

Computer Networks Protocols

Lecture No.1: Introduction

Network Architecture

A *set of layers and protocols* is called the network architecture.

Protocol Hierarchies

- Networks are organized as layers to **reduce design complexity**.
- Each layer offers services to the higher layers. Between adjacent layers is an interface.

<i>Services</i>	<i>Interface</i>	<i>Primitives</i>
connection oriented and connectionless.	defines which primitives and services the lower layer will offer to the upper layer.	operations such as request, indicate, response, confirm.

Design Issues for the Layers(functions)

1. Mechanism for **connection establishment**
2. Rules for **data transfer**
3. **Error** control
4. Fast sender **swamping** a slow receiver
5. **Routing** in the case of multiple paths

Network Protocols

- **Protocol**: is a format order of messages sent and received among the net entities and action taken on msgs transmission receipt.
- **Protocol process** :
 1. The **format** or structure of the message
 2. The **process** by which networking devices share information about **pathways** with other networks
 3. How and when **error and system messages** are passed between devices
 4. The **setup and termination** of data transfer sessions

Layering In Networked Computing

- OSI Model (open system interconnection)
- TCP/IP Model

Why a layered model?

1. **Breaks down** communication into smaller, simpler parts.
2. **Easier to teach** communication process.
3. **Allows** different hardware and software to work together.
4. **Reduces** complexity

The OSI model

The Open Systems Interconnection is the model developed by the International Standards Organization.

- helps us understand *how data gets from one user's* computer to another.

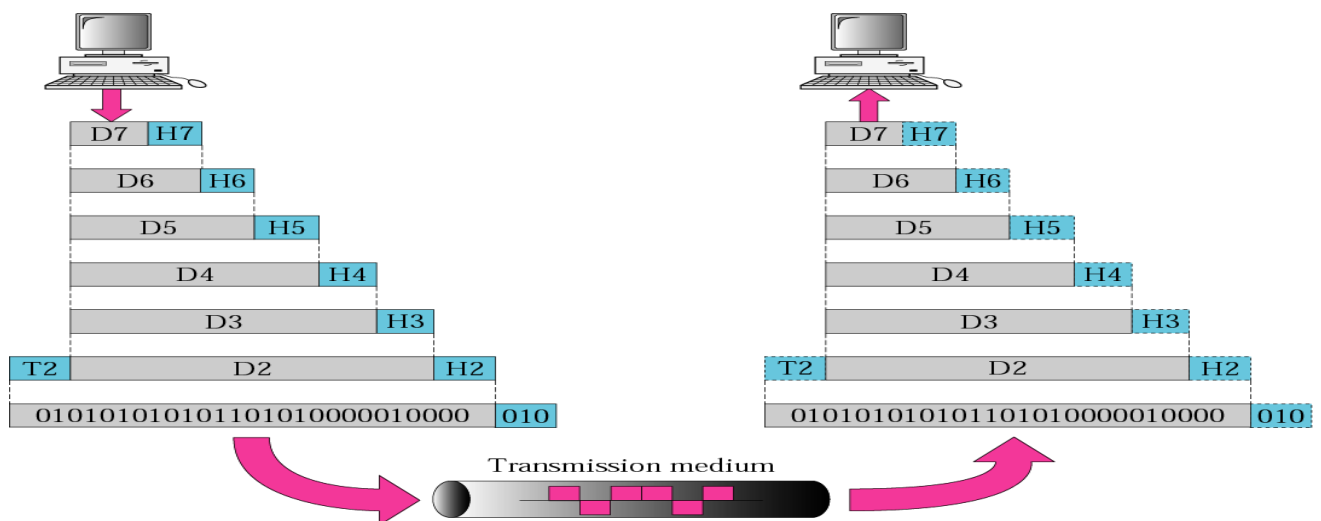
-It aids to *provide an organized structure for hardware and software developers to follow.*

Why use a reference model?

- **Serves** as an outline of rules for **how protocols can be used to allow communication between computers.**
- Each layer has its **own function and provides support to other layers.**

OSI model

Layer	Name	Example protocols
7	Application Layer	HTTP, FTP, DNS, SNMP, Telnet
6	Presentation Layer	SSL, TLS
5	Session Layer	NetBIOS, PPTP
4	Transport Layer	TCP, UDP
3	Network Layer	IP, ARP, ICMP, IPSec
2	Data Link Layer	PPP, ATM, Ethernet
1	Physical Layer	Ethernet, USB, Bluetooth, IEEE802.11



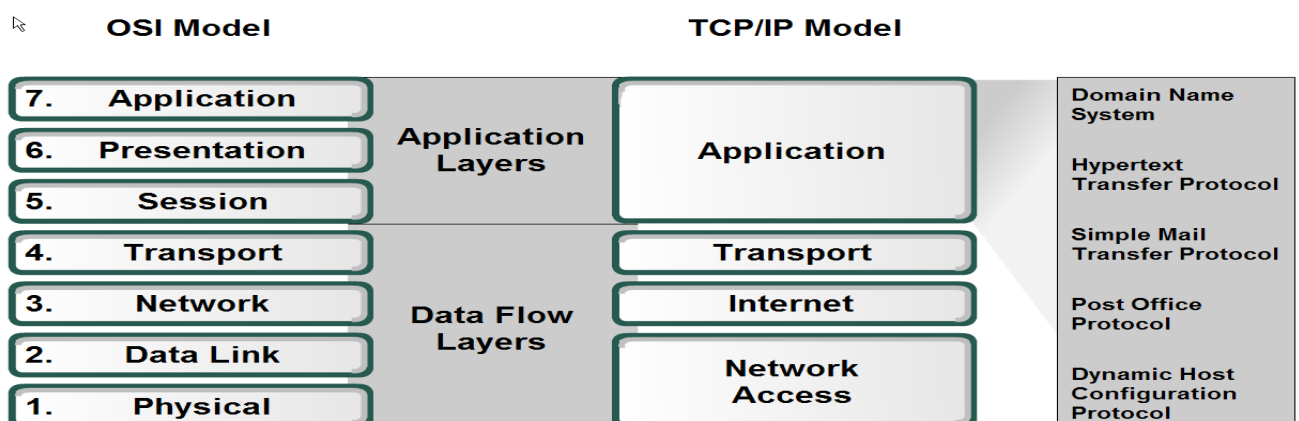
Benefits(Advantage)	Negative Aspect (disadvantage)
• Interconnection of different systems (open) • Not limited to a single vendor solution	• Systems might be less secure • Systems might be less stable

<u>Layer</u>	<u>Main Topics</u>
Physical Layer	• Transmission mediums (transmit bits over medium) • Encoding • Modulation • Repeaters • Hubs (multi-port repeater) • To provide mechanical and electrical specification
Data Link Layer	• Error detection and correction methods • Hop to hop delivery • Flow control • Frame format • IEEE LAN standards • Bridges & Switches (multi-port bridges) • physical addressing(MAC Address)
Network Layer	• Internetworking • Controls the operation of the subnet. • Routing algorithms(Routing packets from source to destination) • Internet Protocol (IP) addressing (Logical addressing) • Routers
Transport Layer	• Connection-oriented and connectionless services • Provide reliable process to process message delivery & error recovery • Transmission Control Protocol (TCP) • User Datagram Protocol (UDP) • Provides additional Quality of Service. • Port address • End-to-end flow control.
Session Layer	• Allows users on different machines to establish sessions (dialogue) between them. • managing dialogue control. • Token management. • Synchronization.
Presentation Layer	• Concerned with the syntax and semantics of the information. • Preserves the meaning of the information. • Data compression. • Data encryption.
Application Layer	• Provides protocols that are commonly needed. • To allow access to network resource • (FTP), (HTTP), (SMTP), (SNMP),(NFS),(Telnet)

SERVICES

Connection-Oriented	Connectionless
before data is sent, the service from the sending computer must establish a connection with the receiving computer.	data can be sent at any time by the service from the sending computer.

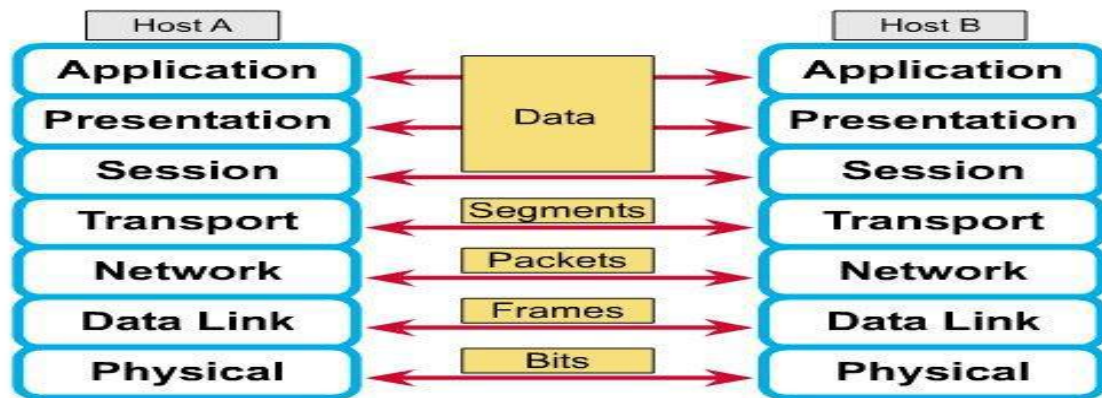
OSI(Open System Interconnection)	TCP/IP(Transmission Control Protocol / Internet Protocol)
1. OSI provides layer functioning and also defines functions of all the layers.	1. TCP/IP model is more based on protocols and protocols are not flexible with other layers.
2. OSI model has a separate presentation layer	2. TCP/IP does not have a separate presentation layer
3. OSI is a general model.	3. TCP/IP model cannot be used in any other application.
4. Network layer of OSI model provide both connection oriented and connectionless service.	4. The Network layer in TCP/IP model provides connectionless service.
5. OSI model has a problem of fitting the protocols in the model	5. TCP/IP model does not fit any protocol
6. Protocols are hidden in OSI model and are easily replaced as the technology changes.	6. In TCP/IP replacing protocol is not easy.
7. OSI model defines services, interfaces and protocols very clearly and makes clear distinction between them.	7. In TCP/IP it is not clearly separated its services, interfaces and protocols.
8. It has 7 layers	8. It has 4 layers



Data Encapsulation

- Each layer contains a **Protocol Data Unit (PDU)**
 - PDU's are used for **peer-to-peer contact** between corresponding layers.

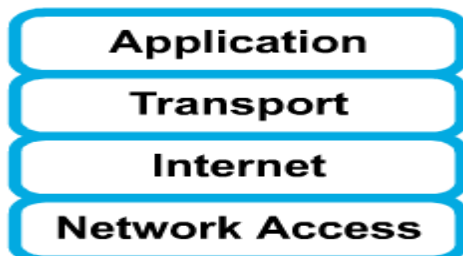
The Layer	Shape of data (PDU)
top three layers	Data
Transport layer	Segment
Network layer	packets
Data Link layer	frames
Physical layer	bits



4 layers of the TCP/IP model

- Layer 4: Application
- Layer 3: Transport
- Layer 2: Internet
- Layer 1: Network access

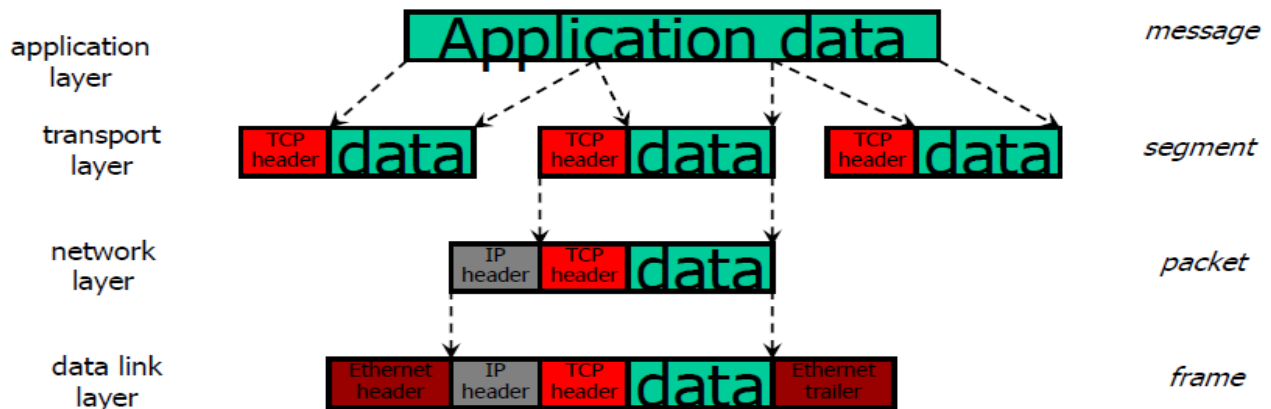
It is important to note that some of the layers in the TCP/IP model have the same name as layers in the OSI model. Do not confuse the layers of the two models.



