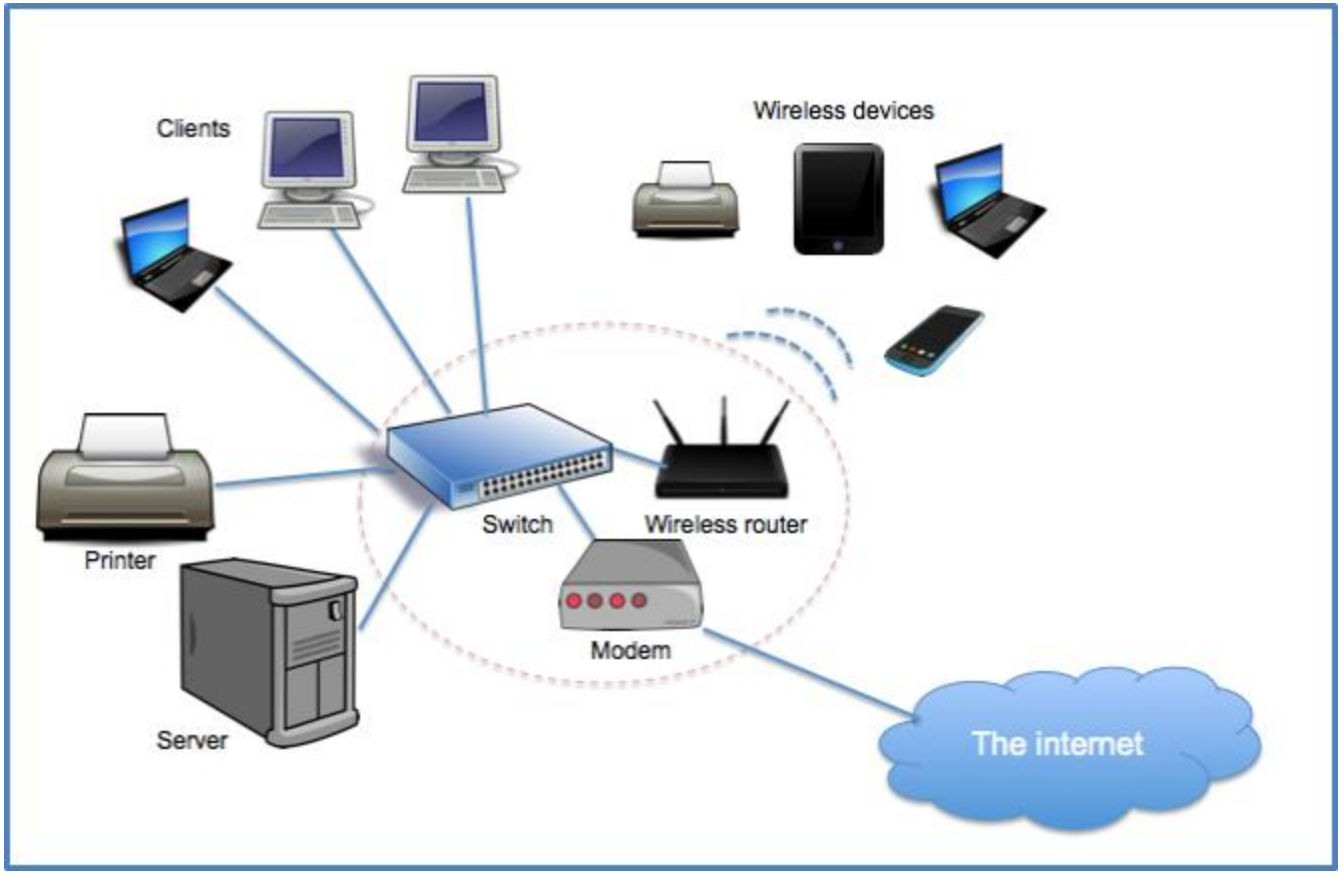
COMPUTER NETWORKS

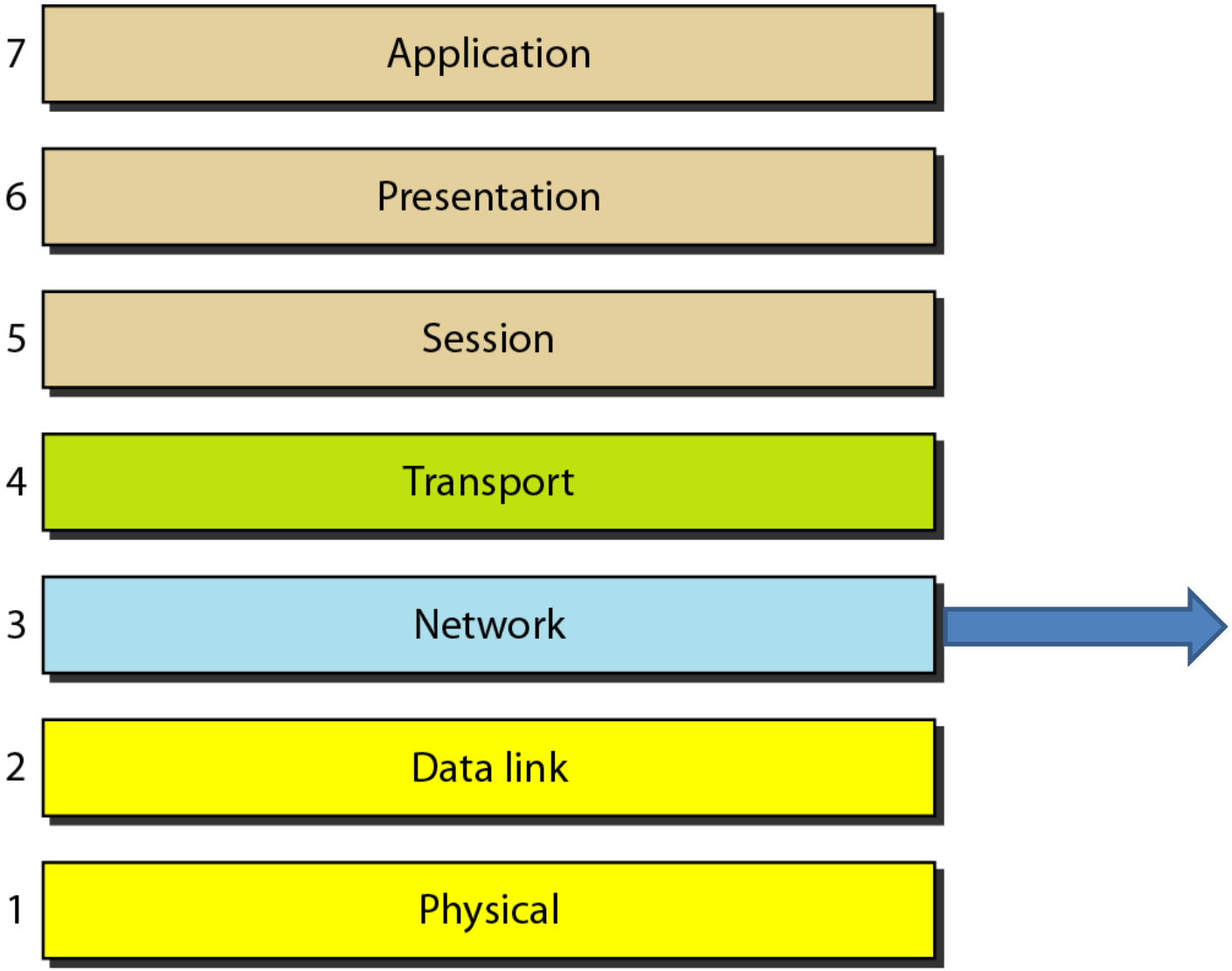


Instructor: Mr. B. V. Sathish Kumar, Assistant Professor

Department of Electronics and Communication Engineering

UNIT – IV
NETWORK LAYER

Figure: Seven layers of OSI Model

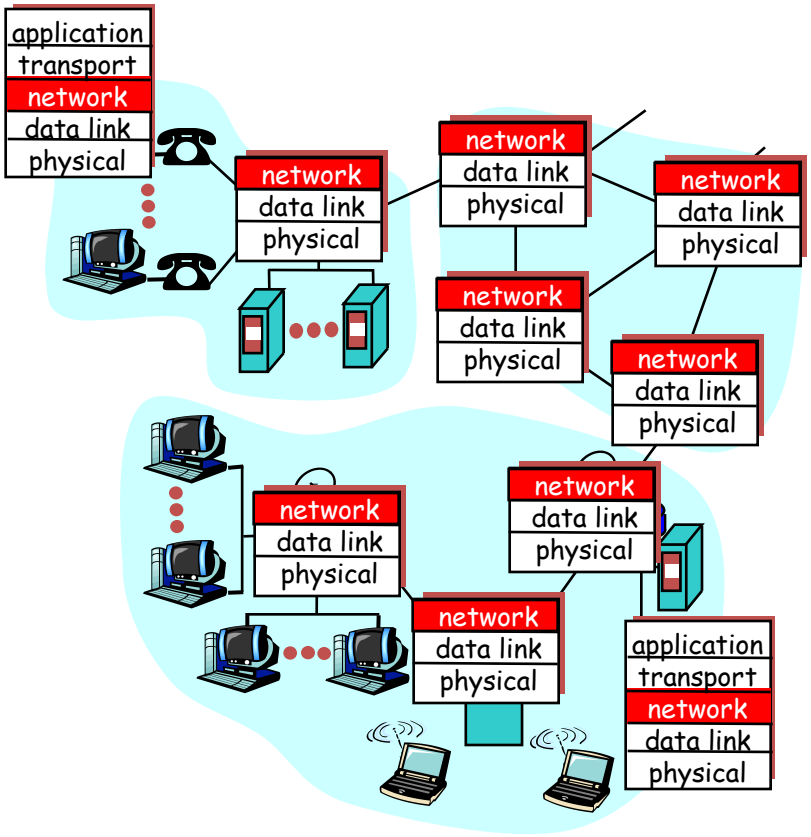


Network layer functions

- Transport packet from sending to receiving hosts
- Network layer protocols in every host, router

Three important functions:

1. *Path determination:* route taken by packets from source to destination. Routing algorithms
2. *Switching:* move packets from router's input to appropriate router output
3. *Call setup:* some network architectures require router call setup along path before data flows



UNIT-IV Syllabus

- Network Layer Design Issues
- Routing Algorithms
- Congestion Control Algorithms
- Internet Protocol Header
- IP Addresses
- subnetting and supernetting

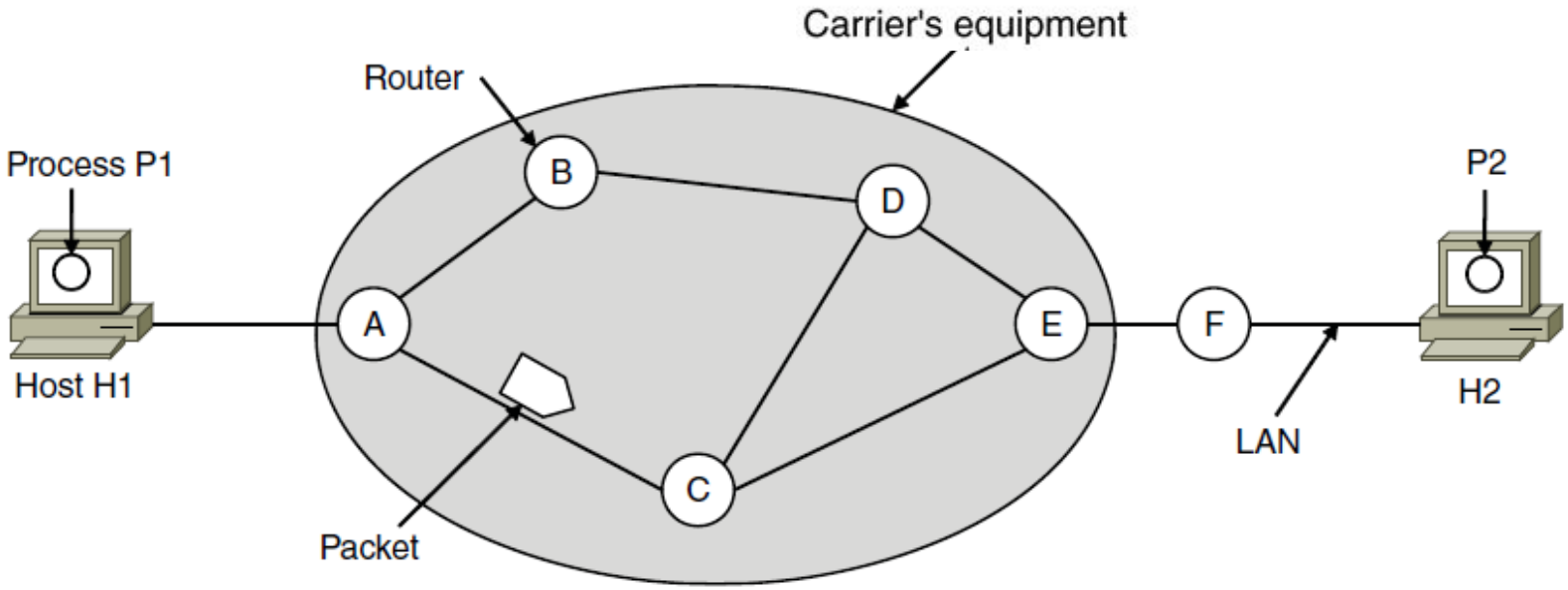
Network Layer Design Issues

Topics discussed in this section:

- Store-and-forward packet switching
- Services provided to transport layer
- Implementation of connectionless service
- Implementation of connection-oriented service
- Comparison of Virtual Circuit subnets and Datagram Networks

Store and Forward Packet Switching

The major components of the system are the carrier's equipment (routers connected by transmission lines inside the subnet) and customers equipment.



The environment of the network layer protocols.

Cntd...

A host sends a packet to the nearest router either on its own LAN or over a point-to-point link to the ISP.

The packet is stored there until it has fully arrived and the link has finished its processing by verifying the checksum.

Then it is forwarded to the next router along the path until it reaches the destination host, where it is delivered.

This mechanism is called store and forward mechanism.

