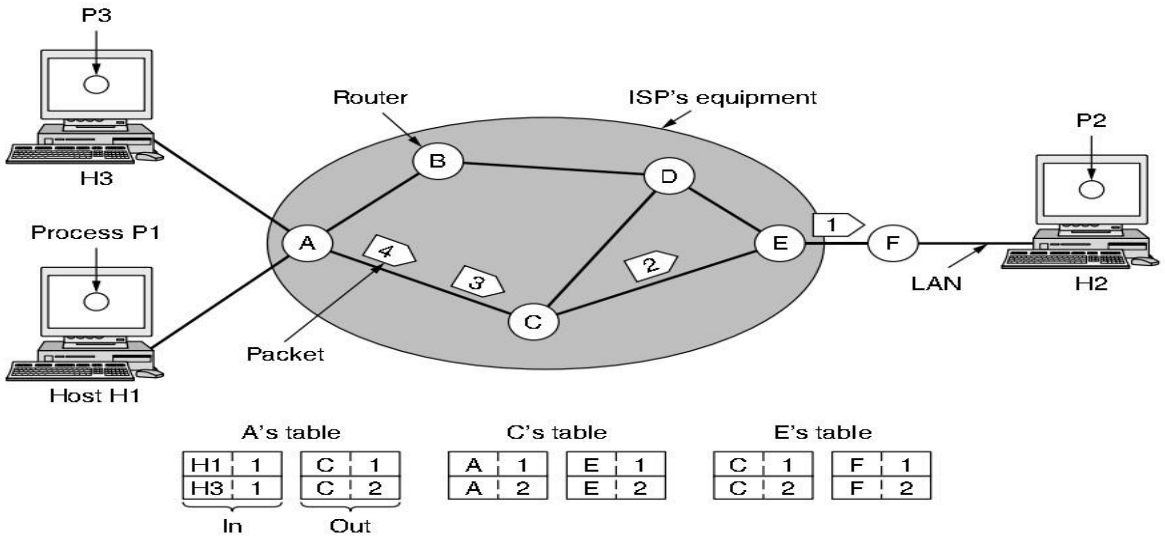


Figure 5-3. Routing within a virtual-circuit network.

Comparison of Virtual-Circuit and Datagram Networks

Issue	Datagram network	Virtual-circuit network
Circuit setup	Not needed	Required
Addressing	Each packet contains the full source and destination address	Each packet contains a short VC number
State information	Routers do not hold state information about connections	Each VC requires router table space per connection
Routing	Each packet is routed independently	Route chosen when VC is set up; all packets follow it
Effect of router failures	None, except for packets lost during the crash	All VCs that passed through the failed router are terminated
Quality of service	Difficult	Easy if enough resources can be allocated in advance for each VC
Congestion control	Difficult	Easy if enough resources can be allocated in advance for each VC

Figure 5-4. Comparison of datagram and virtual-circuit networks.

Routing algorithms

A routing algorithm is a procedure that lays down the route or path to transfer data packets from source to the destination. hey help in directing Internet traffic efficiently. After a data packet leaves its source, it can choose among the many different paths to reach its destination. Routing algorithm mathematically computes the best path, i.e. "least – cost path" that the

packet can be routed through. The **main function** of the network layer is routing packets from the source machine to the destination machine.
In most networks, packets will require multiple hops to make the journey.

- ✓ The Routing protocol is a routing algorithm that provides the best path from the source to the destination. The best path is the path that has the "least-cost path" from source to the destination.
- ✓ Routing is the routing algorithm determines the process of forwarding the packets from source to the destination but the best route to send the packets.
- ✓ The **routing algorithm** is that part of the network layer software responsible for deciding which output line an incoming packet should be transmitted on.
- ✓ In this process, a routing table is created which contains information regarding routes that data packets follow.
- ✓ Various routing algorithms are used for the purpose of deciding which route an incoming data packet needs to be transmitted on to reach the destination efficiently.

Classification of Routing Algorithms

The routing algorithms can be classified as follows:

Adaptive Algorithms/ dynamic routing

The algorithms that change their routing decisions whenever network topology or traffic load changes. These make use of dynamic information such as current topology, load, delay, etc. to select routes. A router may select a new route for each packet (even packets belonging to the same transmission) in response to changes in the condition and topology of the networks. Optimization parameters are distance, number of hops, and estimated transit time.

Non-AdaptiveAlgorithms/ static routing

The algorithms that do not change their routing decisions once they have been selected, as a route to be taken is computed in advance and downloaded to routers when a router is booted. Once the pathway to the destination has been selected, the router sends all packets for that destination along that one route. **Non-adaptive algorithms** do not base their routing decisions on any measurements or estimates of the current topology and traffic.

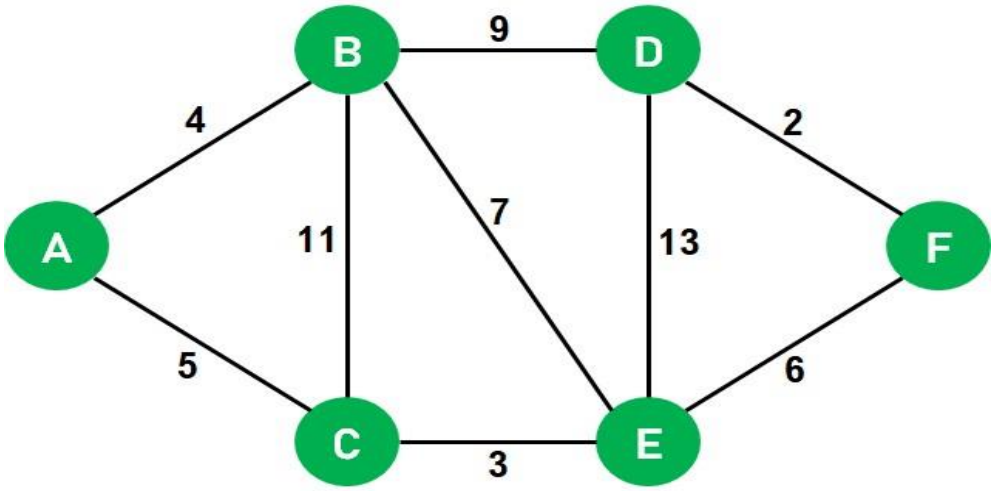
Types of Routing Algorithms

1. Shortest path routing
2. Flooding
3. Hierarchical routing,
4. Broadcast,
5. Multicast,
6. Distance vector routing

Shortest path routing

Shortest path routing finds the most efficient path (time, hops, distance) between two points in a network. Think of it as GPS for data packets, optimizing delivery across wired, wireless, or even transportation networks. It uses algorithms like Dijkstra's to analyze connections and costs, ensuring smooth data flow and reducing congestion. Examples include internet routing and traffic optimization.

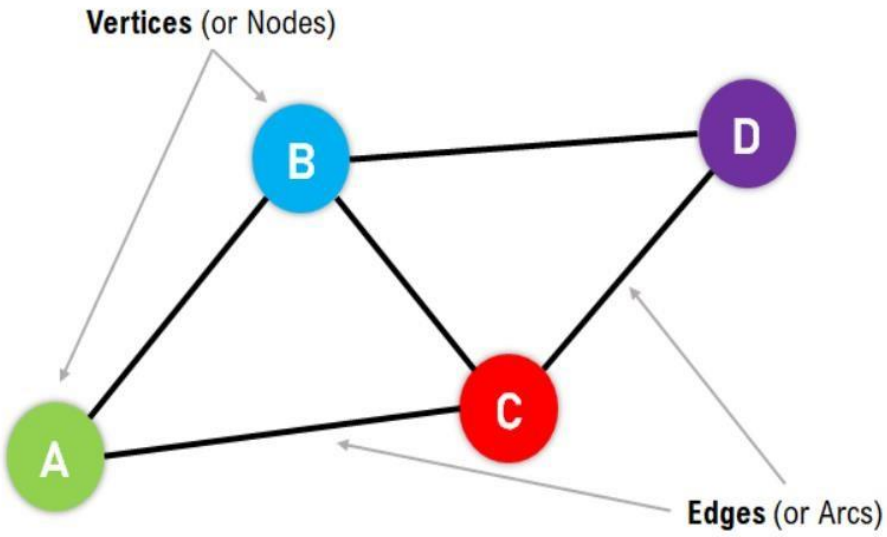
- ✓ **Dijkstra's Shortest Path Algorithm** which was developed by Dutch computer scientist **Edsger W. Dijkstra** in 1956.
- ✓ Dijkstra's algorithm is a popular algorithms for solving many single-source **shortest path problems** having non-negative edge weight in the graphs i.e., it is to find the shortest distance between two vertices on a graph.
- ✓ Finds shortest paths from given source nodes to all other nodes.
- ✓ The aim is to find the optimal paths between the network nodes so that routing cost is minimized.



Graphs

Graph is non-linear data structures representing the "connections" between the **vertices** through **edges**.

- ✓ **Vertices:** Vertices are the basic units of the graph used to represent real-life, objects, persons, or entities. Sometimes, vertices are also known as Nodes.
- ✓ **Edges:** Edges are drawn or used to connect two vertices of the graph. Sometimes, edges are also known as Arcs.



Example : Shortest path routing

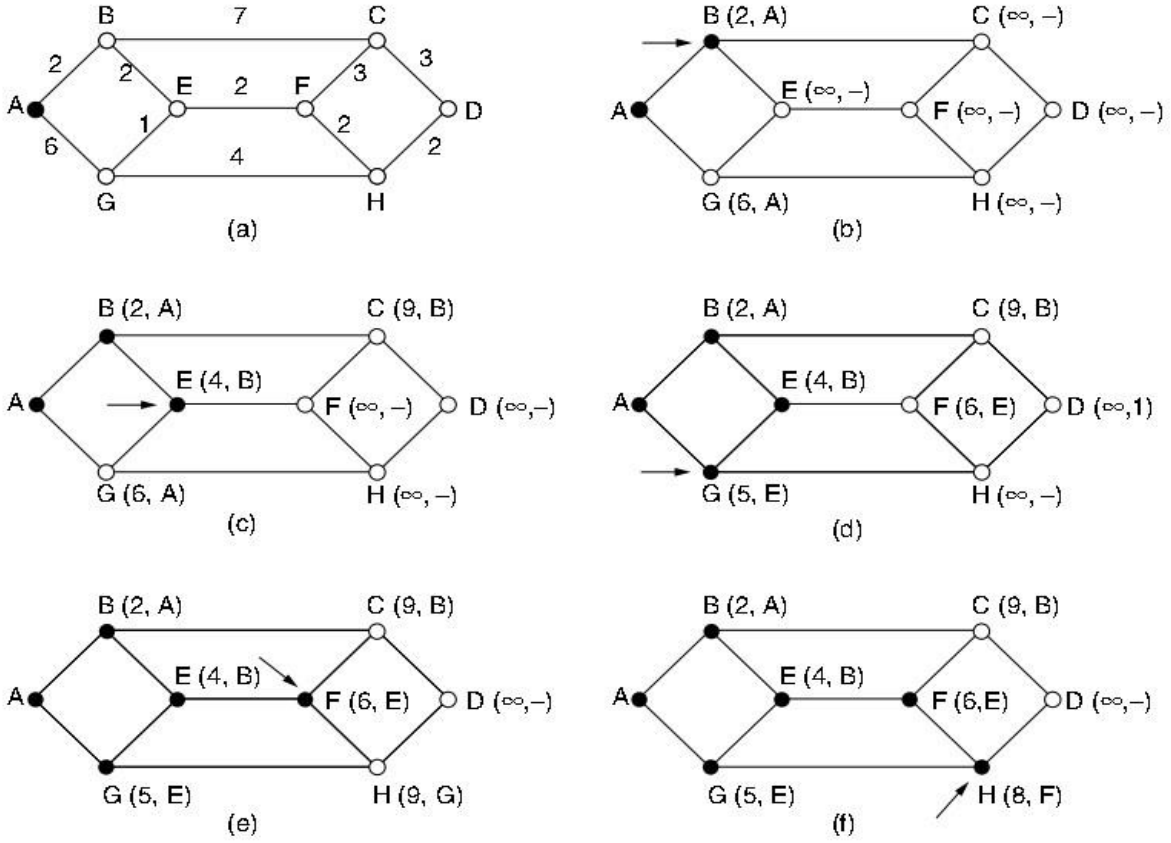
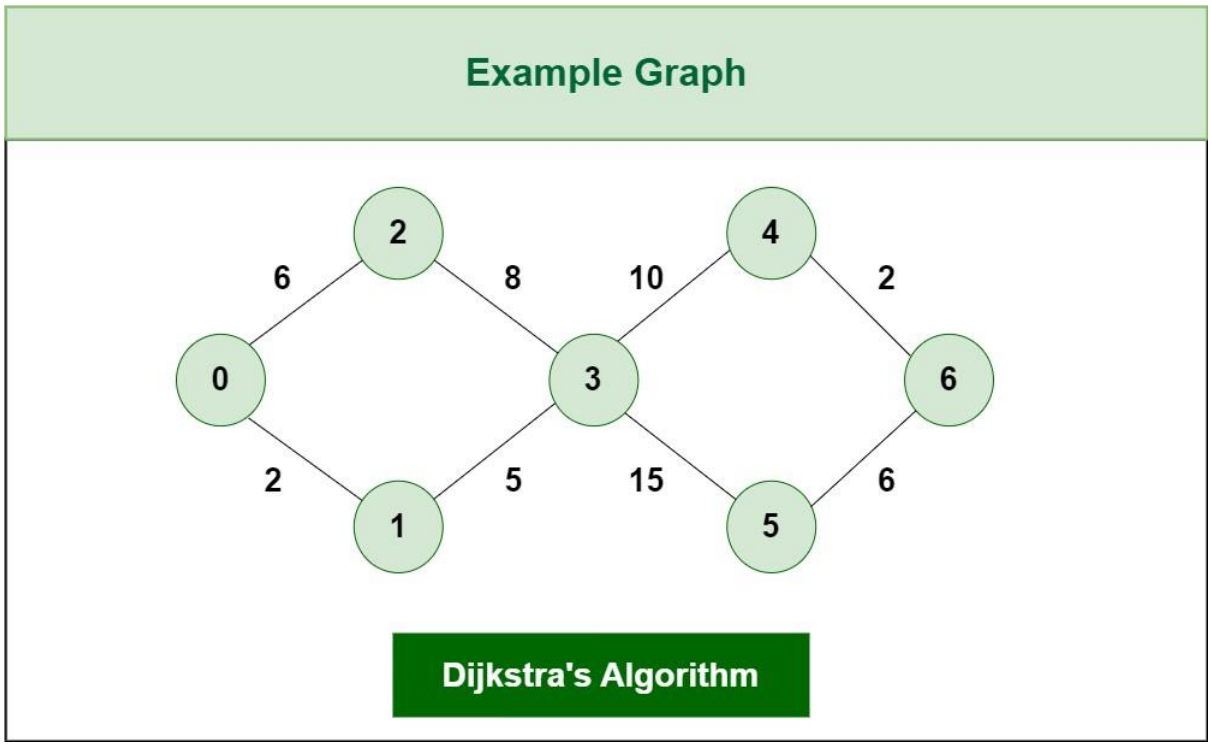
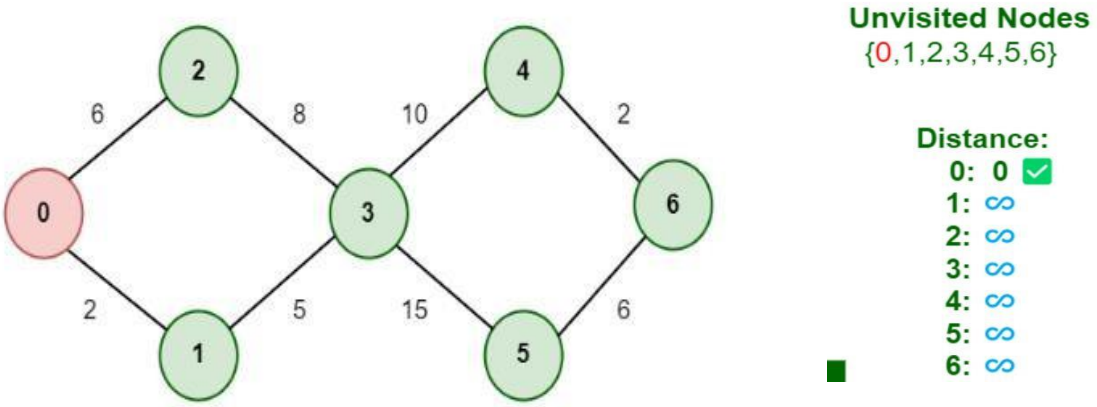


Figure 5-7. The first six steps used in computing the shortest path from *A* to *D*. The arrows indicate the working node.

