



SLIIT

Discover Your Future

Lecture 01

Introduction to Routers

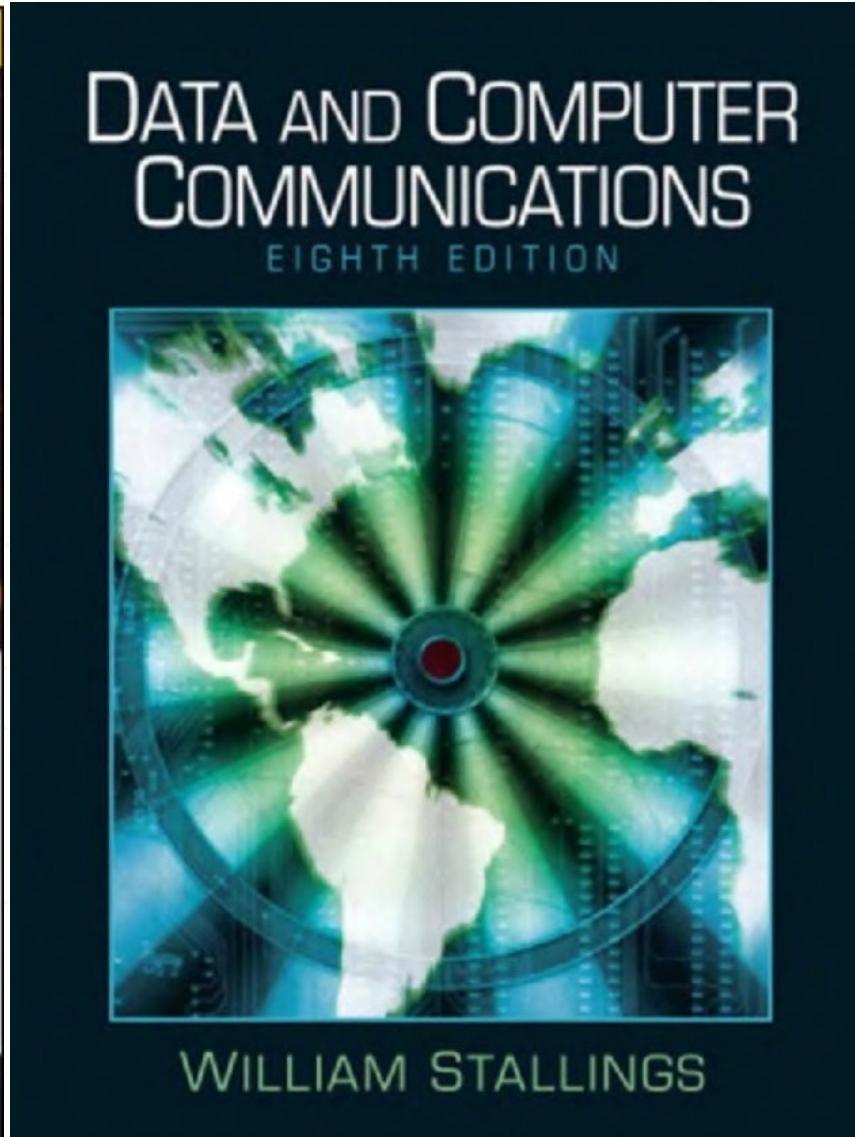
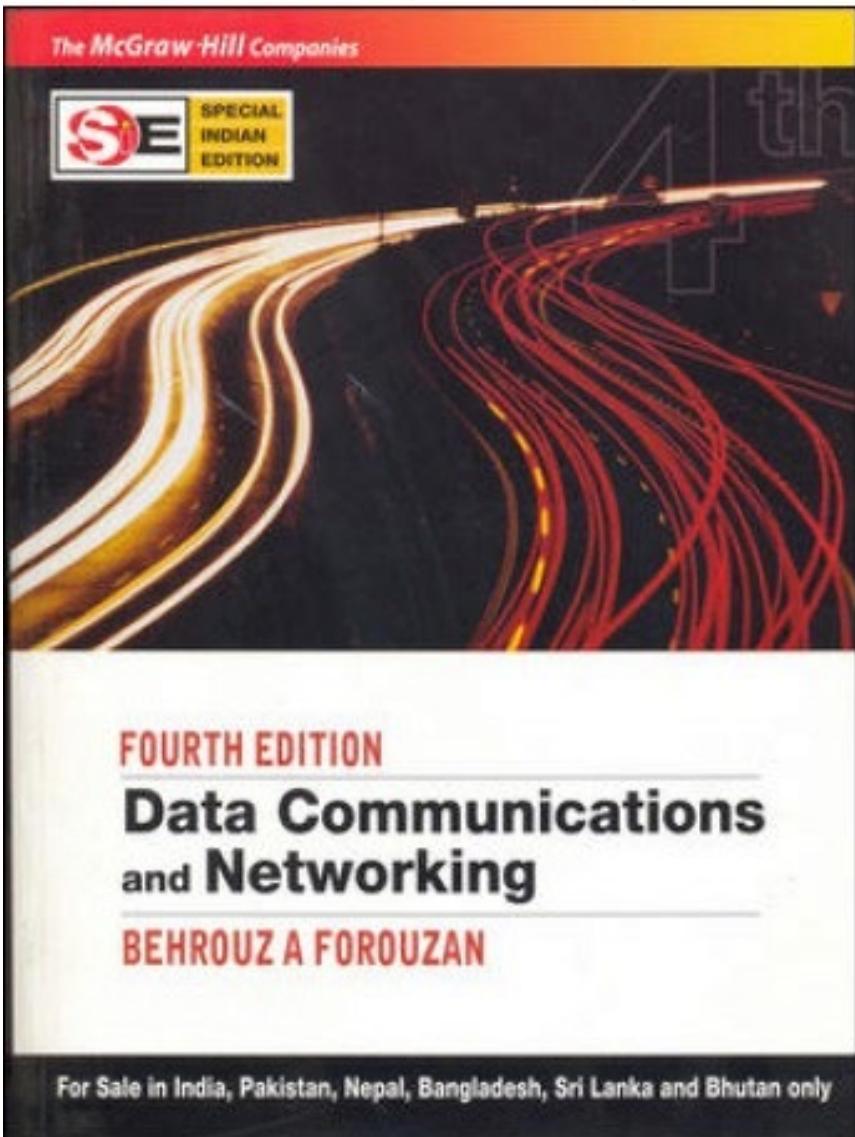
Module Delivery

- Per Week
 - 2hr Lecture
 - 1hr Tutorial
 - 2hr Practical session (once in 2 weeks)
- Module delivery clarifications
 - Within the lecture, tutorial and lab sessions
- Panel of Lecturers
 - Mr.Dhammadika De Silva - Metro
 - Ms.Hansika Mahaadikara - Malabe

Module Assessment Criteria

- Continues Assessments – 40 %
 - Online practical Exam 1 - 1 hr - (week 5) – 10 %
 - Online practical Exam 2 - 1 hr - (week 12) – 10 %
 - Mid Online - 1 hr - (week 8) - 20 %
- Final Examination – 60%

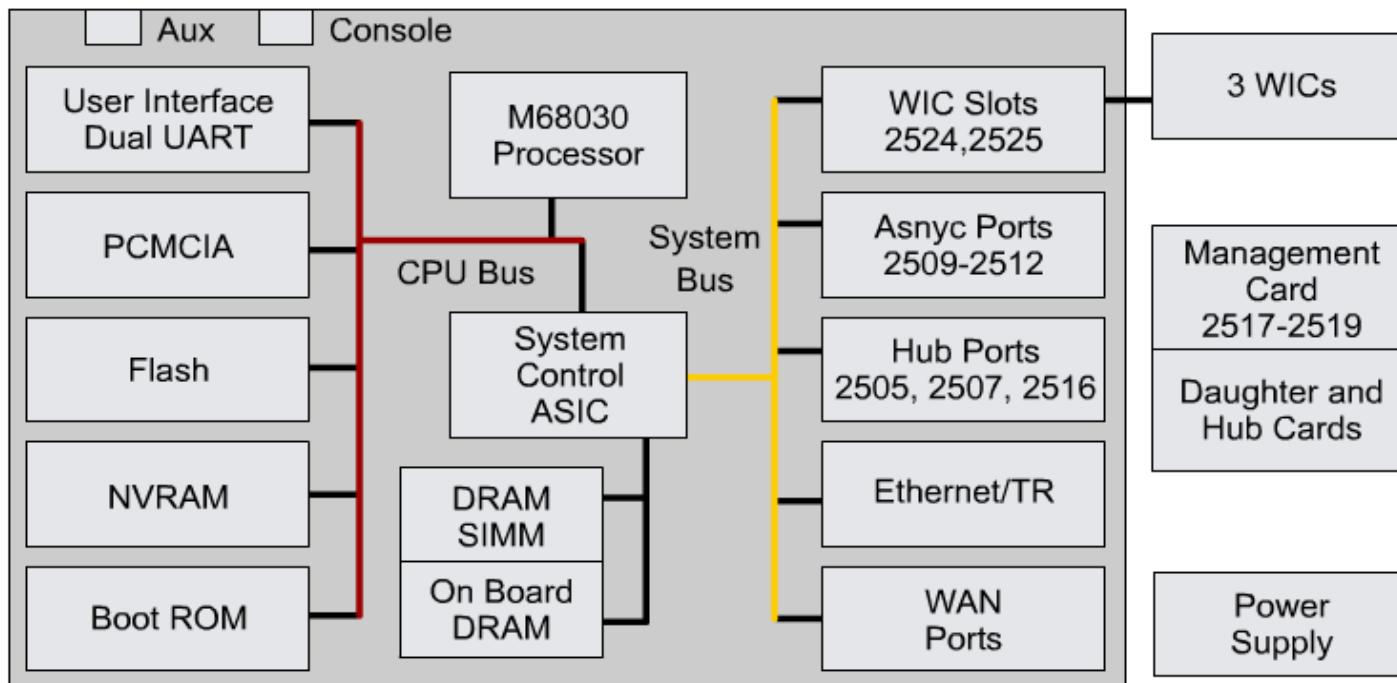
Recommended Books



Lecture 1

Overview of Configuration of Network Devices

Network Devices – Internal Components



- CPU
- RAM
- Flash
- NVRAM

- Buses
- ROM
- Interfaces
- Power Supply

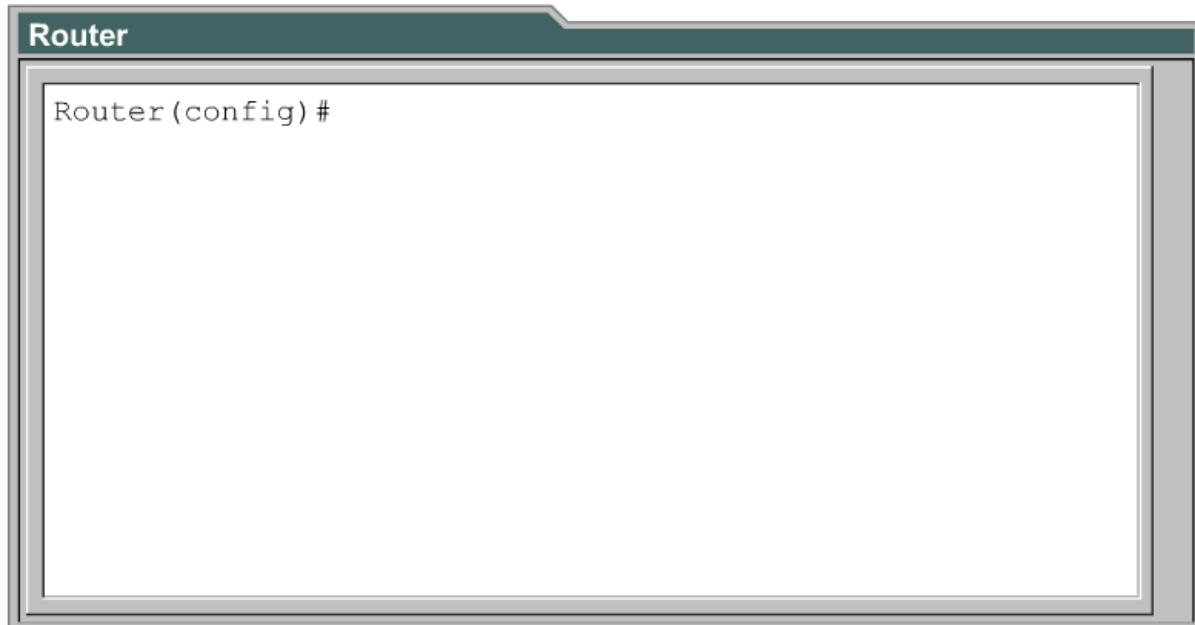
Cisco IOS Software

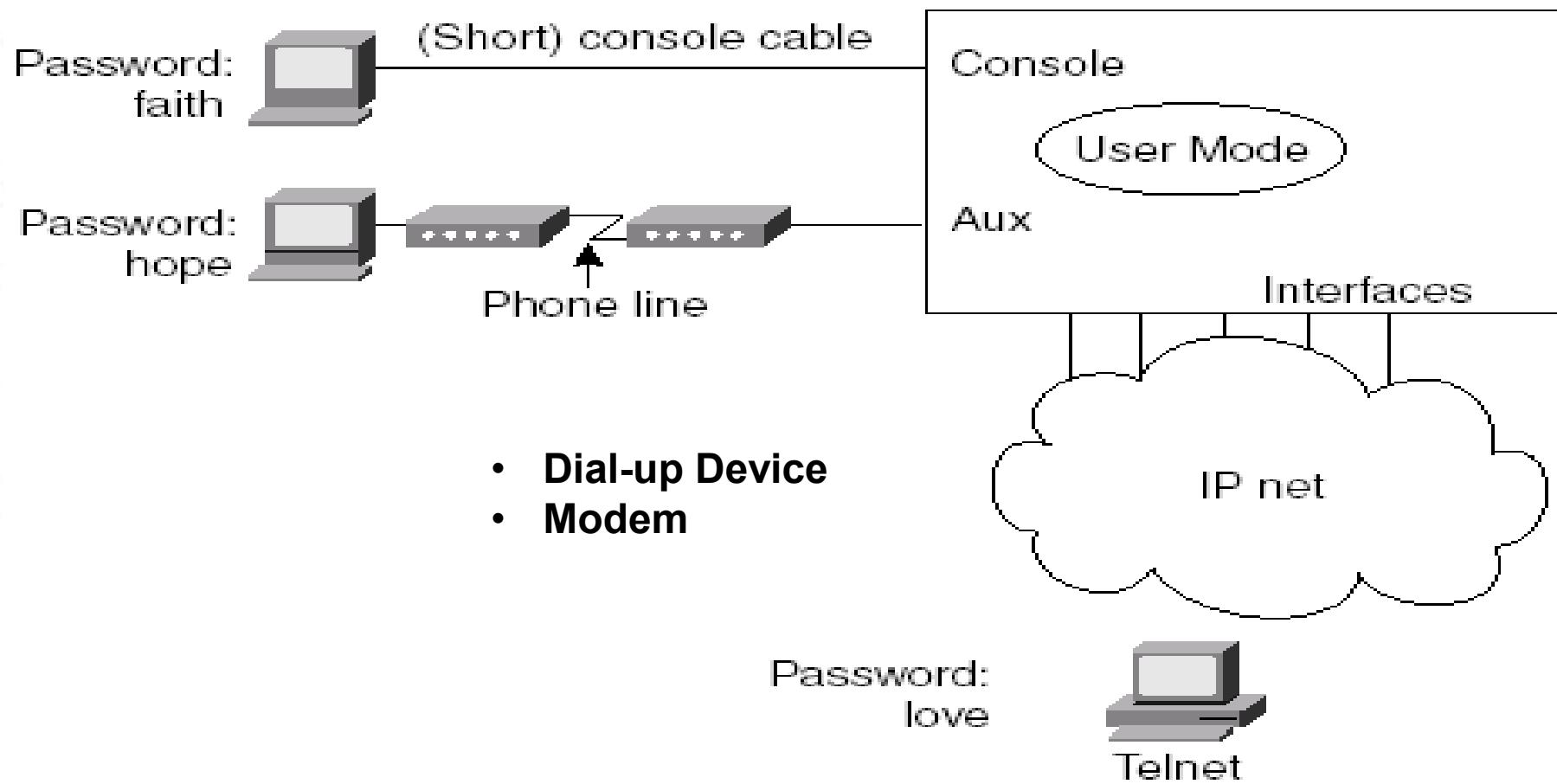


- As with a computer, a network device cannot function without an operating system.
- Cisco calls its OS as the **Cisco Internetwork Operating System** or **Cisco IOS**.

Command Line Interface (CLI)

- The Cisco IOS software uses a command-line interface (CLI) as the traditional console environment.
- This environment is accessible through several connection methods:
 - Console
 - AUX port
 - Telnet

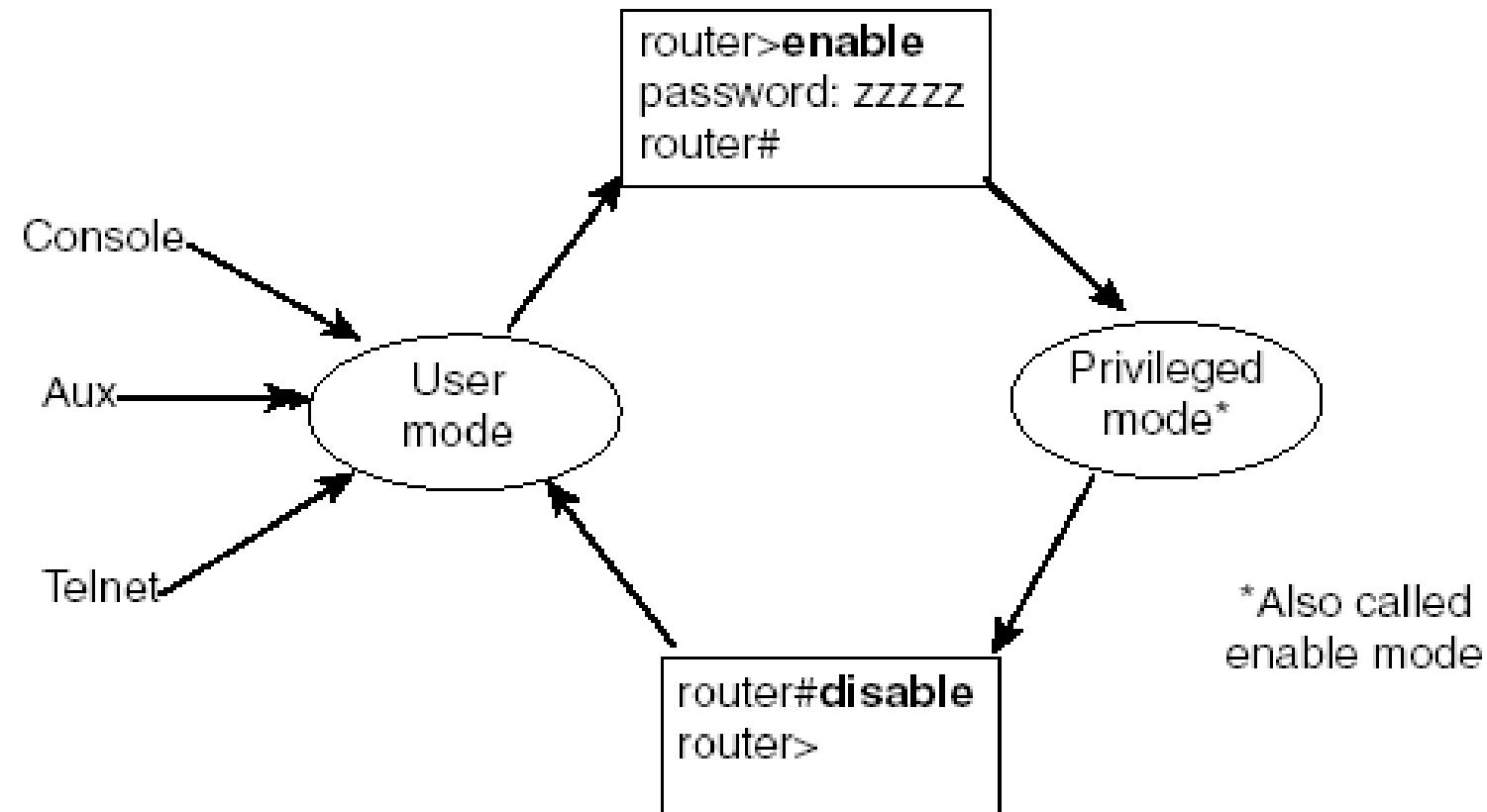




User Level Passwords

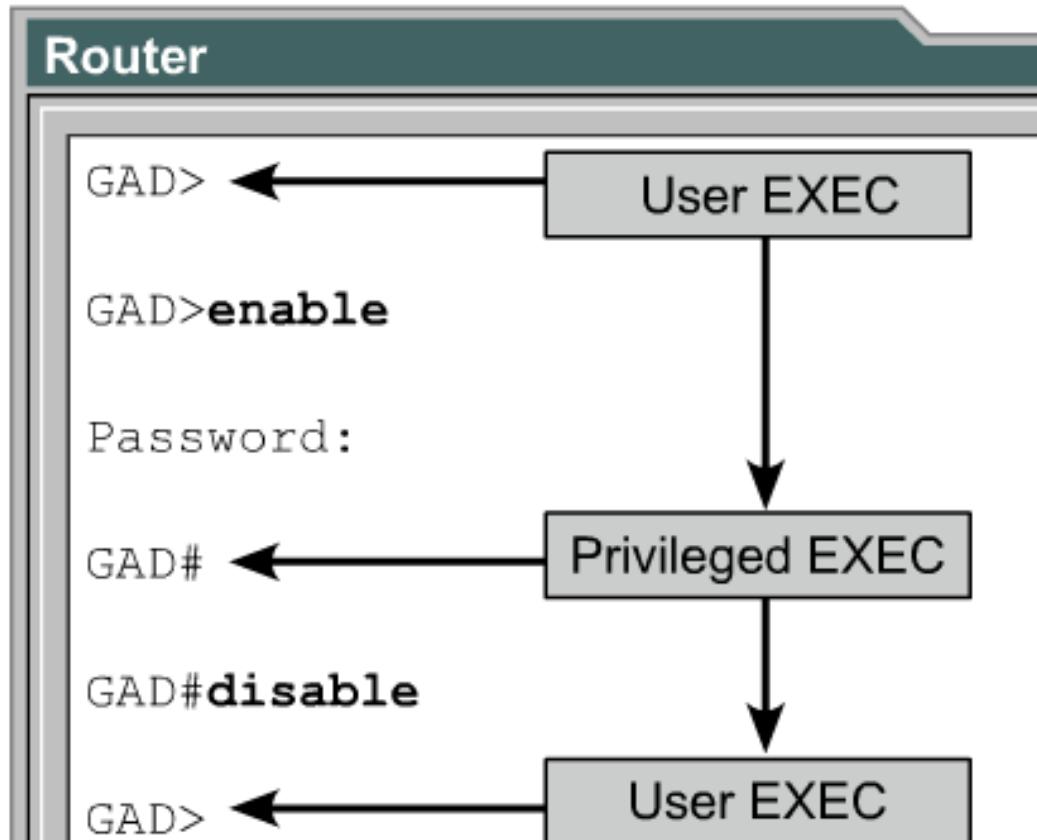
Access from ...	Password Type	Configuration
Console	Console password	line console 0 login password <i>faith</i>
Auxiliary	Auxiliary password	line aux 0 login password <i>hope</i>
Telnet	vty password	line vty 0 4 login password <i>love</i>

Router Modes

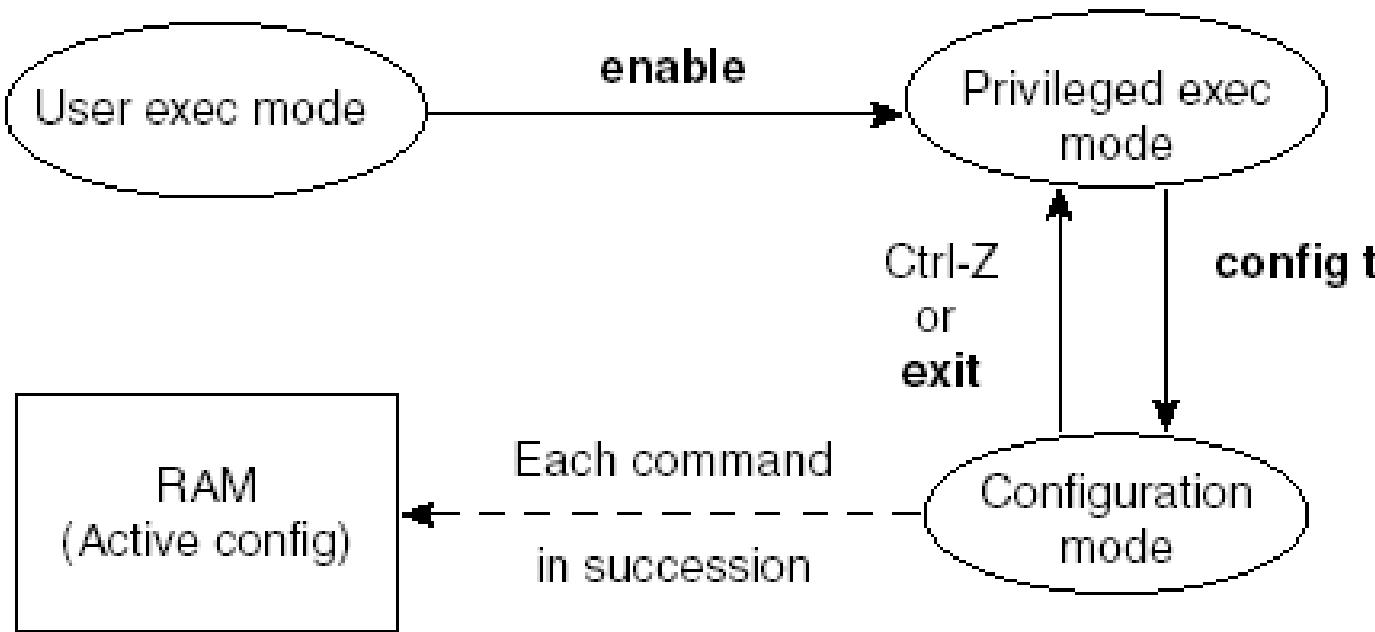


Router Modes

EXEC Mode	Prompt	Typical Use
User	GAD>	check the router status
Privileged	GAD#	accessing the router configuration modes
...



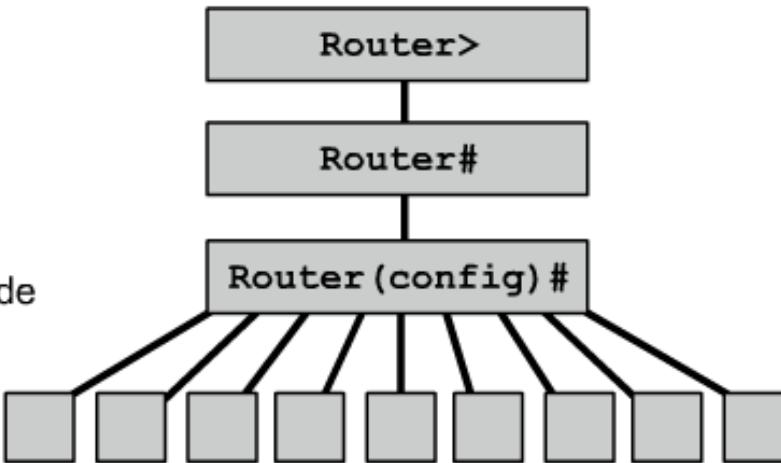
Router Modes



```
Router>
Router>enable
Router#
Router#configure terminal
Router(config)#hostname AtlantaHQ
AtlantaHQ(config)#
...
```

Router Modes

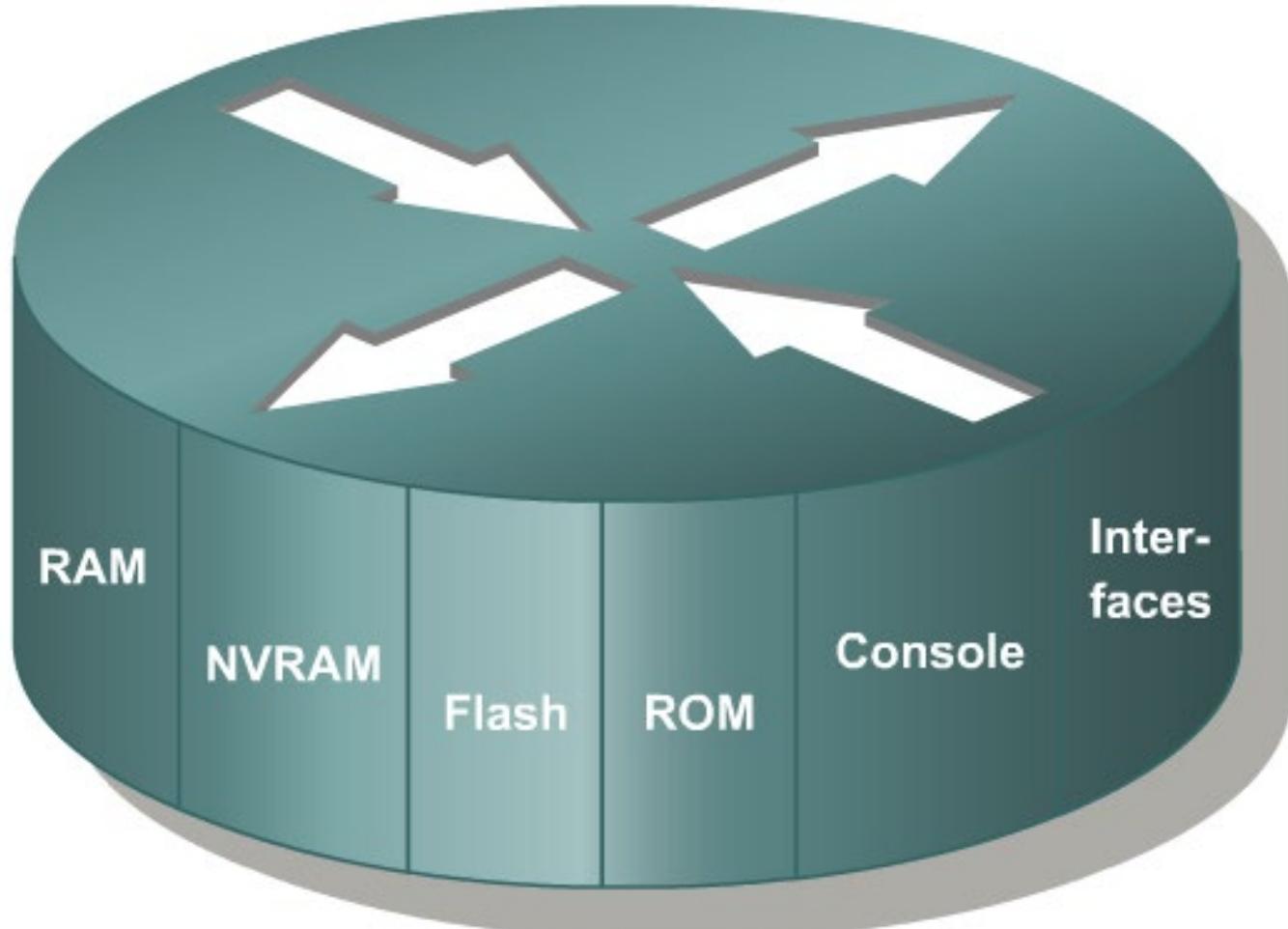
- User EXEC mode
- Privileged EXEC mode
- Global configuration mode
- Specific configuration modes
- • •
- • •
- • •
- • •
- • •



* *
* *
* *
* *

Configuration Mode	Prompt
Interface	Router (config-if)#
Subinterface	Router (config-subif)#
Controller	Router (config-controller)#
Map-list	Router (config-map-list)#
Map-class	Router (config-map-class)#
Line	Router (config-line)#
Router	Router (config-router)#
IPX-router	Router (config-ipx-router)#
Route-map	Router (config-route-map)#

Router Memory



Router Memory cont.

❖ RAM

- Store *running or active configuration* file
- Loses content when router is powered down
- A working storage

⋮ ⋮
⋮ ⋮
⋮ ⋮
⋮ ⋮
⋮ ⋮
⋮ ⋮
⋮ ⋮
⋮ ⋮

❖ ROM

- Read-Only Memory
- Stores **bootable IOS image and bootstrap program**

Router Memory cont.

❖ NVRAM

- Provides storage for the **startup configuration file**
- Retains content when router is powered down

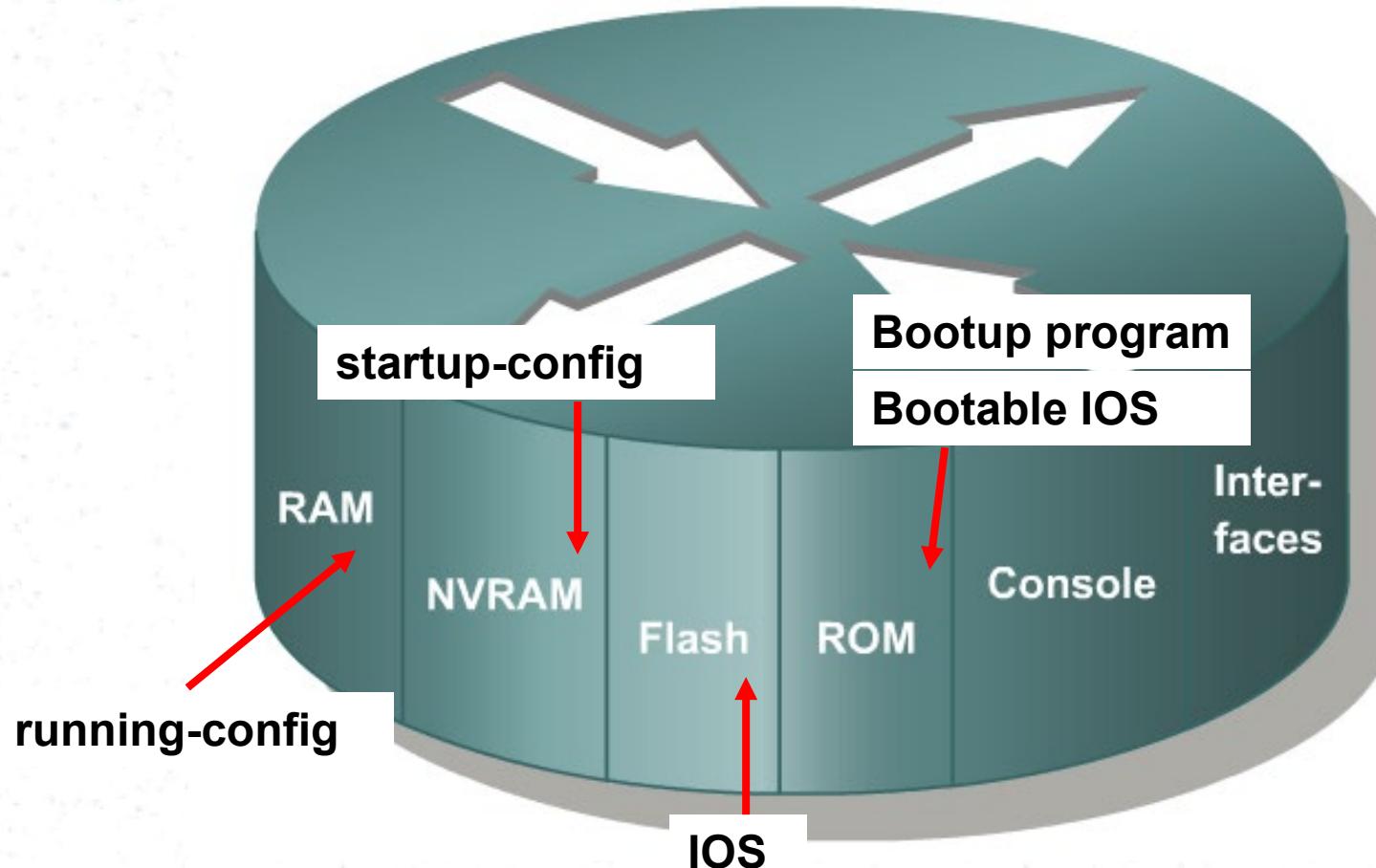
⋮
⋮
⋮
⋮
⋮

❖ Flash memory

- Holds the **fully functional IOS image**
- Retains content when router is powered down
- Is a type of electronically erasable, programmable ROM (EEPROM)

⋮
⋮
⋮
⋮
⋮

Router Memory cont.



Displaying configuration files

`show running-config`

Command Output

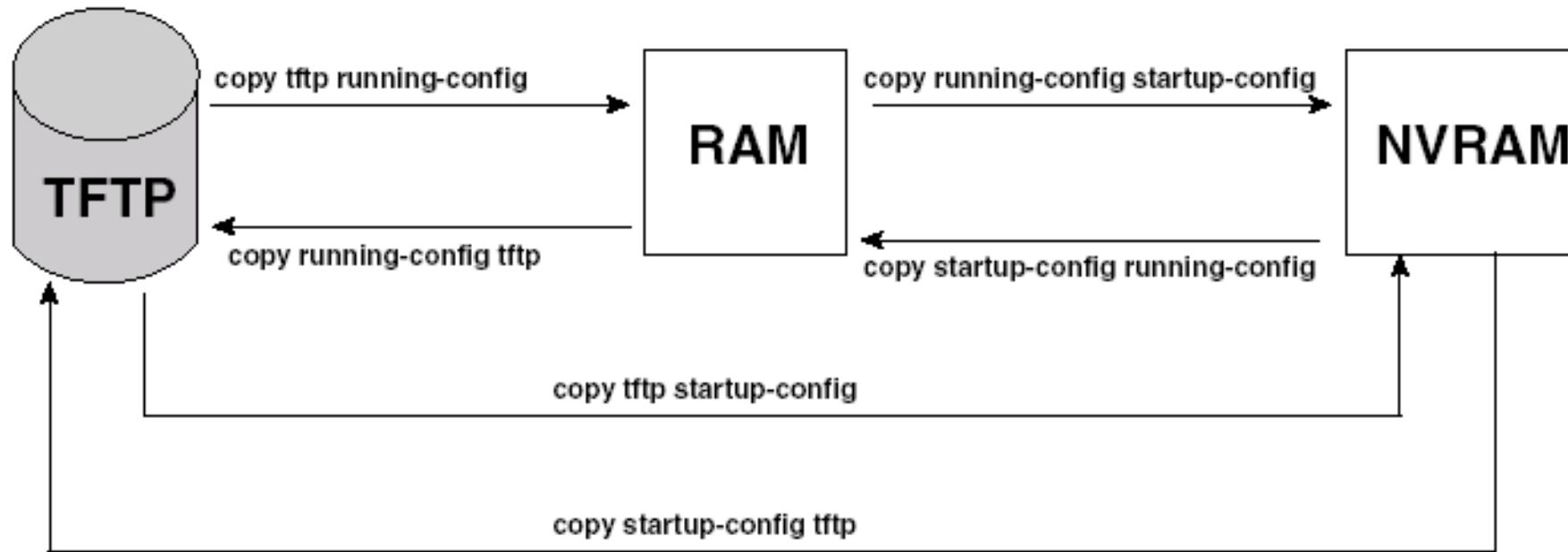
```
Router#show running-config
Building configuration...
.
.
.
Current configuration:
!
version 11.1
!
-- More --
```

`show startup-config`

Command Output

```
Router#show startup-config
Using 1108 out of 130048 bytes
!
version 11.2
!
hostname router
.
.
.
-- More --
```

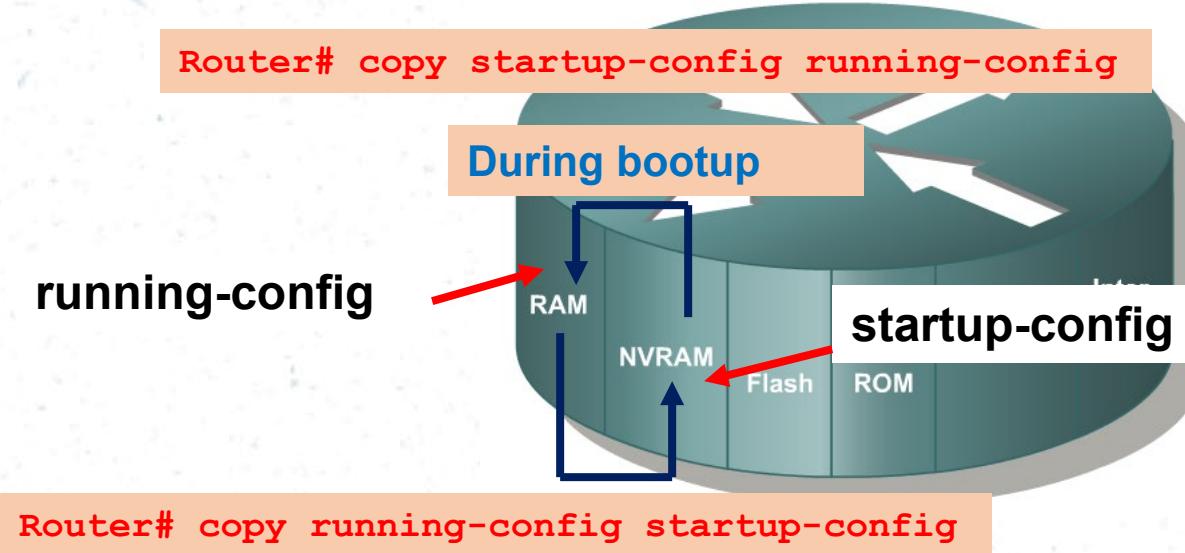
Managing configuration files



Copy Command

- copy files in a router (configuration file, new version of the IOS Software)
- Move configuration files among RAM, NVRAM, and TFTP server

copy running-config startup-config



- Changes to the router are put in the running-config file.
- If the router loses power or reboots, everything in RAM is lost including the running-config file.
- To make sure the changes to the router's configuration remain saved, you must copy the running-config from RAM into the startup-config into NVRAM:

Router# copy running-config startup-config

copy running-config startup-config cont.

```
Router#copy running-config startup-config
```

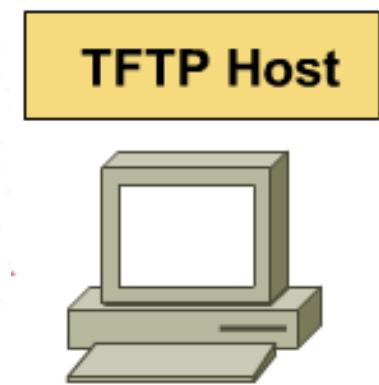
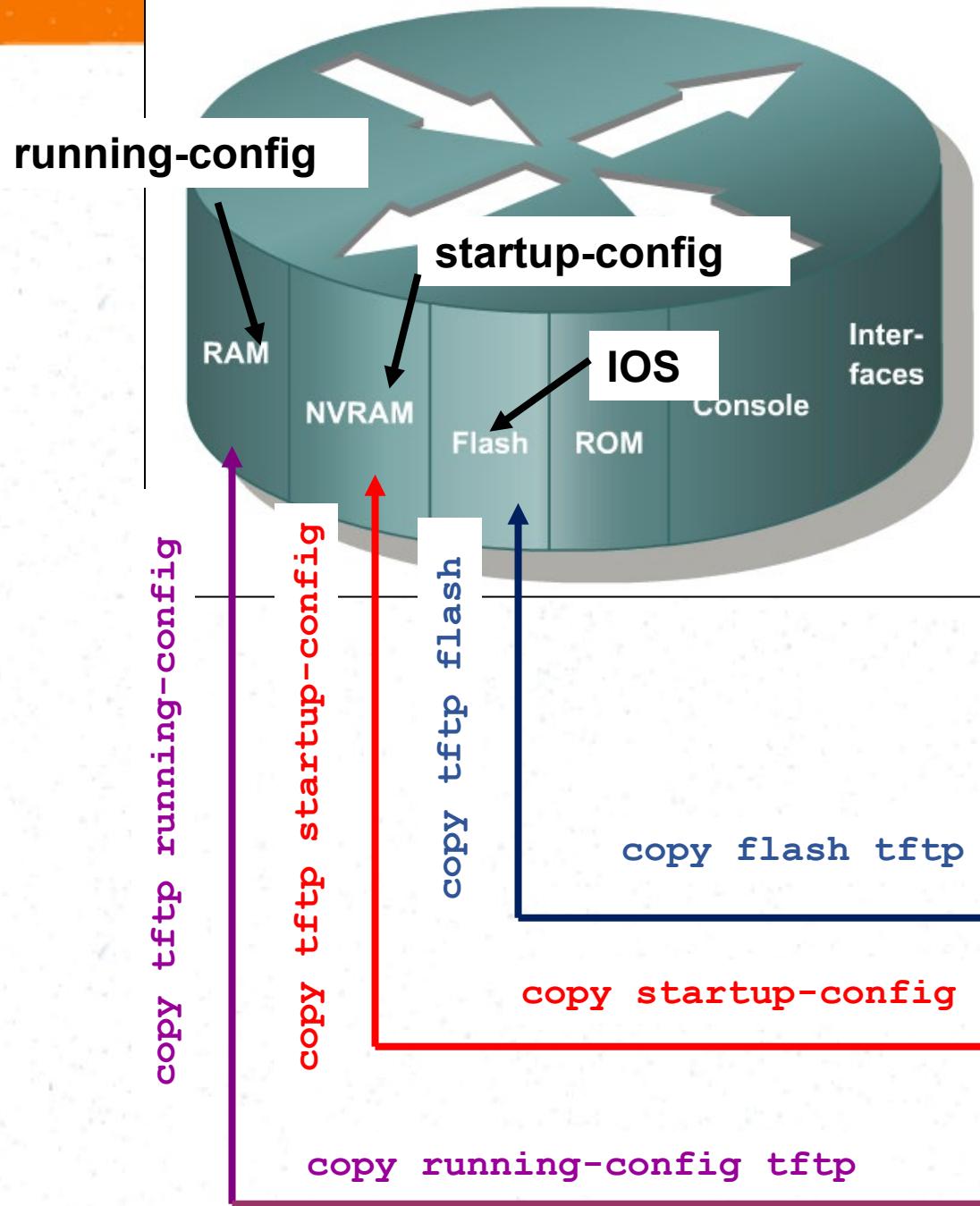
```
Destination filename [startup-config]?
```

```
Building configuration...
```

```
Router#show startup-config
```

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router
!
!
ip subnet-zero
!
interface Ethernet0
  no ip address
  no ip directed-broadcast
  shutdown
!
```

The startup-config file now identical to running-config and the router will also have these changes if the router reboots.



Router

```
Router#copy running-config tftp  
Remote host []? 131.108.2.155  
Name of configuration file to write[tokyo-config]?tokyo.2  
Write file tokyo.2 to 131.108.2.155? [confirm] y  
Writing tokyo.2 !!!!! [OK]
```

Router