Services provided to Transport layer

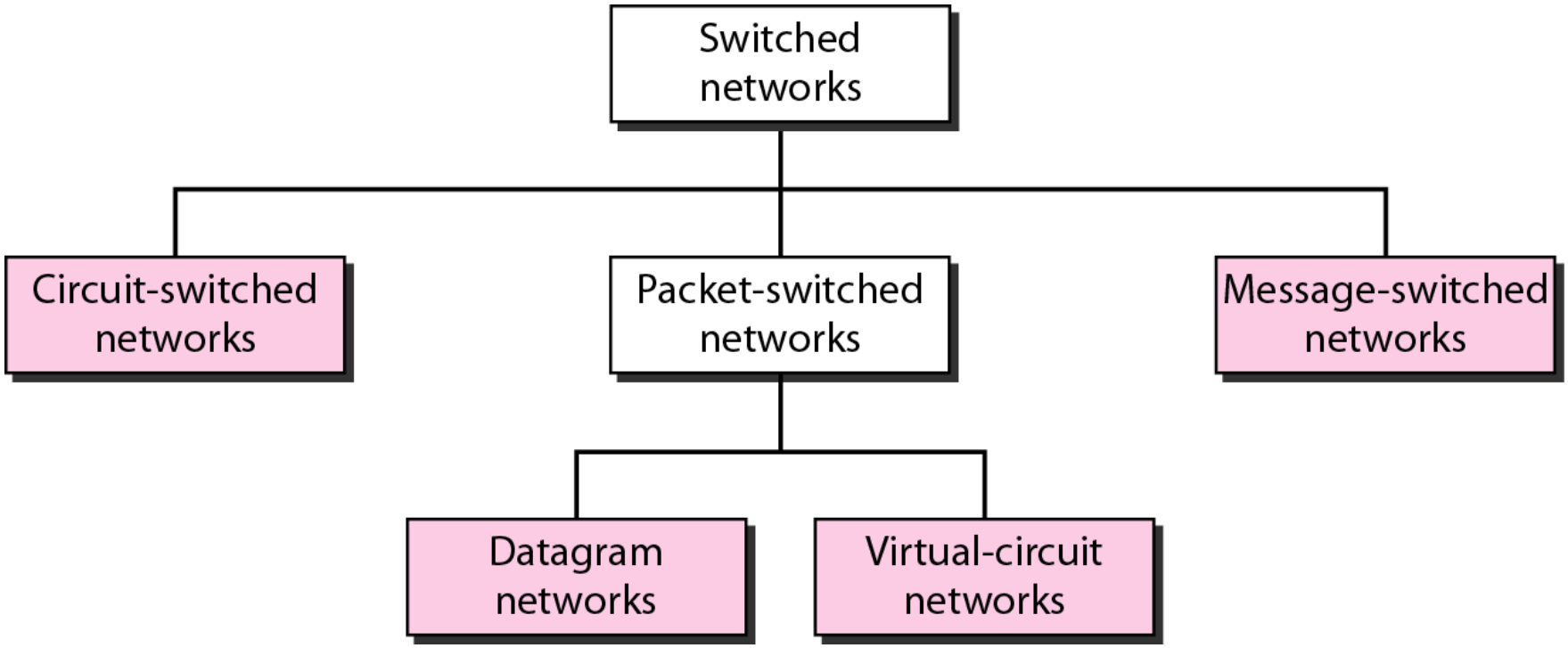
The network layer provides services to the transport layer at the network layer/transport layer interface.

1. The services should be independent of the router technology.

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

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

Figure: Taxonomy of switched networks



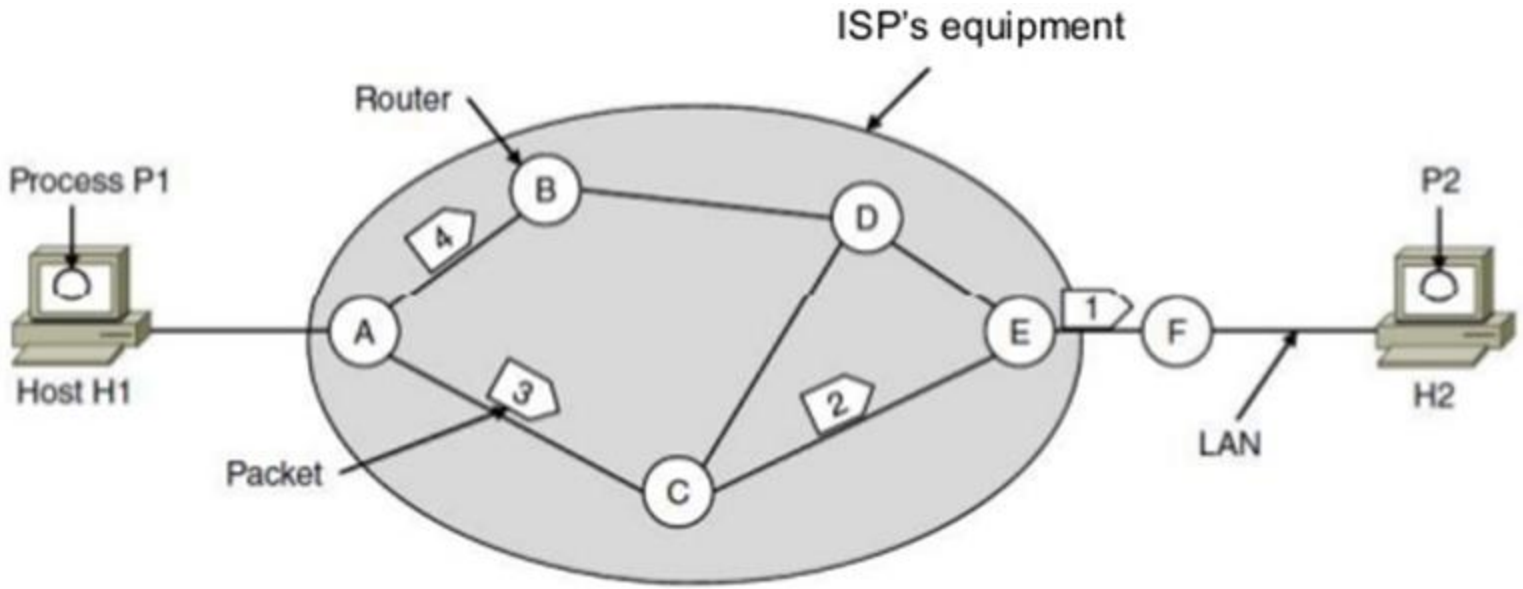
Connectionless service or Datagram Subnet

In this method packets are injected into the subnet individually and routed independently.

No advance setup is needed.

Packets are called as datagrams (in analogy with telegrams) and subnet is called as Datagram subnet.

Figure: Routing with a datagram network



A's table (initially)

Dest.	Line
A	⊠
B	B
C	C
D	B
E	C
F	C

A's table (later)

A	⊠
B	B
C	C
D	B
E	D
F	D

C's Table

A	A
B	A
C	⊠
D	E
E	E
F	E

E's Table

A	C
B	D
C	C
D	D
E	⊠
F	F

Cntd…

- Let us assume 4 packets (1,2,3,4) are sending from Host1 to Host2.
- First Host1 sends all packets to Router A using point to point protocol(PPP).
- Every router has routing table telling it where to send packets for each possible destination
- Each table has two columns

  1st column – destination router

  2nd column – outgoing line to reach destination router
- In the given example packets 1,2 and 3 used the path ACE to reach destination Host2.(by using routing tables A's table, C's table and E's table).
- Due to some reasons packet 4 used different path (ABDE) other than that of the first three.

The algorithm that manages the tables and makes routing decisions is called "*Routing Algorithm*"

Note

A switch in a datagram network uses a routing table that is based on the destination address.

Note

The destination address in the header of a packet in a datagram network remains the same during the entire journey of the packet.

Note

Switching in the Internet is done by using the datagram approach to packet switching at the network layer.

Connection Oriented Service or Virtual Circuit Subnet

In this method , path is established from source to destination before packets can be sent.

This connection is called VC (virtual circuit) and subnet is called virtual circuit subnet.

Each router has two tables 1st table represents incoming path and 2nd table represents outgoing path.

Figure: Virtual-circuit identifier

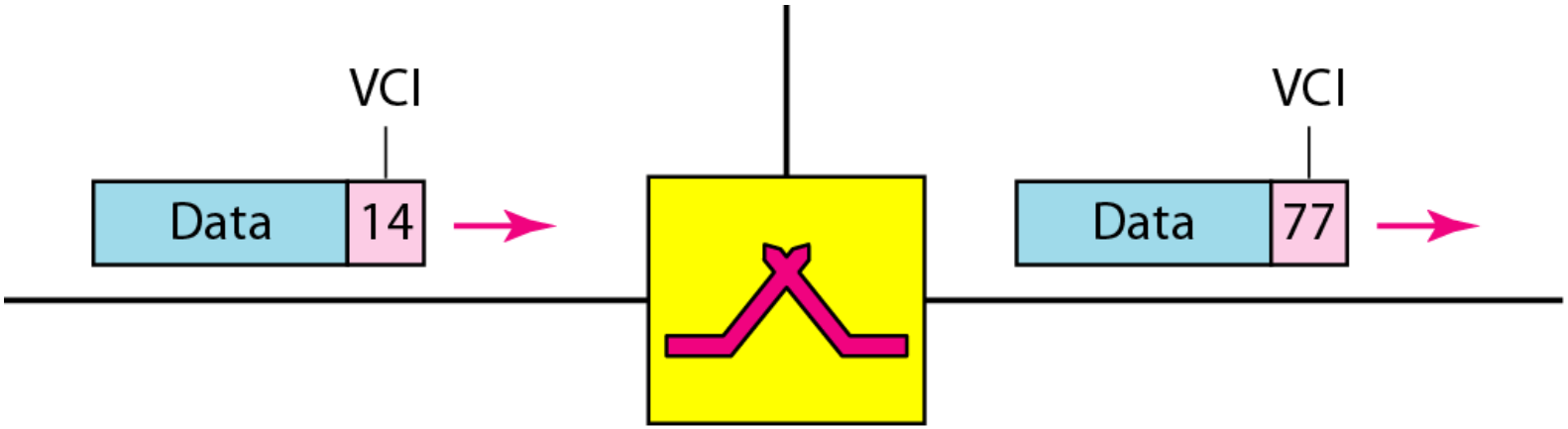


Figure: Switch and tables in a virtual-circuit network

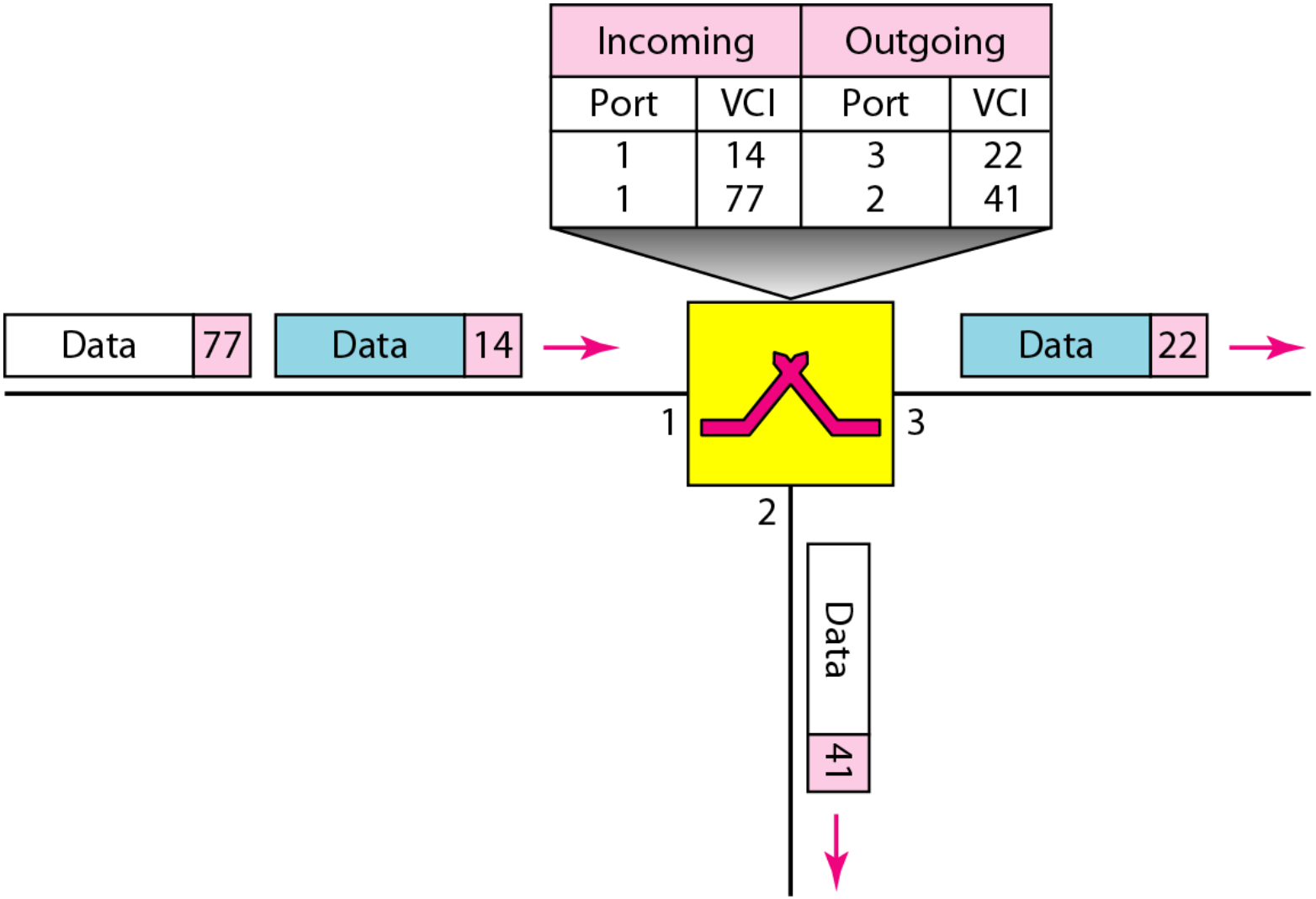
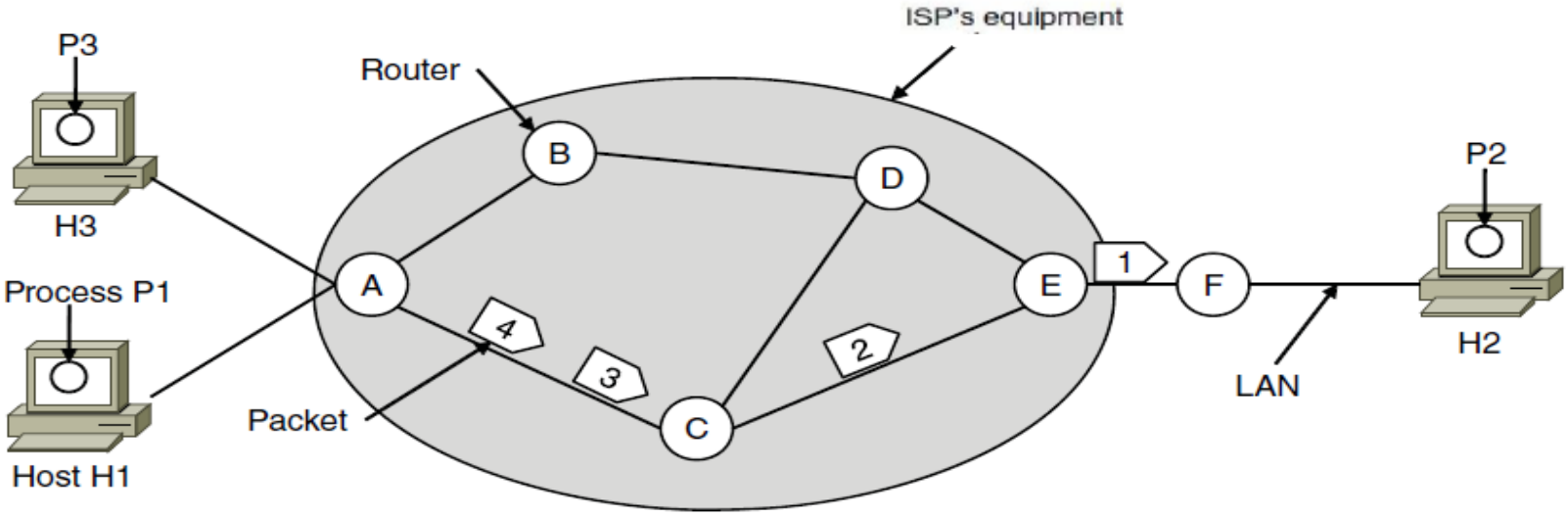