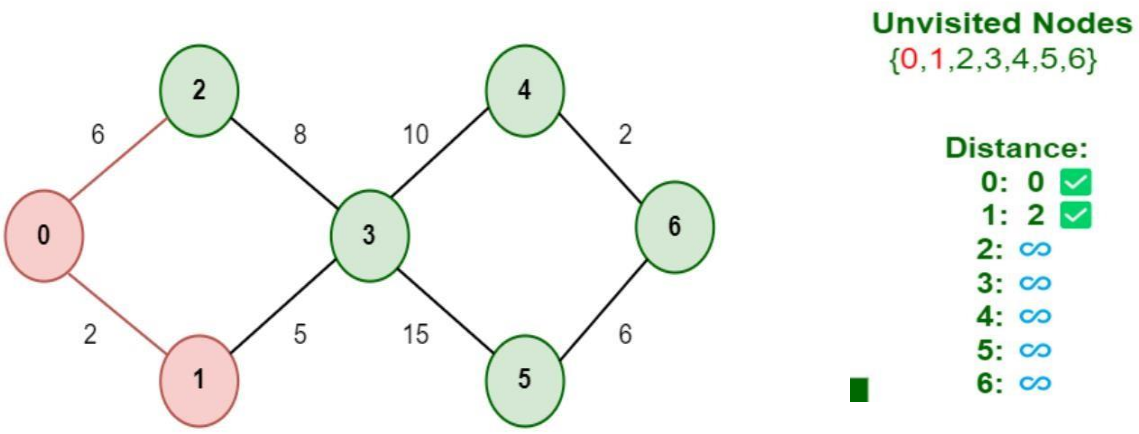
Example



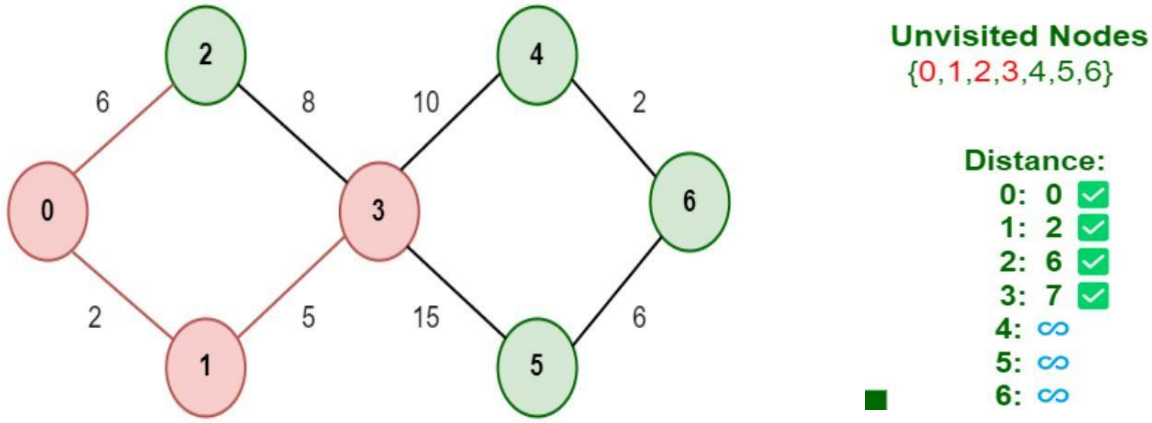
Step 1: Start from Node 0 and mark Node 0 as visited and check adjacent nodes



Step 2: Check for adjacent Nodes, (Either choose Node1 with distance 2 or either choose Node 2 with distance 6) and choose Node with minimum distance.
Distance: Node 0 -> Node 1 = 2

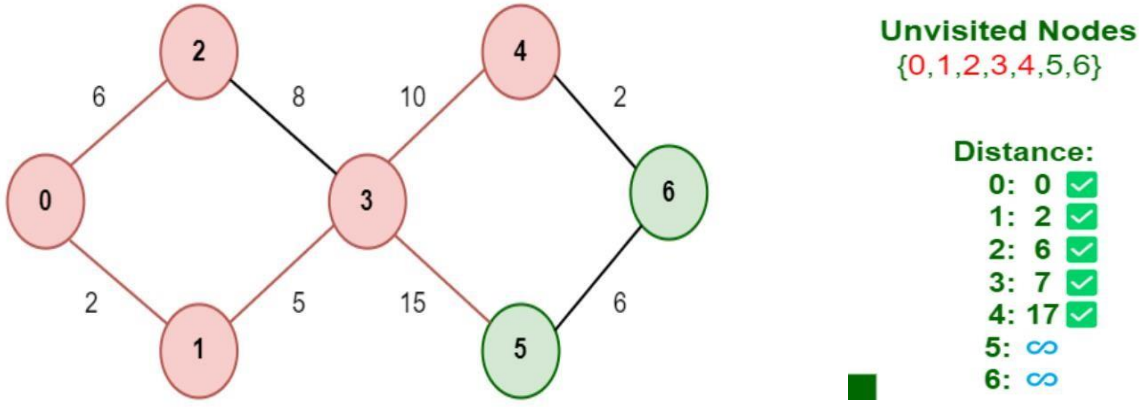


Step 3: Then Move Forward and check for adjacent Node which is Node 3, so marked it as visited and add up the distance, Now the distance will be: **Distance: Node 0 -> Node 1 -> Node 3 = 2 + 5 = 7**

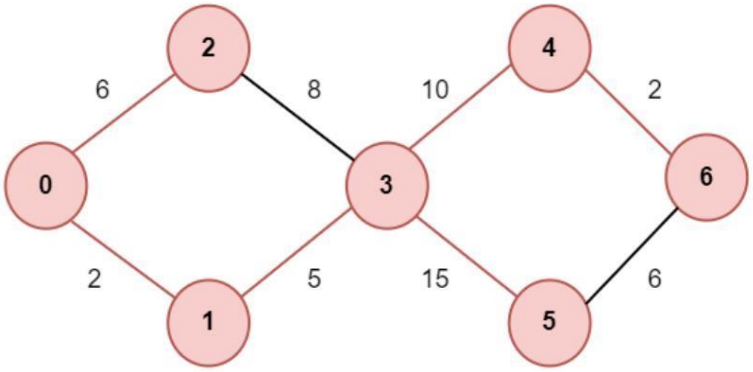


Step 4: Again two choices for adjacent Nodes (Either choose Node 4 with distance 10 or either choose Node 5 with distance 15) so choose Node with minimum distance.

Node 4 is Minimum distance adjacent Node, so marked it as visited and add up the distance.
Distance: Node 0 -> Node 1 -> Node 3 -> Node 4 = 2 + 5 + 10 = 17



Step 5: Again, Move Forward and check for adjacent Node which is **Node 6**, so marked it as visited and add up the distance, Now the distance will be:
Distance: Node 0 -> Node 1 -> Node 3 -> Node 4 -> Node 6 = 2 + 5 + 10 + 2 = 19



So, the Shortest Distance from the Source Vertex is 19 which is optimal one

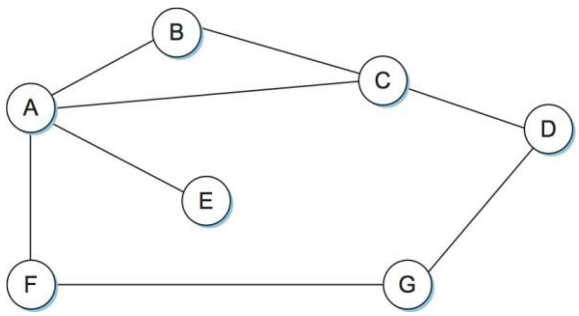
Flooding

Flooding is a technique of routing in computer networking, in which a **sender node transmits packets** via all the **outgoing links**. Flooding is similar to broadcasting in that it happens when sender packets are transferred without routing data to each network node attached.

- ✓ In a computer network, flooding occurs when a router uses a non-adaptive routing algorithm to send an incoming packet to every outgoing link except the node on which the packet arrived.
- ✓ Flooding is a way to distribute routing protocols updates quickly to every node in a large network.

Working process of flooding algorithms?
Flooding algorithms can be configured in one of two ways:

i. Every node acts as a sender and a receiver;
ii. Every node tries to send the packet to each of its counterparts except for the source node.



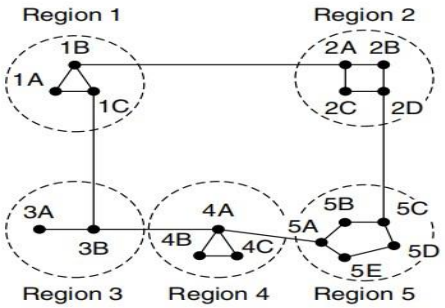
Types of flooding

i. **Controlled flooding:** Use two algorithms to control the transmission of packets to the neighbouring nodes.
   a **Sequence Number Controlled Flooding** (SNCF) and
      Each node maintains a list of the **source address** and **sequence number** of each broadcast packet it has already received, duplicated, and forwarded.
   b **Reverse Path Forwarding** (RPF).
      Only know the **next neighbour** on its unicast shortest path to the sender
ii. **Uncontrolled flooding:** Each router unconditionally transmits the incoming data packets to all its neighbours.
iii. **Selective flooding:** Nodes are configured to only send incoming packets to routers in one direction.
   This can help to prevent some of the mishaps that occur with uncontrolled flooding, but is not as sophisticated as controlled flooding.

Hierarchical routing

Hierarchical routing algorithm is **one of the adaptive algorithms used to reduce the size of routing table**. Drawback of this algorithm is that the reduced table size comes at the expense of increased path length. Hierarchical routing is the procedure of arranging routers in a hierarchical manner. As networks grow in size, the router routing tables grow proportionally.

- ✓ The routers are divided into regions.
- ✓ Each router has complete details about how to route packets to destinations within its own region, but has no information about routers in other regions.
- ✓ When different networks are **interconnected**, it is natural to regard each one as a separate region to free the routers in one network from having to know the topological structure of the other ones.
- ✓ For huge networks, a two-level hierarchy may be insufficient:
- ✓ It may be necessary to group the regions into clusters, the clusters into zones, the zones into groups, and **so on**.



Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

(c)

Figure 5-14. Hierarchical routing.

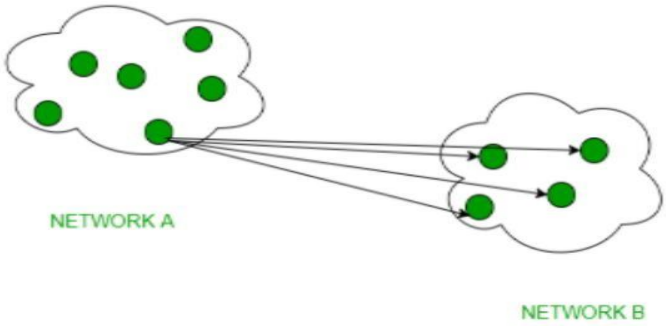
Figure 5-14 gives a quantitative example of routing in a two-level hierarchy with five regions. **The full routing table for router 1A has 17 entries**, as shown in Fig. 5-14(b). When routing is done hierarchically, as in Fig. 5-14(c), there are entries for all the local routers, as before, but all other regions are condensed into a single router, so all traffic for region 2 goes via the 1B-2A line, but the rest of the remote traffic goes via the 1C-3B line. **Hierarchical routing has reduced the table from 17 to 7 entries.**

Broadcast Routing

Broadcast routing is a networking concept that facilitates the transmission of data, messages or signals, from a source to destinations within a network. Unlike routing (one to one) or multicast routing (one to many) broadcast routing ensures that information reaches all devices or nodes in the network. Broadcast routing sends a single message to every device on a network segment, like a group chat message. It uses a special address and routers forward it to all connected devices.

Hosts need to send messages to many or all other hosts.

- Sending a packet to all destinations simultaneously is called broadcasting.
- Broadcast routing ensures that packets reaches all devices or nodes within the network.



An improvement is **multidestination routing**, in which each packet contains either a list of destinations or a bit map indicating the desired destinations. When a packet arrives at a router, the router checks all the destinations to determine the set of output lines that will be needed.

- ✓ A **spanning tree** is a subset of the network that includes all the routers but contains no loops. **Sink trees** are **spanning trees.**

Reverse path forwarding: a broadcast packet arrives at a router, the router checks to see if the packet arrived on the link that is normally used for sending packets toward the source of the broadcast.

Reverse path forwarding: a broadcast packet arrives at a router, the router checks to see if the packet arrived on the link that is normally used for sending packets toward the source of the broadcast.

Multicast routing

Multicast routing is **a networking method for efficient distribution of one-to-many traffic**. A multicast source, such as a live video conference, sends traffic in one stream to a multicast group. The multicast group contains receivers such as computers, devices, and IP phones.

- ✓ Multicast routing is a networking method for efficient distribution of **one-to-many** traffic.