```
Router#copy tftp running-config  
Host or network configuration file [host]?  
IP address of remote host [255.255.255.255]? 131.108.2.155  
Name of configuration file [Router-config]? tokyo.2  
Configure using tokyo.2 from 131.108.2.155? [confirm] y  
Booting tokyo.2 from 131.108.2.155:!! [OK-874/16000 bytes]
```



SLIIT

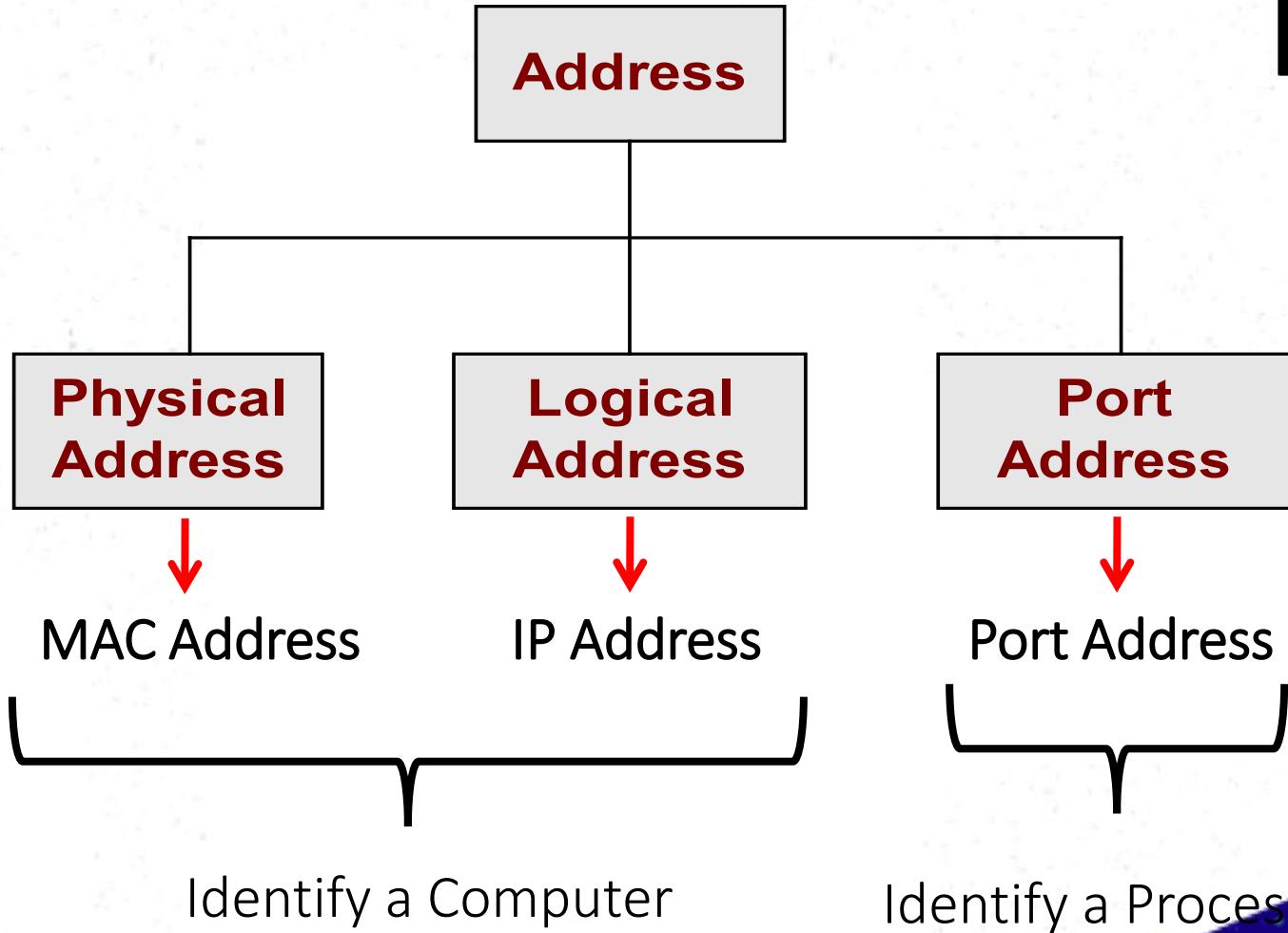
Discover Your Future

IT1020 - COMPUTER NETWORKS

Lecture 2

IP Addressing

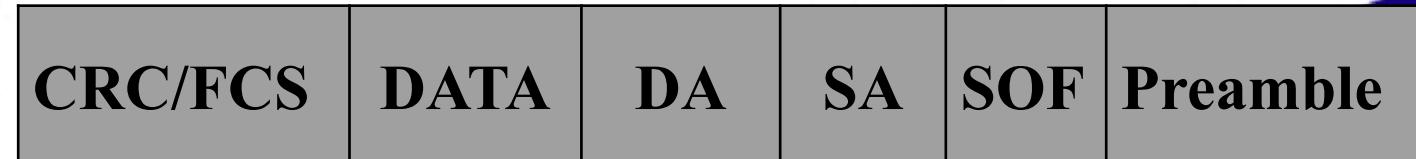
Addressing with TCP/IP



Physical Address

- Stored in the Network Interface Card (NIC)
- A hardware setting set by the manufacturer of NIC .
- Unchangeable
 - Ex :- *MAC address*
- For Ethernet, the MAC address is a 48 bit or 12 Hex number
 - Ex : 5A:B3:87:F1:93:7C
 - 5A-B3-87-F1-93-7C
- MAC address operates in the Data Link Layer (Layer 2)

Ethernet Frame



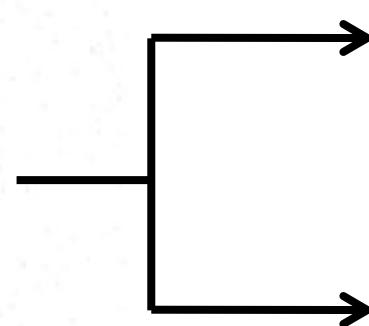
Logical Address

- Address scheme depends on the used protocol
- Widely used protocol is TCP/IP
 - Ex :- IP Address
 - 192.168.16.53
 - 10.39.40.3
- Logical address operates at the Network Layer (Layer 3)

IP Address

- Uniquely identifies devices

- IP Addresses



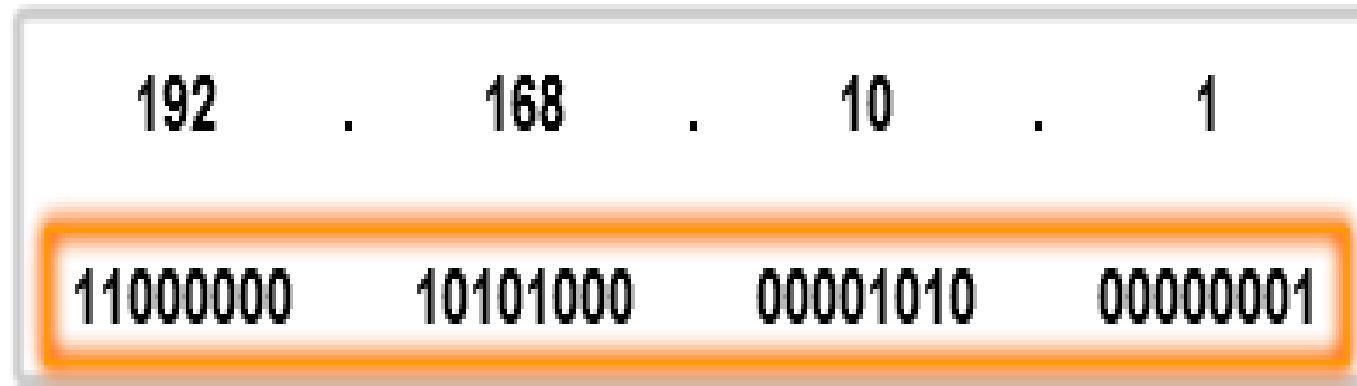
IP Version 4 (IPV4)
32 bit scheme

IP Version 6 (IPV6) (IPng)
128 bit scheme

IP Version 4 (IPV4)

- The 32 bits are represented in following manner.

Byte 1. Byte 2. Byte 3. Byte 4
(1 byte = 8 bits)



32-Bit Address

IP Version 4 (IPV4) cont.

192	.	168	.	10	.	1
11000000	10101000	00001010	00000001			

Dotted Decimal Address

IP Version 4 (IPV4) cont.

- The minimum value of a byte

00000000 = 0

- The maximum value of a byte

11111111 = 255

- The minimum IP Address

0.0.0.0

- The maximum IP Address

255.255.255.255

Network ID and Host ID

- IP Addresses → Network ID + Host ID

Classes of IP addresses

Class	Net ID	Host ID
A	1 Byte	3 Bytes
B	2 Bytes	2 Bytes
C	3 Bytes	1 Byte



Network

IPv4 Address Classes

Class A	Network	Host		
Octet	1	2	3	4

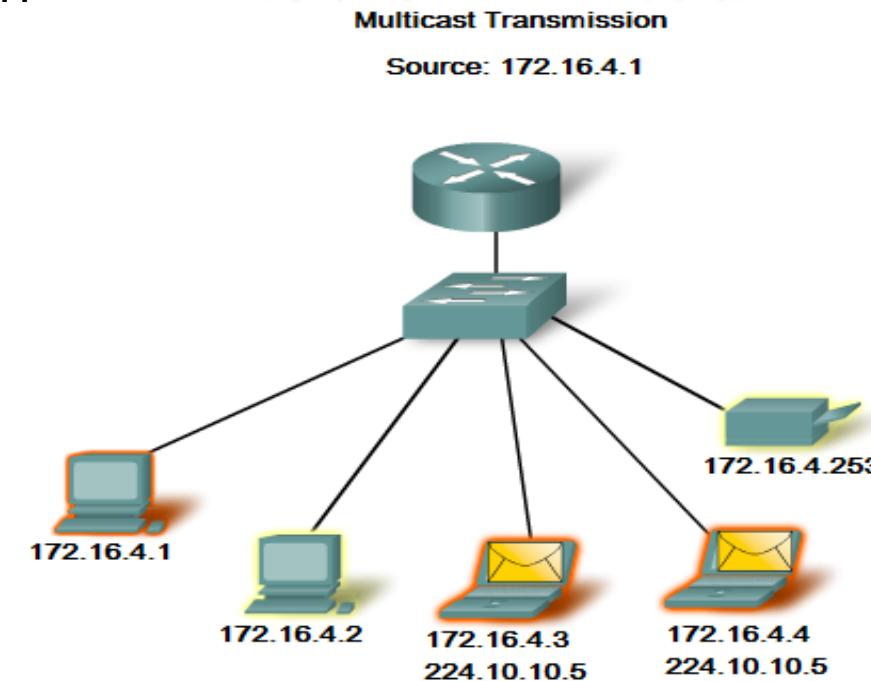
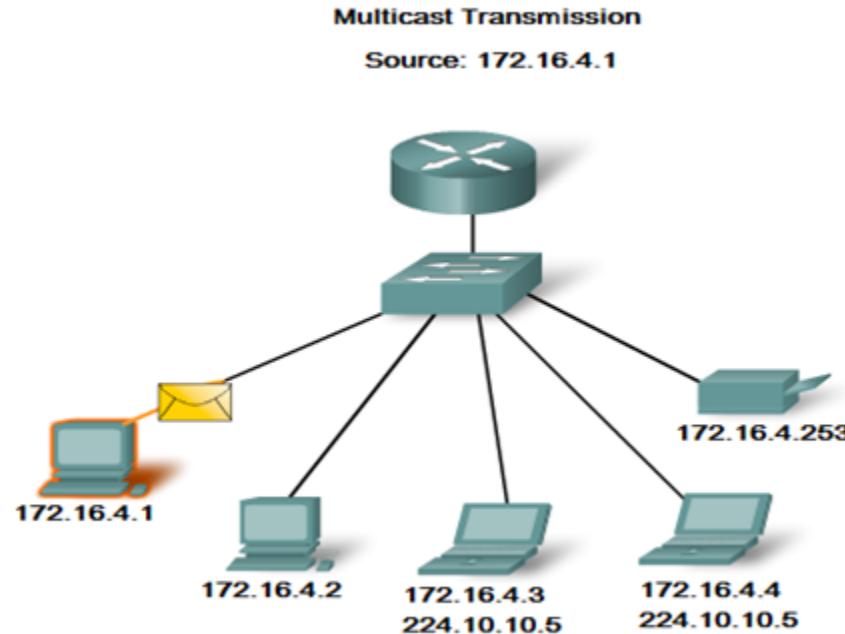
Class B	Network		Host	
Octet	1	2	3	4

Class C	Network			Host
Octet	1	2	3	4

Class D	Host			
Octet	1	2	3	4

Classes of IP addresses cont.

- Class D is introduced for Multicasting



- Class E is reserved

Classes of IP addresses cont.

Class D Addresses

- A Class D address begins with binary 1110 in the first octet.
- First octet range 224 to 239.
- Class D address can be used to represent a group of hosts called a host group, or multicast group.
-
-
-
-

Class E Addresses

- First octet of an IP address begins with 1111
- Class E addresses are reserved for experimental purposes and should not be used for addressing hosts or multicast groups.

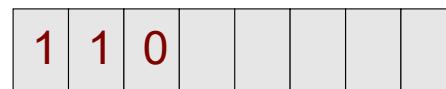
Class A byte 1



Class B byte 1



Class C byte 1



Class	Minimum Network ID	Maximum Networks ID
A	0 0000000 0	0 1111111 127
B	10 000000.00000000 128.0	10 111111.11111111 191.255
C	110 00000.00000000.00000000 192.0.0	110 11111.11111111.11111111 223.255.255

- Class A – 2^7
- Class B – 2^{14}
- Class C – 2^{21}

Address Class	First Octet Range	Number of Possible Networks	Number of Hosts per Network
Class A	0 to 127	128 (2 are reserved)	16,777,214
Class B	128 to 191	16,348	65,534
Class C	192 to 223	2,097,152	254

Network Address and Broadcast Address

- For the Network Address, the Host ID part of the IP Address will be considered as All 0s
- For the Broadcast Address, the Host ID part of the IP Address will be considered as All 1

Ex : 103.58.35.1

This is a Class A address

Net ID is = 103

Host ID is = 58.35.1

Network Address → 103.0.0.0

Broadcast Address → 103.255.255.255

198

.

8

.

0

.

1

Class C

1100 0110 . 0000 1000 . 0000 0000 . 0000 0001

Network ID : 3 bytes (24 bits)

Host ID : 1 byte (8 bits)

- Both in Network ID and Host ID all 0s and all 1s are reserved for special purposes.

The actual maximum no. of Hosts per Network

$$=2^8 - 2 = 254$$

- Network Address :

1100 0110 . 0000 1000 . 0000 0000 . 0000 0000 (198.8.0.0)

- Broadcast Address :

1100 0110 . 0000 1000 . 0000 0000 . 1111 1111 (198.8.0.255)

Classful Addressing - Subnet Mask

<i>Class</i>	<i>Mask in binary</i>	<i>Mask in dotted-decimal</i>
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

Net ID part : All 1's

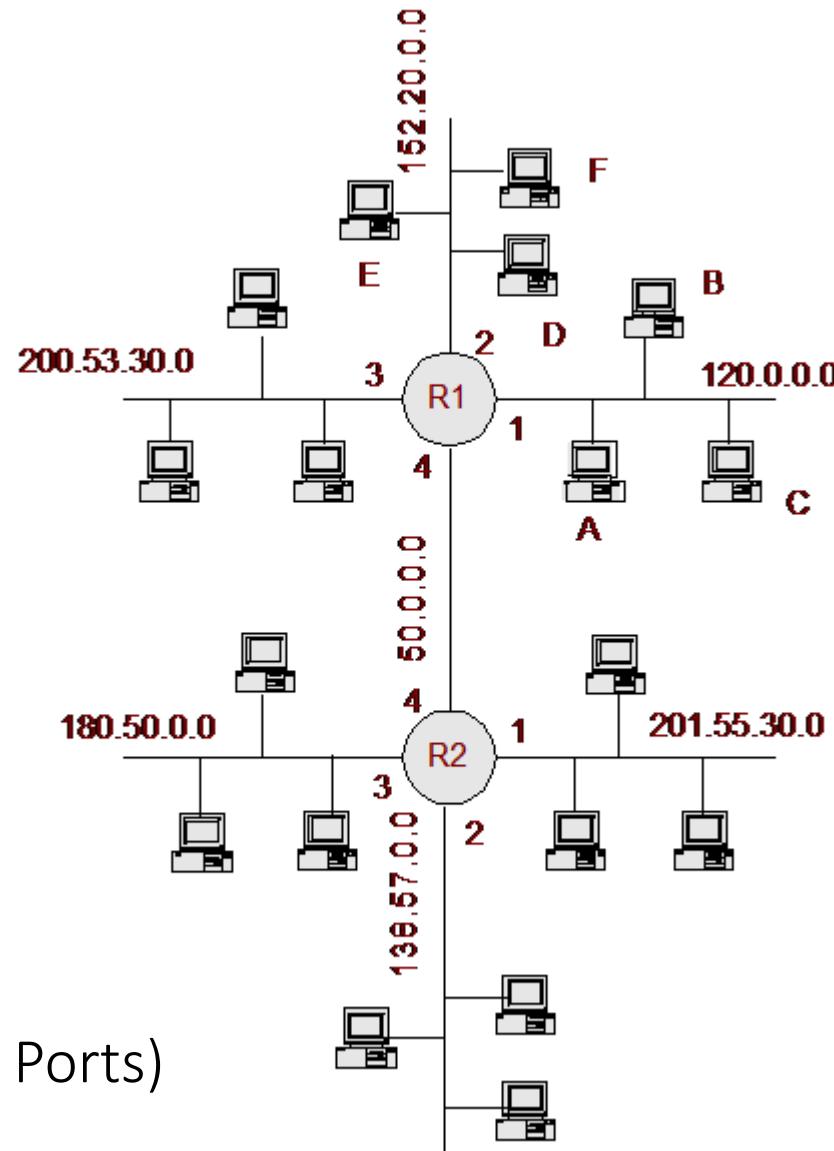
Host ID part : All 0's

Exercise

IP Address	Class	Subnet Mask	Actual No.of hosts	Network Address	Broadcast Address
140.35.45.55					
50.60.70.5					
201.35.40.201					
125.38.55.185					
193.201.55.105					
127.53.35.10					

IP address of a Router

Host/Port	IP Address
A	120.0.0.1
B	120.0.0.2
C	120.0.0.3
Port 1 R1	120.0.0.50
D	150.20.0.1
E	150.20.0.2
F	150.20.0.3
Port 2 R1	150.20.0.50
Port 3 R1	200.53.30.50
Port 4 R1	50.0.0.1
Port 4 R2	50.0.0.2
Port 1 R2	201.55.30.50
Port 2 R2	138.57.0.50
Port 3 R2	180.50.0.50

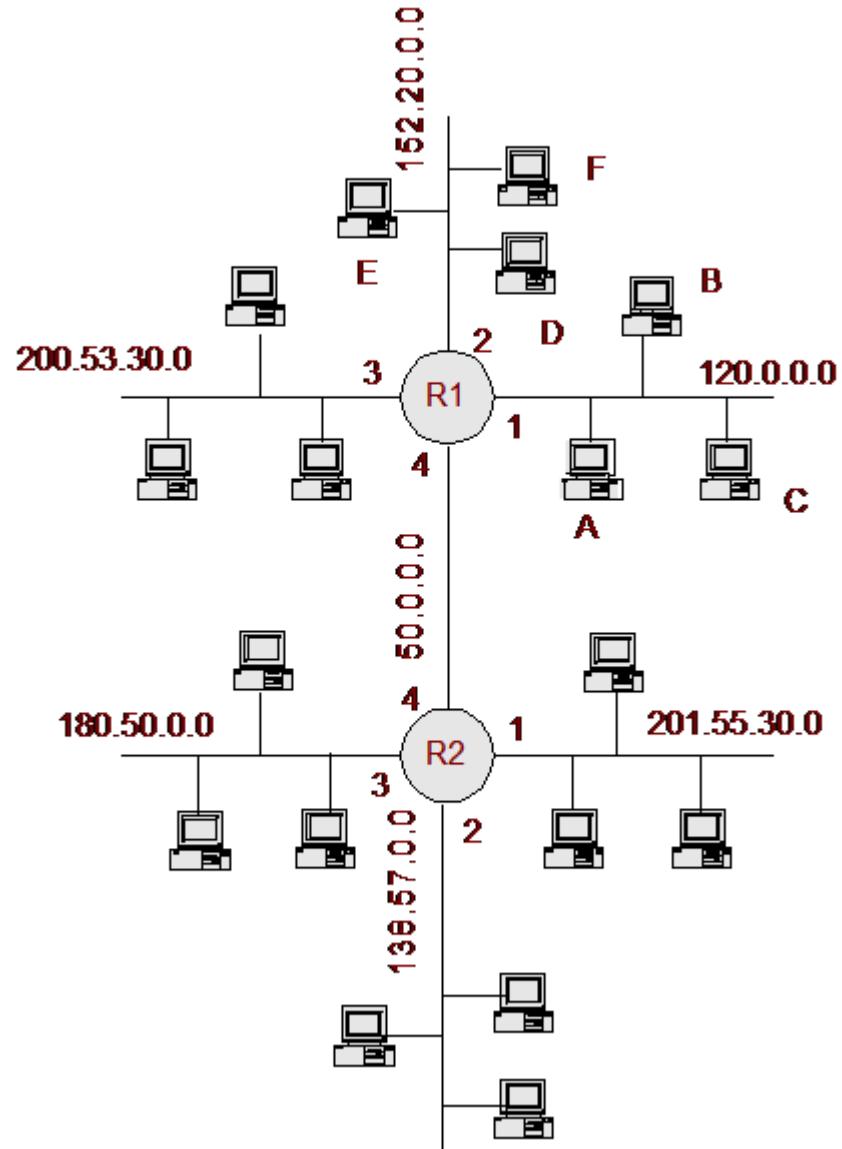


- A router has many ports. (LAN and WAN Ports)
- An IP address is assigned to each port.

Default Gateway IP Address

Network Address	Gateway IP Address
120.0.0.0	120.0.0.50
152.20.0.0	152.20.0.50
200.53.30.0	200.53.30.50
201.55.30.0	201.55.30.50
138.57.0.0	138.57.0.50
180.50.0.0	180.50.0.50

The IP address of router port which is connected to a particular LAN is called the “Gateway IP Address” of the LAN



Public IP Addresses

- **A public IP address is any valid address that can be accessed over the Internet**
- The Internet is a Public Computer Network which is spread all over the world.
- Allocations of IP addresses are controlled by the Internet Assigned Number Authority (IANA) which responsible for the IP address ranges allocation to different countries.
- CINTEC assigns different range of IP address to different Internet Service Providers (ISPs)
- The ISPs allocate IP addresses to their customers
- Sri Lanka Telecom(SLT) provides allocates 8 IP addresses for each 64 kb/s leased line.

Private IP Addresses

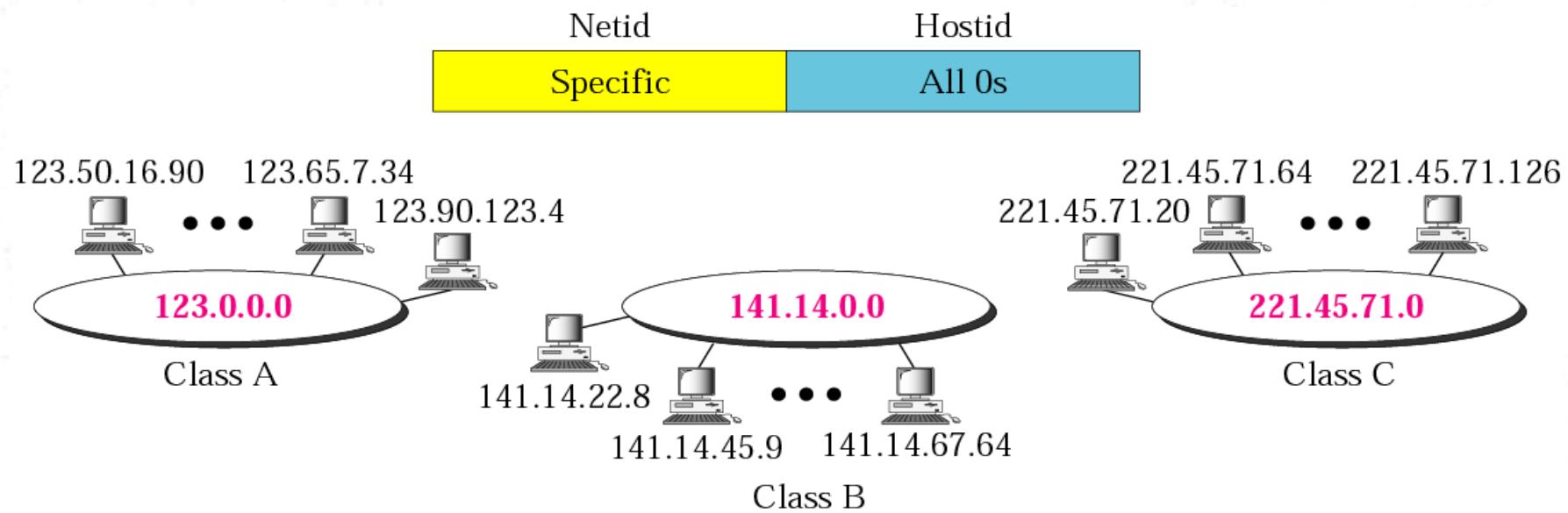
- A private IP address is address assigned to a device on a private LAN that is accessible only within the LAN.
- A network which is not connected to Internet can use any IP address range without obtaining any permission
- It is not advisable to use any IP address since the network may connect to Internet in the future
- To avoid such problems, IANA has reserved some IP address ranges for private use

Class	Private Network Address	No.of Networks
A	10.0.0.0	1
B	172.16.0.0 to 172.31.0.0	16
C	192.168.0.0 to 192.168.255.0	256

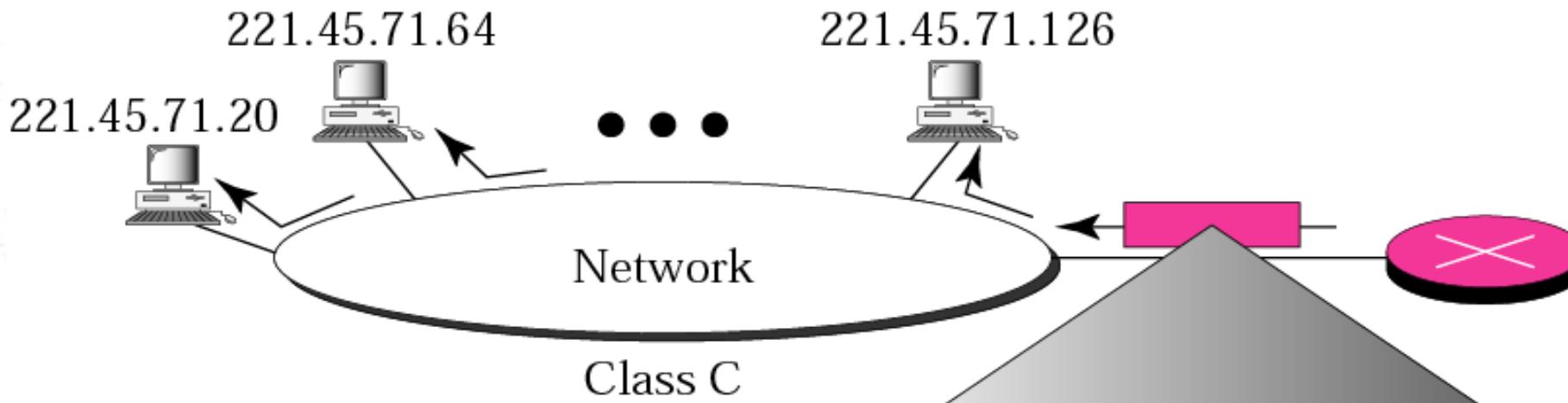
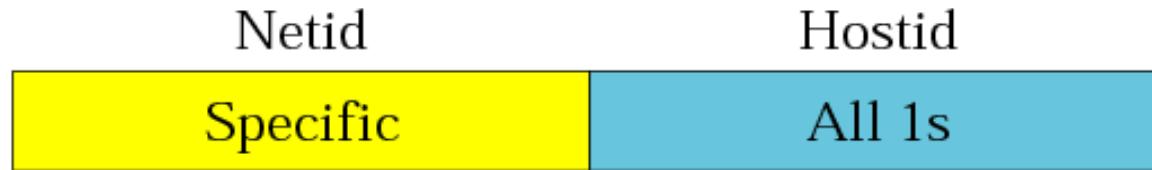
IP special addresses

	Net ID	Host ID	Remarks
Network Address	Specific	All 0's	None
Direct Broadcast Address	Specific	All 1's	Destination Address
Limited Broadcast Address	All 1's	All 1's	Destination Address
This Host on this Network	All 0's	All 0's	Source Address
Specific host on this network	All 0's	Specific	Destination Address
Loopback Address	127	Any	Destination Address

Network Address



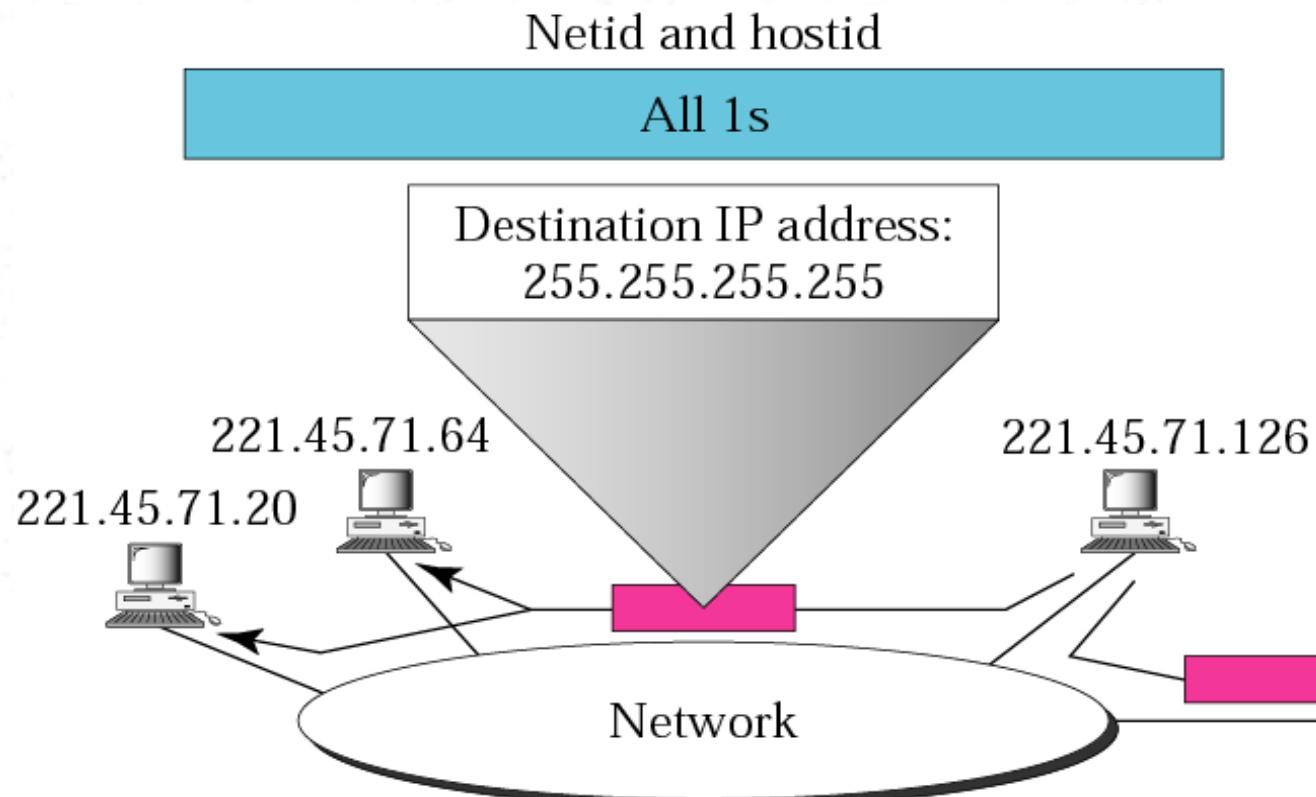
Direct Broadcast Address



The direct broadcast address is used by a router to send a message to every host on a local network. Every host/router receives and processes the packet with a direct broadcast address.

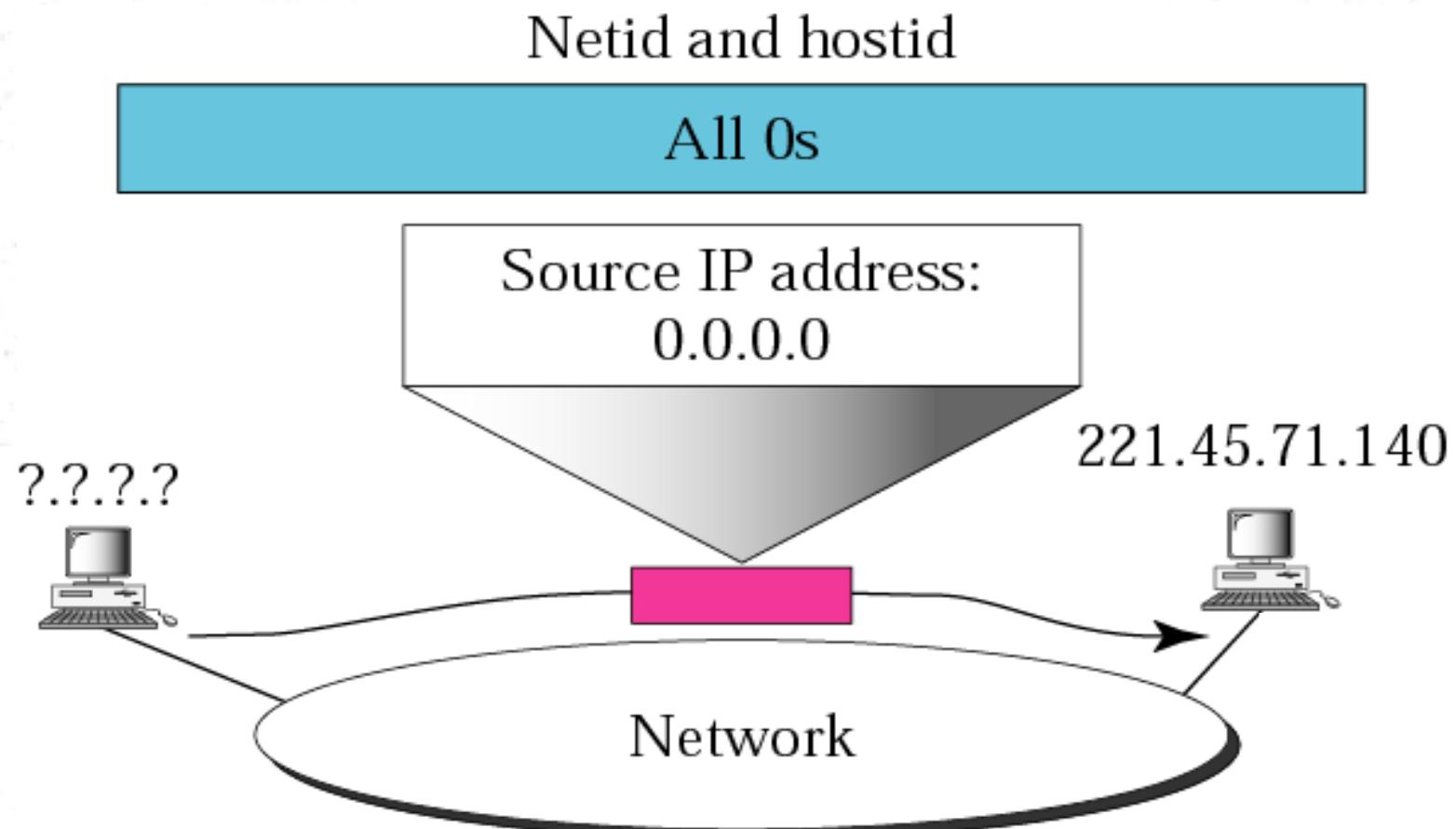
Destination IP address:
221.45.71.255
Hostid: 255

Limited Broadcast Address

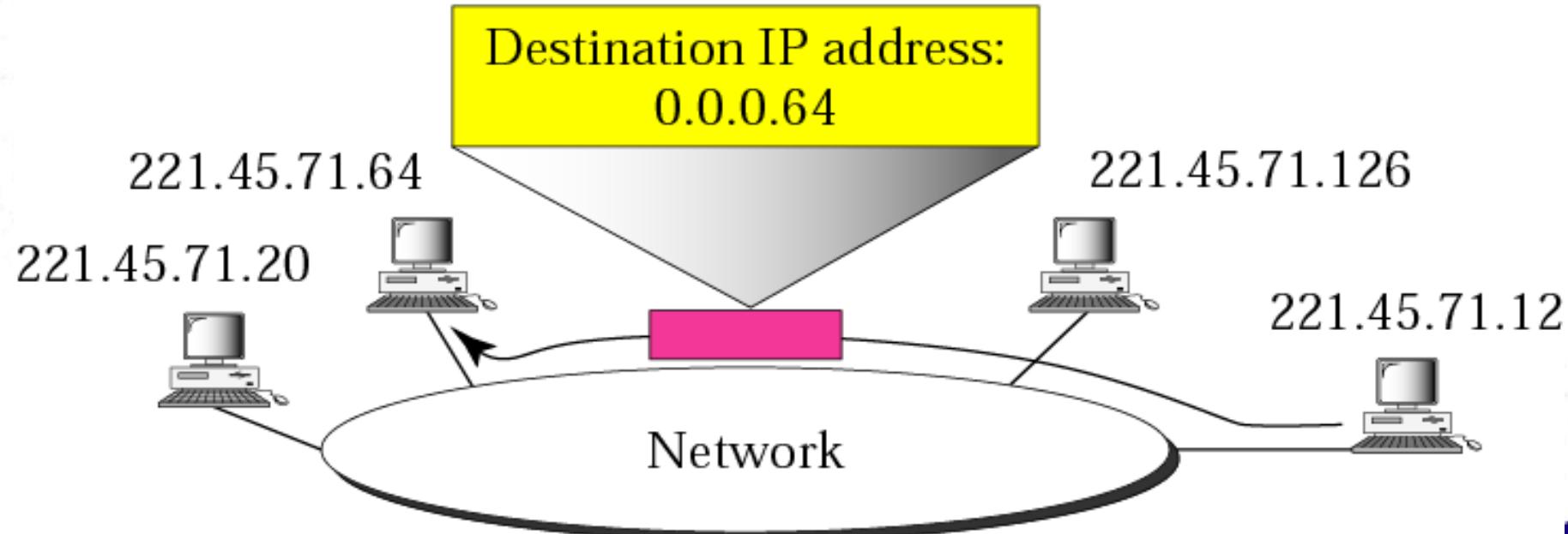
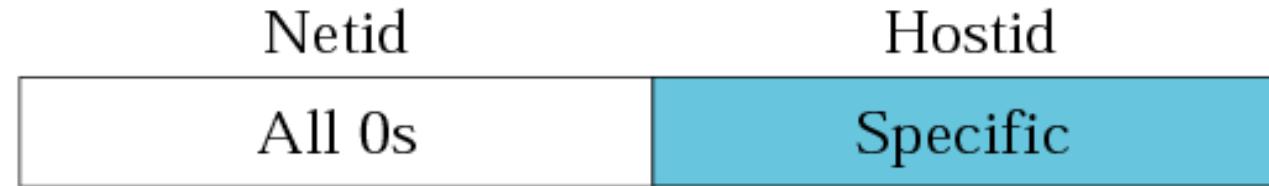


A limited broadcast address is used by a host to send a packet to every host on the same network. However, the packet is blocked by routers to confine the packet to the local network.

This host on this network

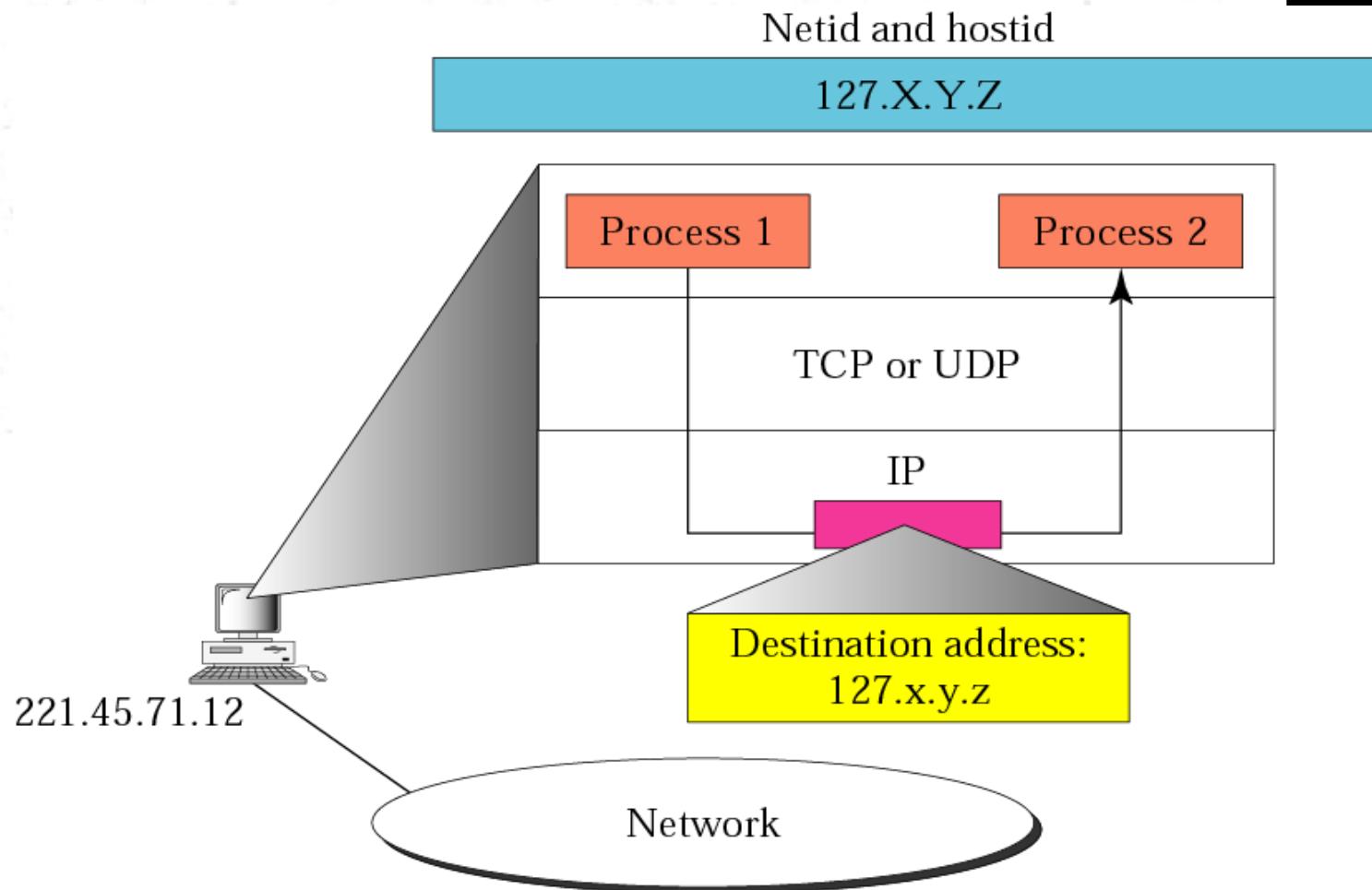


Specific host on this network



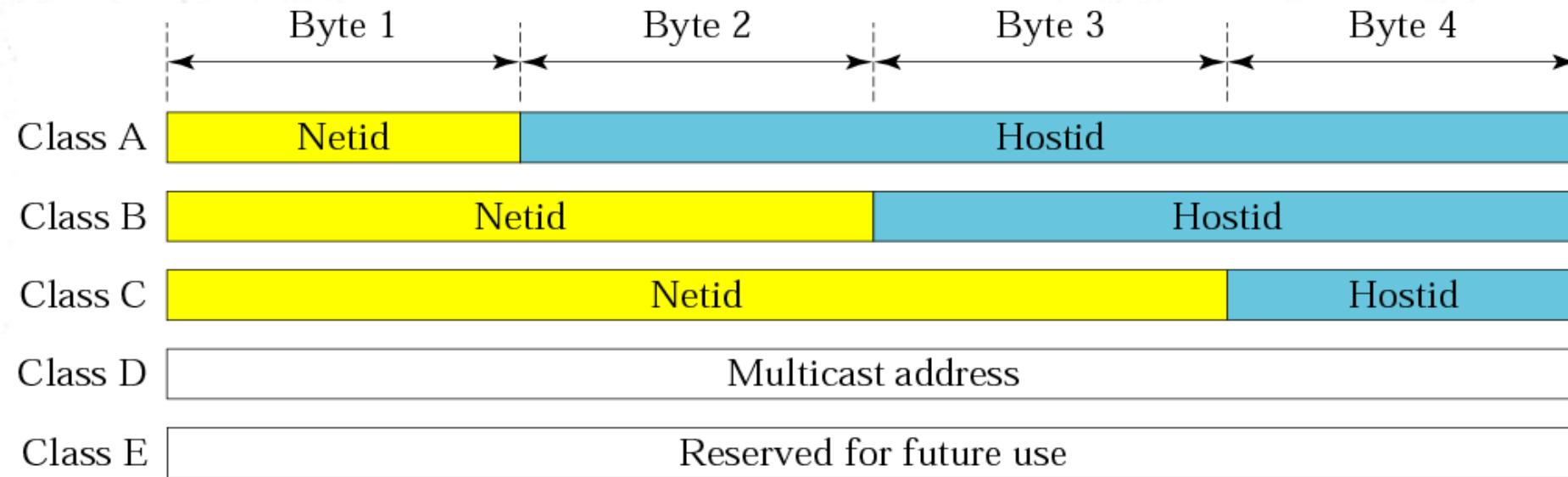
This address is used by a router or host to send a message to a specific host on the same network.

Loopback address

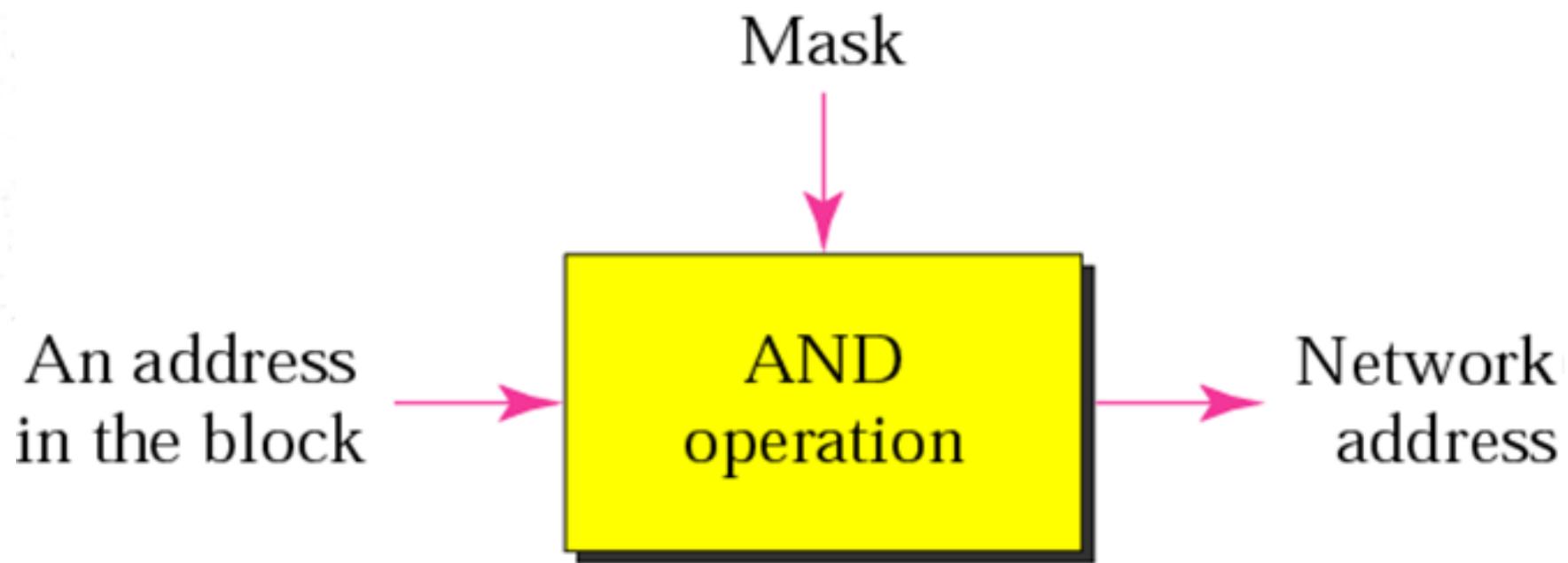


A packet with a loopback address
will not reach the network.

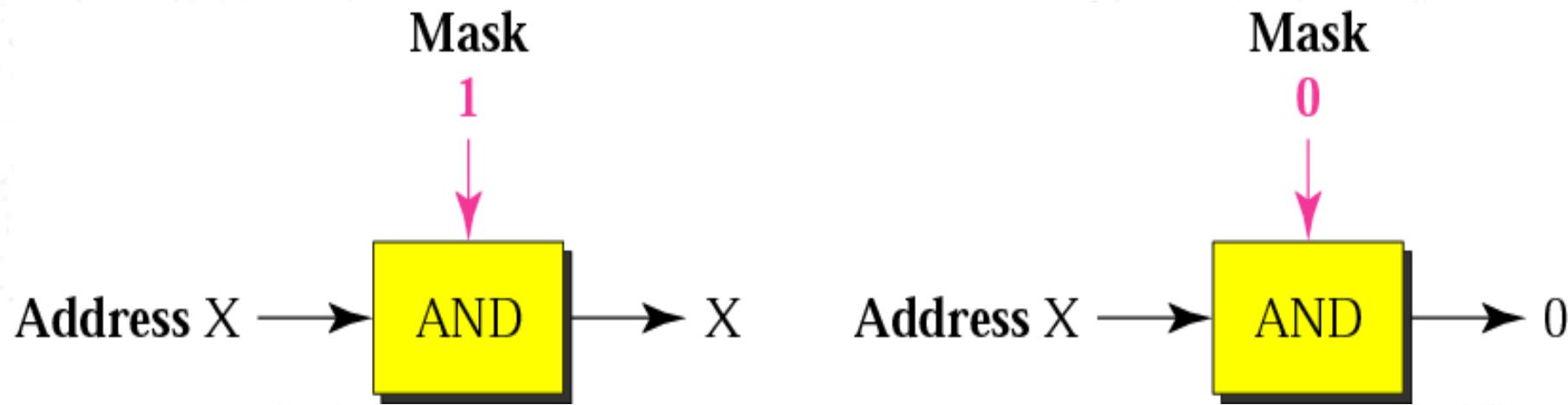
Classful Addressing



Masking Concept



AND Operation



Subnetting – Classless Addressing

- Suppose you are given a network address 150.100.0.0 /16 for your network.
10010110.01100100.00000000.00000000
- You have the computers of Finance, Production and Administration Sections. In order to enhance the efficiency of network you want divide this into three networks. But you cannot get another two network addresses. This requirement can be satisfied from the same network address by using the subnet concept.

- Now the IP address is divided into three parts.

Net ID Subnet ID Host ID

Classless Addressing cont

- The original Net ID bits not changed.
- Part of Host ID is allocated for “Subnet ID”.
- Most significant bits allocated as Subnet ID.

XXXX XXXX. XXXX XXXX.. **XXXX XXXX. XXXX XXXX**

Net ID Subnet ID Host ID

Classless Addressing cont.

- subnets can be written as

Subnet 0 10010110.01100100.**00**000000.00000000

Subnet 1 10010110.01100100.**01**000000.00000000

Subnet 2 10010110.01100100.**10**000000.00000000

Subnet 3 10010110.01100100.**11**000000.00000000

- In dotted decimal, it can be written as,

Subnet 0 address 150.100.0.0 /18

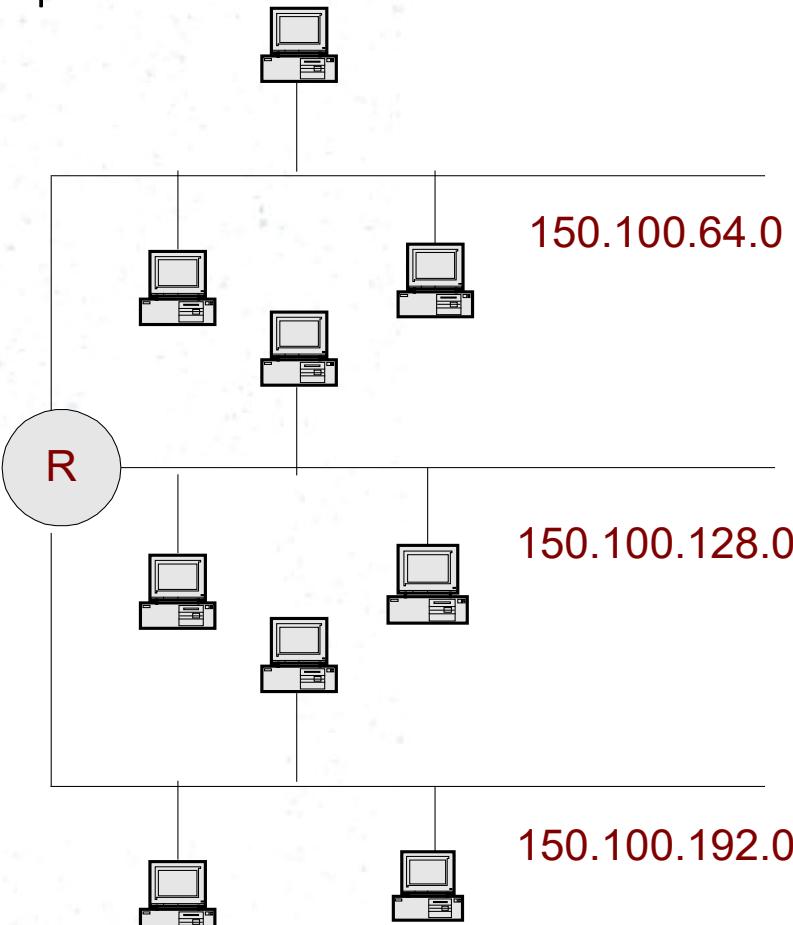
Subnet 1 address 150.100.64.0 /18

Subnet 2 address 150.100.128.0 /18

Subnet 3 address 150.100.192.0 /18

Classless Addressing cont.

For the above example the Finance, Production and Administration can be put to three subnets as follows.



Consider the hosts in subnet
150.100.64.0

The IP addresses can be given as
150.100.64.1
150.100.64.2
150.100.64.3
150.100.64.4 etc.

Classless Addressing cont.

- In classless addressing the number of bits for network address cannot be decided.
- Indicated with a “/” symbol.
- The IP address is written as,

150.100.64.1 /18

150.100.64.2 /18

150.100.64.3 /18

the subnet mask will be,

11111111.11111111.11000000.00000000

255.255.192.0

- Write the possible 12 subnet addresses of 150.72.0.0 / 16 network.

- 150.72.0.0 / 20
- 150.72.16.0 / 20
- 150.72.32.0 / 20
- 150.72.48.0 / 20
- 150.72.64.0 / 20
- 150.72.80.0 / 20
- 150.72.96.0 / 20
- 150.72.112.0 / 20
- 150.72.128.0 / 20
- 150.72.144.0 / 20
- 150.72.160.0 / 20
- 150.72.176.0 / 20

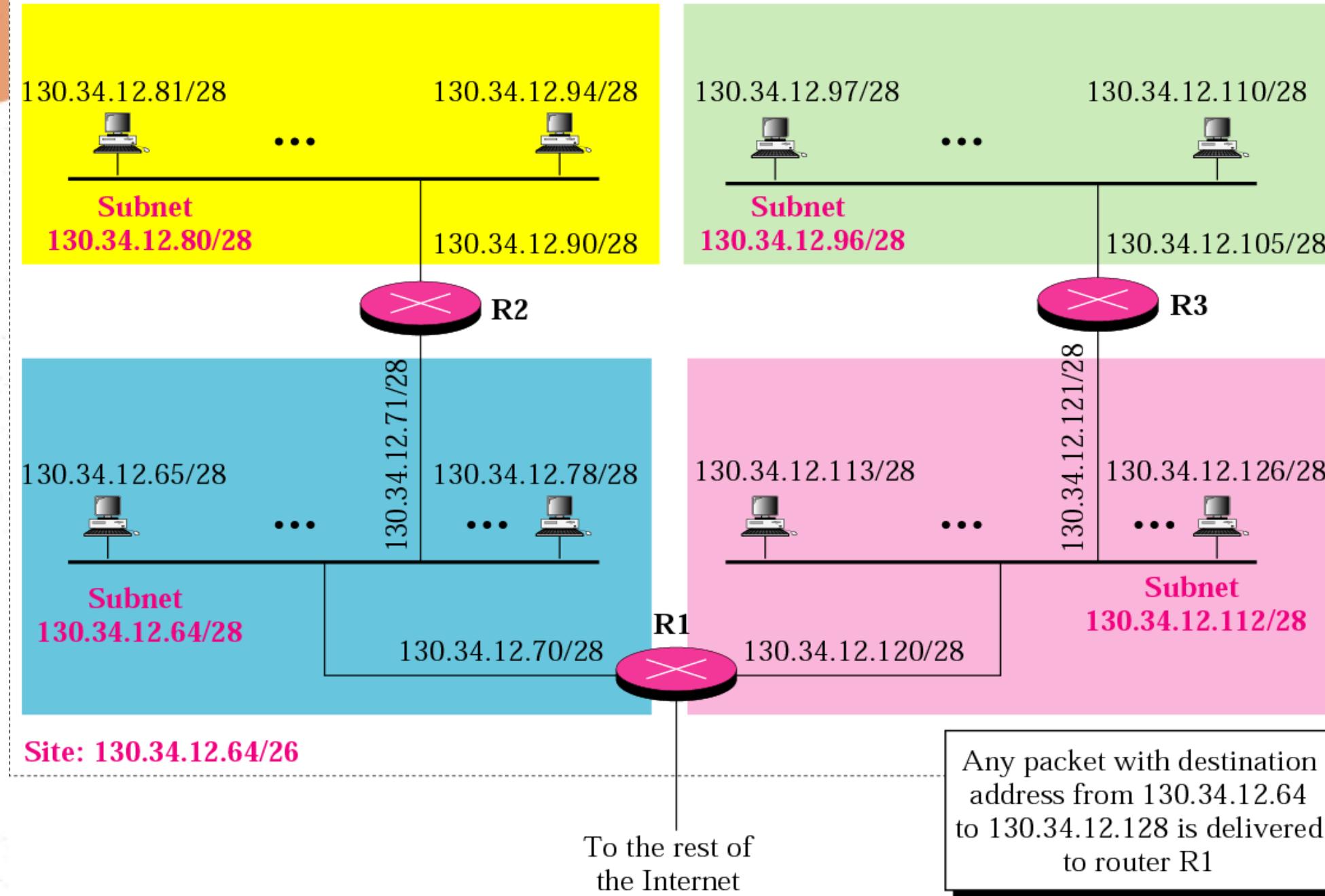
VLSM

Variable Length Sub-netting

- *An organization is granted the block 130.34.12.64/26. The organization needs 4 subnets. What is the subnet prefix length?*
-
-
-
-
-
-
-

Solution

We need 4 subnets, which means we need to add two more bits ($\log_2 4 = 2$) to the site prefix. The subnet prefix is then /28



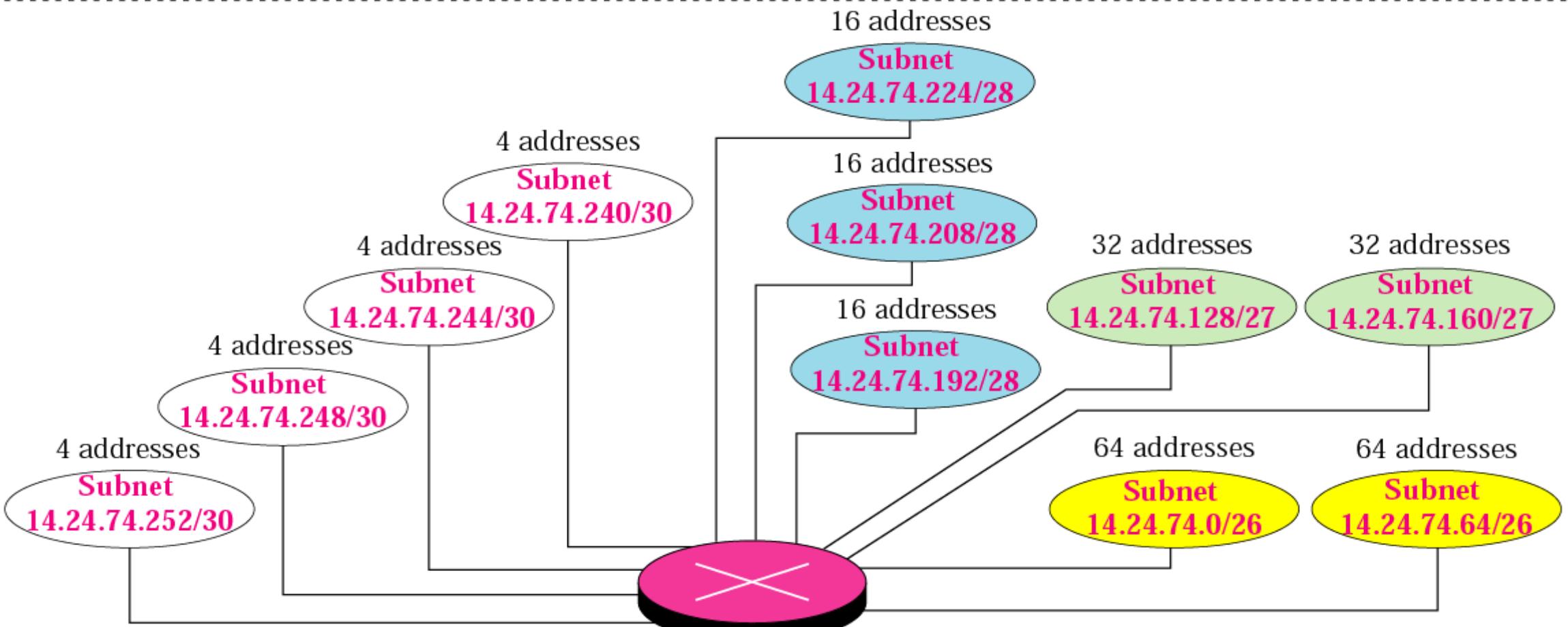
VLSM

- Variable Length subnet Masking
 - The number of devices are not equal in all the subnets



- Class-full routing
 - Only allows for one subnet mask for all networks
- VLSM & Classless routing
 - The process of subnetting a subnet
 - More than one subnet mask can be used
 - More efficient use of IP addresses as compared to classfull IP addressing

- *An organization is granted a block of addresses with the beginning address 14.24.74.0/24. There are $2^{32-24} = 256$ addresses in this block. The organization needs to have 11 subnets as shown below:*
 - a. *2 subnets, each with 64 addresses.*
 - b. *2 subnets, each with 32 addresses.*
 - c. *3 subnets, each with 16 addresses.*
 - d. *4 subnets, each with 4 addresses.*
- *Design the subnets*



Site: 14.24.74.0/24

To the rest of
the Internet

VLSM Example using /30 subnets

207.21.24.0/24 network subnetted into eight /27 (255.255.255.224) subnets

- This network has seven /27 subnets with 30 hosts each AND eight /30 subnets with 2 hosts each.
- /30 subnets are very useful for serial networks.

Subnet 0	207.21.24.0	/27
Subnet 1	207.21.24.32	/27
Subnet 2	207.21.24.64	/27
Subnet 3	207.21.24.96	/27
Subnet 4	207.21.24.128	/27
Subnet 5	207.21.24.160	/27
Subnet 6	207.21.24.192	/27
Subnet 7	207.21.24.224	/27

Sub-subnet 0	207.21.24.192	/30
Sub-subnet 1	207.21.24.196	/30
Sub-subnet 2	207.21.24.200	/30
Sub-subnet 3	207.21.24.204	/30
Sub-subnet 4	207.21.24.208	/30
Sub-subnet 5	207.21.24.212	/30
Sub-subnet 6	207.21.24.216	/30
Sub-subnet 7	207.21.24.220	/30

207.21.24.192/27 subnet, subnetted into eight /30 (255.255.255.252) subnets

Subnet 0	207.21.24.0	/27
Subnet 1	207.21.24.32	/27
Subnet 2	207.21.24.64	/27
Subnet 3	207.21.24.96	/27
Subnet 4	207.21.24.128	/27
Subnet 5	207.21.24.160	/27
Subnet 6	207.21.24.192	/27
Subnet 7	207.21.24.224	/27

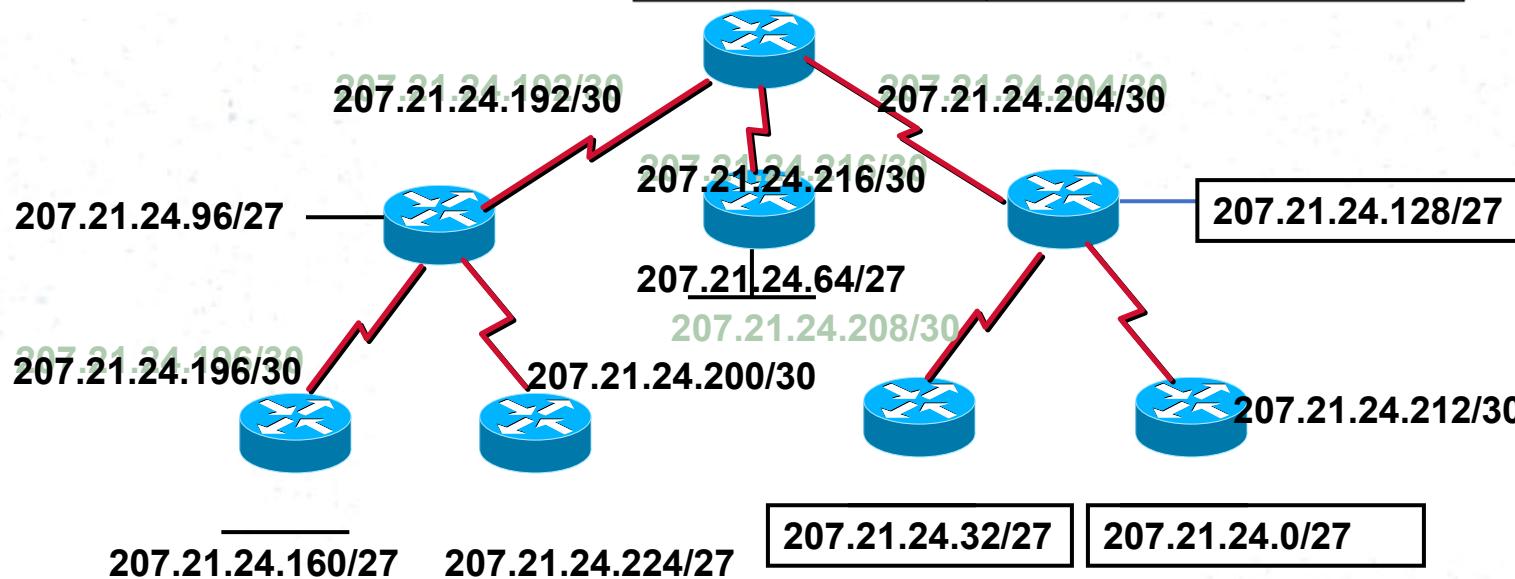
Sub-subnet 0	207.21.24.192	/30
Sub-subnet 1	207.21.24.196	/30
Sub-subnet 2	207.21.24.200	/30
Sub-subnet 3	207.21.24.204	/30
Sub-subnet 4	207.21.24.208	/30
Sub-subnet 5	207.21.24.212	/30
Sub-subnet 6	207.21.24.216	/30
Sub-subnet 7	207.21.24.220	/30

207.21.24.192/27 207.21.24. **11000000**

			/30	Hosts	Bcast	<u>2 Hosts</u>	
0	207.21.24.192/30	207.21.24.	110 00000	01	10	11	.193 & .194
1	207.21.24.196/30	207.21.24.	110 00100	01	10	11	.197 & .198
2	207.21.24.200/30	207.21.24.	110 01000	01	10	11	.201 & .202
3	207.21.24.204/30	207.21.24.	110 01100	01	10	11	.205 & .206
4	207.21.24.208/30	207.21.24.	110 10000	01	10	11	.209 & .210
5	207.21.24.212/30	207.21.24.	110 10100	01	10	11	.213 & .214
6	207.21.24.216/30	207.21.24.	110 11000	01	10	11	.217 & .218
7	207.21.24.220/30	207.21.24.	110 11100	01	10	11	.221 & .222

Subnet 0	207.21.24.0	/27
Subnet 1	207.21.24.32	/27
Subnet 2	207.21.24.64	/27
Subnet 3	207.21.24.96	/27
Subnet 4	207.21.24.128	/27
Subnet 5	207.21.24.160	/27
Subnet 6	207.21.24.192	/27
Subnet 7	207.21.24.224	/27

Sub-subnet 0	207.21.24.192	/30
Sub-subnet 1	207.21.24.196	/30
Sub-subnet 2	207.21.24.200	/30
Sub-subnet 3	207.21.24.204	/30
Sub-subnet 4	207.21.24.208	/30
Sub-subnet 5	207.21.24.212	/30
Sub-subnet 6	207.21.24.216	/30
Sub-subnet 7	207.21.24.220	/30



- This network has seven /27 subnets with 30 hosts each AND seven /30 subnets with 2 hosts each (one left over).
- /30 subnets with 2 hosts per subnet do not waste host addresses on serial networks .

VLSM and the Routing Table

Routing Table without VLSM

```
RouterX#show ip route
      207.21.24.0/27 is subnetted, 4 subnets
C        207.21.24.192 is directly connected, Serial0
C        207.21.24.196 is directly connected, Serial1
C        207.21.24.200 is directly connected, Serial2
C        207.21.24.204 is directly connected, FastEthernet0
```

Displays one subnet mask for all child routes. Classful mask is assumed for the parent route.

Each child routes displays its own subnet mask.
Classful mask is included for the parent route.

Routing Table with VLSM

```
RouterX#show ip route
      207.21.24.0/24 is variably subnetted, 4 subnets, 2 masks
C        207.21.24.192/30 is directly connected, Serial0
C        207.21.24.196/30 is directly connected, Serial1
C        207.21.24.200/30 is directly connected, Serial2
C        207.21.24.96/27 is directly connected, FastEthernet0
```

- Parent Route shows classful mask instead of subnet mask of the child routes.
- Each Child Routes includes its subnet mask.

Computer Networks

Lecture 3

IPv6 Addressing



Why IPv6

- ▶ IPv4 has a theoretical maximum of 4.3 billion addresses
- ▶ plus private addresses in combination with NAT
- ▶ NAT having limitations in peer-to-peer communications
- ▶ With an Internet of things, devices other than computers, tablets, and smartphones, sensors, Internet-ready devices, automobiles, biomedical devices, household appliances, natural ecosystems etc... need to connect to the internet.

Why IPv6

RIR IPv4 Exhaustion Dates





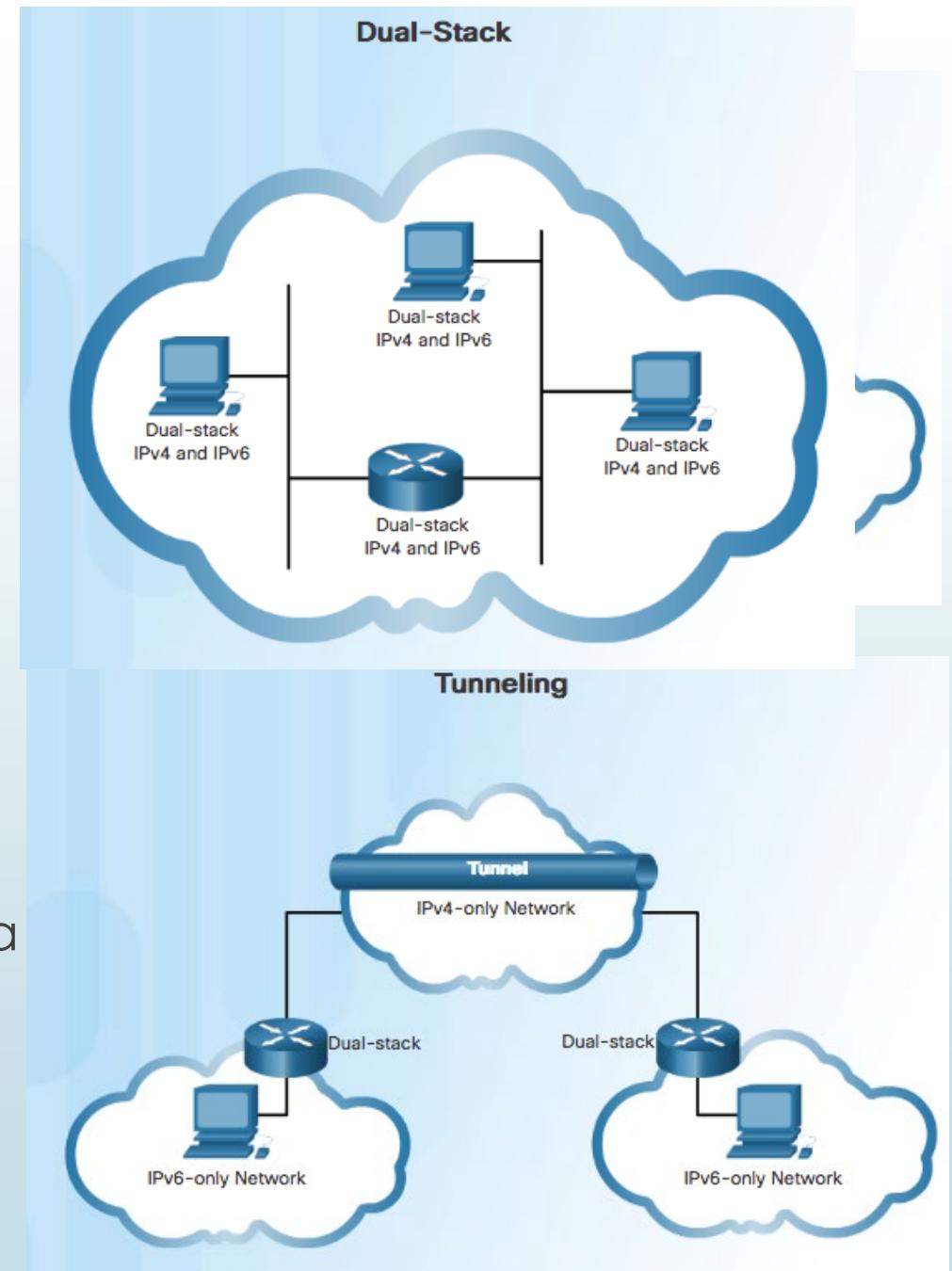
How it looks like

- ▶ IPv6 has a larger 128-bit address space
- ▶ 340 undecillion addresses. (That is the number 340, followed by 36 zeroes.)
- ▶ When the IETF began its development of a successor to IPv4, so it fix the limitations of IPv4 and include additional enhancements
- ▶ Ex- 2001:0DB8:0000:1111:0000:0000:0200

Hextet used to refer to a segment of 16 bits or four hexadecimals

IPv4 and IPv6 Coexistence

- **Dual Stack** – dual stack allows **IPv4 and IPv6 to coexist on the same network segment**. Dual stack devices run both IPv4 and IPv6 protocol stacks simultaneously.
- **Tunneling** – tunneling is a method of transporting an IPv6 packet over an IPv4 network. **The IPv6 packet is encapsulated inside an IPv4 packet**, similar to other types of data.
- **Translation** – Network Address Translation 64 (NAT64) allows IPv6-enabled devices to communicate with IPv4-enabled devices using a translation technique similar to NAT for IPv4. **An IPv6 packet is translated to an IPv4 packet** and vice versa.



Term

Description

IPv6

128-bit address/340 undecillion addresses.

IPv4

32-bit address/4.3 billion addresses.

Tunneling

Transports an IPv6 packet over IPv4 networks.

Translation

Uses NAT64 to convert between IPv6 and IPv4.

Dual Stack

Allows IPv4 and IPv6 to coexist on the same network segment.

Address formats

IPv6 Address - Rule 1 (Omitting Leading 0s)

- ▶ The first rule to help reduce the notation of IPv6 addresses is any leading 0s (zeros) in any 16-bit section or hexet can be omitted
 - ▶ 01AB can be represented as 1AB
 - ▶ 09F0 can be represented as 9F0
 - ▶ 0A00 can be represented as A00
 - ▶ 00AB can be represented as AB

Preferred

2 0 0 1 : 0 D B 8 : 0 0 0 0 : 1 1 1 1 : 0 0 0 0 : 0 0 0 0 : 0 2 0 0

No leading 0s

2 0 0 1 : D B 8 : 0 : 1 1 1 1 : 0 : 0 : 0 : 2 0 0

IPv6 Address -Rule 2 (Omitting All 0 Segments)

- A double colon (:) can replace any single, contiguous string of one or more 16-bit segments (hextets) consisting of all 0's

Preferred	2 0 0 1 : 0 DB 8 : 0 0 0 0 : 0 0 0 0 : A B C D : 0 0 0 0 : 0 0 0 0 : 0 1 0 0
Preferred	2 0 0 1 : 0 DB 8 : 0 0 0 0 : 1 1 1 1 : 0 0 0 0 : 0 0 0 0 : 0 0 0 0 : 0 2 0 0
No leading 0s	2 0 0 1 : DB 8 : 0 : 1 1 1 1 : 0 : 0 : 0 : 2 0 0
Compressed	2 0 0 1 : DB 8 : 0 : 1 1 1 1 : : 2 0 0
Compressed	2 0 0 1 : DB 8 : 0 : 0 : A B C D : : 1 0 0

Only one :: may be used.

IPv6 Address Types

- ▶ There are three types of IPv6 addresses:

- ▶ Unicast
- ▶ Multicast
- ▶ Anycast

*** IPv6 does not have broadcast addresses.

IPv6 Unicast Addresses

- ▶ **Global unicast**

- ▶ Similar to a public IPv4 address.
- ▶ Globally unique, Internet routable addresses.
- ▶ Global unicast addresses can be configured statically or assigned dynamically.
- ▶ Currently, only global unicast addresses with the first three bits of 001 or 2000::/3 are being assigned. (The first hextet has a range of (2000) to (3FFF).)

- ▶ **Link-local**

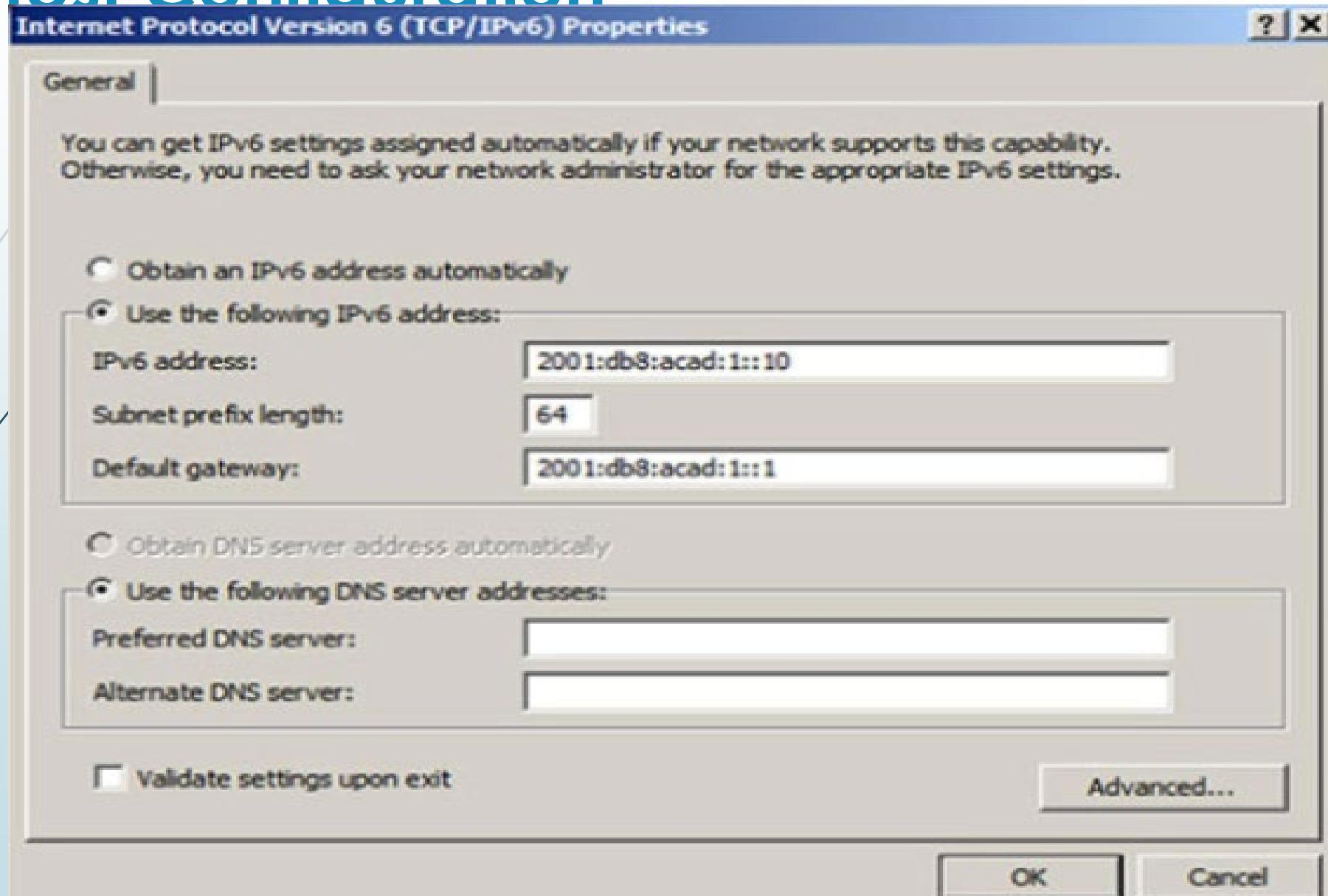
- ▶ Link-local addresses are used to communicate with other devices on the same local link. (The first hextet has a range of (FE80) to (FEBF).)

- ▶ **Unique local**

- ▶ Similar to the private addresses for IPv4, but there are significant differences.
- ▶ (FC00::/7 to FDFF::/7)

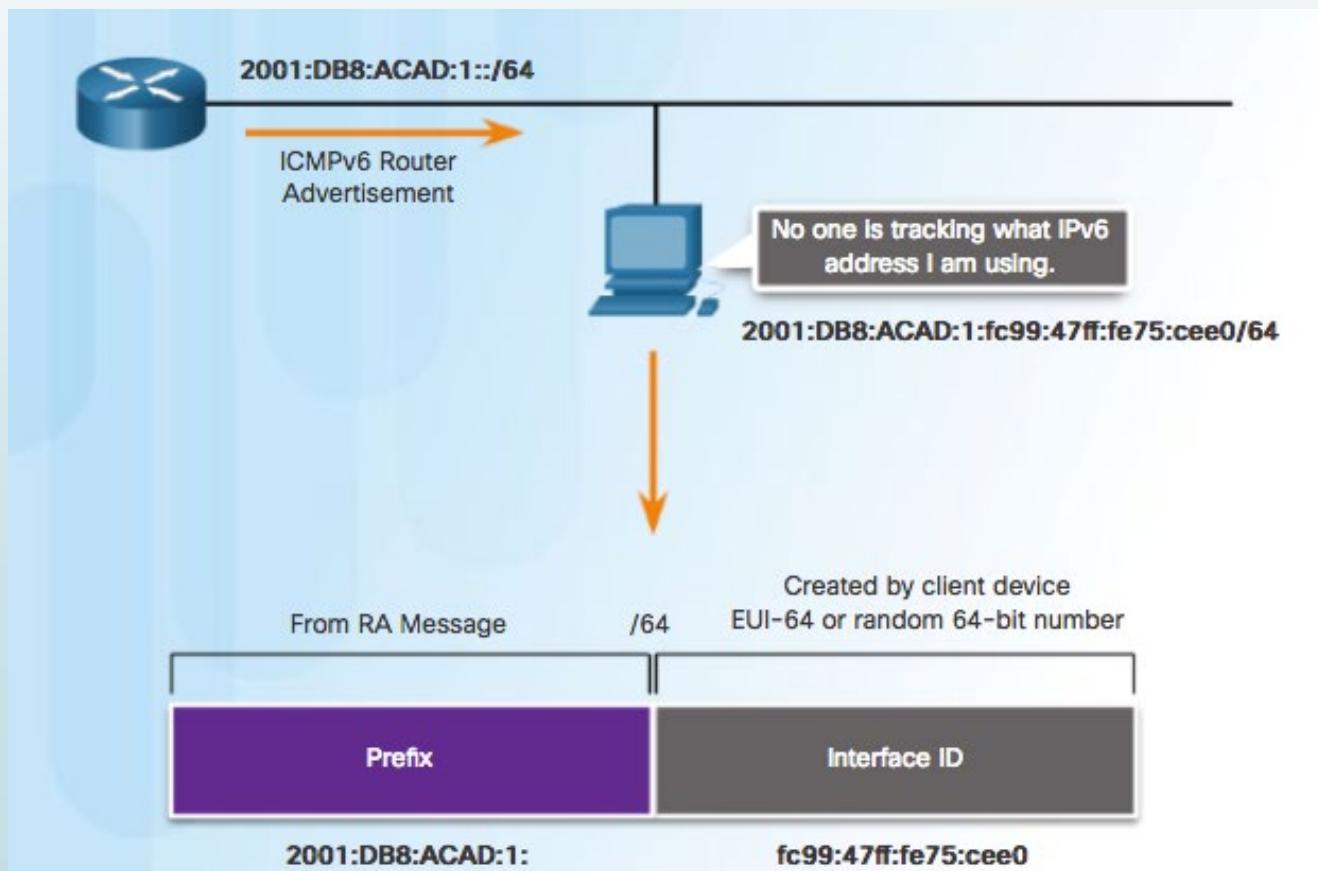
*** 2001:0DB8::/32 address has been reserved for documentation purposes

Host Configuration



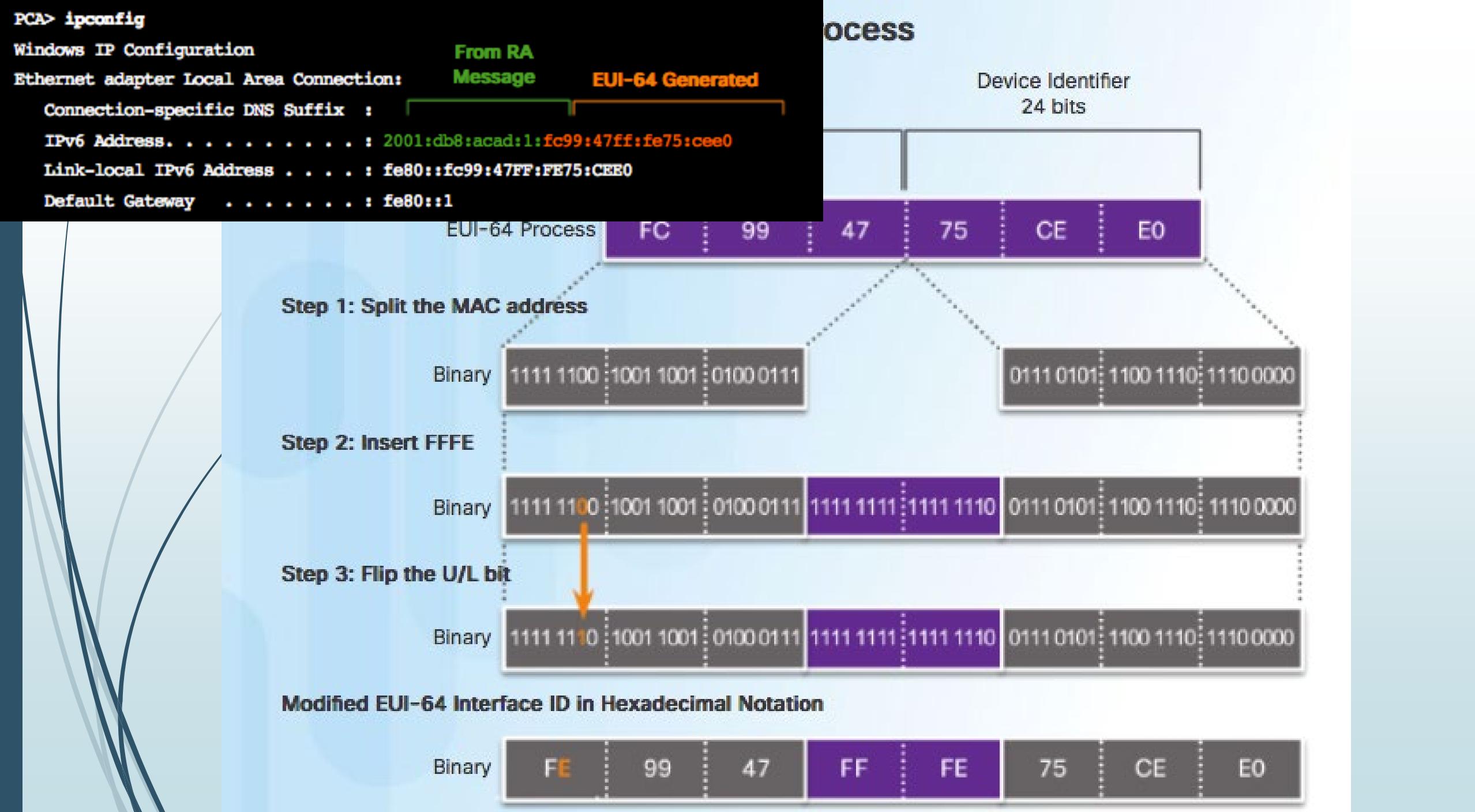
Dynamic Configuration - SLAAC

- Stateless Address Autoconfiguration (SLAAC) is a method that allows a device to obtain its prefix, prefix length, default gateway address, and other information from an IPv6 router without the use of a DHCPv6 server.



EUI-64 Process

- IEEE defined the Extended Unique Identifier (EUI) or modified EUI-64 process. This process uses a client's 48-bit Ethernet MAC address, and inserts another 16 bits in the middle of the 48-bit MAC address to create a 64-bit Interface ID.
- **Step 1:** Divide the MAC address between the OUI and device identifier.
- **Step 2:** Insert the hexadecimal value FFFE, which in binary is: 1111 1111 1111 1110
- **Step 3:** Convert the first 2 hexadecimal values of the OUI to binary and flip the U/L bit (bit 7). In this example, the 0 in bit 7 is changed to a 1





Questions ?



SLIIT

Discover Your Future

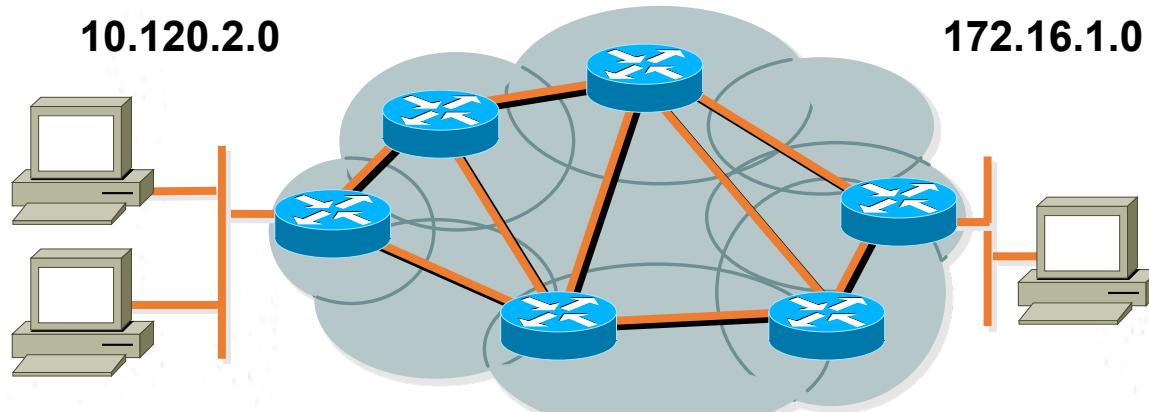
IT2050 - Computer Networks

Lecture 3 Routing Protocols

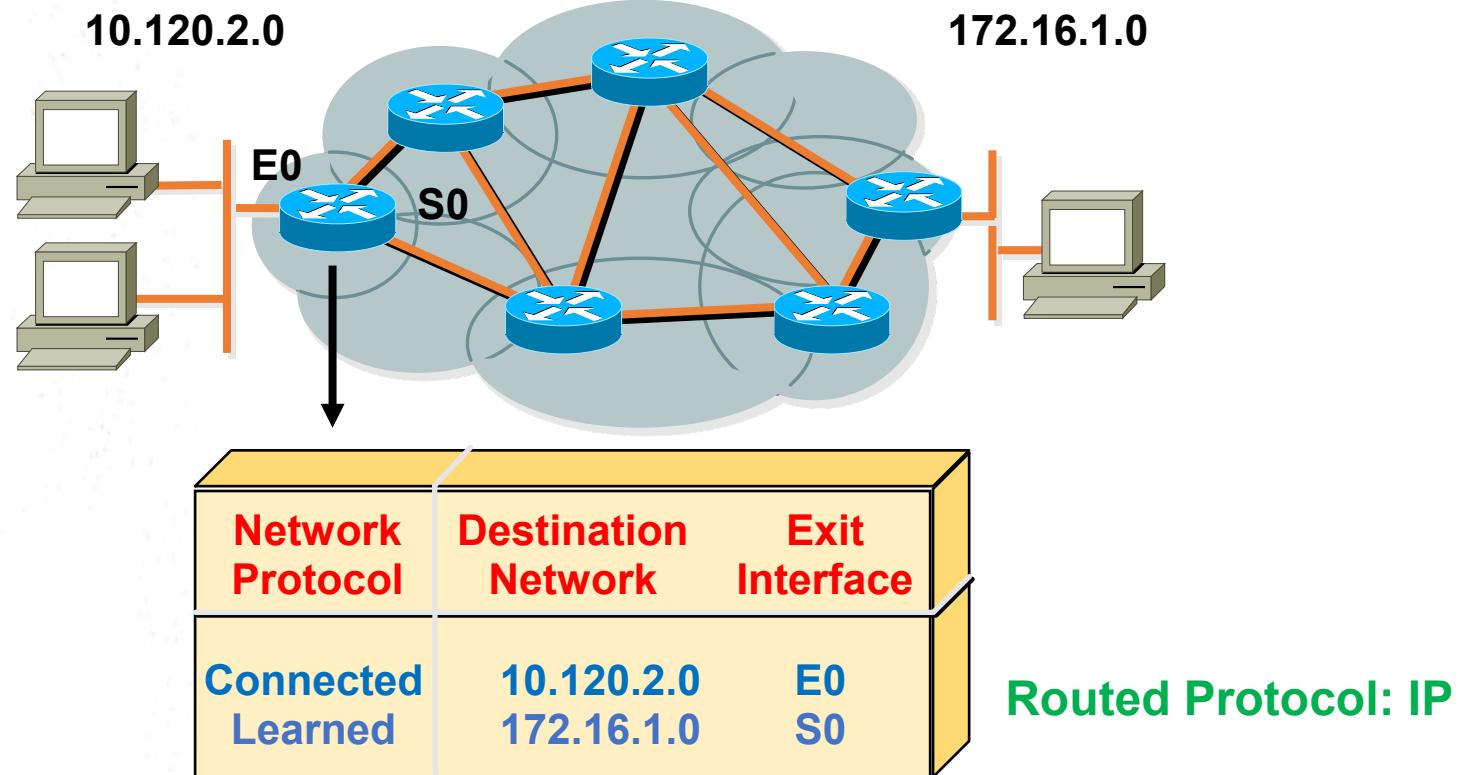
Ms. Hansika Mahaadikara

What Is Routing?

- To route, a router needs to do the following:
 - Know the destination address.
 - Identify the sources it can learn from.
 - Discover possible routes.
 - Select the best route.
 - Maintain and verify routing information.



What Is Routing? (cont.)



- **Routers must learn destinations that are not directly connected.**

Identifying Static & Dynamic Routes

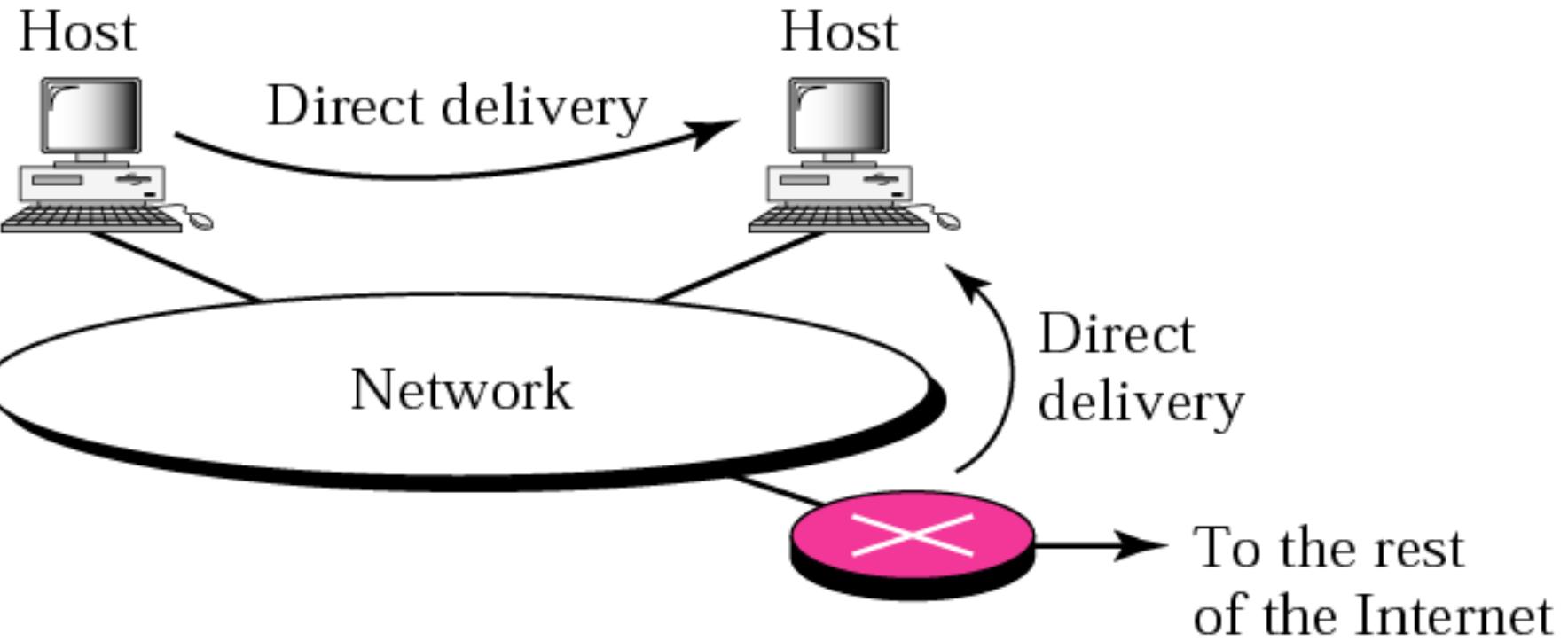
- Static Route

- Uses a route that a network administrator enters into the router manually

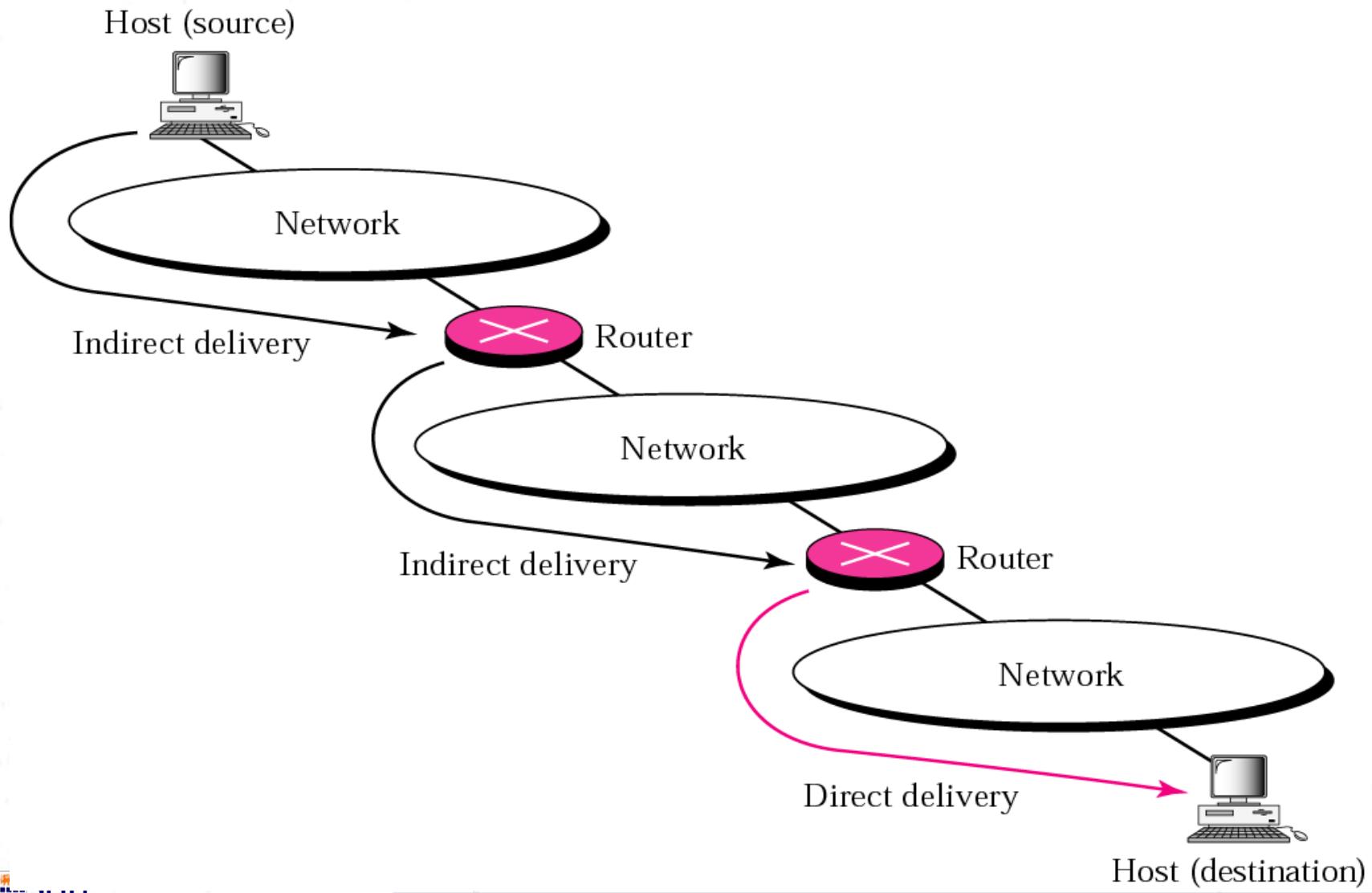
- Dynamic Route

- Uses a route that a network routing protocol adjusts automatically for topology or traffic changes

Direct Delivery



Indirect Delivery



Indirect Delivery cont.

- To send a packet from source to destination, need to go to the network
 - (packet should go from router to router)
- All routers should maintain a routing table
- IP packet is analyzed at the router and correct path is selected from the routing table
- The packet is sent through that path
- Indirect delivery is done using the routing strategies
-
-
-

Routing Table

```
R1#show ip route
```

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route

* Gateway of last resort is not set

- * 172.16.0.0/24 is subnetted, 3 subnets
 - S 172.16.1.0 [1/0] via 172.16.2.2
 - C 172.16.2.0 is directly connected, Serial0/0/0
 - C 172.16.3.0 is directly connected, FastEthernet0/0
- S 192.168.1.0/24 [1/0] via 172.16.2.2
- S 192.168.2.0/24 [1/0] via 172.16.2.2

Adaptive Routing

Adaptive Routing

- Each router maintains a routing table
- Routing table modifies itself according to the network changes
- Advantages
 - Network traffic is minimized
 - Low latency
 - The best route will be selected most
- Disadvantages
 - Router memory need to keep a routing table

Routing Methods used in Adaptive Routing

- Next hop routing
 - Host specific
 - Network specific
- Default routing

Host Specific Routing

- Each router keeps one record/entry for each
- Table entry has Host IP and the Interface

Host Address	Interface
192.168.50.1	E0
192.168.50.6	E0
172.18.2.9	S1
172.18.5.96	S1

Disadvantages

- Large number of records
- Table updating is difficult and complex as it should be done for each and every host (if the host IP changes)

Network Specific Routing

- Each router keeps a table entry for each network (one record for one network)
- Table entry has Network address and Interface

Network Address	Interface
192.168.50.0	E0
172.18.0.0	S1
⋮	⋮

Advantages

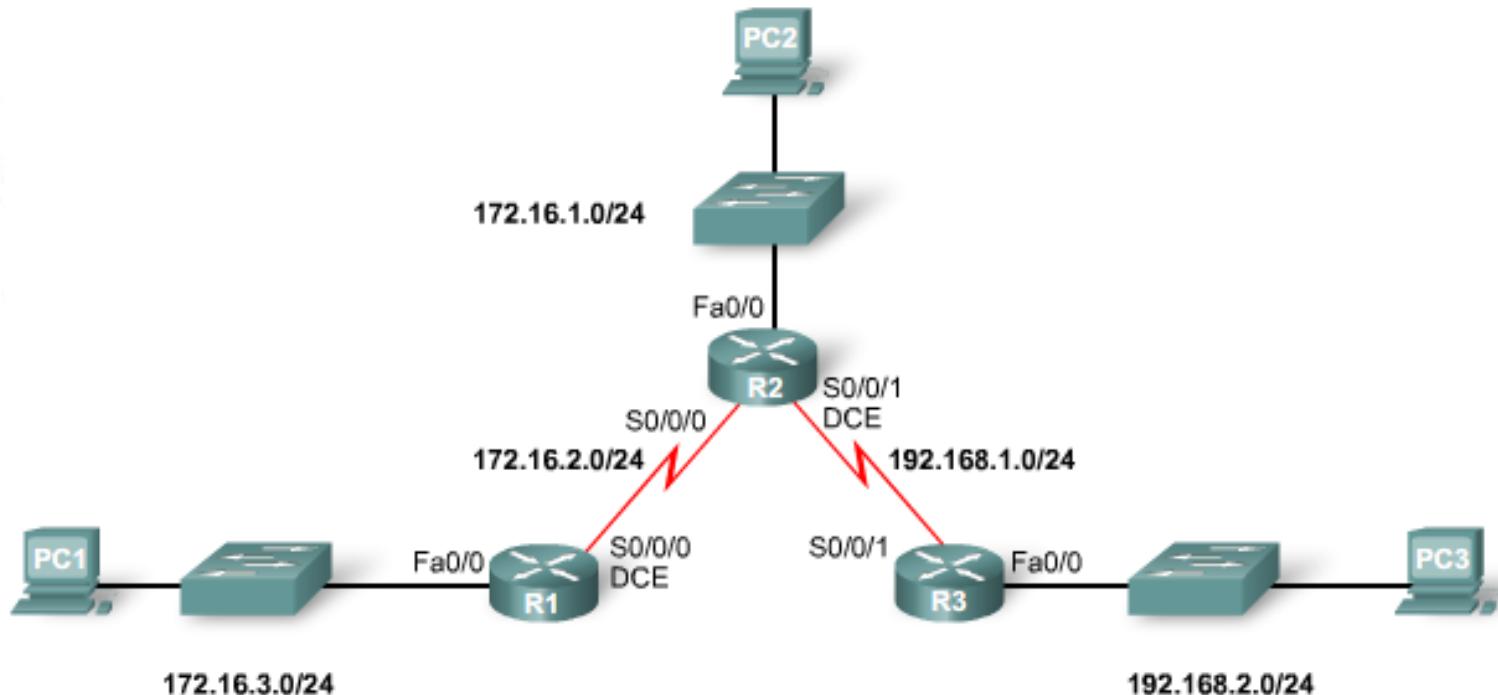
- Number of records are limited (Table updates are not for each host but for a network)
- Update is easy

Routing Table update Methods

- Basic methods to update routing tables
 - Connected
 - Static
 - Dynamic
- •
• •
• •
• •
• •
• •

Connected

- Once the router is connected to the network its interfaces are given IP addresses
- With that router automatically identifies the network addresses to which it connected



Connected cont.

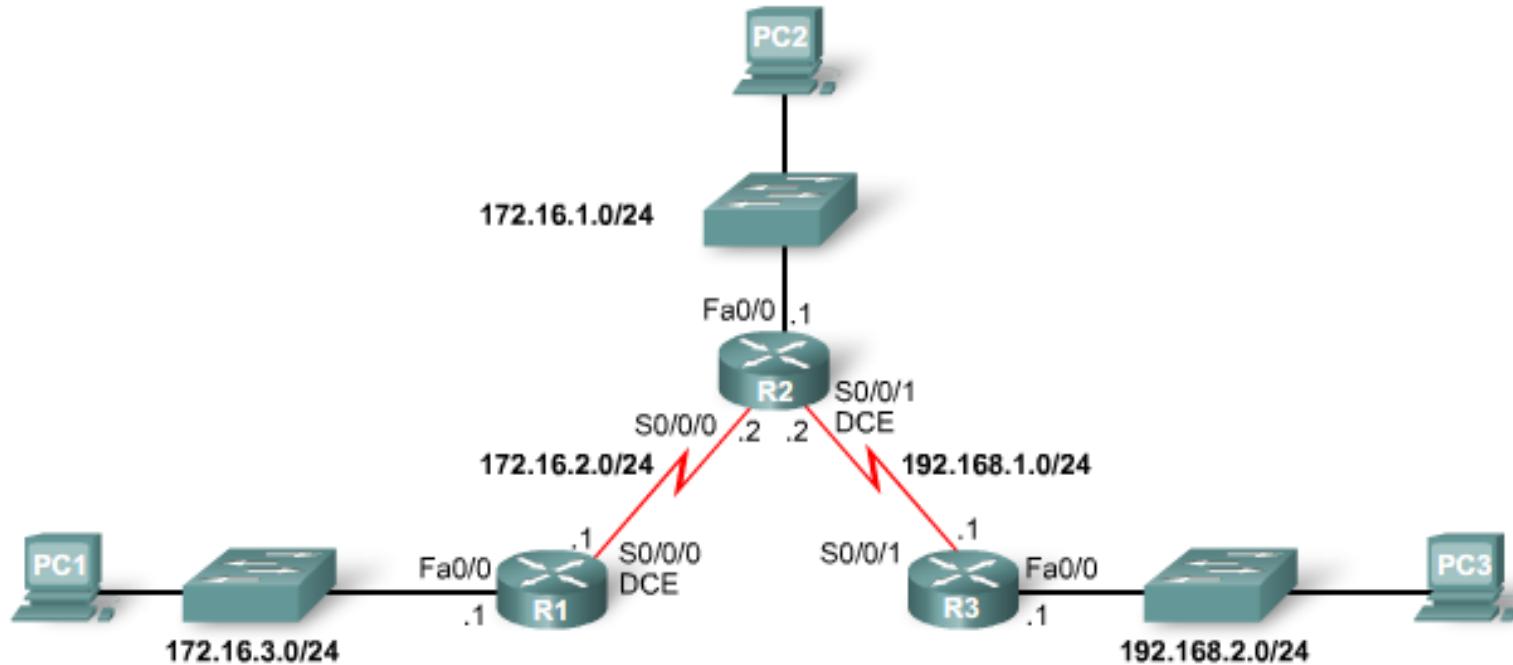
```
R1#show ip route
```

Codes: C - connected, S - static,
Gateway of last resort is not set

172.16.0.0/24 is subnetted, 2 subnets

C 172.16.2.0 is directly connected, Serial0/0/0
C 172.16.3.0 is directly connected, FastEthernet0/0

- Administrator can manually give routing table records



```
Router(config)#ip route <destination network>
              <destination network subnet mask>
              <next hop address | exit interface | Both>
```

Static cont.