Figure: Routing with a virtual-circuit network



A's table

In		Out	
H1	1	C	1
H3	1	C	2

C's Table

A	1	E	1
A	2	E	2

E's Table

C	1	F	1
C	2	F	2

Cntd...

- host H1 has established connection 1 with host H2.
- The first line of A's table says that if a packet bearing connection identifier 1 comes in from H1, it is to be sent to router C and given connection identifier 1.
- Similarly, the first entry at C routes the packet to E, also with connection identifier 1.
- H3 also wants to establish a connection to H2, it chooses connection identifier 2.
- For avoiding confusion to router C , router A assigns a different connection identifier to the outgoing traffic for the second connection.
- Router has the ability to change the connection identifier in outgoing packets this method is called label switching.

Note

In virtual-circuit switching, all packets belonging to the same source and destination travel the same path; but the packets may arrive at the destination with different delays if resource allocation is on demand.

Note

Switching at the data link layer in a switched WAN is normally implemented by using virtual-circuit techniques.

Table: Comparison of datagram and virtual-circuit 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

Routing

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.

Routing algorithm:: that part of the Network Layer responsible for deciding on which output line to transmit an incoming packet.

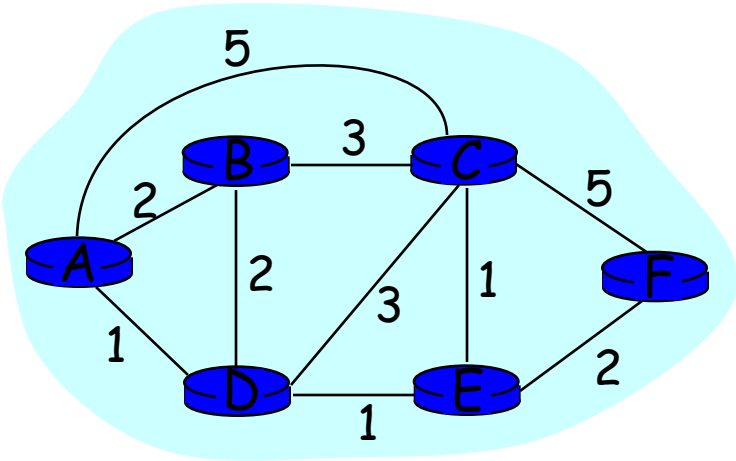
- Remember: For virtual circuit subnets the routing decision is made ONLY at set up.

Algorithm properties:: correctness, simplicity, robustness, stability, fairness, optimality, and scalability.

Cntd…

Routing protocol

Goal: determine "good" path (sequence of routers) thru network from source to dest.



Graph abstraction for routing algorithms:

- graph nodes are routers
- graph edges are physical links
  - link cost: delay, $ cost, or congestion level

- "good" path:
  - typically means minimum cost path
  - other definitions possible

Routing Classification

Global or decentralized information?

Global:

- all routers have complete topology, link cost info
- "link state" algorithms

Decentralized:

- router knows physically-connected neighbors, link costs to neighbors
- iterative process of computation, exchange of info with neighbors
- "distance vector" algorithms

Static or dynamic?

Static:

- routes change slowly over time (usually by humans)

Dynamic:

- routes change more quickly/automatically
  - periodic update
  - in response to link cost changes

Cntd…

Adaptive Routing (Dynamic)

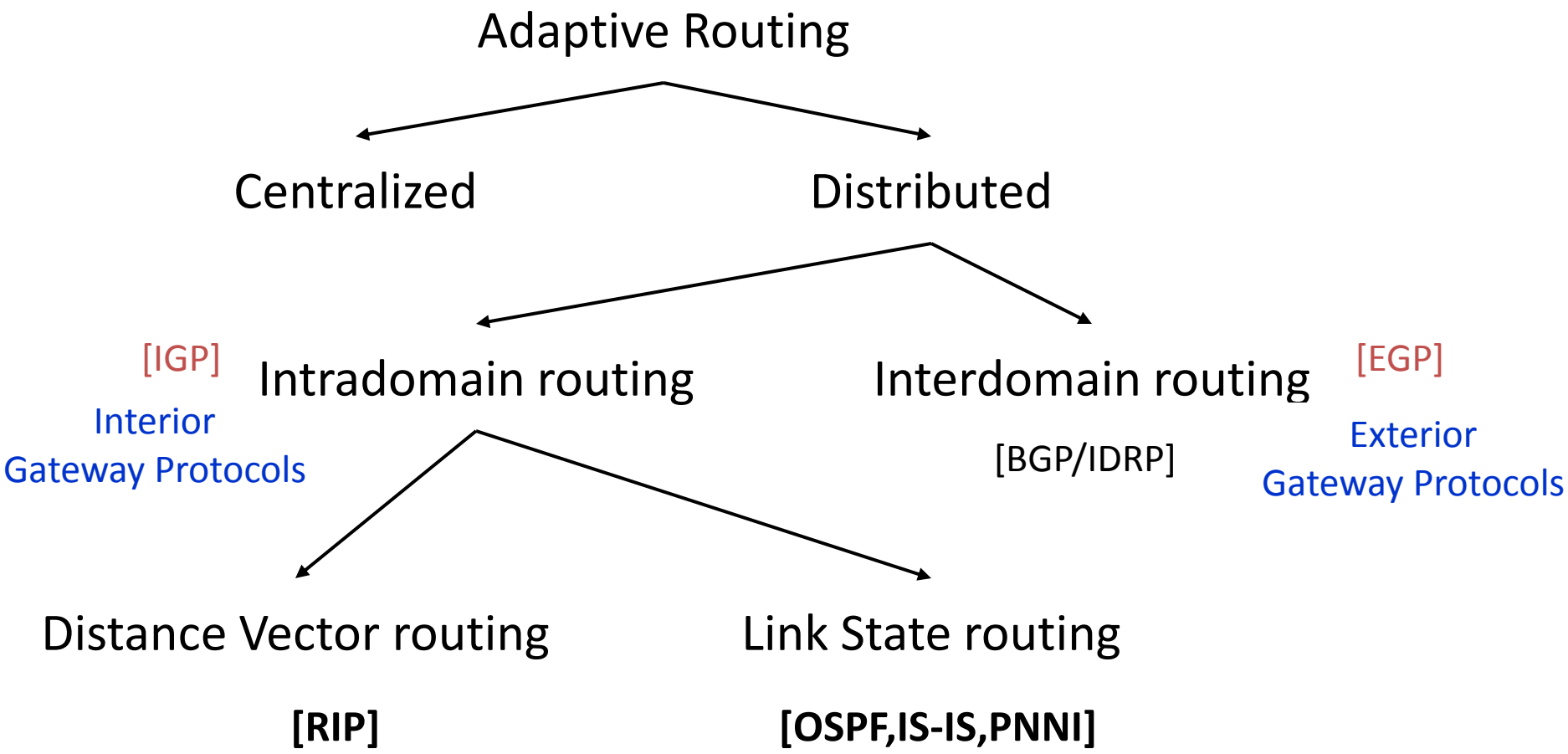
based on current measurements of traffic and/or topology.

1. centralized
2. isolated
3. distributed

Non-Adaptive Routing (Static)

1. flooding
2. static routing using shortest path algorithms

Adaptive Routing



S.No	Intradomain Routing	Interdomain Routing
1.	Routing algorithm works only within domains.	Routing algorithm works within and between domains.
2.	It need to know only about other routers within their domain.	It need to know only about other routers within and between their domain.
3.	Protocols used in intradomain routing are known as Interior-gateway protocols.	Protocols used in interdomain routing are known as Exterior-gateway protocols.
4.	In this Routing, routing takes place within an autonomous network.	In this Routing, routing takes place between the autonomous networks.
5.	Intradomain routing protocols ignores the internet outside the AS(autonomous system).	Interdomain routing protocol assumes that the internet contains the collection of interconnected AS(autonomous systems).
6.	Some Popular Protocols of this routing are RIP(resource information protocol) and OSPF(open shortest path first).	Popular Protocols of this routing is BGP(Border Gateway Protocol) used to connect two or more AS(autonomous system).

Routing Algorithms

Topics discussed in this section:

- Optimality principle
- Shortest path algorithm
- Flooding
- Hierarchal Routing
- Distance vector routing
- Multicast routing
- Broadcast routing

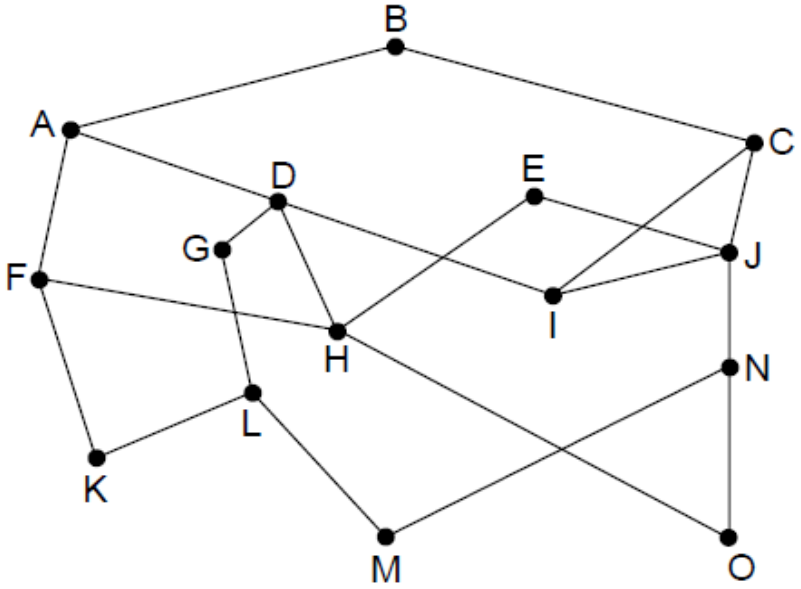
Static / Non-Adaptive Routing Algorithms

Dynamic / Adaptive Routing Algorithm

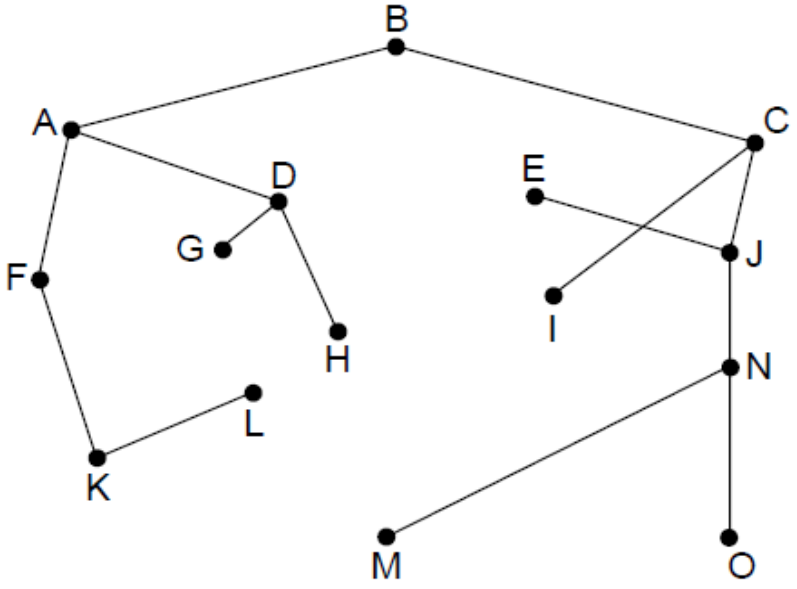
Optimality Principle

- The statement about optimal routes without regard to network topology or traffic is known as the optimality principle.
- It states that if router J is on the optimal path from router I to router K, then the optimal path from J to K also falls along the same route.
- The set of optimal routes from all sources to a given destination form a tree rooted at the destination.
- Such a tree is called a sink tree

Cntd...