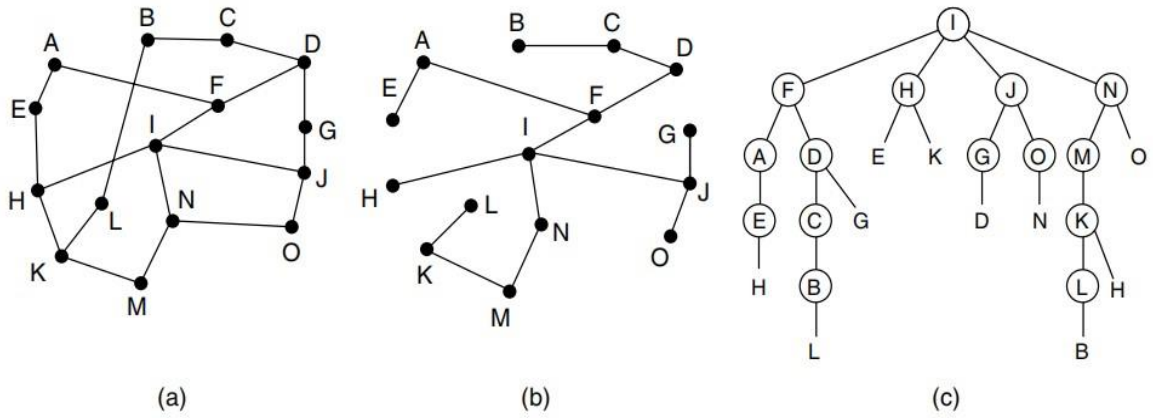
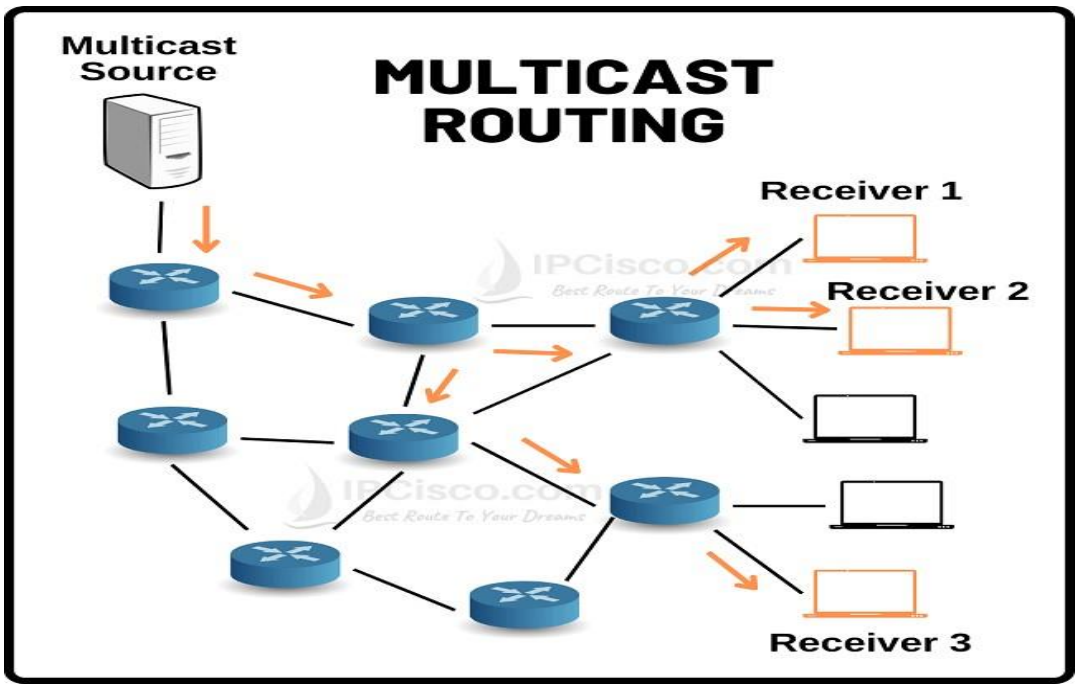


Figure 5-15. Reverse path forwarding. (a) A network. (b) A sink tree. (c) The tree built by reverse path forwarding.

- ✓ Multicast routing begins by **sending a select group of receivers** the data, which they filter out to other necessary receivers.
- ✓ Sending a message to such a group is called multicasting, and the routing algorithm used is called **multicast routing.**

Multicast routing schemes build on the broadcast routing schemes we have already studied, sending packets along spanning trees to deliver the packets to the members of the group while making efficient use of bandwidth.



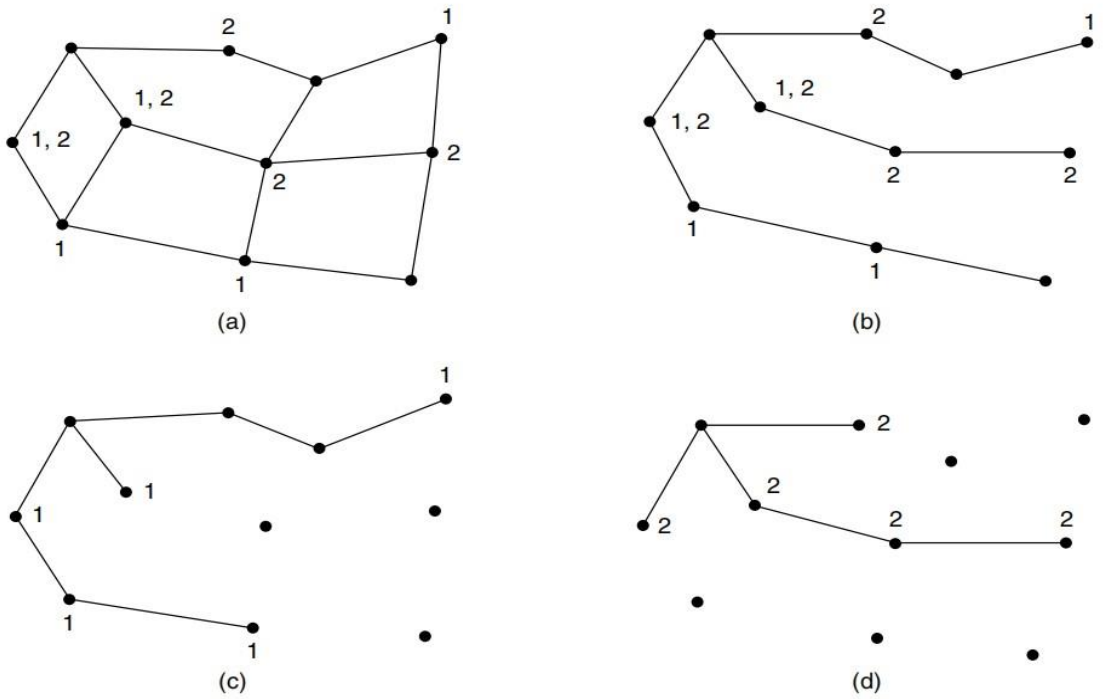


Figure 5-16. (a) A network. (b) A spanning tree for the leftmost router. (c) A multicast tree for group 1. (d) A multicast tree for group 2.

Difference between Broadcast and Multicast Routing

Features	Broadcast	Multicast
Definition	Broadcasting is a method of sending a message to all recipients simultaneously.	It is a group communication method in which data is sent simultaneously to a group of target computers.
Mapping	It contains one-to-all mapping.	It contains one-to-many mapping.
Bandwidth	The bandwidth of the broadcast is wasted.	The bandwidth of multicast is utilized effectively.
Management	It doesn't need any group management.	It needs group management to specify the group of hosts and stations which will receive packets.
Process	The bandwidth process is slow.	The multicast process is fast.
Traffic	It creates a large amount of network traffic by delivering each packet to every site on the network.	It keeps traffic under control by delivering packets only to interested hosts, lowering the network load.

Distance vector routing

The distance vector routing algorithm is **one of the most commonly used routing algorithms**. It is a distributed algorithm, meaning that it is run on each router in the network. The algorithm works by each router sending updates to its neighbours about the best path to each destination. A **distance-vector protocol** calculates the distance and direction of the vector of the next hop from the information obtained by the neighboring router. Distant vector routing protocol also called as **Bellman-Ford algorithm** or **Ford Fulkerson** algorithm used to calculate a path. Historically known as the **old ARPANET routing algorithm {or known as Bellman Ford (BF) algorithm}.**

Key points of distance vector routing protocol:

- ✓ **Network Information:** Every node in the network have information about its neighboring node.
- ✓ Each node in the network is designed to share information with all the nodes in the network.
- ✓ **Routing Pattern:** In DVR the data shared by the nodes are transmitted only to that node that is linked directly to one or more nodes in the network.
- ✓ **Data sharing:** The nodes share the information with the neighboring node from time to time as there is a change in network topology.

Bellman-Ford algorithm

The **Bellman–Ford algorithm** is an algorithm that computes shortest paths from a single source vertex to all of the other vertices in a weighted digraph.

- ✓ Bellman ford algorithm is a single-source shortest path algorithm.
- ✓ Used to find the shortest distance from the single vertex (node) to all the other vertices (nodes) of a weighted network.
- ✓ It is similar to **Dijkstra's algorithm** but it can work with network in which edges can have **negative weights.**

Step to calculates shortest distances used (**V - 1**) times/Iteration, where **V** is the number of nodes in given network.

To **calculate** the distance between X and Y node using bellmen- ford equation.

$$d_x(y) = \min_v \{c(x, v) + d_v(y)\}$$

where, $d_x(y)$ = The least distance from **x** to **y**

c(x,v) = Node **x**'s cost from each of its neighbor

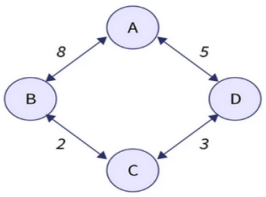
$vd_v(y)$ = Distance to each node from initial node

min_v = Selecting shortest distance

Example

Step - 1

As we can see in the above diagram of the DVR network, the routers in the network start sharing their information with the neighboring routers in the network.



Routing table of A:

Destination	distance	Hop
A	0	A
B	8	B
C	infinity	-
D	5	D

Routing table of C:

Destination	distance	Hop
A	infinity	-
B	2	B
C	0	C
D	3	D

Routing table of B:

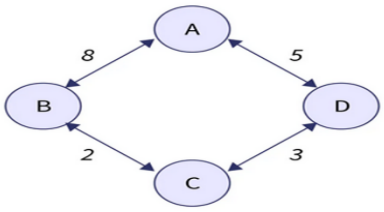
Destination	distance	Hop
A	8	A
B	0	B
C	2	C
D	infinity	-

Routing table of D :

Destination	distance	Hop
A	5	A
B	infinity	-
C	3	C
D	0	D

Step - 2

After creating the separate local table this information is shared with the neighboring node having a direct link.



For Router A:

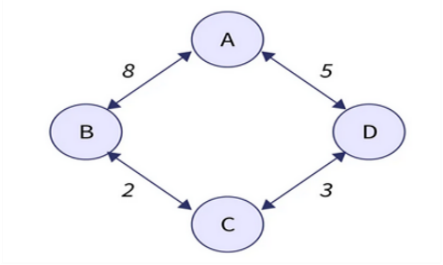
The router A has a direct connection to neighboring routers B and D.

Destination	Vector B	Vector D
A	8	5
B	0	infinity
C	2	3
D	infinity	0

✓ Consequently, A's new routing table is:

Destination	distance	Hop
A	0	A
B	8	B
C	8	D
D	5	D

For router B:
Router B receives information from A and C.



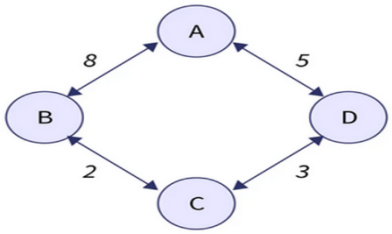
✓The new routing table for B is calculated as:

Destination	Vector A	Vector C
A	0	infinity
B	8	2
C	infinity	0
D	5	3

Consequently, B's new routing table is:

Destination	distance	Hop
A	8	A
B	0	B
C	2	C
D	5	C

For router C:
The router C receives information from B and D.



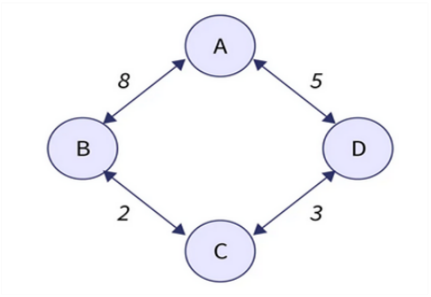
✓**The new routing table for C is calculated as:**

Destination	Vector B	Vector D
A	8	5
B	0	infinity
C	2	3
D	infinity	0

Consequently, C's new routing table is:

Destination	distance	Hop
A	8	D
B	2	B
C	0	C
D	3	D

For router D:
The router D receives information from A and C.



✓ **The new routing table for D is calculated as:**

Destination	Vector A	Vector C
A	0	infinity
B	8	2
C	infinity	0
D	5	3

Consequently, D's new routing table is:

Destination	distance	Hop
A	5	A
B	5	C
C	3	C
D	0	D

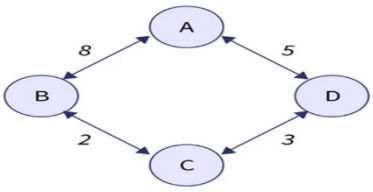
- **Step - 3**

✓ After this, the **router again exchanges the distance vector** obtained in step 2 with its neighboring router.

✓ After exchanging the distance vector, the router prepares a new routing table.

For router A:

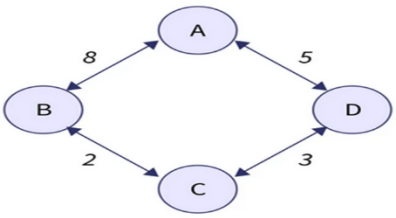
Destination	Vector B	Vector D
A	8	5
B	0	5
C	2	3
D	5	0



Consequently, A's new routing table is:

Destination	distance	Hop
A	0	A
B	8	B
C	8	D
D	5	D

For router B:
The router B receives information from A and C.



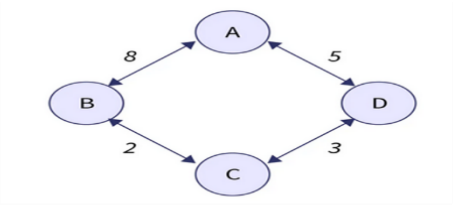
✓ **The new routing table for B is calculated as:**

Destination	Vector A	Vector C
A	0	8
B	8	2
C	8	0
D	5	3

Consequently, B's new routing table is:

Destination	distance	Hop
A	8	A
B	0	B
C	2	C
D	5	C

For router C:
The router C receives information from B and D.



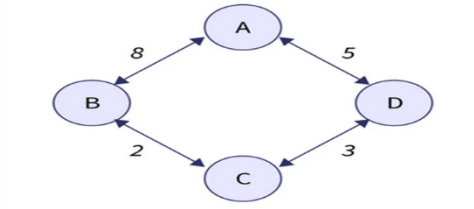
✓ **The new routing table for C is calculated as:**

Destination	Vector B	Vector D
A	8	5
B	0	5
C	2	3
D	5	0

Consequently, C's new routing table is:

Destination	distance	Hop
A	8	D
B	2	B
C	0	C
D	3	D

For router D:
The router D receives information from A and C.



✓ **The new routing table for D is calculated as:**

Destination	Vector A	Vector C
A	0	8
B	8	2
C	8	0
D	5	3

Consequently, D's new routing table is:

Destination	distance	Hop
A	5	A
B	5	C
C	3	C
D	0	D

As you can see in the above network all the link has been used.
- ✓ In the routing table of A link AD and AB is used.
- ✓ In the routing table of B only link BA and BC.
- ✓ In the routing table of C, only links CB and CD are used and in D's routing table only links DA and DC are used.

Congestion Control Algorithms,

Congestion:

A state occurring in **network layer** when the message traffic is **so heavy** that it slows down network response time. When too many packets are present in the network it causes packet delay and loss of packet which degrades the performance of the system. This situation is called **congestion**.

The **network layer** and **transport layer** share the responsibility for handling congestions. One of the most effective ways to control congestion is trying to reduce the load that transport layer is placing on the network.

Effects of Congestion

- ✓ As delay increases, performance decreases.
- ✓ If delay increases, retransmission occurs, making situation worse.

Congestion collapse

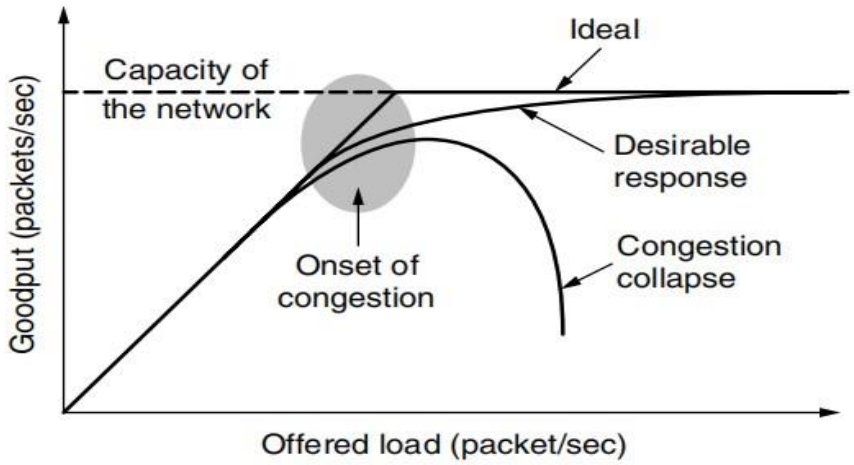


Figure 5-21. With too much traffic, performance drops sharply.