```
R1(config)#
R1(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.2
R1(config)#ip route 192.168.1.0 255.255.255.0 172.16.2.2
R1(config)#ip route 192.168.2.0 255.255.255.0 172.16.2.2
R1(config)#

```

```
R1#show ip route
```

Codes: C - connected, S - static

Gateway of last resort is not set

172.16.0.0/24 is subnetted, 3 subnets

S 172.16.1.0 [1/0] via 172.16.2.2

C 172.16.2.0 is directly connected, Serial0/0/0

C 172.16.3.0 is directly connected, FastEthernet0/0

S 192.168.1.0/24 [1/0] via 172.16.2.2

S 192.168.2.0/24 [1/0] via 172.16.2.2

Static cont.

Advantages:

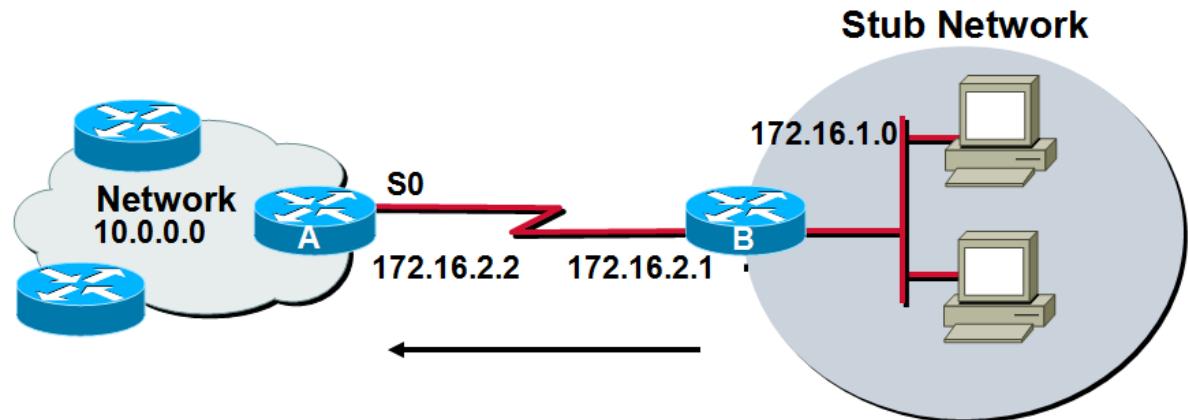
- Minimal CPU processing
- Easier for administrator to understand and configure

Disadvantages:

- Configuration and maintenance is time-consuming
- Configuration is error-prone
- Administrator should maintain changing route information
- Does not scale well with growing networks; maintenance becomes complex
- Requires complete knowledge of the whole network for proper implementation

Default Routing

- Last record in the routing table
- Indicates the route/path to be taken, if any of the records does not match with the IP packet destination IP address
- Stub networks only use default routing , Stub networks have only one exit port out of the network



```
R(config)#ip route 0.0.0.0 0.0.0.0  
<next hop ip addr | exit interface name | both>
```

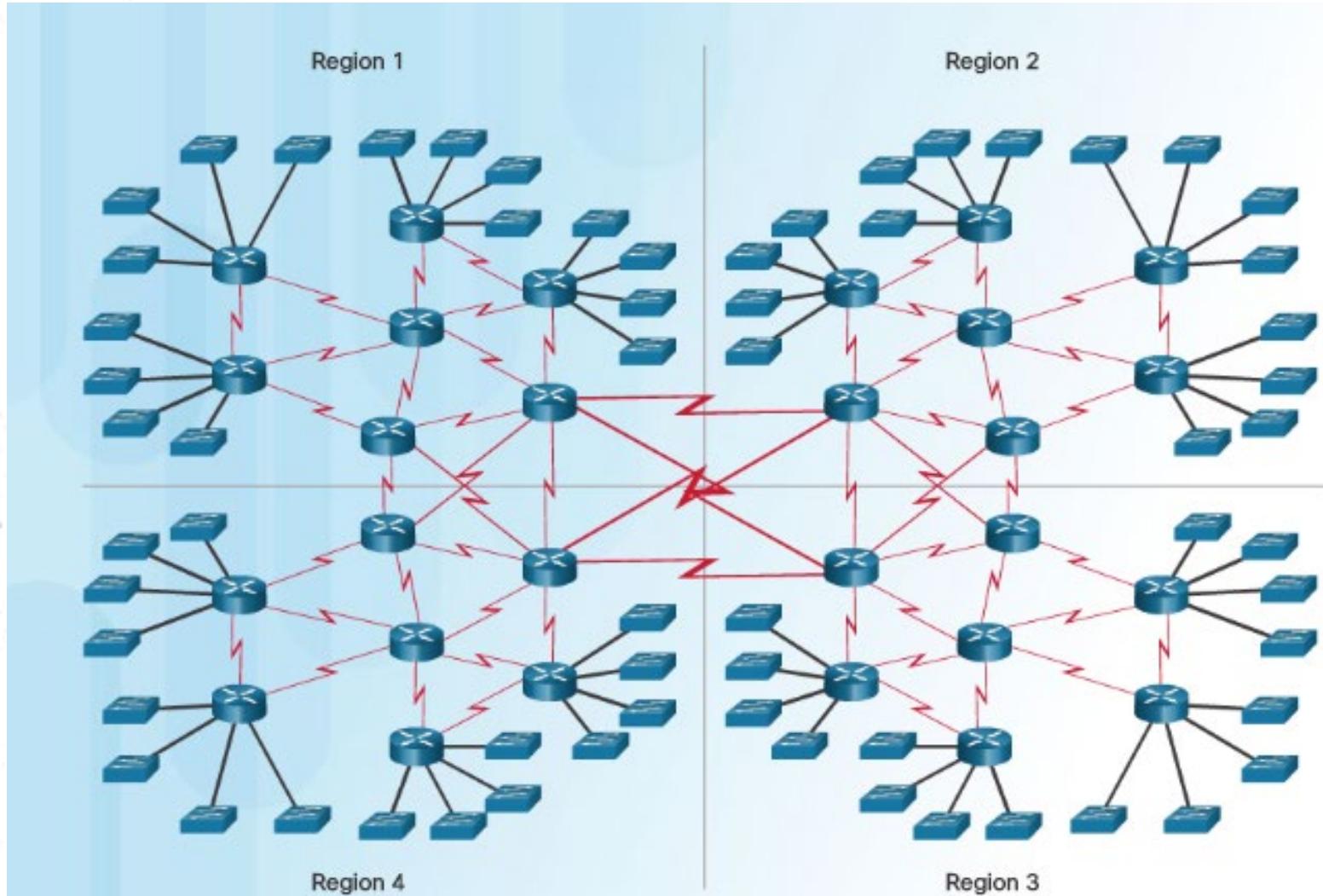
Default Routing cont.

```
B(config)#  
B(config)#ip route 0.0.0.0 0.0.0.0 172.16.2.2  
B(config)#+
```

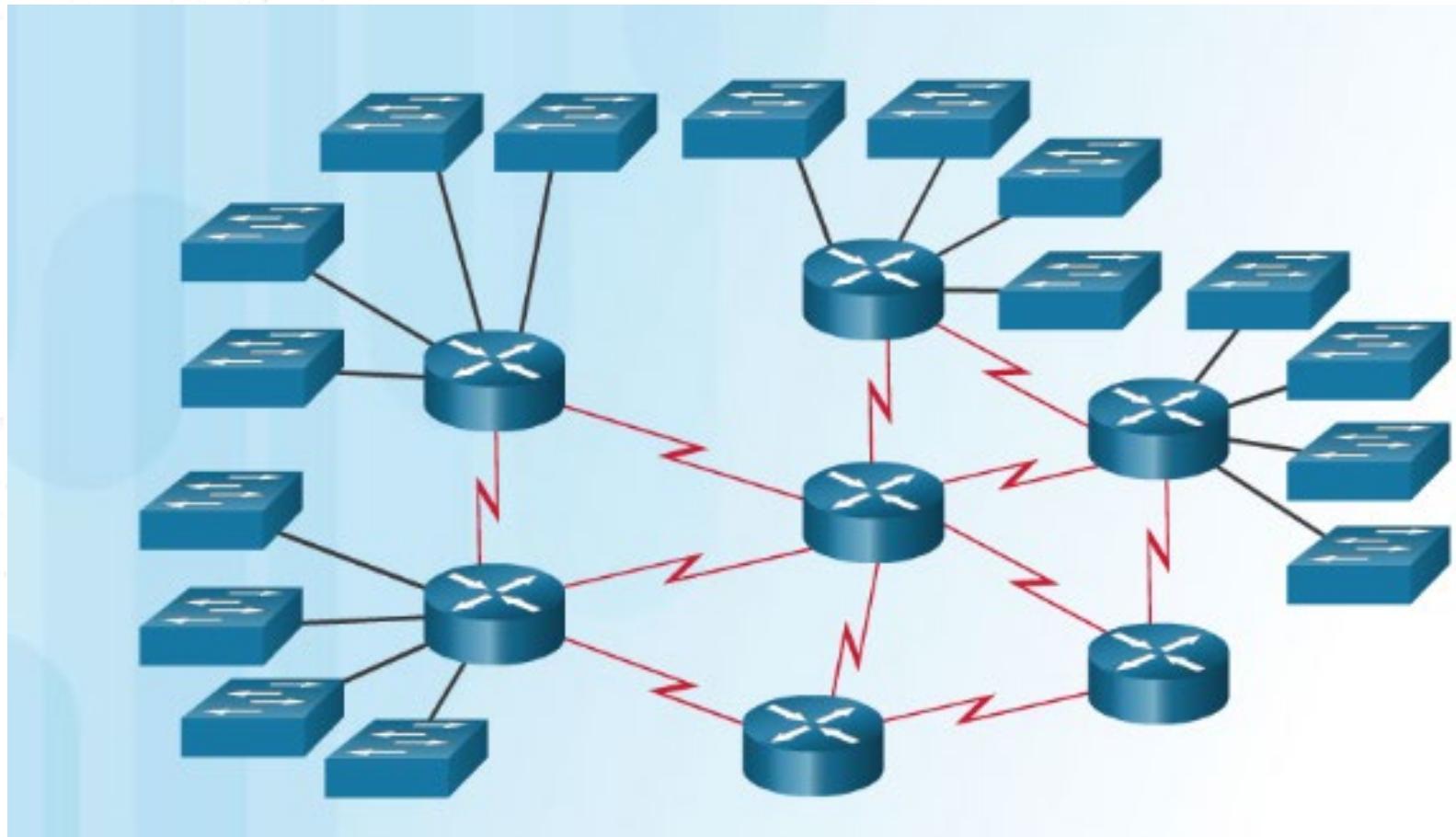
```
B#show ip route  
Codes: C - connected, S - static  
  
Gateway of last resort is 172.16.2.2 to network 0.0.0.0
```

```
    172.16.0.0/24 is subnetted, 2 subnets  
C        172.16.1.0 is directly connected, FastEthernet0/0  
C        172.16.2.0 is directly connected, Serial2/0  
S*    0.0.0.0/0 [1/0] via 172.16.2.2  
B#
```

Dynamic Routing Scenario



Dynamic Routing Scenario



Dynamic

- Routing tables are updated automatically by using routing protocols
- Routing tables have
 - Initially only connected records
 - Then add static' records
 - Then automatic dynamic updates

Dynamic cont.

Advantages:

- Administrator has less work maintaining the configuration when adding or deleting networks
- Protocols automatically update, according to the topology changes.
- Configuration is less error-prone
- Suitable for More scalable, growing networks

Disadvantages:

- Router resources are used (CPU cycles, memory and bandwidth)
- More administrator knowledge is required for configuration, verification, and troubleshooting

Routing Protocols

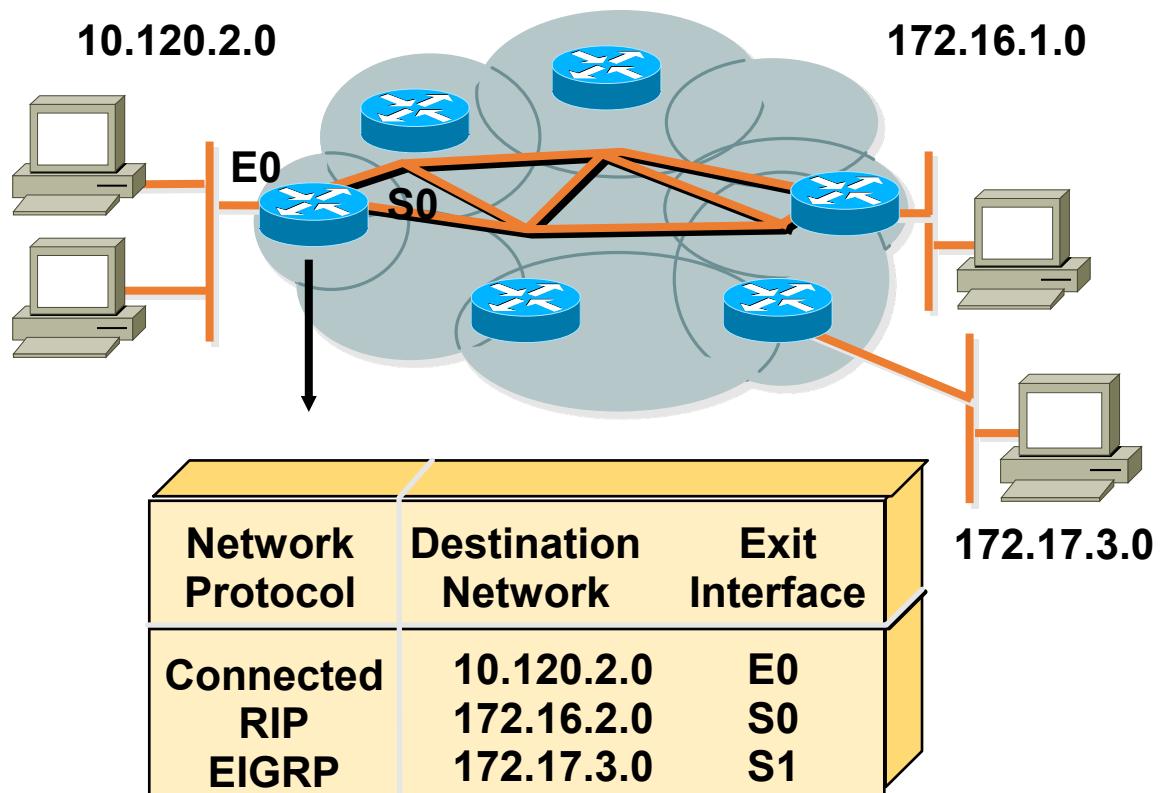
- *
- *
- *
- *
- *
- *
- *
- *
- *
- *
- *

Features of Routing Protocols

- Network changes (addition or removal or fault) are automatically updated in routing tables of all routers
- When there are many routes to a destination, the best route should be selected
- Share the traffic through different routes

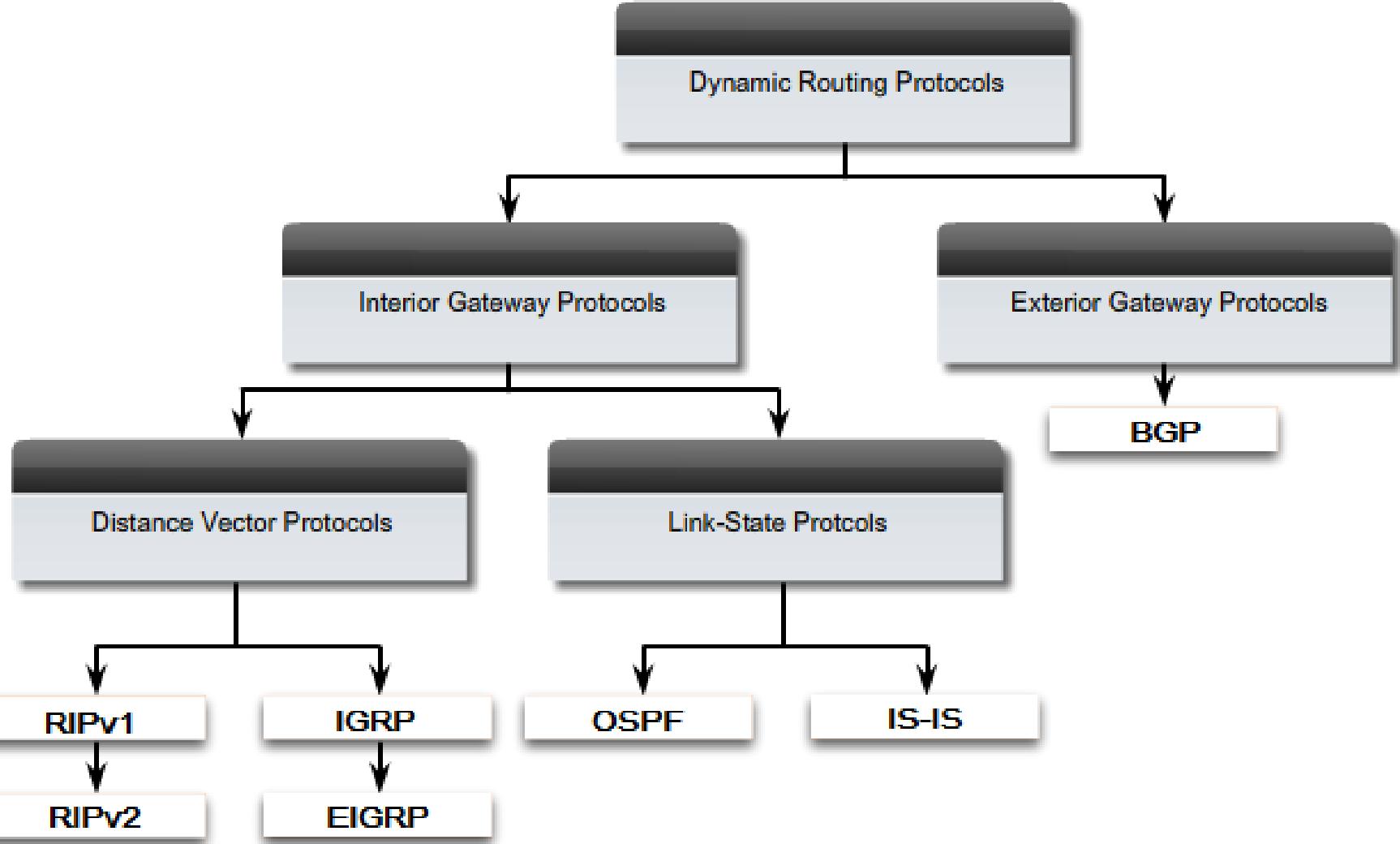
What Is a Routing Protocol?

- Routing Protocols allow routers to dynamically advertise and learn routes,
- determine which routes are available
- and which are the most efficient routes to a destination
-



Routing Protocol: RIP, EIGRP, OSPF

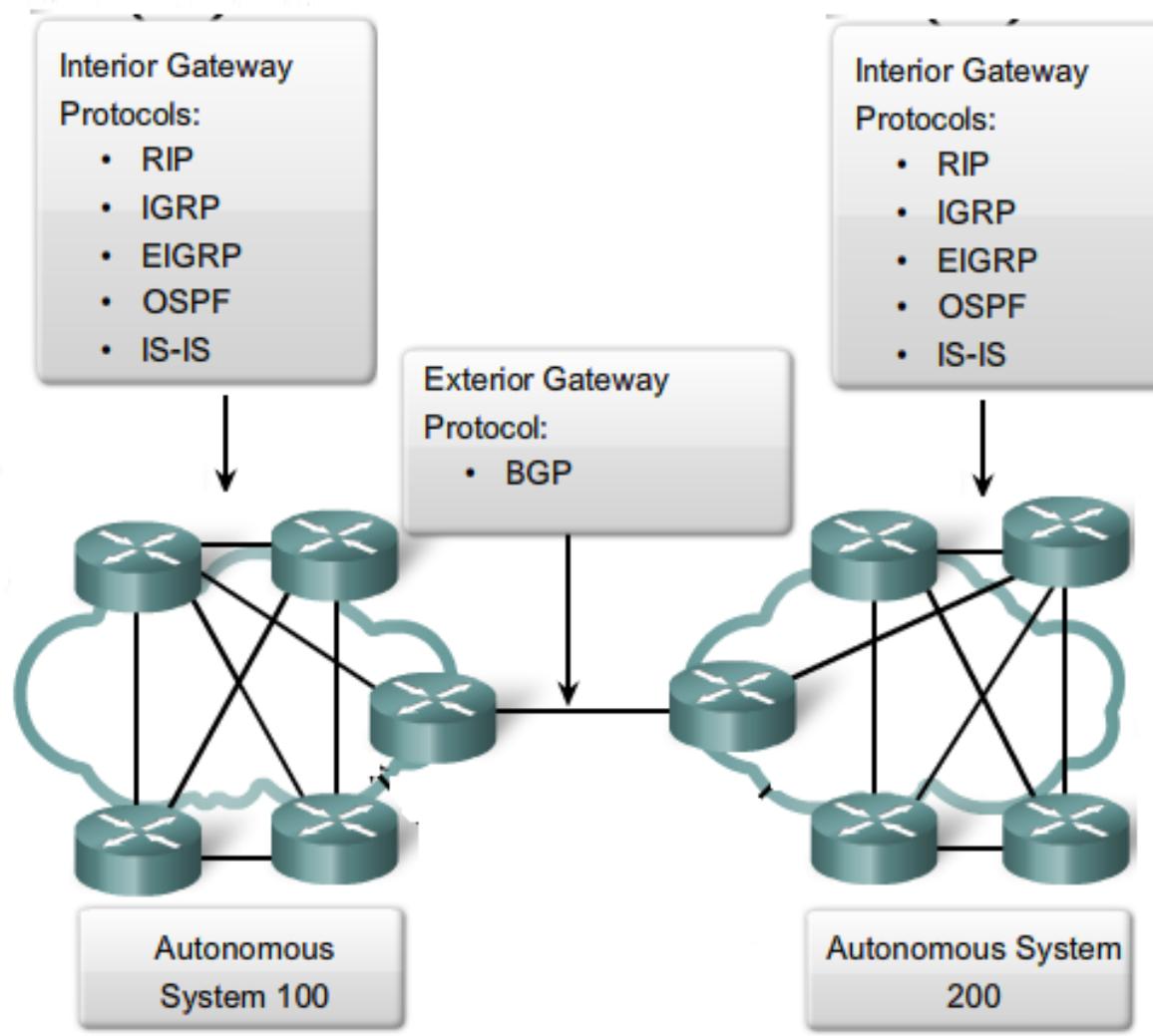
Routing Protocols



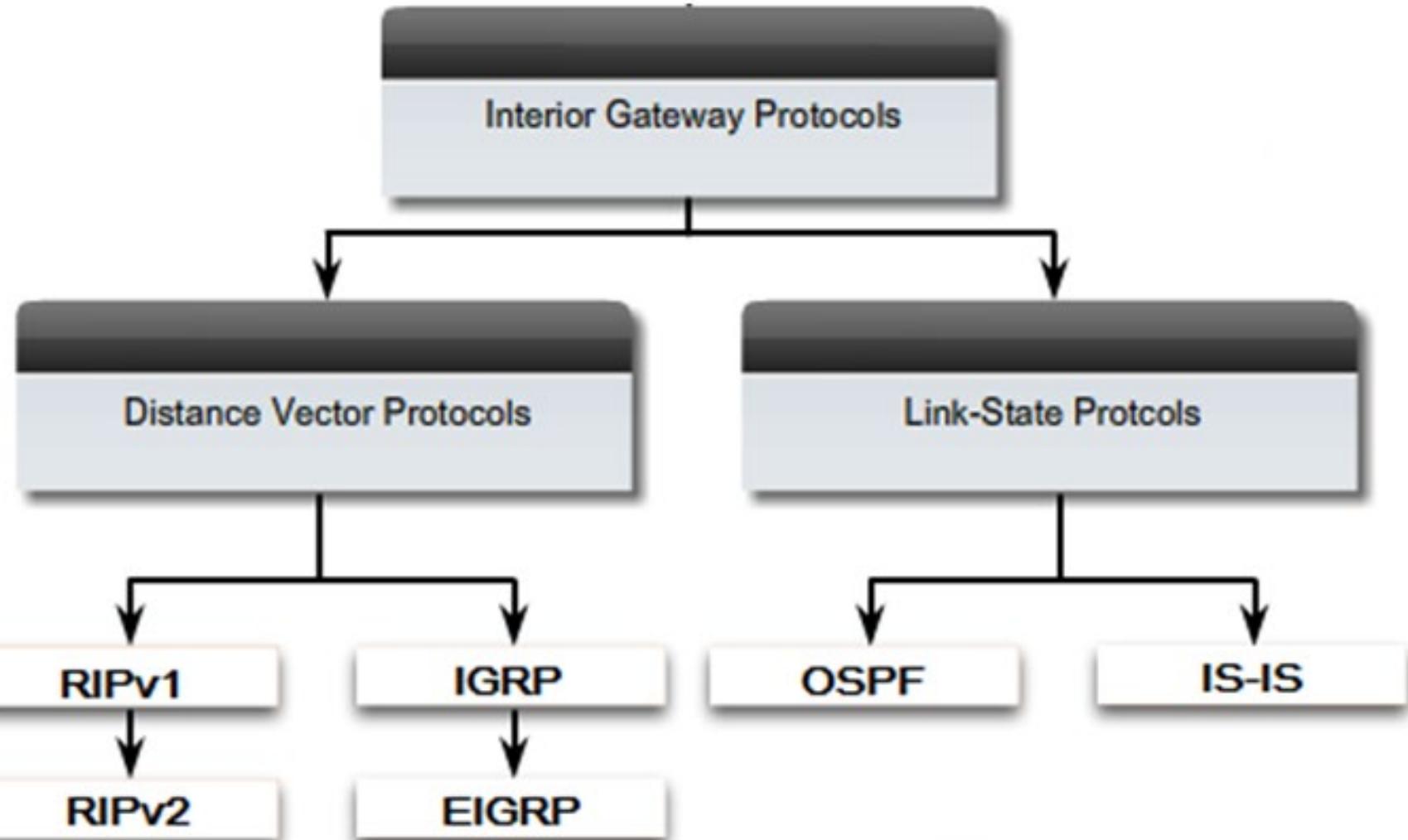
Routing Protocols cont.

- An autonomous system (AS) is a collection of routers under a common administration
 - ex : a company's internal network
- Interior Gateway Protocols (IGP) are used for
 - intra-autonomous system routing
 - (routing inside an autonomous system)
- Exterior Gateway Protocols (EGP) are used for
 - inter-autonomous system routing
 - (routing between autonomous systems)

Routing Protocols cont.



Interior Gateway Protocols (IGP)



RIP (Routing Information Protocol)

RIP (Routing Information Protocol)

- A Distance-vector routing protocol
- It sends the complete routing table out to all active interfaces in every 30 seconds
- Only uses hop count to select best way to a remote network
- RIP works well in small networks, but it is inefficient on large networks
- There are two versions
 - RIP v1, RIP v2

RIP Configuration

```
Router(config)#router rip
```

```
Router(config-router)#network <network-address>
```

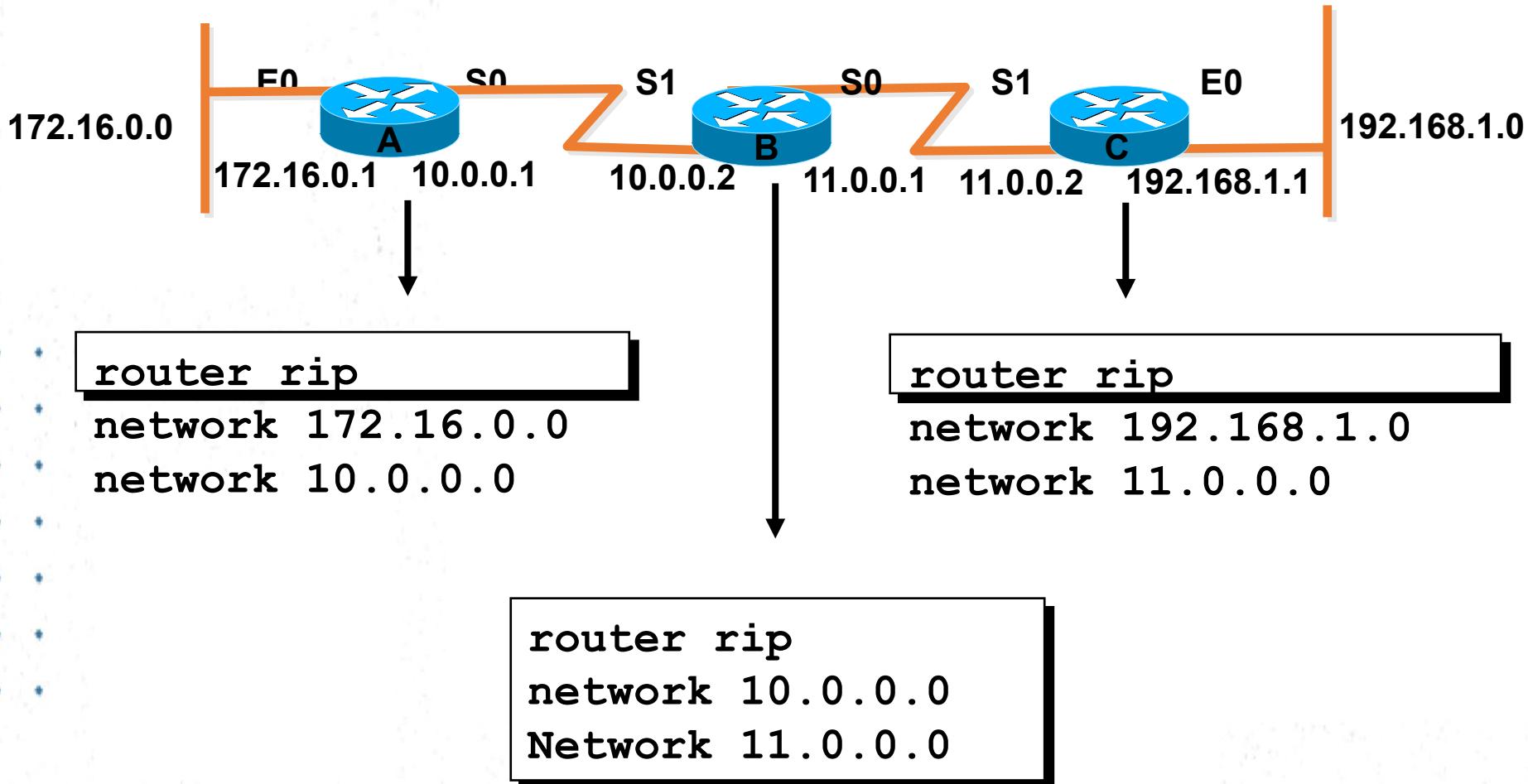
* * * * *

< **network-address** >

Directly connected network addresses

RIP Configuration Example

Version 1



Configure RIP V2

Classless
Sub-networks

```
Router(config)#router rip
```

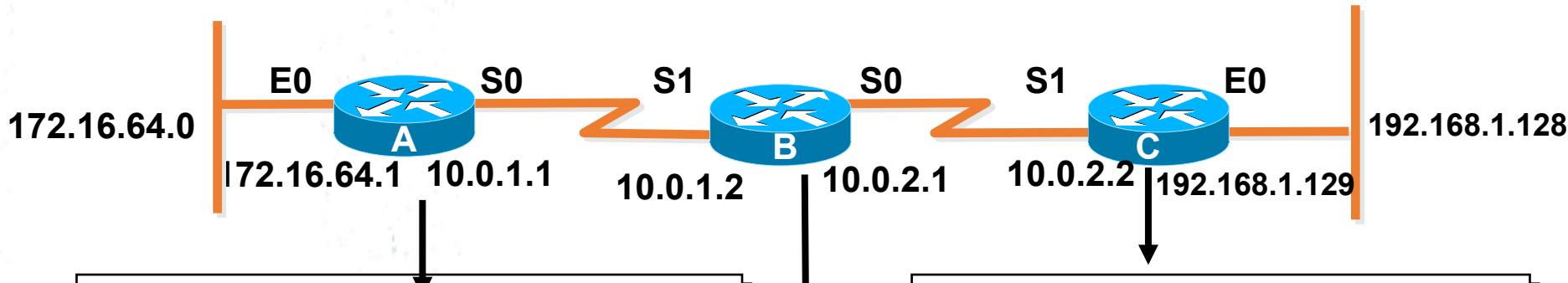
```
Router(config)#version 2
```

```
Router(config-router)#network <network-address>
```

- <network-address> : Directly connected sub-network addresses

RIP Configuration Example

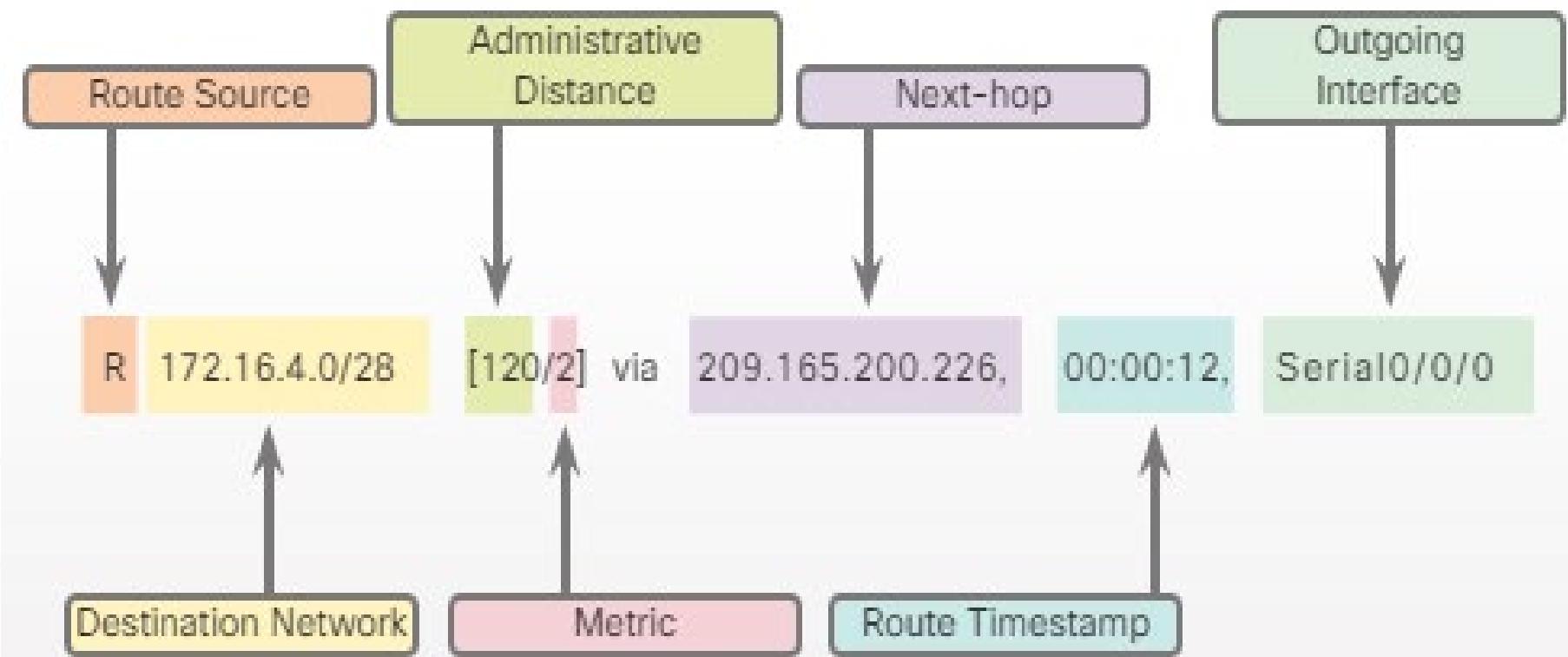
Version 2



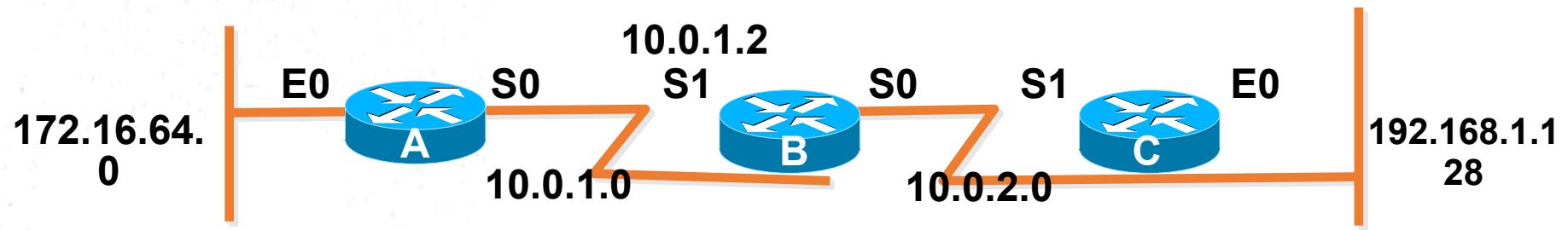
```
router rip  
Version 2  
No auto-summary  
network 172.16.64.0  
network 10.0.1.0
```

```
router rip  
Version 2  
No auto-summary  
network 192.168.1.0  
network 10.0.2.0
```

```
router rip  
Version 2  
No auto-summary  
network 10.0.1.0  
Network 10.0.2.0
```



Displaying the IP Routing Table

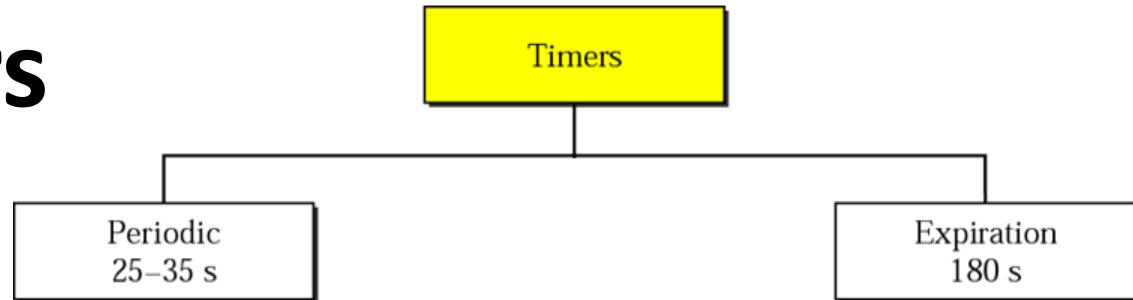


```
RouterA#sh ip route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP
```

```
172.16.0.0/24 is subnetted, 1 subnets
C 172.16.64.0 is directly connected, Ethernet0
10.0.0.0/8 is subnetted, 2 subnets
R 10.0.2.0/24 [120/1] via 10.0.1.2, 00:00:07, Serial0
C 10.0.1.0/24 is directly connected, Serial0
R 192.168.1.128/26 [120/2] via 10.0.1.2, 00:00:07,
Serial2
```

RIP Timers



- **Periodic Timer**

- A timer kept at each router for sending its routing table information to its neighbors in every 30 seconds.

- **Expiration Timer**

- If a router does not get the updates from a neighboring router for a long time ,(means it is a problem with the neighboring router) the main router removes the updates got from that neighboring router
- Is called expiration time (180 seconds)

Problems with RIP

Slow Convergence

- Routing tables are sent to neighbors every 30 seconds
- When there are large number of routers in the network ,it will take some time to get all the details to each and every router .There is a delay in getting an updated routing table.

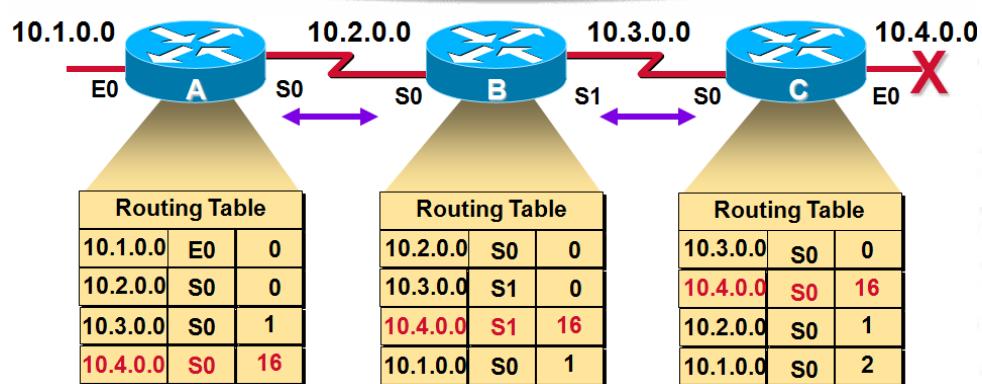
Solution

- Triggered updates
 - Information that needed to be updated immediately is informed to the other routers without waiting for the periodic time.

Counting to infinity

Solution - Route Poisoning

- When a network goes down the router that is connected to that network will get that information first
- So that router updates its table saying this network is down (unreachable)
- In the routing table it says number of hops for that particular network as infinity (or in RIP as 16)



Instability

- Once a router (P) get some updates from other router (Q) router P will update its routing table and new routing table sent again to previous router.
- With time this will lead to having wrong updated tables in the routers and ultimately to an unstable situation
- •
- •
- •

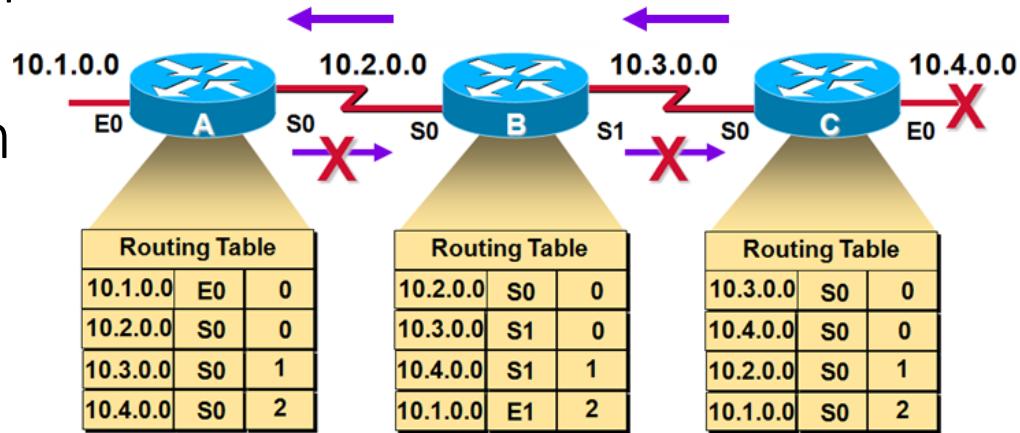
Solution

- Split Horizon
 - Do not send same information via the link which that information came from

Solutions

Split Horizon

- When the router sends routing table information to the neighbors, it will not send the information that it got from that particular router
- So the routing table information will be selected and send



Hold down Timer

- Once a network goes down, that information will be immediately sent to the other routers
- Because of the network connections there is a possibility to get some wrong information about that particular network from other routers
- Therefore once a network down information is received, the router will start the hold down timer, during which time any updates regarding that particular network is ignored.

Poison Reverse

- In general split horizon will apply for information passing
 - But the split horizon will not be applied in the case of the information like network is down
- * *
* *
* *
* *
* *
* *
* *

IGRP

AD - 100

(Interior Gateway Routing Protocol)

- A cisco proprietary distance-vector routing protocol
- Maximum hop count is 255
- Used in large networks
- EIGRP is the enhanced version of IGRP

EIGRP

Interior Gateway Protocols				Exterior Gateway Protocols	
Distance Vector Routing Protocols		Link State Routing Protocols		Path Vector	
IPv4	RIPv2	EIGRP	OSPFv2	IS-IS	BGP-4
IPv6	RIPng	EIGRP for IPv6	OSPFv3	IS-IS for IPv6	BGP-4 for IPv6

EIGRP

(Extended Interior Gateway Routing Protocol)

Features

- EIGRP was initially released in 1992 as a proprietary protocol available only on Cisco devices.
- In 2013, Cisco released a basic functionality of EIGRP as an open standard to the IETF as an informational RFC.
- Other networking vendors can now implement EIGRP on their equipment to interoperate with both Cisco and non-Cisco routers running EIGRP.

EIGRP Metric AD - 90

- A '*Composite metric*' is used
- EIGRP uses **bandwidth and delay of the line** by default as a metric for determining the best route to an internetwork
- Metric is a combination of bandwidth, delay of the line , Reliability, load and Maximum Transmission Unit (MTU)
- Reliability, load, and Maximum Transmission Unit (MTU) are not used by default

EIGRP metric values

- **Bandwidth** - The slowest bandwidth among all of the outgoing interfaces, along the path from source to destination.
- **Delay** - The cumulative (sum) of all interface delay along the path (in microseconds).

EIGRP Composite Metric

Default Composite Formula:

$$\text{metric} = [\text{K1} * \text{bandwidth} + \text{K3} * \text{delay}] * 256$$

Complete Composite Formula:

$$\text{metric} = [\text{K1} * \text{bandwidth} + (\text{K2} * \text{bandwidth}) / (256 - \text{load}) + \text{K3} * \text{delay}] * [\text{K5} / (\text{reliability} + \text{K4})]$$

(Not used if " K" values are 0)

Note: This is a conditional formula. If K5 = 0, the last term is replaced by 1 and the formula becomes: Metric = [K1*bandwidth + (K2*bandwidth)/(256-load) + K3*delay]

Default values:

K1 (bandwidth) = 1

K2 (load) = 0

K3 (delay) = 1

K4 (reliability) = 0

K5 (reliability) = 0

" K" values can be changed with the `metric weights` command

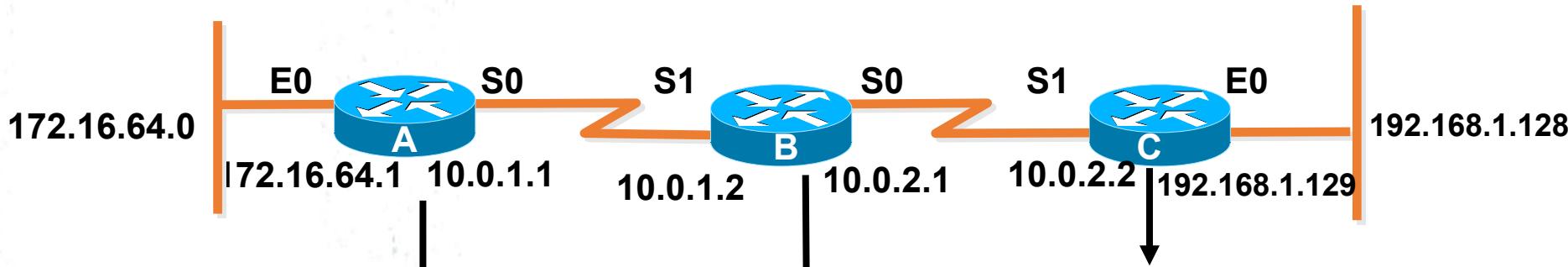
EIGRP Configuration

```
Router(config)#router Eigrp <AS number>
```

```
Router(config-router)#network <network-address>
```

- < network address > : Directly connected network addresses
- < AS number > : Autonomous Systems Number

EIGRP Configuration Example