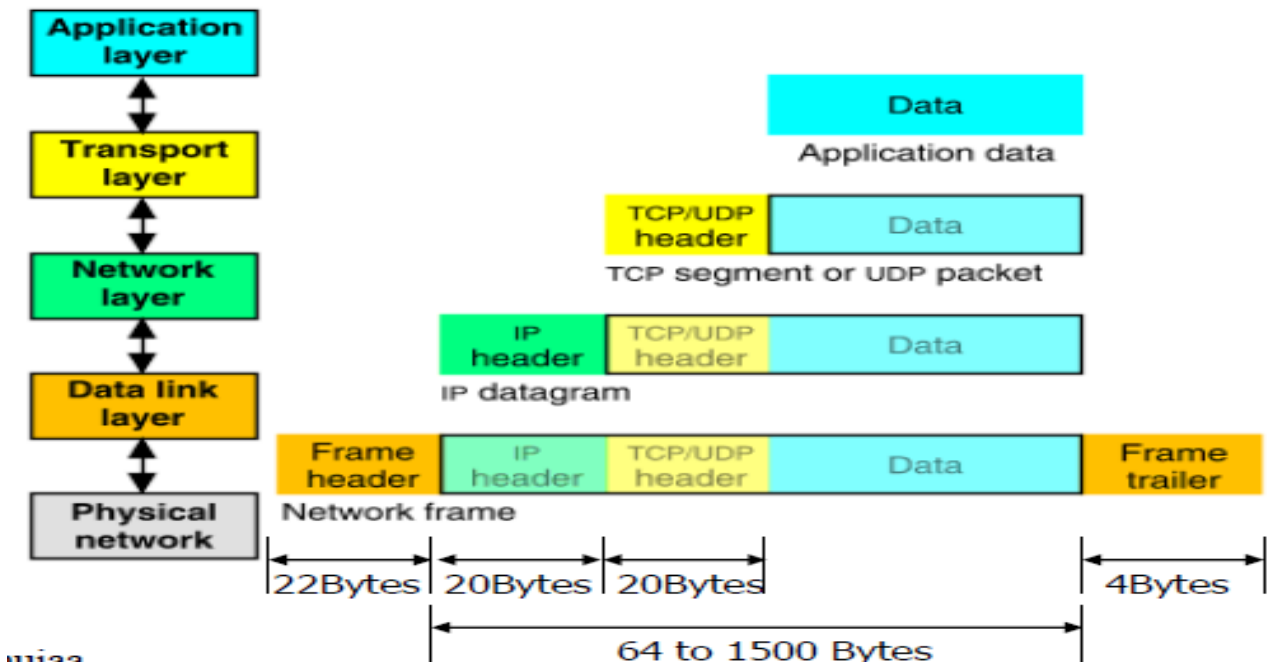
Data Encapsulation In TCP/IP

- Outgoing data is packaged and identified for **delivery** to the layer underneath
- PDU – Packet Data Unit – the “envelop” information attached to a packet at a particular TCP/IP protocol e.g. header and trailer
- Header (Identifies the protocol in use, the sender and intended recipient)
- Trailer (or packet trailer) (Provides data integrity checks for the payload)

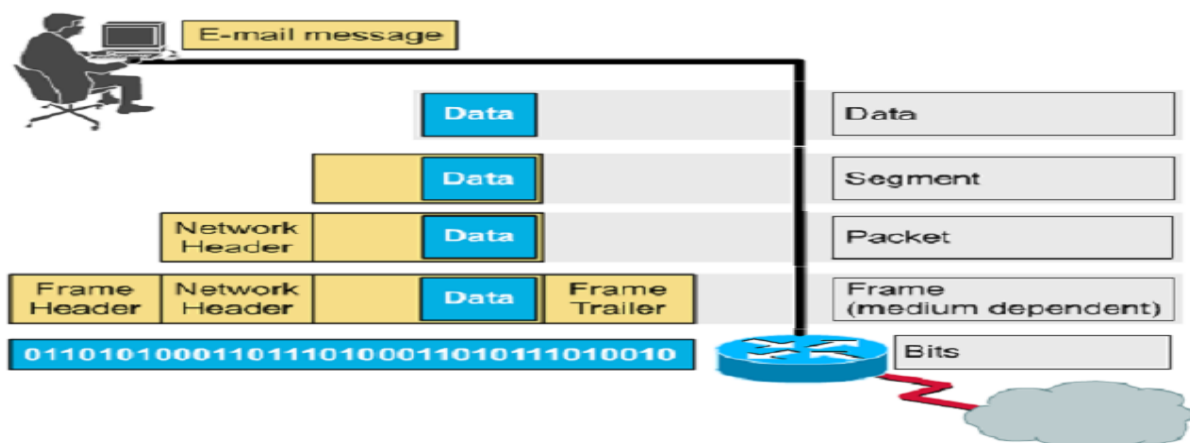
Data Formats



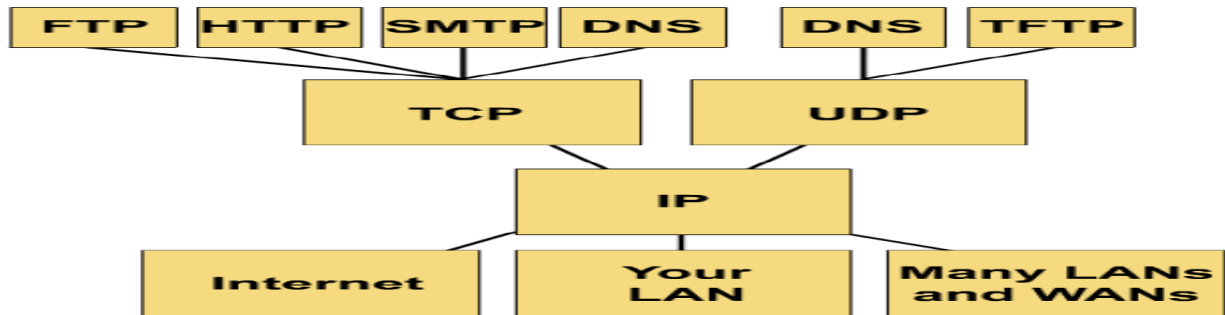
Encapsulation (TCP/IP)



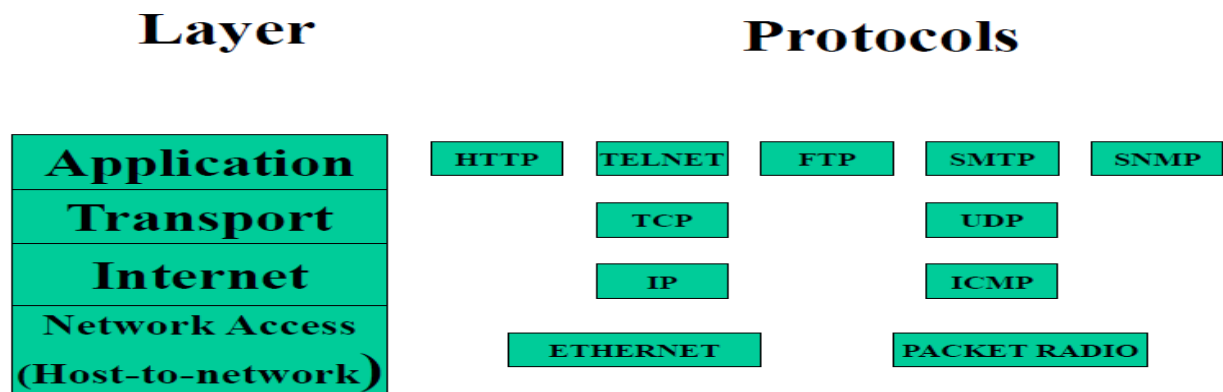
Encapsulation example: E-mail



TCP/IP protocol stack



TCP/IP Reference Model



What is a socket?

- An interface between application and network(each application create socket)
- Socket(Protocolfamily, type-of-communication, specific- protocol);
- The socket *type* dictates the style of communication

reliable vs. best effort

connection-oriented vs. connectionless

Q/Explain the delivery of data in Layered model?

Type of delivery	Layer	Shape of data	Type of addressing
End to End	Transport	Segment	Port (socket)
Source To Destination	Network	Packet	Logical (IP)
Node to Node	Data Link	Frame	Physical(MAC)

Computer Networks Protocols

Lecture No.2: Physical & Data link layer

PHYSICAL LAYER

SONET\SDH Networks

- SONET\SDH, that is used as a **transport network to carry loads from other WANs.**

SDH(Synchronous Digital Hierarchy)	SONET(Synchronous Optical Network)
• Is European standard network. • Is a standard developed by ITU-T. • Define a hierarchy of signals called synchronous transfer modules (STMs)	• Is American standard network. • Is a standard developed by ANSI for fiber-optic networks. • Define a hierarchy of signals called synchronous transport signals (STs) where each STS level (STS-1 to STS-192) supports a certain data rate.

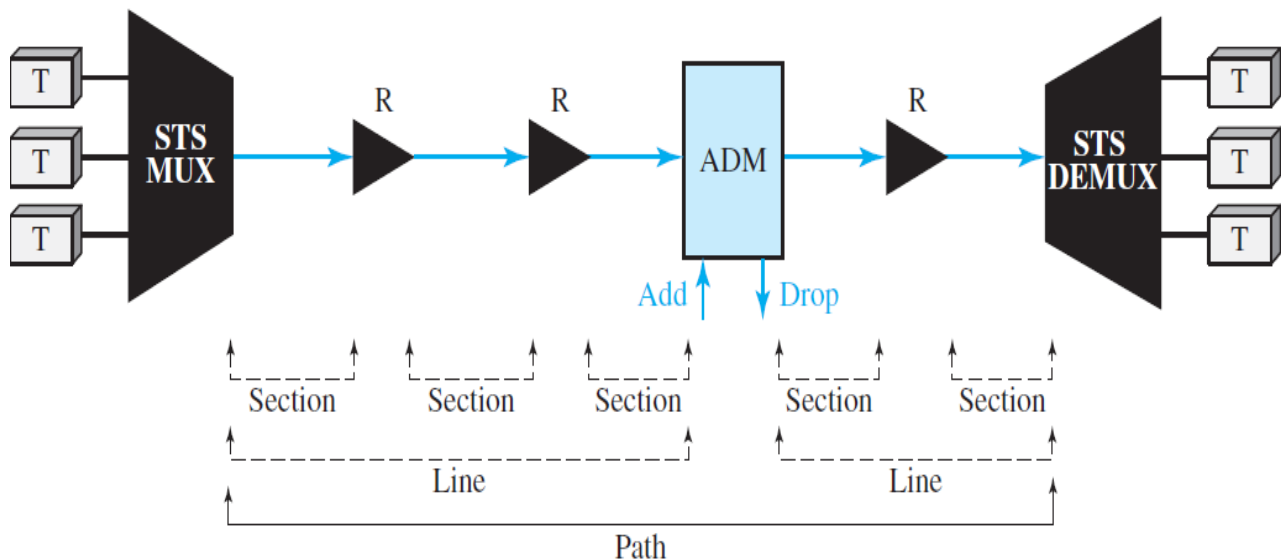
ADM: Add/drop multiplexer

R: Regenerator

STS MUX: Synchronous transport signal multiplexer

T: Terminal

STS DEMUX: Synchronous transport signal demultiplexer



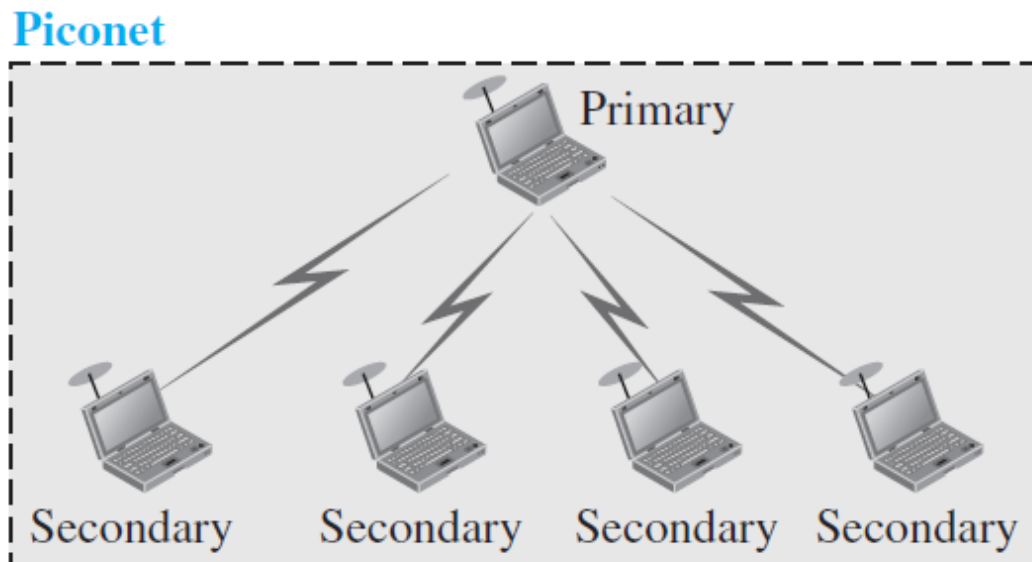
BLUETOOTH

- **Bluetooth is a wireless LAN technology designed to connect devices of different functions** such as telephones, notebooks, computers (desktop and laptop), cameras, printers, and even coffee makers when they are at a **short distance** from each other.