When the number of **packets hosts** send into the network is well within its **carrying capacity**, the number delivered is proportional to the number sent. If twice as many are sent, twice as many are delivered.

Causes of Congestion

If all of a sudden, streams of packets begin **arriving on three** or **four input lines** and all need the same output line, a queue will build up.

✓ If there is **insufficient memory** to hold all of them, packets will be lost.

i **Slow processors** can also cause congestion.

i. If the routers' CPUs are slow at performing the bookkeeping tasks required of them (queueing buffers, updating tables, etc.) queues can build up even though there is **excess line capacity**.

ii. Low-bandwidth lines can also cause congestion.

ii **Low-bandwidth** links or routers that process packets more slowly than the line rate can also become congested.

Example:

Case 1: consider a network made up of **100-Gbps** fiber optic links on which a supercomputer is trying to force feed a large file to a **personal computer** that is capable of handling only 1 Gbps. Although there is **no congestion** (the network itself is not in trouble), flow control is needed to force the supercomputer to stop frequently to give the personal computer a chance to breathe.

Case 2: consider a network with **1-Mbps** lines and **1000 large computers**, half of which are trying to transfer files at 100 kbps to the other half. Here, the problem is not that of fast senders overpowering slow receivers, but that the total offered traffic exceeds what the network can handle.

Congestion control algorithms

Congestion control in network layer occurs when a node or link carries data beyond its limit. This often leads to the queuing of packets—and in the worst case, loss of packets—as well as a decrease in the network's Quality of Service (QoS).

- **Congestion Control** is a mechanism that controls the entry of data packets into the network, enabling a better use of a shared network infrastructure and avoiding congestive collapse.
- **Congestive-Avoidance Algorithms** (CAA) are implemented at the **TCP layer** as the mechanism to avoid congestive collapse in a network.
  - ✓ By detecting congestion and adjusting the data transmission rate to avoid it.

Approaches to Congestion Control

- ✓ The presence of congestion means that the load is greater than the resources can handle.
- ✓ Two solutions come to mind: **increase the resources or decrease the load**.

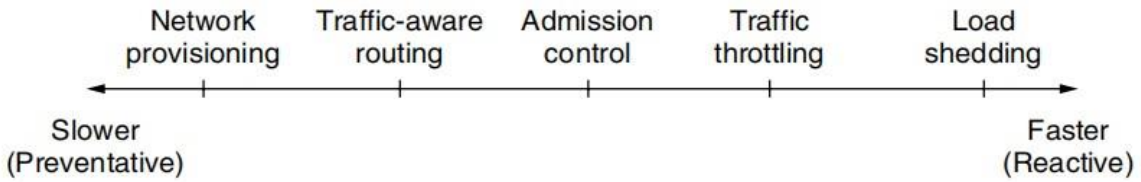


Figure 5-22. Timescales of approaches to congestion control.

Network provisioning

Network provisioning is **the process of setting up a network so that authorized users, devices, and servers can access it**. In practice, network provisioning primarily concerns connectivity and security, which means a heavy focus on device and identity management.

- ✓ Sometimes resources can be **added dynamically** when there is serious congestion.

- ✓ More often, links and routers that are **regularly heavily utilized** are upgraded at the earliest opportunity happens on a **time scale of months**, driven by long-term traffic trends. **Traffic-aware routing**
- ✓ To make the most of the existing network capacity, routes can be tailored to traffic patterns that change during the day as **network users wake** and **sleep in different time zones**.
- ✓ Splitting traffic across multiple paths is also helpful

Admission control

Admission control (AC) is a mechanism used in computer networks and telecommunications to ensure that new connections or traffic do not exceed the network's capacity or cause a degradation in the quality of service (QoS) provided to existing connections. Admission control can be performed at different levels of the network, such as at the application, transport, network, or link layer. In this article, we will focus on admission control at the network layer, which is also known as network admission control (NAC).

- ✓ Sometimes it is **not possible to increase capacity.**
- ✓ **New connections** can be **refused** if they would cause the network to become congested.

Traffic throttling

Traffic Throttling is **an approach used to avoid congestion**. In networks and the internet, the senders try to send as much traffic as possible as the network can readily deliver. In a network when congestion is approaching it should tell the senders of packets to slow down them.

- ✓ Routers can monitor the **average load**, **queueing delay**, or **packet loss**. In all cases, rising numbers indicate growing congestion.

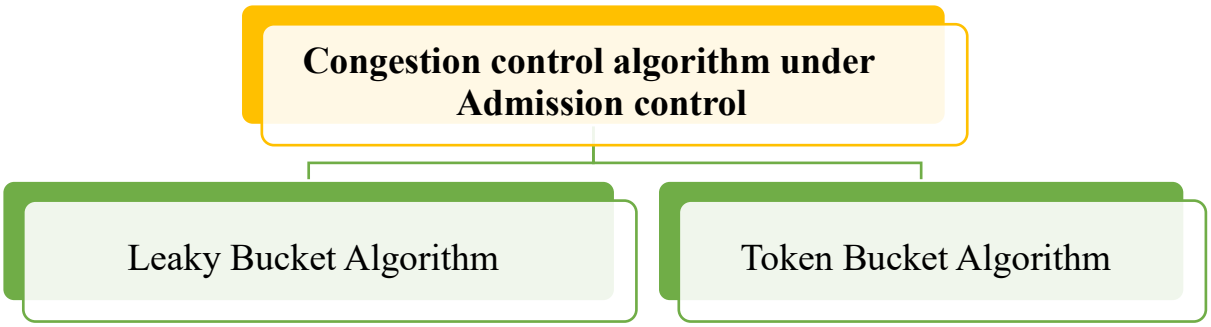
Load shedding

Load shedding is one of the techniques used for congestion control. A network router consists of a buffer. This buffer is used to store the packets and then route them to their destination. Load shedding is defined as an approach of discarding the packets when the buffer is full according to the strategy implemented in the data link layer. The selection of packets to discard is an important task. Many times packets with less importance and old packets are discarded.

- ✓ When all else **fails**, the network is forced to **discard packets** that it cannot deliver.
- ✓ A good policy for choosing which packets to discard can help to prevent congestion collapse

There are **two congestion control algorithm** which are under **admission control approach** as follows:

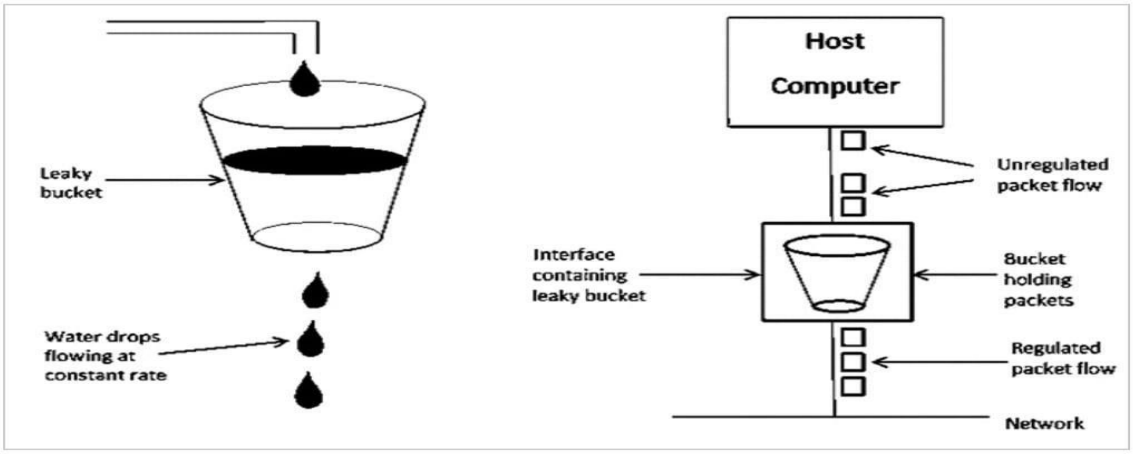
i. **Leaky Bucket Algorithm**
ii. **Token Bucket algorithm**



Leaky Bucket Algorithm

A leaky bucket algorithm is **primarily used to control the rate at which traffic enters the network**. It provides a mechanism for smoothing bursty input traffic in a flow to present a steady stream into the network. Leaky Bucket Algorithm *mainly controls the total amount and the rate of the traffic sent to the network*.

- ✓ The Leaky bucket algorithm is a "**traffic shaping**" algorithm to reduce the load, the transport layer places on the network layer and reduce congestion in the network.
- ✓ **Traffic shaping** is a congestion management technique, It control the amount of traffic sent to network and regulates the rate of data transmission.



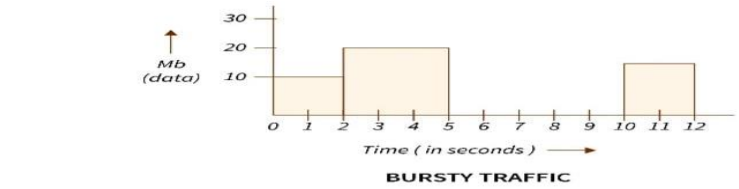
Goal of Leaky Bucket

The goal is to *reduce the load the transport layer places on the network to reduce congestion and improve* network performance. One commonly used method for traffic shaping is the leaky bucket algorithm.

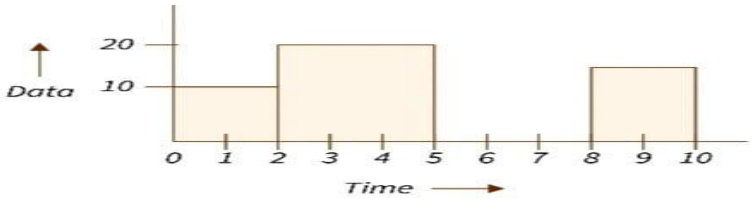
Example

Suppose Host A sends :

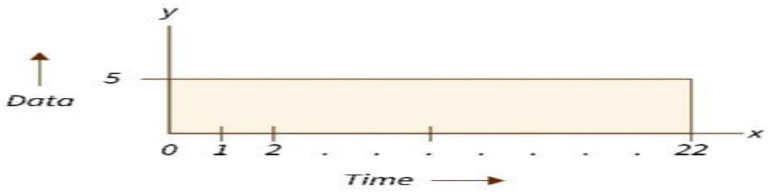
- 10 Mbps data for the first 2 seconds.
- 20 Mbps data for the next 3 seconds.
- No data for the next 5 seconds.
- 15 Mbps data for the next 2 seconds.



BURSTY TRAFFIC



BUSTY



UNIFORM

Bursty traffic is sudden, unexpected network volume traffic, peak and depression in a network

Suppose data enters the network from various sources at different speed.

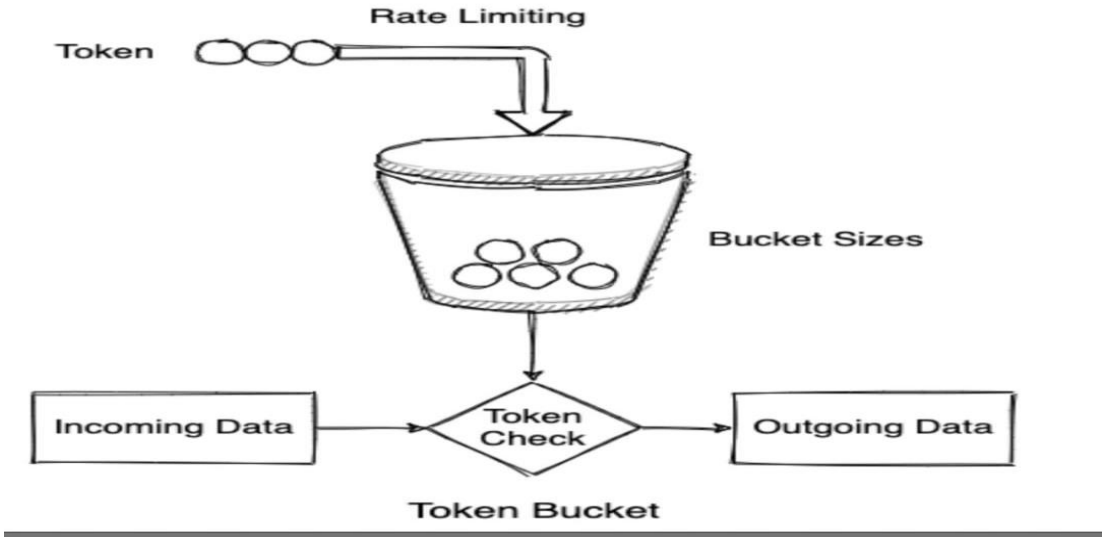
- Consider **one bursty source** that
  - ✓ Sends data at **20 Mbps** for **2 seconds** for total of **40 Mb**.
  - ✓ Then it **silent**, sending no data for **5 seconds**.
  - ✓ Then it again transmits data at a rate of **10 Mbps** for **3 seconds**, thus sending a total of **30 Mbps**.
  - ✓ So, in a time span of **10 seconds** the source sends **70 Mb data**.
  - ✓ The network has only committed a bandwidth of 5 Mbps for this source.
  - ✓ It uses the leaky bucket algorithm to output traffic at the rate of **5 Mbps** during the same time period of **10 Seconds**, which smooths out the network traffic.

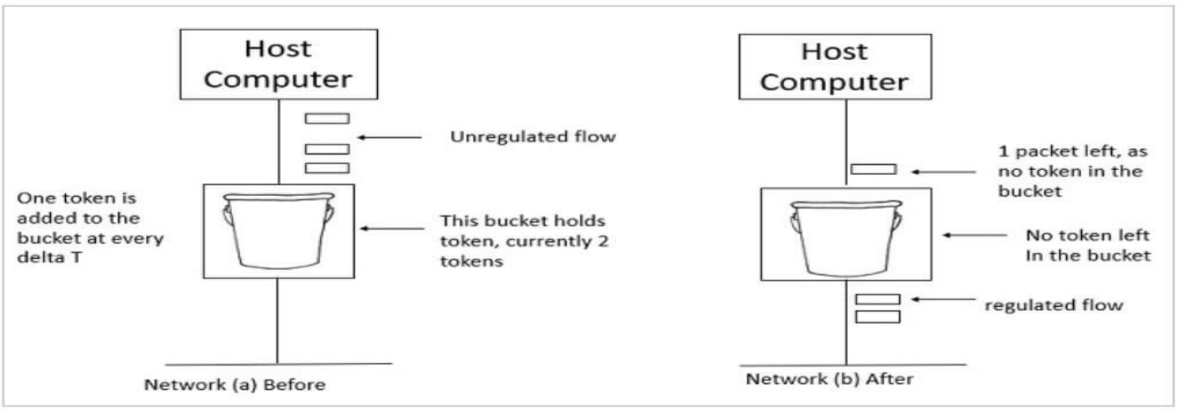
Token Bucket Algorithm

Token bucket algorithm is one of the techniques for congestion control algorithms. When too many packets are present in the network it causes packet delay and loss of packet which degrades the performance of the system. This situation is called congestion. Token bucket algorithm is based on **analogy of a fixed capacity bucket** into which tokens, normally representing a unit of bytes or a single packet of predetermined size, are added a fixed rate.

It employs a metaphorical "**token bucket**" that holds tokens at a fixed rate.

- ✓ Each token represents permission to perform a specific action or transmit a unit of data.
- ✓ Requests or events require a **certain number of tokens** to proceed, and the system consumes tokens from the bucket accordingly.
- ✓ If there are **insufficient tokens**, the request may be **delayed or denied**.
- ✓ To control the rate of actions to prevent network congestion and ensure more predictable resource usage.