(a)



(b)

(a) A network.

(b) A sink tree for router *B.*

Shortest Path Routing

What does it mean to be the shortest (or optimal) route?

a. Minimize mean packet delay

b. Maximize the network throughput

c. Minimize the number of hops along the path

- Shortest path routing is a form of routing which attempts to send packets of data over a network in such a way that the path taken from the sending computer to the recipient computer is minimized.

- The path can be measured in either physical distance or in the number of hops.

- This form of routing uses a non-adaptive routing algorithm.

Cntd…

Several algorithms for computing the shortest path between two nodes of a graph are known.

- Dijkstra's Algorithm [Link State]
- Bellman-Ford Algorithm [Distance Vector]

Dijkstra's algorithm

Initially mark all nodes (except source) with infinite distance.

working node = source node

Sink node = destination node

While the working node is not equal to the sink

1. Mark the working node as permanent.
2. Examine all adjacent nodes in turn

   If the sum of label on working node plus distance from working node to adjacent node is less than current labeled distance on the adjacent node, this implies a shorter path. Relabel the distance on the adjacent node and label it with the node from which the probe was made.
3. Examine all tentative nodes (not just adjacent nodes) and mark the node with the smallest labeled value as permanent. This node becomes the new working node.

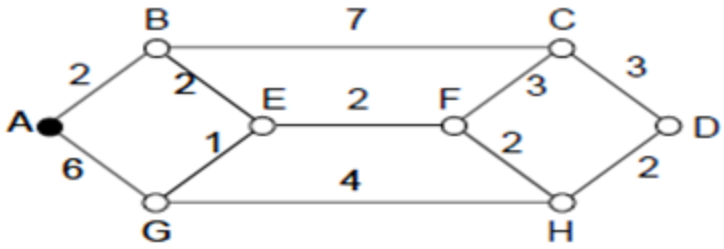
Reconstruct the path backwards from sink to source.

Cntd...

- Notation:

  c(i, j): link cost from node i to j.

  cost infinite if not direct neighbors

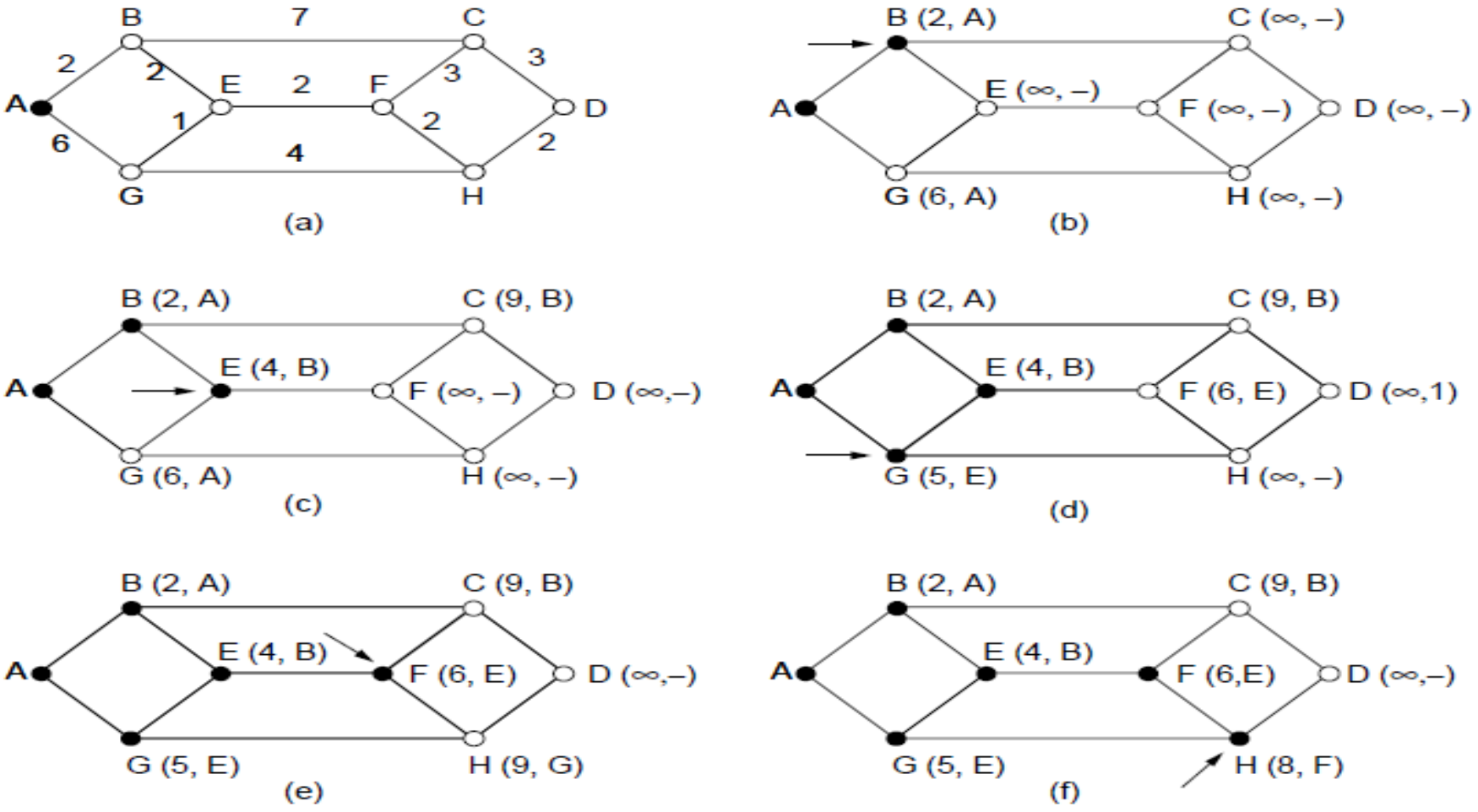


- Example : We want to find the shortest path from A to D.

- Distance from A to E through router B is 2+2=4; distance from A to E through router G is 6+1=7. Among these two distances ABE is shortest distance so that path is selected and marked as visited path.

- In this way shortest path is selected from A to D.

Cntd...



The first five steps used in computing the shortest path from A to D.

The arrows indicate the working node

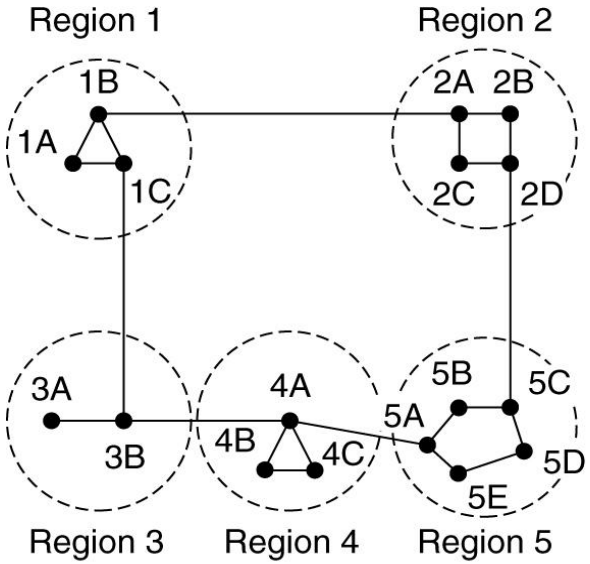
Flooding

- Flooding is a static algorithm in which every incoming packet is sent out on every outgoing line except the one it arrived on.
- Flooding generates duplicate packets at the destination system.
- For avoiding flooding sequence no is assigned to each packet at the source router.
- Flooding is highly robust, and could be used to send emergency messages (e.g., military applications).

Selective Flooding

- In this algorithm the routers do not send every incoming packet out on every line, only on those lines that are going approximately in the right direction.
- The selective flooding controls the amount of traffic in the network.
- Flooding always chooses the shortest path

Hierarchical Routing



(a)

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)

Cntd…

- When network size increases
  - Larger tables
  - More CPU time needed to compute …
  - More bandwidth needed

- Routers grouped in regions
- Each routers knows how to reach:
  - Other routers in its own group
  - Other regions

- The full routing table for router 1A has 17 entries.
- Hierarchical routing has reduced the table from 17 to 7 entries.

Distance Vector Routing

- Distance Vector Routing is one of the dynamic routing algorithm.
- It is suitable for packet switched network.
- Historically known as the old ARPANET routing algorithm {or known as ***Bellman-Ford algorithm***}.

Basic idea: each network node maintains a Distance Vector table containing the distance between itself and ALL possible destination nodes.

- Distances are based on a chosen metric and are computed using information from the neighbors' distance vectors.

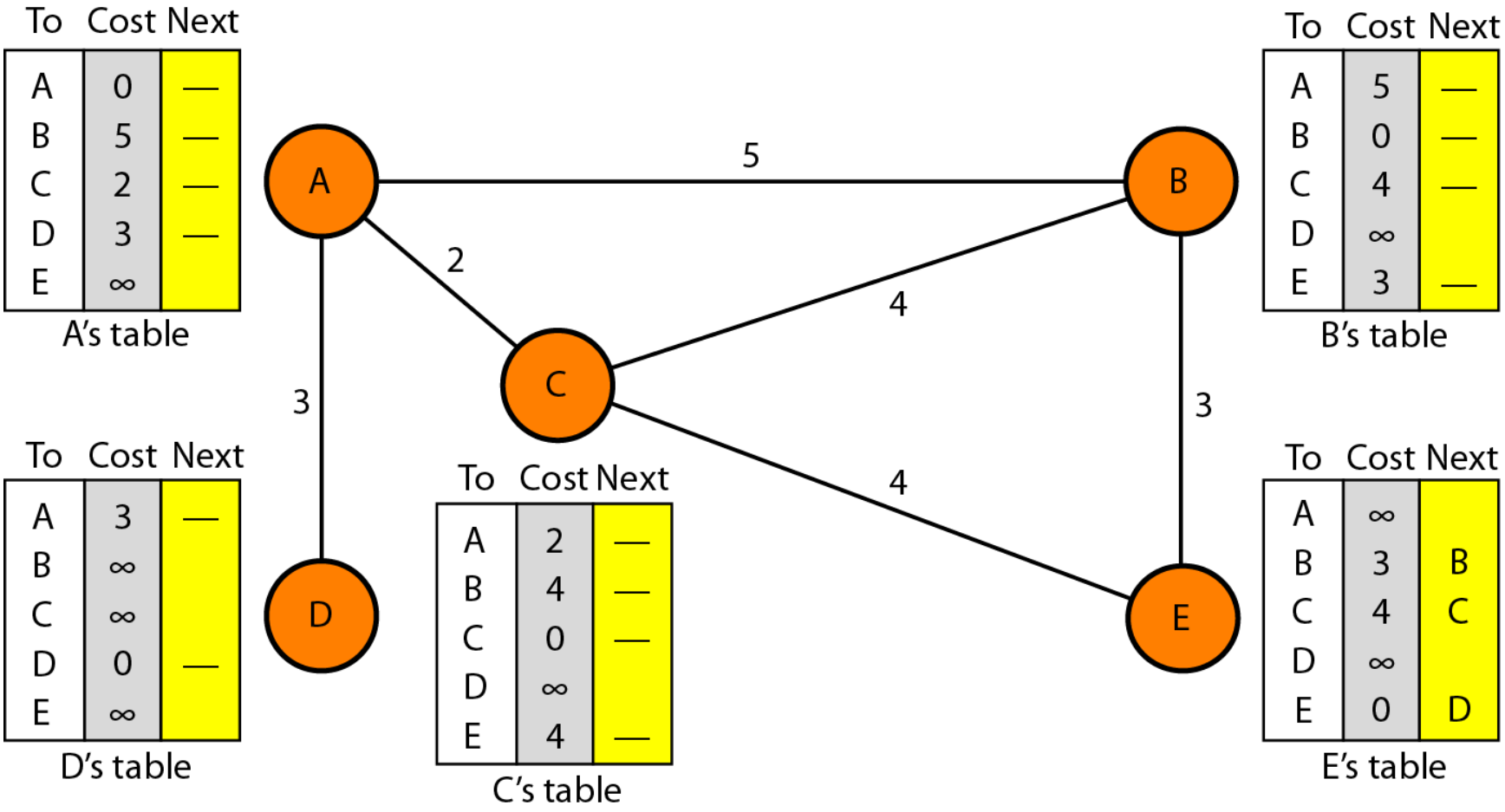
Metric: usually hops or delay

Distance Vector Algorithm

1. Router transmits its distance vector to each of its neighbors.
2. Each router receives and saves the most recently received distance vector from each of its neighbors.
3. A router recalculates its distance vector when:
   a. It receives a distance vector from a neighbor containing different information than before.
   b. It discovers that a link to a neighbor has gone down (i.e., a topology change).