```
router eigrp 100
```

```
network 172.16.64.0  
network 10.0.1.0
```

```
router eigrp 100
```

```
network 192.168.1.0  
network 10.0.2.0
```

```
router eigrp 100
```

```
network 10.0.1.0  
Network 10.0.2.0
```

Computer Networks

Lecture 5

Internet Protocol (IP)

OSI

7	APPLICATION
6	PRESENTATION
5	SESSION
4	TRANSPORT
3	NETWORK
2	DATA LINK
1	PHYSICAL

TCP/IP

APPLICATION
TRANSPORT
INTERNET
NETWORK ACCESS

EXAMPLES

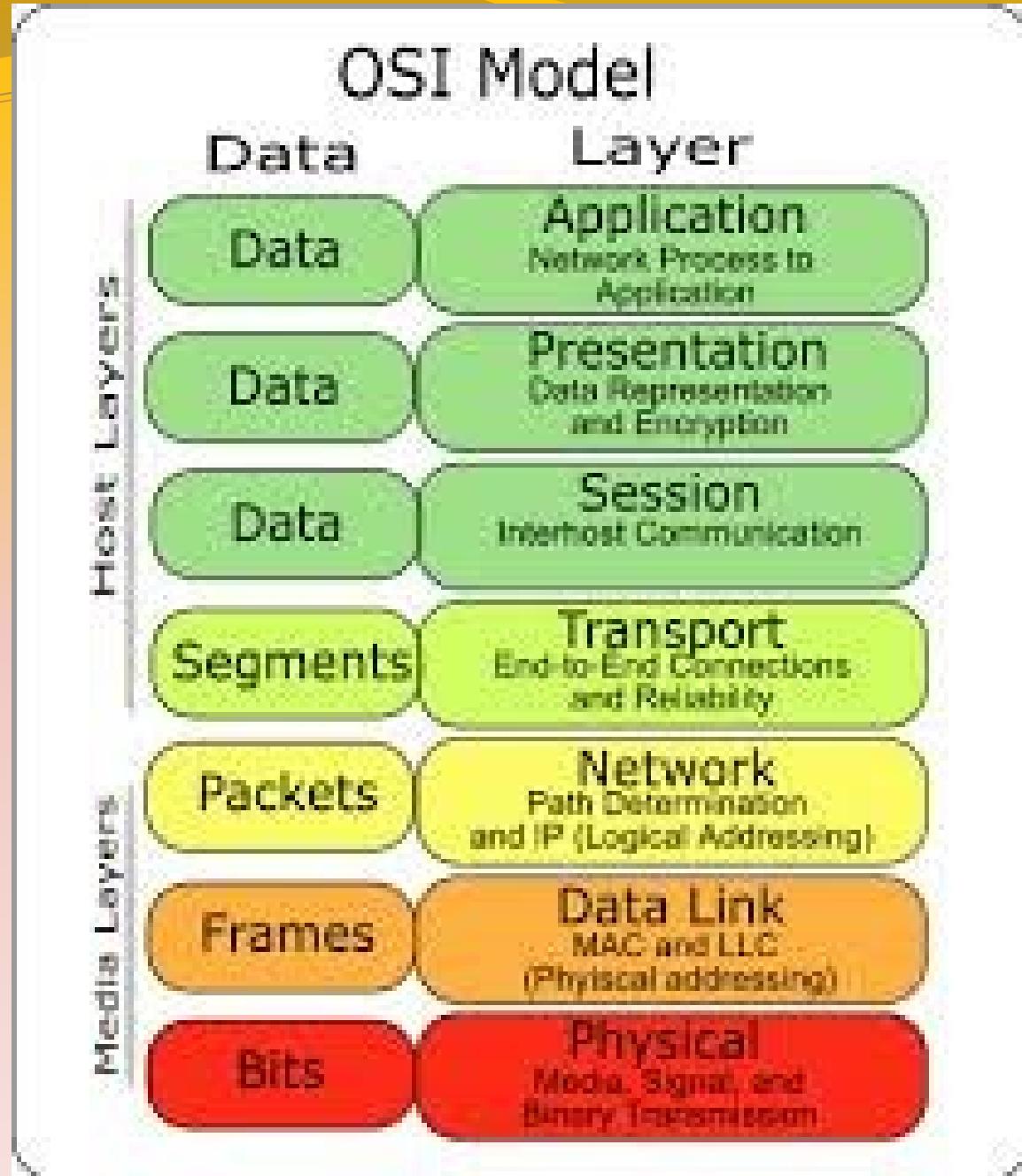
FTP, HTTP, HTTPS,
SMTP, SSH

TCP, UDP

IP (IPv4, IPv6), IPsec,
ICMP, ICMPv6

802.3 (Ethernet),
802.11 (WLAN), PPP,
ATM, Frame Relay

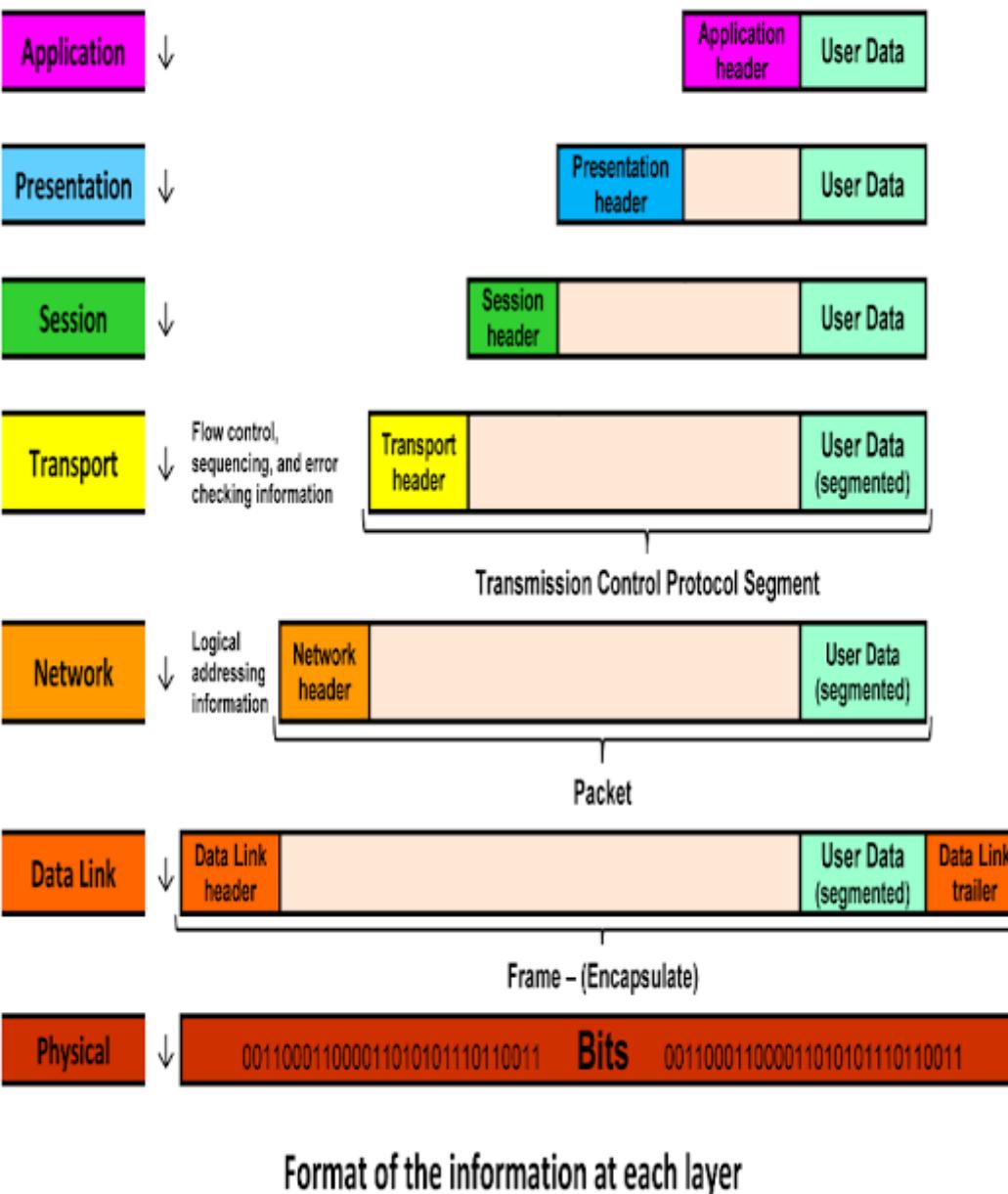
OSI Model



7 LAYERS

OSI FIGURE

DATA TRANSFORMATI



Overview of IP

- IP is the network layer protocol of TCP/IP
- No Error control, flow control and congestion control
 - Hence IP is an unreliable protocol
- Combination TCP/IP is reliable
 - But UDP/IP is an unreliable combination
- IP packets operate as datagram
- IP packets originated from same source can travel through different routes and reach the destination at different times
- Therefore IP packets may reach the destination out of order

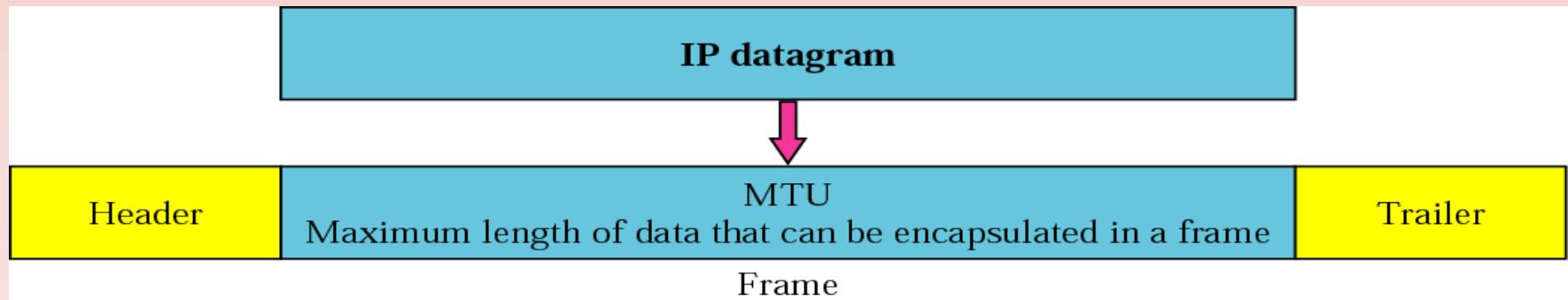
Identification

- Each IP packet is identified by a serial number called “Identification”
- This sequence will be helpful to the receiver to reassemble the packets in the correct order, although they may receive in out of order

Maximum Transmission Unit (MTU)

- Maximum amount of data that can be accommodated in a frame

Protocol	MTU
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

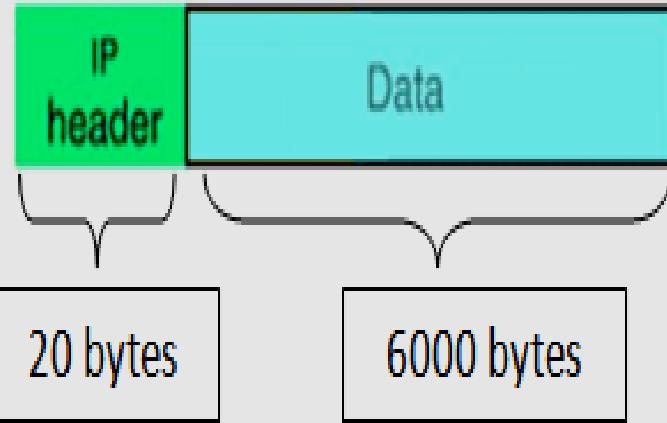


Fragmentation

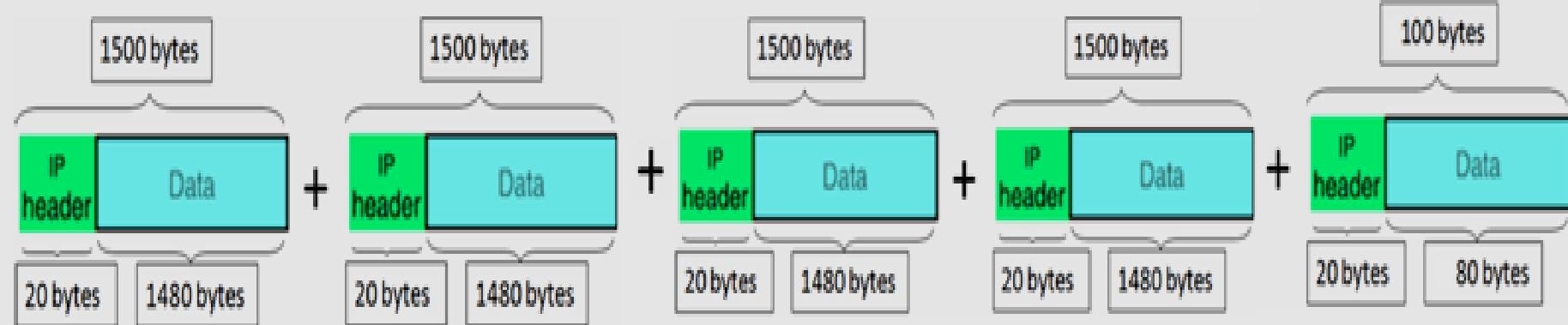
- If the IP packet size is bigger than MTU, it should be fragmented

Ex : If the original packet has 6000 bytes of data

1. Separate data and Header of IP Packet
2. Break data part into MTUs (Fragments)
3. Add 20 byte header to each fragment



Fragmentation



Fragmentation offset

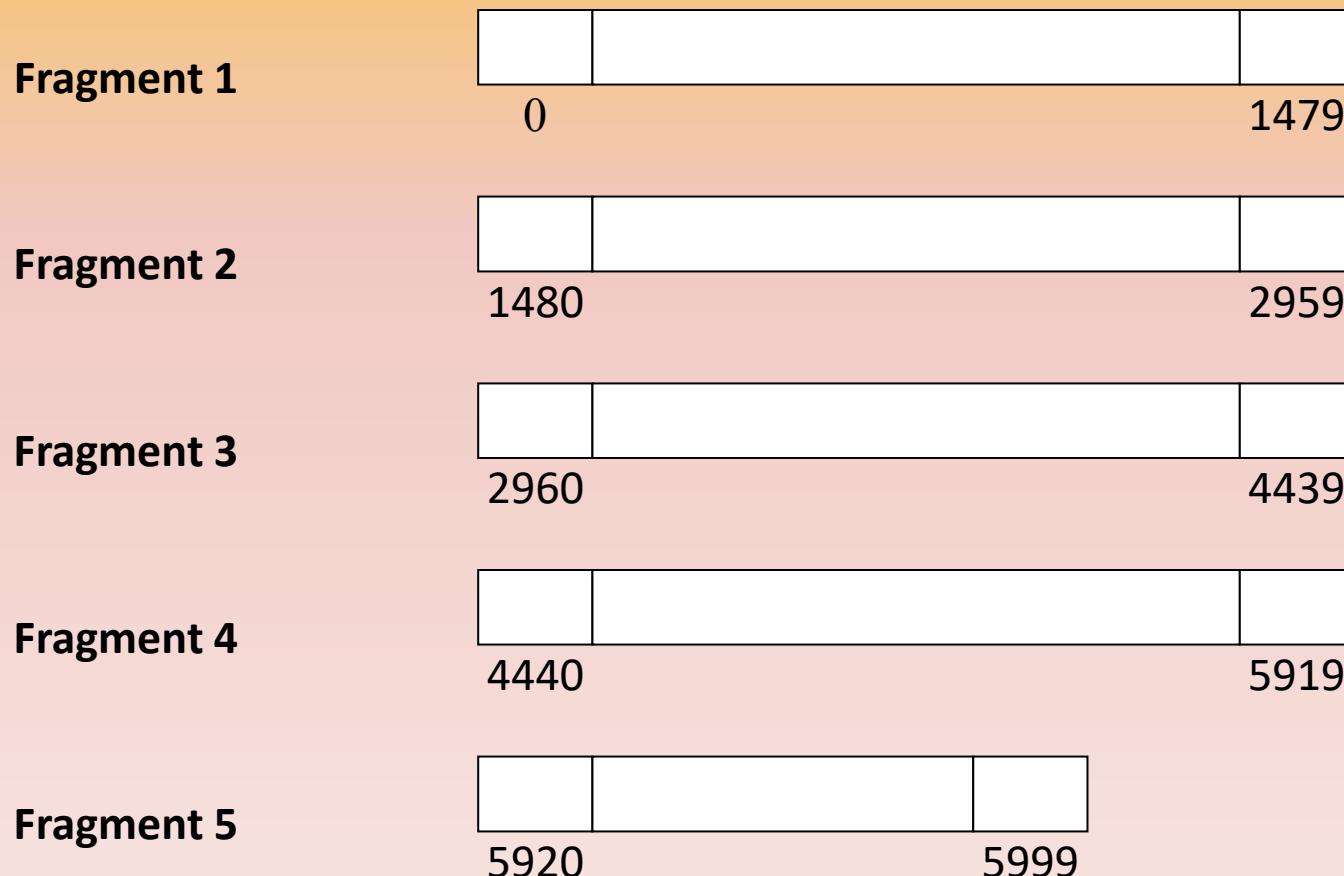
- The identification of each fragmented IP packet is equal to identification of original IP packet

Ex : If the identification of original IP packet is 2000,
identification of all five fragments is 2000

- “**Fragmentation offset**” is an another parameter used to identity the order of fragments

Fragmentation offset cont.

- If the original packet has 6000 bytes of data , the numbering of data bytes are as follows

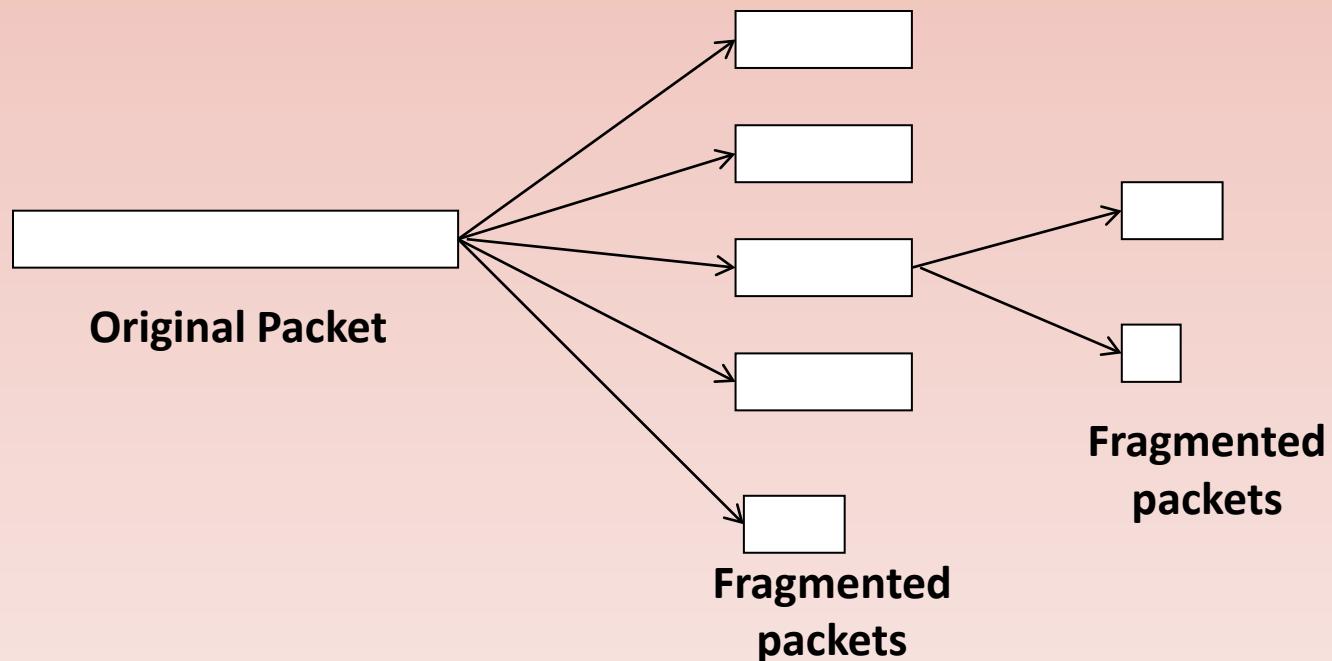


Fragmentation offset cont.

- Offset value of fragment 1 = $\frac{0}{8} = 0$
- Offset value of fragment 2 = $\frac{1480}{8} = 185$
- Offset value of fragments 3 = $\frac{2960}{8} = 370$
- Offset value of fragment 4 = $\frac{4440}{8} = 555$
- Offset value of fragment 5 = $\frac{5920}{8} = 740$

Fragmentation offset cont.

- Fragmented packets travel independently
- They may travel through different routes to the destination
- While it is traveling it can be further fragmented at another intermediate network



Fragmentation offset cont.

- Fragmented packets reach to the destination out of order.
- The fragmented packets are combined (defragmented) at the final destination by using the *OFFSET* values.

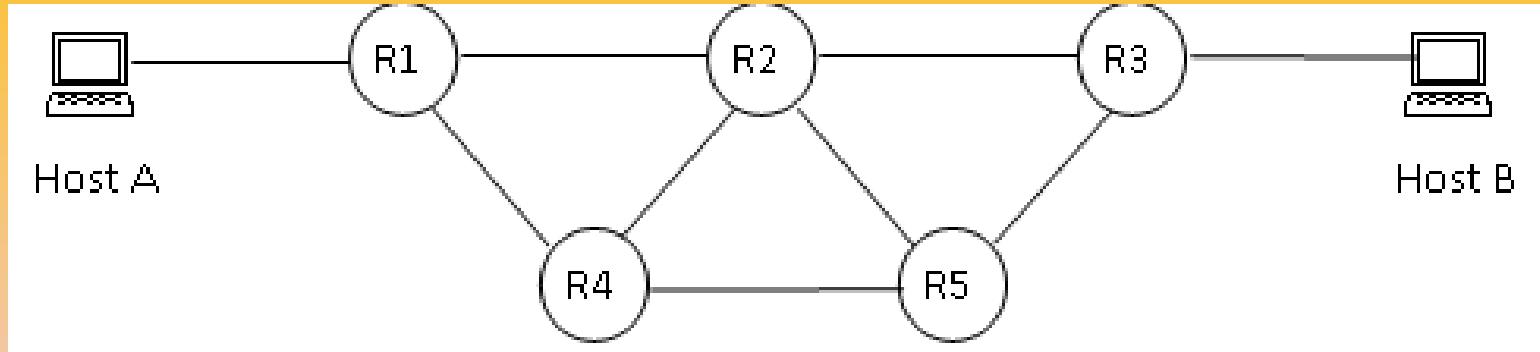
Time To Live (TTL)

- IP packets travel through many routers in the network
- Each router routes the packet according to information in the routing table
- If there is a problem in a routing table the packet may be sent in a wrong direction and it can be randomly flow in the network. This kind of IP packets can even overload the network and finally crash the network
- In order to avoid such a situation, a parameter called “Time To Live” (TTL) is defined for each IP packet

Time To Live (TTL) cont.

- TTL value can be initialized to any value at the transmitting router (A) (maximum is 255)
- The TTL value is decremented at each router by 1
- If the TTL value becomes zero at a router (B) , the packet will be discarded and an ICMP message is sent to the transmitted router(A) from the discarding router (B)

Time To Live (TTL) cont.

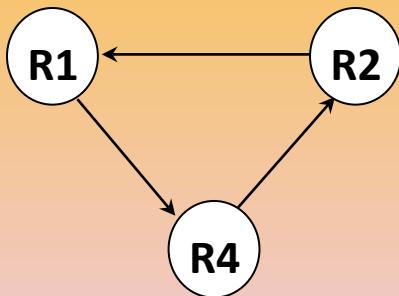


- Suppose host A sends an IP packet to Host B
- The TTL value is set to 6
- If the packet goes through Host A → R1 → R2 → R3 → Host B,

Router	TTL Value
R1	= 5
R2	= 4
R3	= 3

Time To Live (TTL) cont.

- Suppose there is a routing problem and the packet loops through the routes $R1 \rightarrow R4 \rightarrow R2 \rightarrow R1 \rightarrow R4 \rightarrow R2 \rightarrow R1 \rightarrow R4 \rightarrow R2$



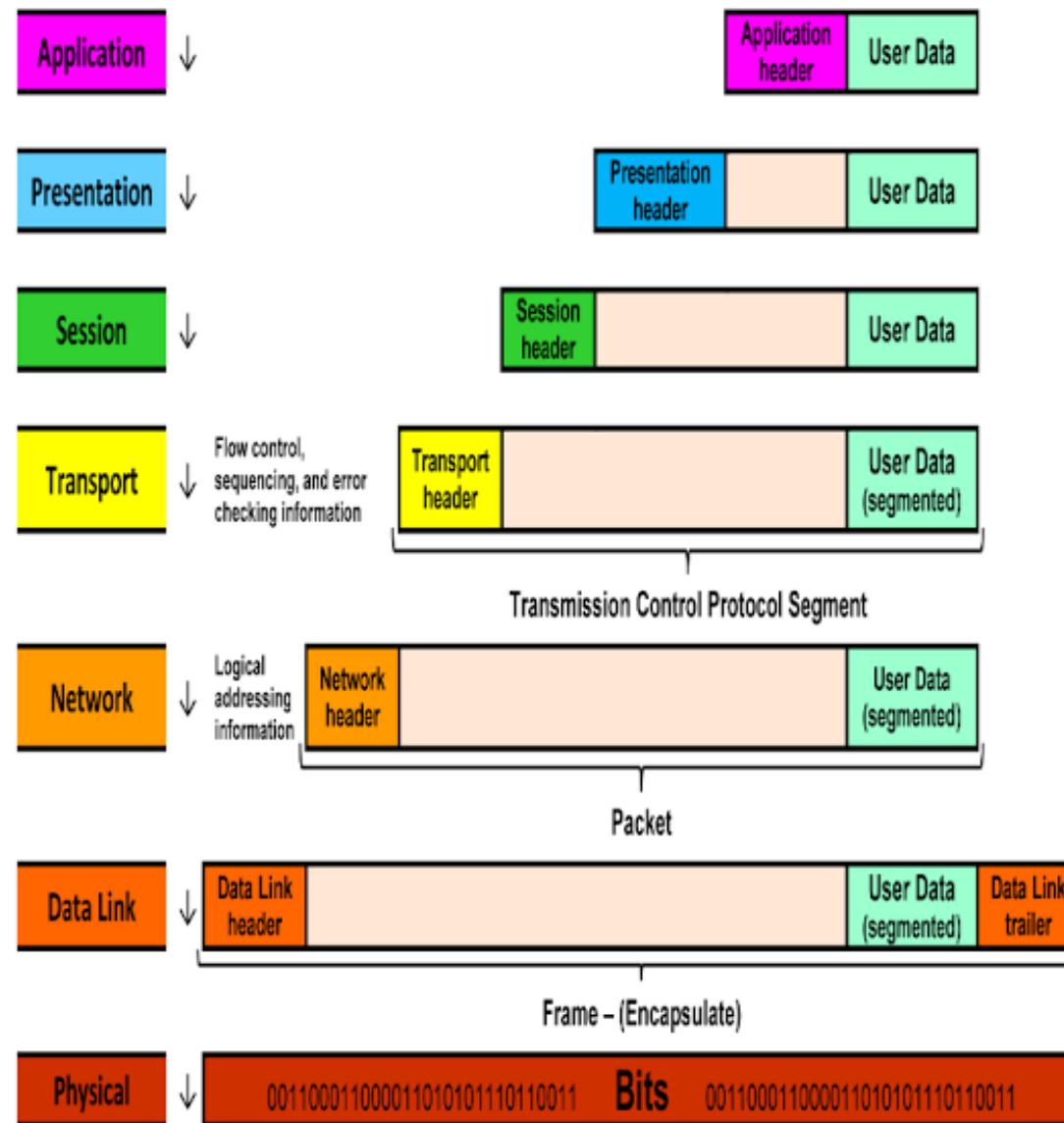
Router	TTL Value	Action
R1	$6 - 1 = 5$	
R4	$5 - 1 = 4$	
R2	$4 - 1 = 3$	
R1	$3 - 1 = 2$	
R4	$2 - 1 = 1$	
R2	$1 - 1 = 0$	Discards the Packet Send ICMP message to Host A

- The TTL value becomes zero at router R2
- Therefore IP packet is discarded

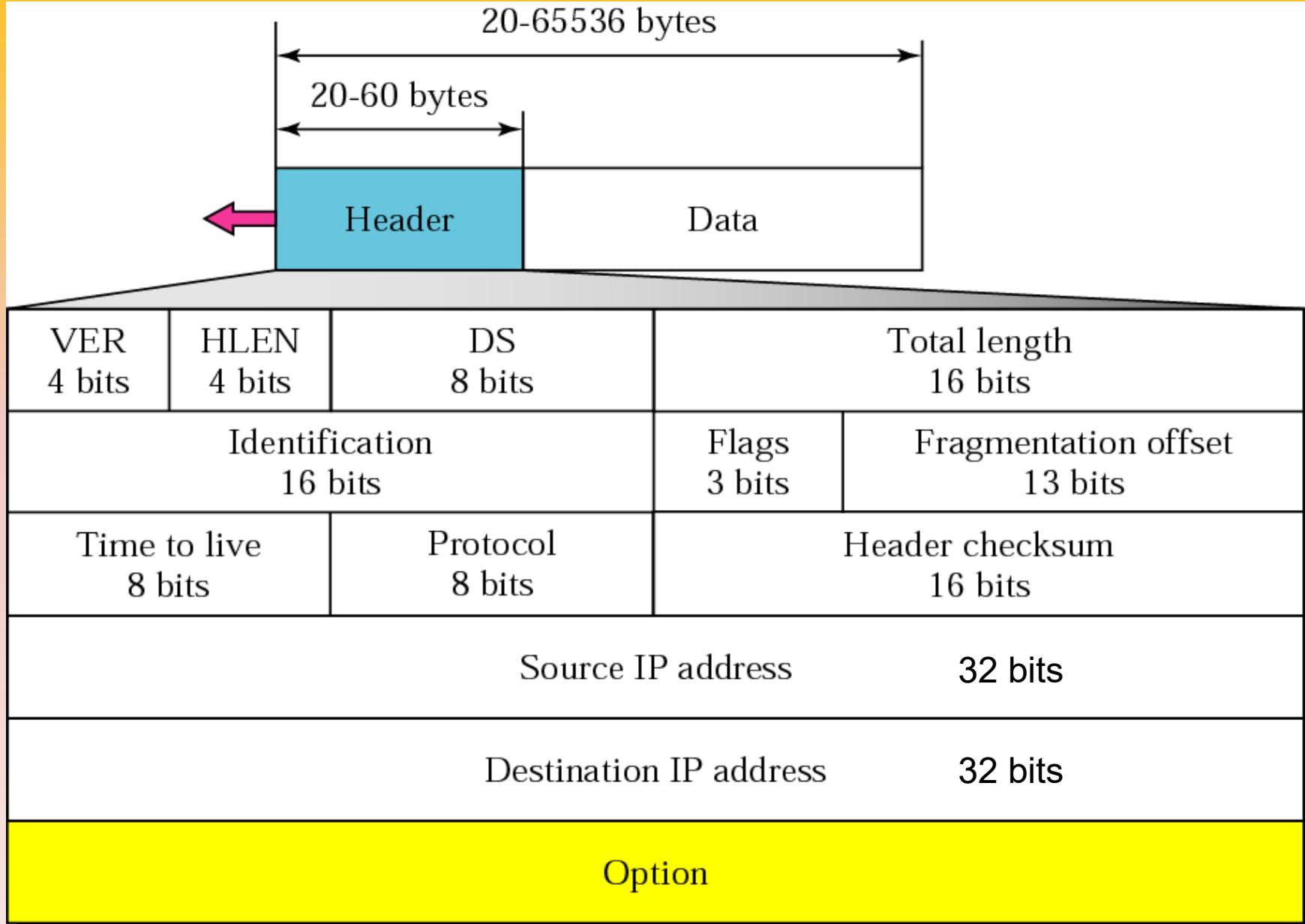
7 LAYERS

OSI FIGURE

DATA TRANSFORMATI



IP header



Version (VER)

- A field of 4 bits
- Indicates the version of the using IP addresses in the IP packet

IPv4 : 0100

IPv6 : 0110

Header Length (HLEN)

- A 4 bit field indicates the number of 4 bytes in the header
- Header size in bytes = HLEN x 4
- The standard header size = 20 bytes

$$20 = 5 \times 4$$

$$\text{HLEN} = 5 \quad (0101)_2$$

- The standard header size = 60 bytes

$$60 = 15 \times 4$$

$$\text{HLEN} = 15 \quad (1111)_2$$

Service Type

- A 8 bit field
- IETF has changed the name of this field as **Differentiated Services**



- **Precedence** defines the priority of the packet
- **Precedence** is not used in IPv4

Service Type cont.

- A 4-bit field
- Each bit has a special meaning
- There are five types of services

<i>TOS Bits</i>	<i>Description</i>
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

Service Type cont.

The application can select a specific type of service

<i>Protocol</i>	<i>TOS Bits</i>	<i>Description</i>
ICMP	0000	Normal
BOOTP	0000	Normal
NNTP	0001	Minimize cost
IGP	0010	Maximize reliability
SNMP	0010	Maximize reliability
TELNET	1000	Minimize delay
FTP (data)	0100	Maximize throughput
FTP (control)	1000	Minimize delay
TFTP	1000	Minimize delay
SMTP (command)	1000	Minimize delay
SMTP (data)	0100	Maximize throughput
DNS (UDP query)	1000	Minimize delay
DNS (TCP query)	0000	Normal
DNS (zone)	0100	Maximize throughput

Total length

- A 16-bit field
- Gives the total length of the IP packet.

Total length = data length + header length

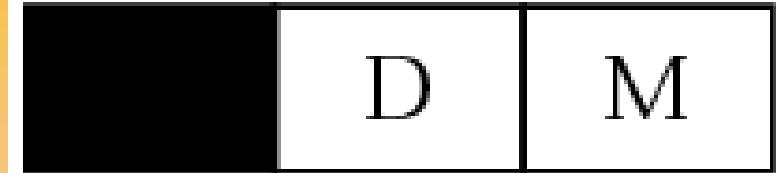
- If total length value is 300 and if this is a normal IP packet
Header length = 20 bytes
Data length = $300 - 20$
= 280 bytes

Identification

- Each IP packet is identified by a serial number called “**Identification**”
- A 16 bit field
- The identification of each fragmented IP packet is equal to identification of original IP packet

Flags

D: Do not fragment
M: More fragments



- **$D = 1$** , means is not allowed to be fragmented
- **$D = 0$** , means is allowed to be fragmented
- **$M = 0$** , means that there are no more fragments;
The fragment is the last one.
Non fragmented packet is considered the last fragment
- **$M = 1$** , The fragment is not the last one.

Fragmentation offset

- A 13-bit field
- This gives the offset value of the fragment

Time To Live (TTL)

- A 8 bit field
- Defines the maximum number of hops the packet can travel

Protocol

- The IP packet data can be UDP, TCP, ICMP, IGMP, EGP
- Used to identify the type of data a special field called “protocol”
- A a 8-bit field which defines the protocol number

<i>Value</i>	<i>Protocol</i>
1	ICMP
2	IGMP
6	TCP
17	UDP
89	OSPF

Header Checksum

- A 16-bit field
- Checks the errors of the header only.
- If errors are found in the header, the whole IP packet is discarded.

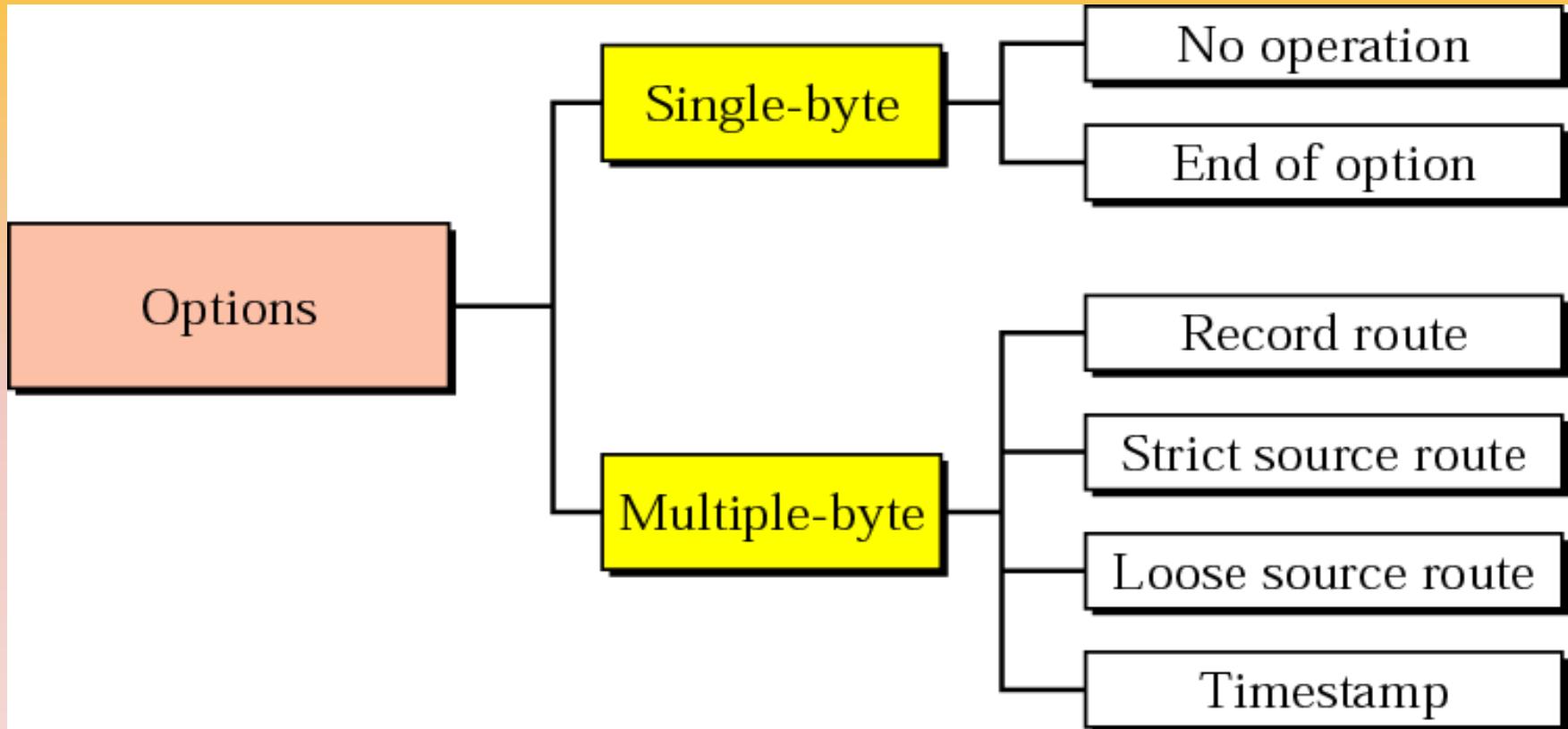
Source IP Address

- A 32-bit field
- This gives the IP address of the source

Destination IP Address

- A 32-bit field
- This gives the IP address of the destination

IP option



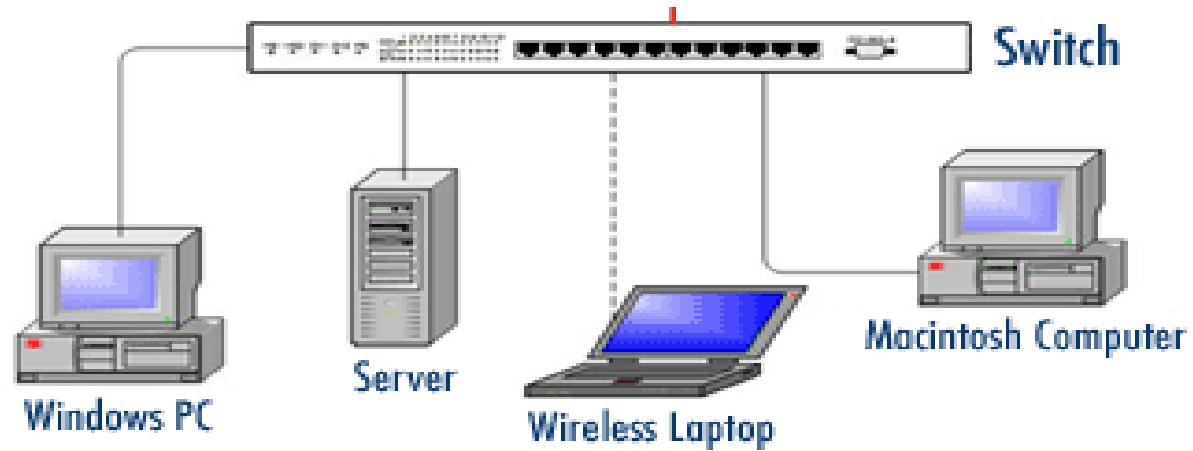
IT2050 – Computer Networks

Lecture 04
Switched Networks

Switch



Catalyst
Switch



An intelligent device

Operates in layer 2 – layer2 switch

Operates in layer 3 – layer3 switch

Form Factors

Fixed Configuration

Modular Configuration

Stackable Configuration



Business Considerations On Selecting switches

- Cost
 - Speed and #of Interfaces , Supported Features
 - Expansion Capability
 - Port Density
 - #of devices on the Network
 - Power
 - Power access points , PoE , Redundant Power Supply
 - Reliability
 - 24/7 Continues access
 - Port Speed
 - Ethernet , FastEthernet , GigabitEthernet
 - Scalability
 - Network growth
- •
• •
• •
• •
• •
• •
• •

Switch Functions

- Address learning
- Forward/filter decisions
- Loop avoidance

Mac Address Table

- The switch learns the relationship of ports to devices, it builds a table called a MAC address.
- LAN switches determine how to handle incoming frames by maintaining the MAC address table. Switch builds its MAC address table by recording the MAC address of each device connected to each of its ports.
- The switch uses the information in the MAC address table to send frames destined for a specific device out the port which has been assigned to that device.

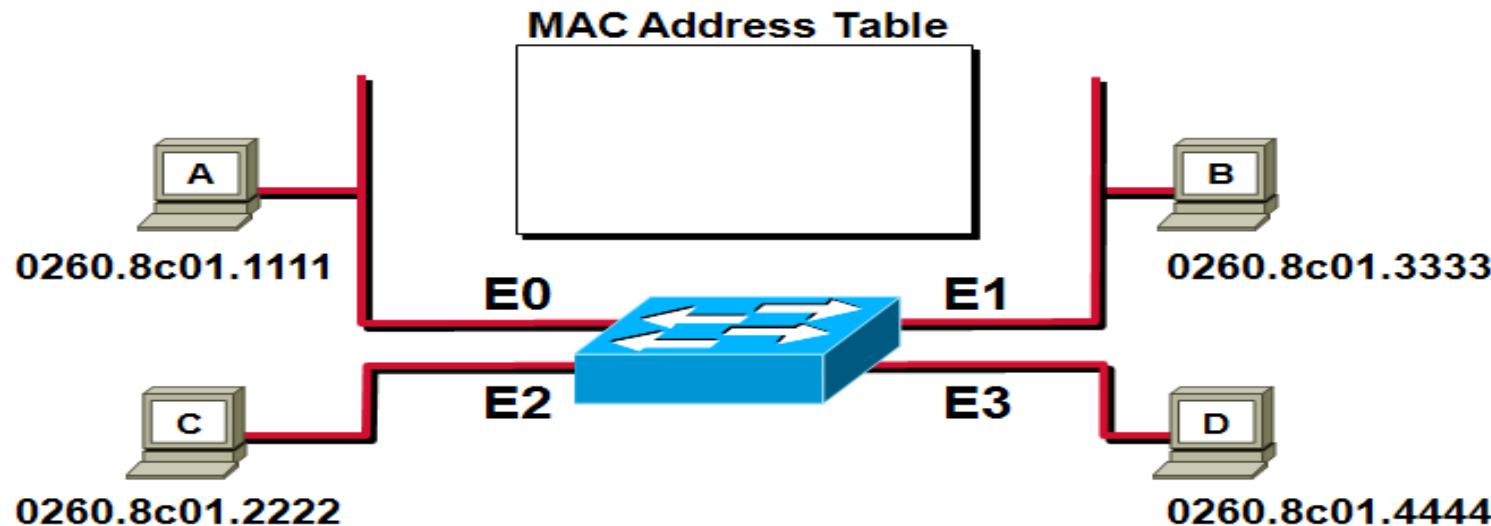
Address learning

- Layer 2 switches and bridges remember the source MAC address of each frame received on an interface, and they enter this information into a MAC database called a MAC address table

Switches use the following logic to learn MAC address table entries:

- a. For each received frame, examine the source MAC address and note the interface from which the frame was received.
- b. If they are not already in the table, add the address and interface, setting the inactivity timer to 0.
- c. If it is already in the table, reset the inactivity timer for the entry to 0.

Address learning cont.



- Initial MAC address table is empty.

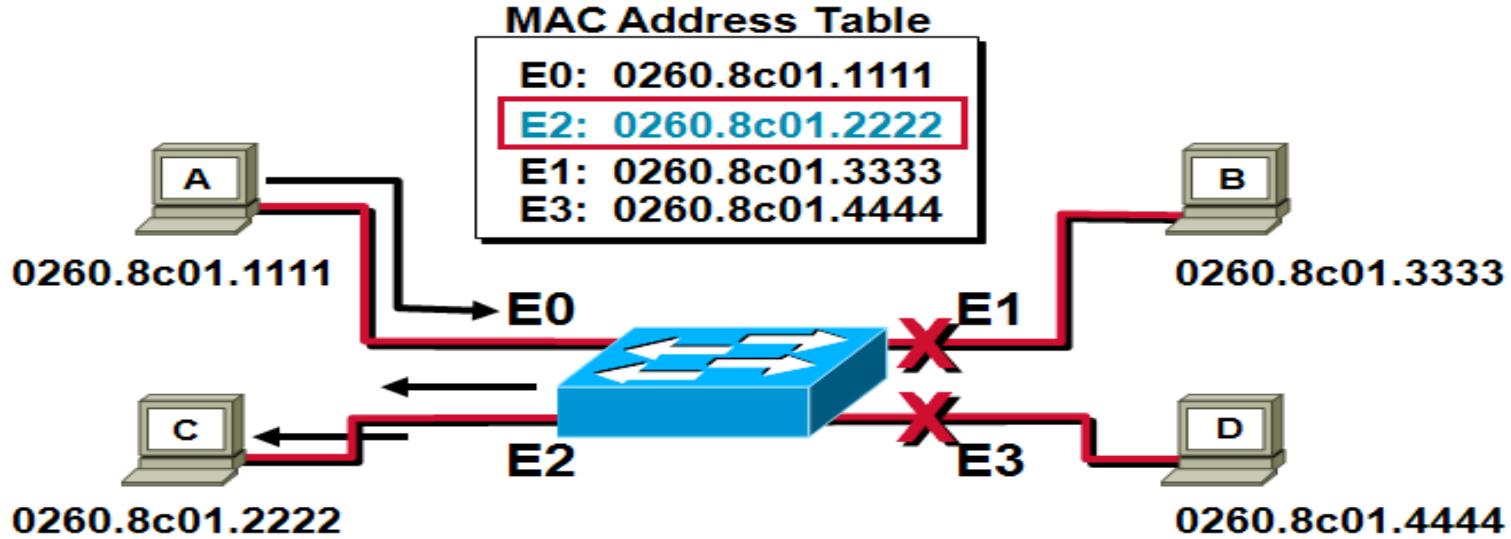
Forward/filter decisions

- When a frame is received on an interface, the switch looks at the destination MAC address and finds the exit interface in the MAC address table. Frame is only forwarded out the specified destination port.

Switches forward frames based on the destination address:

- a. If the destination address is a broadcast, multicast, or unknown destination unicast (a unicast not listed in the MAC table), the switch floods the frame.
- b. If the destination address is a known unicast address (a unicast address found in the MAC table):
 - i. If the outgoing interface listed in the MAC address table is different from the interface in which the frame was received, the switch forwards the frame out the outgoing interface.
 - ii. If the outgoing interface is the same as the interface in which the frame was received, the switch filters the frame, meaning that the switch simply ignores the frame and does not forward it.

Forward/filter decisions cont



- **Station A sends a frame to station C.**
- **Destination is known; frame is not flooded.**

Loop Avoidance

- If multiple connections between switches are created for redundancy purposes, network loops can occur
- Spanning Tree Protocol (STP) is used to stop network loops while still permitting redundancy

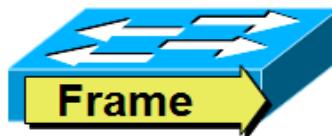
Switch Internal Processing

Switching Method	Description
Store-and-forward	The switch fully receives all bits in the frame (store) before forwarding the frame (forward). This allows the switch to check the FCS before forwarding the frame.
Cut-through	The switch forwards the frame as soon as it can. This reduces latency but does not allow the switch to discard frames that fail the FCS check.
Fragment-free	The switch forwards the frame after receiving the first 64 bytes of the frame, thereby avoiding forwarding frames that were errored due to a collision.

Switch Internal Processing cont.

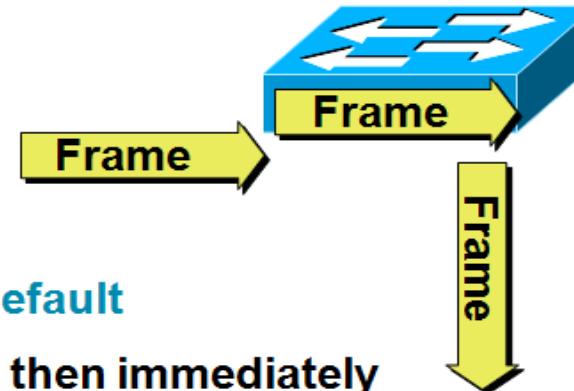
Cut-Through

- Switch checks destination address and immediately begins forwarding frame.



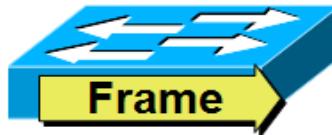
Store and Forward

- Complete frame is received and checked before forwarding.



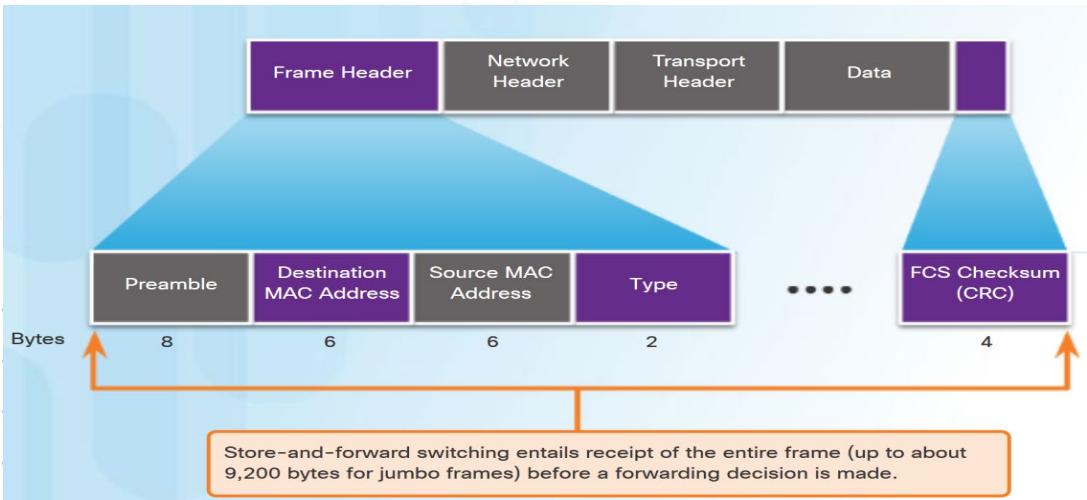
Fragment-Free (Modified Cut-Through)—Cat1900 Default

- Switch checks the first 64 bytes, then immediately begins forwarding frame.



Frame Forwarding

Store-and-Forward Switching



- **Error Checking**— After receiving the entire frame, the switch compares the frame-check-sequence (FCS) value in the last field against its own FCS calculations. Only error-free frames are forwarded

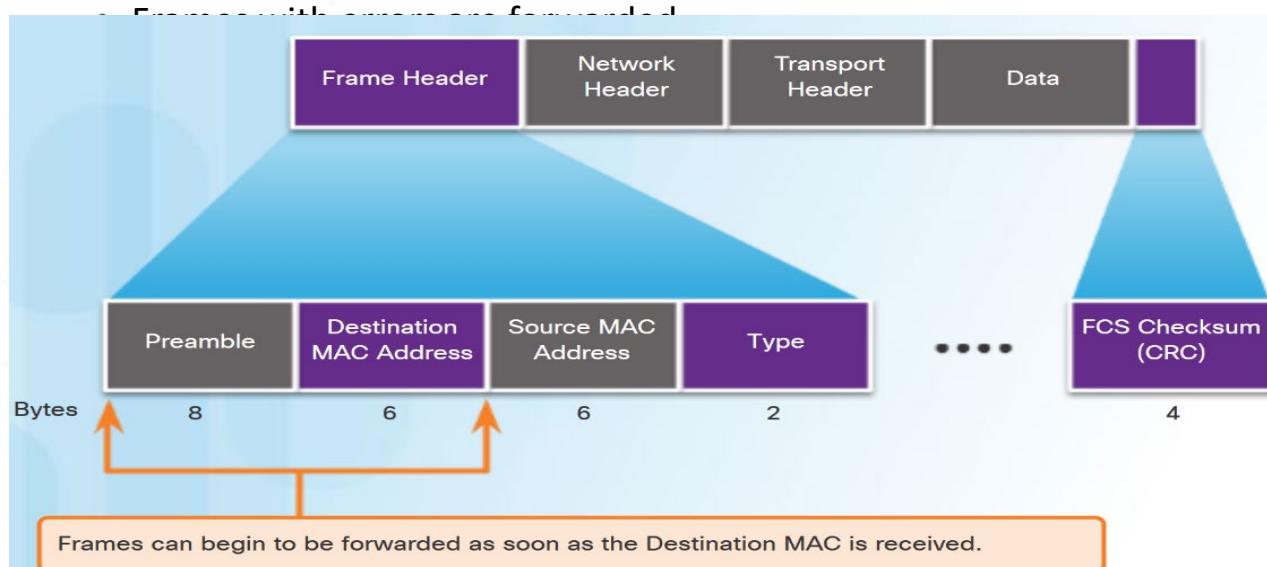
- Store-and-Forward is Cisco's primary LAN switching method.

Frame Forwarding

Cut-Through Switching

- Cut – Through Switching (Rapid Frame Forwarding) –

The switch makes a forwarding decision as soon as it has looked up the destination MAC address.



Frame Forwarding

Fragment Free Switching

- Fragment Free - modified form of cut-through switching. The switch waits for the collision window (64 bytes) to pass before forwarding the frame.
 - Provides better error checking than cut-through, with practically no increase in latency.



Basic Switch Configurations

- Each port/interface does not need an IP address because the switch is not performing Layer 3 routing
- Can assign IP address to manage the switch or else IP would not be needed on the switch at all

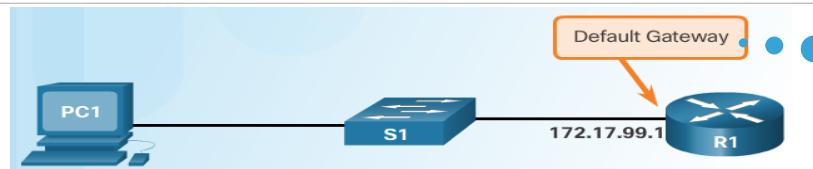
* *
* *
* *
* *
* *
* *
* *
* *

Configuring Basic Switch Management Access with IPv4

Cisco Switch IOS Commands

Enter global configuration mode.	S1# configure terminal
Enter interface configuration mode for the SVI.	S1(config)# interface vlan 99
Configure the management interface IP address.	S1(config-if)# ip address 172.17.99.11 255.255.255.0
Enable the management interface.	S1(config-if)# no shutdown
Return to the privileged EXEC mode.	S1(config-if)# exit
Configure the default gateway for the switch.	S1(config)# ip default-gateway 172.17.99.1
Return to the privileged EXEC mode.	S1(config)# end
Save the running config to the startup config.	S1# copy running-config startup-config

Important Concept



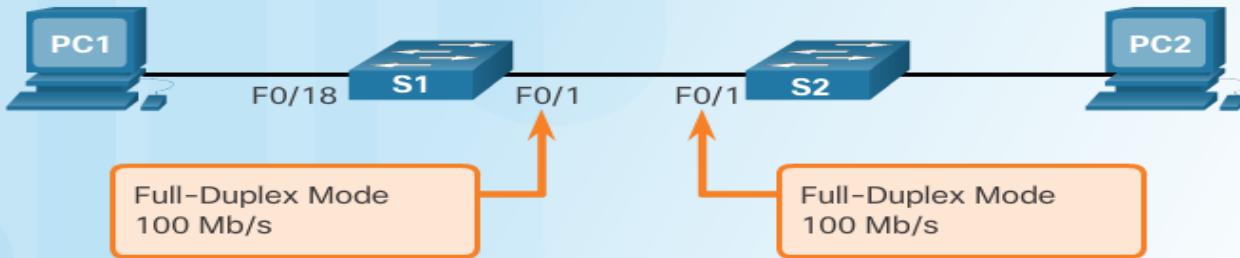
The default gateway is the router address and is used by the switch to communicate with other networks.

Configure Switch Ports

Verifying Switch Port Configuration

Cisco Switch IOS Commands

Display interface status and configuration.	S1# show interfaces [interface-id]
Display current startup configuration.	S1# show startup-config
Display current operating config.	S1# show running-config
Display information about flash file system.	S1# show flash
* Display system hardware and software status.	S1# show version
* Display history of commands entered.	S1# show history
* Display IP information about an interface.	S1# show ip [interface-id]
* Display the MAC address table.	S1# show mac-address-table OR S1# show mac address-table
* *	
* *	



Cisco Switch IOS Commands

Enter global configuration mode.	<code>S1# configure terminal</code>
Enter interface configuration mode.	<code>S1(config)# interface FastEthernet 0/1</code>
Configure the interface duplex.	<code>S1(config-if)# duplex full</code>
Configure the interface speed.	<code>S1(config-if)# speed 100</code>
Return to the privileged EXEC mode.	<code>S1(config-if)# end</code>
Save the running config to the startup config.	<code>S1# copy running-config startup-config</code>



SLIIT

Discover Your Future

IT2050 - Computer Networks

Lecture 7

Securing Switched Networks

MAC Address Table

- Dynamic MAC addresses
 - Sticky MAC addresses
 - Permanent MAC addresses
- ⋮ ⋮
⋮ ⋮
⋮ ⋮
⋮ ⋮
⋮ ⋮
⋮ ⋮
⋮ ⋮
⋮ ⋮

- Port security limits the number of valid MAC addresses allowed to transmit data through a switch port.
- If a port has port security enabled and an unknown MAC address sends data, the switch presents a security violation.
- Default number of secure MAC addresses allowed is 1.

- Methods used to configure MAC addresses within port security:
 - Static secure MAC addresses – manually configure **switchport port-security mac-address *mac-address***
 - Dynamic secure MAC addresses – dynamically learned and removed if the switch restarts
 - Sticky secure MAC addresses – dynamically learned and added to the running configuration (which can later be saved to the startup-config to permanently retain the MAC addresses)
- **switchport port-security mac-address sticky *mac-address***

Dynamic MAC Addresses

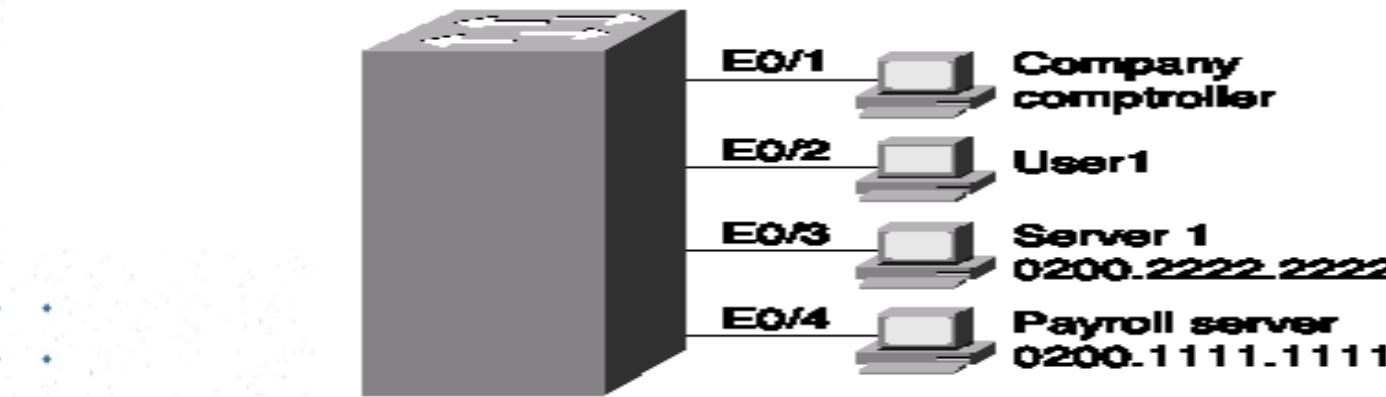
- MAC addresses are added to the MAC address table through normal switch processing
- When a frame is received, the source MAC of the frame is associated with the incoming port/interface

```
wg_sw_a#show mac-address-table
```

```
* * wg_sw_a#sh mac-address-table
Number of permanent addresses : 0
* * Number of restricted static addresses : 0
* * Number of dynamic addresses : 6
* *
* * Address          Dest      Interface   Type    Source Interface List
* *
* * -----
* * 00E0.1E5D.AE2F   Ethernet   0/2        Dynamic  All
* * 00D0.588F.B604   FastEthernet 0/26      Dynamic  All
* * 00E0.1E5D.AE2B   FastEthernet 0/26      Dynamic  All
* * 0090.273B.87A4   FastEthernet 0/26      Dynamic  All
* * 00D0.588F.B600   FastEthernet 0/26      Dynamic  All
* * 00D0.5892.38C4   FastEthernet 0/27      Dynamic  All
```

Permanent MAC addresses

- A MAC address is associated with a port



```
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address 0200.1111.1111
```

Switch Port Security

Secure Unused Ports

The **interface range** command can be used to apply a configuration to several switch ports at one time.

Disable Unused Ports

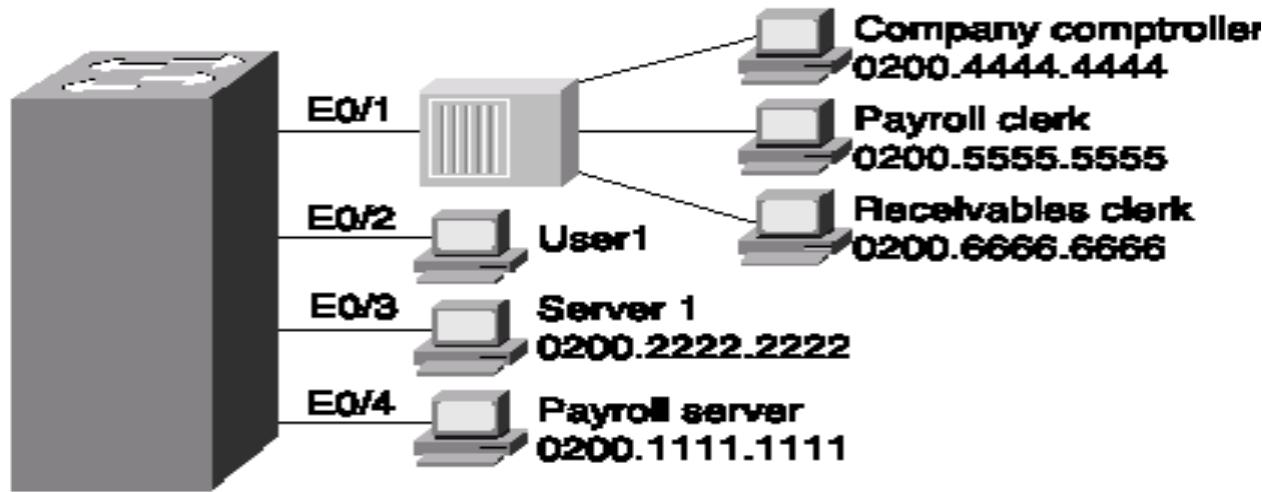


```
S1# show run
Building configuration...
...
version 15.0
hostname S1
...
interface FastEthernet0/4
    shutdown
!
interface FastEthernet0/5
    shutdown
!
interface FastEthernet0/6
    description web server
!
interface FastEthernet0/7
    shutdown
!
...
```

Disable unused ports using the **shutdown** command.

Port Security

- Limits the number of MAC addresses associated with a port (limits number of sources that can forward frames into that switch port)



```
Switch(config)#interface <interface name>
```

```
Switch(config-if)#switchport port-security maximum <number>
```

Port Security cont.

- Restrict port 0/1 so that only three MAC addresses can be learned on port 0/1

```
Switch(config)#interface Ethernet 0/1
```

```
Switch(config-if)# switchport port-security maximum 3
```

Address violation

- What should the switch do when a fourth MAC address sources a frame that enters E0/1?
- An address violation occurs when a secured port receives a frame from a new source address that, if added to the MAC table, would cause the switch to exceed its address table size limit for that port

Port Security: Violation Modes

- Protect
 - data from unknown source MAC addresses are dropped; a security notification **IS NOT** presented by the switch
- Restrict –
 - data from unknown source MAC addresses are dropped; a security notification **IS** presented by the switch and the violation counter increments.
- Shutdown –
 - (default mode) interface becomes error-disabled and port LED turns off. The violation counter increments. Issues the shutdown and then the no shutdown command on the interface to bring it out of the error-disabled **state**.

Violation Mode	Forwards Traffic	Sends Syslog Message	Displays Error Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No	No
Restrict	No	Yes	No	Yes	No
Shutdown	No	No	No	Yes	Yes

Security Violations Occur In These Situations

- A station with MAC address that is not in the address table attempts to access the interface when the table is full.
- An address is being used on two secure interfaces in the same VLAN.

Switch Port Security

Port Security: Configuring

Feature	Default Setting
Port security	Disabled on a port
Maximum number of secure MAC addresses	1
Violation mode	Shutdown. The port shuts down when the maximum number of secure MAC addresses is exceeded.
Sticky address learning	Disabled

* *
* *
* *
* *
* *
* *
* *

Switch Port Security

Port Security: Configuring (Cont.)

- Before configuring port-security features, place the port in access mode and use the **switchport port-security** interface configuration command

Configure Dynamic Port Security



Cisco IOS CLI Commands

Specify the interface to be configured for port security.

```
S1(config) # interface fastethernet 0/18
```

Set the interface mode to access.

```
S1(config-if) # switchport mode access
```

Enable port security on the interface.

```
S1(config-if) # switchport port-security
```

Most common configuration error is to forget this command!

Switch Port Security

Port Security: Configuring (Cont.)

Configure Sticky Port Security

The diagram illustrates a network setup with a switch labeled S1. It has two ports, F0/18 and F0/19, each connected to a computer. The connection from S1 to PC1 is labeled F0/18 and the connection to PC2 is labeled F0/19. PC1 is associated with the MAC address 0025.83e6.4b01, and PC2 is associated with the MAC address 0025.83e6.4b02.

Cisco IOS CLI Commands

Specify the interface to be configured for port security.	S1(config)# interface fastethernet 0/19
Set the interface mode to access.	S1(config-if) # switchport mode access
Enable port security on the interface.	S1(config-if) # switchport port-security
Set the maximum number of secure addresses allowed on the port.	S1(config-if) # switchport port-security maximum 10
Enable sticky learning.	S1(config-if) # switchport port-security mac-address sticky

A large blue arrow points diagonally across the command table, highlighting the last command: `S1(config-if) # switchport port-security mac-address sticky`. A text overlay on the arrow reads: "Most common configuration error is to forget this command!"

Port Security: Verifying

- Use the **show port-security interface** command to verify the maximum number of MAC addresses allowed on a particular port and how many of those addresses were learned dynamically using sticky.
- .
- .
- .
- .

```
S1# show port-security interface fastethernet 0/18
+
* Port Security : Enabled
* Port Status   : Secure-up
* Violation Mode: Shutdown
* Aging Time   : 0 mins
* Aging Type   : Absolute
SecureStatic Address Aging : Disabled
* Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0025.83e6.4b01:1
Security Violation Count : 0
```

```
S1# show port-security interface fastethernet 0/19
+
* Port Security : Enabled
* Port Status   : Secure-up
* Violation Mode: Shutdown
* Aging Time   : 0 mins
* Aging Type   : Absolute
SecureStatic Address Aging : Disabled
* Maximum MAC Addresses : 10
Total MAC Addresses : 1
Configured MAC Addresses : 0
Sticky MAC Addresses : 1
Last Source Address:Vlan : 0025.83e6.4b02:1
Security Violation Count : 0
```



Port Security: Verifying (Cont.)

- Use the **show running-config** command to see learned MAC addresses added to the configuration.

```
* * *  
* . . S1# show run | begin FastEthernet 0/19  
* . . interface FastEthernet0/19  
* . .   switchport mode access  
* . .   switchport port-security maximum 10  
* . .   switchport port-security  
* . .   switchport port-security mac-address sticky  
* . .   switchport port-security mac-address sticky 0025.83e6.4b02  
* . .  
* * *
```



SLIIT

Discover Your Future

IT2050 – Computer Networks

Lecture 7

Virtual Local Area Networks (VLAN)

.....

Sections & Objectives

VLAN Segmentation

- Explain the purpose of VLANs in a switched network.
- Explain how a switch forwards frames based on VLAN configuration in a multi-switch environment.

VLAN Implementations

- Configure a switch port to be assigned to a VLAN based on requirements.
- Configure a trunk port on a LAN switch.
- Troubleshoot VLAN and trunk configurations in a switched network.

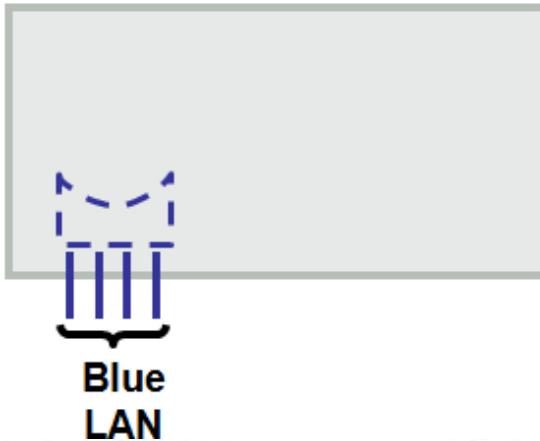
Inter-VLAN Routing Using Routers

- Describe the two options for configuring Inter-VLAN routing.
- Configure Router-on-a-Stick Inter-VLAN Routing

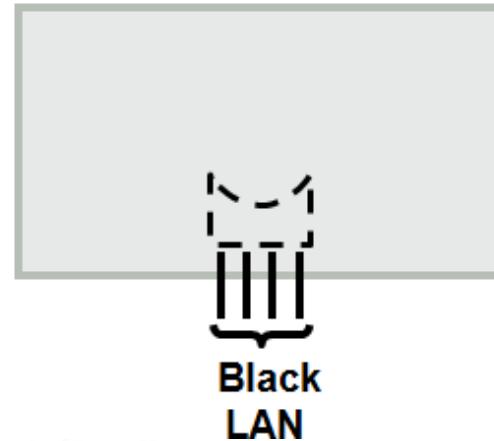
VLAN Segmentation

Broadcast Domains

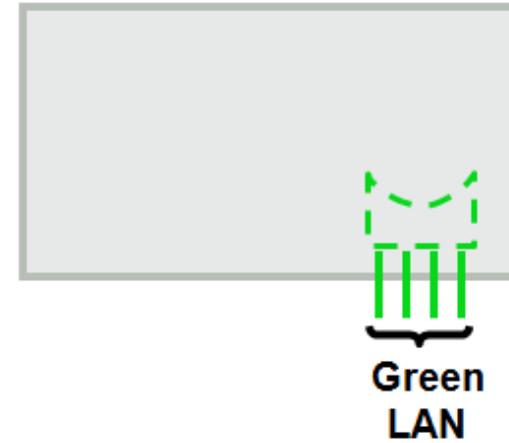
Switch X



Switch Y



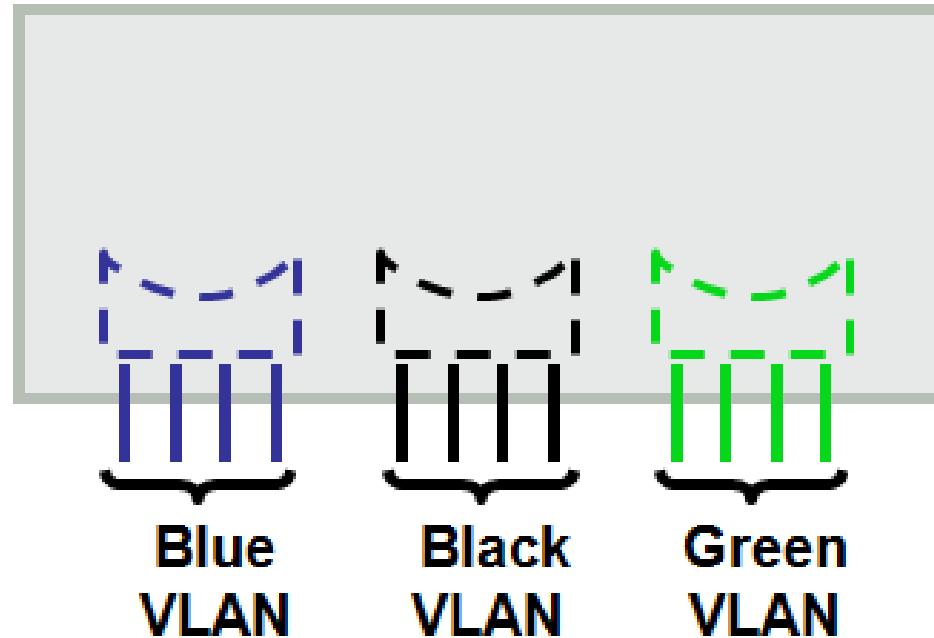
Switch Z



- Three separate broadcast domains
- Requires three switches

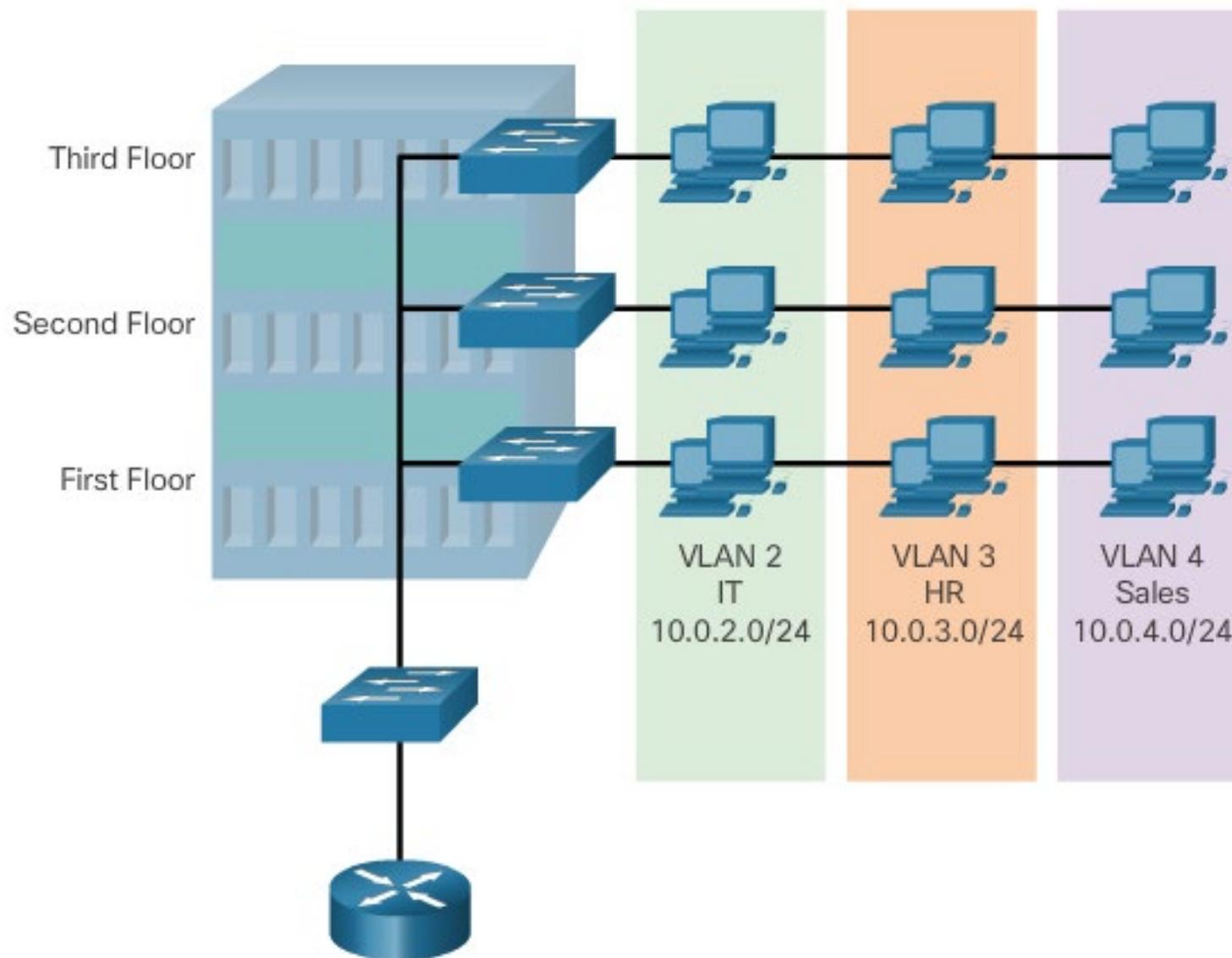
VLAN cont.

Switch A



- Each logical VLAN is like a separate physical switch
 - Each VLAN is a separate broadcast domain (3 broadcast domains)
 - Each VLAN contains a separate MAC address table
 - Computer in Blue VLAN will not be able to send a frame to Black VLAN or Green VLAN

Defining VLAN Groups



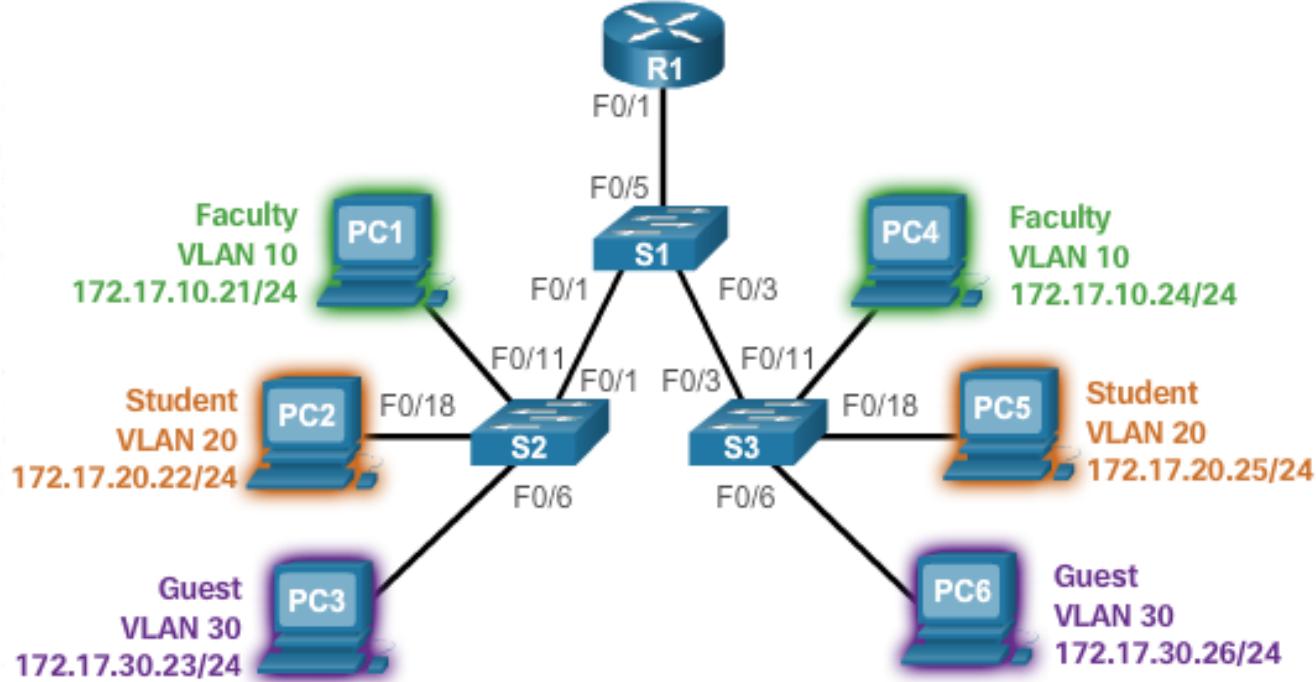
VLAN Definitions (cont.)

- VLANs allow an administrator to segment networks based on factors such as function, project team, or application, without regard for the physical location of the user or device.
- VLANs enable the implementation of access and security policies according to specific groupings of users.
- A VLAN is a logical partition of a Layer 2 network.
- Multiple partitions can be created, allowing for multiple VLANs to co-exist.

VLAN Definitions (cont.)

- Each VLAN is a broadcast domain, usually with its own IP network.
- VLANs are mutually isolated, and packets can only pass between them via a router.
- The partitioning of the Layer 2 network takes place inside a Layer 2 device, usually via a switch.
- The hosts grouped within a VLAN are unaware of the VLAN's existence.

Benefits of VLANs



- Improved Security
- Reduced Cost
- Better Performance
- Smaller Broadcast Domains
- IT Efficiency
- Management Efficiency
- Simpler Project and Application Management

Types of VLANs

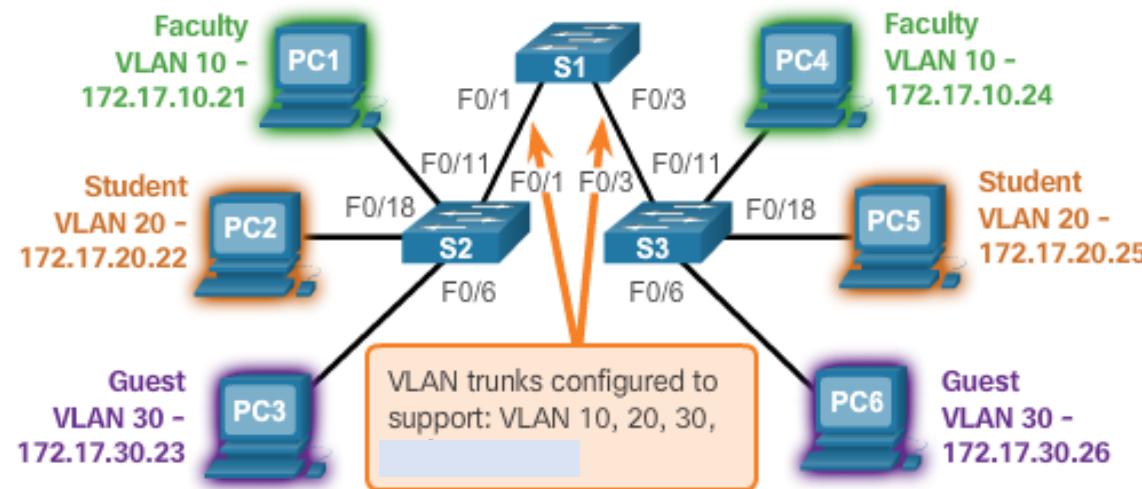
- **Data VLAN** – user generated traffic
- **Default VLAN** – all switch ports become part of this VLAN until switch is configured,
- **Management VLAN** – used to access management capabilities

VLAN Trunks

VLAN 10 Faculty/Staff - 172.17.10.0/24
VLAN 20 Students - 172.17.20.0/24
VLAN 30 Guest - 172.17.30.0/24

F0/1-5 are 802.1Q trunk interfaces

F0/11-17 are in VLAN 10.
F0/18-24 are in VLAN 20.
F0/6-10 are in VLAN 30.

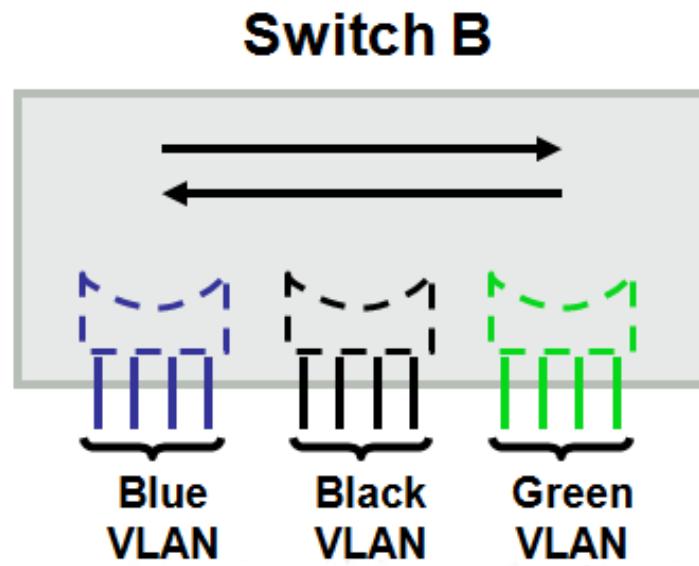
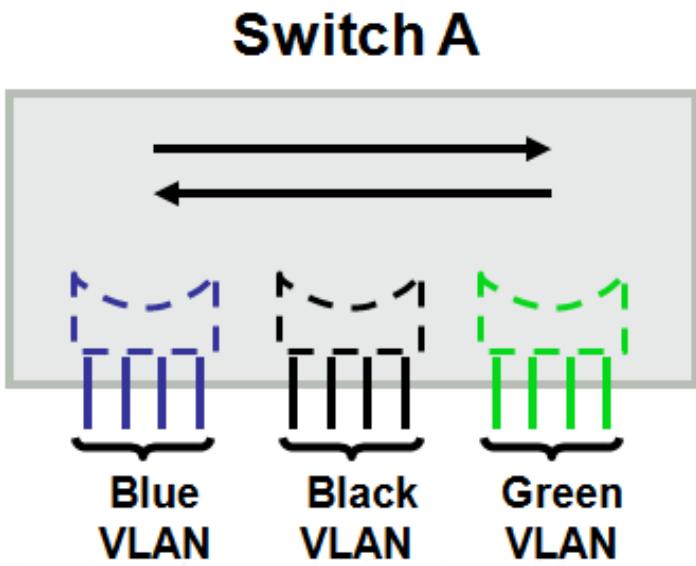


The links between switches S1 and S2, and S1 and S3 are configured to transmit traffic coming from VLANs 10, 20, 30 the network. This network could not function without VLAN trunks.

VLAN Trunks (cont.)

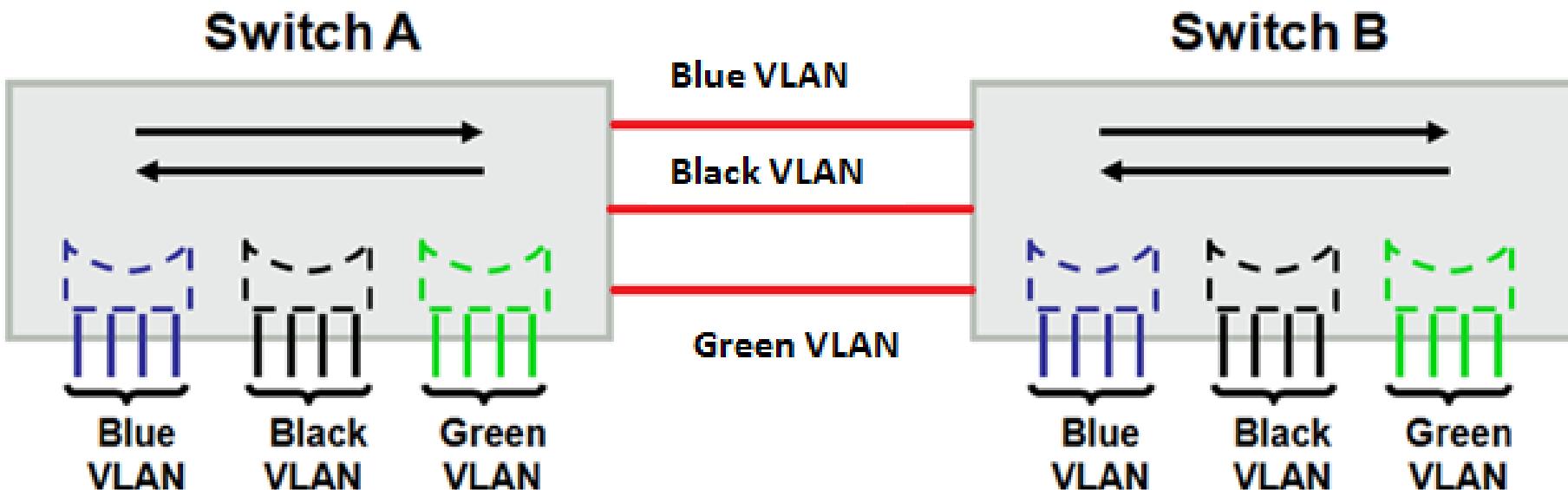
- A VLAN trunk is a point-to-point link that carries more than one VLAN.
- A VLAN trunk is usually established between switches so same-VLAN devices can communicate, even if physically connected to different switches.
- A VLAN trunk is not associated to any VLANs; neither is the trunk ports used to establish the trunk link.
- Cisco IOS supports IEEE802.1q, a popular VLAN trunk protocol.

VLAN cont.

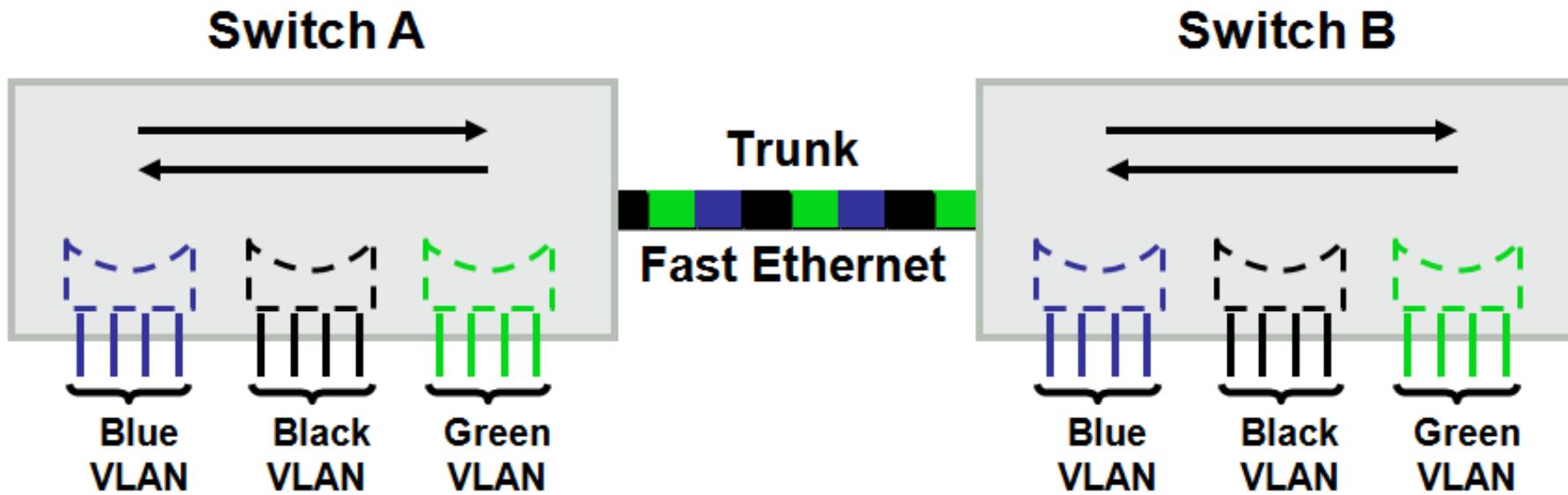


- VLANs can span across multiple switches

VLAN cont.



VLAN tagging for source identification



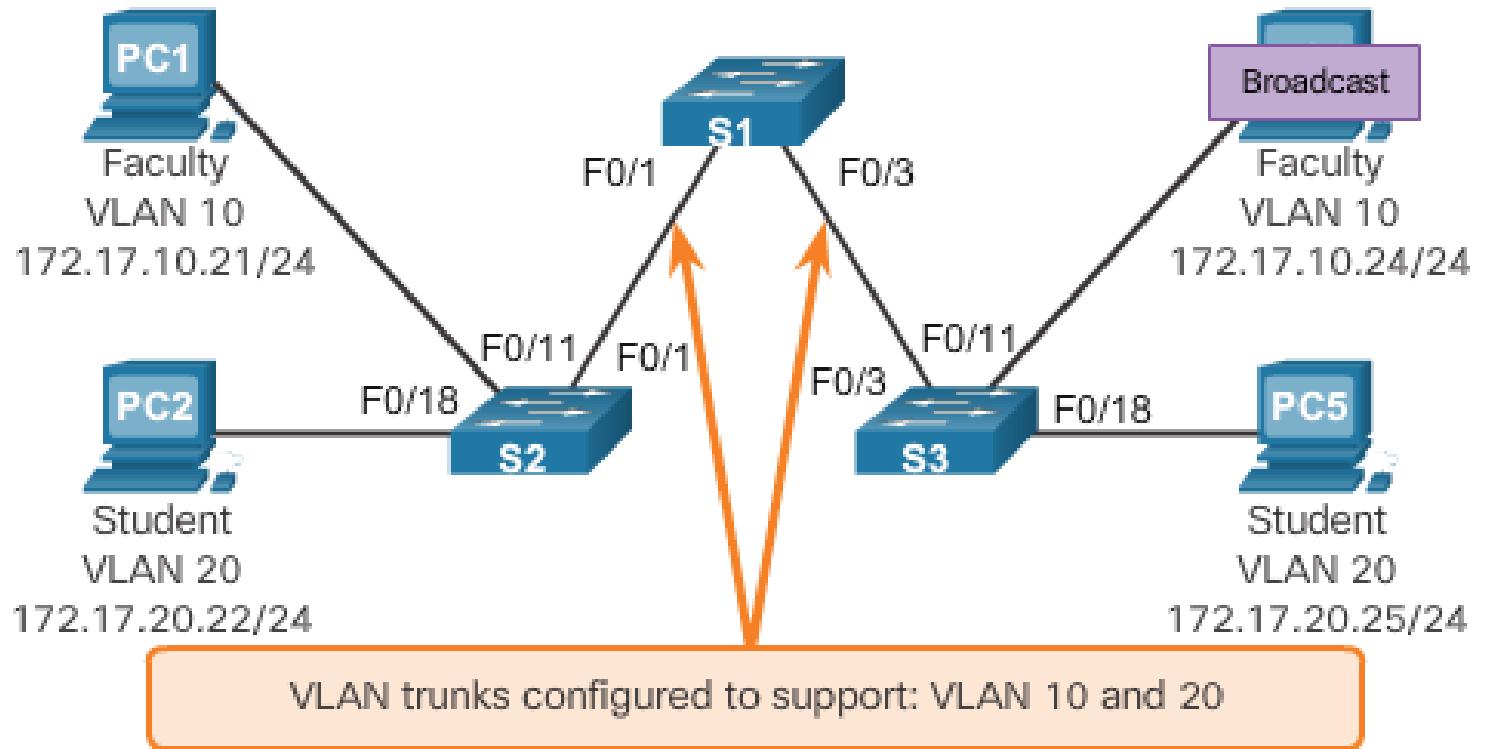
- The process of adding an additional header to a LAN frame
- Used to identify the VLAN to which the frame belongs
- Cisco refers to this as **TRUNKING**
- Trunks carry traffic for multiple VLANs

VLANs in a Multi-Switched Environment

Controlling Broadcast Domains with VLANs

With VLAN Segmentation

PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame only out ports configured for VLAN10.



Controlling Broadcast Domains with VLANs

- ❖ VLANs can be used to limit the reach of broadcast frames.
- ❖ A VLAN is a broadcast domain of its own.
- ❖ A broadcast frame sent by a device in a specific VLAN is forwarded within that VLAN only.
- ❖ VLANs help control the reach of broadcast frames and their impact in the network.
- ❖ Unicast and multicast frames are forwarded within the originating VLAN.

Tagging Ethernet Frames for VLAN Identification

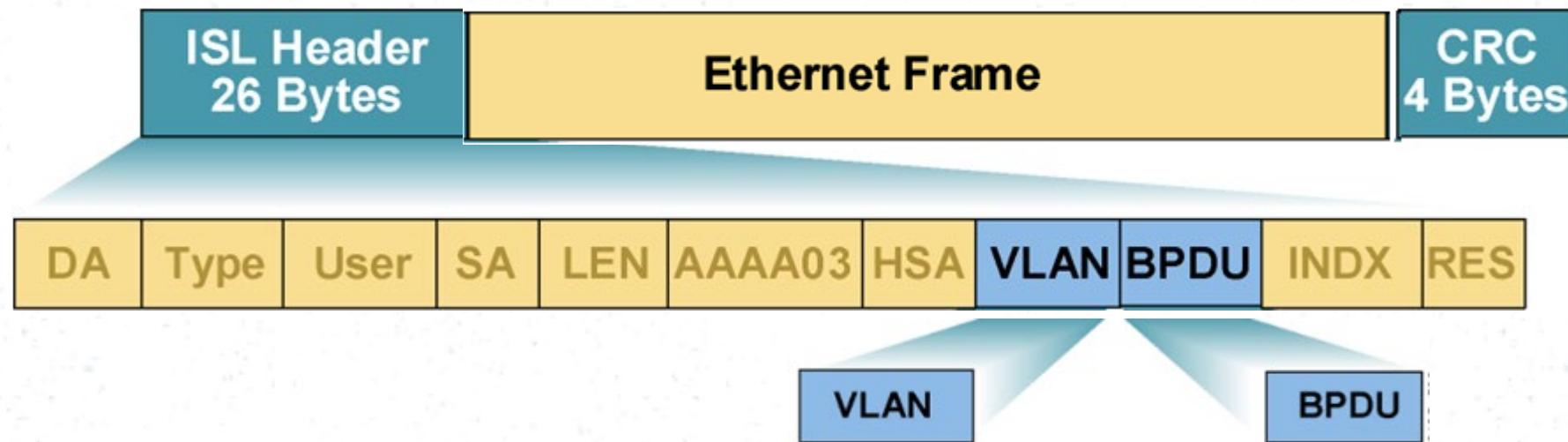
- Frame tagging is the process of adding a VLAN identification header to the frame.
- It is used to properly transmit multiple VLAN frames through a trunk link.
- Switches tag frames to identify the VLAN to which they belong.
- Different tagging protocols exist; ISL , IEEE 802.1Q.
- The protocol defines the structure of the tagging header added to the frame.
- Switches add VLAN tags to the frames before placing them into trunk links and remove the tags before forwarding frames through non-trunk ports.
- When properly tagged, the frames can transverse any number of switches via trunk links and still be forwarded within the correct VLAN at the destination.

Trunking

Tagging	Method	Media	Description
Inter-Switch Link (ISL)	Fast Ethernet	ISL header encapsulates the LAN frame and there is a VLAN ID field in the ISL header	Frame is lengthened.
802.1Q	Fast Ethernet	IEEE defined Ethernet VLAN protocol	Header is modified.

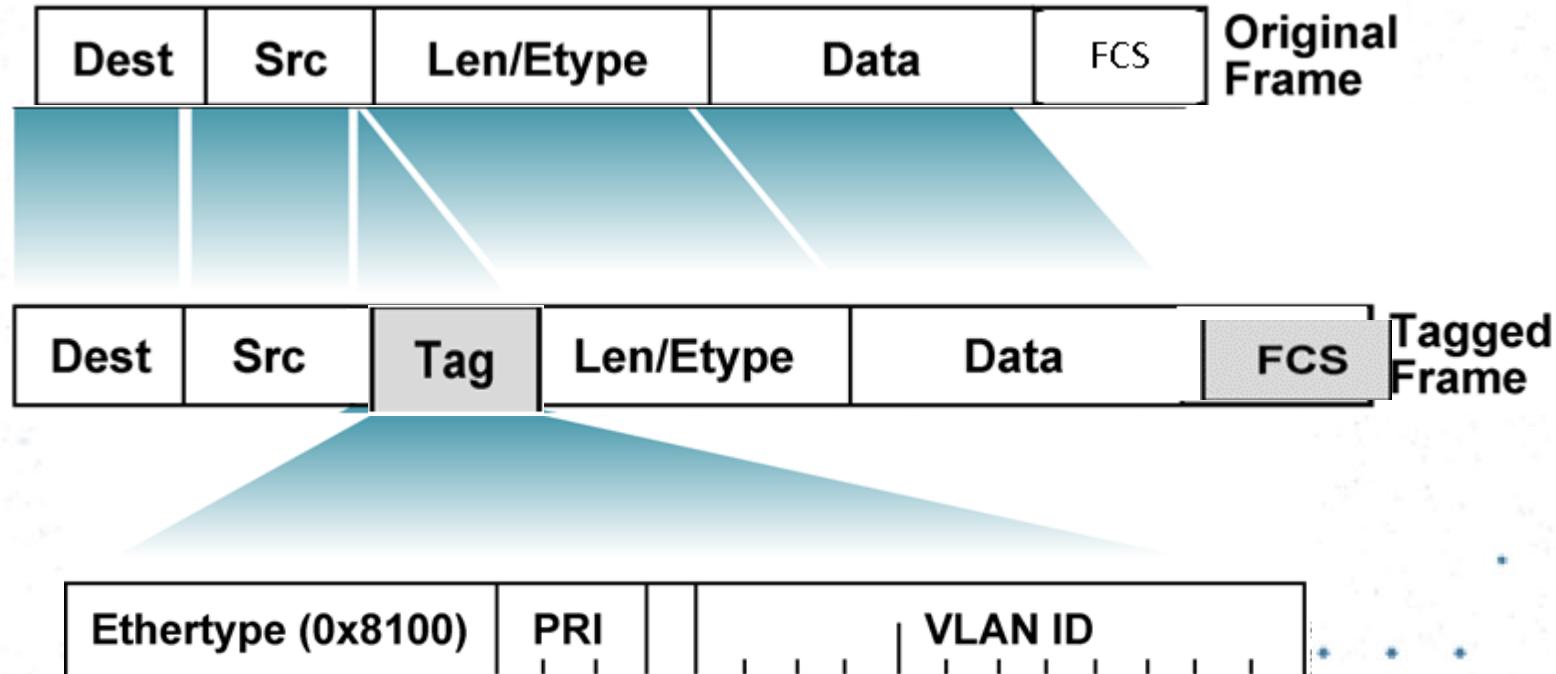
- There are two types of VLAN Trunking:
 - ISL (Inter-Switch Link) – Cisco Proprietary
 - IEEE 802.1Q

ISL (Inter-Switch Link)



- Full Ethernet frame is encapsulated with a ISL
- Indicate the VLAN ID (12 bit) to identify the VLAN
- CISCO proprietary

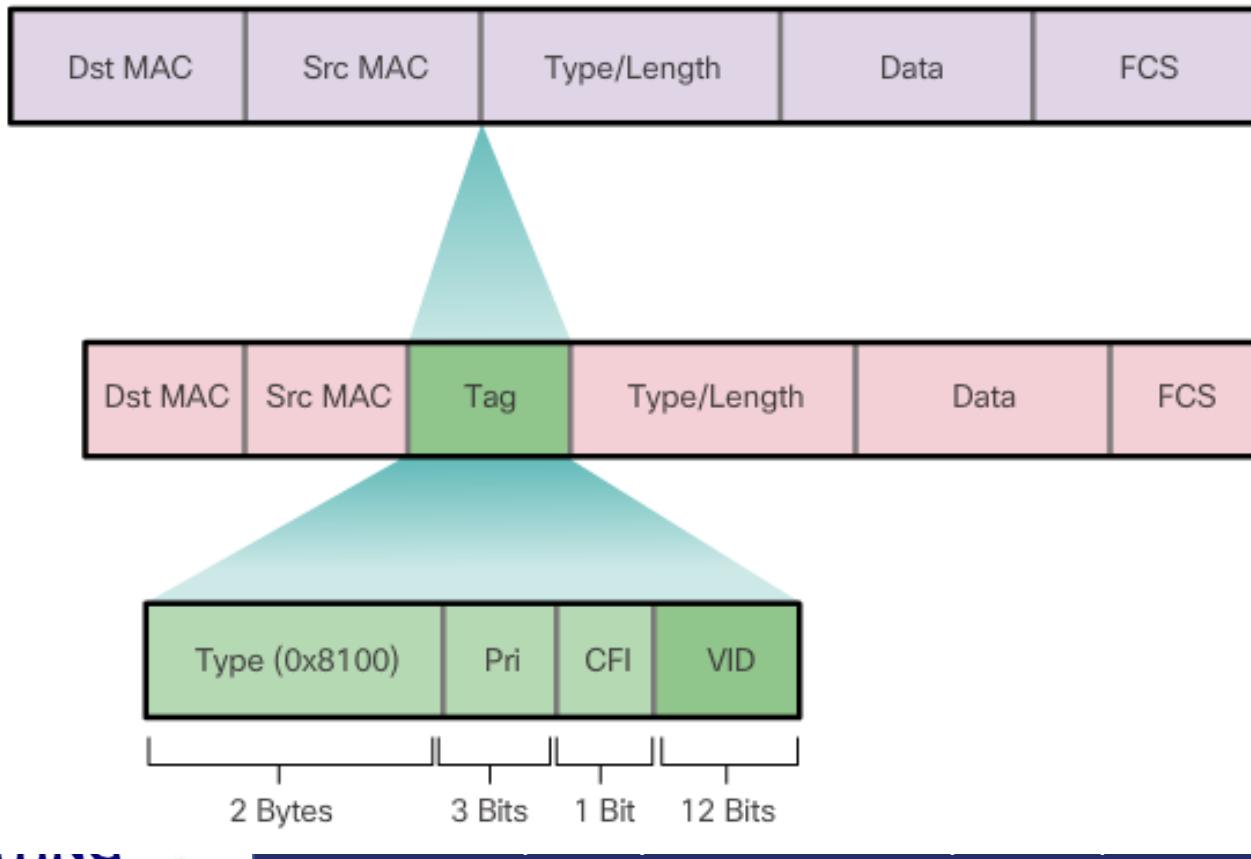
IEEE 802.1Q



- The IEEE 802.1Q tag is inserted by the switch before sending the frame across the trunk
 - Indicate the VLAN ID (12 bit) to identify the VLAN

802.1Q Tagging

Fields in an Ethernet 802.1Q Frame



VLAN Trunks

Configuring IEEE 802.1Q Trunk Links

Trunk Configuration