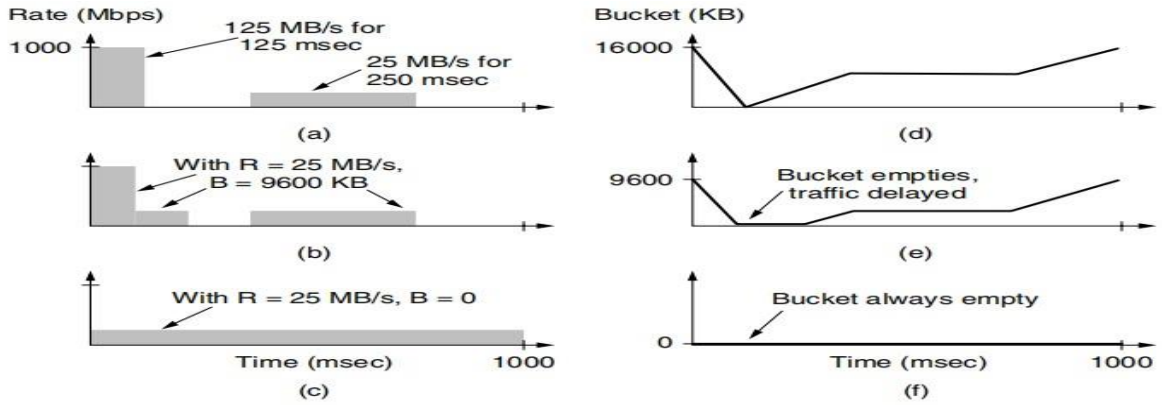


Figure 5-29. (a) Traffic from a host. Output shaped by a token bucket of rate 200 Mbps and capacity (b) 9600 KB and (c) 0 KB. Token bucket level for shaping with rate 200 Mbps and capacity (d) 16,000 KB, (e) 9600 KB, and (f) 0 KB.

QUALITY OF SERVICE

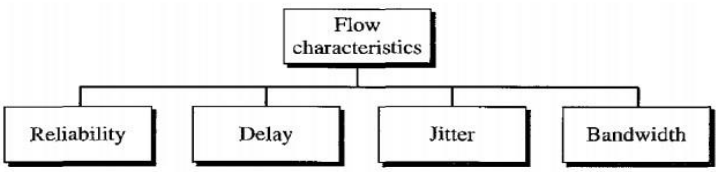
Quality of service (QoS) is **the use of mechanisms or technologies that work on a network to control traffic and ensure the performance of critical applications with limited network capacity**. It enables organizations to adjust their overall network traffic by prioritizing specific high-performance applications.

Quality of service (QoS) is a set of technologies that work on a network to guarantee its ability to dependably run high-priority applications and traffic under limited network capacity. QoS technologies accomplish this by providing differentiated handling and capacity allocation to specific flows in network traffic. This enables the network administrator to assign the order in which packets are handled and the amount of bandwidth afforded to that application or traffic flow.

A stream of packets from a source to a destination is called a **flow**.

- ✓ A flow might be all the packets of a connection in a connection-oriented network, or all the packets sent from one process to another process in a connectionless network.
- ✓ The needs of each flow can be characterized by four primary parameters:
- ✓ **Reliability, delay, jitter and Bandwidth**.
- ✓ Together, these determine the **QoS** (**Quality of Service**) the flow requires.

Figure 24.15 *Flow characteristics*



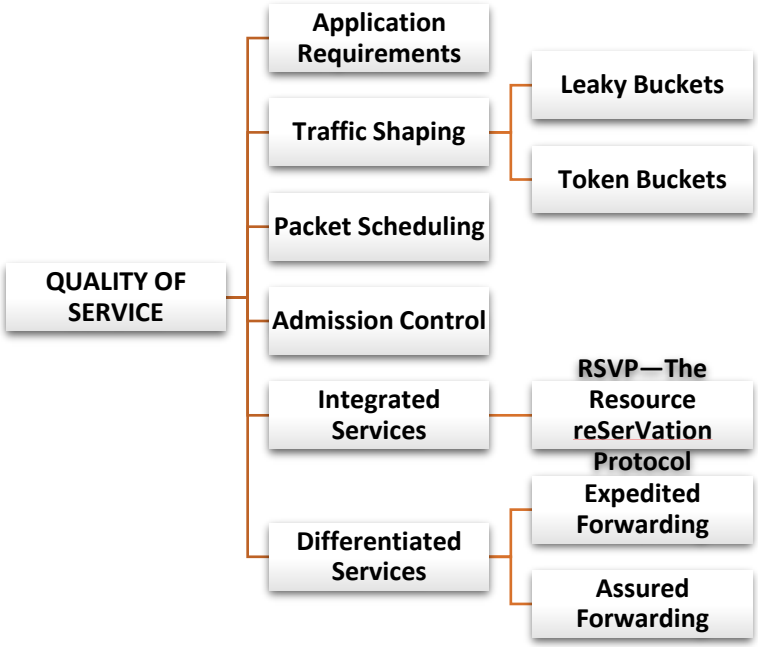
Flow Characteristics

- ***Reliability***
  - ✓ Reliability is a characteristic that a **flow needs**.
- ***Delay***
  - ✓ **Source-to-destination delay** is another flow characteristic.
- ***Jitter***
  - ✓ Jitter is the **variation in delay for packets** belonging to the same flow.
- ***Bandwidth***
  - ✓ Different applications need **different bandwidths**.

Quality of Service (QoS) is an **internetworking issue** that has been discussed more than defined.

Four issues must be addressed to ensure quality of service:

i. What applications need from the network
ii. How to regulate the traffic that enters the network. iii. How to reserve resources at routers to guarantee performance.
iii. Whether the network can safely accept more traffic

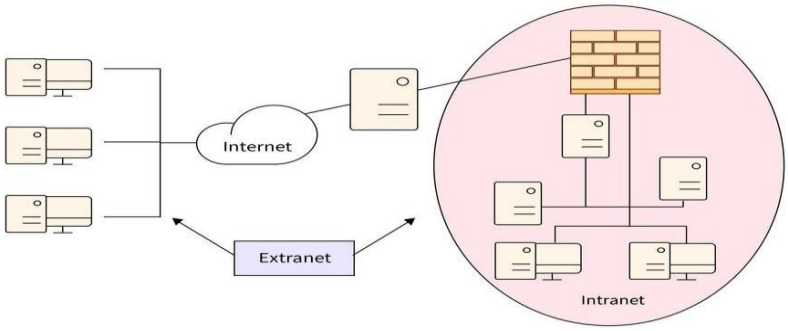


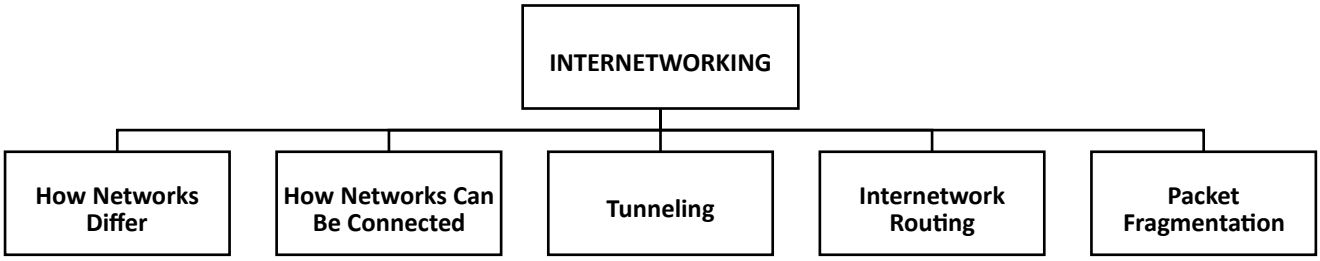
INTERNETWORKING

Internetworking is **the practice of interconnecting multiple computer networks**, such that any pair of hosts in the connected networks can exchange messages irrespective of their hardware-level networking technology. Connecting **computer networks** to **additional networks** using **gateways** and **routers** is commonly known as internetworking. These **interconnected networks** are called **internetworks**. It would be much simpler to join networks together if everyone used a single networking technology, and it is often the case that

there is a dominant kind of network, such as **Ethernet**. A router that can handle multiple network protocols is called a **multiprotocol router**.

Since networks often differ in important ways, **getting packets from one network to another is not always so easy**. The problems of **heterogeneity**, and also problems of **scale** as the resulting **internet grows very large.**





How Networks Differ

Networks can **differ** in many ways.

- ✓ Some of the differences, such as different modulation techniques or frame formats, are internal to the physical and data link layers.
- ✓ When packets sent by a **source** on one network must transit one or more foreign networks before reaching the destination network, many problems can occur at the **interfaces between networks**.
- ✓ To start with, the **source** needs to be able to address the destination.

If the **source** is on an Ethernet network and the **destination** is on a WiMAX network?

- ✓ Assuming, even specify a **WiMAX destination** from an **Ethernet network**, packets would cross from a connectionless network to a connection-oriented one.

- ✓ This may require that a new connection be set up on short notice, which injects a delay, and much overhead if the connection is not used for many more packets.

Item	Some Possibilities
Service offered	Connectionless versus connection oriented
Addressing	Different sizes, flat or hierarchical
Broadcasting	Present or absent (also multicast)
Packet size	Every network has its own maximum
Ordering	Ordered and unordered delivery
Quality of service	Present or absent; many different kinds
Reliability	Different levels of loss
Security	Privacy rules, encryption, etc.
Parameters	Different timeouts, flow specifications, etc.
Accounting	By connect time, packet, byte, or not at all

Figure 5-38. Some of the many ways networks can differ.

How Networks Can Be Connected

There **are two basic choices** for connecting different networks:

- ✓ Can build devices that translate or convert packets from each kind of network into packets for each other network.
- ✓ A router that can handle multiple network protocols is called a **multiprotocol router**.

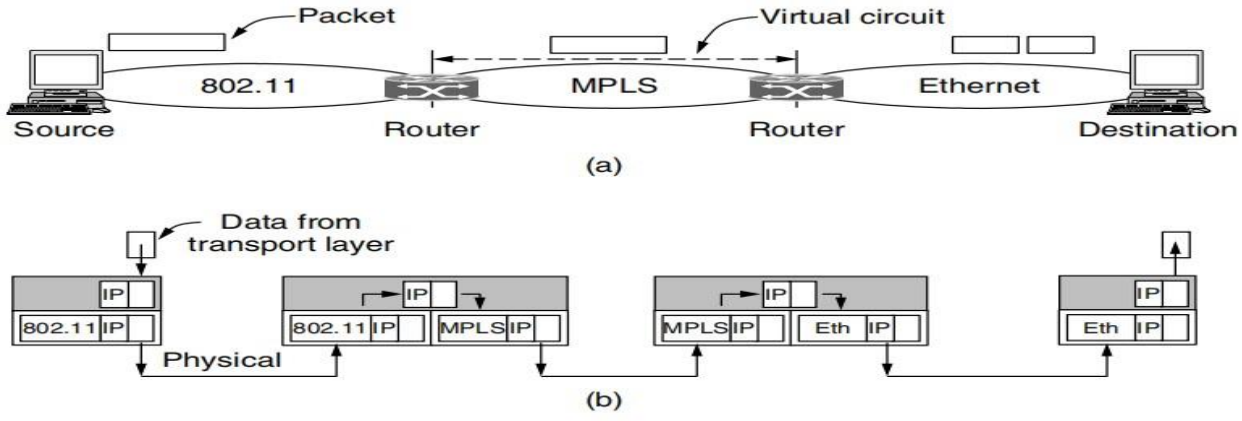


Figure 5-39. (a) A packet crossing different networks. (b) Network and link layer protocol processing.

Tunneling

Tunneling is **a way to move packets from one network to another**. Tunneling works via encapsulation: wrapping a packet inside another packet. Networking basics. Network layer. How Internet works. A technique of inter-networking called **Tunneling** is used when source and destination networks of the same type are to be connected through a network of different types. A *tunneling* protocol is a communication protocol which allows for the movement of data from one network to another. *Tunneling* is a way for communication to be conducted over a private network but tunneled through a public network. Tunneling uses a **layered protocol model** such as those of the OSI or TCP/IP protocol suite.

- ✓ Handling the two different networks interwork is exceedingly difficult.
- ✓ However, there is a common special case that is manageable even for different network protocols.
- ✓ This case is where the source and destination hosts are on the same type of network, but there is a different network in between.

Deployment of a network protocol with a new feature is a common reason, as our "**IPv6 over IPv4**" example shows.

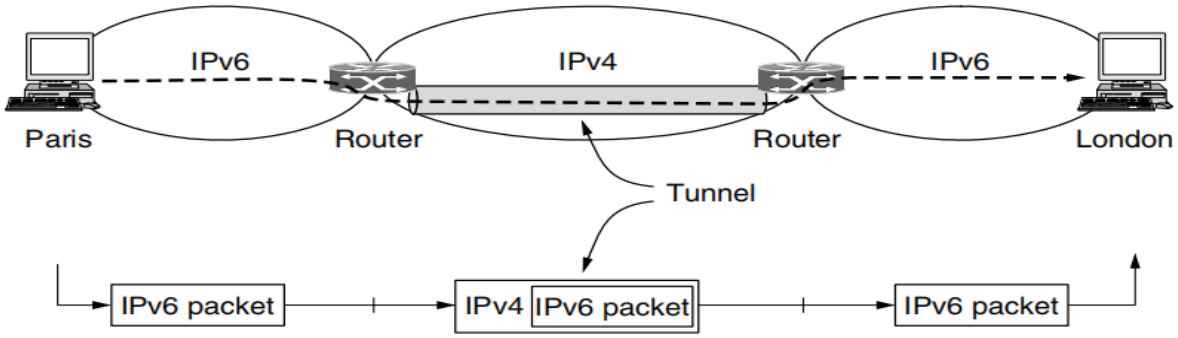


Figure 5-40. Tunneling a packet from Paris to London.

The limitation of tunnels is turned into an advantage with **VPNs** (**Virtual Private Networks**). A VPN is simply an overlay that is used to provide a measure of security. **Tunneling** is widely used to **connect isolated hosts and networks** using **other networks**. The network that results is called an **overlay** since it has effectively been overlaid on the base network.