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

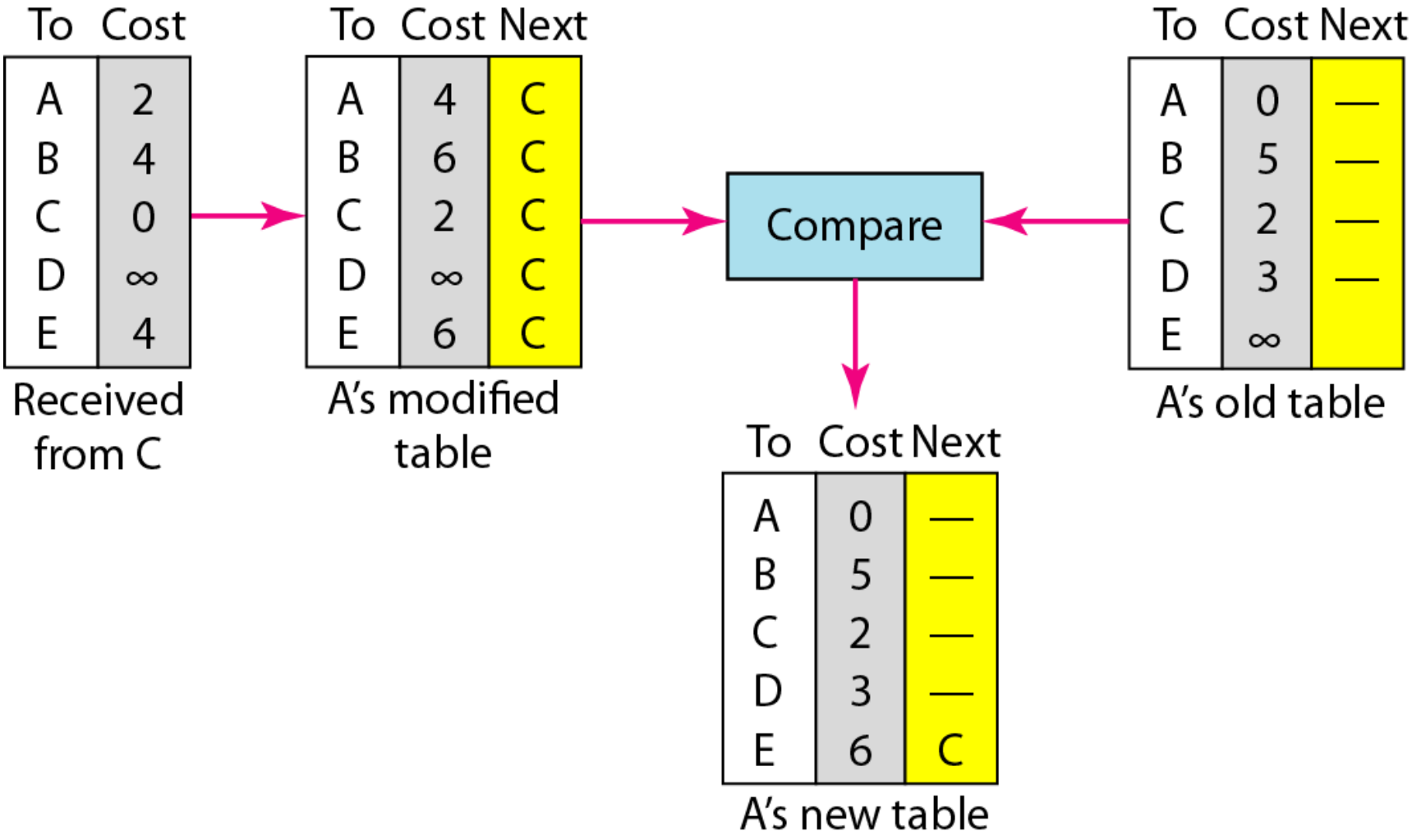
Figure: Initialization of tables in distance vector routing



Note

In distance vector routing, each node shares its routing table with its immediate neighbors periodically and when there is a change.

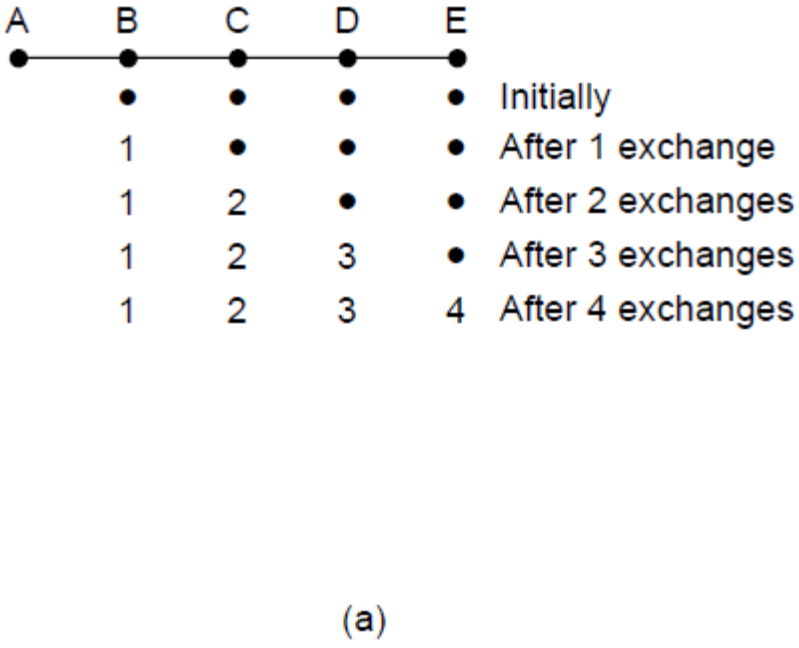
Figure: Updating in distance vector routing



Count to Infinity Problem

- One of the important issue in Distance Vector Routing is County of Infinity Problem.
- Counting to infinity is just another name for a routing loop.
- In distance vector routing, routing loops usually occur when an interface goes down.
- It can also occur when two routers send updates to each other at the same time.
- Consider the example, link between A and B is broken.

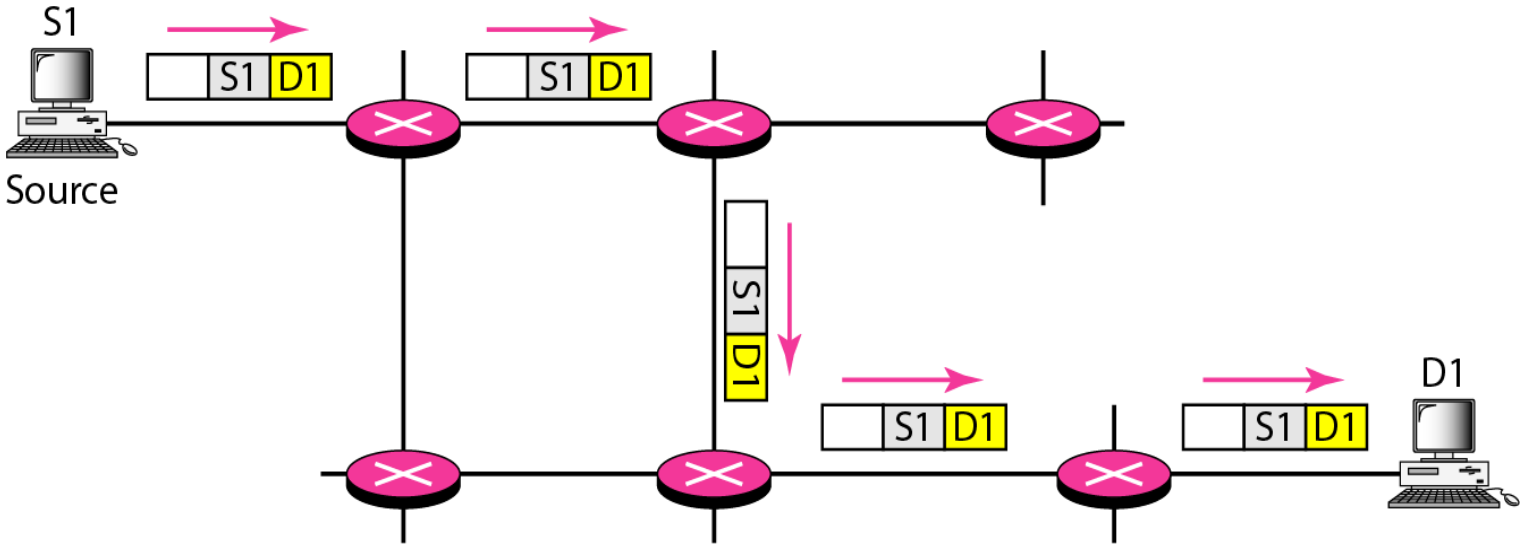
Cntd...


A B C D E
Initially
After 1 exchange
After 2 exchanges
After 3 exchanges
After 4 exchanges
(a)
A B C D E
Initially
After 1 exchange
After 2 exchanges
After 3 exchanges
After 4 exchanges
After 5 exchanges
After 6 exchanges
(b)

Unicast Routing

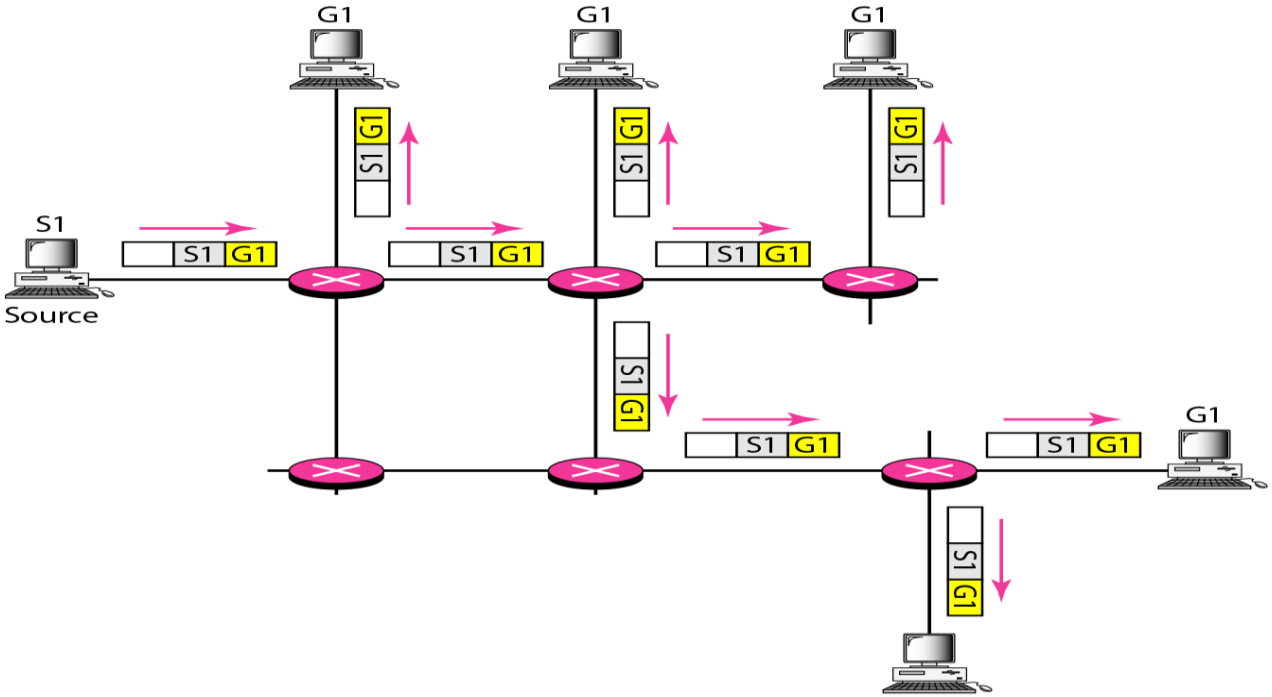
- There is one source and on destination. The relation between source and destination is one to one.

- In unicasting the router forwards the received packet through only one of its interfaces.

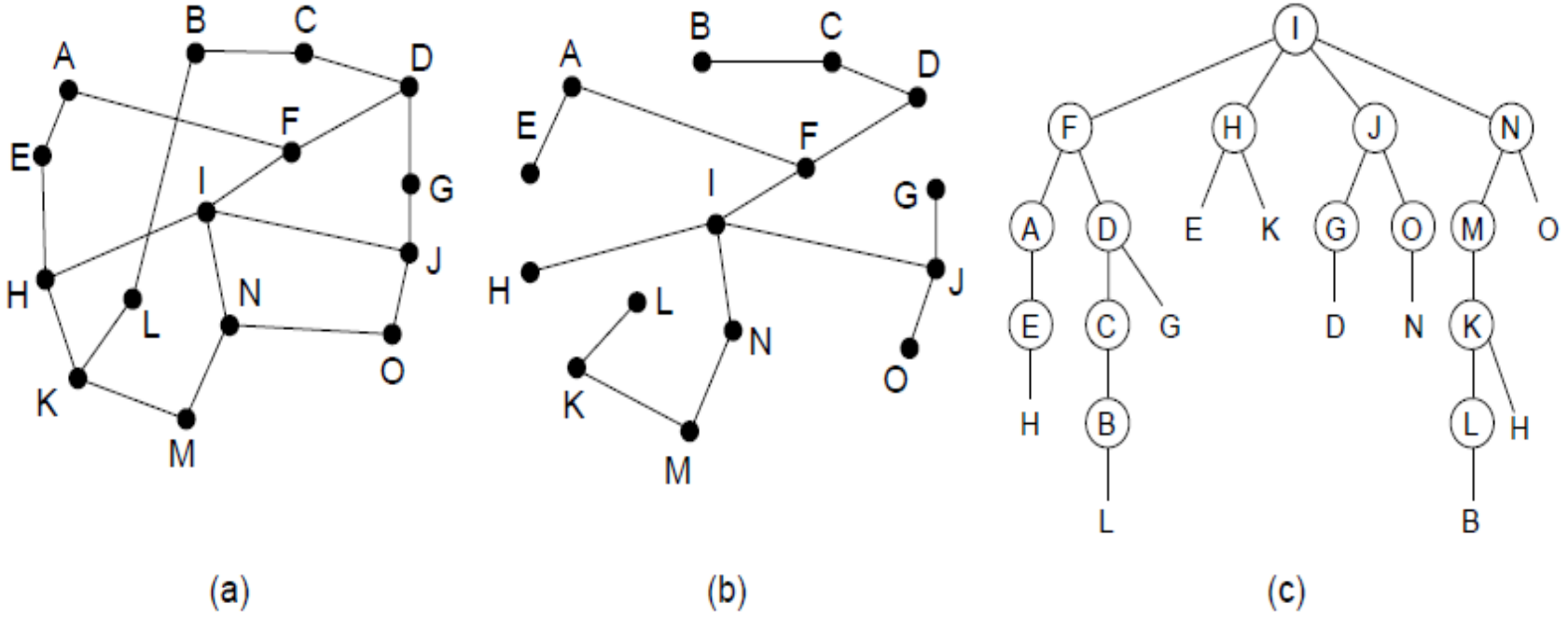


Multicast Routing

- One source and group of destinations
- The relationship is one to many.
- The router may forward the received packet through several of its interfaces.



Broadcast Routing



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

Cntd…

- The relationship between the source and destination is one to all.
- A spanning tree is a subset of the subnet that includes all the routers but contains no loops.
- Broadcast algorithm is an attempt to approximate the behavior of the previous one, even when the routers do not know anything at all about spanning trees.
- The idea is called reverse path forwarding.