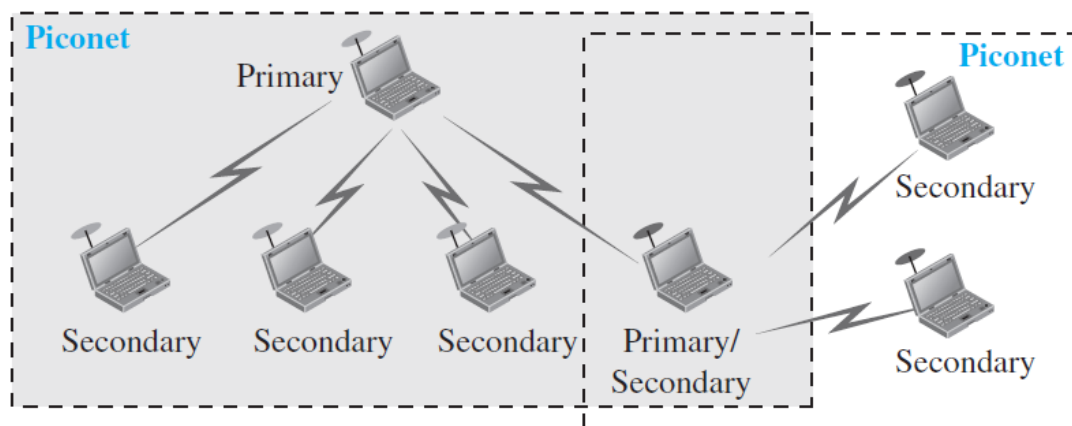
Architecture of Bluetooth:

- Bluetooth defines two types of networks: **piconet and scatternet**.
- A Bluetooth network is called a **piconet, or a small net**. *A piconet can have up to eight stations, one of which is called the primary; the rest are called secondaries.*

Piconet Network



Scatternet Network



Data Link Layer

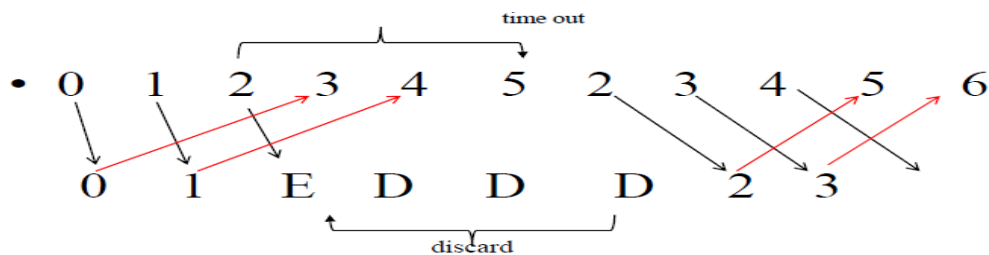
1.Elementary Data Link Protocols

An Unrestricted Simplex Protocol (SP)	one direction transmitted data
A Simplex Stop-and-Wait Protocol(SWP)	flooding control
A Simplex Protocol for a Noisy Channel(SPN)	limit send and receive between sender and receiver, capacities are limited

2. Sliding Window Protocols

A One-Bit Sliding Window Protocol(SWP)	1- assign variable 2- define frame 3- accept frame
A Protocol Using Go Back N protocol	Discarding & Buffering
A Protocol Using Selective Repeat (SRP)	accept and buffer delay and effected frame) without ACK

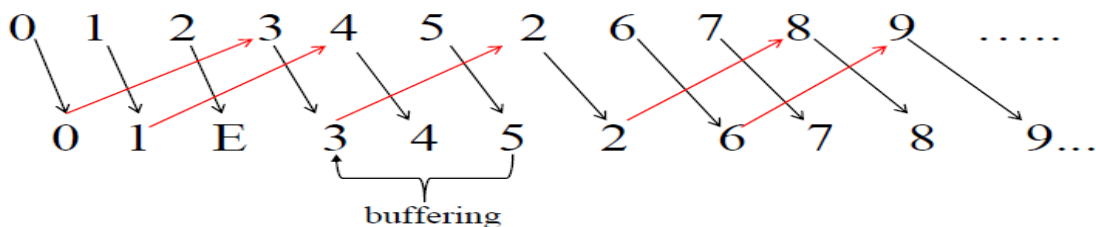
Go Back N Protocol



Discarding operation

Selective repeat Protocol SRP

• Buffering



Sender may transmit up to max. without waiting for ACK

PPP – Point to Point Protocol

- Carry network data of any network layer protocol at the same time
- Error detection (no correction)
- has a very simple mechanism for **error control**(A CRC field is used to detect errors)
- Does not provide flow control
- Connection life, signal link, negotiator

Address Resolution Protocol (ARP)

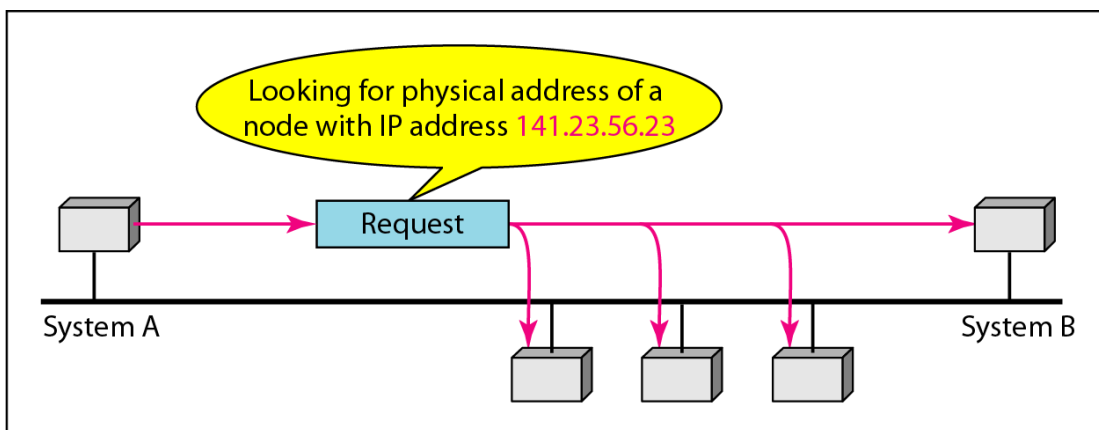
•The delivery of a packet to a host or a router requires two levels of addressing: logical and physical.

–ARP Maps IP addresses to MAC addresses

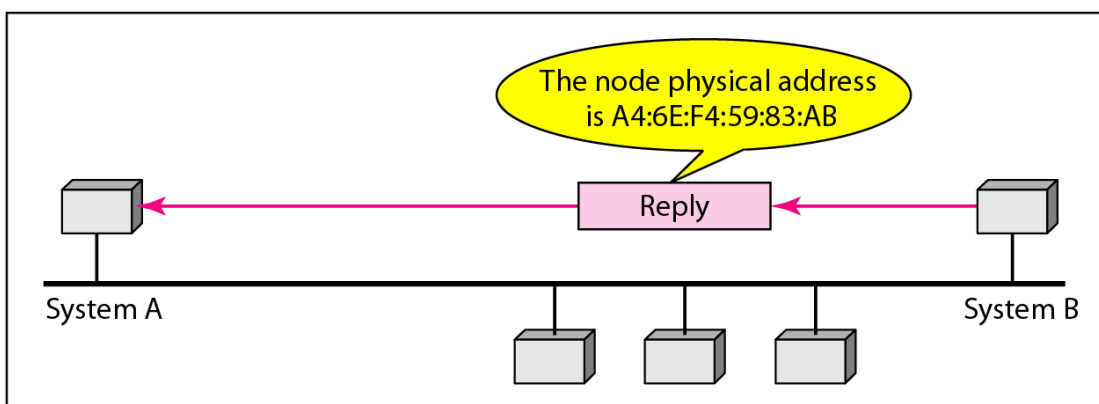
–ARP **Request** is a broadcast but ARP **reply** is Unicast .

–**ARP tables** contain the MAC and IP addresses of other devices on the network

ARP operation:



a. ARP request is broadcast



b. ARP reply is unicast

Layer 2 Tunneling Protocol (L2TP)

- is an **extension** of the Point-to-Point Tunneling Protocol (PPTP).
- **used by** an Internet service provider (ISP) to enable the operation of a **virtual private network** (VPN) over the Internet.
- VPN The goal of a Virtual Private Network (VPN) is to **provide private communications within the public Internet Infrastructure**

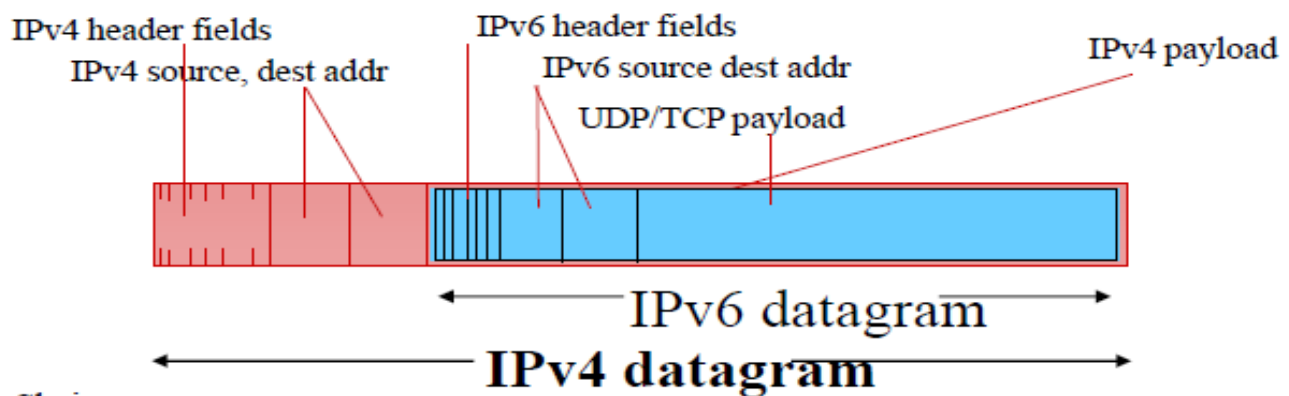
Why is there a need for VPN?

- **Internet has insufficient security mechanisms**
- IP packets are not authenticated or encrypted
- Users with access to network can read content of IP traffic

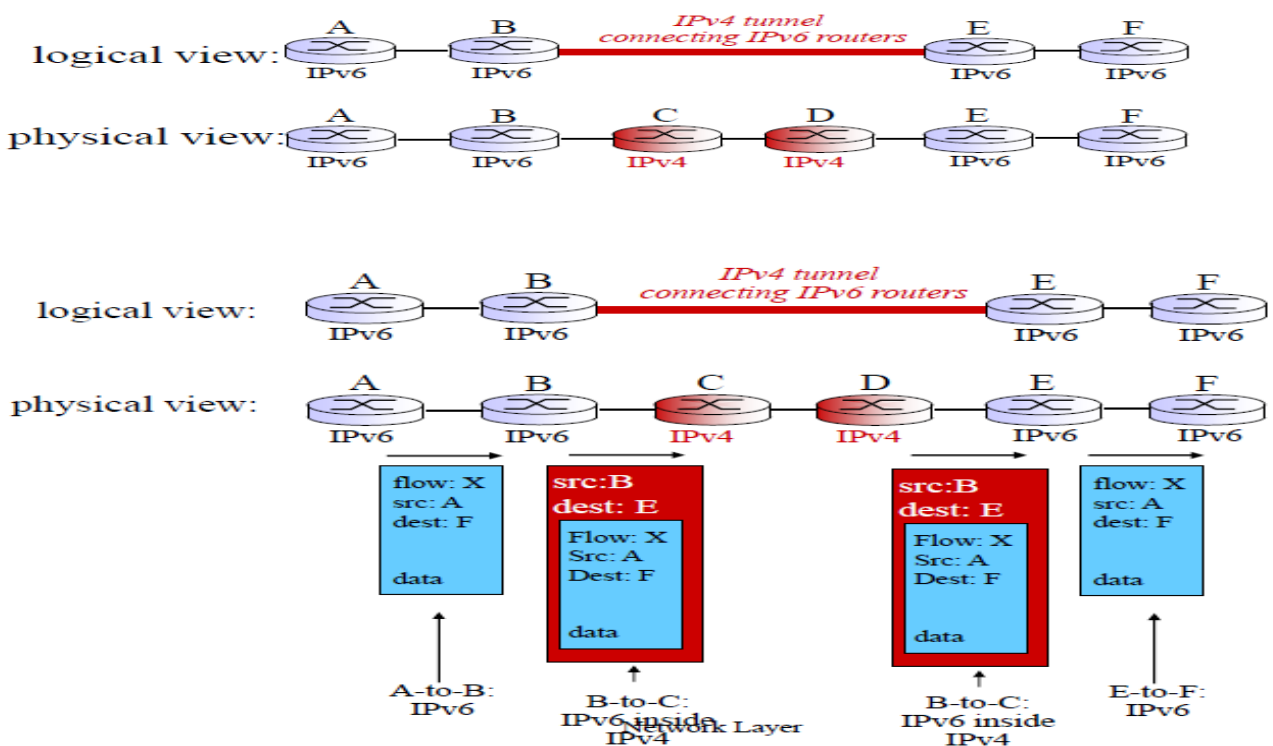
Transition from IPv4 to IPv6

not all routers can be upgraded simultaneously

tunneling: IPv6 datagram carried as *payload* in IPv4 datagram among IPv4 routers



Tunneling

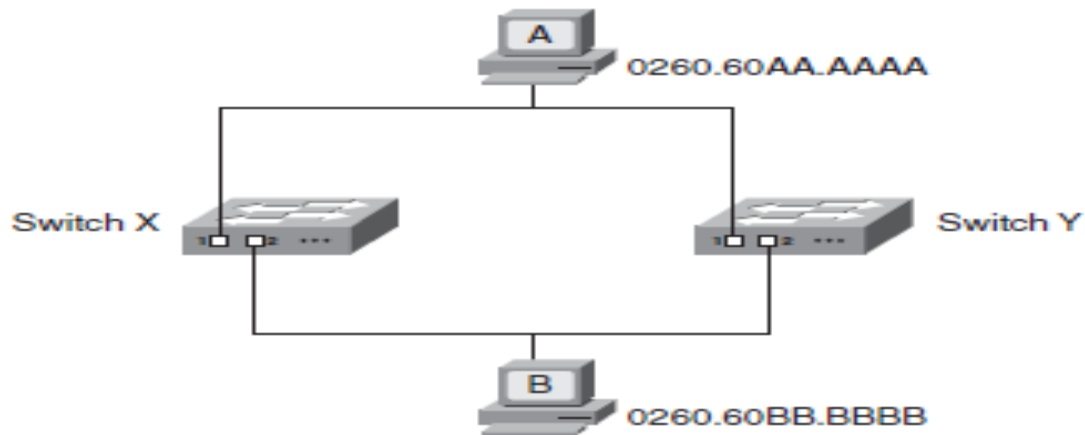


Spanning Tree Protocol(STP)

Redundancy in a network, such as that shown in Figure below, is **desirable** so that communication can still take place if a link or device fails.