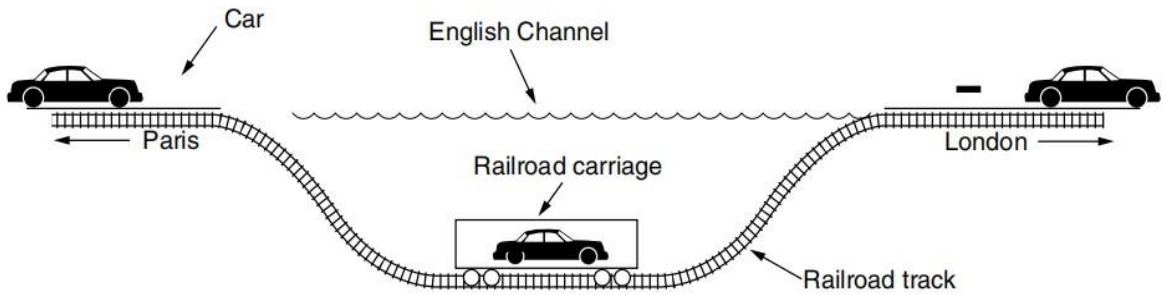
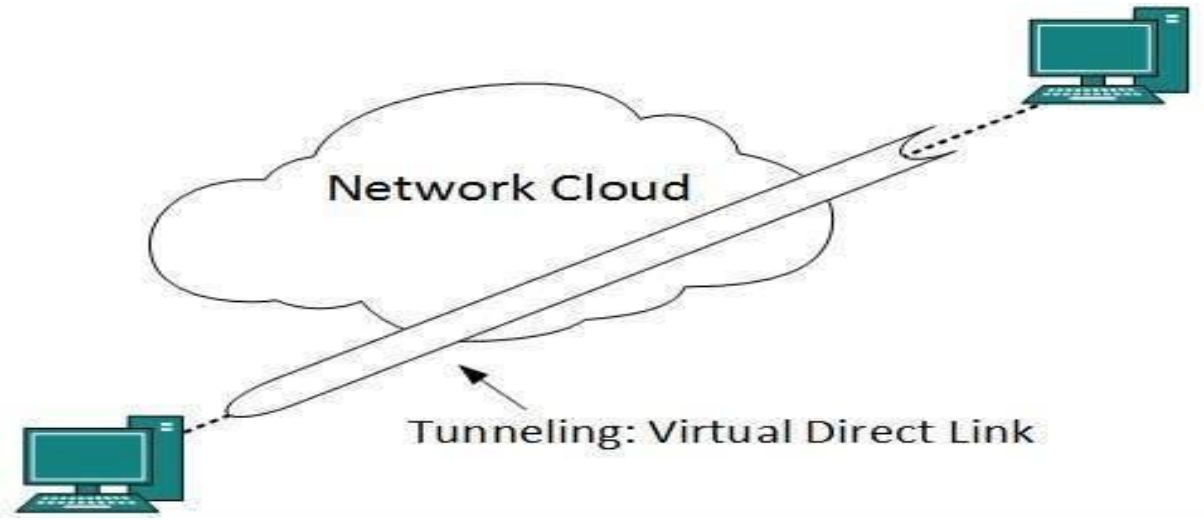


Figure 5-41. Tunneling a car from France to England.

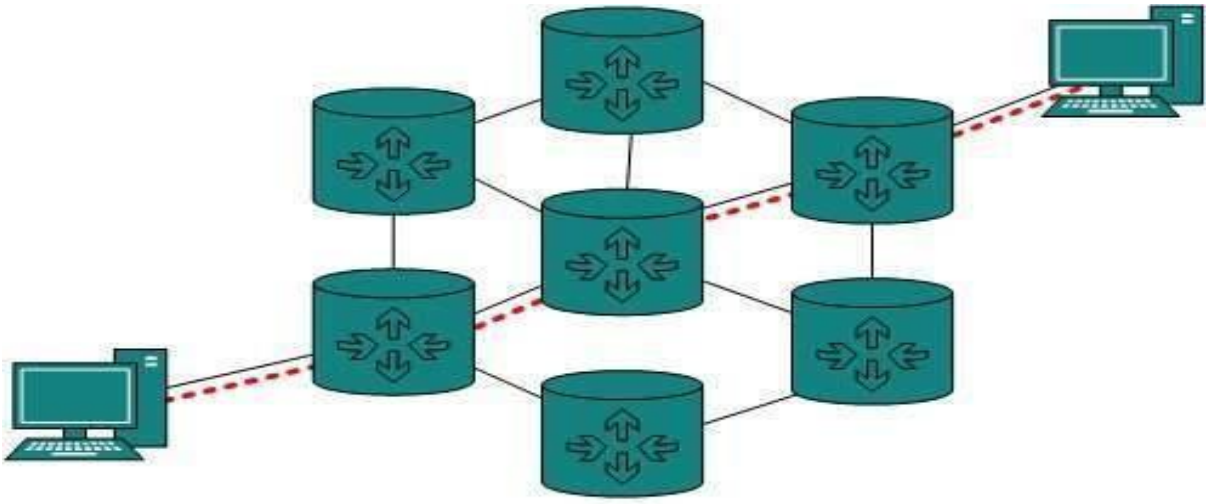
- ✓ Tunneling is a mechanism by which two or more same networks communicate with each other, by passing intermediate networking complexities.
- ✓ Tunneling is configured at both ends.



Internetwork Routing

Routing between two networks is called internetworking. Networks can be considered different based on various parameters such as, Protocol, topology, Layer-2 network and addressing scheme. In internetworking, routers have knowledge of each other's address and addresses beyond them. Routing through an internetwork is similar to routing within a single subnet, but with some added complications.

In **internetworking**, routers have knowledge of each other's address and addresses beyond them. They can be statically configured go on different network or they can learn by using internetworking routing protocol.



Routing protocols

A routing protocol **specifies how routers exchange routing information with each other**, enabling them to determine routes between any two nodes on a computer network.
Within each network, an **intradomain** or **interior gateway protocol** is used for routing. (‘‘**Gateway**’’ is an older term for ‘‘**router**’’). Across the networks that make up the internet, an **interdomain** or **exterior gateway protocol** is used. The networks may all use different intradomain protocols, but they must use the same interdomain protocol.

- ✓ Routing protocols which are used within an organization or administration are called **Interior Gateway Protocols (IGP)**.
- ✓ RIP, OSPF are examples of IGP.
- ✓ Routing between different organizations or administrations may have **Exterior Gateway Protocol** and there is only one **EGP** i.e. **Border Gateway Protocol**.
- ✓ In the Internet, the interdomain routing protocol is called **BGP** (**Border Gateway Protocol**).

Packet Fragmentation

Fragmentation dissects the ***packets*** into smaller pieces so that they can fit the smaller links as they travel the network. Every packet based network has an MTU (**Maximum Transmission Unit**) size. The MTU is the size of the largest packet that network can transmit. **Fragmentation:** when the maximum size of datagram is greater than maximum size of data that can be held in a frame i.e., its Maximum Transmission Unit, The network layer divides the datagram received from the transport layer into fragments so that data flow is not disrupted. **Packets** larger than the allowable MTU must be divided into smaller packets or fragments to enable them to traverse the network.

These limits have various causes, among them:

i. Hardware (e.g., the size of an Ethernet frame).

ii. Operating system (e.g., all buffers are 512 bytes).
iii. Protocols (e.g., the number of bits in the packet length field).
iv. Compliance with some (inter)national standard.
v. Desire to reduce error-induced retransmissions to some level.
vi. Desire to prevent one packet from occupying the channel too long.

IP fragmentation is an Internet Protocol (IP) process that breaks packets into smaller pieces (fragments), so that the resulting pieces can pass through a link with a smaller maximum transmission unit (MTU) than the original packet size. The fragments are reassembled by the receiving host.

Packet Fragmentation

- **Transparent fragmentation** is straightforward but has some problems.
- **Nontransparent fragmentation** strategy is to refrain from recombining fragments at any intermediate routers.

The main advantage of nontransparent fragmentation is that it requires routers to do less work.

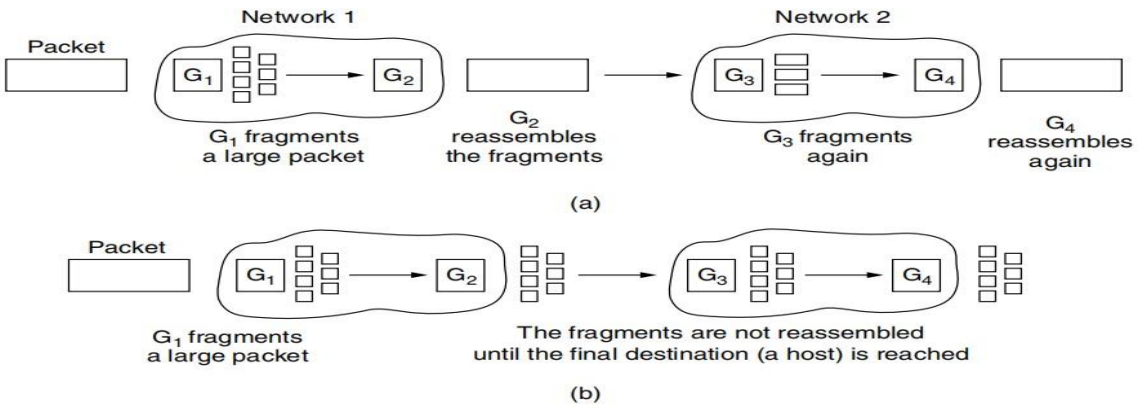


Figure 5-42. (a) Transparent fragmentation. (b) Nontransparent fragmentation.

THE NETWORK LAYER IN THE INTERNET

In the network layer, the Internet can be viewed as a collection of networks or **ASes** (**Autonomous Systems**) that are interconnected. **ISP**s (Internet Service Providers) that provide Internet access to homes and businesses, data centers and colocation facilities full of server machines, and regional (mid-level) networks. The data centers serve much of the content that is sent over the Internet. Attached to the regional networks are more **ISP**s, **LAN**s at many universities and companies, and other edge networks.

- ✓ The glue that holds the whole Internet together is the network layer protocol, **IP** (**Internet Protocol**).
- ✓ The Network layer protocols, **IP** was designed from the beginning with internetworking in mind.

To provide a best-effort (i.e., not guaranteed) way to transport packets from source to destination, without regard to whether these machines are on the same network or whether there are other networks in between them.

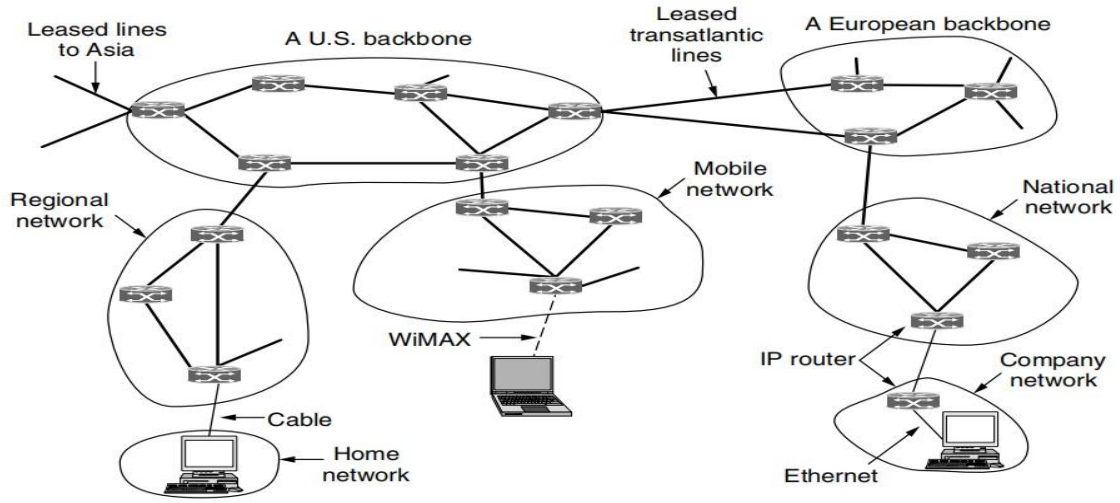


Figure 5-45. The Internet is an interconnected collection of many networks.

THE NETWORK LAYER IN THE INTERNET

i. The IP Version 4 Protocol,
ii. IP Addresses,
iii. IP Version 6,
iv. Internet Control Protocols,
v. Label Switching and MPLS,
vi. OSPF—An Interior Gateway Routing Protocol,
vii. BGP—The Exterior Gateway Routing Protocol,
viii. Internet Multicasting,
ix. Mobile IP,

The IP Version 4 Protocol

Internet Protocol version 4 (IPv4) is **the fourth version of the Internet Protocol (IP)**. It is one of the core protocols of standards-based internetworking methods in the Internet and other packet-switched networks.

The network layer in the **Internet** is with the format of the IP datagrams themselves. An IPv4 datagram consists of a **header part** and a **body** or **payload part**. The **header** has a 20-byte fixed part and a variable-length optional part. The bits are transmitted from **left to right** and **top to bottom**, with the high-order bit of the *Version* field going first.

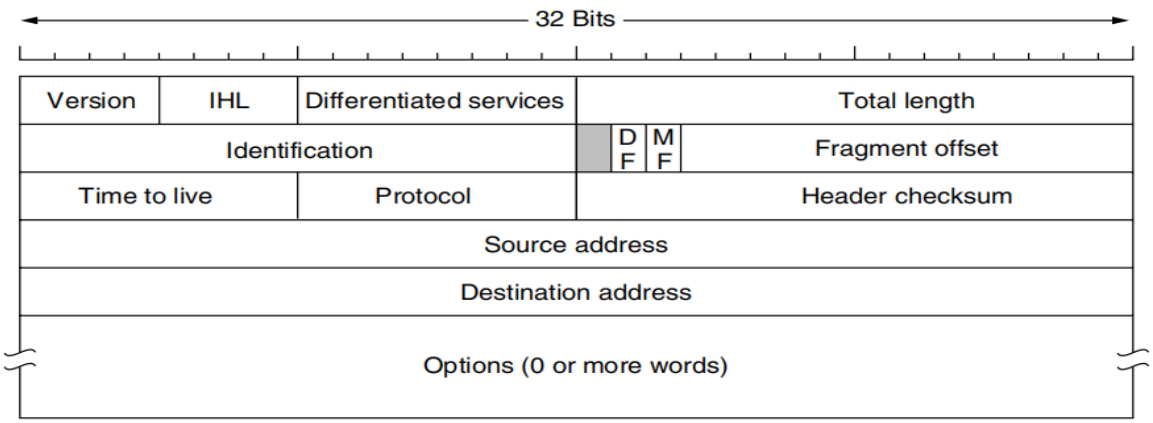


Figure 5-46. The IPv4 (Internet Protocol) header.

The IPv4 (Internet Protocol) header

- **Version – The IP version number, 4.**
- **Header length** – The length of the datagram header in **32-bit words**.
- **Type of service (*Differentiated services*)** – Contains five subfields that specify the precedence(**priority** 07), **delay**, **throughput**, **reliability**, and **cost desired** for a packet.
- **Total length** – The length of the datagram in bytes including the **header**, **options**, and the appended transport protocol segment or packet. The maximum length is bytes.
- **Identification** – An integer that **identifies** the datagram.
- **DF** – Don't fragment
- **MF** – More Fragments. All fragments except the last one have this **bit set**.
- **Fragment offset** – The relative position of this fragment measured from the **beginning of the original datagram** in units of **8 bytes**.
- **Time to live** – How many routers a datagram can pass through. Each router decrements this value by **1** until it reaches **0** when the datagram is discarded.
- **Protocol** – The **high-level protocol** type.
- **Header checksum** – A number that is computed to ensure the integrity of the header values.
- **Source address** – The **32-bit IPv4 addr**ess of the sending host.
- **Destination address** – The **32-bit IPv4 address** of the receiving host.
- **Options** – A list of optional specifications for **security restrictions**, **route recording**, and **source routing**. Not every datagram specifies an options field.
- **Padding** – **Null bytes** which are added to make the **header length an integral multiple of 32 bits** as required by the header length field.

Option	Description
Security	Specifies how secret the datagram is
Strict source routing	Gives the complete path to be followed
Loose source routing	Gives a list of routers not to be missed
Record route	Makes each router append its IP address
Timestamp	Makes each router append its address and timestamp

Figure 5-47. Some of the IP options.

IP address (Internet Protocol address)

An Internet Protocol (IP) address is **the unique identifying number assigned to every device connected to the internet**. An IP address definition is a numeric label assigned to devices that use the internet to communicate. An IP address definition is a numeric label assigned to devices that use the internet to communicate. Computers that communicate over the internet or via local networks share information to a specific location using IP addresses.

Public IP Address

A public IP address, or external-facing IP address, applies to the main device people use to connect their business or home internet network to their internet service provider (ISP). In most cases, this will be the router. All devices that connect to a router communicate with other IP addresses using the router's IP address.

Knowing an external-facing IP address is crucial for people to open ports used for online gaming, email and web servers, media streaming, and creating remote connections.