```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)#
S1(config-if)# switchport trunk allowed vlan 10,20,30,99
S1(config-if)# end
```

• •
• •
• •
• •
• •
• •
• •
• •

Resetting the Trunk to Default State

Resetting Configured Values on Trunk Links

Cisco Switch IOS Commands	
Enter global configuration mode.	S1# configure terminal
Enter interface configuration mode.	S1(config)# interface interface_id
Set trunk to allow all VLANs.	S1(config-if)# no switchport trunk allowed vlan
Reset native VLAN to default.	S1(config-if)# no switchport trunk native vlan
Return to the privileged EXEC mode.	S1(config-if)# end

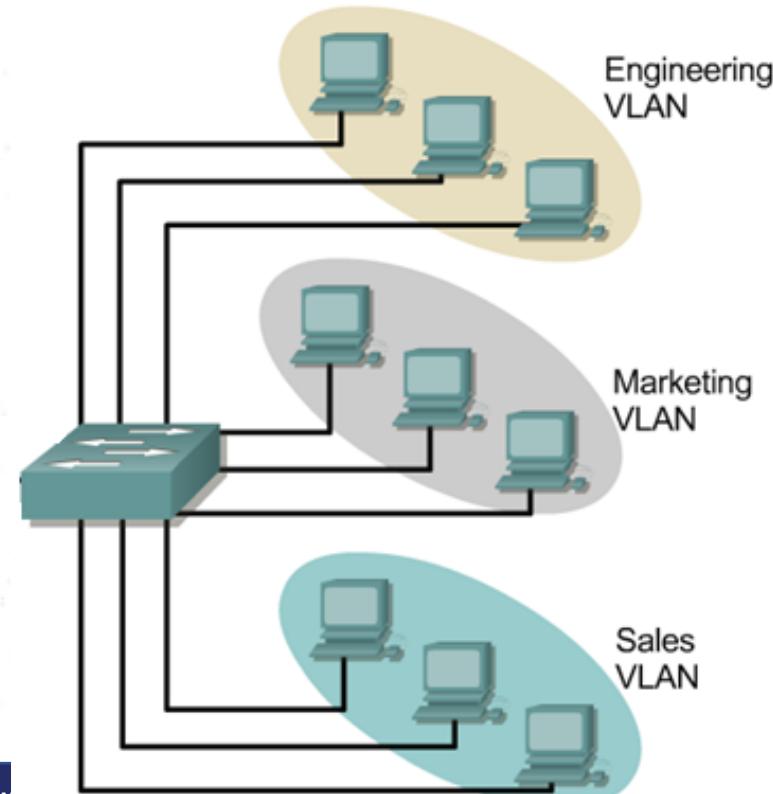
Troubleshoot VLANs and Trunks

- VLANs must be allowed in the trunk before their frames can be transmitted across the link.
- Use the **switchport trunk allowed vlan** command to specify which VLANs are allowed in a trunk link.
- Use the **show interfaces trunk** command to ensure the correct VLANs are permitted in a trunk.

Inter-VLAN Routing Using Routers

Passing traffic between VLANs

- Each VLAN will have different IP subnets
 - VLANs don't send data frames to other VLAN
(Separate MAC address table for each VLAN)
- * * * * *



Inter-VLAN Routing

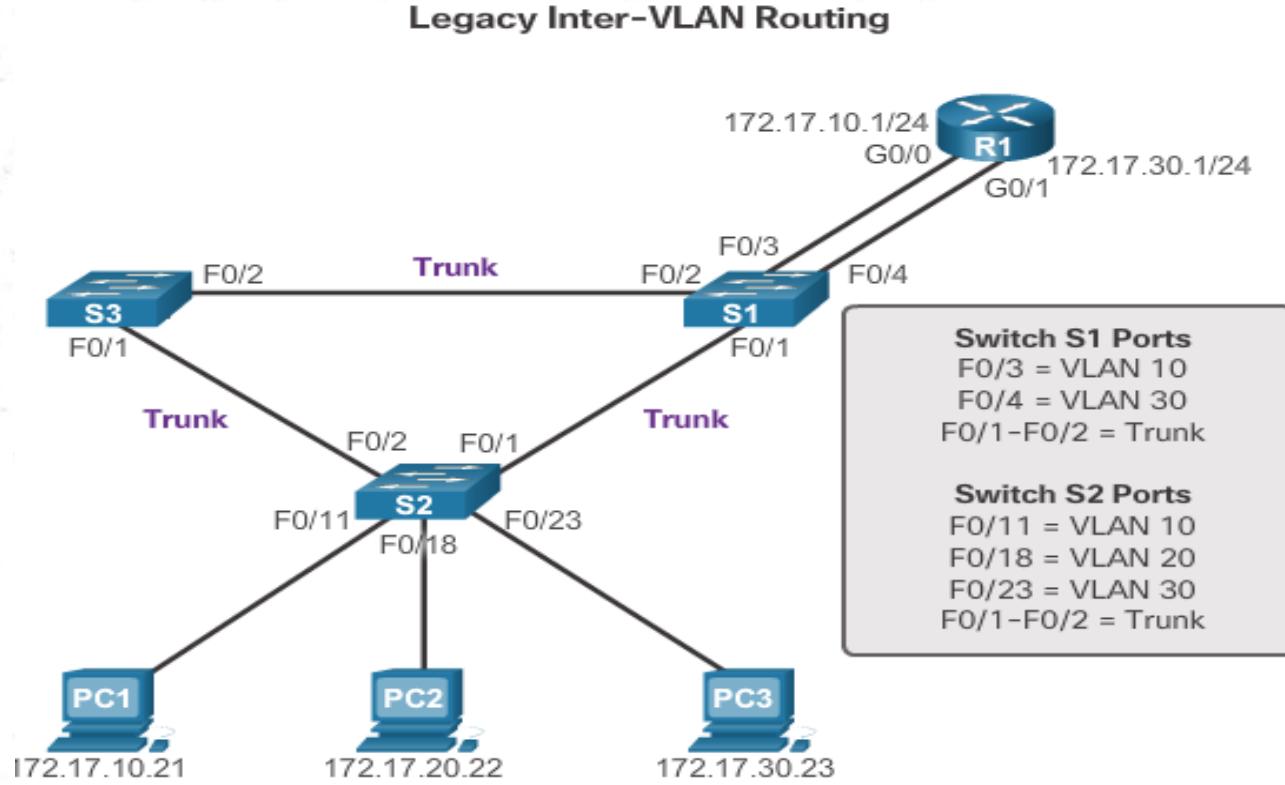
- Layer 2 switches cannot forward traffic between VLANs without the assistance of a router.
- Inter-VLAN routing is a process for forwarding network traffic from one VLAN to another, using a router.

Legacy Inter-VLAN Routing

In the past:

- Actual routers were used to route between VLANs.
- Each VLAN was connected to a different physical router interface.
- Packets would arrive on the router through one interface, be routed and leave through another.
- Because the router interfaces were connected to VLANs and had IP addresses from that specific VLAN, routing between VLANs was achieved.
- Large networks with large number of VLANs required many router interfaces.

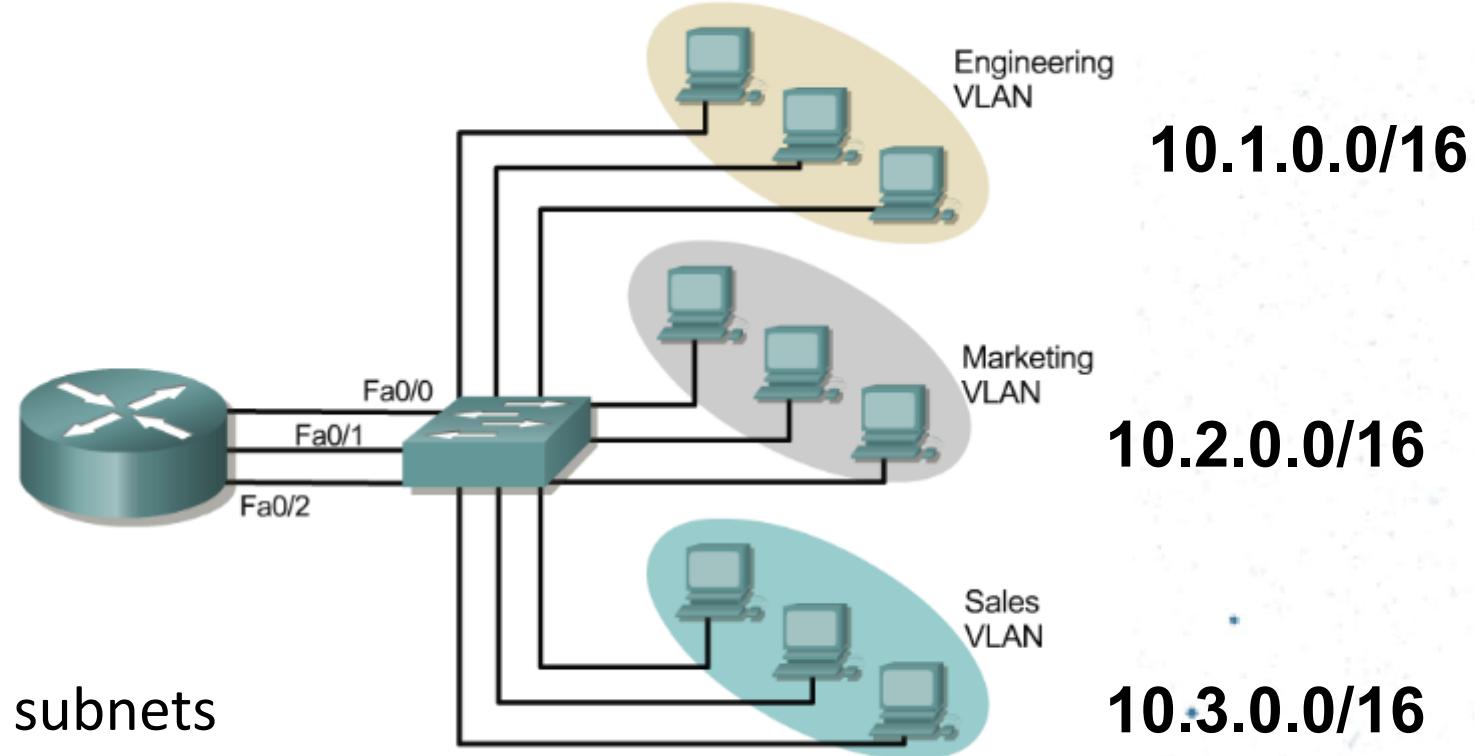
Legacy Inter-VLAN Routing



In this example, the router was configured with two separate physical interfaces to interact with the different VLANs and perform the routing.

Passing traffic between VLANs cont.

- 3 VLANs in 1 switch



- Three IP subnets
- Router with 3 LAN ports
- Waste of resources

Router-on-a-Stick Inter-VLAN Routing

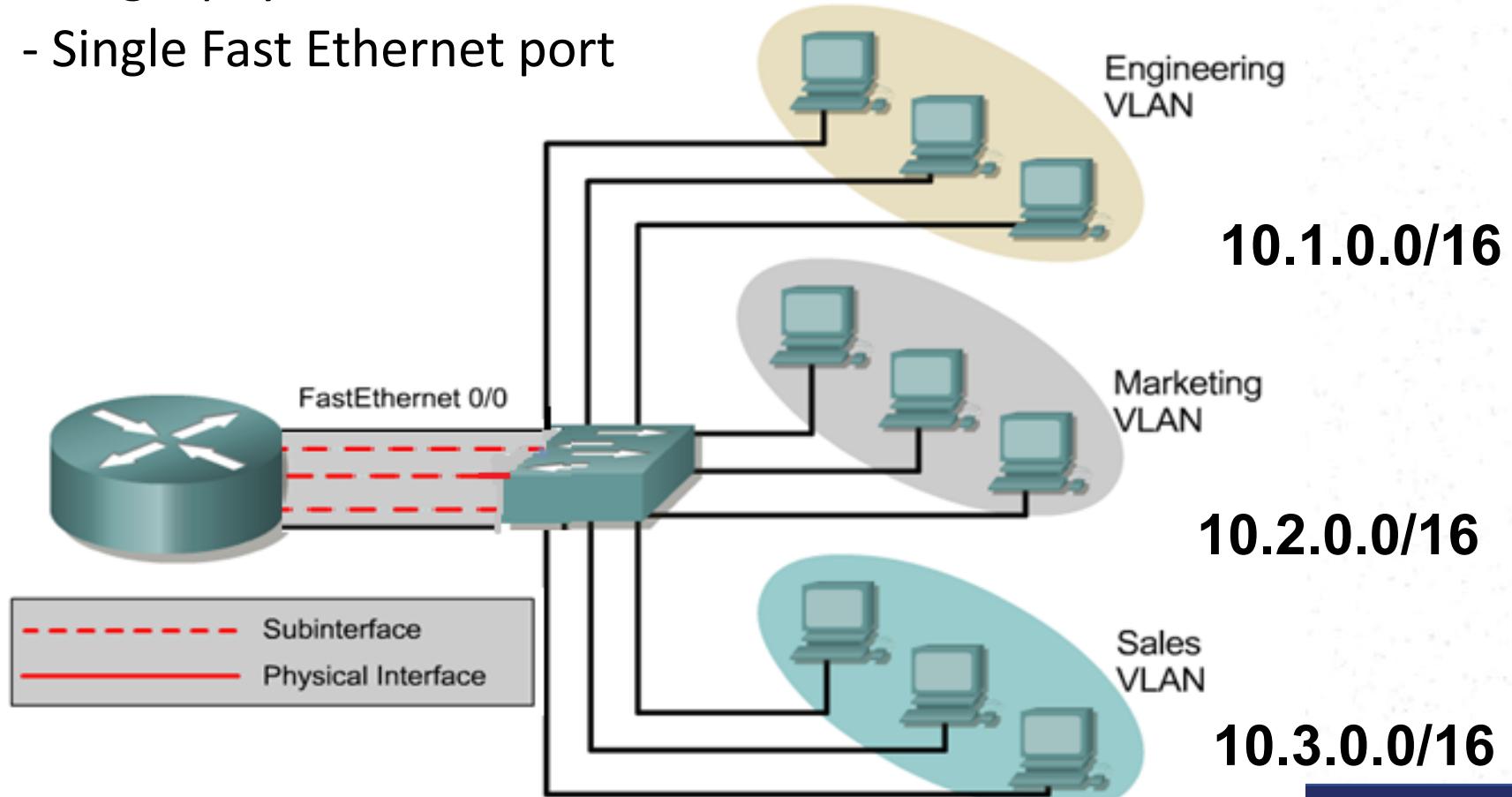
- The router-on-a-stick approach uses only one of the router's physical interface.
- One of the router's physical interfaces is configured as a 802.1Q trunk port so it can understand VLAN tags.
- Logical sub-interfaces are created; one sub-interface per VLAN.
- Each sub-interface is configured with an IP address from the VLAN it represents.
- **VLAN members (hosts) are configured to use the sub-interface address as a default gateway.**

Passing traffic between VLANs cont.

- Solution

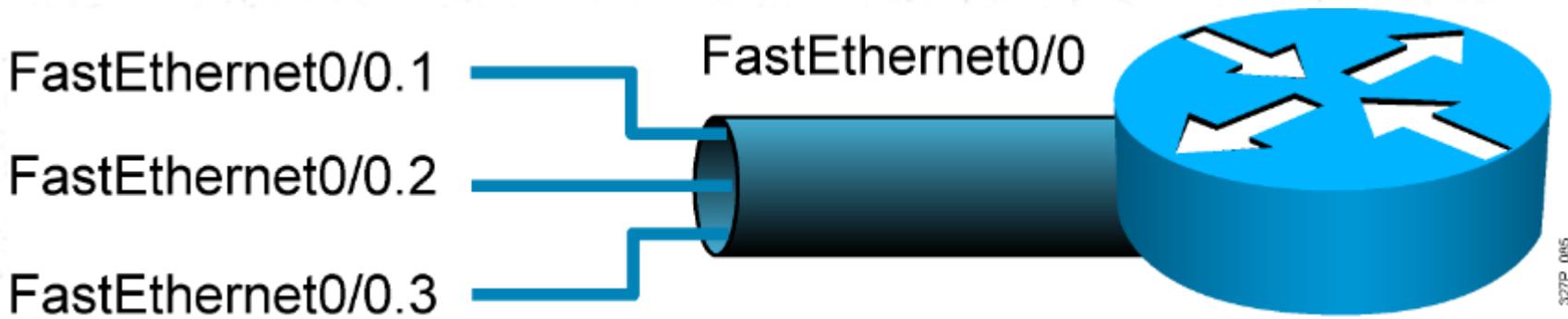
Router supports trunking (Inter VLAN routing)

- Single physical connection
- Single Fast Ethernet port



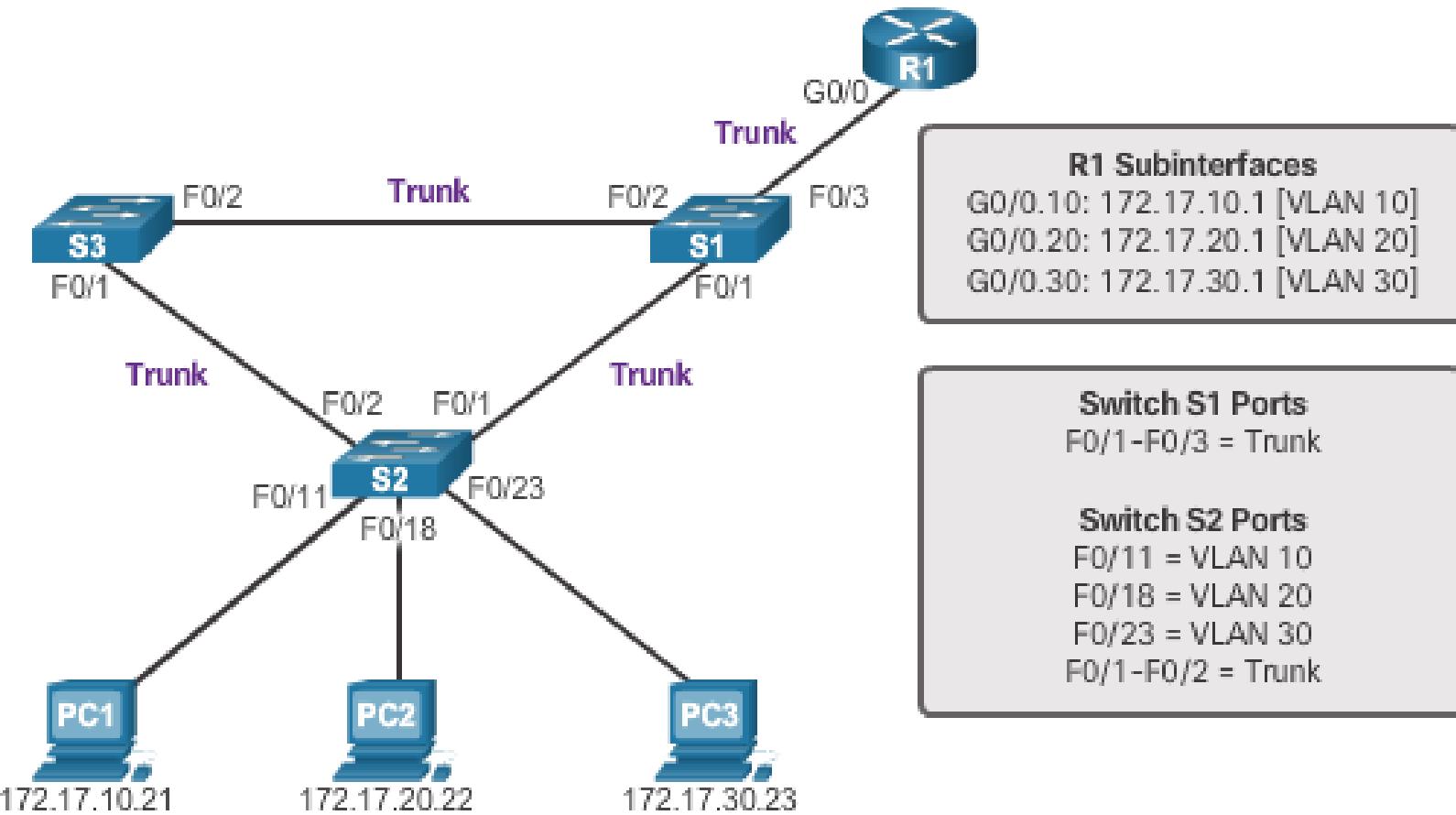
Inter VLAN routing

- Sub interfaces on a router can be used to divide a single physical interface into multiple logical interfaces
- Each physical interface can have up to 65,535 logical interfaces



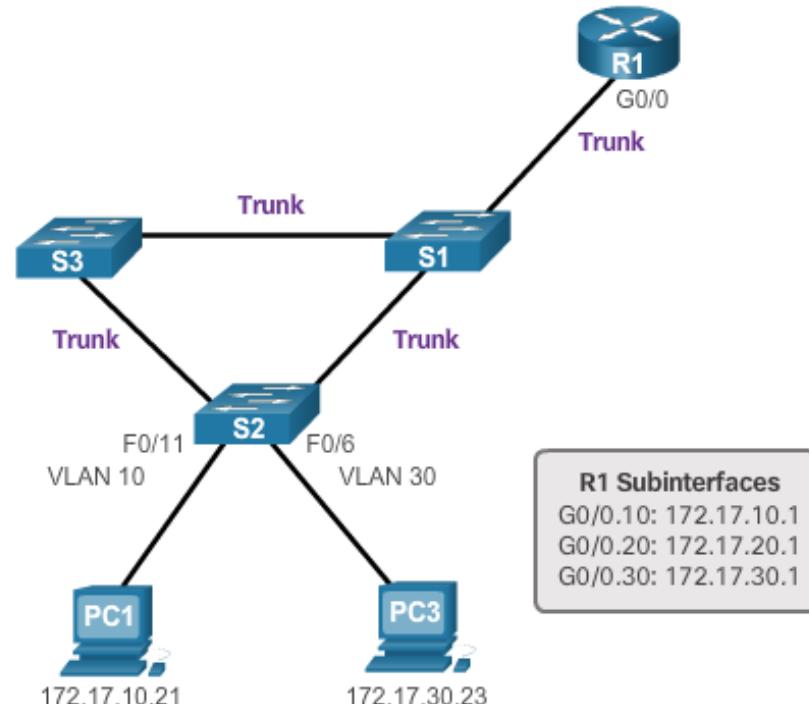
Router-on-a-Stick Inter-VLAN Routing

'Router-on-a-Stick' Inter-VLAN Routing

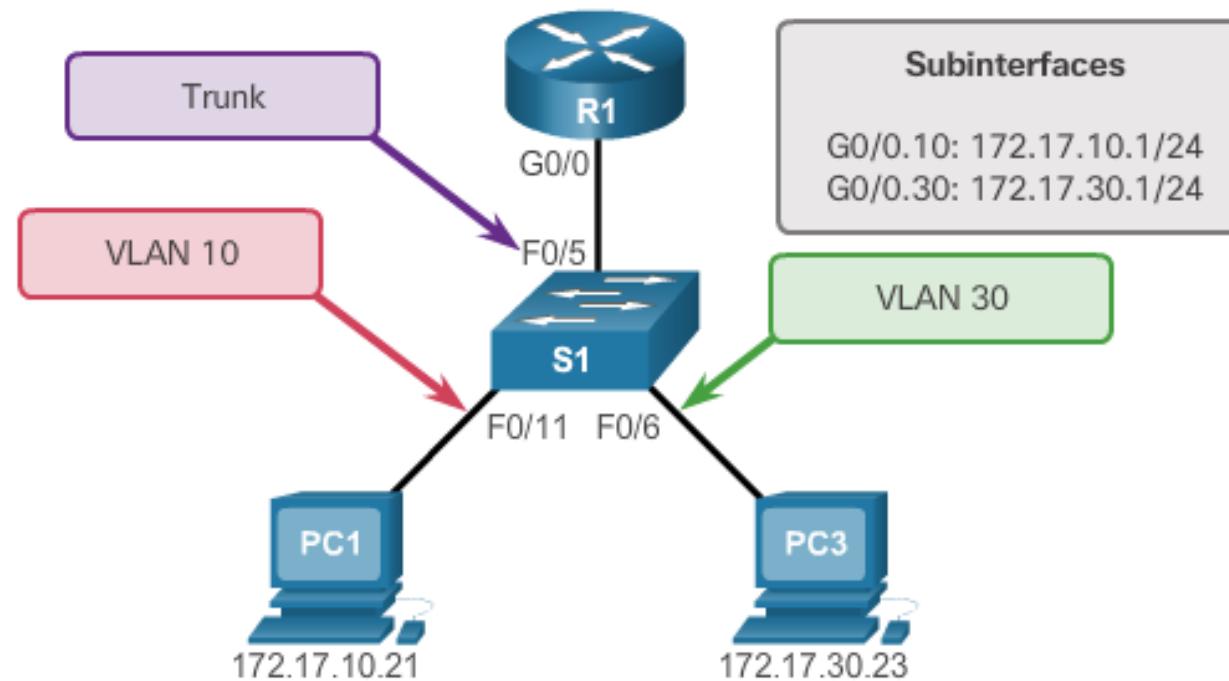


Configure Router-on-a Stick:

- VLAN trunking allows a single physical router interface to route traffic for multiple VLANs.
- The physical interface of the router must be connected to a trunk link on the adjacent switch.
- On the router, sub-interfaces are created for each unique VLAN.
- Each sub-interface is assigned an IP address specific to its subnet or VLAN and is also configured to tag frames for that VLAN.



Configure Router-on-a Stick: Switch Configuration



```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```

Configure Router-on-a Stick: Router Subinterface Configuration

```
R1 (config) # interface g0/0.10
R1 (config-subif) # encapsulation dot1q 10
R1 (config-subif) # ip address 172.17.10.1 255.255.255.0
R1 (config-subif) # interface g0/0.30
R1 (config-subif) # encapsulation dot1q 30
R1 (config-subif) # ip address 172.17.30.1 255.255.255.0
R1 (config) # interface g0/0
R1 (config-if) # no shutdown
```

Configure Router-on-a Stick: Verifying Subinterfaces (cont.)

```
R1# show ip route
```

Codes: L - local, C - connected, S - static, R - RIP, M - mobile,

Gateway of last resort is not set

172.17.0.0/16 is variably subnetted, 4 subnets, 2 masks

```
C    172.17.10.0/24 is directly connected, GigabitEthernet0/0.10
L    172.17.10.1/32 is directly connected, GigabitEthernet0/0.10
C    172.17.30.0/24 is directly connected, GigabitEthernet0/0.30
L    172.17.30.1/32 is directly connected, GigabitEthernet0/0.30
```

VLAN Implementations

Types of VLANs (cont.)

VLAN 1

```
Switch# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fd dinet-default	act/unsup	
1005	tr net-default	act/unsup	

- All ports assigned to VLAN 1 by default.
- Native VLAN is VLAN 1 by default.
- Management VLAN is VLAN 1 by default.

VLAN Ranges on Catalyst Switches

- Cisco Catalyst 2960 and 3560 Series switches support over 4,000 VLANs.
- VLANs are split into two categories:
 - Normal range VLANs
 - VLAN numbers from 1 to 1,005
 - Configurations stored in the `vlan.dat` (in the flash memory)
 - IDs 1002 through 1005 are reserved for Token Ring and Fiber Distributed Data Interface (FDDI) VLANs, automatically created and cannot be removed
 - Extended Range VLANs
 - VLAN numbers from 1,006 to 4,096
 - Configurations stored in the running configuration (NVRAM)
 - VLAN Trunking Protocol (VTP) does not learn extended VLANs

VLAN Ranges on Catalyst Switches

- Normal Range VLANs

```
Switch# show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/11, Fa0/12 Fa0/13, Fa0/14, Fa0/15, Fa0/16 Fa0/17, Fa0/18, Fa0/19, Fa0/20 Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
1002	fdci-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

VLAN Assignment

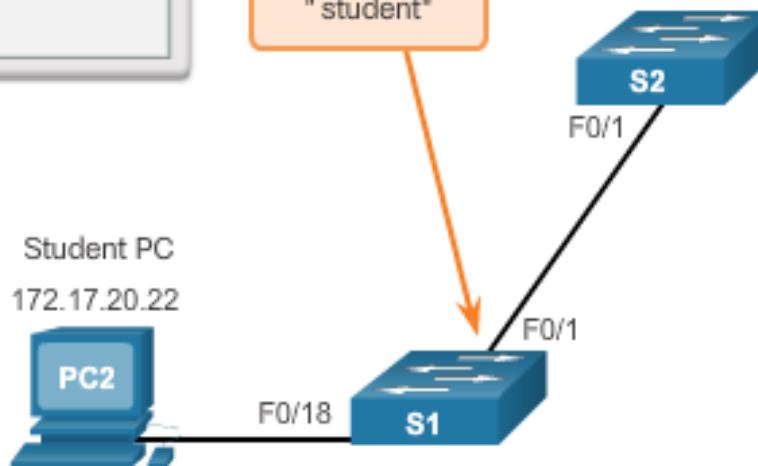
Creating a VLAN

Sample Configuration

```
s1# configure terminal  
S1(config)# vlan 20  
S1(config-vlan)# name student  
S1(config-vlan)# end
```

Switch S1:
VLAN 20
"student"

Student PC
172.17.20.22



Cisco Switch IOS Commands

Enter global configuration mode.	S1# configure terminal
Create a VLAN with a valid id number.	S1(config)# vlan vlan-id
Assign a unique name to identify the VLAN.	S1(config-vlan)# name vlan-name
Return to the privileged EXEC mode.	S1(config-vlan)# end

Assigning Ports to VLANs

```
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```



F0/1

Student PC
172.17.20.22



F0/18



Switch S1:
Port F0/18
VLAN 20

Changing VLAN Port Membership

- Remove VLAN Assignment

Cisco Switch IOS Commands

Enter global configuration mode.	S1# configure terminal
Remove the VLAN assignment from the port.	S1(config-if)# no switchport access vlan
Return to the privileged EXEC mode.	S1(config-if)# end

- Interface F0/18 was previously assigned to VLAN 20 which is still active, F0/18 reset to VLAN1

```
S1(config)# int F0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1# show vlan brief

VLAN Name          Status    Ports
---- --
1   default        active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                           Fa0/5, Fa0/6, Fa0/7, Fa0/8
                           Fa0/9, Fa0/10, Fa0/11, Fa0/12
                           Fa0/13, Fa0/14, Fa0/15, Fa0/16
                           Fa0/17, Fa0/18, Fa0/19, Fa0/20
                           Fa0/21, Fa0/22, Fa0/23, Fa0/24
                           Gi0/1, Gi0/2
20  student         active
1002 fddi-default   act/unsup
1003 token-ring-default act/unsup
1004 fddinet-default act/unsup
1005 trnet-default  act/unsup
S1#
```

Changing VLAN Port Membership (cont.)

Verification

```
s1# sh interfaces F0/18 switchport
Name: F0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

Deleting VLANs

```
S1# conf t  
S1(config)# no vlan 20  
S1(config)# end  
S1#  
S1# sh vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4 Fa0/5, Fa0/6, Fa0/7, Fa0/8 Fa0/9, Fa0/10, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Verifying VLAN Information

show vlan Command

Cisco IOS CLI Command Syntax

`show vlan [brief | id vlan-id | name vlan-name | summary]`

Display one line for each VLAN with the VLAN name, status, and its ports.

brief

Display information about a single VLAN identified by VLAN ID number.
For *vlan-id*, the range is 1 to 4094.

id *vlan-id*

Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.

name *vlan-name*

Display VLAN summary information.

summary

Verifying VLAN Information

```
S1# show vlan name student

VLAN Name          Status    Ports
-----            -----
20    student       active   Fa0/11, Fa0/18

VLAN Type SAID MTU Parent RingNo BridgeNo Stp BrdgMode Trans1 Trans2
-----            -----      -----      -----      -----      -----      -----
20    snet 100020 1500 -        -        -        -        -        0        0

Remote SPAN VLAN
-----
Disabled

Primary Secondary Type          Ports
-----            -----      -----
S1# show vlan summary
Number of existing VLANs       : 7
Number of existing VTP VLANs   : 7
Number of existing extended VLANs : 0