For example, if switch X in this figure stopped functioning, devices A and B could still communicate through switch Y. However, in a switched network, redundancy can cause problems.

Redundancy in a Switched Network Can Cause Problems



There are 3 problems:

1. occurs if a broadcast frame is sent on the network(*broadcast storm*).
2. that can occur in redundant topologies is that devices can receive multiple copies of the same frame.
3. that can occur in a redundant situation is within the switch itself—the MAC address table can change rapidly and contain wrong information.

To overcome these problems:

you must have a way to **logically disable** part of the redundant network for regular traffic while **maintaining redundancy** for the case when an error occurs. STP does just that.

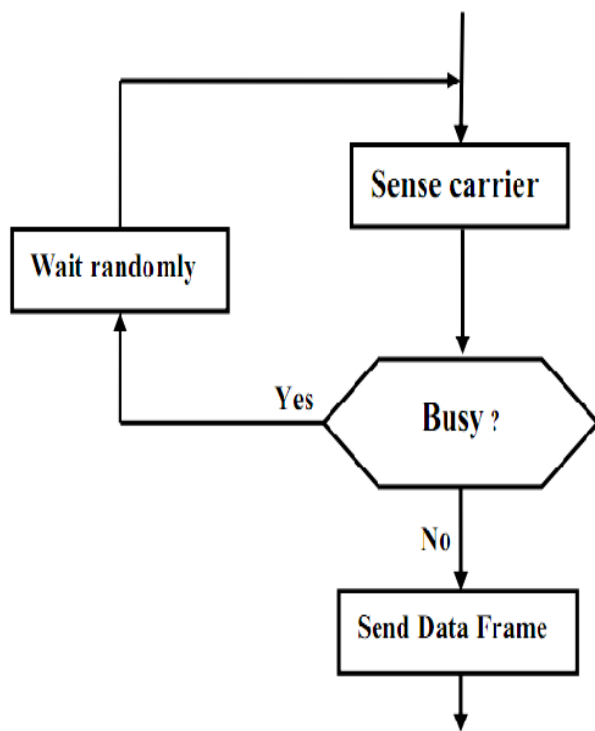
Access Method: CSMA/CD

- Whenever multiple users have unregulated access to a single line, there is a danger of **signals overlapping and destroying each other**. Such overlaps, which turn the signals into unusable noise, are called collisions.
- **As traffic increases** on a multiple access link, so do collisions. A LAN therefore needs a mechanism to coordinate traffic, minimize the number of collisions that occur, and maximize the number of frames that are delivered successfully.
- The access mechanism used in an Ethernet is called *carrier sense multiple access with collision detection (CSMA/CD)*, standardized in IEEE 802.3).
- CSMA/CD is the result of an evolution from multiple access (**MA**) to carrier sense multiple access (**CSMA**), and finally, to carrier sense multiple access with collision detection (CSMA/CD).

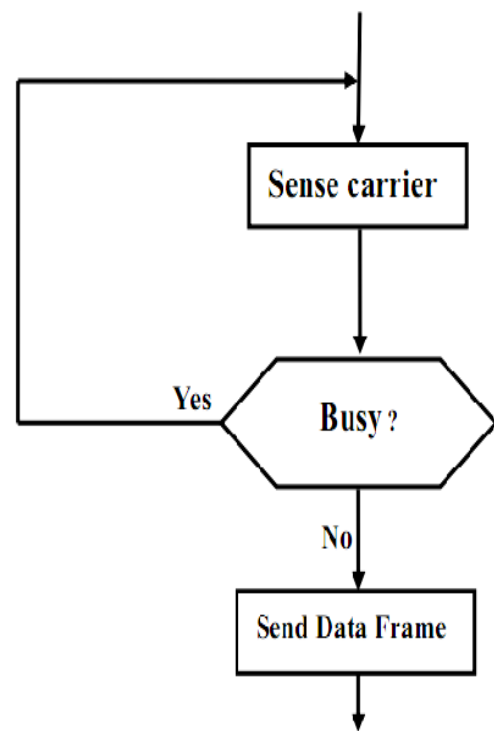
•**Carrier Sense**: when a station in an Ethernet network has data to transmit ,it first see the network if it is use by other stations this is carrier sense .under three case of persistence strategy

Non-persistence	senses the line if it is idle it sends immediately if the line busy ,it waits a random time then sense the line again this method reduce the chance of collision but it also reduced network efficiency.
1-persistence	after the station finds the line idle it sends its data immediately (with probability 1) this method increase the chance of collision.
p-persistence	after the station finds the line idle it may transmit or no . here the probability of sending is defined by P and probability of refusing is (1-P) for example if $p=0.3$ then station sends with 30% of the time and refusing 70% of the time . The station generates a random number between 1 and 100 if the number generated is less than 30 the station sends its data else it waits one slot time before sensing the medium again this method reduces the chance of collision and increasing network efficiency.

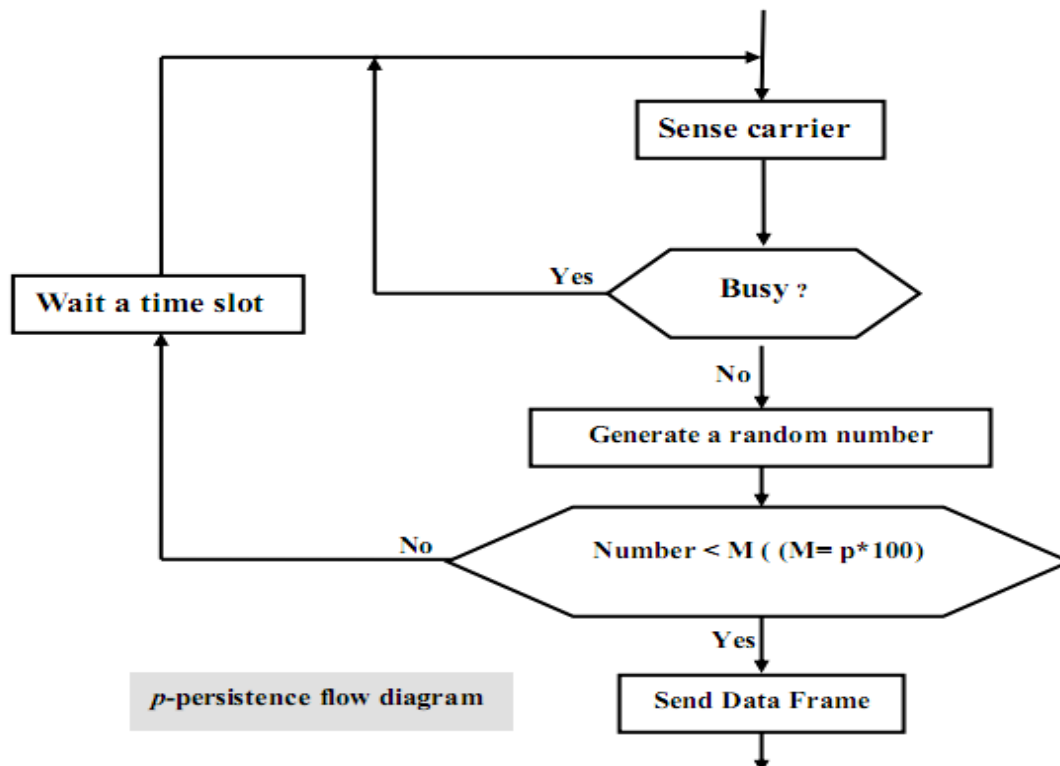
.Jam signal : when system detected a collision it immediately stop transmitting data and starts sending this signal any system received packet must discard this packet and should not attempt to transmit any data until network has cleared.



Non-persistence flow



1-persistence flow diagram



p -persistence flow diagram

Cyclical Redundancy Check (CRC)

The *most powerful redundancy technique*, unlike the VRC and LRC, CRC is based on binary division.