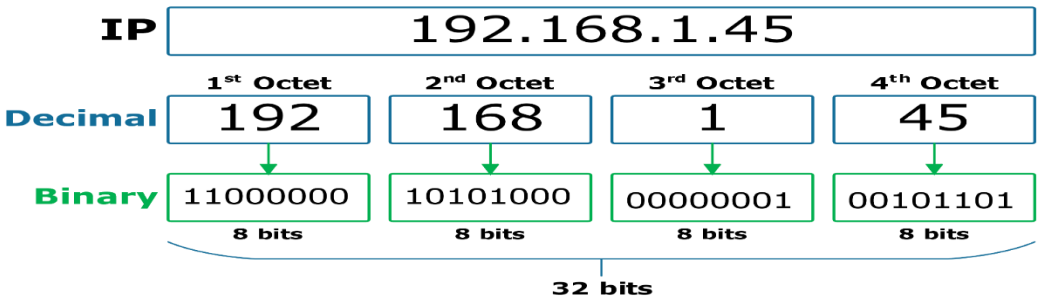
Private IP Address

A private IP address, or internal-facing IP address, is assigned by an office or home intranet (or local area network) to devices, or by the internet service provider (ISP). The home/office router manages the private IP addresses to the devices that connect to it from within that local network. Network devices are thus mapped from their private IP addresses to public IP addresses by the router.

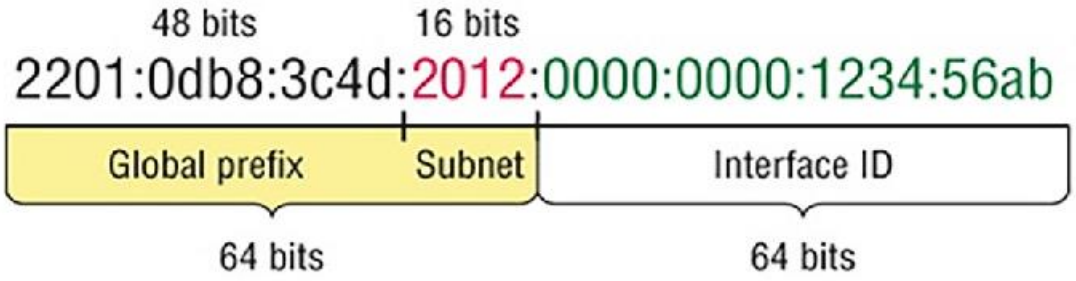
Private IP addresses are reused across multiple networks, thus preserving valuable IPv4 address space and extending addressability beyond the simple limit of IPv4 addressing (4,294,967,296 or 2^32).

- An **Internet Protocol** (IP) address is a unique numerical identifier for every device or network that connects to the internet.
- There are **two versions** of IP addresses that are commonly used on the internet:• **IPv4 and IPv6.**

- An **IPv4** address is expressed as a set of **four dotted decimal numbers**, where each octet is separated by a period, such as **192.168.35.4**
- A full IP address ranges from 0.0.0.0 to 255.255.255.255.
- An **IPv6** address represents eight groups of four hexadecimal digits separated by **colons**, such as 2620:cc:8000:1c82:544c:cc2e:f2fa:5a9b.



IPv4 IP Address format



IPv6 IP Address format

IPv4 Addresses

The IPv4 address consists of a ***network address*** and a ***host address***. Within the Internet, a central authority, the Network Information Center (NIC), assigns the network addresses. The class of address determines the portion of the IPv4 address that is used for each of these addresses.
A defining feature of **IPv4 is its 32-bit addresses**. Every host and router on the Internet has an **IP address** that can be used in the *Source address* and *Destination address* fields of **IP packets**. An **IPv4** address is a 32-bit address that ***uniquely*** and ***universally*** defines the connection of a device to the Internet.

- ✓ In IPv4, a unique sequence of bits is assigned to a computer, a total of (**2^32**) devices approximately = **4,294,967,296** can be assigned with IPv4.

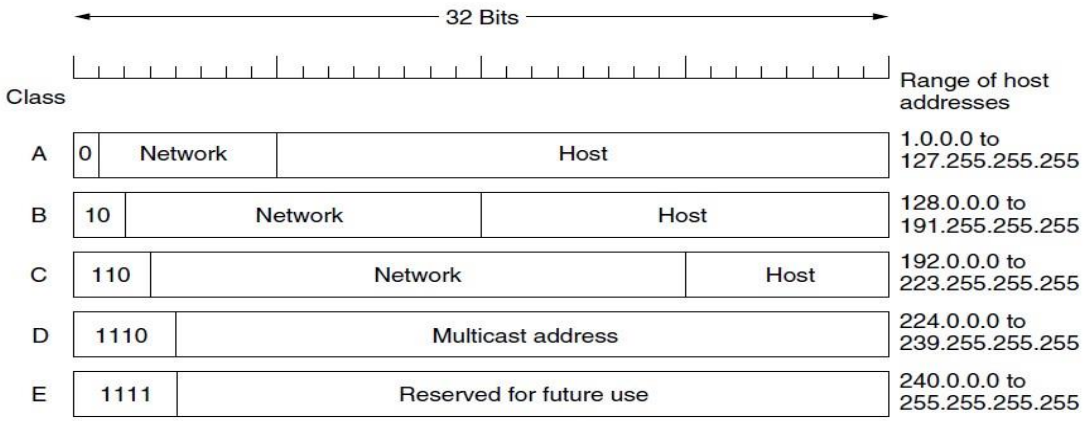
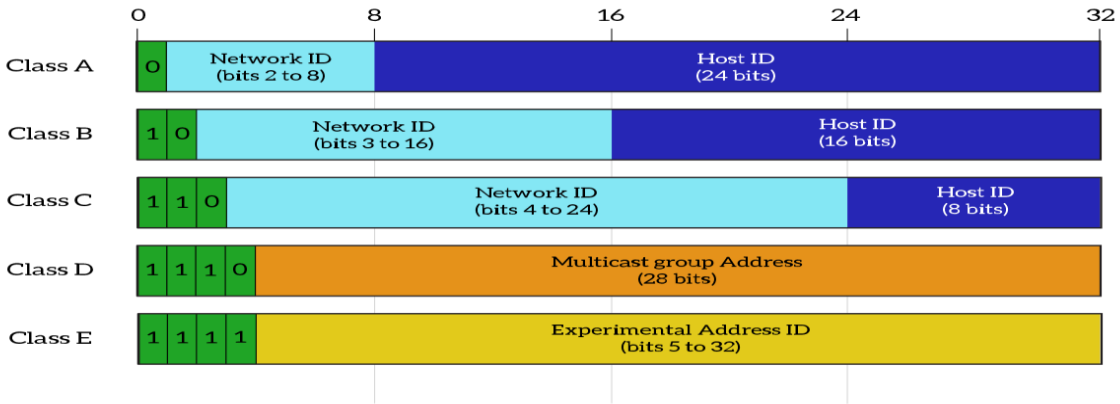


Figure 5-53. IP address formats.

An IP address is an **online device address** used for communicating across the internet. It really refers to a **network interface**, so if a host is on two networks, it must have two IP addresses. However, in practice, most hosts are on one network and thus have one IP address.
In contrast, **routers** have multiple interfaces and thus multiple IP addresses

- ✓ The **0.0.0.0** is a **Non-routable address** is that indicates an invalid, or inapplicable end-user address.
- ✓ A **loopback address** is a distinct reserved IP address range that starts from **127.0.0.0** ends at **127.255.255.255.**
- ✓ **127.255.255.255** is the **broadcast address** for **127.0.0.0/8**.
- ✓ The **loopback addresses** are built into the IP domain system, enabling devices to transmit and receive the data packets.
- ✓ The **loopback address 127.0.0.1** is generally known as **localhost**.

IP addresses are assigned and managed by a nonprofit corporation called **ICANN** (**Internet Corporation for Assigned Names and Numbers**), to avoid conflicts. **ICANN** has delegated parts of the address space to various regional authorities, which dole out IP addresses to ISPs and other companies. This is the process by which a company is allocated a block of IP addresses.



IP Class	Address Range	Maximum number of networks
Class A	1-126	126 (2^7-2)
Class B	128-191	16384
Class C	192-223	2097152
Class D	224-239	Reserve for multitasking
Class E	240-254	Reserved for Research and development

Subnetting is **the process of creating a subnetwork.** It is also known as a **subnet** within a network. Network interfaces and devices within a subnet can communicate with each other directly. Routers facilitate communication between different subnets.

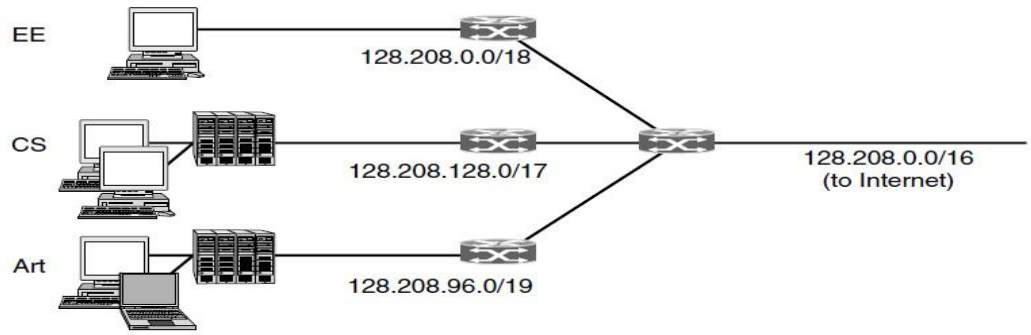


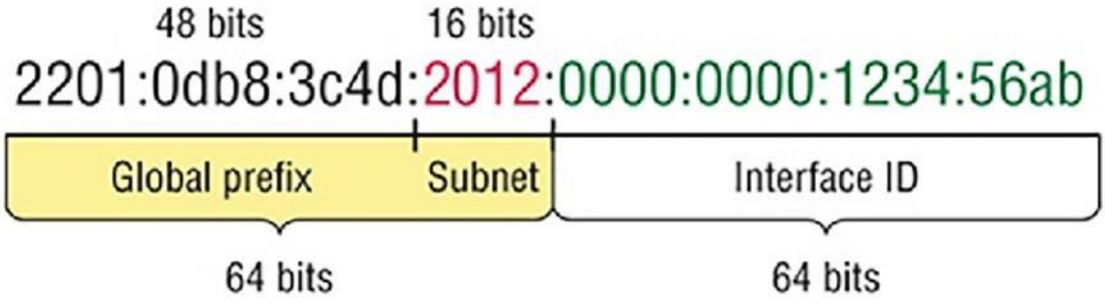
Figure 5-49. Splitting an IP prefix into separate networks with subnetting.

IP Version 6

IPv6 or Internet Protocol Version 6 is a network layer protocol that allows communication to take place over the network. Internet Engineering Task Force (IETF) designed IPv6 in

December 1998 with the purpose of superseding the IPv4 due to the global exponentially growing internet users.

Internet Protocol (**IP**) version 6 (**IPv6** or IP*ng*) is the next generation of **IP** and has been designed to be an evolutionary step from **IP** version 4 (**IPv4**). An **IPv6 address** is a 128-bit alphanumeric value that identifies an endpoint device in an Internet Protocol Version 6 (IPv6) network. **IPv6** was developed by **Internet Engineering Task Force** (IETF) to deal with the problem of IPv4 exhaustion. IPv6 is a **128-bits** address having an address space of $\mathbf{2^{128}}$, which is way bigger than IPv4. An **IPv6** address is 128 bits long and is arranged in eight groups, each of which is 16 bits. Each group is expressed as **four hexadecimal digits** and the groups are separated by **colons (:).**



An **IPv6** address is split into **two parts**: a **network** and a node component.

- ✓ The **network component** is the first 64 bits of the address and is used for routing.
- ✓ The **node component** is the later 64 bits and is used to identify the address of the interface.

It is derived from the physical, or MAC address, using the 64-bit extended unique identifier (EUI-64) format defined by the **Institute of Electrical and Electronics Engineers** (IEEE).

The Main IPv6 Header

The IPv6 header is more streamlined: it contains **8** fields,

- ✓ The ***Version*** field is always 6 for IPv6.
- ✓ The ***Differentiated services*** field (originally called ***Traffic class***) is used to distinguish the class of service for packets with different real-time delivery.
- ✓ ***Flow label*** field provides a way for a source and destination to mark groups of packets that forming a pseudo connection.
- ✓ ***Payload length*** field tells how many bytes follow the 40-byte header.
- ✓ ***Next header*** field lets the cat out of the bag.
- ✓ ***Hop limit*** field is used to keep packets from living forever.
- ✓ ***Source address*** and ***Destination address*** fields.

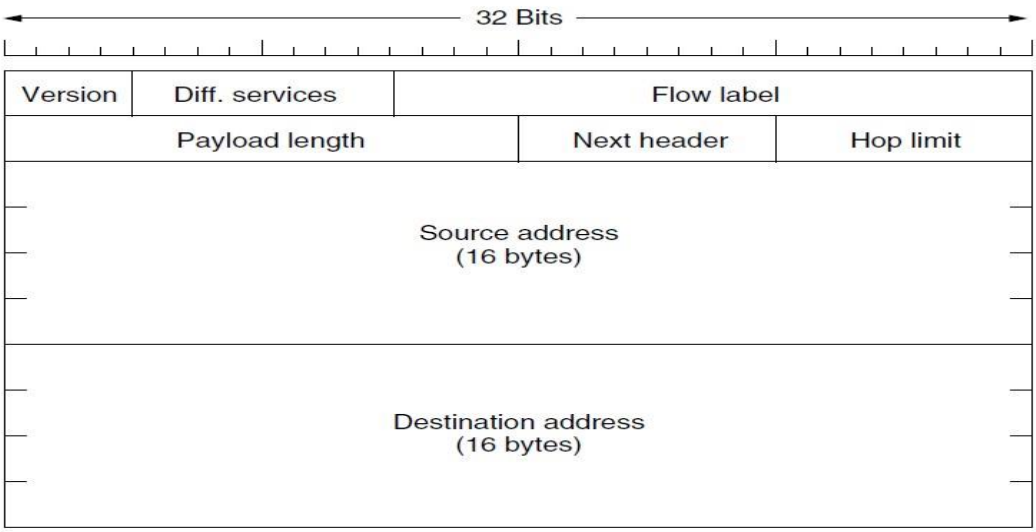
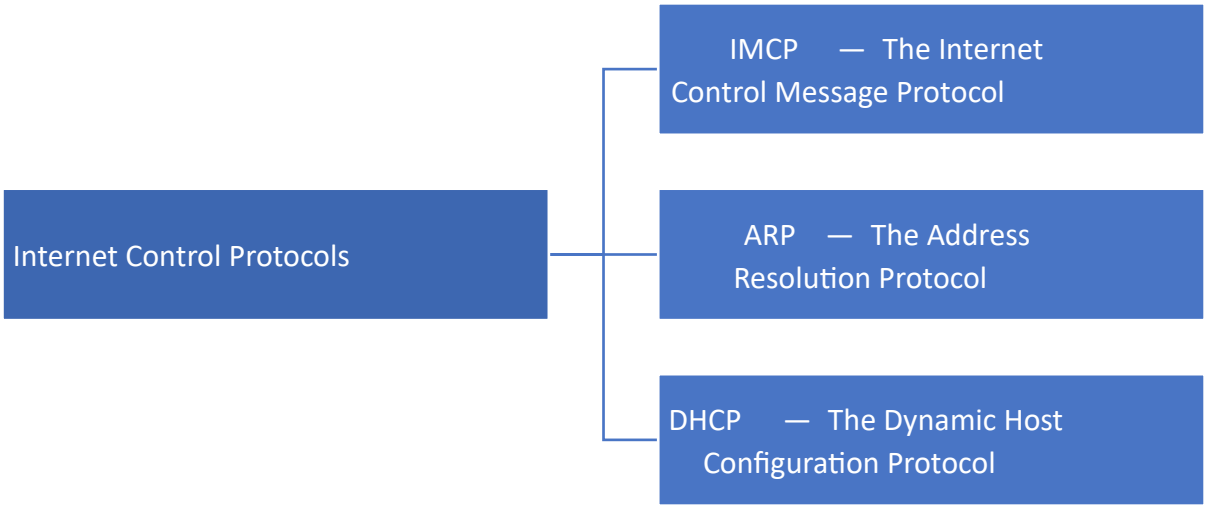


Figure 5-56. The IPv6 fixed header (required).