S1#
```

Computer Networks

Lecture 8

1

Transmission Control Protocol (TCP)

Introduction

2

- TCP is one of the transport layer protocols of TCP/IP
- Error control, flow control and congestion control exist
- TCP can be categorized as a reliable protocol
- Combination TCP/IP is reliable

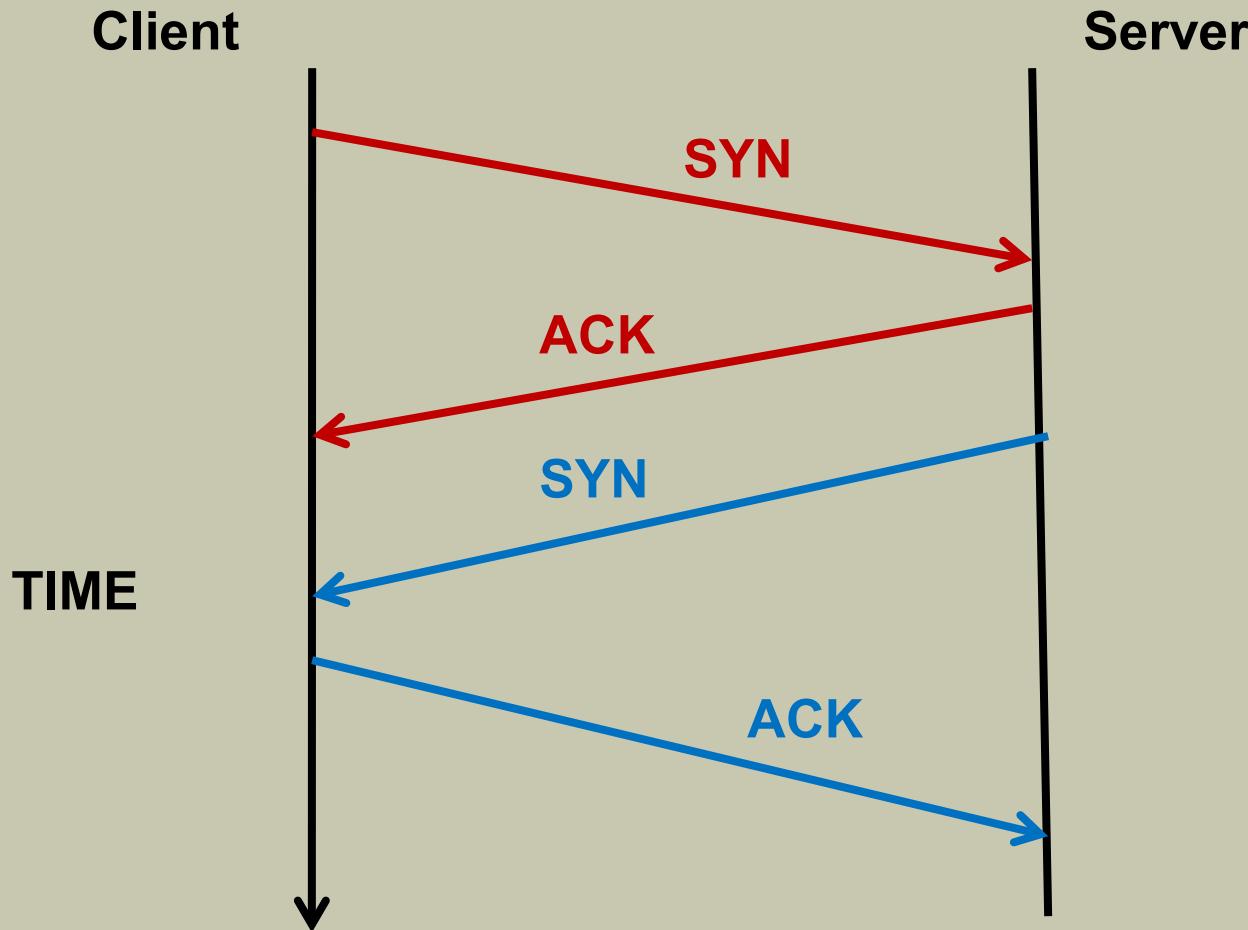
TCP Connection Process

3

- TCP-Client and TCP-Server connection process has three phases
 - Connection Establishment
 - Data Transferring
 - Connection Termination

Connection Establishment

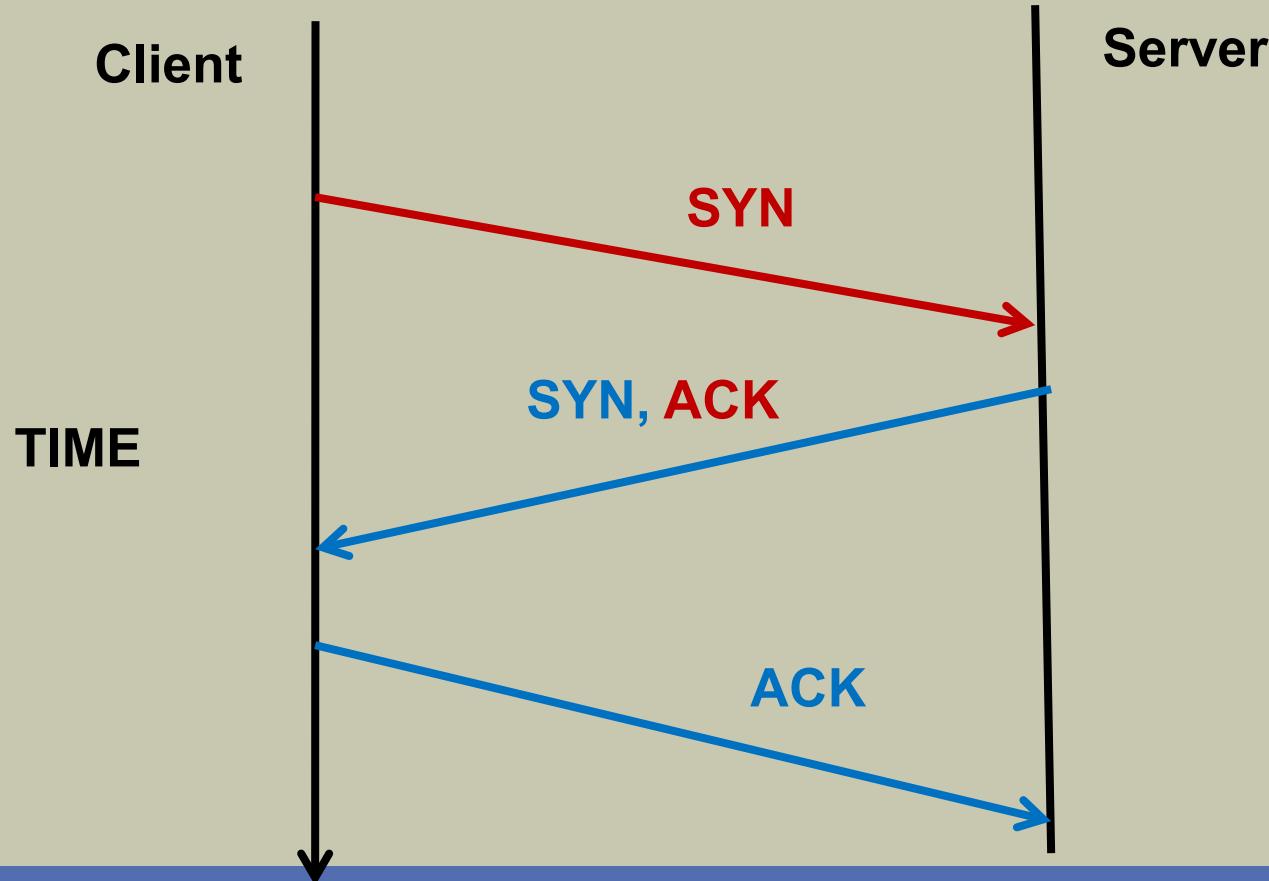
4



Three way handshake

5

- Four steps can be reduced to three steps



Three way handshake cont.

6

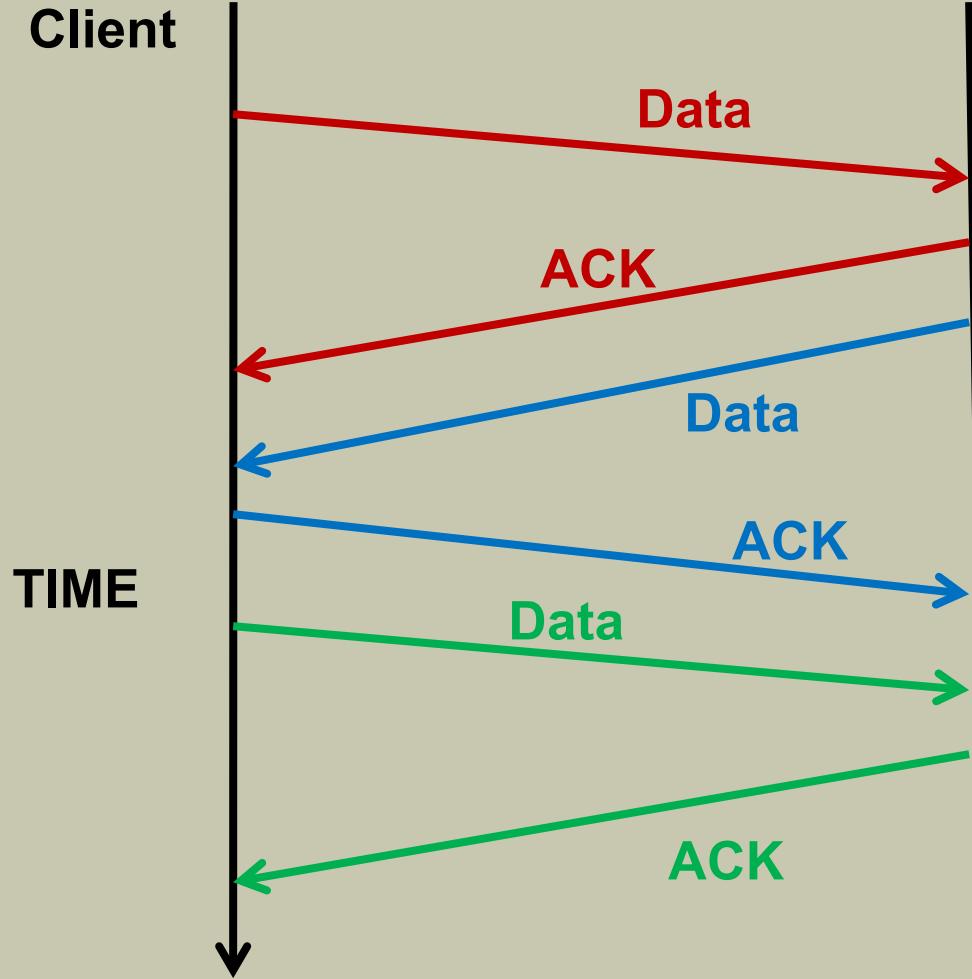
- The SYN, SYN/ACK and ACK are 1-byte messages
- After the connection is established, data can be transmitted in full duplex mode between a client and a server

Data Transfer

7

Client

Server



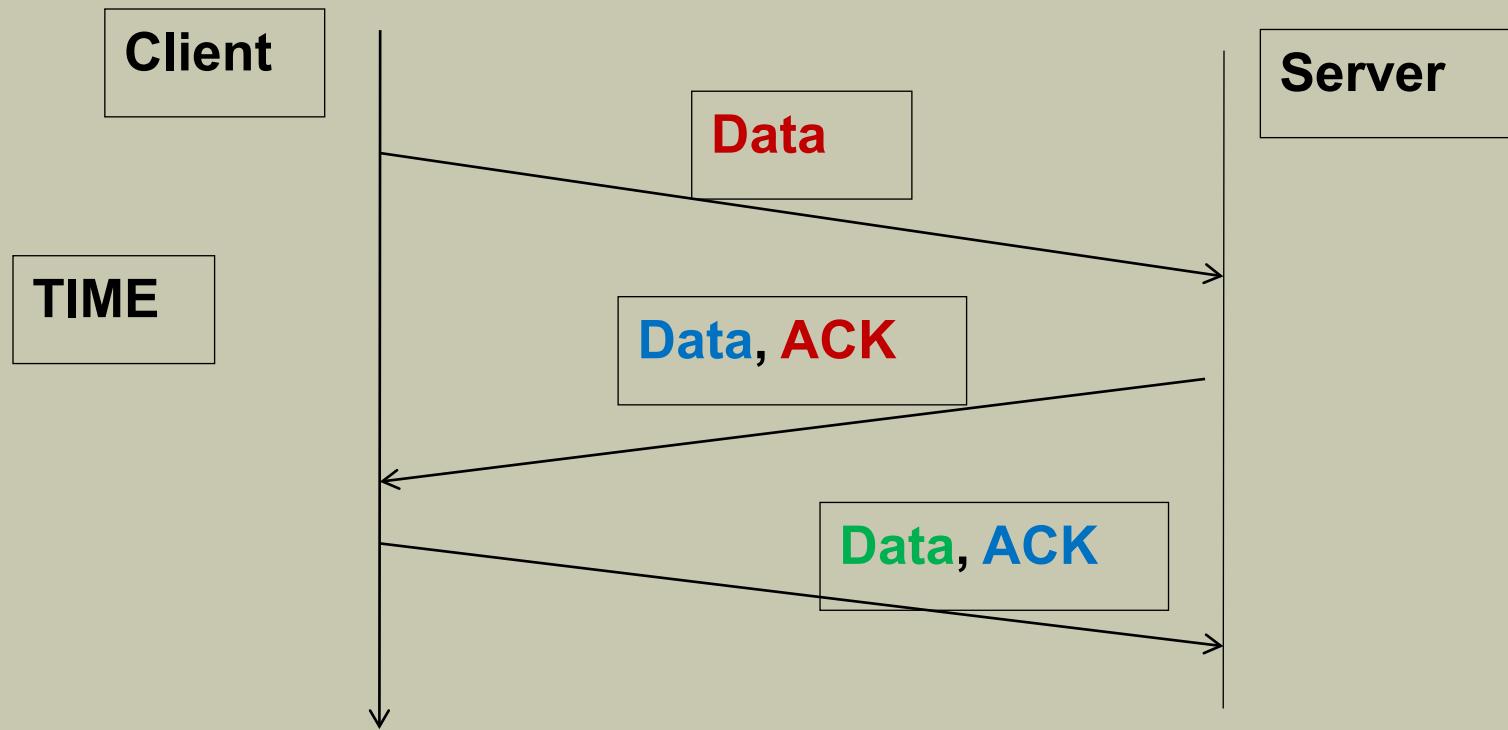
- TCP is a reliable protocol.
- TCP sends an Acknowledgement (ACK) for each segment of received data.

Data Transfer cont.

8

- **Piggybacking**

Sending Data and ACK together.



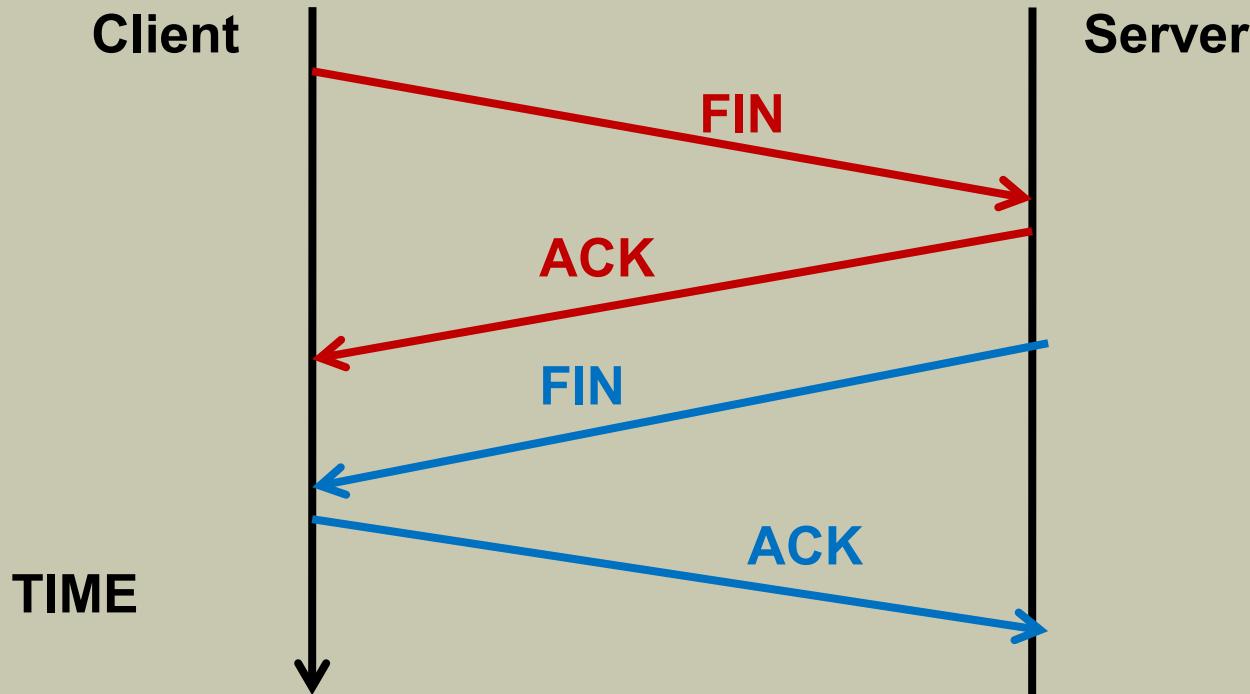
Data Transfer cont.

9

- Data is transferred as **Segments**
- Each segment is given an identification called a **Sequence Number**.
- Acknowledgement Number =
Sequence Number (Received) + Number of bytes in the segment

Terminating the connection

10



- Normally the connection termination request is initiated by the client
- FIN and ACK are considered one-byte messages

Problems related to data transfer

11

- The following three problems must be addressed in data transferring process for a better data transmission
 - Error control
 - Flow control
 - Congestion control

Error Control

12

- TCP receiver uses checksum bits for error detection
- If there are no errors it sends an acknowledgement to the sender
- If errors are found, the receiver does not send any negative acknowledgement to the sender

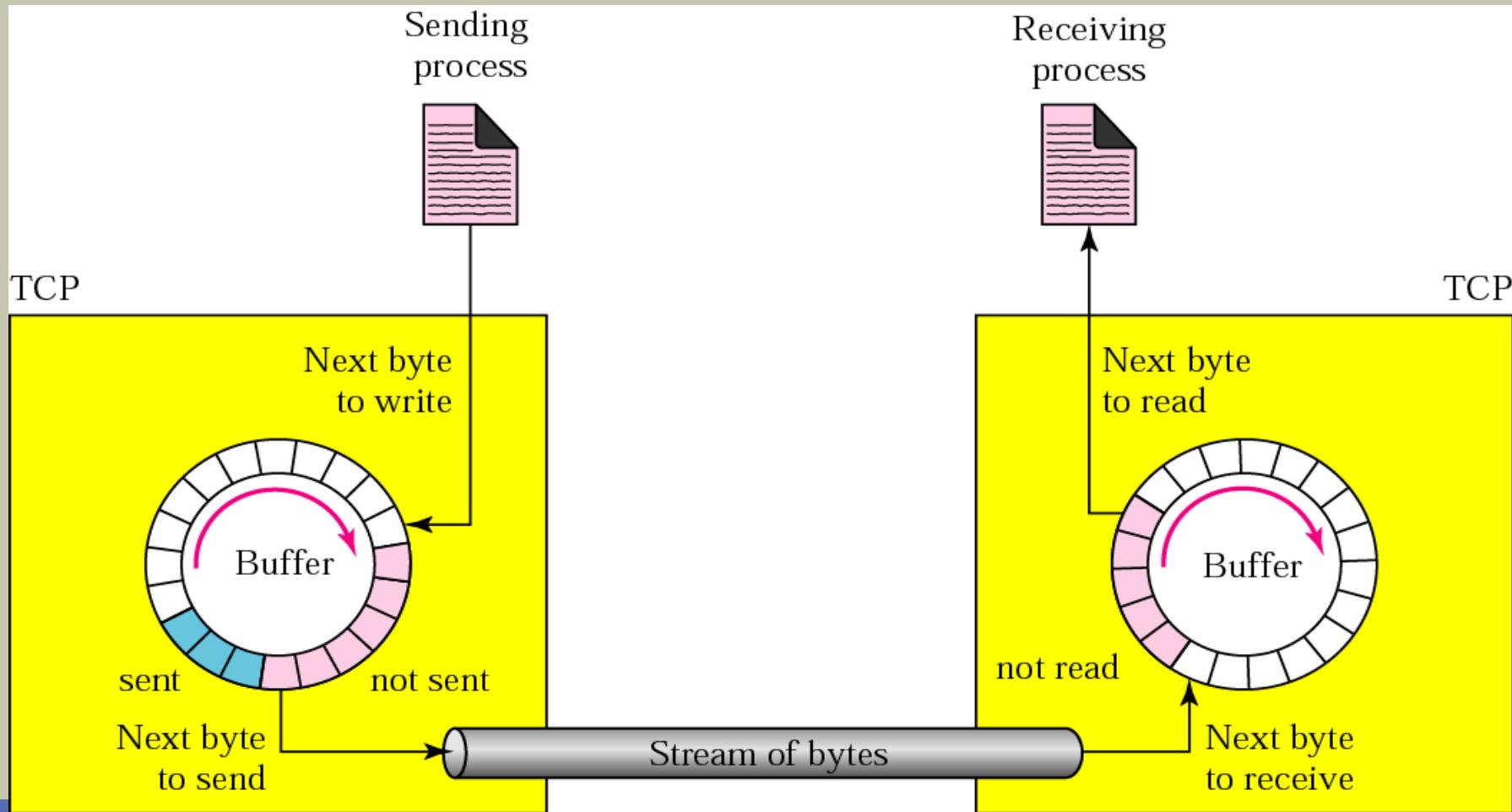
Error Control cont.

13

- In this process, the sender and receiver should have the following facilities
 - Sender buffer
 - Receiver buffer
 - Timer
- Sender buffer needs to keep the segments, until it receives an acknowledgement from the receiver
- Receiver buffer needs to keep the segment, until the error checking is over
- The sender needs a timer to check whether the Retransmission Time is expired after sending the segment

Flow control

14



Slow Applications

15

- If the application is very slow and it sends 1 byte at a time
- Application layer send data to the Tx buffer of the TCP layer
- The TCP protocol adds a 20byte TCP header and sends to IP layer
- The IP layer adds 20 bytes of IP header and sends data link layer
- Data link layer also adds a header and a trailer (say 26 bytes)
- Altogether $20+20+26 = 66$ byte overhead is added to application data

Slow Applications cont.

16

- 1 byte of data is combined with 66 byte overhead bits
- This is a very inefficient data transfer
- TCP has the facility to improve such a situation by defining the minimum data required for a segment
- TCP waits until such an amount of data is collected
- After that the TCP segment is sent to the IP layer

Fast application/ Slow network/ Slow receiver

17

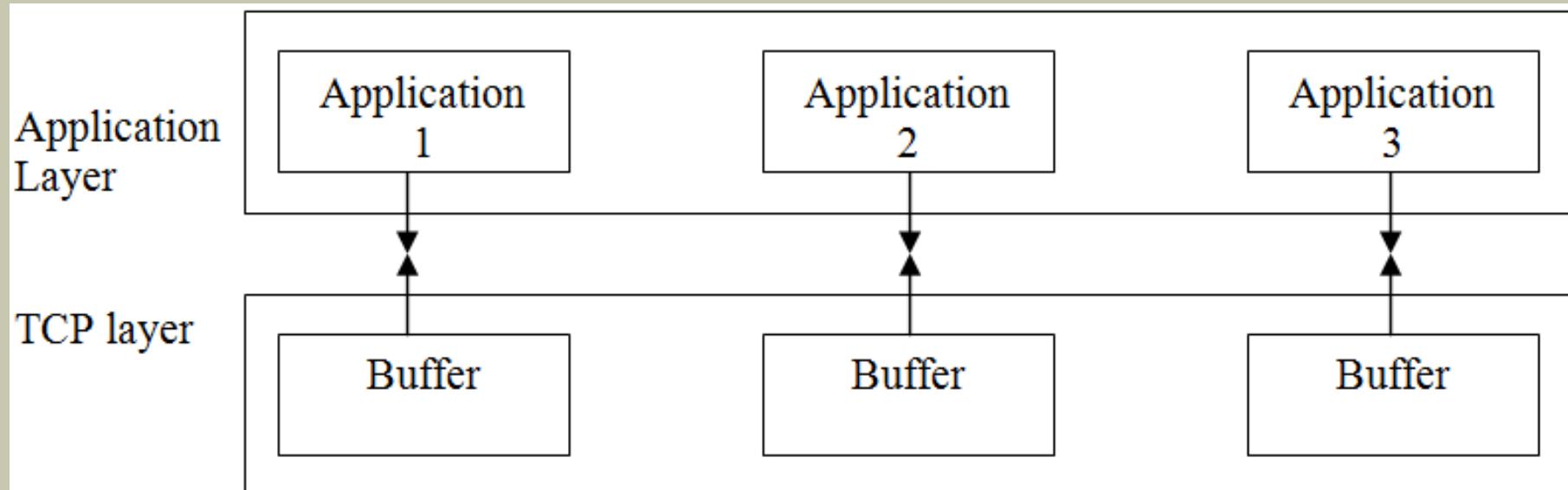
- Application layer buffers and TCP layer buffer sizes are decided on the following factors
 - Speed of application
 - Speed of computer
 - Speed of the network
 - Congestion of network
- If the sender application is faster than the network, it will overflow the TCP buffer and gives a “**runtime error**” – **PCs Stuck**

Needs to Restart

Multiplexing

18

- TCP layer can handle several application processes at the same time
 - - E-mail, Web browsing , Transfer files
- Port Number identifies the application



TCP with IP layer

19

- IP layer receives data from the transport layer
- Therefore the type of data in IP packet can be TCP, UDP.
- Each type of data is given a unique protocol number

Application Layer

DATA

TCP layer

DATA

IP Layer

DATA

Port number

20

- The port number is a 16 bit binary number in the TCP
- It is in the range of 0-65535
- The port numbers are divided into three ranges.
 - Well known ports
 - Registered ports
 - Dynamic ports/ Ephemeral ports

Well-known ports

21

- Port numbers ranging from 0-1023 is called well-known ports

**Assigned for
Standard
Server
Processes**

<i>Port</i>	<i>Protocol</i>	<i>Description</i>
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
20	FTP, Data	File Transfer Protocol (data connection)
21	FTP, Control	File Transfer Protocol (control connection)
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

Registered ports

22

- The ports ranging from 1024 - 49,151 are to be registered with IANA to prevent duplicating
- Used for proprietary server processors or any client process
- **Normally not used**

Dynamic ports

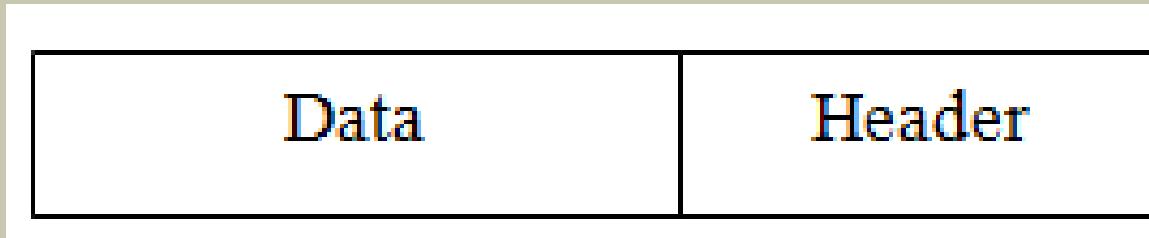
23

- The ports numbers from 49,152 to 65,535 are dynamic or ephemeral ports
- They are used by **client processes temporarily**

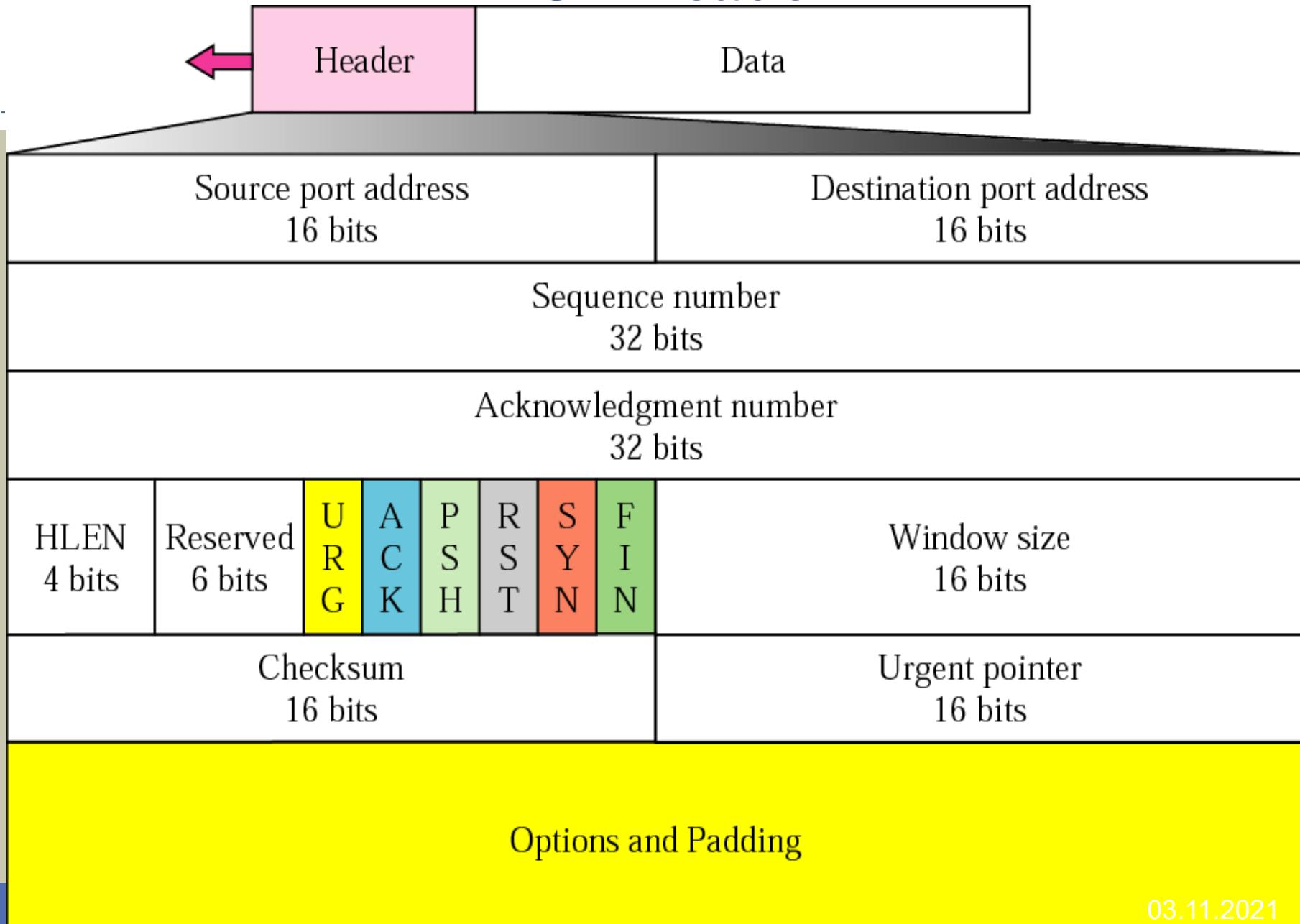
TCP segment

24

- TCP segment consists of data and TCP header
- The standard TCP header length is 20 bytes
- With the option fields it can be expanded up to 60 bytes



TCP Header



TCP header cont.

26

Source port address

- A 16-bit field
- Port number range = 0 – 65535
- **For client TCP header this is a dynamic port number**
- **For server TCP header this is a well-known port number**

Destination port address

- Is the destination process port number
- A 16-bit field

Sequence number

27

- A 32-bit field
- At the time of establishing TCP connection the first sequence number should be decided

Initial Sequence Number (ISN)

- It can be any arbitrarily number between 0 and $2^{32}-1$.

Sequence number cont.

28

- The allocation of sequence number uses the following process
 - Suppose the first data segment has 200 bytes
 - Second data segment has 300 bytes
 - Sequence number of first segment (ISN) is 1000

1	2	3		200
---	---	---	--	-----

1000 ↑ 1002
1001

Segment 1

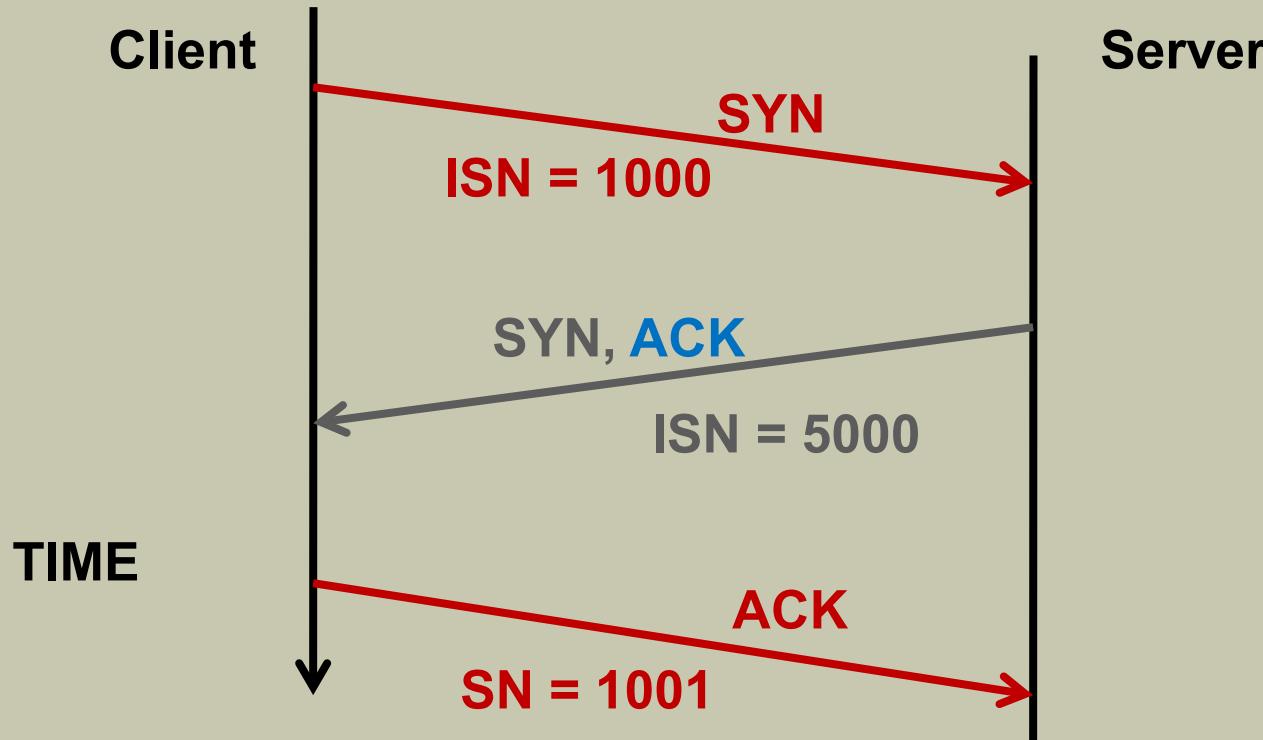
1	2	3		300
---	---	---	--	-----

1199 1200 1499

Segment 2

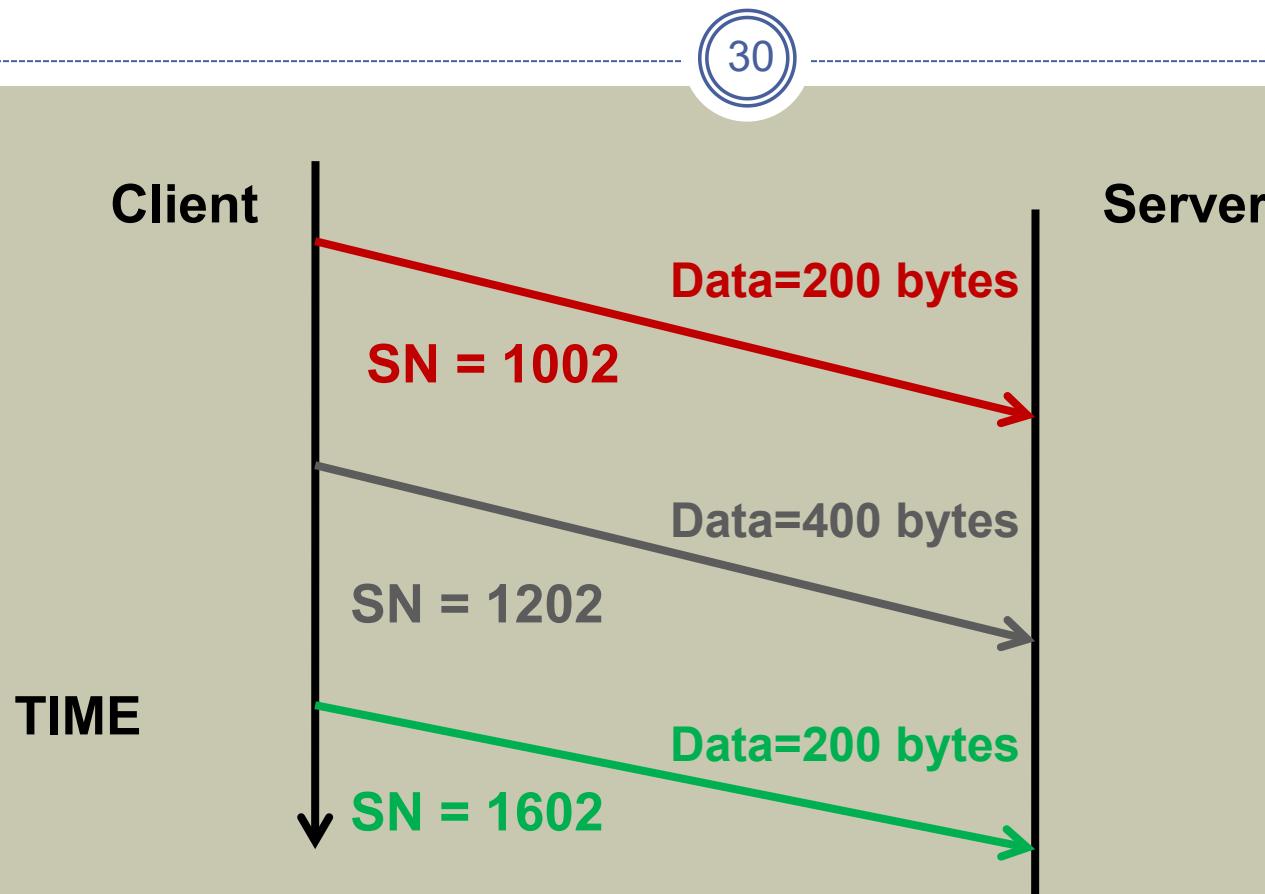
Sequence numbers of three-way handshake

29



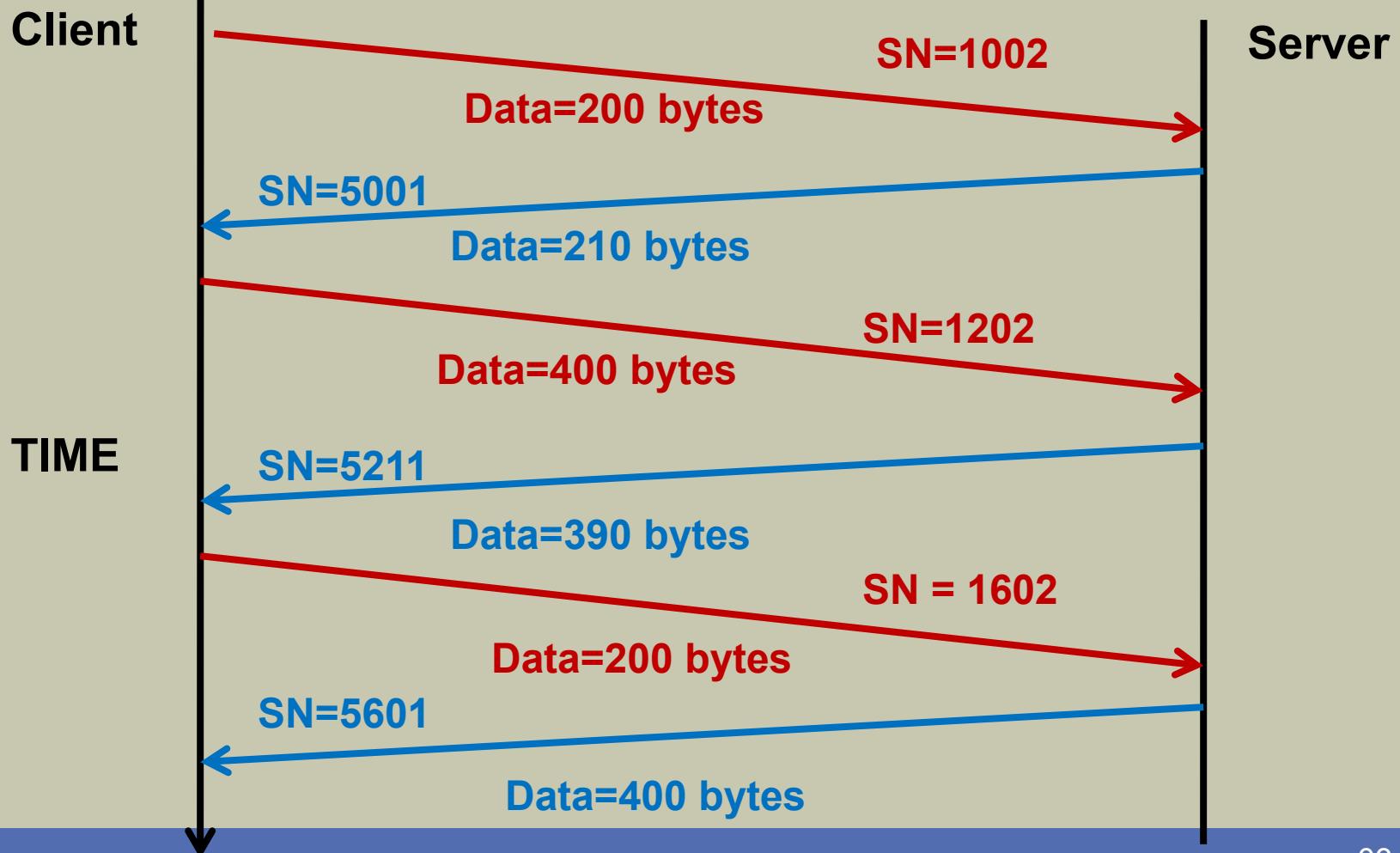
- SYN and ACK : 1 byte each

Sequence numbers of data segments

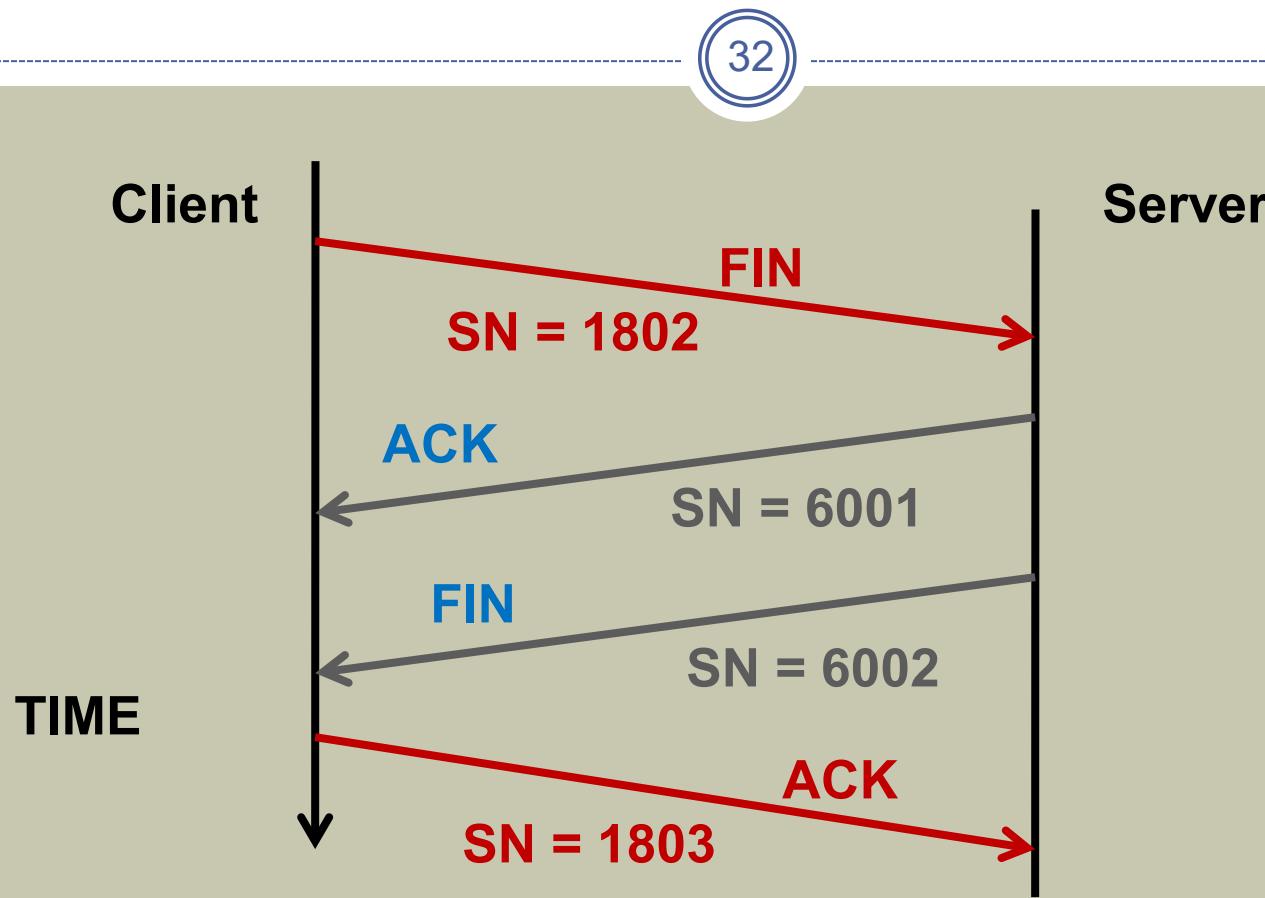


Sequence numbers of data segments cont.

31



Sequence numbers of connection termination



- FIN and ACK : 1 byte each

Acknowledgement Number

33

- A 32-bit field
- An acknowledgement number is sent by the receiver for each data segment it receives
- It is the next sequence number expected by the receiver

Acknowledgement Number cont.

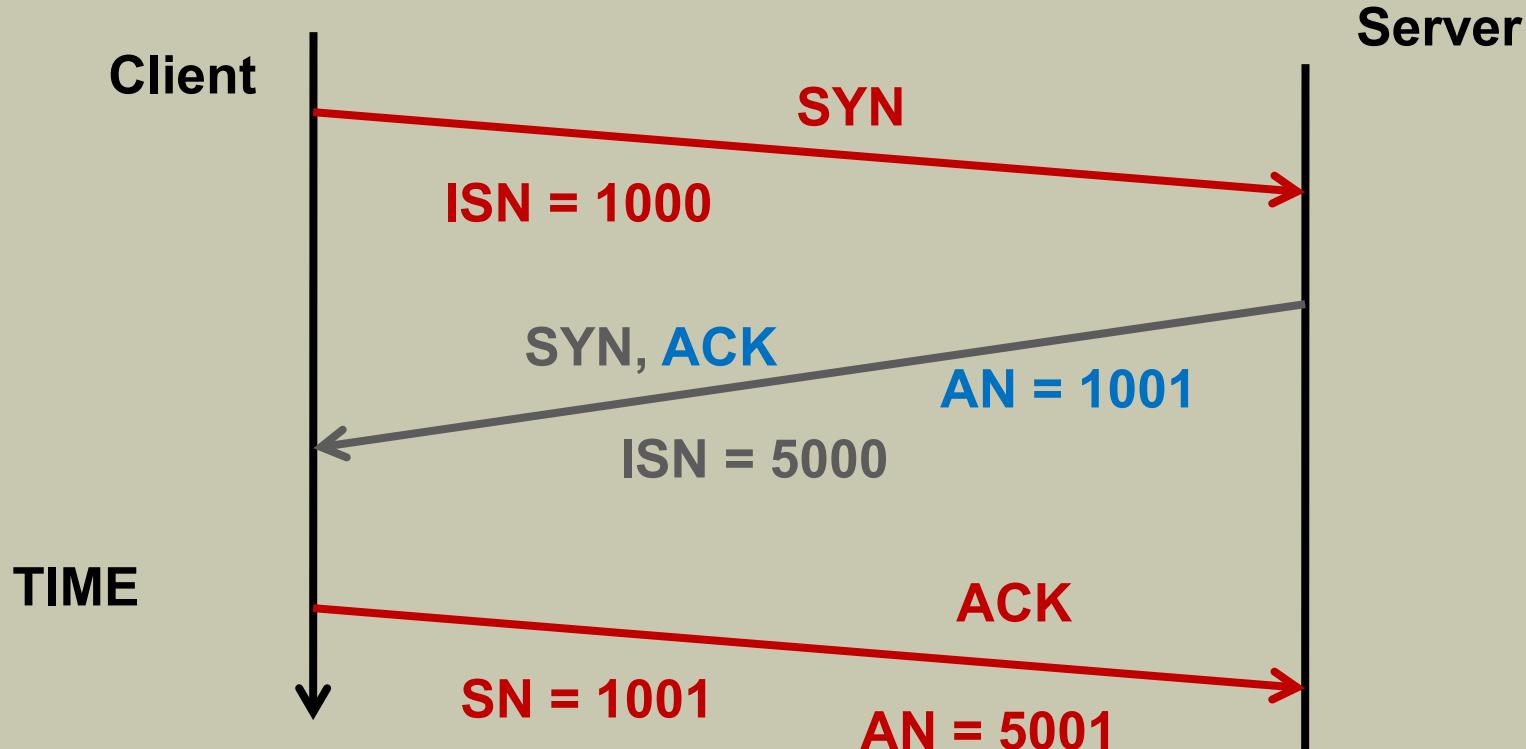
34

- Relationship among sequence number, number of bytes in a segment and the acknowledgement number sent by the receiver

Sequence Number of segment	No. of bytes in the segment	Acknowledgement number send by receiver
1000 (SYN)	1	1001
1001 (ACK)	1	1002
1002	200	1202
1202	400	1602
1602	200	1802
1802 (FIN)	1	1803

Acknowledgement numbers of three-way handshake

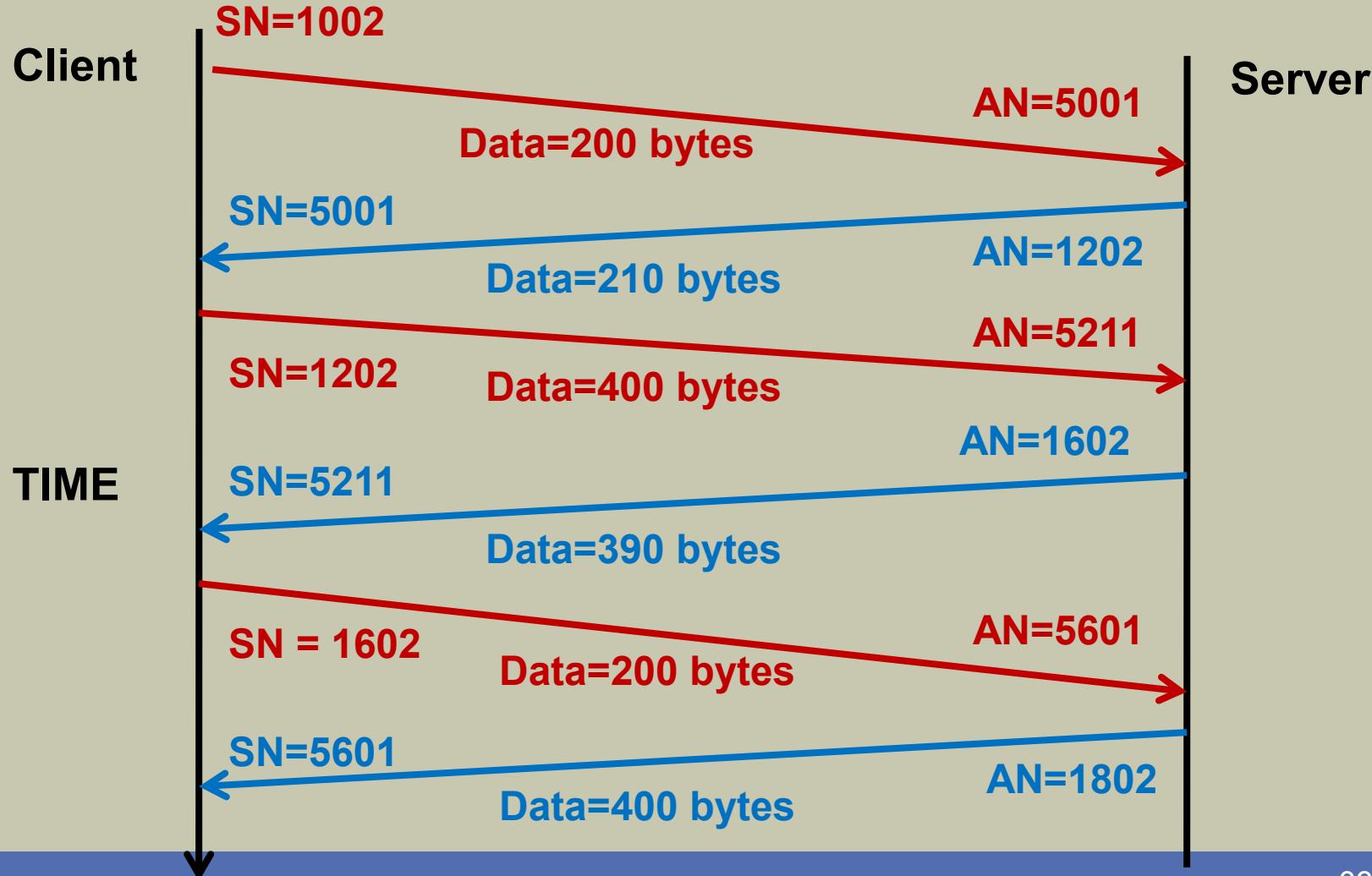
35



- SYN and ACK : 1 byte each

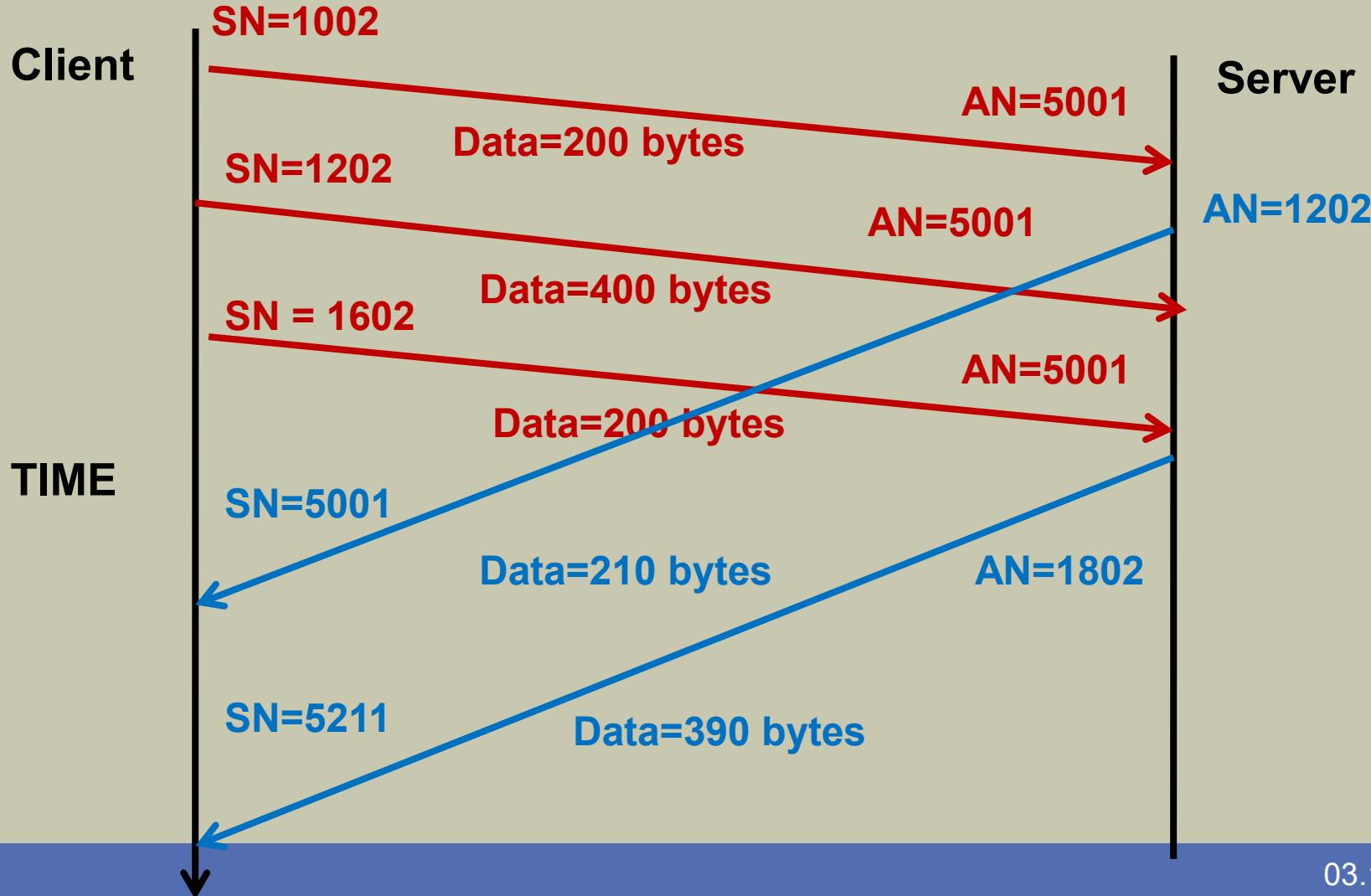
Acknowledgement numbers of data segments cont.

36



Acknowledgement numbers of data segments cont.

37

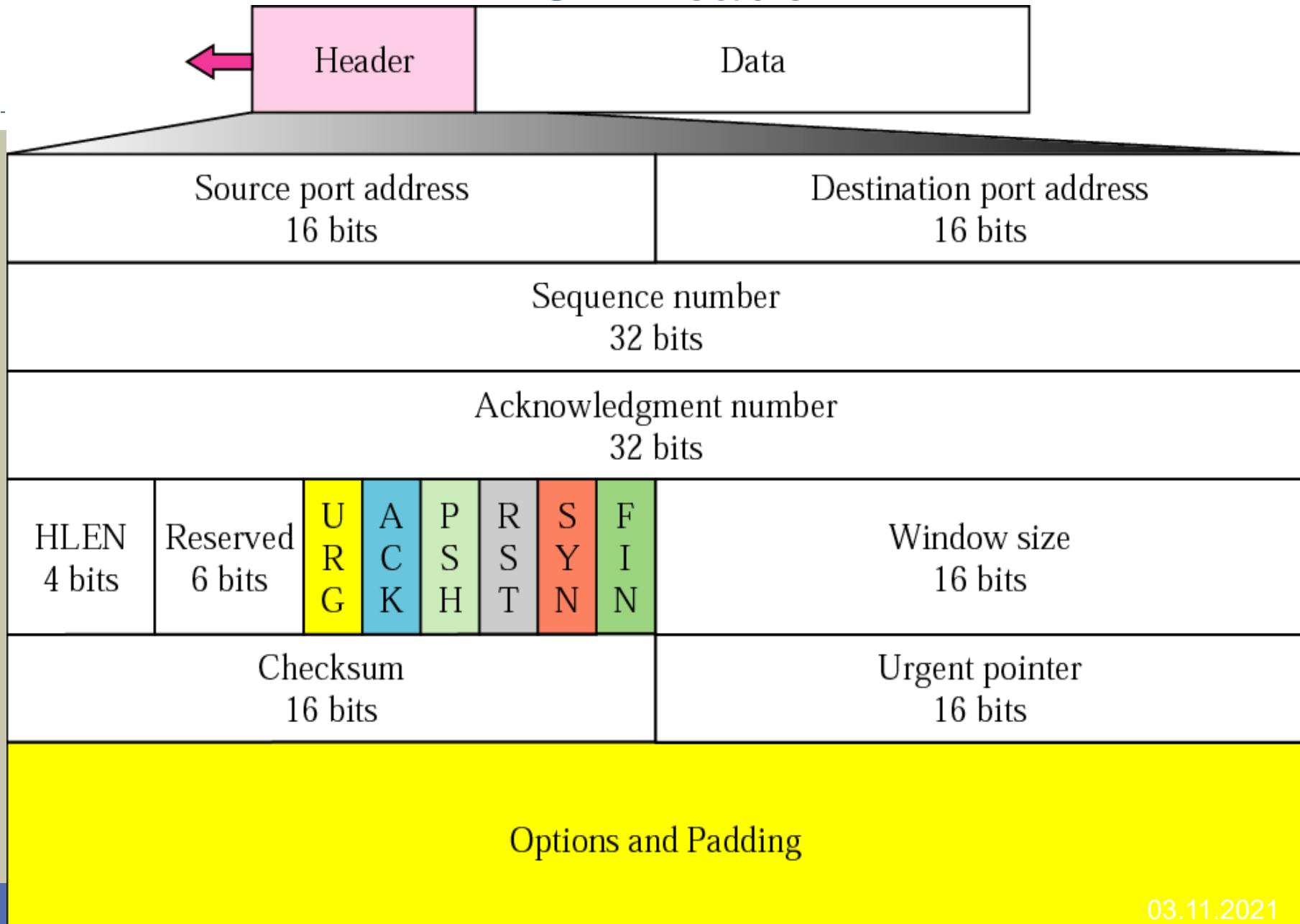


SN and AN in Segment transfer

38

Client				Server			
Segment	No. of byte(s)	SN	AN	Segment	No. of byte(s)	SN	AN
SYN	1	5000	-				
				SYN, ACK	1	2000	5001
ACK	1	5001	2001				
Data	100	5002	2001				
				Data	1500	2001	5102
Data	1000	5102	3501				
Data	2000	6102	3501				
				Data	3000	3501	8102
Data	500	8102	6501				
				Data	1000	6501	8602
FIN	1	8602	7501				
				ACK	1	7501	8603
				FIN	1	7502	8603
ACK	1	8603	7503				

TCP Header

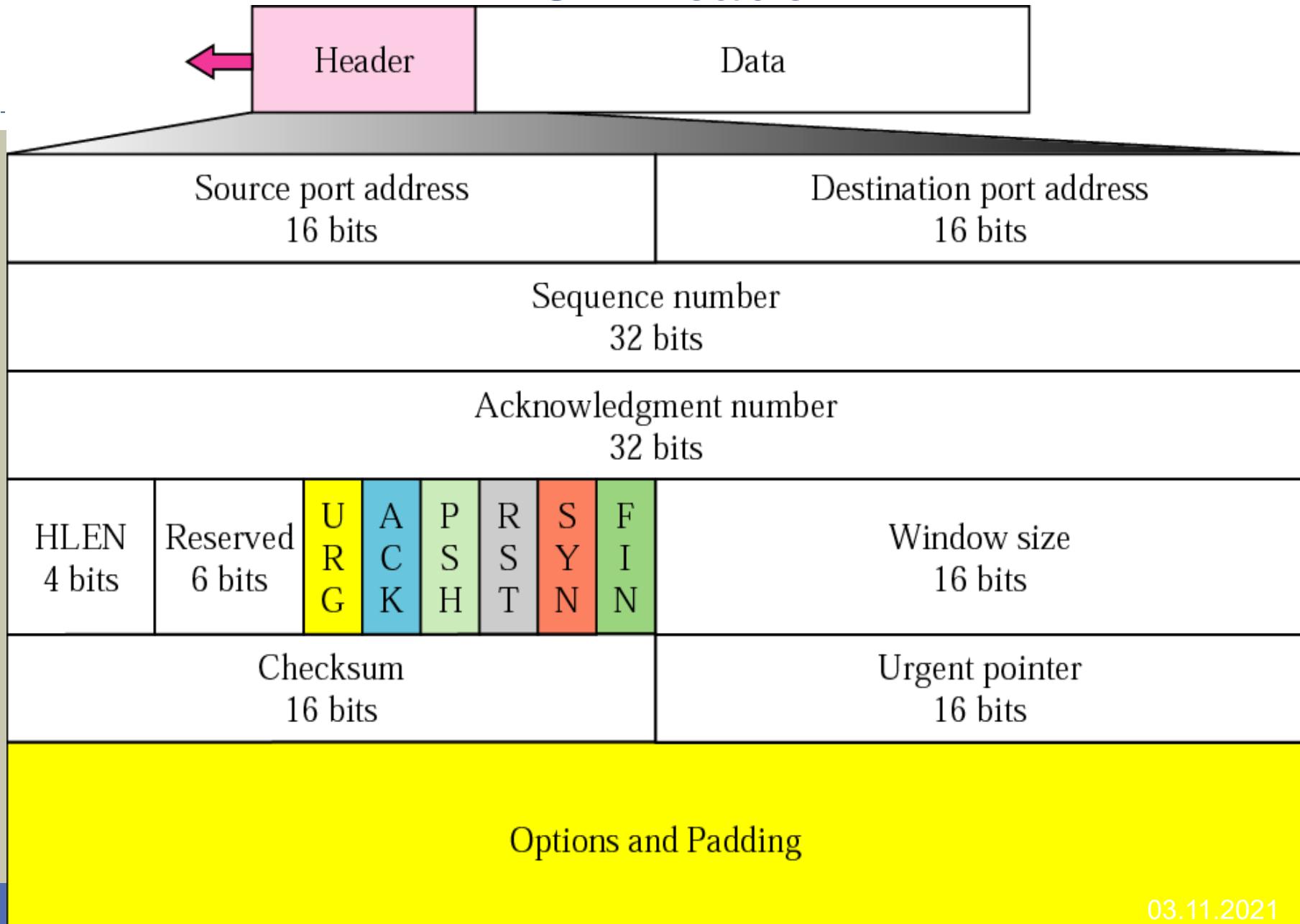


Header Length (HLEN)

40

- This is a 4-bit field
- Header length in bytes = HLEN x 4
- The standard size of header is 20 bytes
- The maximum size of header is 60 bytes
(20 standard bytes and 40 optional bytes)

TCP Header

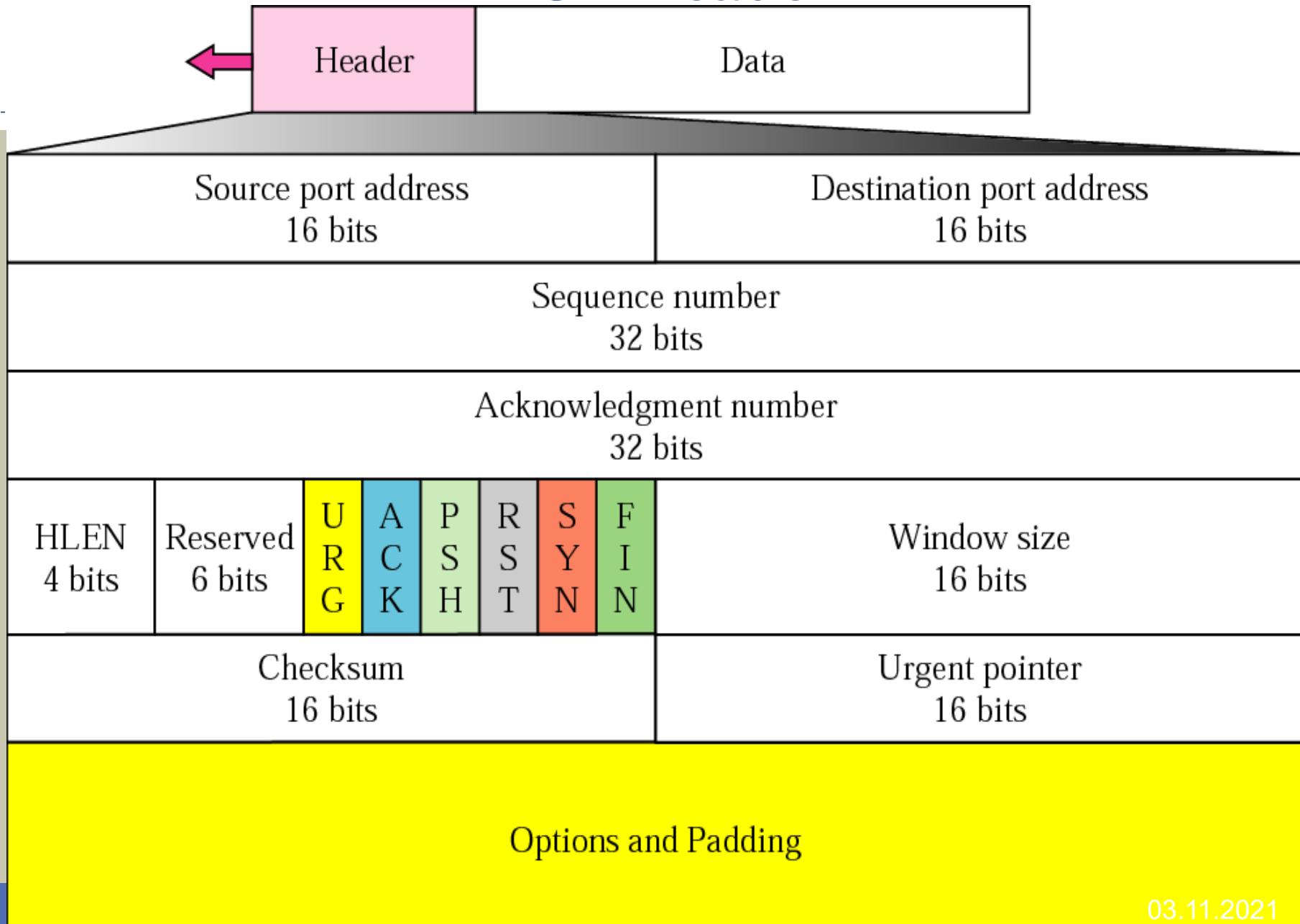


Reserved

42

- This 6 bit field reserved for future use

TCP Header



Control

44

- This is also a six bit field

URG: Urgent pointer is valid

ACK: Acknowledgment is valid

PSH: Request for push

RST: Reset the connection

SYN: Synchronize sequence numbers

FIN: Terminate the connection

URG

ACK

PSH

RST

SYN

FIN

URG - Urgent

45

- Normally receiver reads segments according to ascending order
- If this flag is set, that segment should be read immediately

ACK - Acknowledgement

46

- If data is not available in the segment,
then this is an ACK segment
- If data is available in the segment,
and if the acknowledgement number is ‘n’
it indicates that data bytes up to byte $n-1$ is OK and waiting for
sequence number n

PSH - Push

47

- If push flag is set, it does not care about the **window size** recommended by other party and **start the data transmission** to the other party

RST - Reset

48

- The connection must be reset (Destroy / Terminate)
- This can happen due to three reasons
 - Request for an unidentified port
 - Client or server has a problem
 - The other side TCP is idle for a long time

RST - Reset cont.

49

Reason 1 :

- The client requests a connection for server to an unidentified port
- In such situation server send RST to client to destroy the connection

RST - Reset cont.

50

Reason 2 :

- The connection has been established
- After some time the client or server has a problem and request the other party to destroy the connection
- Then it (client or server) sends RST to other party.

RST - Reset cont.

51

Reason 3 :

- The other side TCP is idle for a long time
- Then RST is sent to the other party to destroy the connection

SYN - Synchronize

52

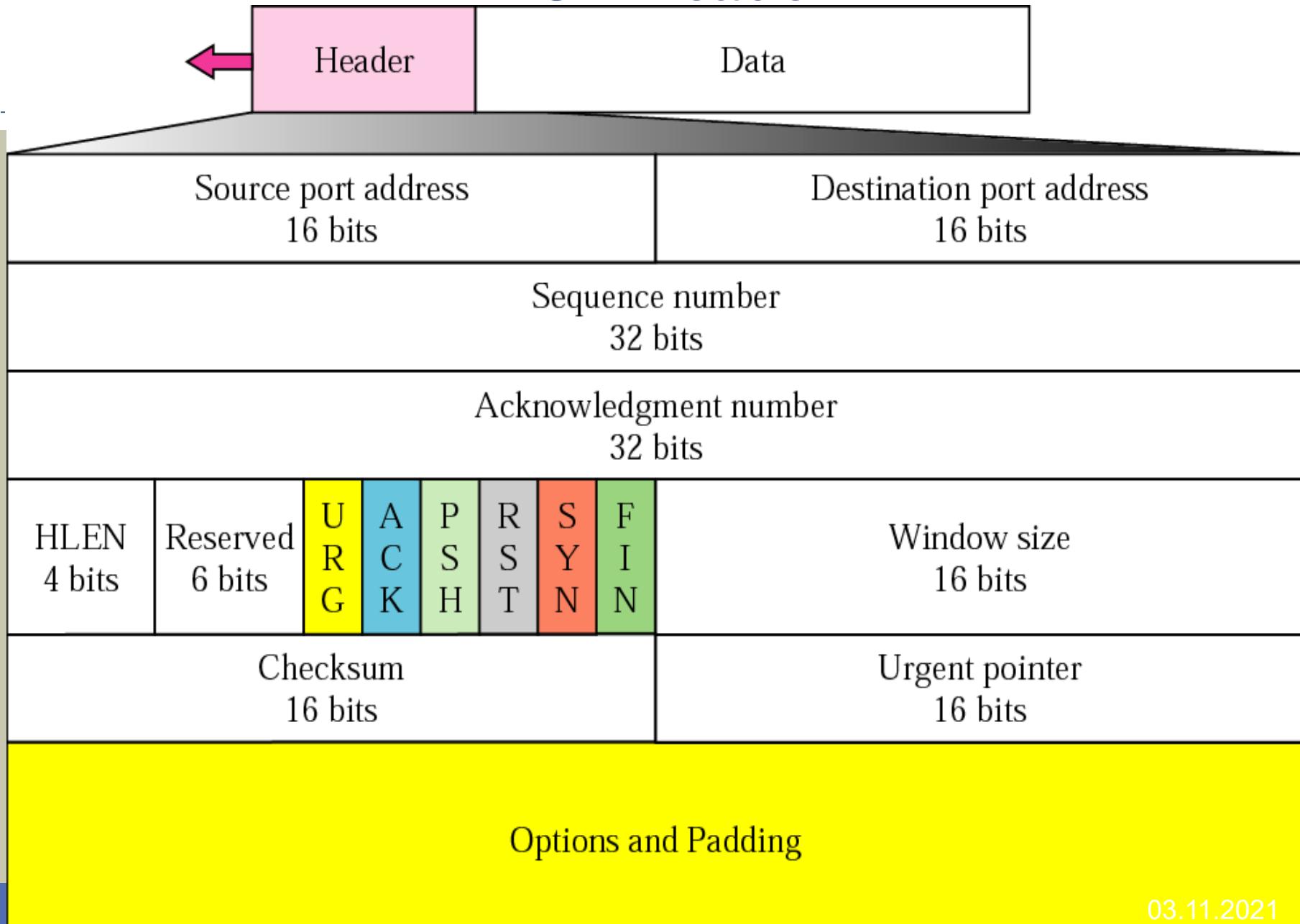
- Synchronize to sequence numbers (Initial Sequence Number) suggested at the time of connection establishment

FIN - Finish

53

- Request to terminate the connection to that direction
- If client sent FIN (that is set FIN flag) to server, it means that client request from server to disconnect the connection of client server direction

TCP Header

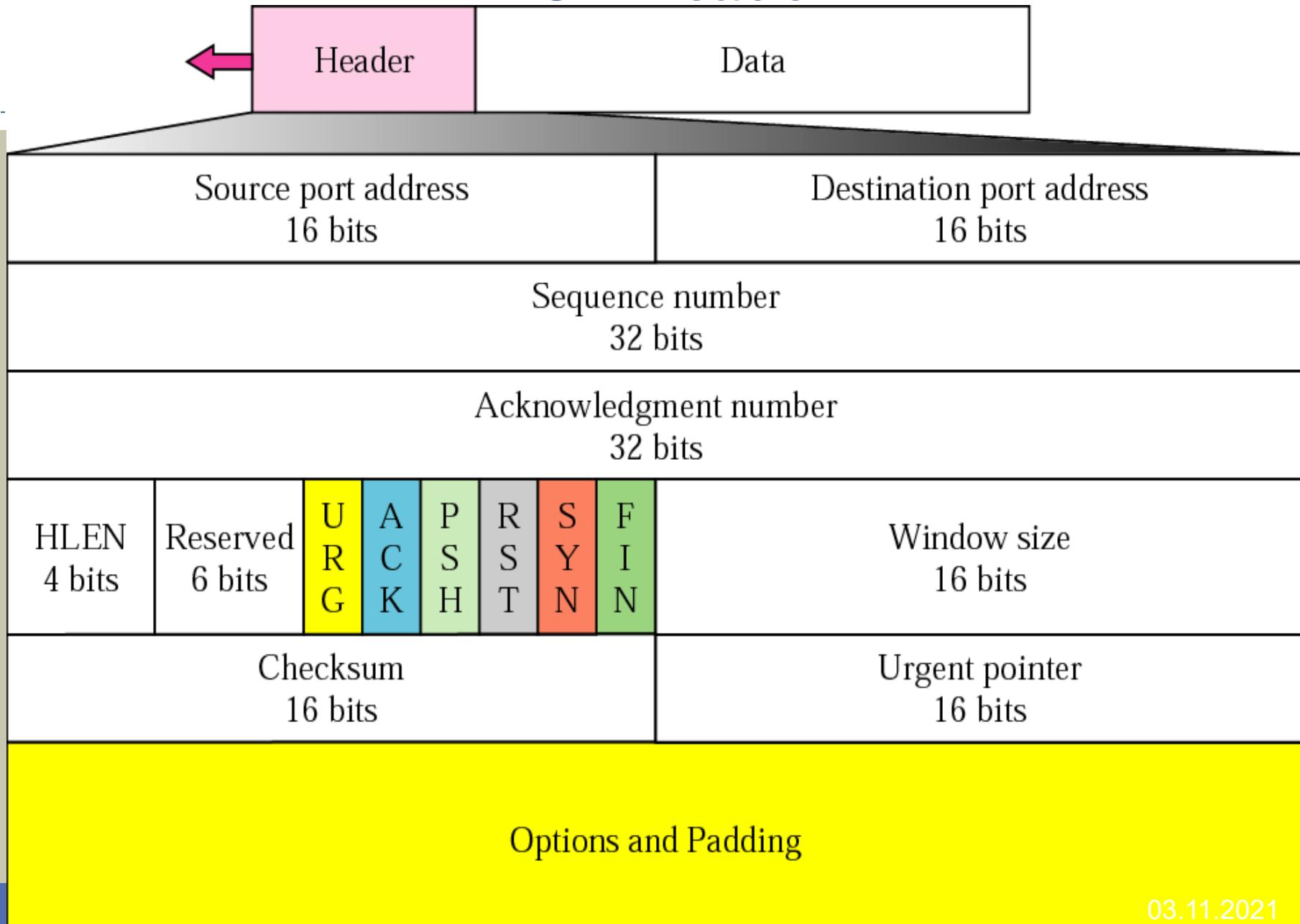


Window size

55

- This is a 16-bit field
- Indicates how many bytes (segment data) can be maintained in the other party

TCP Header

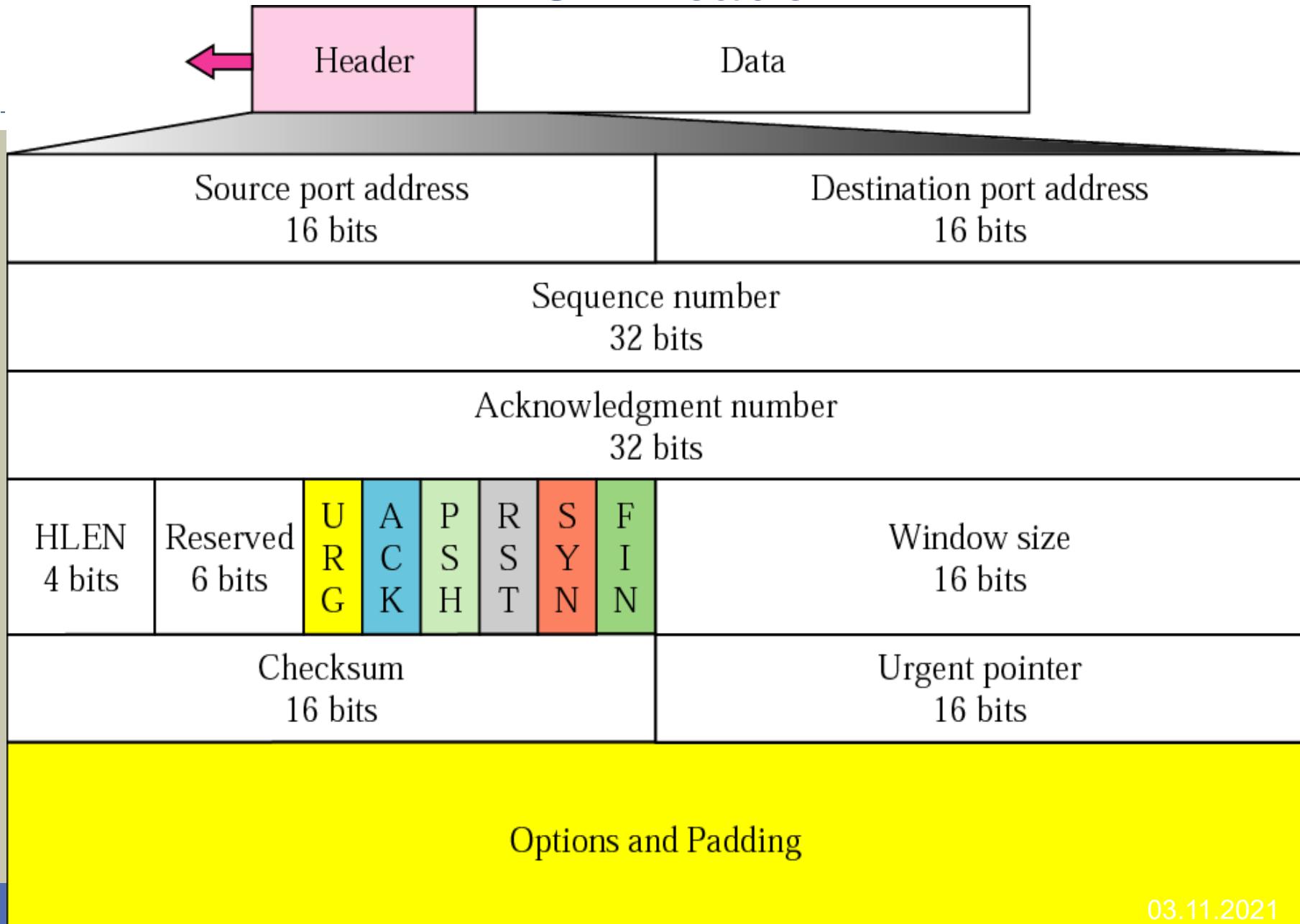


Checksum

57

- This is a 16 bit field
- Used to check whether there are any errors

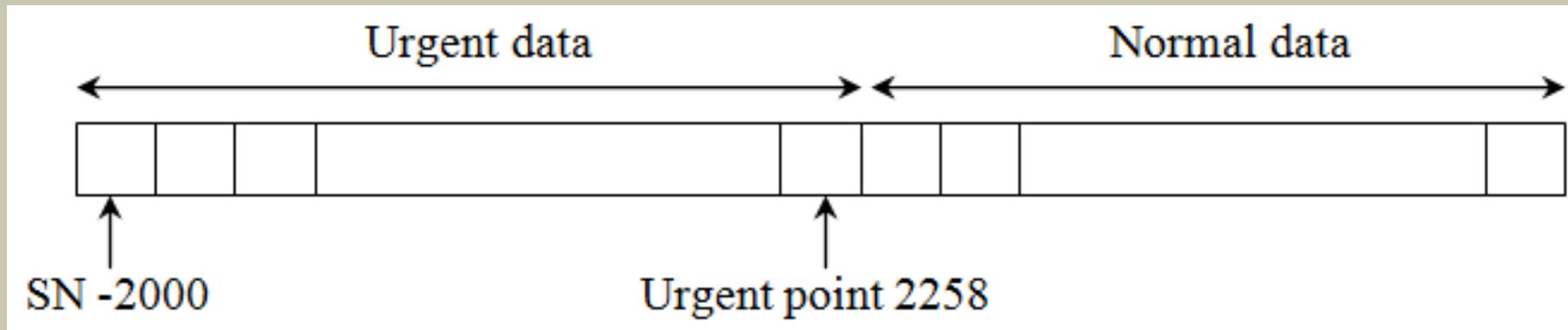
TCP Header



Urgent Pointer

59

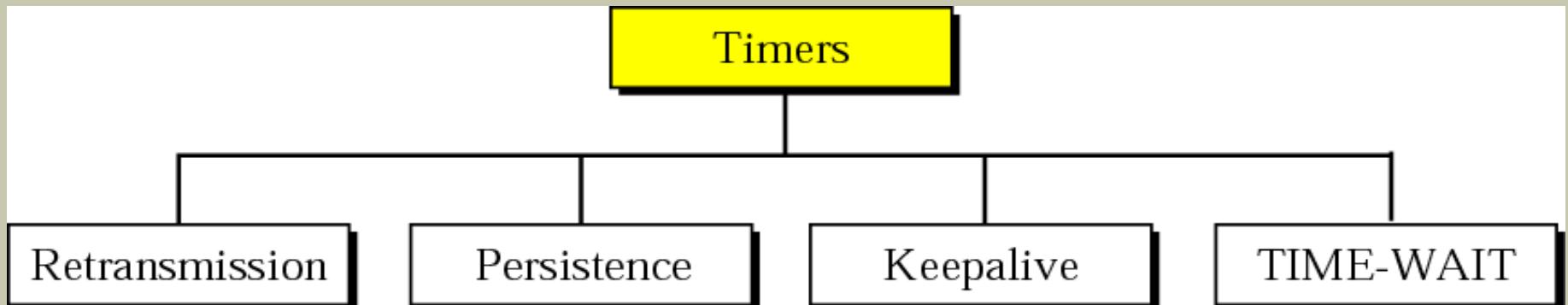
- This is a 16-bit field valid only if the urgent flag is set
- This value gives the byte value **at the end of urgent data**



- The bytes 2000 to 2258 are urgent data

TCP Timers

60



TCP Timers cont.

61

Timer	Purpose
Retransmission	For error control
Persistence	To avoid problems of zero window size advertisement
Keep alive	To check whether client is alive if it is idle for a long time
Time-waited	To avoid problems with delayed FIN segments

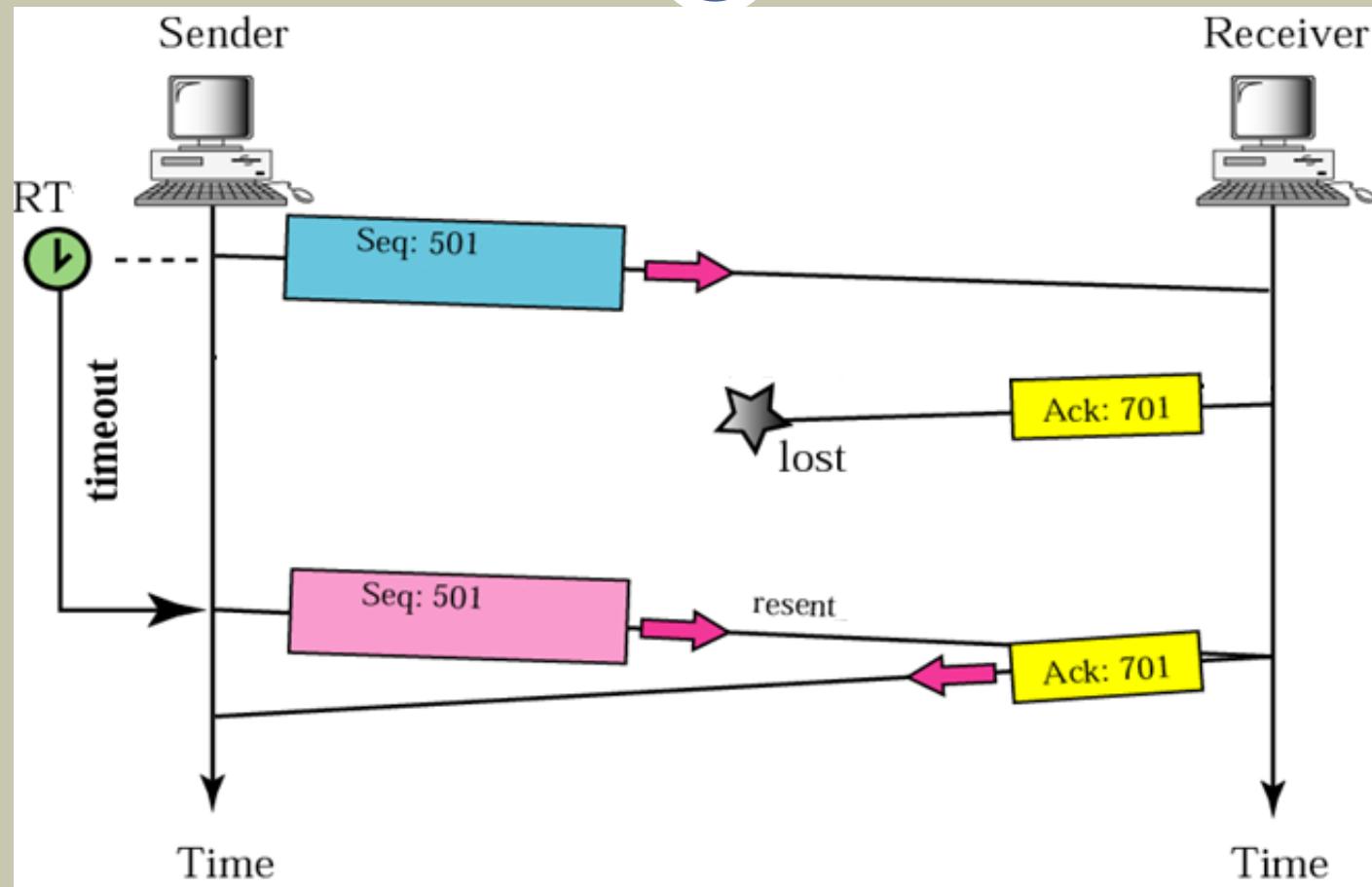
Retransmission Timer

62

- This timer starts after sending a segment
- If the acknowledgement is not received before this timer expires, the same segment is re-transmitted and the timer is reset
- If the acknowledgement is received before retransmission timer expires that timer will be destroyed (Timer will be stopped)

Retransmission Timer cont.

63

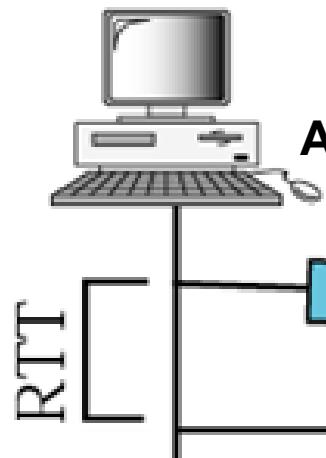


- Retransmission time = $2 \times$ Round Trip Time

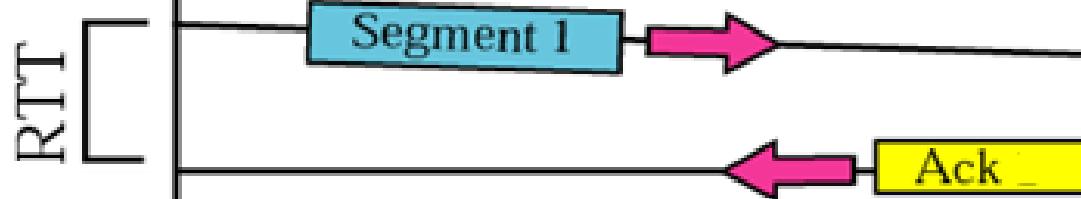
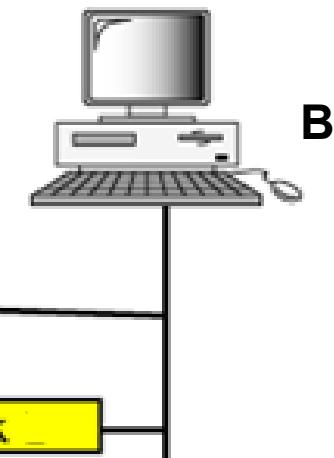
Round Trip Time

(64)

Sender



Receiver



The time involved here are

- Propagation delay from A to B
- Processing time at B
- Propagation delay from B to A
- The total of above times are called Round Trip Time

Measured Round Trip Time

65

- Can measure **Round Trip Time** Using the “time stamp” obtained from the option field of TCP header
- TCP sends a segment, starts a timer, and waits for acknowledgement
- It measures the time between sending of the segment and receiving of the acknowledgement

Setting the Round Trip Time

66

Setting RTT= $\alpha \times \text{Previous RoundTT} + (1-\alpha) \text{ Current RoundTT}$

$$\alpha = 90\%$$

Setting RTT= $0.9 \times \text{Previous RoundTT} + 0.1 \text{ Current RoundTT}$

- There is a difference between measured Round Trip Time and setting Retransmission Time
 - Retransmission timer = $2 \times \text{Setting RTT}$

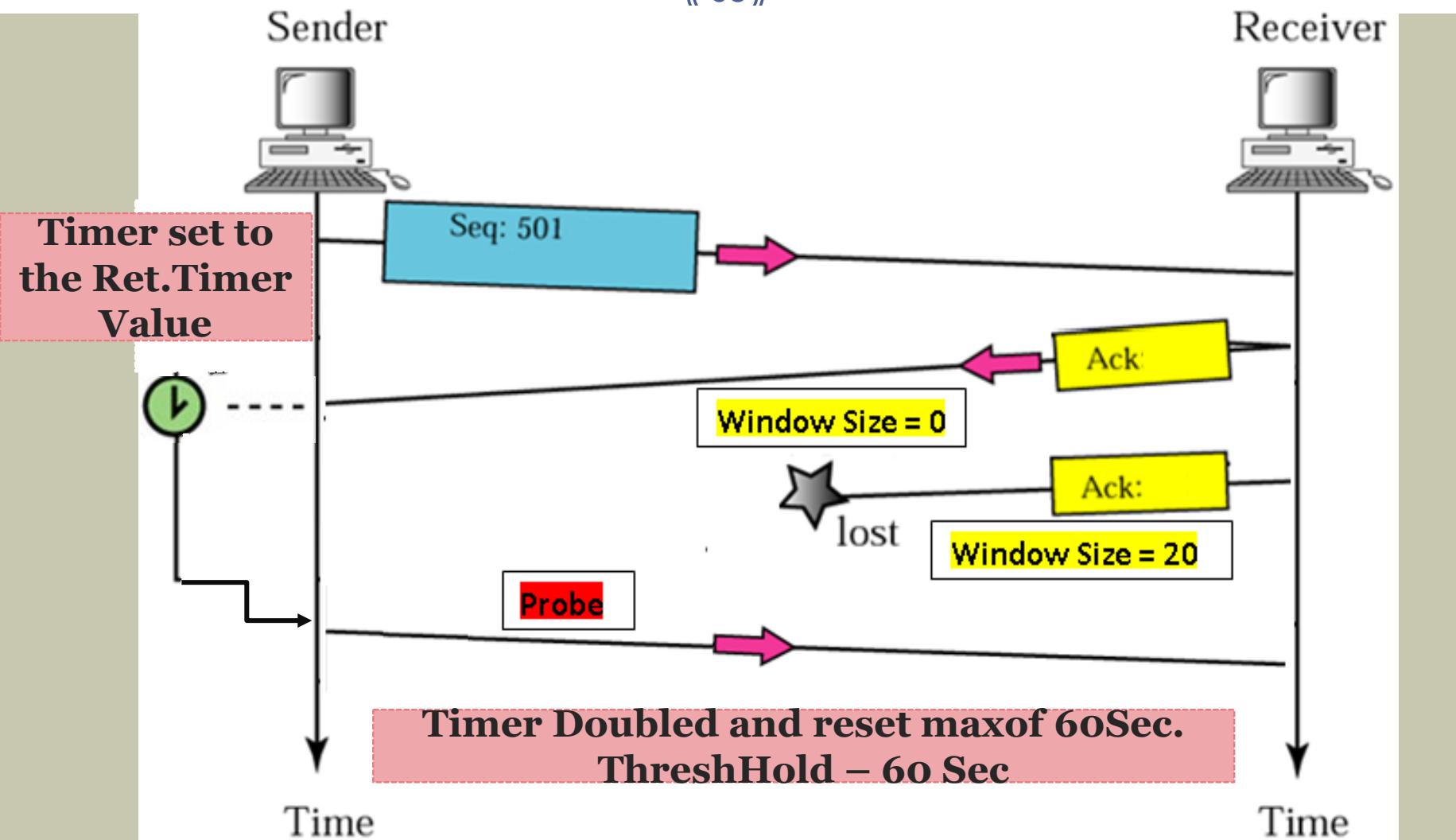
RTT cont.

67

Segment	Measured RTT (ms)	Set RTT (ms)	Ret Timer
n	250	---	
n+1	200	---	500
n+2	180	$90\%250 + 10\%200 = 245$	490
n+3	220	$90\%200 + 10\%180 = 198$	396

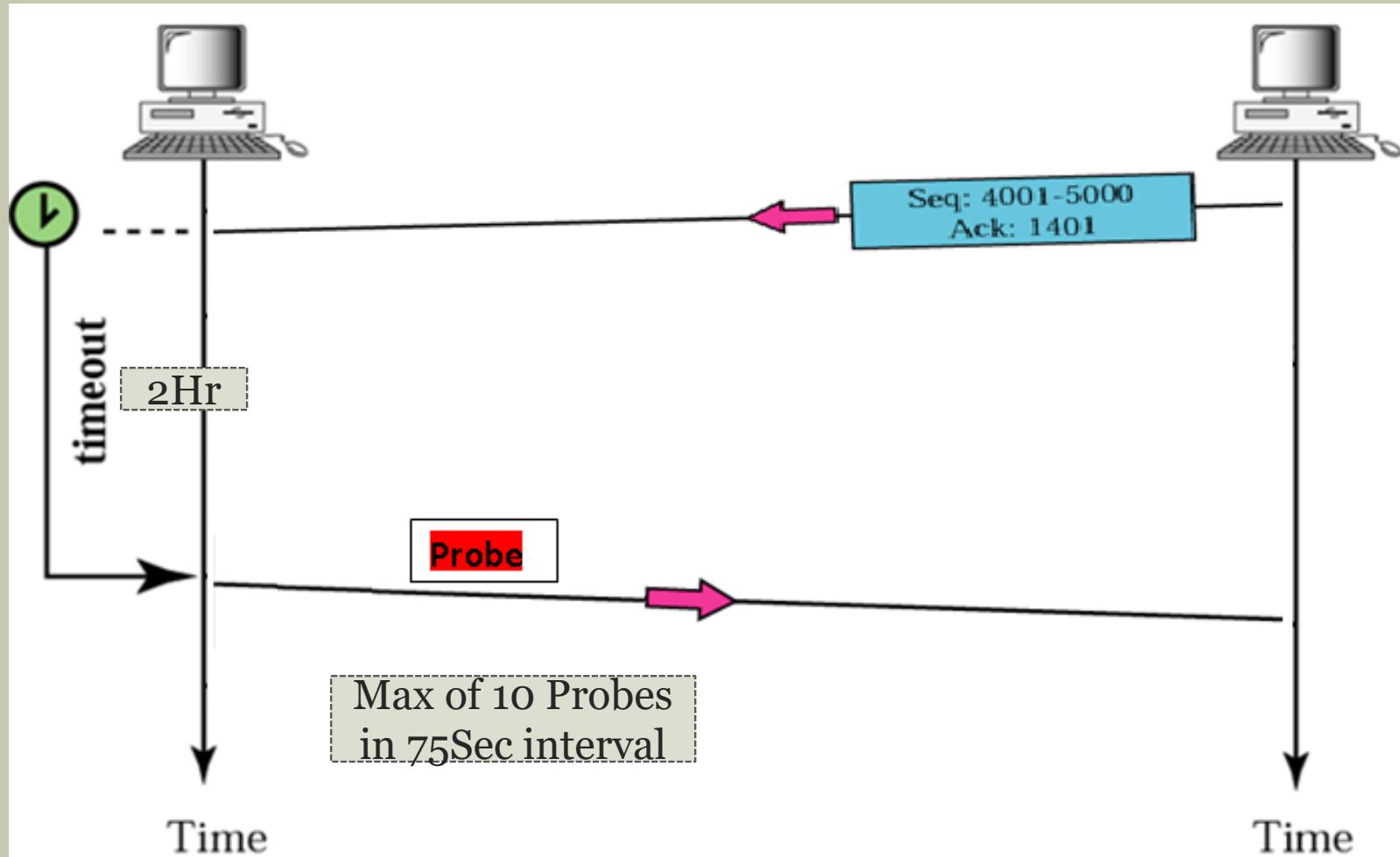
Persistence Timer

(68)



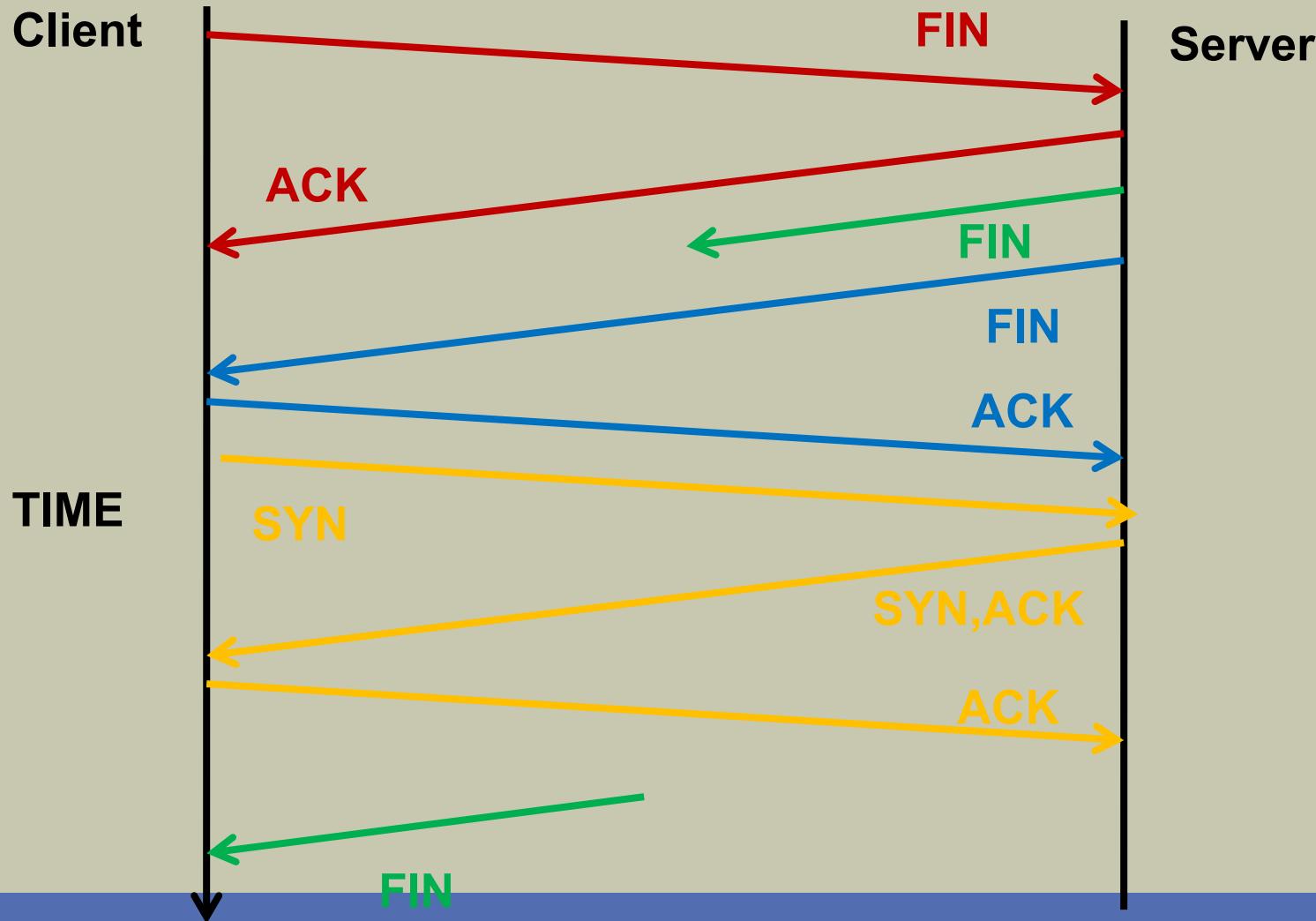
Keep alive Timer

69



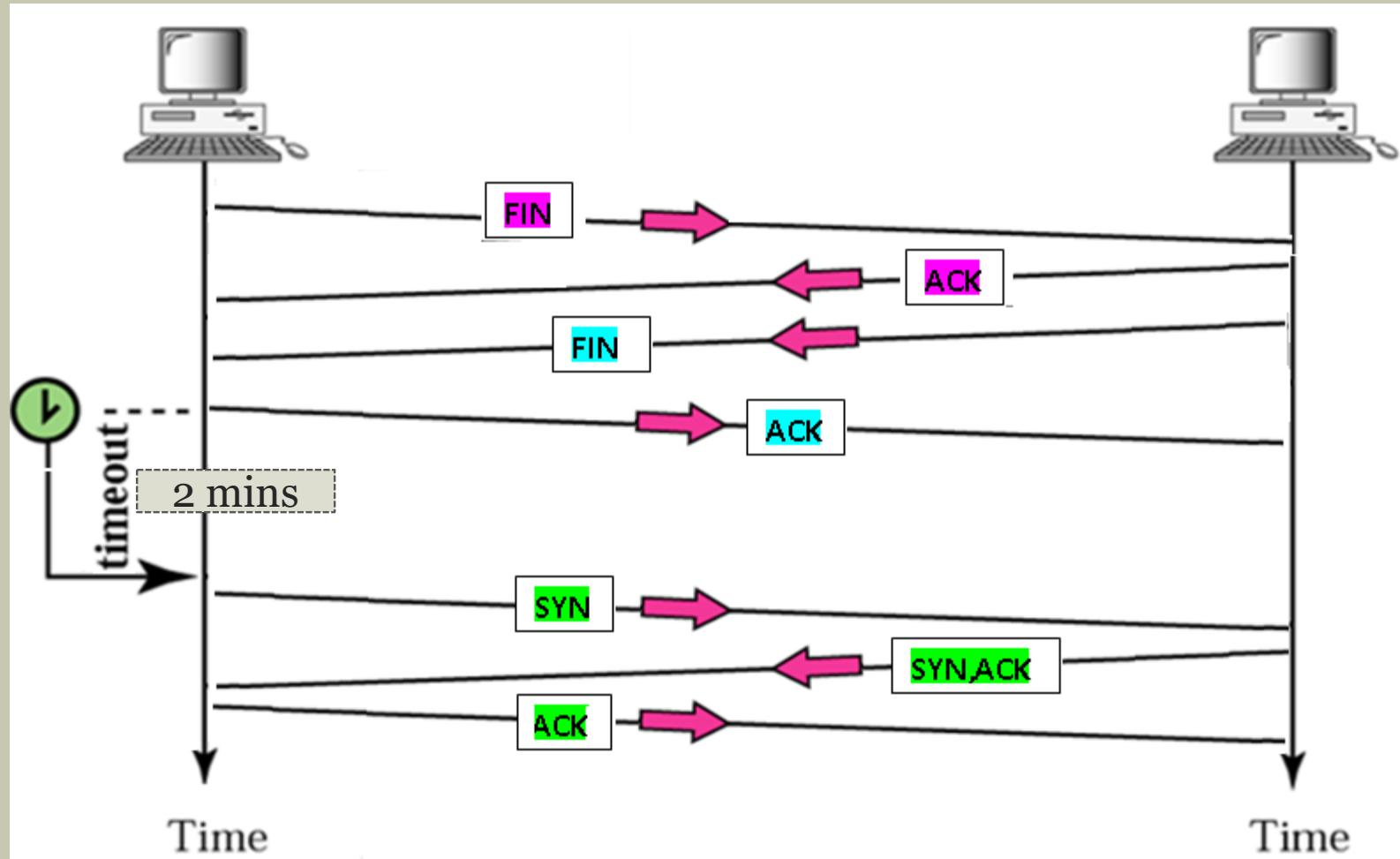
Time Waited Timer

70



Time Waited Timer cont.

71



Error Control

72

- TCP uses the backward error control
- For error detection, the checksum bits in the TCP header is used by the receiver
- If the receiver detects errors, it will discard that segment
- The receiver will not send any negative acknowledgement to sender

Error Control cont.

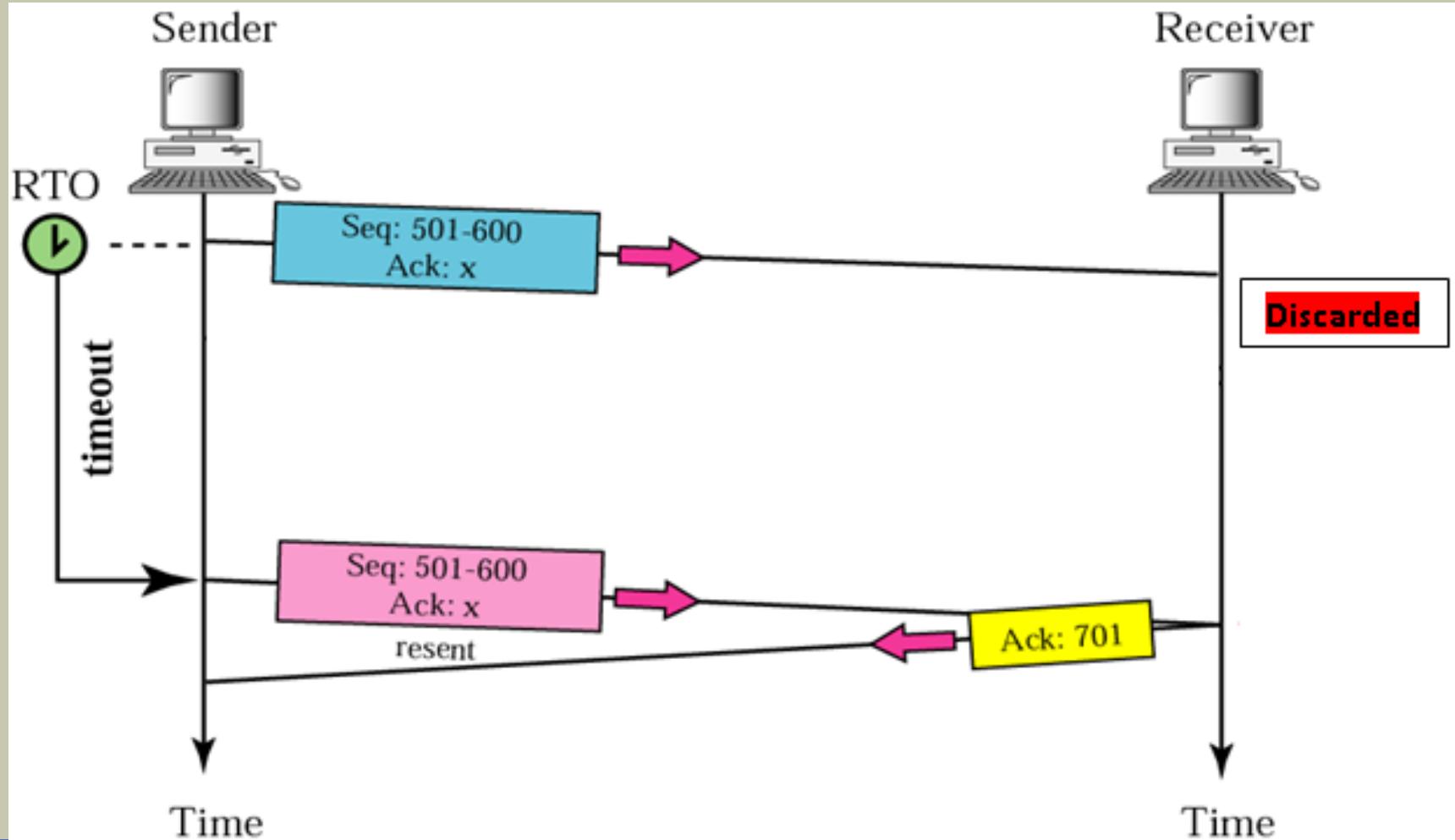
73

Error control process considers,

- Errors in the received segment (corrupted segments)
- Segment is lost on the way before reaching the receiver (last segment)
- Duplicate received segments
- Out of order segments (the segment numbers are not received in order)
- Lost an acknowledgement on the way

Corrupted Segment

74



Out of order segment

75

- The IP packets can travel through different routers
- Therefore the segments can reach the receiver TCP layer out of order
- The TCP layer waits until previous segment(s) are received and then acknowledges

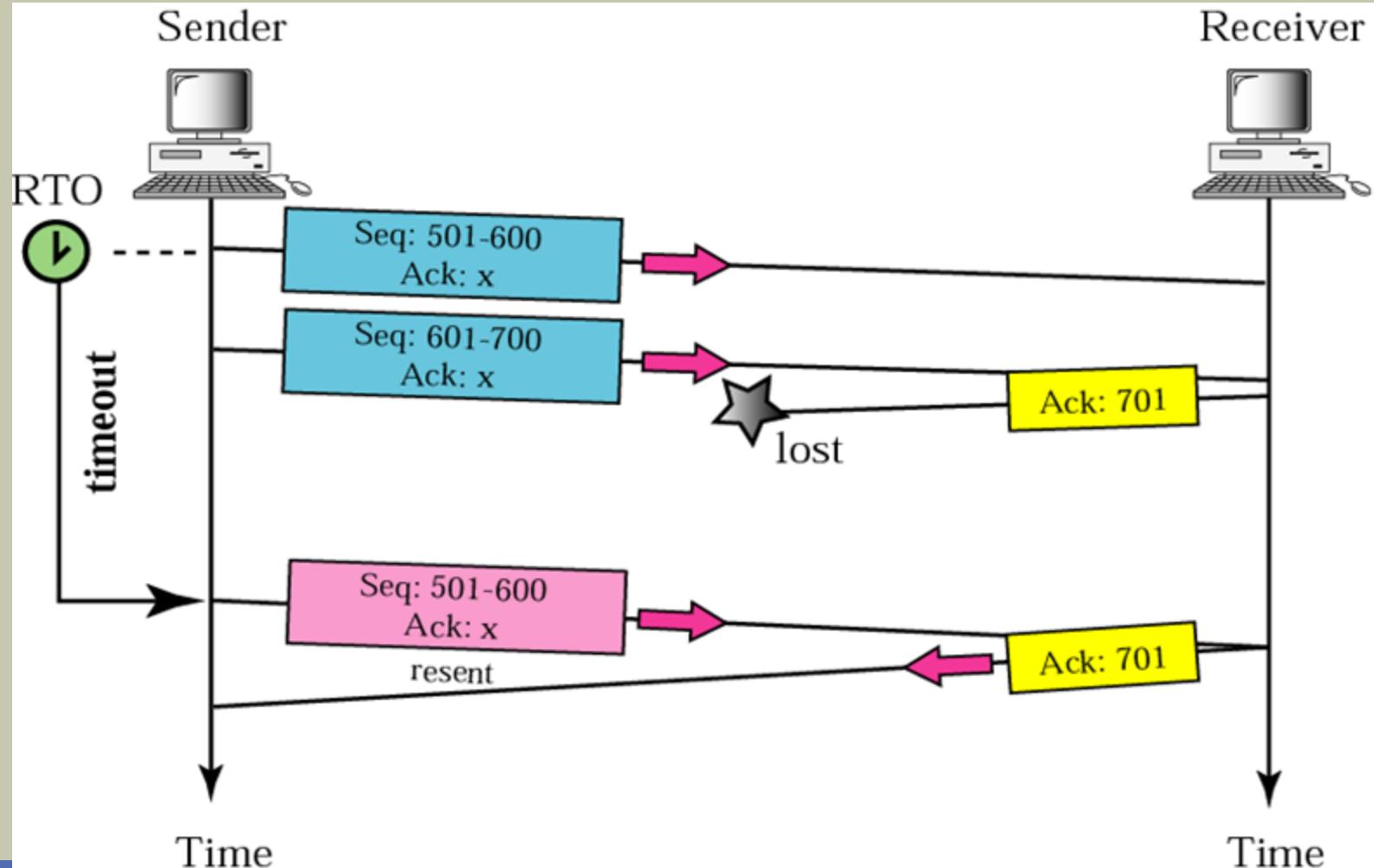
Duplicate segment

76

- If IP packet travels through a long way the retransmission timer expire and sender retransmit the same segment
- The receiver receives both segments
- If the first segment received has no errors, it is accepted and acknowledged
- The second segment is ignored by the TCP layer

Lost acknowledgement

77



Window Size

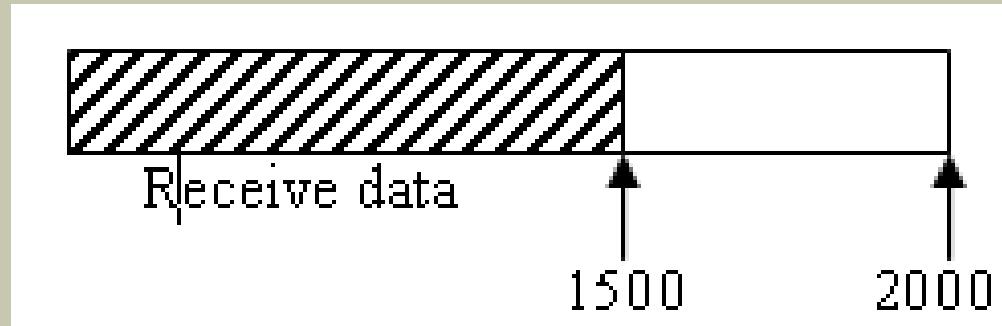
78

- Receiver TCP buffer can be overflowed due to two reasons
 - The receiver TCP buffer receives data very fast
 - The receiver application consumes data very slowly
- Receiver TCP should inform the sender TCP how much bytes of data it can accommodate
- It is called the window size

Windows Size cont.

79

- Scenario 1 : Suppose the TCP buffer size is 2000 bytes



- If it receives 1500 bytes of data, 500 bytes buffer space is free
- Then it informs the sender the window size is 500

Windows Size cont.

80

- Scenario 2 : Application may have consumed another 800 bytes,
- The remaining data bytes in the buffer is

$$1500 - 800 = 700 \text{ bytes}$$

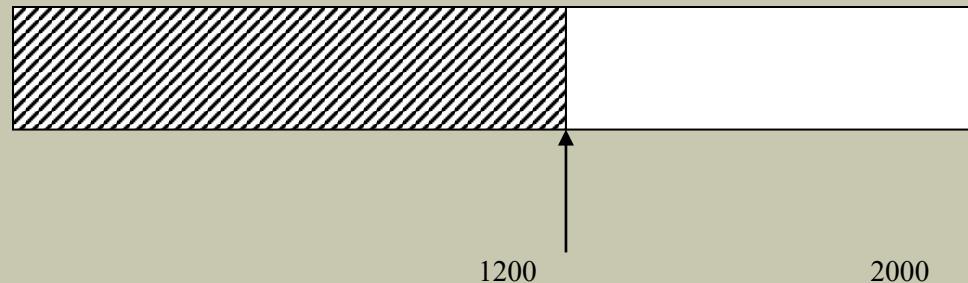
- New window size is

$$2000 - 700 = 1300$$

Windows Size cont.

81

- Scenario 3 : Sender may send 500 bytes
- The remaining data bytes in the buffer is
 $700 + 500 = 1200$ bytes
- New window size is
 $2000 - 1200 = 800$



Windows Size cont.

82

- Scenario 4 : Sender may send 800 bytes. But the receiver application was busy and it did not consume any data.
- The remaining data bytes in the buffer is
 $1200 + 800 = 2000$ bytes
- New window size is
 $2000 - 2000 = 0$



Windows Size cont.

83

- Scenario 5 : Receiver application consumed 200 bytes of data
- The remaining data bytes in the buffer is

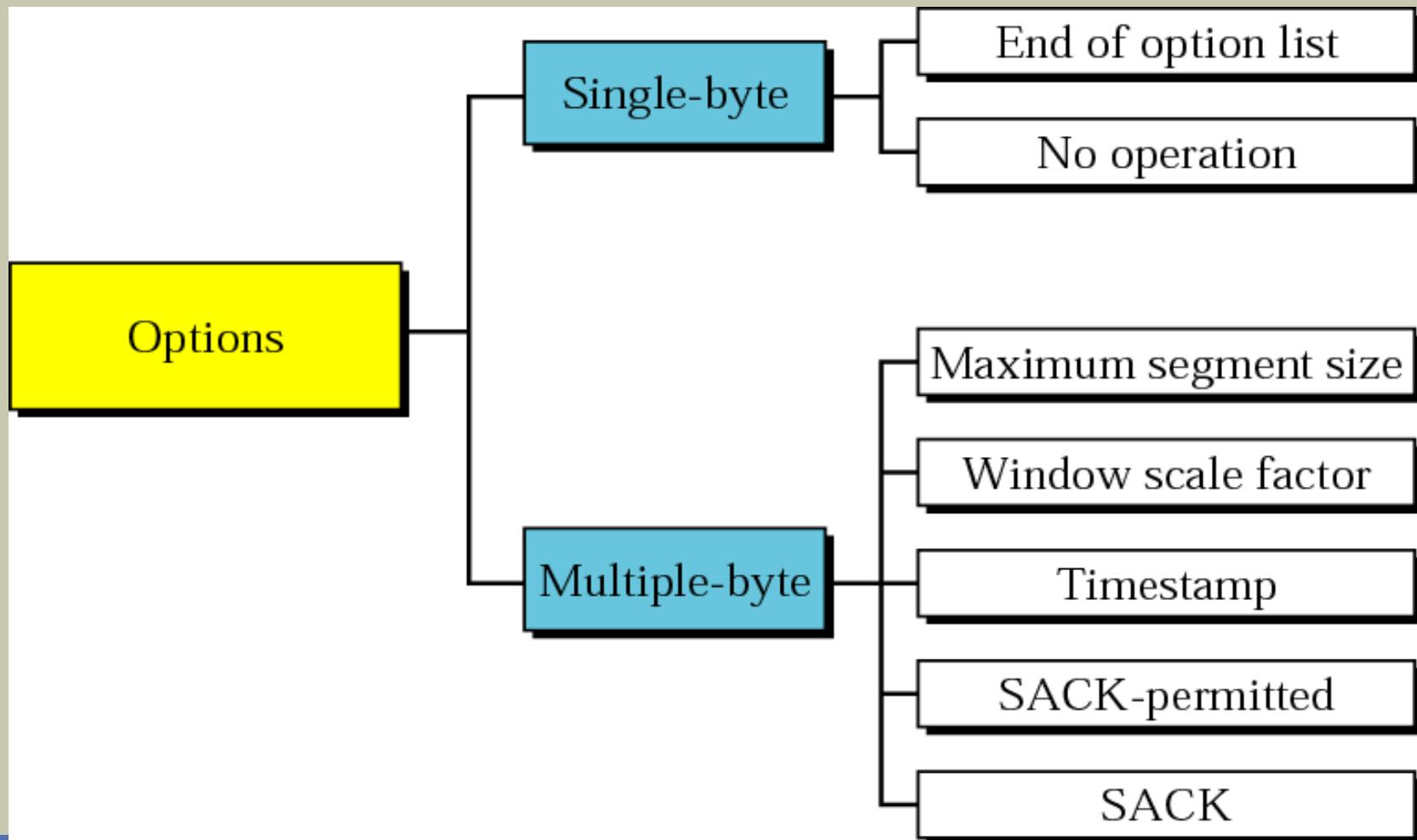
$$2000 - 200 = 1800 \text{ bytes}$$

- New window size is

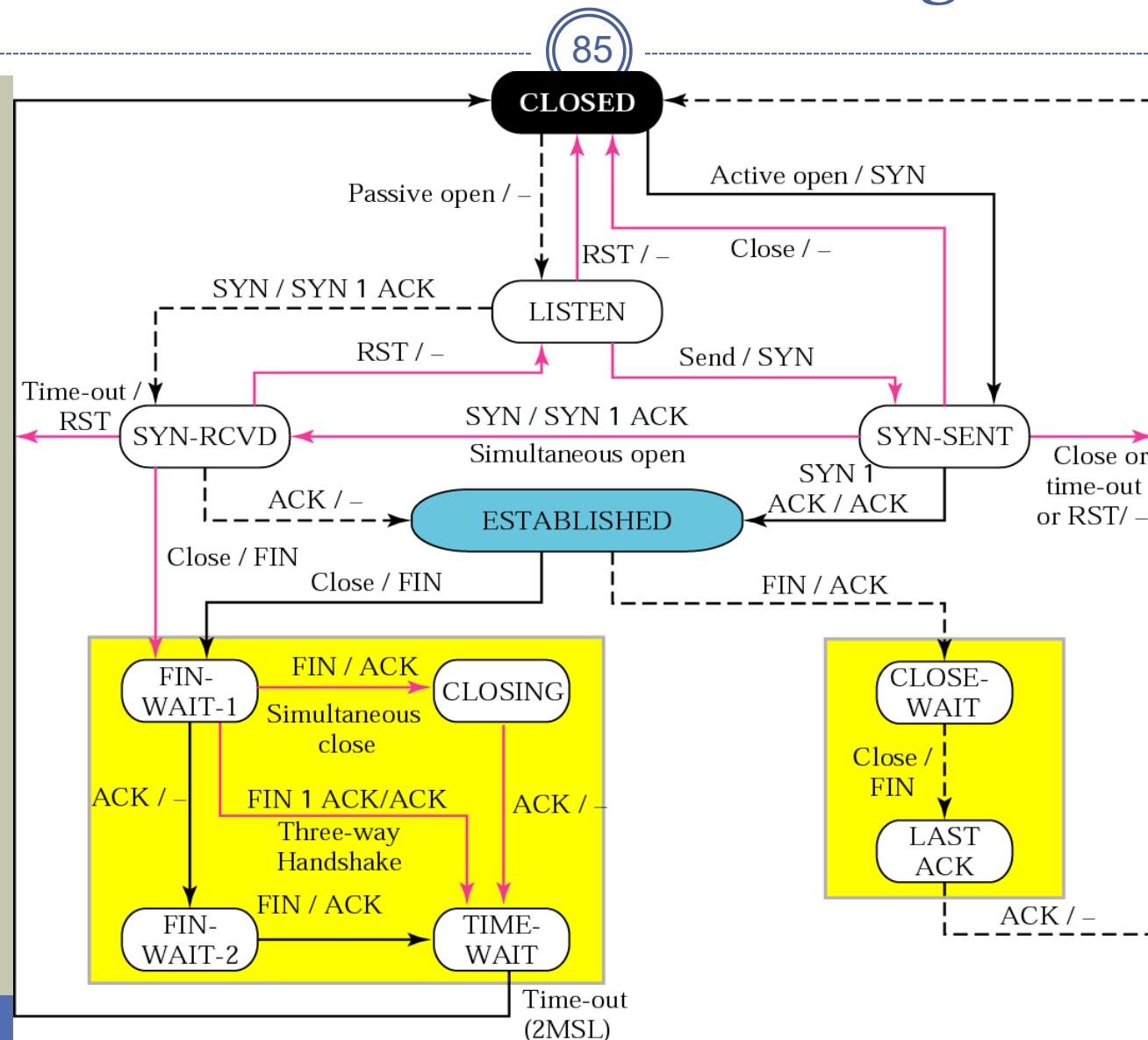
$$2000 - 1800 = 200$$

TCP Option

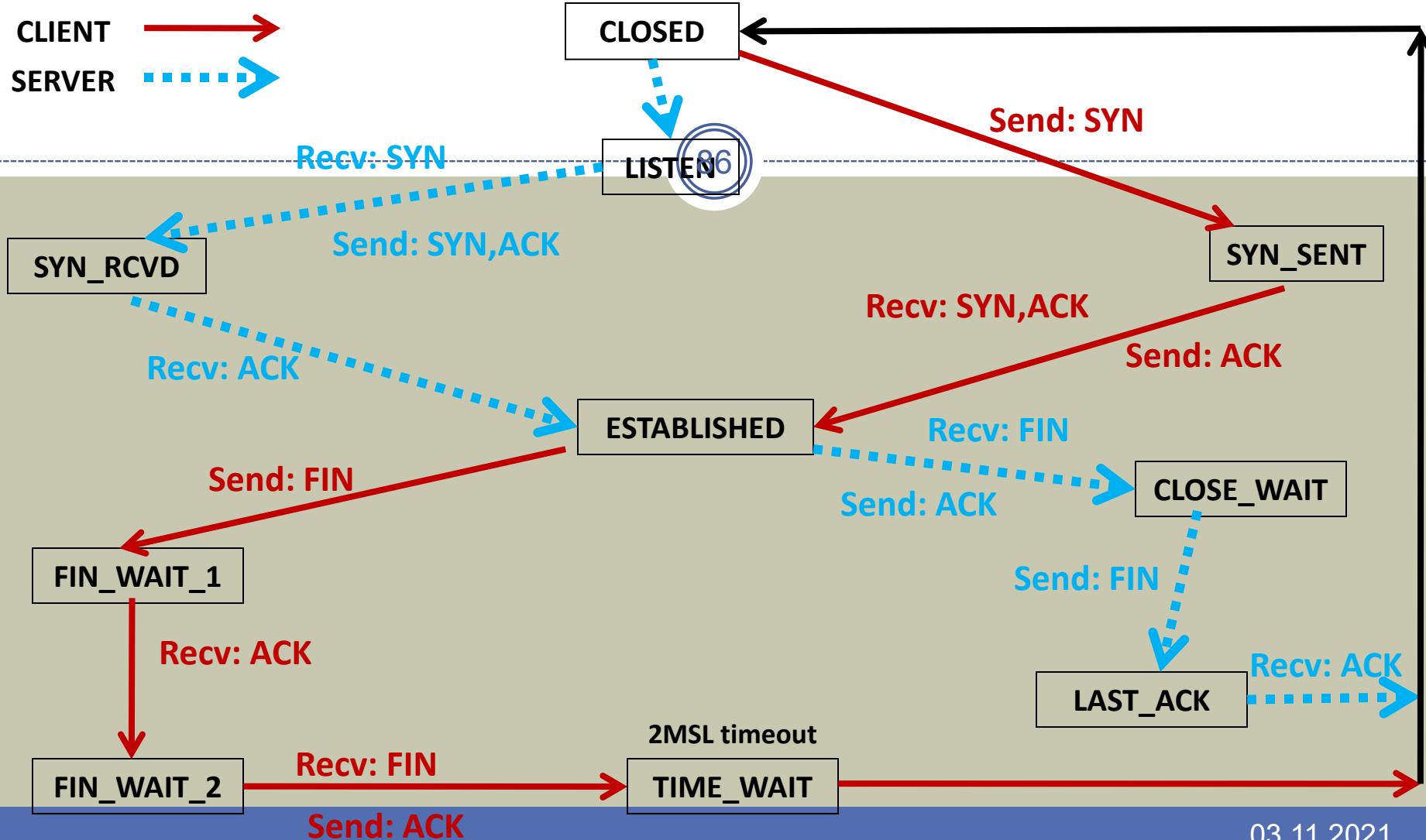
84

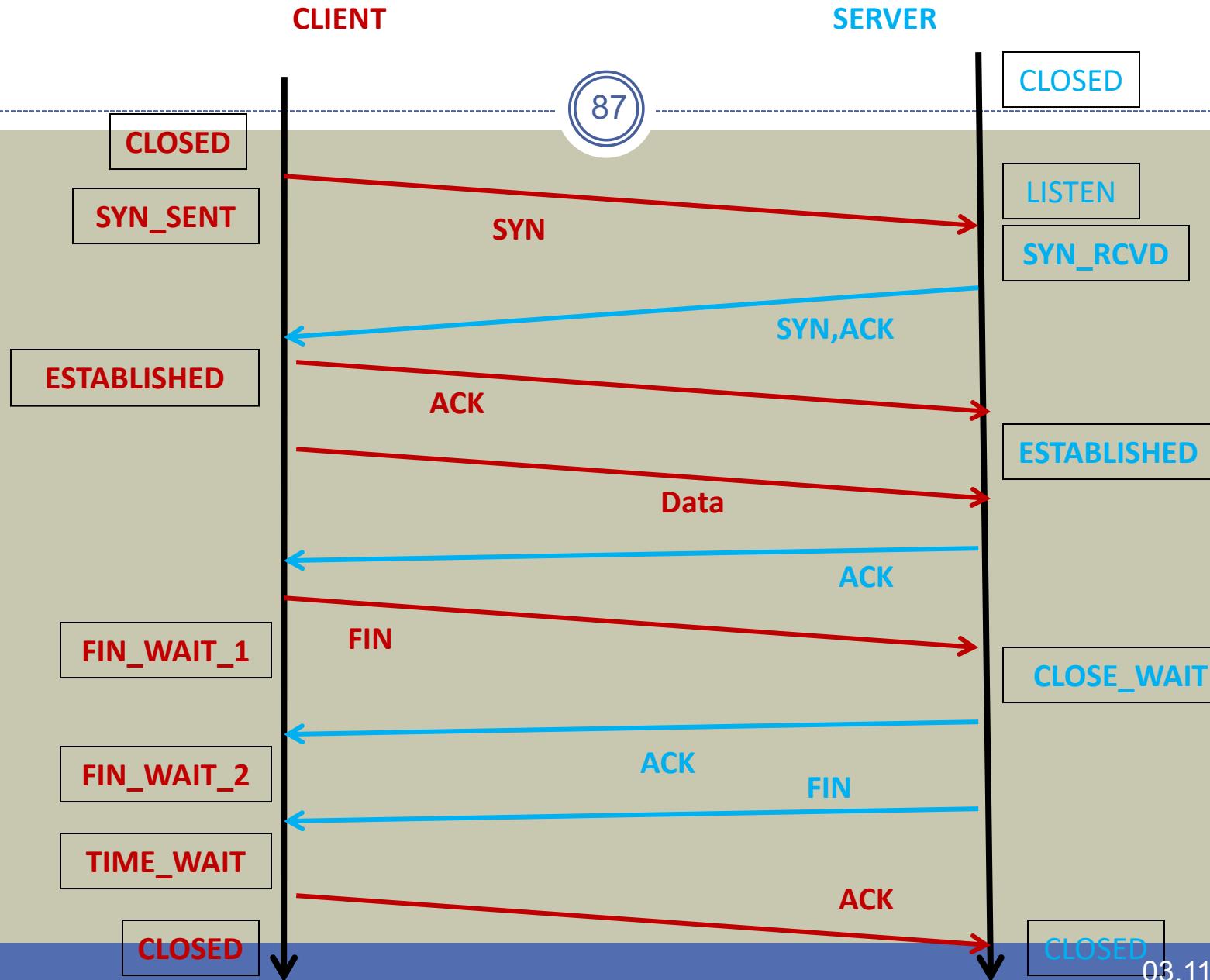


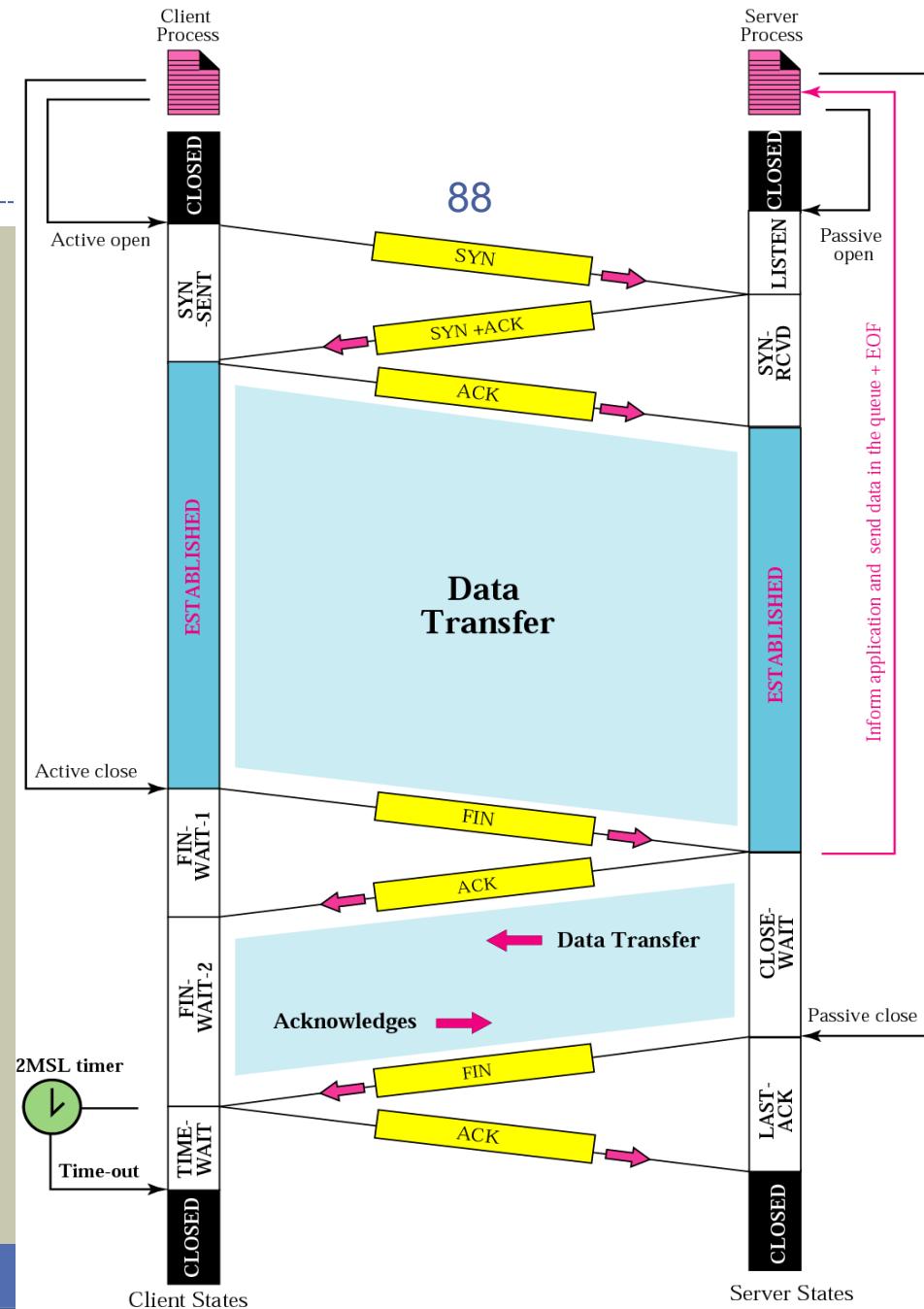
TCP state Transition Diagram

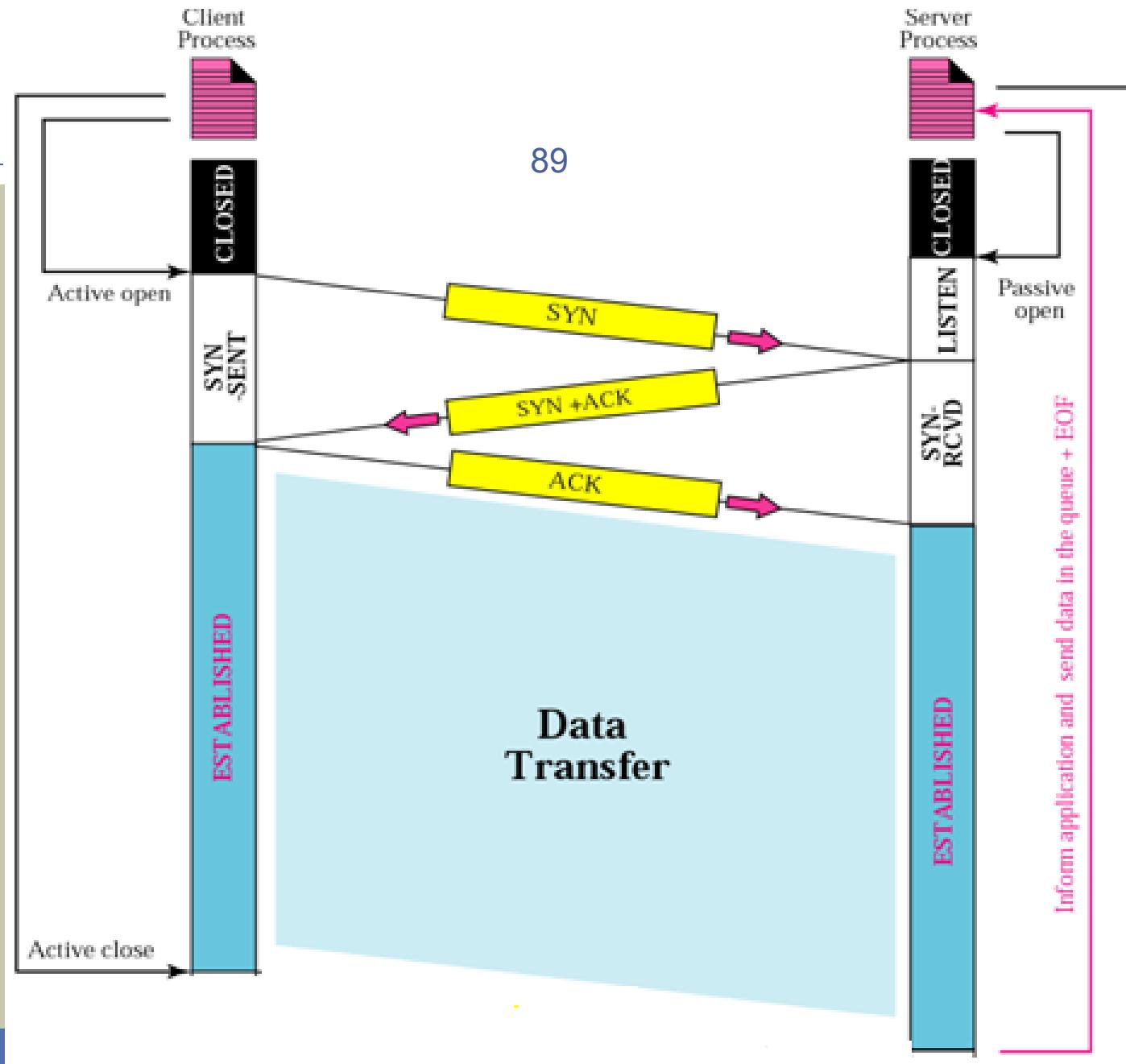


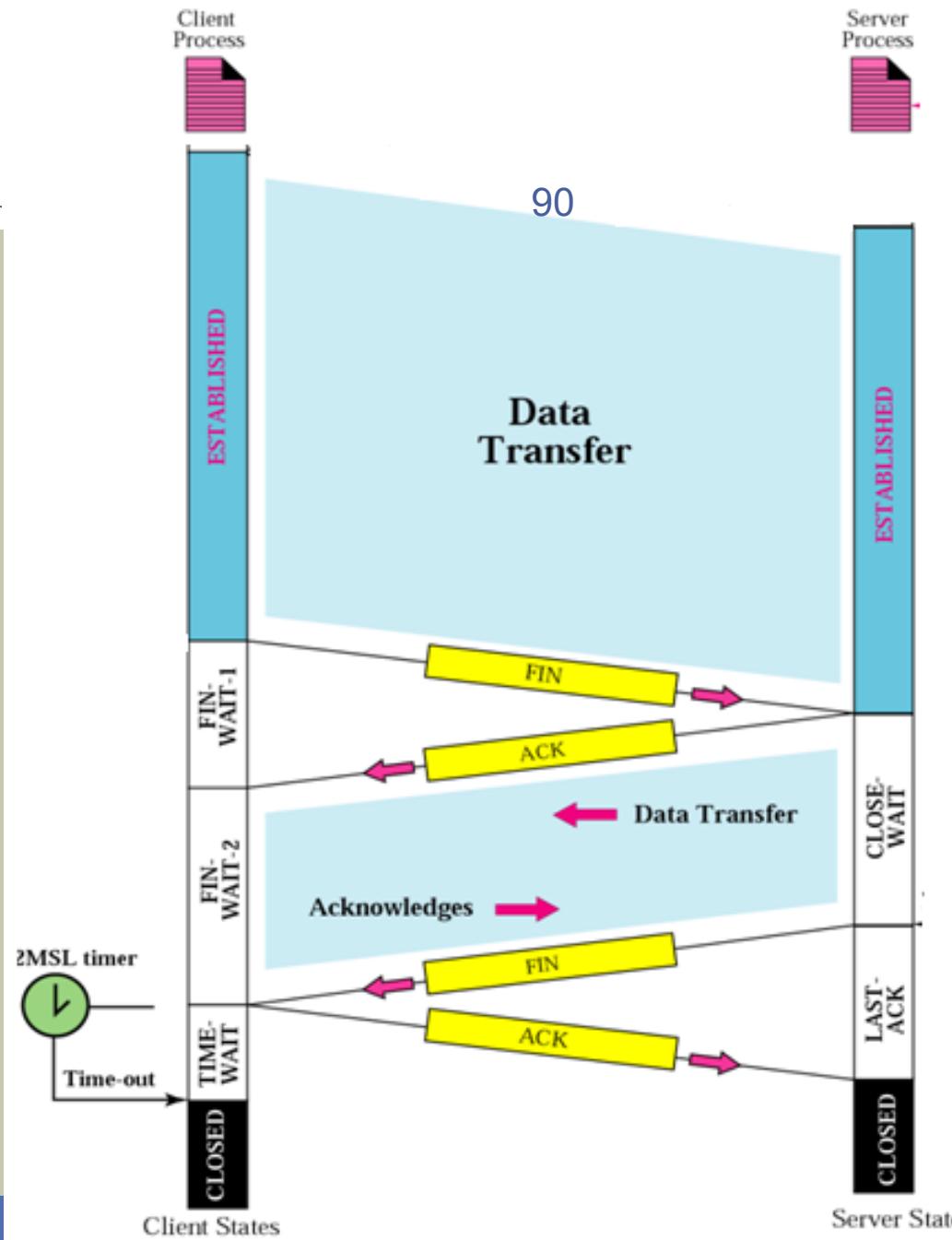
TCP state transition











<i>State</i>	<i>Description</i>
CLOSED	There is no connection
LISTEN	Passive open received; waiting for SYN
SYN-SENT	SYN sent; waiting for ACK
SYN-RCVD	SYN+ACK sent; waiting for ACK
ESTABLISHED	Connection established; data transfer in progress
FIN-WAIT-1	First FIN sent; waiting for ACK
FIN-WAIT-2	ACK to first FIN received; waiting for second FIN
CLOSE-WAIT	First FIN received, ACK sent; waiting for application to close
TIME-WAIT	Second FIN received, ACK sent; waiting for 2MSL time-out
LAST-ACK	Second FIN sent; waiting for ACK
CLOSING	Both sides have decided to close simultaneously

User Datagram Protocol (UDP)

92

The UDP operation is same as TCP with the following differences

- UDP does not have a connection establishment process
- UDP does not have a connection termination process
- UDP does not have error control, flow control and congestion control mechanisms
- UDP header has only 8 bytes

UDP cont.

93

- Since UDP does not get any feedback from the receiver, there is no guarantee of delivering data to the receiver by UDP
- Therefore UDP is an unreliable simple protocol
- Because of its simplicity it is used for specific applications especially the broadcast type applications

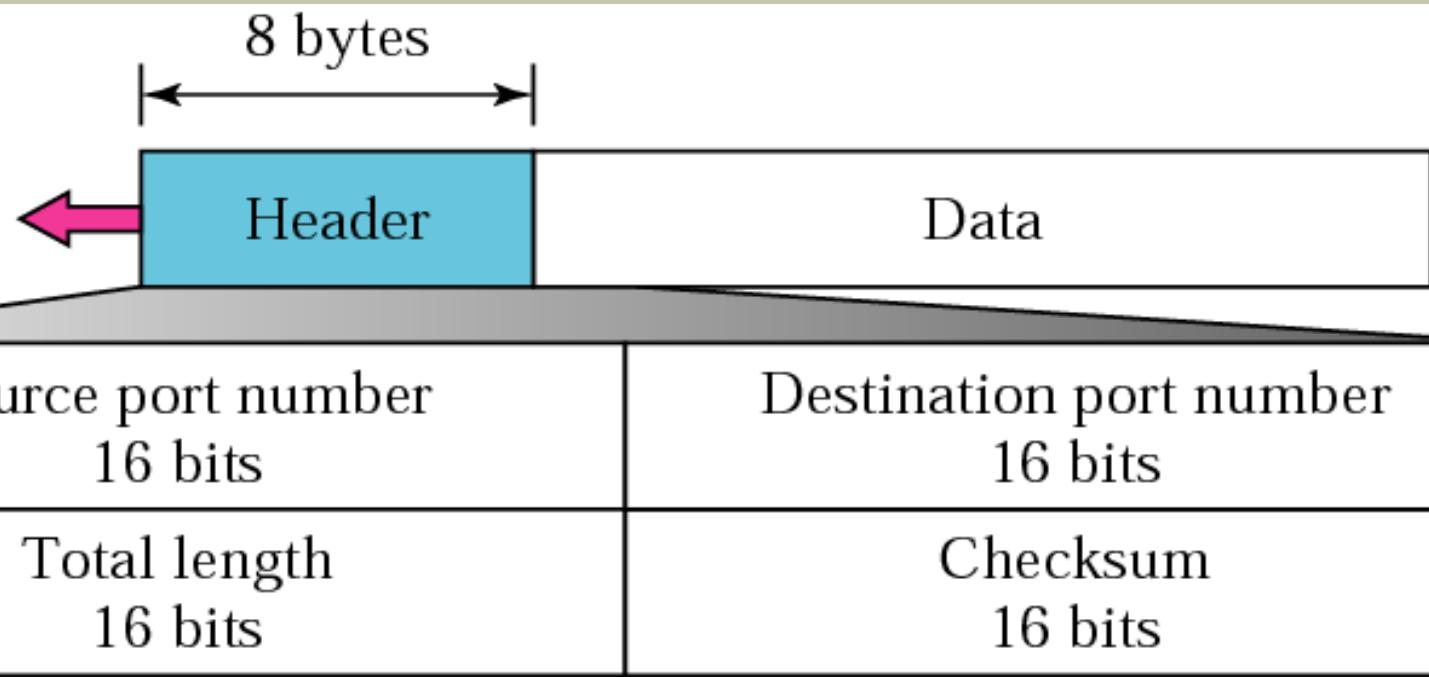
UDP Port numbers

94

Port Number	Application
69	TFTP
53	DNS
161	SNMP
520	RIP

UDP Header

95





SLIIT

Discover Your Future

IT2050 - Computer Networks

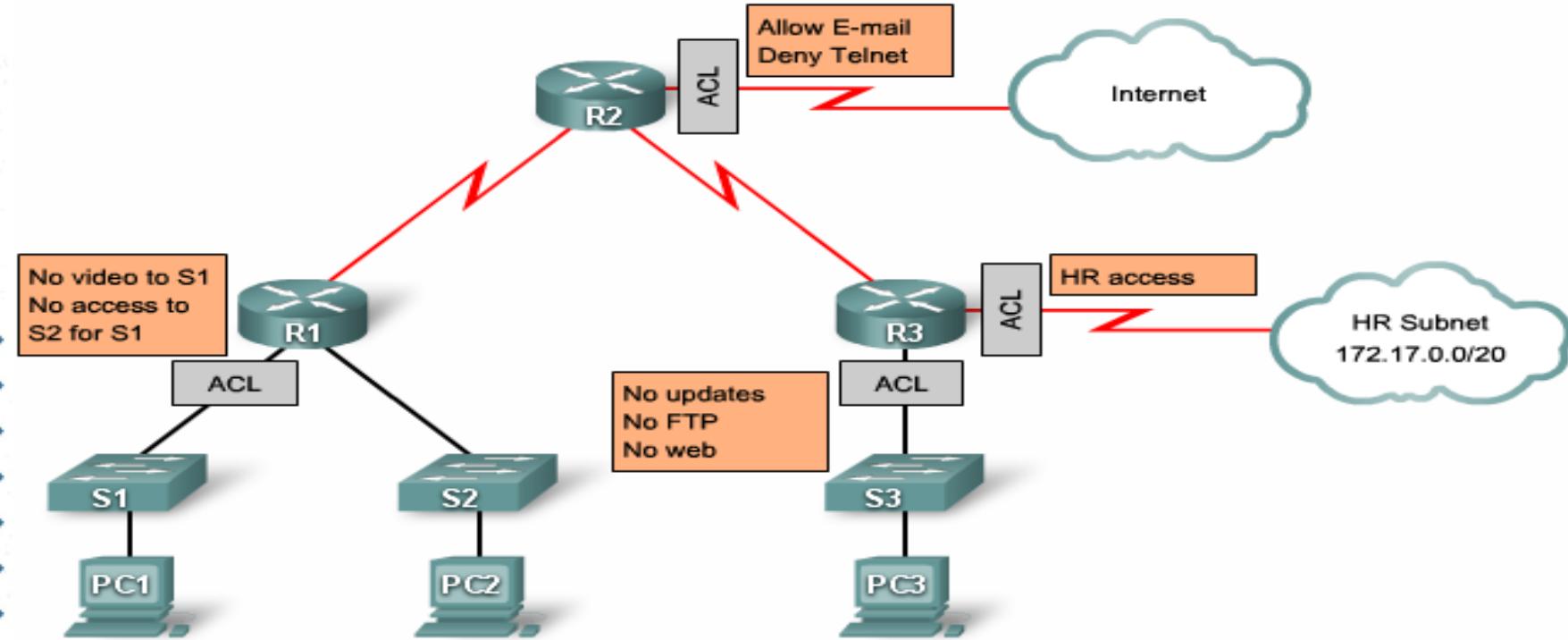
Lecture 8
Access Control Lists (ACL)

Ms. Hansika Mahaadikara

Introduction

- ACLs are lists of conditions used to test network traffic that tries to travel across a router interface
- ACLs tell the router what types of packets to accept or deny
- Acceptance and denial can be based on specified conditions
- Conditions are based on source address, destination address, protocols, and upper-layer port numbers.

Introduction cont.



What are the things an ACL can do ?

- Prevent unwanted traffic in the network
- Prevent hackers from penetrating the network
- Prevent employees from using systems in unauthorized manner
- Filter routing updates
- Match packets for prioritization
- match packets for VPN tunneling
- Match packets for implementing quality of service features

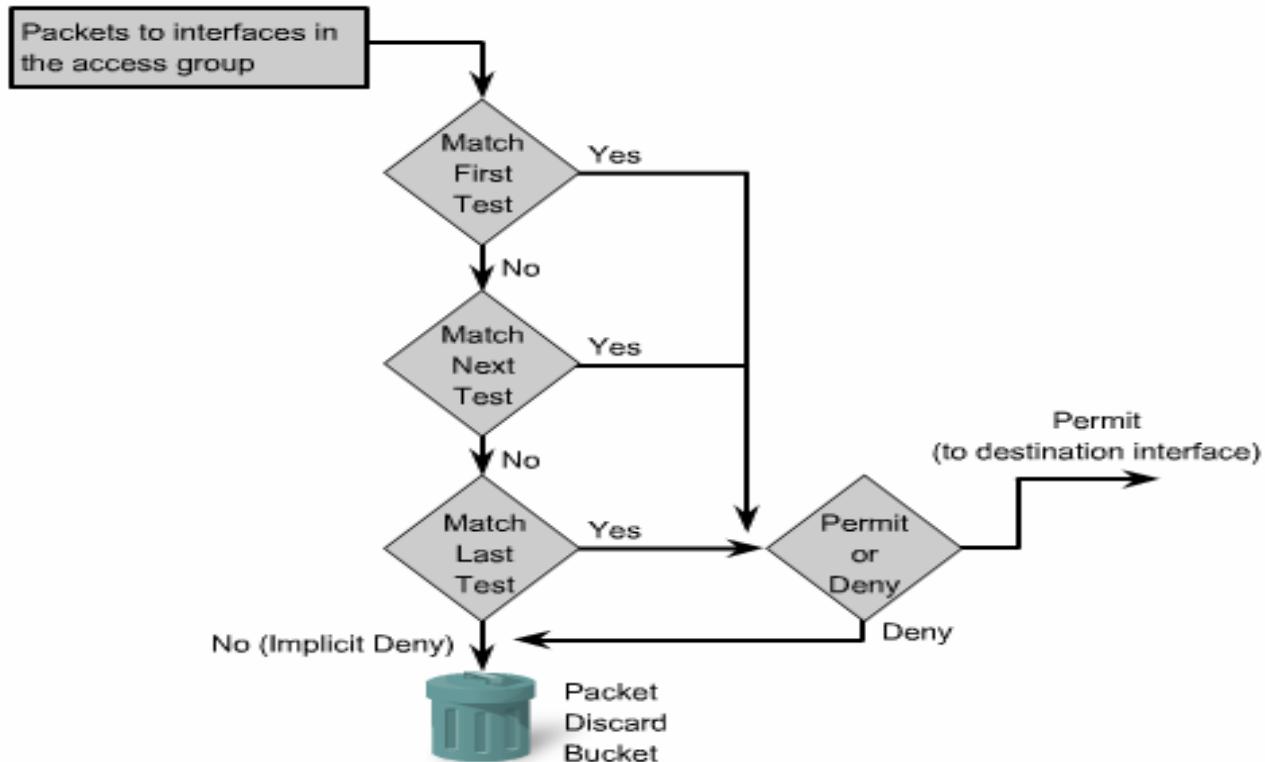
How ACL works ?

- In the ACL you can have several statements
- ACL statements operate in sequential, logical order
- If statement 1 is matched, router has to carry out the action defined in that statement
- If it isn't matched, router has to examine the next statement
- If it matches, router has to carry out the action it defines
-
-
-
-
-

How ACL works ? cont.

- Router has to continue looping through the list until a statement is matched or until the last statement in the list is not matched
- If none of the statements is matched, it will be passed to the final implied statement (DENY ANY)
 - It results in a deny and the packet is discarded.
 - Instead of proceeding in or out an interface, all these remaining packets are dropped.

How ACL works ? cont.



Wildcard Mask

- ACLs use wildcard masking
- Wildcard Masking for IP address bits uses the number 1 and the number 0 to identify how to treat the corresponding IP address bits.
 - A wildcard mask bit 0 means
 - “check the corresponding bit value”
 - A wildcard mask bit 1 means
 - “do not check (ignore) that corresponding bit value”

Wildcard Bits: How to Check the Corresponding Address Bits

128	64	32	16	8	4	2	1
0	0	0	0	0	0	0	0
0	0	1	1	1	1	1	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
0	0	0	0	1	1	1	1
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
1	1	1	1	1	1	0	0
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
1	1	1	1	1	1	1	1

Octet Bit Position and Address Value for Bit

Examples

Check All Address Bits
(Match All)

Ignore Last 6 Address Bits

Ignore Last 4 Address Bits

Check Last 2 Address Bits

Do Not Check Address
(Ignore Bits in Octet)

- 0 means check value of corresponding address bit.
- 1 means ignore value of corresponding address bit.

Wildcard Bits to Match a Specific IP Host Address

➤ **Check all the address bits (match all).**

- Verify an IP host address, for example:

172.30.16.29



Wildcard Mask: 0.0.0.0
(Checks All Bits)

- For example, 172.30.16.29 0.0.0.0 checks all the address bits.
- Abbreviate this wildcard mask using the IP address preceded by the keyword host (host 172.30.16.29).

Wildcard Bits to Match Any IP Address

➤ **Test conditions: Ignore all the address bits (match any).**

- An IP host address, for example:

198.10.0.1

Wildcard Mask: 255.255.255.255
(Ignore All)

- Accept any address: 198.10.0.1 255.255.255.255.
- Abbreviate the expression using the keyword **any**.

Wildcard Bits to Match IP Subnets

- Check for IP subnets 172.30.16.0/24 to 172.30.31.0/24.

Network .Host									
172.30.16.0									
0	0	0	1	0	0	1	0	0	0
0	0	0	0	1	1	1	0	1	0
0	0	0	1	0	0	0	0	=	16
0	0	0	1	0	0	0	1	=	17
0	0	0	1	0	0	1	0	=	18

Wildcard Mask:

Wildcard Mask cont.

Wildcard Mask	Binary Version of the Mask	Description
0.0.0.0	00000000.00000000.00000000.00000000	The entire IP address must match.
0.0.0.255	00000000.00000000.00000000.11111111	Just the first 24 bits must match.
0.0.255.255	00000000.00000000.11111111.11111111	Just the first 16 bits must match.
0.255.255.255	00000000.11111111.11111111.11111111	Just the first 8 bits must match.
255.255.255.255	11111111.11111111.11111111.11111111	Don't even bother to compare; it's automatically considered to match (0 bits need to match).

Wildcard Mask cont.

Wildcard Mask	Binary Version of the Mask	Description
0.0.15.255	00000000.00000000.00001111.11111111	Just the first 20 bits must match.
0.0.3.255	00000000.00000000.00000011.11111111	Just the first 22 bits must match.
32.48.0.255	00100000.00110000.00000000.11111111	All bits except the 3rd, 11th, 12th, and last 8 must match.
*		
*		
*		

ACL Configurations

- Create ACL
- Apply ACL to an interface

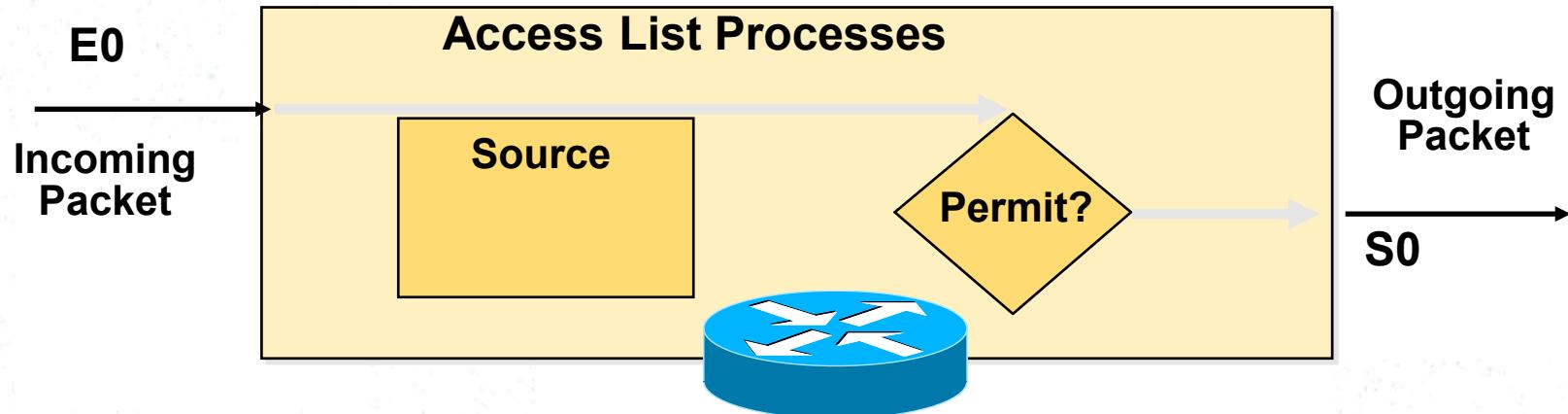
Create ACL cont.

- There are two types of ACLs
 - Standard ACLs
 - Extended ACLs

* *
* *
* *
* *
* *
* *
* *
* *

Standard ACLs

- ACL number is in between 1-99
- Checks source address
- Generally permits or denies entire protocol suite



Standard ACLs cont.

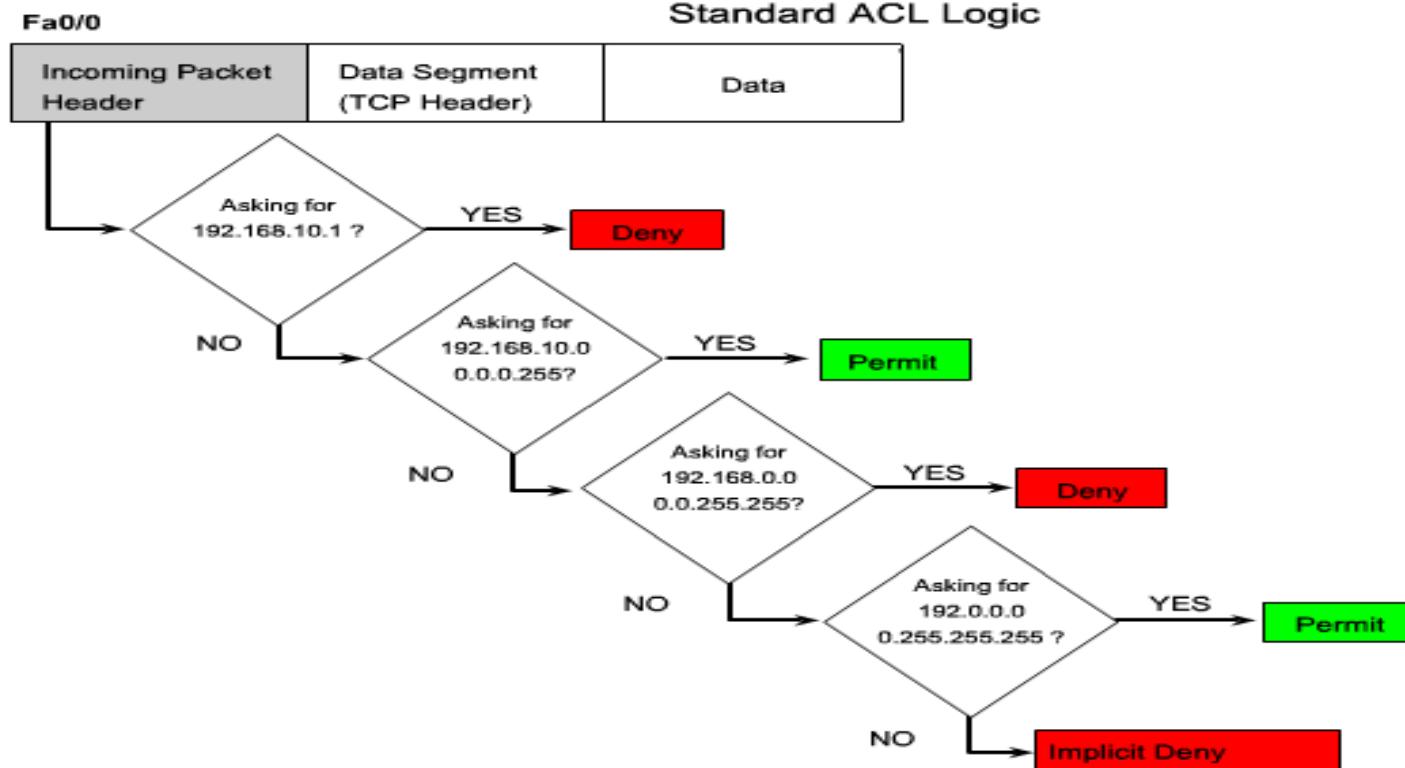
```
Router(config)# access-list access-list-number
              {permit | deny} {Source address}
              {wildcard mask}
```

- R1(config)# access-list 10 permit 192.168.10.0 0.0.0.255

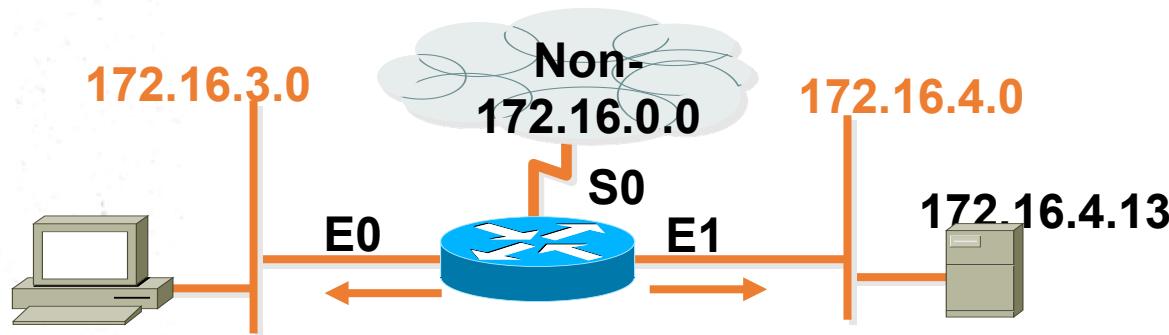
Standard ACLs cont.

- access-list 2 deny host 192.168.10.1
- access-list 2 permit 192.168.10.0 0.0.0.255
- access-list 2 deny 192.168.0.0 0.0.255.255
- access-list 2 permit 192.0.0.0 0.255.255.255

Standard ACLs cont.



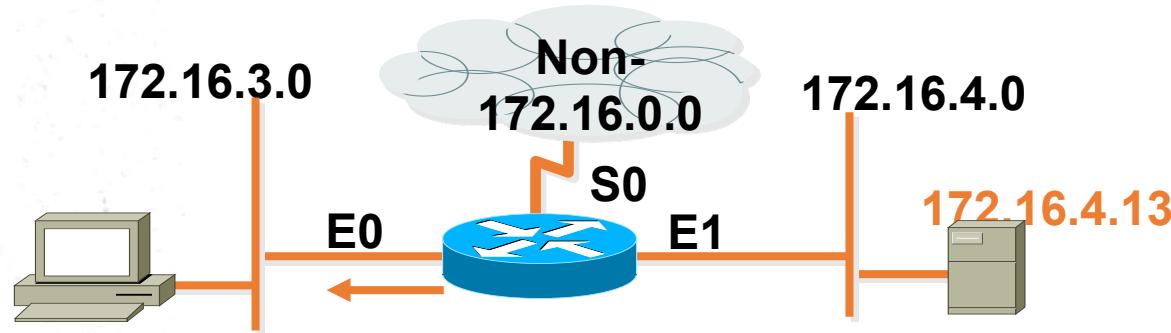
Standard ACL cont.