Figure 10.7 CRC generator and checker

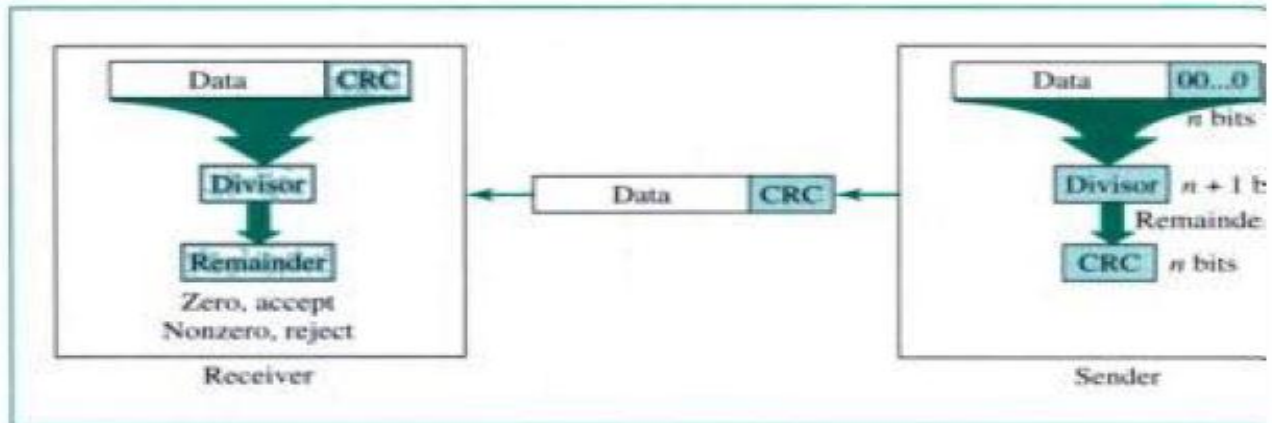


Figure 10.8 Binary division in a CRC generator

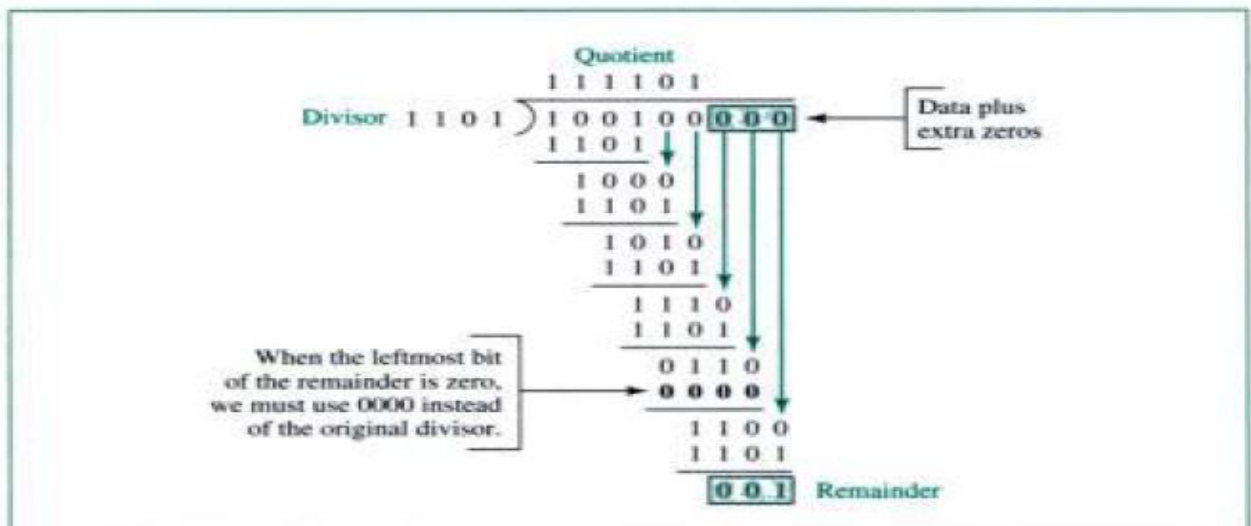
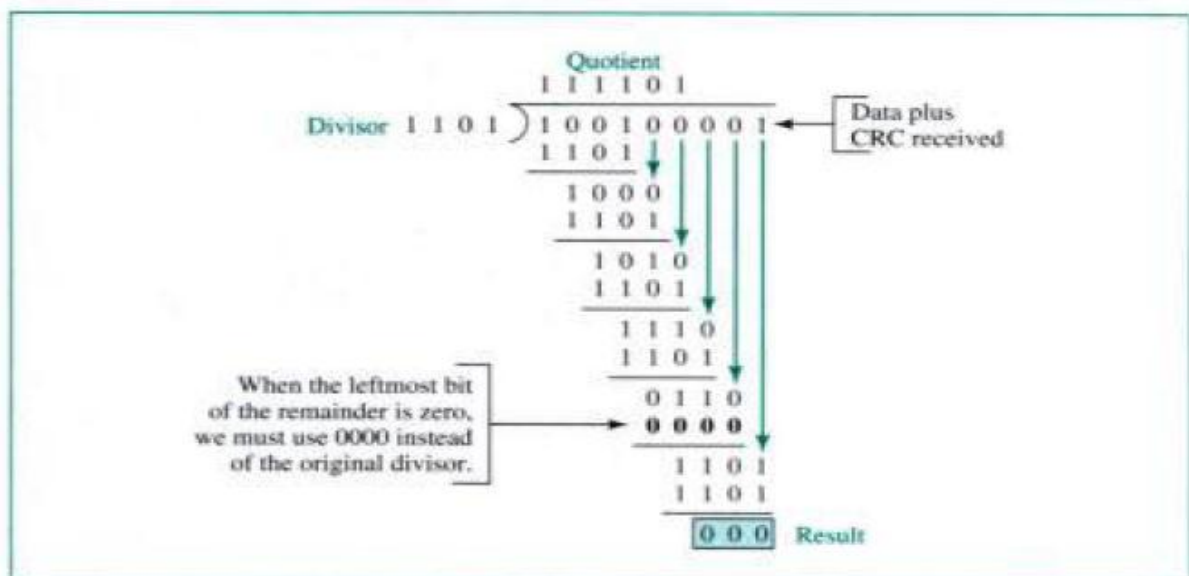
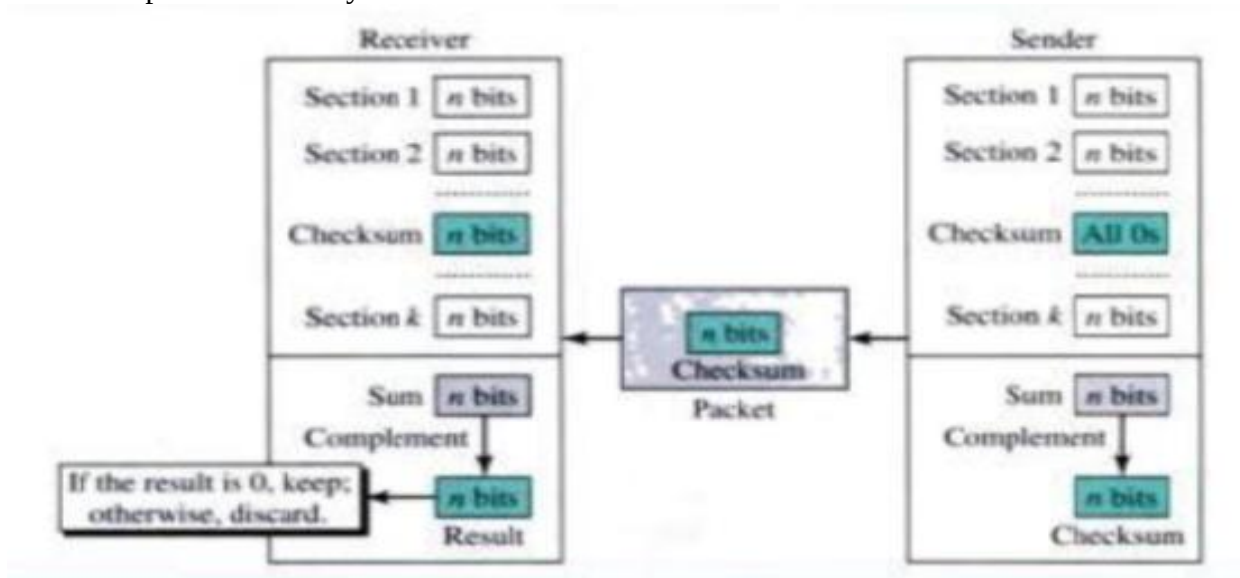


Figure 10.9 Binary division in CRC checker



Checksum

The error detection method used by the *higher layer protocols*. Like other methods, it depends on the concept of redundancy.



The sender follows these steps:

- The unit is divided into k sections, each of n bits.
- All sections are added using ones complement to get the sum.
- The sum is complemented and becomes the checksum.
- The checksum is sent with the data.

Example

Now suppose there is a burst error of length 5 that affects 4 bits.

1010111111111001 00011101

When the receiver adds the three sections, it gets

	10101111
	11111001
	00011101
Partial Sum	1 11000101
Carry	1
Sum	11000110
Complement	00111001 the pattern is corrupted.

Example

Now suppose there is a burst error of length 5 that affects 4 bits.

1010111111111001 00011101

When the receiver adds the three sections, it gets

	10101111
	11111001
	00011101
Partial Sum	1 11000101
Carry	1
Sum	11000110
Complement	00111001 the pattern is corrupted.

Example

Now suppose the receiver receives the pattern sent in Example 7 and there is no error.

10101001 00111001 00011101

When the receiver adds the three sections, it will get all 1s, which, after complementing, is all 0s and shows that there is no error.

	10101001	
	00111001	
	00011101	
Sum	11111111	
Complement	00000000	means that the pattern is OK.

Example

Now suppose there is a burst error of length 5 that affects 4 bits.

10101111 11111001 00011101

When the receiver adds the three sections, it gets

	10101111	
	11111001	
	00011101	
Result	1 11000101	
Carry	1	
Sum	11000110	
Complement	00111001	means that the pattern is corrupted.

Computer Networks Protocols

Lecture No.3: Network Layer Part 1

Routing Concept

ROUTING is **forwarding** of packets from one network to another network choosing the best path from the routing table.

Routing table consist of only the best routes for every destinations.

Types of Routing:

Static	• It is configure by Administrator manually • Need for destination network ID • It is secure and fast • Used for small organization which have network of 10-15 routers
Dynamic	• Means automatically routing • Dynamic routes means that the router learns of paths of destinations by receiving periodic updates from other routers • Is automatically choose the best shortest path • Can be done by using routing protocol
Default	• Is configured for unknown destination • When there is no entry for the destination network in a routing table, the router will forward the packet to its default router. • It is last preferred routing

Q/ list the Advantages of dynamic over static?

- There is **no need** to know the destination networks
- **Updates** the topology changes **dynamically**
- Administrative work **reduced**
- Used for **large organizations**

Routing Algorithm

Routing Algorithms

- The main function of the network layer is **routing packets from source to destination**.
- The **routing algorithm** is that part of the network layer software responsible for **deciding** which output line an incoming packet should be transmitted on.
- Routing algorithms can be grouped into two major classes: non adaptive and adaptive.

Non adaptive algorithms (static routing)	Adaptive algorithms (dynamic routing)
• Do not base their routing decisions on measurements or estimates of the current traffic and topology. • It is called static algorithm.	• Change their routing decisions to reflect changes in the topology , and usually the traffic as well. • It is called dynamic.

Static Algorithm

1. Flooding routing.

2.Shortest path routing.

Flooding	• A simple local technique, where each router must make decisions based on local knowledge, <u>not the complete picture of the network</u>. • is a simple algorithm to send a packet along all paths(Every incoming packet is sent out on every outgoing line <u>except</u> the one it arrived on). • generates infinite number of duplicate packets unless some measures are taken to damp the process. • One such measure is to have a hop counter in the header of each packet, which is decremented at each hop, with the packet being discarded when the counter reaches zero.
Shortest Path Routing	• Shortest path routing first developed by Dijkstraalgorithm. • Find the shortest path from a specified source to all other destinations in the network. • In the general case, the labels on the lines could be computed as a function of the distance, bandwidth, average traffic, communication cost, measured delay, and other factors.

Q/ Find the shortest path from router A to router H?

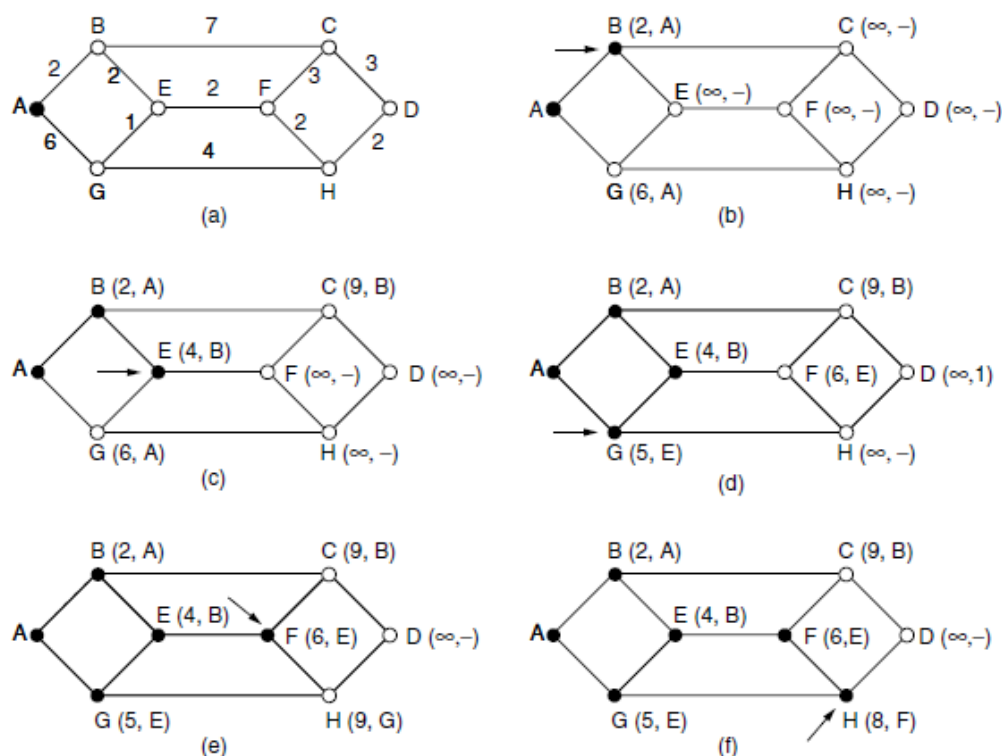


Figure The first six steps used in computing the shortest path from A to D. The arrows indicate the working node.

Dynamic Routing Algorithm

1. Distance Vector Routing.

2. Link state routing.

1. Distance Vector Routing.

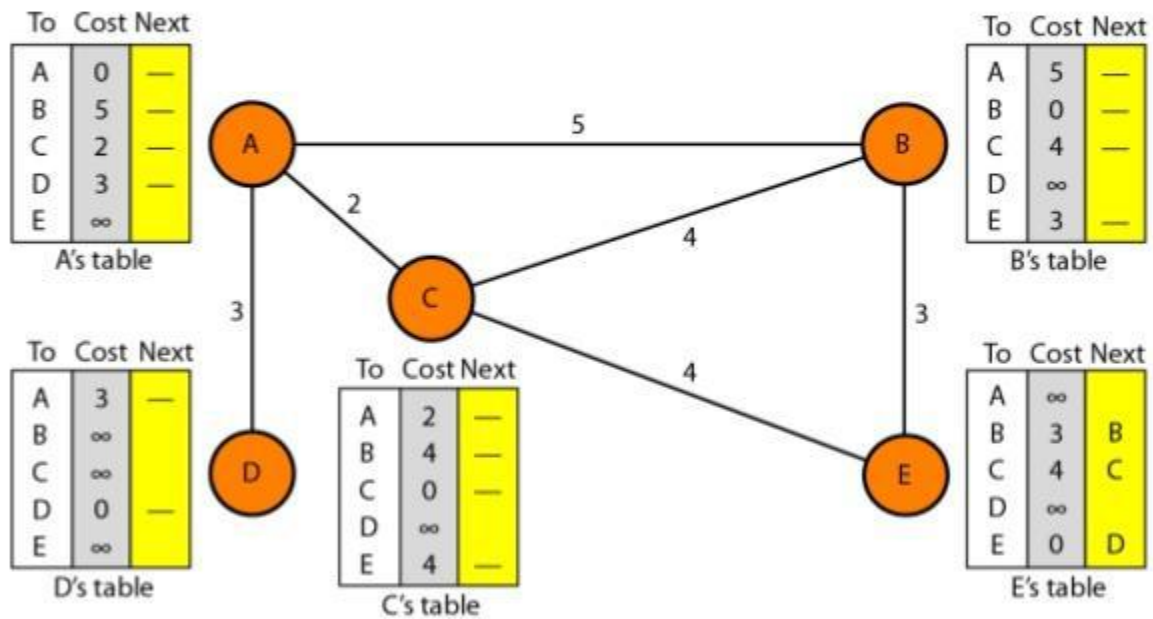
- Distance Vector routing is **intra-domain** protocols, **inside** Autonomous system, but not between Autonomous system.
- distance-vector routing are based on the **least-cost** goal.
- Distance Vector developed by **Bellman-Ford** algorithm.
- Bellman **equation** is used to find the **least cost (shortest distance)** between a source to destination.
- A **distance vector routing algorithm** operates by having each router **maintain a table** (i.e., a **vector**) giving the best known distance to each destination.
- These tables are **updated by exchanging** information with the neighbors router. Every router knows the **best link** to reach each destination.
- RIP** based on distance vector routing, each router **shares, at regular intervals**, its knowledge about entire AS with its neighbor.