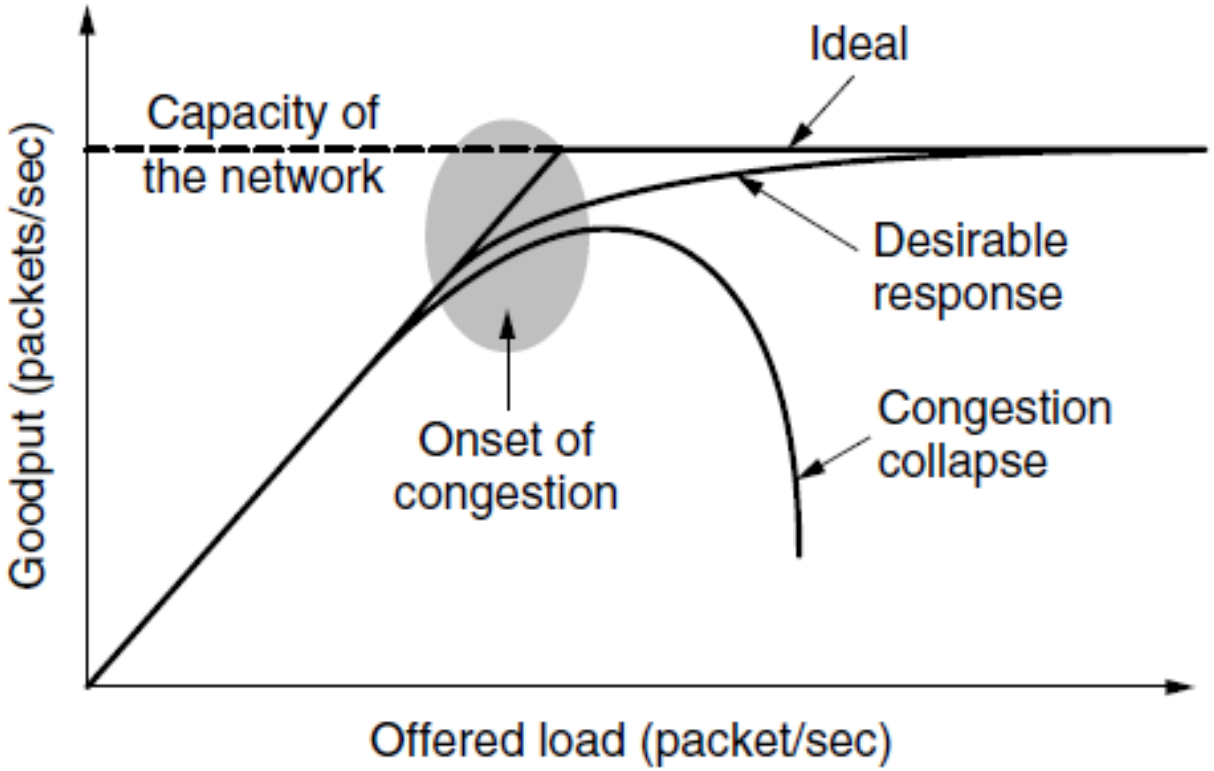
Congestion

Congestion in a network may occur if the load on the network—the number of packets sent to the network—is greater than the capacity of the network—the number of packets a network can handle.

Too many packets present in (a part of) the network causes packet delay and loss that degrades performance. This situation is called **congestion**.

Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

Cntd…



When too much traffic is offered, congestion sets in and performance degrades sharply.

Figure: Queues in a router

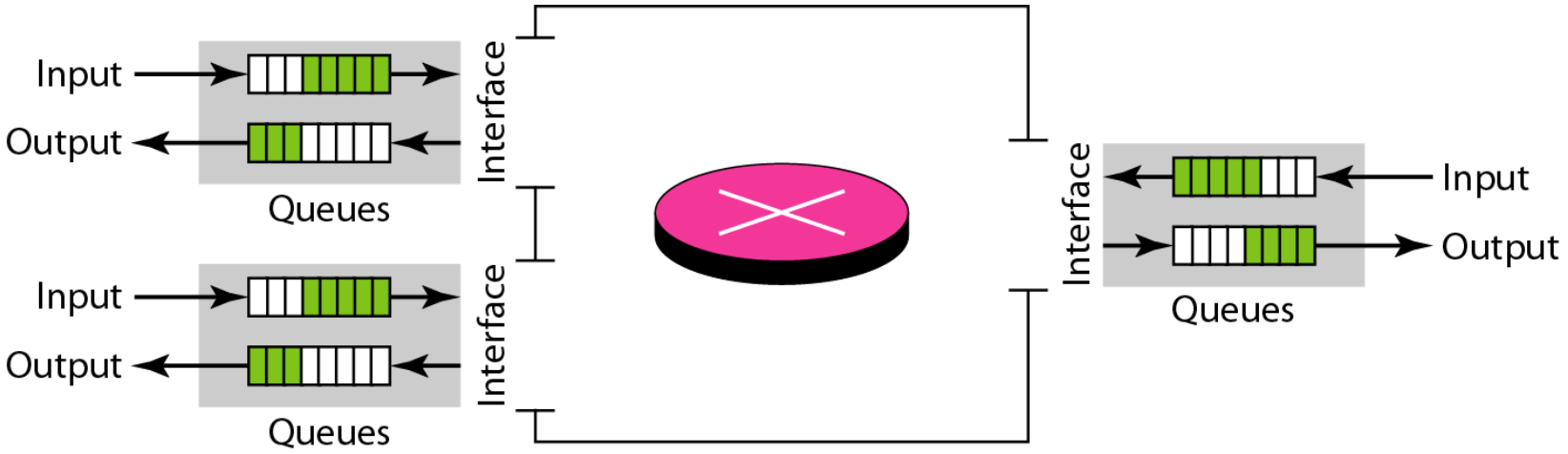
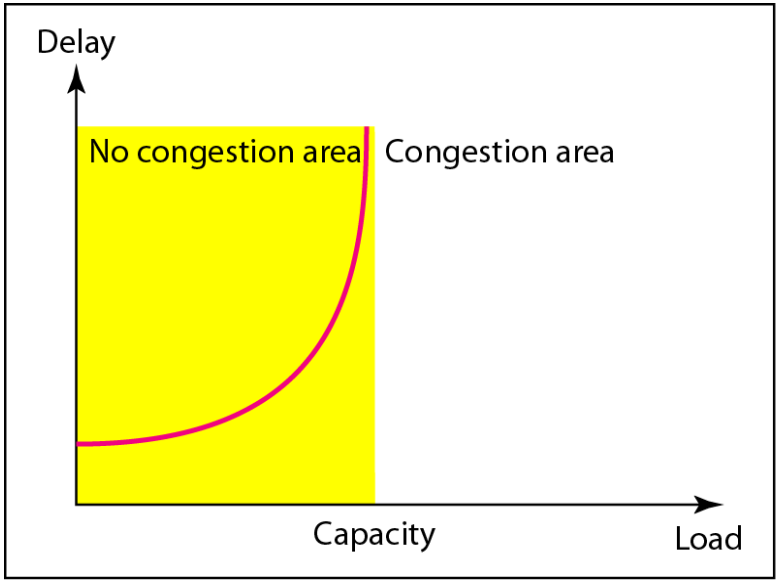
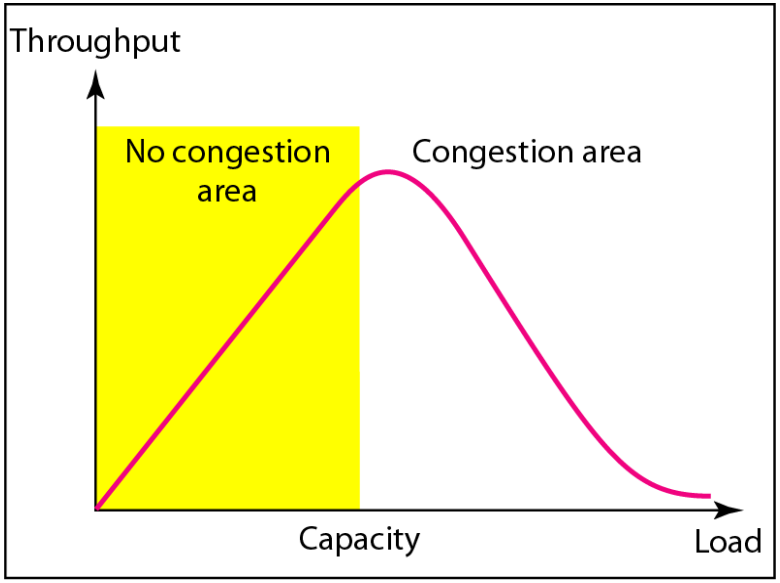


Figure: Packet delay and throughput as functions of load



a. Delay as a function of load



b. Throughput as a function of load

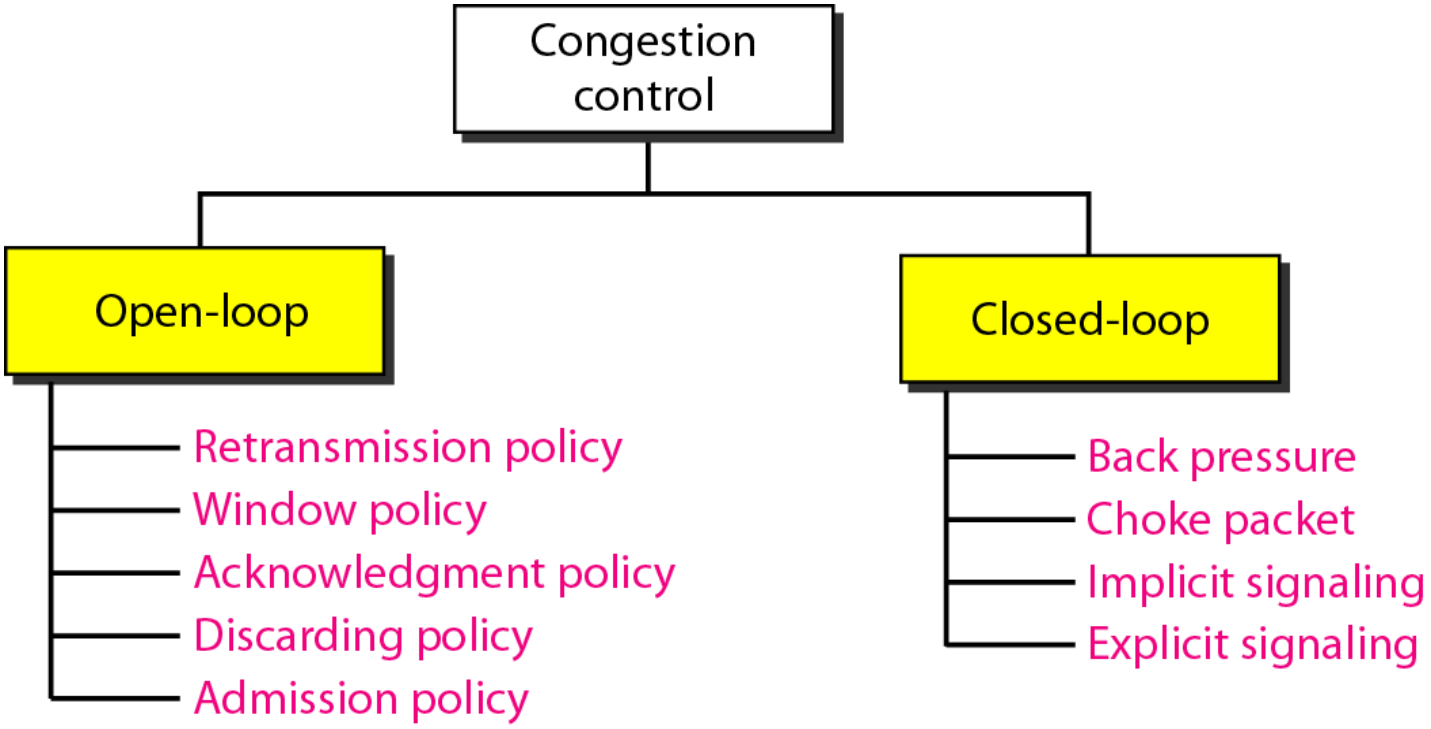
Congestion Control

Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened.

In general, we can divide congestion control mechanisms into two broad categories:

- open-loop congestion control (prevention) and
- closed-loop congestion control (removal)

Figure: Congestion control categories



Congestion Control Algorithms

Topics discussed in this section:

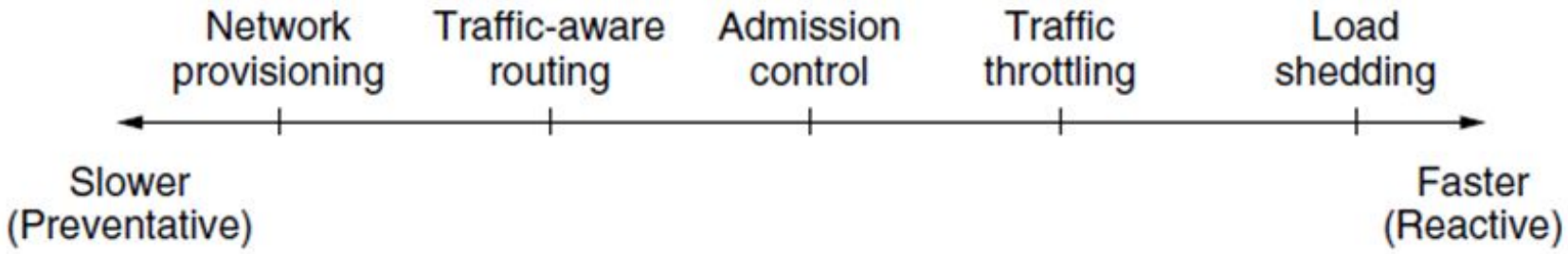
- Approaches to Congestion Control
- Traffic Aware Routing
- Admission Control
- Traffic Throttling
- Load Shedding

Approaches to Congestion Control

Two solutions possible:

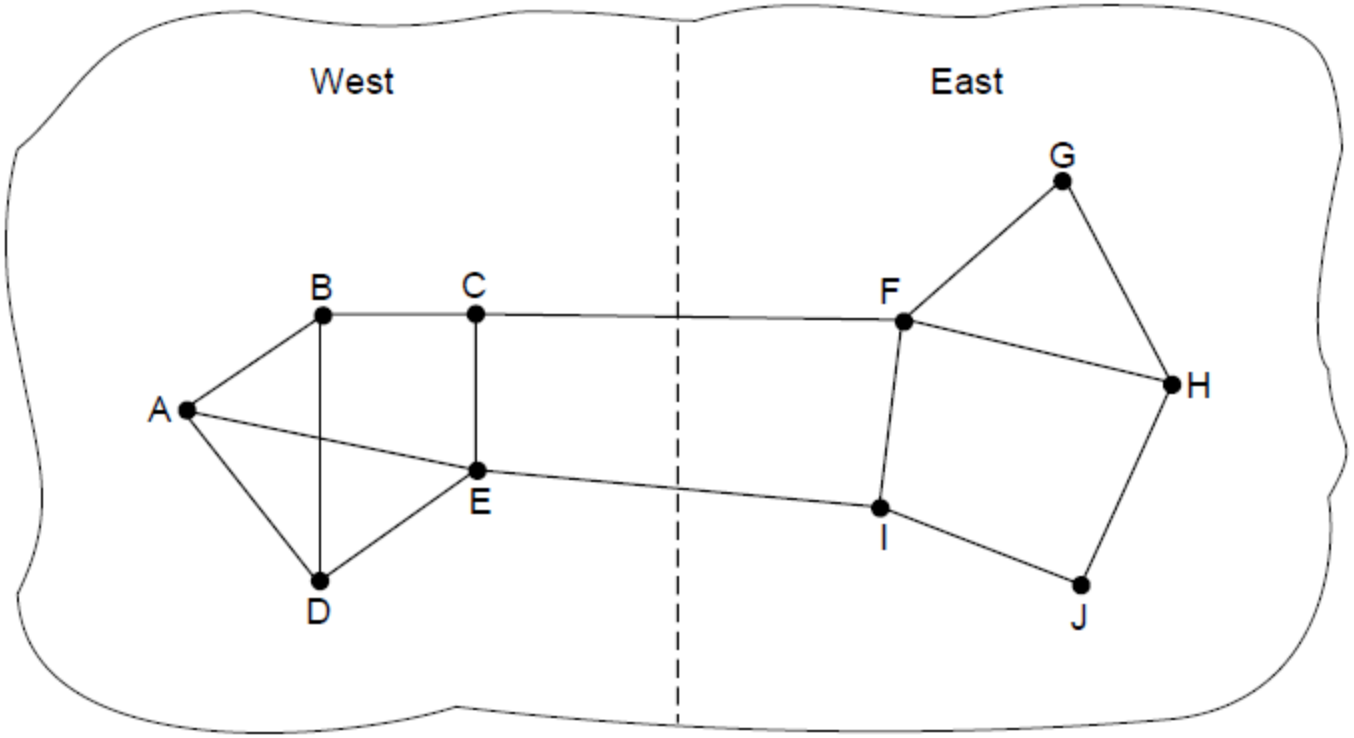
1)Increase resources

2)Decrease load



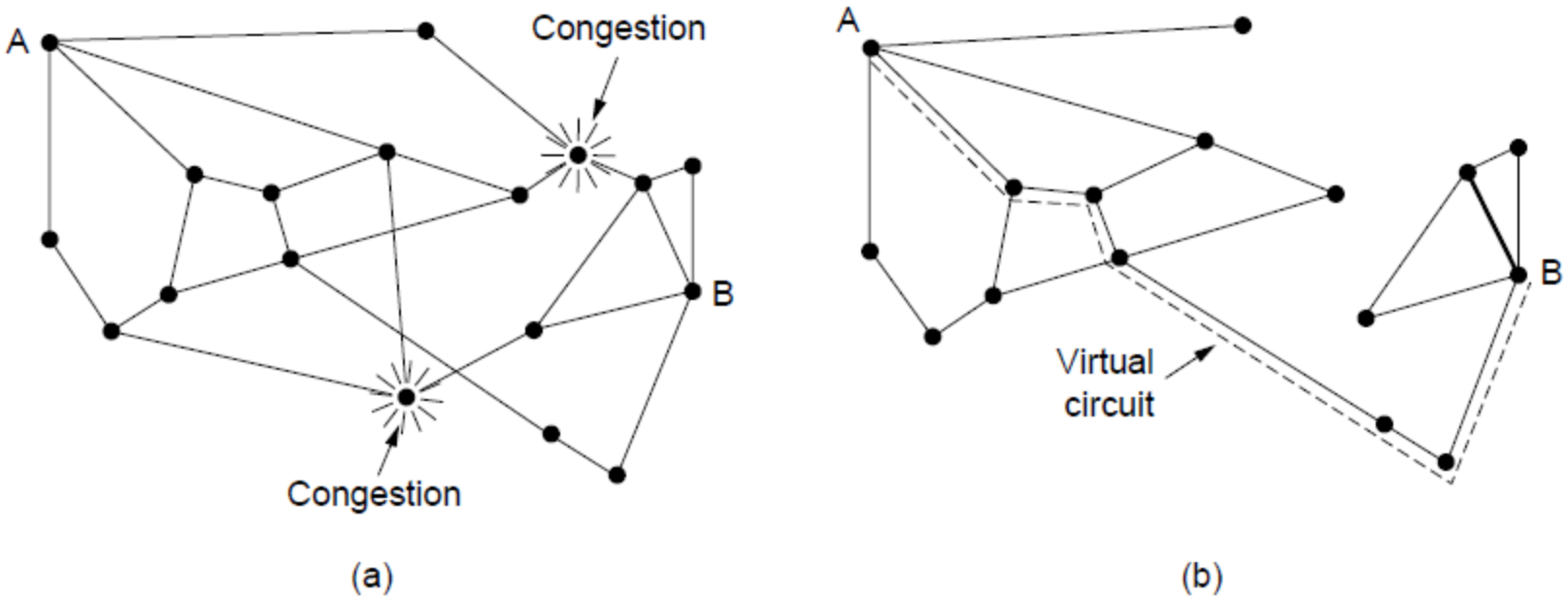
Timescales of approaches to congestion control.

Traffic-Aware Routing



A network in which the East and West parts are connected by two links.

Admission Control



(a)A congested network. (b) The portion of the network that is not congested. A virtual circuit from A to B is also shown.

Problem is in virtual circuits – there may be provisioning but not real usage.

Traffic Throttling: Congestion Detection

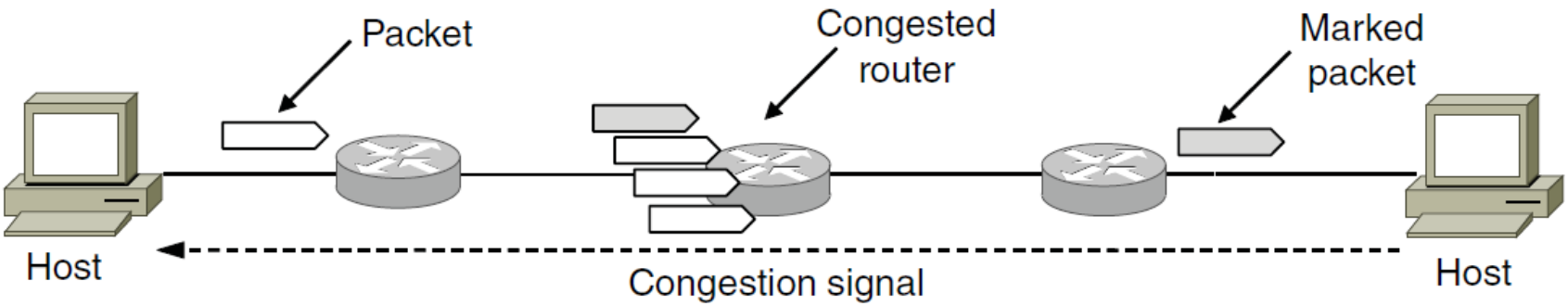
- Routers must determine when congestion is approaching, ideally before it has arrived.
- Each router can continuously monitor the resources it is using.
- 3 possibilities:
  1. utilization of the output links
  2. buffering of queued packets inside the router (most useful)
  3. no. of packets that are lost due to insufficient buffering

Traffic Throttling: Feedback

- Routers must deliver timely feedback to the senders that are causing the congestion.
- The router must identify the appropriate senders.
- It must then warn them carefully, without sending many more packets into the already congested network.

- Many feedback mechanisms:

Mechanism 1: Explicit Congestion Notification (ECN)



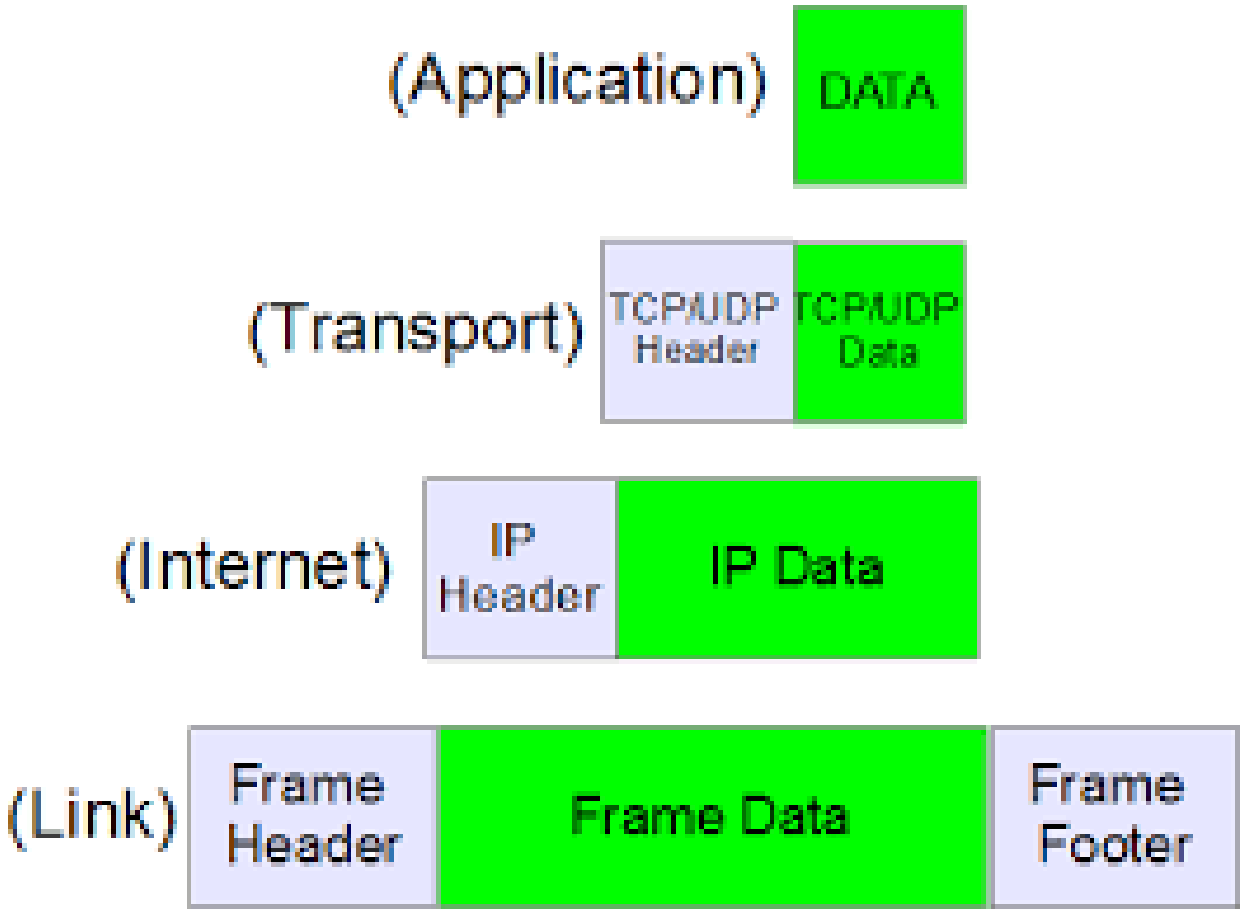
Load Shedding

- Performed when all other strategies fail.
- Cause blackout in some areas to save the entire network from failing.
- Intelligent packet drop policy desired.
- Which packets to discard may depend on application

  Multimedia – old packets (full frame not to be discarded)

  Text – Recent Packets
- Packet's importance can be marked in the beginning (application layer), then decision on which packets to discard can be taken.