```
access-list 1 permit 172.16.0.0  0.0.255.255  
(implicit deny all - not visible in the list)  
(access-list 1 deny 0.0.0.0    255.255.255.255)
```

❖ Permit my network only.

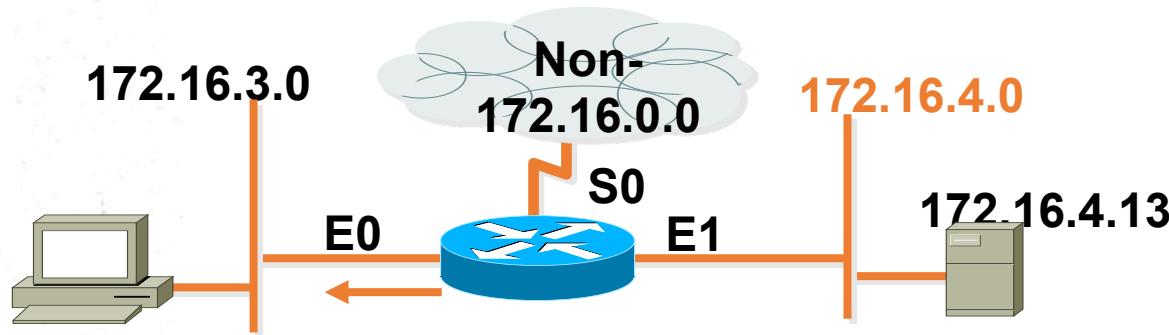
Standard ACL cont.



```
access-list 1 deny 172.16.4.13 0.0.0.0
access-list 1 permit 0.0.0.0  255.255.255.255
(implicit deny all)
(access-list 1 deny 0.0.0.0      255.255.255.255)
```

❖ Deny a specific host.

Standard ACL cont.

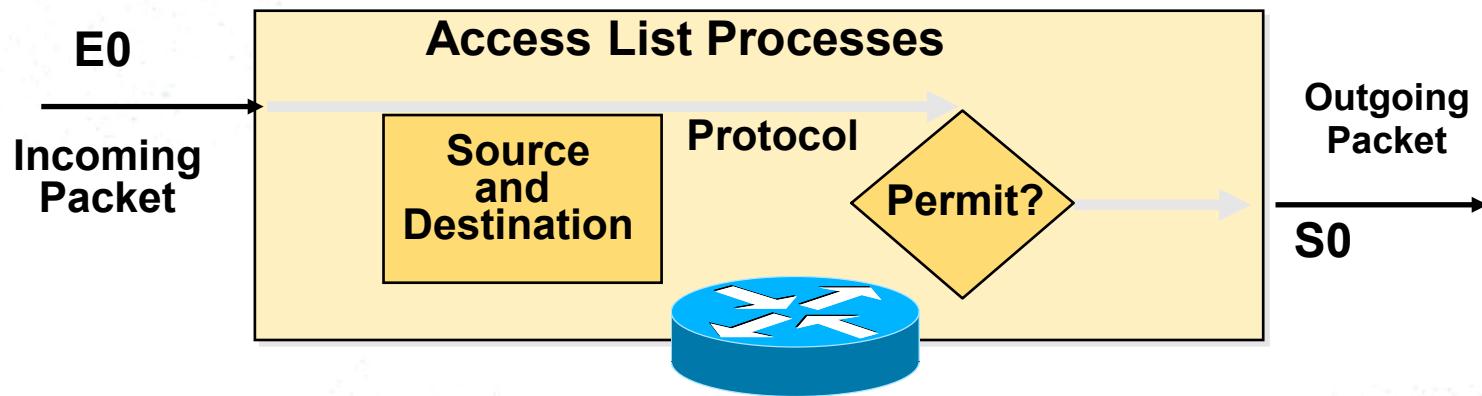


```
* * access-list 1 deny 172.16.4.0  0.0.0.255
* * access-list 1 permit any
* * (implicit deny all)
* * (access-list 1 deny 0.0.0.0  255.255.255.255)
```

❖ Deny a specific subnet.

Extended ACLs

- ACL number is in between 100-199
- Checks source and destination address
- Generally permits or denies specific protocols



Extended ACLs cont.