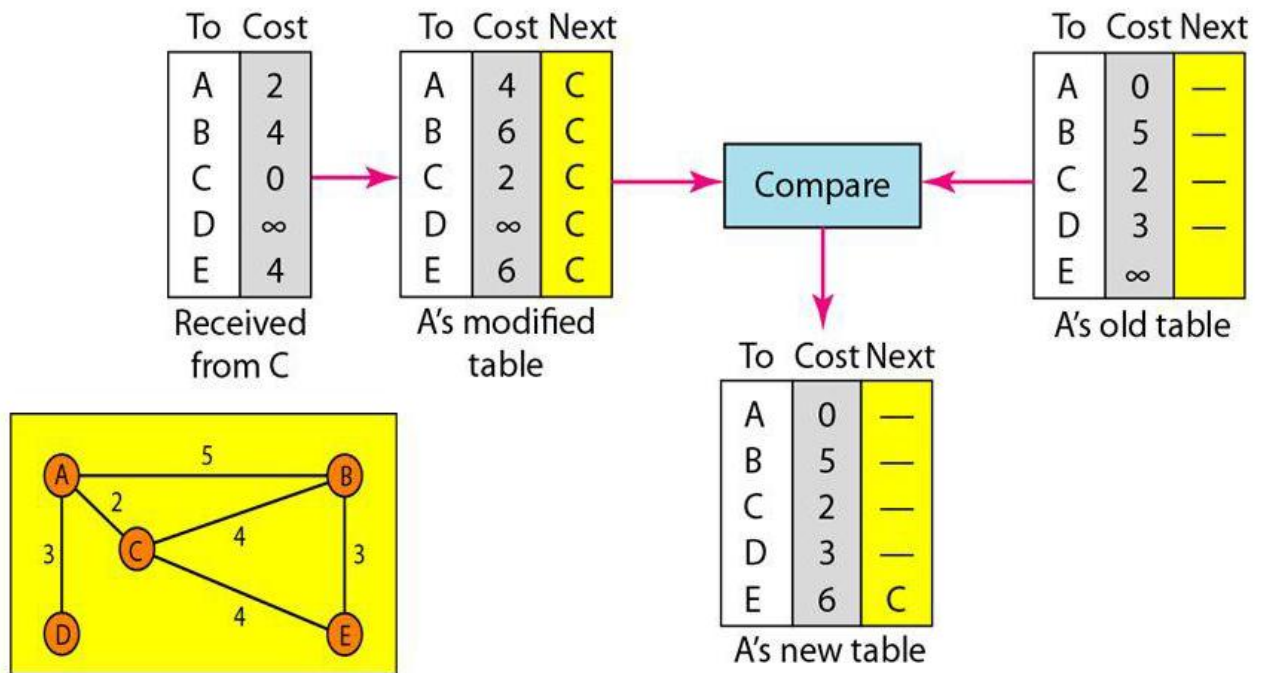
- It is so **slow** and does not take **Bandwidth** into consideration when choose the root.

Q/Update the Router A using Distance vector algorithm?



Initialization of tables in distance vector routing (DVR)





Distance vector algorithm

Bellman-Ford equation (dynamic programming)

let

$d_x(y) := \text{cost of least-cost path from } x \text{ to } y$

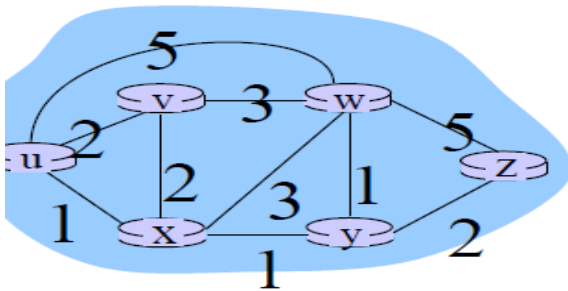
Then

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

$\min$ taken over all neighbors v of x
 $c(x,v)$ cost to neighbor v
 $d_v(y)$ cost from neighbor v to destination y

- $D_x(y)$ = estimate of least cost from x to y
 x maintains distance vector $\mathbf{D}_x = [D_x(y): y \in N]$
- node x :
 - knows cost to each neighbor v : $c(x,v)$
 - maintains its neighbors' distance vectors. For each neighbor v , x maintains $\mathbf{D}_v = [D_v(y): y \in N]$

Bellman-Ford example



clearly, $d_v(z) = 5$, $d_x(z) = 3$, $d_w(z) = 3$

B-F equation says:

$$\begin{aligned} d_u(z) &= \min \{ c(u,v) + d_v(z), \\ &\quad c(u,x) + d_x(z), \\ &\quad c(u,w) + d_w(z) \} \\ &= \min \{ 2 + 5, \\ &\quad 1 + 3, \\ &\quad 5 + 3 \} = 4 \end{aligned}$$

node achieving minimum is next
hop in shortest path, used in forwarding table

2. Link State Routing

The **primary problem in distance vector** that the algorithm often took **too long to converge** after the network topology changed (due to the count-to-infinity **problem**). Consequently, it was **replaced by** a new algorithm, now called link state routing.

The idea behind link state routing is simple and can be stated as five parts. Each router must:

- 1) **Discover** its neighbors and learn their network addresses.
- 2) **Measure** the delay or cost to each of its neighbors.
- 3) **Construct** a packet telling to all it has just learned.
- 4) **Send** the packet to all other routers.
- 5) **Compute** the shortest path to every other router.

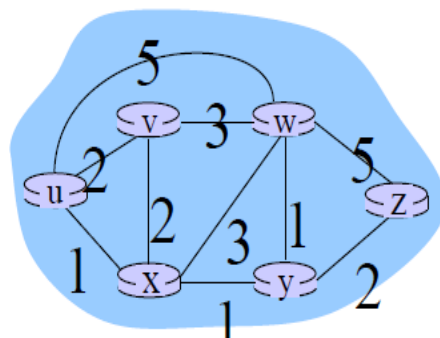
Compared to distance vector routing, link state routing requires **more memory and computation**. Also, the **computation time** grows faster

Nevertheless, in many practical situations, link state routing works **well because it does not suffer from slow convergence problems**.

Q/Consider the following network, define OSPF protocol & construct shortest path tree using dijkstra algorithms :

Dijkstra's algorithm: example

Step	N'	D(v),p(v)	D(w),p(w)	D(x),p(x)	D(y),p(y)	D(z),p(z)
0	u	2,u	5,u	1,u	∞	∞
1	ux	2,u	4,x		2,x	∞
2	uxy	2,u	3,y			4,y
3	uxyv		3,y			4,y
4	uxyvw					4,y
5	uxyvwz					



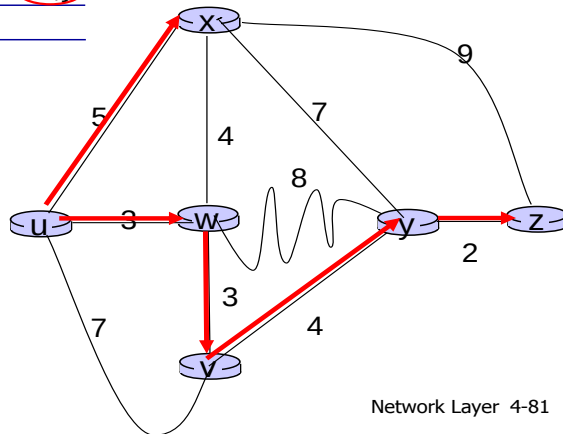
Q/Consider the following network, define OSPF protocol & construct shortest path tree using dijkstra algorithms :

Dijkstra's algorithm: example

Step	N'	D(v) p(v)	D(w) p(w)	D(x) p(x)	D(y) p(y)	D(z) p(z)
0	u	7,u	3,u	5,u	∞	∞
1	uw	6,w		5,u	11,w	∞
2	uwx	6,w			11,w	14,x
3	uwxv				10,v	14,x
4	uwxvy					12,y
5	uwxvyz					

notes:

- ❖ construct shortest path tree by tracing predecessor nodes
- ❖ ties can exist (can be broken arbitrarily)



Comparison of LS and DV algorithms

message complexity

- **LS:** with n nodes, E links, $O(nE)$ msgs sent
- **DV:** exchange between neighbors only
 - convergence time varies

speed of convergence

- **LS:** $O(n^2)$ algorithm requires $O(nE)$ msgs
 - may have oscillations
- **DV:** convergence time varies
 - may be routing loops
 - count-to-infinity problem

robustness: what happens if router malfunctions?

LS:

- node can advertise incorrect *link* cost
- each node computes only its *own* table

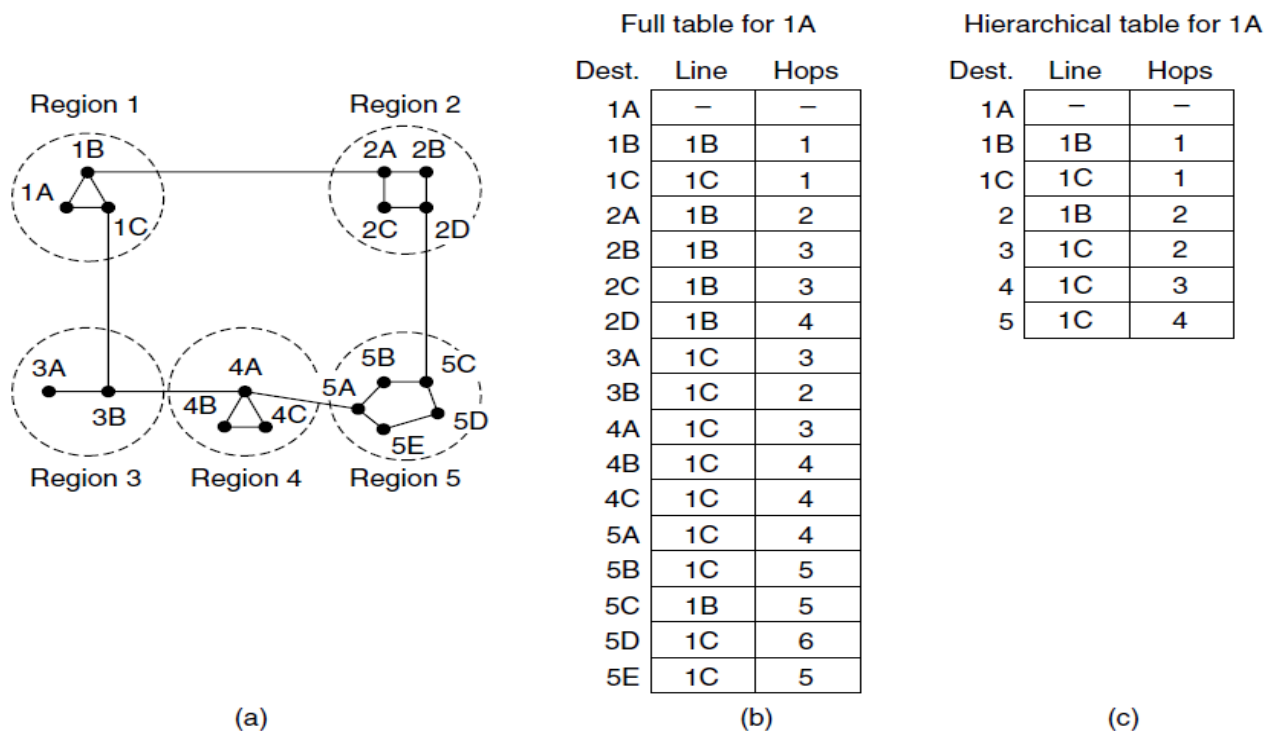
DV:

- DV node can advertise incorrect *path* cost
- each node's table used by others
 - error propagate thru network

Hierarchical Routing

- As networks **grow in size**, the **router routing tables grow proportionally**.
- Not only is router **memory** consumed by ever-increasing tables, but more **CPU time** is needed to scan them and **more bandwidth** is needed to send status reports about them.
- So router can not have table about the entire network.
- **When hierarchical routing is used**, the routers are divided into what we will call **regions**.