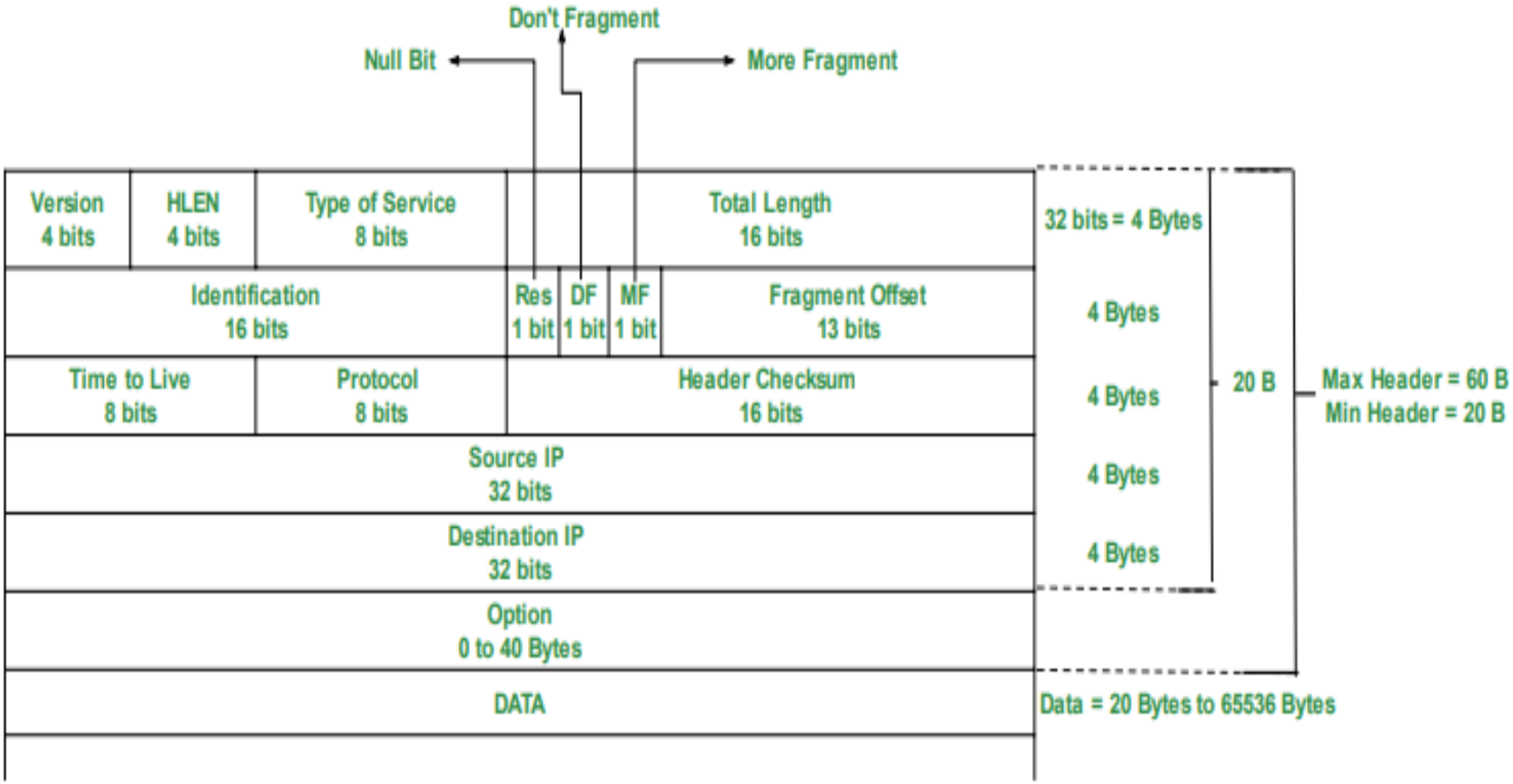
IP Header


(Application)
DATA
(Transport)
TCP/UDP Header
TCP/UDP Data
(Internet)
IP Header
IP Data
(Link)
Frame Header
Frame Data
Frame Footer

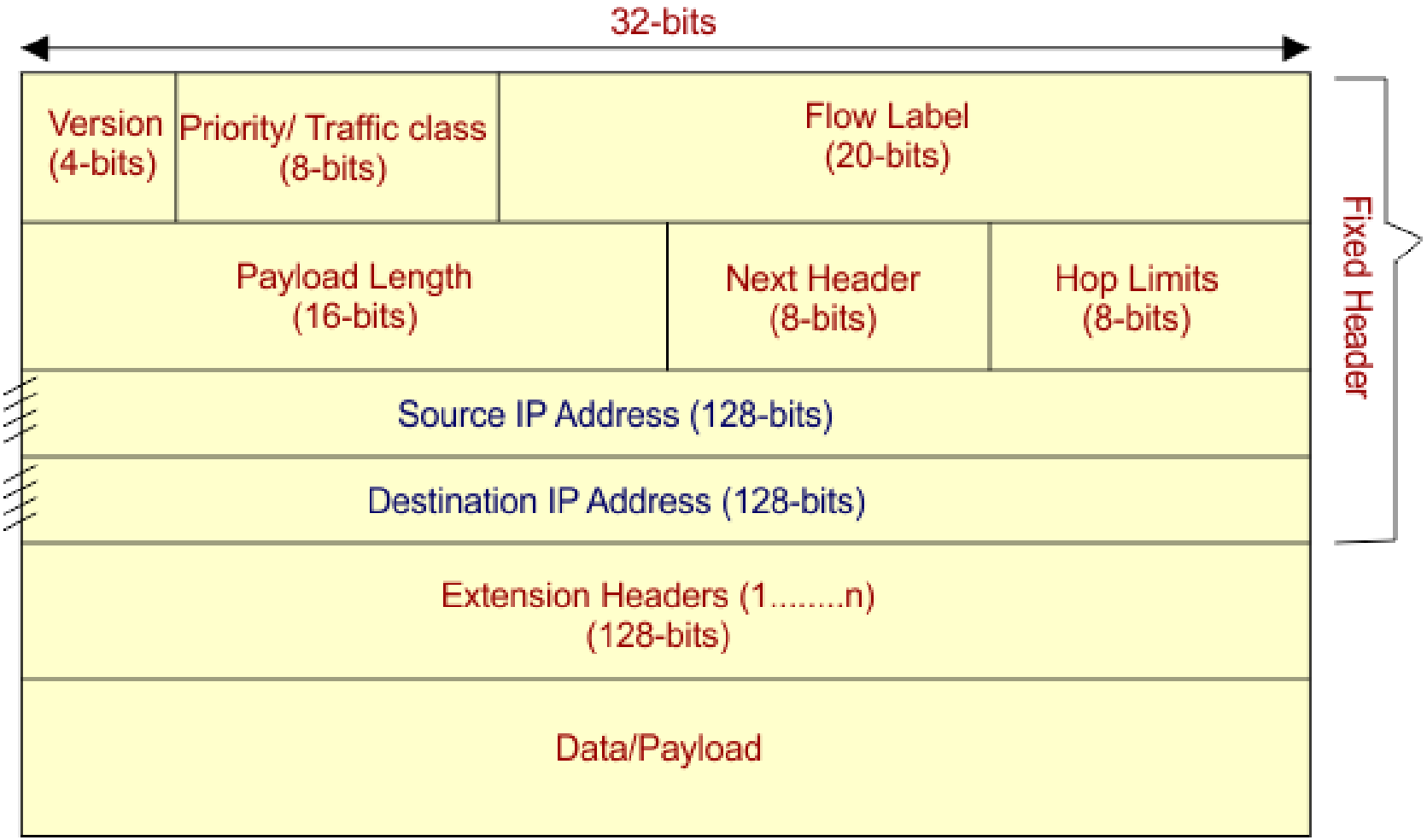
IP ADDRESS

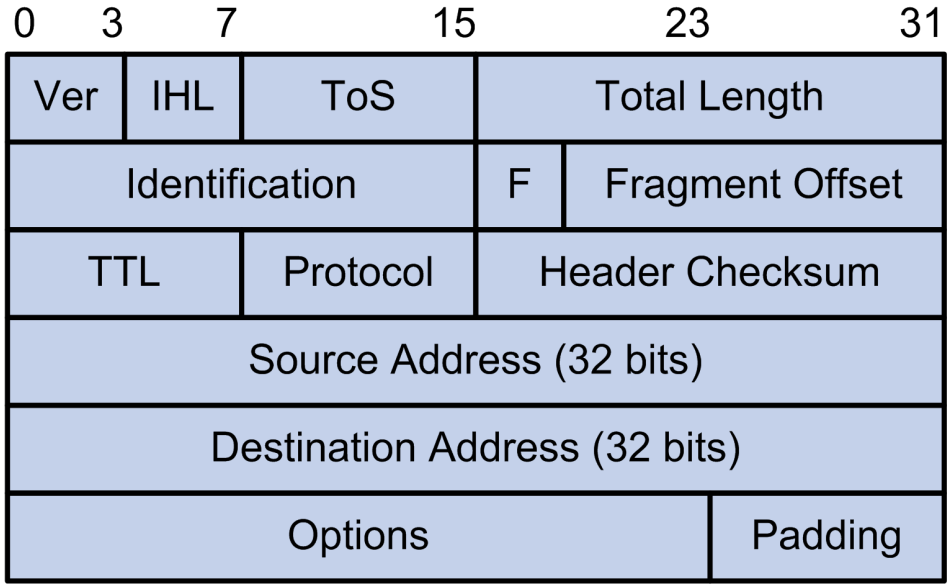
	Internet Protocol version 4 (IPv4)	Internet Protocol version 6 (IPv6)
Deployed	1981	1999
Address Size	32-bit number	128-bit number
Address Format	Dotted Decimal Notation: 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00: 0123:4567:8901:ABCD
Prefix Notation	192.149.0.0/24	3FFE:F200:0234::/48
Number of Addresses	2^{32} = ~4,294,967,296	2^{128} = ~340,282,366, 920,938,463,463,374, 607,431,768,211,456

IPv4

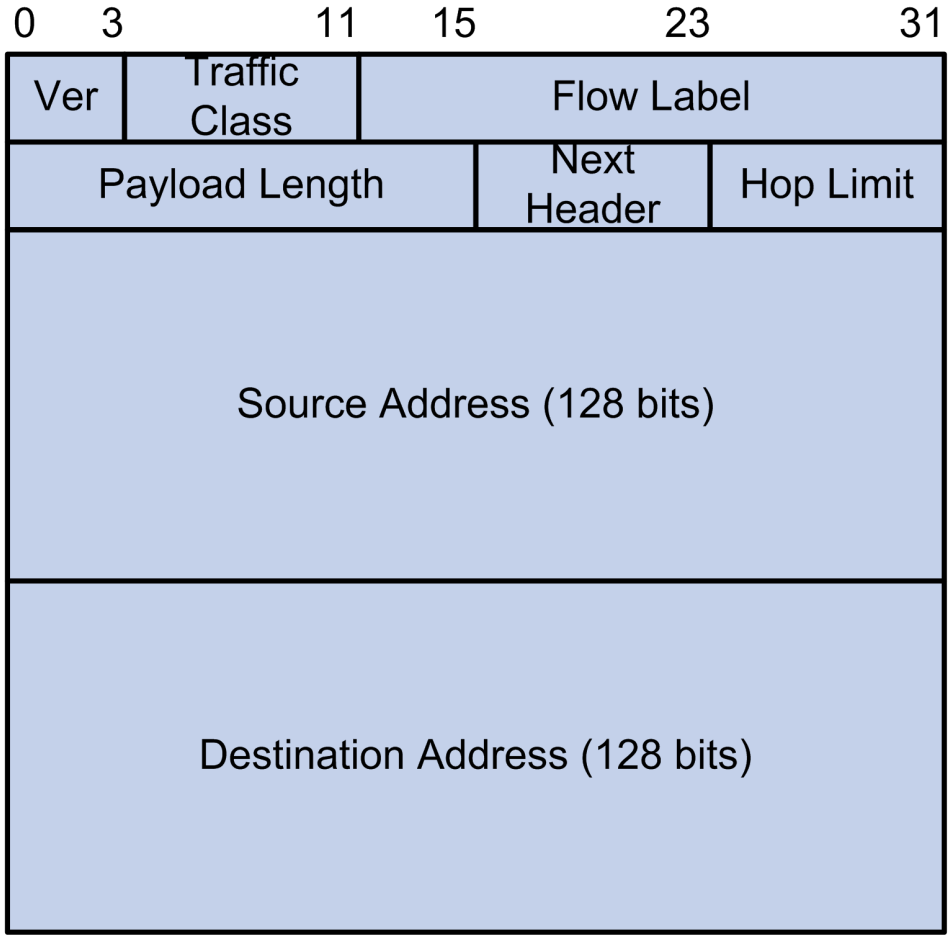

Don't Fragment
Null Bit
More Fragment
Version
4 bits
HLEN
4 bits
Type of Service
8 bits
Total Length
16 bits
32 bits = 4 Bytes
Identification
16 bits
Res
1 bit
DF
1 bit
MF
1 bit
Fragment Offset
13 bits
4 Bytes
Time to Live
8 bits
Protocol
8 bits
Header Checksum
16 bits
4 Bytes
20 B
Max Header = 60 B
Min Header = 20 B
Source IP
32 bits
4 Bytes
Destination IP
32 bits
4 Bytes
Option
0 to 40 Bytes
DATA
Data = 20 Bytes to 65536 Bytes

IPv6


32-bits
Version (4-bits)
Priority/ Traffic class (8-bits)
Flow Label (20-bits)
Payload Length (16-bits)
Next Header (8-bits)
Hop Limits (8-bits)
Source IP Address (128-bits)
Destination IP Address (128-bits)
Extension Headers (1.....n) (128-bits)
Data/Payload
Fixed Header



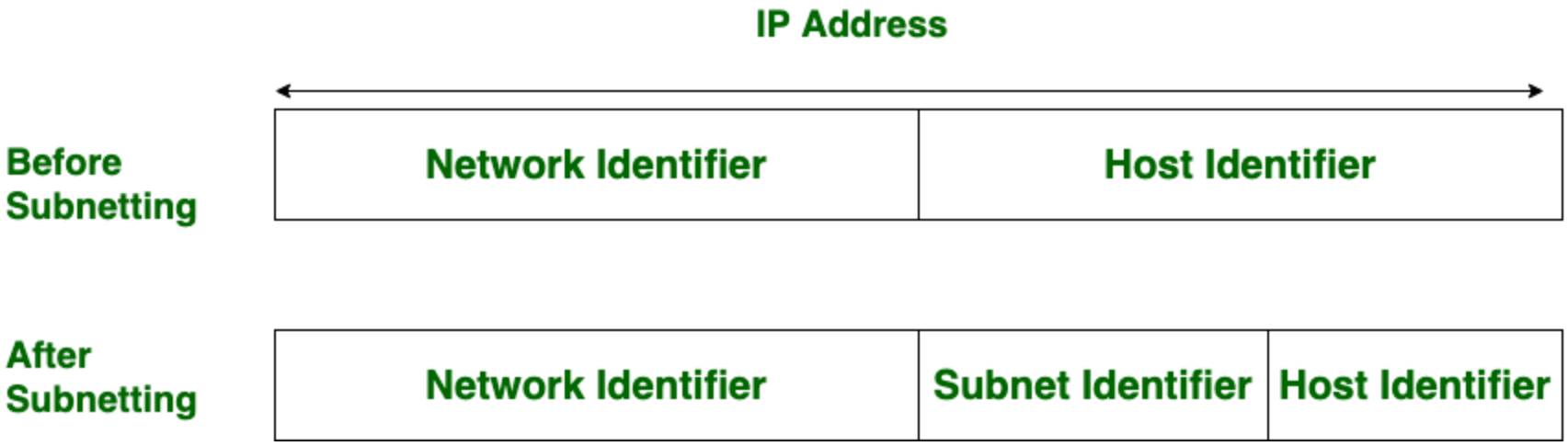
IPv4 header



Basic IPv6 header

SUBNETTING

- The procedure to divide the network into sub-networks or small networks, these smaller networks are known as subnets.



SUPERNETTING

- The procedure to combine small networks into larger spaces.

- In subnetting, Network addresses' bits are increased. on the other hand, in supernetting, Host addresses' bits are increased.