```
Router(config)# access-list access-list-number
    {permit | deny} {protocol}
    {Source address} {wildcard mask}
    {destination address} {wildcard mask}
    {eq | lt | gt} {port number}
```

* *
* *
* *
* *

Extended ACLs cont.

Using port numbers

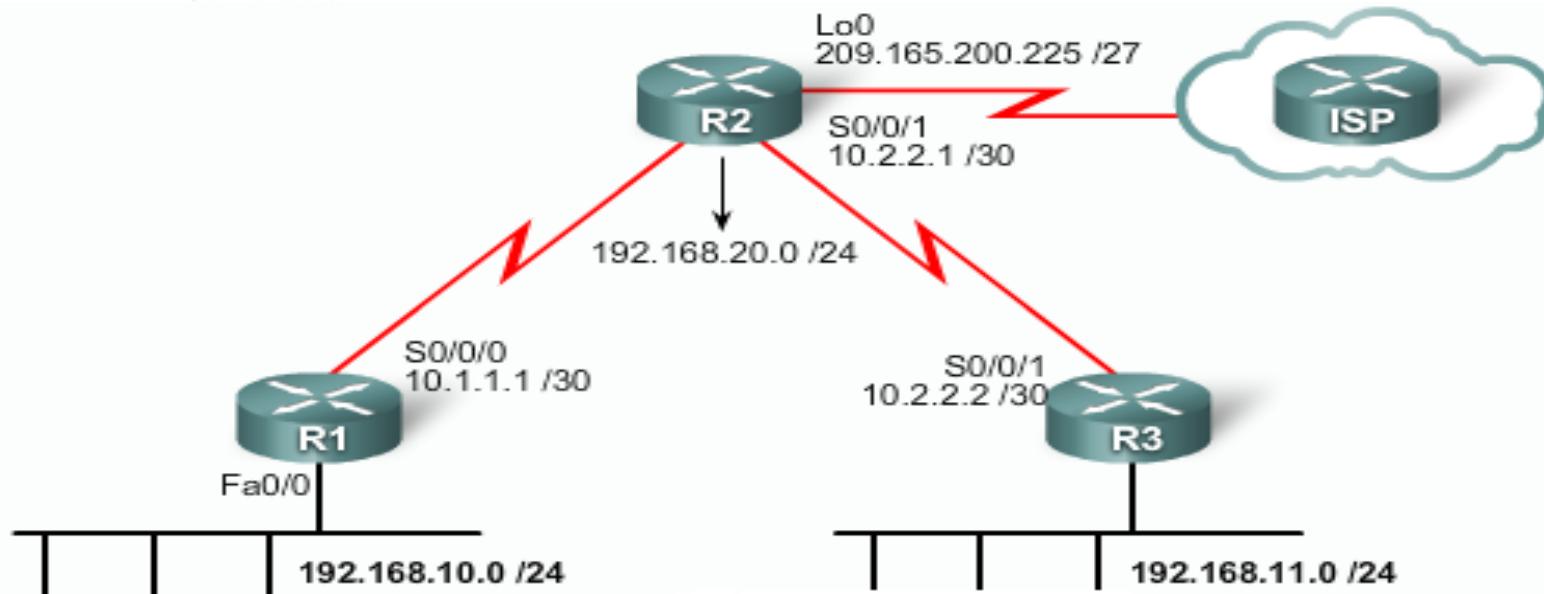
```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23  
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21  
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 22
```

Using keywords

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet  
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp  
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```

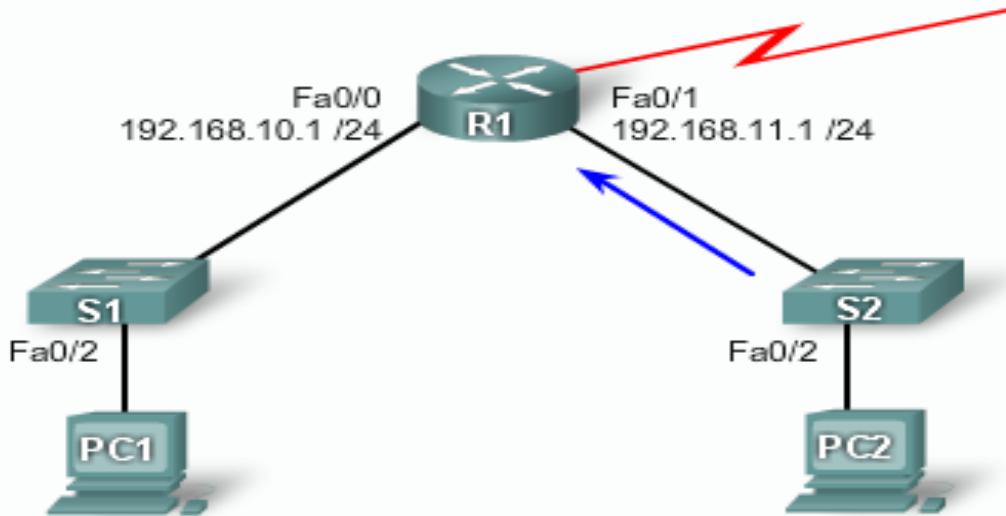
Extended ACLs cont.

- Network administrator needs to restrict Internet access of 192.168.10.0 to allow only website browsing



Extended ACLs cont.

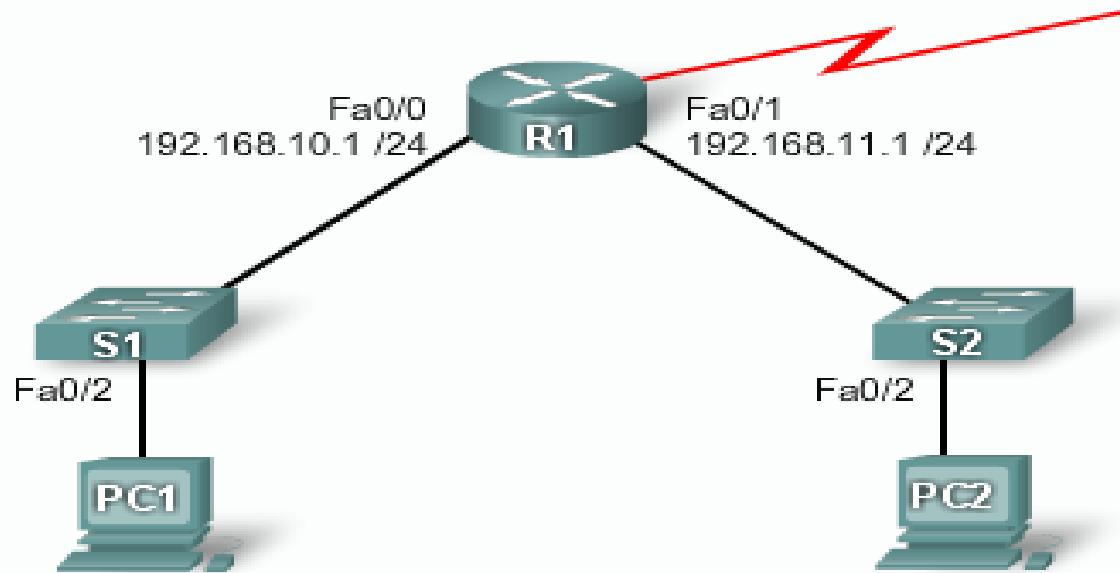
Extended ACL to Deny FTP from Subnets



```
R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0  
0.0.0.255 eq 21  
R1(config)# access-list 101 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0  
0.0.0.255 eq 20  
R1(config)# access-list 101 permit ip any any
```

Extended ACLs cont.

Extended ACL to Deny Only Telnet from Subnet



```
R1(config)#access-list 101 deny tcp 192.168.11.0 0.0.0.255 any eq 23  
R1(config)#access-list 101 permit ip any any
```

Access List Configuration Guidelines

- Access list numbers indicate which protocol is filtered.
- One access list per interface, per protocol, per direction is allowed.
- The order of access list statements controls testing.
- The most restrictive statements should be at the top of list.
-
-
-
-
-
-

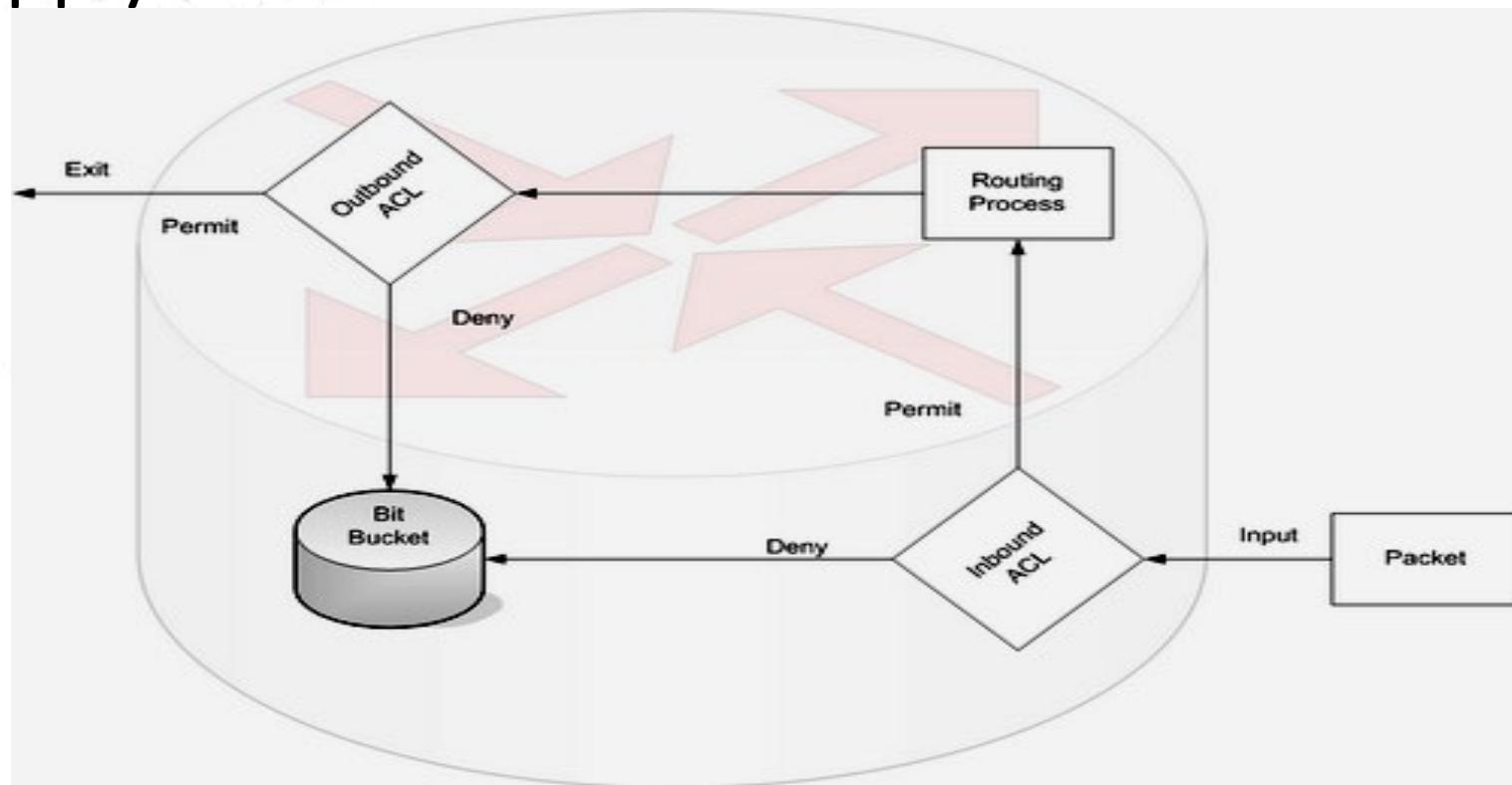
Access List Configuration Guidelines Contd....

- There is an implicit deny any as the last access list test— every list should have at least one permit statement.
- Access lists should be created before to interfaces being applied.
- Access lists filter traffic going through the router; they do not apply to traffic originated from the router.

Apply ACL to an interface

- ACLs are configured either to apply to inbound traffic or to apply to outbound traffic
- Inbound ACLs-Incoming packets are checked with the ACLs before taking the routing decisions
- An inbound ACL is efficient because it saves the overhead of routing lookups if the packet is discarded
- If the packet is permitted by the tests, it is then processed for routing
- Outbound ACLs-Incoming packets are first process for the routing decisions and then checked with the outbound ACL

Apply ACL to an interface cont.



Apply ACL to an interface cont.

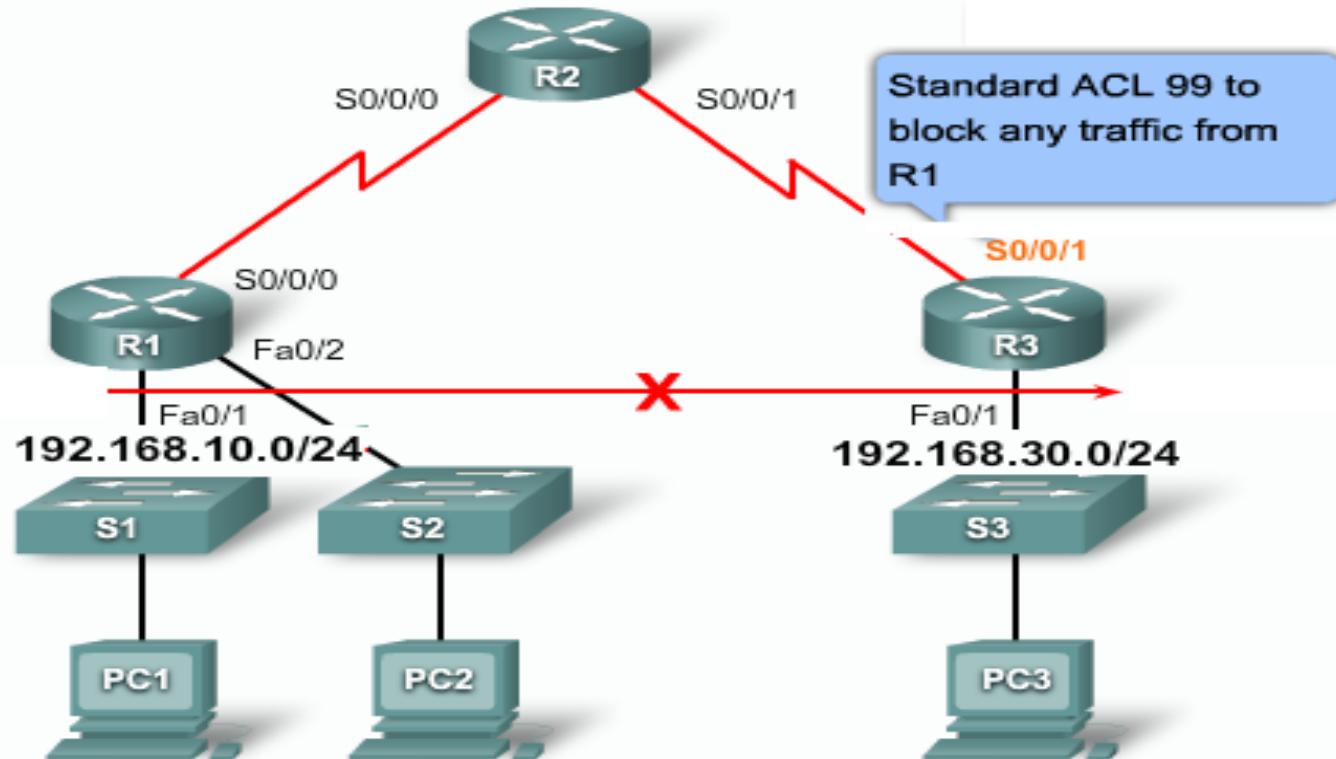
```
Router(config-if)# {protocol} access-group  
access-list-number {in | out}
```

```
R1(config)# interface S0/0/0  
R1(config-if)# ip access-group 103 out  
R1(config-if)# ip access-group 104 in
```

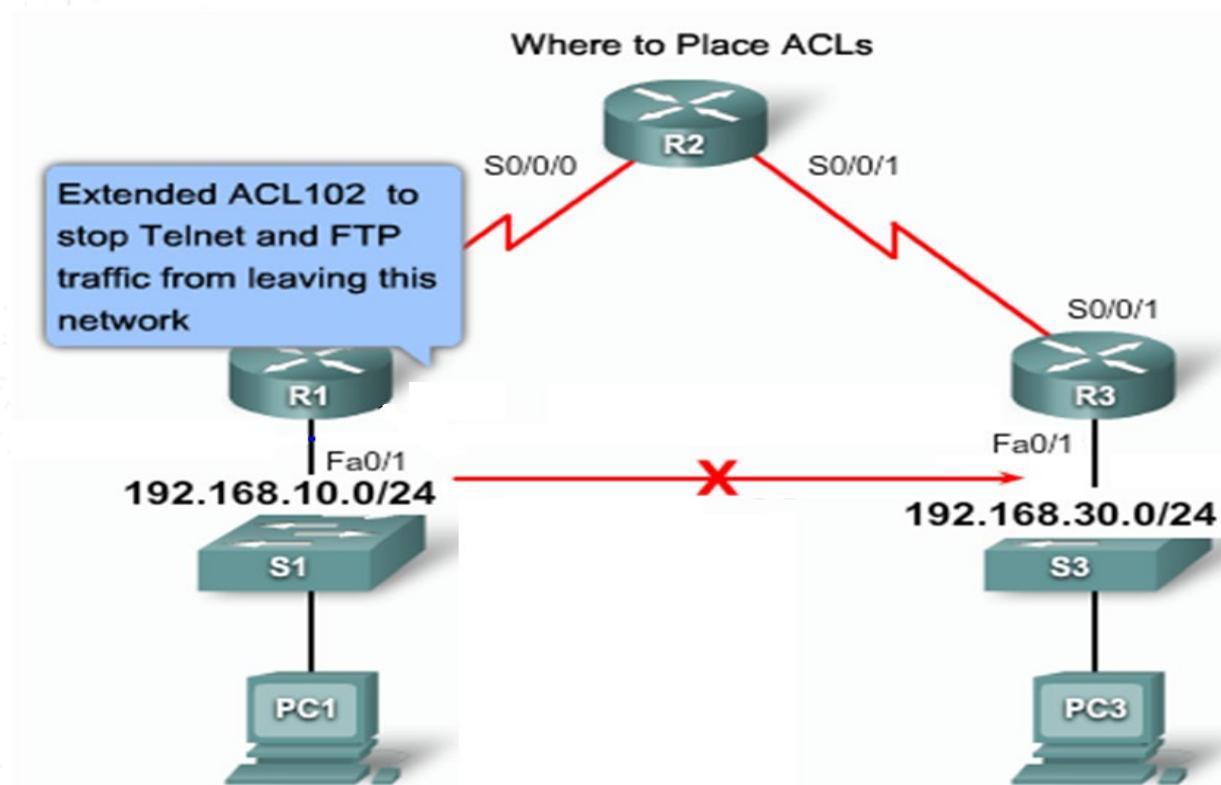
Placing ACLs

- Proper ACL placement will filter traffic and make the network more efficient
- The ACL should be placed where it has the greatest impact on efficiency.
- The general rule is to put the Extended ACLs as close as possible to the source of the traffic denied
- Standard ACLs should be placed as close to the destination as possible

Placing ACLs cont.



Placing ACLs cont.



Named ACLs

- Naming an ACL makes it easier to understand its function
- For example, an ACL to deny FTP could be called NO_FTP
- ACL names are alphanumeric
- and must be unique
- and must not begin with a number

Creating Named ACLs

```
Router(config)# ip access-list  
{standard | extended} {name}
```

```
Router(config-std-nacl)# {permit | deny}  
{source address} {wild card mask}
```

Creating Named ACLs cont.

```
R1(config)#ip access-list standard NO_ACCESS
R1(config-std-nacl)#deny host 192.168.11.10
R1(config-std-nacl)#permit 192.168.11.0 0.0.0.255
R1(config-std-nacl)#interface Fa0/0
R1(config-if)#ip access-group NO_ACCESS out
.
.
.
.
```

Advantages of Named ACLs

- it is easier to understand the function of ACL because you have used the function of ACL as its name
- It is easier to edit because Named ACLs allow you to delete individual entries in a specific ACL
- Can use sequence numbers to insert statements anywhere in the named ACL

Other types of ACLs

- Dynamic ACLs
- Time based ACLs
- Reflexive ACLs
- Turbo ACLs
- •
- •
- •
- •

IE2050 – Computer Networks

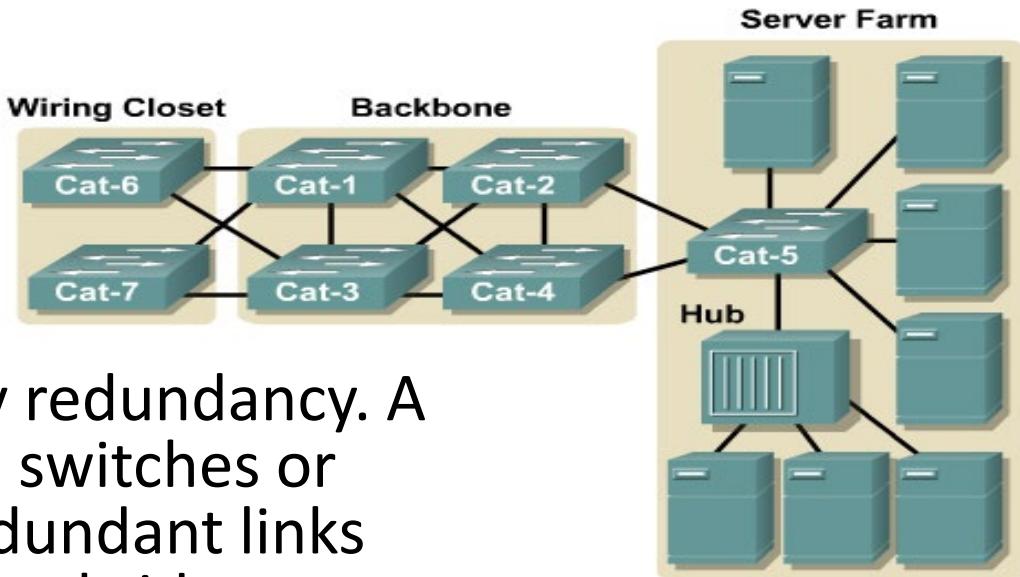
Lecture 10 Spanning Tree Protocol

Ms.Hansika Mahaadikara

Redundant Topologies

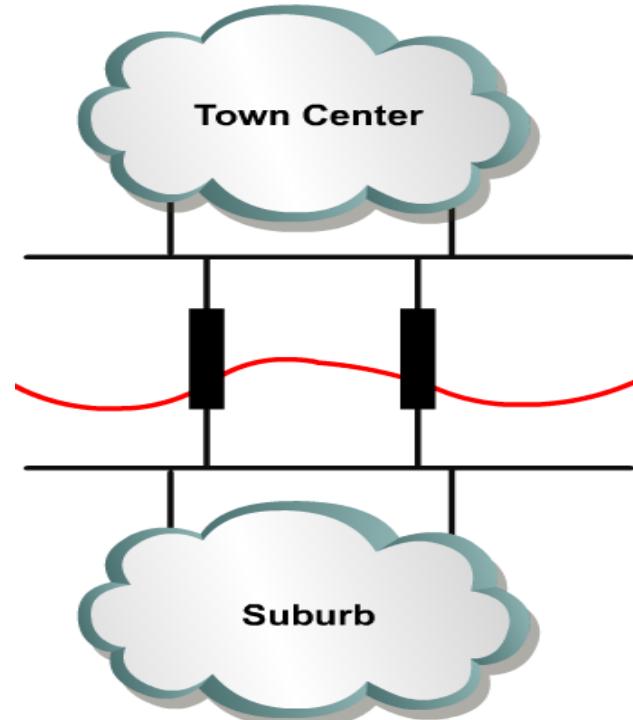
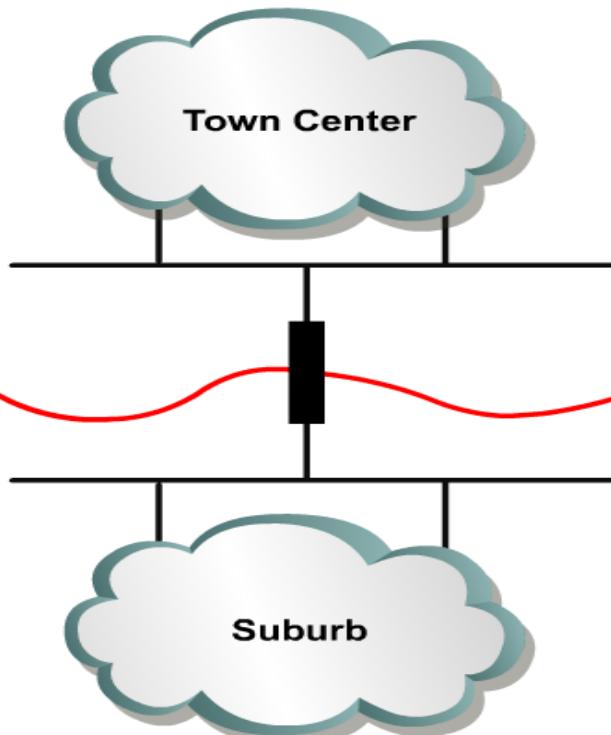
- Many companies and organizations increasingly rely on computer networks for their operations.
- Access to file servers, databases, the Internet, intranets and extranets is critical for successful businesses.
- If the network is down, productivity and customer satisfaction decline.

- This is interpreted to mean one hour of downtime on average, for every 4000 days, or approximately 5.25 minutes of downtime per year.
- To achieve such a goal ,extremely reliable networks are required.

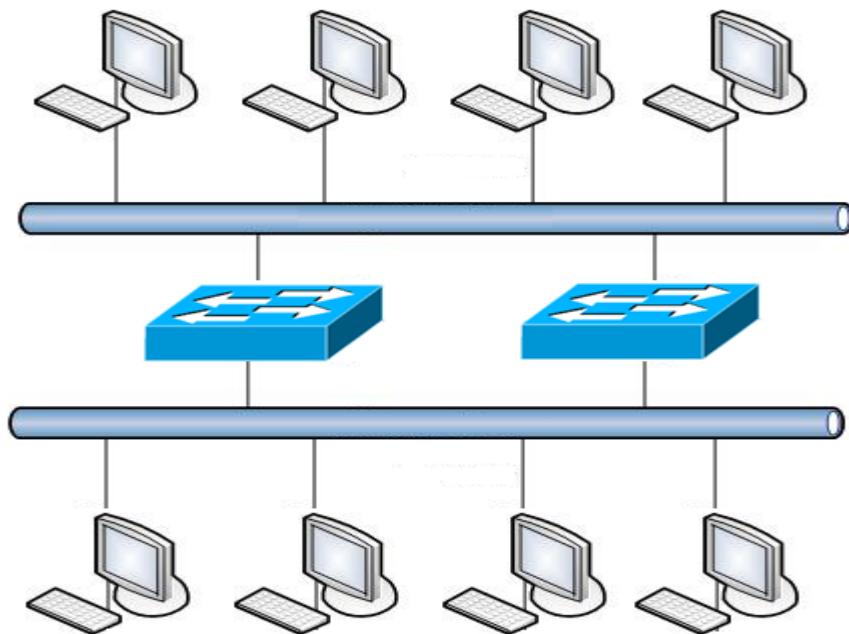
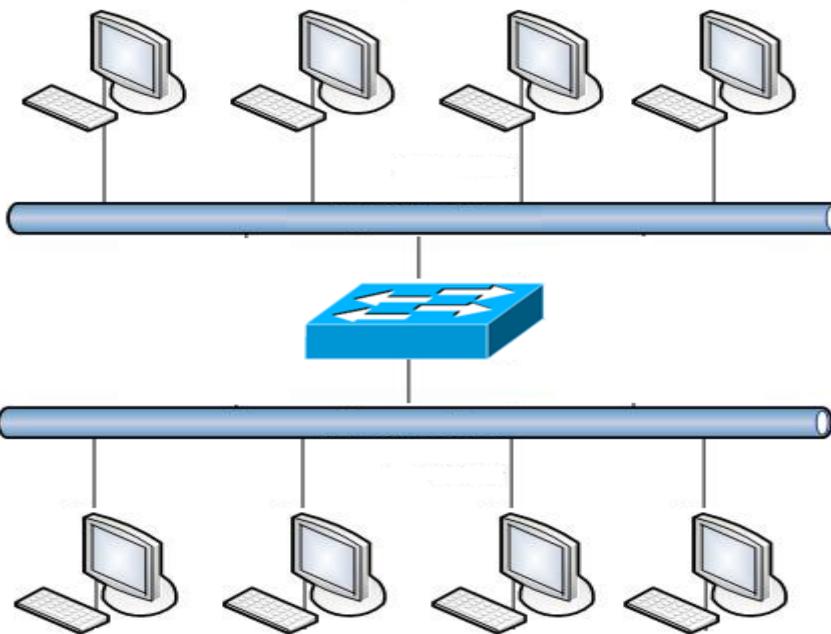


- Reliability is increased by redundancy. A network that is based on switches or bridges will introduce redundant links between those switches or bridges to overcome the failure of a single link.
- •
- •
- •
- •

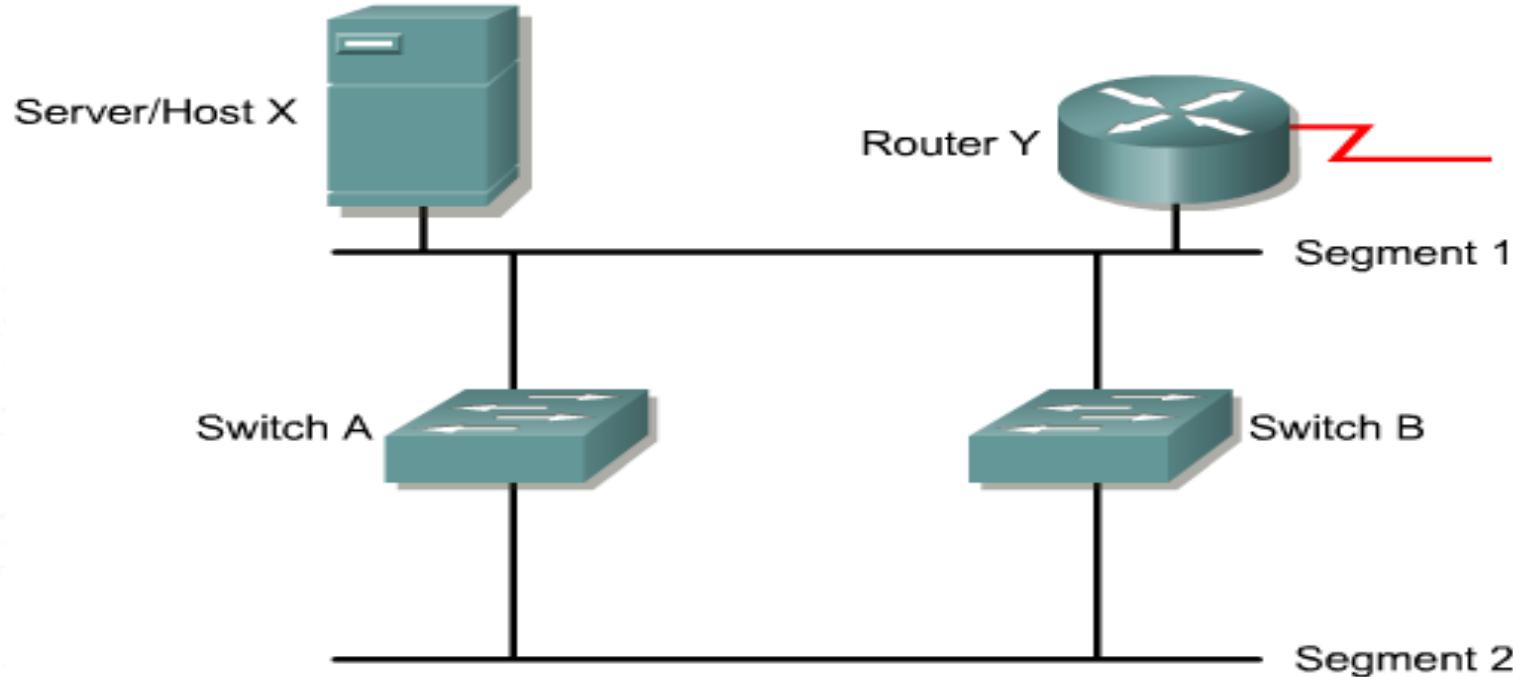
Redundancy



Redundancy



Redundancy Creates Loops

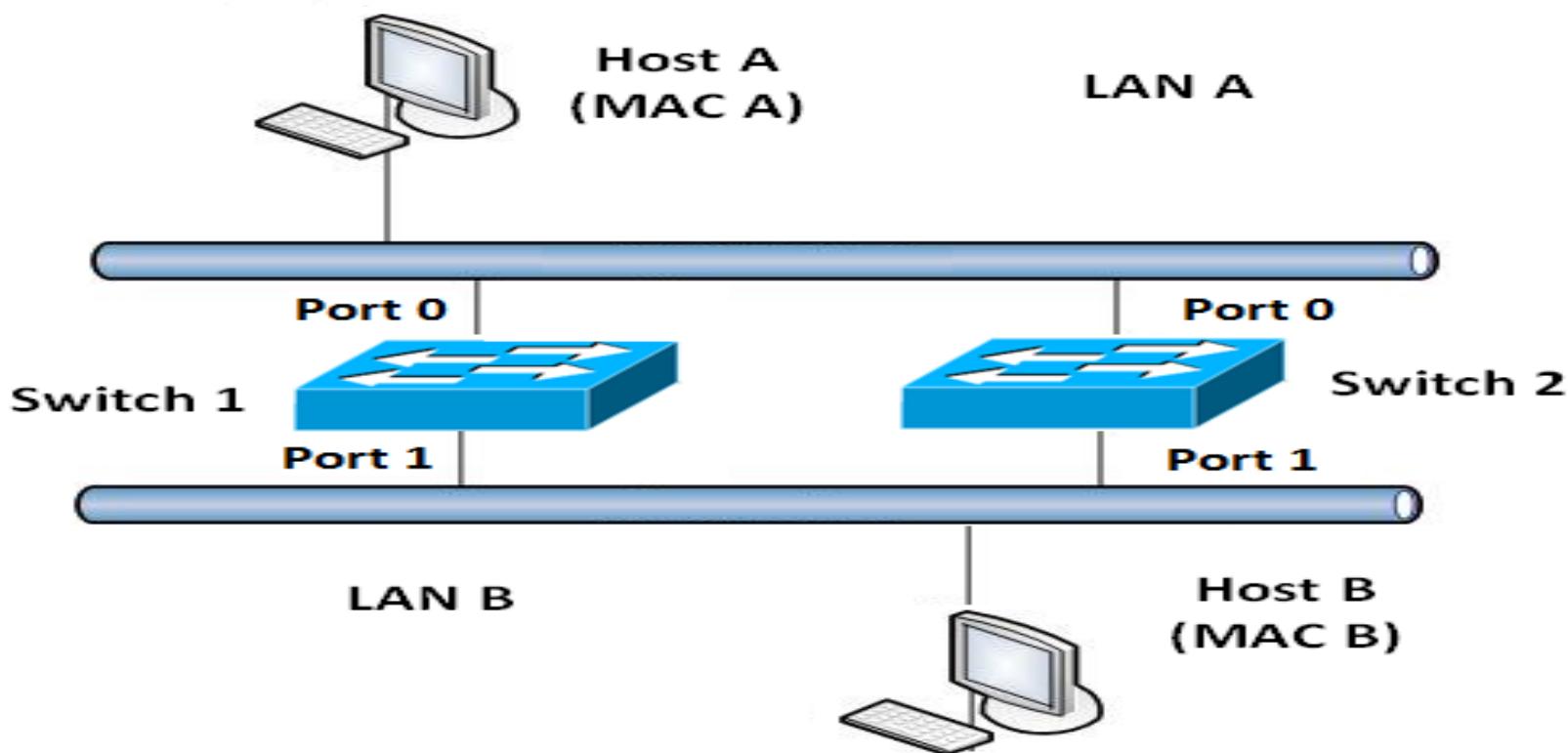


- Loops may occur in a network as part of a design strategy for redundancy.
 - STP is not needed if there are no loops the network.
- ⋮
- However, DO NOT disable STP!
 - Loops can occur accidentally from network staff or even users!
- ⋮

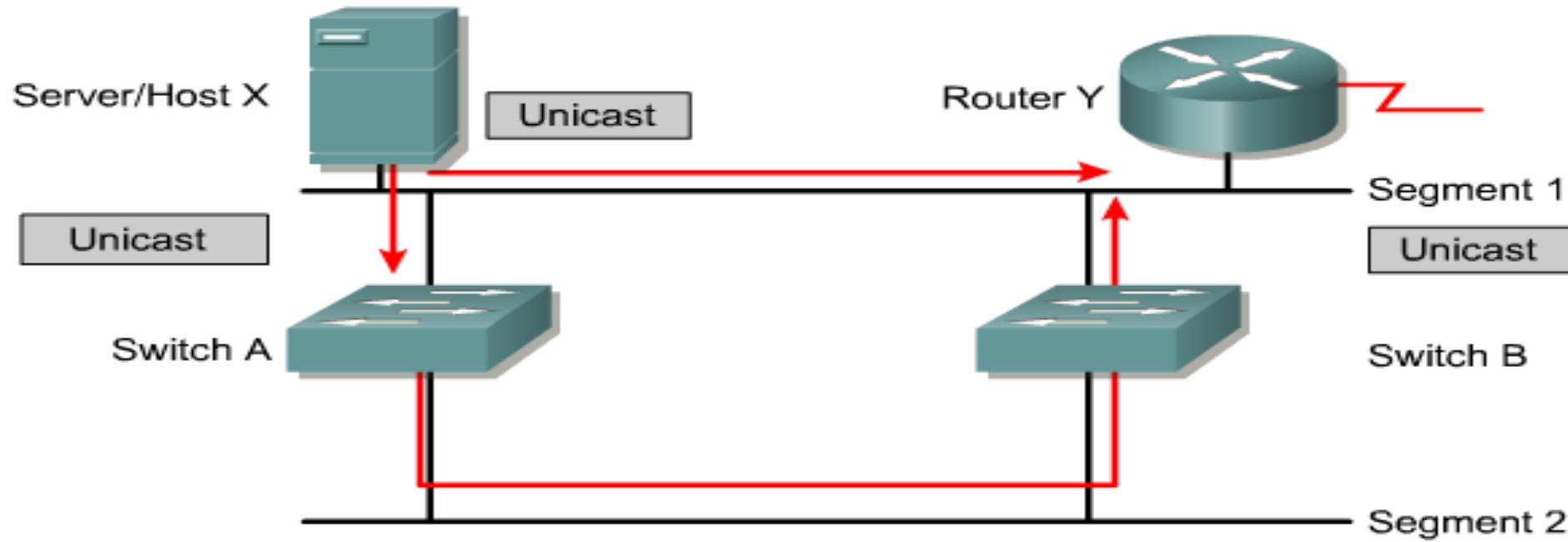
L2 Loops

- Broadcasts and Layer 2 loops can be a dangerous combination.
- Ethernet frames have no TTL field
- After an Ethernet frame starts to loop, it will probably continue until someone shuts off one of the switches or breaks a link.

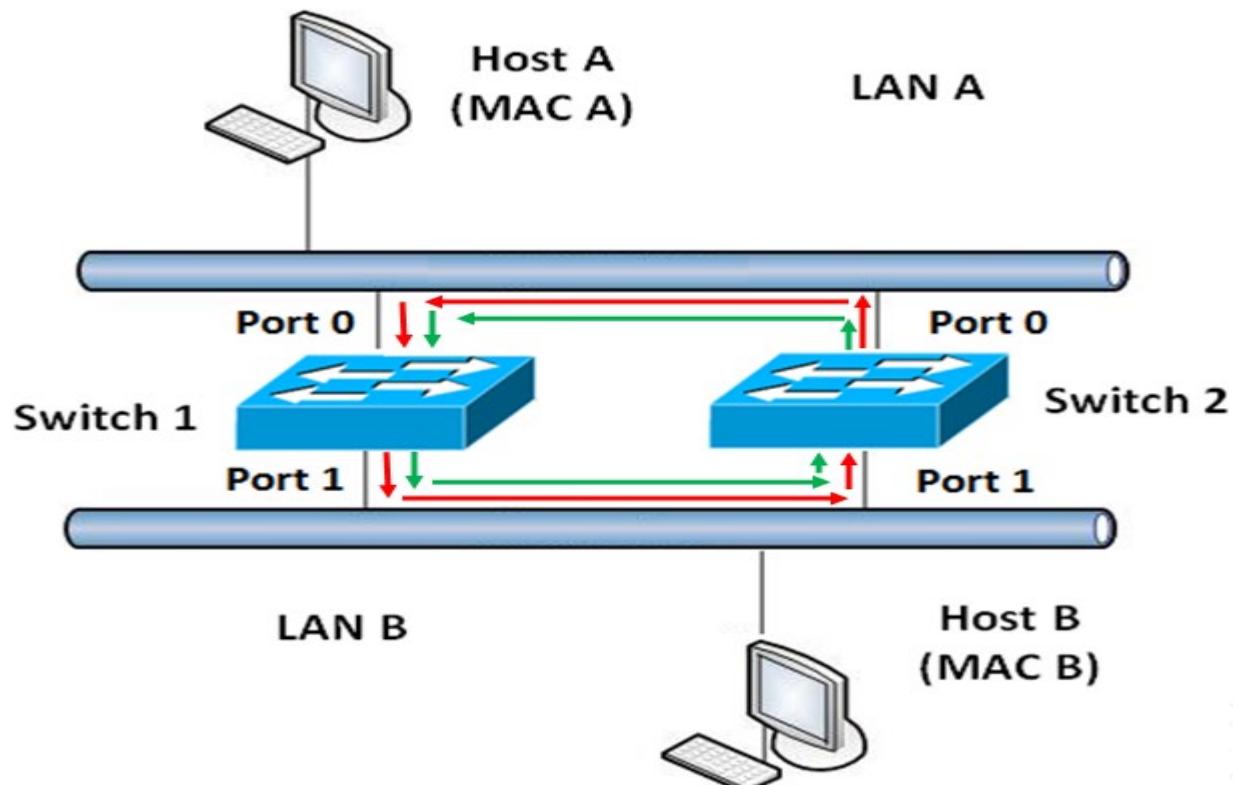
Looping Problems



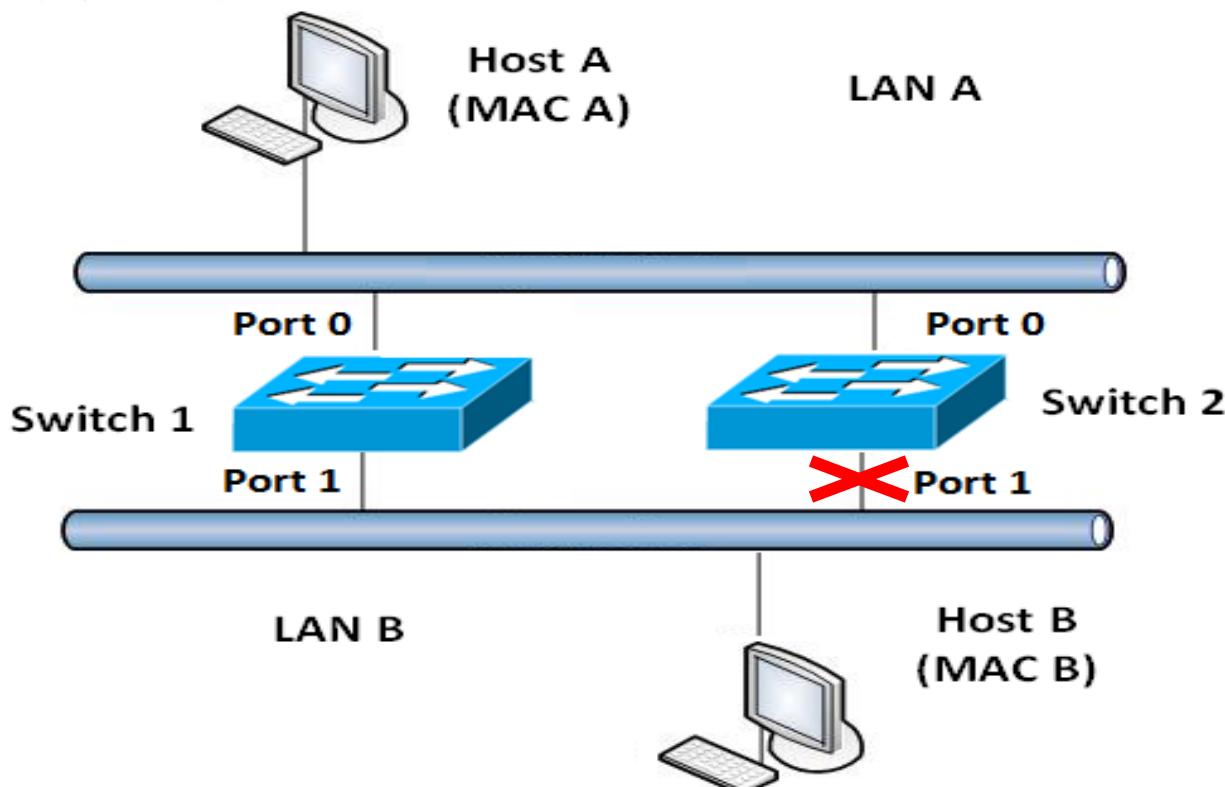
Multiple frame transmissions



Looping Problems cont.



Avoid Looping Problems



Avoid Looping Problems cont.

- To avoid loops, all switches use Spanning Tree Protocol (STP)

Spanning-Tree Protocol

- Ethernet bridges and switches can implement the IEEE 802.1d Spanning-Tree Protocol and use the spanning-tree algorithm to construct a loop free shortest path network.
- Shortest path is based on cumulative link costs. Link costs are based on the speed of the link.

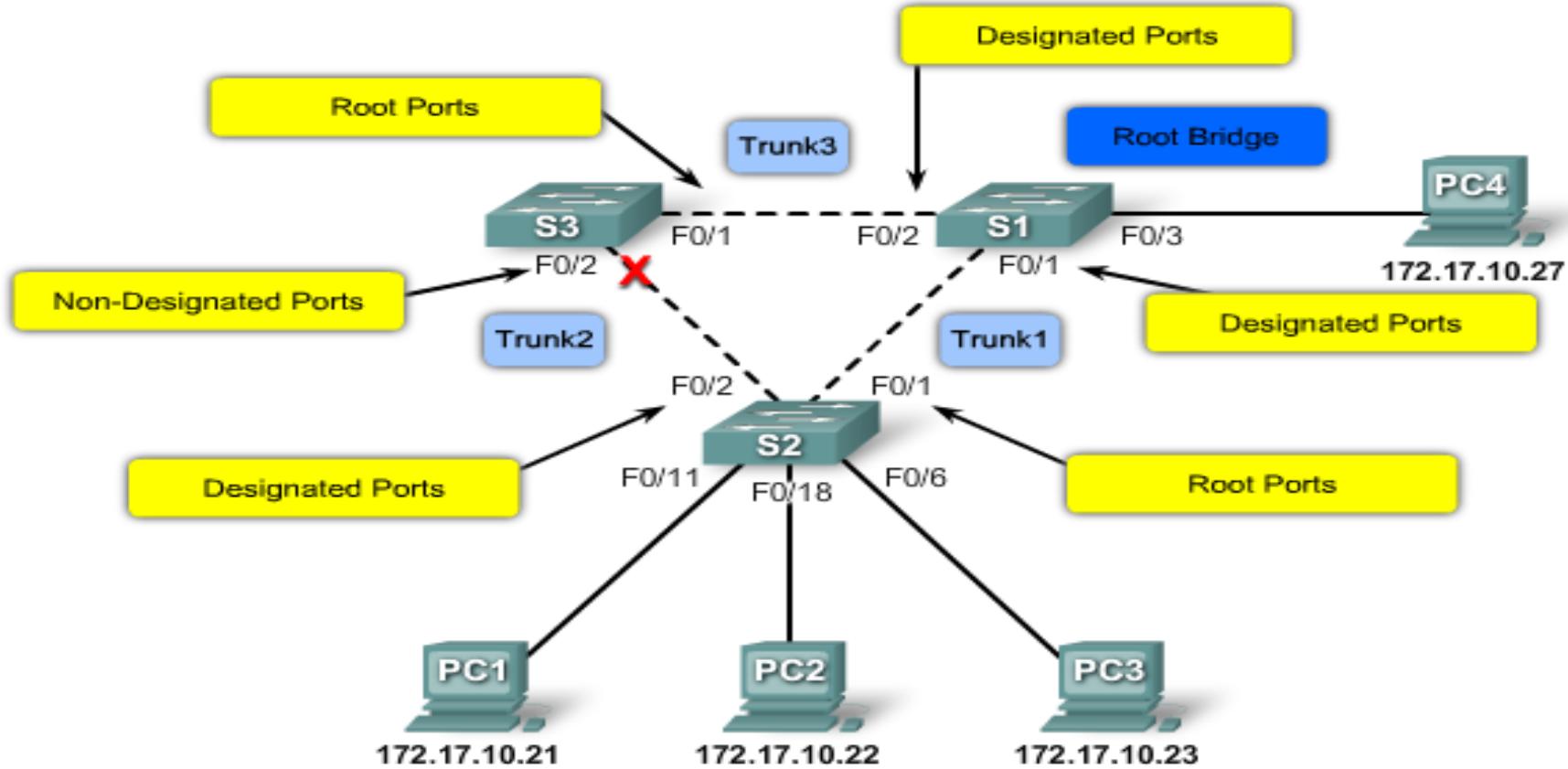


- STP ensures that there is only one logical path between all destinations on the network by intentionally blocking redundant paths that could cause a loop.
- A port is considered blocked when network traffic is prevented from entering or leaving that port.

Spanning Tree Algorithm

- STP uses the Spanning Tree Algorithm (STA) to determine which switch ports on a network need to be configured for blocking to prevent loops from occurring. The STA designates a single switch as the **root bridge** and uses it as the reference point for all path calculations
- All switches participating in STP exchange **BPDU** frames to determine which switch has the lowest bridge ID (BID) on the network. The switch with the lowest BID automatically becomes the root bridge for the STA calculations..

STP Algorithm



Spanning Tree Protocol (STP)

- STP blocks some ports so that only one active path exists between any pair of LAN segments
- STP causes each interface on a bridging device to settle into a **blocking state** or a **forwarding state**
- Blocking means that the interface cannot forward or receive data frames, but it can send and receive bridge protocol data units (BPDUs)
- Forwarding means that the interface can both send and receive data frames as well as BPDUs

Pros & Cons.

Advantages

- Frames do not loop infinitely, which makes the LAN usable

• •

Disadvantages

- Network does not actively take advantage of some of the redundant links because they are blocked
- Some users' traffic travels a seemingly longer path through the network because a shorter physical path is blocked.

Bridge Protocol Data Unit (BPDU)

- STP uses a special frame called BPDU to exchange information about BridgeIDs and root path costs
- Each BPDU contains
 - Bridge ID of the source
 - Accumulated root path cost
 - Source bridge
 - Other information
- When a BPDU is initiated from a bridge the accumulated root path cost is 0

- Exchange of BPDU messages results in the following:
 - The election of a unique root switch for the stable spanning-tree network topology.
 - The election of a designated switch for every switched LAN segment.
 - The removal of loops in the switched network by placing redundant switch ports in a blocking state.

How STP works

- I. Elects a root bridge
- II. Elects a root port for Each non root bridge
- III. Elects a designated bridge for LAN segment
- IV. Elects a designated port for each designated bridge
- ⋮
- ⋮
- ⋮
- ⋮
- ⋮

I. Elects a root bridge

- An identification number is given to each bridge
- Assigned manually or by the manufacturer
- Sometimes Bridge's MAC address is considered as the bridge ID
- **The bridge with the least BridgeID is selected as root bridge**
- BridgeID → 8 Bytes
 - MAC Address + Bridge priority value

I. Elects a root bridge cont.

- The election process begins with every switch sending out BPDU messages with a Root Bridge ID equal to its own Bridge ID
- Received BPDU messages are analyzed for a lower Root Bridge ID value
 - If the BPDU message has a Root Bridge ID of the lower value than the switch's own Root Bridge ID, it replaces its own Root Bridge ID with the Root Bridge ID announced in the BPDU
 - The switch is then nominated the new Root Bridge ID in its own BPDU messages
- Once the process has converged, all switches will agree on the Root Bridge until a new switch is added

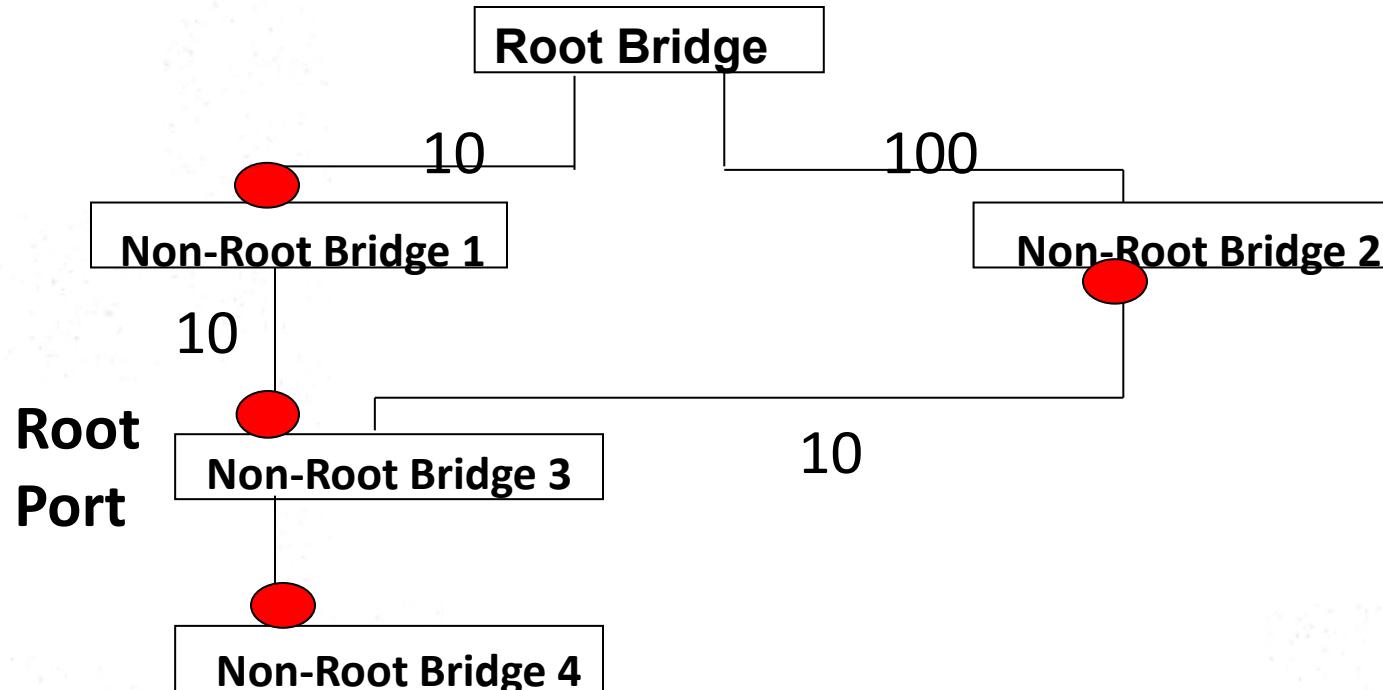
II. Elect Root Ports

- A bridge's **Root Port** is the port closest to the Root Bridge.
- Bridges use the **cost** to determine closeness.
- **Every non-Root Bridge will select one Root Port!**
- Specifically, bridges track the **Root Path Cost**, the cumulative cost of all links to the Root Bridge.
- •
- •
- •

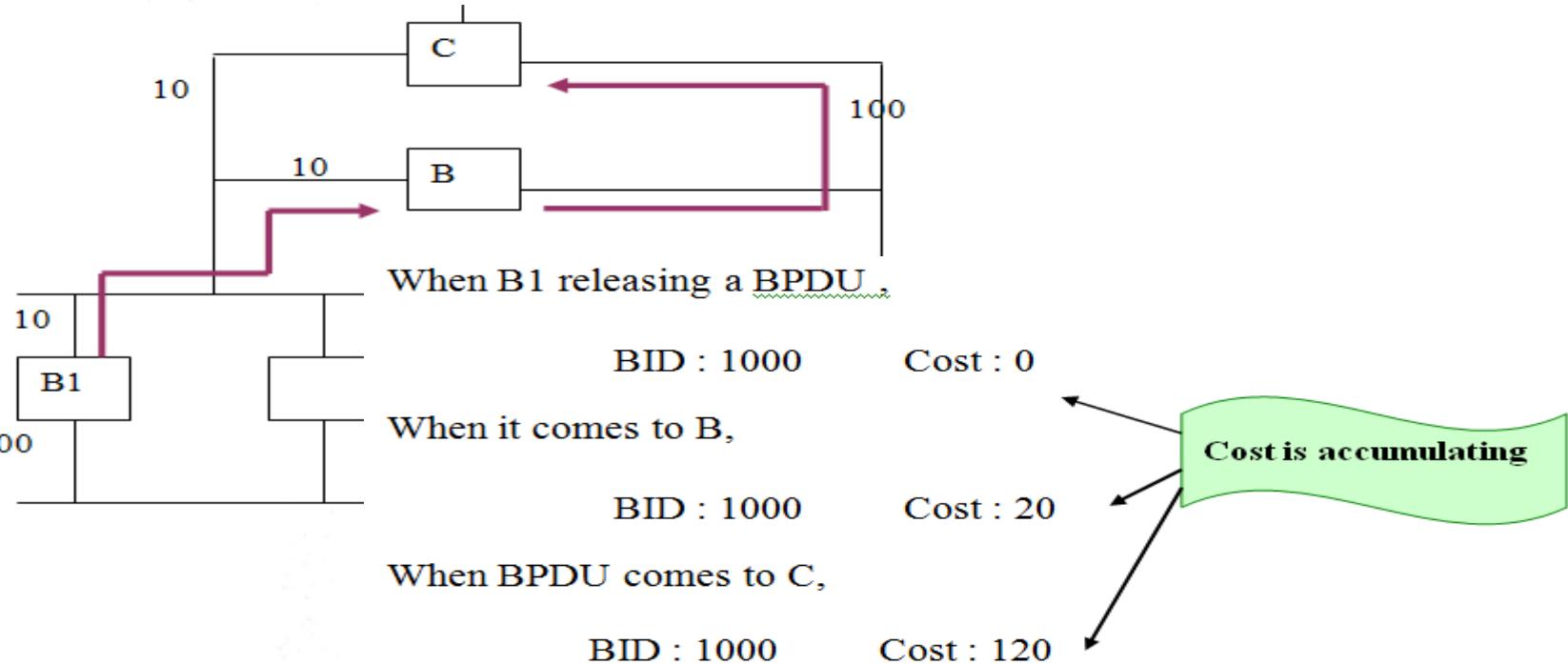
II. Elects a root port for Each non root bridge

- **The port which has the least cost path to the root bridge** is considered as the root port of that particular non root bridge
- Each path is given a “cost”
- Cost is inversely proportionate to bandwidth
 - 10 mbps – 100
 - 100 mbps – 10
 - 1Gbps – 2
- Root Bridge does not have a root port

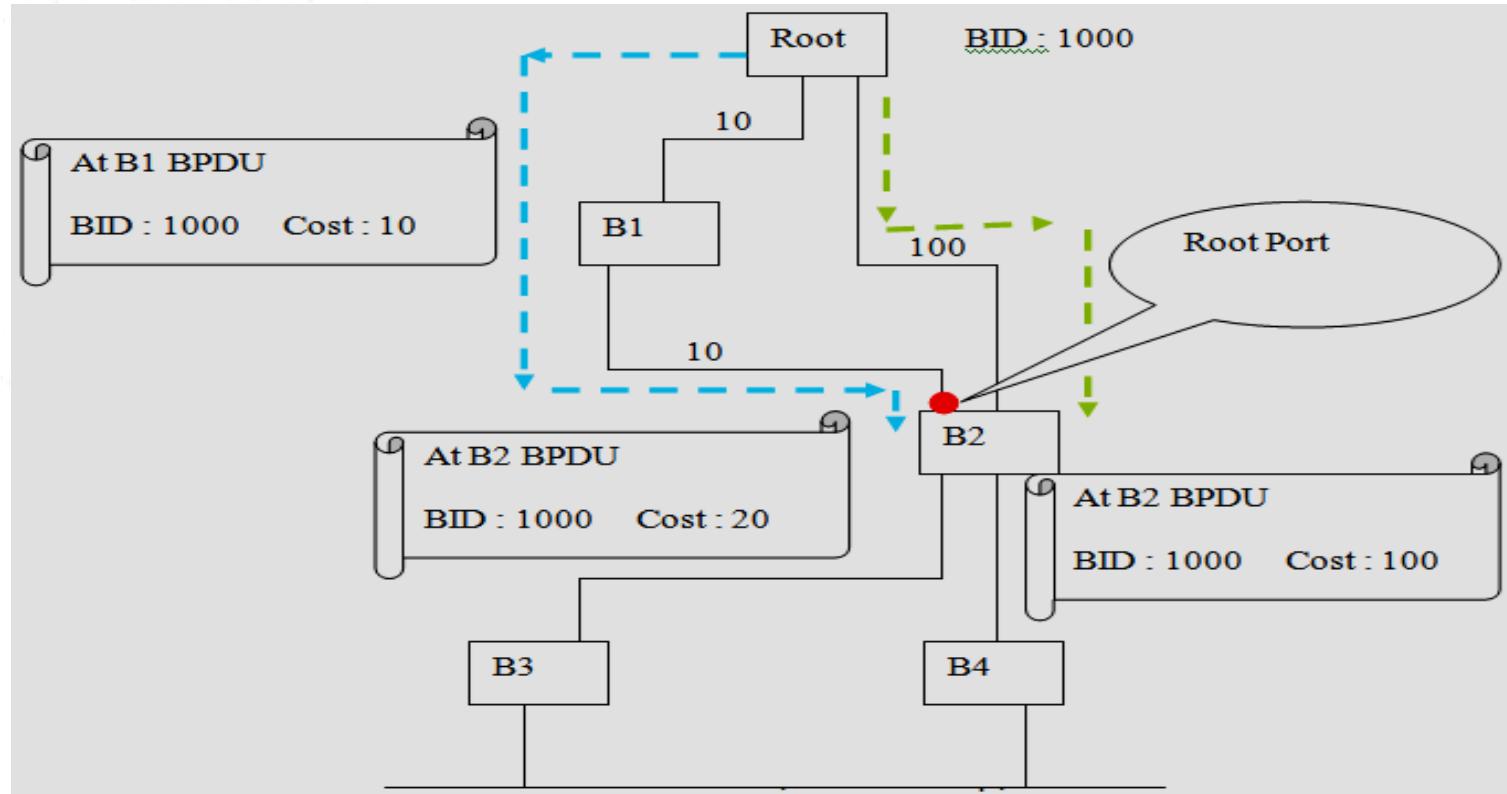
II. Elects a root port for Each non root bridge cont.



- The Root port of a bridge is the port who's BPDU has the minimum accumulated root cost



II. Elects a root port for Each non root bridge cont.



III. Elect Designated Bridge for LAN segment

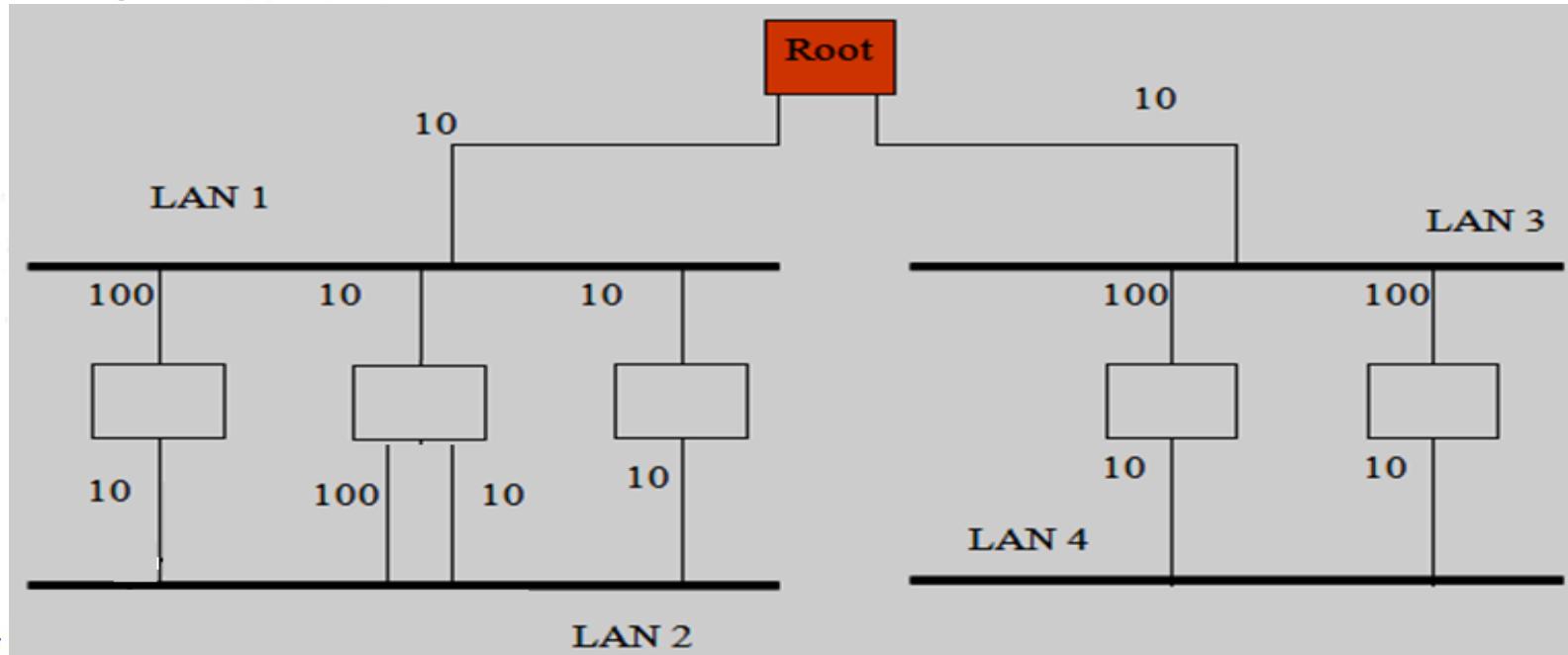
- A Designated Port is elected for every segment. The Designated Port is the only port that sends and receives traffic to/from that segment to the Root Bridge, the best port towards the root bridge.
- Each segment in a bridged network has one Designated Port, chosen based on cumulative Root Path Cost to the Root Bridge.

III. Elects a designated bridge for LAN segment

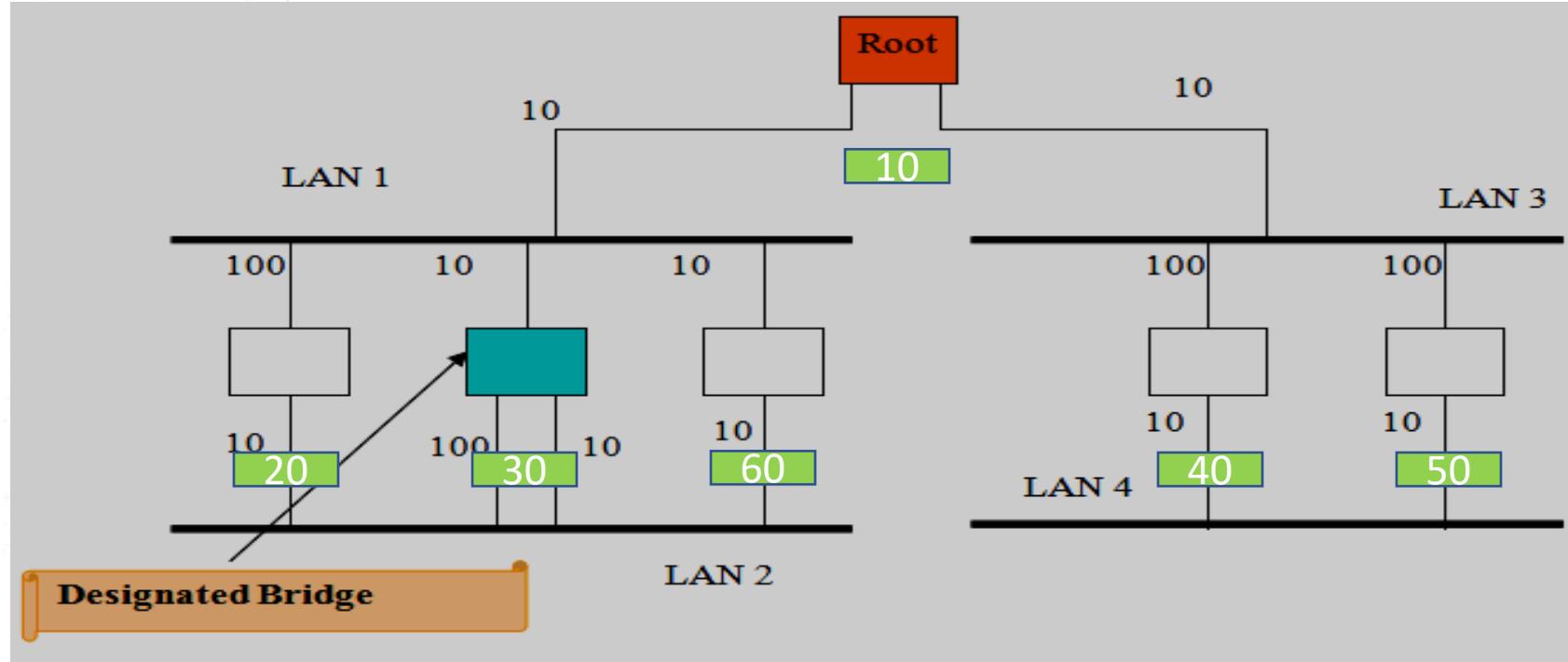
- Designated Bridge is the bridge with the least cost to the root in each LAN segment
- If two LAN segments have several paths with same cost to the Root Bridge
 - Then select the low BridgeID Bridge as the Designated Bridge
- Designated ports are open and others are blocked

III. Elects a designated bridge for LAN segment

- Designated Bridge is the bridge with the least cost to the root in each LAN segment

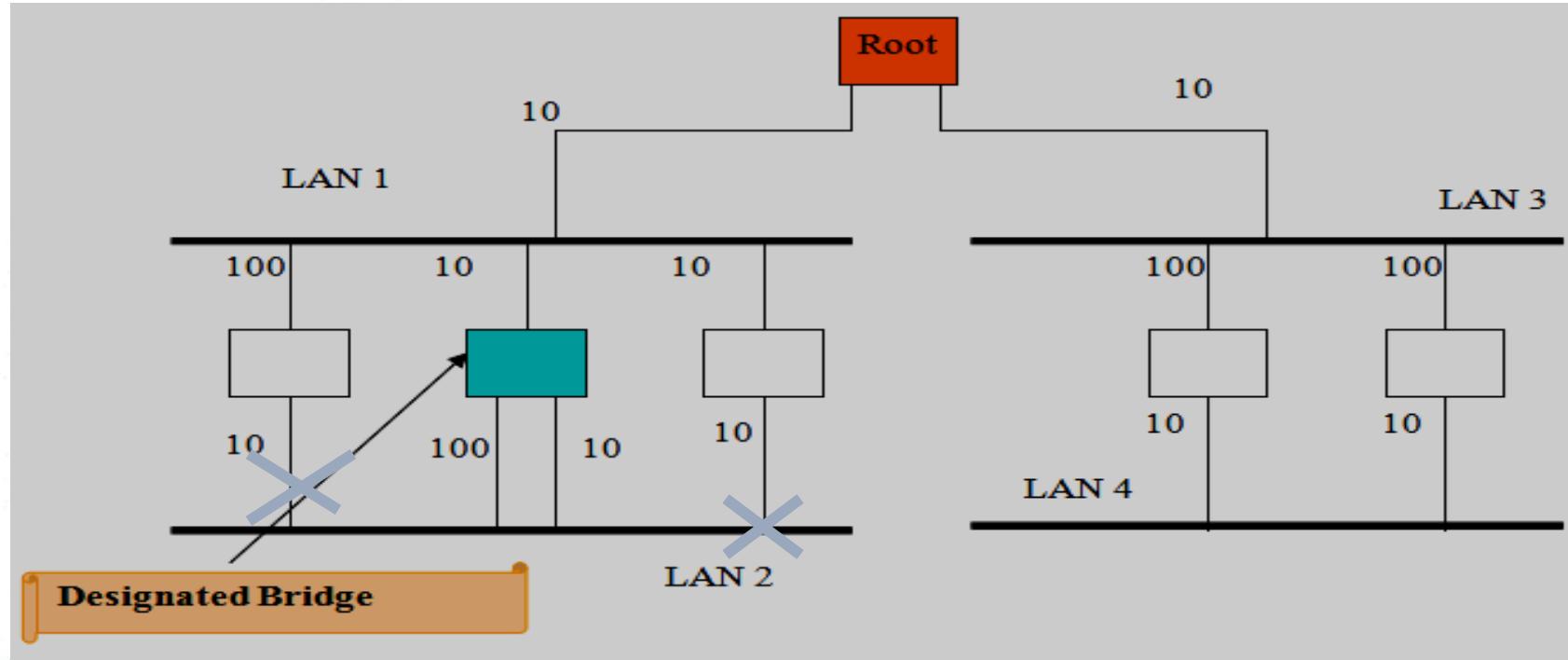


III. Elects a designated bridge for LAN segment cont.



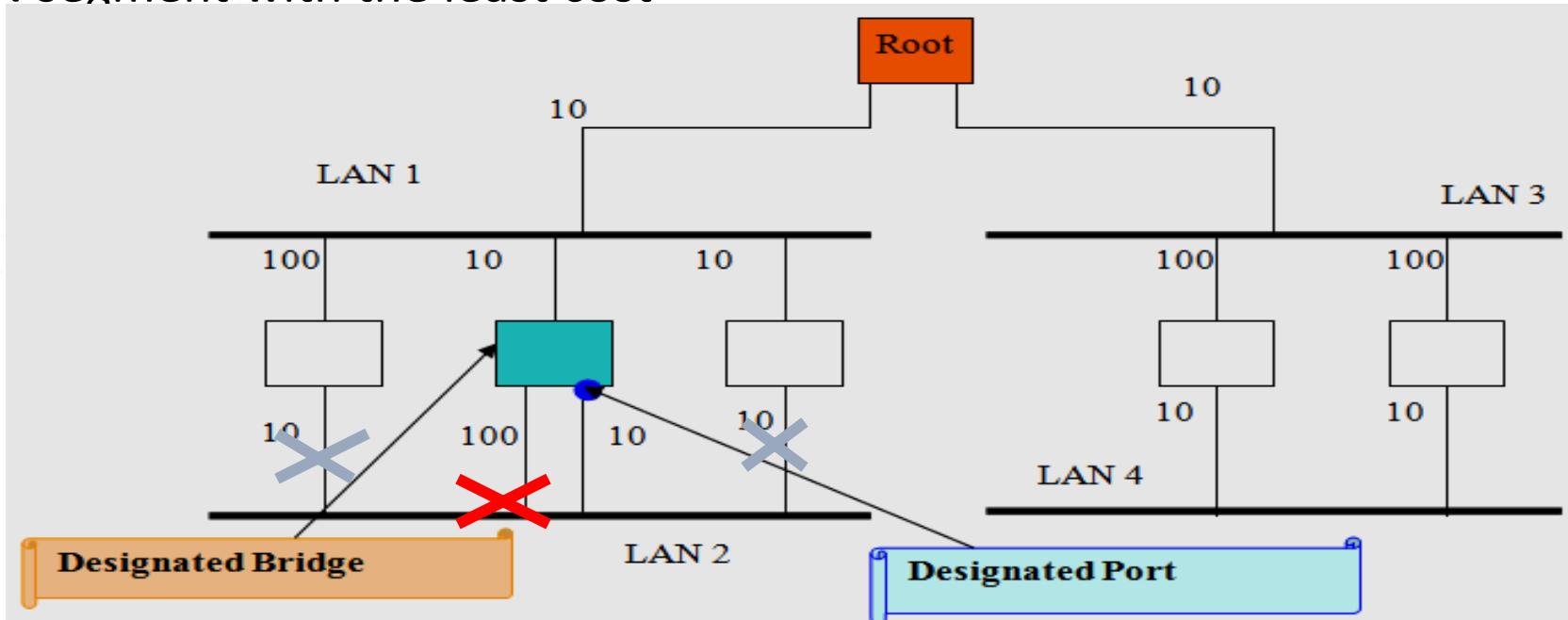
III. Elects a designated bridge for LAN segment cont.

- Path through the designated bridge is open and other paths are blocked



IV. Elects a designated port for designated bridge of LAN segment

- Designated Port is the Port in the designated bridge connected to the LAN segment with the least cost



- Each port on a switch using Spanning-Tree Protocol exists in one of the following five states:
 - Blocking
 - Listening
 - Learning
 - Forwarding
 - Disabled

- In the blocking state
 - ports can only receive BPDUs. Data frames are discarded and no addresses can be learned. It may take up to 20 seconds to change from this state.
- In the listening state
 - Ports transition from the blocking state to the listening state. The listening period is called the forward delay and lasts for 15 seconds. In the listening state, data is not forwarded and MAC addresses are not learned. BPDUs are still processed.
- In the learning state
 - Data is not forwarded, but MAC addresses are learned from traffic that is received. The learning state lasts for 15 seconds and is also called the forward delay. BPDUs are still processed.

- In the forwarding state.
 - User data is forwarded and MAC addresses continue to be learned. BPDUs are still processed.
 - A port can be in a disabled state. This disabled state can occur when an administrator shuts down the port or the port fails.
- ⋮ ⋮

Processes	Blocking	Listening	Learning	Forwarding	Disable
Receives and process BPDUs	✓	✓ ¹	✓	✓	✗
Forward data frames received on interface	✗	✗	✗	✓	✗
Forward data frames switched from another interface	✗	✗	✗	✓	✗
Learn MAC addresses	✗	✗	✓	✓	✗

¹Return to blocking if not lowest cost path to root bridge

Example