- Each router knows all the details about how to route packets to destinations within its **own region** but knows nothing about the internal structure of other regions.



Broadcast Routing

- For some applications, hosts need to send messages to **many or all other hosts**. **Broadcast routing** is used for that purpose.
- The source should send the packet to **all** the necessary destinations. One of the problems of this method is that the source has to have the complete list of destinations.
- We have already seen a better broadcast routing technique: **flooding**.

Multicast Routing

- Sending a message to such a **group** is called **multicasting**, and the routing algorithm used is called **multicast routing**.
- All multicasting schemes require some way to **create and destroy groups and to identify which routers are members of group**.

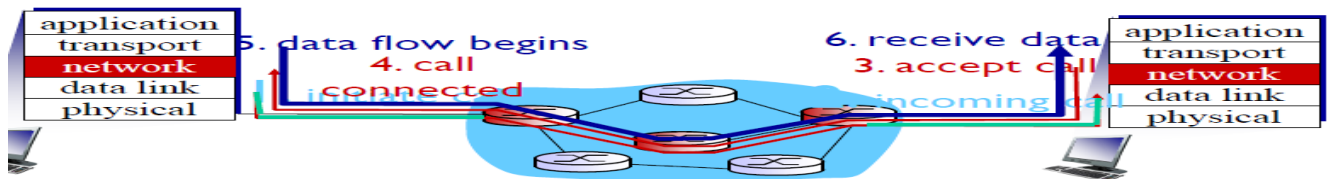
Network service model

Q:What service model for “channel” transporting datagrams from sender to receiver?

<i>individual datagrams</i>	<i>flow of datagrams</i>
- guaranteed delivery - guaranteed delivery with less than 40 msec delay	- in-order datagram delivery - guaranteed minimum bandwidth to flow.

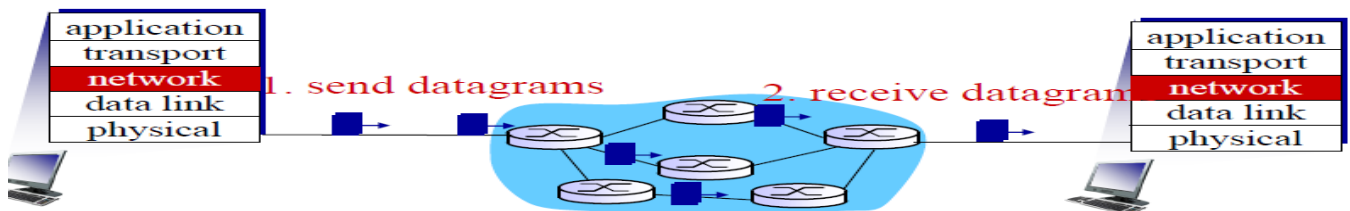
Virtual circuits: signaling protocols

- used to setup, maintain, teardown VC
- used in ATM, frame-relay, X.25
- not used in today's Internet



Datagram networks

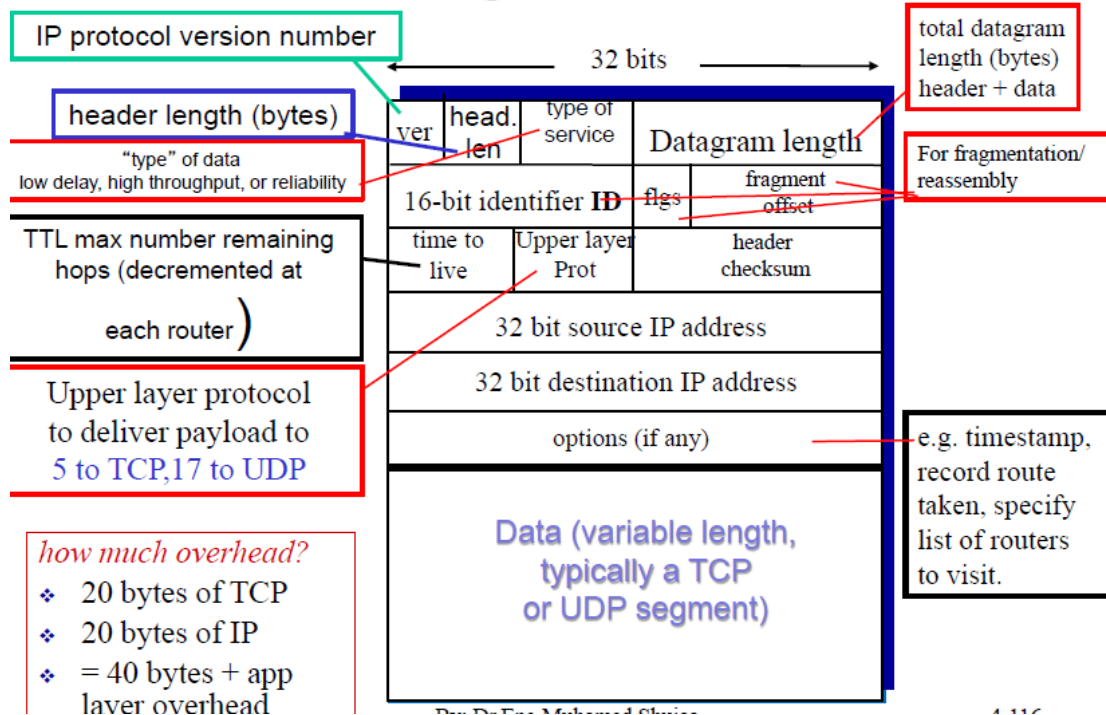
- no call setup at network layer
- routers: no state about end-to-end connections
 - no network-level concept of “connection”
- packets forwarded using destination host address



Q/ Datagram or VC network: why?

<i>Internet (datagram)</i>	<i>ATM (VC) virtual circuit</i>
• data exchange among computers –“elastic” service, no strict timing req • many link types –different characteristics –uniform service difficult • “smart” end systems (computers) –can adapt, perform control, error recovery –<i>simple inside network, complexity at “edge”</i>	• evolved from telephony • human conversation: –strict timing, reliability requirements –need for guaranteed service • “dumb” end systems –telephones –<i>complexity inside network</i>

IP datagram format



Computer Networks Protocols

Lecture No.4:Network Layer Part 2

Routing Protocols

- A **routing protocol** is a combination of **rules and a procedure that lets** routers in the internet inform each other of **changes**.
- **Routing metric**: a method by which routing algorithms determines that one route is better than another route ,Metric may be(hop count, bandwidth,delay,load)

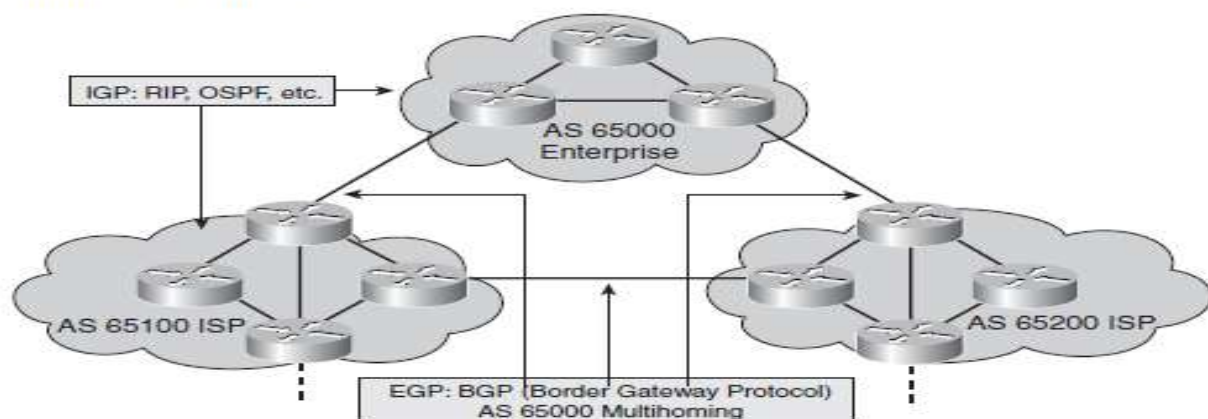
Interior Versus Exterior Routing Protocols

An **autonomous system (AS)**, also known as a domain, is a **collection of routers** that are **under a common administration**, such as a company's internal network or an Internet service provider's (ISP's) network.

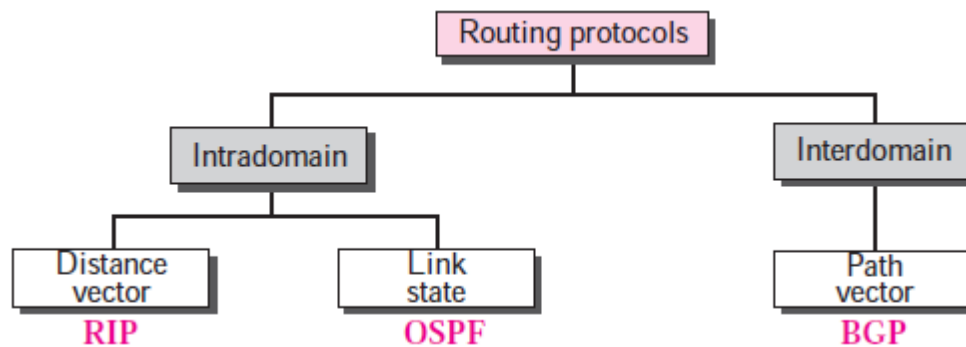
Because the Internet is based on the AS concept, two types of routing protocols are required:

Interior gateway protocols (IGP)	Exterior gateway protocols (EGP)
Intra-AS (inside an AS) routing protocols.	Inter-AS (between autonomous systems) routing protocols.
Examples of IGPs include: Routing Information Protocol (RIP) RIP version 2 (RIPv2), Open Shortest Path First (OSPF), and Enhanced Interior Gateway Routing Protocol (EIGRP).	Border Gateway Protocol (BGP) is the only widely used EGP protocol on the Internet. BGP version 4 (BGP-4) is considered the acceptable version of BGP on the Internet.
use less-complicated metrics to ease configuration and speed up the decisions about best routing paths for faster convergence	Slower to converge and more complex to configure.

Interior Protocols Are Used Inside and Exterior Protocols Are Used Between Autonomous Systems



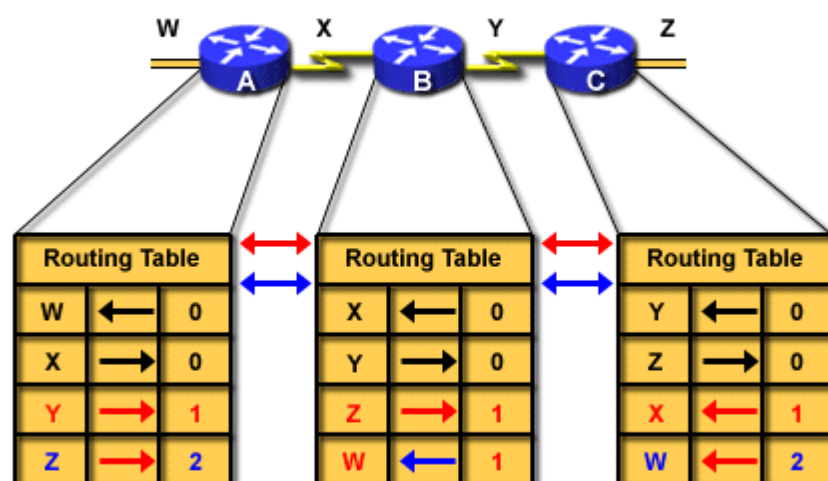
Popular routing protocols



RIP (Routing Information Protocol)

- RIP is a routing protocol **for exchanging routing table information between routers**.
- It is a very simple protocol based on **distance vector routing**.
- simple **intra-domain** protocol
- Uses **hop count** as a path selection metric. (RIP **prevents routing loops** by implementing a **limit on the number of hops** allowed in a path from the source to a destination. The maximum number of hops allowed for RIP is 15. This hop limit, however, also limits the size of networks that RIP can support, a hop count of 16 is considered an infinite distance, in other words the route is considered unreachable).
- **Three** types of timers.

Distance Vector Network Discovery



- Routers discover the best path to destinations from each neighbor

Timers

Routing-update timer (periodic timer)

- The **periodic timer** controls the advertising of **regular update** messages.
- By default, routers send updates **every 30 seconds**.

Route timeout (*Expiration Timer*)

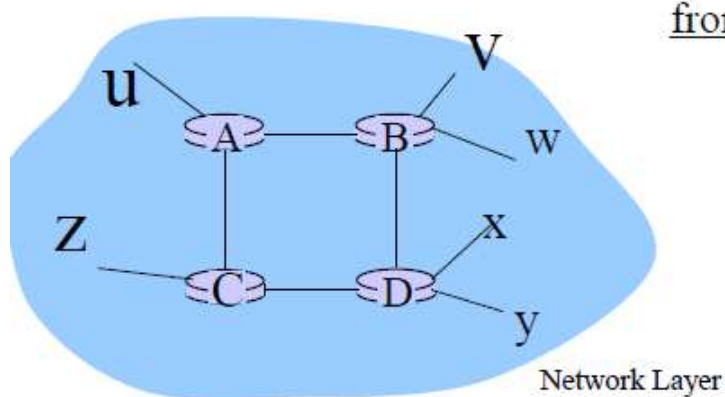
- If there is a **problem** on an internet and **no update** is received within the allotted 180 s, the route is considered expired and the hop count of the route is set to 16, which means the **destination is unreachable**.