Internet Control Protocols

- The Internet has several companion control protocols that are used in the network layer.

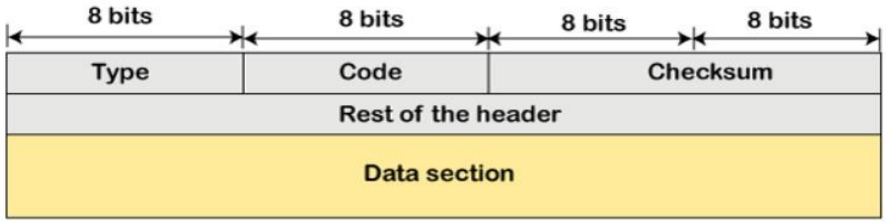


ICMP—Internet Control Message Protocol

The **Internet Control Message Protocol (ICMP)** is a protocol that devices within a network use to communicate problems with data transmission. It is used for error handling in the network layer, and it is primarily used on network devices such as routers. The use of ICMP is for reporting errors.

For example: extremely large packets of data may be too big for a router to manage.
In that case, the router will discard the data packet and transmit an ICMP message to the sender informing it of the issue.

The ICMP message contains the following fields:



- ✓ Type: It is an 8-bit field. It defines the ICMP message type. The values range from 0 to 127 are defined for ICMPv6, and the values from 128 to 255 are the informational messages.
- ✓ Code: It is an 8-bit field that defines the subtype of the ICMP message.
- ✓ Checksum: It is a 16-bit field to detect whether the error exists in the message or not.

ICMP—The Internet Control Message Protocol

Each ICMP message type is carried encapsulated in an IP packet. The most important ones are listed in Fig. 5-60.

Message type	Description
Destination unreachable	Packet could not be delivered
Time exceeded	Time to live field hit 0
Parameter problem	Invalid header field
Source quench	Choke packet
Redirect	Teach a router about geography
Echo and echo reply	Check if a machine is alive
Timestamp request/reply	Same as Echo, but with timestamp
Router advertisement/solicitation	Find a nearby router

Category	Type	Message
Error-Reporting Messages	3	Destination unreachable
	4	Source quench
	11	Time Exceeded
	12	Parameter Problem
	5	Redirection
Query Message	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply
	17 or 18	Address mask request or reply
	10 or 9	Router Solicitation or advertisement

Figure 5-60. The principal ICMP message types.

-

ARP—The Address Resolution Protocol

Address Resolution Protocol (ARP) is a communication protocol used to find the MAC (Media Access Control) address of a device from its IP address. This protocol is used when a device wants to communicate with another device on a Local Area Network or Ethernet. It is **a layer 2 protocol used to map MAC addresses to IP addresses**. All hosts on a network are

located by their IP address, but **NICs** do not have IP addresses, they have MAC addresses. ARP is the protocol used to associate the IP address to a MAC address.

There are **different versions and use cases of ARP**.

i. **Proxy ARP**
   - ✓ Proxy ARP is a technique by which a proxy device on a given network answers the ARP request for an IP address that is not on that network.
   - ✓ The proxy is aware of the location of the traffic's destination and offers its own MAC address as the destination. **ii. Gratuitous ARP**
   - ✓ Gratuitous ARP is an administrative procedure, carried out as a way for a host on a network to simply announce or update its **IP-to-MAC address**.

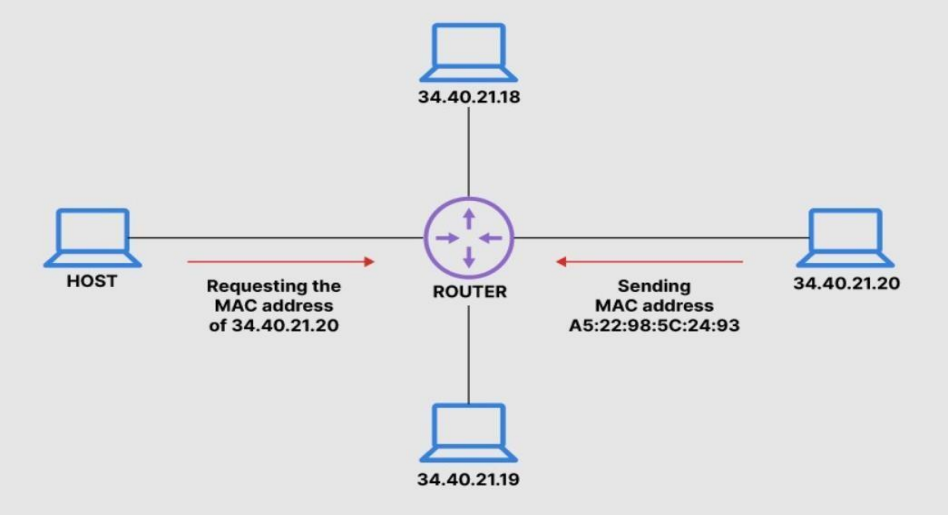
ii. **Reverse ARP (RARP)**
   - ✓ Host machines that do not know their own IP address can use the Reverse Address Resolution Protocol (RARP) for discovery.

iii. **Inverse ARP (IARP)**
   - ✓ Whereas ARP uses an IP address to find a MAC address, IARP uses a MAC address to find an IP address.

ARP—The Address Resolution Protocol

The **ARP** program to find a MAC address that matches the IP address.

- ✓ The ARP cache keeps a list of each IP address and its matching MAC address.
- ✓ The ARP cache is dynamic, but users on a network can also configure a static ARP table containing **IP addresses** and **MAC addresses**.



DHCP—The Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the **subnet mask** and **default gateway**. **DHCP** helps enterprises to smoothly manage the allocation of IP addresses to the end-user clients' devices such as **desktops**, **laptops**, **cellphones**, etc.

It is an application layer protocol that is used to provide:

```
Subnet Mask (Option 1 - e.g., 255.255.255.0)
Router Address (Option 3 - e.g., 192.168.1.1)
DNS Address (Option 6 - e.g., 8.8.8.8)
Vendor Class Identifier (Option 43 - e.g.,
'unifi' = 192.168.1.9 ##where unifi = controller)
```

- ✓ **DHCP** maintaining a unique IP Address for a host using the server.
- ✓ DHCP servers maintain information on TCP/IP configuration and provide configuration of address to DHCP-enabled clients in the form of a lease offer.

How Does DHCP Work?

To fully understand the working of DHCP, we must look at the **components of the DHCP** network:

- ✓ **DHCP server:** This is the central device that holds, assigns, and manages IP addresses.
- ✓ It can be a **server, router**, or **SD-WAN appliance**.
- ✓ **DHCP client:** This is the endpoint that requests for IP addresses and can be installed on any type of peripheral device, although most are part of the default settings.
- ✓ **Subnets:** These are parts of a more extensive network.
- ✓ **DHCP relay:** This refers to devices like routers that acts as a middleman between clients and server, amplifying the messages to reach their destination goal.

Label Switching and MPLS

Multi Protocol Label Switching (MPLS) is an IP packet routing technique that routes IP packet through paths via labels instead of looking at complex routing tables of routers. This feature helps in increasing the delivery rate of IP packets. MPLS is a networking technology that routes traffic using the shortest path based on "labels," rather than network addresses, to handle forwarding over private wide area networks. MPLS is multiprotocol, which means it can handle multiple network protocols. MPLS is highly versatile and unifying, as it provides mechanisms to carry a multitude of traffic, including Ethernet traffic. One of the key

differentiators between MPLS and traditional routers is it doesn't need specialized or additional hardware.

A new MPLS header had to be added in front of the IP header.

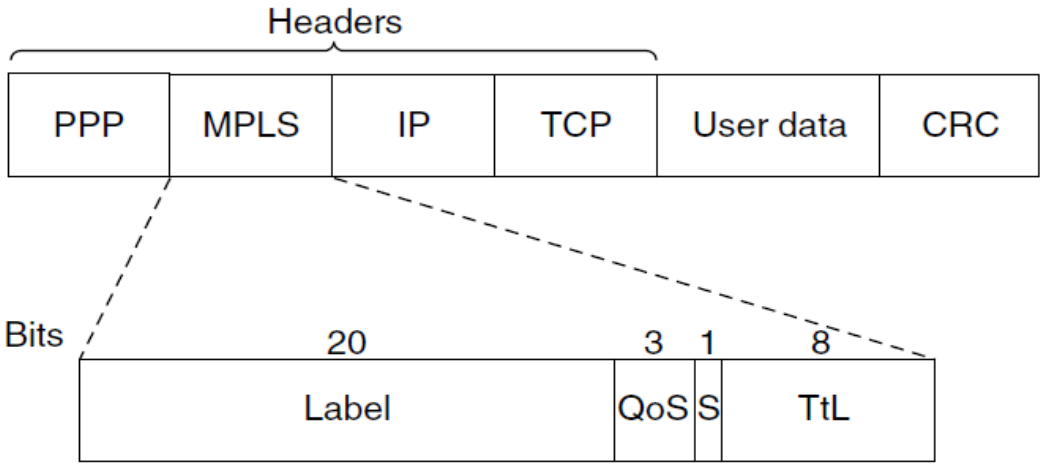


Figure 5-62. Transmitting a TCP segment using IP, MPLS, and PPP.

- ✓ On a router-to-router line using PPP as the framing protocol, the frame format, including the PPP, MPLS, IP, and TCP headers, is as shown in Fig. 5-62.

Label Switching and MPLS

The MPLS network, this label is used to forward the packet. At the other edge of the MPLS network, the label has served its purpose and is removed, revealing the IP packet again for the next network.

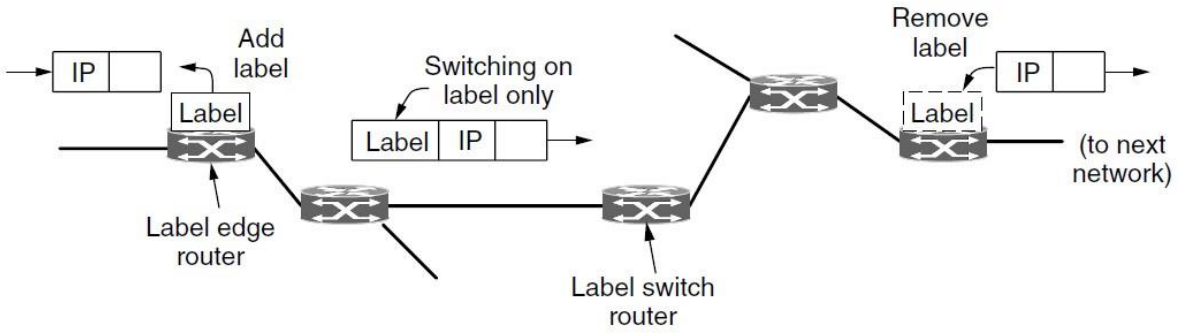


Figure 5-63. Forwarding an IP packet through an MPLS network.

OSPF—An Interior Gateway Routing Protocol

The **OSPF** (**Open Shortest Path First**) protocol is a IP Routing protocols, and is an **Interior Gateway Protocol** (**IGP**) for the Internet, **used to distribute IP routing information throughout a single Autonomous System (AS)** in an **IP network.**

The protocol which aims at moving the packet within a large autonomous system or routing domain. It is an intradomain protocol, which means that it is used within an area or a network. It is based on a link-state routing algorithm in which each router contains the information of every domain, and based on this information, it determines the shortest path. The goal of routing is to **learn routes**.

The OSPF achieves by learning about every router and subnet within the entire network. OSPF uses a link-state routing algorithm. Each router has information about every link and router in the network. It finds the shortest path to each destination. OSPF learns about all routers and subnets in the network to build a **link-state database** (LSDB). Routers exchange **link-state advertisements** (LSAs) to share information about **routers**, **subnets**, and more.

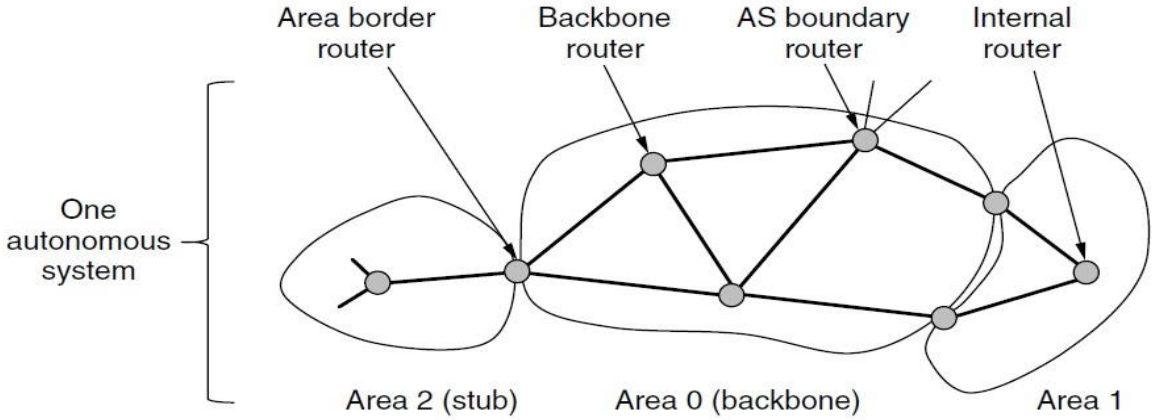


Figure 5-65. The relation between ASes, backbones, and areas in OSPF.

BGP—The Exterior Gateway Routing Protocol

Border Gateway Protocol (BGP) is a standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems (AS) on the Internet. **BGP** is one of a family of IP Routing protocols, and is an Exterior Gateway Protocol (EGP) designed to distribute routing information between ASs.

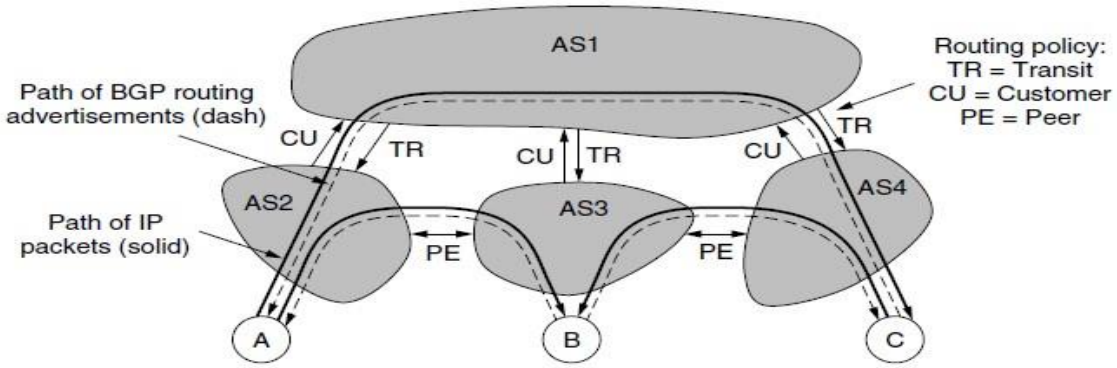


Figure 5-67. Routing policies between four autonomous systems.