Route-flush timer (*Garbage Collection Timer*)

- After the route **timeout expires**, the route-flush timer eventually expires, **deleting** the route from the table.

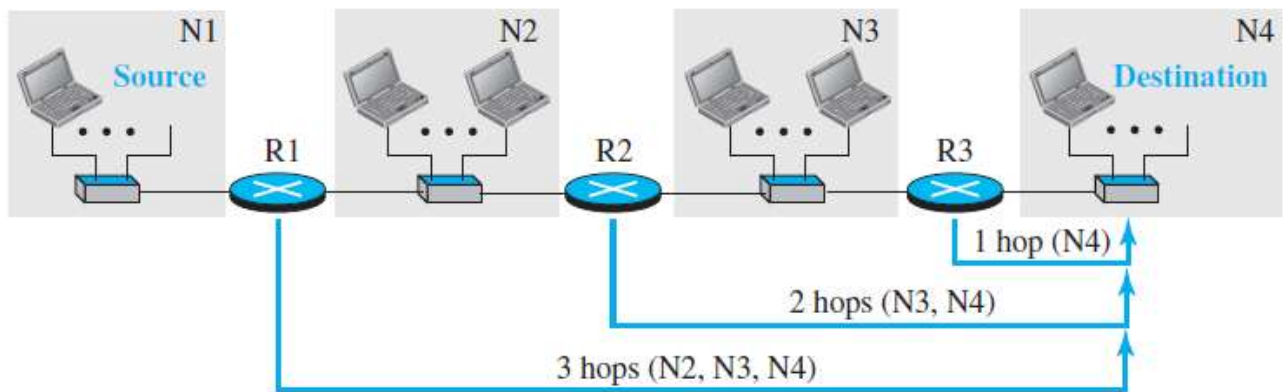
Drawbacks

- RIP has **slow convergence** and count to infinity problems
- The **hop count cannot exceed 15**, or routes will be dropped.



from router A to destination *subnets*:

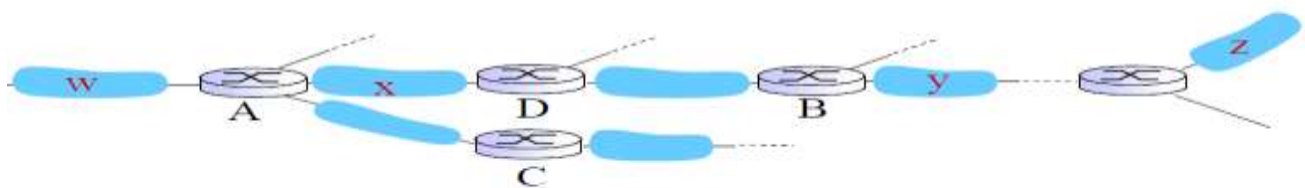
<u>subnet</u>	<u>hops</u>
u	1
v	2
w	2
x	3
y	3
z	2



Forwarding table for R1

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

RIP: example



routing table in router D

destination subnet	next router	# hops to dest
w	A	2
y	B	2
z	B	7
x	--	1
....		

routing table in router D

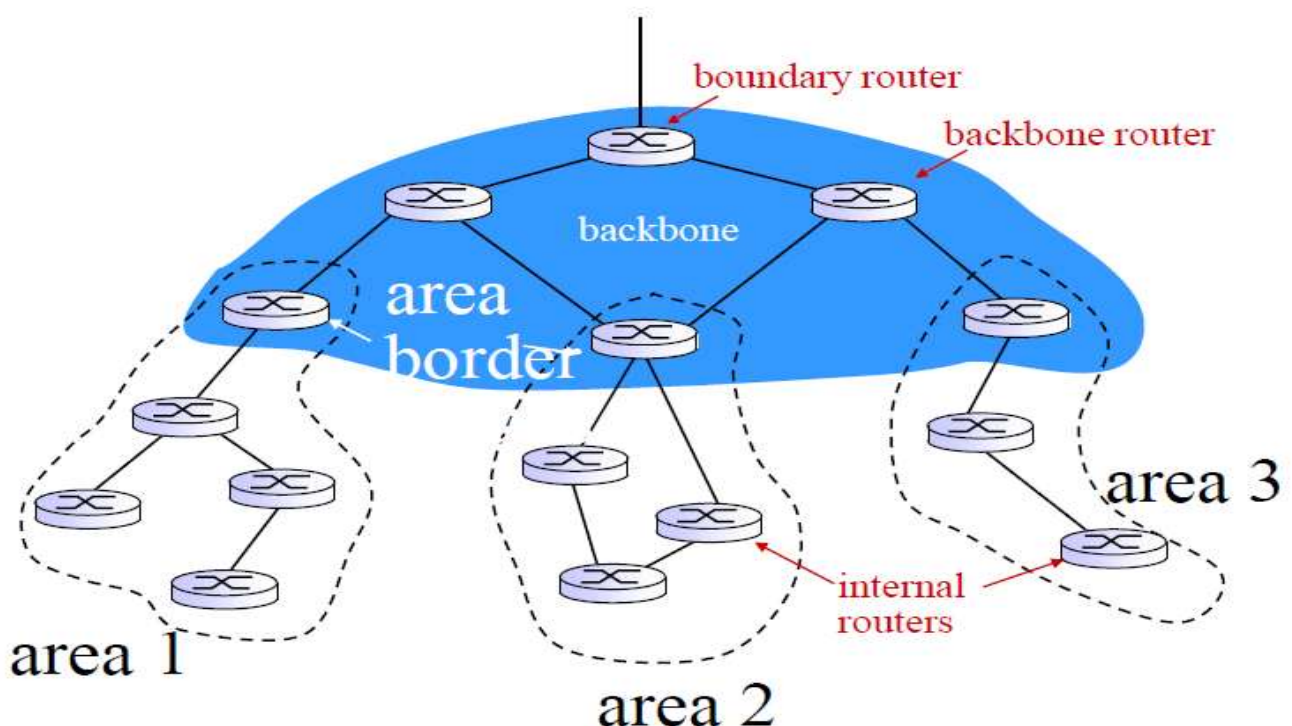
destination subnet	next router	# hops to dest
w	A	2
y	B	2
z	~~B~~ → A	~~7~~ → 5
x	--	1
....		

OSPF (Open Shortest Path First)

- It uses a **link state routing algorithm** and falls into the group of interior routing protocols, operating within a single autonomous system (AS).
- **topology map** at each node
- route computation using **Dijkstra's algorithm**
- OSPF is perhaps the most widely **used interior gateway protocol (IGP)** in large enterprise networks.'
- The metric of OSPF is the **cost** of sending packets across a certain interface
- “**open**”: publicly **available**
- “**security**”: all OSPF messages authenticated (to **prevent malicious intrusion**)
- Hierarchical OSPF in large domains.

Hierarchical OSPF

- *Two-level hierarchy: local area, backbone.*
- Link-state advertisements only in **area**
- Each node has **detailed area topology**; only know direction (shortest path) to nets in other areas.
- **Area border routers**: “**summarize**” distances to nets in own area, advertise to other Area Border routers.
- **Backbone routers**: run OSPF routing limited to backbone.
- **Boundary routers**: connect to other AS's.



OSPF is superior to RIP in all aspects, including the following:

- It converges much faster.
- It supports hierarchical structures.
- It has improved metric calculation for best path selection.
- It does not have hop-count limitations

- At its inception, OSPF supported the largest networks.
- Compare to RIP, OSPF has no limitation due to hops (RIP has a limit of 15 hops so any network with more than 15 hops cannot be achieved by RIP).

EIGRP

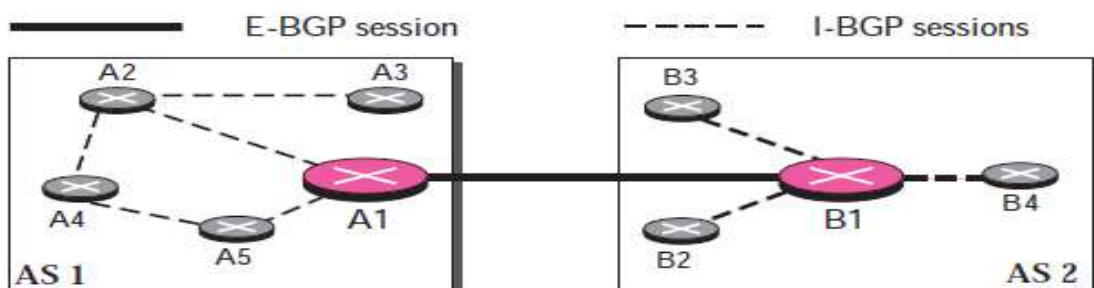
- EIGRP is a protocol for routing IPv4 and IPv6 .
- EIGRP, however, is a hybrid routing protocol—it is a **distance vector protocol with additional link-state protocol features**.
- Uses triggered updates (EIGRP has **no periodic** updates).
- provide **fast convergence to minimize network traffic**.
- uses the **minimum bandwidth** on the path of the destination network, and calculate a route from the total delay metrics.

Border Gateway Protocol(BGP)

- **Inter-domain routing protocol** for routing between autonomous systems (holds the Internet together)
- BGP is **neither a link state, nor a distance vector protocol**. Routing messages in BGP contain complete routes.
- Network administrators can specify routing policies(**BGP supports flexibility** -- paths could be chosen by a provider based on a policy).
- Network administrators can specify routing policies.
- BGP's goal is to find **any path** (not an optimal one).

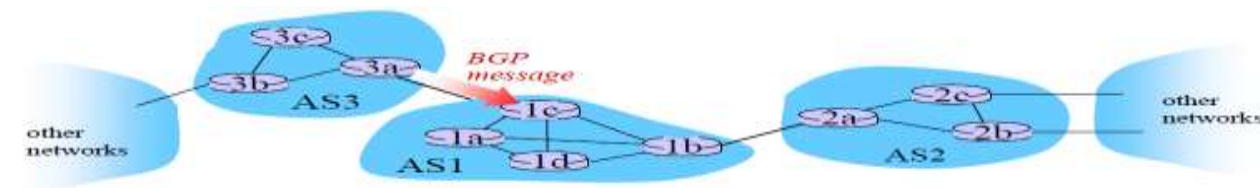
Internal and external BGP sessions

iBGP	eBGP
• used to connect different routers have same AS(same company) • propagate reach ability information to all AS-internal routers.	• used to connect different routers have different AS(different company) • obtain subnet reach ability information from neighboring ASs.



Example: when AS3 advertises a prefix to AS1:

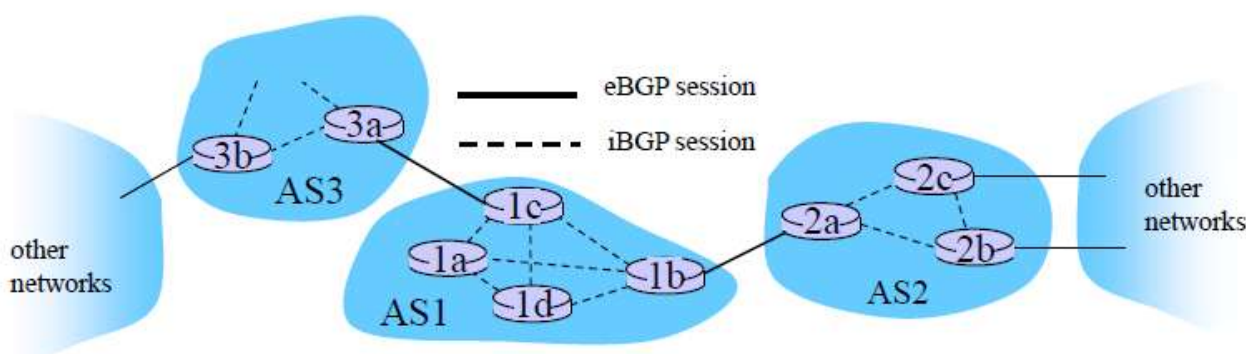
- AS3 *promises* it will forward datagrams towards that prefix
- AS3 can aggregate prefixes in its advertisement



BGP basics: distributing path information

Using eBGP session between 3a and 1c, AS3 sends prefix reachability info to AS1.

- 1c can then use iBGP to **distribute new** prefix info to all routers in AS1
- 1b can then **re-advertise** new reachability info to AS2 over 1b-to-2a eBGP session
- When router learns of new prefix, it creates **entry for prefix** in its forwarding table.



BGP route selection

Router may learn about more than 1 route to destination AS, **selects route based on:**

1. Local preference value attribute: **policy decision**
2. **Shortest AS-PATH**
3. **Closest NEXT-HOP router.**
4. **Additional criteria**

BGP Messages

BGP messages exchanged between peers over TCP connection, **BGP has four types of messages**

- **OPEN:** Establish a connection with a BGP peer
- **UPDATE** -- advertise or withdraw routes to a destination
- **KEEPALIVE:** Inform a peer that the sender is still alive but has no information to send.
- **NOTIFICATION:** Notify that errors are detected, also used to close connection